BUNDESNOTARKAMMER
ZERTIFIZIERUNGSSTELLE

Anleitung zur Zertifikatsverwaltung

Ihrer Signaturkarte und

Beantragung Ihrer Folgekarte

Erscheinungsdatum: 21.10.2019

Inhalt

1. Allgemeine Voraussetzungen

Unterstützte Betriebssysteme

- Microsoft Windows 7 - 10
- Apple Mac OS X 10
- Ubuntu Desktop 14.04 LTS

Java

Die Signaturkartenanwendung ist Java-basiert. Bitte stellen Sie sicher, dass Sie Java ab Version 8 auf Ihrem System installiert haben und aktualisieren diese bei Bedarf unter folgendem Link: https://java.com/de/download/.
Unter **Mac OS** und **Linux** wird das Java Development Kit benötigt.

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

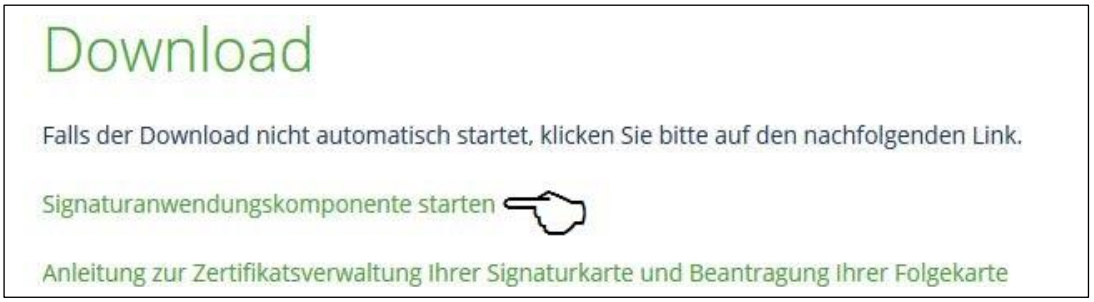
Für den erstmaligen Einsatz Ihrer Signaturkarte benötigen Sie den PIN-Brief, der Ihnen separat zu Ihrer Signaturkarte zugestellt wurde. Den PIN-Brief erhalten Sie, wenn Sie den Erhalt der zugehörigen Signaturkarte bestätigt haben, indem Sie auf den Link klicken, den wir Ihnen per E-Mail („Bestätigung 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

Öffnen Sie die Webseite https://zertifizierungsstelle.bnotk.de/sak und folgen bitte den Anweisungen auf dem Bildschirm. Die Anwendung zur PIN-Verwaltung ist Java-basiert und startet je nach verwendetem Browser automatisch. Bitte vergewissern Sie sich, dass Java ab Version 8 auf Ihrem Rechner installiert ist.
Sollte die Anwendung ‚cardtool.jnlp' in Ihrem Browser nicht automatisch geöffnet werden, führen Sie diesen Schritt bitte manuell durch.

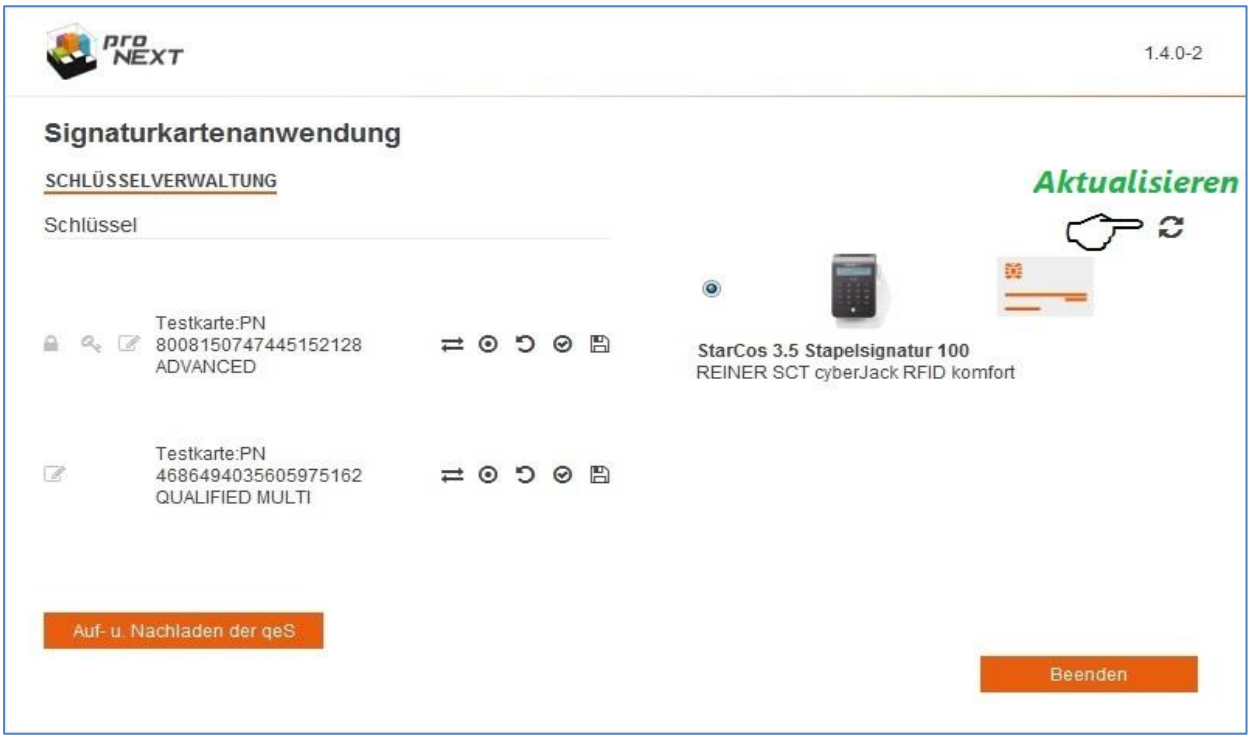


Unter Umständen befindet sich die Anwendung ‚cardtool.jnlp' in Ihrem Download-Verzeichnis und ist aus diesem zu öffnen. In der Regel wird die Anwendung bei installiertem Java automatisch mit dem Java Web Start Launcher gestartet. Sollte die Datei nicht korrekt mit dem Java Web Start Launcher geöffnet werden, sondern mit einer anderen Anwendung, muss die Dateiverknüpfung neu gesetzt werden (siehe 4.5).

Die Einrichtung bzw. die PIN-Änderung Ihrer neuen Signaturkarte können Sie alternativ auch über Ihre bereits eingesetzte Signaturkartenanwendung, wie z.B. SigNotar durchführen.

Start der Anwendung

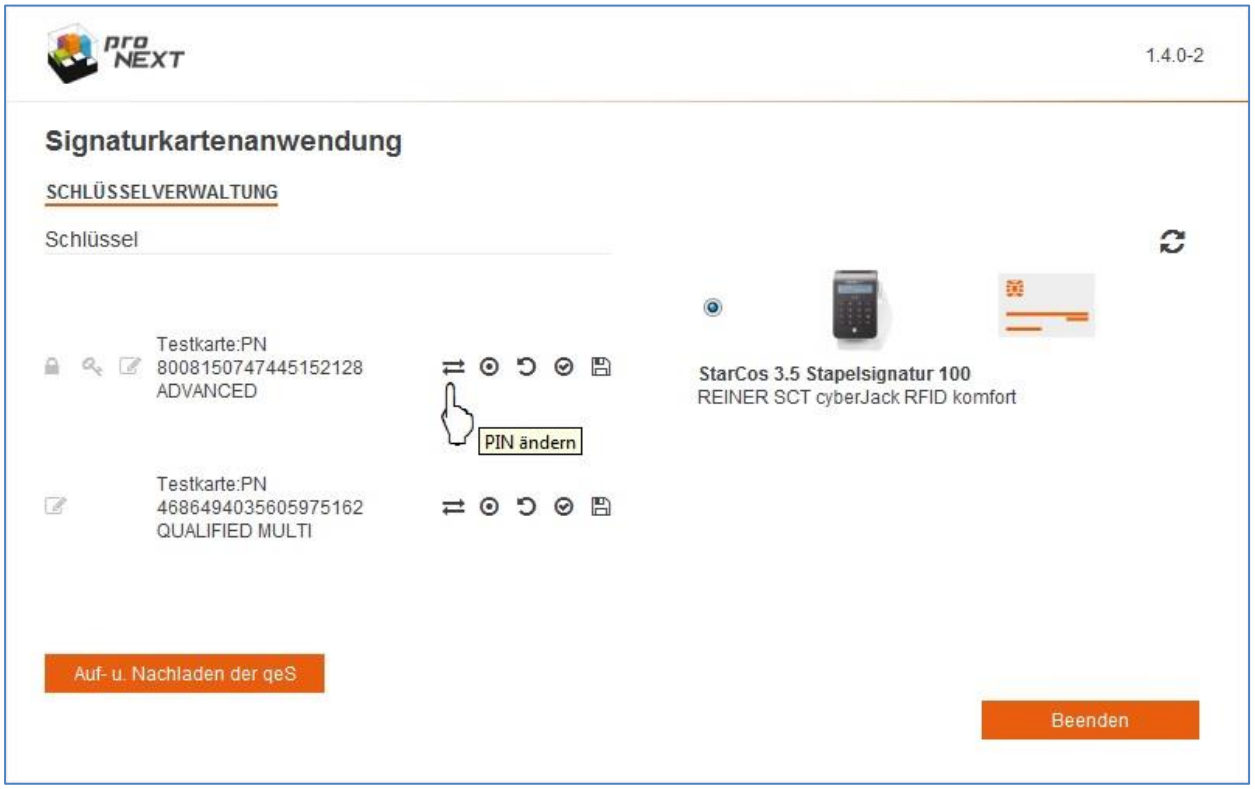
Insofern das Kartenlesegerät ordnungsgemäß angeschlossen und Ihre Signaturkarte eingesteckt ist, sollte die Anwendung wie unten dargestellt beides darstellen. Werden Kartenlesegerät und Signaturkarte nicht angezeigt, prüfen Sie bitte, ob beides korrekt angeschlossen ist und klicken auf den Button „Aktualisieren".



PIN-Änderung

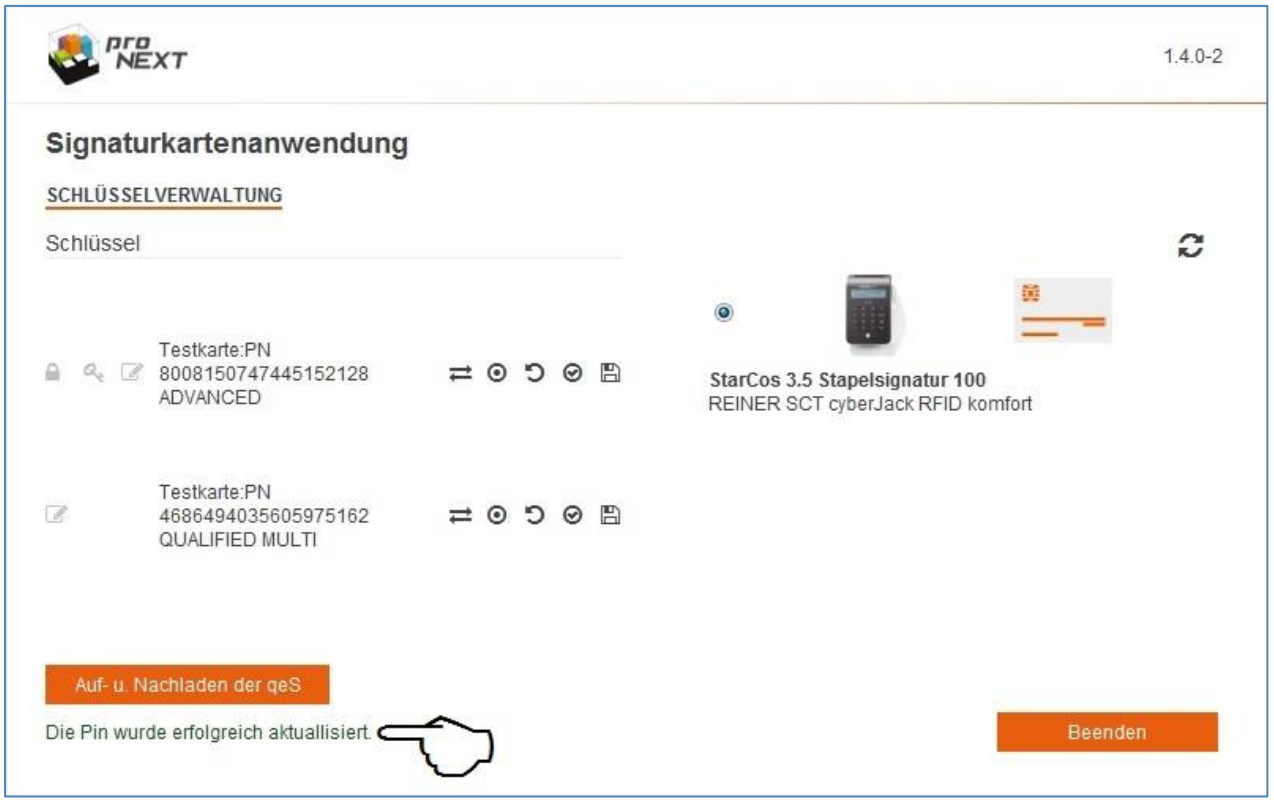
PIN für die Anmeldung (fortgeschrittenes Zertifikat/ADVANCED)

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".



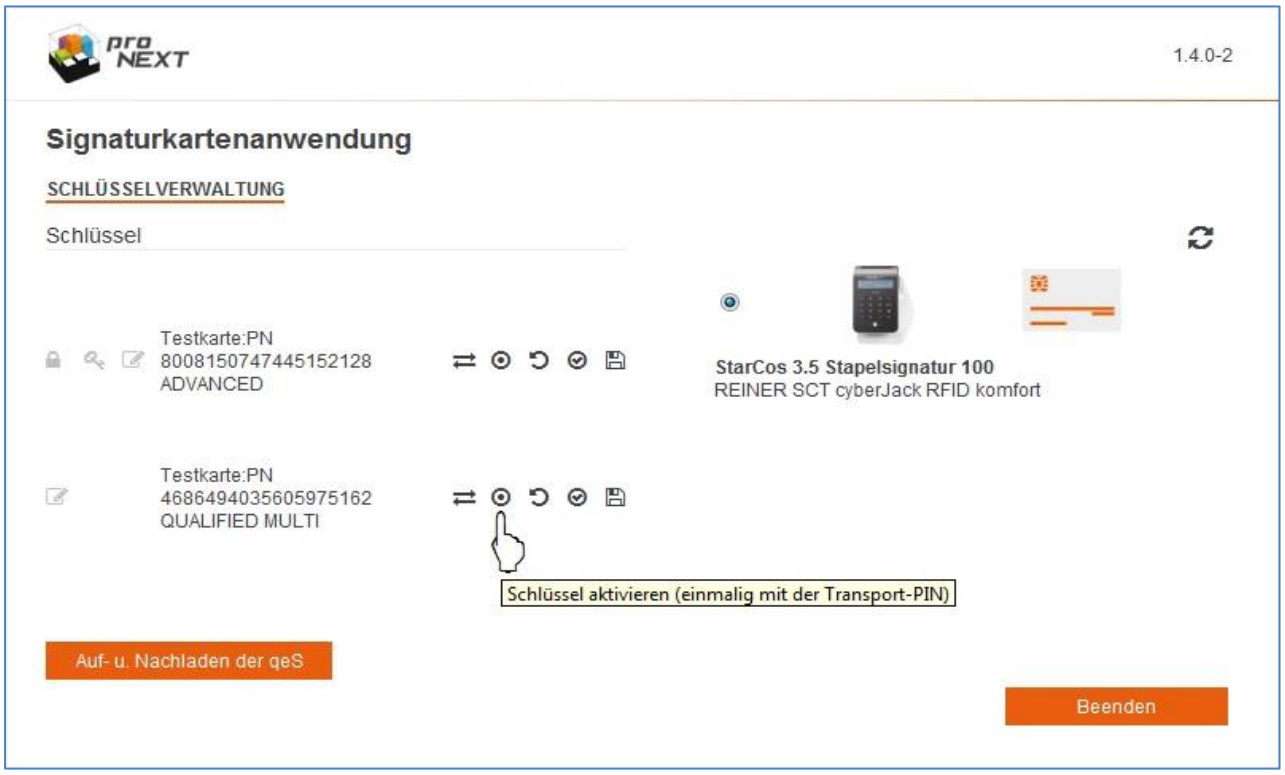
Der Änderungsprozess wird auf dem Display Ihres Kartenlesegeräts mit dem Befehl „PIN Änderung" eingeleitet. Sobald auf dem Display Ihres Kartenlesegerätes „PIN" angezeigt wird, geben Sie bitte die PIN 1 aus dem Ihnen separat zur Signaturkarte zugestellten PIN-Brief ein und drücken die Taste „OK". Im 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 sowie in der Signaturkartenanwendung der Hinweis, dass Sie Ihre PIN erfolgreich aktualisiert haben. 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.

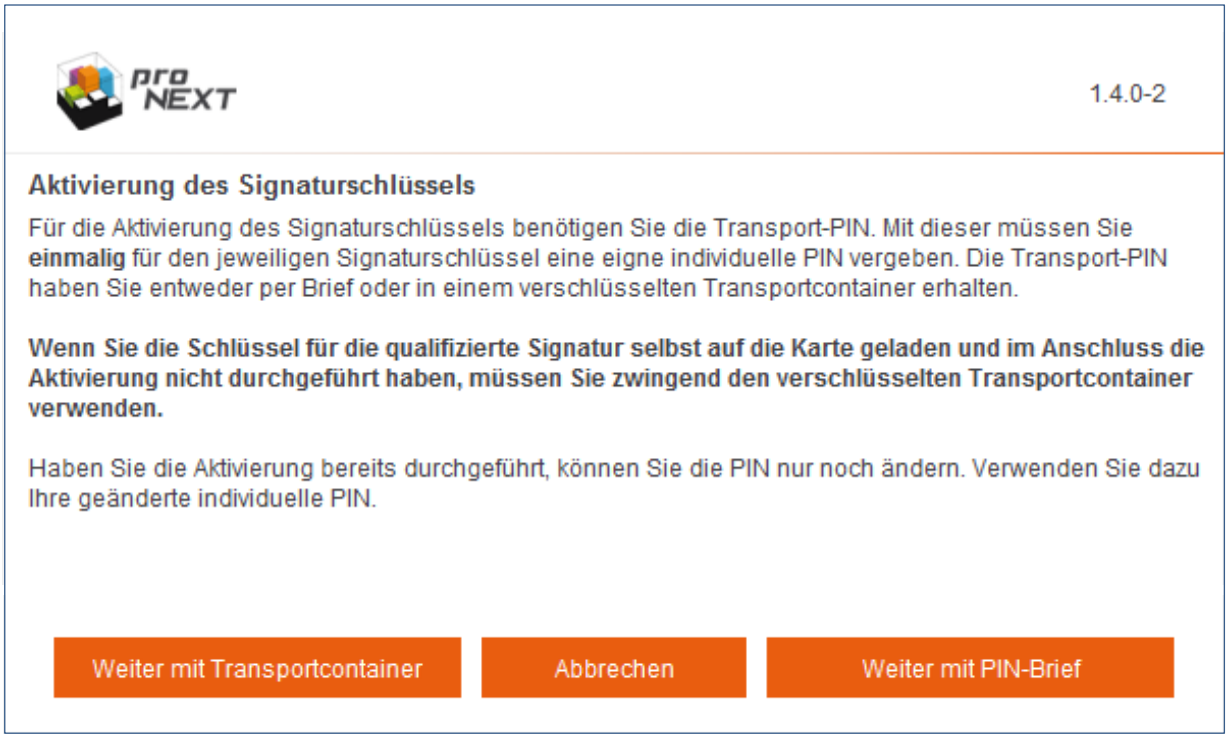


2.2. Aktivierung des qualifizierten Signaturzertifikates (Qualified Multi/ PIN2)

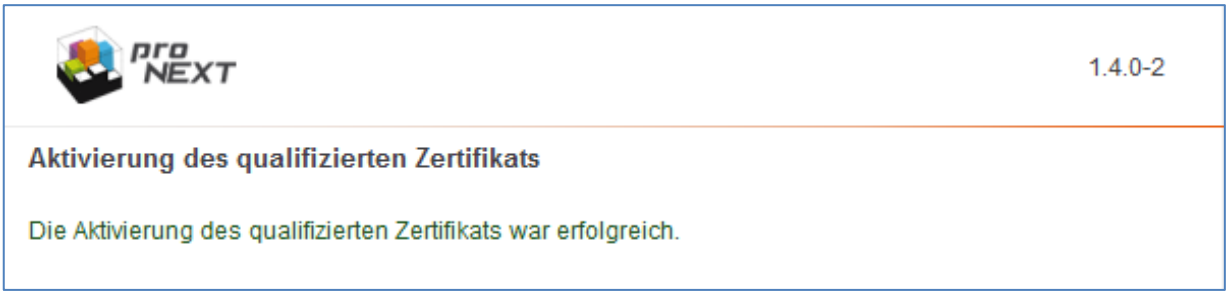
Für die Aktivierung des qualifizierten Signaturzertifikates benötigen Sie die 5-stellige Transport-PIN (PIN 2), aus dem PIN-Brief. Bitte klicken Sie zur Aktivierung in der Signaturkartenanwendung bei dem unteren Zertifikat (QUALIFIED MULTI) auf das Symbol „Schlüssel aktivieren".



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.

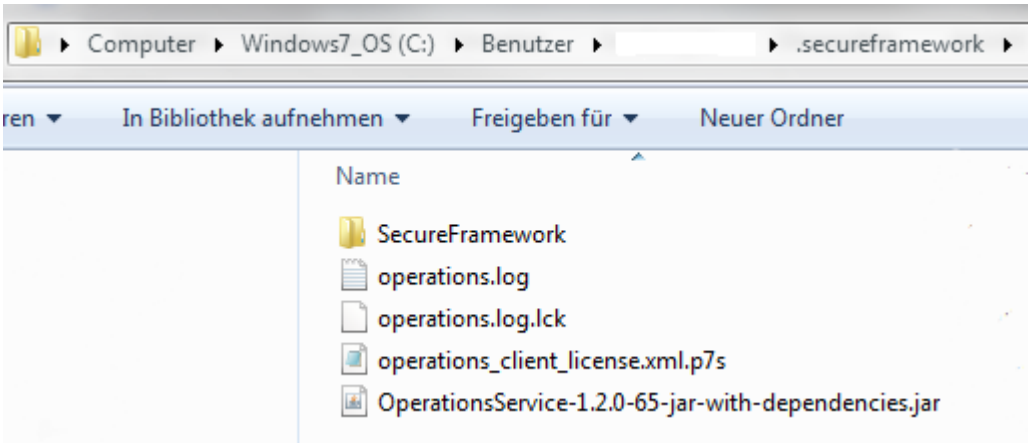
Unter Windows:

C:\Users\[Benutzername]\.secureframework\operations.log bzw.

C:\Benutzer\[Benutzername]\.secureframework\operations.log

Mac OS:

/Users/[Benutzername]/.secureframework/operations.log



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)

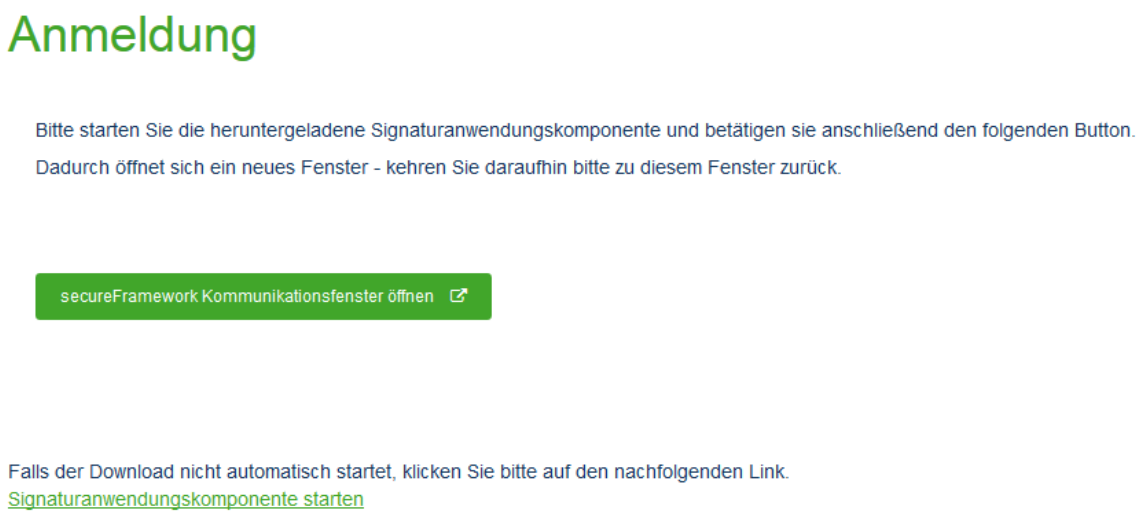
QUALIFIED MULTI: PIN 2 (für das Signieren)

3. Beantragung Ihrer Folgekarte

Sollte die Gültigkeit Ihrer Signaturkarte in Kürze ablaufen, werden Sie von uns rechtzeitig auf elektronischem Weg über die weiteren Schritte zur Beantragung Ihrer Folgekarte informiert. Bitte halten Sie hierfür folgende Dinge bereit:

- Benachrichtigung zu Ihrer Folgekarte mit dem Link zum Start des Folgekartenprozesses
- Bestehende und zu tauschende Signaturkarte
- PIN-Brief bzw. PIN2 für die Anmeldung/ Authentisierung
- Ggf. eine beidseitige digitale Kopie Ihres Ausweisdokumentes im PDF-Format (wird benötigt, falls Ihr bei der Antragstellung für Ihre Signaturkarte angegebenes Identifikationsdokument abgelaufen ist)
- Kartenlesegerät der Sicherheitsklasse 3

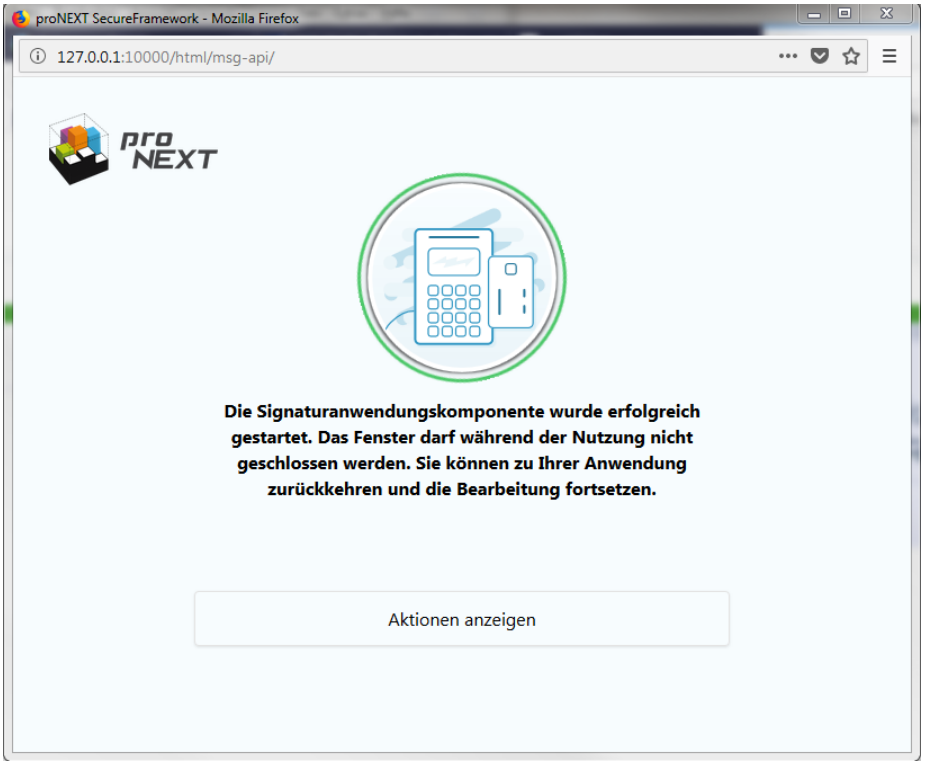
Insofern die zuvor genannten Voraussetzungen erfüllt sind, klicken Sie bitte auf den Link in der „Benachrichtigung zu Ihrer Folgekarte". Sie werden nun auf die unten Anmeldeseite zur Folgekarte weitergeleitet.



Sollte die für die Anmeldung notwendige Java-Anwendung nicht automatisch starten, klicken Sie bitte auf „Signaturanwendungskomponente starten" und bestätigen den aufkommenden Dialog mit „OK". Bitte warten Sie, bis die Anwendung vollständig heruntergeladen und gestartet wurde. Sie erkennen das an dem folgenden Symbol in Ihrer Taskleiste.

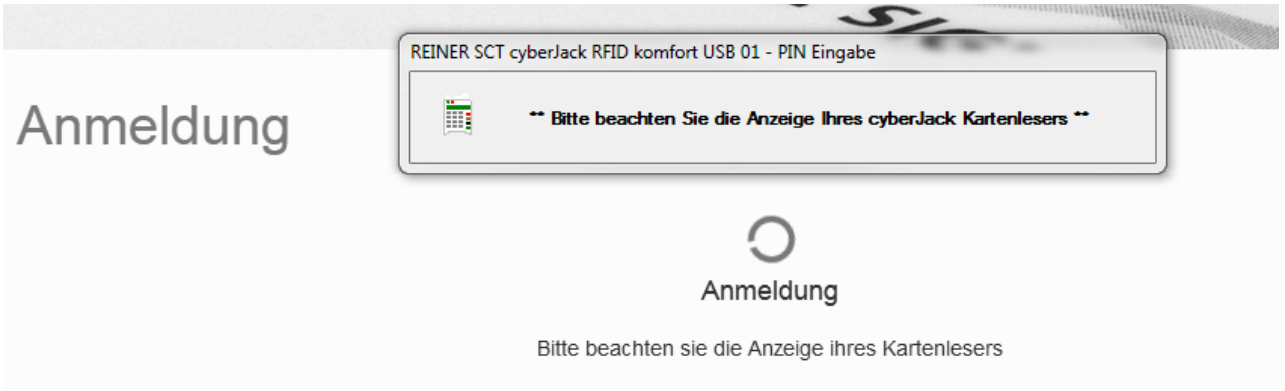
Danach klicken Sie bitte auf die grüne Schaltfläche „secureFramework Kommunikationsfenster öffnen" und

lassen das sich öffnende Fenster im Hintergrund laufen.



Es wird nun Ihre Signaturkarte vom Kartenlesegerät ausgelesen, bis Ihr Name angezeigt wird.

Sie können im Anschluss auf der Anmeldeseite auf „Anmelden" klicken und werden zur Eingabe Ihrer PIN (PIN 1 bzw. PIN für die Anmeldung/ Authentisierung) aufgefordert.

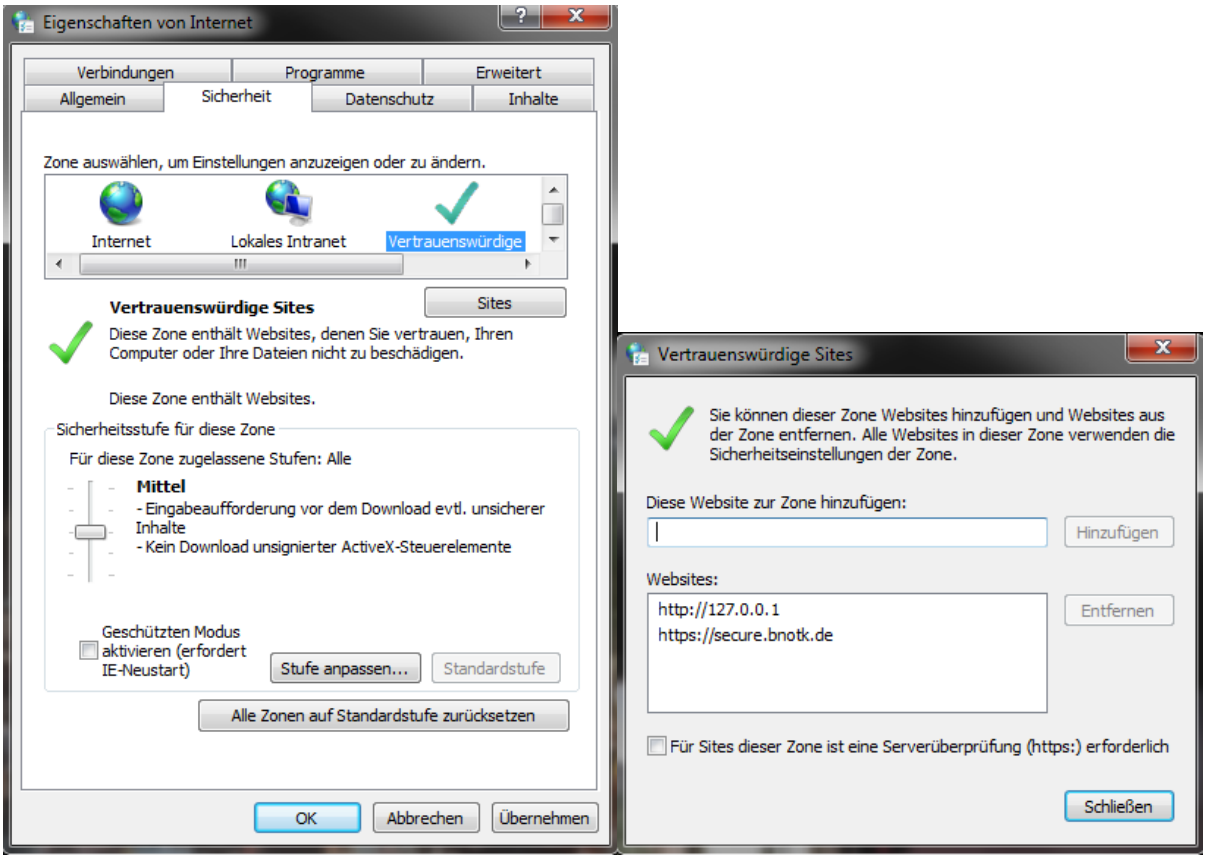


Nachdem Sie Ihre PIN korrekt eingegeben haben, sind Sie erfolgreich angemeldet und können mit der Beantragung der Folgekarte beginnen. Bitte folgen Sie hierzu den Angaben im Folgekartenprozess und aktualisieren bei Bedarf Ihre bei uns hinterlegten Antrags- bzw. persönlichen Daten.

Internet Explorer

Für die Anmeldung am Folgekartenantrag mit Internet Explorer sind folgende Einstellungen in den Internetoptionen vorzunehmen.

- Öffnen Sie im Internet Explorer oder über die Systemsteuerung die Internetoptionen
- Wechseln Sie zum Reiter „Sicherheit" und wählen die Zone „Vertrauenswürdige Sites" aus



- Klicken Sie auf „Sites" und fügen bitte die folgenden Internetseiten hinzu:
    - http://127.0.0.1
    - https://secure.bnotk.de
- evtl. Haken vor "Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich" entfernen
- Bitte schließen Sie das Fenster und wechseln zur Zone „Internet"
- Setzen Sie bitte **nur in dieser Zone** den Haken bei „Geschützten Modus aktivieren"

Nach einem Neustart des Internet Explorers sollte die Anmeldung am Folgekartenantrag laufen.

4. Mögliche Fehlermeldungen/ Fehlerbehebung

4.1. PIN gesperrt bzw. Fehlbedienungszähler abgelaufen

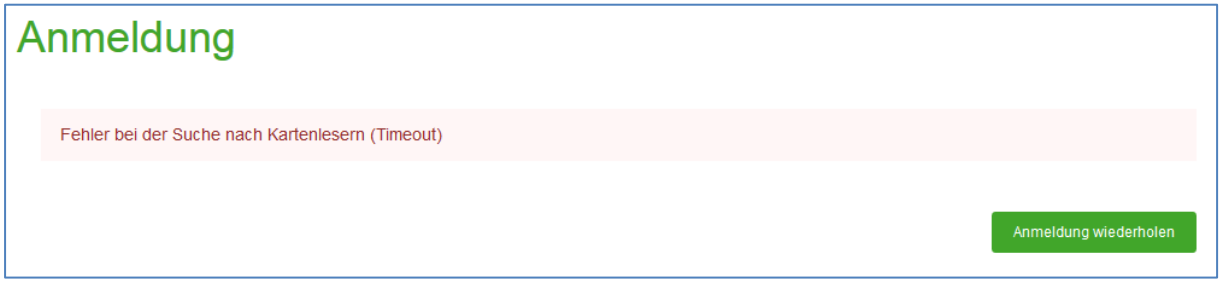
In diesem Fall gehen Sie bitte zu 2.3 PIN-Eingabe mit der PUK freischalten (Fehlbedienungszähler) und folgen den Anweisungen.

4.2. 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.

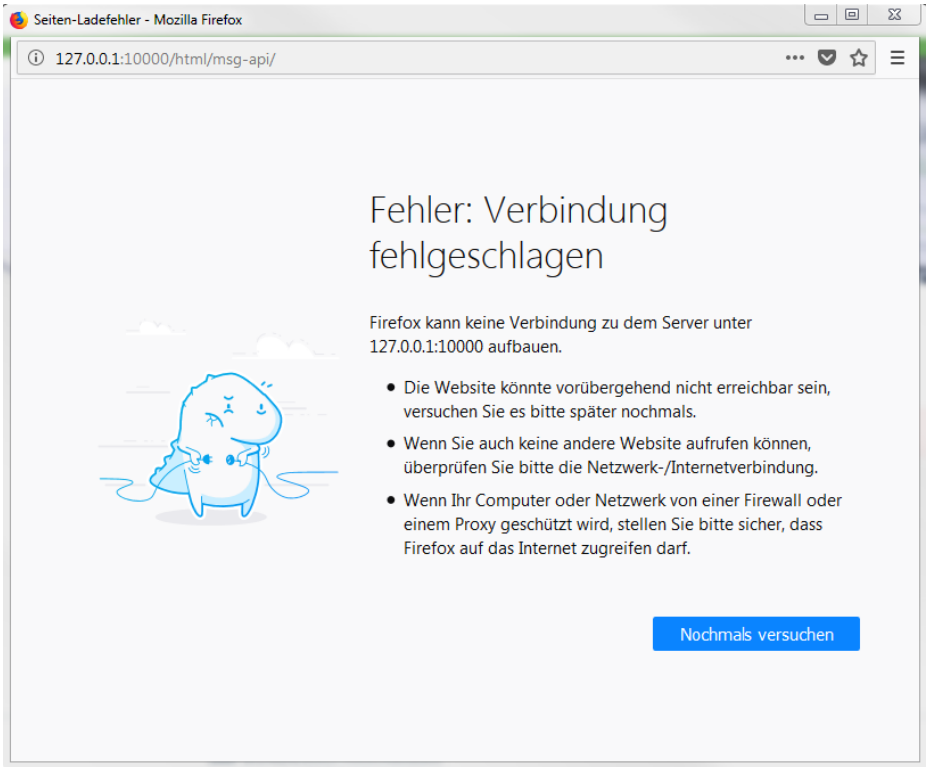
4.3. Die Karte bzw. der Kartenleser wurde nicht gefunden

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.

4.4. Fehler: Verbindung fehlgeschlagen



In diesem Fall wurde die Java-Anwendung nicht ordnungsgemäß heruntergeladen und gestartet. Bitte schließen Sie alle Browserfenster und löschen den Ordner .secureframework:

Unter Windows:

C:\Users\[Benutzername]\.secureframework

C:\Benutzer\[Benutzername]\.secureframework

Mac OS:

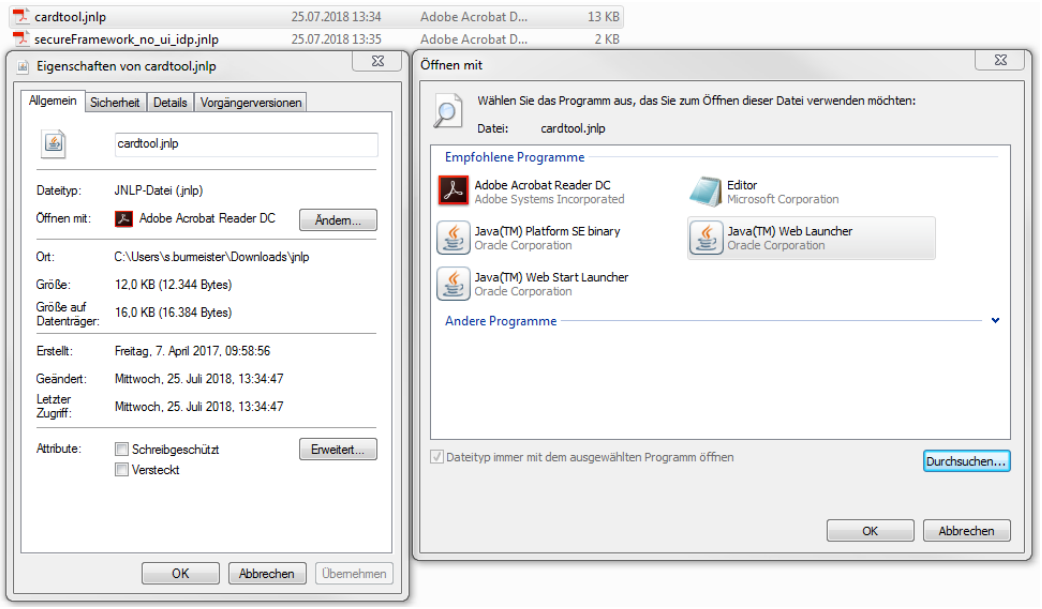
/Users/[Benutzername]/.secureframework/

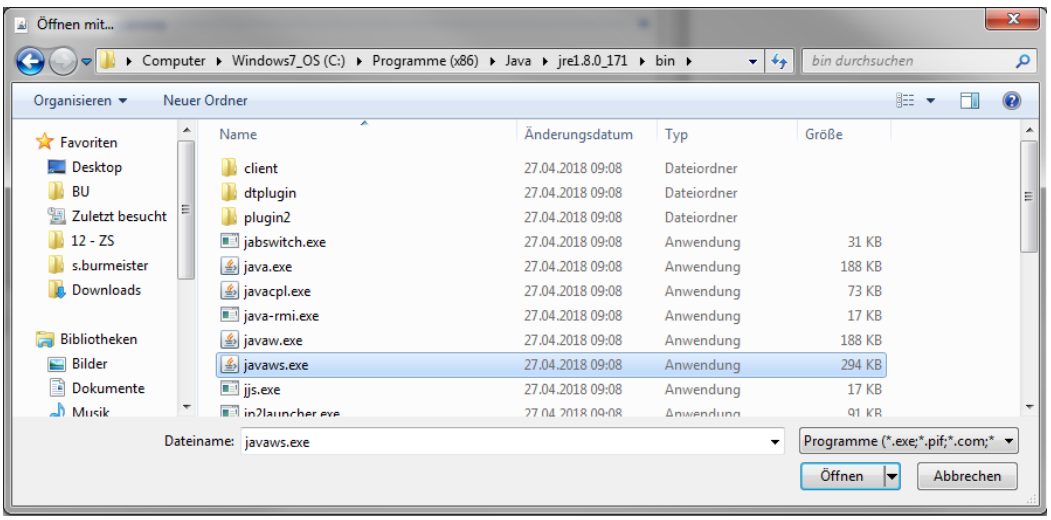
Bitte öffnen Sie danach die E-Mail zum Start des Folgekartenprozesses erneut und starten die Java-Anwendung gemäß 2 PIN-Verwaltung. Sollten weiterhin Verbindungsprobleme auftreten, wechseln Sie bitte einmal den Browser. Bei anhaltenden Verbindungsproblemen übersenden Sie uns bitte die Datei operations.log analog Seite 9.

4.5. Java

Verknüpfung mit dem Java Web Start Launcher herstellen

Werden unsere Java-Anwendungen (jnlp-Datei) nicht korrekt mit dem Java Web Start Launcher geöffnet, kann unsere Anwendung nicht starten und die Dateiverknüpfung muss neu gesetzt werden.
Bitte laden Sie zu diesem Zweck eine unserer Java-Dateien, z.B. auf https://zertifizierungsstelle.bnotk.de/sak herunter und speichern diese. Im nächsten Schritt öffnen Sie bitte diese Datei mit einem Rechtsklick und gehen auf „Eigenschaften". Klicken Sie bitte wie unten dargestellt auf „Ändern" und in dem neuen Fenster auf „Durchsuchen", sollte der Java Web Start Launcher nicht bereits bei den empfohlenen Programmen erscheinen. Danach wählen Sie bitte die Datei „javaws.exe" im dargestellten Pfad aus. Je nach Betriebssystem liegt der Ordner Java in „Programme" oder „Programme (x86)". Bitte achten Sie darauf, dass ein Häkchen bei „Dateityp immer mit dem ausgewählten Programm öffnen" gesetzt ist.





Java-Konsole anzeigen

Aus der Java-Konsole können bei Verbindungsproblemen weitere Informationen bezogen werden. Um diese zu aktivieren, gehen Sie bitte wie folgt vor:

Unter Windows:

Gehen Sie bitte dazu in die Systemsteuerung und Öffnen das Element „Java". Klicken Sie bitte in dem sich öffnenden Fenster auf den Reiter „Erweitert" und markieren in diesem Fenster unter der Überschrift „Java-Konsole" den Punkt „Konsole anzeigen". Bei dem nächsten Start der Anwendung zur PIN-Verwaltung öffnet sich nun zusätzlich die Java-Konsole und zeichnet im Hintergrund die Java-Aktivitäten auf. Klicken Sie bitte in der Java-Konsole auf „Kopieren" und senden uns diese Daten zu.

Mac OS:

1. Klicken Sie auf das Apple-Symbol in der oberen linken Ecke des Bildschirms.
2. Gehen Sie zu „Systemeinstellungen…"
3. Klicken Sie auf das Java-Symbol, um das Java Control Panel aufzurufen.
4. Aktivieren Sie bitte unter dem Punkt „Erweitert" die Java-Konsole.

Bei dem nächsten Start der Anwendung zur PIN-Verwaltung öffnet sich nun zusätzlich die Java-Konsole und zeichnet im Hintergrund die Java-Aktivitäten auf. Klicken Sie bitte in der Java-Konsole auf „Kopieren" und senden uns diese Daten zu.

4.6. 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: Oktober 2019

https://zertifizierungsstelle.bnotk.de/