

REINERSCT[®]

Bedienungsanleitung

cyberJack[®]
RFID standard



Inhaltsverzeichnis

1 / Vorwort	1
2 / Gerätebeschreibung	2
3 / cyberJack RFID standard	3
3.1 Chipkartenleser auspacken und aufstellen	3
3.2 Beschreibung der Bedienelemente	4
4 / Installation der Hardware am PC	6
4.1 Treiberinstallation unter Windows	6
4.2 Treiberinstallation unter Linux	6
4.3 Treiberinstallation unter Mac	7
5 / Die Funktionen Ihres Chipkartenlesers	10
5.1 Gerätemenü	10
5.2 Gerätemanager	11
5.3 Die Funktion sichere PIN-Eingabe	15
5.4 Revisionsanzeige	17
5.5 Ausschalten des RFID-Feldes	19
5.6 Integration des cyberJack-Chipkartenlesers in Anwendungen	20
6 / TAN-Generierung	21
6.1 Manuelle TAN-Generierung	21
6.2 Manuelle TAN-Generierung mit ATC	21
6.3 TAN-Generierung mit chipTAN USB	21
7 / Sicherheitshinweise	23
8 / Support	24
9 / Technische Referenzen	25
9.1 LED-Funktionen	25
9.2 Technische Einsatzumgebung	26
9.3 Sicherheitsfunktionen	26
Index	29

1 / Vorwort

Liebe Kundin, lieber Kunde,

vielen Dank, dass Sie sich für einen RFID-Chipkartenleser aus der cyber**Jack**® **RFID** 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 des cyber**Jack**® **RFID** Chipkartenlesers informieren.

Was ist RFID?

Die Radio-Frequency Identification (RFID) Technologie erlaubt eine kontaktlose Kommunikation zwischen einer Chipkarte und einem Lesegerät. Immer mehr Systeme unterstützen diese Funktechnik. So zum Beispiel: kontaktloses Bezahlen mit Geld- oder Kreditkarte, Zeiterfassung, Zutrittskontrolle, Tieridentifikation, Waren- und Bestandsmanagement. Neben Mitarbeiterausweisen und dem elektronischen Reisepass kommuniziert auch der neue elektronische Personalausweis via RFID mit dem Lesegerät.

Diese zeitgemäße Technologie vereinfacht die Handhabung von Chipkarten und ermöglicht die Nutzung in vielen neuen Anwendungen.

Der Personalausweis

Neben der hoheitlichen Ausweisfunktion dient der Personalausweis auch als Ausweis im Internet. Der so genannte elektronische Identitätsnachweis (eID) erhöht die Sicherheit und den Komfort bei der Authentisierung im Internet wesentlich. Im RFID-Chip sind die notwendigen Personendaten des Ausweisinhabers gespeichert, um sich damit zum Beispiel beim Online-Shopping oder bei einem Besuch im Online-Rathaus elektronisch ausweisen zu können. Selbstverständlich können nur Daten ausgelesen werden, die der Ausweisinhaber mittels PIN-Eingabe freigibt.

Viel Erfolg mit Ihrem neuen Gerät wünscht Ihnen

REINER SCT
Reiner Kartengeräte GmbH & Co. KG
Baumannstraße 18
78120 Furtwangen
Germany

www.reiner-sct.com

V1.30 14.08.2018

2 / Gerätebeschreibung

Der cyber**Jack**® **RFID standard** wurde primär für die Nutzung des elektronischen Identitätsnachweises mit dem neuen Personalausweis entworfen, bei dem der nPA als Ausweis im Internet verwendet werden kann.

Der RFID-Chipkartenleser baut nach der PIN-Eingabe an der PC-Tastatur eine gesicherte Verbindung zwischen der Webanwendung und dem nPA auf. Berechtigte eBusiness- und eGovernment-Diensteanbieter dürfen so freigegebene Personendaten, die auf dem nPA gespeichert sind, zur Identifikation und Authentifikation auslesen.

Ein typischer Anwendungsfall hierfür ist z.B. die Adresseingabe und Identitätsverifikation mittels nPA gegenüber einem Internetshop, um dort ein Kundenkonto einzurichten und einzukaufen. Neben den Anwendungen des nPA unterstützt der Chipkartenleser auch alle weiteren RFID-Anwendungen, wie z.B. das eTicketing mit RFID-Karten.

Der cyber**Jack**® **RFID standard** eignet sich ebenfalls für die Nutzung von Anwendungen der elektronischen Signatur gemäß Signaturgesetz und Signaturverordnung für kontaktbehaftete Chipkarten. Anwendungen der elektronischen Signatur sind z.B. die fortgeschrittene elektronische Signatur (FES) oder die qualifizierte elektronische Signatur (QES).

Selbstverständlich hat der cyber**Jack**® **RFID standard** die SECODER-Zulassung. Der SECODER-Standard wurde von der deutschen Kreditwirtschaft spezifiziert. Ziel war es, ein einfaches Verfahren zur definieren, damit Onlinetransaktionen durch eine Datenvisualisierung im Display des Chipkartenlesers noch besser abgesichert werden können.

Für die elektronische Signatur mit einer kontaktlosen Chipkarte (z.B. nPA-QES) kann dieser Chipkartenlesertyp nicht verwendet werden.



cyberJack® RFID standard

Neben dem cyber**Jack**® **RFID standard** sind noch zwei weitere RFID-Chipkartenleser der nPa-Chipkartenleserkategorie basis und komfort lieferbar. Weitere Informationen unter www.reiner-sct.com.

3 / cyberJack RFID standard

3.1 Chipkartenleser auspacken und aufstellen

Auspacken

In der Verpackung sind enthalten¹⁾:

- cyberJack® RFID standard
- Kurzanleitung zur Geräteinstallation

1)

Je nach Variante und Bezugsquelle befinden sich gegebenenfalls noch weitere Komponenten in der Verpackung.

Aufstellen cyberJack® RFID standard

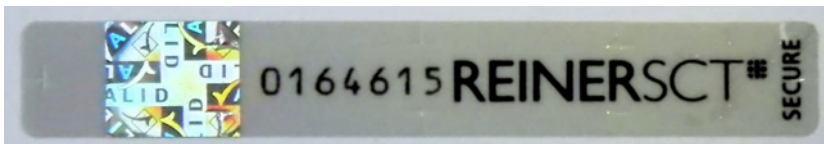
Bitte entnehmen Sie Gerät und Standfuß aus der Verpackung und schieben Sie den Standfuß in die Führung auf der Rückseite des Geräts komplett ein, so dass der Chipkartenleser einen sicheren Stand hat. Das Anschluss-Kabel können Sie in die am Standfuß angebrachte Kabelführung einlegen, so dass der Kabelabgang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

Bitte beachten Sie, dass metallische oder metallisierte, leitende oder wasserhaltige Materialien unterhalb oder in näherer Umgebung des Chipkartenlesers aus physikalischen Gründen zu einer Beeinflussung der Chipkartenlesereigenschaften führen können. Vermeiden Sie deshalb das Gerät in der Nähe solcher Materialien zu betreiben.

Dieses Gerät ist für die Nutzung in einer Büro- oder Heimumgebung bestimmt.

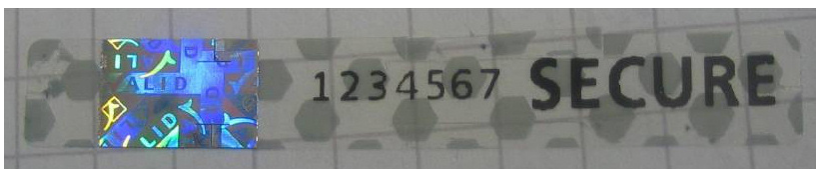
Sicherheitshinweis Gerätesiegel

Achten Sie darauf, dass das aufgebrachte Siegel unbeschädigt ist und der Abbildung auf dem Foto entspricht.



Unbeschädigtes Siegel

Die Merkmale zur Fälschungssicherheit – Hologramm, Firmenlogo und Nummerierung - müssen, wie in der Abbildung, vorhanden sein. Die Hintergrundfarbe des Siegels muss einheitlich sein. Bei einem abgelösten Siegel ist ein Schachbrettmuster erkennbar oder/und das Siegel ist beschädigt (Siehe Abbildungen abgelöster Siegel).



Abgelöstes Siegel mit Schachbrettmuster



Beschädigtes Siegel mit Schachbrettmuster

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® RFID standard, rechte Seite

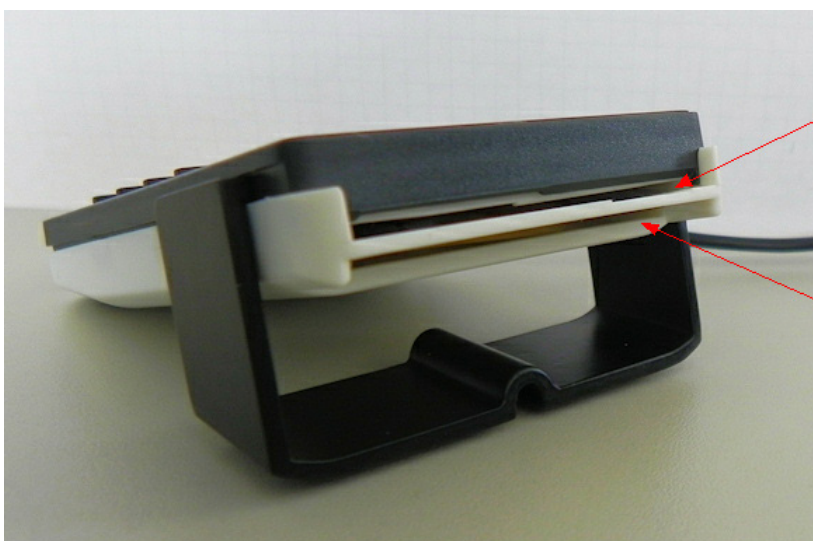


Sicherheitsversiegelung
cyberJack® RFID standard, linke Seite

3.2 Beschreibung der Bedienelemente

Aufnahme für Chipkarten

Mit dem cyberJack® RFID standard können sowohl kontaktbehaftete als auch kontaktlose Chipkarten ausgelesen werden. Dazu sind zwei separate Karteneinschübe vorgesehen. Der vordere Einschub ist für die kontaktbehafteten Chipkarten und der hintere Einschub ist für die kontaktlosen Chipkarten, wie den Personalausweis, gedacht.



Einschub für
kontaktbehaftete Chipkarten

Einschub für kontaktlose
Chipkarten

Leuchtdioden (LEDs)

Grüne LED Anzeige des Betriebszustandes

Gelbe LED Anzeige sicherer Betrieb, Anzeige Fehlerzustand

Genauere Informationen zu den LED-Funktionen erhalten Sie im Kapitel [LED-Funktionen](#)^[25].

Display

Der cyber**Jack**[®] **RFID standard** verfügt über ein Display mit zwei Zeilen á 16 Zeichen. Auf dem Display werden Steuertexte für die Eingabe der PIN ausgegeben.

Beschreibung der Bedienelemente

Tastenbezeichnung	Beschriftung	Funktion
C-Taste	C	Vorgang abbrechen oder im Menü zurück
Clear-Taste	CLR	Einzelne Zeichen löschen
Menü-Taste	@	Aufruf des Gerätemenüs
OK-Taste	OK	Bestätigung Ihrer Eingabe / Auswahl
Pfeiltasten	▲ ▼	Navigieren durch das Menü

4 / Installation der Hardware am PC

4.1 Treiberinstallation unter Windows



Dieser RFID-Chipkartenleser wird aktuell von allen von Microsoft offiziell veröffentlichten und vom erweiterten öffentlichen Support eingeschlossenen Windows Betriebssysteme für PC und Server (32 / 64 Bit) unterstützt.



Bitte installieren Sie die Gerätetreiber (cyberJack BaseComponents) unbedingt mit Administrator-Rechten!
-> Rechte Maustaste „Als Administrator ausführen“

Der cyberJack® RFID standard wird an die USB-Schnittstelle Ihres Computers, bzw.an einen USB-Hub angeschlossen.



Die Installation cyberJack® Base Components ist zum Betrieb der cyberJack® RFID standard Chipkartenleser unbedingt erforderlich. Hierin sind die Systemtreiber enthalten. Desweiteren wird der Gerätemanager mit den Funktionen Gerätetest, Treiberupdate und Online-Support installiert. Die cyberJack® BaseComponents benötigen Sie auch, um die Firmware des cyberJack® RFID standard zu aktualisieren. Die cyberJack® BaseComponents finden Sie unter www.reiner-sct.com/treiber

Laden Sie die entsprechende Treiber-Datei herunter und starten Sie das Installationsprogramm **bc_x_x_x.exe** mit einem Doppelklick.



Folgen Sie bei der Installation den jeweiligen Hinweisen des Installationsprogramms. 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.

4.2 Treiberinstallation unter Linux

Zur Installation der Treiber für den cyberJack® RFID standard benötigen Sie eine Internetverbindung. Stecken Sie den Chipkartenleser noch nicht ein!

Die Installation der Treiber für den cyberJack® RFID standard teilt sich grundsätzlich in zwei Schritte auf:

- a) Installation des PCSCD-Treibers und dessen Abhängigkeiten zu installieren

b) Installation des aktuellen Treiber für den cyber**Jack**[®] **RFID standard**

Vorgehensweise:

1. Bitte installieren Sie zuerst den PCSCD-Treiber mit Hilfe der Paketverwaltung Ihrer Distribution.
2. Laden Sie sich danach den aktuellen Treiber passend für Ihre Distribution und Ihren Prozessor unter www.reiner-sct.com/treiber herunter.
3. Führen Sie die Installation dieses Treibers mittels Doppelklick aus.
4. Bitte führen Sie einen Neustart durch.
5. Die Treiberinstallation ist nun abgeschlossen. Sie können nun den cyber**Jack**[®] **RFID standard** in eine USB-Buchse Ihres Computers einstecken und verwenden.

4.3 Treiberinstallation unter Mac



Dieser Chipkartenleser wird aktuell von allen von Apple offiziell veröffentlichten und vom aktuellen öffentlichen Support eingeschlossenen OS X 10.6 Betriebssysteme (32 / 64 Bit) unterstützt.

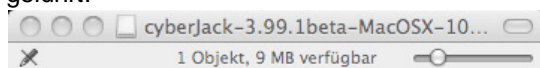
Der cyber**Jack**[®] **RFID standard** wird an die USB-Schnittstelle Ihres Computers, bzw. an einen USB-Hub angeschlossen. **Bitte lesen Sie vor dem Einstecken des RFID-Chipkartenlesers unbedingt die nachfolgenden Informationen!**



Für den cyber**Jack**[®] **RFID standard** ist eine Treiberinstallation notwendig.

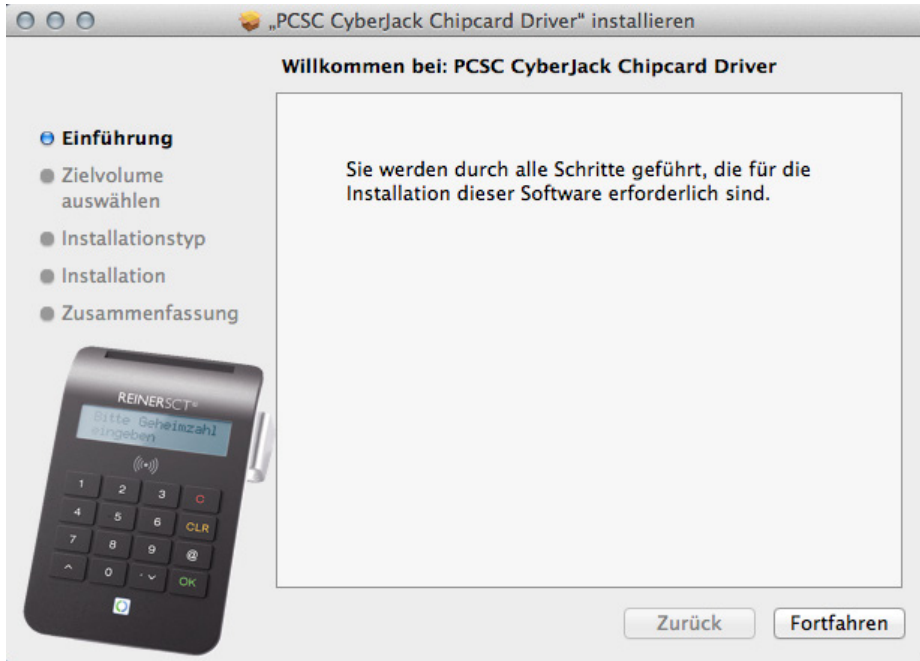
Zur Installation der Treiber für den cyber**Jack**[®] **RFID standard** benötigen Sie eine Internetverbindung. Stecken Sie den Chipkartenleser noch nicht ein!

Laden Sie sich den Treiber für den cyber**Jack**[®] **RFID standard** unter www.reiner-sct.com/treiber herunter und führen Sie die Treiberdatei mittels Doppelklick aus. Sie werden nun durch die Installation geführt.



cyberJack-3.99.1beta.pkg

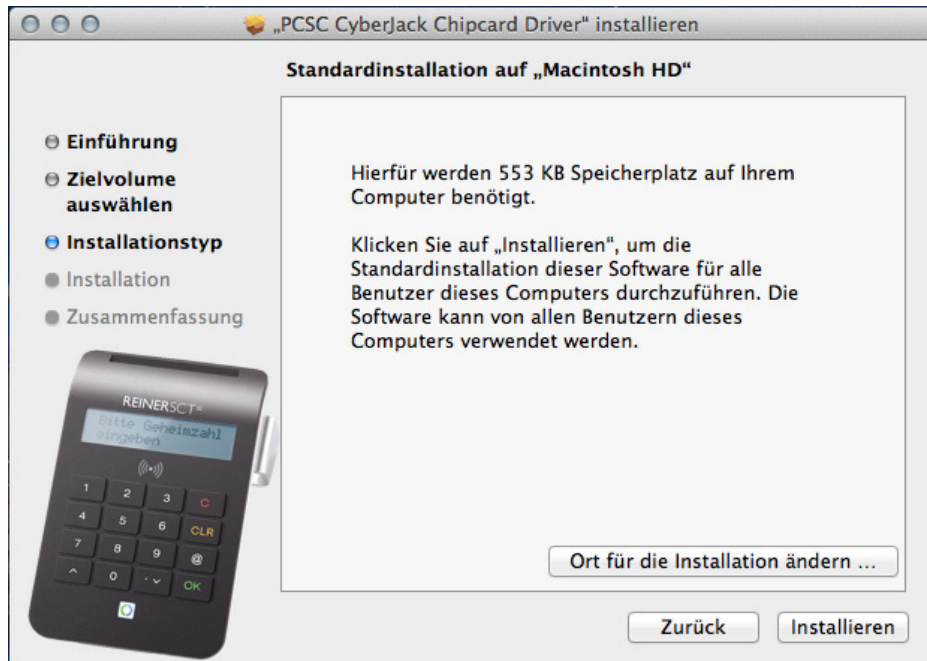
Klicken Sie auf den Button "Fortfahren" um die Installation des Treibers zu starten.



Die Installation erfolgt im Standardverzeichnis. Klicken Sie dazu auf den Button "Fortfahren".



Klicken Sie auf den Button "Installieren".



Erlauben Sie nun durch Eingabe Ihres Benutzernamen und Ihres Kennworts die Treiberinstallation. Bitte beachten Sie, dass der Benutzer die Rechte hierfür besitzen muss.

Die Treiber-Installation ist nun abgeschlossen.



Sie können nun den cyber**Jack**[®] **RFID standard** in eine USB-Buchse Ihres Computers einstecken und verwenden.

Funktionstest: Legen Sie die login**Card** oder den neuen elektronischen Personalausweis auf den angeschlossenen Chipkartenleser. Bei korrekter Installation leuchtet die grüne Leuchtdiode (LED) am Chipkartenleser.

Hinweis: Zur Nutzung des cyber**Jack**[®] **RFID standard** benötigen Sie ein Anwendungsprogramm und eine RFID-Chipkarte bzw. den elektronischen Personalausweis.

5 / Die Funktionen Ihres Chipkartenlesers

5.1 Gerätemenü

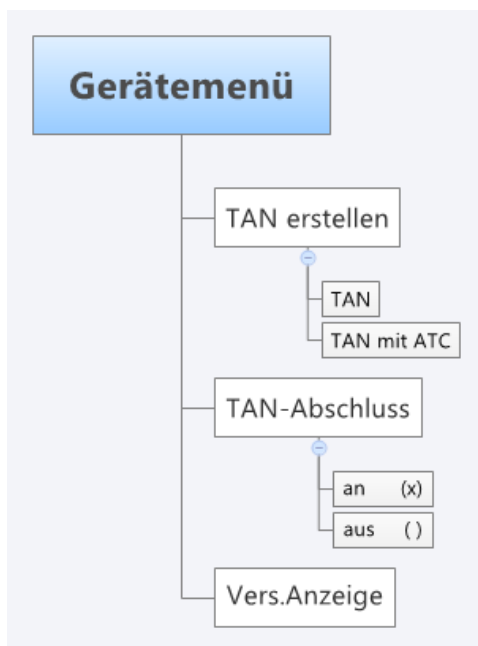
Im Gerätemenü können Sie verschiedenste Einstellungen vornehmen und Anwendungen starten. Gehen Sie bitte dabei folgendermaßen vor.

Um ins Gerätemenü zu gelangen, drücken Sie bei eingestecktem Gerät die **@-Taste**. Im Display wird folgendes angezeigt.



Mit den Pfeiltasten können Sie durch das Menü navigieren. Mit der **OK-Taste** gelangen Sie in das jeweilige Untermenü. Mit der **C-Taste** verlassen Sie das Untermenü.

Das Gerätemenü des cyber**Jack**® RFID standard hat folgenden Aufbau, der im Folgenden erklärt wird.



TAN erstellen

TAN: Hier können Sie eine TAN manuell generieren. Siehe Kapitel [Manuelle TAN-Generierung](#)^[21].

TAN mit ATC: Hier können Sie die manuelle TAN-Generierung mit Anzeige des ATCs starten. Siehe Kapitel [Manuelle TAN-Generierung mit ATC](#)^[21]

TAN-Abschluss

Mit dieser Einstellung können Sie die Übertragung der generierten TAN beschleunigen.

TAN-Abschluss an (x) - Default-Einstellung -> normale TAN-Übertragung

TAN-Abschluss aus (x) -> Beschleunigte TAN-Übertragung

Weiterführende Informationen finden Sie im Kapitel [TAN-Generierung mit chipTAN USB](#)^[21]

Vers.Anzeige: Es werden Ihnen nacheinander die Versionen und Funktionen des cyber**Jack**® RFID standard am Display angezeigt

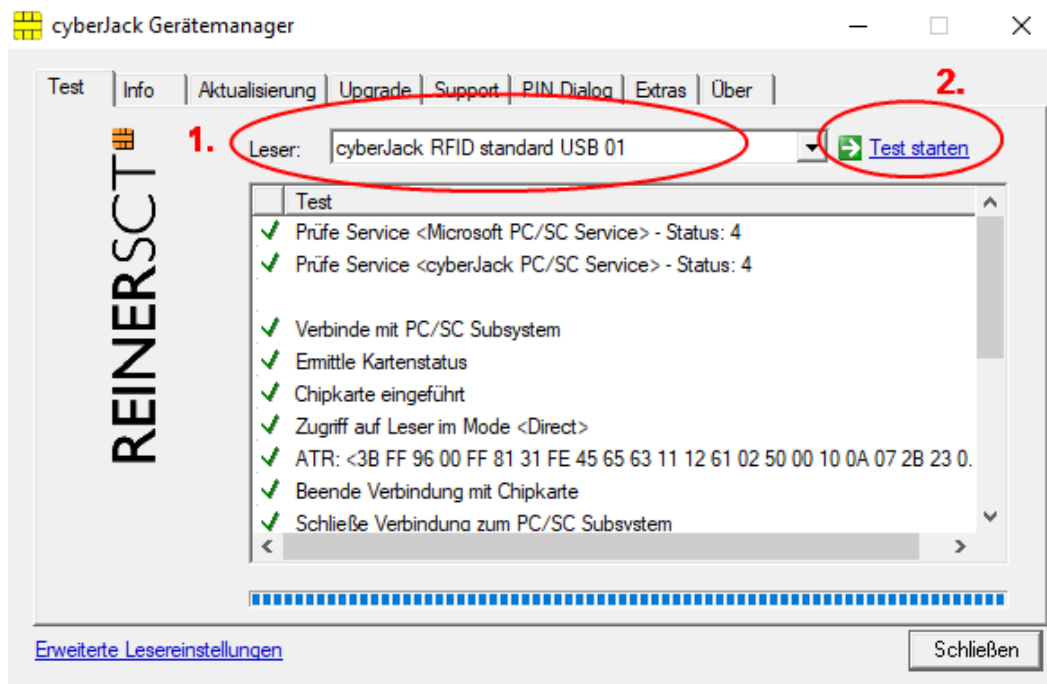
5.2 Gerätemanager

! Der cyberJack Gerätemanager steht momentan nur für das Betriebssystem Windows zur Verfügung.

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 cyberJack® bieten.

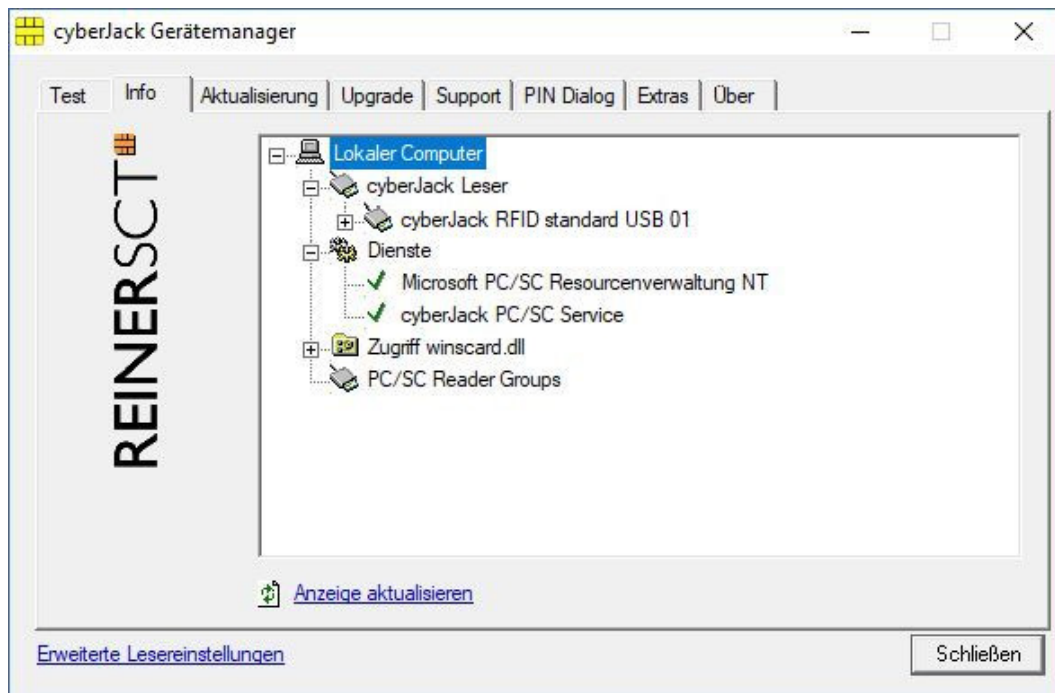
Registerkarte Test

Wenn Sie mehrere Chipkartenleser angeschlossen haben, können Sie unter (1) den entsprechenden Chipkartenleser 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 cyberJack® 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 cyberJack 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.



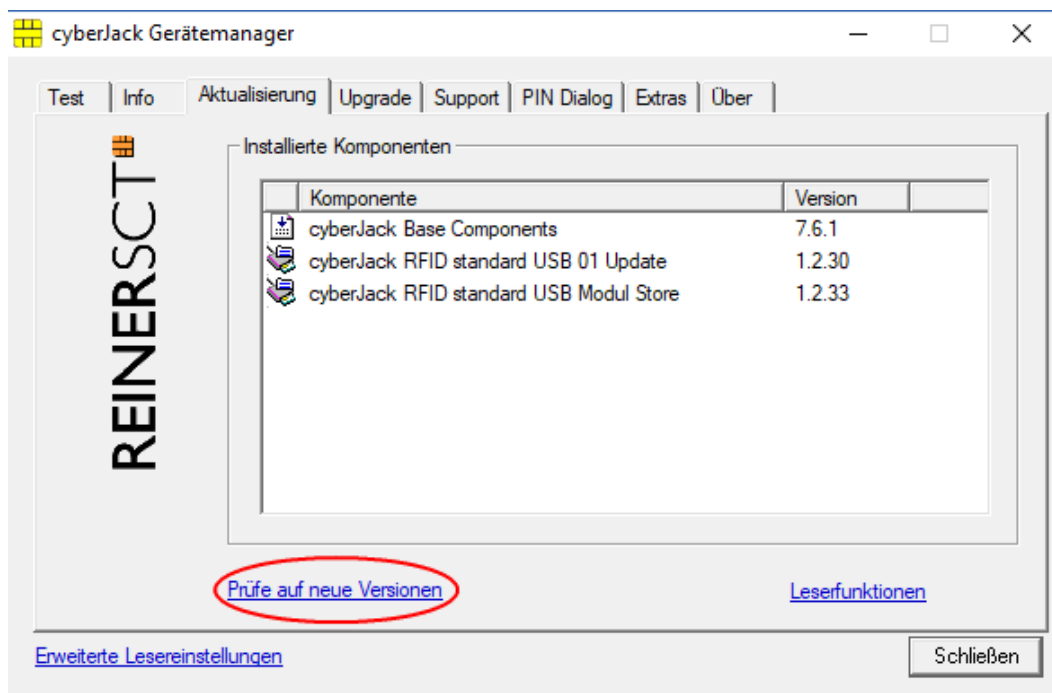
Registerkarte Info

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 sowie Firmware für den cyberJack® RFID standard 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.

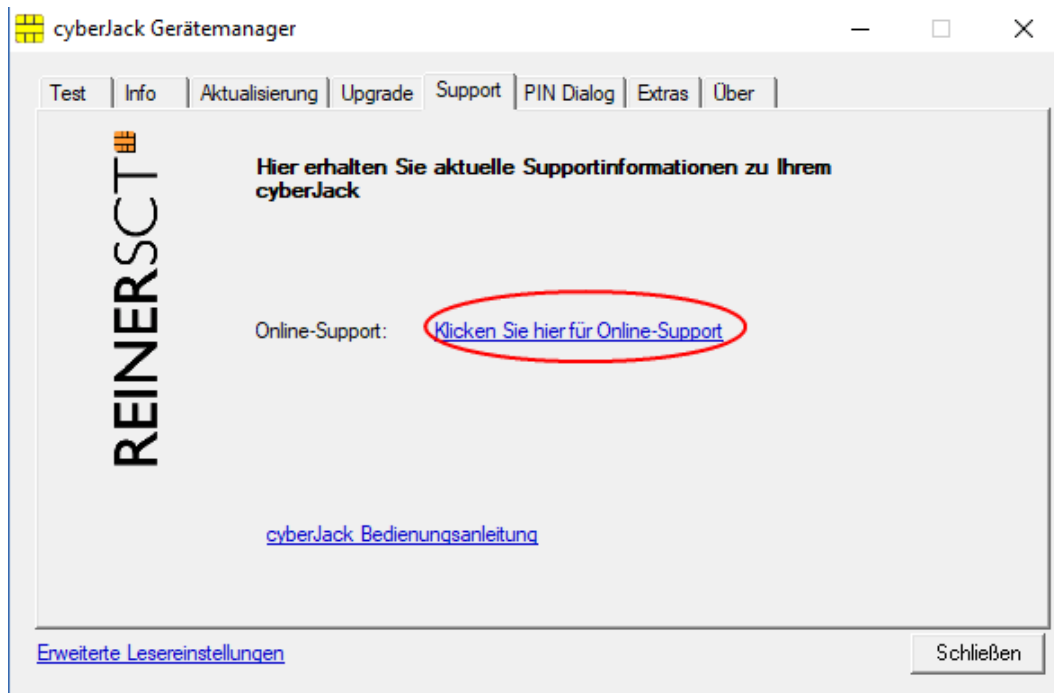


Danach können Sie in der Modulverwaltung Ihre vorhandenen Module und die Firmware des Chipkartenleser aktualisieren.

Weitere Informationen hierzu finden Sie auch im Kapitel Modulverwaltung.

Registerkarte Support

Über Support haben Sie die Möglichkeit, direkt mit dem REINER SCT Support Kontakt aufzunehmen. Hierzu werden Ihre aktuellen cyberJack® 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 in Verbindung setzen.

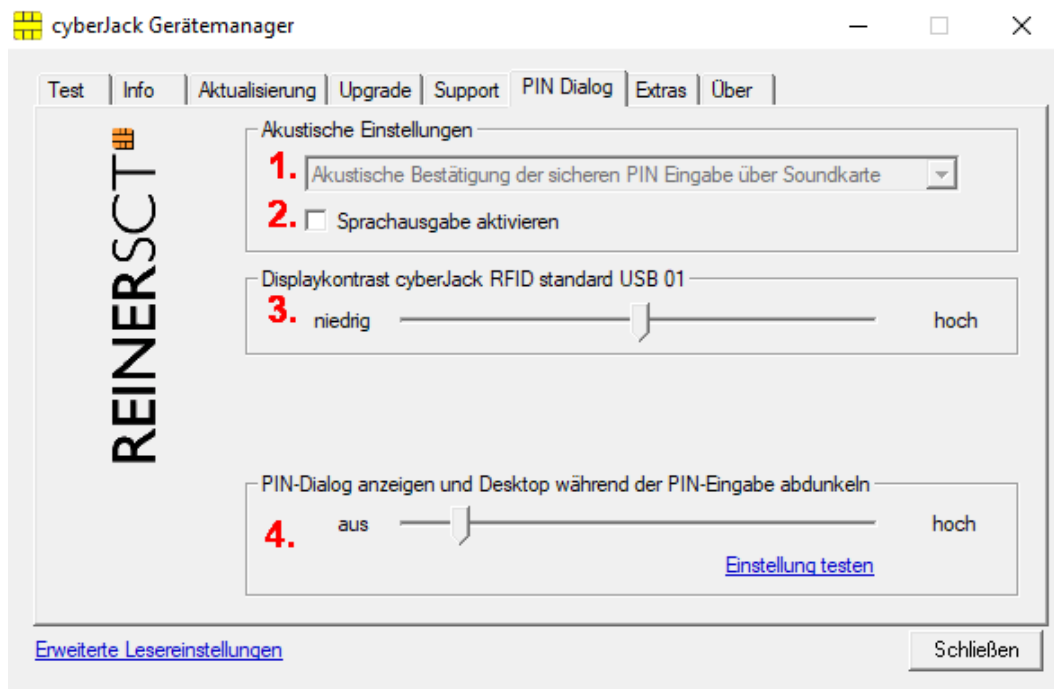


Registerkarte PIN Dialog

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

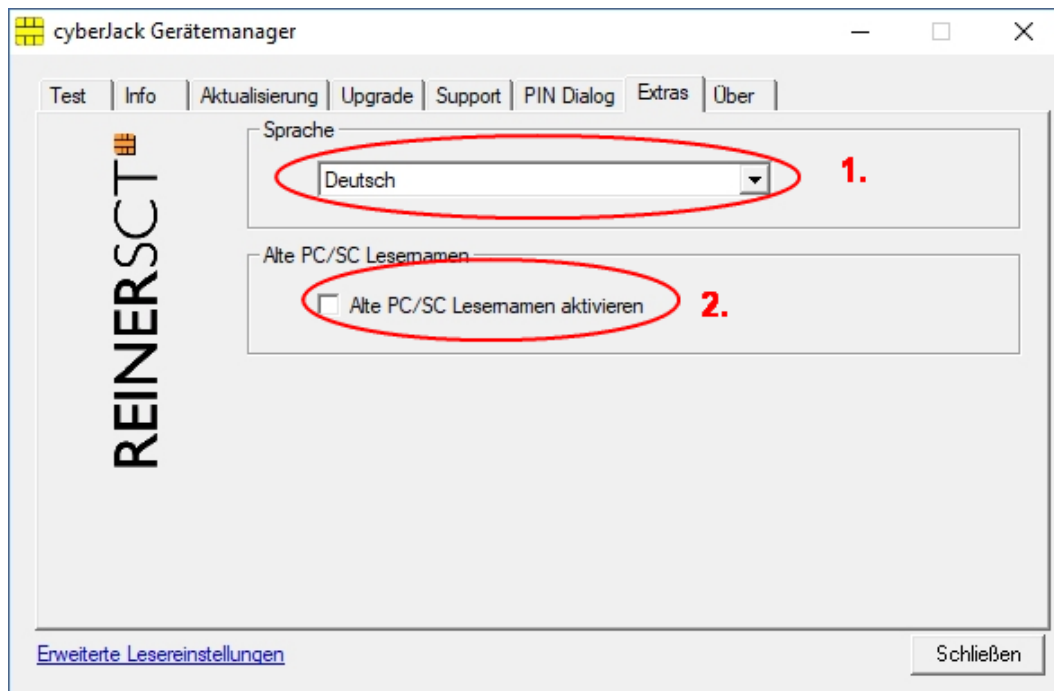
- (1) Hier können Sie auswählen, ob bei der PIN-Eingabe der Tastendruck einen Ton erzeugen soll.
- (2) Setzen Sie hier den Haken und die Aufforderung der PIN ertönt akustisch mit einer freundlichen Stimme.
- (3) Hier können Sie den Displaykontrast des Chipkartenlesers einstellen und somit die optimale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



Registerkarte Extras

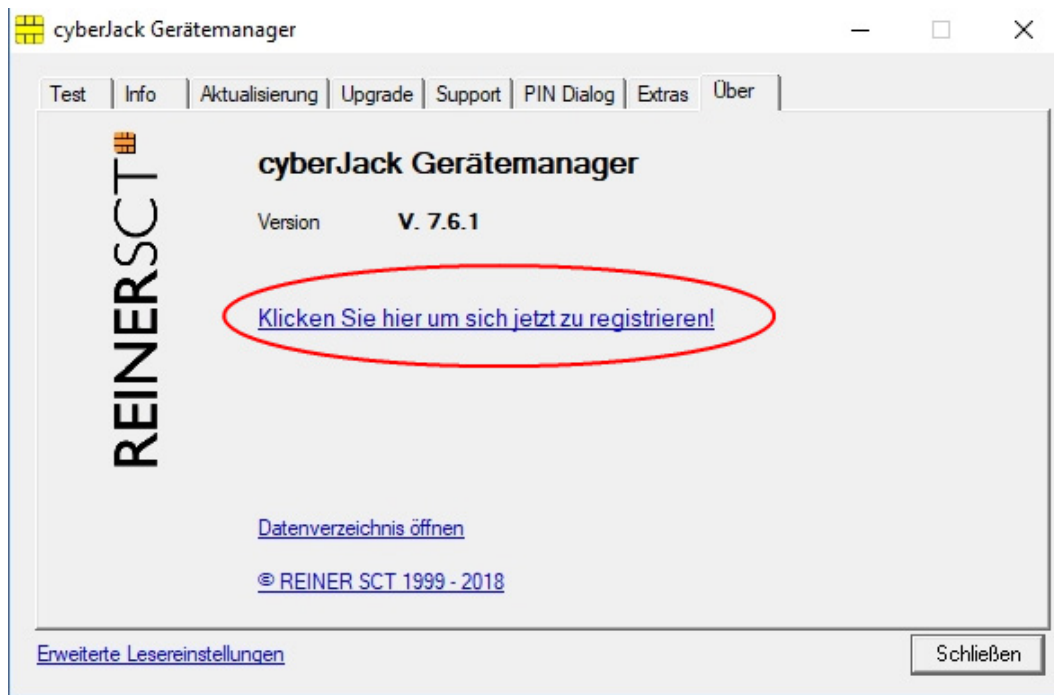
Hier können Sie die Sprache des Gerätemanagers (1) auswählen.

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



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.



5.3 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.

! Die PIN darf nur eingegeben werden, wenn das Vorhandensein eines sicheren Kanals zwischen Tastatur und cyberJack® RFID standard durch die blinkende gelbe LED signalisiert wird. Zusätzlich leuchtet die grüne Duo-LED beim Zugriff auf eine kontaktbehaftete Chipkarte bzw die blaue Duo-LED beim Zugriff auf eine kontaktlose Chipkarte. Bitte achten Sie darauf, dass Sie während der Eingabe der PIN niemand beobachtet und geben Sie die PIN verdeckt ein!

Display- und LED-Anzeige bei der PIN-Eingabe

Wird die sichere PIN-Eingabe bei einer kontaktbehafteten Chipkarte durch die Anwendung gestartet blinkt die gelbe LED und die grüne Duo-LED leuchtet. Wird die PIN-Eingabe bei einer kontaktlosen Chipkarte durch die Anwendung gestartet blinkt die gelbe LED und die blaue Duo-LED leuchtet. Die PIN kann dann innerhalb der vorgegebenen Zeit eingegeben werden. Die PIN kann dann 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. Der PIN-Dialog wird auf dem Display des Chipkartenlesers dargestellt. Die `*`-Zeichen stehen hierbei als Rückmeldung für einen Tastendruck. Die PIN-Ziffern selber verlassen den Chipkartenleser nicht und können aus diesem zu keinem Zeitpunkt ausgelesen werden.

Folgende Displayanzeige erscheint beim Chipkartenleser, wenn eine sichere PIN-Eingabe erforderlich ist.

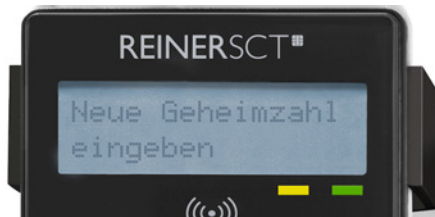


Sicheres Ändern der PIN

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. Folgende Displayanzeigen erscheinen.



1. Aktuelle PIN eingeben



2. Neue Pin eingeben



3. Neue Pin wiederholen



Das sichere Ändern der PIN wird nicht von allen Chipkarten unterstützt. Im Zweifel kontaktieren Sie bitte den Kartenemittenten (Bank, Trust-center etc.). Der cyberJack® RFID standard unterstützt nicht die qualifizierte elektronische Signatur (QES) mit dem neuen Personalausweis (nPA).

Bedeutung der Tasten des Pinpads

0 - 9	Eingabe der PIN-Ziffern
OK	Bestätigung von Transaktionen, z.B. der eingegebenen PIN
C	Abbruch der PIN-Eingabe
CLR	Löschen der PIN
@	Anzeige der Revision (Siehe Kapitel Revisionsanzeige ¹⁷⁾)
Pfeiltaste nach oben	Funktion anwendungsspezifisch
Pfeiltaste nach unten	Funktion anwendungsspezifisch

Sicherheitsfunktion bei der Sicheren PIN-Eingabe

Die Sichere PIN-Eingabe ist eine der wichtigsten Sicherheitsfunktionen eines Chipkartenlesers ab der Sicherheitsklasse 2. Die Sichere PIN-Eingabe für die Qualifizierte Elektronische Signatur ist nur mit einer kontaktbehafteten Chipkarte möglich. Um sicherzustellen, dass die PIN nicht im Chipkartenleser 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 Authentifizierungszwecken 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.

5.4 Revisionsanzeige

Es gibt zwei Möglichkeiten die Revision des Chipkartenlesers anzuzeigen. Beim Einstecken in den USB-Port des Computers bzw. durch Drücken der **@-Taste** am eingesteckten Chipkartenleser werden Ihnen im Display die Version und die eventuell vorhandenen Applikationen angezeigt. Während der Revisionsanzeige blinkt die gelbe LED gleichmäßig bis zur Betriebs-Standardanzeige. Das gleichmäßige Blinken signalisiert, dass der angezeigte Text authentisch ist.

Alle folgenden Displayanzeigen sind beispielhaft und können je nach Versionsstand variieren.

Reihenfolge der Displayanzeigen ohne geladener Applikation



Anzeige der Version

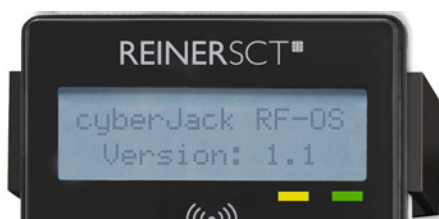


Anzeige der Chipkartenleser-ID



Standardanzeige im Betrieb des Chipkartenlesers

Reihenfolge der Displayanzeige mit geladener Applikation



Anzeige der Version



Anzeige der Chipkartenleser-ID



Anzeige der geladenen Applikation



Anzeige der Revision der geladenen Applikation



Standardanzeige im Betrieb des Chipkartenlesers bei geladener Applikation

5.5 Ausschalten des RFID-Feldes

Sie haben die Möglichkeit das RFID-Feld des Chipkartenlesers zu deaktivieren. Dies kann sinnvoll sein, wenn Sie z.B. nur kontakbehaftete Karten verwenden.

Dazu betätigen Sie die **Pfeiltaste nach oben** des Chipkartenlesers.



Im Display des Chipkartenlesers wird der Status des RFID-Feldes angezeigt.

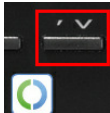


RFID-Feld ist eingeschaltet



RFID-Feld ist ausgeschaltet

Um den Status des Feldes zu ändern, betätigen Sie die **Pfeiltaste nach unten** des Chipkartenlesers.



Änderungsabfrage

Bestätigen Sie die Displayanzeige mit der **OK-Taste**.



Das RFID-Feld ist jetzt ausgeschaltet

5.6 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 Betriebssystem enthalten.

GeldKarte

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

Elektronische Identitätsfunktion mit dem neuen Personalausweis

Nach Installation der Gerätetreiber (siehe Kapitel 4) kann der cyber**Jack**® **RFID standard** durch die AusweisApp für die elektronische Identitätsfunktion genutzt werden. Eine aktuelle Version der AusweisApp finden Sie unter www.ausweisapp.bund.de^[1].

6 / TAN-Generierung

Mit dem cyberJack® RFID standard können Sie auf verschiedenen Wege eine TAN generieren. Dies wird im folgenden erklärt.



Bitte prüfen Sie bei Ihrem Kreditinstitut nach, ob diese Verfahren der TAN-Generierung unterstützt werden.

6.1 Manuelle TAN-Generierung

Mit Hilfe der manuellen TAN-Generierung können Sie TANs durch manuelle Eingabe der Transaktionsdaten generieren. Dazu benötigen Sie einen Start-Code, den Ihnen Ihre Online-Banking-Anwendung bereit stellt.

Um mit dem cyberJack® RFID standard manuell eine TAN zu erzeugen, drücken Sie die **@-Taste** bei eingeführter Chipkarte. Wechseln Sie ins Menü **TAN erstellen**. Bestätigen Sie Ihre Wahl mit der **OK-Taste**. Wechseln Sie nun in das Menü **TAN**. Bestätigen Sie Ihre Wahl mit der **OK-Taste**. Es erscheint „**Start-Code:**“ im Display.



Geben Sie nun den Start-Code mit Hilfe der Ziffern des Tastenfeldes ein, den Ihnen Ihre Online-Banking-Anwendung anzeigt. Bestätigen Sie den Start-Code durch kurzes Drücken der **OK-Taste**. Geben Sie nacheinander Ihre Transaktionsdaten ein und bestätigen Sie diese mit der **OK-Taste**. Zum Schluss wird Ihnen dann die TAN angezeigt, die Sie dann in Ihrer Online-Banking-Anwendung eingeben können.

6.2 Manuelle TAN-Generierung mit ATC

Der ATC (Application Transaction Counter) zeigt die Anzahl der bereits erzeugten TANs an. Dieser Wert ist für eine Synchronisierung Ihrer Chipkarte mit Ihrer Bank oder Sparkasse notwendig. Ihr Online-Banking-System wird Sie ggf. auffordern diese Synchronisierung durchzuführen.

Um den ATC sich anzeigen zu lassen, drücken Sie die **@-Taste** bei eingeführter Chipkarte. Wechseln Sie in das Menü **TAN erstellen**. Bestätigen Sie Ihre Wahl mit der **OK-Taste**. Wechseln Sie nun mit Hilfe der Pfeiltasten in das Menü **TAN mit ATC**. Bestätigen Sie Ihre Wahl mit der **OK-Taste**. Es erscheint „**Start-Code:**“ im Display. Drücken Sie nun die **OK-Taste**, neben der TAN wird Ihnen dann auch der ATC angezeigt.



6.3 TAN-Generierung mit chipTAN USB

Der cyberJack® RFID standard kann bereits das neue chipTAN USB Verfahren. Um diese Funktion nutzen zu können, muss Ihre Bankingsoftware dieses Verfahren unterstützen. Schauen Sie hierzu in die Anleitung Ihrer Bankingsoftware, ob diese bereits das chipTan USB Verfahren unterstützt. Fragen Sie ggf. beim Support des Software-Herstellers nach.

Wie Sie unseren Chipkartenleser in den gängigsten Banking-Programmen einbinden können, haben wir in unserem [Forum](#) dargestellt.

Einstellung TAN Abschluss

Mit dieser Einstellung können Sie die Übertragung der generierten TAN an die Online-Banking App beschleunigen.

Sofort nach der Anzeige und Bestätigung der Transaktionsdaten wird die generierte TAN zur Online-Banking Software gesendet und die nächste Transaktion kann danach gleich gestartet werden. D.h. die Bestätigung der Anzeige der Transaktionsdaten ist bereits die Willenserklärung für diese Transaktion.
Vorteile : Verringerung der Betätigungen der OK-Taste, schnellere Transaktionen

TAN-Generierung mit TAN-Abschluss an (x)

So sehen die nacheinanderfolgenden Displayanzeigen der TAN-Generierung aus, wenn der TAN-Abschluss angeschaltet ist.



TAN-Generierung mit TAN-Abschluss aus (x)

Sie sehen die Displayanzeigen aus, wenn der TAN-Abschluss ausgeschaltet ist. Die TAN wird direkt nach Drücken der OK-Taste an die Banking-Software übermittelt.



7 / Sicherheitshinweise

Organisatorische Sicherheitsmaßnahmen:

- Sorgen Sie dafür, dass unbefugte Personen keinen Zugang zum Kartenlesegerät erhalten. Das Lesegerät ist so zu betreiben, dass der Missbrauch auszuschließen ist.
- Tragen Sie dafür Sorge, dass der PC geeignete Schutzmaßnahmen (wie Virens Scanner, Firewall) besitzt und eine Manipulation durch unbefugte Personen verhindert wird.
- Stellen Sie bei jeder Verwendung des Chipkartenlesers die Unversehrtheit des Chipkartenlesers und der Sicherheitsmerkmale (z.B. Siegel) durch Überprüfung sicher.
- Beachten Sie den Status des Gerätes, der Ihnen durch die LEDs angezeigt wird (Siehe Kapitel [LED-Funktionen](#)^[25]).
- Folgen Sie den Anzeigen auf dem Display durch den Ablauf der sicheren PIN-Eingabe (dem sog. PIN-Dialog, siehe Kapitel [Funktion Sichere PIN-Eingabe](#)^[15]).

Sicherheit von Kleinkindern

Die Geräte und ihr 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 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 **cyberJack® RFID** 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.

8 / Support

Hilfe bei Störungen

Bei Störungen, die sich nicht durch eine erneute Inbetriebnahme (siehe Kapitel 4) Ihres cyberJack® RFID beheben lassen, kontaktieren Sie bitte unsere Serviceabteilung 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 jederzeit eine Supportanfrage an unsere Serviceabteilung unter support@reiner-sct.com 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

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

9 / Technische Referenzen

9.1 LED-Funktionen

Leuchtdioden (LEDs)

Der cyber**Jack**[®] **RFID standard** ist mit einer gelben und einer Duo-LED ausgestattet. Die Duo-LED kann die Farben Blau und Grün annehmen. Grün bedeutet Interaktion mit einer kontaktbehafteten Chipkarte und blau zeigt die Interaktion mit einer kontaktlosen Chipkarte an.

Die Funktion der Duo-LED kann überprüft werden, indem zuerst eine kontaktbehaftete Karte in den Chipkartenleser eingesteckt wird (grüne LED blinkt kurz) und danach eine kontaktlose Karte in den Chipkartenleser eingesteckt wird (blaue LED blinkt kurz).

Die Funktion der gelben-LED kann nach dem Einstecken des USB Steckers überprüft werden. Während der Anzeige der Revisionsnummer im Display des Chipkartenlesers muss diese gelb blinken.

Sollte dies nicht der Fall sein, ist das Gerät defekt. Wenden Sie sich bitte unter support@reiner-sct.com an unseren Support.

Folgende Zustände der Leuchtdioden (LED) sind möglich:

Gelbe LED	Duo-LED Grün	Duo-LED Blau	Bedeutung
blinkt gleichmäßig	leuchtet dauerhaft		Modus Sichere PIN-Eingabe bei der qualifizierten elektronischen Signatur mit kontaktbehafteten Signaturkarten; angezeigter Text ist authentisch.
blinkt gleichmäßig		leuchtet dauerhaft	PIN-Eingabe mit kontaktloser Chipkarten; angezeigter Text ist authentisch.
blinkt gleichmäßig			Der cyber Jack [®] RFID standard führt ein Firmware-Update durch oder zeigt den Text authentisch im Display an.
blinkt gleichmäßig		blinkt gleichmäßig	Bei synchron blinkender gelber LED und blauer Duo-LED befindet sich der Chipkartenleser aufgrund absichtlich herbeigeführten oder aufgrund technischen Versagens in einer Endlosschleife, in der nur noch das Blinken der LEDs möglich ist. Weitere Funktionen sind nicht mehr möglich. Der Chipkartenleser kann nur durch Abziehen und erneutes Einstecken wieder gestartet werden. 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.
	leuchtet dauerhaft		Interface zur kontaktbehafteten Chipkarte ist aktiviert (Betriebszustand).
	blinkt		Innerhalb der letzten 3 Sekunden hat eine Kartenkommunikation zur kontaktbehafteten Chipkarte stattgefunden.
		leuchtet dauerhaft	Interface zur kontaktlosen Chipkarte ist aktiviert (Betriebszustand).
		blinkt	Innerhalb der letzten 3 Sekunden hat eine Kartenkommunikation zur kontaktlosen Chipkarte stattgefunden.



Das gleichzeitige oder abwechselnde Leuchten der Duo-LED in beiden Farben ist nicht möglich, da immer nur eine Schnittstelle aktiv ist.

9.2 Technische Einsatzumgebung

Das technische Umfeld für den cyberJack® RFID standard bildet ein mit USB-Schnittstelle und Treibern ausgestatteter PC, an welchen der cyberJack® RFID standard angeschlossen wird.

Kontaktbehaftete Chipkartenschnittstelle

Die cyberJack® RFID standard Chipkartenleser verarbeiten Chipkarten deren Kartenkörper in den ISO-Normen 7810, 7813 und 7816 Teil 1 physikalisch spezifiziert ist. Durch die Kontaktiereinheit des Chipkartenlesers werden elektrische Kontakte eines auf dem Kartenkörper aufgebrachten Mikroprozessors kontaktiert. Deren Lage und elektrische Zuordnung ist in der ISO-Norm 7816 Teil 2 definiert. Die cyberJack® RFID standard Chipkartenleser verarbeiten sowohl Prozessorkarten mit den asynchronen Kommunikationsprotokollen T=0 und T=1, als auch Speicherkarten mit den synchronen Kommunikationsprotokollen 2-wire, 3-wire und I²C-Bus. Diese Kommunikationsprotokolle sind in der ISO 7816 Teil 3 (asynchron) bzw. in herstellerspezifischen Datenblättern (synchron) spezifiziert.

Kontaktlose Chipkartenschnittstelle

Der Chipkartenleser unterstützt die Protokolltypen TYP A und Typ B nach ISO/IEC 14443. Der Betrieb von kontaktlosen Chipkarten durch den Chipkartenleser erfolgt gem. der Norm ISO/IEC 14443-2, ISO/IEC 14443-3 und ISO/IEC 14443-4.

Sichere PIN-Eingabe für die QES

Die sichere PIN-Eingabe für die QES wird über die in ISO 7816 Teil 3 spezifizierten Kommunikationsprotokolle durchgeführt. Während des Modus Sichere PIN-Eingabe wird durch die Sicherheitsfunktion Befehlsfilter sichergestellt, dass nur zugelassene Kommandos zur Chipkarte gesendet werden. Alle anderen Befehle zur Chipkarte werden vom Chipkartenleser blockiert (Vergleiche Kapitel [Sicherheitsfunktion^{\[26\]}](#)).

9.3 Sicherheitsfunktionen

Die Sichere PIN-Eingabe ist eine der wichtigsten Sicherheitsanwendung eines Chipkartenlesers ab der Sicherheitsklasse 2. Die Sichere PIN-Eingabe für die Qualifizierte Elektronische Signatur ist nur mit einer kontaktbehafteten Chipkarte möglich. Um sicherzustellen, dass die PIN nicht im Chipkartenleser gespeichert wird, wurden spezielle Sicherheitsfunktionen im cyberJack RFID standard implementiert und die Hard- und Software des Chipkartenlesers strengen sicherheitstechnischen Evaluierungen unterzogen. Die nachfolgenden Sicherheitsfunktionen sind im cyberJack® RFID standard realisiert:

Applikationstrennung

Der cyberJack® RFID standard verhindert mit der Applikationstrennung, dass sich Applikationen gegenseitig beeinflussen. Die vom PC empfangenen Kommandos werden an die entsprechende Applikation übergeben und durch diese vollständig abgearbeitet. Erst nach Abarbeitung des Kommandos werden neue Kommandos vom PC angenommen.

Modulupdate

Es ist möglich den Chipkartenleser mit Hilfe des Gerätemanagers (Siehe [Kapitel Gerätemanagers^{\[11\]}](#)) mit neuen Modulen (Kernel, Applikation) zu versehen, welche von den Webseiten von REINER SCT (www.reiner-sct.com) bezogen werden können. Um in den Chipkartenleser ein neues Modul zu laden, wird als wichtige Sicherheitsfunktion die Überprüfung der Herkunft des Moduls durch den Chipkartenleser selbst durchgeführt. So akzeptiert der Chipkartenleser nur Module die mittels RSA-Verfahren von REINER SCT elektronisch signiert wurden. Der Chipkartenleser führt jeweils vor dem Aufbringen eines neuen Moduls eine Signaturprüfung durch. Module können einzeln oder komplett geladen und aktualisiert werden. Geladene Module beeinflussen die Funktionalität der anderen Module nicht. Ein Speichern eines nicht von REINER SCT elektronisch signierten Moduls im Chipkartenleser ist nicht möglich. Es werden von REINER-SCT nur evaluierte und vom BSI zugelassene Versionen bereitgestellt. Ein Update des cyberJack® RFID standard auf eine ältere Version ist nicht möglich.

Kommunikationstrennung

Nach Anstoßen des Modus "Sichere PIN-Eingabe" durch eine Applikation unterbricht der cyberJack® RFID standard die Kommunikation zum PC, schaltet die gelbe LED in den Blinkmodus sowie die

entsprechende Duo-LED ein (grün für kontaktbehaftet, blau für kontaktlose Chipkarten). In der Sicheren PIN-Eingabe nimmt der **cyberJack® RFID standard** alle Tastatureingaben auf und leitet diese ausschließlich an die Karte weiter. Vor Freigabe der Kommunikationstrennung werden diese Daten durch eine weitere Sicherheitsfunktion (Wiederaufbereitung) gelöscht.

Die Kommunikationsunterbrechung zum PC erfolgt softwaregesteuert durch eine Sperre, welche sicherstellt, dass im Modus Sichere PIN-Eingabe keine Werte aus dem Speicher (PIN-Daten) übertragen werden. Es werden ausschließlich Protokollinformationen an den PC übertragen, die stets als Konstanten direkt an das Hardwareinterface übergeben werden.

Sollte der Chipkartenleser durch eine Fehlfunktion doch in die Routine für die PC-Kommunikation wechseln, wird dort der Modus Sichere PIN-Eingabe erkannt und in die Sicherheitsroutine „Halt“ gewechselt. In dieser wird der Chipkartenleser neu initialisiert, das gesamte Interruptsystem abgeschaltet und die gelbe LED blinkt synchron mit der blauen Duo-LED. Ein Verlassen ist nur durch Abziehen und wieder Anstecken des Chipkartenlesers möglich.

Die Kommunikationstrennung kann über Schnittstellen von außen nicht beeinflusst werden.

Wiederaufbereitung

Mit der Sicherheitsfunktion Wiederaufbereitung wird derjenige Bereich des Speichers, in welchem die PIN-Daten während dem Modus Sichere PIN-Eingabe zwischengespeichert sind, wiederaufbereitet (Überschreiben der Speicherstellen der PIN-Daten mit Nullen). Damit wird ein mögliches Auslesen der im temporären Speicher befindlichen PIN-Daten verhindert.

Das Überschreiben des Speicherbereichs mit Nullen wird vor dem Wiederherstellen der Kommunikation zum PC (nach der Sicheren PIN-Eingabe) vorgenommen. Dies erfolgt sowohl nach erfolgreicher Übertragung der PIN-Daten zur kontaktbehafteten Signaturerstellungseinheit (Chipkarte) oder im Falle eines Abbruchs der PIN-Eingabe durch den Benutzer (Cancel) oder durch einen Timeout.

Kommt es während der Sicheren PIN-Eingabe zu einem Fehler mit anschließendem Systemstart wird der entsprechende Speicherbereich neu initialisiert und damit eventuell vorhandene PIN-Daten ebenfalls gelöscht.

Durch Überschreiben der Speicherstellen der PIN-Daten mit Nullen gewährleistet der **cyberJack® RFID standard**, dass diese Daten in den Speicherbereichen nicht mehr enthalten sind und somit nach Beenden der Sicheren PIN-Eingabe nicht ausgelesen werden können.

Neuinitialisierung

Mit der Sicherheitsfunktion Neuinitialisierung wird der Speicher des **cyberJack® RFID standard** neu initialisiert. Dies geschieht durch Überschreiben des gesamten RAMs mit Nullen. Ausnahme sind hier ein paar Bytes für den Stackspeicher und wenige Bytes, die den Ist-Zustand des USB-Systems speichern. Diese sind für die Funktion des Controllers und damit des System unbedingt erforderlich.

Die Sicherheitsfunktion wird beim Start des **cyberJack® RFID standard** durch Einstecken des Chipkartenlesers in den PC, nach einem Watchdog-Reset oder nach einem Controller-Reset angewendet.

Zu einem Watchdog-Reset kommt es, wenn bei absichtlich herbeigeführten oder aufgrund technischen Versagens entstehenden Störungen des funktionalen Ablaufs des **cyberJack® RFID standard** (insbesondere durch Nicht-Interpretierbarkeit der Befehlssätze) der Watchdog-Timer nicht innerhalb eines bestimmten Zeitintervalls zurückgesetzt wird und der Watchdog daher einen Reset des Controllers auslöst.

Nach einem Reset durch den Watchdog wird der Chipkartenleser anschließend angehalten und die gelbe LED und die blaue Duo-LED blinken synchron.

Bei einem normalen Startvorgang wird die aktuell gültige Versionsnummer der aktiven Firmware am Display des Chipkartenlesers angezeigt. Die Authentizität der Versionsanzeige wird dem Benutzer dabei durch Blinken der gelben LED angezeigt.

Befehlsfilter

Der **cyberJack® RFID standard** verhindert mit dieser Sicherheitsfunktion, dass Befehle an die Chipkarte weitergeleitet werden könnten, die geeignet sind, PIN-Daten auf der Chipkarte zu speichern oder zu manipulieren. Daher werden innerhalb des Modus "Sichere PIN-Eingabe" nur Befehle an die Chipkarte weitergeleitet, die zu Authentifizierungszwecken 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.

Index

- A -

Auspacken und Aufstellen 3

- F -

Firmwaredownload 26

- G -

Gerätemanager 11

Gerätemenü 10

Gerätesiegel 3

- L -

LED-Funktion 25

- R -

RFID

deaktivieren 19

- S -

Sichere PIN-Eingabe 15

Sicheres Ändern der PIN 15

Sicherheitsfunktion 26

Sicherheitshinweise 23

Siegel 3

Support

Gewährleistung 24

Service 24

- T -

TAN-Generierung

chipTAN USB 21

Manuell 21

Mit ATC 21

Treiberinstallation

MAC 7

Windows 6

REINER Kartengeräte GmbH & Co. KG

Baumannstr. 18
78120 Furtwangen
Germany
Tel.: +49 (7723) 5056-0
info@reiner-sct.com
www.reiner-sct.com