

Anleitung zur Zertifikats- verwaltung Ihrer beA-Karte

(PIN-Änderung, Auf- und Nachladen
des qualifizierten Signaturzertifikats)



beA - besonderes
elektronisches
Anwaltspostfach



Inhaltsverzeichnis

1. Allgemeine Voraussetzungen	Seite 3
2. Schritt-für-Schritt-Anleitung zur PIN-Änderung	Seite 4
Öffnen der Anwendung zur PIN-Änderung	4
PIN-Änderung	5
Häufige Fehlermeldungen	6
3. Schritt-für-Schritt-Anleitung für das Auf- bzw. Nachladen des qualifizierten Signaturzertifikats	Seite 8
Signaturrechtlicher Antrag	8
Anmeldung	8
Herunterladen des elektronischen Transportcontainers	9
Auf- und Nachladen des qualifizierten Zertifikats	10
4. beA-Postfach	Seite 12
Kein geeigneter Sicherheits-Token gefunden	12
Karte noch nicht initialisiert / Sie haben Ihre Karte noch nicht freigeschaltet	12
5. Problembehandlung	Seite 14
Sicherheitsprogramme	14
Proxy-Server	14
Datev	15
Systemuhrzeit	15
Java	16
Die Verbindung zur Server-Komponente ist fehlgeschlagen / Bitte überprüfen Sie, ob die lokale proNEXT Secure Framework Komponente gestartet wird.	18

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 die aktuellste Java-Version auf Ihrem System installiert haben und aktualisieren diese bei Bedarf unter folgendem Link: <https://java.com/de/download/>

Mac OS

Hier ist es erforderlich, das Development Kit in der aktuellsten Version (<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>) zu installieren.

Unterstützte Chipkartenlesegeräte

Für die Änderung Ihrer PIN-Daten bzw. das Auf- oder Nachladen des qualifizierten Signaturzertifikates mithilfe der Signaturkartenanwendung ist ein nach Signaturgesetz bestätigtes 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 e-com 3.0
- 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/>

Sollten 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 beA-Karte benötigen Sie die Initial-PIN aus dem Ihnen separat zu Ihrer beA-Karte zugestellten PIN-Brief. Den PIN-Brief erhalten Sie, wenn Sie den Erhalt der zugehörigen beA-Karte bestätigt haben, indem Sie auf den Link klicken, den wir Ihnen per E-Mail nach Produktion der beA-Karte zugesandt haben. Wir empfehlen Ihnen, die darin befindliche PIN mithilfe der folgenden Anleitung umgehend in eine neue PIN zu ändern.

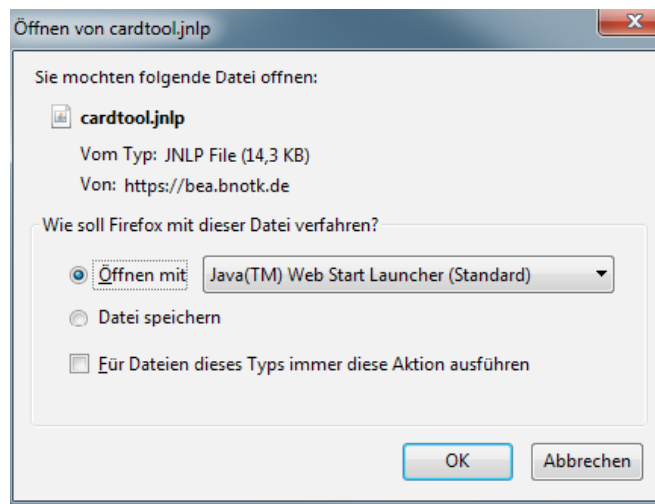




2. Schritt-für-Schritt-Anleitung zur PIN-Änderung

Öffnen der Anwendung zur PIN-Änderung

Öffnen Sie die Webseite <https://bea.bnotk.de/sak/> und folgen Sie bitte den Anweisungen auf dem Bildschirm. Die Anwendung zur PIN-Verwaltung ist Java-basiert und zeigt nach dem Aufruf der Website den folgenden Dialog. Bitte vergewissern Sie sich, dass die aktuellste Java-Version auf Ihrem Rechner installiert ist.



Bitte bestätigen Sie den Dialog und öffnen die Datei mit dem Java Web Start Launcher wie dargestellt. 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 [Problembehandlung Java](#)).

Bitte achten Sie darauf, dass die jnlp-Datei direkt geöffnet und nicht separat gespeichert wird.

Mac OS

Sollte Ihnen unter OSX angezeigt werden, dass die Anwendung von einem nicht verifizierten Entwickler stammt, gehen Sie bitte wie folgt vor:

Bitte öffnen Sie die Systemeinstellungen und wählen dort „Sicherheit“ aus. Hier findet sich im Reiter „Allgemein“ der Hinweis: „Das Öffnen von ‚secureFramework_no_ui.jnlp‘ wurde blockiert, da die App nicht von einem verifizierten Entwickler stammt.“ Bitte aktivieren Sie den Schalter „Dennoch öffnen“.

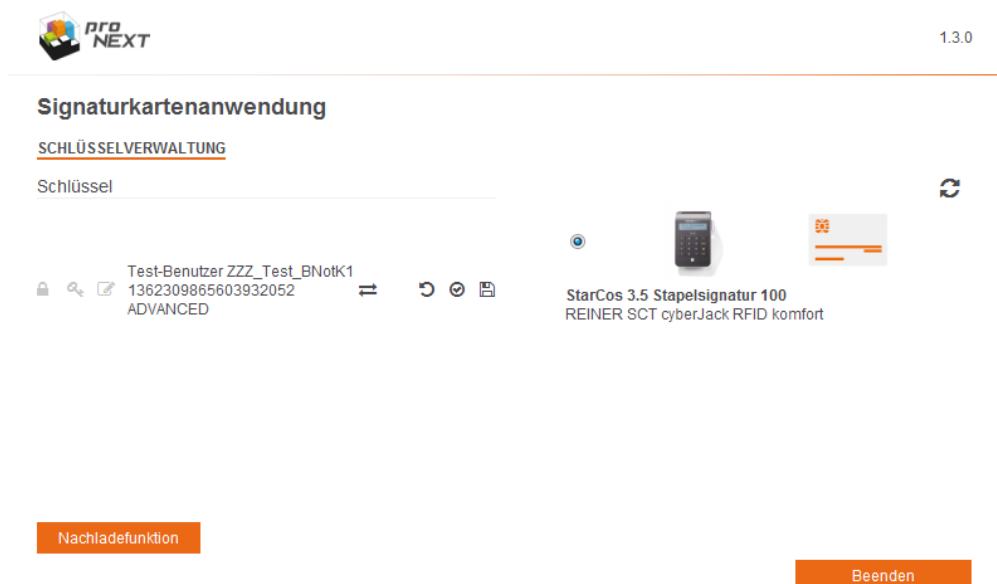
Öffnen Sie jetzt die Internetseite mit der Anwendung erneut. Es erscheint eine Dialogbox mit dem Hinweis „secureFramework_no_ui.jnlp ist ein aus dem Internet geladenes Programm. Möchten Sie es wirklich öffnen?“. Bitte klicken Sie hier auf „Öffnen“, jetzt sollte die Anwendung starten. Unter Umständen erscheint an dieser Stelle eine weitere Dialogbox, in der gefragt wird: „Möchten Sie diese Anwendung ausführen?“ Bitte klicken Sie in diesem Fall auf „Ausführen“. Sollte es weiterhin nicht starten, laden die Seite bitte erneut.

Eine weitere Möglichkeit ist, die Anwendung manuell zu starten, indem Sie im Download-Ordner auf diese (doppel-)klicken.

Auswählen des Kartenlesegeräts


Auf der rechten Seite der Anwendung werden Ihnen die angeschlossenen Kartenlesegeräte angezeigt. Bitte vergewissern Sie sich vorab, dass Ihr Kartenlesegerät angeschlossen ist und Sie Ihre beA-Karte in das Gerät eingesteckt haben.

Die Anwendung erkennt das Kartenlesegerät nur, wenn sich in diesem eine beA-Karte befindet. Sollte Ihr Kartenlesegerät nicht angezeigt werden, prüfen Sie bitte, ob die beA-Karte richtig eingesteckt 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 nach dem Erhalt der Karte zu ändern. Klicken Sie hierzu auf das Symbol  „Pin ändern“.



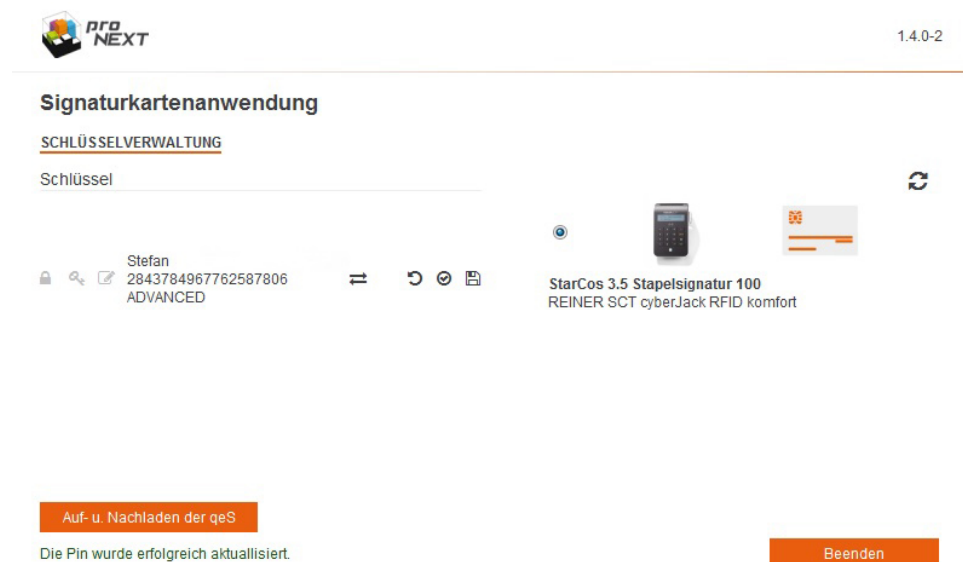
Der Änderungsprozess wird auf dem Display Ihres Kartenlesegeräts mit dem Befehl „PIN Änderung“ eingeleitet. Sobald auf dem Display Ihres Kartenlesegeräts „PIN“ angezeigt wird, geben Sie bitte die PIN aus dem Ihnen separat zur beA-Karte zugestellten PIN-Brief ein und drücken die Taste „OK“. Im nächsten Schritt „Pin neu“ vergeben Sie eine neue mindestens 6-stellige PIN für Ihre beA-Karte und bestätigen diese ein weiteres Mal. Erfolgt nach der



Aufforderung zur PIN-Änderung nicht innerhalb von 60 Sekunden eine Eingabe am Kartenlesegerät, wird die Anwendung aus Sicherheitsgründen beendet.


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

Nachdem Sie die neue PIN bestätigt haben, erhalten Sie im unteren Bereich der Anwendung den Hinweis, dass die PIN erfolgreich aktualisiert wurde.



Häufige Fehlermeldungen

Der Bedienzähler ist abgelaufen / PIN-Eingabe mit der PUK freischalten

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 wird nicht die ursprüngliche PIN 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.

„Bitte überprüfen Sie, ob die lokale proNEXT Secure Framework Komponente gestartet ist.“

Sollte Ihnen anstatt der Meldung „Die Pin wurde erfolgreich aktualisiert“ in der Signaturkartenanwendung angezeigt werden: „Bitte überprüfen Sie, ob die lokale proNEXT Secure Framework Komponente gestartet ist.“, wurde Ihre PIN sehr wahrscheinlich erfolgreich geändert. In diesem Fall gab es einen Fehler in der Übertragung vom Kartenlesegerät zu der Anwendung. Sollte jedoch am Ende des Prozesses „PIN bzw. PUK korrekt“ auf dem Display Ihres Kartenlesers erscheinen, war der Vorgang in jedem Fall erfolgreich.

Um wirklich sicher zu gehen, dass die PIN-Änderung erfolgreich war, senden Sie uns bitte die Datei operations.log an bea@bnotk.de.

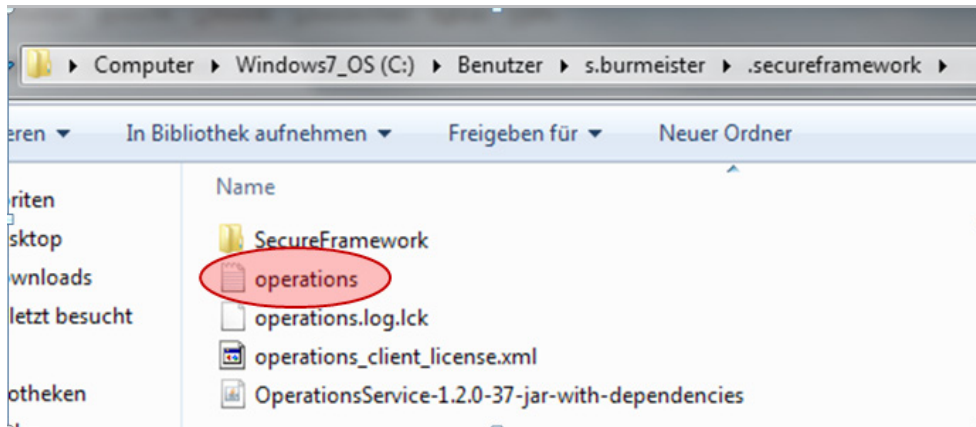
Unter Windows:

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

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

Mac OS:

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



PIN für das qualifiziert elektronische Signieren (qualifiziertes Zertifikat / qualified multi)

Sollten Sie auf Ihre beA-Karte Signatur bereits das qualifizierte Zertifikat erfolgreich aufgeladen haben (siehe Schritt 3), zeigt die Signaturkartenanwendung auf der linken Seite zwei verschiedene Einträge bzw. Zertifikate. Neben dem fortgeschrittenen Zertifikat (Advanced) für die Authentisierung wird weiterhin das qualifizierte Zertifikat (qualified multi) für das qualifiziert elektronische Signieren angezeigt.

Bitte beachten Sie, dass eine PIN-Änderung für das qual. Zertifikat erst erfolgen kann, wenn dieses erfolgreich aufgeladen **und** aktiviert wurde. Anderenfalls kann es zu einer irreparablen Sperrung des Zertifikats kommen.



3. Schritt-für-Schritt-Anleitung für das Auf- bzw. Nachladen des qualifizierten Signaturzertifikats (optional)

Signaturrechtlicher Antrag

Bevor Sie das qualifizierte Signaturzertifikat auf- bzw. nachladen können, ist zunächst ein signaturrechtlicher Antrag zu stellen. Inhaber einer beA-Karte Signatur bekommen automatisch eine E-Mail mit den erforderlichen Schritten für den Antragsprozess.

Alternativ ist es jederzeit möglich, den Antragsprozess nach der erfolgreichen Anmeldung an unserem Bestellportal <https://bea.bnotk.de/bestellung/#/products> mit Klicks auf „Mein Konto“ und „Aufladeverfahren“ zu starten. Bitte beachten Sie, dass für die Anmeldung ein angeschlossenes Kartenlesegerät samt eingesteckter beA-Karte erforderlich ist.

Anschließend ist nach dem Signaturrecht zwingend eine individuelle Identifizierung erforderlich. Dazu wird der Karteninhaber aufgefordert, sich bei einem Notar mittels Unterschriftsbeglaubigung oder – sofern sie dies anbietet – bei seiner zuständigen Rechtsanwaltskammer zu identifizieren. Dabei können u. U. weitere Kosten entstehen. Bitte drucken Sie die Antragsunterlagen zu diesem Zweck aus.

Sollten Sie die Antragsunterlagen zu einem späteren Zeitpunkt noch einmal ausdrucken wollen, gehen Sie bitte wie folgt vor:

Bitte gehen Sie unter <https://bea.bnotk.de/bestellung/#/products> auf „Mein Konto“ und „Anmelden“ und loggen sich mit Ihrer beA-Karte und Ihrer PIN ein.

Wenn Sie sich erfolgreich am System angemeldet haben, starten Sie bitte folgende Seite: <https://bea.bnotk.de/bestellung/index.html#/qes/Q-Nummer/documents>

Bitte beachten Sie, dass Sie an der Stelle Q-Nummer bitte die Q-Nummer Ihres signaturrechtlichen Antrages einfügen, bevor Sie den Link aufrufen.

Anmeldung

Nachdem der erforderliche signaturrechtliche Antrag erfolgreich geprüft wurde, erhalten Sie eine E-Mail mit folgendem Link, unter dem Sie Ihr qualifiziertes Signaturzertifikat für Ihre beA-Karte herunterladen können:

<https://bea.bnotk.de/bestellung/#/qes/certificates>

Alternativ ist es außerdem möglich, sich über das Bestellportal auf

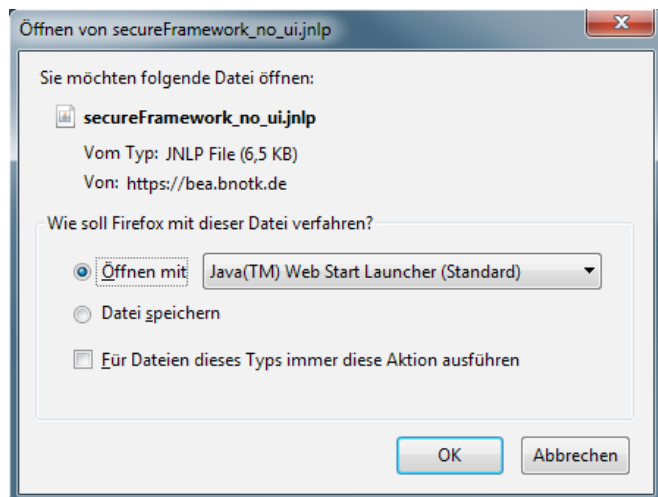
<https://bea.bnotk.de/bestellung>

unter dem Punkt „Mein Konto“ anzumelden und unter „Meine Zertifikate“ das qualifizierte Signaturzertifikat herunterzuladen.



Sobald Sie den oben zuerst genannten Link bzw. unter „Mein Konto“ auf „Anmelden“ klicken, beginnt im nächsten Schritt der Anmeldeprozess. Bitte vergewissern Sie sich vorab, dass Ihr Kartenlesegerät angeschlossen ist und Sie Ihre beA-Karte in das Gerät eingesteckt haben.

Im folgenden Schritt wird Ihre beA-Karte ausgelesen. Zu diesem Zweck bestätigen Sie bitte den aufkommenden Dialog mit OK.



Wurden die Kartendaten erfolgreich ausgelesen, werden Ihnen diese auf der nachfolgenden Seite angezeigt.

Bitte klicken Sie jetzt auf „Anmelden“ und folgen den Anweisungen auf dem Bildschirm zur PIN-Eingabe.

Herunterladen des elektronischen Transportcontainers

Nach der erfolgreichen Anmeldung klicken Sie bitte auf „Mein Konto“ und anschließend auf „Meine Zertifikate“. Hier können Sie Ihr qualifiziertes Signaturzertifikat in Form eines elektronischen Transportcontainers zunächst herunterladen.

Meine Zertifikate

Auf dieser Seite können Sie die produzierten Zertifikate herunterladen und den Empfang der Zertifikate bestätigen. Klicken Sie dazu bitte auf die entsprechend beschrifteten Links neben dem gewünschten Zertifikat.

Kartenummer	Karteneintrag	Bestätigt	
20001063	QES1	Nein	Herunterladen
20001328	QES1	Nein	Herunterladen

Ihr qualifiziertes Signaturzertifikat wird Ihnen hier in Form eines elektronischen Transportcontainers in einer Datei zum Herunterladen zur Verfügung gestellt.

Sie können die Datei mit Hilfe der unten bereitgestellten Signaturanwendungskomponente auf Ihre beA-Karte aufspielen.

Eine Anleitung, wie Sie ihr Zertifikat herunterladen und auf ihre beA-Karte auf- bzw. nachladen, finden Sie [hier](#).

[Signaturanwendungskomponente starten](#)

Klicken Sie dazu bitte auf den Button „Herunterladen“ neben dem Zertifikat, das Sie auf Ihre beA-Karte auf- bzw. nachladen möchten. Hierbei bestätigen Sie gleichzeitig verbindlich den Erhalt Ihres qualifizierten Signaturzertifikates.

Kartenummer 20001328

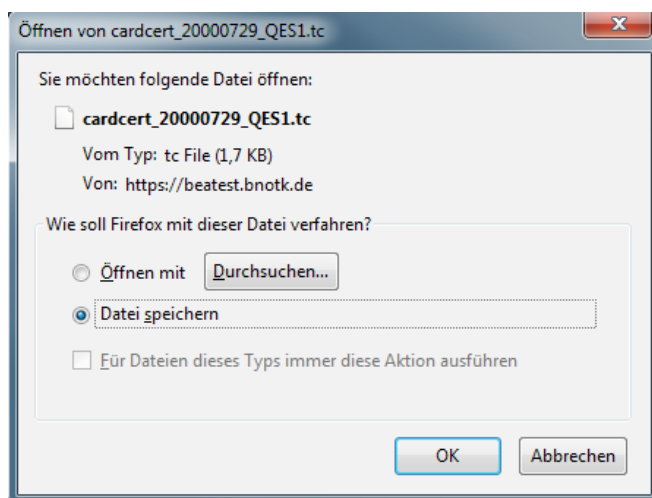


Mit dem Herunterladen des Transportcontainers für das qualifizierte Signaturzertifikat bestätigen Sie, dass Sie aktuell im Besitz der beA-Karte mit der Kartenummer 20001328 sind. Nach der Bestätigung können Sie den Transportcontainer beliebig oft von dieser Seite herunterladen.

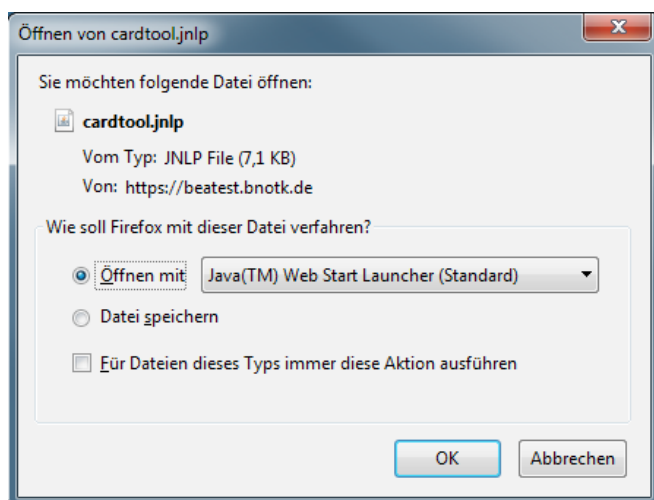
[Verbindlich bestätigen und herunterladen](#)



Wenn Sie den elektronischen Transportcontainer heruntergeladen und gespeichert haben, können Sie das Aufladen des qualifizierten Signaturzertifikats mit einem Klick auf „Signaturanwendungskomponente starten“ beginnen. Bitte merken Sie sich, an welcher Stelle Sie den elektronischen Transportcontainer gespeichert haben, da Sie diesen im weiteren Prozess benötigen.



Bitte bestätigen Sie nach einem Klick auf „Signaturanwendungskomponente starten“ bzw. den Link <https://bea.bnotk.de/sak/> den folgenden Dialog mit OK und öffnen die Datei mit dem Java Web Start Launcher.

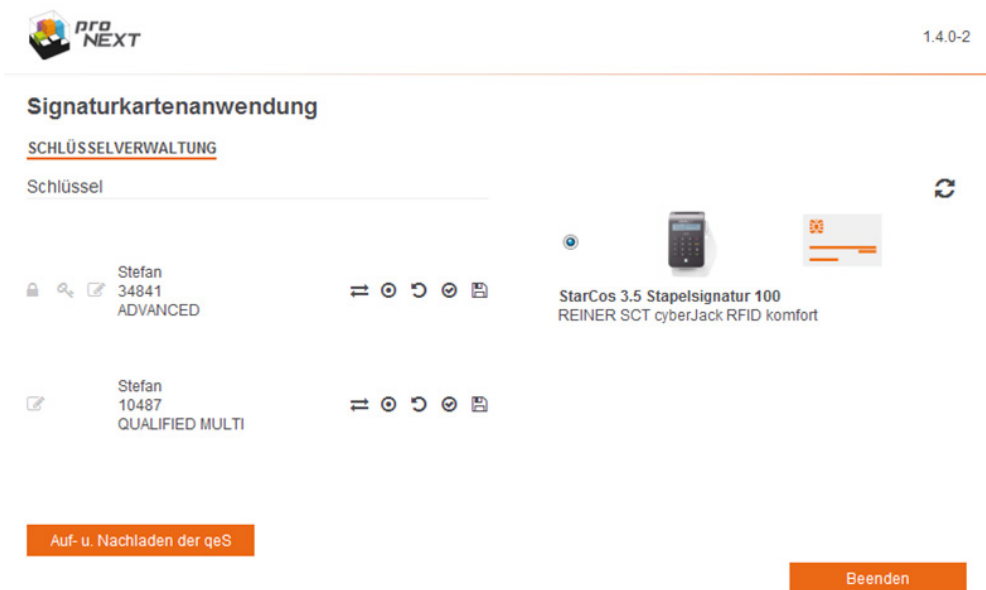


Auf- und Nachladen des qualifizierten Zertifikats

Im Anschluss wird die Signaturkartenanwendung, mit deren Hilfe Sie das qualifizierte Zertifikat auf Ihre beA-Karte aufladen können, gestartet. Alternativ kann diese auch über <https://bea.bnotk.de/sak/> aufgerufen werden. Klicken Sie bitte in der Anwendung auf „Auf- u. Nachladen der qeS“ und folgen den einzelnen Schritten des Aufladeprozesses. Haben Sie den Prozess erfolgreich durchlaufen und Ihr qualifiziertes Signaturzertifikat aufgeladen, werden in der Signaturkartenanwendung, wie unten dargestellt, zwei Einträge auf der linken Seite angezeigt. In diesem Fall haben Sie ihr qualifiziertes Signaturzertifikat zunächst erfolgreich auf die beA-Karte aufgeladen.

Folgen Sie hierzu während des Aufladeprozesses den Anweisungen auf Ihrem Bildschirm. Zum Aufladen des qual. Zertifikates und Entschlüsseln der Transport-PIN werden Sie zweimalig um Eingabe Ihrer PIN für die Anmeldung gebeten (advanced). Während des Aktivierungsvorgangs erscheint die 5-stellige Transport-PIN auf Ihrem Bildschirm, die einmalig

eingetragen und anschließend direkt in eine selbstgewählte 6- bis 12-stellige PIN für das Signieren (qualified) geändert wird. Erst nach der erfolgreichen Beendigung dieses Vorgangs ist Ihr qual. Zertifikat erfolgreich aufgeladen und aktiviert.



Achtung: Für die Aktivierung des qual. 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 Aufladeprozesses zu einem Fehler oder einer Fehleingabe gekommen sein bzw. die Anwendung wurde unerwartet geschlossen, kontaktieren Sie in diesem Fall unseren Support unter bea@bnotk.de und übersenden uns bitte die Datei operations.log (siehe Screenshot S. 7)

Unter Windows:

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

Mac OS:

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



4. beA-Postfach

Das beA wird von der Bundesrechtsanwaltskammer betrieben und ist unter

<https://www.bea-brak.de/>

erreichbar. Auf der folgenden Seite hat die Bundesrechtsanwaltskammer eine Anwenderhilfe zur Einrichtung und dem Umgang mit dem Postfach bereitgestellt.

<https://www.bea-brak.de/xwiki/bin/view/BRAK/>

Bitte haben Sie Verständnis dafür, dass wir diesbezügliche Fragen inhaltlich nicht beantworten können. Weitere Fragen zum Postfach direkt, bitten wir Sie an den Support des Postfachs zu stellen.

Für Fragen zum beA oder Störungen hat das mit der Entwicklung und dem Betrieb des beA beauftragte Unternehmen ATOS einen Service Desk eingerichtet, der unter

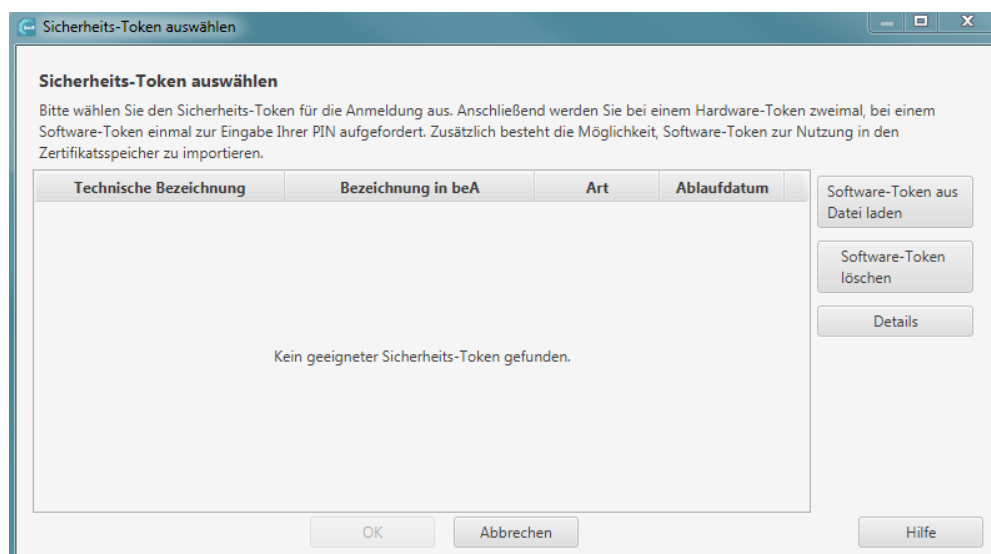
bea-servicedesk@atos.net oder telefonisch unter der Nummer 030-520009444

erreichbar ist.

Kein geeigneter Sicherheits-Token gefunden

Wird Ihre beA-Karte bei der Anmeldung am Postfach nicht erkannt, prüfen Sie bitte zunächst, ob Ihre beA-Karte in unserer Signaturkartenanwendung unter <https://bea.bnotk.de/sak/> ordnungsgemäß ausgelesen wird.

Darüber hinaus ist vor der Anmeldung eine einmalige Erstregistrierung am Postfach durchzuführen. Erst danach kann die Anmeldung erfolgen.



Sollte die beA-Karte in der Signaturkartenanwendung einwandfrei erkannt werden und die Erstregistrierung bereits erfolgt sein, kontaktieren Sie in diesem Fall bitte den Support des Postfachs (siehe oben).

beA-Karte Mitarbeiter und beA-Softwarezertifikat

Mit der beA-Karte Mitarbeiter bzw. beA-Softwarezertifikaten ist eine Anmeldung erst möglich, wenn diese in dem jeweiligen Postfach für den Zugang berechtigt wurden. Wir empfehlen Ihnen hierzu die Anwenderhilfe des Postfachs bzw. die Kontaktaufnahme zum beA-Support (siehe oben).

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

Möchten Sie eine Nachricht bzw. Anlage signieren und erhalten die unten dargestellte Fehlermeldung, haben Sie Ihr qualifiziertes Zertifikat noch nicht aktiviert. In diesem Fall ist das qual. Zertifikat zwar auf die Karte aufgeladen, jedoch die 5-stellige Transport-PIN noch nicht in Ihre eigene, mind. 6-stellige PIN für das Signieren geändert worden.



Bitte kontaktieren Sie in diesem Fall unseren Support unter bea@bnotk.de und übersenden uns bitte die Datei operations.log (siehe Screenshot S. 7)

Unter Windows:

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

Mac OS:

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



5. Problembehandlung

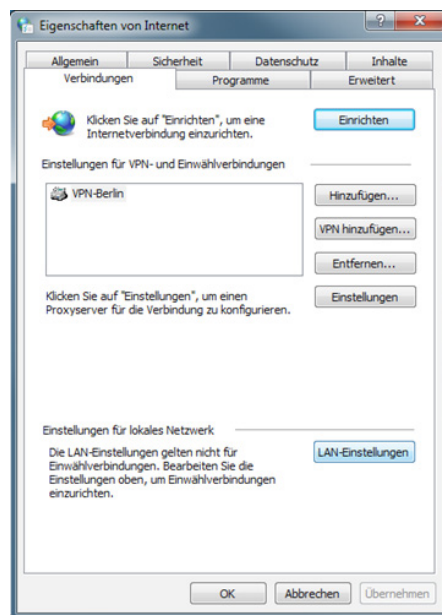
Sicherheitsprogramme

Generell sollten Sie die Webseite <https://bea.bnotk.de/sak> in sämtlichen Sicherheitsprogrammen (Antivirenprogramm, Firewall, Antispyware) als Ausnahme hinzufügen.

In der Firewall muss nach außen eine Verbindung über den Port 443 (Standard-SSL) möglich sein, damit mit dem Managementsystem kommuniziert werden kann. Auf dem jeweiligen Arbeitsplatz muss eine lokale Verbindung zu Port 10.000 möglich sein.

Proxy-Server

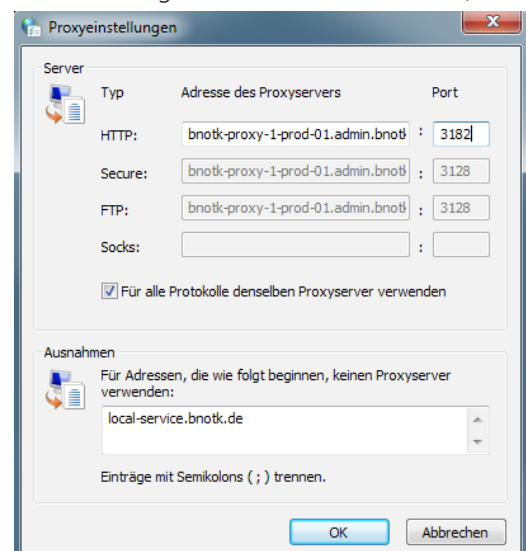
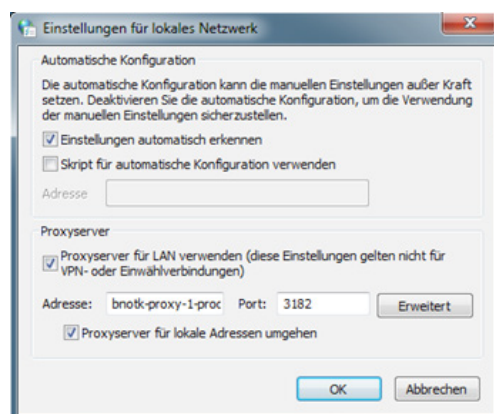
Sollten Sie einen Proxy-Server verwenden, übernehmen Sie bitte folgende Einstellungen.



Bitte gehen Sie in die Systemsteuerung und öffnen die Internetoptionen. Klicken Sie auf den Reiter „Verbindungen“ und öffnen die „LAN-Einstellungen“.

Bei Ihnen sollte das Kontrollkästchen Proxyserver für LAN verwenden aktiviert sein. Klicken Sie bitte auf „Erweitert“ und tragen im Feld „Ausnahmen“ folgendes ein: „local-service.bnotk.de“

Bitte bestätigen Sie mit „OK“ und starten die Anwendung erneut. Bitte beachten Sie, dass der Proxy-Server nur ein Beispiel ist und individuell eingestellt werden muss.



Bitte hinterlegen Sie die Einstellungen für den Proxy-Server samt Ausnahmen ebenfalls in den Netzwerkeinstellungen von Java.

Datev

Sollte die Signaturkartenanwendung nicht starten bzw. die Anmeldung auf unserem Bestellportal fehlschlagen und Sie haben eine der folgenden Anwendungen im Einsatz, folgen Sie bitte den unten stehenden Hilfestellungen der Fa. Datev.

- Datev Anwalt pro - <http://www.datev.de/lexinform-infodb/1046541>
- DATEVnet - <http://www.datev.de/lexinform-infodb/1017622>

Systemuhrzeit

Bitte überprüfen Sie die lokale Uhrzeit auf Ihrem Rechner bzw. in Ihrem Netzwerk. Ist die Abweichung Ihrer lokalen Systemzeit zur Serversystemzeit (<http://www.uhrzeit.org/atomuhr.php>) von bea.bnotk.de zu groß, kann die Anwendung nicht initiiert werden. Zur Lösung des Problems aktualisieren Sie bitte Ihre lokale Systemzeit.

Bitte führen Sie die Änderungen als Administrator sowohl lokal als auch am Server bzw. der Domain durch. Unter Umständen hilft es aber auch, wenn Sie die Uhrzeit manuell über die Taskleiste unten rechts am Bildschirm anpassen.

Unter Windows:

Klicken Sie auf Start - Ausführen „cmd“ und geben Sie „w32tm /resync“ ein und bestätigen Sie mit Enter. Sollten Sie dabei folgenden Fehler bekommen: „Folgender Fehler ist aufgetreten: Zugriff verweigert (0x80070005)“ befinden Sie sich in einer Domäne und der Domänen-Controller muss synchronisiert werden.

Die Synchronisation lässt sich genauso ausführen, wie für einen normalen Client.

Klicken Sie auf Start - Ausführen „cmd“ und geben Sie „w32tm /resync“ ein und bestätigen Sie mit Enter. Wichtig hierfür ist, sich auf dem Server anzumelden (vorzugsweise der Domänen-Admin) und dann diesen Befehl in der „cmd“ oder „Powershell“ auszuführen.

Unter Linux:

Starten Sie eine Konsole z.B. Bash und geben Sie „/usr/sbin/ntpdate -s pool.ntp.org“ ein, um ihre Systemzeit zu synchronisieren.

Unter OSX:

Bitte klappen Sie in der Menüleiste das Apple-Menü auf und wechseln von dort in die „Systemeinstellungen...“. Gehen Sie zum Bereich „Datum & Uhrzeit“ und klicken auf den linken Tab „Datum & Uhrzeit“. Sollte das Schlosssymbol im unteren Bildschirmbereich nicht offen sein, bitte einmal darauf klicken und das Admin-Kennwort eintippen. Anschließend, falls nötig, den Haken setzen bei „Datum und Uhrzeit automatisch einstellen“. In das Textfeld dahinter Folgendes eintippen:

ptbtime1.ptb.de, ptbtime2.ptb.de (falls Mac OS X 10.6 Snow Leopard oder höher)

beziehungsweise ptbtime1.ptb.de (falls Mac OS X 10.5 Leopard oder niedriger)

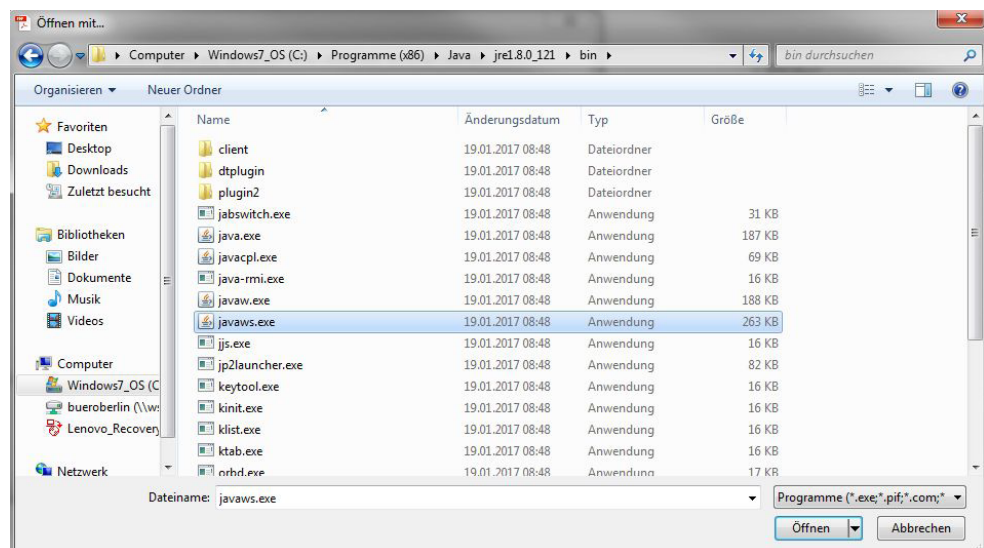
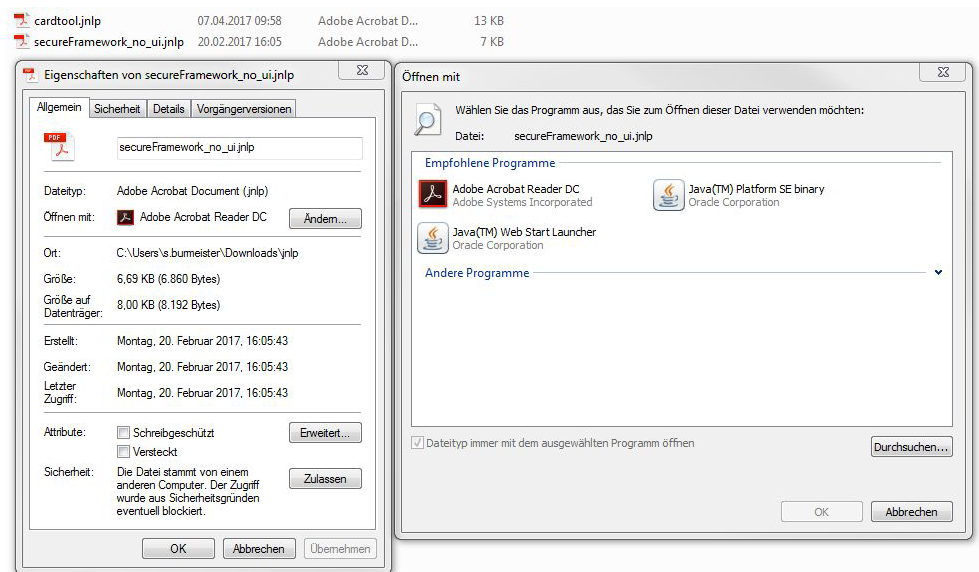
Zum Schluss das Fenster per Klick auf die rote Kugel oben links schließen – fertig!

Java

Verknüpfung mit dem Java Web Start Launcher herstellen

Werden unsere Javaanwendungen (jnlp-Datei) nicht korrekt mit dem Java Web Start Launcher geöffnet, kann unsere Anwendung nicht starten und die Dateiverknüpfung muss neu gesetzt werden.

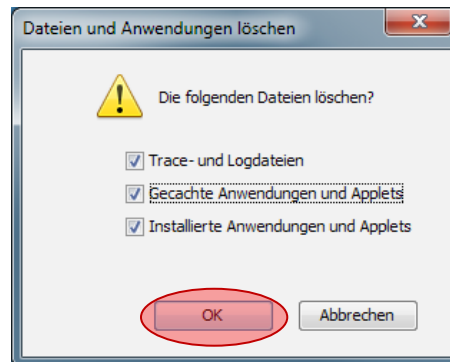
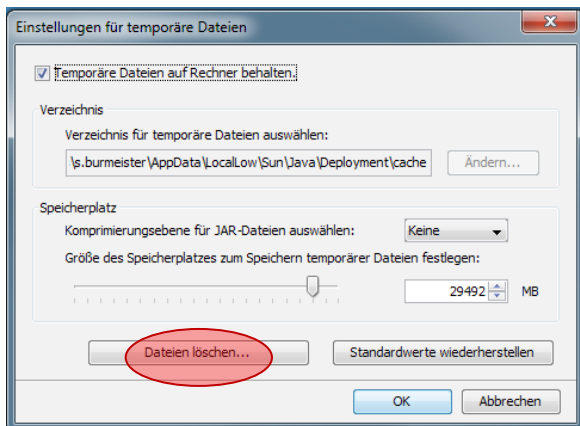
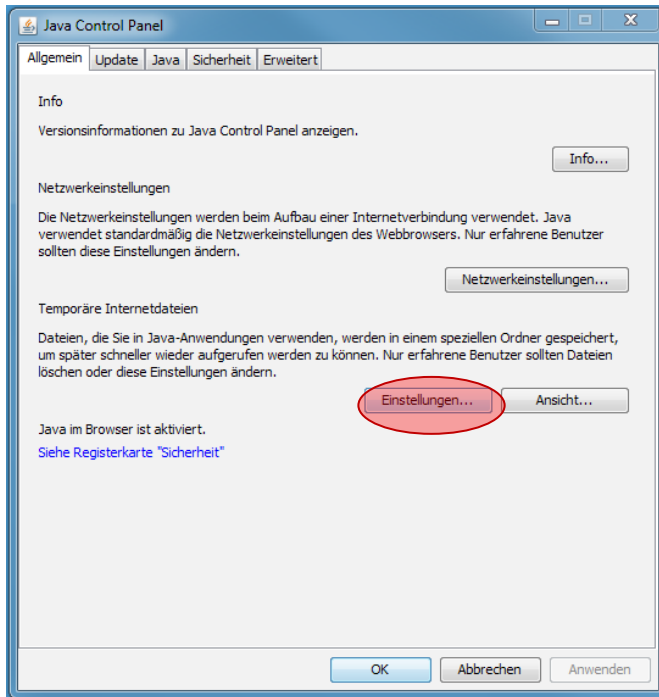
Bitte laden Sie zu diesem Zweck eine unserer Java-Dateien, z.B. auf <https://bea.bnotk.de/sak/> herunter und speichern diese. Im nächsten Schritte öffnen Sie bitte diese Datei mit einem Rechtsklick und gehen auf „Eigenschaften“. Klicken Sie bitte wie unten dargestellt auf „Ändern“ und in dem neuen Fenster 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-Cache löschen

Sollte die Anwendung auf Ihrem Windows-Betriebssystem nicht automatisch gestartet werden, gehen Sie bitte wie folgt vor:

- Löschen Sie bitte den Ordner „secureframework“ in Ihrem Benutzerverzeichnis unter C:\Users\ bzw. C:\Benutzer\
- Gehen Sie bitte in die Systemsteuerung und Öffnen das Element „Java“
 - o Klicken Sie bitte in dem sich öffnenden Fenster auf „Einstellungen“
 - o Im folgenden Fenster klicken Sie bitte auf „Dateien löschen“ und bestätigen in dem sich sodann öffnenden Fenster mit „OK“



Wenn Sie nun erneut die Webseite <https://bea.bnotk.de/sak/> aufrufen, sollte die Anwendung starten.

Sollten Sie weiterhin Probleme mit dem Start der Anwendung haben, senden Sie uns bitte die Log-Datei (siehe Screenshot S. 7) der Anwendung inklusive einer kurzen Fehlerbeschreibung an bea@bnotk.de.

Java-Konsole

Ist diese Datei auf Ihrem System nicht vorhanden, senden Sie uns bitte den Auszug aus der Java-Konsole.

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. Es kann vorkommen, dass sowohl die Anwendung als auch die Java-Konsole abbrechen. In diesem Fall ist es ratsam, möglichst schnell mehrmals auf „Kopieren“ zu klicken, bevor die Konsole abbricht.

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.

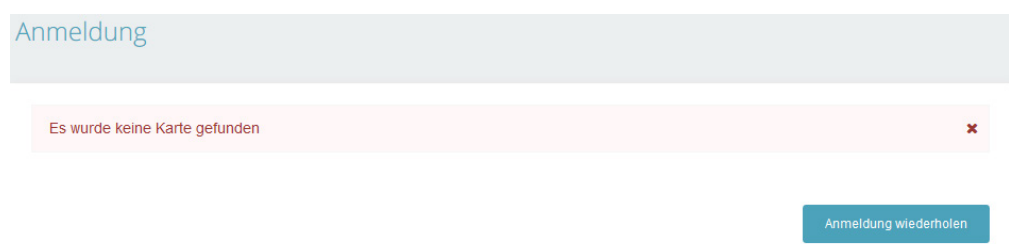
Bei dem nächsten Start der Anwendung zur PIN-Verwaltung öffnet sich nun zusätzlich die Java-Konsole und zeichnet im Hintergrund die Java-Aktivitäten auf. Klicken Sie bitte in der Java-Konsole auf „Kopieren“ und senden uns diese Daten zu. Es kann vorkommen, dass die sowohl die Anwendung als auch die Java-Konsole abbrechen. In diesem Fall ist es ratsam, möglichst schnell mehrmals auf „Kopieren“ zu klicken, bevor die Konsole abbricht.

Es wurde keine Karte gefunden

Sollte Ihre Karte nicht erkannt bzw. gefunden werden, prüfen Sie, 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 im cyberJack Gerätemanager unter dem Reiter „Aktualisierung“ und „Prüfe auf neue Versionen“, dass die neueste Firmware für Ihr Kartenlesegerät installiert ist.

Darüber hinaus kann es hilfreich sein, wenn Sie einmal den Browser wechseln.



Die Verbindung zur Server-Komponente ist fehlgeschlagen / Bitte überprüfen Sie, ob die lokale proNEXT Secure Framework Komponente gestartet ist.

Tritt einer dieser Fehler bei Ihnen auf, konnte keine Verbindung mit der Signaturkartenanwendung hergestellt werden. Bitte prüfen Sie in diesem Fall, ob Sie bereits alle Schritte der Problembehandlung durchgeführt haben und die Verbindung nicht durch Firewall, Proxy, Netzwerk-Infrastruktur (VPN etc.) oder Einstellungen am Server blockiert wird. Wird Ihnen dieser Fehler trotz der Durchführung der Problembehandlung angezeigt, senden Sie uns bitte die Log-Datei der Anwendung (siehe Screenshot S. 7) inklusive einer kurzen Fehlerbeschreibung an bea@bnotk.de



Herausgeber:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

Stand: April 2017

<https://bea.bnotk.de>