BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Anleitung zur

Zertifikatsverwaltung Ihrer Signaturkarte

Erscheinungsdatum: 18.08.2021

Inhalt

1. Allgemeine Voraussetzungen 3
2. PIN-Verwaltung 4
2.1. Änderung der PIN für das fortgeschrittene Zertifikat (Advanced/ PIN2) 4
2.2. Aktivierung des qualifizierten Signaturzertifikates (Qualified Multi/ PIN1) 6
2.3. PIN-Eingabe mit der PUK freischalten (Fehlbedienungszähler) 9
3. Mögliche Fehlermeldungen/ Fehlerbehebung 12
3.1. PIN gesperrt bzw. Fehlbedienungszähler abgelaufen 12
3.2. Karte noch nicht initialisiert/ Sie haben Ihre Karte noch nicht freigeschaltet 12
3.3. Die Karte bzw. der Kartenleser wurde nicht gefunden 13
3.4. Systemzeit 13

1. Allgemeine Voraussetzungen

Unterstützte Betriebssysteme

- Microsoft Windows 10
- Apple Mac OS X 10.14

Signaturanwendungskomponente (SAK)

Die Signaturanwendungskomponente muss vorab installiert werden. Gehen Sie dazu bitte auf die Webseite https://zertifizierungsstelle.bnotk.de/signaturkartenverwaltung/ und laden sich dort passend für Ihr Betriebssystem den Installer runter und installieren diesen.

Unterstützte Chipkartenlesegeräte

Für die Änderung Ihrer PIN-Daten bzw. das Auf- oder Nachladen des qualifizierten Signaturzertifikates mithilfe der Signaturkartenanwendung ist ein Chipkartenlesegerät der Sicherheitsklasse 3 erforderlich, welches mit PIN-Pad und eigenem Display ausgestattet ist. Dadurch ist es möglich, eine PIN unabhängig von der Computertastatur einzugeben, wodurch hardwareseitig gewährleistet wird, dass die PIN-Eingabe nicht durch Viren, Trojaner oder andere Malware von Dritten eingesehen werden kann. Wir empfehlen folgende Geräte:

- ReinerSCT cyberJack one
- ReinerSCT cyberJack RFID
- ReinerSCT cyberJack RFID komfort
- ReinerSCT cyberJack secoder

Sollten Sie noch nicht die notwendige Treibersoftware auf Ihrem Rechner installiert haben, so bitten wir Sie, sich die zu Ihrem Betriebssystem passenden Treiber herunterzuladen. Die aktuellste Treibersoftware steht unter dem folgenden Link für Sie bereit:
https://www.reiner-sct.com/support/support-anfrage/

Insofern Sie eine CD mit Ihrem Chipkartenlesegerät bekommen haben, so können Sie die Treibersoftware von der CD installieren. Bitte überprüfen Sie auch im cyberJack Gerätemanager unter dem Reiter „Aktualisierung“ und „Prüfe auf neue Versionen“, dass die neueste Firmware für Ihr Kartenlesegerät installiert ist.

PIN-Brief

Für den erstmaligen Einsatz Ihrer Signaturkarte benötigen Sie den PIN-Brief, der Ihnen separat zu Ihrer Signaturkarte zugestellt wurde. Den PIN-Brief erhalten Sie, wenn Sie den Erhalt der zugehörigen Signaturkarte bestätigt haben, indem Sie auf den Link klicken, den wir Ihnen per E-Mail („Bestätigung des Erhalts ihrer Signaturkarte“) zugesandt haben. Wir empfehlen Ihnen, die darin befindlichen PINs mithilfe der folgenden Anleitung umgehend in neue PINs zu ändern und Ihre Signaturkarte zu aktivieren. Erst danach ist Ihre Signaturkarte einsatzbereit.

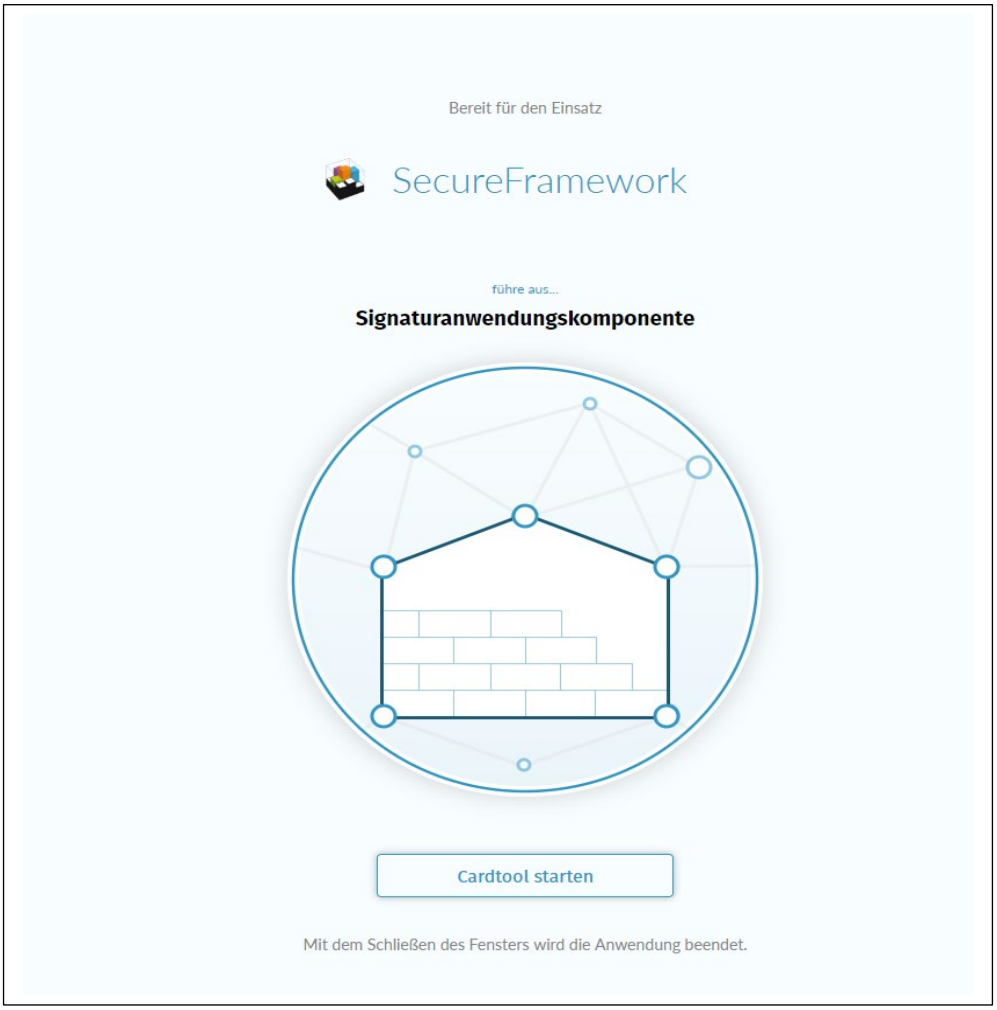
2. PIN-Verwaltung

2.1. Änderung der PIN für das fortgeschrittene Zertifikat (Advanced/ PIN 1)

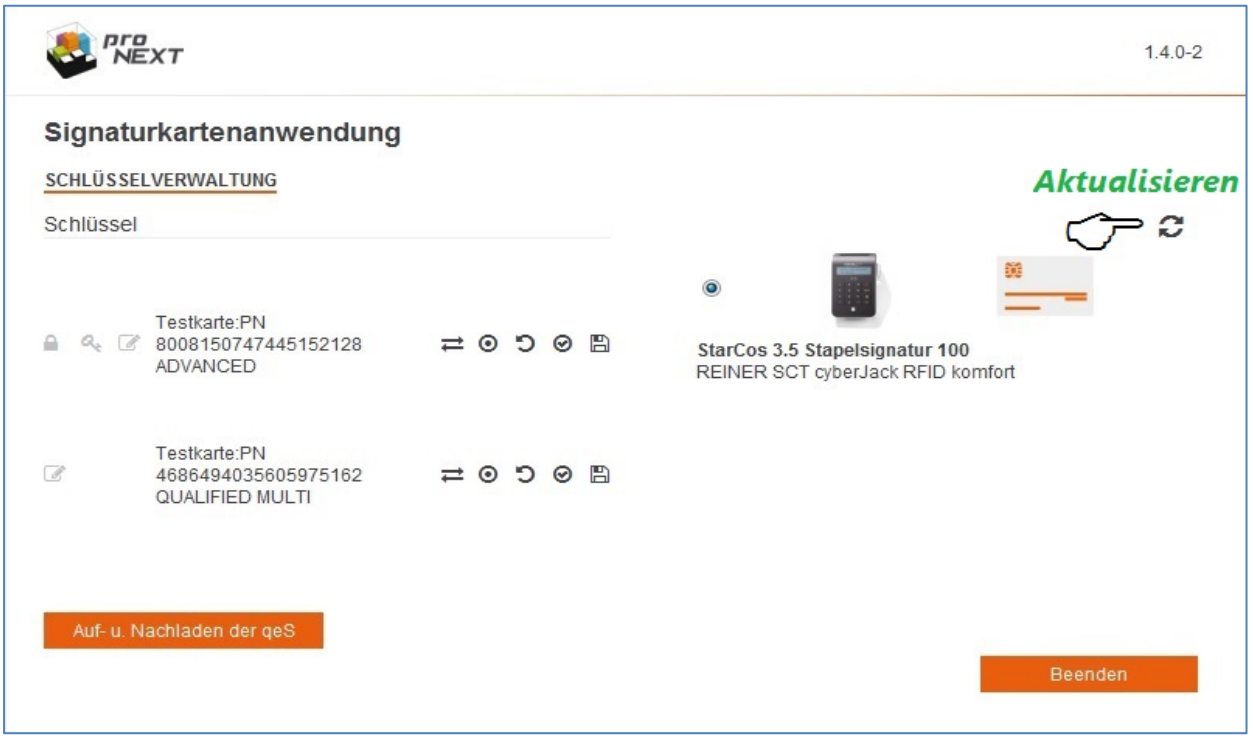
Öffnen der Signaturkartenanwendung

Wenn Sie, wie unter Punkt 1 beschrieben, die Signaturanwendungskomponente (SAK) für Ihr Betriebssystem heruntergeladen und installiert haben, starten Sie über das Icon  auf Ihren Desktop die Anwendung.
Nach erfolgreichem Start der Anwendung, zu erkennen am Symbol unten in der Taskleiste 

, klicken Sie bitte in der Anwendung auf „Cardtool starten".



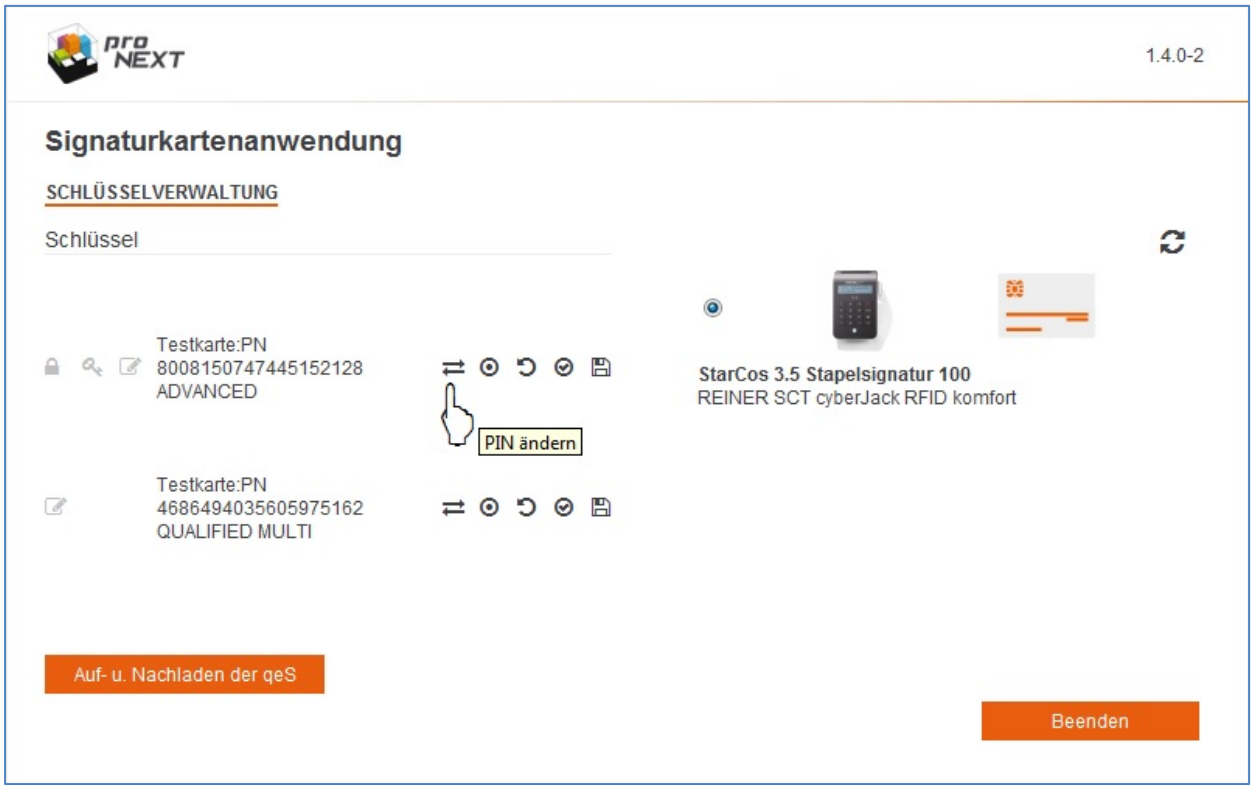
Es öffnet sich nun die Pronext-Anwendung, über die Sie die PIN-Änderung bzw. -Aktivierung vornehmen können.
Insofern das Kartenlesegerät ordnungsgemäß angeschlossen und Ihre Signaturkarte eingesteckt ist, sollte die Anwendung wie unten dargestellt beides darstellen. Werden Kartenlesegerät und Signaturkarte nicht angezeigt, prüfen Sie bitte, ob beides korrekt angeschlossen ist und klicken auf den Button „Aktualisieren".



PIN-Änderung

PIN für die Anmeldung (fortgeschrittenes Zertifikat/ADVANCED)

Wir empfehlen Ihnen, die im PIN-Brief enthaltene PIN 1 für die Anmeldung/ Authentisierung nach dem Erhalt der Karte zu ändern. Klicken Sie hierzu auf das Symbol „Pin ändern".

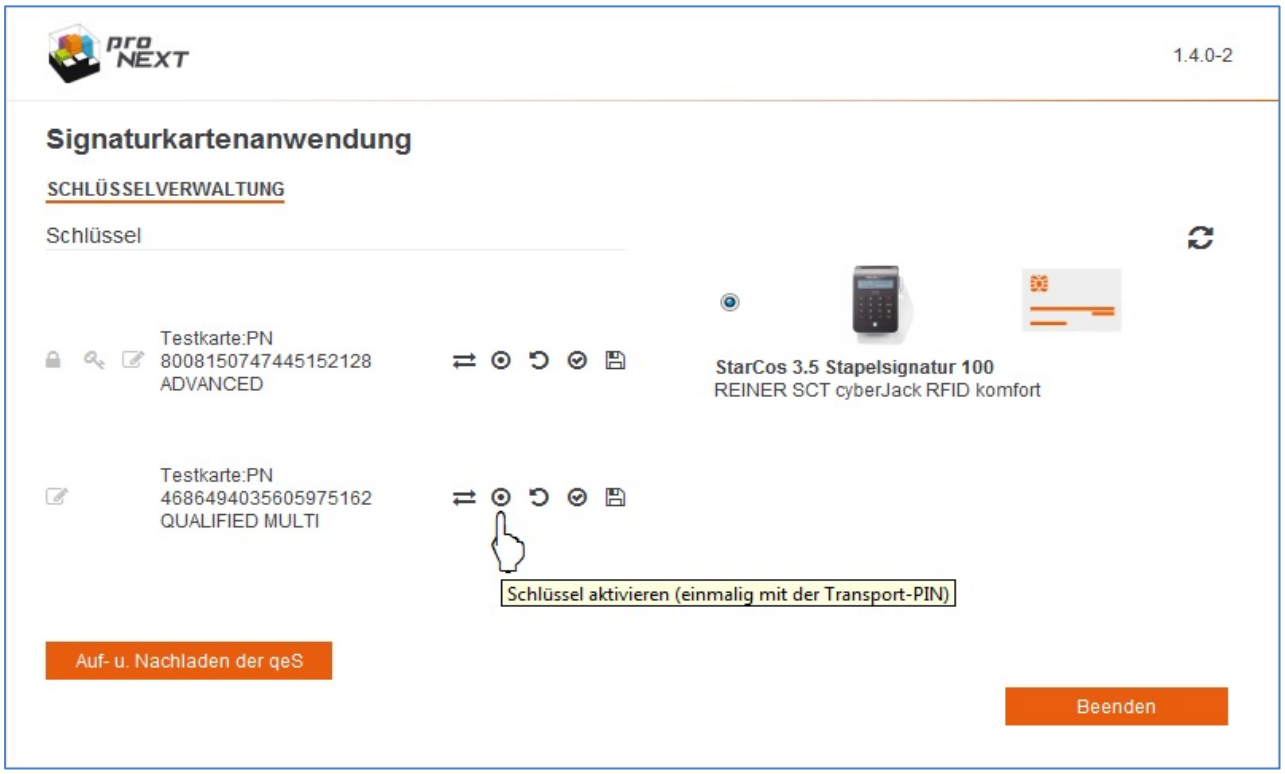


Der Änderungsprozess wird auf dem Display Ihres Kartenlesegeräts mit dem Befehl „**PIN Änderung**“ eingeleitet. Sobald auf dem Display Ihres Kartenlesegerätes „**PIN**“ angezeigt wird, geben Sie bitte die PIN 1 aus dem Ihnen separat zur Signaturkarte zugestellten PIN-Brief ein und drücken die Taste „OK“. Im nächsten Schritt „**PIN neu**“ vergeben Sie eine neue mindestens 6-stellige PIN für Ihre Signaturkarte, drücken „OK“ und geben diese PIN zur Bestätigung ein weiteres Mal ein. Auf dem Kartenlesegerät sollte nun „**PIN korrekt**“ erscheinen. Erfolgt nach der Aufforderung zur PIN-Änderung nicht innerhalb von 60 Sekunden eine Eingabe am Kartenlesegerät, wird die Anwendung aus Sicherheitsgründen beendet und der Änderungsprozess wird abgebrochen.

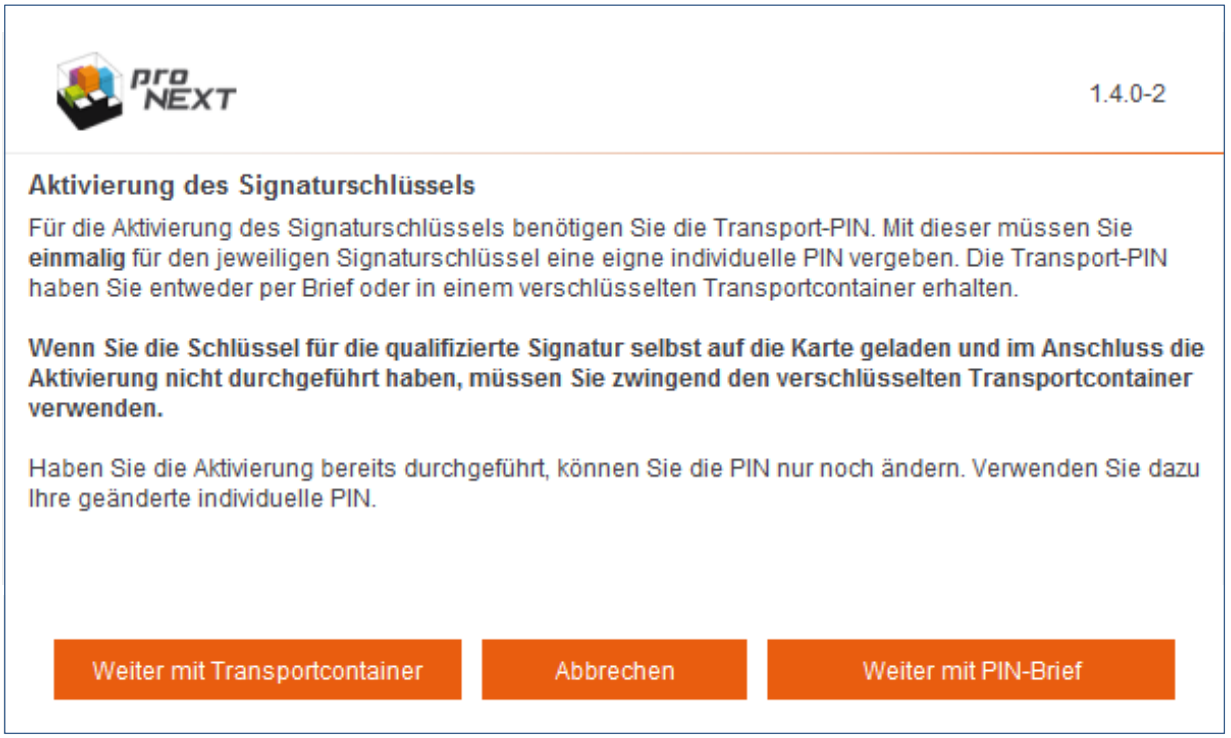
Achtung: Die unterstützte PIN-Länge beträgt 6 bis 12 Stellen.

2.2. Aktivierung des qualifizierten Signaturzertifikates (Qualified Multi/ PIN2)

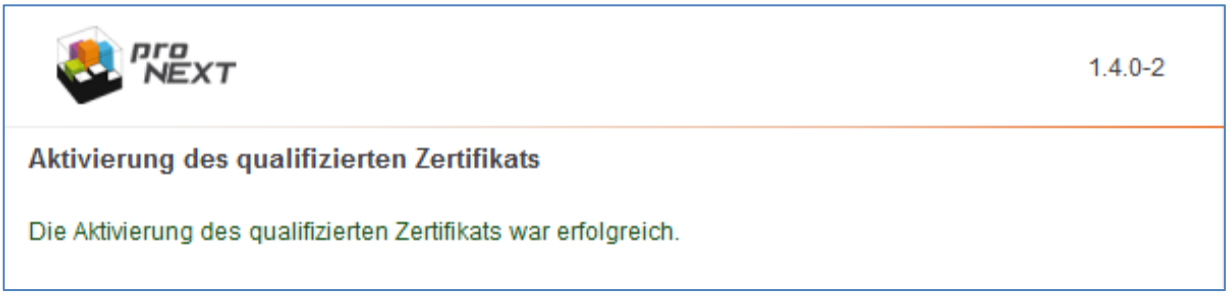
Für die Aktivierung des qualifizierten Signaturzertifikates benötigen Sie die 5-stellige Transport-PIN (PIN 2), aus dem PIN-Brief. Bitte klicken Sie zur Aktivierung in der Signaturkartenanwendung bei dem unteren Zertifikat (QUALIFIED MULTI) auf das Symbol „Schlüssel aktivieren“.



In dem sich öffnenden Fenster wählen Sie bitte die Option „Weiter mit PIN-Brief“.



Im nächsten Schritt müssen Sie die Transport-PIN in eine Ihnen bekannte PIN für das Signieren ändern, damit das qualifizierte Zertifikat aktiviert wird. Klicken Sie hierfür bitte auf „Weiter" und geben **nachdem** die Aufforderung „**PIN Änderung**" auf dem Display des Kartenlesers **erloschen ist** die 5-stellige Transport-PIN ein und bestätigen mit „OK". Im nächsten Schritt „PIN neu" vergeben Sie eine neue mindestens 6-stellige PIN für Ihre Signaturfunktion, drücken „OK" und geben diese PIN zur Bestätigung ein weiteres Mal ein. Auf dem Kartenlesegerät sollte nun „PIN korrekt" erscheinen sowie in der Signaturkartenanwendung der Hinweis: „Die Aktivierung des qualifizierten Zertifikats war erfolgreich". Erfolgt nach der Aufforderung zur PIN-Änderung nicht innerhalb von 60 Sekunden eine Eingabe am Kartenlesegerät, wird die Anwendung aus Sicherheitsgründen beendet und der Änderungsprozess wird abgebrochen.



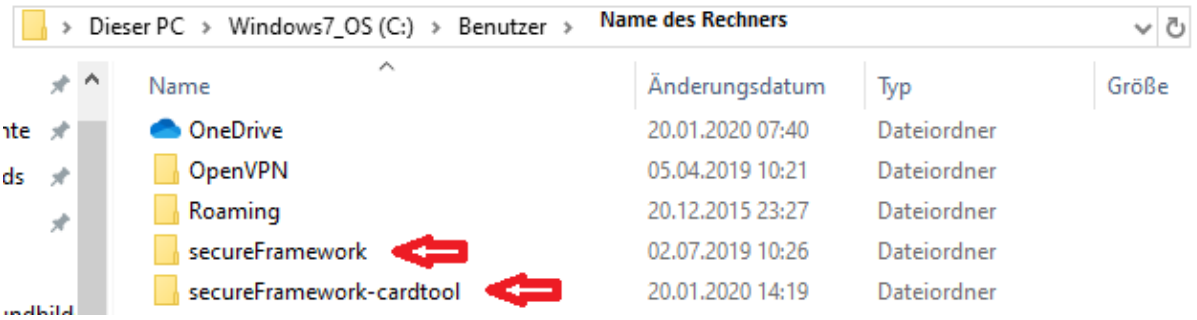
Achtung: Für die Aktivierung des qualifizierten Zertifikats, d.h. die Änderung der Transport-PIN, stehen Ihnen insgesamt 3 Versuche zur Verfügung, bis das Zertifikat aufgrund von Fehleingaben irreparabel gesperrt wird.

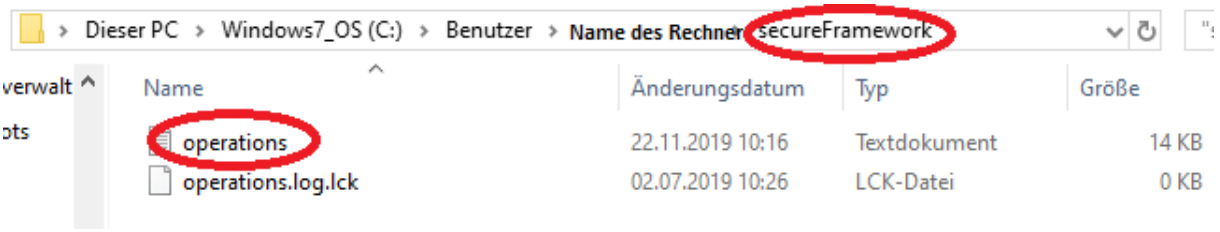
Sollte es während des Aktivierungsprozesses zu einem Fehler oder einer Fehleingabe gekommen bzw. die Anwendung unerwartet geschlossen worden sein, kontaktieren Sie in diesem Fall unseren Support unter sak@bnotk.de und übersenden uns bitte die Datei operations.log.

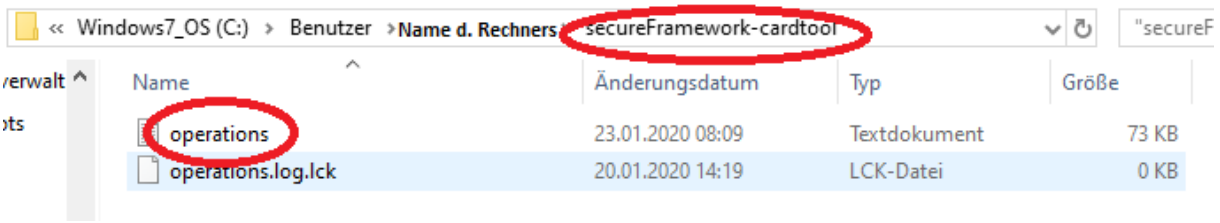
Unter Windows:

C:\Users\[Benutzername]\secureFramework\operations.log bzw.
C:\Benutzer\[Benutzername]\secureFramework\operations.log und

C:\Benutzer\[Benutzername]\secureFramework-cardtool\operations.log







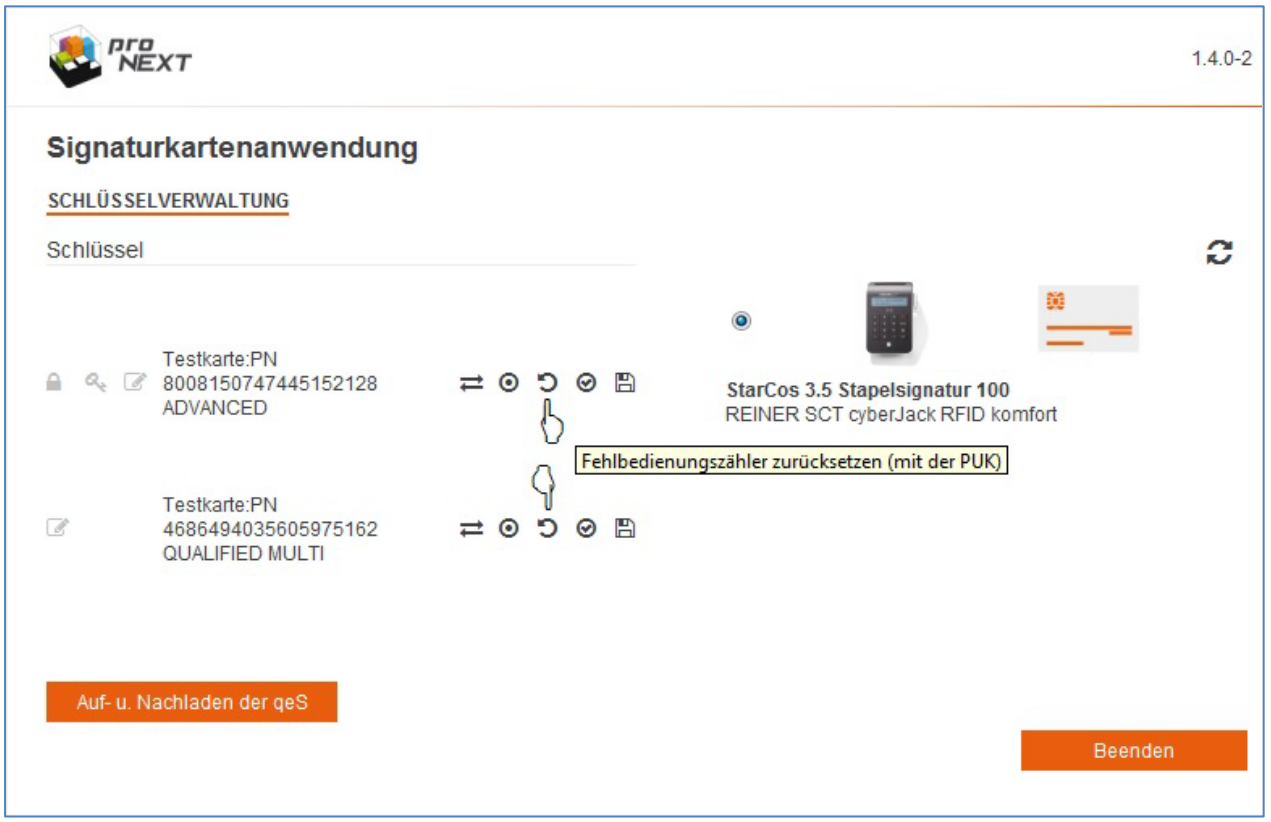
Unter Mac OS:

https://bea.bnotk.de/documents/operations.log_unter_Mac_OS_191024.pdf

2.3. PIN-Eingabe mit der PUK freischalten (Fehlbedienungszähler)

Sollten Sie Ihre PIN dreimal falsch eingegeben haben, wird die PIN-Eingabe gesperrt. Um die PIN-Eingabe wieder freizuschalten, wird die PUK aus dem PIN-Brief benötigt. Klicken Sie in diesem Fall in der Signaturkartenanwendung bei dem jeweiligen Zertifikat auf „Fehlbedienungszähler zurücksetzen" und geben Sie die PUK aus dem PIN-Brief ein. Nach erfolgreicher Eingabe ist die PIN-Eingabe wieder freigeschaltet.

Achtung: Es werden nicht die ursprünglichen PINs aus dem PIN-Brief wiederhergestellt, sondern lediglich der Fehlbedienungszähler für die PIN-Eingabe zurückgesetzt. Haben Sie Ihre PIN bereits erfolgreich geändert, bleibt diese bis zu einer weiteren Änderung aktiv, unabhängig vom Zurücksetzen des Fehlbedienungszählers mithilfe der PUK.



ADVANCED: PIN 1 (für die Anmeldung/ Authentisierung)

QUALIFIED MULTI: PIN 2 (für das Signieren)

3. Mögliche Fehlermeldungen/ Fehlerbehebung

3.1. PIN gesperrt bzw. Fehlbedienungszähler abgelaufen

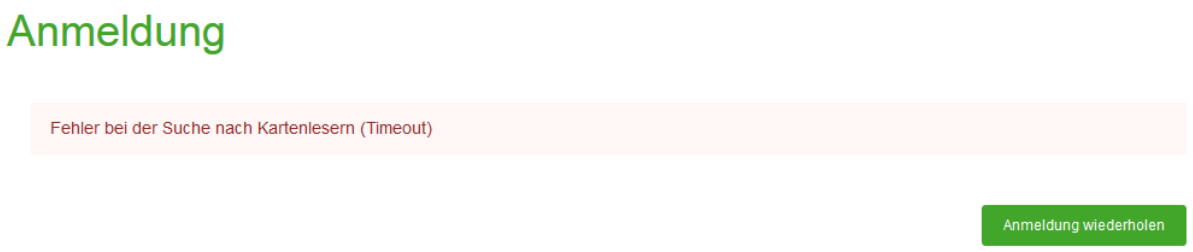
In diesem Fall gehen Sie bitte zu 2.3 PIN-Eingabe mit der PUK freischalten (Fehlbedienungszähler) und folgen den Anweisungen.

3.2. Karte noch nicht initialisiert/ Sie haben Ihre Karte noch nicht freigeschaltet

Möchten Sie eine Nachricht bzw. Anlage signieren und erhalten die zuvor genannte Fehlermeldung, haben Sie Ihr qualifiziertes Zertifikat noch nicht aktiviert bzw. die 5-stellige Transport-PIN noch nicht geändert. In diesem Fall gehen Sie bitte zu 2.2 Aktivierung des qualifizierten Signaturzertifikates (Qualified Multi/ PIN2) und folgen den Anweisungen.

3.3. Die Karte bzw. der Kartenleser wurde nicht gefunden

Sollte Ihre Karte nicht erkannt bzw. gefunden werden, prüfen Sie bitte, ob diese richtig eingesteckt ist. Es kann darüber hinaus hilfreich sein, die Karte noch einmal aus dem Lesegerät zu entfernen und erneut einzustecken.



Nach einem Klick auf „Anmeldung wiederholen" sollte die Karte erkannt werden. U. U. müssen Sie diese Prozedur mehrfach wiederholen. Bitte überprüfen Sie auch die korrekte Installation Ihres Kartenlesegerätes. Im Falle von Kartenlesern von ReinerSCT überprüfen Sie bitte im cyberJack Gerätemanager unter dem Reiter „Aktualisierung" und „Prüfe auf neue Versionen", dass die neueste Firmware für Ihr Kartenlesegerät installiert ist. Im Reiter Test kann die generelle Funktionsfähigkeit von Karte Kartenleser getestet werden.
Darüber hinaus kann es hilfreich sein, wenn Sie einmal den Browser wechseln

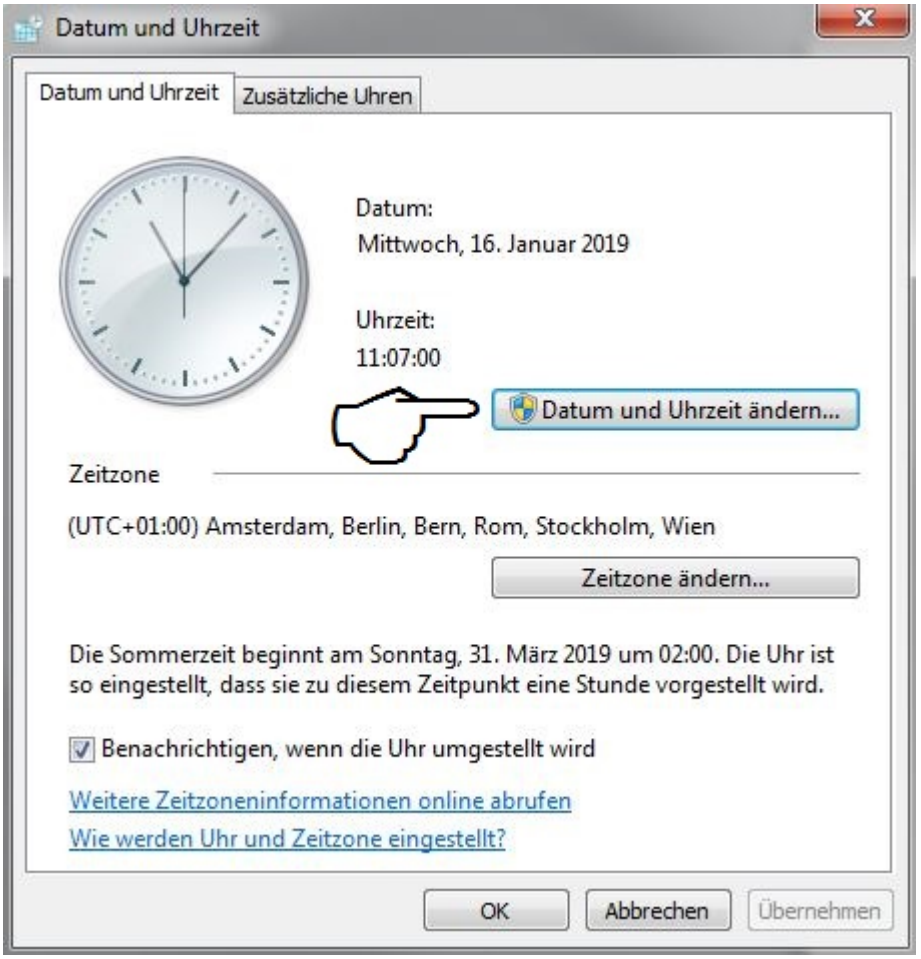
3.4. Systemzeit

Die Systemzeit liegt außerhalb der Toleranz

Sollte beim Starten der Signaturanwendungskomponente diese Fehlermeldung auftreten, ist die Abweichung Ihrer lokalen Systemzeit zur Serversystemzeit (https://www.uhrzeit.org/atomuhr) von bea.bnotk.de zu groß. Bitte überprüfen Sie Ihre lokale Systemzeit auf Ihrem Rechner.

Unter Windows:

Systemsteuerung | Datum und Uhrzeit | Datum und Uhrzeit ändern…



Sofern beim Versuch der Änderung der Uhrzeit Administratorrechte benötigt werden und diese nicht bekannt sind, wenden Sie sich bitte an Ihren zuständigen Systemadministrator.

BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Herausgeber:

Zertifizierungsstelle der
Bundesnotarkammer Burgmauer 53
50667 Köln

Stand: August 2021

https://zertifizierungsstelle.bnotk.de/