eBroschüre

Dr. Wolfram Viefhues (Hrsg.)

Elektronischer Rechtsverkehr

Rückschritte statt Fortschritte beim beA? – Sicherheitsfragen im Fokus

www.juris.de

juris®

eBroschüre

Elektronischer Rechtsverkehr

Rückschritte statt Fortschritte beim beA? – Sicherheitsfragen im Fokus

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

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

juris® Das Rechtsportal

Rückschritte statt Fortschritte beim beA? – Sicherheitsfragen im Fokus

Inhalt

	Rdn
A. Einleitung	1
B. Das beA ist offline – wie geht es weiter?	4
I. Abschaltung des beA im Dezember 2017	5
II. Folgen der Abschaltung des beA	9
III. Diskussion der technischen Architektur des beA	10
C. beA außer Betrieb – vom Dilemma bis zur Aussicht auf eine Lösung	14
I. Sicherheitsproblem: beA-Zertifikat	15
II. Wie kann die passive Nutzungspflicht erfüllt werden?	18
III. Welche Alternativen gibt es?	19
1. EGVP-Classic-Client	20
2. EGVP-Drittanwendungen	21
3. De-Mail	22
IV. Mahnverfahren	23
V. Schutzschriften	24
VI. Kanzleisoftware	25
VII. beA-Sicherheit auf dem Prüfstand	26
VIII. Alte beA-Client-Security	28
IX. Fazit	29
D. Infos aus Bund und Bundesländern	30
I. Bundesamt für Justiz stellt Online-Formular bereit	30
II. Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT)	31
III. Rechtliche Hürden der Verwaltungsdigitalisierung	32
IV. Ergebnisse der Herbstkonferenz 2017 der Justizminister	33
E. Ausgewählte Rechtsprechung zum ERV	34
I. Eingangsbestätigung per EGVP bei nicht mehr auffindbarer Klageschrift	34
II. Einlegung einer Beschwerde per EGVP ohne qualifizierte elektronische Signatur	35
III. Verweigerung der Mitbestimmung des Personalrates per E-Mail	36
IV. Keine sofortige Beschwerde per einfacher E-Mail	37
V. Erfolglose Rechtssatzverfassungsbeschwerde gegen Einführung des besonderen elektronischen Postfachs (beA)	38
VI. Form der Berichtigung einer notariellen Gesellschafterliste durch elektronisch beglaubigte Abschrift	39

A. Einleitung

Verfasser: Dr. Wolfram Viefhues

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

Die Probleme beim beA schlagen auch in der Diskussion unter Anwälten und Anwältinnen hohe Wellen. Wie konnte das passieren? Was muss repariert werden? Wie lange wird es dauern? Ist damit der elektronische Rechtsverkehr am Ende? Um die letzte Frage zuerst zu beantworten: Nein, der elektronische Rechtsverkehr ist keinesfalls am Ende. Das beA ist zwar ein – wichtiger – Baustein in der Gesamtkonstruktion und der zeitweise Ausfall des beA bereitet zweifellos Schwierigkeiten, das bedeutet aber nicht im Geringsten, dass die allgemeine und stetige Entwicklung des elektronischen Rechtsverkehrs hierdurch aufgehalten wird. 1

Grund für die Abschaltung des beA ist ein jetzt erst entdecktes Sicherheitsproblem, dessen Details für Außenstehende nur schwer verständlich sind. In den Beiträgen von *Brosch* und *Cosack* werden dazu nähere Einzelheiten mitgeteilt. Man wird sicherlich noch lebhaft der Frage nachgehen, warum man diesen Mangel nicht schon früher erkannt hat und wer ihn zu verantworten hat. Die Bundesrechtsanwaltskammer (BRAK) hat jedenfalls gut daran getan, wenn auch nach anfangs etwas chaotischen Informationen, das beA vorerst stillzulegen. Da die teilweise fehlerhaften Informationen und „Verschlimmbesserungen" über die Weihnachtstage erfolgt sind, an denen in den wenigsten Anwaltskanzleien gearbeitet wurde, dürften die praktischen Auswirkungen gering gewesen sein – also „Glück im Unglück".

Die BRAK hat die bisherigen Abläufe auch zum Anlass genommen, ihre Informationspolitik zu überdenken. Um den gemeldeten Sicherheitsproblemen beim beA auf die Spur zu kommen, hat die BRAK am 26.1.2018 den „Sicherheitsdialog beAthon" mit einem intensiven und konstruktiven Austausch über Sicherheitsfragen zum besonderen elektronischen Anwaltspostfach (beA) durchgeführt (Näheres hierzu siehe Rdn 6). Dort wurde die von der Firma Atos, die von der BRAK mit der Erstellung des beA beauftragt worden war, vorgestellte neue Version der beA Client Security diskutiert. Zusammengefasst (für technisch Interessierte): Durch Installation eines individuellen, lokalen Zertifikats auf dem Rechner des Nutzers wird eine prinzipiell als sicher eingestufte Lösung erreicht und die zuvor kritisierte Sicherheitslücke kann so geschlossen werden. Die BRAK ist jedoch gut beraten, diese Lösung durch den von ihr beauftragten Gutachter erst noch einer näheren Überprüfung unterziehen zu lassen, bevor das beA wieder freigeschaltet wird (hierzu sowie zu zwischenzeitlichen Aktivitäten des Deutschen Anwaltvereins (DAV) siehe unten Rdn 27).

Die Diskussion auch in den Anwaltskammern dreht sich nun um die Frage, ob der **Programmcode des beA öffentlich bekanntgegeben** werden soll. Einerseits wird argumentiert, dass dies den „guten Hackern" die Möglichkeit geben würde, noch vorhandene Schwachstellen zu finden und zu melden, damit diese rechtzeitig beseitigt werden können. Andererseits wird darauf verwiesen, dass damit auch die „bösen Hacker" eine gute Gelegenheit bekommen, ihrerseits Schwachstellen zu finden, die sie dann für kriminelle Ziele ausnutzen können. Hierbei spielen auch diffizile vertragliche Regelungen eine Rolle (z.B.: Wem „gehört" der Programmcode? Wer hat hieran Urheberrechtsschutz?). 2

Meine persönliche Einschätzung der Diskussion über dieses Thema, vor allem wie sie in verschiedenen Internetforen stattfindet, ist allerdings, dass nicht immer fair und mit Augenmaß argumentiert wird. Ich fürchte, dass einige der Kritiker, die lautstark und polemisch die Sicherheitslücken beim beA monieren, täglich Anwaltskorrespondenz per unverschlüsselter E-Mail oder per Fax übermitteln, obwohl in beiden Fällen das Dokument völlig offen und ohne jede Sicherung gegen unbefugte Zugriffe übertragen wird. Ab dem Tag der Geltung der Datenschutz-Grundverordnung – das ist der 25.5.2018 – kann dies empfindliche

Geldbußen nach sich ziehen (Einzelheiten unter https://www.datenschutzbeauftragter-info.de/aufsichtsbehoerde-aeussert-sich-zur-verschluesselungspflicht-von-anwaelten/). Auch bei den fast alle Computernutzer betreffenden kürzlich bekannt gewordenen Sicherheitslücken im Computerchip („Spectre“ und „Meltdown“) herrscht weitaus weniger Aufregung als beim beA. Dazu *Erbguth* in JurPC Web-Dok. 21/2018:

> *„Gravierende Sicherheitslücken treten leider in fast allen IT-Systemen auf. Zuletzt hielten uns Meltdown und Spectre in Atem, die praktisch alle Rechner unsicher gemacht haben. Entscheidend ist dabei, dass professionell auf diese Sicherheitslücken reagiert wird. Selbst große Firmen wie z.B. Intel passiert es da, dass sie durch beschönigende Kommunikation, fehlerhafte Patches oder unprofessionelles Sicherheitsmanagement den entstandenen Schaden unnötig vergrößern.“*

Völlig zu Unrecht sind im Zusammenhang mit der beA-Problematik im Übrigen auch Bedenken gegen die Sicherheit des EGVP und des diesem zugrunde liegenden OSCI-Standards geäußert worden. Nach einer Pressemeldung der Vitako – Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V. – ist kein Sicherheitsvorfall bekannt, der solche Rückschlüsse von den Problemen in der beA-Projektlösung auf bewährte Standardlösungen, Produkte und Infrastrukturkomponenten in eGoverment zulässt.

Um einer in der Anwaltschaft weit verbreiteten Befürchtung den Wind aus den Segeln zu nehmen: So- **3**
lange das beA nicht läuft, kann den Berufsträgern derzeit weder berufs- noch haftungsrechtlich angekreidet werden, dass sie trotz gesetzlicher Vorgaben den elektronischen Kanal nicht nutzen. Insoweit besteht Einigkeit.

Fazit ist:

- Das beA als solches steht nicht zu Diskussion. Man wird mit vereinten Kräften Wege finden, das derzeitige System mit notwendigen Verbesserungen schnell wieder ans Laufen zu bringen.
- Parallel dazu werden unter dem Stichwort „beA+“ Überlegungen angestellt, weiterführende Verbesserungen vorzunehmen. Denn für die Zukunft der digitalen Justiz ist es viel wichtiger, ob und wie die Architektur des Anwaltspostfachs fortentwickelt werden kann und soll. Zu diesem Thema veranstaltet der Deutsche EDV-Gerichtstag am 5.3.2018 in der Landesvertretung des Saarlandes ein Symposium (siehe https://www.edvgt.de).
- Der elektronische Rechtsverkehr wird weiter vorangetrieben. So hat inzwischen der Bundesrat der Änderung der ERVV zugestimmt. Aufgrund der Ermächtigung nach § 32a Abs. 2 S. 2, Abs. 4 Nr. 3 StPO wird durch eine Ergänzung der am 1.1.2018 in Kraft getretenen Elektronischer-Rechtsverkehr-Verordnung (ERVV) der Anwendungsbereich der ERVV auf das Strafverfahren – und damit zugleich auf den gerichtlichen Rechtsschutz in Strafvollzugssachen und das Ordnungswidrigkeitenverfahren – erweitert bzw. nach besonderer Maßgabe für anwendbar erklärt (BR-Drucks 4/18 v. 10.1.2018).
- „Legal tech“ ist in aller Munde – so nicht zuletzt beim Anwaltstag 2017. Auch hiermit wird sich der EDV-Gerichtstag in einem Symposium in Berlin am 14.3.2018 in der Landesvertretung des Saarlandes befassen (siehe https://www.edvgt.de/veranstaltung/8397/).

Zu den folgenden Beiträgen möchte ich zusammenfassend mit einer Formulierung des Vorsitzenden des Deutschen Anwaltsvereins *Schellenberg* aus der Deutschen Richterzeitung 2018, 61 überleiten:

> *„Die Einführung des elektronischen Rechtsverkehrs sollten wir trotz aller Herausforderungen als große Chance für die Anwaltschaft und Gerichte ansehen. Es ist nur ein erster Schritt für eine umfassende digitale Transformation in der Rechtspflege. Wir haben viel zu tun – packen wir es an.“*

B. Das beA ist offline – wie geht es weiter?

Verfasser: Christopher Brosch
Rechtsanwalt, Berlin

Das besondere elektronische Anwaltspostfach (beA) sollte nach den Plänen des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten und späterer Änderungen seit dem 1.1.2018 die Basis des elektronischen Rechtsverkehrs in Deutschland bilden. Nach einer Übergangsphase gemäß § 31 RAVPV sieht seit dem 1.1.2018 der neue § 31a Abs. 6 BRAO eine sog. passive Nutzungspflicht für alle Inhaber eines Postfachs vor; zudem sind grundsätzlich alle Gerichte für elektronische Eingänge erreichbar. Doch seit kurz vor Weihnachten 2017 ist das beA offline. Dieser Beitrag gibt einen Überblick über die Hintergründe und die Auswirkungen der Abschaltung des beA sowie die weiteren Entwicklungen. 4

I. Abschaltung des beA im Dezember 2017

Am 20.12.2017 informierte ein Mitglied des Chaos Computer Clubs, Herr *Markus Drenger*, die Bundesrechtsanwaltskammer (BRAK) über die Ergebnisse seiner Untersuchung der **beA Client Security**. Dabei handelt es sich um die lokal zu installierende Softwarekomponente, die für den Zugriff auf das beA erforderlich ist und von jedermann über die Startseite der beA-Webanwendung heruntergeladen werden kann. Herr *Drenger* konnte daher die Software dekompilieren, d.h. zurück in für Menschen lesbare Programmiersprache übersetzen, und den Quellcode untersuchen. In diesem Quellcode fand Herr *Drenger* insbesondere einen privaten Schlüssel. 5

Dieser Schlüssel kam in der beA Client Security zum Einsatz, um Verbindungen des Webbrowsers zu der beA Client Security zu verschlüsseln. Bei der Nutzung der beA-Webanwendung unter https://www.bea-brak.de/ unterhält der Webbrowser des Anwenders Verbindungen sowohl zu dem beA-Webserver als auch zu der auf dem eigenen Computer installierten Client Security, welche insbesondere Funktionen zur Nutzung der beA-Karte bereitstellt. Aus Sicherheitsgründen muss diese lokale, nicht über das Internet erfolgende Verbindung zu dem eigenen Computer nicht verschlüsselt werden – ein Angreifer, der Zugriff auf den Arbeitsplatz des Rechtsanwalts hat, könnte ohnehin sämtliche Dokumente einsehen.

Moderne Webbrowser blockieren jedoch den Zugriff auf Webseiten, die aus „mixed content" bestehen, d.h. aus verschlüsselt übertragenen und nicht verschlüsselt übertragenen Elementen.[1] Die Gründe, die bei Webseiten im Internet für die Blockierung von „mixed content" sprechen, gelten jedoch bei rein lokalen Verbindungen nicht. Gleichwohl würden Browser auch bei lokalen Verbindungen „mixed content" blockieren. Allein um dies zu verhindern, setzt die beA Client Security auch bei lokalen Verbindungen eine **verschlüsselte Übertragung (HTTPS)** ein – Teil der Verschlüsselung von Nachrichten ist dies nicht. 6

HTTPS sieht den Einsatz eines Schlüsselpaares aus einem öffentlichen und einem privaten Schlüssel vor. Der öffentliche Schlüssel befindet sich im Webbrowser des Anwenders, der private Schlüssel bei dem Gegenüber – in diesem Fall der Client Security. Private Schlüssel müssen jedoch geheim gehalten werden. Bei der beA Client Security konnte der private Schlüssel, wie von Herrn *Drenger* gezeigt, aus dem Quellcode extrahiert werden. Aufgrund des Hinweises von Herrn *Drenger* sperrte daher die zuständige

1 Vgl. u.a. https://support.mozilla.org/en-US/kb/mixed-content-blocking-firefox

Zertifizierungsstelle am 22.12.2017 das zu dem Schlüssel gehörende Zertifikat, was zur Folge hatte, dass dieses nicht mehr nutzbar war.[2]

Am 22.12.2017 stellte der Softwareentwickler der BRAK ein anderes Zertifikat zur Verfügung, das ersatzweise installiert werden und so die Nutzbarkeit des beA wiederherstellen sollte. Noch am selben Tag erhielt die BRAK von ihrem Dienstleister den Hinweis, dass dieses neue Zertifikat fehlerhaft sei und zu Sicherheitsproblemen führen könne. Es handelte sich um ein Zertifikat, das aufgrund einer falschen Konfiguration dazu eingesetzt werden kann, weitere Zertifikate für fremde Webseiten auszustellen. Nach Installation des Zertifikats könnte demzufolge der Anwender über die Identität einer Webseite (z.B. seiner Bank) getäuscht werden. Die BRAK hat daher noch am selben Tag die weitere Verbreitung dieses fehlerhaften Zertifikats gestoppt. 7

Aufgrund dieser technischen Probleme wurde das beA insgesamt vom Netz genommen und ist seitdem nicht mehr erreichbar. Am 27.12.2017 teilte die BRAK mit, dass der Dienstleister das technische Problem während der Weihnachtstage nicht beheben konnte und dass das beA weiter offline bleiben werde.[3] Das beA kann seitdem weder von Gerichten noch von anderen Absendern adressiert werden. Auch ist ein Zugriff auf im beA gespeicherte Nachrichten nicht möglich.

Das beA soll erst nach einer Überprüfung der Lösung zur Behebung der technischen Probleme der beA Client Security durch ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenes Unternehmen wieder in Betrieb genommen werden.[4] Am 26.1.2018 fand zudem auf Einladung der BRAK eine Diskussionsveranstaltung mit dem Namen „beAthon" statt, in welcher die gefundene technische Lösung erörtert wurde. Diese wurde von anwesenden Experten als grundsätzlich geeignet bewertet.[5] Aufgrund einer weiteren bei dem beAthon erörterten Sicherheitslücke der bisherigen Version der beA Client Security rät die BRAK dazu, die Anwendung zu deinstallieren oder zu deaktivieren, bis die neue Version der beA Client Security bereitsteht. Diese **neue Version der beA Client Security** soll auch weitere von Herrn *Drenger* festgestellte Mängel, wie die Verwendung veralteter Softwarebibliotheken, beheben. 8

Einen Termin zur Wiederinbetriebnahme hat die BRAK bislang noch nicht genannt; dies soll auf Grundlage des Gutachtens des von der BRAK beauftragten Unternehmens erfolgen.[6] Einen Termin zur Wiederinbetriebnahme und sonstige Informationen zum beA wird die BRAK u.a. über ihre Webseiten und den beA-Newsletter[7] bekannt geben. Die BRAK hat mitgeteilt, dass sie mit „*einer angemessenen Frist zwischen Ankündigung und Wiederinbetriebnahme der beA-Plattform*" plane.

II. Folgen der Abschaltung des beA

Die Abschaltung des beA hat erhebliche Auswirkungen auf den elektronischen Rechtsverkehr in Deutschland. Gleichwohl stellen sich diese Auswirkungen bei genauer Betrachtung deutlich weniger dramatisch dar: 9

- § 31a Abs. 6 BRAO sieht seit dem 1.1.2018 die sog. passive Nutzungspflicht für Inhaber eines beA-Postfachs vor. Insbesondere müssen nach dieser Vorschrift Rechtsanwälte und Rechtsanwältinnen Zustellungen und sonstige Nachrichten über das beA zur Kenntnis nehmen. Da aufgrund der Abschal-

2 beA-Sondernewsletter v. 3.1.2018, http://www.brak.de/zur-rechtspolitik/newsletter/bea-newsletter/2018/sondernewsletter-v-03012018.news.html

3 BRAK, Presseerklärung Nr. 15 v. 27.12.2017.

4 BRAK, Presseerklärung Nr. 2 v. 18.1.2018.

5 U.a. *Reiling*, Was ist eigentlich beim „beAthon" passiert? Tipp: beA-Client-Security deinstallieren; https://anwaltsblatt.anwaltverein.de/de/anwaeltinnen-anwaelte/anwaltspraxis/beathon

6 BRAK, Presseerklärung Nr. 4 v. 26.1.2018.

7 https://www.brak.de/bea-newsletter/

tung des beA keinerlei Nachrichten in das Postfach gelangen können, kann sich die Frage eines möglichen Verstoßes gegen die berufsrechtliche Regelung nicht stellen.

- Der EGVP-Bürgerclient wird nach einer Mitteilung der Justiz weiterhin bereitgestellt und kann im elektronischen Rechtsverkehr genutzt werden. Über den Zeitpunkt der Abschaltung des EGVP-Bürgerclients soll nun im Mai 2018 entschieden werden. Zu beachten ist jedoch, dass die Signaturfunktion des EGVP-Bürgerclients eine sog. Containersignatur erzeugt, die seit dem 1.1.2018 im Anwendungsbereich der Elektronischer-Rechtsverkehr-Verordnung (ERVV) unzulässig ist.[8]
- Das Zentrale elektronische Schutzschriftenregister (ZSSR), für das § 49c BRAO für Rechtsanwältinnen und Rechtsanwälte schon seit dem 1.1.2017 eine berufsrechtliche Nutzungspflicht vorsieht, kann auch ohne das beA genutzt werden. Das Schutzschriftenregister ermöglicht eine Einreichung sowohl über weitere EGVP-Clients als auch über ein Online-Formular.[9] § 2 Abs. 5 Schutzschriftenregisterverordnung sieht zudem seit 1.1.2018 mit der „absenderbestätigten" De-Mail einen alternativen „sicheren Übermittlungsweg" zum ZSSR vor, bei dessen Verwendung eine qualifizierte elektronische Signatur nicht erforderlich ist.
- Für das automatisierte Mahnverfahren gilt seit dem 1.1.2018 eine erweiterte Nutzungsverpflichtung, d.h. über den Mahnantrag hinaus müssen weitere Anträge und Erklärungen im automatisierten Mahnverfahren eingereicht werden.[10] Hierfür können der EGVP-Bürgerclient oder eine andere EGVP-Anwendung verwendet werden, solange das beA nicht zur Verfügung steht. Teil des automatisierten Mahnverfahrens ist zudem auch bis mindestens 31.12.2019 das auf Papier basierende Barcodeverfahren.

III. Diskussion der technischen Architektur des beA

Gleichzeitig dehnte sich die Diskussion, über die von Herrn *Drenger* festgestellten Probleme hinaus, auf andere Fragen im Zusammenhang mit dem beA aus. Einen großen Raum nimmt dabei die Diskussion des Verschlüsselungsverfahrens beim beA ein, bei dem eine **sog. Umschlüsselung** in speziellen Hardware Security Modulen (HSM) zum Einsatz kommt. Der digitale Schlüssel der Nachricht, nicht die Nachricht selbst, wird in besonders gesicherten HSMs mit dem Schlüssel des berechtigten Nutzers neu verschlüsselt („umgeschlüsselt"), wobei Berechtigungen nur vom Postfachinhaber oder von durch diesen berechtigte Personen vergeben werden können.[11] Gewählt wurde diese Lösung, um – entsprechend der Regelung des § 31a Abs. 3 S. 3 BRAO und der Ergebnisse der von der BRAK durchgeführten Workshops mit Rechtsanwälten und Mitarbeitern[12] – die Arbeitsteilung von Rechtsanwälten und Mitarbeitern abzubilden. **10**

Die BRAK hat seit dem Beginn der Entwicklung des beA das Verschlüsselungsverfahren immer wieder in Veröffentlichungen und Vorträgen beschrieben und dabei als **„Ende-zu-Ende"-Verschlüsselung** bezeichnet.[13] Eingewandt wird nun, es handele sich aufgrund der im beA umgesetzten Architektur tatsächlich nicht um eine „Ende-zu-Ende"-Verschlüsselung. Über die Frage, ob die Bezeichnung richtig gewählt ist, kann man unterschiedlicher Auffassung sein: Die Nachricht selbst bleibt bis zum Empfänger ununter- **11**

8 Vgl. zum Verbot der Containersignatur auch *Viefhues*, Elektronischer Rechtsverkehr Ausgabe 4/2017, Rn 12, die Erläuterungen im beA-Newsletter Ausgabe 46/2017 v. 16.11.2017, die Hinweise zur Anbringung einer qualifizierten elektronischen Signatur in der zulässigen Form im beA-Newsletter Ausgabe 4/2018 v. 15.2.2018 sowie Nr. 4 der Bekanntmachung nach § 5 ERVV (BAnz AT 28.12.2017 B2).

9 Vgl. die Erläuterungen im Handbuch des ZSSR ab S. 13, https://schutzschriftenregister.hessen.de/sites/schutzschriftenregister.hessen.de/files/handbuch_zssr_of.pdf

10 beA-Newsletter Ausgabe 41/2017 v. 12.10.2017.

11 Eine ausführliche Beschreibung des Verschlüsselungsverfahrens findet sich unter http://bea.brak.de/wie-sicher-ist-das-bea/sichere-nachrichtenuebermittlung/

12 *Lummel*, BRAK Magazin 5/2013, S. 4.

13 Z.B. *Brosch*/*Fiebig*, BRAK Magazin 4/2015, S. 10.

brochen verschlüsselt, und **Berechtigungen zum Umschlüsseln** können **nur vom Postfachinhaber** vergeben werden. Aus diesem Grund erhalten Zustellungsbevollmächtigte, Vertreter und Abwickler Zugriff nur auf die Postfachübersicht und können den Inhalt von Nachrichten nicht lesen, sofern der Postfachinhaber nicht weiter gehende Rechte vergeben hat. Die Möglichkeit in den Raum zu stellen, die BRAK habe heimlich und ohne Information ihrer Mitglieder aufgrund staatlicher Vorgaben das Umschlüsselungsverfahren als eine „Abhörschnittstelle" konzipiert,[14] sollte jedem neutralen Beobachter abwegig erscheinen. Insgesamt lohnt bei der Diskussion des Verschlüsselungsverfahrens eine Versachlichung.

Darüber hinaus wird aktuell über verschiedene Verbesserungsvorschläge und Forderungen an den Gesetzgeber im Bereich des elektronischen Rechtsverkehrs, die bereits seit mehreren Monaten und ohne Bezug zu den aktuellen Ereignissen Gegenstand der Diskussion sind, gesprochen. Die Einrichtung eines „Kanzleipostfachs" etwa wäre ohne gesetzliche Anpassungen voraussichtlich nicht möglich und würde zu erheblichen technischen Änderungen am beA führen, zudem sind im beA „Workarounds" möglich.[15] Warum die Wiederinbetriebnahme des beA mit solchen Fragen verknüpft wird, ist nicht ersichtlich; die Diskussion über gesetzliche und technische Gestaltungsmöglichkeiten kann und sollte während des laufenden Betriebs des beA geführt werden. **12**

Schließlich sind auch mehrere Missverständnisse Teil der aktuellen Diskussion. So wird vorgebracht, es könne mit dem beA nur alle 15 Minuten eine Nachricht versandt werden. Dass dies unzutreffend ist, können jeder Rechtsanwalt und jede Rechtsanwältin bestätigen, die in der Vergangenheit das beA genutzt haben. Auch wird dem beA vorgeworfen, es sei eine technische Insellösung; wieso die BRAK nicht vorhandene technische Lösungen zur E-Mail-Verschlüsselung eingesetzt habe, sei nicht nachvollziehbar. Das beA ist jedoch nach der Konzeption des Gesetzgebers Teil der seit vielen Jahren etablierten EGVP-Kommunikationsinfrastruktur: Die Kommunikation über EGVP wird seit mehr als zehn Jahren von Gerichten und Verwaltungen genutzt; Basis ist der XÖV-Standard OSCI-Transport. Der Gesetzgeber des Gesetzes zur Förderung des elektronischen Rechtsverkehrs hat daher das beA als Teil dieser bestehenden Infrastruktur vorgesehen.[16] § 20 Abs. 1 S. 1 RAVPV bestimmt demzufolge für das beA den Einsatz des OSCI-Kommunikationsstandards. Derartige Missverständnisse lassen sich schnell aufklären und sollten nicht den Blick auf die wesentlichen Fragen verstellen. **13**

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

C. beA außer Betrieb – vom Dilemma bis zur Aussicht auf eine Lösung

Verfasserin: Ilona Cosack

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

Viele Kanzleien hatten sich auf den Starttermin zum 1.1.2018 gut vorbereitet. Um die passive Nutzungspflicht zu erfüllen, wurden beA-Karten und Kartenlesegeräte bestellt, die Kanzleiorganisation auf die neuen Erfordernisse abgestimmt. Die Rechtsanwaltskammer Koblenz verschickte schon am 21.12.2017 **14**

14 So z.B. *Erbguth*, JurPC Web-Dok. 13/2018, Abs. 22.
15 *Brosch*, Elektronischer Rechtsverkehr Ausgabe 4/2017, Rn 24.
16 BR-Drucks 818/12, S. 33, http://dipbt.bundestag.de/dip21/brd/2012/0818–12.pdf#page=41

ihren Weihnachtsgruß über das beA. Mancher Anwalt bekam einen Schrecken, weil er nicht sofort in sein Postfach sehen konnte. Andere hatten das beA verdrängt und sich vorgenommen, zwischen den Jahren die Einrichtung des beA vorzunehmen. Doch dann kam alles ganz anders.

I. Sicherheitsproblem: beA-Zertifikat

Am vorletzten Arbeitstag vor Heiligabend, 22.12.2017, informierte der EGVP-Newsletter morgens darüber, dass ein für die beA-Anwendung notwendiges Zertifikat nicht mehr gültig sei. Aus diesem Grund sei es erforderlich, dass alle beA-Nutzer ein zusätzliches Zertifikat lokal installieren. 15

Das in aller Schnelle „gestrickte" Zertifikat machte die Sicherheitslücke nur noch größer, deshalb wurde am Freitag, 23.12.2017, davor gewarnt und eilends eine Deinstallationsanweisung veröffentlicht. 16

Ein Hacker des Chaos Computer Clubs Darmstadt (C3), *Markus Drenger*, hatte von befreundeten Rechtsanwälten erfahren, dass das beA ab 1.1.2018 passiv genutzt werden muss. Er schaute sich die Software mit ein paar Freunden an einigen Abenden an und fand eine Sicherheitslücke beim Anmeldeverfahren der beA-Client-Security. Über diese Lücke informierte er am 20.12.2017 sowohl die BRAK als auch das Bundesamt für Sicherheitstechnik in der Informationstechnik (BSI) und die das Zertifikat ausstellende T-Systems. Nach den Regeln muss ein solches Zertifikat dann binnen 24 Stunden gesperrt werden, was auch geschah. Daraufhin nahm die BRAK das beA „*wegen Wartungsarbeiten am 23. und 24. Dezember sowie an den Weihnachtsfeiertagen vom Netz*". Am 27.12.2017 informierte die BRAK, dass beA offline bleiben muss: „*Sicherheit und Datenschutz haben Priorität*". Dringend wurde nochmals geraten, das am 22.12.2017 zur Verfügung gestellte Zertifikat zu entfernen. 17

II. Wie kann die passive Nutzungspflicht erfüllt werden?

Am 27.12.2017 veröffentlichte die BRAK 16 Fragen und Antworten, die bei Bedarf aktualisiert werden. Dort heißt es unter Punkt 9.: 18

> *Frage: Welche Auswirkung hat die Abschaltung des beA-Systems auf die passive Nutzungspflicht für Rechtsanwälte?*
>
> *Antwort: Rechtsanwälte können die am 1.1.2018 eintretende passive Nutzungspflicht nicht erfüllen, solange die beA-Plattform vom Netz ist. Weder Rechtsanwälte noch Gerichte können im Moment Nachrichten in ein beA senden oder von dort abholen und müssen deshalb auf andere Medien ausweichen.*

Der DAV geht davon aus, dass Rechtsanwälte nicht verpflichtet sind, einen anderen Kommunikationskanal als Alternative zum beA zur Verfügung zu stellen. Wer also bislang herkömmlich mit Briefpost und Fax gearbeitet hat, kann das auch weiterhin tun, da zum 1.1.2018 lediglich die passive Nutzungspflicht (Empfangsbereitschaft) hergestellt werden sollte.

III. Welche Alternativen gibt es?

Rechtsanwälte, die den elektronischen Rechtsverkehr aktiv nutzen wollen, haben verschiedene Möglichkeiten: 19

1. EGVP-Classic-Client

Bis Mai 2018 steht der EGVP-Classic-Client zur Verfügung. Wichtig ist, dass Schriftsätze und Anlagen, die hierüber eingereicht werden, mit einer qualifizierten elektronischen Signatur (qeS) versehen sein 20

müssen. Da die bisherige Container-Signatur seit dem 1.1.2018 nicht mehr zulässig ist, muss das Dokument mit einem externen Signaturprogramm, z.B. Sec Signer, signiert werden. Zum Signieren kann die beA-Karte Basis mit einer Nachladesignatur aufgewertet werden oder direkt die beA-Karte Signatur oder eine anderweitige Signaturkarte genutzt werden.

2. EGVP-Drittanwendungen

Wer noch nicht mit dem EGVP-Classic-Client gearbeitet hat, kann direkt mit einer EGVP-Drittanwendung, z.B. dem Governikus Communicator Justiz Edition, starten. Eine Identifikation ist nicht erforderlich. Die Registrierung erfolgt so, wie in der eBroschüre ERV 4/2017 (Rdn 28 ff.) zur Kommunikation mit Mandanten über das Bürgerpostfach beschrieben. Der Governikus Communicator ist als Nachfolgeprodukt des EGVP-Classic-Clients von der Bedienung her identisch, die Daten aus der EGVP-Classic-Client-Anwendung können dorthin exportiert werden. 21

3. De-Mail

Für den Betrieb eines De-Mail-Postfachs muss man sich bei einem Anbieter von De-Mail, z.B. der Telekom, registrieren und kann dann per absenderbestätigter De-Mail mit den Gerichten kommunizieren. Zur Einrichtung siehe z.B. http://ejustice-bw.de/pb/,Lde/Startseite/Buerger/De-Mail. Derzeit sind die De-Mail-Adressen der Gerichte noch nicht ordnungsgemäß im öffentlichen Verzeichnis sichtbar. Alle bundesdeutschen Gerichte sind unter der Stadt Taucha in Sachsen gelistet. Dort befindet sich der Dienstleister, der das De-Mail-Programm der Justiz betreibt. Allerdings entstehen für jede Nachricht, die über De-Mail versendet wird, Kosten wie für Briefpost. 22

IV. Mahnverfahren

Wer bisher mit dem Barcode-Mahnverfahren gearbeitet hat, kann dieses Verfahren mindestens bis zum 31.12.2019 nutzen. Die erweiterte Nutzungspflicht für die **Folgeanträge im Mahnverfahren** ab 1.1.2018 kann ebenfalls über das Online-Mahnantragsportal erfüllt werden. Alternativ können EGVP-Classic-Client und -Drittanwendungen genutzt werden. 23

V. Schutzschriften

Diese sind über das zentrale Schutzschriftenregister bereits seit dem 1.1.2017 ausschließlich elektronisch einzureichen. Das geht entweder mit dem Governikus Communicator oder auch online über das Justizportal des Bundes und der Länder. Die Besonderheit beim Schutzschriftenregister ist, dass es sich um ein **vollautomatisiertes Verfahren** handelt, sodass die Einreichung von Schutzschriften an bestimmte technische Rahmenbedingungen geknüpft ist, um eine ordnungsgemäße Verarbeitung zu ermöglichen. 24

VI. Kanzleisoftware

Die Kanzleisoftwarehersteller nutzen für die Schnittstellen einen anderen Zugang, sodass die Anwender bei der Verwendung der Schnittstelle **von der Sicherheitslücke nicht betroffen** sind. Gleichwohl ist das beA für alle Nutzer derzeit nicht nutzbar. 25

VII. beA-Sicherheit auf dem Prüfstand

Am 9. und 18.1.2018 trafen sich die Präsidenten der regionalen Rechtsanwaltskammern mit der BRAK. Es wurde beschlossen, dass eine externe IT-Firma, die auf der Liste der vom BSI empfohlen Firmen steht, ein Gutachten über die Sicherheit des beA erstellen soll. Des Weiteren wurde ein sog. „beAthon" für den 26. Januar festgelegt. Dazu hatte die BRAK *Markus Drenger* und zwei Kollegen vom C3 sowie eine Handvoll ausgewählte Vertreter vom DAV, dem EDV-Gerichtstag, der externen IT-Firma secunet Security Networks AG, der neuen Kommunikationsagentur der BRAK und zwei Pressevertreter eingeladen. Der Dienstleister des beA, die Firma Atos, erklärte kurz vorher, dass er nicht am beAthon teilnehmen werde. Atos erklärte vielmehr in einer ebenfalls am 26.1.2018 veröffentlichten Presseerklärung, dass die Sicherheitslücken des beA behoben seien und es nunmehr an der BRAK liege, wann das beA wieder online gehe. 26

Eine Vielzahl von Veranstaltungen mit *Markus Drenger* reihte sich in den letzten Wochen aneinander: Der Chaos Computer Club Darmstadt widmete am 16.1.2018 dem beA einen Abend, an dem *Markus Drenger* mit seinem Kollegen *Felix Rohrbach* vielen IT-Experten und einigen Anwälten darlegte, welche Sicherheitslücken gefunden wurden. Es gibt eine Aufzeichnung dieser Veranstaltung bei YouTube. 27

Am 22.1.2018 richtete der DAV eine Veranstaltung zum beA aus, auch hier gibt es eine Aufzeichnung. Eine Zusammenfassung können Sie hier lesen:

https://bea-abc.de/blog/anwaltspostfach-bea-bestandsaufnahme-und-ausblick/

Am 25.1.2018 befasste sich das Legal Tech & Innovation Forum Frankfurt mit dem beA. Im Live-Stream, mit Aufzeichnung und zeitgemäßem Chat konnten die Fragen an *Markus Drenger* und erstmals auch an den Präsidenten der Rechtsanwaltskammer Berlin, *Dr. Marcus Mollnau*, gestellt werden. Dieser erklärte, dass nach Vorlage des Gutachtens von secunet in einer weiteren Hauptversammlung der BRAK entschieden werde, wann das beA wieder online geht. Die Zusammenfassung können Sie hier lesen:

https://bea-abc.de/blog/anwaltspostfach-bea-panel-diskussion-beim-legal-tech-innovation-forum-frankfurt/

Am 1.2.2018 richteten der Berliner Anwaltsverein und die Arbeitsgemeinschaft IT-Recht im DAV (davit) eine öffentliche Diskussion für Anwälte und IT-Interessierte aus. Dort informierte *Markus Drenger*:

> *„Ich gehe davon aus, dass man das beA in relativ kurzer naher Zeit wieder in Betrieb nehmen kann. Mich hat es gewundert, dass sich nur 65.000 Anwälte registriert hätten, die anderen 100.000 sollten das jetzt dringend tun."*

Eine Aufzeichnung gibt es bei YouTube und eine Zusammenfassung der Diskussion findet sich hier:

https://bea-abc.de/blog/hic-sunt-leones-anwaltspostfach-bea-kann-bald-wieder-in-betrieb-gehen/

VIII. Alte beA-Client-Security

Im Rahmen des beAthon warnte *Markus Drenger* nochmals vor einer Sicherheitslücke, die sich aus dem Autostart der Client Security ergibt. Danach veröffentlichte die BRAK direkt nach dem beAthon einen Sonder-Newsletter, in dem sie empfahl, die **Client Security** zu **deaktivieren oder** ganz zu **deinstallieren**. Eine Anleitung dazu findet sich auf der Seite der Rechtsanwaltskammer Berlin: 28

https://www.rak-berlin.de/mitglieder/aktuelles/2018/180201_ErgebnissebeAthon.php

IX. Fazit

Derzeit wartet die BRAK auf das Gutachten der Firma secunet. Nach Vorlage des Gutachtens soll die Hauptversammlung darüber entscheiden, wie es mit beA weitergeht. In den „Fragen und Antworten" ist unter Punkt 16 allerdings nachzulesen: 29

> *Frage: Wird die BRAK den Rechtsanwälten eine angemessene Frist zwischen Ankündigung und Wiederinbetriebnahme der beA-Plattform einräumen?*
>
> *Antwort: Ja, die BRAK plant mit einer angemessenen Frist zwischen Ankündigung und Wiederinbetriebnahme der beA-Plattform. Wie lange dieser Zeitraum genau sein wird, wird die BRAK bekannt geben, sobald technische Fragen mit dem entsprechenden Dienstleister geklärt sind. Die Frist kann einen Zeitraum von zwei Wochen umfassen.*

Wer also noch nicht alle Voraussetzungen zur Erfüllung der passiven Nutzungspflicht erfüllt, sollte die Zeit nutzen, um beA-Karten in ausreichender Zahl, vor allem beA-Mitarbeiterkarten, und Kartenlesegeräte zu besorgen. Innerhalb von zwei Wochen wird die BNotK einen Bestellansturm nicht bewältigen können.

D. Infos aus Bund und Bundesländern

Verfasser: Dr. Wolfram Viefhues

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

I. Bundesamt für Justiz stellt Online-Formular bereit

Das Bundesamt für Justiz (BfJ) stellt seit Jahresbeginn 2018 ein Meldeformular für Hinweise auf Verstöße gegen das Netzwerkdurchsetzungsgesetz online zur Verfügung. Die für die sozialen Netzwerke geltenden Übergangsfristen sind abgelaufen. Sie sind jetzt verpflichtet, ein wirksames und transparentes Beschwerdemanagement für den Umgang mit rechtswidrigen Inhalten (Hasskriminalität und andere strafbare Inhalte) bereitzuhalten. Wird ein derartiges Beschwerdeverfahren nicht, nicht richtig oder nicht vollständig vorgehalten, prüft dasBfJ, ob ein Bußgeldverfahren einzuleiten ist. Alle betroffenen Nutzerinnen und Nutzer können dem BfJ mitteilen, dass trotz ihrer Beschwerde beim sozialen Netzwerk ein rechtswidriger Inhalt innerhalb der genannten Fristen weder gelöscht noch gesperrt wurde. Diesen Hinweis können alle Betroffenen über das vom Bundesamt auf seinen Internetseiten bereitgestellte Online-Formular übermitteln. Das Bundesamt selbst kann keine Löschungen oder Sperrungen vornehmen, sondern prüft die Einleitung eines Bußgeldverfahrens wegen systemischer Mängel im Beschwerdemanagement. 30

Das Meldeformular steht auf der Internetseite *www.bundesjustizamt.de* unter dem Pfad Themen > Bürgerdienste > Rechtsdurchsetzung in sozialen Netzwerken > Service > Formulare zur Verfügung.

II. Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT)

Die Ende letzten Jahres eingerichtete Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) ist eine Sondereinheit der Generalstaatsanwaltschaft Frankfurt am Main. Sie dient den örtlich zuständigen Staatsanwaltschaften und der Polizei als kompetenter Ansprechpartner in allen Fällen der Computer- und Internetkriminalität. In Einzelfällen kann die ZIT als Task-Force Verfahren mit Internetbezug aus allen Be- 31

reichen des Strafrechts mit besonders hohen Anforderungen an die technische Beweisführung übernehmen und damit die Staatsanwaltschaften in komplexen Verfahren entlasten.

Aus- und Fortbildung der Dezernentinnen und Dezernenten der örtlichen Staatsanwaltschaften ist ein weiterer wesentlicher Aufgabenbereich der Zentralstelle. Bei der ZIT sind derzeit zwei Stellen für Oberstaatsanwälte vorgesehen. Darüber hinaus sind aktuell drei weitere Vollzeitstellen im Wege zeitlich befristeter Abordnungen von Staatsanwältinnen und Staatsanwälten von den örtlichen Staatsanwaltschaften an die ZIT besetzt. Die Zentralstelle wird durch ein Sekretariat mit gegenwärtig drei Bediensteten unterstützt.

Die Schaffung der ZIT korrespondiert mit der Einrichtung entsprechender Fachkommissariate bei der Polizei und optimiert dadurch die Zusammenarbeit der mit der Strafverfolgung befassten Behörden. Zudem ist die ZIT unmittelbarer Ansprechpartner für das Bundeskriminalamt und das Hessische Landeskriminalamt im Zusammenhang mit anlassunabhängigen Recherchen in Datennetzen, bei der Ermittlung unbekannter Opfer von über Internet verbreiteter Kinderpornographie sowie bei Verfahren größeren Umfangs wegen Internet- und Computerkriminalität.

III. Rechtliche Hürden der Verwaltungsdigitalisierung

Eine aktuelle juristische Studie der Bundesdruckerei benennt eine grundlegende Hürde bei der Digitalisierung von Verwaltungsdienstleistungen. Beanstandet wurde vor allem, dass die Gesetze für viele Verwaltungsdienstleistungen digitale Prozesse nicht vorsehen. Zudem werden neue vor allem durch die eIDAS-Verordnung geschaffenen Möglichkeiten, wie etwa die elektronische Fernsignatur oder das sog. Behördensiegel noch nicht genutzt. Der eIDAS-Werkzeugkasten könnte dazu beitragen, die Hürden beim E-Government abzubauen. Die Bundesdruckerei-Studie gibt der Politik konkrete Handlungsempfehlungen auf den Weg, damit die Verwaltungen ihre E-Government-Dienste digitalisieren können. *https://www.bundesdruckerei.de/de/WP-Detailseite-Studie-Regelungsbedarf-bei-E-Government-und-digitaler-Signatur* **32**

IV. Ergebnisse der Herbstkonferenz 2017 der Justizminister

Die Justizminister der Länder haben sich auf ihrer Herbstkonferenz mit einer Fülle von Themen befasst, die auch den Bereich der Elektronik abdecken: **33**

- Ein Thema war die Beeinflussung von Nutzern sozialer Netzwerke durch Meinungsroboter (sog. Social Bots), zu dem die Politikerrunde auf Initiative Hamburgs bereits eine Arbeitsgruppe eingesetzt hatte. Die umstrittenen Bots erzeugten mit falschen Profilen und plakativen Äußerungen Nähe und täuschten Gemeinsamkeiten vor. Gefordert wurde eine umfassende bußgeldbewährte Kennzeichnungspflicht.
- Im Einklang mit dem EU-Parlament sprechen sich die Länder dafür aus, Whistleblower rechtlich besser abzusichern, und wollen insbesondere den Anspruch auf Vertraulichkeit von Hinweisgebern prüfen lassen.
- Weiterhin haben die Beschlüsse die Bekämpfung von Terrorismus und Cybercrime aufgegriffen. Schwere Straftaten sollen auch in den schwerer zu durchdringenden, nicht von Suchmaschinen indexierten Teilen des Internets (sog. Darknet) besser geahndet werden können.
- Betont wurde neben den gesetzlichen Löschpflichten der Betreiber sozialer Netzwerke und sonstiger Kommunikationsplattformen auch die Bedeutung einer konsequenten Strafverfolgung strafrechtlich relevanter Äußerungen im Internet.

http://www.jm.nrw.de/JM/jumiko/beschluesse/2017/Herbstkonferenz-2017/index.php

E. Ausgewählte Rechtsprechung zum ERV

Verfasser: Wolfgang Kuntz

Rechtsanwalt und Fachanwalt für IT-Recht, Saarbrücken

I. Eingangsbestätigung per EGVP bei nicht mehr auffindbarer Klageschrift

VGH Hessen, Beschl. v. 26.9.2017 – 5 A 1193/17 34

Das Gericht hatte über den Fall einer im Gericht nicht mehr auffindbaren Klageschrift zu entscheiden. Der klägerische Anwalt hatte die Klageschrift mit qualifizierter elektronischer Signatur per EGVP am 22.4.2015 an das VG Frankfurt am Main gesandt und dafür eine automatisch erzeugte EGVP-Eingangsbestätigung erhalten. Ein Klageeingang war beim Gericht jedoch nicht verzeichnet worden. Nach sechs Monaten werden die Daten über Klageeingänge auf dem Server des Gerichts automatisch gelöscht. Im Januar 2017 sei dem Rechtsanwalt dann erst aufgefallen, dass das Gericht keine Eingangsverfügung verschickt habe. Danach hat der klägerische Anwalt qualifiziert signiert am 12.1.2017 bei Gericht nachgefragt und die Klageschrift vom 22.4.2015 erneut vorgelegt. Das VG Frankfurt hatte die Klage wegen Versäumung der Klagefrist abgewiesen.

Das Gericht entschied, dass der Beweis des ersten Anscheins dafür spreche, dass das Schriftstück zu dem auf der Eingangsbestätigung ausgewiesenen Zeitpunkt auf dem Gerichtsserver eingegangen ist, wenn ein Verfahrensbeteiligter einen Ausdruck der vom gerichtlichen Empfangsserver automatisch versandten Eingangsbestätigung für den Eingang eines Schriftstücks per EGVP vorlegt.

II. Einlegung einer Beschwerde per EGVP ohne qualifizierte elektronische Signatur

Schleswig-Holsteinisches LSG, Beschl. v. 24.10.2017 – L 6 AS 159/17 B 35

Die Beteiligten stritten im einstweiligen Rechtsschutzverfahren über die Höhe der zu berücksichtigenden Bedarfe für Unterkunft und Heizung. Mit Beschl. v. 13.9.2017 hat das Sozialgericht den Antragsgegner im Wege der einstweiligen Anordnung vorläufig verpflichtet, der Antragstellerin weitere Leistungen i.H.v. mtl. 28,62 EUR zu gewähren und den Antrag im Übrigen – insbesondere auch wegen des Differenzbetrags zwischen den als angemessen anerkannten und den tatsächlichen Unterkunftskosten i.H.v. mtl. 290,00 EUR – abgelehnt.

Gegen den der Antragstellerin am 14.9.2017 zugestellten Beschluss ist am selben Tag für sie Beschwerde eingelegt worden. Der Beschwerdeschriftsatz ist an das elektronische Gerichts- und Verwaltungspostfach (EGVP) übersandt worden. Die Nachricht hat keine qualifizierte elektronische Signatur enthalten.

Mit Verfügung vom 22.9.2017 hat der Berichterstatter die Antragstellerin darauf hingewiesen, dass die Beschwerde in elektronischer Form, aber ohne die erforderliche qualifizierte elektronische Signatur erhoben worden sei und deshalb den Formerfordernissen an eine wirksame Beschwerdeerhebung nicht genüge. Der Formmangel könne entweder durch schriftliche Übersendung eines handschriftlich unterschriebenen Beschwerdeschriftsatzes oder durch erneute elektronische Übersendung unter Verwendung einer qualifizierten elektronischen Signatur innerhalb der Beschwerdefrist geheilt werden.

Am 23.9.2017 hat die Antragstellerin mitgeteilt, dass sie über keine Signaturkarte verfüge. Am 26.9.2017 ist beim Landessozialgericht ein Schriftsatz vom 23.9.2017 unter dem Briefkopf der Antragstellerin eingegangen, mit dem (erneut) Beschwerde gegen den Beschl. v. 13.9.2017 eingelegt worden ist und der die handschriftliche Paraffe „gez." und danach den maschinenschriftlich geschriebenen Namen der Antragstellerin enthalten hat.

Am 5.10.2017 ging unter dem Namen der Antragstellerin ein weiterer Schriftsatz in Reaktion auf ein Schreiben des Antragsgegners vom 29.9.2017 ein, wiederum über das EGVP ohne qualifizierte elektronische Signatur übermittelt. Dieser Schriftsatz enthielt eine eingescannte handschriftliche Unterschrift der Antragstellerin.

Das Gericht entschied:

1. Die Beschwerde gegen eine Entscheidung des Sozialgerichts, die durch Einreichung über das elektronische Gerichts- und Verwaltungspostfach (EGVP) erhoben wird, genügt den Anforderungen an die elektronische Form nur, wenn sie mit einer qualifizierten elektronischen Signatur versehen ist.

2. Dem Schriftformerfordernis des § 173 SGG genügt es nicht, wenn der maschinenschriftlichen Bezeichnung von Vor- und Nachnamen handschriftlich die Paraphe „gez" beigefügt wird.

3. Wählt der Beteiligte – durch Einreichung über das EGVP – die elektronische Form, sind für die Zulässigkeit allein deren Anforderungen maßgebend; der Ausdruck einer Beschwerdeschrift durch das Gericht vermag unabhängig davon, wie die Unterschrift generiert wurde (hier: eingescannte Unterschrift), den Anforderungen an die Schriftform nicht zu genügen (Anschluss an BSG vom 12.10.2016 – B 4 AS 1/16 R = SozR 4–1500 § 65a Nr. 3).

III. Verweigerung der Mitbestimmung des Personalrates per E-Mail

■ **VG Düsseldorf, Beschl. v. 24.11.2017 – 39 K 5920/15.PVB** 36

Der Personalrat kann die Zustimmung zu einer mitbestimmungspflichtigen Maßnahme durch eine einfache E-Mail seines Vorsitzenden (Stellvertreters) an den Dienststellenleiter wirksam verweigern, wenn die Gründe der Zustimmungsverweigerung darin enthalten sind. Auch die einfache E-Mail kann dem Formerfordernis „schriftlich" in § 69 Abs. 2 S. 5 BPersVG genügen.

IV. Keine sofortige Beschwerde per einfacher E-Mail

■ **OLG Hamm, Beschl. v. 28.12.2017 – III-4 Ws 241/17** 37

Die nach § 306 Abs. 1 StPO vorgeschriebene Form, d.h. zu Protokoll der Geschäftsstelle oder schriftlich, wird bei Einlegung einer sofortigen Beschwerde durch einfache, nicht über eine elektronische Signatur nach § 41a StPO verfügende E-Mail, nicht gewahrt.

V. Erfolglose Rechtssatzverfassungsbeschwerde gegen Einführung des besonderen elektronischen Postfachs (beA)

■ **BVerfG, Nichtannahmebeschl. v. 20.12.2017 – 1 BvR 2233/17** 38

Bei den Vorschriften über den anwaltlichen elektronischen Rechtsverkehr und die Einführung des besonderen elektronischen Anwaltspostfachs (beA) handelt es sich um bloße Berufsausübungsregelungen und nicht um solche, die die Zulassung zur Rechtsanwaltschaft betreffen, mithin nicht um subjektive Berufszugangsregelungen.

Regelungen, die lediglich die Berufsausübung betreffen, sind mit Art. 12 Abs. 1 GG vereinbar, soweit vernünftige Erwägungen des Gemeinwohls sie als zweckmäßig erscheinen lassen und das Grundrecht nicht unverhältnismäßig eingeschränkt wird. Die Beschwerdeschrift lässt nicht erkennen, dass es an vernünftigen Erwägungen des Allgemeinwohls zur Rechtfertigung der angegriffenen Regelungen fehlen könnte. Die angegriffenen Regelungen bezwecken die Förderung des elektronischen Rechtsverkehrs, die Schaffung einer rechtssicheren und schnellen Kommunikation mit den Gerichten sowie eine Kosten-

reduktion bezüglich Porto- und Druckkosten (vgl. Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 6.3.2013, BT-Drucks 17/12634, S. 1 bis 6). Anhaltspunkte dafür, dass es sich insoweit nicht um spezifische berufsbezogene Gemeinwohlgründe handeln könnte, werden nicht aufgezeigt.

VI. Form der Berichtigung einer notariellen Gesellschafterliste durch elektronisch beglaubigte Abschrift

■ **OLG Nürnberg, Beschl. v. 28.12.2017 – 12 W 2005/17** 39

„1. Eine notarielle Gesellschafterliste kann auch noch nach Einreichung beim Handelsregister und Aufnahme in den Registerordner wegen offenbarer Unrichtigkeit gemäß § 44a Abs. 2 BeurkG berichtigt werden.

2. Die Urschrift der entsprechend berichtigten Gesellschafterliste bleibt gemäß § 45 Abs. 1 BeurkG in Verwahrung des Notars. Die Berichtigung erfolgt durch Einreichung einer elektronisch beglaubigten Abschrift der berichtigten Gesellschafterliste beim Handelsregister. Hierfür reicht nicht aus, dass bei dem insoweit gemäß § 12 Abs. 2 HGB einzureichenden elektronischen Dokument die Berichtigung allein im Text der Urkunde vorgenommen wird; vielmehr muss auch die elektronisch beglaubigte Abschrift der berichtigten Gesellschafterliste einen Berichtigungsvermerk gemäß § 44a Abs. 2 BeurkG enthalten, der Umstand und Zeitpunkt der Berichtigung erkennen lässt.“