

Anleitung

- **SignLive Toolbox
T-Telesec**



© Copyright 2014

Dieses Dokument und zugehörige Arbeitsunterlagen sind von X-Sign GmbH zur Verfügung gestellt worden. Sie sind Eigentum von X-Sign und unterliegen dem Urheberrecht. Jede Art der Verwertung bedarf immer einer Freigabe oder Genehmigung von X-Sign.
Version: 2.0 v. 12/2014

X-Sign GmbH

Bahnhofweg 1

77975 Ringsheim

FON: (+49) 7822 4335180

FAX : (+49) 7822 4335182

mail : info@x-sign-gmbh.de

Inhaltsverzeichnis

Toolbox.....	3
1 Hard- und Softwareanforderungen.....	3
2 Kartenleser Installation.....	3
3 Erläuterungen	3
3.1 Begriffe und Abkürzungen	3
3.2 Funktionen	4
3.3 Wechselseitiges Freischalten von PINs.....	4
4 Nutzung der Toolbox.....	4
4.1 Download und Installation.....	4
4.2 PIN-Details.....	5
4.3 Setzen der PINs.....	5
5 Überprüfung der Zertifikate auf der Karte.....	12
6 Fragen & Antworten (FAQ)	13
7 Hilfe zur Online – Empfangsbestätigung	14
7.1 Online – Empfangsbestätigung.....	14

Toolbox

1 Hard- und Softwareanforderungen

Betriebssystem:

Ab Windows XP (32 / 64 –bit)

Kartenleser:

mit sicherer PIN-Eingabe über die Tastatur aller gängigen Kartenleser kompatibel
(bei SCM SPR 532Chipdrive ist die Vergabe von PIN 2 nicht möglich)

Smartcard:

TCOS 3.0, TCOS 3.0 V2

2 Kartenleser Installation

Um die Toolbox nutzen zu können muss der Kartenleser angeschlossen und installiert sein. Wir empfehlen den aktuellen Treiber des Herstellers zu verwenden. Bitte beachten Sie, dass es evtl. notwendig sein kann, nach der Installation des Kartenlesers einen Neustart ihres Systems durchzuführen.

3 Erläuterungen

3.1 Begriffe und Abkürzungen

Global-PIN1: (Karten-PIN)	Die Global-PIN wird für die Nutzung der fortgeschrittenen Zertifikate und die Freischaltung der Karte für erstmalige Nutzung von Signaturanwendungen benötigt.
Global-PIN2:	Die Global-PIN2 wird dazu verwendet, die Global-PIN1 im Falle einer dreimaligen Falscheingabe wieder neu zu setzen.
Fortgeschrittenes Zertifikat:	Das fortgeschrittene Zertifikat kann beispielsweise für die Datei- und E-Mail-Entschlüsselung, Datei- und E-Mail Signatur sowie den Smartcard-Logon am Arbeitsplatz sowie an Web-Portalen verwendet werden
SigG-PIN1:	SigG ist die Abkürzung für das Signatur Gesetz. Diese PIN wird benötigt um das qualifizierte Signaturzertifikat für gesetzeskonforme Unterschriften zu verwenden.
SigG-PIN2:	Die SigG-PIN2 wird dazu verwendet, die SigG-PIN1 im Falle einer dreimaligen Falscheingabe wieder frei zu schalten.
SigG-Zertifikat:	Das SigG-Zertifikat wird ausschließlich für die gesetzeskonforme Unterschrift verwendet.
Fehlbedienungs- zähler:	Der Fehlbedienungs-zähler zählt die Falscheingaben bei der PIN-Eingabe. Steht der Fehlbedienungs-zähler auf 3, ist die PIN gesperrt. Jede PIN führt einen eigenen Fehlbedienungs-zähler. Gibt man nach einer Falscheingabe die PIN korrekt ein, wird der Fehlbedienungs-zähler wieder auf 0 gesetzt.

Null-PIN Verfahren: Mit dem Null-PIN-Verfahren beschreibt man den Zustand einer noch nicht gesetzten PIN. Das NPV ist ein Verfahren zum sicheren Versand von Signaturkarten, bei dem ein PIN-Brief mit vorgegeben PINs nicht mehr notwendig ist. Die Signaturkarte kann erst genutzt werden, wenn die Null-PIN durch den Empfänger ersetzt wurde. Diese PIN und die damit verbundenen Funktionen können nicht benutzt werden, bis die entsprechende PIN vom Benutzer festgelegt wurde.

Sichere PIN Eingabe: Unter einer sicheren PIN-Eingabe versteht man die direkte PIN-Eingabe am Kartenleser.

3.2 Funktionen

Funktion	Benötigte PIN
SigG Signatur	SigG-PIN1
E-Mail- und Dateientschlüsselung	Global-PIN1
E-Mail-Signatur	Global-PIN1
Smartcard Logon	Global-PIN1

3.3 Wechselseitiges Freischalten von PINs

Unter wechselseitigem Freischalten von PINs im Falle einer Sperrung versteht man, dass sich die SigG-PIN1 mit der SigG-PIN2 neu setzen lässt und umgekehrt. Genau so verhält es sich mit der Global-PIN1 und der Global-PIN2. SigG-PIN2 oder Global-PIN2 können nur zum Zurücksetzen benutzt werden, aber nicht zum Signieren oder Verschlüsseln. Zum Signieren oder Verschlüsseln wird immer die Global-PIN1 bzw. SigG-PIN1 benötigt.

4 Nutzung der Toolbox

Bevor Sie die Toolbox starten, stellen Sie sicher, dass der Kartenleser angeschlossen und installiert ist, und Ihre Karte sich im Kartenleser befindet.

4.1 Download und Installation

[SignLive! Toolbox Windows](#) T-Systems Signaturkarten - Administrationsanwendung
(Systemvoraussetzungen: Ab Windows XP® mit sicherer PIN-Eingabe über die Tastatur aller gängigen Kartenleser kompatibel)

[SignLive! Toolbox MAC](#) T-Systems Signaturkarten - Administrationsanwendung
(Systemvoraussetzungen: Mac OS X ab Version 10.7 (Lion); mit sicherer PIN-Eingabe über die Tastatur mit vielen gängigen Kartenlesern kompatibel)

4.2 PIN-Details

	Min.	Max.	
Global-PIN1	6 Stellen	64 Stellen	darf gleich sein mit anderen PINs
Global-PIN2	8 Stellen	64 Stellen	darf gleich sein mit anderen PINs
SigG-PIN1	6 Stellen	64 Stellen	darf gleich sein mit anderen PINs
SigG-PIN2	8 Stellen	64 Stellen	darf gleich sein mit anderen PINs

Nur bei der 1. Vergabe der PINs ist die Anzahl der Stellen wie folgt begrenzt:

PIN1 genau 6 Stellen

Bei einer Änderung der PIN1 gelten die o. g. PIN-Details.

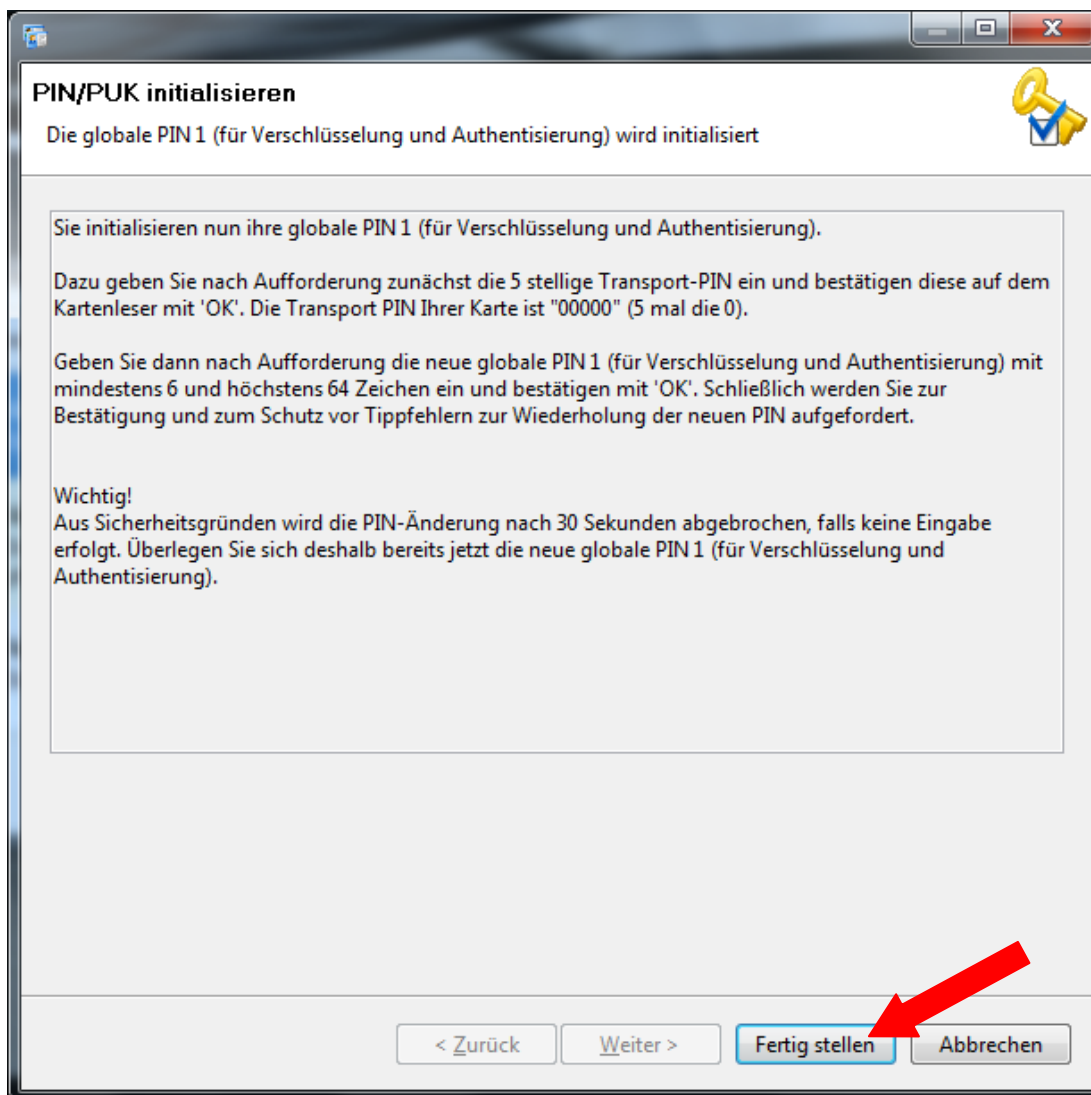
4.3 Setzen der PINs

Wenn Sie die Toolbox starten, dann erhalten sie das nachstehende Bild:



Wählen Sie jetzt „**PIN Management**“ aus und klicken Sie darauf.

Sie sehen nun dieses Fenster: Klicken Sie bitte auf SigG PIN 1.



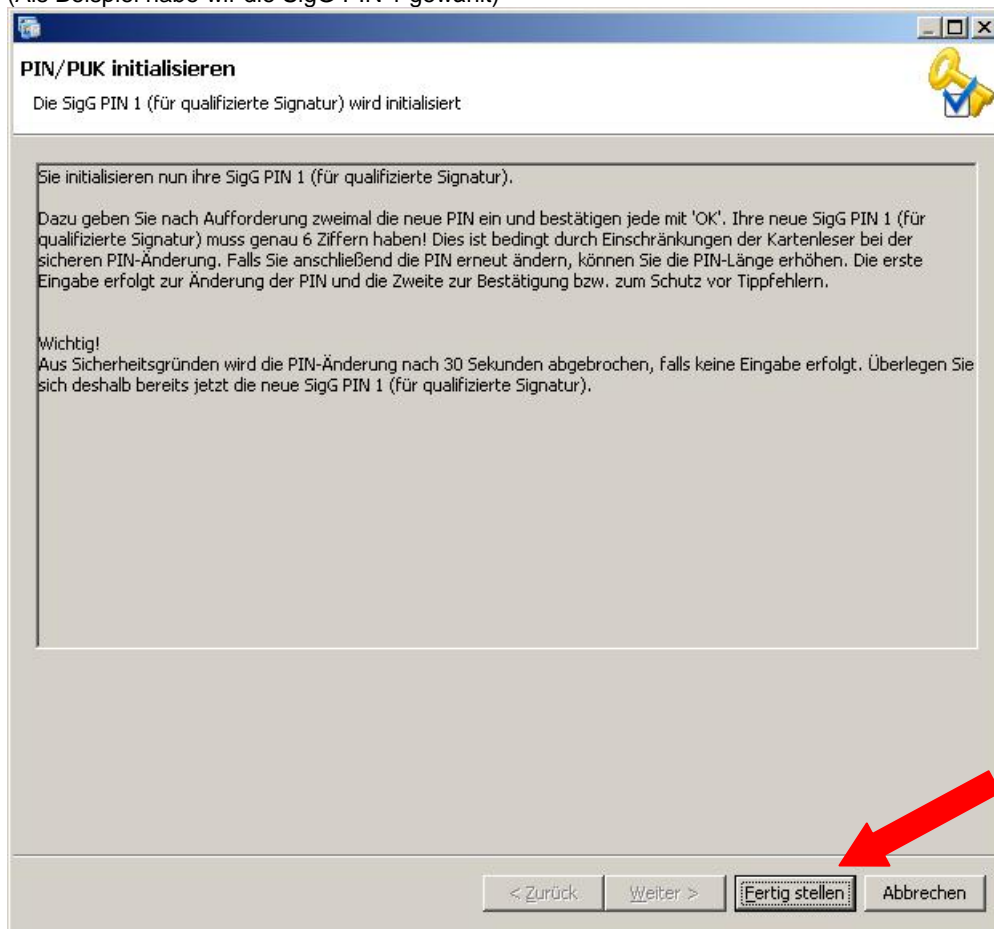
Bestätigen Sie nun dieses Fenster mit „Fertig stellen“.

Sollten Sie dieses Bild sehen, so geben Sie bitte den Transport-PIN wie folgt über Ihren Kartenleser ein:

00000 (5 mal die 0) und bestätigen Sie diesen PIN mit OK auf Ihrem Kartenleser.

Danach können Sie mit der PIN-Vergabe fortfahren.

Es erscheint dann das folgende Bild:
(Als Beispiel habe wir die SigG PIN 1 gewählt)

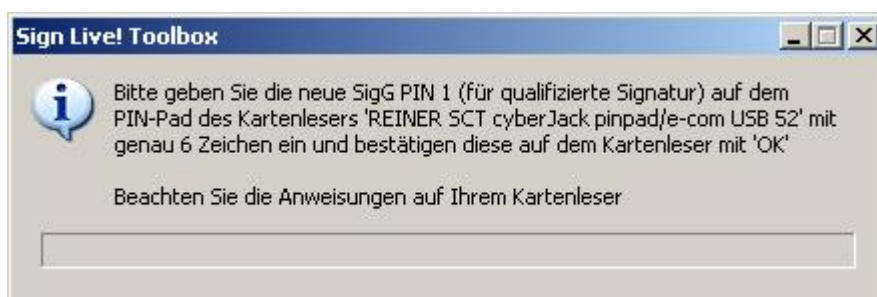


Bestätigen Sie nun dieses Fenster mit „Fertig stellen“.

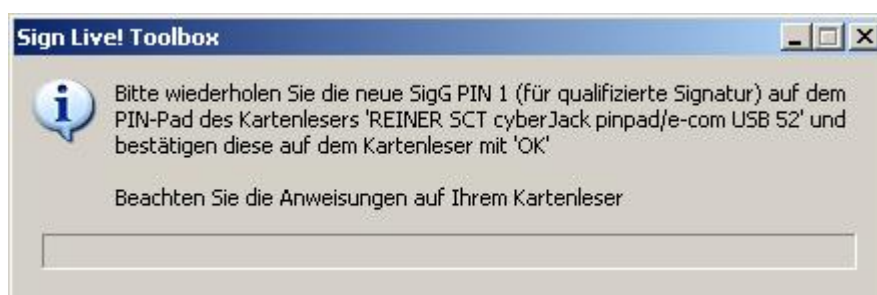
Es erscheint nach einigen Sekunden ein Eingabefenster (siehe z. B. unten).

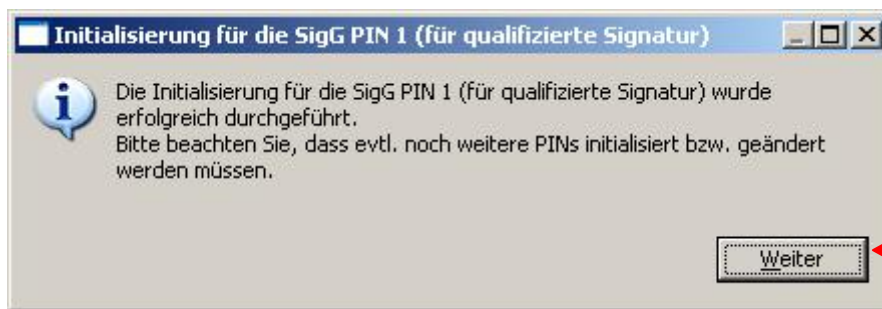
Geben Sie erst jetzt die PIN ein!

Sie können nun die globale PIN 1 (genau 6 Stellen) über den Kartenleser eingeben.

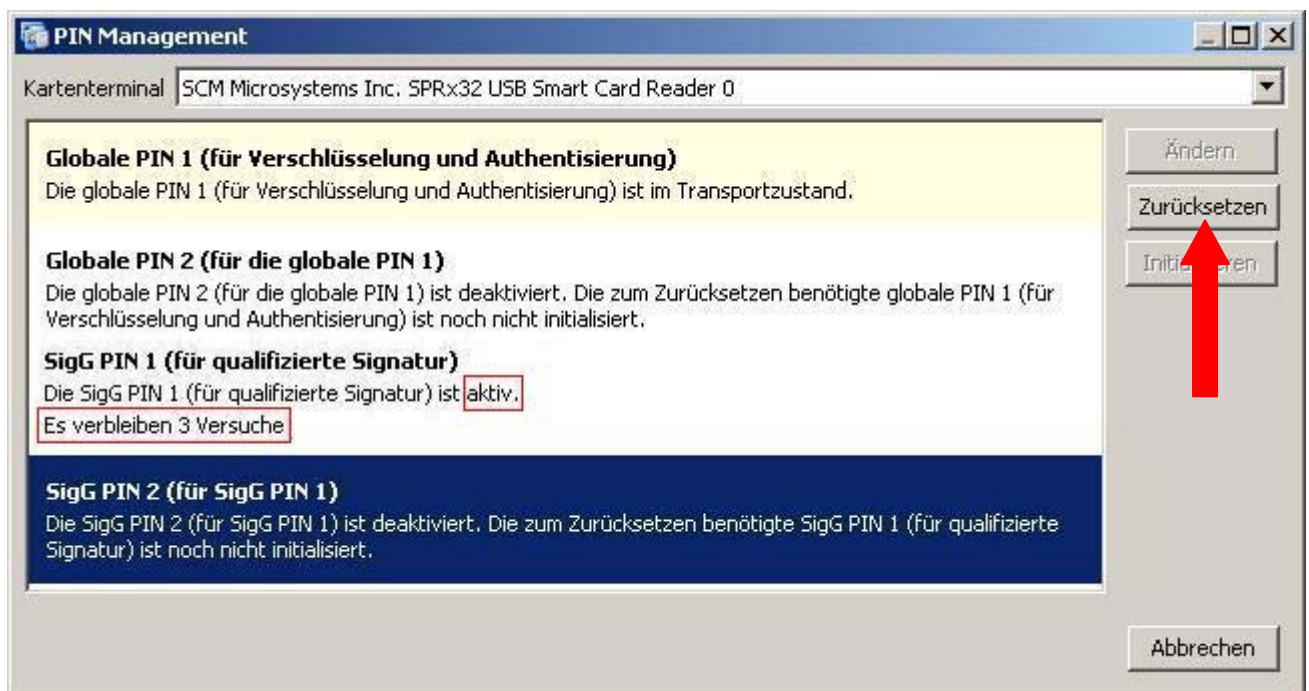


Nach Abschluss der Eingabe muss die neue PIN durch erneute Eingabe bestätigt werden.

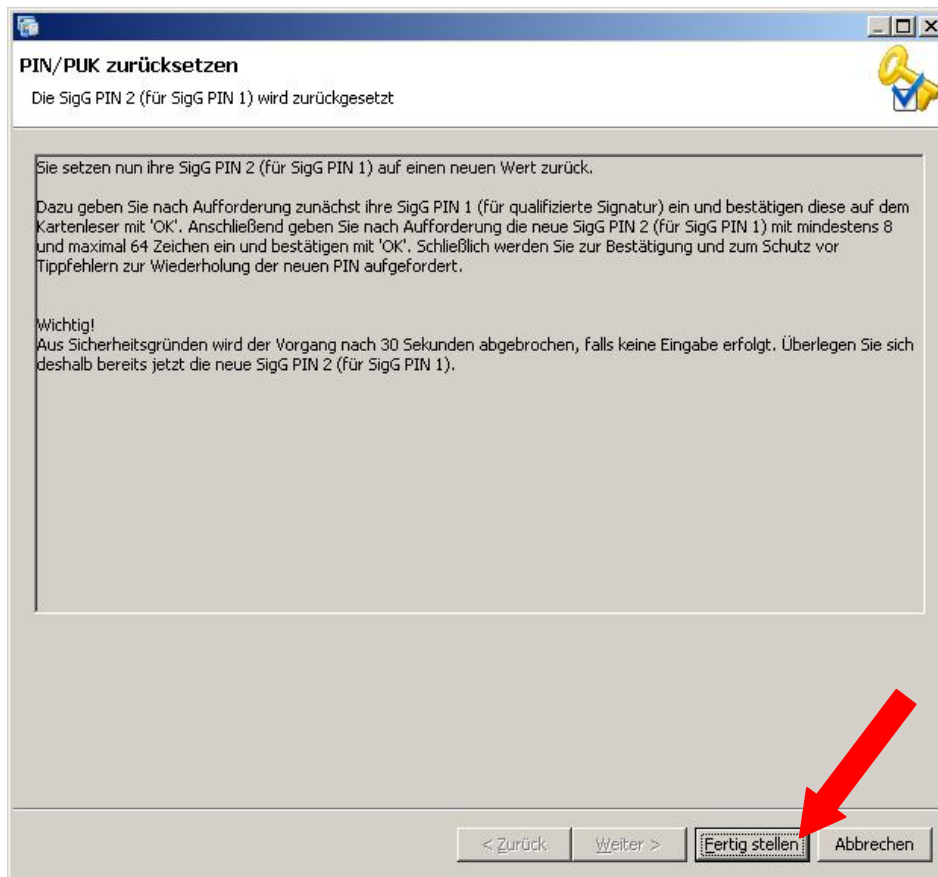




Dieses Bild bestätigt Ihnen, die erfolgreiche Initialisierung (Vergabe) Ihrer PIN 1. Mit „Weiter“ kommen Sie zurück zum Auswahlbildschirm.



Im oberen Bild wurde die SigG PIN1 frei geschaltet. Mit dieser kann nun die SigG PIN2 gesetzt werden. Wählen Sie SigG PIN2 aus und klicken Sie auf „Zurücksetzen“

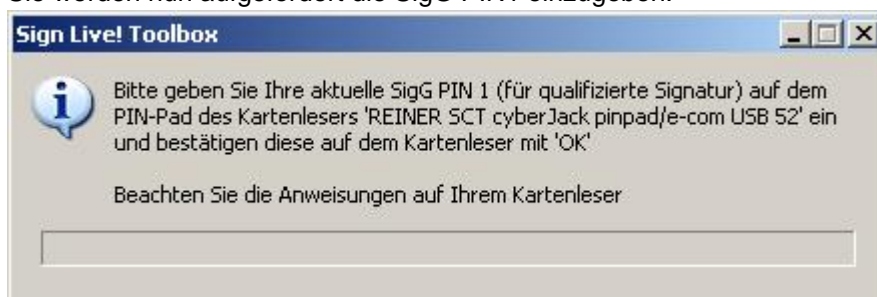


Bestätigen Sie nun dieses Fenster mit „Fertig stellen“.

Es erscheint nach einigen Sekunden ein Eingabefenster (siehe z. B. unten).

Geben Sie erst jetzt die PIN ein!

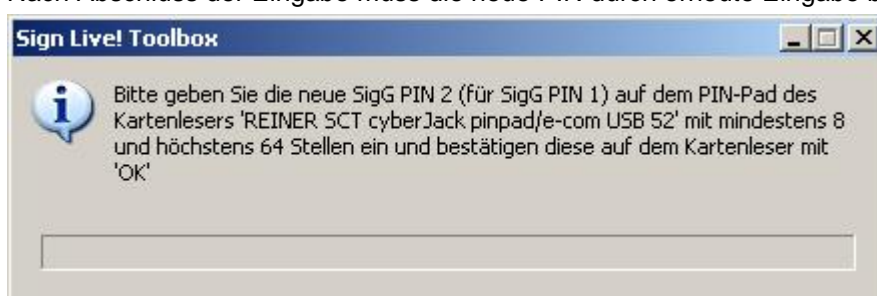
Sie werden nun aufgefordert die SigG PIN1 einzugeben.

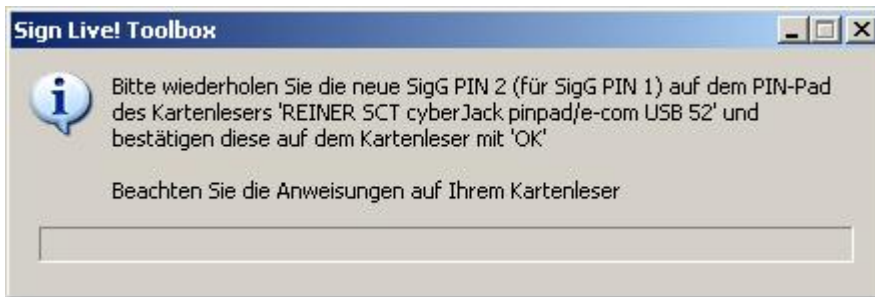


Die PIN Abfrage wird gestartet. Nach erfolgreicher Eingabe wird die 8-stellige Global-PIN2 angefragt. Diese muss von ihnen neu vergeben werden.

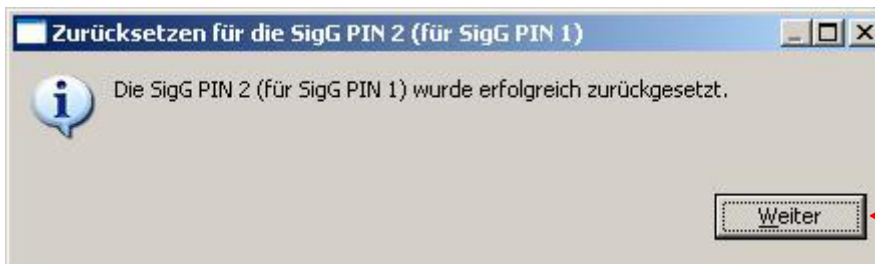
Geben Sie die gewünschte PIN 2 (min. 8 Stellen) **auf Ihrem Kartenleser** ein und schließen die Eingabe ab (grüne Taste bzw. Enter-Taste am Ziffernblock beim Cherry-Smartboard).

Nach Abschluss der Eingabe muss die neue PIN durch erneute Eingabe bestätigt werden.

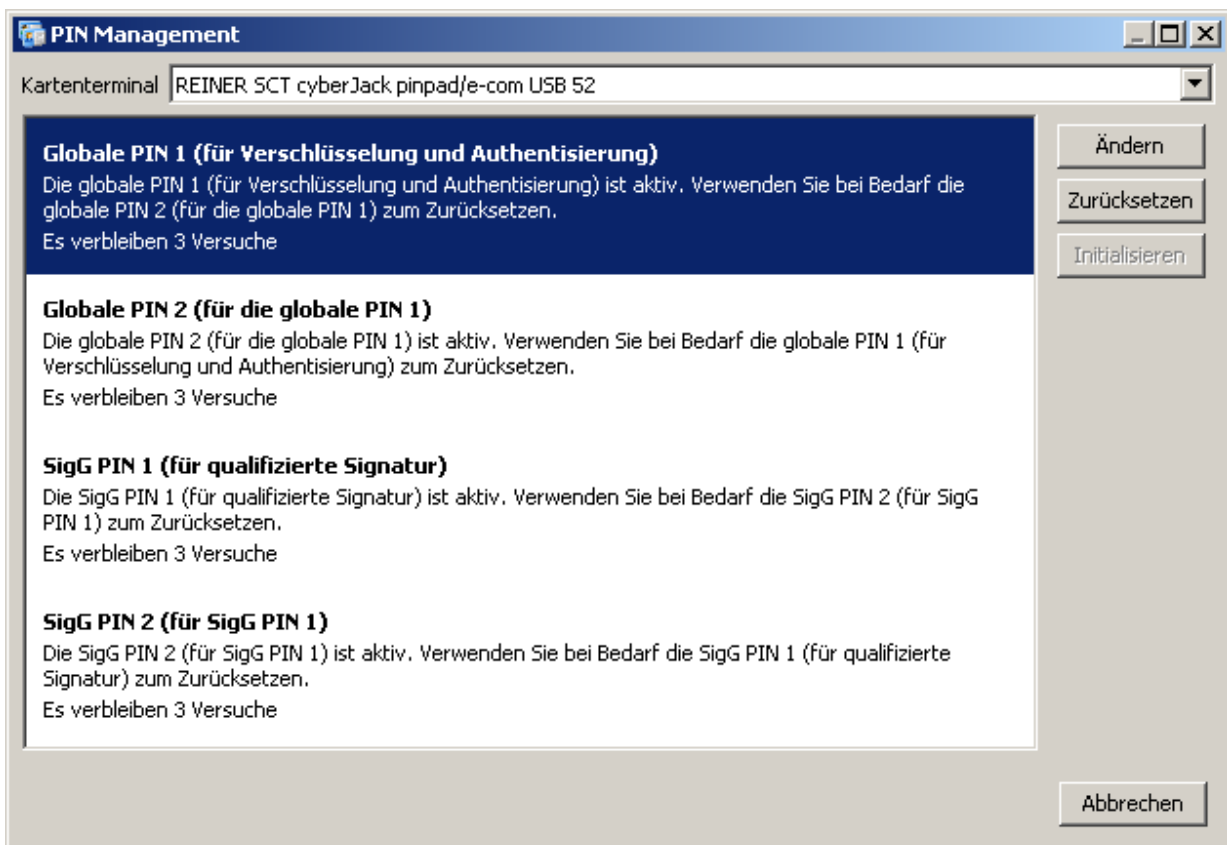




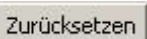
Nachdem die PIN erfolgreich gesetzt wurde, erscheint eine Erfolgsmeldung:



Im PIN Manager steht jetzt neben der frei geschalteten PIN der Zustand „Es bleiben 3 Versuche“ :
Auf die gleiche Art und Weise werden auch die Globale PIN1 und PIN2 gesetzt.



Durch dreimalige Falscheingabe gesperrte PINs können mit diesem Verfahren wieder neu gesetzt werden. Beachten Sie hierbei bitte Punkt 3.2 um festzustellen, welche PIN Sie zum Freischalten benötigen.

Dafür benötigen Sie die Funktion  . Alle anderen Schritte sind ähnlich.

5 Überprüfung der Zertifikate auf der Karte

Sie können sich Ihre Zertifikate auch ansehen.

Wählen Sie bitte hierzu „Zertifikat exportieren...“

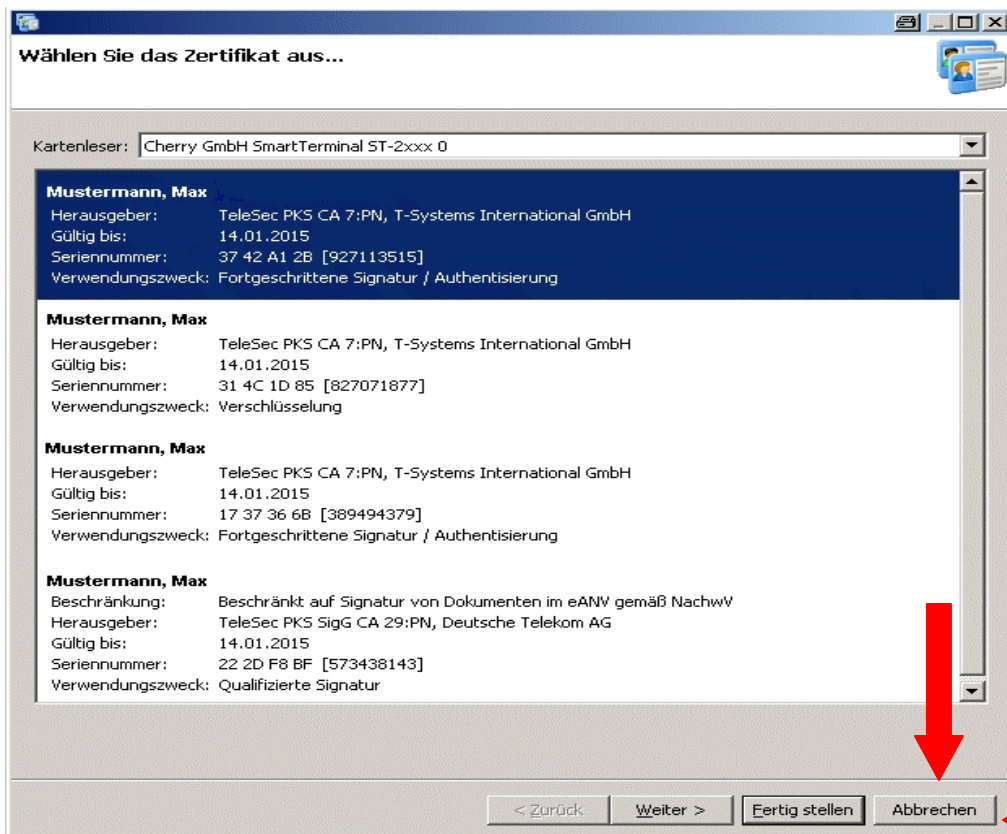


Für die Teilnahme am eANV ist es nicht nötig, die Zertifikate zu exportieren.

Diese Export-Funktion dient Ihnen hier einzig und allein zu Ansicht Ihrer Zertifikate.

Hier sehen Sie wer Zertifikatsinhaber ist.

Sie sehen jetzt alle Ihre Zertifikate:



6 Fragen & Antworten (FAQ)

F: *Bei der Anmeldung an meinen Rechner wird eine PIN abgefragt. Welche PIN wird hier benötigt?*

A: Windows erkennt beim Start den Kartenleser und die Karte und geht davon aus, dass diese zur Anmeldung verwendet werden soll. Die Karte bietet aber nicht ohne weiteres die Möglichkeit einer Windows Anmeldung. Ziehen Sie die Karte bei der Anmeldung um zum normalen Anmeldebildschirm zu gelangen. Prinzipiell sollten Sie Ihre Signaturkarte nicht im Kartenleser belassen. Sie sollten die Signaturkarte nur bei der Verwendung in den Kartenleser einstecken.

F: *Ich habe meine SigG-PIN1 dreimal falsch eingegeben. Was kann ich tun?*

A: Mit der Toolbox können Sie, wie unter Punkt 4.2 beschrieben, die SIG-PIN1 durch die Taste „Zurücksetzen“ wieder neu setzen.

F: *Ich habe meine PIN vergessen. Kann ich diese irgendwo finden?*

A: Ihre PINs lassen sich nicht aus der Karte auslesen. Mit der Toolbox können Sie, wie unter Punkt 4.2 beschrieben, die SIG-PIN1 wieder neu setzen.

F: *Wozu dient der Button „Ändern“ ?*

A: Mit dem Button „Ändern“ könne Sie eine PIN ändern, wenn Sie sie kennen.

F: *Beim Benutzen einer Signatur-Software wird oft eine Karten-Pin verlangt, um die Karte freizuschalten. Um welche PIN handelt es sich hier?*

A: Mit der Karten-PIN ist die Global-PIN1 gemeint.

F: *Darf ich meine PINs aufschreiben?*

A: Es ist nicht verboten, die PINs aufzuschreiben. Das Trust Center der Deutschen Telecom AG schreibt dazu: „ Halten Sie Ihre PIN und Ihr Telepasswort, wie bei Ihrer EC-Karte geheim. Wechseln Sie in gewissen Zeitabständen Ihre PIN und vermeiden Sie es, sich die PIN zu notieren. Bei dem Verdacht, dass jemand von Ihrer PIN Kenntnis erlangt hat, ändern Sie die PIN sofort.“
Mehr zum Thema finden Sie unter: http://www.telesec.de/pks/info_pks.pdf

F: *Was muss ich machen, wenn meine Karte gestohlen / verloren wurde?*

A: Bitte rufen Sie in solchen Fällen die Sperrhotline der T-TeleSec an: **0180 5/ 26 82 02** (14 Ct/Minute aus dem Festnetz der Deutschen Telekom, Mobilfunkpreise können davon abweichen) oder schriftlich veranlassen. Bitte halten Sie bei einer telefonischen Sperrung **unbedingt** Ihr Telepasswort bereit!
Hinweis: Eine Sperrung kann nur **innerhalb** der Zertifikatsgültigkeit durchgeführt werden. Die Sperrung einer Karte ist **unwiderruflich**.

Sie müssen nach der Sperrung eine neue Signaturkarte (Ersatzkarte) beantragen.

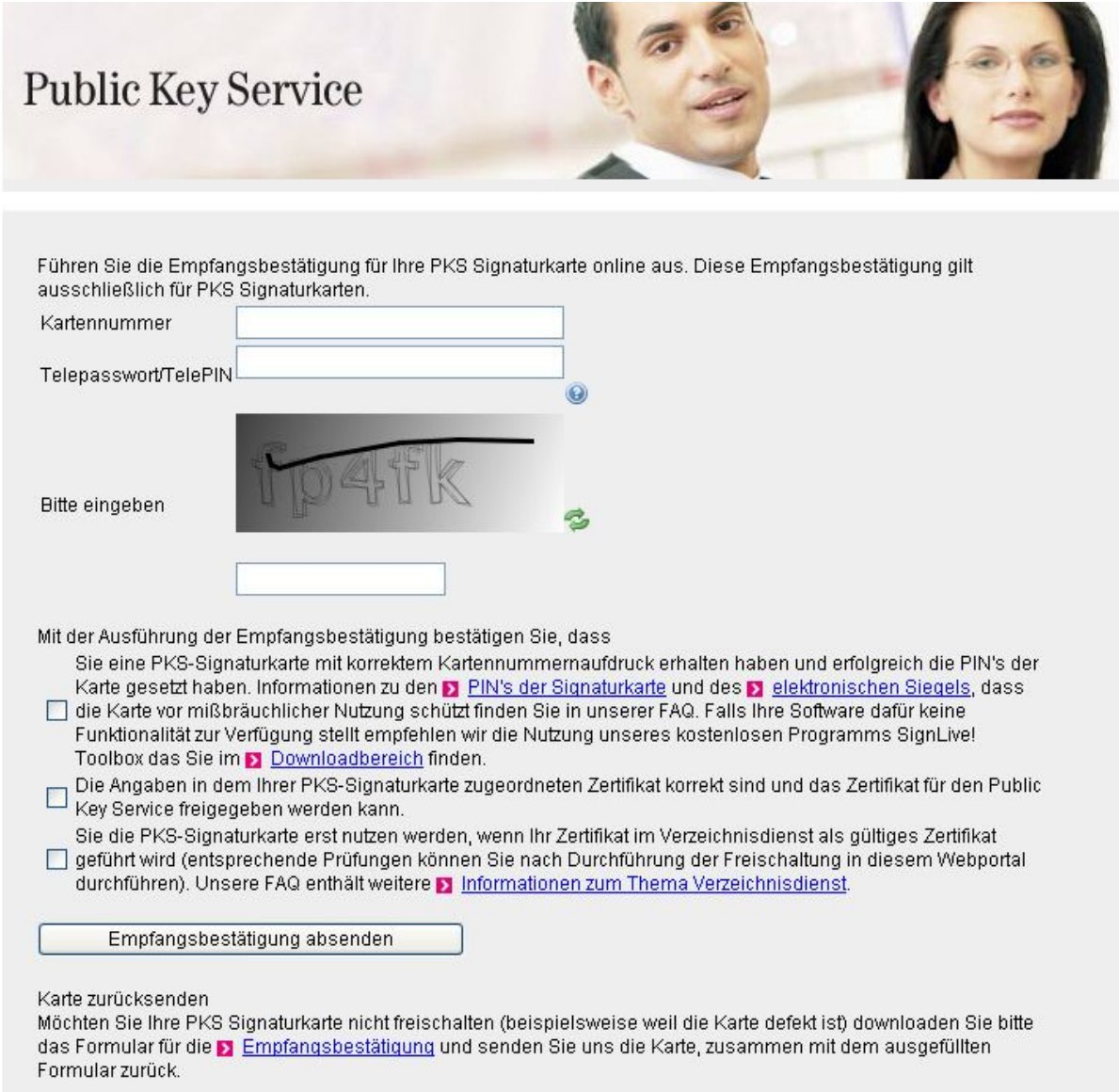
7 Hilfe zur Online – Empfangsbestätigung

7.1 Online – Empfangsbestätigung

Öffnen Sie dafür bitte den folgenden Link:

<https://www.telesec.de/de/pks/empfangsbestaetigung>

Sie sehen nun das Startfenster:




Public Key Service

Führen Sie die Empfangsbestätigung für Ihre PKS Signaturkarte online aus. Diese Empfangsbestätigung gilt ausschließlich für PKS Signaturkarten.

Kartenummer

Telepasswort/TelePIN


Bitte eingeben 

Mit der Ausführung der Empfangsbestätigung bestätigen Sie, dass

- Sie eine PKS-Signaturkarte mit korrektem Kartennummernaufdruck erhalten haben und erfolgreich die PIN's der Karte gesetzt haben. Informationen zu den [PIN's der Signaturkarte](#) und des [elektronischen Siegels](#), dass die Karte vor mißbräuchlicher Nutzung schützt finden Sie in unserer FAQ. Falls Ihre Software dafür keine Funktionalität zur Verfügung stellt empfehlen wir die Nutzung unseres kostenlosen Programms SignLive! Toolbox das Sie im [Downloadbereich](#) finden.
- Die Angaben in dem Ihrer PKS-Signaturkarte zugeordneten Zertifikat korrekt sind und das Zertifikat für den Public Key Service freigegeben werden kann.
- Sie die PKS-Signaturkarte erst nutzen werden, wenn Ihr Zertifikat im Verzeichnisdienst als gültiges Zertifikat geführt wird (entsprechende Prüfungen können Sie nach Durchführung der Freischaltung in diesem Webportal durchführen). Unsere FAQ enthält weitere [Informationen zum Thema Verzeichnisdienst](#).

Karte zurücksenden
Möchten Sie Ihre PKS Signaturkarte nicht freischalten (beispielsweise weil die Karte defekt ist) downloaden Sie bitte das Formular für die [Empfangsbestätigung](#) und senden Sie uns die Karte, zusammen mit dem ausgefüllten Formular zurück.

Führen Sie die Empfangsbestätigung für Ihre PKS Signaturkarte online aus. Diese Empfangsbestätigung gilt ausschließlich für PKS Signaturkarten.

Kartennummer  1

Telepasswort/TelePIN  2


Bitte eingeben   3

Mit der Ausführung der Empfangsbestätigung bestätigen Sie, dass

Sie eine PKS-Signaturkarte mit korrektem Kartennummernaufdruck erhalten haben und erfolgreich die PIN's der Karte gesetzt haben. Informationen zu den [PIN's der Signaturkarte](#) und des [elektronischen Siegels](#), dass die Karte vor mißbräuchlicher Nutzung schützt finden Sie in unserer FAQ. Falls Ihre Software dafür keine Funktionalität zur Verfügung stellt empfehlen wir die Nutzung unseres kostenlosen Programms SignLive! Toolbox das Sie im [Downloadbereich](#) finden.

- Die Angaben in dem Ihrer PKS-Signaturkarte zugeordneten Zertifikat korrekt sind und das Zertifikat für den Public Key Service freigegeben werden kann.

Sie die PKS-Signaturkarte erst nutzen werden, wenn Ihr Zertifikat im Verzeichnisdienst als gültiges Zertifikat geführt wird (entsprechende Prüfungen können Sie nach Durchführung der Freischaltung in diesem Webportal durchführen). Unsere FAQ enthält weitere [Informationen zum Thema Verzeichnisdienst](#).

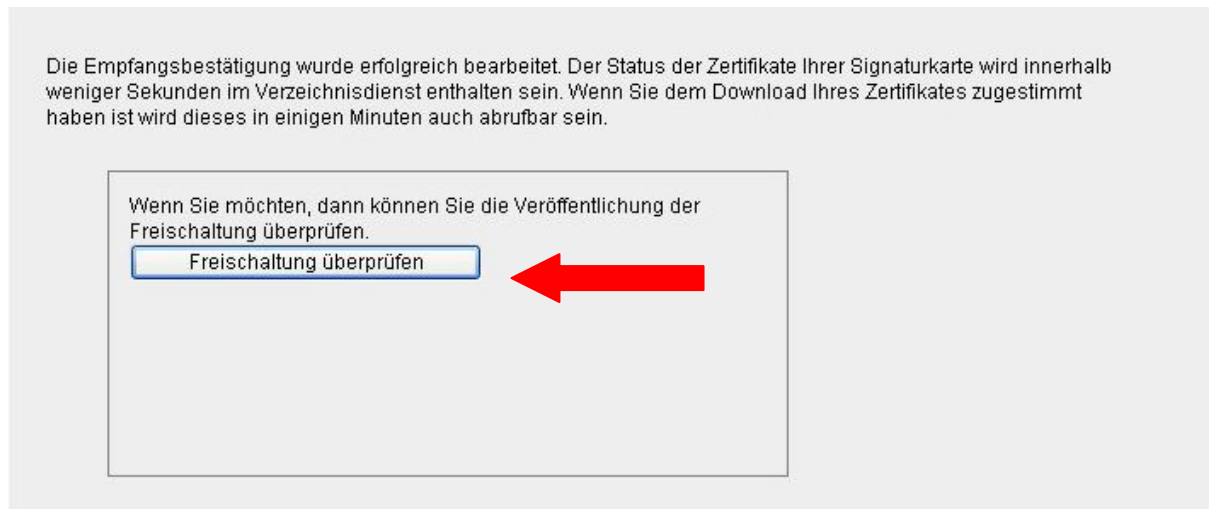
 5

Karte zurücksenden

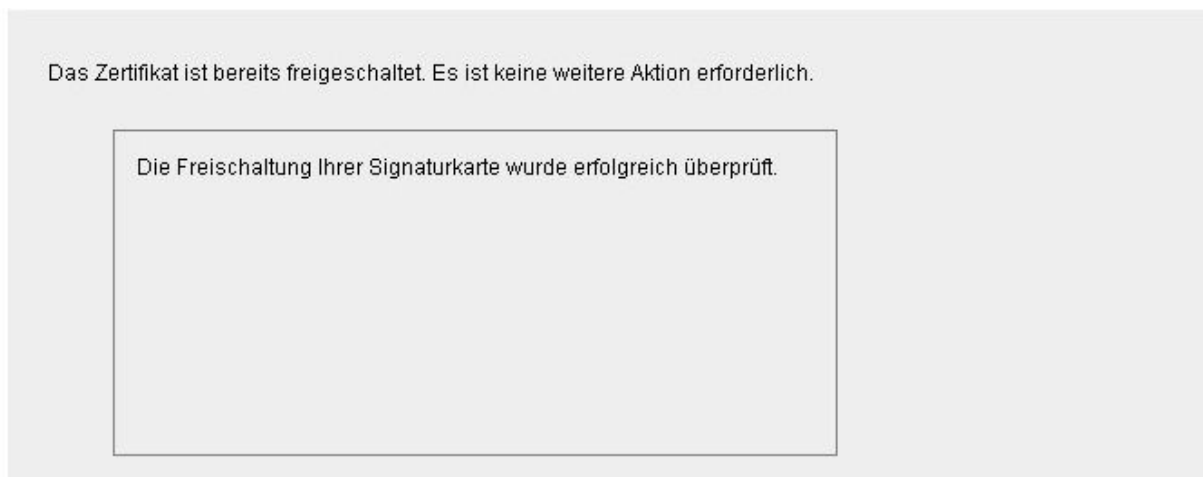
Möchten Sie Ihre PKS Signaturkarte nicht freischalten (beispielsweise weil die Karte defekt ist) downloaden Sie bitte das Formular für die [Empfangsbestätigung](#) und senden Sie uns die Karte, zusammen mit dem ausgefüllten Formular zurück.

- 1 Tragen Sie bitte hier Ihre Kartennummer komplett ein!
- 2 Tragen Sie bitte hier Ihre Telepin komplett ein!
Die Telepin finden Sie auf der Seite: **Persönliche Informationen zu Ihrem Public Key Service Auftrag** welche bei Ihrem Antrag erzeugt wurde. (Muster siehe Seite 5)
- 3 Tragen Sie bitte hier die Zeichen der Sicherheitsabfrage ein.
- 4 Bestätigen Sie die Angaben. (Anklicken)
- 5 Klicken Sie nun auf „Empfangsbestätigung absenden“

Es erscheint nun das folgende Fenster:



Wenn Sie nun auf „ Freischaltung überprüfen“ klicken, sehen Sie das folgende Bild:



Ihre Karte wurde nun für die Nutzung der qualifizierten digitalen Signatur freigeschaltet und ist nun einsetzbar.