NICOLAS BAUM Rechtsanwalt

An den
Anwaltsgerichtshof Berlin
Elßholzstraße 30-33
D-10781 Berlin

Rechtsanwalt Baum, Görlitzer Straße 74, 10997 Berlin

Görlitzer Straße 74
10997 Berlin
Tel +49(0)30 6112021
Fax +49(0)30 6112315
baum@ra-baum.com

in Bürogemeinschaft mit
Johannes Eisenberg,
Prof. Dr. Stefan König,
Dr. Stefanie Schork
Rechtsanwälte

12. November 2018

In dem Rechtsstreit
Conen u. a. ./. Bundesrechtsanwaltskammer
– I AGH 6/18 –

wird zu der dem Prozessbevollmächtigten am 21. September 2018 vorab per Telefax ohne Anlagen übersandten, sodann am 25. September 2018 inklusive Anlage zugestellten, vom 12. September 2018 datierenden Begründung der Beklagten zu ihrem Klageabweisungsantrag vom 13. Juli 2018 (im Folgenden: Klageerwiderung vom 12. September 2018) wie folgt Stellung genommen:

GLIEDERUNG

I. „Allgemeine Bedenken“ der Beklagten 4

1. Kein Ausschluss des Unterlassungsbegehrs durch bereits erfolgte rechtswidrige Einrichtung des beAs 4

2. Unerheblichkeit der Unmöglichkeit einer Einrichtung von Ende-zu-Ende-verschlüsselten Postfächern allein für die Klägergemeinschaft 5

II. Zur Ansicht der Beklagten, eine Ende-zu-Ende-Verschlüsselung des beAs sei rechtlich nicht gefordert 6

1. Ende-zu-Ende-Verschlüsselung von Gesetzgeber gefordert 6

a) Gebotene vollständige Gesetzesauslegung verlangt Ende-zu-Ende-Verschlüsselung 7

b) Ermessensreduzierung auf Null 7

c) Insbesondere: unwahre Tatsachenbehauptung der Beklagten zu Gesetzgebungsmaterialien, die ausdrücklich Ende-zu-Ende-Verschlüsselung fordern 7

d) Eingeständnis früherer irreführender Falschangaben - Beklagte ging selbst von Notwendigkeit der Ende-zu-Ende-Verschlüsselung aus 9

3. Unerheblichkeit Der behaupteten Sicherheit des beAs in seiner jetzigen Ausgestaltung 10

4. Hilfsweise: Keine Gewährleistung eines sicheren Übermittlungsweges durch die aktuelle beA-Ausgestaltung mit HSM 11

a) Bewiesene Unsicherheit 11

b) „Insecurity by Design“ 13

c) „Single Point of Failure” – das beA als zentrales Einfallstor zum Ausspähen vertraulicher Anwaltskorrespondenz 13

d) Keine durchgängige Verschlüsselung von Nachrichten 14

e) Kein Vertrauen in die Beklagte 15

III. Einrichtung des beAs mit Ende-zu-Ende-Verschlüsselung nicht unmöglich 15

1. Secunet-Gutachten geht von Machbarkeit aus 16

2. Keine gesetzliche Vorgabe zur Umschlüsselung durch HSM 17

3. Alternativkonzepte 18

a) „Zertifikate-Lösung" 19

b) Weitere Alternativkonzepte 22

4. Hilfsweise: Rechtswidrigkeit von Vorschriften der RAVPV, die einer Ende-zu-Ende-Verschlüsselung entgegenstehen könnten - Normverwerfungskompetenz des Anwaltsgerichtshofes 23

I. „Allgemeine Bedenken" der Beklagten

1. Kein Ausschluss des Unterlassungsbegehrs durch bereits erfolgte rechtswidrige Einrichtung des beAs

Die Beklagte trägt vor, der **Klageantrag zu 1** – die Beklagte zu verurteilen es zu unterlassen, für die Klägerin und die Kläger ein besonderes elektronisches Anwaltspostfach im Sinne des § 31a BRAO ohne eine Ende-zu-Ende-Verschlüsselung empfangsbereit einzurichten, bei der sich die privaten Schlüssel ausschließlich in der Verfügungsgewalt der Postfachinhaberinnen und -inhaber befinden – **gehe „ins Leere**, weil die Beklagte die elektronischen **Anwaltspostfächer bereits am 28.11.2016 dauerhaft eingerichtet**" habe (Klageerwiderung vom 12. September 2018, S. 1 f.).

Diese Argumentation **erschließt sich nicht**. Ein **etwaiger allgemeiner Rechtsgrundsatz**, aus dem sich ergeben sollte, dass die Vornahme und Perpetuierung einer rechtswidrigen Handlung einen diesbezüglichen Unterlassungsausspruch ausschließen sollte, ist **nicht bekannt**. Ein solcher Grundsatz könnte **jedenfalls in einem Rechtsstaat auch keine Geltung** beanspruchen, da er schlechterdings jeglichen Rechtsschutz gegen rechtswidriges Handeln unterbinden würde.

So ist denn auch die **Existenz der einfachen Unterlassungsklage**, die auf einen Anspruch auf Unterlassung einer bereits eingetretenen und bestehenden rechtswidrigen Handlung gestützt wird, **in ständiger Rechtsprechung anerkannt**.

Statt vieler siehe nur BVerwGE 112, 69 m. w. N.

Im Übrigen wird höchst vorsorglich darauf hingewiesen, dass für den **Umfang des Klagebegehrens** nicht allein die wortwörtliche Fassung des Klageantrages maßgebend ist, sondern „**das wirkliche Rechtsschutzziel, wie es sich aus dem**

gesamten Parteivorbringen, insbesondere der Klagebegründung, erschließt"; dem ist vom Gericht auch im Anwaltsprozess Rechnung zu tragen.

BVerwG, Beschluss vom 13. Januar 2012 – 9 B 56/11, Leitsatz, juris.

Über das von der Klägergemeinschaft verfolgte **Rechtsschutzziel, den von der Beklagten verantworteten Betrieb des beAs ohne Ende-zu-Ende-Verschlüsselung zu unterbinden**, dürfte kein Zweifel bestehen. Andernfalls wird höflich um richterlichen Hinweis gebeten.

2. Unerheblichkeit der Unmöglichkeit einer Einrichtung von Ende-zu-Ende-verschlüsselten Postfächern allein für die Klägergemeinschaft

Weiter erklärt die Beklagte, das Klagebegehren sei „**auf eine unmögliche Leistung gerichtet**", da es ihr **nicht möglich sei, das beA allein für die Klägerin und die Kläger mit einer Ende-zu-Ende-Verschlüsselung auszustatten** (Klageerwiderung vom 12. September 2018, S. 2).

Die Argumentation rekurriert vermeintlich auf den Rechtsgrundsatz „**impossibilium nulla est obligatio**" („zum Unmöglichen gibt es keine Verpflichtung"), **führt diesen aber ad absurdum**, da es sich letztlich um eine **selbstverschuldete Scheinunmöglichkeit** handelt – oder, mit anderen Worten: um eine **bloße Schutzbehauptung**.
Denn zum einen ist die **Beklagte selbst verantwortlich** dafür, das beA – ohne Not – so eingerichtet zu haben, dass ihr Änderungen an nur einem Teil der Postfächer nicht mehr möglich sind. Hierauf ist die Beklagte auch bereits vom Anwaltsgerichtshof Berlin eindrücklich hingewiesen worden:

> „Soweit die Antragsgegnerin auf einen vom Gesetzgeber vorgegebenen ‚Automatismus' bei der technischen Gestaltung verweist (Schriftsatz vom 18. April 2016, Satz 3), **wonach es ihr technisch nicht möglich sei, die Einrichtung des beA nur für einzelne Rechtsanwälte vorzunehmen, überzeugt dies nicht**. Dass eine solche Funktion bei Auftragserteilung nicht vorgesehen worden ist, **führt nicht dazu, dass der Anspruch der Antragsteller entfällt**. Es hätte der Antragsgegnerin

> freigestanden, eine entsprechende technische Lösung in Auftrag zu geben".
>
> AGH, Anwaltsgerichtshof Berlin, Beschluss vom 06. Juni 2016 – II AGH 15/15, juris-Rn. 33. Hervorhebungen sind hier und im Folgenden solche des Unterzeichners, sofern nicht anders gekennzeichnet.

Zum anderen liegt aber auch im Ergebnis **keine Unmöglichkeit** vor. Der Umstand, dass eine technische Umgestaltung einzelner Postfächer nicht möglich ist, hat vielmehr **lediglich zur Folge, dass die Beklagte sämtliche Postfächer gleichermaßen ändern muss**. Dies ist schließlich auch **geboten**, denn wenn die hiesige Klägergemeinschaft einen Anspruch hierauf hat, weil rechtlich eine Ende-zu-Ende-Verschlüsselung gefordert ist, so **haben diesen Anspruch auch alle anderen beA-Nutzer**. Damit ist die Beklagte vice versa ohnedies **verpflichtet, den rechtmäßigen Zustand einer Ende-zu-Ende-Verschlüsselung für alle Betroffenen herzustellen**.

II. Zur Ansicht der Beklagten, eine Ende-zu-Ende-Verschlüsselung des beAs sei rechtlich nicht gefordert

Die Beklagte sucht ihre Klageerwiderung insbesondere darauf zu stützen, dass die gesetzlichen Vorschriften keine Ende-zu-Ende-Verschlüsselung verlangten (Klageerwiderung vom 12. September, S. 3-11) und eine solche auch nicht erforderlich sei (ebd., S. 11-13), weil das beA in seiner aktuellen Ausgestaltung einen sicheren Übermittlungsweg gewährleiste (ebd., S. 13-19).

1. Ende-zu-Ende-Verschlüsselung von Gesetzgeber gefordert

Die Rechtsansicht der Beklagten, dass der Bundesgesetzgeber keine Ende-zu-Ende-Verschlüsselung des beAs verlange, ist **unzutreffend**.

Zur Vermeidung von Wiederholungen wird auf die **Ausführungen in der Klageschrift vom 15. Juni 2018, S. 35-46** verwiesen.

A) Gebotene vollständige Gesetzesauslegung verlangt Ende-zu-Ende-Verschlüsselung

Während die **Beklagte nur auf den Wortlaut der einschlägigen Vorschriften abstellt**, wurde bereits ausführlich dargelegt, dass die – **gebotene – vollständige Auslegung** nach Systematik, Historie und Telos im Lichte des Verfassungsrechts **keinen anderen Schluss zulässt, dass eine Ende-zu-Ende-Verschlüsselung des beAs rechtlich geboten ist** (Klageschrift vom 15. Juni 2018, S. 38-46).

B) Ermessensreduzierung auf Null

Soweit die Beklagte meint, sie habe „einen weiten Spielraum bei der Einrichtung des besonderen elektronischen Anwaltspostfachs" und ihr komme insoweit eine „**Handlungsprärogative**" zu (Klageerwiderung vom 12. September 2018, S. 3 f.), ist darauf hinzuweisen, dass sich freilich auch die Ausübung eines **Beurteilungsspielraumes**, ebenso wie Ermessensentscheidungen, **in den Grenzen des Rechts** bewegen muss. Wie in der Klageschrift bereits dargelegt (S. 34) hat die Beklagte **bei vollständiger Auslegung der einschlägigen Vorschriften keinen Entscheidungsspielraum**, das beA mit oder ohne Ende-zu-Ende-Verschlüsselung einzurichten; ihr **Ermessen reduziert sich insoweit auf Null** (Klageschrift vom 15. Juni 2018, S. 54).

C) Insbesondere: unwahre Tatsachenbehauptung der Beklagten zu Gesetzgebungsmaterialien, die ausdrücklich Ende-zu-Ende-Verschlüsselung fordern

Die Beklagte führt wörtlich aus:

> „Soweit die Kläger die Begründung zu § 19 RAVPV zitieren, sei zum anderen darauf hingewiesen, dass sie **keine Ende-zu-Ende-Verschlüsselung von Nachrichten als Grundelement des beA** anführt".
>
> Klageerwiderung vom 12. September 2018, S. 5.

Dies ist eine **nachweislich falsche Tatsachenbehauptung.**

Die betroffene – **für das hiesige Verfahren höchst wesentliche – Textpassage lautet wörtlich**:

> „Soweit auch dabei stets die Beachtung der **elementaren Grundelemente des besonderen elektronischen Anwaltspostfachs (wie beispielsweise die Ende-zu-Ende-Verschlüsselung von Nachrichten) sichergestellt** sein muss, wird dies dadurch gewährleistet, dass auch für die Kommunikation mit anderen Stellen und Personen die Vorgaben des § 20 Absatz 1 RAVPV gelten".
>
> Verordnung des Bundesministeriums der Justiz und für Verbraucherschutz über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (Rechtsanwaltsverzeichnis- und -postfachverordnung - RAVPV), BR-Drs. 417/16 vom 10. August 2016, S. 35 zu § 19 Absatz 1 (**Anlage K 22**).

Demnach besagt die Begründung zu § 19 RAVPV ihrem klaren und eindeutigen Wortlaut nach, dass gerade die **Ende-zu-Ende-Verschlüsselung sehr wohl eines der „elementaren Grundelemente" des beAs ist.**

Die gegenteilige Behauptung der Beklagten ist somit **kontrafaktisch.**

Des Weiteren ist darauf hinzuweisen, dass **auch bereits in der Begründung des Referentenentwurfs des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV)** zur RAVPV **ausdrücklich eine Ende-zu-Ende-Verschlüsselung des beAs verlangt** wird:

> „Zur **Gewährleistung einer sicheren Kommunikation mit Ende-zu-Ende-Verschlüsselung** hat der Betrieb der besonderen elektronischen Anwaltspostfächer nach Absatz 1 Satz 1 auf der Grundlage des Protokollstandards „Online Services Computer Interface" (OSCI) oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu erfolgen".
>
> BMJV, Referentenentwurf – Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (Rechtsanwaltsverzeichnis- und -postfachverordnung – RAVPV), S. 34 zu § 20 (**Anlage K25**).

Nachdem die **Ende-zu-Ende-Verschlüsselung folglich bereits im Referentenentwurf des Justizministerium als notwendiges Merkmal des beAs** vorgesehen war, wurde dies **im weiteren Verlauf des Gesetzgebungsverfahrens noch verstärkt**, indem der Gesetzgeber die Ende-zu-Ende-Verschlüsselung schließlich als „**elementares Grundelement**" des beAs noch expliziter hervorhob.

D) EINGESTÄNDNIS FRÜHERER IRREFÜHRENDER FALSCHANGABEN - BEKLAGTE GING SELBST VON NOTWENDIGKEIT DER ENDE-ZU-ENDE-VERSCHLÜSSELUNG AUS

Die Beklagte führt aus:

> „Die Kläger tragen vor, die **Beklagte habe in der Vergangenheit immer wieder behauptet, dass das beA über eine Ende-zu-Ende-Verschlüsselung verfüge, obwohl dies nicht der Fall sei**".
>
> Ebd., S. 11.

Hierzu ist zunächst anzumerken, dass sich ein **derartiger Vortrag in der Klageschrift nicht findet**. Gleichwohl machen sich die Klägerin und die Kläger den ihnen von der Beklagten zugeschriebenen Vortrag **zu eigen**, da er **zutreffend ist – wie die Beklagte selbst darlegt**, wenn sie zugibt:

> „**Richtig ist, dass das beA nicht über eine Ende-zu-Ende-Verschlüsselung im herkömmlichen Sinn verfügt**. Das **Grundprinzip der Ende-zu-Ende-Verschlüsselung** sieht vor, dass die **Nachricht vom Absender verschlüsselt wird und nur vom Empfänger der Nachricht entschlüsselt** werden kann. Im beA hingegen verschlüsselt der Absender seine Nachricht nicht gegen den Schlüssel des Empfängers, sondern gegen einen Postfachschlüssel".
>
> Ebd., S. 11.

Anzumerken ist zu diesem **Eingeständnis** lediglich, dass es freilich **kein „herkömmliches" Verständnis** von Ende-zu-Ende-Verschlüsselung gibt, **sondern nur eines**, wie in der Klageschrift ausführlich dargelegt (a. a. O., S. 16

ff.). Wenn die Beklagte in der Vergangenheit das beA als Ende-zu-Ende-verschlüsselt bezeichnet hat, dann **nicht in einem „anderen", sondern schlichtweg in einem irreführend falschen Sinne**; auch dies gibt sie letztlich zu verstehen:

> „Das Präsidium der Beklagten hat in seiner Sitzung am 14.02.2018 beschlossen, den **Begriff 'Ende-zu-Ende-Verschlüsselung' nicht mehr zu verwenden**, weil er **irreführend** sein könnte".
> Klageerwiderung vom 12. September 2018, S. 13.

Im Ergebnis stellt die Beklagte den Vortrag der Klägergemeinschaft, dass das **beA nicht über eine Ende-zu-Ende-Verschlüsselung verfügt, damit unstreitig**.

Offenkundig ging die **Beklagte bei der technischen Umsetzung der rechtlichen Vorgaben zum beA selbst davon aus, dass sie eine Ende-zu-Ende-Verschlüsselung gewährleisten muss**. Anders ist nicht zu erklären, warum sie dies in der Vergangenheit stets betonte – bis sie schließlich widerlegt wurde und einsehen musste, die Behauptung nicht mehr aufrecht halten zu können.

3. Unerheblichkeit Der behaupteten Sicherheit des beAs in seiner jetzigen Ausgestaltung

Die Beklagte möchte glauben machen, dass eine **Ende-zu-Ende-Verschlüsselung für einen sicheren Übermittlungsweg „nicht erforderlich"** sei (Klageerwiderung vom 12. September 2018, S. 11-13) und macht geltend, das **beA in seiner jetzigen Konstruktion sei ebenfalls „sicher"** (ebd., S. 13-19).

Dieser Vortrag ist **unerheblich**.

Wie in der Klageschrift ausführlich dargelegt (a. a. O., S. 35 ff.), ist es **von Gesetzes und Rechts wegen zwingend geboten**, dass das beA eine **Ende-zu-Ende-verschlüsselte Kommunikation der Nutzer** ermöglicht.

Es liegt daher **neben der Sache** und ist **ohne Belang**, ob das beA in seiner von der Beklagten gewählten Architektur unter Verwendung des HSM – die nach dem eigenen Vortrag der Beklagten **keine Ende-zu-Ende-Verschlüsselung** aufweist – **auch „irgendwie sicher" sein mag**.

4. Hilfsweise: Keine Gewährleistung eines sicheren Übermittlungsweges durch die aktuelle beA-Ausgestaltung mit HSM

Obgleich es wie dargelegt unerheblich ist, inwieweit die von der Beklagten gewählte beA-Konstruktion als „sicher" bezeichnet werden kann, da **sie schlechterdings mangels Ende-zu-Ende-Verschlüsselung schon per se nicht den rechtlichen Anforderungen genügt**, wird **hilfsweise bestritten, dass das beA in seiner aktuellen HSM-Konstruktion „einen sicheren Übermittlungsweg"** i. S. v. § 31a Absatz 1 BRAO i. V. m. § 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO sowie § 31a Absatz 1 i. V. m. § 31c Nr. 3 Buchstabe b BRAO i. V. m. den §§ 19 Absatz 1 Satz 1, 20 Absatz 1 Satz 2 RAVPV darstellt.

a) Bewiesene Unsicherheit

Die von der Beklagten selbst mit der Überprüfung der Sicherheit des beAs beauftragte secunet Security Networks AG stellt in ihrem Abschlussgutachten (im Folgenden: **secunet-Gutachten**) zum beA fest:

> „Elementar geht es um die Sicherheit der verschlüsselten Arbeitsschlüssel (Master-Key-Sets) für die verschiedenen Zwecke des HSM und der Schlüssel (Key Encryption Keys, KEKs), mit denen die Arbeitsschlüssel verschlüsselt sind, sowie die Verwahrung der mit den KEKs verschlüsselten Master-Key-Sets. **Wer sich in den Besitz dieses Schlüsselmaterials bringt, kann die im beA-System gespeicherten Nachrichten auch ohne HSM entschlüsseln, unverzüglich und umfassend, d.h. jede Nachricht kann davon betroffen sein.**
>
> (...)

Der Missbrauch dieser Schlüssel kann auf zwei Arten geschehen: **die Key Custodians des Auftraggebers und ein Helfer beim Betreiber des beA führen den verschlüsselten Nachrichtenbestand und die Schlüssel zusammen und sind dann in der Lage, die Nachrichten zu entschlüsseln**. Oder es wurde unberechtigt beim Betreiber des beA nach der Erzeugung der Schlüssel vor der Übergabe an den Auftraggeber an einer Stelle eine Kopie erstellt. **Dann kann das Personal des Betreibers alleine die Nachrichten entschlüsseln.**

Vor diesem Hintergrund besteht zudem die Möglichkeit, dass der **Auftraggeber im Rahmen von Beschlagnahmen von Postfächern gezwungen werden könnte, Nachrichten offenzulegen**. Damit sind rechtliche Fragen verbunden, die im Rahmen dieses Gutachtens nicht beantwortet werden können. Daher wurde diese Möglichkeit auch nicht in die Bewertung der Ausnutzbarkeit einbezogen.

Die Verwahrung der Schlüssel außerhalb der HSM dient der Inbetriebnahme neuer HSM. Diese Praxis ist nicht unüblich und findet z.B. im Bankwesen oft Anwendung. Damit sie für das beA geeignet ist, ist es **erforderlich, dass die beA-Anwender als potentiell vom Bruch der Vertraulichkeit Bedrohte dem Auftraggeber und dem Betreiber des beA ausreichend vertrauen**. Ob dies der Fall ist, kann im Rahmen dieses Gutachtens nicht beurteilt werden. Ist ausreichendes Vertrauen vorhanden, kann die hier aus technischer Sicht (Möglichkeit und Umfang des Schadens) als betriebsbehindernd riskant bewertete Praxis fortgesetzt werden.

(...)

Der Angriff erlaubt die umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten. Die Bedrohung wird daher als hoch eingeschätzt".

Secunet, Technische Analyse und Konzeptprüfung des beA – Abschlussgutachten im Auftrag der Bundesrechtsanwaltskammer Körperschaft des öffentlichen Rechts, Littenstraße 9, 10179 Berlin, Version 1.0, Stand: 18.06.2018, S. 85 f. (**Anlage K26**).

Mit dem Hinweis auf das Gutachten der Secunet erfolgt keine Anerkennung des Gutachtens als geeignete Grundlage zur Beurteilung der Sicherheit des beA. Es handelt sich um ein Parteigutachten mit offenbar eingeschränktem Auftrag, das nur teilweise öffentlich ist.

B) „INSECURITY BY DESIGN“

Es ist auch **unerheblich, ob „nur“ ein Postfachschlüssel umgeschlüsselt** wird (so die Darstellung in der Klageerwiderung vom 12. September 2018, S. 12) oder die Nachricht selbst. Wer in der Lage ist, einen der beA-Server zu kompromittieren, hat **Zugriff auf die verschlüsselte Nachricht und den zur Entschlüsselung notwendigen Schlüssel**. Das ist genau so unsicher wie eine Umschlüsselung der Nachricht selbst. Dies hat **secunet** wie vorstehend zitiert bereits **unmissverständlich festgestellt** (siehe oben bei II.4.a)).
Zudem gilt: Ein System, dessen **„Sicherheit“ maßgeblich abhängig vom Vertrauen seiner Nutzerinnen und Nutzer ist, kann per se nicht als sicher** angesehen werden.

Ein Kommunikationssystem ist gerade **nur dann sicher, wenn die Nutzerinnen und Nutzer nicht auf den Systembetreiber vertrauen müssen!** Und eben dies zu gewährleisten ist Sinn und Zweck der Ende-zu-Ende-Verschlüsselung (siehe ausf. Klageschrift vom 15. Juni 2018, S. 16-23). Bei gesetzlichem Zwang mit Auswirkung auf die informationstechnischen Systeme der Gesamtheit der Rechtsanwälte kann dies nicht genügen. Freiwillige Systeme mögen geringeren Standards entsprechen (z.B. Fax).

C) „SINGLE POINT OF FAILURE” – DAS BEA ALS ZENTRALES EINFALLSTOR ZUM AUSSPÄHEN VERTRAULICHER ANWALTSKORRESPONDENZ

Die von der Beklagten vorgenommene technische Umsetzung des beAs erlaubt secunet zufolge „die **umfassende Aufdeckung des Inhalts aller in beA-Postfächern gespeicherten Nachrichten**“ (secunet, a. a. O., S. 86).

Allein der Umstand, dass dies **nur durch „Innentäter“** soll ausgenutzt werden können, ist dabei ein sehr schwacher – zu schwacher – Trost in Anbetracht des **unermesslichen potentiellen Schadens**. Denn auf dem Spiel steht nicht weniger als ein **heimliches, unbegrenztes Ausspähen sämtlicher anwaltlicher Korrespondenz mit Gerichten**, die – hieran sei in diesem Zusammenhang

nochmals erinnert – **ab dem 01. Januar 2022 verpflichtend über das beA** abzuwickeln sein wird (siehe Klageschrift vom 15. Juni 2018, S. 13). Das Risiko eines Ausspähens ist deshalb jedenfalls im Verhältnis zum drohenden Schaden **für die gesamte Anwaltschaft und die Rechtspflege untragbar**.

D) KEINE DURCHGÄNGIGE VERSCHLÜSSELUNG VON NACHRICHTEN

Die Beklagte trägt vor:

> „Die **Nachricht selbst** wird hingegen – anders als die Kläger vortragen – zu keiner Zeit im HSM oder außerhalb des HSM auf dem Transportweg entschlüsselt. Sie liegt während der gesamten Übertragung bis zur Entschlüsselung durch den berechtigten Empfänger **durchgängig verschlüsselt** vor".
>
> Klageerwiderung vom 12. September 2018, S. 11 f.

Dies ist **falsch** und wird **bestritten**. Die **Beklagte selbst** hat dies bereits **widerlegt**:

> „Nur der begleitende **Nachrichtentext**, welcher für Hinweise an den Empfänger genutzt werden kann, **wird im Klartext mittelbar in die JavaScript-Komponente übermittelt** bzw. mit ihrer Hilfe erzeugt', schreibt Brak-Pressesprecherin Stephanie Beyrich dazu. ‚Die relevanten Schriftsätze gegebenenfalls nebst Anlagen werden im Gegensatz dazu als Anhänge zur Nachricht im beA beigefügt. **Der Schutzbedarf des begleitenden Nachrichtentextes ist hinsichtlich Vertraulichkeit aus fachlicher Sicht als deutlich geringer als der Schutzbedarf der Anhänge einzustufen. Denn die dem Mandatsgeheimnis unterliegenden Inhalte sind in den verschlüsselten Anhängen enthalten**".
>
> Böck, Anwaltspostfach beA – Geheimhaltung von Nachrichten ist nicht so wichtig, Beitrag vom 10. September 2018, golem.de (**Anlage K27**).

Die Auffassung der Beklagten, dass die **über das beA versandten Nachrichten nicht so schützenswert** sein sollen wie Anlagen, ist nicht nachzuvollziehen.

e) Kein Vertrauen in die Beklagte

Schließlich ist nach alledem zu konstatieren, dass die Klägerin und die Kläger **nicht das laut secunet-Gutachten für die Sicherheit des beA-Systems unentbehrliche Vertrauen in die Beklagte** haben.

So hat die Beklagte in der Vergangenheit insbesondere, wie sie selbst einräumen muss (siehe oben bei II.1.d)), **das beA-System bereits in irreführender Weise als Ende-zu-Ende-verschlüsselt** dargestellt und damit den **Sicherheitsstandard nicht transparent und zutreffend wiedergegeben**.

Auch spricht das soeben (siehe oben bei II.4.d)) zitierte **Sicherheitsverständnis zum Schutzniveau auch von beA-Textnachrichten** nicht dafür, dass die Beklagte eine hinreichende Sicherheit des beA-Systems garantieren will bzw. kann.

Insofern ist im Ergebnis festzuhalten, dass die **vermeintliche Sicherheit** des beA-Systems in seiner derzeitigen Ausgestaltung **allein auf ein fiktives Vertrauen in die Beklagte gestützt** wird.

III. Einrichtung des beAs mit Ende-zu-Ende-Verschlüsselung nicht unmöglich

Die Beklagte trägt vor:

> „Dass die Beklagte nicht die herkömmliche Ende-zu-Ende-Verschlüsselung, sondern eine andere Form der Verschlüsselung gewählt hat, ist dadurch begründet, dass sie **auch gewillkürten Vertretern und Mitarbeitern des Rechtsanwalts Zugriff auf die Postfächer einräumen musste**. Dies ergibt sich zunächst aus **§ 31a Abs. 3 Satz 2** BRAO, wonach sie auch Vertretern, Abwicklern und Zustellungsbevollmächtigten die Nutzung des besonderen elektronischen Anwaltspostfachs zu ermöglichen hat. Nach **§ 53 Abs. I BRAO** muss der Rechtsanwalt für seine Vertretung sorgen, wenn er länger als eine Woche daran gehindert ist, seinen Beruf auszuüben bzw. sich länger als eine Woche von seiner Kanzlei entfernen will. Er kann nach **§ 53 Abs. 2 BRAO** seinen Vertreter unter bestimmten Voraussetzungen selbst

> bestellen. So, wie der Rechtsanwalt in der analogen Welt seinem Vertreter die Briefkastenschlüssel aushändigt, muss er in der Lage sein, seinem Vertreter den Zugriff zu seinem besonderen elektronischen Anwaltspostfach zu ermöglichen. Nähere Regelungen enthält **§ 23 RAVPV**. Danach kann der Postfachinhaber weiteren Personen Zugang zu seinem besonderen elektronischen Anwaltspostfach gewähren. Da er aber nach **§ 26 RAVPV** seine PIN nicht weitergeben darf, **muss die Möglichkeit des Zugangs zum Postfach technisch geregelt werden**. Diese Lösung gewährleistet die **Umschlüsselung des Postfachschlüssels auf den privaten Schlüssel der durch den Postfachinhaber zum Lesen der Nachricht berechtigten Person**".
>
> Klageerwiderung vom 12. September 2018, S. 12.

Damit versucht die Beklagte den Eindruck zu erwecken, dass die von ihr gewählte technische Konzeption des beAs die einzig faktisch mögliche sei. Dies wird **bestritten**.

1. SECUNET-GUTACHTEN GEHT VON MACHBARKEIT AUS

Dass die **Behauptung der Beklagten falsch** ist, ist bereits dem von ihr selbst in Auftrag gegebenen secunet-Gutachten zu entnehmen:

> „Das erkennbare Ziel, die **Sicherheit der Nachrichten ausschließlich durch Kryptographie zu schützen, ist aber nicht in vollem Umfang erreicht** worden. An einigen Stellen verlässt sich das beA in seiner dem Gutachten zugrunde liegenden Realisierung auf organisatorisch-physikalischen Schutz wichtiger Systemkomponenten (HSM-Schlüssel, SAFE BRAK), was **bei voller Ausnutzung der kryptographischen Möglichkeiten, die das Konzept und die eingesetzte Technik bieten, nicht notwendig wäre**".
>
> Secunet, a. a. O., S. 11.

Demnach wäre eine **volle Ausnutzung kryptographischer Möglichkeiten machbar** gewesen und hätte **die HSM-Schlüsselverwaltung entbehrlich** gemacht.

2. Keine gesetzliche Vorgabe zur Umschlüsselung durch HSM

Im Übrigen **verlangen die von der Beklagten angeführten Vorschriften keine Umschlüsselung in einem HSM** zum Zwecke der Weiterleitung von Nachrichten an Vertreter.

Weder die **Regelungen zur Vertretungsbefugnis** noch der angestrengte **„Umkehrschluss" aus § 26 RAVPV** können die Behauptung der Beklagten stützen, dass die von ihr gewählte technische Lösung die einzig mögliche sei.

Vielmehr sieht § 31a Absatz 3 Sätze 2 und 3 BRAO lediglich vor:

> „Sie (Anm.: die BRAK) hat auch Vertretern, Abwicklern und Zustellungsbevollmächtigten die Nutzung des besonderen elektronischen Anwaltspostfachs **zu ermöglichen**; Absatz 2 gilt sinngemäß. Die Bundesrechtsanwaltskammer kann unterschiedlich ausgestaltete Zugangsberechtigungen für Kammermitglieder und andere Personen vorsehen".

Wie die BRAK Vertretern, Abwicklern und Zustellungsbevollmächtigten die beA-Nutzung ermöglicht, **lässt die BRAO offen**.

Und **auch in der RAVPV finden sich keine Regelungen**, aus denen sich ergeben sollte, dass sich diese allein durch die von der Beklagten gewählte HSM-Umschlüsselungstechnik umsetzen ließen.
So sieht etwa § 25 Absatz 1 RAVPV zunächst nur vor, dass **Vertreter, Abwickler und Zustellungsbevollmächtigte ein eigenes beA-Postfach** haben sollen und in Absatz 3 Sätze 1 und 2 wird festgelegt, dass diese einen **beschränkten Zugang zum beA-Postfach des Vertretenen** sollen haben dürfen:

> „Wird ein Vertreter oder Abwickler bestellt oder ein Zustellungsbevollmächtigter benannt, so räumt die Bundesrechtsanwaltskammer diesem für die Dauer seiner Bestellung einen auf die Übersicht der eingegangenen Nachrichten **beschränkten Zugang zum besonderen elektronischen Anwaltspostfach der Person ein, für die er bestellt oder benannt wurde**. Dabei müssen für den

> Vertreter, Abwickler oder Zustellungsbevollmächtigten der Absender und der Eingangszeitpunkt der Nachricht einsehbar sein; der Betreff, der Text und die Anhänge der Nachricht dürfen nicht einsehbar sein".

Damit **steht die Regelung einer Umschlüsselung geradezu entgegen**, da sie **keine Umleitung** von Nachrichten vorsieht, sondern stattdessen ausdrücklich vorschreibt, dass der Vertreter (bzw. Abwickler oder Zustellungsbevollmächtigte) lediglich **eingeschränkte Zugriffsrechte auf das Postfach des Vertretenen** erhalten soll, einen **„beschränkten Zugang" i. S. d. § 25 Absatz 1 RAVPV.**

3. ALTERNATIVKONZEPTE

Vor dem Hintergrund der geltenden Regelungen in BRAO und RAVPV sind **mehrere Alternativ-Konzepte denkbar**, die eine Einrichtung des beA-Systems mit einer Ende-zu-Ende-Verschlüsselung, wie von der Klägergemeinschaft begehrt, erlauben.

Dabei ist darauf hinzuweisen, dass **nur die Beklagte weitere technische Möglichkeiten zur Umsetzung einer Ende-zu-Ende-Verschlüsselung des beAs kennen kann**. Mit der **bloßen Behauptung**, das alternative Konzepte zur Ausstattung des beAs mit einer Ende-zu-Ende-Verschlüsselung unter Verzicht auf den Einsatz eines HSM nicht möglich sein sollen, kann sie daher nicht gehört werden.
Des Weiteren ist es nicht die Aufgabe der Klägergemeinschaft, sondern vielmehr die **Obliegenheit der Beklagten, ein rechtskonformes Umsetzungskonzept vorzulegen**, zumal auch nur sie Kenntnis über sämtliche technischen Begebenheiten hat.

A) „ZERTIFIKATE-LÖSUNG“

Als „Zertifikate-Lösung“ soll ein Konzept beschrieben werden, das sich **unmittelbar aus § 23 RAVPV ableiten** lässt und eine einfache Möglichkeit bietet, eine Ende-zu-Ende-Verschlüsselung einzurichten, **die zugleich i. S. d. § 25 Absatz 3 RAVPV einen beschränkten Zugang** von Vertretern, Abwicklern und Zustellungsbevollmächtigten zum beA-Postfach des Vertretenen erlaubt. Insofern stehen die Regelungen in den §§ 23, 25 RAVPV, anders als die Beklagte dies darzustellen sucht (Klageerwiderung vom 12. September 2018, S. 12), einer Ende-zu-Ende-Verschlüsselung nicht entgegen.

§ 23 RAVPV regelt die Möglichkeit, weitere Zugangsberechtigungen zum Postfach zu erteilen, wie folgt:

> „(1) Der **Postfachinhaber kann** mit einem auf einer Hardwarekomponente gespeicherten Zertifikat **weitere ihm zugeordnete Zertifikate berechtigen**, ihm Zugang zu seinem besonderen elektronischen Anwaltspostfach zu gewähren. Diese Zertifikate **müssen nicht auf einer Hardwarekomponente gespeichert sein**. Zu ihnen muss jedoch ebenfalls eine **Zertifikats-PIN** gehören. Zudem müssen sie von einem von der Bundesrechtsanwaltskammer anerkannten Zertifizierungsdiensteanbieter authentifiziert sein.
> (2) **Der Postfachinhaber kann auch anderen Personen Zugang zu seinem besonderen elektronischen Anwaltspostfach gewähren.** Verfügen die anderen Personen nicht über ein eigenes besonderes elektronisches Anwaltspostfach, hat der Postfachinhaber für sie ein **Zugangskonto** anzulegen. Der Zugang der anderen Personen über ihr Zugangskonto erfolgt unter Verwendung eines ihnen zugeordneten Zertifikats und einer zugehörigen Zertifikats-PIN. Der Postfachinhaber kann hierzu mit einem auf einer Hardwarekomponente gespeicherten Zertifikat weitere Zertifikate berechtigen, anderen Personen Zugang zu seinem Postfach zu gewähren. Für diese Zertifikate gilt Absatz 1 Satz 2 bis 4 entsprechend.
> (3) Der Postfachinhaber kann, wenn er mit einem auf einer Hardwarekomponente gespeicherten Zertifikat angemeldet ist, **anderen Personen unterschiedlich weit reichende Zugangsberechtigungen zu seinem besonderen elektronischen Anwaltspostfach erteilen.** Er kann anderen Personen, deren Zertifikat auf einer Hardwarekomponente gespeichert ist, auch die Befugnis einräumen, weitere Zugangsberechtigungen zu erteilen. Für die Erteilung weiterer Zugangsberechtigungen durch entsprechend ermächtigte andere Personen gelten die Absätze 1 und 2 entsprechend. Der Postfachinhaber kann anderen Personen zudem die Befugnis einräumen, Nachrichten zu

> versenden. Das Recht, nicht-qualifiziert elektronisch signierte Dokumente auf einem sicheren Übermittlungsweg zu versenden, kann er jedoch nicht auf andere Personen übertragen.
> (4) Der Postfachinhaber und die von ihm entsprechend ermächtigten anderen Personen können **erteilte Zugangsberechtigungen jederzeit ändern und widerrufen**".

Damit besteht die Möglichkeit, dass der Empfänger verschiedenen Personen unterschiedlich weit reichende und damit auch i. S. v. § 25 Absatz 3 RAVPV beschränkte Zugriffsrechte auf sein Postfach einräumen kann.

Nachrichten könnten an das Postfach des Empfänger ohne Weiteres Ende-zu-Ende-verschlüsselt gesandt werden und die vom Betroffenen als Vertreter, Abwickler oder Zustellungsbevollmächtigter ermächtigte Person könnte **auf die eingegangenen Nachrichten entsprechend eingeschränkt zugreifen**. Die Information der vertretungsberechtigten Person über den Eingang neuer Nachrichten könnte per einfacher E-Mail erfolgen, so wie es im beA-System bereits jetzt zur Information des Postfachinhabers vorgesehen ist.

Schon dieses – **in der RAVPV ausdrücklich vorgesehene Verfahren – macht jede Form der Umschlüsselung obsolet**.

Die **Beklagte hat dieses Verfahren auch bereits implementiert** und schlüsselt dennoch um. Das beA verfügt schon jetzt über ein diversifiziertes **Rechteverwaltungssystem**. So können etwa Mitarbeitern und Kollegen bestimmte Zugriffsbefugnisse auf das eigene beA-Postfach eingeräumt werden. Hierzu gehört insbesondere auch das „**Recht 01 – Nachrichtenübersicht öffnen**", das wie folgt definiert ist:

> „Der Benutzer mit diesem Recht kann den Dialog Nachrichtenübersicht öffnen und sich hier die **Nachrichten in dem jeweiligen Postfach anzeigen lassen, diese nicht aber lesen**. Es handelt sich hierbei um ein festes Recht, das jedem Benutzer, der einem Postfach als Mitarbeiter zugeordnet wird, automatisch erteilt wird.
>
> Das Recht **berechtigt den Benutzer nicht, den Text in der Betreffzeile einer Nachricht zu lesen**. Die Spalte Betreff in der Liste der Nachrichten in einem Postfach bleibt daher immer leer, solange der Benutzer (noch)

nicht über das Recht 06 - Nachricht öffnen oder 11 - Nachricht (persönlich/vertraulich) öffnen verfügt".

BRAK, beA-Anwenderhilfe, Release 2.1, Liste der Rechte (**Anlage K28**).

Demnach entspricht das „Recht 01" dem **beschränkten Zugang** i. S. d. § 25 Absatz 3 RAVPV. Darüber hinaus ist es selbstverständlich auch möglich, weitergehende Rechte zu vergeben, etwa das „Recht 06 – Nachricht öffnen", welches das Lesen von Nachrichten ermöglicht.

Will ein Rechtsanwalt einem Dritten beschränkten oder auch vollen Zugriff auf sein beA-Postfach gewähren, so kann er sich hierfür neben seiner eigenen eine **weitere beA-Karte ausstellen** lassen, die so konfiguriert ist, dass sie **nur den vom Rechtsanwalt bestimmten Zugriff auf sein Postfach erlaubt**. Diese Karte kann er sodann **dem Dritten aushändigen**, wobei er jederzeit berechtigt ist, der beA-Karte und damit ihrem Nutzer die Rechte wieder zu entziehen. Das beA kann dann automatisch und überprüfbar – **ohne zwischengeschaltetes HSM – auf alle beA-Karten des Rechtsanwalts Ende-zu-Ende-verschlüsseln**, also sowohl auf seine eigene wie auch eine weitere beA-Karte mit beschränkten oder auch vollen Zugriffsrechten, die er an einen Dritten weitergegeben hat.

Im Ergebnis könnten bei dem durch die Klägergemeinschaft aufgezeigten Vorgehen **Nachrichten an den gewünschten Empfänger ohne Weiteres an dessen Postfach Ende-zu-Ende-verschlüsselt gesandt** werden und die vom Postfachinhaber ermächtigte Person könnte **auf die eingegangenen Nachrichten entsprechend eingeschränkt (§ 25 RAVPV) oder mit Leseberechtigung (§ 23 RAVPV) zugreifen**.

Insgesamt bietet dieses Verfahren den Vorteil, dass der **Postfachinhaber selbst – anstelle eines HSM – entscheidet und veranlasst**, wem er für welchen Zeitraum welche Zugriffsrechte verleiht. Dies macht ein **Vertrauen in nicht nachvollziehbare automatisierte technische Vorgänge in einem HSM entbehrlich**.

Im Gegensatz zu dieser einfachen Umsetzung implementierte die Beklagte durch den Einsatz des HSM rechtswidrig die Möglichkeit des Mitlesens durch nicht vom Rechtsanwalt befugte Dritte. Denn das **beA verschlüsselt in seiner derzeitigen Konzeption nicht Ende-zu-Ende, sondern nachträglich und außerhalb der Sphäre des Rechtsanwalts für diesen unkontrollierbar auf Dritte**. Dadurch können letztlich nur die Beklagte (und ihr Dienstleister) sicher wissen, auf wen verschlüsselt wird. Die Vorgehensweise der **nachträglichen Umschlüsselung** hat zur Folge, dass – völlig ohne Not – der Beklagten als „Postbotin" vertraut werden muss.

Hingegen bildet das hier vorgestellte Verfahren auch die bislang geübte **„analoge" Praxis** ab: **Allein der Rechtsanwalt – und nicht die Bundesrechtsanwaltskammer – entscheidet, wem der Rechtsanwalt welche Vertretungsrechte einräumt**. Der **Gesetzgeber hat der Beklagten denn auch lediglich die Rolle einer „Postbotin" zugeteilt**, indem er ihr den Betrieb des beAs auferlegt hat, **ohne sie dabei mit weitergehenden Kompetenzen zur Lenkung und Überwachung des Nachrichtenflusses auszustatten**. Die Beklagte hat sich vielmehr mit der Konzeption der jetzigen beA-Struktur **selbst Kompetenzen einräumt, die ihr in der realen Welt – zu Recht – bislang nicht zukamen**.

B) Weitere Alternativkonzepte

Weitere konkrete Konzepte für eine Konzeption des beAs ohne HSM hat auch bereits Professor Dr. Frederik Armknecht beim **Symposium „Brauchen wir das beA+ mit besserer Software und optimierter Ausrichtung auf den Kanzleialltag?" des Deutschen EDV-Gerichtstages** vom 05. März 2018 vorgelegt, an dem u.a. mit Dr. Abend ein Vizepräsident der Beklagten als Redner teilnahm.

> Armknecht, Kryptografische Alternativen zum Hardware Security Module (HSM), 08.03.2018 (**Anlage K29**).

Beweisangebot:

Sachverständigenanhörung des Herrn Professor Dr. Frederik Armknecht, zu laden über

Universität Mannheim
Lehrstuhl Praktische Informatik IV: Dependable Systems Engineering
68131 Mannheim

4. Hilfsweise: Rechtswidrigkeit von Vorschriften der RAVPV, die einer Ende-zu-Ende-Verschlüsselung entgegenstehen könnten - Normverwerfungskompetenz des Anwaltsgerichtshofes

Sollte – entgegen der hier vertretenen Ansicht – eine Vorschrift der RAVPV der Einrichtung des beAs mit Ende-zu-Ende-Verschlüsselung entgegenstehen, so **verstieße sie gegen das gesetzliche Gebot eines sicheren elektronischen Übermittlungsweges** gemäß § 31a Absatz 1 BRAO i. V. m. § 174 Absatz 3 Sätze 3 und 4 i. V. m. § 130a Absatz 4 Nr. 2 ZPO und wäre im Übrigen **unvereinbar mit der verfassungsrechtlich geschützten Freiheit der Advokatur**, deren rechtsstaatliches Fundament die **anwaltliche Verschwiegenheitspflicht zum Schutze des Mandantengeheimnisses** ist.

Die Sicherheit des elektronischen Rechtsverkehrs zur **Gewährleistung anwaltlicher Verschwiegenheit** und damit zur Wahrung des Mandantengeheimnisses **wiegt schwerer als etwa eine rein formalistische Vertretungsregelung**.

Sollte der **Senat** der Ansicht sein, dass eine bestimmte Regelung in der RAVPV der von der Klägergemeinschaft geforderten Ende-zu-Ende-Verschlüsselung des beAs entgegenstehen sollte, so wird um entsprechenden **richterlichen Hinweis** gebeten.

Dabei wird vorsorglich darauf aufmerksam gemacht, dass das **Gericht die Normverwerfungskompetenz inne hat**, rechtswidrige Vorschriften der RAVPV für ungültig zu erklären.

Vgl. zur Normverwerfungskompetenz bezüglich Vorschriften in Rechtsverordnungen im Rahmen von verwaltungsgerichtlichen Verfahren BVerwGE 111, 276; BVerfGE 115, 81.

Zwei Abschriften anbei.

Baum
Rechtsanwalt