PKS ERGÄNZUNGSZERTIFIKATE

Austausch und Installation

Deutsche Telekom Security GmbH
Telekom Security

öffentlich

Version:	1.1	Gültig ab:	29.07.2020
Status:	Freigegeben	Letztes Review Datum:	29.07.2020

Mit Veröffentlichung dieses Dokumentes verlieren alle bisherigen Versionen ihre Gültigkeit!

T · · Systems ·

IMPRESSUM

Tabelle 1 Impressum

Herausgeber	Deutsche Telekom Security GmbH Telekom Security

Dateiname	**Gültig ab**	**Titel**
Installation PKS Ergänzungszertifikate v1.1.docx	29.07.2020	PKS Ergänzungszertifikate

Version	**Letztes Review**	**Status**
1.1	29.07.2020	Freigegeben

Inhaltsverzeichnis

1 EINLEITUNG

In diesem Dokument ist die Installation von PKS Ergänzungszertifikaten (nicht qualifizierten bzw. fortgeschrittenen Zertifikaten) beschrieben.

Diese Installation ist notwendig, wenn Sie Ihre PKS Signaturkarte mit Anwendungen nutzen, die Funktionen zur Verschlüsselung, Authentisierung oder nicht qualifizierter Signaturen erfordern. Wir empfehlen Ihnen, diese Installation nur vorzunehmen, wenn Sie die oben aufgeführten Funktionen wirklich benötigen. Diese Vorgehensweise schützt Sie zum Beispiel vor Missverständnissen zwischen der qualifizierten und der nicht qualifizierten Signatur.

Bitte prüfen Sie anhand der Dokumentation Ihrer Fachanwendung, ob Sie diese Funktionen benötigen oder fragen Sie bei den entsprechenden Ansprechpartnern der Fachanwendung nach. Wir empfehlen diese Installation nur dann vorzunehmen, wenn Sie die Zertifikate für Ihre Fachanwendung benötigen.

Bitte beachten: Wenn Sie die Zertifikate tauschen, kann es sein, dass Sie die neuen Zertifikate zur Anmeldung bei Ihrer genutzten Anwendung neu registrieren müssen. Bitte kontaktieren Sie hierzu den entsprechenden Ansprechpartner Ihrer Fachanwendung.

Unser Support kann Fragen zu Ihrer Fachanwendung nicht beantworten und ist hier kein Ansprechpartner!

Falls Sie nicht qualifizierte Zertifikate eines anderen Ausstellers auf Ihrer Signaturkarte installiert haben, brauchen Sie nichts zu tun.

Alte fortgeschrittene Zertifikate erkennen Sie am Ausstellerzertifikat *TeleSec PKS CA 7:PN* oder *TeleSec PKS CA 8*. PKS Signaturkarten, die bis Mitte Mai 2019 ausgeliefert wurden, enthielten im Auslieferungszustand Zertifikate ausgestellt von *TeleSec PKS CA 7:PN*.

Zertifikate, ausgestellt von *TeleSec PKS CA 8* wurden bis zum 17.07.2020 erzeugt. Auf Grund von Anforderungen durch die Browser Hersteller (Google und Mozilla) müssen diese Zertifikate ausgetauscht werden.

Für den Austausch von Ergänzungszertifikaten benötigen Sie keine neue Signaturkarte. Diese Anleitung erklärt Ihnen, wie Sie den Austausch vornehmen.

Löschen Sie auf keinen Fall Zertifikate von anderen Ausstellern als von *TeleSec PKS CA 7:PN* oder *TeleSec PKS CA 8* von Ihrer Signaturkarte!

2 ZERTIFIKATE HERUNTERLADEN

Der erste Schritt zur Installation bzw. zum Austausch nicht qualifizierter Zertifikate für Ihre PKS Signaturkarte besteht darin, diese aus unserem Webportal herunterzuladen.

Nicht qualifizierte Zertifikate zur PKS Signaturkarte werden von einem öffentlichen Wurzelzertifikat ausgestellt. Aus diesem Grund unterliegen diese Zertifikate strengen Sicherheitsanforderungen, die von den Browserhersteller (z.B. Microsoft, Mozilla, Google) definiert wurden. Die Vorgaben der Browserhersteller bedingen, dass die Zertifikate zum Teil anderen Anforderungen bzgl. des Zertifikatsinhalts unterliegen.

Folgende Abweichungen zu Ihrem qualifizierten Zertifikat sind zu beachten:

- Die Zertifikate beinhalten immer Ihren Namen. Dies gilt auch dann, wenn Sie im qualifizierten Zertifikat ein Pseudonym nutzen.
- Die Zertifikate beinhalten immer Ihre E-Mail-Adresse.
- Die Zertifikate beinhalten nie Ihre Zugehörigkeit zu einer Organisation.
- Die Zertifikate beinhalten nie Zertifikatserweiterungen zur Selbstbeschränkung, Vertretung oder berufsrechtliche Zulassung.

Vor Ausstellung der Zertifikate müssen wir erneut die E-Mail-Adresse prüfen, die Sie in Ihr Zertifikat eintragen möchten. Bei diesem Vorgang kann die E-Mail-Adresse nicht geändert werden. Wir senden Ihnen an diese E-Mail-Adresse eine E-Mail mit einer Prüfnummer. Diese Prüfnummer müssen Sie im Webformular eintragen.

Für den Download öffnen Sie bitte die folgende URL:
https://www.pks.telesec.de/Webauftrag/faces/ergaenzungszertifikate/index.xhtml

Sie sehen die folgende Webseite:

Geben Sie in den Feldern Ihre Kartennummer, Name, Vorname und die Prüfnummer ein. Übernehmen Sie das Captcha in das nachfolgende Eingabefeld.

Nachdem Sie auf *Ergänzungszertifikate erzeugen* geklickt haben, erhalten Sie drei Zertifikate als komprimierte ZIP Datei zum Download. Bitte speichern Sie die Datei ab und entpacken den Inhalt in ein beliebiges Verzeichnis.

Sie können den Vorgang bedenkenlos mehrfach starten, sie erhalten immer die gleichen Zertifikate.

3 INSTALLATION DER ZERTIFIKATE

Für die Installation der Zertifikate benötigen Sie das Programm TCOS Kartenmanager, das Sie von unserer Webseite herunterladen können. Bitte öffnen Sie dafür die URL https://www.telesec.de/de/service/downloads/produkte-und-loesungen/. Den Kartenmanager finden Sie im Bereich *Secure Element & Smartcard* auf dieser Seite.

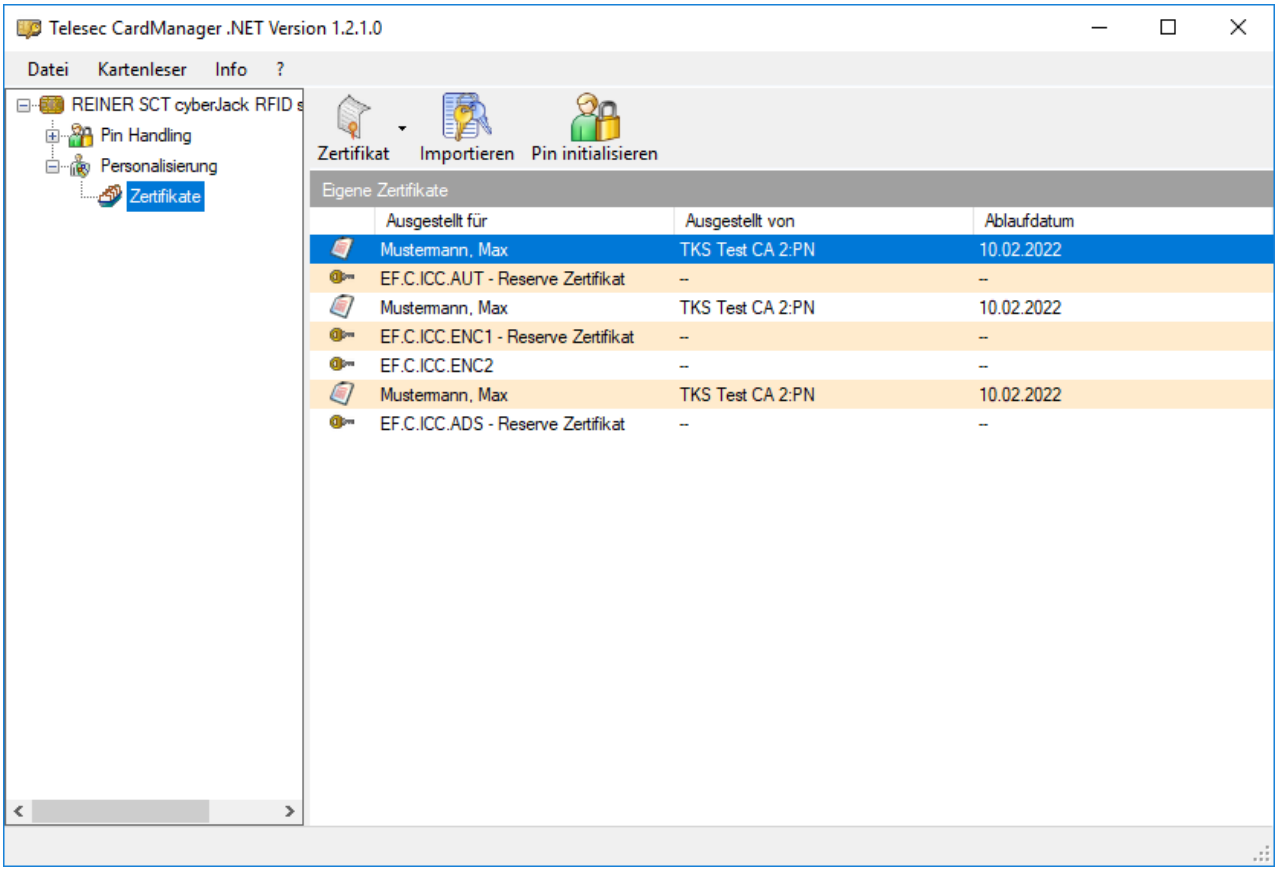
Bevor Sie diesen Vorgang starten, sollten Sie alle anderen Programme auf Ihrem PC, die eventuell auf die Signaturkarte zugreifen, beenden. Ebenso darf die Signaturkarte während des gesamten nachfolgend beschriebenen Vorgangs nicht aus dem Kartenleser entfernt werden.

3.1 Kartenmanager starten

Nachdem Sie den Kartenmanager gestartet haben und Ihre Signaturkarte erkannt wurde, navigieren Sie in den Bereich *Personalisierung -> Zertifikate*. Der nachfolgende Screenshot zeigt eine Test Signaturkarte mit vorinstallierten fortgeschrittenen Zertifikaten.

Es ist möglich, dass in Abhängigkeit von Ihrem Bestelldatum und Ihrer Zugehörigkeit zu einer Kundengruppe keine Zertifikate angezeigt werden.

Sollten Sie an dieser Stelle jedoch Zertifikate sehen, die nicht von TeleSec PKS CA 7:PN oder TeleSec PKS CA 8 ausgestellt wurden, brechen Sie den Vorgang ab. **Bitte löschen Sie auf keinen Fall Zertifikate von Ausstellern aus Ihrer Organisation.** Dies könnte dazu führen, dass Sie anschließend eine neue Signaturkarte benötigen.



3.2 Optional: Alte Zertifikate löschen

Wenn Sie bei dem vorherigen Schritt Zertifikate, ausgestellt von TeleSec PKS CA 7:PN oder TeleSec PKS CA 8 gesehen haben, kann es sinnvoll sein diese zu löschen.

Falls Sie Ihre Signaturkarte zur Verschlüsselung bzw. Entschlüsselung von Daten (Dateien oder Emails) verwendet haben, dürfen Sie auf keinen Fall das alte Zertifikat aus dem Speicherplatz EF.C.ICC.ENC1 löschen, ohne es aufzuheben. Das würde bedeuten, dass Sie alte Daten anschließend nicht mehr entschlüsseln können. Wir empfehlen Ihnen in diesem Fall das alte Zertifikat zu speichern, danach zu löschen, dann das neue Zertifikat zu installieren und zum Abschluss das alte Zertifikat als Reservezertifikat wieder zu installieren.

Ihre Signaturkarte verfügt über genügend freien Speicherplatz, um 2 Generationen nicht qualifizierte Zertifikate aufzunehmen. Zu beachten ist, dass nicht alle Anwendungen die Speicherplätze für Reservezertifikate auslesen.

Wenn Ihre Signaturkarte keinen freien Speicherplatz für neue Ergänzungszertifikate mehr hat, so empfehlen wir Ihnen die Löschung der alten Zertifikate, die von TeleSec PKS CA 8 ausgestellt wurden.

Wenn Ihre Signaturkarte noch freien Speicher hat, so empfehlen wir Ihnen diesen Schritt erst einmal nicht auszuführen. Bitte speichern Sie die neuen Zertifikate auf die Signaturkarte, auch wenn dort bereits Zertifikate vorhanden sind. Die neuen Zertifikate werden dann in die Speicherplätze für Reservezertifikate geschrieben.

Wichtig: Löschen Sie keine Zertifikate, die nicht von TeleSec PKS CA 7:PN oder TeleSec PKS CA 8 ausgestellt wurden. Dies kann dazu führen, dass Sie eine neue Signaturkarte benötigen!

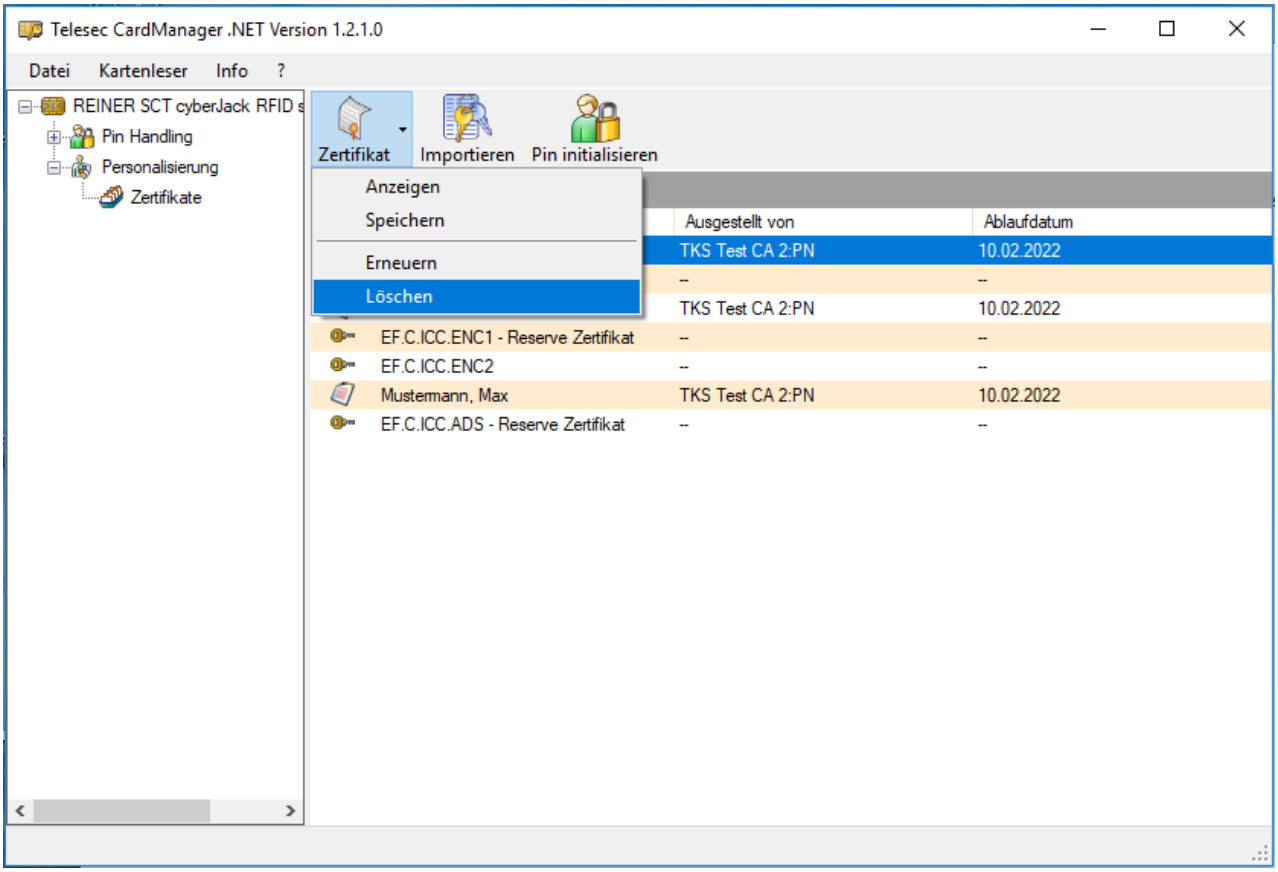
Ob Sie eventuell vorhandene alte Zertifikate löschen müssen, können Sie selbst testen. Alternativ befragen Sie den Ansprechpartner Ihrer Fachanwendung.

Zum Selbsttest: Installieren Sie die neuen Zertifikate, ohne die alten zu löschen. Sollten Sie bei Ihrer nächsten Nutzung der Signaturkarte sowohl die alten als auch die neuen Zertifikate sehen, war die Installation erfolgreich. Wenn Sie nur die alten Zertifikate (erkennbar am Aussteller Telesec PKS CA 7:PN bzw. TeleSec PKS CA 8) sehen, müssen Sie vermutlich diese von Ihrer Signaturkarte löschen.

Bitte vergewissern Sie sich vor dem Löschen der alten Zertifikate, ob die neuen Zertifikate in Ihrer Fachanwendung hinterlegt werden müssen. Dies ist üblicherweise nur dann möglich, wenn die Signaturkarte noch mit den alten Zertifikaten angemeldet ist. Weitere Informationen dazu erhalten Sie ebenfalls beim Ansprechpartner Ihrer Fachanwendung.

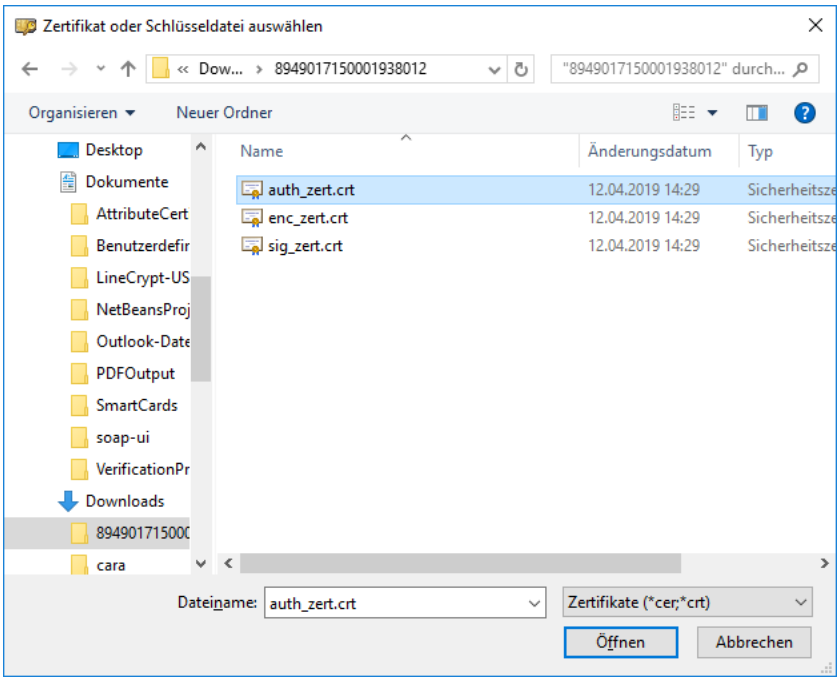
Es ist ratsam, alte Zertifikate vor dem Löschen abzuspeichern, damit diese ggf. bei Bedarf erneut installiert werden können.

Sie Löschen ein Zertifikat, in dem Sie es in der Liste markieren und dann im Untermenü des Buttons *Zertifikat* auf den Menüpunkt *Löschen* klicken (siehe nachfolgende Abbildung). Nach dem anklicken von *Löschen,* müssen Sie Ihre Globale PIN1 eingeben. Die Eingabe erfolgt entweder über die Tastatur des Kartenlesers oder über Ihre normale Computertastatur. Über den Menüpunkt *Speichern* können Sie ein Zertifikat abspeichern.



3.3 Zertifikate installieren

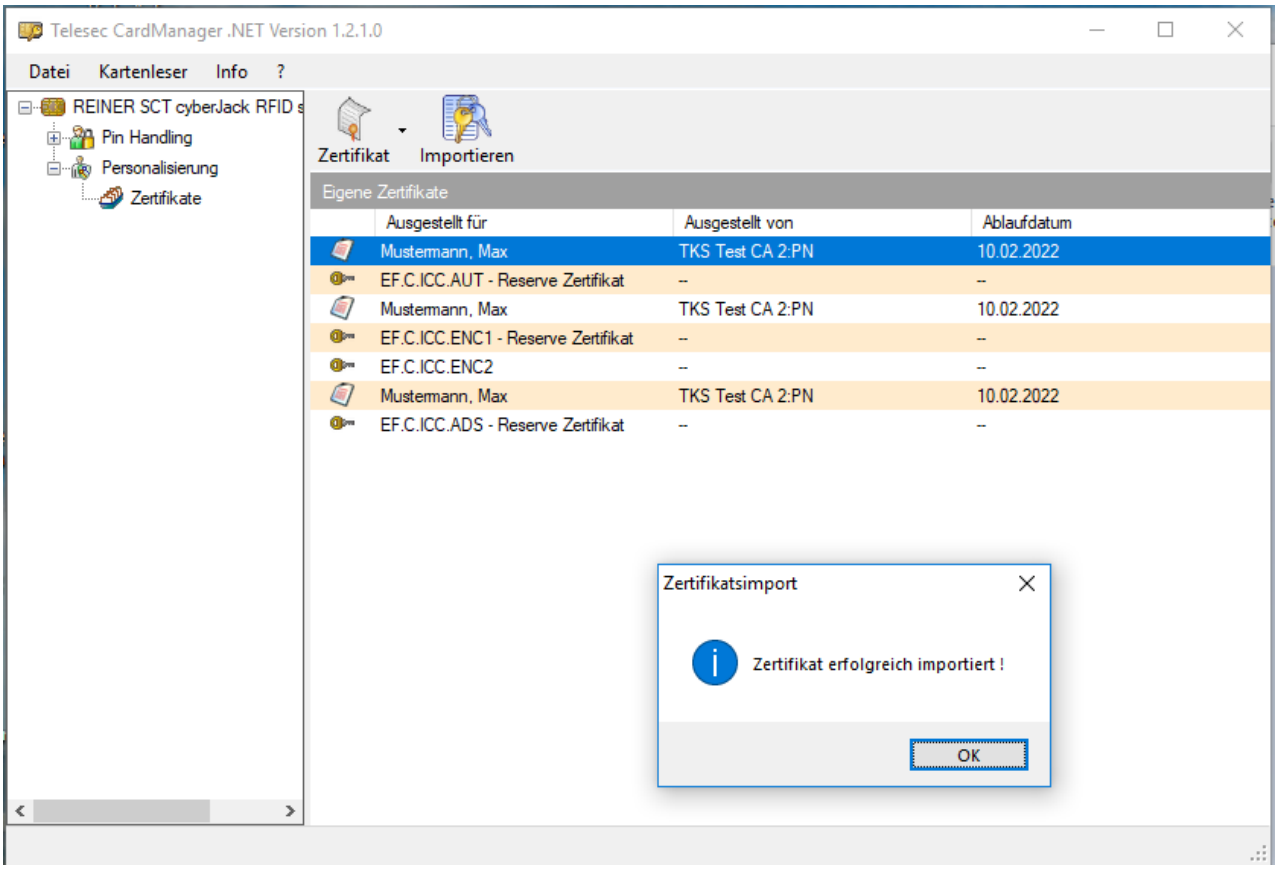
Sie installieren die Zertifikate auf Ihrer Signaturkarte in dem Sie auf den Button *Importieren* klicken. Es öffnet sich ein Dateiauswahl Fenster. Bitte wählen Sie hier eines der neuen Zertifikate aus.



Die Reihenfolge, in der Sie die Zertifikate installieren, ist nicht relevant.

Nach der Auswahl des Zertifikats müssen Sie die Globale PIN 1 Ihrer Signaturkarte eingeben (dieser Schritt entfällt beim Import des zweiten und dritten Zertifikats und wenn Sie vorher schon Zertifikate gelöscht haben). Die Eingabe erfolgt über die Tastatur des Kartenlesers oder über die normale Computertastatur.

Das Programm bestätigt Ihnen den erfolgreichen Import.

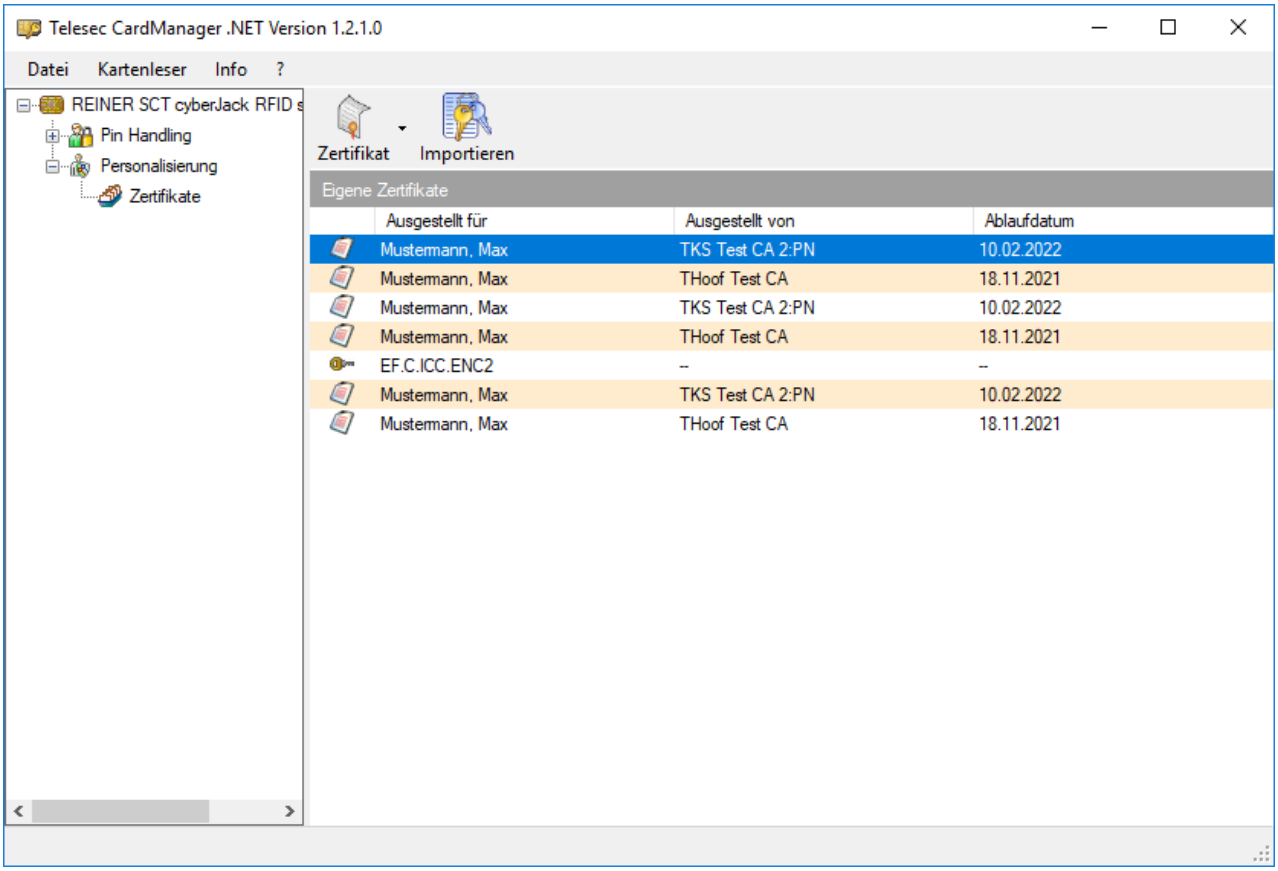


Bitte wiederholen Sie den Vorgang mit den beiden anderen Zertifikaten.

Die Anzeige wird vom Programm nach der Installation eines neuen Zertifikats nicht aktualisiert.

3.4 Abschluss

Aktualisieren Sie zum Abschluss die Anzeige, in dem Sie in einen anderen Bereich (außerhalb Personalisierung -> Zertifikate) navigieren und danach wieder zurückkehren. Wenn Sie eine Karte mit vorinstallierten nicht qualifizierten Zertifikaten besitzen, werden Ihnen anschließend 6 Zertifikate angezeigt.



Sollten Sie eine Karte ohne vorinstallierte nicht qualifizierte Zertifikate besitzen oder diese bereits gelöscht sein, so sehen Sie 3 Zertifikate.

Gelöschte, aber gespeicherte Zertifikate, können nun erneut installiert werden. Dies kann beispielsweise zur Datensicherung sinnvoll sein bzw. es ist zur Entschlüsselung von Daten unbedingt erforderlich. Siehe hierzu Kapitel 3.2.