

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 3
Öffnen der Anwendung zur PIN-Änderung	3
PIN-Änderung	5
PIN für das qualifizierte elektronische Signieren „Qualified multi“	7
Häufige Fehlermeldungen	7
3. Schritt-für-Schritt-Anleitung für das Auf- bzw. Nachladen des qualifizierten Signaturzertifikats	Seite 9
Signaturrechtlicher Antrag	9
Anmeldung	10
Herunterladen des elektronischen Transportcontainers	12
Auf- und Nachladen des qualifizierten Zertifikats	13
4. beA-Postfach	Seite 14
Kein geeigneter Sicherheits-Token gefunden	14
beA-Karte Mitarbeiter und beA-Softwarezertifikat	15
Karte noch nicht initialisiert / Sie haben Ihre Karte noch nicht freigeschaltet	15
5. Problembehandlung	Seite 15
Sicherheitsprogramme	15
Proxy-Server	16
Datev	17
Die Systemzeit liegt außerhalb der Toleranz	17
Fehler bei der Suche nach Kartenlesern (Keine Kartenleser erkannt) / Fehler bei der Suche nach Kartenlesern (Timeout)	18
Firewall und Virens Scanner blockieren Signaturanwendungskomponente (SAK)	19

1. Allgemeine Voraussetzungen

Unterstützte Betriebssysteme

- Microsoft Windows 7 - 10 nur 64 bit Version
- Mac OS Mojave 10.14.1 +

Unterstützte Chipkartenlesegeräte

Für die Änderung Ihrer PIN-Daten, das Zurücksetzen der PIN-Eingabe mittels der PUK bzw. das Auf- oder Nachladen des qualifizierten Signaturzertifikates mithilfe der Signaturkartenanwendungskomponente 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:

- Reiner SCT cyberjack RFID standard
- Reiner SCT cyberjack RFID secoder
- ReinerSCT cyberJack RFID komfort
- ReinerSCT cyberJack RFID one

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 aus Sicherheitsgründen umgehend in eine neue PIN zu ändern. Gleichwohl ist die beA-Karte mit der übersandten PIN einsatzbereit.

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

Öffnen der Anwendung zur PIN-Änderung

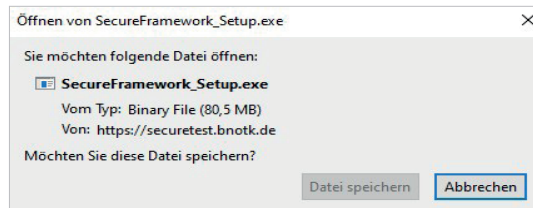
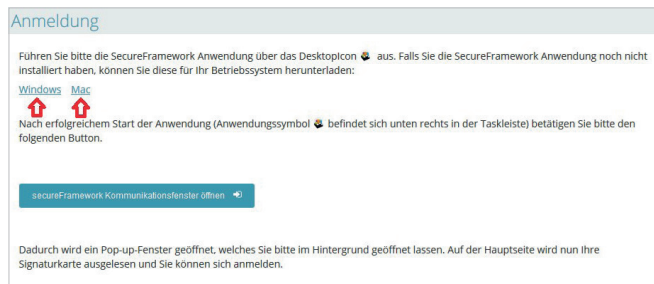
Öffnen Sie bitte die Webseite <https://bea.bnotk.de/bestellung>, klicken auf „Mein Konto“ und „Anmelden“ und laden auf der Folgeseite für Ihr Betriebssystem passend den Installer herunter. Nach erfolgreichem Herunterladen starten Sie aus dem Speicherort bitte den Installer und befolgen die angezeigten Anweisungen.



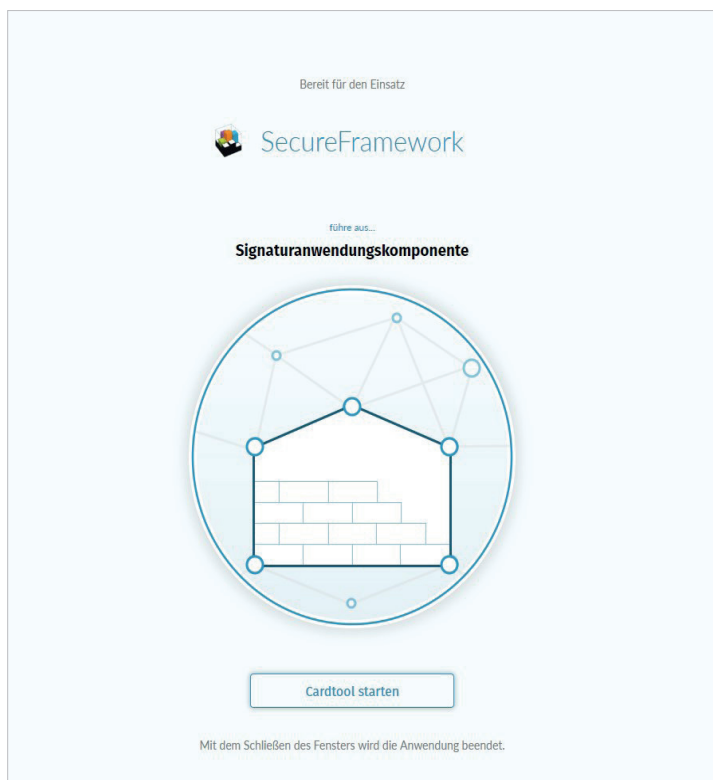



Unter Firefox:

Installer über die Webseite <https://bea.bnotk.de/bestellung> herunterladen, speichern und aus dem Speicherort starten.



Die Anwendung wird geladen und sobald diese gestartet ist, erscheint dieses Fenster:



Das Fenster wird sich unten in die Taskleiste ablegen, dies erkennen Sie am folgenden Symbol in der Leiste . Klicken Sie in der Taskleiste auf diese Anwendung, sie wird sich im Vordergrund wieder öffnen.

Drücken Sie bitte auf den unteren Button „Cardtool starten“, es wird nun die Schlüsselverwaltung gestartet, in der Sie Ihre PIN-Änderung vornehmen können.

Signaturkartenanwendung

SCHLÜSSELVERWALTUNG

Schlüssel

Test-Benutzer ZZZ_Test_BNotK
 7941739319163003178
 ADVANCED



Test-Benutzer ZZZ_Test_BNotK
 6067874462296753293
 QUALIFIED MULTI

Auf- u. Nachladen der qeS

Beenden



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“ oben rechts .

Auf der rechten Seite der Anwendung wird Ihnen das angeschlossene Kartenlesegerät angezeigt.

PIN-Änderung

Um Ihre Initial-PIN aus dem PIN-Brief zu ändern, klicken Sie bitte beim Eintrag „**Advanced**“ auf den Button mit den beiden Pfeilen \rightleftharpoons „**PIN ändern**“. Es erscheint im Display Ihres Kartenlesegeräts die Anzeige „**PIN Änderung**“. Sobald das Wort „**Änderung**“ erloschen ist, geben Sie die Initial-PIN aus dem PIN-Brief ein und bestätigen dies mit „**OK**“. Erfolgt nach der Aufforderung zur PIN-Änderung nicht innerhalb von 60 Sekunden eine Eingabe am Kartenlesegerät, wird die Anwendung aus Sicherheitsgründen beendet. Sie müssen den Änderungsprozess dann von vorne beginnen.

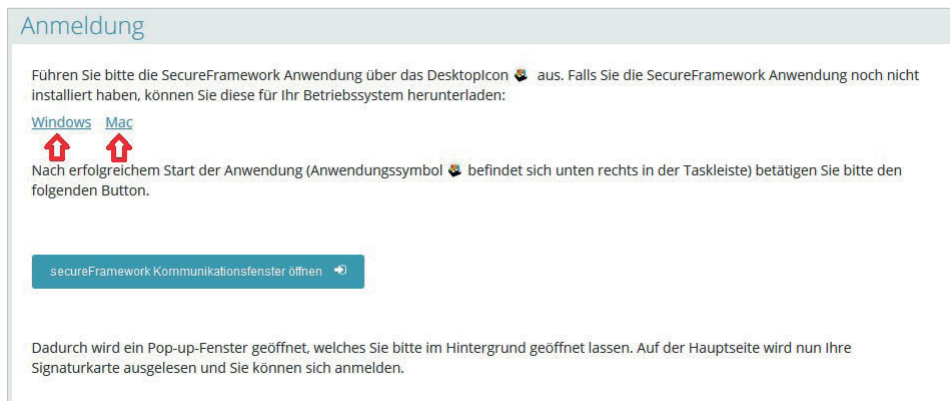
Achtung! Die unterstützte PIN-Länge beträgt 6 bis 12 Stellen.

Im Display erscheint jetzt die Anzeige „**PIN neu**“, geben Sie hier Ihre neue Authentifizierungs-PIN ein. Nach drücken von „**OK**“ werden Sie nochmals gebeten die neue PIN einzugeben. Bitte bestätigen Sie dies erneut mit „**OK**“. Jetzt sollte im Display des Kartenlesegeräts „**PIN korrekt**“ angezeigt werden.

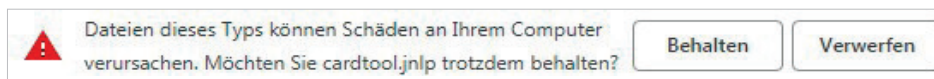


Unter Chrome:

Öffnen Sie bitte die Webseite <https://bea.bnotk.de/bestellung>, klicken auf „Mein Konto“ und „Anmelden“ und laden auf der Folgeseite für Ihr Betriebssystem passend den Installer herunter. Ihres Kartenlesers erscheinen, war der Vorgang in jedem Fall erfolgreich.



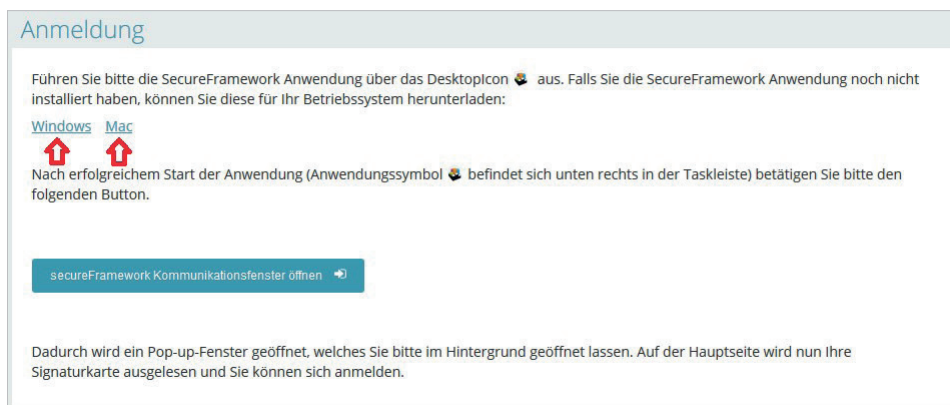
Wird bei Ihnen der folgende Hinweis angezeigt,



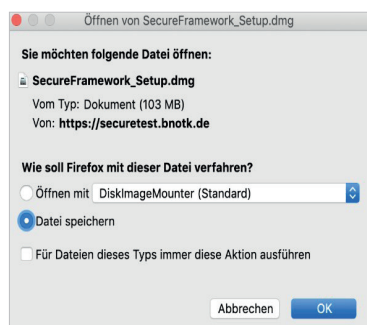
Drücken Sie bitte auf „Behalten“ und danach auf die Datei „**Secureframework.exe**“ und die Anwendung wird gestartet. Nachdem die Anwendung geladen ist verfahren Sie bitte genauso weiter wie unter **Firefox** bis zur erfolgreichen Änderung der PIN.

Unter Mac OS:

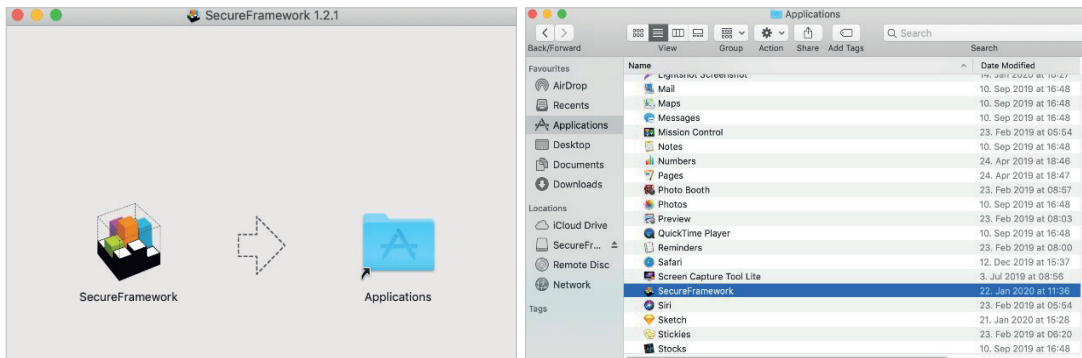
Öffnen Sie bitte die Webseite <https://bea.bnotk.de/bestellung>, klicken auf „Mein Konto“ und „Anmelden“ und laden auf der Folgeseite für Ihr Betriebssystem passend den Installer herunter.



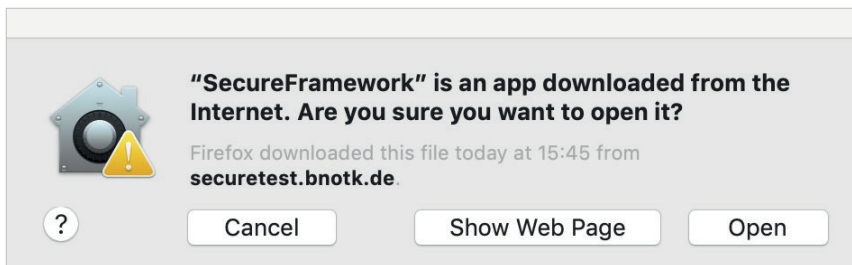
Nach dem Klicken auf Ihr Betriebssystem, werden Sie aufgefordert, die Datei zu speichern. Klicken Sie nun unten in der Taskleiste auf Ihren Downloadordner und wählen die Datei „SecureFramework_Setup.dmg“ aus.




Es wird nun das Setup ausgeführt und Sie werden gebeten die Datei in den Ordner „Programme“ zu verschieben. Gehen Sie nun über den Finder in den Ordner „Programme“ und starten die Anwendung mit einem Doppelklick.



Sie erhalten nun die Aufforderung das Öffnen der Anwendung zu bestätigen.



Nach erfolgreichem Start der Anwendung (erkennbar an dem Desktop Icon in der Taskleiste ) können Sie diese nutzen.

PIN für das qualifiziert elektronische Signieren „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.

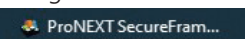
Neben dem fortgeschrittenen Zertifikat „**Advanced**“ für die Authentisierung, wird zusätzlich das qualifizierte Zertifikat „**Qualified multi**“ für das qualifiziert elektronische Signieren angezeigt.

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

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. Hierzu starten Sie bitte die Anwendung „ProNext“ auf Ihrem Desktop.

Nach erfolgreichem Start der Anwendung, zu erkennen am Programmsymbol in der Taskleiste , öffnen Sie das Programmfenster und klicken auf „**Cardtool starten**“.



Je nachdem welches Zertifikat betroffen ist, wählen Sie entweder **„Advanced“**, für Ihr Authentisierungs-PIN oder **„Qualified multi“** für Ihr Signaturzertifikat, aus.

Klicken Sie in der Signaturkartenanwendung bei dem jeweiligen Zertifikat auf das mittlere Symbol **„Fehlbedienungszähler zurücksetzen“** und geben Sie die PUK aus dem PIN-Brief ein sobald im Display des Kartenlesegeräts **„PUK“** steht.

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. Bei dreimal erfolglosem Einsetzen der PUK wird dieser aus Sicherheitsgründen gesperrt und Sie benötigen eine kostenpflichtige Ersatzkarte in Höhe von einmalig 30,-€ netto.

„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 folgendes 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.

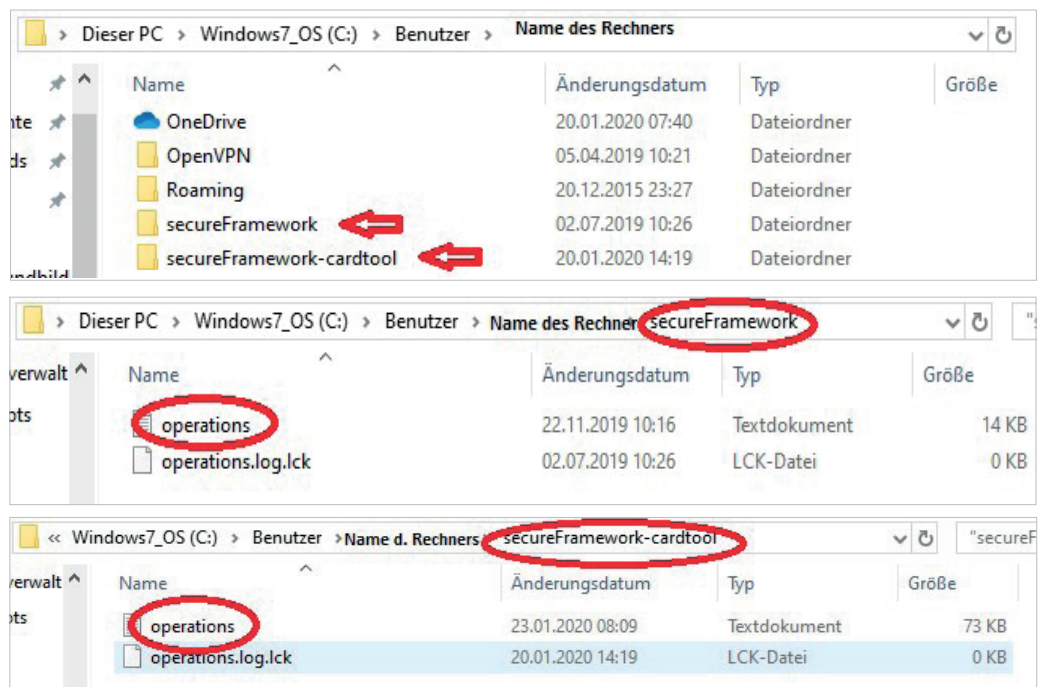
Um wirklich sicher zu gehen, dass die PIN-Änderung erfolgreich war, senden Sie uns bitte die Dateien operations.log (bzw. operations) aus den folgenden beiden Ordnern an sak@bnotk.de.

Unter Windows:

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

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

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



Mac OS:

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

3. Schritt-für-Schritt-Anleitung für das Auf- und 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 an unserem Bestellportal <https://bea.bnotk.de/bestellung/#/products> mit Klick auf „Mein Konto“ und „Anmelden“ und nach der erfolgreichen Anmeldung 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.

Die Q-Nummer finden Sie in Ihrer Bestellbestätigung bei Antragserstellung.

Sie können sie aber auch unter „Mein Konto“ ▶ „Aufladeverfahren“ ▶ „Kartenauswahl“ sehen.



Produzierte Karten

Bestellnummer	Kartennummer	Kartentyp	Kartenkategorie	Antrag
B-20161210-00008	20109289	beA-Karte Basis	1. Karte	offen
B-20170215-00011	20111636	beA-Karte Basis	1. Karte	offen
B-20170215-00011	20111639	beA-Karte Basis	2. Karte	Gestellt Q-20181107-00015
B-20180311-00001	20166486	beA-Karte Basis	1. Karte	offen
B-20181002-00078	20179992	beA-Karte Basis	1. Karte	offen

Bestellte Karten

Keine bestellten Karten verfügbar.

Anmeldung an „Mein Konto“

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/index.html#/certificates>

Hierzu ist es notwendig sich über das Bestellportal auf <https://bea.bnotk.de/bestellung> unter dem Punkt „Mein Konto“ anzumelden.

Sobald Sie den oben zuerst genannten Link bzw. unter „Mein Konto“ auf „Anmelden“ klicken, beginnt im nächsten Schritt der Anmeldeprozess.

beA-Produkte der Zertifizierungsstelle

Im Folgenden erscheint diese Seite:

Anmeldung

Führen Sie bitte die SecureFramework Anwendung über das Desktopicon aus. Falls Sie die SecureFramework Anwendung noch nicht installiert haben, können Sie diese für Ihr Betriebssystem herunterladen:

[Windows](#) [Mac](#)

Nach erfolgreichem Start der Anwendung (Anwendungssymbol befindet sich unten rechts in der Taskleiste) betätigen Sie bitte den folgenden Button.

secureFramework Kommunikationsfenster öffnen

Dadurch wird ein Pop-up-Fenster geöffnet, welches Sie bitte im Hintergrund geöffnet lassen. Auf der Hauptseite wird nun Ihre Signaturkarte ausgelesen und Sie können sich anmelden.



Sollten Sie die SecureFramework Anwendung noch nicht installiert haben, wählen Sie bitte das Betriebssystem Ihres Rechners aus, speichern die Datei und führen die heruntergeladene Datei aus Ihrem Speicherort aus.

Sobald die SecureFramework Anwendung erfolgreich gestartet ist, zu erkennen an dem Anwendungssymbol und am Programmsymbol in der Taskleiste ProNEXT SecureFram..., drücken Sie bitte den Button „secureFramework Kommunikationsfenster öffnen“.

Es öffnet sich nun das folgende Fenster:

127.0.0.1:10000/html/msg-api/

PRO NEXT

Die Signaturanwendungskomponente wurde erfolgreich gestartet. Das Fenster darf während der Nutzung nicht geschlossen werden. Sie können zu Ihrer Anwendung zurückkehren und die Bearbeitung fortsetzen.

Aktionen anzeigen

Bitte lassen Sie dieses Fenster im Hintergrund geöffnet. Wurden die Kartendaten erfolgreich ausgelesen, werden Ihnen diese auf der nachfolgenden Seite angezeigt.

Anmeldung

Test-Benutzer ZZZ_Test_BNotK

SN: 7941739319163003178

Anmelden

Bitte klicken Sie jetzt auf „Anmelden“ und folgen den Anweisungen auf dem Display Ihres Kartenlesegeräts 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.

Kartennummer	Karteneintrag	Bestätigt	
20111639	QES1	Ja	1. ↓ Herunterladen
20179992	QES1	Ja	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 des im "ProNEXT SecureFramework" Programm bereitgestellten "Cardtool starten" auf Ihre beA-Karte aufspielen. Eine Anleitung, wie Sie ihr Zertifikat herunterladen und auf Ihre beA-Karte auf- bzw. nachladen, finden Sie hier.

2. ↓
3. ↑

Klicken Sie dazu bitte auf den Button „Herunterladen“ (1.) neben dem Zertifikat, das Sie auf Ihre beA-Karte auf- bzw. nachladen möchten. Hierbei bestätigen Sie gleichzeitig verbindlich den Erhalt Ihres qualifizierten Signaturzertifikates.

Kartennummer 20179992

Mit dem Herunterladen des Transportcontainers für das qualifizierte Signaturzertifikat bestätigen Sie, dass Sie aktuell im Besitz der beA-Karte mit der Kartennummer 20179992 sind. Nach der Bestätigung können Sie den Transportcontainer beliebig oft von dieser Seite herunterladen.

Verbindlich bestätigen und herunterladen

Kartennummer	Karteneintrag	Bestätigt	
20111639	QES1	Ja	Herunterladen
20179992	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

Wenn Sie den elektronischen Transportcontainer heruntergeladen und gespeichert haben, merken Sie sich bitte den Speicherort (im Regelfall ist dies der Downloadordner), wechseln Sie zurück zum ProNext SecureFramework Programmfenster.

Sie finden dies unten in der Taskleiste ProNEXT SecureFram...

Bereit für den Einsatz

SecureFramework

Bitte ...

Signaturanwendungskomponente

Cardtool starten

Mit dem Schließen des Fensters wird die Anwendung beendet.

Secure Framework:

Klicken Sie hier bitte auf „Cardtool starten“ (2.) damit die Anwendung für die Aufladung gestartet wird.

Unter „Meine Zertifikate“ finden Sie ebenfalls die Schritt-für-Schritt-Anleitung zur PIN-Verwaltung (3.).

Auf- und Nachladen des qualifizierten Zertifikats

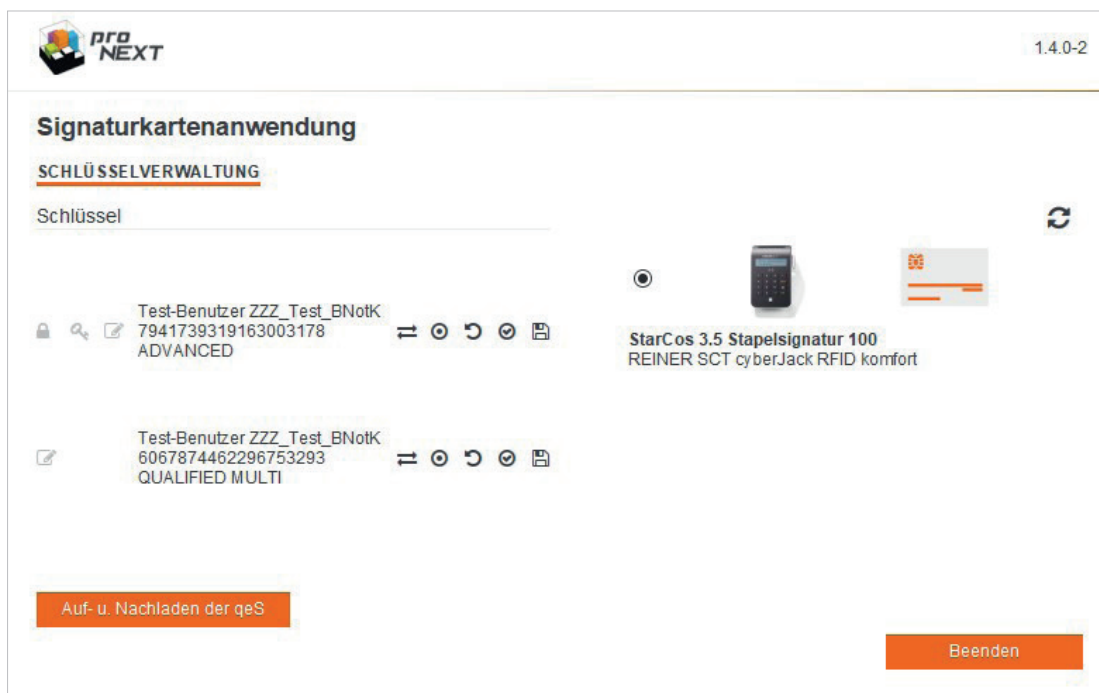
Im Anschluss wird die Signaturkartenanwendung, mit deren Hilfe Sie das qualifizierte Zertifikat auf Ihre beA-Karte aufladen können, gestartet.

Klicken Sie bitte in der Anwendung auf „**Auf- u. Nachladen der qeS**“ und folgen den einzelnen Schritten des Aufladeprozesses.

Zum Aufladen des qualifizierten Zertifikats und Entschlüsseln der Transport-PIN werden Sie zweimalig um Eingabe Ihrer Karten-PIN gebeten. Während des Aktivierungsvorgangs erscheint die 5-stellige Transport-PIN auf Ihrem Bildschirm. Im nächsten Schritt wird diese Transport-PIN in eine Ihnen bekannte PIN für das Signieren geändert und das qualifizierte Zertifikat aktiviert. 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, welche Sie zuvor freigeschaltet haben und bestätigen mit „OK“. Danach geben Sie bitte zweimal Ihre neue PIN (mindestens 6 Stellen) ein und bestätigen jeweils mit „**OK**“, sodass PIN korrekt auf dem Kartenlesegerät erscheint.

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 erfolgreich auf die beA-Karte aufgeladen.



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. Sollten die 3 Versuche zur Aktivierung erfolglos verlaufen, benötigen Sie eine kostenpflichtige Ersatzkarte in Höhe von einmalig 30,-€ netto.

Nach erfolgreicher Aufladung des qualifizierten Zertifikats schließen Sie bitte einmal die beA Client Security und starten diese über Ihren Desktop-Icon neu, sodass die neuen Daten von der beA-Karte abgerufen werden können. Danach ist ein Signieren mit der beA-Karte im beA Postfach möglich.



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. 8)

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

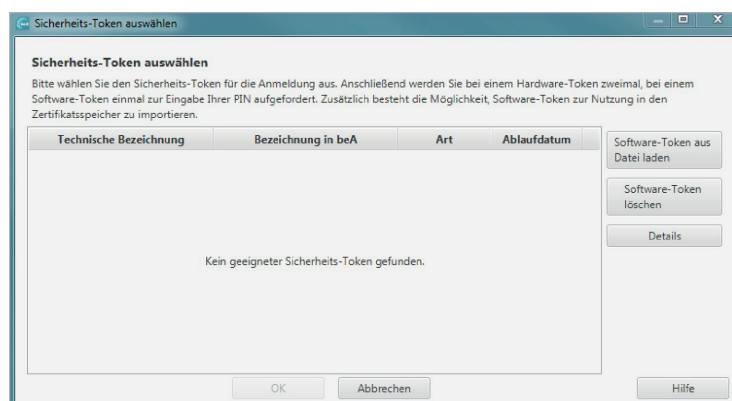
4. beA Postfach

Das beA wird von der Bundesrechtsanwaltskammer betrieben und ist unter <https://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 Wesroc einen Service Desk eingerichtet, der unter servicedesk@beasupport.de oder telefonisch unter der Nummer 030-21787017 erreichbar ist.

Kein geeigneter Sicherheits-Token gefunden



Wenn der Token nicht angezeigt wird, schließen Sie hierzu bitte einmal die beA Client Security sowie Ihren Browser und starten beides neu. Danach sollte der Token wieder sichtbar sein.

Sollte der Token wider Erwarten noch immer nicht sichtbar sein, wenden Sie sich bitte an den Support des beA Postfachs unter der Telefonnummer 030-21787017 oder

per Mail an servicedesk@beasupport.de

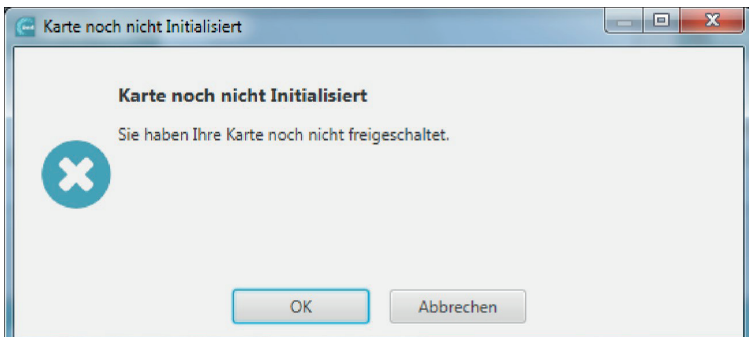
beA-Karte Mitarbeiter und beA-Softwarezertifikat

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 qualifizierte 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 sak@bnotk.de und übersenden uns bitte die Datei operations.log (siehe Screenshot S. 8)

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:

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

5. Problembehandlung

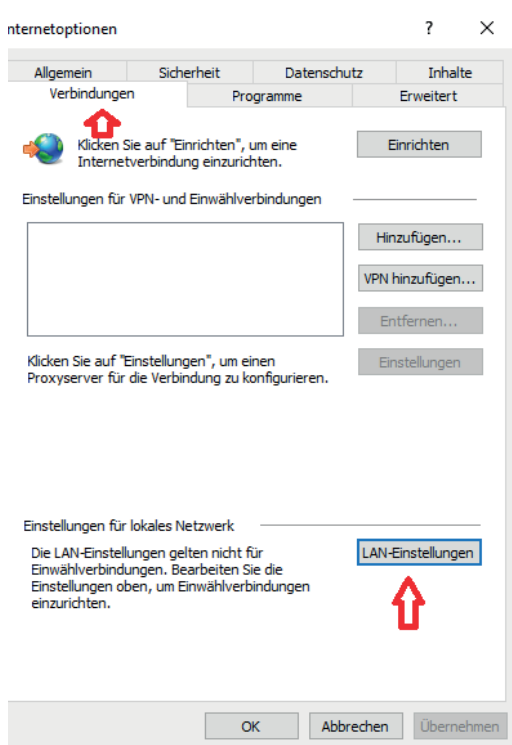
Sicherheitsprogramme

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.

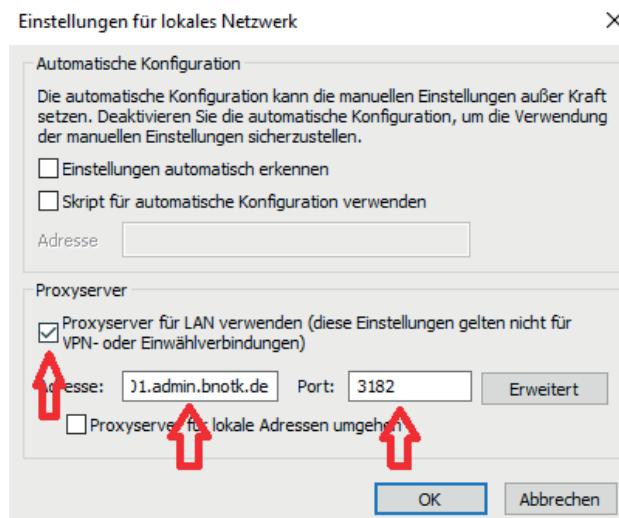


Proxy-Server

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“.



Wenn bei Ihnen im Kontrollkästchen „Proxyserver für LAN verwenden“ ein Haken gesetzt wurde und eine Hostadresse und Port eingetragen ist, müssen Sie zusätzlich noch ein Proxy-Element in der „operations.xml“ hinterlegen. Den Pfad zu dieser Datei finden Sie auf diesem Wege:

C:\Users\Benutzername\AppData\Local\Programs\secureframework-cardtool\secureframework-data-CardTool\operations.xml

Öffnen Sie die operations.xml und fügen bitte das rote Proxy-Element wie angezeigt hinzu:

```
<?xml version="1.0"?>
<operationsConfiguration>
<managementBaseUrl>
https://secure.bnotk.de/SecureFrameworkManagement/api</managementBaseUrl>
<bindAddress>http://127.0.0.1:10000</bindAddress>
<licence>./license.xml.p7s</licence>
<algorithmCatalog>./SecureFramework-Operations/dssc-de.xml.p7s</algorithmCatalog>
<libraryChecksumFile>./SecureFramework-Operations/operations-
checksums.sha512.p7s</libraryChecksumFile>
<proxy>
<host>__ip__</host>
<port>__port__</port>
<username>username</username>
<password>password</password>
</proxy>
</operationsConfiguration>
```

Ihr Systembetreuer wird die Hostadresse und Port eintragen und sofern dies eingerichtet wurde, auch einen Benutzernamen und Passwort. Andernfalls kann der Benutzername und Passwort auch leer bleiben. Löschen Sie in diesem Fall das in der Mitte stehende Wort „**username**“ und „**password**“ raus. Schließen Sie nun die Datei und speichern sie, wenn Sie danach gefragt werden.

Datev

Sollte die Signaturkartenanwendung nicht starten bzw. die Anmeldung auf unserem Bestellportal fehlschlagen und Sie die Anwendung Datev im Einsatz haben, folgen Sie bitte der untenstehenden Hilfestellung der Fa. Datev.

- Datev - <http://www.datev.de/lexinform-infodb/1046541>

Die Systemzeit liegt außerhalb der Toleranz

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 <https://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 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 draufklicken 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!

Fehler bei der Suche nach Kartenlesern (Keine Kartenleser erkannt) Fehler bei der Suche nach Kartenlesern (Timeout)

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, den USB-Stecker vom Kartenlesegerät am Rechner rauszunehmen, einen kurzen Augenblick zu warten und dann erneut alles wieder 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.

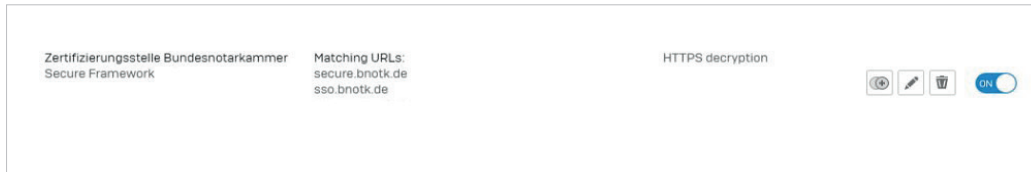
Wenn die Meldung „Fehler bei der Suche nach Kartenlesern (Timeout)“ kommt, schließen Sie bitte einmal die beA Client Security und führen die Anmeldung erneut durch.



Firewall und Virenschanner blockieren Signaturanwendungskomponente (SAK)

Diverse Firewalls können den Start der SAK blockieren.

Sie müssen z.B. bei der Firewall „Sophos“ folgende Einträge vornehmen:



bzw. die IP-Adressen:

secure.bnotk.de ▶ 77.76.215.9 und sso.bnotk.de ▶ 77.76.215.10

Des Weiteren sollte in Sophos der Aufruf von „https“-Seiten erlaubt werden.

Bei dem Virenschanner Kaspersky muss der Passwort-Manager ausgeschaltet werden, wenn die SAK nicht startet.

Wenn die empfohlenen Schritte nicht zu einem Erfolg führen, wenden Sie sich, wie auch bei allen anderen Firewalls oder Virenschanner, an Ihren Systembetreuer, damit lokale oder netzwerkseitige Einstellungen vorgenommen werden, die einen Zugriff auf Seiten der Bundesnotarkammer erlauben.





Herausgeber:

Zertifizierungsstelle der Bundesnotarkammer
Burgmauer 53
50667 Köln

Stand: Juni 2020

<https://bea.bnotk.de>