REINERSCT

cyber*Jack*® RFID komfort

Installations- und Bedienungsanleitung

Inhaltsverzeichnis

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 neue Personalausweis (nPA)

Neben der hoheitlichen Ausweisfunktion dient der neue Personalausweis (nPA) 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. Zusätzlich kann der nPA auch für die qualifizierte elektronische Signatur (eSign) nach dem Signaturgesetz genutzt werden. So können zum Beispiel Dokumente rechtsverbindlich elektronisch unterzeichnet werden, ohne dass eine händische Unterschrift benötigt wird.

Viel Erfolg mit Ihrem neuen Gerät wünscht Ihnen

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

www.reiner-sct.com

V1.10 11.01.2013

2 Gerätebeschreibung

2.1 cyberJack RFID komfort

Der cyber***Jack***® **RFID komfort** wurde primär für die Nutzung des elektronischen Identitätsnachweises und der qualifizierten elektronischen Signatur (eSign) 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 komfort** eignet sich ebenfalls für die Nutzung von Anwendungen der elektronischen Signatur gemäß Signaturgesetz und Signaturverordnung für kontaktbehaftete und kontaktlose Chipkarten. Anwendungen der elektronischen Signatur sind z.B. die fortgeschrittene elektronische Signatur (FES) oder die qualifizierte elektronische Signatur (QES, eSign).

Selbstverständlich hat der cyber***Jack***® **RFID komfort** 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.

cyberJack® RFID komfort

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

2.1.1 Leser auspacken und aufstellen

Auspacken

In der Verpackung sind enthalten[1)]:

- cyber***Jack***® **RFID komfort**
- Standfuß
- USB-Kabel
- Kurzanleitung zur Geräteinstallation
- Treiber-CD

1)
Je nach Variante und Bezugsquelle kann der Inhalt variieren oder sich weitere Komponenten in der Verpackung befinden.

Aufstellen cyber*Jack*® RFID komfort

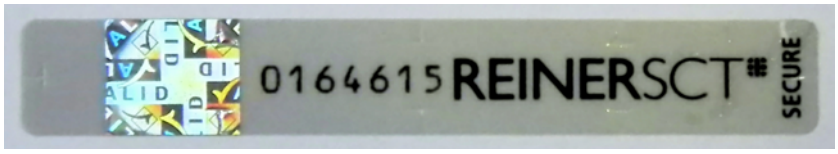
Bitte entnehmen Sie das Gerät und das mitgelieferte USB-Kabel aus der Verpackung und stecken Sie das USB-Kabel in die dafür vorgesehene Kabelbuchse auf der Geräterückseite Ihres cyber***Jack***® **RFID komfort** ein. Der Pfeil, der sich auf dem kleinen Stecker befindet, muss für Sie sichtbar sein. Legen Sie danach das USB-Kabel in die Kabelführung ein, so dass das Kabel nach hinten oder seitlich abgeführt wird. Wenn Sie das Kabel nach hinten führen, können Sie auch die weitere Kabelführung im Standfuß nutzen. 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.

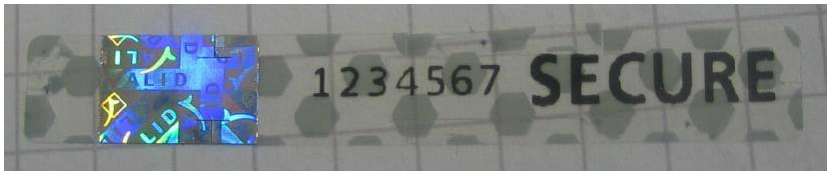
Sicherheitshinweis Gerätesiegel

Achten Sie darauf, dass die beiden aufgebrachte Siegel unbeschädigt sind und der Abbildung auf dem Foto entsprechen.

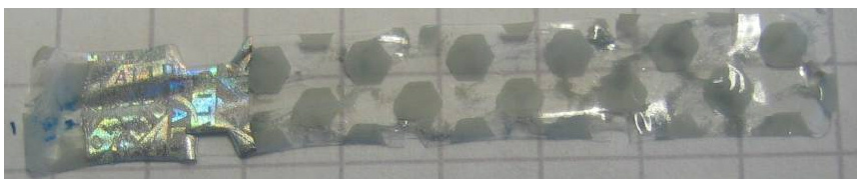


Unbeschädigtes Siegel

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

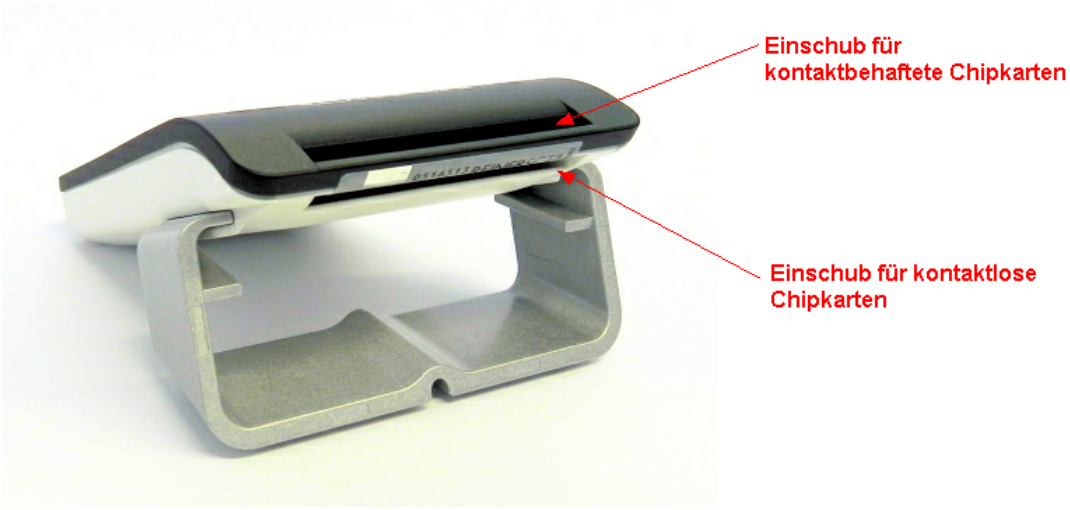
Bei einer Beschädigung der Gerätesiegel besteht Manipulationsverdacht. Bitte wenden Sie sich in diesen Fall umgehend an Ihren Fachhändler und verwenden Sie das Gerät nicht.

Sicherheitsversiegelung unten cyberJack® RFID komfort

Sicherheitsversiegelung oben cyberJack® RFID komfort

Kartenhandhabung

Mit dem cyber***Jack***® **RFID komfort** 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 neuen Personalausweis, gedacht.



3 Die Funktionen Ihres Chipkartenlesers

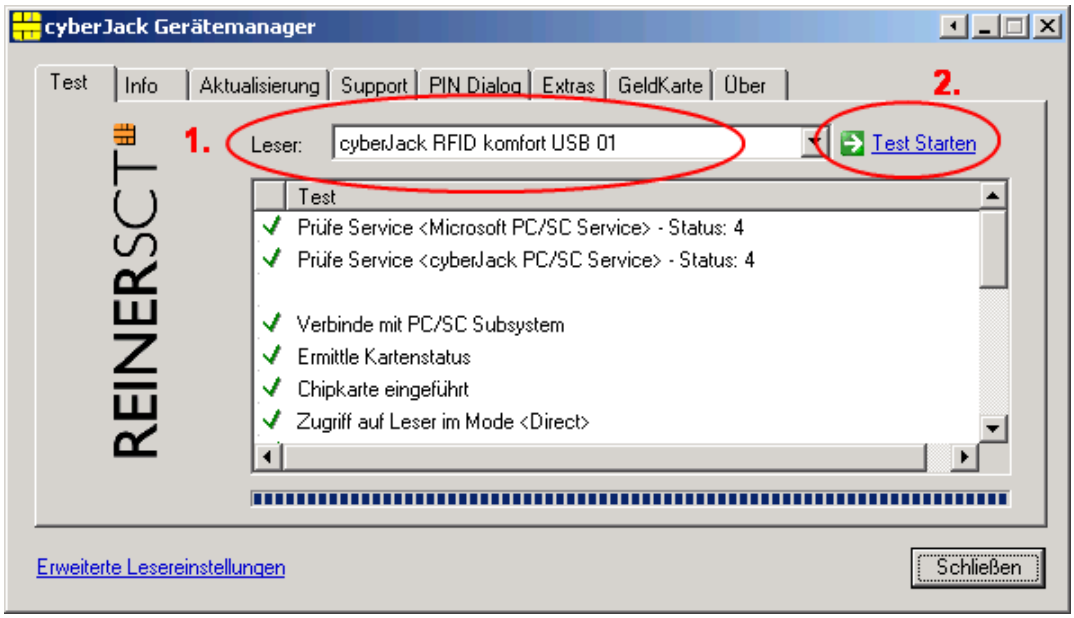
3.1 Gerätemanager

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 cyber***Jack***® bieten.

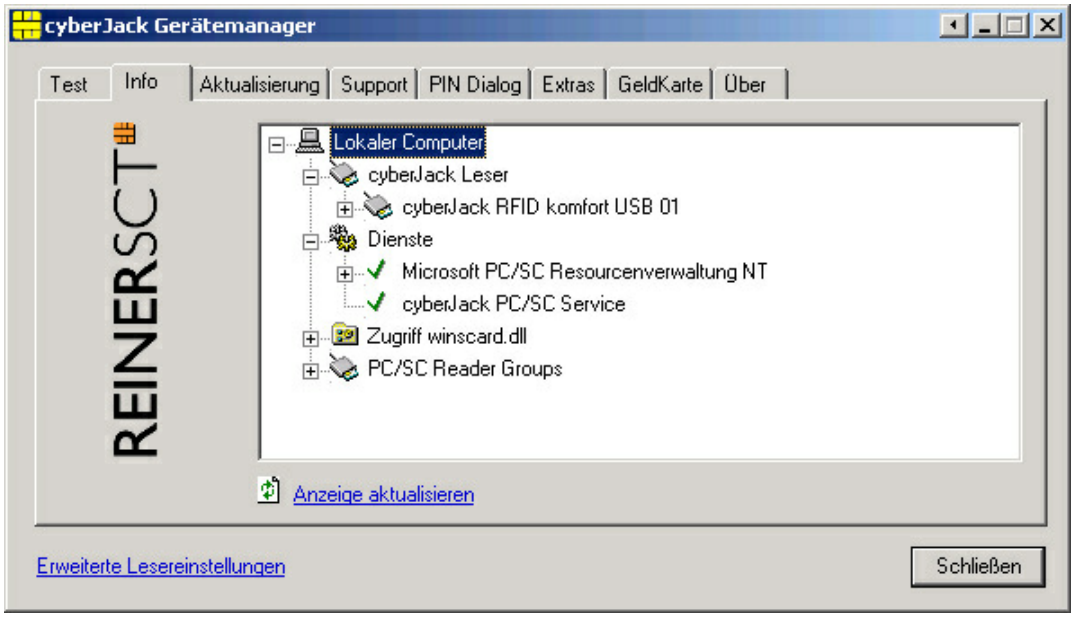
Registerkarte Test

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 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.



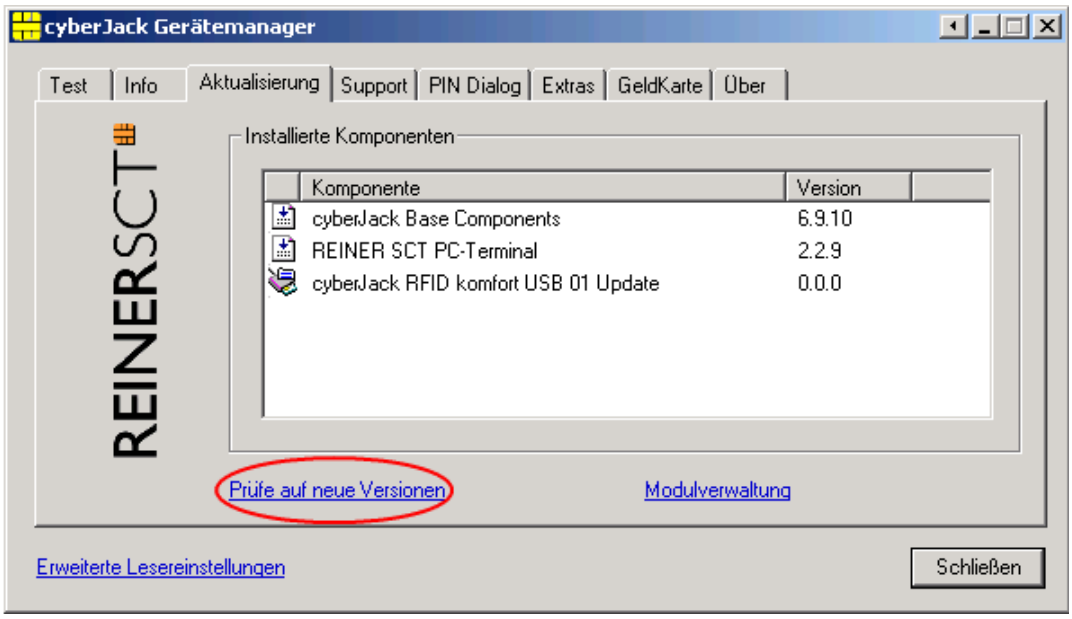
Registerkarte Info

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



Registerkarte Aktualisierung

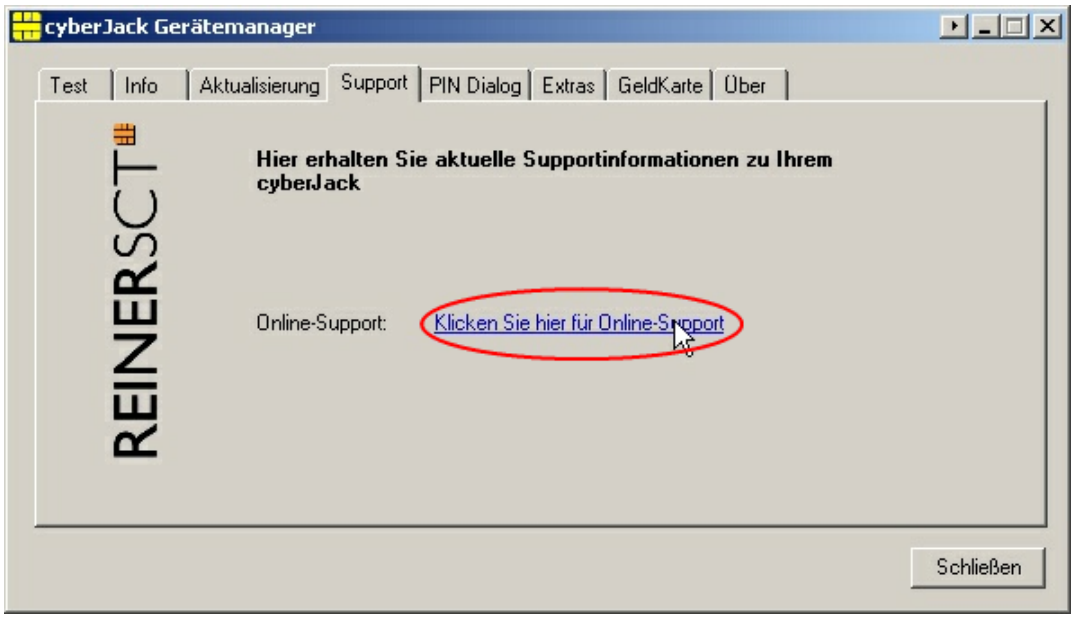
In Aktualisierung können Sie überprüfen, ob Sie noch über den aktuellen Treiberstand sowie Firmware für den cyber***Jack***® **RFID komfort** verfügen. Durch Betätigung des Links **Prüfe auf neue Versionen** wird Ihr Internet Browser gestartet und eine Verbindung zum REINER SCT Download Server hergestellt. Sollte Ihr Browser nicht komfortmäßig 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 Sicherer Firmwaredownload. 14

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.

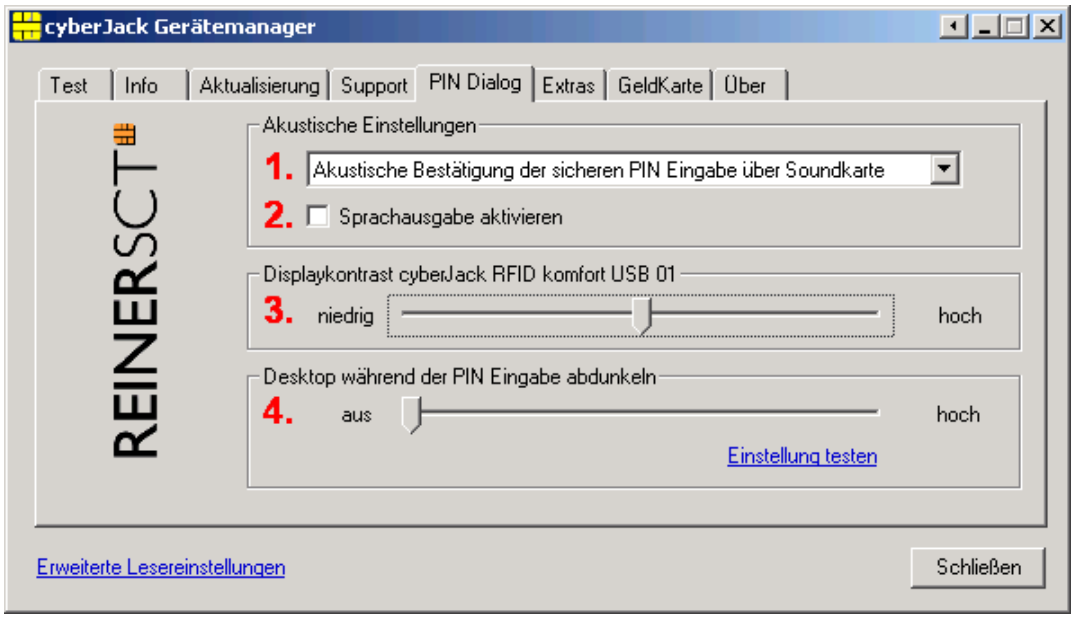


Registerkarte PIN Dialog

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

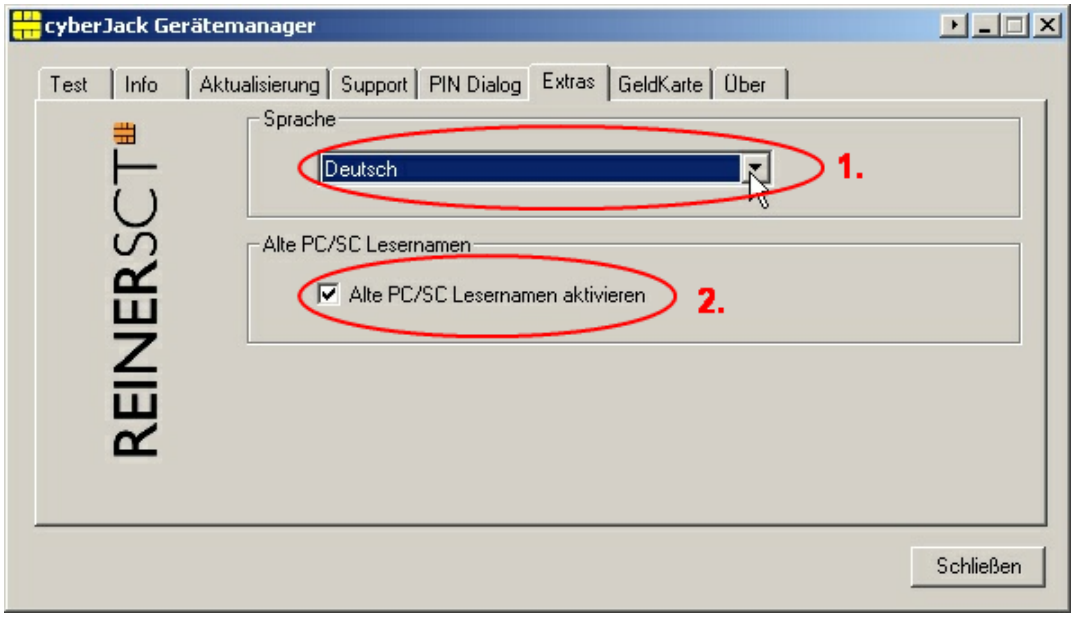
(1) Hier können Sie auswählen, ob bei der PIN-Eingabe der Tastendruck einen Ton erzeugen soll.
(2) Setzen Sie hier den Haken und die Aufforderung der PIN ertönt akustisch mit einer freundlichen Stimme.
(3) Hier können Sie den Displaykontrast des Chipkartenlesers einstellen und somit die optimale Einstellung 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

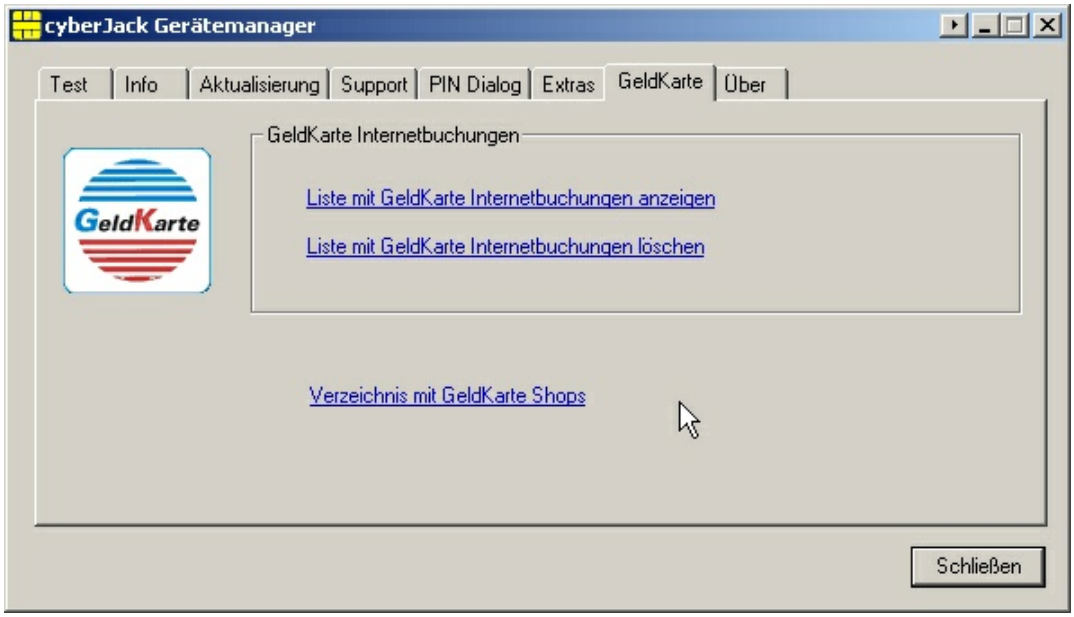
Hier können Sie die Sprache des Gerätemanagers (1) auswählen.

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



Registerkarte GeldKarte

Diese Registerkarte kann nur bei einem installierten cyber***Jack***® **e-com** verwendet werden.. GeldKarte-Transaktionen werden vom Chipkartenleser 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.

3.2 Die Funktion sichere PIN-Eingabe

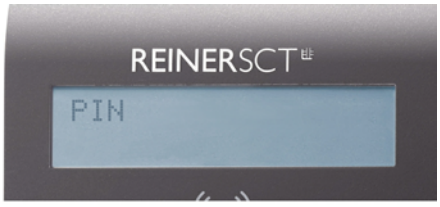
Die Funktion Sichere PIN-Eingabe dient dazu, dass Ihre Geheimzahl in einer sicheren Umgebung bleibt. Verschiedene Hackerangriffe hatten bereits das Ausspähen der PIN zum Ziel. Die Angreifer machen sich hierbei die Tatsache zunutze, dass der PC eine unsichere Umgebung darstellt, bei der Tastatureingaben 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.

Die PIN darf nur eingegeben werden, wenn das Vorhandensein eines sicheren Kanals zwischen Tastatur und cyberJack® RFID komfort 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 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 Displayanzeigen erscheinen beim Chipkartenleser, wenn eine sichere PIN-Eingabe erforderlich ist.



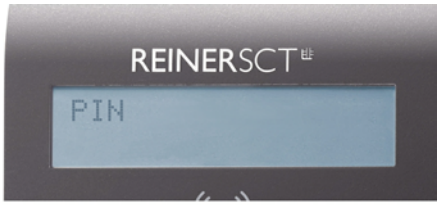
Abfrage Sichere PIN

Abfrage Signatur-PIN

Folgende Displayanzeigen erscheinen beim Chipkartenleser, bei Nutzung des neuen Personalausweises (nPa).

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.).

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
Pfeiltaste nach oben	Funktion anwendungsspezifisch
Pfeiltaste nach unten	Funktion anwendungsspezifisch

Bei jedem Tastendruck, der vom Chipkartenleser verarbeitet wird, wird ein kurzer Signalton ausgegeben. Dieser Signalton ist für jede Taste immer gleich.

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 mit einer kontaktbehafteten und kontaktlosen 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

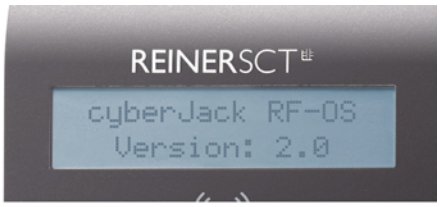
Alle anderen Befehle zur Chipkarte werden vom Chipkartenleser blockiert.

3.3 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



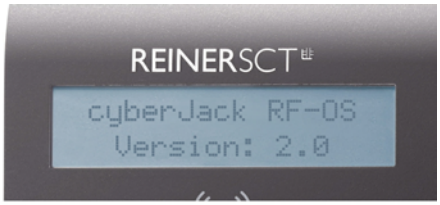
Anzeige der Version

Anzeige der Chipkartenleser-ID (Anzeige erfolgt nur beim Drücken der @-Taste)

Standardanzeige im Betrieb des Chipkartenlesers

Es war bereits eine Applikation geladen

Reihenfolge der Displayanzeige mit geladener Applikation



Anzeige der Version

Anzeige der Chipkartenleser-ID (Anzeige erfolgt nur beim Drücken der @-Taste)

Anzeige der geladenen Applikation (Anzeige erfolgt nur beim Drücken der @-Taste)

Anzeige der Revision der geladenen Applikation (Anzeige erfolgt nur beim Drücken der @-Taste)

Anzeige bei geladenen Zertifikaten (Anzeige erfolgt nur beim Drücken der @-Taste)

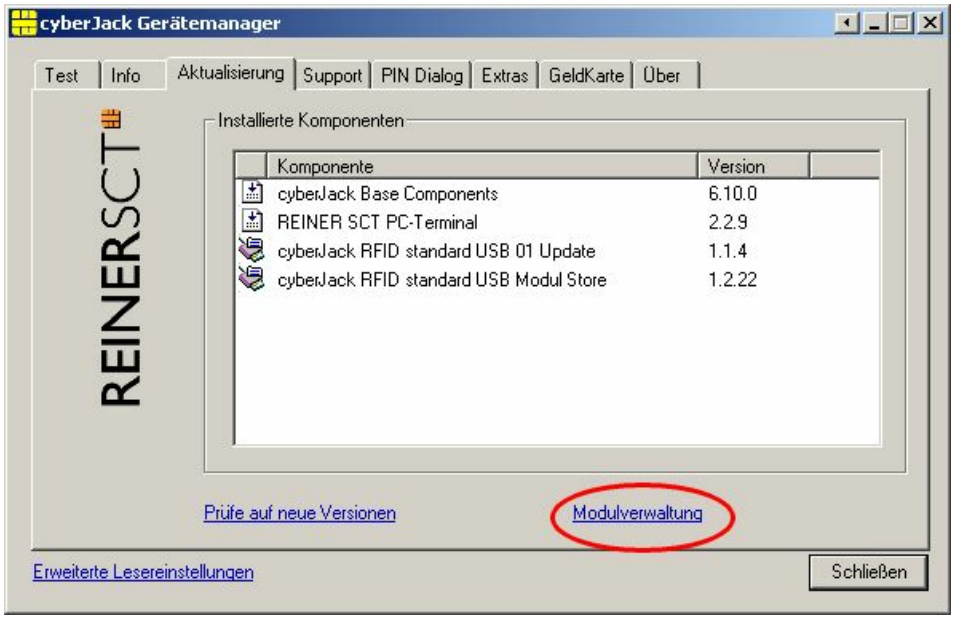
Anzeige bei geladenen Zertifikaten (Anzeige erfolgt nur beim Drücken der @-Taste)

Standardanzeige im Betrieb des Chipkartenlesers bei geladener Applikation

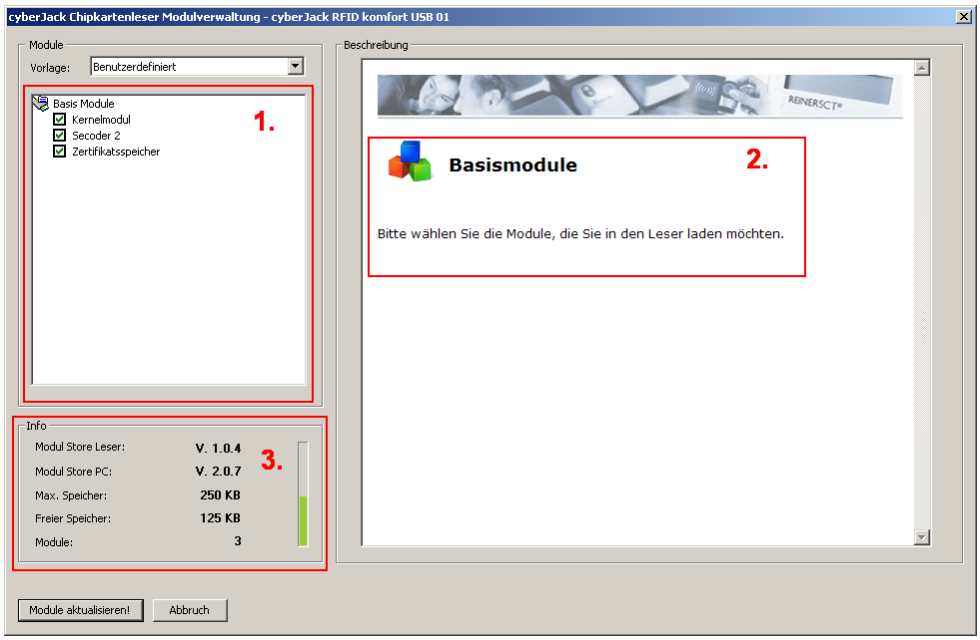
3.4 Modulverwaltung

Es ist möglich den Chipkartenleser mit Hilfe des Gerätemanagers (Siehe Kapitel Gerätemanager 5) mit neuen Modulen zu versehen.

Diese verschiedenen Module werden im Modul Store zusammengefaßt. Den Modul Store finden Sie in der Modulverwaltung.



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.
Der Modul Store Leser ist der Versionsstand, den der angeschlossene Chipkartenleser hat. Der Modul Store PC ist der Stand des Modul Store, der aktuell auf dem PC gespeichert ist. Dieser kann gegebenenfalls über den **Reiter Aktualisierung > Prüfe auf neue Version** upgedatet werden.

Beschreibung des Modul Store Downloads

1. Gerätemanager starten.
2. Auf Registerkarte **Aktualisierung** wechseln.
3. Link **Prüfen auf neue Versionen** anklicken (hier wird online das Vorhandensein einer neuen Version auf der REINER SCT Website geprüft)
4. Gegebenenfalls neue Version mit anklicken von Weiter herunterladen und dem InstallShield Wizzard folgen.
5. In der Registerkarte **Aktualisierung** klicken Sie auf **Modulverwaltung**.
6. **Module aktualisieren** anklicken.
7. Der Chipkartenleser fragt in seinem Display nach "Firmware aktualisieren".
8. Nach Betätigen der OK-Taste blinkt während der Verifikation der Firmware (Prüfen der Signatur) kurz die gelbe LED.
9. Das Ende des Downloads wird im Gerätemanager angezeigt.

Wenn noch nie eine Secoder-Applikation auf dem Chipkartenleser war, dann fragt der Chipkartenleser bei der Aktualisierung in seinem Display nach, ob alle Applikationen gelöscht werden sollen. Dabei blinkt die gelbe LED. Nach Betätigen der OK-Taste auf dem Chipkartenleser wird gefragt, ob der Kernel aktualisiert werden soll. Dabei blinkt die gelbe LED. Bitte folgen Sie den Displayanzeigen des Chipkartenlesers.

Um in den Chipkartenleser eine neue Firmware (Kernelmodul) 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 elektronisch 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. Es werden von REINER SCT nur evaluierte Module und vom BSI zugelassene Versionen des Kernels bereitgestellt.
Ein Update des cyber***Jack***® **RFID komfort** auf eine ältere Version 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). Die aktuelle Firmwareversion wird auch direkt nach dem Einstecken des Chipkartenlesers oder durch Drücken der @-Taste im Display angezeigt. Während der Anzeige der Revisionsnummer blinkt die gelbe LED.

Sollte sich nach einem Modulupdate in der Displayanzeige **"Bereit für Update"** (Siehe Kapitel 3.3) stehen, bzw. nach einem Druck auf die @-Taste, die Revision der Applikation nicht mehr angezeigt werden, muss das Modulupdate wiederholt werden.

3.5 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. Sie sehen im Display, den Status des RFID-Feldes.

RFID-Feld ist eingeschaltet

RFID-Feld ist ausgeschaltet

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

Änderungsabfrage

Bestätigen Sie die Displayanzeige mit der OK-Taste.

Das RFID-Feld ist jetzt ausgeschaltet

3.6 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 Betriebsystem 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 komfort** durch die AusweisApp für die elektronische Identitätsfunktion genutzt werden. Eine aktuelle Version der AusweisApp finden Sie unter www.ausweisapp.bund.de.
Zusätzlich kann der Chipkartenleser in Verbindung mit dem nPA auch für die qualifizierte elektronische Signatur (eSign) nach dem Signaturgesetz genutzt werden. So können zum Beispiel Dokumente rechtsverbindlich elektronisch unterzeichnet werden, ohne dass eine händische Unterschrift benötigt wird.

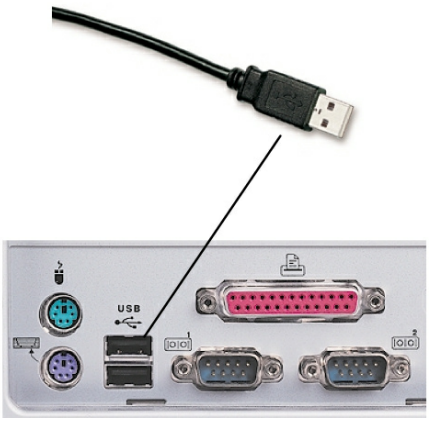
4 Installation der Hardware am PC

4.1 Treiberinstallation unter Windows

Dieser RFID-Chipkartenleser wird aktuell von folgenden Betriebssystemen unterstützt: Windows 2000 / Windows XP 32 Bit, Windows Vista 32/64 Bit / Windows 7 32/64 Bit, sowie Windows Server 2003 – 2008 R2 32/64 Bit.

Der cyber***Jack***® **RFID komfort** mit USB-Anschluss darf erst nach erfolgter Installation des Treibers und erfolgtem Neustart an die USB-Schnittstelle des Rechners angeschlossen werden.
Der cyber***Jack***® **RFID komfort** 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 unter Installation der Softwarekomponente 17 beschrieben.
2. Stecken Sie anschließend den USB-Stecker des cyber***Jack***® **RFID komfort** 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.



Wie Sie bei der Treiberinstallation für die verschiedenen Betriebssysteme vorgehen, erfahren Sie in den folgenden Kapiteln:

4.2 Installation der Softwarekomponente

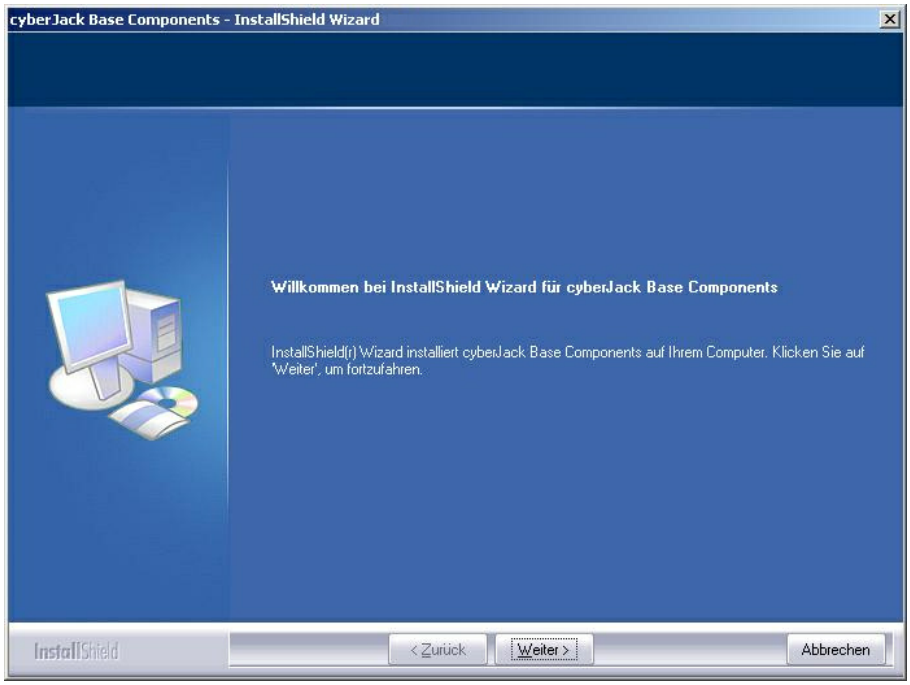
Legen Sie die cyber***Jack***® Treiber-CD in das CD-Laufwerk Ihres Computers ein. Mit dem daraufhin startenden Installation Manager können Sie verschiedene Softwarekomponenten für die cyber***Jack***® Chipkartenleserfamilie komfortabel und einfach installieren. Unterstützt Ihr System nicht die Autostart-Funktion, 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.

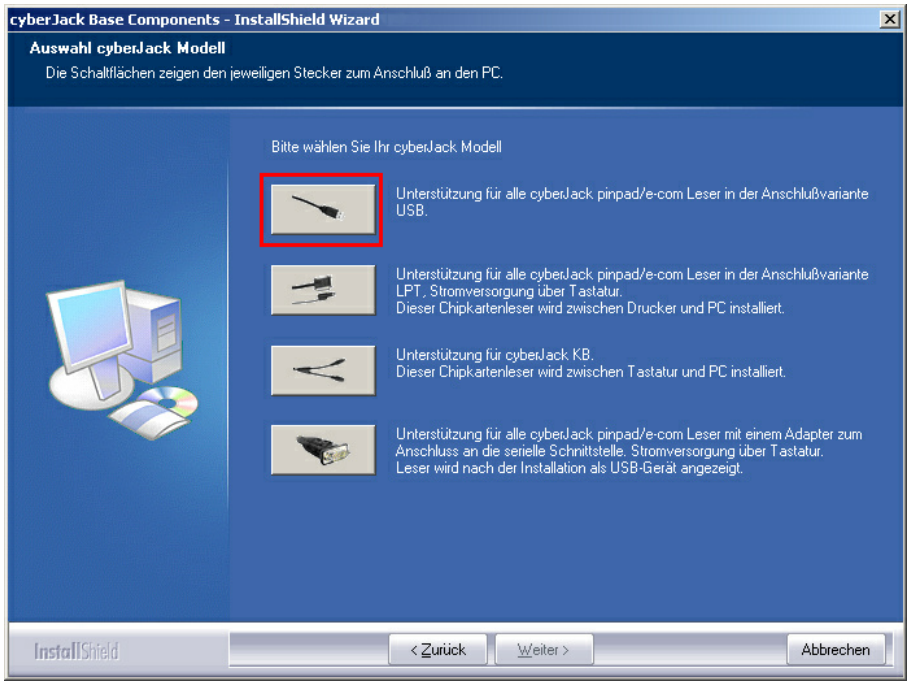
Die Installation cyber***Jack***® Base Components ist zum Betrieb der cyber***Jack***® **RFID komfort** Chipkartenleser unbedingt erforderlich. Hierin sind die Systemtreiber enthalten. Desweiteren wird der Gerätemanager mit den Funktionen Gerätetest, Treiberupdate und Online-Support installiert.

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.

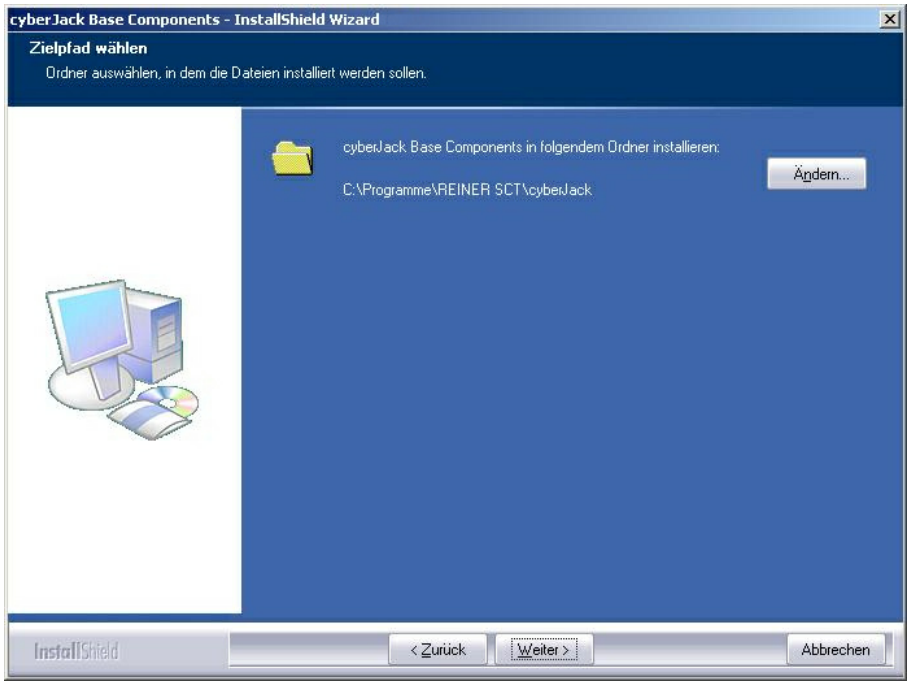
Wollen Sie die cyber*Jack*® Base Components unter Windows 2000/XP/2003 Server/Vista installieren, müssen Sie über Administratorrechte verfügen. Beachten Sie weiterhin, dass alle Programme geschlossen werden müssen, bevor Sie mit der Installation beginnen.



Stimmen Sie im Fenster Lizenzvereinbarung den Lizenzvereinbarungen zu und klicken auf den Button [Weiter]. Wählen Sie im nächsten Schritt Ihre Anschlussart USB aus.

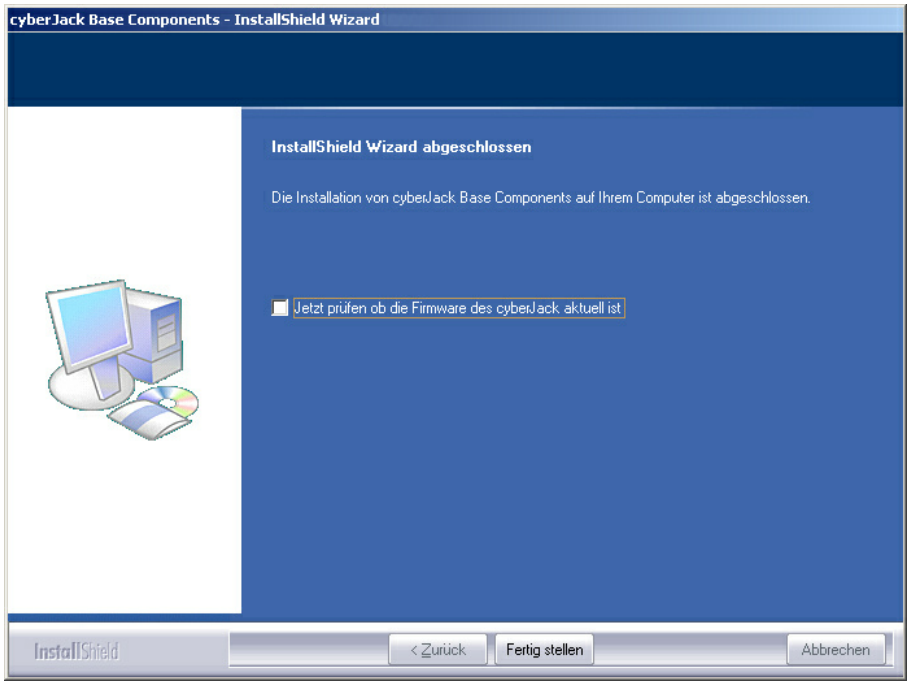


Durch Anklicken des entsprechenden Kästchens wählen Sie den Treiber für Ihren Chipkartenleser aus. Klicken Sie auf [Weiter].



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.

4.3 Treiberinstallation unter Linux

Dieser RFID-Chipkartenleser wird aktuell von folgenden Betriebssystemen unterstützt: openSuSE-11.1-i586, openSuSE-11-1-x86_64, openSuSE-11-2-i586, openSuSE-11-2-x86_64, debian-500-i386, debian-500-amd64, ubuntu-9.04-desktop-i386, ubuntu-9.04-desktop-amd64, ubuntu-10.04.1-desktop-i386,ubuntu-10.04.1-desktop-amd64.

4.3.1 Linux.deb

4.3.1.1 Beschreibung für ubuntu

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

Die Installation der Treiber für den cyber***Jack***® **RFID komfort** 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 komfort**

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. Fügen Sie Ihren Benutzer der Gruppe cyberjack hinzu. Nutzen Sie dazu den Befehl *usermod –aG cyberjack „benutzername“* in der Terminaleingabe.
5. Bitte führen Sie einen Neustart durch.
6. Die Treiberinstallation ist nun abgeschlossen. Sie können nun den cyber***Jack***® **RFID komfort** 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 komfort** benötigen Sie ein Anwendungsprogramm und

eine RFID-Chipkarte bzw. den neuen elektronischen Personalausweis.

4.3.1.2 Beschreibung für debian

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

Die Installation der Treiber für den cyber***Jack***® **RFID komfort** 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 komfort**

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 folgendem Befehl in der Terminaleingabe aus. Befehl: *dpkg -i (Dateiname).deb*
4. Fügen Sie Ihren Benutzer der Gruppe cyberjack hinzu. Nutzen Sie dazu den Befehl *usermod –aG cyberjack „benutzername“* in der Terminaleingabe.

Bitte beachten Sie, dass diese Befehle als root auszuführen sind.

5. Bitte führen Sie einen Neustart durch.
6. Die Treiberinstallation ist nun abgeschlossen. Sie können nun den cyber***Jack***® **RFID komfort** 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 komfort** benötigen Sie ein Anwendungsprogramm und eine RFID-Chipkarte bzw. den neuen elektronischen Personalausweis.

4.3.2 Linux.rpm

Beschreibung für SuSE Linux

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

Die Installation der Treiber für den cyber***Jack***® **RFID komfort** teilt sich grundsätzlich in zwei Schritte auf:

a) Installation des PCSCD-Treibers und dessen Abhängigkeiten zu installieren
b) Installation des aktuellen Treibers für den cyber***Jack***® **RFID komfort**

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 komfort** 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 komfort** benötigen Sie ein Anwendungsprogramm und eine RFID-Chipkarte bzw. den neuen elektronischen Personalausweis.

4.4 Treiberinstallation unter Mac

Dieser RFID-Chipkartenleser wird aktuell von MAC OS X unterstützt. Genauere Informationen finden Sie hier.

Der cyber***Jack***® **RFID komfort** 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 komfort** ist eine Treiberinstallation notwendig.

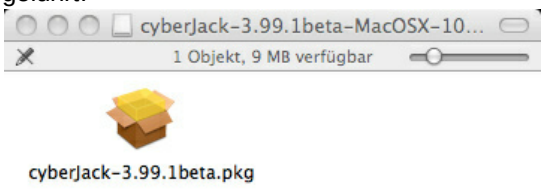
Wie Sie bei der Treiberinstallation für das Betriebssystem vorgehen, erfahren Sie im folgenden Kapitel:

- Mac OS X 22

4.4.1 Mac OS X

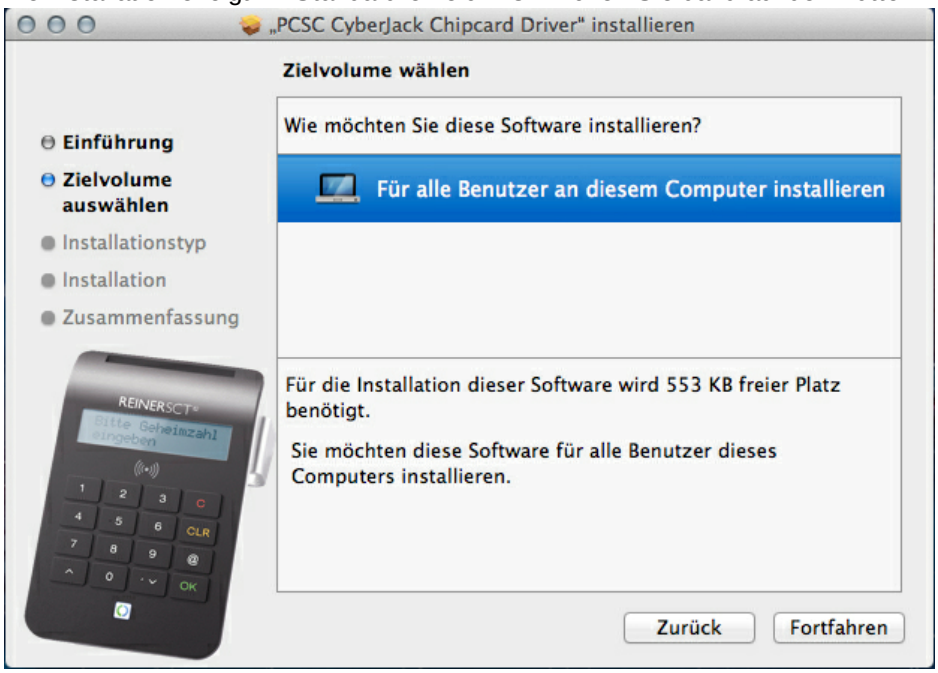
Zur Installation der Treiber für den cyber***Jack***® **RFID komfort** benötigen Sie eine Internetverbindung. Stecken Sie den Chipkartenleser noch nicht ein!

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

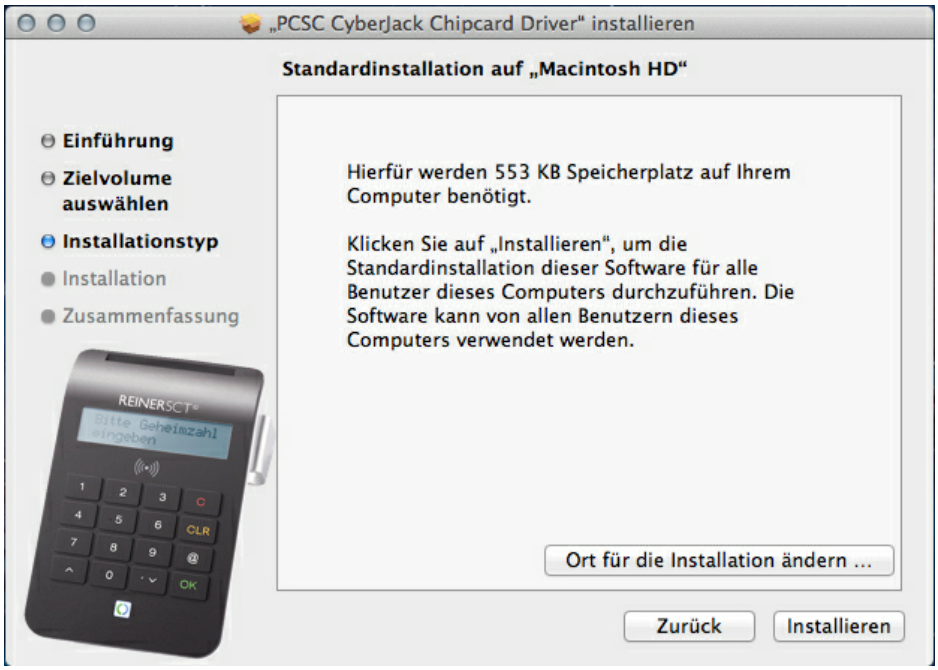


Klicken Sie auf den Button "**Fortfahren**" um die Installation des Treibers zu starten.

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 komfort** 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 komfort** benötigen Sie ein Anwendungsprogramm und eine RFID-Chipkarte bzw. den neuen elektronischen Personalausweis.

5 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 Virenscanner, 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 27).
- Folgen Sie den Anzeigen auf dem Display durch den Ablauf der sicheren PIN-Eingabe (dem sog. PIN-Dialog, siehe Kapitel Funktion Sichere PIN-Eingabe 9).

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 cyber***Jack***® **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.

6 Support

Hilfe bei Störungen

Bei Störungen, die sich nicht durch eine erneute Inbetriebnahme (siehe Kapitel 4) Ihres cyber***Jack***® **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 60 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 cyber***Jack***® **RFID** Chipkartenleser in Ihre Anwendungen integrieren wollen, können sich mit Fragen jederzeit gerne an support@reiner-sct.com wenden.

7 Technische Referenzen

7.1 LED-Funktionen

Leuchtdioden (LEDs)

Der cyber***Jack***® **RFID komfort** 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 kontaktlosen Signaturkarten; angezeigter Text ist authentisch.
blinkt gleichmäßig	leuchtet dauerhaft		Modus Sichere PIN-Eingabe bei der qualifizierten elektronischen Signatur mit kontaktbehafteten Signaturkarten; angezeigter Text ist authentisch.
blinkt gleichmäßig		leuchtet dauerhaft	Modus Sichere PIN-Eingabe bei der qualifizierten elektronischen Signatur mit kontaktlosen Signaturkarten; angezeigter Text ist authentisch.[1)]
blinkt gleichmäßig			Der cyber***Jack***® **RFID komfort** 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.

[1)] Nur V2.0; Bei V1.0 PIN-Eingabe mit kontaktloser Chipkarten; angezeigter Text ist authentisch.

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

7.2 Technische Einsatzumgebung

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

Kontaktbehaftete Chipkartenschnittstelle

Die cyber***Jack***® **RFID komfort** 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 cyber***Jack***® **RFID komfort** 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 28).

7.3 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 mit einer kontaktbehafteten oder kontaktlosen Chipkarte möglich. Um sicherzustellen, dass die PIN nicht im Chipkartenleser gespeichert wird, wurden spezielle Sicherheitsfunktionen im cyber***Jack***® **RFID komfort** implementiert und die Hard- und Software des Chipkartenlesers strengen sicherheitstechnischen
Evaluierungen unterzogen. Die nachfolgenden Sicherheitsfunktionen sind im cyber***Jack***® **RFID komfort** realisiert:

Applikationstrennung

Der cyber***Jack***® **RFID komfort** 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 5) mit neuen Modulen (Kernel, Applikation, Zertifikat) 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 cyber***Jack***® **RFID komfort** auf eine ältere Version ist nicht möglich.

Kommunikationstrennung

Nach Anstoßen des Modus ”Sichere PIN-Eingabe” durch eine Applikation unterbricht der cyber***Jack***® **RFID komfort** 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 cyber***Jack***® **RFID komfort** 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 dem 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 cyber***Jack***® **RFID komfort**, 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 cyber***Jack***® **RFID komfort** 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 cyber***Jack***® **RFID komfort** 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 cyber***Jack***® **RFID komfort** (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.

Secure Messaging

Die Kommunikation von sicherheitskritischen Daten (z.B. QES-PIN, PUK und Nutzdaten) über die kontaktlose Schnittstelle erfolgt stets in verschlüsselter Form (Secure Messaging) mit freigegebenen Verschlüsselungsverfahren und lässt einen Übertragungsfehler erkennen. Dabei wird Secure Messaging zwischen dem Chipkartenleser und der kontaktlosen Chipkarte ausgehandelt, um damit

sicherzustellen, dass kein Dritter die übertragenen Daten lesen kann.

Befehlsfilter

Der cyber***Jack***® **RFID komfort** 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.

Freigegebene Verschlüsselungsverfahren

Für die verschlüsselte Datenkommunikation und für den sicheren Download (Modulupdate) werden freigegebene Verschlüsselungsverfahren genutzt.

Als Zufallszahlengenerator wird eine AES-basierte Lösung verwendet. Der Generator entspricht damit der nach TR-03119 geforderten Klasse K3 gem. AIS 20 mit der Mechanismenstärke hoch.

Terminal – und Passive Authentisierung

Die Terminal- und Passiveauthentisierung für die nPA-QES erfolgt mit dem im Leser befindlichen zertifizierten Chip im Sicherheitsmodul sowie den Zertifikaten aus dem Zertifikatsspeicher. Die Identifikationsdaten des Chips (Passwort) werden manipulationssicher im Speicher des Chipkartenlesers gespeichert und im Rahmen der Initialisierung zur Authentisierung gegenüber dem Chip verwendet.

MPU-Regeln

Um sicherzustellen, dass die Firmware nicht in nicht verifizierten Code springt, sind MPU-Regeln (Zugriffsregeln für den Speicher) in den cyber***Jack***® **RFID komfort** implementiert. Das heißt der Chipkartenleser greift nie auf nicht von Reiner SCT zugelassenen Speicherbereich zu.

8 Konformitätserklärung

8.1 cyberJack RFID komfort

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

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

erklärt, in alleiniger Verantwortung, dass das Produkt:

cyber*Jack*® RFID komfort
(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten R&TTE-Richtlinie 1999/5/EG einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 09. März 1999 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach Schuhwerk-EMV-Labor-Nr.: 2011024

EN 301489-1 V1.8.1: 2008

RF nach Schuhwerk-EMV-Labor-Nr.: 2011025

EN 300 330-2: 2010, Frequenz 13.56 MHz

EN 60950-1: 2006

(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 ZN205105000000 archiviert*

Furtwangen, 17.07.2012
(Ort und Datum der Ausstellung)

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

REINER SCT PDM
PC-20510500-000-1 KFT
KONFORMITÄTSERKLÄRUNG cj_RFID_komfort

Index

- A -

- F -

- G -

- K -

- L -

- R -

- S -

- T -

REINER Kartengeräte GmbH & Co. KG

Goethestrasse 14
78120 Furtwangen
Germany
Telefon: +49 (7723) 5056-0
Telefax: +49 (7723) 5056-778
E-Mail: sales@reiner-sct.com
Internet: www.reiner-sct.com