Der Newsletter zum besonderen elektronischen Anwaltspostfach
Ausgabe 16/2017 v. 19.04.2017

Der Trend geht zur Zweitkarte

Sobald der elektronische Rechtsverkehr Fahrt aufgenommen hat, wird es von elementarer Bedeutung sein, jederzeit auf das beA zugreifen zu können. Eingehende elektronische Post muss zeitnah abgerufen werden können; Schriftsätze an die Gerichte dürfen spätestens ab 1.1.2022 nur noch elektronisch an die Gerichte übermittelt werden. Nur ausnahmsweise bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wenn die elektronische Übermittlung aus technischen Gründen vorübergehend nicht möglich ist, § 130d Satz 2 ZPO n.F.

Den Zugriff auf das beA auch bei Ausfällen technisch abzusichern, ist in der Kanzlei mit überschaubarem Aufwand umsetzbar. So hilft es, mehrere Systeme zu schaffen, die den Zugriff auf das beA erlauben, also beispielsweise neben dem PC des Anwalts noch mindestens einen weiteren PC bereit zu halten, auf dem die beA Client Security installiert ist, zum Beispiel im Sekretariat. Vielleicht besteht zudem die Möglichkeit, ein „stand-alone-Gerät“ – evtl. in Form eines Laptops - vorsorglich für den Zugriff auf das beA einzurichten und mit einem eigenen Zugang in das Internet über Mobilfunk auszustatten. Dieser Laptop könnte dann zugleich für den mobilen Einsatz genutzt werden. Werden mehrere Systeme konfiguriert, werden in der Regel auch mehrere Kartenleser vorhanden sein, die bei Ausfällen untereinander ersetzt werden können. Es empfiehlt sich unabhängig davon, mehr als einen Kartenleser in der Kanzlei vorzuhalten.

Last but not least sind auch Vorkehrungen bei den Sicherungsmitteln zu treffen, die den Zugriff auf das beA ermöglichen. So kann eine beA-Karte jederzeit verloren gehen. Oder der Chip wird versehentlich mechanisch zerstört. In diesen Fällen kann zwar nach Sperrung der ursprünglichen beA-Karte eine Ersatzkarte für einmalig 30 Euro netto bei der BNotK (bea@bnotk.de) bestellt werden. Allerdings werden Sperrung der alten Karte sowie Ausstellung und Übersendung einer neuen Karte einige Tage in Anspruch nehmen.

Für diese Fälle empfiehlt es sich dringend, den Zugriff auf das beA mit einem zweiten Zugangsmedium, das für diese Fälle an einem sicheren Ort aufbewahrt wird, zu ermöglichen. Denkbar ist sowohl, dass der Anwalt eine zweite beA-Karte beantragt, als auch, dass er zumindest eine beA-Karte Mitarbeiter oder ein beA-Softwarezertifikat für diese Fälle bereithält. Dabei hat der Anwalt diese zusätzlichen Zugangsmedien bzw. Sicherungs-Token zuvor in seinem Profil zu hinterlegen. Hier haben wir erklärt, wie das geht (vgl. dazu **Newsletter 2/2016**).

Zusätzlich ist daran zu denken, dass jedenfalls bis 31.12.2017 für den Versand an die Gerichte eine qualifizierte elektronische Signaturkarte benötigt wird. Gegebenenfalls muss auch hier eine Ersatzkarte vorgehalten werden. Insbesondere für die Kollegen, die elektronischen Rechtsverkehr in größerem Umfang betreiben, z.B. viele Mahnverfahren durchführen oder Schutzschriften hinterlegen, ist es dringend geboten, eine zweite Signaturkarte zu bestellen, die nach Möglichkeit nicht die gleiche Laufzeit wie die Erstkarte haben sollte. Sofern Sie bereits eine alternative Signaturkarte besitzen, können Sie selbstverständlich diese als Ersatzkarte für den Zugang zum beA nutzen. **Hier** können Sie prüfen, ob diese zusätzlich für den Zugriff auf das beA freigeschalten werden kann.

Häufig wird die Frage zur Verwendbarkeit des neuen Personalausweises (nPA) mit eID-Funktion gestellt. Dieser kann zwar mit einem qualifizierten elektronischen Zertifikat nachgeladen werden; er kann also als Signaturkarte eingesetzt werden. Für die Anmeldung im beA ist aber neben dem Authentifizierungszertifikat auch ein Verschlüsselungszertifikat notwendig. Dieses enthält der nPA nicht. Daher kann zwar mit ihm im beA signiert werden, er kann aber nicht als alternatives Zugangsmedium im beA eingesetzt werden.

Schließlich kann der Zugriff auf das eigene beA im Notfall natürlich auch durch einen Kollegen oder Kanzleimitarbeiter sichergestellt werden, dem zuvor entsprechende Rechte eingeräumt wurden. Dabei muss allerdings klar sein, dass weder der Kollege noch der Kanzleimitarbeiter – auch nach dem 1.1.2018 – unsignierte Nachrichten aus dem betroffenen Postfach wirksam bei Gericht einreichen kann (vgl. dazu **Newsletter 12/2017**). Gleiches gilt, wenn der betroffene Kollege aus einem fremden Postfach Nachrichten an Gerichte versenden möchte. Im Zweifel wird somit immer auch noch eine Ersatz-Signaturkarte des betroffenen Kollegen benötigt.

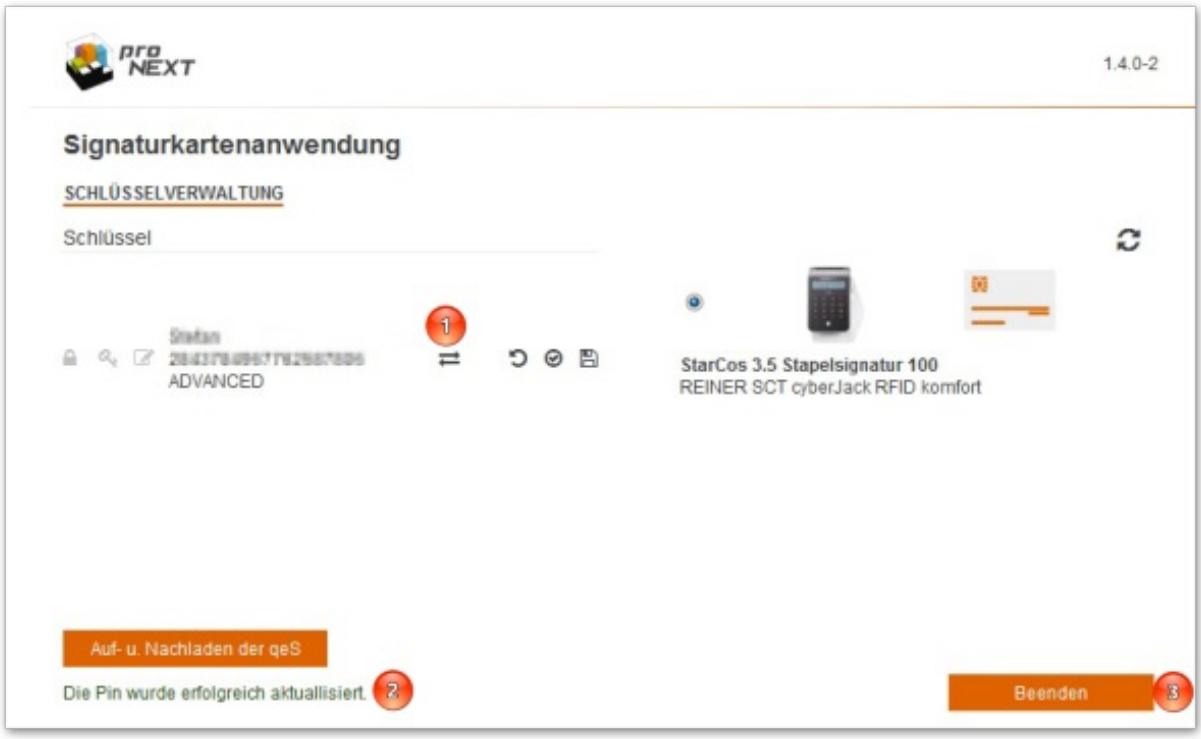
Penible PINs

Der Gesetzgeber schreibt in § 31a III 1 BRAO vor, dass der Zugang zum beA nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln möglich sein darf. Mit den beiden Sicherungsmitteln sind die Wissens- und die Besitzkomponente gemeint, also der Einsatz einer PIN und eines Sicherungs-Tokens wie der beA-Karte. Mit der PIN werden sowohl das Authentifizierungszertifikat für die Anmeldung am beA als auch das Verschlüsselungszertifikat für die Entschlüsselung der Nachrichten im beA freigeschaltet. Für die jeweilige Freischaltung ist die Eingabe der PIN erforderlich. Bei der Anmeldung mit einem Hardware-Token (z.B. beA-Karte) ist daher in der Regel zwei Mal die Eingabe der PIN erforderlich. Je nach Kartenleser erfolgt die Eingabe der PIN über die Computertastatur oder auch über die Zifferntastatur des Kartenlesers. Beim Einsatz eines Softwarezertifikats muss die PIN aus technischen Gründen immer nur einmal eingegeben werden, und zwar über die Computertastatur.

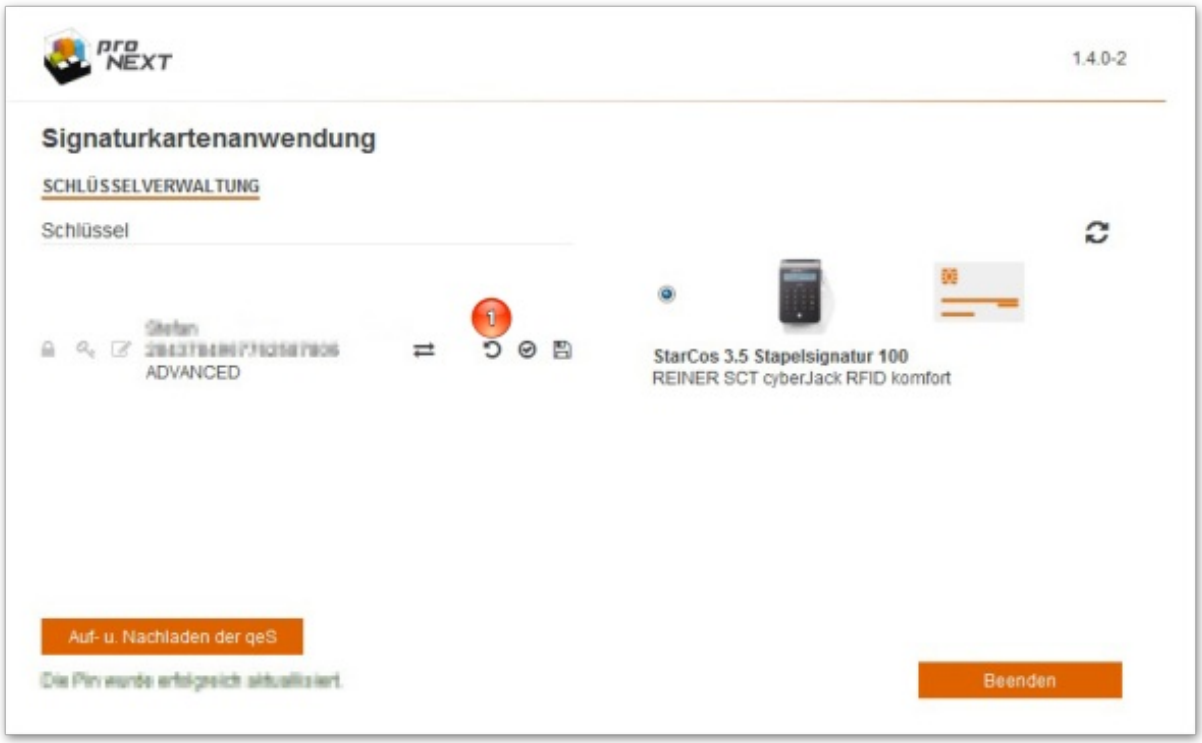
Nachdem die beA-Karte nach der Bestellung von der BNotK geliefert wurde, ist der Empfang über ein Online-Formular zu bestätigen. Erst anschließend wird der „PIN-Brief“ übersandt. Er enthält PIN und PUK. Beide Ziffernkombinationen sind durch ein spezielles Druckverfahren nicht sofort lesbar. Sie können auch nicht – wie vielleicht sonst – „freigerubbelt“ werden. Vielmehr ist das Papier an der Rückseite des Anschreibens zu knicken und vorsichtig zu entfernen. Auf der Vorderseite bleibt dann eine Plastikfolie, auf der die Ziffernkombinationen gelesen werden können.

In dem PIN-Brief wird dazu aufgefodert, die mitgeteilte PIN aus Sicherheitsgründen alsbald zu ändern. Für die PIN-Änderung und das Nachladen des Signaturzertifikates der beA-Karte Signatur über die Signaturanwendungskomponente der BNotK wird ein Chipkartenlesegerät der Klasse 3 benötigt. Angaben zu den unterstützten Chipkartenlesegeräten finden Sie **hier** in dem von der BNotK bereitgestellten Hilfedokument. Die beA-Karte wird zunächst in den Kartenleser eingeführt. Anschließend wird unter der Adresse **www.bea.bnotk.de/sak** die Signaturanwendungskomponente, eine Online-Anwendung der BNotK, temporär heruntergeladen und ausgeführt.

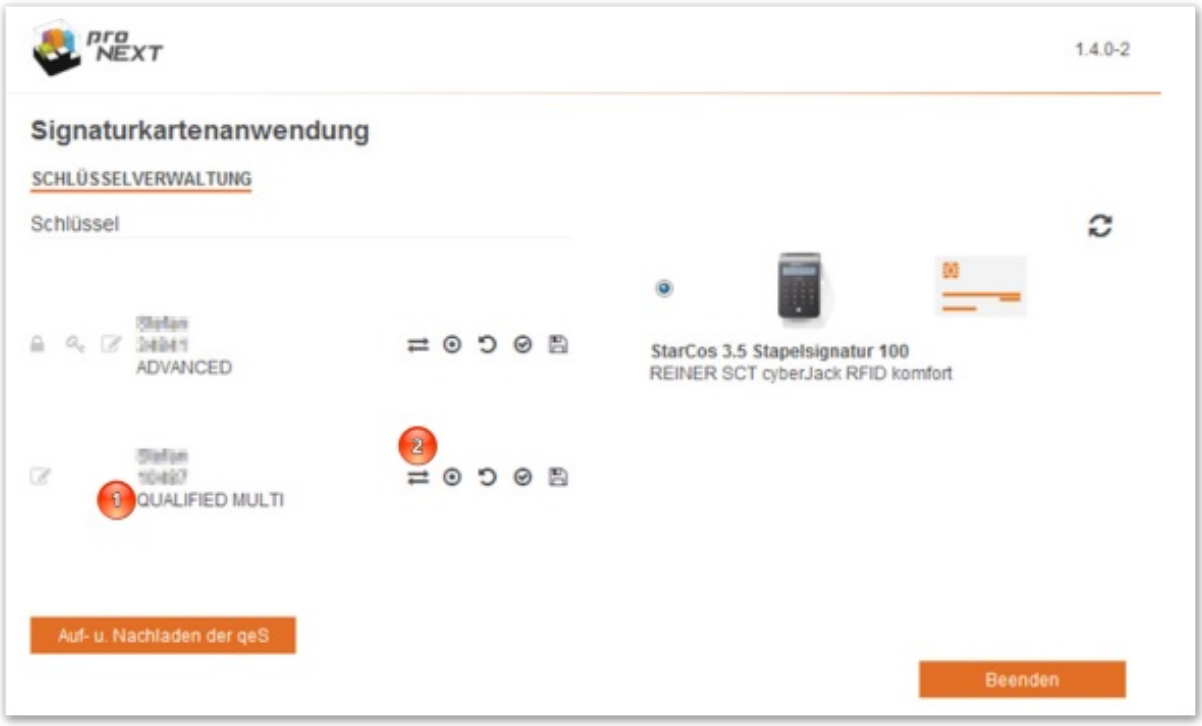
Ist die Signaturanwendungskomponente gestartet und wurden Kartenleser sowie gesteckte Karte erkannt, kann mit dem Drücken auf den Doppelpfeil (1) die PIN-Änderung eingeleitet werden. Dabei werden zunächst die alte und anschließend zwei Mal die neue PIN vom Kartenleser abgefragt. Die unterstützte PIN-Länge beträgt 6 bis 12 Stellen. Anschließend vermeldet das Programm die erfolgreiche PIN-Änderung (2) und es kann beendet werden (3).



Wurde die PIN in der Folgezeit bei einer Anwendung drei Mal falsch eingegeben, so erfolgt deren Sperrung. Mit der im PIN-Brief mitgelieferten PUK kann der sog. Fehlbedienungszähler zurückgesetzt werden. Hierzu ist das Symbol mit dem rotierenden Pfeil zu wählen (1). Dabei wird allerdings nicht die ursprüngliche PIN wieder hergestellt. Vielmehr erhält der Nutzer nur drei weitere Versuche die zuletzt vergebene PIN richtig einzugeben.



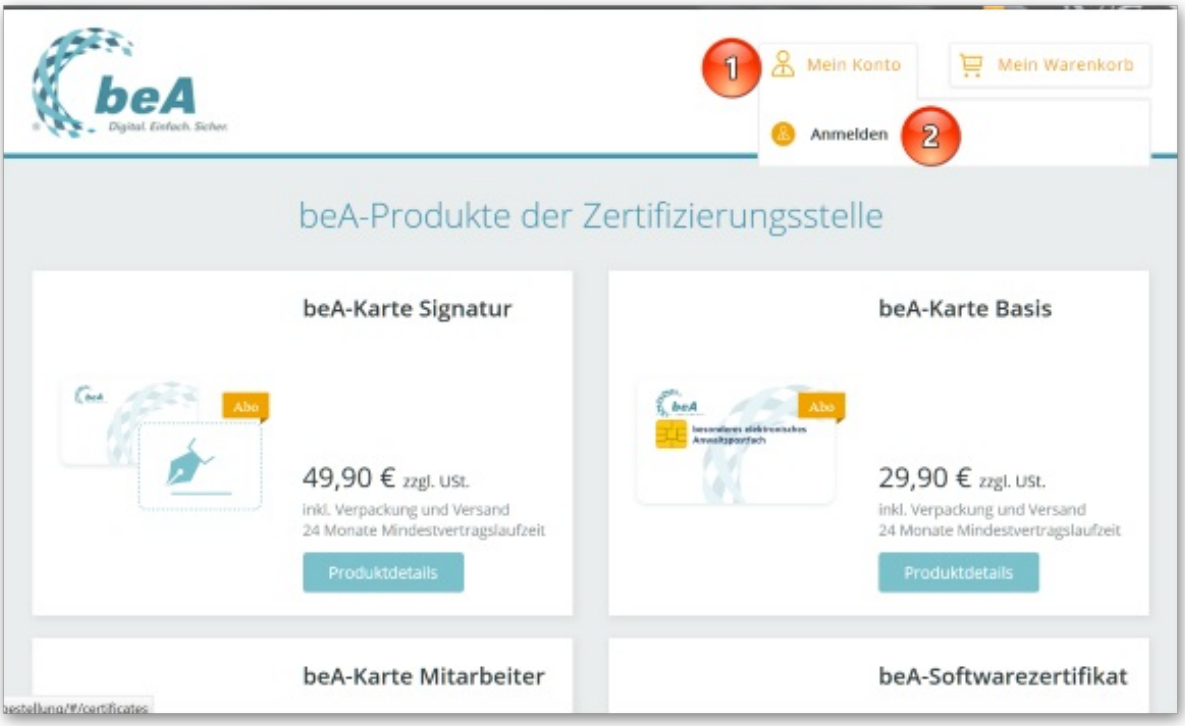
Auch qualifizierte Zertifikate sind durch eine PIN abgesichert. Diese kann sich von der PIN für Authentifizierung und Verschlüsselung unterscheiden, muss es technisch aber nicht; für alle Zertifikate kann also die gleiche PIN vergeben werden. Die PIN kann für die qualifizierte Signatur allerdings erst geändert werden, nachdem das entsprechende Zertifikat auf die Karte geladen und aktiviert wurde. Dieses zusätzliche Zertifikat erscheint in der Signaturanwendungskomponente als „Qualified“ (1). Der Klick auf den entsprechenden Doppelpfeil (2) führt zur PIN-Änderung (ebenfalls 6- bis 12-stellig).



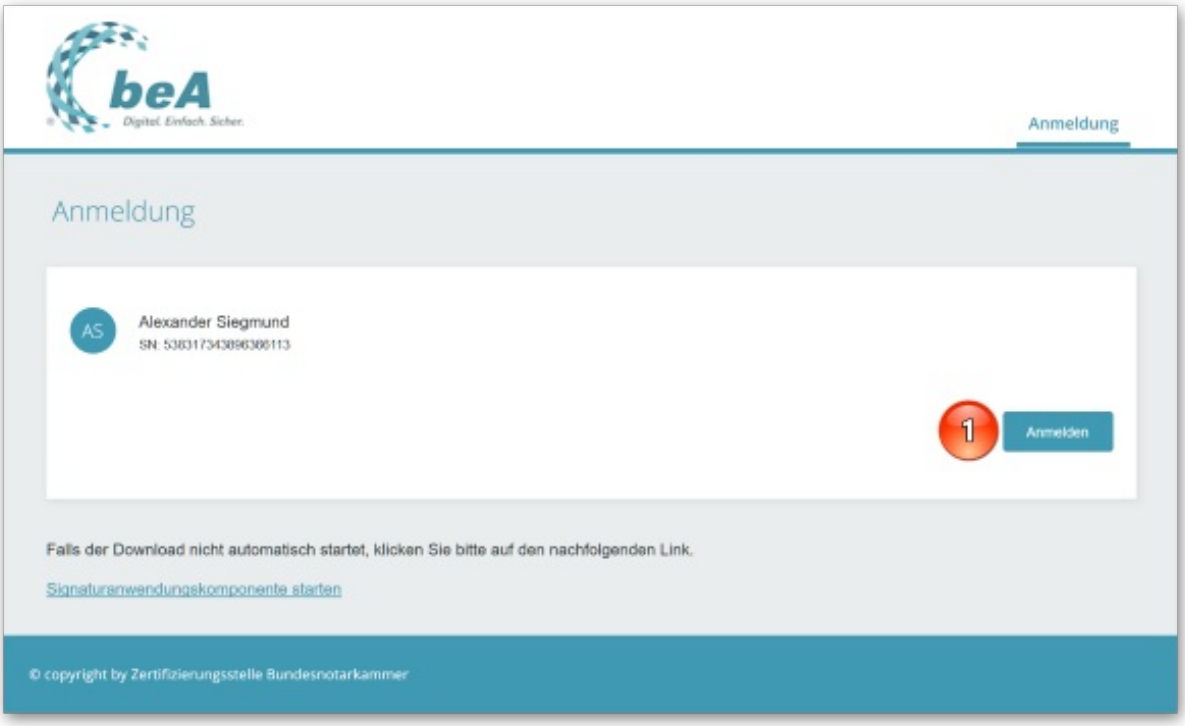
beA-Karte Basis zur Signaturkarte „upgraden“

Aus jeder beA-Karte Basis kann eine Signaturkarte werden. In vertraglicher Hinsicht ist hierzu entweder gleich eine beA-Karte Signatur zu bestellen oder es ist nachträglich eine „Nachladesignatur“ zu beantragen (vgl. **Übersicht beA-Produkte der Zertifizierungsstelle**). Wichtig zu wissen: In allen Fällen wird immer erst eine beA-Karte Basis ausgeliefert, die auch sofort den Zugang zum beA ermöglicht. Die zusätzliche Abonnementform „Nachladesignatur“ ermöglicht es nur, nachträglich ein qualifiziertes elektronisches Zertifikat zu beantragen und dieses nach Ausstellung auf die beA-Karte zu laden.

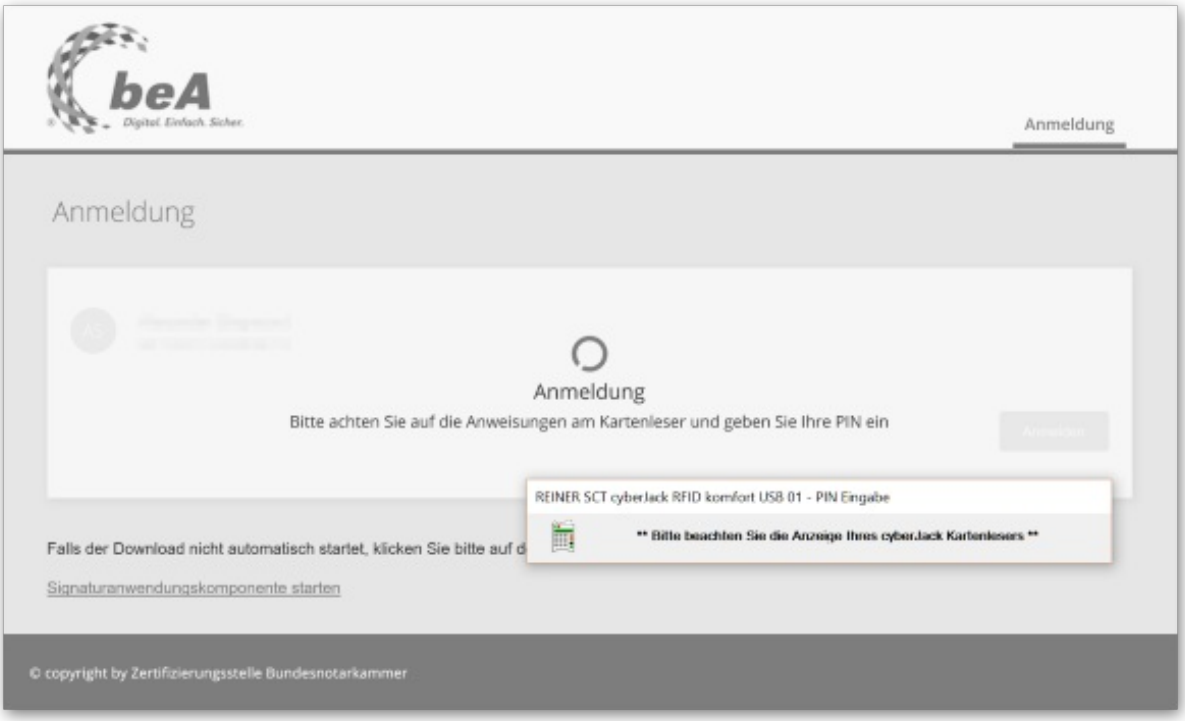
Sobald das Abonnement für die Signatur abgeschlossen wurde, können Sie sich im Bestellmanager mit Ihrer beA-Karte in ihrem Konto einloggen und die Antragsunterlagen erstellen. Stellen Sie sicher, dass Ihr Kartenleser angeschlossen (ggf. installiert) ist und Ihre beA-Karte steckt. Klicken Sie anschließend auf „Mein Konto“ (1) und „Anmelden“ (2).



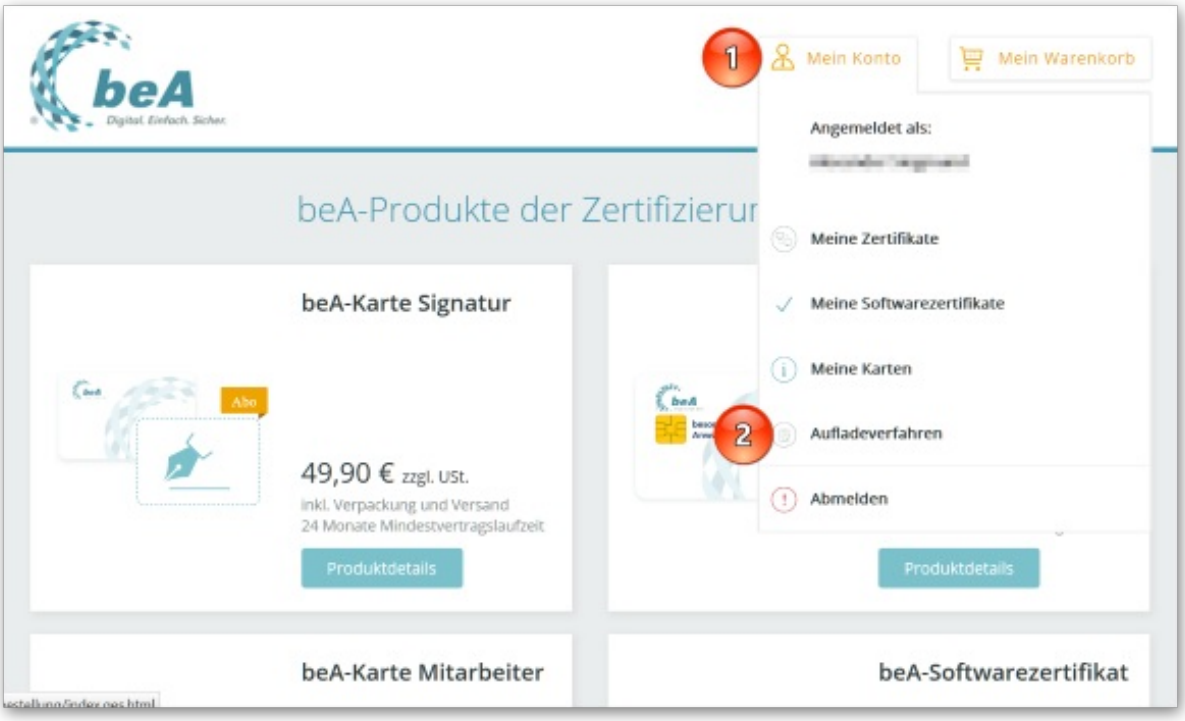
Sobald Kartenleser und Karte erkannt wurden, können Sie auf einen gesonderten Button „Anmelden“ klicken (1).



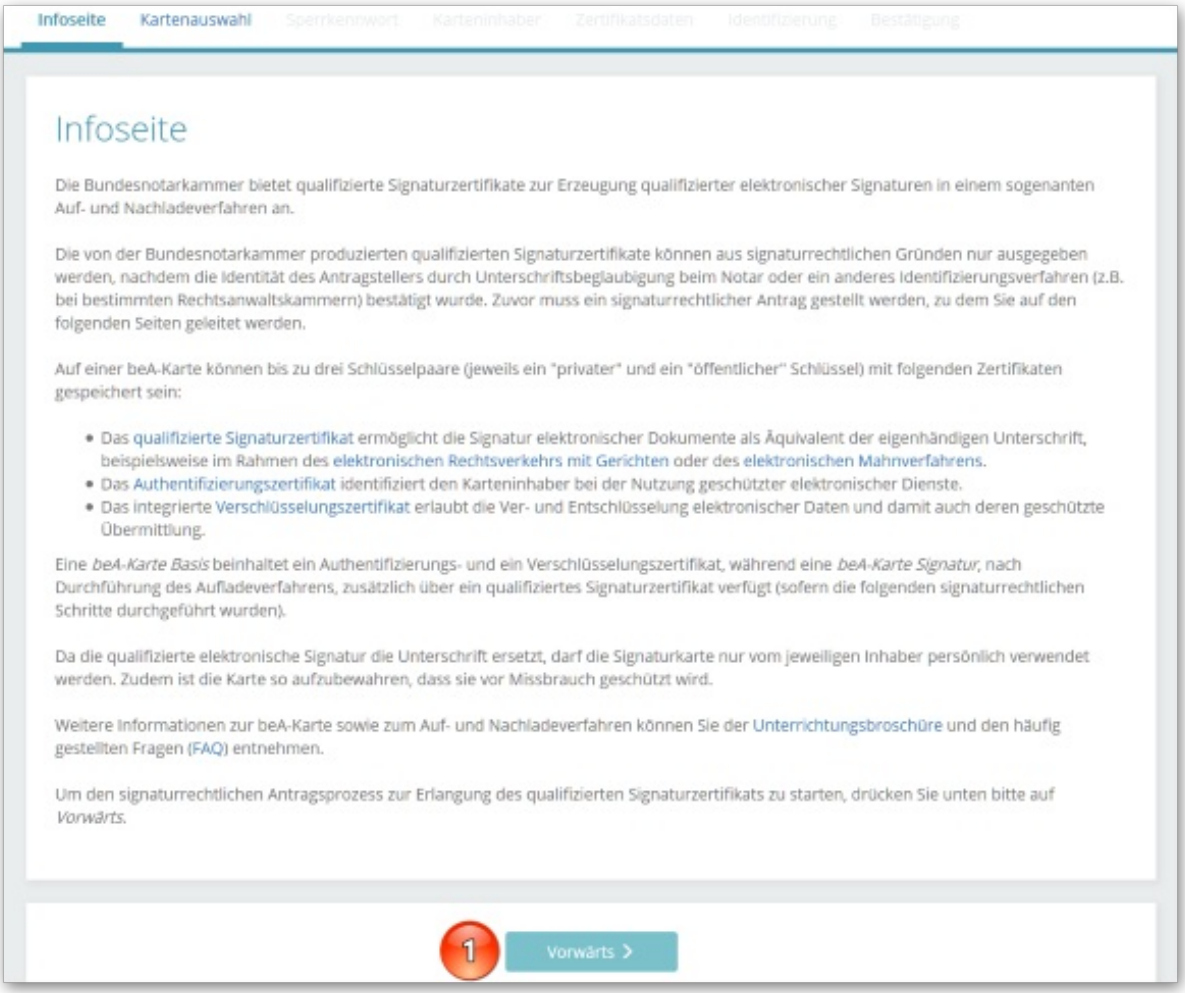
Es erfolgt einmalig die Abfrage der Authentifizierungs-PIN (im Regelfall über den Kartenleser).



Anschließend befinden Sie sich wieder im Bestellmanager. Klicken Sie nochmals auf „Mein Konto“ (1) und auf den Menüpunkt „Aufladeverfahren“ (2).

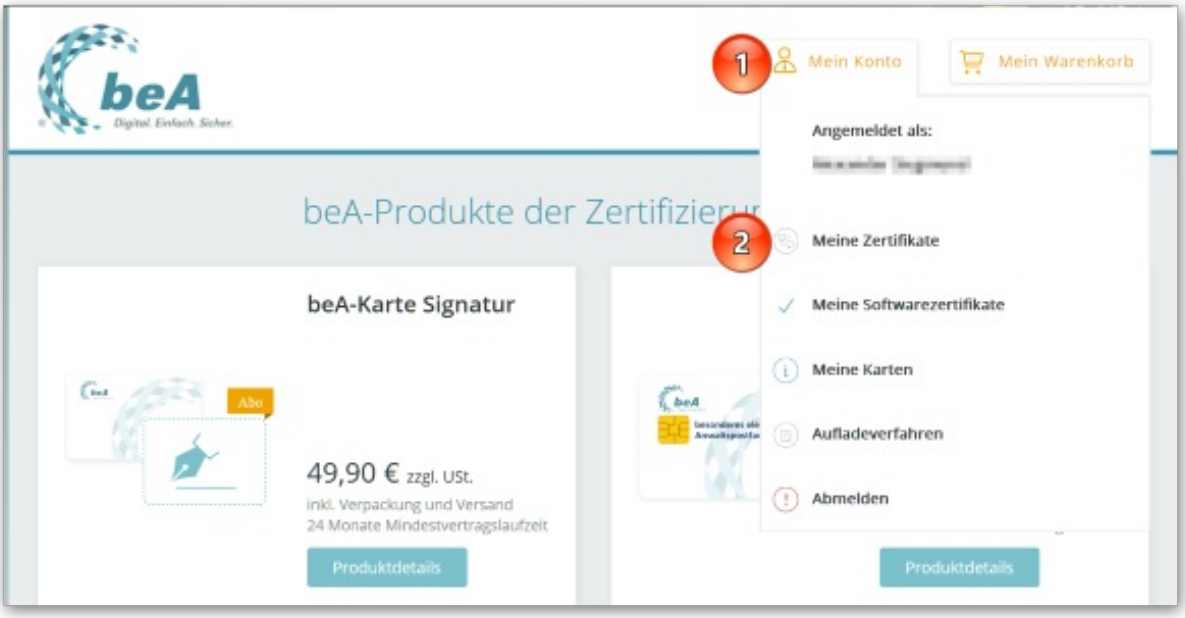


Auf der nachfolgenden Website erhalten Sie umfangreiche Informationen zur Beantragung des qualifizierten Zertifikats (vgl. auch **FAQ beA Nachladeverfahren**). Klicken Sie anschließend auf „Vorwärts“ (1) um auf der Folgeseite die beA-Karte auszuwählen, für die das Zertifikat erstellt werden soll.

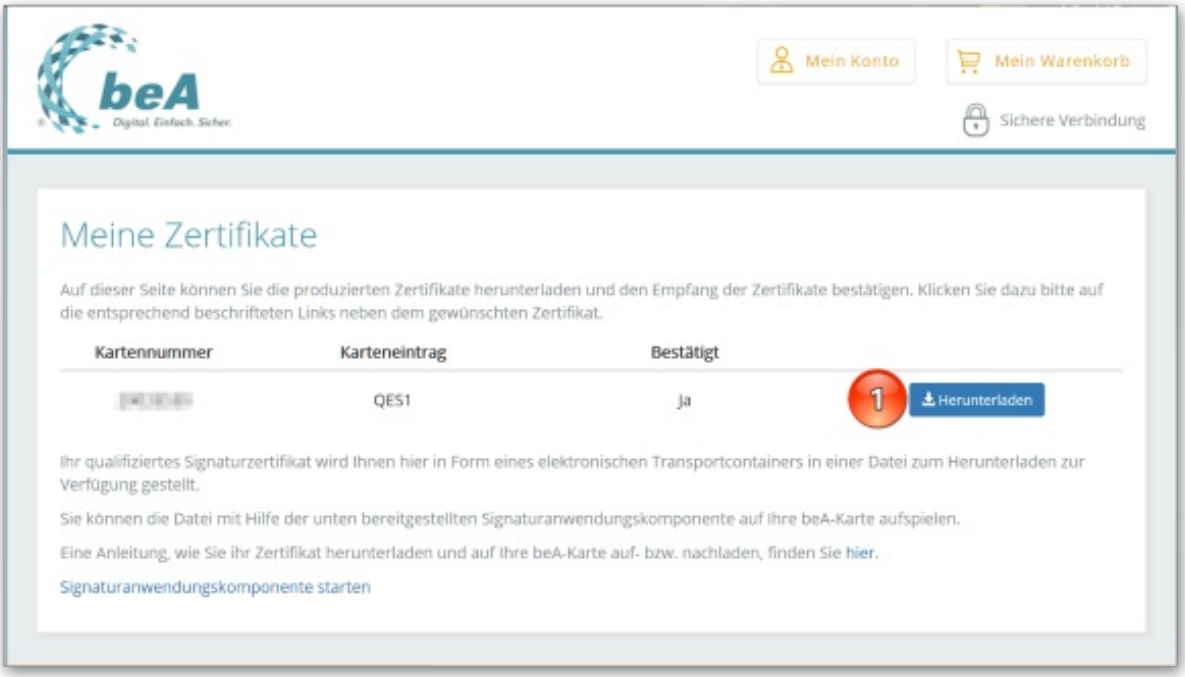


Auf weiteren Unterseiten müssen persönliche Daten eingegeben werden, um am Ende einen digitalen Antragssatz zu erhalten und ausdrucken zu können. Mit dem Antrag gehen Sie anschließend zur Identifizierung zu einem Notar. Alternativ können Sie prüfen, ob Ihre Kammer ebenfalls die Identifizierung anbietet (vgl. auch **Kammerident-Verfahren**).

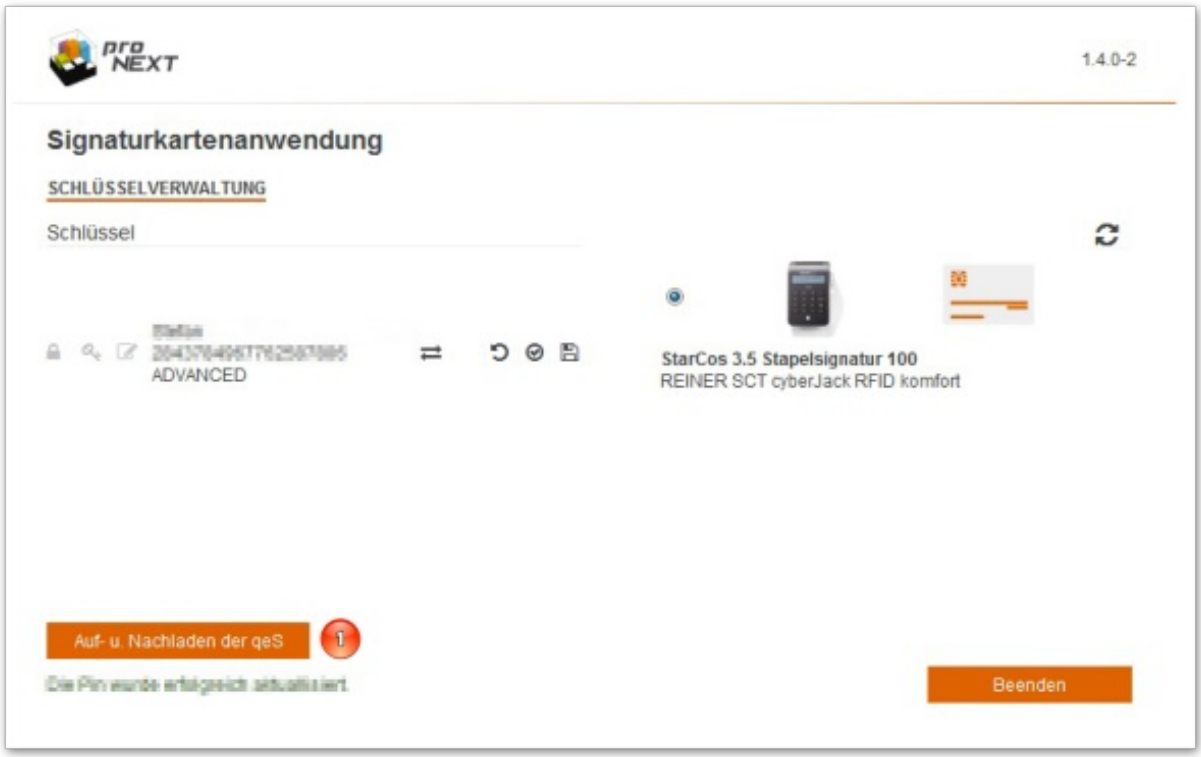
Sobald der Antragssatz durch die Identifizierungsstelle an die BNotK übermittelt wurde, beginnt die Produktion des qualifizierten Zertifikats. Nach kurzer Zeit erhalten Sie die Benachrichtigung per E-Mail, dass das Zertifikat zur Verfügung steht. Sie können es wieder im Bereich „Mein Konto“ (1) unter dem Menüpunkt „Meine Zertifikate“ (2) aufrufen.



Auf der Folgeseite können Sie es herunterladen (1) und an einem bestimmten Speicherort auf Ihrem PC ablegen.



Anschließend öffnen Sie die Signaturanwendungskomponente (**https:www.bea.bnotk.de/sak**). Unter dem Button „Auf- u. Nachladen der qeS“ (1) können Sie die gerade abgelegte Datei wieder auswählen.

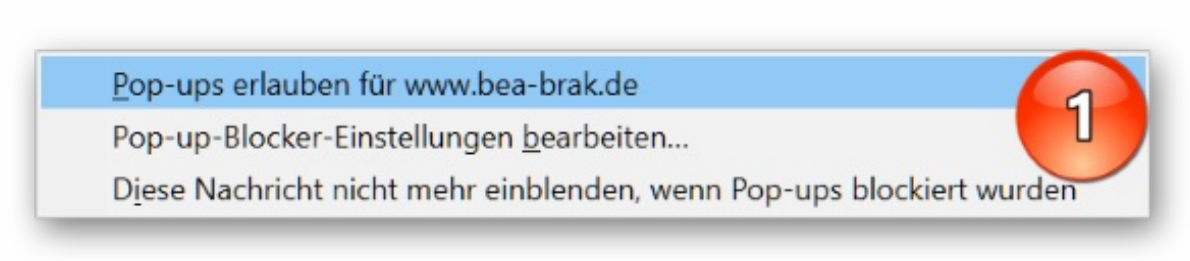


Bevor das Zertifikat auf die Karte geladen wird, muss zwei Mal die PIN der beA-Karte Basis eingegeben werden, um die Authentisierung zu ermöglichen und die ebenfalls digital übersandte Transport-PIN zu entschlüsseln. Die Transport-PIN des qualifizierten Zertifikats wird anschließend auf Ihrem Bildschirm angezeigt. Dieser fünfstellige Code wird nun in den Kartenleser eingegeben, um die eigentliche Signatur-PIN (6- bis 12-stellig) vergeben zu können. Weitere Infos finden Sie **hier**.

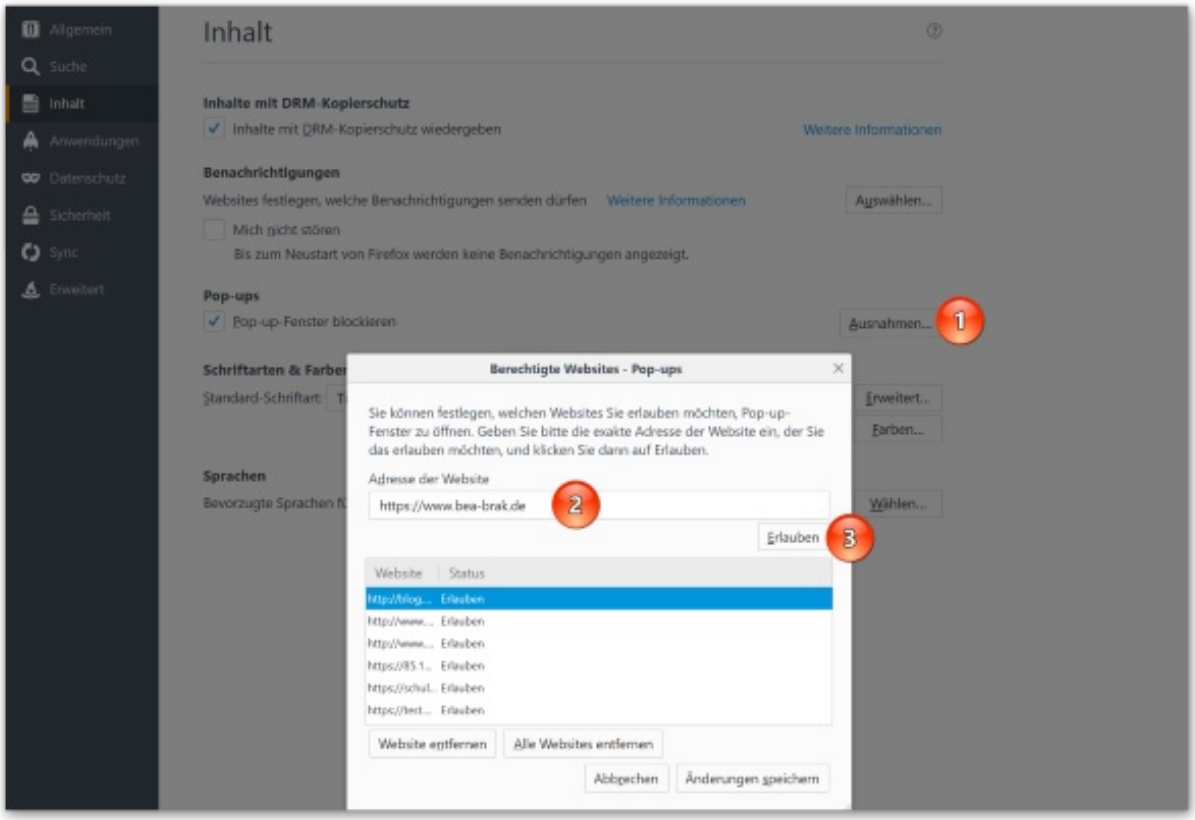
Tipps und Tricks: Pop-up-Blocker deaktivieren

Bei einigen Funktionen des beA werden im jeweiligen Internet-Browser neue Register geöffnet. Das ist beispielsweise beim Aufruf der **Hilfefunktion** (1) so oder auch beim Öffnen bzw. Erstellen von neuen Nachrichten (vgl. dazu **Newsletter 1/2017**). Manche Browser sind dabei so eingestellt, dass sie fälschlicherweise von unerwünschter Werbung ausgehen, die durch das neue Register angezeigt werden soll, und diese dann unterdrücken (Pop-up-Blocker). Meist wird der Nutzer durch einen Hinweistext darauf hingewiesen und hat sofort die Möglichkeit, die notwendigen Einstellungen vorzunehmen (2).

In den Einstellungen sollte sodann der Befehl „Pop-ups erlauben für **www.bea-brak.de**“ ausgewählt werden (1). Diese Einstellung wird anschließend dauerhaft im Browser gespeichert. Der weitere Aufruf von Registern aus dem beA geschieht in Zukunft problemlos.



Die Browser bieten im Übrigen auch eine gesonderte Konfigurationsmöglichkeit. So können in den Einstellungen des Browsers meist die Ausnahmen (1) gesondert konfiguriert werden. Tragen Sie alternativ hier die Adresse des beA ein (2) und klicken Sie auf den Button „Erlauben“ (3).



Impressum
Bundesrechtsanwaltskammer (BRAK)
Büro Berlin, Littenstraße 9, 10179 Berlin,
Tel: 030/ 28 49 39 - 0, Fax: 030/ 28 49 39 - 11, E-Mail: **zentrale@brak.de**
Redaktion: RAin Stephanie Beyrich, RAin Dr. Tanja Nitschke, Mag. rer. publ. (verantwortlich), RA Dr. Alexander Siegmund
Bearbeitung: Cornelia Kaschel-Blumenthal

Alle Informationen zum beA unter **www.bea.brak.de**.