

DAS BESONDERE ELEKTRONISCHE ANWALTSPOSTFACH (BEA)

Friederike Lummel / Thomas Fenske / Heiner Boyn

Rechtsanwältin und Geschäftsführerin, Projektleiterin beA, Bundesrechtsanwaltskammer
Littenstraße 9, 10179 Berlin, DE
lummel@brak.de; <http://www.brak.de>

Geschäftsführer, Projektleiter beA, Bundesrechtsanwaltskammer
Littenstraße 9, 10179 Berlin, DE
fenske@brak.de; <http://www.brak.de>

Senior Managing Consultant, externer Berater im Projekt beA, Capgemini Deutschland GmbH
Lübecker Strasse 128, 22087 Hamburg, DE
heiner.boyn@capgemini.com; <http://www.capgemini.com>

Schlagworte: *Barrierefreiheit, beA, besonderes elektronisches Anwaltspostfach, BRAK, Bundesrechtsanwaltskammer, Datenschutz, Datensicherheit, elektronischer Rechtsverkehr, Ende-zu-Ende-Verschlüsselung, Qualitätsziele, Sicherheitsarchitektur, Support, Webanwendung, Zwei-Faktor-Authentifizierung*

Abstract: *Die Bundesrechtsanwaltskammer (BRAK) hat über das ERV-Gesetz die Aufgabe erhalten, den rund 165.000 zugelassenen Anwältinnen und Anwälten in Deutschland ein «besonderes elektronisches Anwaltspostfach» einzurichten.
Die Qualitätsziele in dem Projekt sind maßgeblich durch Datenschutz und Datensicherheit sowie die Wahrung der anwaltlichen Verschwiegenheit geprägt.
Die Sicherheitsarchitektur realisiert u.a. die Ende-zu-Ende-Verschlüsselung und die Zwei-Faktor-Authentifizierung für den Zugang zu beA.
Im Projekt beA stellen sich besondere Herausforderungen, die sich insb. aus der Anzahl und Verschiedenheit der Beteiligten und der hohen Anforderungen an die Sicherheit ergeben.*

1. Elektronischer Rechtsverkehr, rechtliche Grundlage für die Einführung des beA in Deutschland

Rechtliche Grundlage für das beA ist das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (ERV-Gesetz) vom 10. Oktober 2013. Hauptziel ist die stufenweise flächendeckende Einführung des elektronischen Rechtsverkehrs. Dazu wird der elektronische Schriftverkehr mit den Gerichten verbindlich eingeführt. Der Bundesrechtsanwaltskammer (BRAK) obliegt als Selbstverwaltungskörperschaft gemäß § 31a Bundesrechtsanwaltsordnung (BRAO) n.F. die Aufgabe, für jede und jeden der rund 165.000 Rechtsanwältinnen und Rechtsanwälte ein beA einzurichten, das im Sinne des § 130a IV Nr. 2 ZPO n.F. als «sicherer Übermittlungsweg» gilt. Das beA ist damit ein Teilbeitrag zur Erfüllung des gesetzlich statuierten Ziels.

2. Qualitätsziele des Projektes

Die gesetzlichen Anforderungen bestimmen die Qualitätsziele des Projektes, dabei prägen die Realisierung von Datenschutz und Datensicherheit sowie die Wahrung der anwaltlichen Verschwiegenheit durch das beA den hohen Qualitätsmaßstab und sind das entscheidende Kriterium für den Erfolg des beA. Die in Abbildung 1 dargestellten Maßnahmen flankieren den hohen Qualitätsmaßstab:

- Nur über die Zwei-Faktor-Authentifizierung wird der Zugang zum beA eröffnet. Sie ist ein weiterer wichtiger Aspekt im Hinblick auf den gesetzlich geforderten «sicheren Übermittlungsweg».
- Jede Rechtsanwältin und jeder Rechtsanwalt erhält ein beA. Viele stehen diesem «Pflichtpostfach» sehr skeptisch gegenüber, einige verfügen nicht einmal über eine E-Mail-Adresse. Die Nutzerakzeptanz dieser heterogenen und unabhängigen Berufsgruppe ist ein wesentlicher Schlüssel zum Erfolg des Projekts.
- Die Einhaltung des Einführungstermins ist für die BRAK ein wichtiges Qualitätsziel, das den beiden vorstehenden jedoch untergeordnet ist.
- Die Barrierefreiheit ist eine notwendige Konsequenz der für jeden Rechtsanwalt und jede Rechtsanwältin verpflichtenden Nutzung. Sie ist als Voraussetzung für einen breiten Zugang ein weiteres wichtiges Qualitätsziel des beA.

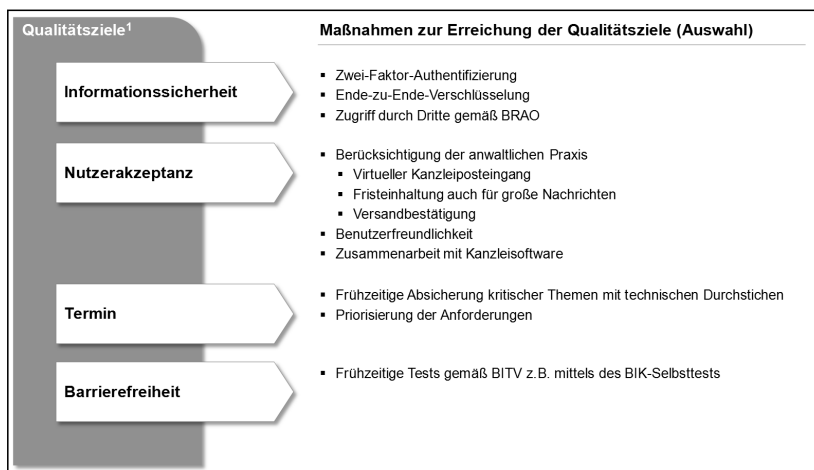


Abbildung 1: Qualitätsziele von beA und abgeleitete Maßnahmen

Die mit den Qualitätszielen von beA beschriebenen Ambitionen wurden zwischenzeitlich von der Realität eingeholt: Die letzten Tests im Herbst 2015 haben gezeigt, dass die BRAK nicht sicher sein konnte, dass das beA den hohen Anforderungen, die die BRAK an die Nutzerfreundlichkeit gestellt hat, tatsächlich bereits zu dem geplanten Start-Termin Anfang 2016 genügt hätte.

Es gab nun zwei Möglichkeiten: die Anforderungen zu senken oder den Start des beA zu verschieben. Nach langer und intensiver Diskussion im Präsidium der BRAK hat sich die BRAK für die zweite Alternative entschieden. Die BRAK möchte erst dann das beA übergeben, wenn sie sicher sein kann, dass alle Funktionalitäten verlässlich zur Verfügung stehen.

Atos, das mit der Entwicklung des beA beauftragte Unternehmen, und die BRAK sind in Abstimmung eines neuen Projektplans, aus dem sich dann auch ein neuer Starttermin für das beA ergeben wird.

3. Aufbau und Architektur des beA

Für das System beA wurde eine umfangreiche Sicherheitsarchitektur entwickelt, um den besonderen Anforderungen im elektronischen Rechtsverkehr zwischen Rechtsanwälten und Gerichten gerecht zu werden. Eine wichtige Anforderung war die Ende-zu-Ende-Verschlüsselung. Die per beA verschickten Nachrichten und an-

gehängte Dokumente bleiben dabei sowohl bei der Übertragung als auch im Posteingang des Empfängers stets verschlüsselt und werden zu jeder Ansicht oder Bereitstellung aus dem beA-System neu decodiert.

Für die Anmeldung der Nutzer am beA-System ist die gesetzliche Anforderung der Zwei-Faktor-Authentifizierung umgesetzt worden. Zur Absicherung des Zugriffs muss sich der Benutzer dabei mit zwei voneinander getrennten Sicherungsmitteln (Besitz und Wissen) anmelden. Dieses wurde für das beA wie folgt realisiert:

- Besitz
 - Der Anwender muss im Besitz eines persönlichen Sicherungsmittels (Token) sein
 - Dieses muss vor dem Zugriff durch Dritte geschützt sein
 - Typische Token sind Smart-Karten mit oder ohne Signaturfunktionen
- Wissen
 - Zur Nutzung des Besitzes ist zusätzlich ein Geheimnis erforderlich, das nur der rechtmäßige Besitzer kennt und das nirgends gespeichert werden darf
 - Typische Form: PIN oder Passwort.

Neben der Authentifizierung sind auch die Übertragung der Nachrichten und der Zugriff auf diese besonders geschützt. Wie Abbildung 2 zeigt, wahrt das beA-HSM (Hardware Security Module) dabei die Ende-zu-Ende-Verschlüsselung, insbesondere auch beim Nachrichtenzugriff durch mehrere Leser. Dafür muss nicht nur der Nachrichtenzugriff sondern auch die Rechtevergabe besonders abgesichert werden.

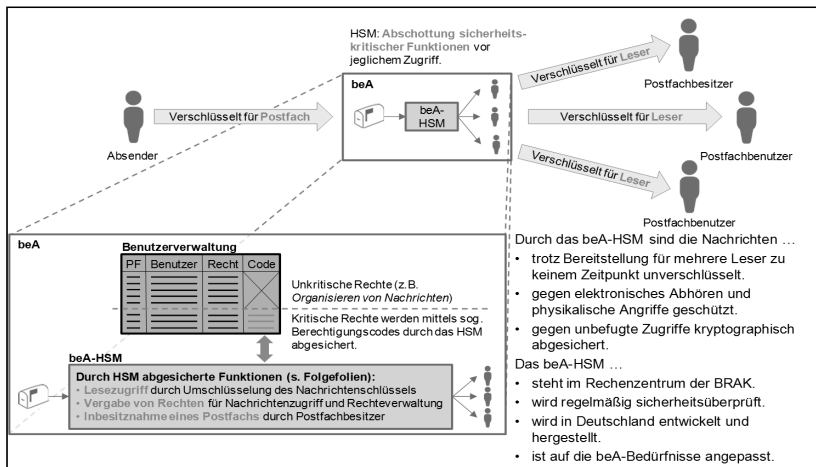


Abbildung 2: Verschlüsselung und Absicherung des Nachrichtenzugriffs

Das Postfach ist stets der Rechtsanwältin bzw. dem Rechtsanwalt persönlich zugeordnet. Über die Benutzerverwaltung wird die Zuweisung von unterschiedlichen Rechten und damit die kanzleitypische Arbeitsteilung mit Kollegen und Mitarbeitern ermöglicht. Ein Organisationspostfach für eine Kanzlei hat der Gesetzgeber nicht vorgesehen. Durch Rechtevergaben innerhalb der Kanzlei kann eine zentrale Posteingangsbearbeitung

realisiert werden. Zur elektronischen Kommunikation der Anwaltschaft mit den regionalen Rechtsanwaltskammern und Amtsgerichten erhalten diese ebenfalls ein Postfach.

Um den Sicherheitsanforderungen gerecht zu werden, ist eine enge Zusammenarbeit mit den regionalen Rechtsanwaltskammern zu Identifizierungsverfahren notwendig. Auch im Hinblick auf die Umsetzung und Akzeptanz des beA in der Anwaltschaft ist die Zusammenarbeit mit den Regionalkammern ein wichtiger Aspekt.

4. Besondere Projektherausforderungen

Es stellen sich im beA Projekt besondere Herausforderungen, die sich aus der Konstellation mit vielen Beteiligten und dem Projektauftrag mit den besonderen Rahmenbedingungen ergaben.

- Hohe Anzahl und sehr verschiedene Beteiligte
 - Nutzer (Anwaltschaft, Justiz, Kammern), Dienstleister (Atos, BNotK, Capgemini), SW-Anbieter (Kammern und Kanzlei), Schulungsanbieter mussten in Kommunikation, Terminabstimmung sowie die Koordination von Aktivitäten und Ergebnissen eingebunden werden
 - Empfunderer Zwang zur Nutzung des beA führt zu Widerstand/Diskussion eines Teils der Anwaltschaft
 - Hohe Anzahl der Nutzer (165.000 Rechtsanwältinnen und Rechtsanwälte sowie deren Mitarbeiter) führt zu sehr dynamischem Anfragevolumen an den Support (über telefonischen Help Desk, E-Mail und Portal)
- Hohe Anforderungen an die Sicherheit
 - Besondere Sicherheitsarchitektur (Zugang (beA-Karten), Verschlüsselung, Hardware Security Module) bedeutete in vielen Fällen den Einsatz von Experten und Aufbau von Verständnis für die eingesetzte Lösung bei allen Beteiligten
 - Besondere Sicherheitsanforderungen (geschützte Umgebungen) bedeuten erhöhte Aufwände auch bei Routinetätigkeiten wie Einspielen von Testdaten, Logging, kein Anwendungszugang durch Support
 - In Planung und Durchführung durch viele Beteiligte aufwendige Tests, bestehende Abhängigkeiten und zu betrachtende Schnittstellen (Justiz/Gerichte, Kammer-SW, Kanzlei-SW, bestehende Intermediäre (SAFE-Instanzen), Verzeichnisse (BRAV, Find A Lawyer), Zertifikatsdienste und Trustcenter)
- Dynamik des Umfeldes
 - Viele zukünftige Anforderungen (Fachlichkeit, Ausbau) werden schon jetzt gestellt und müssen durch das Projektteam bewertet und geplant werden

5. Fazit

Das Projekt beA war und ist durch den hohen Qualitätsmaßstab und die besonderen Rahmenbedingungen gekennzeichnet. Das beA ist ein wichtiger Teilbeitrag zur Erfüllung des gesetzlichen Ziels und im Hinblick auf die zeitgemäße Realisierung des ERV.