eBroschüre

Dr. Wolfram Viefhues (Hrsg.)

Elektronischer Rechtsverkehr

Neuer Fahrplan für Wiederinbetriebnahme des beA

www.juris.de

juris®

eBroschüre

Elektronischer Rechtsverkehr

Neuer Fahrplan für Wiederinbetriebnahme des beA

Hrsg. von
Aufsicht führender Richter am Amtsgericht Oberhausen a. D.
Dr. Wolfram Viefhues
Gelsenkirchen

Zitiervorschlag:
Viefhues, Elektronischer Rechtsverkehr Ausgabe 3/2018, Rn 1

juris® Das Rechtsportal

Neuer Fahrplan für Wiederinbetriebnahme des beA

Inhalt

A. Einleitung

Verfasser: Dr. Wolfram Viefhues

weitere Aufsicht führender Richter am Amtsgericht a.D., Gelsenkirchen

„Wie geht es weiter mit dem beA?“ ist die in der Anwaltschaft, aber auch der Justiz derzeit meist gestellte Frage. Und da gibt es positive Nachrichten, auch wenn es noch nicht gelungen ist, vollständig „die Kuh vom Eis“ zu bringen. Die Bundesrechtsanwaltskammer (BRAK) hat entschieden, das beA zum 3.9.2018 wieder freizuschalten. 1

Über die Details informiert Sie der Beitrag von RAin *Witte*. Frau *Cosack*, die unsere Leser bisher schon regelmäßig über die praktische Anwendung des beA informiert hat, fasst auch in dieser Ausgabe wieder in aller Kürze zusammen, was jetzt ganz konkret in den Anwaltskanzleien zu tun ist.

Nach dem von der BRAK eingeholten Gutachten der Fa. secunet zur Sicherheit des beA sind intensive Härtungsmaßnahmen für des System vorgesehen und teilweise bereits umgesetzt worden, um der Forderung nach einem hohen Sicherheitsstandard für die elektronisch übertragene anwaltliche Korrespondenz so weit wie möglich Rechnung zu tragen. Dennoch ist die Diskussion im Internet noch nicht beendet. Das Gutachten wurde intensiv analysiert und der vorgeschlagene Zeitplan bewertet:

https://www.lto.de/recht/juristen/b/bea-anwaltspostfach-gutachten-sicherheits-luecken-sicherheitskonzept-lueckenhaft-keine-ende-zu-ende-verschluesselung/

https://www.golem.de/news/bundesrechtsanwaltskammer-sicherheitsgutachten-zum-anwaltspostfach-enttaeuscht-1806–135104.html

Eine Stellungnahme von Richterseite befasst sich vor allem mit den Auswirkungen auf die Einführung der elektronischen Akte:

https://www.lto.de/recht/justiz/j/nrv-verdi-offener-brief-drosselung-geschwindigkeit-einfuehrung-elektronische-akte-justiz/

Auch Anwälte, die sich z.B. in Foren äußern, lassen in ihrer Kritik am beA nicht selten jede Sachlichkeit vermissen. Es werden ungehemmt Forderungen aufgestellt, deren technische Umsetzbarkeit und Finanzierung jedoch völlig außen vor gelassen. Denn wer zur Wahrung der anwaltlichen Verschwiegenheit absolute IT-Sicherheit fordert, müsste eigentlich auch deutlich machen, welche Folgen sich daraus für die alltägliche Arbeit ergeben.

So ist z.B. das heute heftig gescholtene HSM (Hardware Security Modul) anstelle einer „echten“ Ende-zu-Ende-Verschlüsselung in die Konzeption eingebaut worden, weil man nur auf diese Weise praktikabel erreichen konnte, dass auch ein – berechtigter – Vertreter eine verschlüsselte Nachricht empfangen kann. Bei der geforderten „echten“ Ende-zu-Ende-Verschlüsselung ist dies nicht möglich. Die Situation ist dann vergleichbar mit einem Anwalt, der zu seinem Briefkasten nur selbst Zugang hat (technisch realisierbar über ein Schloss mit Fingerabdruckscanner). Das wäre ein absolut sicheres System, das fremde Zugriffe zum Briefkasten ausschließt – allerdings auch die Kanzleiarbeit unmöglich macht, wenn der Anwalt abwesend ist. Dies vorausgesetzt, ist die „echte“ Ende-zu-Ende-Verschlüsselung die richtige Wahl. Die von Einzelnen geforderte absolute Sicherheit wird aber dann für die Alltagsarbeit der Mehrheit der Anwälte zur Qual. 2

Und noch ein weiterer Gesichtspunkt bleibt von den Sicherheits-Hardlinern unerwähnt: Die Entwicklung einer solchen absolut sicheren „echten“ Ende-zu-Ende-Verschlüsselung kostet Geld – eine auch nur annähernde Schätzung des Kostenaufwandes ersparen sich die Kritiker des beA allerdings. Dennoch ist in-

zwischen – so meldet es jedenfalls LTO – eine Klage vor dem Anwaltsgerichtshof Berlin eingereicht worden mit dem Ziel, die BRAK zu verpflichten, das beA mit einer solchen „echten" Ende-zu-Ende-Verschlüsselung auszustatten. Man mag gespannt sein auf die nähere Begründung und vor allem auf die behauptete Anspruchsgrundlage, der BRAK eine solche Verpflichtung aufzulegen – mit erheblichen Kostenfolgen für alle Anwälte!

3 In der heftig geführten Diskussion um die Details der Sicherheitsprobleme des beA, die nur noch von IT-Experten wirklich verstanden werden kann, ist allerdings ein Gesichtspunkt verwunderlich. Bei der Forderung nach einer absolut sicheren Ende-zu-Ende-Verschlüsselung wird die herkömmliche Form der Korrespondenz in keiner Weise in die Überlegungen einbezogen, sondern stillschweigend als selbstverständlich und sicher eingestuft. Aber wie sicher ist der Briefumschlag, in den die – unverschlüsselte – anwaltliche Korrespondenz eingelegt wird? Wo bleibt da die Ende-zu-Ende-Verschlüsselung?

Das vielgescholtene HSM ist vergleichbar mit dem Tresorraum einer Bank. Man benutzt den Tresorraum, weil es sicherer ist, das Geld dort zu deponieren, als es in der Schalterhalle offen herumliegen zu lassen – vorausgesetzt natürlich, man vertraut seiner Bank, dass mit dem Tresorraum alles in Ordnung ist und die Tresorschlüssel sicher verwahrt werden. Der BRAK wird hier jedoch offen Misstrauen entgegengebracht; sie wird unverhohlen verdächtigt, Missbrauch treiben zu wollen.

Aber wie vertrauenswürdig ist eigentlich der unterbezahlte und überbelastete Briefzusteller, der den Transport des Briefes übernimmt? Wer garantiert, dass nicht der Inhalt der leicht zu öffnenden Briefumschläge mit Anwaltspost seine Aufmerksamkeit weckt? Wer gewährleistet, dass er nicht im Stress den Umschlag versehentlich in den Briefkasten des Nachbarn einwirft, der sich brennend für die Anwaltspost interessiert? Würde man bei der Briefpost aus Gründen der anwaltlichen Verschwiegenheit die gleichen hohen Anforderungen an den Tag legen wie beim beA, dürfte anwaltliche Korrespondenz auf diesem Wege nicht mehr zugelassen werden. Dann dürfte Anwaltspost nur noch in zugeschweißten Blechbehältern von eigens dazu angestellten vertrauenswürdigen Boten direkt vom Absender zum Empfänger getragen werden. Es wird sich niemand trauen, eine solche Anforderung an die anwaltliche Briefpost ernsthaft zu stellen. Das gilt im Übrigen auch für Telefonate über normale, unverschlüsselte Wege und das Fax, das völlig offen über die Leitungen transportiert wird und bei einem schlichten Zahlendreher in der Faxnummer schon mal bei einem falschen Empfänger ankommen kann. Und von der gerne benutzten unverschlüsselten E-Mail gar nicht zu reden. Es wäre also gut, auch bei der Diskussion über das beA das richtige Augenmaß zu wahren.

4 Die Angst vor einer zu kurzen Übergangsfrist wird sich letztlich ebenfalls als unbegründet herausstellen. Ganz sicher wird nach der Eröffnung des beA noch keine große Welle an elektronischer Korrespondenz von den Gerichten auf die Anwaltskanzleien zurollen. Zustellungen über das beA sind ohnehin nur dann rechtswirksam, wenn der Anwalt das elektronische Empfangsbekenntnis zurückschickt. Daher kann man der passiven Nutzungspflicht eigentlich mit Gelassenheit entgegensehen. Und derzeit besteht noch keine gesetzliche Pflicht zur aktiven Nutzung des beA.

5 Diese Ausgabe unserer eBroschüre ERV widmet sich nicht nur dem beA, sondern behandelt auch weitere Themen, die für den elektronischen Rechtsverkehr von praktischer Bedeutung sind: *Isabelle Biallaß*, Richterin am Amtsgericht Essen und IT-Dezernentin des Gerichts, stellt die Containersignatur vor und geht dabei auch auf kontroverse Entscheidungen des Bundessozialgerichtes und des OLG Brandenburg über deren Zulässigkeit ein. Der Anwaltschaft kann nur geraten werden, aus Gründen der anwaltlichen Vorsicht auf die nach der ERVV verbotene Containersignatur zu verzichten. *Christopher Brosch* macht in seinem Beitrag deutlich, dass elektronischer Rechtsverkehr nicht nur zwischen beA und Gerichten stattfindet. Mit dieser Ausgabe der e-Broschüre ERV bringen wir Sie wieder auf den aktuellen Stand der Entwicklung des elektronischen Rechtsverkehrs!

B. Neues zum beA

Verfasserin: Jennifer Witte
Rechtsanwältin, Berlin

Das beA geht wieder online – dies hat die Hauptversammlung der Bundesrechtsanwaltskammer (BRAK) mehrheitlich in einer außerordentlichen Präsidentenkonferenz am 27.6.2018 beschlossen.[1] Die Wiederinbetriebnahme erfolgt in zwei Schritten: Am 3.9.2018 wird das beA-System insgesamt freigeschaltet. Bereits zwei Monate zuvor, ab dem 4.7.2018, steht die Client Security zum Download und zur Installation bereit; auch eine Erstregistrierung ist dann schon möglich. 6

Demzufolge wird ab dem 3.9.2018 die passive Nutzungspflicht nach § 31a Abs. 6 BRAO auch wieder Wirkung entfalten.

I. Was war passiert?

Die BRAK hatte das beA Ende Dezember 2017 vom Netz genommen, nachdem sie auf einen Schwachpunkt beim Sicherheitszertifikat der beA-Client Security hingewiesen worden war. Deshalb beauftragte sie die secunet Security Networks AG, das beA zu begutachten. Nicht nur die beA-Client Security sollte auf ihre IT-Sicherheit hin analysiert werden, sondern auch die Gesamtlösung des beA-Systems einschließlich der Überprüfung des Hardware Security Moduls – HSM (siehe hierzu zuletzt eBroschüre ERV 2/2018, Rn 6). Die secunet AG legte sodann Mitte April 2018 ein Zwischenergebnis zu den zu diesem Zeitpunkt noch laufenden Sicherheitsüberprüfungen des beA-Systems vor. Bereits nach diesem vorläufigen Stand der Analyse wies das beA-System in seiner Grundstruktur keine grundlegenden Fehler auf (siehe hierzu eBroschüre ERV 2/2018, Rn 8). 7

Das nunmehr von der secunet AG vorgelegte Abschlussgutachten zur technischen Analyse und Konzeptprüfung des beA vom 18.6.2018 bestätigt abschließend das beA als geeignetes System zur vertraulichen Kommunikation im elektronischen Rechtsverkehr.[2] 8

Auf Grundlage dieses Abschlussgutachtens beschloss das Präsidium der BRAK nach ausführlicher Erörterung, den Präsidentinnen und Präsidenten der regionalen Rechtsanwaltskammern die gestufte Wiederinbetriebnahme des beA zu empfehlen. Dies unter der Bedingung, dass die in dem Gutachten dargestellten Schwachstellen bis zum Zeitpunkt der Wiederinbetriebnahme entsprechend der Empfehlung der secunet AG beseitigt werden. Dieser Vorschlag wurde der Hauptversammlung mit Präsidentenschreiben vom 20.6.2018 unterbreitet; verbunden mit einer Einladung zu einer außerordentlichen Präsidentenkonferenz am 27.6.2018, um den Fahrplan zur Wiederinbetriebnahme zu beraten und zu beschließen.[3] Das Abschlussgutachten der secunet AG hat die BRAK – wie angekündigt – veröffentlicht.[4]

In ihrer außerordentlichen Präsidentenkonferenz am 27.6.2018 führte die Hauptversammlung eine intensive Debatte über die von der secunet AG in ihrem Abschlussgutachten dargelegten Ergebnisse der Sicherheitsüberprüfung des beA-Systems; ebenso über die auf dieser Basis vorzunehmende Risikoanalyse sowie über den vorgeschlagenen Fahrplan zur Wiederinbetriebnahme des beA. Auch zwei Vertreter der secunet AG hatten an dieser Sitzung teilgenommen, um der Hauptversammlung zu den im Abschlussgut- 9

1 BRAK-Presseerklärung Nr. 19 v. 27.6.2018.
2 BRAK-Presseerklärung Nr. 18 v. 20.6.2018.
3 Anlage 2 zu BRAK-Presseerklärung Nr. 18 v. 20.6.2018.
4 Anlage 1 zu BRAK-Presseerklärung Nr. 18 v. 20.6.2018 = Abschlussgutachten der secunet AG v. 18.6.2018.

achten beschriebenen Schwachstellen Rede und Antwort zu stehen.[5] Sodann beschlossen die Präsidentinnen und Präsidenten insbesondere die Wiederinbetriebnahme des beA in zwei Stufen.[6]

II. Aufbau und Inhalt des Abschlussgutachtens der secunet AG

Die Begutachtung des beA durch die secunet AG erfolgte im Zeitraum von Februar bis Ende Mai 2018.[7] Um sowohl bereits bekannte technische, organisatorische und konzeptionelle Schwachstellen beurteilen und etwaige weitere vorhandene Schwachstellen feststellen zu können, führte die secunet AG im Rahmen ihrer Analyse diverse Prüfungen durch: Penetrationstests ausgewählter beA-Komponenten und Schnittstellen,[8] Quelltextanalysen[9] und eine konzeptionelle Analyse[10] standen auf dem Prüfungsprogramm.[11] Die aufgedeckten Schwachstellen wurden in den Kategorien „betriebs*ver*hindernd" (Kategorie A), „betriebs*be*hindernd" (Kategorie B) und „sonstige" (Kategorie C) eingestuft. Letztere haben ggf. nur unerhebliche Auswirkungen auf den Betrieb. **10**

Im Ergebnis ist – wie bereits ausgeführt – die secunet AG der Auffassung, dass das beA grundsätzlich ein geeignetes System zur vertraulichen Kommunikation im elektronischen Rechtsverkehr ist. Das Verschlüsselungskonzept biete technisch gesehen einen hinreichenden Schutz für die Vertraulichkeit der vom beA übermittelten Nachrichten. Nicht tragbare Risiken, die noch bestehen, könnten beseitigt werden bzw. seien teilweise bereits beseitigt worden.[12] Im Einzelnen: **11**

- Die Penetrationstests deckten 4 betriebsverhindernde und 13 betriebsbehindernde Schwachstellen auf – wovon bereits 2 bzw. 4 durch die Dienstleisterin der BRAK, die Atos SE, beseitigt wurden und dies auch von der secunet AG im Rahmen eines erneuten Tests (ReTest) bestätigt werden konnte. Die festgestellte betriebsverhindernde Schwachstelle der veralteten Softwareelemente in der beA-Client Security[13] wurde jedoch noch nicht behoben, ebenso wenig die der Modifikation von signierten XML-Nachrichten.[14]
- Der Quelltextanalyse wurden die beA-Anwendung, die beA-Client Security und die BRAV-Search unterzogen. Dabei wurden 6 Schwachstellen als betriebsverhindernd und 4 als betriebsbehindernd klassifiziert. Allerdings konnten alle hierdurch aufgedeckten betriebsverhindernden Schwachstellen bereits durch Atos behoben werden. Auch der ReTest verlief erfolgreich.
- Die konzeptionelle Analyse umfasste die wesentlichen Sicherheitsfunktionen des beA, die dem Schutz von Vertraulichkeit und Authentizität der über das beA-System verschickten Nachrichten dient. Hierbei stand das Verschlüsselungsverfahren beim beA in dem speziellen Hardware Security Modul (HSM) auf dem Prüfstand. Im Rahmen dessen wurden 2 betriebsverhindernde und 3 betriebsbehindernde Schwachstellen identifiziert. Bei den noch bestehenden betriebsverhindernden Schwachstellen handelt es sich um die Verwendung von Javascript bei der beA-Client Security[15] sowie die fehlende Prüfung der Postfachzertifikate durch die beA-Client Security.[16]

5 BeA-Newsletter 10/2018 v. 28.6.2018.
6 BRAK-Pressemitteilung Nr. 19 v. 27.6.2018.
7 Abschlussgutachten der secunet AG, S. 8.
8 A.a.O., S. 24 ff.
9 A.a.O., S. 53 ff.
10 A.a.O., S. 72 ff.
11 A.a.O., S. 8.
12 A.a.O., S. 13.
13 A.a.O., Kap. 3.5.4, S. 36.
14 A.a.O., Kap. 3.5.3, S. 35.
15 A.a.O., Kap. 5.4.1, S. 80.
16 A.a.O., Kap. 5.4.2, S. 81.

■ Exkurs: Hardware Security Modul (HSM) 12

Um die Arbeitsteilung zwischen Rechtsanwältinnen und Rechtsanwälten und ihren Mitarbeiter/innen in Kanzleien nach § 31a Abs. 3 S. 3 BRAO abzubilden, wählte die BRAK die Lösung über das Hardware Security Modul (HSM).[17] Aber auch um Vertretern, Abwicklern und Zustellungsbevollmächtigten die Nutzung des beA nach § 31a Abs. 3 S. 2 BRAO zu ermöglichen. Die sog. Umschlüsselung in einem HSM ist als technischer Zwischenschritt notwendig, um den digitalen Schlüssel der Nachricht mit dem Schlüssel des berechtigten Nutzers – bspw. dem Schlüssel der Mitarbeiterin, der Zugriffsrechte vom Postfachinhaber auf dessen beA eingeräumt wurden – neu zu verschlüsseln. Der Nachrichteninhalt selbst bleibt durchgehend verschlüsselt (siehe hierzu auch *Brosch*, eBroschüre ERV 1/2018, Rn 10 f.).

Vor diesem Hintergrund spricht sich die secunet AG in ihrem Abschlussgutachten aus sicherheitstechnischer Sicht für die erneute Inbetriebnahme aus. Voraussetzung dieser Empfehlung sei allerdings, dass die noch nicht behobenen betriebsverhindernden Schwachstellen vor Wiederinbetriebnahme des beA vollständig beseitigt werden. Darüber hinaus empfiehlt die secunet AG, die als betriebsbehindernd eingestuften Schwachstellen baldmöglichst zu beheben.[18] 13

III. Was hat die Hauptversammlung der BRAK nun konkret entschieden?

Anknüpfend an diese Empfehlung fasste die Hauptversammlung am 27.5.2018 den Beschluss,[19] die beA-Client Security ab dem 4.7.2017 zum Download und zur Installation bereitzustellen. Dies allerdings nur unter der Bedingung, dass die Beseitigung der derzeit noch offenen betriebsverhindernden Schwachstellen,[20] soweit sie die Client Security betreffen, bis dahin von der secunet AG bestätigt sein wird. Insofern hat die secunet AG am 3.7.2018 grünes Licht gegeben, sodass die beA-Client Security planmäßig seit dem 4.7.2018 allen Rechtsanwältinnen und Rechtsanwälten zur Neuinstallation zur Verfügung steht.[21] Ferner soll nach dem Beschluss der Hauptversammlung die Freischaltung des beA-Systems nur dann am 3.9.2018 erfolgen, wenn die secunet AG bis zu diesem Zeitpunkt die Beseitigung von weiteren bislang noch nicht behobenen betriebsverhindernden[22] und -behindernden[23] Schwachstellen bestätigt hat. Zudem sollen weitere Schwachstellen der Kategorie B im laufenden Betrieb beseitigt werden. 14

Hinsichtlich der noch bestehenden betriebsverhindernden Schwachstellen, welche das HSM betreffen,[24] kam die Hauptversammlung überein, diese im laufenden Betrieb, voraussichtlich in den ersten Monaten des Jahres 2019, durch technische Maßnahmen zu beseitigen. Schließlich soll das Betriebs- und Sicherheitskonzept optimiert werden. Diese Arbeiten sollen laut Beschluss spätestens in den ersten Monaten des Jahres 2019 abgeschlossen und von der secunet AG bestätigt werden. Eine dahingehende Empfehlung hatte die secunet AG in ihrem Abschlussgutachten für den nachhaltigen und sicheren Betrieb des beA ausgesprochen.[25] 15

Im Übrigen wird sich die BRAK gegenüber dem BMJV und den Justizministerien der Länder für die Einführung einer mindestens 4-wöchigen Testphase nach Wiederinbetriebnahme des beA einsetzen. Hintergrund ist, dass von Teilen der Anwaltschaft eine solche Übergangs- bzw. Testphase gefordert worden ist, um den reibungslosen Ablauf bei der Implementierung des beA in die bestehende Kanzlei- bzw. Unter- 16

17 *Dr. Nitschke*, BRAK-Magazin 3/2018, S. 11.
18 Abschlussgutachten der secunet AG, S. 13.
19 BRAK-Pressemitteilung Nr. 19 v. 27.6.2018.
20 Abschlussgutachten der secunet AG, Kap. 3.5.4 und 5.4.1.
21 BRAK-Pressemitteilung Nr. 20 v. 3.7.2018.
22 A.a.O., Kap. 3.5.3, 5.4.1 (soweit der Nachrichtenversand betroffen ist) und 5.4.2.
23 A.a.O., Kap. 3.6.1, 3.6.2, 3.6.3, 3.6.7, 3.6.9, 3.6.10, 3.6.12, 3.6.13, 4.5.1, 4.5.2 und 4.5.3.
24 A.a.O., Kap. 5.5.1 und 5.5.3.
25 A.a.O., Kap. 5.7, S. 89 ff.

nehmensstruktur gewährleisten zu können. Hierzu wäre es notwendig, die passive Nutzungspflicht gemäß § 31a Abs. 6 BRAO für diesen Zeitraum auszusetzen.

IV. Was ist nun zu tun?

Am 4.7.2018 ist nicht nur die neue Client Security von der BRAK zum Download und zur Installation bereitgestellt worden. Auch die Erstregistrierung ist den Rechtsanwältinnen und Rechtsanwälten, die dies bislang noch nicht getan haben, schon jetzt möglich.[26] 17

Daher empfiehlt es sich vordergründig[27] – sofern noch nicht geschehen – die beA-Karte zu beantragen, die notwendig ist, um die Erstregistrierung durchzuführen. Gleiches gilt für ein ebenso notwendiges Kartenlesegerät. Beides kann über das Portal der Zertifizierungsstelle der BNotK[28] bestellt werden (siehe hierzu auch eBroschüre ERV 2/2018, Rn 9 f.).

Hinweis: Jennifer Witte ist Rechtsanwältin in Berlin und als Referentin bei der Bundesrechtsanwaltskammer im Bereich des elektronischen Rechtsverkehrs tätig. Der Beitrag gibt ausschließlich ihre persönliche Auffassung wieder.

C. Startklar für das beA zum 3.9.2018?

Verfasserin: Ilona Cosack

Fachbuchautorin und Inhaberin der ABC AnwaltsBeratung Cosack, Fachberatung für Rechtsanwälte und Notare

Nach acht Monaten Zwangspause soll das beA am 3.9.2018 wieder online gehen. Laut Aussage von *Witte* (siehe oben Rn 6) soll die passive Nutzungspflicht nach § 31a Abs. 6 BRAO bereits ab diesem Zeitpunkt gelten. 18

> *Praxistipp*
>
> Klären Sie noch vor der Urlaubszeit in der Kanzlei, ob alle Komponenten für die Nutzung des Postfachs vorhanden sind oder ob Handlungsbedarf besteht!

Prüfen Sie mit der folgenden Checkliste, ob Sie bereit für die Wiederinbetriebnahme sind: 19

☐ **Haben Sie Ihre beA-Karte (Basiskarte oder Signaturkarte) vorliegen?**

Zum 1.1.2018 waren 165.854 Mitglieder bei der BRAK registriert. Knapp 17.000 Mitglieder haben bislang keine Karte bestellt.

☐ **Haben Sie beA-Mitarbeiterkarten und Softwarezertifikate bestellt?**

Bislang sind lediglich ca. 36.000 Mitarbeiterkarten und Softwarezertifikate bestellt worden. Nach § 26 Abs. 1 RAVPV darf der Inhaber eines für ihn erzeugten Zertifikats (= beA-Karte) dieses keiner weiteren Person (z.B. Mitarbeiter) überlassen und hat die PIN geheim zu halten (ausführlich dazu *Jungbauer*, eBroschüre ERV 2/2017, Rn 11 ff.).

26 BeA-Newsletter 11/2018 v. 4.7.2018.
27 Http://bea.brak.de/was-muss-man-jetzt-tun/
28 Https://bea.bnotk.de/

Bestellungen von allen beA-Karten sind ausschließlich über das Portal der BNotK[29] möglich.

☐ **Haben Sie ein geeignetes Kartenlesegerät?**

Sie benötigen mindestens ein Kartenlesegerät der Gruppe 3[30] für die Registrierung am Postfach.

☐ **Haben Sie sich erstmalig am Postfach angemeldet?**

Seit dem 4.7.2018 ist die Erstregistrierung für Nutzer, die im beA bislang noch nicht registriert sind, möglich. Dies sind noch etwa 70.000 Anwälte.

Hinweis

Inbetriebnahme und Anmeldung finden Sie ausführlich beschrieben in: *Cosack*, eBroschüre ERV 3/2016, Rn 21 ff.

☐ **Laden der neuen Client Security ab 4.7.2018 möglich**

Die neue Client Security steht seit 4.7.2018 auf der Seite http://www.bea.brak.de/ zum Download bereit. Scrollen Sie ganz nach unten und klicken Sie auf Ihr Betriebssystem. Der Download startet automatisch.

☐ **Zugriff auf das Postfach ab 3.9.2018**

Am Montag, 3.9.2018 soll das beA wieder für die Nutzer erreichbar sein. Die BRAK setzt sich für eine 4-wöchige Testphase[31] ein, bevor die passive Nutzungspflicht wieder greifen soll.

☐ **Registrierung der Mitarbeiter**

Eine Arbeitsteilung kann nur dann sinnvoll funktionieren, wenn die Mitarbeiter Zugriff auf Ihr beA haben. Dazu muss sich jeder Mitarbeiter einmalig (nach der Registrierung des Anwalts) registrieren (ausführlich dazu *Cosack*, eBroschüre ERV 3/2016, Rn 24 ff.).

☐ **Rechtevergabe für Mitarbeiter und Vertreter**

Damit Ihr beA auch bei Abwesenheiten überwacht werden kann, vergeben Sie für Mitarbeiter und Vertreter Rechte in der Benutzerverwaltung (ausführlich dazu *Cosack*, eBroschüre ERV 1/2017, Rn 17 ff.). Das Recht Nr. 02: Nachrichtenübersicht exportieren/drucken wurde zwischenzeitlich entfernt.

☐ **beA passiv nutzen**

Auch wenn Sie vorerst nur Ihrer passiven Nutzungspflicht nachkommen wollen, sind Sie verpflichtet, eingehende Empfangsbekenntnisse elektronisch zurückzusenden (vgl. *Cosack*, eBroschüre ERV 2/2017, Rn 27).

D. Elektronischer Rechtsverkehr: nicht nur zwischen beA und Gerichten

Verfasser: Christopher Brosch, Berlin

I. Einleitung

Das beA ist weiterhin offline, auch wenn die BRAK mittlerweile eine Wiederinbetriebnahme ab dem 3.9.2018 beschlossen hat (vgl. oben Rn 6). Elektronischer Rechtsverkehr ist jedoch auch ohne das beA möglich, und der ERV entwickelt sich auch außerhalb des beA weiter. Dieser Beitrag wirft einen kurzen **20**

29 Https://bea.bnotk.de/bestellung/#/products.

30 Https://www.bea-brak.de/xwiki/bin/view/BRAK/%2300014.

31 Https://www.brak.de/fuer-journalisten/pressemitteilungen-archiv/2018/presseerklaerung-19–2018/

Blick auf einige der Entwicklungen der Infrastruktur des ERV außerhalb des von der BRAK aufgrund von § 31a BRAO entwickelten Postfachs.

II. Kommunikation mit Behörden

Während Rechtsanwältinnen und Rechtsanwälte derzeit auf ihr besonderes Postfach verzichten müssen, entwickelt sich der ERV gleichwohl weiter. Im Anwendungsbereich der wichtigsten Verfahrensordnungen sind Gerichte seit dem Jahreswechsel grundsätzlich über die in § 130a Abs. 4 ZPO[32] und vergleichbaren Vorschriften vorgesehen Wege, d.h. per De-Mail und über die EGVP-Infrastruktur erreichbar. Für Nutzer des beA besteht die Möglichkeit, vorübergehend auf De-Mail oder den EGVP-Bürgerclient auszuweichen und so mit Gerichten zu kommunizieren. Hier ist lediglich zu beachten, dass ein Verzicht auf die qualifizierte elektronische Signatur (qeS) bei De-Mail nur bei Beachtung der Voraussetzungen des § 130a Abs. 4 Nr. 1 ZPO möglich ist bzw. dass ein Versand über den EGVP-Bürgerclient keinen „sicheren Übermittlungsweg" i.S.v. § 130a Abs. 3 Alt. 2 ZPO darstellt und eine qeS hier stets erforderlich ist. Zudem kann die Signaturfunktion des EGVP-Bürgerclients nur die mittlerweile nach der ERVV unzulässige Container-Signatur erzeugen (vgl. hierzu unten Rn 28 ff.), eine qeS muss ggf. mit externer Software angebracht werden.[33] 21

ERV im weiteren Sinne findet jedoch nicht nur mit Gerichten statt, sondern in vielen Fällen auch mit Behörden. Hier hilft es, dass aufgrund aktueller gesetzlicher Änderungen auch immer mehr Behörden elektronisch per EGVP erreichbar sind. § 174 Abs. 3 S. 4 ZPO sieht seit dem 1.1.2018[34] vor, dass die „in Absatz 1 Genannten" einen sicheren Übermittlungsweg für elektronische Zustellungen eröffnen müssen. Namentlich genannt werden in § 174 Abs. 1 ZPO Rechtsanwälte, Notare, Gerichtsvollzieher, Steuerberater, Behörden, Körperschaften und Anstalten des öffentlichen Rechts. Die sich aus § 174 Abs. 3 S. 4 ZPO ergebende Pflicht würde zwar von Behörden bereits durch die Einrichtung eines De-Mail-Postfachs erfüllt, das die meisten Behörden aufgrund der E-Government-Gesetze ohnehin einrichten müssen.[35] Jedoch ergibt sich aus einer weiteren zum 1.1.2018 in Kraft getretenen Gesetzesänderung, dass zahlreiche Behörden in weiterem Umfang elektronisch erreichbar sein müssen: 22

Aufgrund des Gesetzes zur Einführung der elektronischen Akte in der Justiz[36] und der Verweisung in § 110c S. 1 OWiG müssen Bußgeldbehörden über sämtliche in § 32a Abs. 4 StPO genannte Übermittlungswege erreichbar sein. Neben insbesondere den Staatsanwaltschaften sind daher zahlreiche weitere Behörden verpflichtet, auch über die EGVP-Infrastruktur erreichbar zu sein. Dabei ist zu berücksichtigen, dass in vielen von Verwaltungsbehörden ausgeführten Gesetzen auch Bußgeldvorschriften enthalten sind. 23

Das Gesetz zur Einführung der elektronischen Akte in der Justiz sieht jedoch die Möglichkeit vor, Opt-out-Regelungen zu erlassen. Bund und Länder können das Inkrafttreten der neuen Regelungen zum ERV durch Rechtsverordnung bis zum 1.1.2020 verschieben. Folge der Nutzung dieser Opt-out-Möglichkeit ist, dass die vorherige Rechtslage weiterhin gilt; für die Eröffnung des ERV in Bußgeldsachen ist dann der Erlass einer Rechtsverordnung gemäß § 110a Abs. 2 StPO a.F. erforderlich. 24

32 Entsprechendes gilt für die Vorschriften anderer Verfahrensordnungen, die hier nicht gesondert aufgeführt werden.

33 Dazu *Brosch*, Nicht mehr im elektronischen Container zu Gericht, BSG zur Unzulässigkeit der Container-Signatur, LTO am 25.5.2018.

34 Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten v. 10.10.2013, BGBl S. 3786.

35 Z.B. § 2 Abs. 2 EGovG (Bund).

36 Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs v. 5.7.2017, BGBl I S. 2208.

Hinweis

Von der Opt-out-Möglichkeit haben der Bund im Geschäftsbereich mehrerer Bundesministerien sowie mehrere Länder für das Bußgeldverfahren, einzelne Bundesländer zudem für den Bereich des Strafverfahrens mit unterschiedlicher Dauer Gebrauch gemacht.[37]

III. Entwicklungen beim EGVP: Weiterbetrieb bis nach dem beA-Start

Einige wichtige Weichenstellungen hat die Justiz auf der 103. Sitzung der Bund-Länder-Kommission für IT in der Justiz im Mai 2018 getroffen:[38] Der EGVP-Bürgerclient, der von der Justiz kostenfrei zur Verfügung gestellt wird, soll noch bis einen Monat nach dem Datum der Wiederinbetriebnahme des beA genutzt werden können, d.h. voraussichtlich bis zum 3.10.2018, und danach nicht mehr für die Kommunikation zur Verfügung stehen. **25**

Zur Erinnerung: Der Beschluss bezieht sich nicht auf „das EGVP" insgesamt, sondern lediglich auf die von der Justiz angebotene Software. Wer nach dem Datum, das sich aus dem Beschluss ergibt, über EGVP am ERV teilnehmen will, muss lediglich eine andere Software als den EGVP-Bürgerclient verwenden.

EGVP wird unverändert eine wesentliche technische Basis des ERV sein. Sämtliche „besonderen" Postfächer nutzen die EGVP-Infrastruktur; ebenso ist es möglich, neben dem EGVP-Bürgerclient mit EGVP-Drittprodukten[39] am ERV teilzunehmen. Die besonderen Wirkungen eines Versands aus einem besonderen Postfach stehen allerdings in diesem Fall nicht zur Verfügung.

IV. Identifizierungsverfahren für das EGVP

Die Nutzung des ERV außerhalb der besonderen Postfächer betrifft ein weiterer Beschluss der BLK, nach dem ein Identifizierungsverfahren für das EGVP eingeführt werden soll. Wesentliche Eigenschaft von beA, beBPo, beN und den Postfächern von Gerichten ist, dass ein Postfach nur nach Durchführung eines Identifizierungsverfahrens angelegt wird. Ansonsten kann ein EGVP-Postfach von Bürgern hingegen bislang ohne weitere Voraussetzungen angelegt werden. Name, Vorname und sämtliche weitere Angaben werden nicht überprüft; ein solches Postfach erscheint unmittelbar im EGVP-Adressverzeichnis. Hierbei ist die Sichtbarkeit des Eintrags für Kommunikationspartner u.U. aufgrund des EGVP-Rollenkonzepts zwar eingeschränkt, so können etwa Postfächer der Rolle „egvp_buerger" einander nicht im Adressverzeichnis sehen.[40] Gesehen und angeschrieben werden (und umgekehrt auch Nachrichten an diese Empfänger versenden) können die so angelegten Postfächer jedoch insbesondere von Gerichten und – nach der Konfiguration vor der Abschaltung im Dezember 2017[41] – auch von Rechtsanwältinnen und Rechtsanwälten über das beA. **26**

Dieser Umstand war bereits in der Vergangenheit Gegenstand der Kritik u.a. des Deutschen Anwaltvereins;[42] auch im Zusammenhang mit der Diskussion der Sicherheit des beA in den letzten Monaten ist die Möglichkeit erörtert worden, ein Postfach eines falschen Gerichts anzulegen. Dem ließe sich zwar entgegenhalten, dass anhand der EGVP-Rolle („egvp_buerger") erkennbar wäre, dass es sich nicht um

37 Die BRAK hat unter http://bea.brak.de/wann-kommt-das-bea/achtung-opt-out/ ohne Anspruch auf Vollständigkeit eine Übersicht über erlassene Opt-out-Regelungen veröffentlicht.

38 Https://justiz.de/BLK/beschluesse/103.pdf.

39 Vgl. https://egvp.justiz.de/Drittprodukte/index.php

40 Vgl. hierzu das Dokument „SAFE – Die Rollen", abrufbar unter http://www.justiz.de.

41 Die BRAK plant, bei der Wiederinbetriebnahme des beA auf eine Anbindung der EGVP-Bürgerpostfächer zu verzichten; BRAK-Presseerklärung Nr. 18 v. 20.6.2018, Anlage 2 (Begleitschreiben).

42 U.a. DAV, Stellungnahme 38/2017, Mai 2017, S. 7 f.

ein echtes Gerichtspostfach handelte. Allerdings besaß die beA-Webanwendung in der letzten im Betrieb befindlichen Version keine Funktion zur Anzeige der EGVP-Rolle, und die entsprechende Funktion des EGVP-Bürgerclients dürfte vielen Anwendern unbekannt sein.[43]

Auf der 103. Sitzung der BLK wurde nun der Beschluss gefasst, ein Identifizierungsverfahren für das gesamte EGVP vorzusehen; am ERV sollen nach Ablauf einer Übergangsfrist nur noch authentifizierte Nutzer teilnehmen. Für die Inhaber der derzeitigen nicht authentifizierten EGVP-Postfächer sollen kurzfristig Möglichkeiten zur Authentifizierung geschaffen werden. Hierzu wird ein Konzept mit den technischen und organisatorischen Anforderungen erarbeitet. Ergebnis wird sein, dass das EGVP auch außerhalb des Bereichs der „besonderen" Postfächer künftig auf einem sicheren Verzeichnisdienst basieren wird – ein „sicherer Übermittlungsweg" i.S.v. § 130a Abs. 4 ZPO kann ein solches EGVP-Postfach jedoch nicht ohne Regelung durch Gesetz oder Rechtsverordnung werden. **27**

Hinweis: Christopher Brosch war bis Februar 2018 bei der Bundesrechtsanwaltskammer im Bereich des elektronischen Rechtsverkehrs tätig. Der Beitrag gibt seine persönliche Meinung wieder.

E. Die Verwendung von Container-Signaturen im ERV

Verfasser: Isabelle Désirée Biallaß

Richterin am Amtsgericht Essen und dort IT-Dezernentin

I. Hintergrund

1. Der elektronische Rechtsverkehr mit dem Gericht

Seit dem 1.1.2018 ist der elektronische Rechtsverkehr mit den Gerichten kraft Gesetzes eröffnet. Betroffen sind in der ordentlichen Gerichtsbarkeit sämtliche Rechtsgebiete mit Ausnahme der Grundbuchsachen, die – mit einer weiteren Ausnahme bezüglich der Beschwerden – noch ausgenommen sind. Seitdem dürfen gemäß § 130a Abs. 1 S. 1 ZPO bzw. § 14 Abs. 2 S. 1 FamFG bestimmende und vorbereitende Schriftsätze der Parteien sowie darüber hinaus Auskünfte, Aussagen, Gutachten und alle sonstigen Erklärungen am Verfahren beteiligter Dritter sowie über die Verweisungsnormen in §§ 253 Abs. 4, 519 Abs. 5, 520 Abs. 5, 549 Abs. 2, 551 Abs. 4 ZPO auch bestimmende Schriftsätze (Klage, Berufungs- und Revisionsschrift sowie -begründung) elektronisch eingereicht werden. **28**

Gemäß § 32a Abs. 1 S. 1 StPO dürfen auch bei den Strafverfolgungsbehörden und Strafgerichten elektronische Dokumente eingereicht werden. In § 110c OWiG findet sich ein Verweis auf die Regelungen zum elektronischen Rechtsverkehr in der StPO.

> *Hinweis* **29**
>
> Spätestens ab dem 1.1.2022 müssen Rechtsanwälte gemäß § 130d ZPO bzw. § 32d StPO Eingänge elektronisch einreichen. Durch Landesverordnung kann in Zivilprozesssachen das Inkrafttreten auf den 1.1.2020 oder den 1.1.2021 vorverlegt werden.

Trotz der Verzögerungen bei der Freischaltung des besonderen Anwaltspostfachs (beA) ist es somit höchste Zeit für die Anwaltschaft, sich mit der Frage auseinanderzusetzen, welche technischen Voraussetzungen bei der Einreichung von elektronischen Dokumenten erfüllt werden müssen. Der vorliegende Artikel setzt sich mit der weiteren Verwendung der Container-Signatur auseinander.

43 Vgl. dazu auch BRAK-Presseerklärung Nr. 18 v. 20.6.2018, Anlage 1 (Gutachten), Kap. 5.5.2.

2. Die Container-Signatur

Bei der Container-Signatur handelt es sich um eine **qualifizierte elektronische Signatur**. Nach der eIDAS-VO liegt eine „qualifizierte elektronische Signatur" vor, wenn 30

- sie eindeutig dem Unterzeichner zugeordnet ist,
- dessen Identifizierung ermöglicht,
- unter Verwendung einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann,
- auf einem qualifizierten Zertifikat für elektronische Signaturen beruht und
- mit den auf diese Weise unterzeichneten Daten so verbunden ist, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

> *Hinweis*
>
> Eine qualifizierte elektronische Signatur hat gemäß Art. 25 Abs. 2 eIDAS-VO die **gleiche Rechtswirkung** wie eine **handschriftliche Unterschrift**. Sie ersetzt damit sowohl die prozessuale als auch die materiell-rechtliche Schriftform.

Bei einer **Container-Signatur** bezieht sich die qualifizierte elektronische Signatur nicht auf ein einzelnes elektronisches Dokument, sondern auf einen **elektronischen Container**, der **mehrere elektronische Dokumente enthält**. Bei dem elektronischen Container handelt es sich um einen Dateiordner, z.B. im ZIP-Format oder in Form einer EGVP-Nachricht. Zur Prüfung der Signatur muss daher stets der gesamte Container unverändert verfügbar sein. 31

II. Die Bedeutung der elektronischen Signatur für den elektronischen Rechtsverkehr mit dem Gericht

1. Die Übersendung an das elektronische Gerichts- und Verwaltungspostfach

Im Falle einer elektronischen Einreichung stehen zwei Möglichkeiten zur Verfügung, um das verfahrensrechtliche Schriftformerfordernis einzuhalten: Zum einen kann das Dokument gemäß § 130a Abs. 3 Hs. 1 ZPO mit **einer qualifizierten elektronischen Signatur** der den Inhalt des Dokuments verantwortenden Person versehen werden. 32

> *Hinweis*
>
> Eine Einreichung des mit einer qualifizierten elektronischen Signatur versehenen Dokuments per E-Mail wurde ausgeschlossen.

Gemäß § 4 Abs. 1 ERVV dürfen mit einer qualifizierten elektronischen Signatur versehene elektronische Dokumente nur über einen sicheren Übermittlungsweg oder **an das elektronische Gerichts- und Verwaltungspostfach (EGVP)** übermittelt werden.

2. Sicherer Übermittlungsweg

Zum anderen kann das lediglich mit dem Namen des Verfassers versehene („einfach signierte") elektronische Dokument gemäß § 130a Abs. 3 Hs. 2 ZPO bei der Justiz auf einem **sicheren Übermittlungsweg** i.S.v. § 130a Abs. 4 ZPO eingereicht werden. Sichere Übermittlungswege sind: 33

- der Postfach- und Versanddienst eines **De-Mail-Kontos,**

- das **besondere elektronische Anwaltspostfach (beA),**
- das **besondere elektronische Notarpostfach (beN),**
- das **besondere elektronische Behördenpostfach (beBPo)**.

Auch bei der Einreichung über einen sicheren Übermittlungsweg kann die qualifizierte elektronische Signatur Relevanz haben. Denn durch die Nutzung eines sicheren Übermittlungswegs wird lediglich die prozessuale, **nicht** aber die materiell-rechtliche Schriftform ersetzt. 34

Praxistipp

Wird ein Schriftsatz über einen sicheren Übermittlungsweg bei Gericht eingereicht, der eine Erklärung enthält, die **materiell-rechtlich** der **Schriftform** bedarf, muss dieses elektronische Dokument **qualifiziert elektronisch signiert** werden.

III. Die gesetzlichen Regelungen zur Container-Signatur

Gemäß § 130a Abs. 2 S. 1 ZPO (bzw. § 32a Abs. 2 S. 1 StPO) muss ein elektronisches Dokument für die **Bearbeitung** durch das Gericht **geeignet** sein. Ist ein elektronisches Dokument für das Gericht zur Bearbeitung nicht geeignet, weil der Absender ein nicht zugelassenes Dateiformat verwendet hat, so ist das Gericht **verpflichtet**, dies dem Absender gemäß § 130a Abs. 6 S. 1 ZPO bzw. § 32a Abs. 6 S. 1 StPO unter **Hinweis** auf die Unwirksamkeit des Eingangs und die geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen. **Das Dokument gilt als zum Zeitpunkt der früheren Einreichung eingegangen**, sofern der Absender es unverzüglich in einer für das Gericht zur Bearbeitung geeigneten Form nachreicht und glaubhaft macht, dass das neu eingereichte Dokument mit dem zuerst eingereichten Dokument inhaltlich übereinstimmt. Das Dokument kann folglich ohne negative Rechtsfolgen auf ein zugelassenes Dateiformat umgestellt werden, wenn auf den gerichtlichen Hinweis innerhalb einer angemessenen Frist reagiert wird. 35

In § 4 Abs. 2 ERVV wird geregelt: 36

> „Mehrere elektronische Dokumente dürfen **nicht** mit einer gemeinsamen qualifizierten elektronischen Signatur übermittelt werden."

In der Gesetzesbegründung wird hierzu ausgeführt, dass die Einschränkung geboten sei, weil andernfalls eine Überprüfung der Authentizität und Integrität der elektronischen Dokumente im weiteren Verfahren regelmäßig nicht mehr möglich wäre. Insbesondere könnten der Prozessgegner oder andere Verfahrensbeteiligte nicht mehr nachvollziehen, ob die Authentizität und Integrität der elektronischen Dokumente gewährleistet wäre. Unmöglich werde die nachträgliche Prüfung insbesondere bei Dokumenten, die mehrere Verfahren betreffen, wenn diese nach der (geplanten) verbindlichen Einführung der elektronischen Akte dort zu den jeweiligen Verfahren gespeichert werden, da aus datenschutzrechtlichen Gründen nur die das einzelne Verfahren betreffenden Dokumente zur Akte genommen werden dürften.

IV. Die aktuelle Rechtsprechung zur Verwendung einer Container-Signatur

1. OLG Brandenburg, Beschl. v. 6.3.2018 – 13 WF 45/18

Aktuell ist ungeklärt, inwiefern durch § 4 Abs. 2 ERVV die Verwendung einer Container-Signatur in der ordentlichen Gerichtsbarkeit tatsächlich ausgeschlossen ist. Das OLG Brandenburg vertrat in einem Beschl. v.6.3.2018 (NJW 2018, 1482 ff.) die Ansicht, dass **§ 4 Abs. 2 ERVV teleologisch reduziert** ausgelegt werden müsse, um nicht gegen das Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) zu verstoßen. Hintergrund dieser Überlegungen war, dass in der ordentlichen Gerichtsbarkeit die elektronische Akte nicht 37

zeitgleich mit der Eröffnung des elektronischen Rechtsverkehrs eingeführt wurde. Die elektronisch eingegangenen Schriftsätze werden in der Regel noch ausgedruckt und sodann zu der noch in Papierform geführten Akte genommen.

Das OLG nimmt an, dass es aus dem Gebot, effektiven Rechtsschutz zu gewährleisten, das sich auch an den Gesetzgeber richte, folge, dass Beschränkungen des Zugangs zu einer weiteren Instanz mit den Belangen einer rechtsstaatlichen Verfahrensordnung vereinbar sein müssten und den einzelnen Rechtsuchenden nicht unverhältnismäßig belasten dürften. Diese Grenze werde durch § 4 Abs. 2 ERVV nur eingehalten, wenn er einschränkend ausgelegt werde und die Zulässigkeit eines Rechtsmittels nicht scheitere, wenn die Container-Signatur die **Überprüfung der Authentizität und Integrität** der zur Einlegung des Rechtsmittels übermittelten elektronischen Dokumente zuließe. Eine solche sei **möglich**, weil die Akten nicht elektronisch geführt würden. Der Papierausdruck des elektronischen Eingangs bliebe bis zur Vernichtung der Papierakte verfügbar, sodass geprüft werden könne, was das Ergebnis der Signaturprüfung war, welche Dateien gemeinsam übersandt wurden und welchen Inhalt diese Dateien gehabt hatten. Es wäre ohne großen Mehraufwand möglich, das Ergebnis der Überprüfung der Container-Signatur zu allen Akten zu nehmen, wenn die zugleich übersandten elektronischen Dokumente mehrere Verfahren beträfen. Es bestehe keine Rechtfertigung, die gesteigerte Formstrenge schon zu gebieten, da ihr Zweck erst in Zukunft eventuell hinzutreten werde.

2. BSG, Beschl. v. 9.5.2018 – B 12 KR 26/18 B

Gegen diese Rechtsauffassung wandte sich das Bundessozialgericht mit Beschl. v. 9.5.2018.[44] Die Verwendung einer **Container-Signatur** sei **unzulässig** (§ 65a Abs. 2 S. 2, Abs. 3 SGG i.V.m. § 4 Abs. 2 ERVV). Das BSG vertritt, dass das Gericht unverzüglich auf die fehlerhafte Signatur **hinzuweisen** habe, damit der Einreicher den Mangel fristwahrend beheben könne. Unter Umständen sei ihm zur Gewährleistung effektiven Rechtsschutzes **Wiedereinsetzung in den vorigen Stand nach allgemeinen Regeln** zu gewähren. § 65a Abs. 6 SGG könne nicht angewendet werden, weil die container-signierten elektronischen Dokumente regelmäßig „zur Bearbeitung geeignet" wären. **38**

Hinweis

§ 65a Abs. 1–6 SGG entspricht § 130a Abs. 1–6 ZPO bzw. § 32a Abs. 1–6 StPO.

V. Fazit

Die Argumentation des Bundessozialgerichts zu der Unzulässigkeit der Verwendung einer Container-Signatur überzeugt. Der Unterzeichner autorisiert durch seine Unterschrift den davorstehenden Text als eigene rechtlich wirksame und verbindliche Erklärung. Diese Funktion wird nicht in dem gleichen Maße gewahrt, wenn mehrere in einem Ordner befindliche Dokumente durch die qualifizierte elektronische Signierung des Ordners als signiert gelten. Der Unterzeichner führt sich nicht noch einmal vor Augen, welches Dokument er gerade signiert und prüft nicht, ob er eine entsprechende Erklärung tatsächlich abgeben und gegen sich gelten lassen will. **39**

Zudem würde die Verwendung einer Container-Signatur das Gericht auch schon vor der Einführung der elektronischen Akte vor unlösbare Probleme stellen, wenn der eingegangene Schriftsatz elektronisch an die Gegenseite weitergeleitet werden soll und eines der Dokumente, die mit Hilfe einer Container-Signatur signiert wurden, nicht weitergeleitet werden darf (z.B. die Erklärung zu den persönlichen und wirt-

44 Zum Zeitpunkt der Abfassung dieses Artikels war nur die Pressemitteilung verfügbar.

schaftlichen Verhältnissen). Eine Trennung der Dokumente würde dazu führen, dass der Empfänger die Signatur nicht mehr prüfen kann, da die Integrität des signierten Dokuments nicht länger gewährt ist.

Nach hiesiger Einschätzung stellt das Verbot der Container-Signatur auch keinen Verstoß gegen das Rechtsstaatsprinzip dar. Die Einreichung von mehreren nicht unterzeichneten Schriftstücken in einem unterzeichneten Briefumschlag würde wohl unstreitig als nicht ausreichend angesehen. Die Container-Signatur lässt sich hiermit vergleichen. Ihr Verbot stellt somit keine unverhältnismäßige Belastung für den einzelnen Rechtsuchenden dar.

40 Schon aus anwaltlicher Vorsicht sollte keine Container-Signatur verwendet werden, da durchaus zu erwarten ist, dass die Argumentation des Bundessozialgerichts auch in der ordentlichen Gerichtsbarkeit Anhänger findet. Ob die Fiktion des Eingangs zum Zeitpunkt der früheren Einreichung gemäß § 130a Abs. 6 S. 1 ZPO bzw. § 32a Abs. 6 S. 1 StPO Anwendung findet, sofern der Absender das Dokument unverzüglich in einer für das Gericht zur Bearbeitung geeigneten Form nachreicht und glaubhaft macht, dass das neu eingereichte Dokument mit dem zuerst eingereichten Dokument inhaltlich übereinstimmt – wofür nach hiesiger Einschätzung vieles spricht – oder ob – wie das BSG für den gleichlautenden § 65a Abs. 6 SGG vertrat – dessen Anwendungsbereich nicht eröffnet ist, sodass lediglich ein Verweis auf die allgemeinen Wiedereinsetzungsregeln verbleibt, ist noch völlig offen.

Der Empfehlung von *Mardorf* „Finger weg von der Container-Signatur“[45] kann daher nur beigepflichtet werden.

45 *Mardorf*, jM 2018, 228, 230.