BUNDESRECHTSANWALTSKAMMER

Fragen der Abteilung Digitalisierung des Vorstands der RAK Nürnberg

1. Fragen zur Fernsignatur

Mit der Einführung der Fernsignatur stellen sich für deren Nutzer einige Fragen. Ausgehend davon, dass im Vorfeld derer Einführung ein Austausch zwischen der Bundesrechtsanwaltskammer (BRAK) und der Bundesnotarkammer (BNotK) stattgefunden hat und seitens der BRAK die nachfolgenden Fragen vermutlich bereits antizipiert wurden, wird darum gebeten, diese zu beantworten. Sofern dies nicht möglich ist, wird darum gebeten, die Themen mit der BNotK abzuklären und im Anschluss zu beantworten.

Da die im beA implementierte Fernsignatur ein Dienst der BNotK ist, hat die BRAK die BNotK gebeten, die Frage 1a) bis f) zu beantworten.

a. Sicherheitsaspekte bzgl. hinterlegter Zertifikate

Anders als bei der Offlinesignatur, bei der die Zertifikate dezentral auf den jeweiligen Signaturkarten der Nutzer gespeichert werden, werden sämtliche Signaturzertifikate für die Fernsignatur auf einem zentralen Server vorgehalten. Mit zunehmender Verbreitung digitaler Signaturmöglichkeiten wird auch die Attraktivität für Kriminelle, sich diese Zertifikate zu beschaffen, um im Anschluss dieselben zu missbrauchen, erhöht.

Mit einem Hack des Zertifikatsservers könnten Angreifer (anders als bei der dezentralen Speicherung auf Signaturkarten) mit nur einem Zugriff sämtliche Zertifikatsdateien abgreifen. Der missbräuchlichen Nutzung stünde dann nur noch das jeweils vergebene 6-stellige numerische Passwort im Weg. Dieses im Rahmen einer Brute-Force-Attacke auszulesen stellt keine echte Hürde dar.

Zum Anbringen einer qualifizierten elektronischen Signatur ist der Zugriff auf den privaten Schlüssel notwendig, auf dem das qualifizierte Zertifikat beruht. Ein Hacker müsste sich daher Zugang zu den zentral gespeicherten Signaturschlüsseln verschaffen. Um dem besonders hohen Schutzbedarf gerecht zu werden, wird zur Erstellung und Nutzung der Schlüssel ein sogenanntes Hardware Security Module (HSM) verwendet. Ein HSM ist eine manipulationssichere Spezialhardware, die speziell für die sichere Ausführung von kryptographischen Operationen entwickelt wurde. Die eingesetzten HSM entsprechen den gesetzlichen Anforderungen und Normen und werden in der gemäß der Zertifizierung der Komponenten notwendigen sicheren Umgebung betrieben. Sie schützen die zum Einsatz kommenden Schlüssel gegen physikalische Angriffe und Seitenkanalangriffe.
Die Schlüssel der Teilnehmerzertifikate für Fernsignaturen werden auf einer zertifizierten qualifizierten Signaturerstellungseinheit (QSCD), dem HSM, erzeugt und gespeichert. Rechtzeitig vor Ablauf der Zertifikatsgültigkeit werden neue Schlüsselpaare und Zertifikate generiert, um einen reibungslosen Übergang zu gewährleisten. Der Prozess zur Erstellung von CA-Schlüsseln, die sog. Key Ceremony, erfolgt

Bundesrechtsanwaltskammer
The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus
Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39 - 0
Fax +49.30.28 49 39 -11
Mail zentrale@brak.de

Büro Brüssel
Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

nach den dafür eigens erstellten Vorgaben und wird dokumentiert. Das Rollenkonzept des Vertrauensdiensteanbieters (VDA) BNotK sowie das Vier-Augen-Prinzip finden auf die Schlüsselerzeugung Anwendung. Entsprechend der bisherigen Praxis des VDA BNotK wird die Anzahl der Mitarbeiter des VDA BNotK, die zur Schlüsselerzeugung besonders berechtigt sind, so gering wie möglich gehalten. Ein unabhängiger Auditor begleitet die Schlüsselerzeugung.
Die Schlüssel werden selbst verschlüsselt und können niemals unverschlüsselt aus dem HSM exportiert werden. Da die Schlüssel außerhalb des HSM niemals unverschlüsselt vorliegen, müssen sie für jede Nutzung in das HSM geladen und dort entschlüsselt werden. Der Entschlüsselungsschlüssel liegt dabei nur im HSM vor. Die Implementierung des HSM enthält keine Funktionalität, die diesen Schlüssel im Klartext exportieren kann. Die Schutzmechanismen der Hardware der HSMs stellen sicher, dass kein Anwender im Falle eines Angriffs auf das HSM (etwas das gewaltsame Öffnen und der Versuch des Auslesens des Speichers) Zugriff auf das Klartext Schlüsselmaterial erhalten kann. Dieses Verhalten ist Gegenstand der Produktzertifizierung.
Ein Hacker könnte im schlimmsten Fall also nur verschlüsselte Schlüssel entwenden, die nach aktuellem Stand der Technik nicht entschlüsselt werden können.
Ein Brute-Force-Angriff auf die PIN des Zertifikats zur Auslösung der Fernsignatur ist ebenfalls nicht möglich, da das Zertifikat auf einer Chipkarte gespeichert ist, die nach drei Fehleingaben gesperrt wird.
Das Zertifizierungskonzept für qualifizierte Zertifikate für elektronische Signaturen, das die Anforderungen an das Verfahren bei der Ausgabe, Verwaltung, Widerruf sowie Erneuerung der von der Zertifizierungsstelle der Bundesnotarkammer ausgegebenen qualifizierten Zertifikate darstellt, ist unter folgendem Link abrufbar:
https://zertifizierungsstelle.bnotk.de/fileadmin/user_upload_zs/Dokumente/Downloads/FINAL_-_CPS_-_Zertifizierungskonzept_der_Zertifizierungsstelle_der_Bundesnotarkammer__Version_3.0_-_Stand_0722_.pdf

Auch, wenn in der Presse aktuell noch nicht von systematischen Angriffen auf Zertifikatsserver berichtet wird, wurden in der Vergangenheit eine Vielzahl von Angriffen auf gut gesicherte Infrastrukturen (Yahoo, DropBox, LinkedIn, eBay, FaceBook, die Bank JP Morgan Chase, der Krankenversicherer Anthem Insurance, US-Wählerverzeichnisse Illinois und Arizona, ...) beobachtet, bei denen werthaltige Informationen abgegriffen wurde. Vor diesem Hintergrund erscheint es problematisch, sich alleine darauf zu verlassen, dass es sich bei der von der Bundesnotarkammer gewählten Infrastruktur um einen Vertrauensanbieter handelt.

Zusätzlich zu dem in der vorigen Antwort geschilderten Sicherungsmechanismus gibt es bei der Zertifizierungsstelle der BNotK zahlreiche technische und organisatorische Maßnahmen, die nach dem aktuellen Stand der Technik geeignet sind, ein sehr hohes Maß an Sicherheit zu gewährleisten. Dazu gehören auch Mechanismen, die Angriffe und kleinste Modifikationen an den Systemen erkennen und Alarm schlagen oder die Systeme gänzlich abschalten. All diese Maßnahmen sind Gegenstand von internen und externen Audits sowie mindestens jährlichen Prüfungen durch eine Konformitätsbewertungsstelle.
Die BNotK stellt Informationen zu den Leitlinien der Public-Key-Infrastruktur (PKI) unter folgendem Link zur Verfügung: https://zertifizierungsstelle.bnotk.de/veroeffentlichungen Sie finden hier die Zertifikatsrichtlinie (Certificate Policy) sowie die Zertifizierungskonzepte (Certification Practice Statements).

Wie wird seitens der BRAK sichergestellt, dass die Zertifikate der durch sie beworbenen und implementierten Fernsignatur gegen derartige Angriffe tatsächlich gesichert sind?

Die BRAK bewirbt den Fernsignaturservice der BNotK nicht. Sie hat ihn als eine Alternative zu den weiterhin unterstützten kartengebundenden Signaturverfahren in der beA-Webanwendung implementiert.
Da es sich wie bei den Signaturkarten um ein Produkt eines Fremdanbieters handelt, kann die BRAK selbst nicht sicherstellen, dass die Zertifikate gegen Angriffe tatsächlich gesichert sind. Auch bei der

Produktion und dem Einsatz von Signaturkarten wäre es grundsätzlich denkbar, dass das Signaturzertifikat kompromittiert würde.
beA-Nutzerinnen und -Nutzer, die dem Fernsignaturservice nicht vertrauen möchten, haben Möglichkeit, den sicheren Übermittlungsweg ohne qeS zu nutzen oder andere kartengebundene Signaturverfahren einzusetzen.

Auf welchem Informationskanal wird über versuchte oder erfolgreiche Angriffe auf die Zertifikatsserver berichtet?

Als qualifizierter Vertrauensdiensteanbieter unterliegt die Zertifizierungsstelle der BNotK den Regeln der eIDAS-VO und meldet Sicherheitsvorfälle der Bundesnetzagentur sowie anderen einschlägigen Stellen. Bei Auswirkungen auf natürliche oder juristische Personen werden auch diese umgehend über geeignete Kanäle informiert.

Welche Maßnahmen werden zum Monitoring derartiger Angriffe angewandt?

Siehe Antwort oben.

Wie wird im Falle eines Hacks sichergestellt, dass einerseits die Zertifikate gelöscht/ungültig gemacht werden und andererseits die Signaturmöglichkeit der Nutzer aufrechterhalten bleibt?

Bei einer Kompromittierung würden nur die betroffenen Schlüssel gesperrt. Eine Nutzung des Fernsignaturdienstes für nicht betroffene Zertifikatsinhaber bliebe daher grundsätzlich möglich. Im Rahmen des Business Continuity Managements wurden Prozesse entwickelt, die selbst bei größeren Incidents dabei gewährleisten können, möglichst schnell in einen sicheren Regelbetrieb übergehen zu können. Auch diese Prozesse sind Gegenstand der Zertifizierung.

b. Sicherstellung der Erreichbarkeit des Signaturservers - keine technische Unmöglichkeit, wenn Signatur nicht geleistet werden kann

§ 130d ZPO und vergleichbare Verfahrensvorschriften ermöglichen es, bei einer "vorübergehenden technischen Unmöglichkeit der Übermittlung" auf klassische Kommunikationswege (Post, Telefax, Einwurf) auszuweichen.
Kann ein Schriftsatz mangels Erreichbarkeit des Zertifikatsservers nicht unterzeichnet werden, stellt dies keine technische Unmöglichkeit i. S. d. § 130d ZPO dar. Ein Ausweichen auf analoge Kommunikationswege ist unzulässig, wenn nur die Unterschrift/Signatur nicht geleistet werden kann.
Schon in der Vergangenheit gab es in Einzelfällen Probleme, den Zertifikatsserver (sei es zur Prüfung einer Signatur, sei es zur Anbringung einer Signatur) temporär zu erreichen.

Wie wird seitens der BRAK sichergestellt, dass die von ihr beworbene und implementierte Fernsignatur künftig ununterbrochen möglich ist?

Auch wenn eine dauerhafte Verfügbarkeit von 100% im Kontext von IT-Systemen nicht gewährleistet werden kann, strebt die BNotK eine möglichst hohe Annäherung an diese Quote an. Hierzu werden aufgetretene Störungen stets umfassend analysiert und im Rahmen laufend stattfindender Verbesserungen berücksichtigt. Dies zeigen auch die Verfügbarkeitszahlen der vergangenen Monate:

Monat	Verfügbarkeit
Nov 22	100,00 %
Dez 22	99,66 %
Jan 23	99,87 %
Feb 23	99,90 %

Die BRAK hat darüber hinaus das zentrale Logging im beA-System erweitert, um Ausfälle feststellen zu können und darüber ihrerseits informieren zu können.

Wie wird die Erreichbarkeit des Signaturservers dokumentiert:

Sämtliche Ausfälle werden intern im Rahmen des Incident Managements dokumentiert und im Problem Management aufgearbeitet. Zudem meldet die BNotK aktuelle Störungen stets auf der Webseite https://onlinehilfe.bnotk.de/einrichtungen/bundesnotarkammer/xnp/stoerung-information-wartung.html.

Wie wird über Ausfallzeiten des Servers berichtet, werden diese für Wiedereinsetzungsanträge dokumentiert?

Neben der Meldung aktueller Störungen durch die BNotK auf der Webseite https://onlinehilfe.bnotk.de/einrichtungen/bundesnotarkammer/xnp/stoerung-information-wartung.html erfolgt die Dokumentation von Störungen über die Seite des beA-Anwendersupports: https://portal.beasupport.de/verfuegbarkeit Die BNotK informiert den beA-Anwendersupport über einen eigens für solche Störungsmitteilungen eingerichteten Kanal, so dass der beA-Anwendersupport die Störung in die auf der Seite vorgehaltene Störungsdokumentation aufnehmen kann.
Das Anbringen einer qualifizierten elektronischen Signatur ist für die fristwahrende Einreichung eines Schriftsatzes zudem nicht zwingend erforderlich. § 130a Abs. 3 S. 1 Alt. 2 ZPO und die parallelen Regelungen der weiteren Verfahrensordnungen lassen es genügen, wenn der Schriftsatz mit einer einfachen Signatur versehen und auf einem sicheren Übermittlungsweg an das Gericht übermittelt wird (vgl. auch OLG Düsseldorf, NJW-RR 2022, 999, 1001).

Welche alternativen Möglichkeiten der Nutzung der Fernsignatur werden bereitgestellt, wenn der Signaturserver nicht erreichbar ist?

Ohne Erreichbarkeit des Signaturservers ist eine Anbringung von Signaturen nicht möglich. Dieser Fall tritt jedoch selten und in der Regel nur für kurze Zeit ein.
Alternativ stehen die Nutzung eines vom beA unterstützten kartengebundenen Signaturverfahrens oder die Einreichung über den sicheren Übermittlungsweg zur Verfügung.

Gibt es Anstrengungen, § 130d ZPO und die vergleichbaren Verfahrensvorschriften an die technischen Unmöglichkeiten der Signaturanbringung anzupassen? Falls ja, welche?

Uns sind keine entsprechenden Bestrebungen bekannt.
Eine vorübergehende technische Unmöglichkeit der Anbringung einer qualifizierten elektronischen Signatur allein führt auf Grund der Möglichkeit der Übermittlung mit einfacher Signatur auf einem sicheren Übermittlungsweg auch nicht zur Unmöglichkeit der Fristwahrung. Das Risiko der Unmöglichkeit des qualifiziert elektronischen Signierens besteht zudem auch bei der kartengebundenen Signatur, etwa auf Grund des Defekts oder Verlusts der Karte. Die Bundesrechtsanwaltskammer empfahl daher auch in Zeiten der ausschließlich kartengebundenen Signatur, jedenfalls ein weiteres Zugangsmittel vorzuhalten

oder einen Vertreter zu berechtigen, damit der Versand jedenfalls über den sicheren Übermittlungsweg erfolgen kann (vgl. v. Seltmann, BRAK-Magazin 06/2021).

c. Welche Daten werden bei Nutzung der Fernsignatur übertragen?

Bei der Signaturanbringung findet ein Austausch von Daten zwischen dem Zertifikatsserver und dem Rechner des Nutzers statt.

Welche Daten werden hierbei übertragen?

Bei der Nutzung der Fernsignatur werden sogenannte Signature Activation Data (SAD) übertragen. Hierbei handelt es sich um nicht menschenlesbare Zeichenfolgen. Die SAD beinhalten Daten zur Anmeldung am Dienst (sog. Identity Token), den zur Signatur ausgewählten Signaturschlüssel (KeyID), den Hash-Algorithmus mit dem signiert werden soll und eine Liste von Hashwerten der zu signierenden Dokumente. Bei einem Hashwert handelt es sich um einen mathematischen Fingerabdruck, von welchem – wie bei einem menschlichen Fingerabdruck – jedoch nicht auf den Inhalt des Dokuments (oder auch nur die Art des Dokuments) geschlossen werden kann. Der Hashwert des Wortes „Fernsignatur“ (Hashmethode SHA-256) lautet etwa:
6a6341b48400cd30046240ef2782fbe6a15999b67658e382bdceccee88e47379

In welcher Form sind diese Daten verschlüsselt?

Die Übertragung der Daten wird mittels TLS (Transport Layer Security) nach dem aktuellen Stand der Technik geschützt. Hierbei wird die Technische Richtlinie 02102-2 des Bundesamtes für Sicherheit in der Informationstechnik beachtet.

An wen werden diese Daten übertragen?

Die Daten werden ausschließlich an die Systeme der BNotK übertragen.

d. Welche Daten werden geloggt?

Werden die im Rahmen der Signaturanbringung an die BNotK oder Dritte übermittelten Daten (beispielsweise IP-Adresse, Name, Datum, Zeitpunkt, GeoDaten, Dokumentenname, Hash-Wert, ...) bei der BNotK oder dem Dritten gespeichert?

Die übermittelten Hashwerte, der Signaturzeitpunkt und die ID des für die Signatur genutzten Schlüssels werden in einem sogenannten Auditlog gespeichert. Zusätzlich wird vermerkt, ob die Signaturoperation erfolgreich durchgeführt werden konnte. Diese Daten lassen keinerlei Rückschluss auf die Art und den Inhalt des signierten Dokuments zu. Etwa IP-Adressen oder Geodaten werden nicht gespeichert.

Aus welchem Grund?

Die Speicherung der Daten im Auditlog erfolgt automatisch und ist ein verpflichtender Bestandteil der zertifizierten Fernsignaturlösung. Die Auditlogs dienen dazu, im Streitfall eindeutig nachweisen zu können, ob eine Signatur angebracht wurde oder nicht.

Wofür? Wie lange?

Die Daten werden ein Jahr lang gespeichert.

e. Welche Daten werden genutzt?

Findet eine Auswertung oder sonstige Nutzung der im Rahmen der Signaturanbringung übermittelten Daten durch die BRAK, die BNotK oder Dritte statt? Wenn ja, welche? Wenn ja, zu welchem Zweck?

Aus den Protokollen wird lediglich die Nutzungshäufigkeit pro Zeiteinheit ermittelt („Wie viele Signaturen in welchem Zeitraum?“). Diese aggregierten Daten werden für die Kapazitätsplanung genutzt.

f. Fernsignatur deckt nicht alle Bereiche der Offlinesignatur ab

Die Fernsignatur hat nach aktuellem Stand einen gegenüber der klassischen qualifizierten elektronischen Signatur (qeS) beschränkten Anwendungsbereich. Insbesondere Nutzer aus dem Bereich der Marken- und/oder Patentangelegenheiten stehen mit der alternativlos vorgenommenen Umstellung auf die Fernsignatur vor erheblichen tatsächlichen Problemen, da diese Chipkarten vom DPMA nicht unterstützt werden (siehe hierzu auch: https://www.dpma.de/docs/service/dpmadirekt/newsletter_53.pdf).

Wie wird sichergestellt, dass künftig nur standardisierte Hardware eingesetzt wird, die auch auf allen von unseren Berufsträgern zwingend zu nutzenden Zugangswegen genutzt werden kann?

Bis wann wird den im Marken- und/oder Patentrecht tätigen Kolleginnen und Kollegen eine praktisch umsetzbare Lösung angeboten? Wie wird diese kommuniziert werden?

Die geschilderte Situation beruht nicht auf einem Problem der Hardware, insbesondere nicht auf einer nicht gegebenen Standardkompatibilität der verwendeten Karten, sondern stellt ein reines Softwareproblem dar: Die Anwendung DPMAdirektPro bzw. die darin enthaltene Signaturanwendungskomponente unterstützen bislang keine Fernsignatur. Die Bereitstellung von Softwarekomponenten für eine Anbindung der Signaturfunktion durch Drittthersteller liegt jedoch nicht im Aufgabenbereich der Zertifizierungsstelle der BNotK. Es ist die alleinige Entscheidung des jeweiligen Softwareanbieters, welche Lösungen von seiner Software unterstützt werden und welche nicht.

2. Informationen zu künftigen Änderungen/Entwicklung im beA

Der für viele Nutzerinnen und Nutzer des beA unerwartet eingetretene beA-Kartentausch hat zahlreich zu Irritationen geführt und für Unverständnis gesorgt, nachdem dieser nicht in der gebotenen Breite und Tiefe seitens der BRAK kommuniziert wurde.

Die Kommunikation des Kartentausches erfolgte seit April 2022 durch die BRAK, die Rechtsanwaltskammern, die BNotK und den DAV über die bekannten Medien beA-Newsletter, Nachrichten aus Berlin, Websites der Zertifizierungsstelle der BNotK und des beA-Anwendersupports, BRAKMagazin, DAV-Depesche und mit persönlichen Nachrichten in die beA der Rechtsanwältinnen und Rechtsanwälte. Zusätzlich macht ein regelmäßig veränderter Banner-Text auf der Startseite der beA-Webanwendung auf den Kartentausch und die bereitgestellten Schritt-für Schritt-Anleitungen sowie das Video-Tutorial aufmerk-

sam. Nutzerinnen und Nutzer, die sich noch mit ihrer alten Karte anmelden, erhalten bei jeder Anmeldung einen Warnhinweis, dass dies nur noch bis zum 18.03.2023 möglich ist. Außerdem haben die Kanzleisoftware-Hersteller ihre Kunden auf Bitten der BRAK direkt angeschrieben, und um Hinterlegung der neuen Karten gebeten.
Die verschiedenen Möglichkeiten der Kommunikation in die Anwaltschaft hinein und die Frage, wie die Kolleginnen und Kollegen am besten erreicht werden könnten, hat die BRAK im beA-Anwenderbeirat diskutiert und die Hinweise der Mitglieder in der oben beschriebenen Weise umgesetzt.

Um dieses Kommunikationsdefizit für die Zukunft auszugleichen, wird deshalb nicht nur darum geben, wesentliche Änderungen deutlich früher und breit gestreut zu kommunizieren, sondern auch mitzuteilen,

a. ob aktuell oder in naher/ferner Zukunft Änderungen im beA oder in der beA-Struktur und
b. ob bereits jetzt künftige - auch nicht technische - Entwicklungen geplant sind

Änderungen im beA und Weiterentwicklungen finden laufend statt. Die BRAK entwickelt mit Wesroc gemeinsam das beA-System weiter und passt es an die aktuellen Gegebenheiten an. Anforderungen an die Weiterentwicklung des beA-Systems stammen aus dem Justizumfeld, ergeben sich aus Gesetzesänderungen, sind auf Hinweise der Nutzerinnen und Nutzer zurückzuführen oder werden im Rahmen der Aktualisierung u.a. aus IT-Sicherheitsgründen vorgenommen.
Umstellungen, die wie der beA-Kartentausch besondere Aktivitäten der Nutzerinnen und Nutzer erfordern, sind derzeit nicht geplant.
Die Änderungen, an denen derzeit gearbeitet wird, beziehen sich entweder auf technische Systemanpassungen, die die Nutzerinnen und Nutzer bei ihrer täglichen Arbeit mit dem beA nicht bemerken oder es handelt sich um funktionale Änderungen. Wie in der Vergangenheit auch werden alle Anpassungen und Änderungen am beA-System über den beA-Newsletter sowie die Supportseite des beA-Anwendersupports kommuniziert werden. Dort werden regelmäßig die Release-Notes veröffentlicht und Änderungen aus Nutzersicht beschrieben.

3. Wird auch mittel- und langfristig auf Java gesetzt?

Der beA SecurityClient setzt auf die Laufzeitumgebung Java. Unbestritten hat diese Laufzeitumgebung eine Reihe von Vorteilen, zeichnet sich aber auch immer wieder durch (teilweise gefährliche) Sicherheitslücken aus Alternativ zu der Laufzeitumgebung könnte der Client auch nativ für die entsprechenden Betriebssysteme geschrieben und angeboten werden.

Setzt die BRAK (bzw. der technische Dienstleister) mittel- und langfristig weiter auf Java als Laufzeitumgebung?

Falls ja, aus welchen Gründen wird eine zwar "bequeme" aber vergleichsweise unsichere Software eingesetzt?

Sind alle eingesetzten Softwarekomponenten aktuell lizenziert und werden nur in der je aktuellen Version eingesetzt?

Java ist eine weltweit etablierte Programmiersprache mit einer angemessenen Sicherheitsarchitektur.

Java-Applikationen können i.A. mit Hilfe der Java-Virtual-Machine auf verschiedenen Betriebssystemen

ausgeführt werden. Folglich muss im Rahmen der Entwicklung nur zu einem geringen Anteil auf betriebssystemspezifische Gegebenheiten eingegangen werden. Somit ist es der Software-Entwicklung vielmehr möglich, sich auf die funktionalen sowie die nicht-funktionale Aspekte (u.a. eventuelle Sicherheitsaspekte) innerhalb der jeweiligen Applikation zu konzentrieren.

Für Java, Java-Bibliotheken und weitere Komponenten des Java-Ecosystems besteht aufgrund seiner hohen Verbreitung und seines Umfanges durchaus eine Wahrscheinlichkeit, dass Fehler und Sicherheitslücken gefunden, weitreichend kommuniziert und diskutiert werden. Jedoch ist der Eindruck, dass in Bezug auf andere Programmiersprachen oder Laufzeittechnologien weniger Sicherheitslücken und/oder Fehler gefunden und weniger präsent diskutiert werden, kein valider Indikator für die tatsächliche durchschnittliche Fehleranzahl in diesen Systemen. Insbesondere ist nicht davon auszugehen, dass vornehmlich nativ programmierte Applikationen i.A. weniger Sicherheitslücken aufweisen, als Software, welche auf weit verbreiteten und somit umfangreich getesteten Technologien beruht.

Weitere Vorteile von Java-Technologien sind eine relativ hohe Anzahl von qualifizierten Java-Entwicklern und etablierten Build- und Deployment-Werkzeugpaketen. Java verfügt zudem über etablierte Sicherheits-Funktionen, wie bspw. Bytecode Verification und Secure Class Loading, welche als Sicherheitsgewinn anderen Technologien gegenüber gelten können.

Bei beA wird Java als Technologie auf dem beA-Zentralsystem und in der lokalen Komponente zur Ver- und Entschlüsselung sowie zur Kartenansteuerung verwendet. Diese lokale Komponente wird auf allen Systemen verwendet, die für den Zugang zur beA-Webanwendung genutzt werden. Aufgrund der geringen Abhängigkeit von betriebssystemspezifischen Besonderheiten kann die lokale Komponente auch mit vergleichsweise wenig Aufwand für verschiedene Betriebssystemen der Benutzer der beA-Webanwendung bereitgestellt werden. Die lokale Komponente bringt ihre eigene Java-Laufzeitumgebung mit und wird zusammen mit dieser getestet und aktualisiert. Kritischer zu bewertende Einsatzszenarien kommen bei beA nicht vor.

Alle Anwendungskomponenten und verwendeten Dritt- und Zulieferkomponenten inkl. der Java-Laufzeitumgebung unterliegen regelmäßigen Prüfungen und Bewertungen hinsichtlich ihres Aktualisierungsbedarfs und ihrer Nutzungsbedingungen. Somit wird sichergestellt, dass alle Software-Komponenten in einer entsprechend lizensierten und aktuellen Version eingesetzt werden.

Der Einsatz von Java kann durch einen beA-Benutzer Client-seitig bei Bedarf dadurch vermieden werden, indem der Zugriff auf das beA-Zentralsystem über die beA-Kanzleisoftwareschnittstelle mithilfe einer alternativen Anwendung (Kanzleisoftware) erfolgt.

4. Ist geplant, beA auch auf iOS, Android und ChromeOS anzubieten?

In zunehmendem Maße wird auch auf Berufsträgerseite mit mobilen Endgeräten gearbeitet. Neben den JRE-lauffähigen Betriebssystemen Windows, Linux und MacOS kommen auch Subnotebooks und Tablets mit den Betriebssystemen iOS, ChromeOS und Android zum Einsatz. Da dort der beASecurityClient nicht lauffähig ist, ist ein direkter Zugriff auf das Postfach unmöglich. Abhilfe bieten derzeit nur Applikationen von Drittanbietern, die über die Nutzung des Softwarezertifikats einen (teilweise auch dann nur eingeschränkten) Zugang zu beA ermöglichen.

Ist geplant, auch auf den verbreiteten Betriebssystemen iOS, ChromeOS und Android einen Zugang zu beA zu ermöglichen?

Falls ja, bis wann kann damit gerechnet werden?

Falls nein, aus welchen Gründen sollen diese Betriebssysteme nicht unterstützt werden?

Die BRAK prüft derzeit gemeinsam mit Wesroc die mögliche Bereitstellung einer beA-Anwendung für mobile Endgeräte. Bis voraussichtlich Mitte des Jahres 2023 soll ein Prototyp entwickelt werden, der die wichtigsten Funktionalitäten einer mobilen Anwendung abbildet. Auf dieser Grundlage sollen die weiteren Entscheidungen getroffen werden.

Die funktionalen und technischen Anforderungen an eine mobile Lösung werden derzeit diskutiert. Wann die Prüfungen abgeschlossen sein werden und ob und bis wann mit einer Bereitstellung für die Nutzerinnen und Nutzer zu rechnen ist, hängt von vielen zu prüfenden Faktoren im Hinblick auf die Vorstellungen der Nutzerinnen und Nutzer, rechtliche Gesichtspunkte und Fragen der IT-Sicherheit ab. Sobald diese Fragen geklärt sind, wird der Aufwand abzuschätzen sein, um die Entscheidung über die Umsetzung und den Zeitplan vorzubereiten.

5. Die beA-Basiskarte kann nachträglich um die für das qualifizierte elektronische Signieren erforderliche Signaturkomponente "aufgewertet" werden. Nach Auskunft der BNotK ist es nicht möglich, den Vertrag isoliert hinsichtlich der Signaturkomponente zu kündigen, so dass die Mitglieder ohne großen Aufwand zurück zur Basiskarte kommen. Tatsächlich ist es aktuell so, dass sowohl die beA-Basiskarte als auch die Fernsignatur gekündigt und eine neue beA-Basiskarte bestellt werden muss.

Ist die BRAK an die BNotK bereits herangetreten, um eine Teilkündigung (nur der Signaturkomponente) zu ermöglichen? Damit wäre ein einfacher(er) Wechsel ohne Hardwarewechsel und ohne erforderliche Sperrung des alten HW-Tokens und Hinzufügen des neuen HW-Tokens möglich.

Derzeit besteht in der Tat leider noch keine vertragliche Möglichkeit, die Signaturkomponente isoliert zu kündigen, sodass die Gesamtkündigung und Neubestellung bislang der einzige Weg ist, ein solches „Downgrade" durchzuführen. Die BNotK teilte auf Nachfrage der BRAK mit, dass sie bereits an den abrechnungstechnischen Voraussetzungen arbeite und zuversichtlich sei, in Zukunft für die isolierte Kündigung der Signaturkomponente eine einfachere Lösung anbieten zu können.

6. Wie lange wird die Möglichkeit der Offlinesignatur in der WebApplikation angeboten?

Aus unterschiedlichen, teils rechtlichen, teils faktischen Gründen steht eine Reihe von Nutzerinnen und Nutzern der Fernsignatur skeptisch gegenüber und es besteht das Bedürfnis, auch weiterhin im Offlineverfahren zu signieren. Um nicht auf die Fernsignatur angewiesen zu sein, signieren daher viele Berufsträgerinnen und Berufsträger mit Signaturkarten alternativer zugelassener Anbieter (vgl. https://www.bea-brak.de/xwiki/bin/view/BRAK/%2300013). Diese Nutzerinnen und Nutzer sind - sofern sie nicht über eigene Signatursoftware verfügen - heute und künftig darauf angewiesen, ihre Dokumente über die Web-Plattform zu signieren.
Da mit der Umstellung des beA auf die Fernsignatur an sich die technische Notwendigkeit entfällt, weiterhin die Offlinesignaturfunktion vorrätig zu halten, stellt sich die Frage, wie lange es in beA noch möglich sein wird, neben der Fernsignatur eine klassische qeS anzubringen.

Wird die Möglichkeit, mittels klassischer qeS auch in beA zu signieren, dauerhaft erhalten bleiben?

Falls diese abgekündigt werden soll, zu welchem Zeitpunkt?

Mit welchem Vorlauf wird dies angekündigt werden?

Derzeit bestehen keine Überlegungen, die kartengebundenen Alternativen zur Anbringung qualifizierter elektronsicher Signaturen abzukündigen.

7. Wie lange wird die Möglichkeit der Offlinesignatur über die API angeboten?

Die unter dem vorgenannten Punkt aufgeworfene Frage stellt sich auch für die bereitgestellte API. Die Umstellung der Offlinesignatur zur Fernsignatur stellte viele Softwarehersteller vor Probleme, da die bisher über die API angebotene Möglichkeit zu signieren die Anbringung einer Fernsignatur nicht unterstützt.
Viele Kanzleisoftware nutzende Berufsträgerinnen und Berufsträger legten sich in der Folge Signaturkarten zertifizierter Drittanbieter zu, um auch weiterhin offline innerhalb ihrer Anwaltssoftware signieren zu können.
Auch diese Nutzerinnen und Nutzer sind heute und künftig darauf angewiesen, dass die bisher über die API zur Verfügung gestellte Möglichkeit, offline eine qeS anzubringen, erhalten bleibt.

Wird die Möglichkeit, mittels klassischer qeS auch in beA zu signieren, dauerhaft erhalten bleiben?

Falls diese abgekündigt werden soll, zu welchem Zeitpunkt?

Mit welchem Vorlauf wird dies angekündigt werden?

Es bestehen derzeit keine konkreten Überlegungen, die über die beA-Kanzleisoftwareschnittstelle zur Verfügung gestellte Möglichkeit der Anbringung einer qualifizierten elektronischen Signatur mittels Signaturkarte abzukündigen.
Die BRAK bietet derzeit Funktionen des Governikus-Signers im Toolkit an. Die weitere Unterstützung über die Schnittstelle und das Toolkit hängt daher auch davon ab, inwieweit von Governikus diese Software weiter bereitgestellt und gepflegt wird und ob die BRAK ggf. Nachfolgeprodukte für eine Signaturanwendungskomponente zur Verfügung stellen kann und darf.
Die BRAK befindet sich im intensiven Austausch mit dem Softwareindustrieverband Elektronischer Rechtsverkehr (SIV-ERV). Sollte auf längere Sicht eine Änderung der Schnittstelle im Hinblick auf Signaturmöglichkeiten erfolgen müssen, wird die BRAK die Kanzleisoftware-Hersteller umgehend informieren und Alternativen besprechen sowie die sich daraus ergebenden Fragen im beA-Anwenderbeirat besprechen.

8. § 31a BRAO verpflichtet die BRAK, Zugang zum ERV herzustellen und jedem Mitglied ein besonderes elektronisches Anwaltspostfach empfangsbereit einzurichten.

Da von dieser Leistung alle Mitglieder profitieren, wird diese durch eine Umlage finanziert. Eine Verpflichtung zu weitergehenden Leistungen kennt die BRAO nicht. Insbesondere ist die BRAK

nicht gesetzlich verpflichtet und ermächtigt, neben dem Zugang zum beA weitere Serviceprodukte anzubieten, die aus der Umlage aller Mitglieder finanziert, aber nur von einem Teil der Mitglieder genutzt werden. Hierzu gehören insbesondere die Möglichkeiten zu signieren und Signaturen zu prüfen.

Gibt es eine Evaluation, in welcher Höhe Mittel aus der Umlage für diese Funktionen verwendet wurden?

Gibt es eine Planung, in welcher Höhe künftig Mittel aus der Umlage für derartige Funktionen verwendet werden sollen?

Gibt es eine Evaluation, durch welchen Anteil der Nutzerinnen und Nutzer diese Zusatzfunktionen genutzt werden?

Falls nein, warum?

Falls ja, wie viele Nutzerinnen und Nutzer bedienen sich dieser Funktionen?

Gem. § 31a BRAO besteht für die Bundesrechtsanwaltskammer die Verpflichtung, für jede im Gesamtverzeichnis eingetragene natürliche Person ein besonderes elektronisches Anwaltspostfach empfangsbereit einzurichten. Gem. § 31b BRAO ist die BRAK ebenso verpflichtet, auch für jede im Gesamtverzeichnis eingetragene Ausübungsgesellschaft ein besonderes elektronisches Anwaltspostfach empfangsbereit einzurichten. Darüber hinaus regelt § 177 Abs. 2 Nr. 7 BRAO als Aufgabe der BRAK die Unterstützung der elektronischen Kommunikation der Rechtsanwälte mit Gerichten, Behörden und sonstigen Dritten. Zur Erfüllung der gesetzlichen Aufgaben erhebt die Bundesrechtsanwaltskammer von den Rechtsanwaltskammern gem. § 178 Abs. 1 BRAO Beiträge, die zur Deckung des persönlichen und sächlichen Bedarfs bestimmt sind.

Aus diesen gesetzlichen Verpflichtungen ist zu folgern, dass es nicht nur Aufgabe der BRAK ist, das beA für Rechtsanwältinnen und Rechtsanwälte sowie Berufsausübungsgesellschaften empfangsbereit einzurichten, sondern auch die elektronische Kommunikation mit Gerichten, Behörden und sonstigen Dritten zu fördern. Zur Förderung der elektronischen Kommunikation gehört in erster Linie die – für Rechtsanwältinnen und Rechtsanwälte verpflichtende - Übermittlung elektronischer Dokumente im Sinne des § 130a ZPO. § 130a Abs. 3 ZPO und die entsprechenden Vorschriften in den übrigen Verfahrensordnungen sehen zwei mögliche Übermittlungswege für elektronische Dokumente vor: Entweder muss das Dokument mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Es ist verfahrensrechtlich nicht möglich und v.a. nicht im Interesse der Mitglieder, alle Rechtsanwältinnen und Rechtsanwälte darauf zu verweisen, den sicheren Übermittlungsweg zu nutzen und auf den Einsatz der qualifizierten elektronischen Signatur zu verzichten. Denn die Rechtsprechung setzt für erfolgreiche Wiedereinsetzungsanträge voraus, dass Rechtsanwältinnen und Rechtsanwälte darlegen, dass die fristgerechte Einreichung eines elektronischen Dokuments trotz ordnungsgemäßer Schulung und stets sorgfältigen Handels der Mitarbeiterin und oder des Mitarbeiters versäumt wurde. Nutzt die Rechtsanwältin oder der Rechtsanwalt den sicheren Übermittlungsweg und versendet das elektronische Dokument höchstpersönlich mit einfacher Signatur, bliebe dieser Vortrag im Rahmen des Wiedereinsetzungsantrags verwehrt. Arbeitsteiliges Arbeiten setzt somit die Möglichkeit des Anbringens einer qualifizierten elektronischen Signatur voraus, die im Rahmen der Bereitstellung des beA angeboten wird. Schon daraus folgt, dass die BRAK auf Grundlage des § 177 Abs. 2 Nr. 7 BRAO und im Interesse der Rechtsanwältinnen und Rechtsanwälte die Möglichkeit anbieten muss, dass elektronische Dokumente qualifiziert elektronisch signiert eingereicht werden können.

Darüber hinaus ist das Anbringen qualifizierter elektronischer Signaturen in Vertretungsfällen erforderlich. Dass und wie in diesen Fällen der elektronische Rechtsverkehr genutzt wird, regelt § 25 RAVPV, der auf der Grundlage der Ermächtigungsgrundlage in § 31d BRAO erlassen wurde und durch die BRAK zu beachten ist.

Gem. § 177 Abs. 2 Nr. 7 BRAO unterstützt die BRAK ferner die elektronische Kommunikation mit Behörden. Für die elektronische Kommunikation mit Behörden ist der sichere Übermittlungsweg nicht vorgesehen, das Anbringen einer qualifizierten elektronischen Signatur als Ersatz der handschriftlichen Unterschrift ist somit zwingend. Auch aus diesem Grund muss die BRAK die Möglichkeit zum qualifizierten elektronischen Signieren bereitstellen.

Schließlich regelt die Verordnung über die technischen Rahmenbedingungen des Elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (ERVV) die Einzelheiten der Übermittlung elektronischer Dokumente. Auch danach ist in § 4 ERVV die Übermittlung elektronischer Dokumente mit qualifizierter elektronischer Signatur vorgesehen.

Es ist somit festzuhalten, dass mit den Vorschriften der BRAO i.V.m. den verfahrensrechtlichen Vorschriften sowie den den elektronischen Rechtsverkehr betreffenden Verordnungen eine ausreichende Rechtsgrundlage für die Bereitstellung der Möglichkeit vorliegt, qualifizierte elektronische Signaturen anzubringen.

Gleiches gilt für die Möglichkeit, Signaturen zu prüfen. Die Rechtsprechung verlangt, dass Rechtsanwältinnen und Rechtsanwälte sich bei der Einreichung elektronischer Dokumente versichern, dass die Signaturen, zu denen auch der vertrauenswürdige Herkunftsnachweis (VHN) als Nachweis über den sicheren Übermittlungsweg gehört, wirksam angebracht wurden. Dies kann nur durch eine Signaturprüfung verifiziert werden. Die Prüfprotokolle für die Prüfung des VHN und einer qualifizierten elektronischen Signatur unterscheiden sich nicht.

Es existiert keine Evaluation, in welcher Höhe Mittel aus den Beiträgen der Rechtsanwaltskammern an die Bundesrechtsanwaltskammer bzw. aus den Umlagen, die die Mitglieder an ihre Rechtsanwaltskammern zahlen, für die Signaturfunktion im beA verwendet wurden. Es liegt auch keine Planung vor, in welcher Höhe künftig Mittel aus der Umlage für eine derartige Funktion verwendet werden sollen.

Der BRAK ist nicht bekannt, zu welchem Anteil Nutzerinnen und Nutzer Nachrichten qualifiziert elektronisch signieren. Es existiert keine Protokollierung bzw. kein Logging hierzu. Zu berücksichtigen ist, dass die Signaturanbringung lokal auf Seiten der Anwender stattfindet und nicht im beA-Zentralsystem, auf dessen Logging-Daten der beA-Betrieb Zugriff hat.

Entwicklungswünsche für das beA

Gerade durch die Einführung der aktiven Nutzungspflicht des beA zum 01.01.2022 und der damit verstärkten Nutzung durch unsere Berufsträgerinnen und Berufsträger sind Ideen zur Fortentwicklung der Weboberfläche an uns herangetragen worden.

Das Ergebnis einer nicht repräsentativen Umfrage unter den Nutzerinnen und Nutzern, welche zusätzliche Funktionen bereitgestellt werden sollten bzw. welche Änderungen den Arbeitsprozess mit beA erleichtern würden, möchten wir Ihnen nachfolgend zusammenfassen und um Mitteilung bitten, ob bzw. bis wann seitens der BRAK geplant ist, diese Änderungswünsche umzusetzen:

1. Die Nutzung der Weboberfläche ist nach wie vor sehr klickintensiv. Sollen Anlagen (Schriftsätze und Anhänge) einer Nachricht hinzugefügt werden, muss ein Auswahlfenster geöffnet werden. In diesem müssen nach Auswahl des Zielordners die einzelnen Dateien dort ausgewählt werden, um sie im Anschluss hochladen zu können.

Ein direktes Drag and Drop der lokal gespeicherten Dateien in das Browserfenster mit der erzeugten Nachricht ist nicht möglich. Hier wäre es wünschenswert, wenn Dateien direkt in das Browserfenster "gezogen" werden könnten, ohne dass der Umweg über das erst zu öffnende Auswahlfenster und die folgende Zielordnerauswahl getätigt werden muss.

Im Rahmen der Weiterentwicklung wird die BRAK prüfen, ob die Hinzufügung von Anlagen vereinfacht werden kann. Gegenstand der laufenden Weiterentwicklungen sind auch Anpassungen bei der Nutzerfreundlichkeit und den Oberflächen.

2. Die Nutzung der Weboberfläche ist nach wie vor sehr mausintensiv. Die Verwendung von Tastaturkürzeln ist aktuell nicht vorgesehen, würde die Nutzung aber erheblich beschleunigen und vereinfachen. Wenn beispielsweise mit "Cmd-N " eine neue Nachricht erzeugt, mit "Cmd-E " ausgewählte Nachrichten exportiert, mit "Cmd-Backspace" dieselben gelöscht, etc. werden könnten (und diese Tastaturkombinationen auch direkt in den Buttons angezeigt werden würden) wäre dies eine große Erleichterung.

Die beA-Webanwendung sieht insbesondere auch aus Gründen der Verbesserung der Barrierefreiheit die Verwendung von Tatstarurkürzeln, sogenannten Shortcuts, vor. Folgende Shortcuts sind bereits implementiert:
Alt + n = Erzeugt einen neuen Nachrichtenentwurf
Alt + o = Öffnet die aktuell ausgewählte Nachricht
Alt + p = Öffnet die Druckansicht der Nachricht
Alt + e = Exportiert die aktuelle Nachricht

Diese Liste wird in einem der nächsten beA-Releases erweitert werden. Eine entsprechende Abstimmung mit Kolleginnen und Kollegen, die über eine eingeschränkte Sehfähigkeit verfügen und deshalb auf eine barrierefreie Nutzung des beA angewiesen sind, ist erfolgt.

3. Allgemein zugängliche, dokumentierte API

Gibt es eine allgemein zugängliche Dokumentation für die beA KSW-Schnittstelle und das KSW-Toolkit? Ist geplant, unabhängig von Kanzleisoftwareherstellern eine offene und dokumentierte allgemein zugängliche API anzubieten?

Falls dies der Fall sein sollte, bis wann soll dies umgesetzt werden?
Falls dies nicht geplant ist, aus welchen Gründen ist dies nicht geplant?

Für Software-Hersteller, die die beA-Funktionalität in ihrem Produkt anbieten möchten, bietet das beA eine eigene Schnittstelle und ein zugehöriges Tooling an. Die KSW-Schnittstelle ist ein Webservice basierend auf dem SOAP-Standard und wird um ein optionales Toolkit (Java-Bibliothek) ergänzt.
Die wesentlichen Funktionen des beA werden externen Applikationen, wie bspw. Kanzleisoftware-Lösungen, über die sogenannte Kanzleisoftware-Schnittstelle (KSW-Schnittstelle) zur Verfügung gestellt. Die KSW-Schnittstelle ermöglicht es Software-Herstellern somit, das beA in ihre Produkte zu integrieren bzw. den Zugriff auf ein beA aus ihren Produkten heraus zu implementieren. Die KSW-Schnittstelle ermöglicht ebenfalls die Anbindung an die Justiz-Infrastruktur über das beA System und somit die Kommunikation mit allen möglichen Kommunikationspartnern im elektronischen Rechtsverkehr.

Die Schnittstelle ist grundsätzlich nach einer Prüfung, ob ein berechtigtes Interesse besteht, und einer Registrierung, die zum Austausch von Informationen als Grundlage für die Teilnahme am elektronischen Rechtsverkehr benötigt werden, allgemein zugänglich. Der Zugriff auf die KSW-Schnittstelle ist neben TLS auch durch eine SSL-Client-Authentifizierung abgesichert. Für die Konfiguration der Client-Authentifizierung ist deshalb der direkte Austausch zwischen beA-Betrieb und Software-Hersteller erforderlich. Die Teilnahme am ERV setzt außerdem u.a. die Angabe der Herstellerinformationen voraus. Auch zu Erfüllung dieser Anforderunng ist die Registrierung notwendig.
Die KSW-Schnittstelle ist dokumentiert. Die Dokumentation setzt sich aus der einführenden Dokumentation zur beA-Integration - Online-Hilfe, Benutzerhandbuch zur Integration externer Produkte und Use Cases zur Integration von beA-Prozessen in externe Produkte – sowie die Release-bezogene Dokumentation - kommentierte WSDL, das KSW-Toolkit mit der zugehörigen Javadoc sowie der Quellcode und eine Testsuite mit Quellcode, die verschiedene Standardtestfälle implementiert - zusammen.
Die KSW-Schnittstelle wird zudem supported. Der KSW-Support leistet Unterstützung sowohl im Betrieb als auch in der Entwicklung. Er hilft bei der Analyse und Behebung konkreter betrieblicher Probleme und beantwortet entwicklungsseitig Fragen zur Nutzung des KSW-Toolkits und der KSW-Schnittstelle.

4. Aktuell findet beim Versand der Nachrichten über beA keine Ende-zu-Ende-Verschlüsselung der Nachrichten statt. Mit in der Anzahl und Qualität zunehmenden Cyberangriffen stellt der Versand unverschlüsselter Nachrichten auch in einem an sich geschützten Umfeld ein immer relevanter werdendes Sicherheitsproblem dar.

Ist geplant, eine Ende-zu-Ende-Verschlüsselung einzuführen?
Falls ja, bis wann soll dies umgesetzt werden?
Falls nein, aus welchen Gründen findet keine Entwicklung in diese Richtung statt?

Es ist nicht richtig, dass beA-Nachrichten unverschlüsselt versandt werden. Sämtliche Nachrichten werden vom Sender verschlüsselt und vom Empfänger erst wieder entschlüsselt. Sie bleiben somit durchgehend verschlüsselt. Die Nachricht liegt also zu keiner Zeit – auch nicht im HSM – unverschlüsselt vor.
Es ist derzeit nicht konkret geplant, an dieser Konzeption etwas zu ändern, da BRAO und RAVPV vorsehen, dass der Postfachinhaber anderen Personen das Recht einräumen muss, Nachrichten in seinem Postfach zu entschlüsseln. Für Zustellungsbevollmächtigte ist dies in § 30 Abs. 1 Satz 3 BRAO, für Vertretungen in § 54 Abs. 2 Satz 2 BRAO geregelt.

5. Immer wieder werden zu versendende Nachrichten im beA aufgrund eines (technischen) Fehlers tatsächlich nicht versandt. Dies betrifft die Abgabe von eEBs wie auch den Versand erzeugter Nachrichten in gleichem Maße.

In diesen Fällen ist es aktuell nicht möglich, die nicht gesendete Nachricht oder das eEB erneut zu senden. Vielmehr müssen diese Nachrichten/eEB erst umständlich und wenig intuitiv gelöscht und sodann neu erstellt werden, um einen erneuten Sendevorgang zu starten.

Im Rahmen der Weiterentwicklung wird in einer der nächsten Versionen der beA-Webanwendung die Möglichkeit eingeführt werden, den Nachrichtenversand aus dem Postausgang erneut anzustoßen.
Der beschriebene Fehler ist im Übrigen darauf zurückzuführen, dass bei Nichterreichbarkeit der Intermediäre der Justiz die zu versendende Nachricht im Postausgang verbleibt.

6. Um ein effizientes Arbeiten mit der Weboberfläche zu ermöglichen, ist es sinnvoll, dass mehrere Tabs geöffnet werden können, um beispielsweise während des Sendevorgangs einer Nachricht bereits in einem neuen Fenster den Versand einer weiteren Nachricht vorzubereiten. Die aktuelle Weboberfläche führt zu teilweise nicht unerheblichen Wartezeiten, wenn Nachrichten exportiert oder Anhänge hochgeladen werden.

Während die Funktion, einen Link mittels "Cmd-Klick" in einem neuen Tab zu öffnen, in der Vergangenheit von der Weboberfläche unterstützt wurde, ist diese Funktion mit einem der letzten Updates abgeschafft worden.

Es wäre schön, wenn die Möglichkeit, in parallelen Tabs mit der Weboberfläche arbeiten zu können, wieder eingeführt werden würde.
Aktuell ist dies zwar auf einem Umweg (Rechtsklick auf den Link und "Öffnen in neuem Tab") nach wie vor möglich. Dieser Weg führt aber immer nur zur Eingangsseite der Weboberfläche und zudem zu technischen Schwierigkeiten, da der Sendevorgang der ersten Nachricht ggfs. unterbrochen oder sogar abgebrochen wird.

Die Entscheidung, nicht mehr mehrere Tabs zur Verfügung zu stellen, ist im Rahmen der ersten Stufe der Überarbeitung der beA-Webanwendung erfolgt.
Die Entscheidung wurde mit dem beA-Anwenderbeirat besprochen. Tests mit Nutzerinnern und Nutzern ergaben, dass diese mit der geänderten Oberfläche sehr gut arbeiten konnten.

7. Befinden sich auf der Weboberfläche im Postein- oder Postausgang gespeicherte Nachrichten über mehrere Seiten hinweg und wird beispielsweise eine auf Seite 4 gespeicherte Nachricht geöffnet, wird der Nutzer automatisch beim Schließen der Nachricht zurück auf Seite 1 geleitet und muss erneut die vorherige Seite 4 aufrufen. Dies führt zu einem umständlichen und zeitintensiven Prozess. Hierzu wurde die Anregung geäußert, dies technisch so zu ändern, dass der Nutzer beim Schließen der Nachricht auf derjenigen Seite verbleibt, auf welcher er sich zuvor befunden hat.

Im Rahmen der weiteren Überarbeitung der Oberfläche der beA-Webanwendung wird das Blättern durch einen Scroll-Balken ersetzt werden, so dass sich alle Nachrichten immer auf einer Seite befinden.

8. Im Hinblick auf die erst kürzlich ergangene Entscheidung des BGH vom 20.09.2022 - Az. XI ZB 14/22 zu den Anforderungen an die Überprüfung der ordnungsgemäßen Übermittlung fristgebundener Schriftsätze besteht die Anregung, den Übermittlungsstatus einer Nachricht in der Übersichtszeile der gesendeten Dokumente (Reiter "Gesendet") um eine Ansicht der versandten Dokumente zu erweitern.

Anbieten würde sich hierbei eine Dropdown-Liste in der Spalte “Übermittlungsstatus”, um in Form einer Schnellkontrolle festzustellen, ob ein erfolgreicher Versand aller (und welcher) Dokumente erfolgt ist. In diesem Zusammenhang müssten die Dateinamen der übertragenen Dokumente in der Übertragungsübersicht sichtbar sein.

Die Anregung, den Übermittlungsstatus einer Nachricht in der Übersichtszeile der gesendeten Dokumente um eine Ansicht des versandten Dokuments zu erweitern, wird die BRAK gemeinsam mit Wesroc im Rahmen der Weiterentwicklung prüfen.

9. Um den für Aktualisierungen des beA SecurityClients notwendigen Zeitaufwand besser in den Kanzleialltag einplanen zu können wird gewünscht, dass künftig möglichst frühzeitig über geplante und anstehende Updates auf der Startseite (www.bea-brak.de/bea/) hingewiesen wird. Um den zeitlichen Aufwand möglichst gering zu halten, wäre es wünschenswert, wenn Updates grundsätzlich nicht montags und freitags gefahren werden, da an diesen Tagen die Belastung erfahrungsgemäß höher als an den übrigen Wochentagen ist.

Die Anregung, Aktualisierungen der beA Client-Security so rechtzeitig wie möglich anzukündigen, greift die BRAK gerne auf. Eine entsprechende Überarbeitung der Startseite, die auch Hinweise auf bevorstehende Aktualisierungen erhalten wird, ist derzeit in der Umsetzung. Updates finden im Übrigen grundsätzlich mittwochs in der Zeit zwischen 01:00 Uhr und 06:00 Uhr, ausnahmsweise auch am Wochenende, statt. In der Regel müssten Aktualisierungen der Client-Security also zum Beginn der Bürozeiten am Mittwoch vorgenommen werden.