SecCommerce
INFORMATIONSSYSTEME GMBH

SecCommerce GmbH

SecCardAdmin®

Anwenderhandbuch

Version 3.4
12.02.13

Autoren:
uhl, hl, tk

Dokumentenhistorie

Datum	Version	Inhalt / Änderung	Autor
16.04.03	3.0	Aktualisierung	uhl
27.02.08	3.1	2048-bit-Signaturkarten, Menüführung	hl
27.03.08	3.2	MS JVM obsolet	hl
17.09.09	3.3	PIN-Entsperrung	tk
12/02/13	3.4	PIN2	hl

Inhaltsverzeichnis

1 Einführung

SecCardAdmin® ist ein in Java entwickeltes Produkt zur administrativen Verwaltung von Signaturkarten. Mit der Anwendung kann die initiale PIN der Signaturkarte gesetzt (Null-Pin-Verfahren) oder geändert werden (Transport-PIN-Verfahren, PIN-Brief) und somit die Signaturkarte für den weiteren Einsatz ‚freigeschaltet' werden. Des weiteren kann die bestehende PIN geändert werden. Die auf der Signaturkarte gespeicherten Zertifikate können ausgelesen, angesehen und gespeichert werden. Die SecCardAdmin-Anwendung kann insbesondere in Internetportalen eingesetzt werden und wird in eine HTML-Seite eingebettet, die der Nutzer über eine URL aufruft. Es ist seitens des Anwenders kein manueller Installationsaufwand für die SecCardAdmin® -Anwendung notwendig, da die Anwendung im Browser und installierten SUN Java-Plugin ausgeführt wird.

Eigenschaften:

- Freischaltung der Signaturkarte (Setzen der ersten PIN):
  - Null-PIN-Verfahren,
  - Transport-PIN-Verfahren (PIN-Brief)
- Änderung der PIN
- Auslesen, Anzeigen, Speichern der Zertifikate
- Automatische Kartenlesererkennung
- Automatische Signaturkartenerkennung

1.1 Systemvoraussetzungen Hardware

Eine aktuelle Übersicht aller unterstützter Hard- und Software findet sich im Internet unter:

www.seccommerce.de → Produkte → Unterstützte Hard- und Software

1.2 Systemvoraussetzungen Software

Systemvoraussetzungen:
Betriebssystem: Microsoft Windows

- Microsoft Windows XP, Vista, 7, 8
- Linux
- Mac OS X

Andere Betriebssysteme auf Anfrage.

Internet-Browser in Verbindung mit einem Orcale Java-Plugin in einer vom Hersteller unterstützen Version.

SecCommerce empfiehlt den Einsatz eines Kartenlesers mit sicherer PIN-Eingabe.
Ein für den Browser konfigurierter HTTP-Proxy, wie er in Firmennetzwerken häufig Verwendung findet, wird von SecCardAdmin in der Regel erkannt und für die Kommunikation mit Trustcentern (OCSP) verwendet.

Ist für den Web-Browser keine Java-VM installiert, ist der Download und die Installation des Orcale Java-Plugins für den Web-Browser erforderlich:

Anwendungsvoraussetzungen:
Der Anwender muss dem signierten SecCardAdmin-Applet die erweiterten Rechte zum Zugriff auf den lokalen Rechner des Anwenders beim Start zubilligen, da ansonsten ein Zugriff auf den Kartenleser nicht möglich ist. Es sind Schreibrechte im Nutzerverzeichnis **user.home** (Java-Umgebungsvariable) notwendig.
Es werden zur Ausführung der Anwendung Dateien automatisch im Verzeichnis **<user.home>/.seccommerce** gespeichert, die auch nach Beenden der Anwendung erhalten bleiben. Diese dienen dem Zugriff vom SecCardAdmin-Applet auf den Treiber des Kartenlesers bzw. auf die serielle Schnittstelle.

Unterstützte Hardware-Komponenten:
www.seccommerce.de → Produkte → Unterstützte Hard- und Software

Weitere Kartenleser können von SecCommerce optional über die CTAPI-Schnittstelle angebunden werden (Option). Die sichere PIN-Eingabe wird nicht von allen Kartenlesern unterstützt. In Verbindung mit der T-TeleSec-Signaturkarte ist eine sichere PIN-Eingabe beim Ändern der Null-PIN aus technischen Gründen nicht möglich. In diesem Fall kann die erste PIN (Ändern der Null-PIN) über den Dialog und die Tastatur des PCs eingegeben werden. Danach ist es möglich, mit sicherer PIN-Eingabe über die Tastatur des Kartenlesers die PIN nochmals zu ändern.

Einige Signaturkarten unterstützen das getrennte Ändern der PINs zu den auf der Signaturkarte enthaltenen unterschiedlichen Schlüsseln. Es liegt in der Verantwortung des Anwenders, diese nach seinen Bedürfnissen zu setzen (und zu merken). Die SecCardAdmin-Anwendung unterstützt in diesem Falle das getrennte Setzen und Ändern der PINs. Bei wiederholter Fehleingabe der PIN kann die Signaturkarte zerstört werden (Sicherheitsmerkmal der Signaturkarte).

2 Sicherheitshinweise

Für die sichere Nutzung des SecCardAdmin sind grundsätzlich allgemeine Sicherheitsempfehlungen zu beachten:

www.bsi-fuer-buerger.de

Beachten Sie bitte auch folgendes:

- Durch einen eventuellen Virenbefall eines Microsoft Windows-Anwendersystems können Tastatureingaben und somit auch die geheime PIN ausgespäht werden. Ein Kartenleser mit integrierter PIN- Eingabe macht das unmöglich. Bei sicherheitskritischen Dokumenten sollte daher immer ein Leser dieser Bauart verwendet werden.
- Beachten Sie bitte unbedingt die Benutzungshinweise Ihres Trustcenters zur Nutzung Ihrer Signaturkarte.
- Lassen Sie die Signaturkarte nicht offen herumliegen.
- Ändern Sie die PIN Ihrer Signaturkarte regelmäßig, insbesondere wenn Sie befürchten, dass jemand unberechtigter weise die PIN erfahren hat.
- Wählen Sie eine PIN, die sich nur schwer erraten lässt. Ein Dieb hat drei Versuche, nach mehrmaliger Falscheingabe wird Ihre Signaturkarte automatisch unbrauchbar.
- Teilen Sie die PIN Ihrer Signaturkarte niemandem mit, auch nicht auf Verlangen unserer „Mitarbeiter“.
- Notieren Sie die PIN nicht, insbesondere nicht auf der Signaturkarte!
- Melden Sie den Verlust Ihrer Signaturkarten sofort der kartenausgebenden Stelle (Ihrem Trustcenter) und lassen Sie die Karte sperren. Damit sind Signaturen, die nach der Sperrung erfolgen nicht mehr rechtsverbindlich.
- Bei ungültiger PIN oder abgelaufener Signaturkarte wenden Sie sich bitte an den Herausgeber oder Provider der Karte (Ihr Trustcenter).
- Darüber hinaus sind die Sicherheitseinstellungen des verwendeten Internet-Browsers zu überprüfen und gegebenenfalls gemäß den nachfolgenden Anweisungen einzurichten. Bei Fragen zur Realisierung der Einstellungen ist die Dokumentation des verwendeten Internet-Browsers zu Rate zu ziehen.

2.1 Sicherheitseinstellungen des Browsers

- Vor dem Laden des SecCardAdmin ist der Cache des Internet-Browsers zu löschen.
- Es ist einzustellen, dass immer die aktuelle Seite geladen wird, auch wenn sich im Cache bereits eine entsprechende Seite befindet.
- Der Dialog zur Anforderung zusätzlicher Rechte durch Java-Applets darf nicht deaktiviert sein.
- Das Ausführen von Java muss aktiviert sein.
- Wird ein Proxy-Server verwendet und soll dieser automatisch erkannt werden, so ist das Ausführen von JavaScript zu gestatten.

3 SecCardAdmin verwenden

3.1 Anschluss des Kartenlesers

Beachten Sie bitte die Installationshinweise vom Hersteller Ihres Kartenlesers. Bitte stecken und ziehen Sie Kabel des Kartenlesers nur am ausgeschalteten Rechner, um Schäden an Ihrem PC zu vermeiden.
Falls Sie einen Kartenleser an der seriellen Schnittstelle anschließen, achten Sie bitte darauf, das auch der zweite Stecker (PS2) angeschlossen wird. Dieser wird meistens zwischen das Tastaturkabel und Ihren PC gesteckt und versorgt den Kartenleser mit Strom. Ohne Anschluss dieses zweiten Steckers ist ein Betrieb des Kartenlesers nicht möglich.

3.2 Start der Anwendung

Die Anwendung starten Sie über einen Link:

www.seccommerce.de → SecCardAdmin

Für die Nutzung des Programms ist es erforderlich, dass Sie für Ihren Browser ein SUN-Java-Plugin installiert haben. Sollte die Anwendung nicht starten und Sie folgenden Hinweis bekommen,

Abbildung 1: Fehlende Java-Unterstützung des Browsers

dann schalten Sie bitte die Java-Unterstützung für Ihren Browser ein.

3.2.1 Zugriffsrechte

Für die Ausführung der Anwendung werden zusätzliche Rechte für den Zugriff auf die Festplatte und den Kartenleser angefordert. Bitte bestätigen Sie die Frage nach der Anforderung der Rechte stets mit 'Ja', da Sie ansonsten die Anwendung nicht ausführen können. Die Dialoge für die Rechteanforderung können wie folgt aussehen:


Sicherheitswarnung
Installieren und Ausführen von
"Signaturkartenadministrationsanwendung SecCardAdmin 3.0.0 (Java-Applet)", signiert am 07.04.2004 13:29 und herausgegeben von:
SecCommerce Informationssysteme GmbH
Authentizität des Herausgebers bestätigt durch Thawte Server CA
Hinweis: SecCommerce Informationssysteme GmbH versichert, dass dieser Inhalt sicher ist. Die Installation bzw. das Anzeigen des Inhalts sollte nur erfolgen, wenn Sie SecCommerce Informationssysteme GmbH vertrauen.
Zugelassene Signatur
Volle Zugriffsrechte
Inhalt von SecCommerce Informationssysteme GmbH immer vertrauen
Ja
Nein
Weitere Informationen

3.3 Hauptmenü

Nach erfolgreichen Start wird folgender Dialog angezeigt:

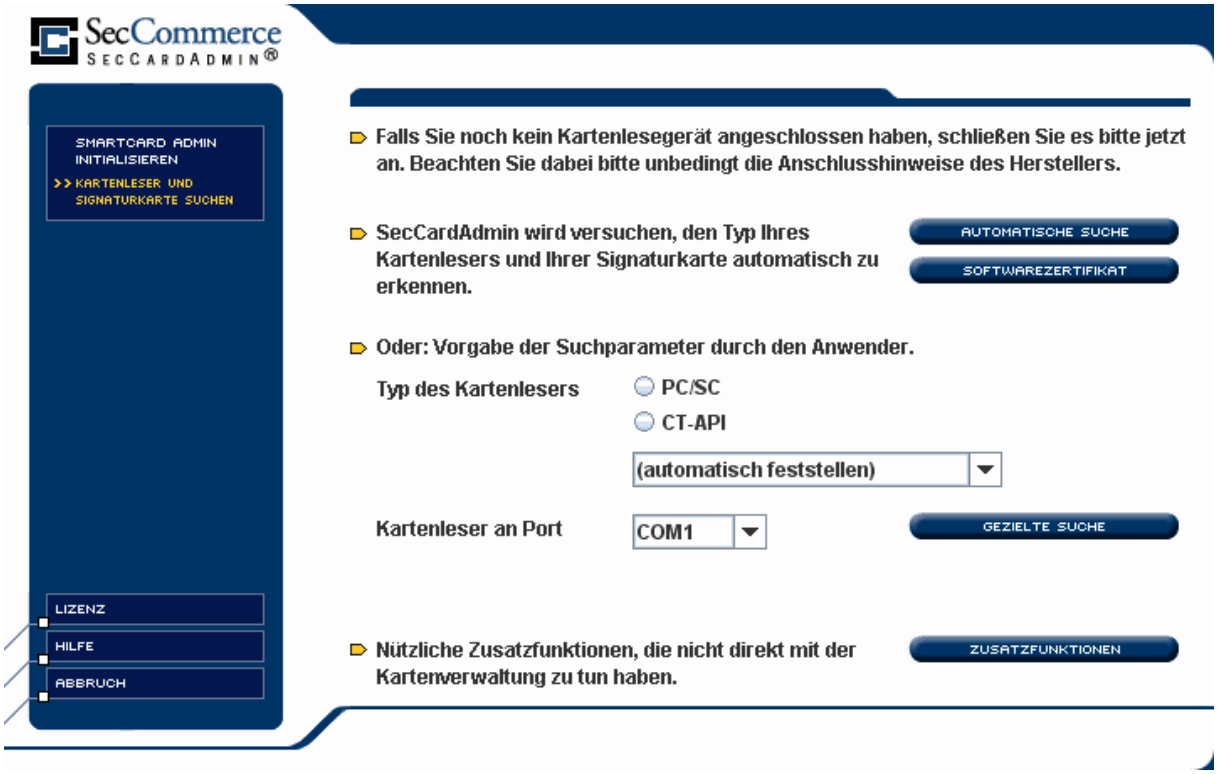

Abbildung 2: Hauptmenü

3.3.1 Kartenleser und Signaturkarte suchen

Sie haben die Wahl, ob Ihr Kartenleser automatisch gesucht und erkannt werden soll oder ob Sie gezielt suchen möchten. In den meisten Fällen führt eine automatische Suche zum Erfolg, nur für Problemfälle wählen Sie bitte 'Gezielte Suche'.

Legen Sie Ihre Signaturkarte in den Kartenleser und wählen Sie 'Automatische Suche'.

Die erforderlichen Programme zum Zugriff auf den Kartenleser werden in Ihrem Verzeichnis **<user.home>/.seccommerce** gespeichert, das ist (unter Windows) meistens eine Pfadangabe wie

```
C:\Dokumente und Einstellungen\[IhrName]\.seccommerce
```

Auf dieses Verzeichnis müssen Sie Rechte für den schreibenden Zugriff haben. Bitte verständigen Sie andernfalls Ihren Systemadministrator.Im Initialisierungsdialog wird Ihnen der Fortschritt der Installation der erforderlichen Treiber angezeigt und es wird der Kartenleser an Ihrem PC gesucht. Falls Sie ein Problem bei der Erkennung des Kartenlesers haben, prüfen Sie bitte, ob dieser korrekt installiert ist und auch die Treiber des Herstellers richtig installiert sind. Falls Ihr Kartenleser nach einer Treiber-Neuinstallation nicht gefunden wird, beachten Sie bitte die Hinweise im Handbuch des Herstellers des Kartenlesers. Viele Hersteller bieten auch Zusatzprogramme und Online-Hilfen an, um Probleme beim Anschluss des Kartenlesers zu erkennen.

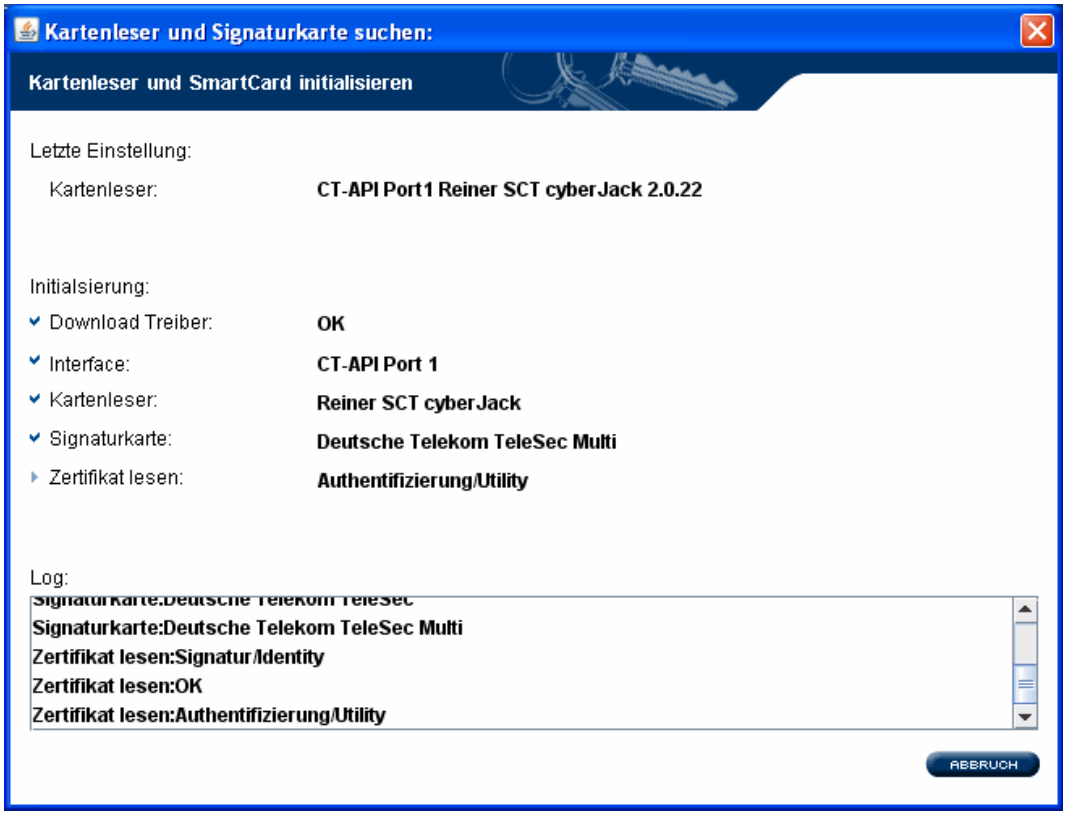

Abbildung 3: Karte suchen

Nach erfolgreicher Erkennung des Kartenlesers und der Signaturkarte gelangen Sie in das Menü 'Kartenverwaltung' (vgl. 3.4) der Anwendung.

3.3.2 Softwarezertifikat

Neben Signaturkarten werden auch Softwareschlüssel (PKCS#8 und PCKS#12) unterstützt. Rufen Sie dazu im Hauptmenü (vgl. 3.3) den Menüpunkt 'Softwarezertifikat' auf und wählen Sie Schlüssel und (für PKCS#8) Zertifikat aus dem Dateisystem aus:

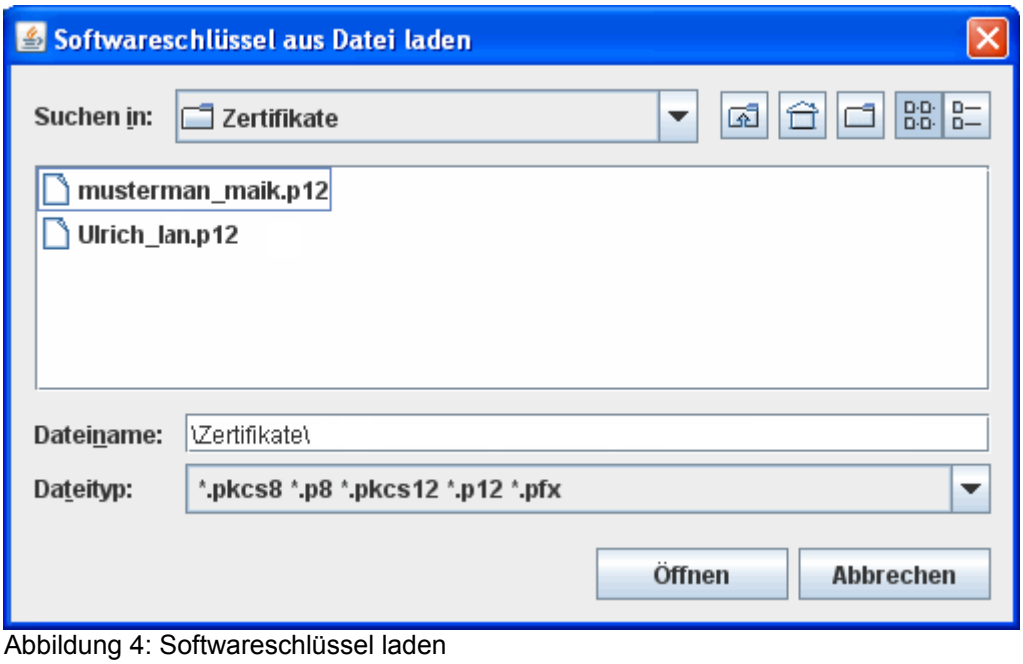

Abbildung 4: Softwareschlüssel laden

Geben Sie dann Ihr Passwort für den Schlüssel ein und wählen Sie die Option 'Weiter':

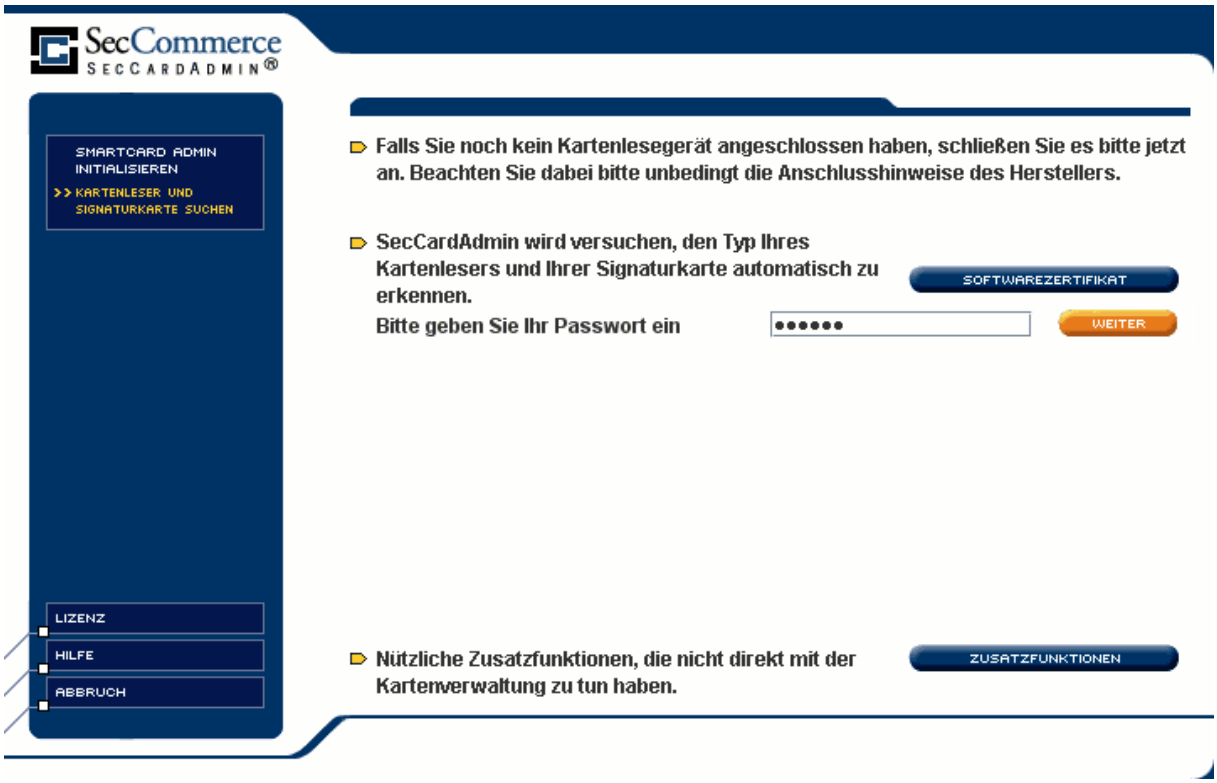

Abbildung 5: Passworteingabe

Anschließend können Sie Ihre Zertifikate verwalten (vgl. 3.7) oder Ihre PIN ändern (vgl. 3.6).

3.3.3 Zusatzfunktionen

Hier finden Sie weitere nützliche Funktionen, wie z.B. die Ansicht von DER-codierten Zertifikaten, die als Datei vorliegen und die Entschlüsselung von Attributzertifikaten (vgl. 3.7.5):

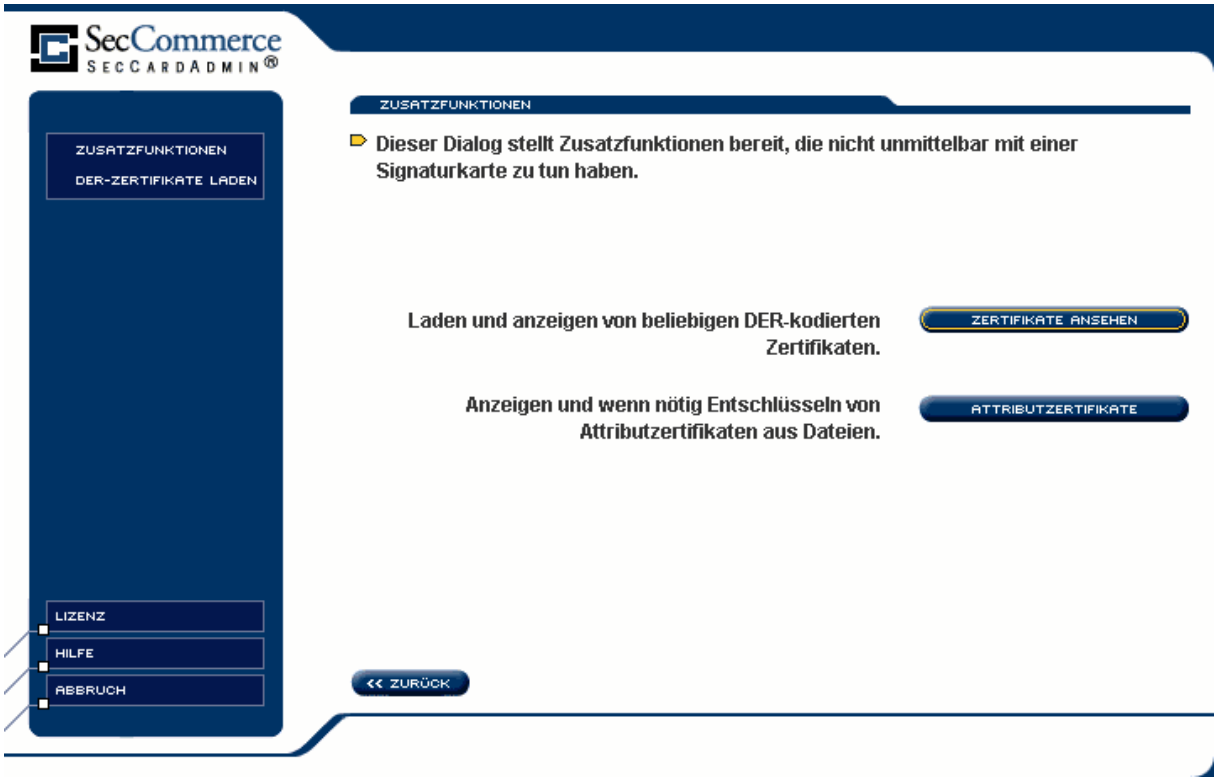

Abbildung 6: Anzeige von Zertifikaten aus dem Dateisystem

3.4 Kartenverwaltung

Abbildung 7: Menü: Kartenverwaltung

Im Hauptmenü haben Sie folgende Möglichkeiten, Ihre Signaturkarte zu administrieren:

- **Zertifikatverwaltung**
  zum Ansehen, Speichern und Prüfen der Zertifikate auf Ihrer Signaturkarte
- **Freischaltung**
  Zur Freischaltung der Signaturkarte nach Erhalt vom Trustcenter. Dies erfordert ggfs. die Eingabe der Transport-PIN
- **PIN ändern**
  Hier können Sie Ihre bestehende(n) PIN(s) der Signaturkarte ändern

Um eine Signaturkarte in Betrieb nehmen zu können, werden verschiedene Verfahren von den Trustcentern angewendet. Ziel ist es, dass sie nach Erhalt der Signaturkarte Ihre persönliche PIN selbst aussuchen und setzen und in regelmäßigen Abständen ändern können.

Manche Signaturkarten verlangen eine bestimmte PIN-Länge, bitte beachten Sie die Hinweise Ihres Trustcenters.

Für die Auslieferung von Signaturkarten und die Inbetriebnahme gibt es verschiedene Verfahren:

- **Null-PIN-Verfahren der T-TeleSec**
  Es wird keine PIN mit ausgeliefert. Die Karte ist durch eine Null-PIN gesichert, die Sie nach Erhalt zuerst ändern müssen, um mit der Karte signieren zu können.
- **Transport-PIN-Verfahren mit PIN-Brief:**
  Ihre Karte ist durch eine Transport-PIN gesichert, die Ihnen in einem PIN-Brief

mitgeteilt wird. Mit der Transport-PIN kann keine Signatur abgegeben werden, Sie müssen die Transport-PIN durch eine eigene PIN ändern.

- **Transport-PIN-Verfahren D-TRUST:**
  Die Transport-PIN Ihrer Signaturkarte kann von der Karte gelesen werden. Bei der Freischaltung der Karte wird die Transport-PIN von SecCardAdmin ausgelesen und bereitgestellt.

Bitte beachten Sie die Hinweise Ihres Trustcenters, welches Verfahren zum Einsatz kommt. **Sie müssen zuerst die Karte freischalten und eine eigene PIN setzen, bevor Sie Ihre Karte zum Signieren nutzen können oder die PIN** über den Menüpunkt '**PIN ändern**' **ändern können**.

3.5 Freischaltung

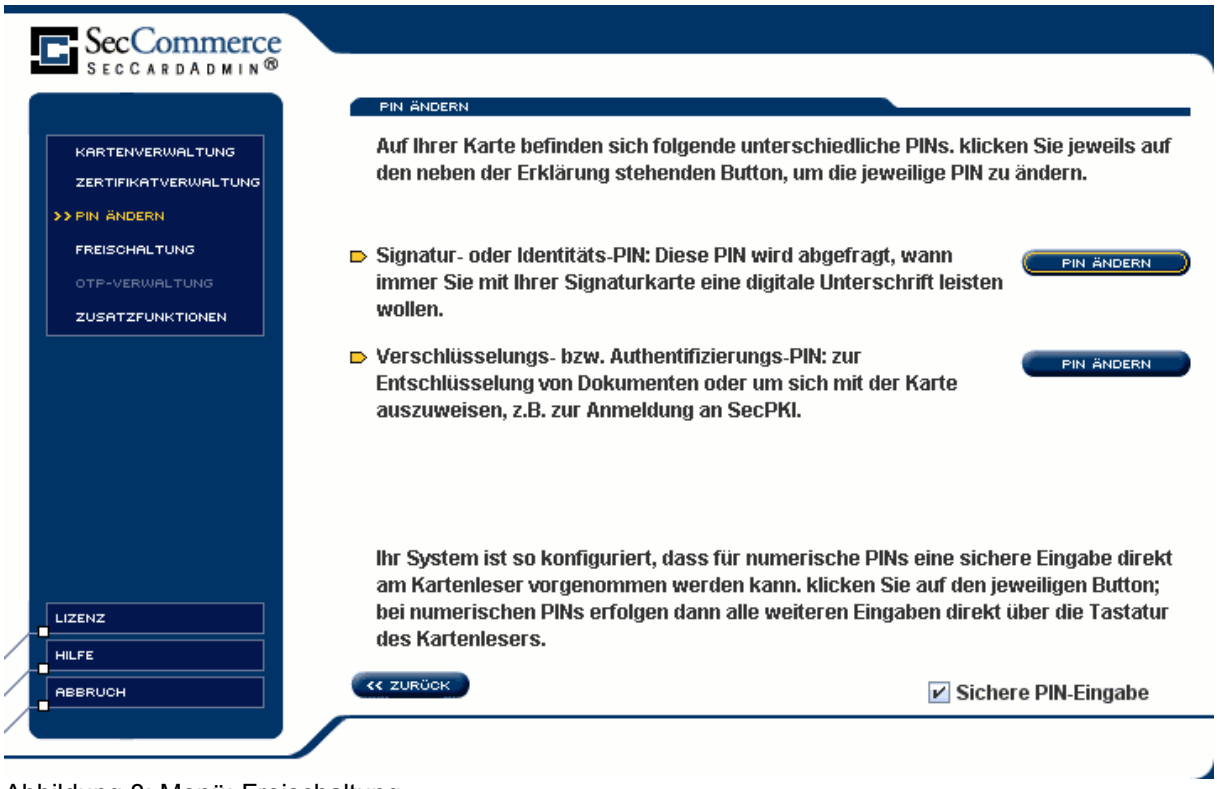

Abbildung 8: Menü: Freischaltung

Hinweis:
Auf der Signaturkarte befinden sich möglicherweise mehrere PINs. Jede PIN muss vor der Nutzung gesetzt werden. Es ist möglich, für verschiedene PINs jeweils den gleichen Wert zu setzen.

3.5.1 Freischaltung TeleSec-Signaturkarte

Für die T-TeleSec-Karte wird das Null-PIN-Verfahren angewendet, Sie brauchen keine Transport-PIN eingeben. Im Null-PIN-Verfahren ist die Eingabe der neuen PIN an der Tastatur des Kartenlesers bei Freischaltung der Karte aus technischen Gründen nicht möglich. Erst bei der PIN-Änderung können Sie die Tastatur des Kartenlesers verwenden. (s.o.)

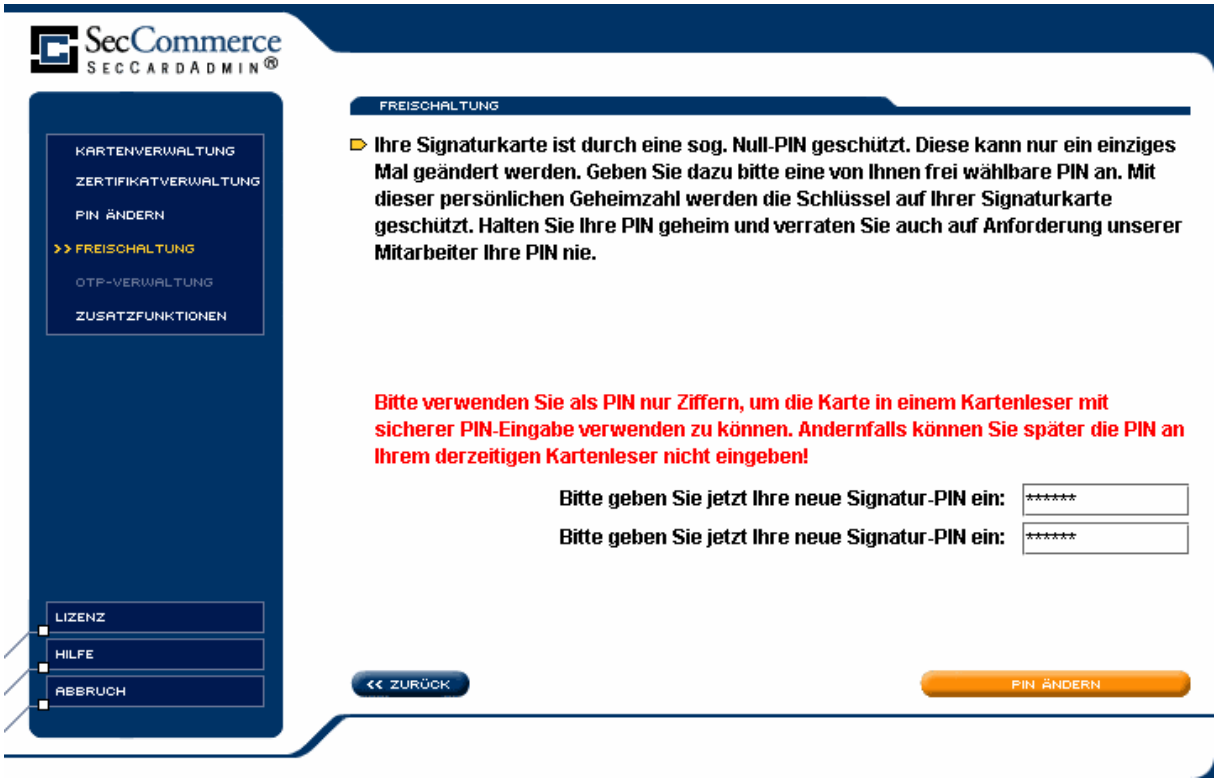

Abbildung 9: Freischaltung: T-TeleSec-Karte

Bitte geben Sie Ihre neue PIN zweimal ein und wählen Sie 'PIN ändern'.

TeleSec-Signaturkarten mit ECC-Verschlüsselung erlauben zudem die Vergabe einer PIN2, mit der später eine durch mehrfache Fehleingabe gesperrte PIN wieder entsperrt werden kann. Sie können die PIN2 im entsprechenden Dialog setzen (vgl. Abschnitt).

3.5.2 Freischaltung Signaturkarten mit Transport-PIN

Sie können zunächst wählen, ob Sie die sichere PIN-Eingabe am Kartenleser verwenden möchten:

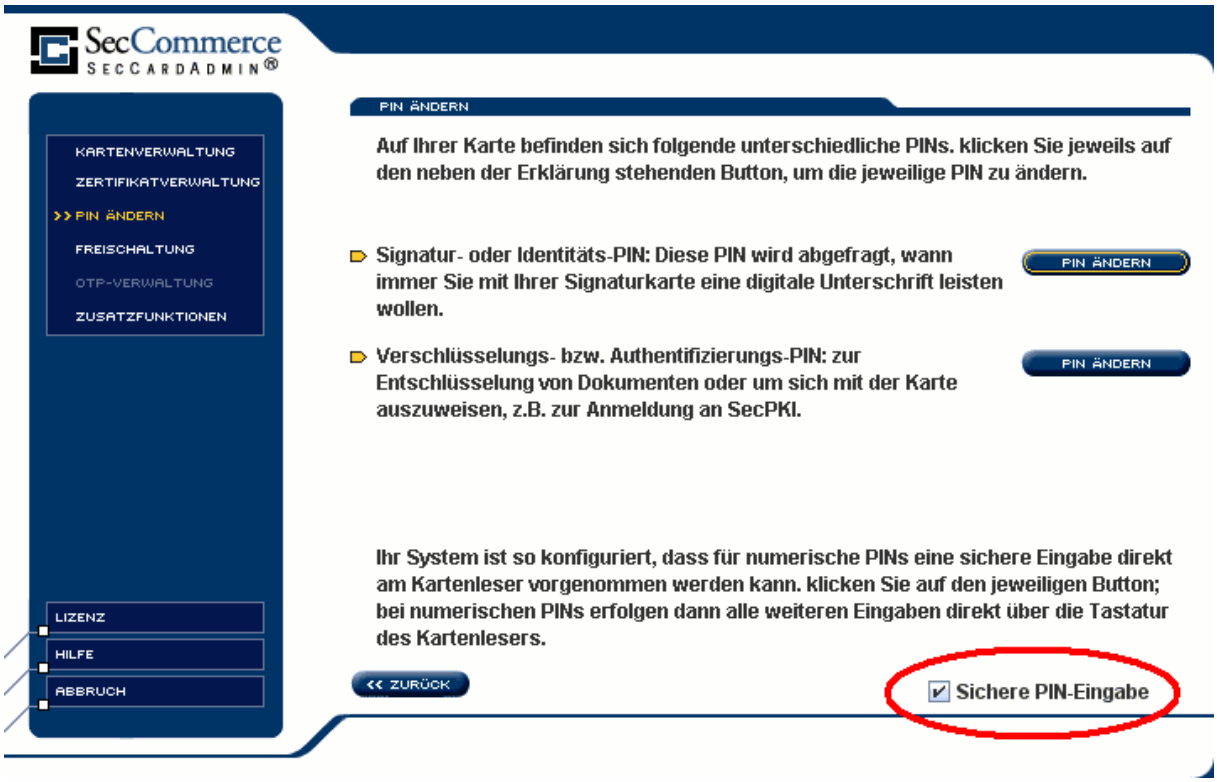

Abbildung 10: Freischaltung: Karten mit Transport-PIN

3.5.2.1 Freischaltung: Sichere PIN-Eingabe

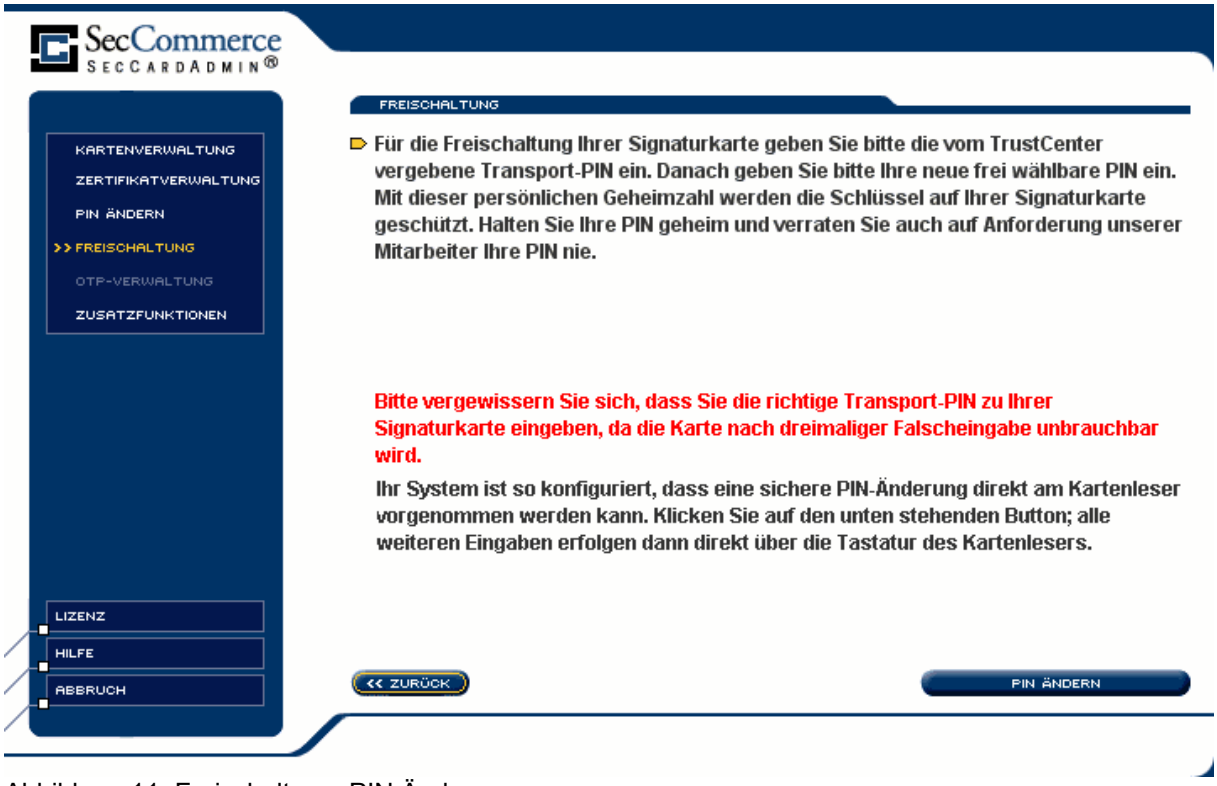

Abbildung 11: Freischaltung: PIN Ändern

Wählen Sie 'PIN ändern' und geben Sie die die im PIN-Brief abgedruckte Transport-PIN, Ihre neue PIN und erneut die neue PIN am Kartenleser ein.

Sie bekommen zunächst einen Hinweis zum Verfahren:

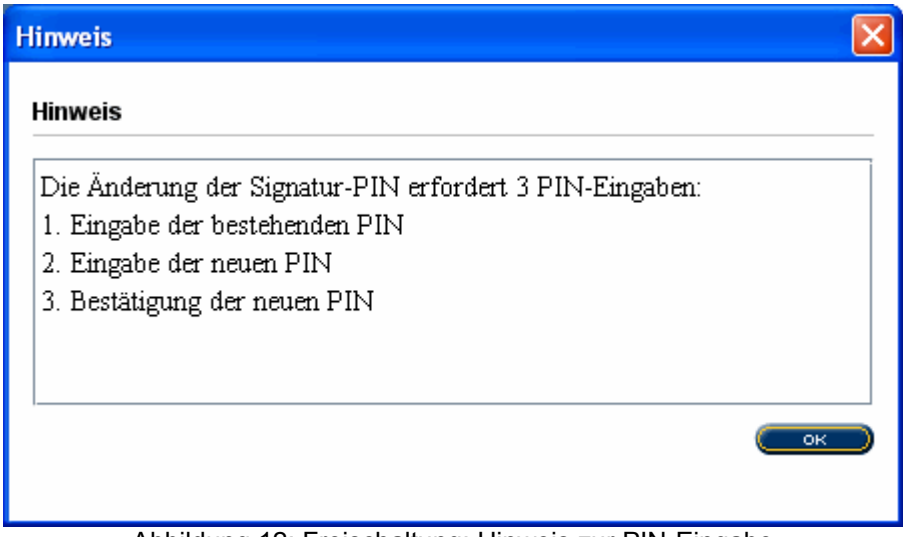

Abbildung 12: Freischaltung: Hinweis zur PIN-Eingabe

Bestätigen Sie den Hinweis und geben Sie in der geforderten Weise die PINs am Kartenleser ein.
Sie erhalten im Erfolgsfall eine Meldung, dass Ihre neue PIN gesetzt wurde.

3.5.2.2 Freischaltung: PIN-Eingabe über das Keyboard

Wenn Sie die sichere PIN-Eingabe am Kartenleser nicht verwenden möchten (vgl. Abbildung 10: Freischaltung: Karten mit Transport-PIN) die PIN-Eingabe alternativ über das Keyboard.

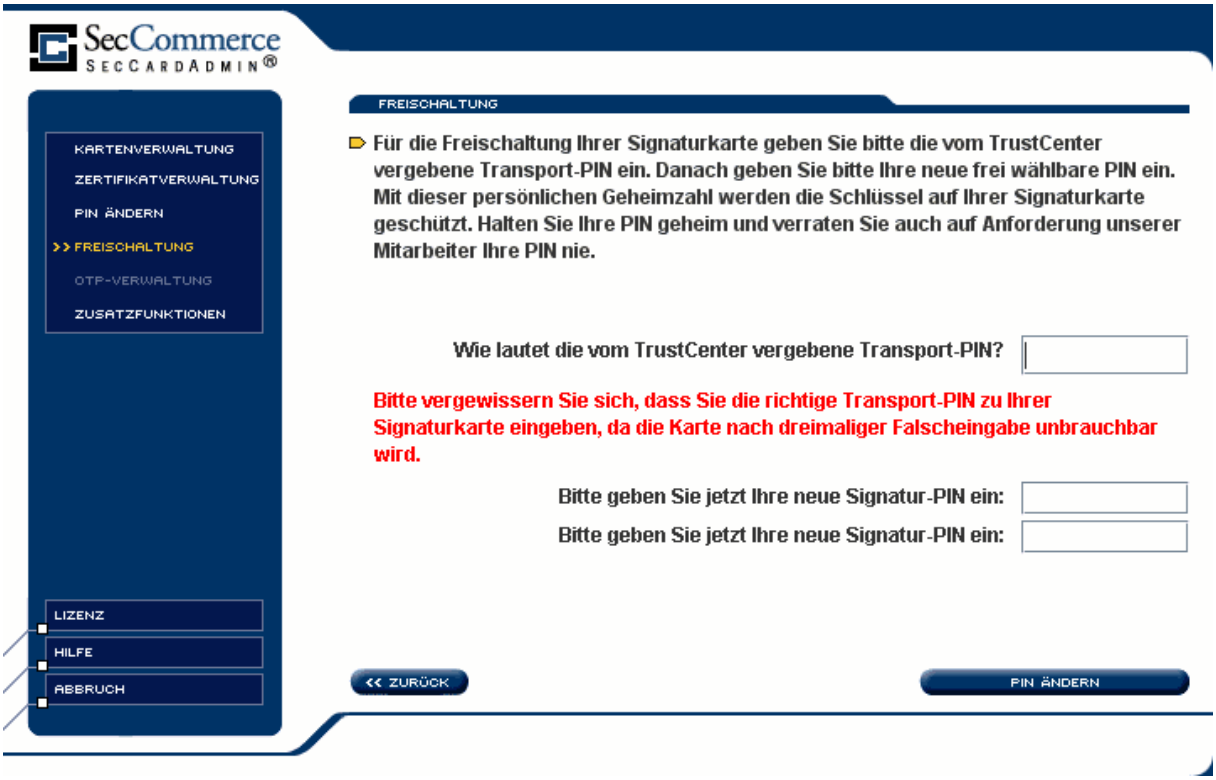

Abbildung 13: Freischaltung: PIN-Eingabe am Keyboard

Wählen Sie nach der Eingabe der PINs den Menüpunkt 'PIN ändern'. Sie erhalten im Erfolgsfall eine Meldung, dass Ihre neue PIN gesetzt wurde.

3.6 PIN ändern

Sie können die PIN Ihrer Karte erst ändern, wenn die Transport-PIN geändert ist (Freischaltung). Bitte beachten Sie die Hinweise Ihres Trustcenters, welches Verfahren angewendet wird. Es ist ggf. vor der ersten Nutzung der Karte und vor der normalen PIN-Änderung eine **Transport-PIN-Änderung** notwendig, **die nicht mit diesem Dialog durchgeführt werden kann!**

Falls Sie Ihre Signaturkarte bereits für Signaturen eingesetzt haben oder diese freigeschaltet haben, können Sie hier die bestehende PIN ändern. Bitte wählen Sie aus, welche PIN Sie ändern möchten und drücken Sie 'PIN ändern'. Je nach Kartenleserart werden Sie aufgefordert, Ihre alte und neue PIN entweder im Dialog oder über die Tastatur des Kartenlesers einzugeben. Sie sollten eine PIN aus Ziffern wählen, um auch mit Kartenlesern mit sicherer PIN-Eingabe arbeiten zu können. Beachten Sie bei der Wahl der PIN die Sicherheitshinweise Ihres Trustcenters.

Manche Signaturkarten verlangen eine bestimmte PIN-Länge, bitte beachten Sie die Hinweise Ihres Trustcenters.

Sie können zunächst wählen, ob Sie die sichere PIN-Eingabe am Kartenleser verwenden möchten:

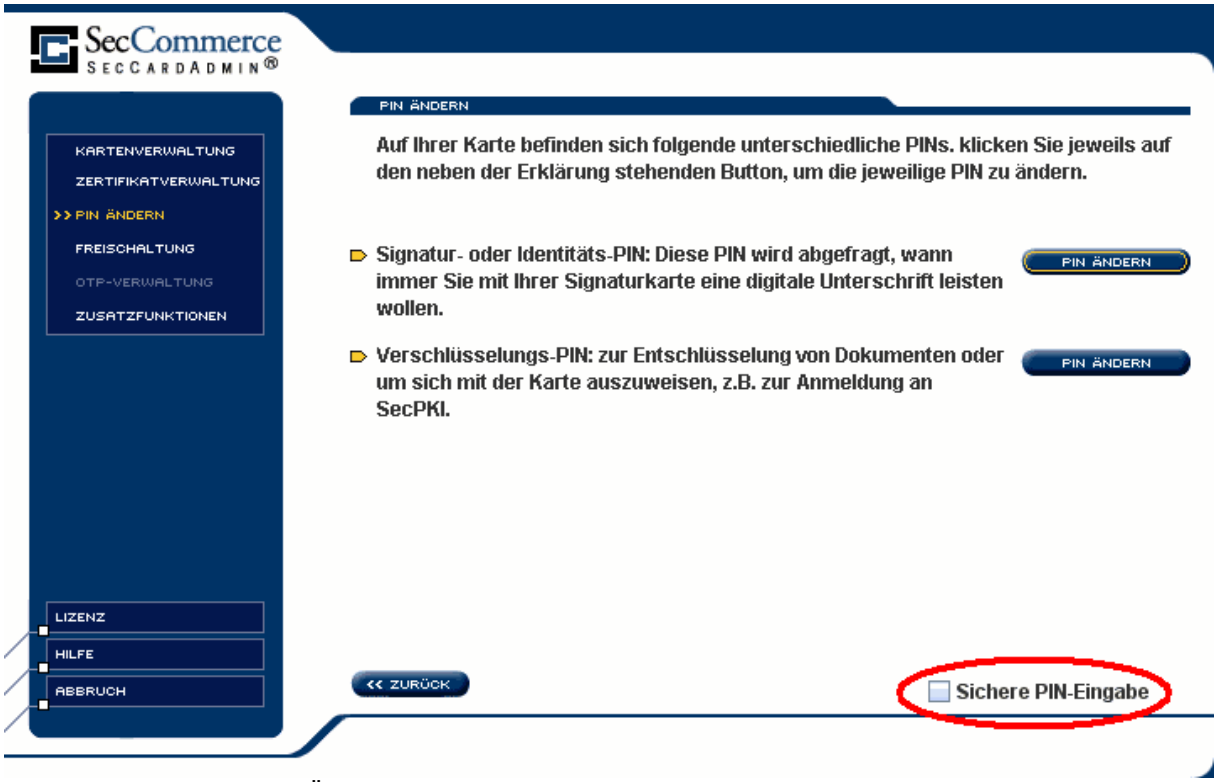

Abbildung 14: Menü: PIN Ändern

3.6.1.1 Sichere PIN-Eingabe an Kartenleser

Sie bekommen zunächst einen Hinweis zum Verfahren:

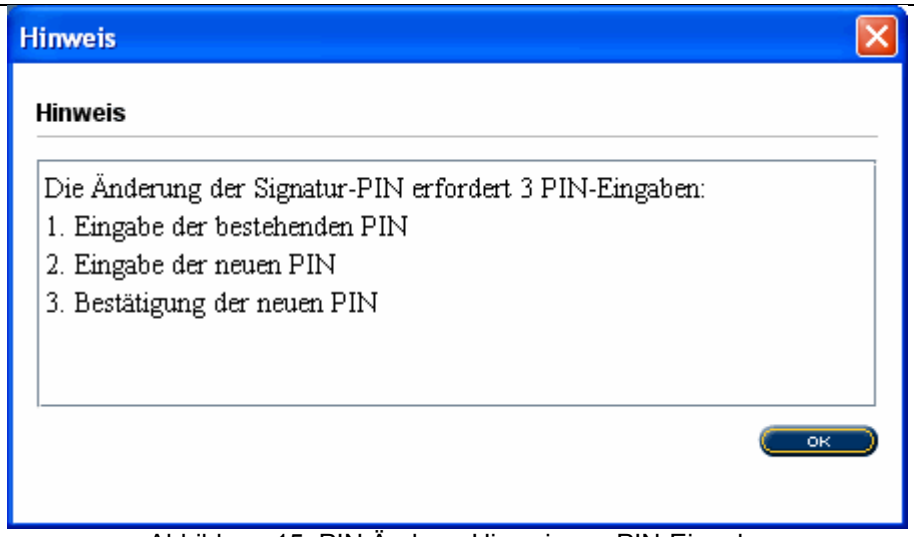

Abbildung 15: PIN Ändern: Hinweis zur PIN-Eingabe

Bestätigen Sie den Hinweis und geben Sie in der geforderten Weise die PINs am Kartenleser ein.

Sie erhalten im Erfolgsfall eine Meldung, dass Ihre PIN geändert wurde.

3.6.1.2 PIN-Eingabe am Keyboard

Wenn Sie die sichere PIN-Eingabe am Kartenleser nicht verwenden möchten (vgl. Abbildung 14: Menü: PIN Ändern) die PIN-Eingabe alternativ über das Keyboard.

Abbildung 16: PIN Ändern: PIN-Eingabe über das Keyboard

Geben Sie in der geforderten Weise die PINs ein und wählen Sie dann 'PIN ändern'.
Sie erhalten im Erfolgsfall eine Meldung, dass Ihre PIN geändert wurde.

Falls sich Ihre PIN nicht ändern lässt, kann das folgende Ursachen haben:

- Bei der Eingabe über die normale Tastatur wurde die Feststelltaste (Caps-Lock oder Num-Lock) versehentlich gedrückt. Bitte prüfen Sie das und stellen dieser Einstellung wieder aus.
- Ihre alte PIN war nicht korrekt. Versuchen Sie es ein zweites Mal. Wenn es jetzt nicht funktioniert, kann Ihre alte PIN mit diesem Programm nicht geändert werden oder es war die falsche PIN. Bitte versuchen Sie jetzt auf keinen Fall weitere Male die PIN zu ändern, da die PIN bei mehrfacher Fehleingabe gesperrt wird wird.

3.7 Zertifikatverwaltung

Abbildung 17: Menü: Zertifikatverwaltung

Mit der Zertifikatverwaltung können Sie bei Interesse die Zertifikate auf Ihrer Signaturkarte im Detail ansehen. Zertifikate sind digitale Ausweise und bescheinigen Ihre Identität, die durch ein Trustcenter durch eine elektronische Signatur Ihres Zertifikats beglaubigt wurde.

3.7.1 Details

Über die Schaltfläche 'Details' können Sie alle Angaben, die in Ihrem Zertifikat stehen im Detail ansehen und bei Bedarf auch in einer Datei speichern. Bei Fragen zum Inhalt Ihres Zertifikats lesen Sie bitte die entsprechende Zertifikat-Politik-Aussage (Certificate Policy Statement) Ihres Trustcenters oder wenden sich an Ihr Trustcenter.

Im Menü 'Details' können Sie das Zertifikat als Datei 'speichern' (DER-codiert).

3.7.2 Signaturzertifikat prüfen

Über die Schaltfläche 'Prüfen' können Sie den Zertifikatstatus Ihres Signaturzertifikats beim Trustcenter online abfragen, wenn dieser Dienst von Trustcenter angeboten und von Ihrem PC aus erreichbar ist. Sie benötigen hierfür eine Internetverbindung.

Bevor Sie Ihre Signaturkarte zum Signieren benutzen können, müssen Sie sicherstellen, dass die Zertifikate der Signaturkarte vom Trustcenter in den Verzeichnisdienst übernommen worden sind. Voraussetzung hierfür ist, dass Sie die Bestätigung über den Erhalt der Signaturkarte entsprechend der Vorgabe des Trustcenters unterschrieben per Post an dieses geschickt haben. Die Bearbeitung erfolgt in der Regel innerhalb weniger Arbeitstage; danach sollte Ihr Zertifikat in den Verzeichnisdienst übernommen worden sein.

Das Signaturzertifikat kann folgende Status mit folgender Bedeutung haben:

Status	**Bedeutung**
good	Sie können die Signaturkarte zum Signieren einsetzen
unknown	Die Zertifikate sind noch nicht im Verzeichnisdienst aufgenommen. Sie dürfen die Signaturkarte noch **nicht** zum Signieren einsetzen. Bitte bestätigen Sie den Erhalt der Signaturkarte schriftlich der T-TeleSec.
revoked	Ihr Zertifikat ist im Verzeichnisdienst gesperrt. Sie dürfen die Signaturkarte **nicht** mehr zum Signieren einsetzen.
Nicht feststellbar	Der Status des Zertifikats konnte nicht festgestellt werden. Bitte prüfen Sie, ob Sie eine Internetverbindung zum Trustcenter aufbauen konnten. Fragen Sie ggf. Ihren Systemadministrator.

Sollte Ihr Zertifikatstatus trotz Absendung des Bestätigungsschreibens nach einer angemessenen Frist immer noch „unknown“ sein, verständigen Sie bitte Ihr Trustcenter.

3.7.3 Zertifikate installieren

Bestimmte Signaturkarten erlauben die Installation weiterer Zertifikate auf der Karte. Dazu dient der Menüpunkt 'Zertifikate installieren'.

3.7.4 Zertifikate in 'secSignerCertStore.txt' speichern

Sie können alle Zertifikate auf Ihrer Karte Base64-codiert in einer Textdatei sichern. Bitte wählen Sie dazu den entsprechenden Menüpunkt in der Kartenverwaltung.

3.7.5 Entschlüsseln des T-TeleSec Attributzertifikats

Die TeleSec bietet Attributzertifikate (z.B. zur Selbstbeschränkung) an, die ihnen per E-Mail oder per Datenträger zugesandt werden und vor der ersten Verwendung entschlüsselt werden müssen. Zur Entschlüsselung benötigen Sie Ihr Telepasswort (siehe Antragsformular).

Haben Sie von der TeleSec Ihr Attributzertifikat per E-Mail verschlüsselt zugeschickt bekommen, so kopieren Sie den Anhang der E-Mail, das verschlüsselte Zertifikat, in Ihre Dateisystem. Als Dateiendung soll dabei "`.cry`" gewählt werden. Es ist empfehlenswert, diese Datei zusätzlich auf einem Datenträger zu sichern.

Wählen Sie den Menüpunkt 'Attributzertifikat' und lesen Sie die "`.cry`"-Datei aus dem Dateisystem ein (Menüpunkt 'Attributzertifikat lesen') und geben Ihr Telepasswort ein.

Abbildung 18: Entschlüsselung Attributzertifikat

Wählen Sie dann ". Wenn das Passwort und die Entschlüsselung korrekt abgelaufen sind, können Sie das entschlüsselte Attributzertifikat im gewünschten Verzeichnis ihr sichern (Datei mit Endung "`.atz`").

3.8 PIN entsperren

Bei wiederholter Fehleingabe wird eine PIN von der Karte gesperrt und der zugehörige Schlüssel kann nicht weiter verwendet werden.
Bestimmte Kartentypen erlauben die Entsperrung einer solchen PIN. In diesem Falle wird die entsprechende Option im Hauptmenü angezeigt:

Abbildung 19: Menü Kartenverwaltung bei Entsperr-Möglichkeit

Durch Wahl der Option 'PIN entsperren' gelangen Sie in das entsprechende Menü:

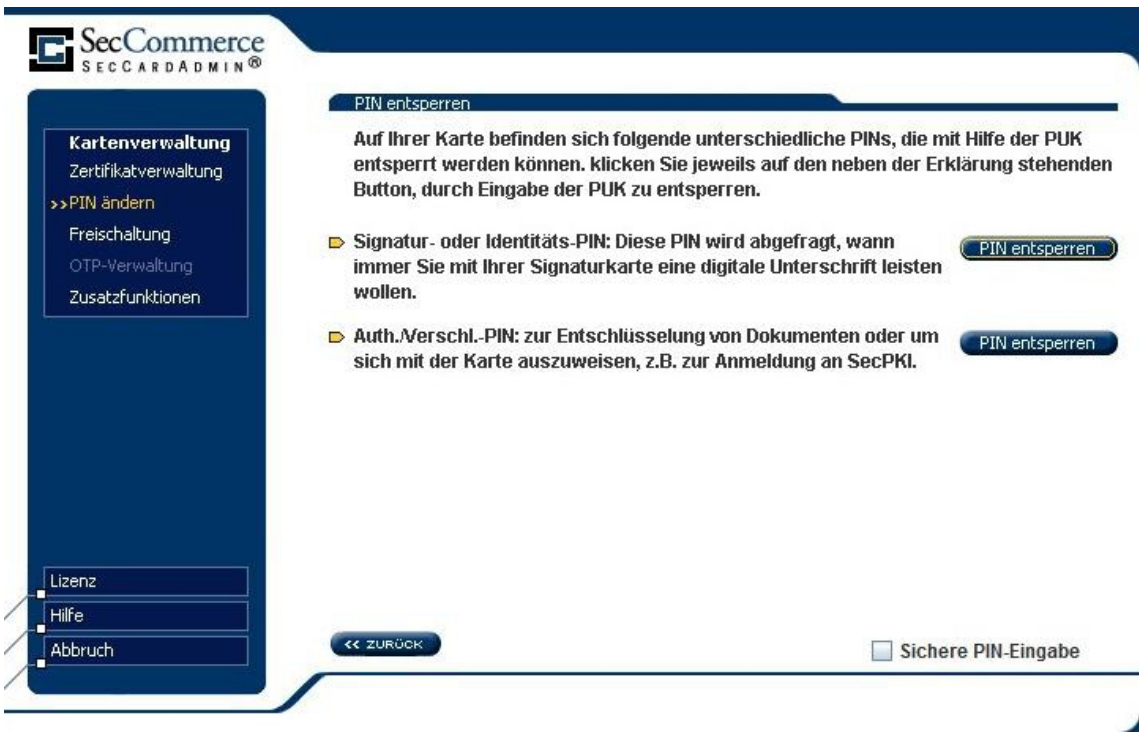

Abbildung 20: Menü: PIN Entsperren

Wählen Sie die gesperrte PIN aus. Dann erhalten Sie die Möglichkeit zur Eingabe der PUK, um die gesperrte PIN zu entsperren:

Abbildung 21: PUK-Eingabe

Sie erhalten im Erfolgsfall eine Meldung, dass Ihre PIN entsperrt wurde.

3.9 TeleSec ECC Signaturkarte: PIN2

Für die TeleSec-Signaturkarten, welche die Verschlüsselung mit dem ECC-Verfahren unterstützen, können Sie eine PIN2 setzen, die zur Entsperrung einer durch mehrfache Fehleingabe gesperrten PIN verwendet werden kann:

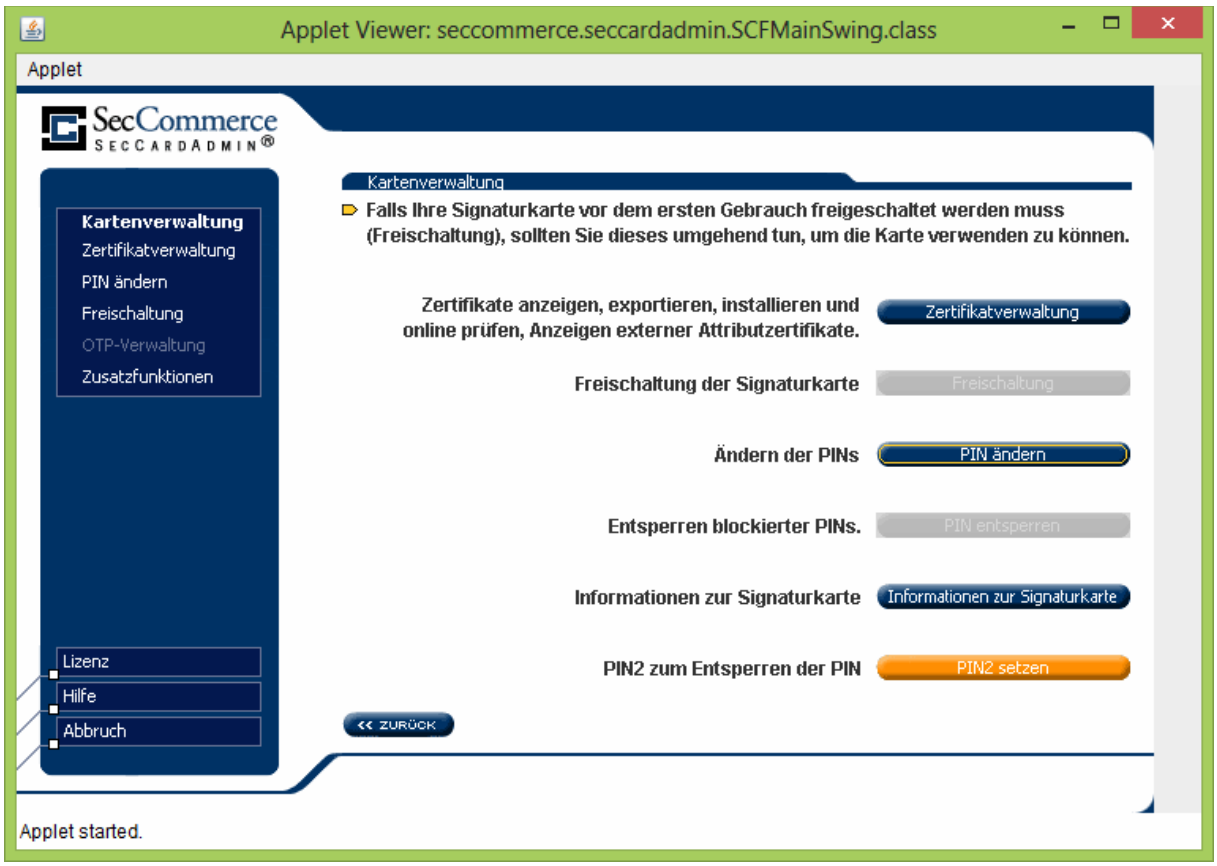

Abbildung 22: TeleSec ECC Karte: PIN2

Um eine entsprechende PIN2 zu setzen, ist es zuerst erfolderlich, die PIN sebst einzugeben:

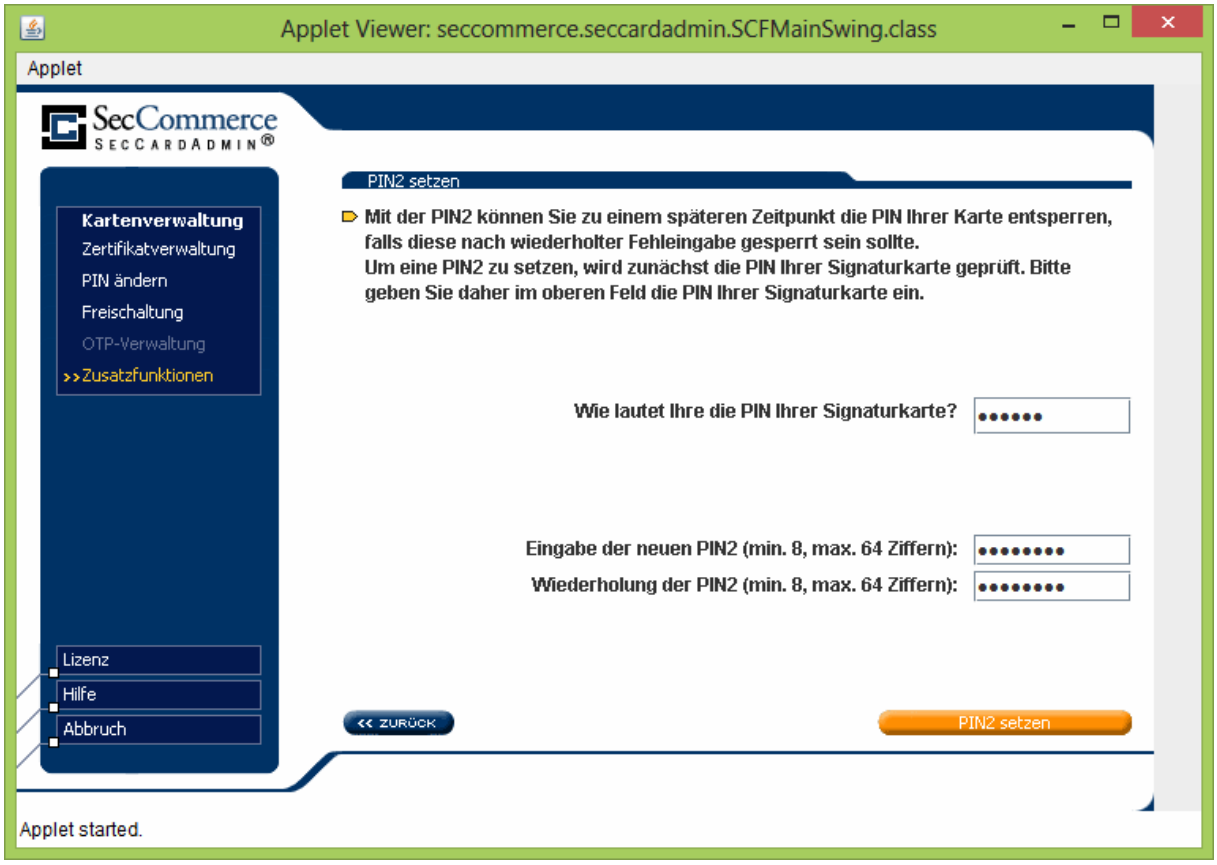

Abbildung 23: PIN2 setzen