

**Antrag zu TOP 6 der Versammlung der RAK Sachsen am 23.03.2018  
gemäß § 8 Nr. 7 Geschäftsordnung der RAK Sachsen**

Die bisher bekannten Sicherheitsdefizite beim Betrieb des beA sowie zunächst die verspätete Inbetriebnahme im Jahr 2016 und sodann die Außerbetriebnahme im Dezember 2017, erfordern eine gründliche und kritische Auseinandersetzung mit den bisherigen Abläufen.

Dies bezieht sich insbesondere auf die **Vergabe und Betreuung der Aufträge**, vor allem hinsichtlich der Überprüfung der Sicherheit des beA und der Vorkehrungen, die Auftragnehmer in Regress nehmen zu können.

Die Aufarbeitung der Fehler ist bei vollständiger personeller Identität der beteiligten Personen in der BRAK nicht gewährleistet.

Sie dokumentierten dies bereits selbst, als sie unsere Kammer-Beiträge auch verwendeten, um ein Kommunikationsbüro (Johanssen + Kretschmer) einzuschalten. Man muss es sich auf der Zunge zergehen lassen: Rechtsanwälte, die ein Kommunikationsbüro für ihre Kommunikation, normalerweise eine Kernkompetenz in der anwaltlichen Tätigkeit, benötigen!

Hinzu tritt, dass die BRAK bisher nicht oder nur mangelhaft die Kammern über die Abläufe informiert hat. Zudem soll das HSM nach den aktuellen Verlautbarungen der BRAK als vermeintlich sicherer Baustein auch zur Wiederinbetriebnahme erhalten bleiben.

Ich beantrage:

**Die Kammerversammlung der Rechtsanwaltskammer Sachsen spricht dem Präsidenten der BRAK, Herrn Kollegen Ekkehard Schäfer, und den bei der BRAK für die Einführung des beA zuständigen Vizepräsidenten der BRAK, Herrn Kollegen Dr. Martin Abend, ihr Misstrauen aus.**

**Die Kammerversammlung fordert den Vorstand der Rechtsanwaltskammer Sachsen auf, auf den Rücktritt der Kollegen Schäfer und Dr. Abend hinzuwirken.**

Anlass für den Antrag ist das Vorwort von Herrn Koll. Schäfer in den BRAK Nachrichten sowie das damit einhergehende Interview mit dem Kollegen Dr. Abend im zugehörigen Magazin.

Beides hat bei mir die Gewissheit erzeugt, dass die Lösung des Problems "beA" mit den beiden Herren nicht zu erwarten ist und der gleichlautende Beschluss der RAK Berlin gibt mir Hoffnung, nicht allein zu sein mit dieser Meinung.

Untermauert hat die BRAK meine Überzeugung mit ihrer Stellungnahme zu einer Anfrage der Vorsitzenden der ARGE IT-Recht im DAV, Frau Kollegin Dr. Astrid Auer-Reinsdorff, vom 16.03.2013, unterzeichnet durch Herrn Kollegen Schäfer (abgedruckt bei der RAK Hamburg)<sup>1</sup>.

Ursprünglich hatte die Bundesrechtsanwaltskammer das beA damit beworben, dass es mit einer Ende-zu-Ende-Verschlüsselung ausgestattet sei. Doch das stimmte nicht, wie sich später herausstellte. Die Nachrichten beim beA werden nicht mit dem Schlüssel des Empfängers verschlüsselt, sondern mit einem Postfachschlüssel. Anschließend werden die Nachrichten in einem sogenannten Hardware Security Module (HSM) "umgeschlüsselt". Das heißt, sie werden erst hier mit dem eigentlichen öffentlichen Schlüssel des Empfängers verschlüsselt.

Hier von einer Ende-zu-Ende-Verschlüsselung zu sprechen, ist selbstverständlich absurd und auch die BRAK, die diesen Begriff jahrelang nutzte, tut dies inzwischen nicht mehr und versucht uns mit

---

<sup>1</sup> [http://www.rak-hamburg.de/uploads/file/Mitglieder/Mitgliederservice/Kammerschnellbriefe/2018/M%C3%A4rz%202018/2018\\_03\\_16%20DAV%20Dr.%20Auer-Reinsdorff%20ARGE%20IT-Recht.pdf](http://www.rak-hamburg.de/uploads/file/Mitglieder/Mitgliederservice/Kammerschnellbriefe/2018/M%C3%A4rz%202018/2018_03_16%20DAV%20Dr.%20Auer-Reinsdorff%20ARGE%20IT-Recht.pdf)

dem Begriff der „durchgehenden Verschlüsselung“ zu beruhigen.

Herr Kollege Dr. Schäfer schreibt in seinem Brief an die ARGE IT-Recht dazu:

*„Kein Nutzer hat im normalen Betrieb des HSM Zugriff auf Schlüsselmaterial. Die Schutzmechanismen des HSM stellen sicher, dass kein Anwender im Falle eines Angriffs auf das HSM (etwa das gewaltsame Öffnen und der Versuch des Auslesens des Speichers) Zugriff auf das Klartext-Schlüsselmaterial erhalten kann. Über das beA versandte und empfangene Nachrichten sind durchgängig verschlüsselt. ... Niemand außer dem vorgesehenen Empfänger (oder einer von diesem berechtigten Person) kann von dem Inhalt der Nachricht Kenntnis nehmen. ... Der Versuch, ein HSM-Modul physisch zu öffnen, führt zur kompletten Löschung der im Modul gespeicherten Daten.“*

um danach, neben einer Umschreibung der physischen Sicherheitshürden in den Gebäuden von Atos jedoch weiter zu erläutern:

*„Um bei einer Wartung eine Betriebsunterbrechung zu vermeiden, werden dabei erst neue Geräte vor Ort gebracht, in das System eingebunden und synchronisiert, danach die alten Geräte herausgenommen und an Atos Worldline zurückgeschickt.“*

Wer uns solches schreibt und gleichzeitig von Sicherheit spricht, hat in seinem Leben scheinbar noch keinen bösen Menschen kennengelernt und keine Zeitung gelesen.

Selbst wenn ich davon ausgehen darf, dass im Regelfall nichts an Daten abgegriffen wird, scheinen diese Herren der BRAK jegliche Augen vor menschlichem Fehlverhalten, Geheimdienstaktivitäten etc. zu verschließen.

Der letzte Satz zeigt doch eindeutig, dass ein Auslesen des HSM durch Synchronisation und damit ein Angriff auf unsere vertrauliche und durch das Berufsgeheimnis vorgeschriebene, geschützte Kommunikation sehr wohl möglich und vorstellbar ist!

Nicht wir als Absender, sondern ein Server der BRAK steuert, wer unsere Nachrichten letztlich lesen kann. Sollen demnächst nicht nur Steuer-CDs aus der Schweiz, sondern auch Postfachschlüssel aus der deutschen Anwaltschaft auf dem freien Markt gehandelt werden können!?

Dass es Möglichkeiten einer echten und kostengünstigen Ende-zu-Ende-Verschlüsselung (E2EE) gibt, haben bereits mehrere Autoren skizziert.<sup>2</sup>

Gleichwohl halten die Herren der BRAK an der bisherigen Architektur fest, weil sie –was ich ihnen unterstelle- bei der Vertragsgestaltung nicht aufgepasst und Sorge um Schadenersatzansprüche haben. BER lässt grüßen!

Ich begrüße und unterstütze die zwischenzeitlich ins Leben gerufene Aktion von einigen Kolleginnen und Kollegen unter dem Titel „beA - aber sicher!“, die unter Beteiligung des Gesellschaft für Freiheitsrechte e.V. (GFF) planen, Klage für eine echte Ende-zu-Ende-Verschlüsselung zu erheben.<sup>3</sup>

Dass wir alle mit dem Kammerbeitrag auch weiterhin für ein derzeit funktionsuntüchtiges beA und (soweit rechtzeitig bestellt) spätestens seit Dezember Jahresgebühren für nutzlose beA-Karten zahlen, muss sicher nicht besonders erwähnt werden.

Danke für Ihre Aufmerksamkeit!

RA Herbert Posner, Plauen, Mitglieds-Nr.: 113056

---

<sup>2</sup> <https://www.golem.de/news/anwaltspostfach-die-unnoetige-ende-zu-mitte-verschluesselung-von-bea-1801-132394.html>

<sup>3</sup> <https://www.bea-aber-sicher.de/sicheres-bea/>