www.jusletter-it.eu

Dominik Leibenger / Ronald Petrlic / Christoph Sorge / Stephanie Vogelgesang

Elektronische Akten: Anforderungen und technische Lösungsmöglichkeiten

Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten («ERV-Gesetz» oder auch «E-Justice-Gesetz») wird der elektronische Rechtsverkehr ab 1. Januar 2022 in Deutschland einziger zugelassener Kommunikationsweg für Anwälte, Behördenvertreter und Vertreter öffentlicher Körperschaften. Für die Justiz bedeutet dies unter anderem die flächendeckende Einführung der elektronischen Akte. Ziel dieses Artikels ist, die Anforderungen an elektronische Akten für den Zivilprozess aus juristischer und technischer Sicht zu beleuchten. Anhand eines beispielhaften Prozesses werden die Rechtsgrundlagen erläutert und technische Anforderungen abgeleitet. Ausgehend davon wird untersucht, welche Verfahren aus der IT die jeweiligen Ziele erreichen können.

Collection: Conference Proceedings IRIS 2015; Top 10 – Peer Reviewed Jury LexisNexis Best Paper Award of IRIS2015
Category: Articles
Field of law: E-Justice
Region: Germany

Citation: Dominik Leibenger / Ronald Petrlic / Christoph Sorge / Stephanie Vogelgesang, Elektronische Akten: Anforderungen und technische Lösungsmöglichkeiten, in: Jusletter IT 26. Februar 2015 – IRIS

Inhaltsübersicht

1 Einleitung

[Rz 1] «Die Prozessakten können elektronisch geführt werden» heißt es in § 298a Abs. 1 ZPO. Damit ist bereits seit April 2005 die gesetzliche Grundlage für die elektronische Aktenführung im Zivilprozess geschaffen.[1] Weite Verbreitung fand sie bislang jedoch nicht. Mit dem Ziel, die Verwaltung zu modernisieren und Ressourcen zu schonen, wurde zum 25. Juli 2013 das Gesetz zur Förderung der elektronischen Verwaltung — das E-Government-Gesetz (EGovG) — eingeführt (BGBl. I S. 2749 ff.). Unter anderem verpflichtet es Behörden des Bundes, der Länder und der Kommunen — eine qualifizierte elektronische Signatur vorausgesetzt — seit Juli 2014 zur Entgegennahme elektronischer Dokumente (§ 2 Abs. 1 EGovG). Bis dato sind Gerichte hiervon aber teilweise ausgenommen: Nach § 1 Abs. 5 S. 1 EGovG gilt das Gesetz nicht für «die Strafverfolgung [und] die Verfolgung und Ahndung von Ordnungswidrigkeiten»; § 1 Abs. 3 EGovG macht zusätzliche Einschränkungen für «die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung».

[Rz 2] Mit dem am 10. Oktober 2013 verabschiedeten Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten (BGBl. I S. 3786) — dem ERV-Gesetz — sollen die Modernisierungspläne nun auch die Gerichte erreichen. § 130a ZPO verpflichtet sie ab Januar 2018 (in Zivilprozessen), elektronische Dokumente entgegenzunehmen. Zu diesem Termin besteht indes noch keine Verpflichtung zur elektronischen Aktenführung: Elektronisch eingereichte Dokumente können in ausgedruckter Form[2] in die Akte übernommen werden (§ 298 ZPO). Dies ändert sich ab Januar 2022 mit Inkrafttreten des § 130d ZPO, der Rechtsanwälten und Behörden die Nutzung elektronischer Dokumente für «[v]orbereitende Schriftsätze und deren Anlagen sowie schriftlich einzureichende Anträge und Erklärungen» vorschreibt. Die Einführung der elektronischen Zivilprozessakte bis 2022 ist damit unabdingbar, ihre technische und praktische Umsetzung jedoch bislang weitgehend ungeklärt.

[Rz 3] Hier knüpft der vorliegende Artikel an. Um eine Grundlage für die praktische Einführung der elektronischen Zivilprozessakte in Deutschland zu schaffen, erarbeiten wir konkrete technische Anforderungen und Lösungsmöglichkeiten. Hierzu betrachten wir beispielhaft ein vergleichbares Projekt — den im Januar 2014 in Österreich eingeführten elektronischen Akt (ELAK) — und arbeiten Detailprobleme dieses Projekts heraus. Außerdem betrachten wir die derzeitige Verwendung und Entwicklung von Prozessakten in deutschen Zivilrechtsverfahren und leiten auf dieser Basis technische Anforderungen an eine elektronische Umsetzung dieser Prozesse und

[1] Eingefügt wurde der Paragraf durch das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz vom 22. März 2005 (BGBl. I S. 837).

[2] Selbstverständlich muss die Signatur zuvor geprüft und das Ergebnis nach § 298 Abs. 3 präzise dokumentiert werden.

dazu passende Technologien ab.

2 Bestehende Lösungen: Der elektronische Akt (ELAK)

[Rz 4] Der *elektronische Akt (ELAK)* hat in Österreich Anfang Januar 2014 den Papier-Akt in den Zentralstellen der Bundesministerien weitgehend abgelöst. Die Einführung von ELAK ist im Kontext der E-Government-Offensive zu sehen, auf deren Grundlage weitere Anwendungen im E-Government entwickelt werden sollen. Das Funktionsmodell des ELAK-Konzepts ist in den Dokumenten zu den *Funktionsanforderungen* und dem *Leistungsverzeichnis* näher spezifiziert[3], die auch Grundlage für unsere Diskussion im vorliegenden Beitrag sind. Die technische Umsetzung von ELAK basiert auf XML. Das Bundesrechenzentrum als Betreiber der Server und Anwendungen spricht im Jahr 2013 von einer Verwendung von ELAK (konkret der eGov-Suite v2012 von Fabasoft) durch 10.200 Benutzer und einem Datenvolumen der Dokumente von 18 TB.[4] Als Vorteile von ELAK werden unter Anderem genannt: Lückenlose Nachvollziehbarkeit der Bearbeitung auf Grund der Versionierung, Reduzierung von Arbeitsschritten durch Automatisierung (automatische Versionserstellung), elektronische Übermittlung von Schriftstücken durch Bürger/innen und Schutz vor unbefugtem Zugriff.

[Rz 5] Wir werden in diesem Beitrag näher auf die oben genannten Aspekte der Versionsverwaltung und den Schutz vor unbefugtem Zugriff eingehen, da sie aus unserer Sicht zentrale Anforderungen an die elektronische Akte insbesondere im Zivilprozess darstellen. Bei einer nicht ordnungsgemäßen Konzeption und Implementierung der Versionsverwaltung können Datenschutz-Probleme entstehen: Wenn für jeden zugriffsberechtigten Nutzer der Akte genau einsehbar ist, wer zu welchem Zeitpunkt Informationen in der Akte geändert hat, kann damit das Arbeitsverhalten von Nutzern beobachtet werden. Diese Form der Überwachung könnte zu Bedenken und Akzeptanzproblemen bei Richter/innen führen, weil sie in die richterliche Unabhängigkeit eingreift.[5] Auf diese Problematik wird im ELAK-Konzept nicht eingegangen. Hinsichtlich Sicherheit finden sich im ELAK-Konzept Anforderungen, die aus unserer Sicht z.T. nicht sinnvoll sind bzw. nicht mehr den Stand der Technik widerspiegeln. So wird in der Funktionsbeschreibung[6] aufgeführt, dass Dokumente auf Basis des Signaturgesetzes verschlüsselt werden, ohne dass Verschlüsselung Gegenstand im Signaturgesetz[7] ist. Das Leistungsverzeichnis geht weiter ins Detail und erwähnt eine Verschlüsselung «mit der asymmetrischen Methodik mit einer Mindestschlüssellänge von 128 Bit». Diese Formulierung suggeriert, dass ganze Dokumente asymmetrisch verschlüsselt werden sollen, was bei größeren Dokumenten — die in elektronischen Akten zu erwarten sind — aus Performanz-Überlegungen nicht sinnvoll ist. Hier wäre der Einsatz hybrider Verschlüsselung

---

3 Bundeskanzleramt: ELAK-Konzept Teil A — Funktionsbeschreibung (Version 1.1 vom 30. November 2001). http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19396 / Bundeskanzleramt: ELAK-Konzept Teil B — Leistungsverzeichnis (Version 1.1 vom 30. November 2001). http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19397.

4 Bundesrechenzentrum: ELAK im Bund. https://www.brz.gv.at/leistungen_services/projekte/2013-10-30-ELAK-im-Bund-Factsheet.pdf?4jwluq.

5 So auch (auf deutsches Recht bezogen) Berlit: Richterliche Unabhängigkeit und elektronische Akte, JurPC Web-Dok. 77/2012, http://www.jurpc.de/jurpc/show?id=20120077, Abs. 38—41. Wie auch Berlit feststellt, führt das Problem nicht zu einer Unzulässigkeit elektronischer Akten, sondern zum Erfordernis entsprechender Schutzmaßnahmen.

6 In Abschnitt 1.3.1.10 «Verschlüsselung von Dokumenten».

7 Bundesgesetz über elektronische Signaturen (Signaturgesetz), BGBl. I Nr. 190/1999 i.d.F. BGBl. I Nr. 59/2008 (VFB).

zu empfehlen. Des Weiteren ist eine Mindestschlüssellänge von 128 Bit bei asymmetrischen Verschlüsselungsverfahren seit vielen Jahren viel zu kurz. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI)[8] empfiehlt bspw. für RSA für langfristige Sicherheitsanwendungen nach 2015 eine Modul-Länge von 3000 Bit. Darüber hinaus wird im Leistungsverzeichnis aufgeführt: «Wahlweise muss die Verschlüsselung auf der Basis von digitalen Zertifikaten der digitalen Signatur erfolgen können». Diese Anforderung birgt die Gefahr einer falschen Umsetzung. Dasselbe Schlüsselpaar darf aus Sicherheitsgründen nie für Signaturerzeugung *und* Verschlüsselung verwendet werden. Überdies wird in der Funktionsbeschreibung gefordert, dass neben der Verschlüsselung auch eine Komprimierung von Dokumenten zu erfolgen hat. Dem Leistungsverzeichnis ist folgender Ablauf bei ELAK zu entnehmen: Erst Signatur, dann Komprimierung, anschließend Verschlüsselung der komprimierten Daten. Es sei darauf hingewiesen, dass durch die vorherige Kompression wichtige kryptographische Sicherheits-Anforderungen[9] verletzt werden: Die Länge des resultierenden Chiffretextes weist auf den Grad der Komprimierbarkeit des unverschlüsselten Dokuments hin und liefert damit in geringem Umfang Informationen über den Klartext. Dies ist insbesondere problematisch, wenn durch Versionierung mehrere Versionen des gleichen Dokuments vorliegen oder dessen Größe aus anderen Gründen (z.B. weil es ein ausgefülltes Formular ist) bekannt ist. Eine Komprimierung nach Verschlüsselung ist keine Alternative, da Chiffretexte aufgrund ihrer hohen Entropie kaum komprimierbar sind. Das Leistungsverzeichnis geht davon aus, dass der Bearbeiter eines elektronischen Akts *wahlweise* einzelne Dokumente oder ganze Geschäftsfälle digital signieren kann. Wie wir in Abschnitt 4 herausarbeiten werden, besteht hier bei der E-Akte im Zivilprozess keine Wahl. Unabhängig von der konkreten technischen Lösung muss immer die Authentizität sowohl einzelner Dokumente als auch der gesamten E-Akte sichergestellt werden, um zu verhindern, dass (signierte) Dokumente unbemerkt aus der Akte entnommen werden können.

3 Zivilprozessakte

[Rz 6] Anhand eines typischen[10] Ablaufs im Zivilprozess vor dem Amtsgericht stellen wir nun abstrakt dar, welche Schritte eine Akte in einem Prozess durchläuft. Im ersten Schritt bringt der Kläger (bzw. dessen Anwalt) seine Klage in Schriftform beim Amtsgericht ein. Die Klage geht in der Geschäftsstelle des Gerichts ein; dort wird eine neue Akte angelegt und die Klage wird — nachdem der Eingangszeitpunkt vermerkt und das Dokument nummeriert[11] wird — in diese aufgenommen. Die Geschäftsstelle vergibt ein Aktenzeichen und leitet die Akte an den (laut Geschäftsverteilungsplan zuständigen) Richter weiter. Sofern dieser seine Zuständigkeit geprüft und bejaht hat, leitet er im nächsten Schritt normalerweise ein schriftliches Vorverfahren (§ 276 ZPO) ein[12], das der Vorbereitung der mündlichen Verhandlung dient. Die Akte geht zusammen

8 BSI TR-02102-1 «Kryptographische Verfahren: Empfehlungen und Schlüssellängen». Version 2014.01.

9 Z.B. IND-CPA-Sicherheit; zu praktischen Angriffen s. Kelsey, Compression and information leakage of plaintext. In: Daemen/Rijmen (Hrsg.), Fast Software Encryption, LNCS Bd. 2365, Springer, Berlin, S. 263—276 (2002).

10 Die Nichteinzahlung des Gerichtskostenvorschusses, das Nachreichen von Schriftstücken, das Nicht-Antworten eines Beklagten, und weitere Sonderfälle — zum Beispiel Notwendigkeit einer Beweisaufnahme, Zurückverweisung der Sache durch das Berufungsgericht an das Amtsgericht — werden aus Platzgründen hier nicht weiter betrachtet.

11 Jedes der Akte hinzugefügte Dokument wird von der Geschäftsstelle durchnummeriert.

12 § 272 Abs. 2 ZPO ermöglicht alternativ die Bestimmung eines frühen ersten Termins (§ 275 ZPO).

mit dem vom Richter unterschriebenen Formular zur Einleitung des schriftlichen Vorverfahrens zur Geschäftsstelle, die die Klageschrift an den Beklagten (bzw. dessen Anwalt) übermittelt. Dieser hat nun — mit Zustellung der Klageschrift — zwei Wochen Zeit, um eine Verteidigungsanzeige bei Gericht einzubringen und mindestens zwei weitere Wochen zur schriftlichen Klageerwiderung. Im Falle einer fristgerecht bei Gericht eingegangenen Verteidigungsanzeige vermerkt die Geschäftsstelle das Eingangsdatum auf dem Schriftstück und legt die Akte, mitsamt der Verteidigungsanzeige, erneut dem Richter vor. Dieser leitet nun das Hauptverfahren ein, wofür er einen Verhandlungstermin terminiert. Das entsprechende unterschriebene Formular geht zusammen mit der Akte zurück an die Geschäftsstelle. Diese wiederum versendet eine Ladung nebst schriftlicher Klagerwiderung an den Kläger und eine Ladung an den Beklagten. Vor dem Verhandlungstermin legt die Geschäftsstelle dem Richter die Akte erneut vor. Nachdem der Richter das Urteil verfasst und unterschrieben hat, retourniert er sie mit dem Urteil zur Geschäftsstelle. Geht keine der beiden Parteien in Berufung, wird die Akte von der Geschäftsstelle an das Archiv überstellt. Wird hingegen Berufung eingelegt, so wird die Akte zur nächsthöheren Instanz (dem Landgericht) übermittelt. Sobald ein Urteil von einer der nächsthöheren Instanzen vorliegt, wird die Akte wieder ans Amtsgericht übermittelt und dort ins Archiv überstellt.

4 Anforderungen

[Rz 7] Um technische Anforderungen herzuleiten, ist zunächst klarzustellen, was eine (E-)Akte eigentlich ist. Die ZPO definiert den Begriff der Akte nicht, sondern setzt ihn voraus. Das Organisationskonzept elektronische Verwaltungsarbeit des Bundesministeriums des Innern (BMI)[13] definiert eine elektronische Akte als «eine logische Zusammenfassung sachlich zusammengehöriger oder verfahrensgleicher Vorgänge und/oder Dokumente»[14]. Neben Dokumenten enthält eine elektronische Akte (die Inhalte beschreibende) Metadaten, die dokumentbezogen sein oder für die ganze Akte gelten können. Der Fokus unserer Betrachtung liegt auf der Akte als logische Zusammenfassung (nur) von *Dokumenten* und zugehörigen *Metadaten*: Eine Zwischenebene zwischen Akte und einzelnem Dokument — etwa, wenn ein Text und zugehörige Bilder als separate Dokumente, aber im gleichen Vorgang übermittelt werden — kann zwar sinnvoll sein, lässt sich aber auf Ebene der Metadaten abbilden.

[Rz 8] Im Folgenden ist also zu unterscheiden zwischen Anforderungen an einzelne Dokumente und Anforderungen an die Akte als Ganzes. Auf abstrakter Ebene können die klassischen Schutzziele der IT-Sicherheit herangezogen und für den Anwendungsfall der Zivilprozessakte konkretisiert werden:

[Rz 9] *Vertraulichkeit*: Wer nicht dazu berechtigt ist, soll nicht auf Informationen zugreifen können. Dies betrifft nicht nur die einzelnen Dokumente; allein das Wissen, *welche* Dokumente überhaupt in der Akte enthalten sind, kann sich zum Nachteil der Betroffenen auswirken. Der Begriff der *Berechtigung* deutet auf ein weiteres Problem hin: Berechtigungen können sich für einzelne Aktenbestandteile unterscheiden — etwa, wenn sich in der Akte ein Antrag auf Gewährung von Prozesskostenhilfe befindet[15]. Berechtigungen können sich außerdem ändern — etwa durch das

[13] BMI, Organisationskonzept elektronische Verwaltungsarbeit: Baustein E-Akte, Berlin (2012), Abschnitt 2.1.

[14] Die weiteren, hier nicht zitierten Aspekte der Definition betreffen die Inhalte der Akte, die hier nicht relevant sind.

[15] Ein solcher Antrag enthält Informationen über die wirtschaftlichen Verhältnisse des Antragstellers und wird der

Ausscheiden eines Richters aus dem Dienst oder die nachträgliche Einbeziehung eines Referendars in die Bearbeitung der Akte.

[Rz 10] *Authentizität und Integrität*: (Datenursprungs-)*Authentizität* ist gegeben, wenn ein Dokument vom behaupteten Autor bzw. Absender stammt — *Integrität* bedeutet, dass es nicht unberechtigt verändert werden kann. Kryptographische Verfahren können eine Verletzung der Schutzziele nicht im engeren Sinne verhindern, aber bemerkbar machen. Die Ziele werden üblicherweise mit den gleichen Verfahren erreicht. Für die Akte als Ganzes bedeuten sie, dass keine Dokumente unberechtigt entfernt oder hinzugefügt werden können. Ein vollständiges Zurücksetzen einer Akte auf einen früheren Zustand lässt sich mit kryptographischen Verfahren jedoch nicht ohne weiteres verhindern.

[Rz 11] *Revisionssicherheit* wird oft als eigenes Schutzziel betrachtet; sie lässt sich aber auch als Integrität der Versionsgeschichte (der Akte und enthaltener Dokumente) betrachten. Technisch fordern wir, dass sich der Zustand der Akte für relevante vergangene Zeitpunkte (z.B. den Zeitpunkt einer Entscheidung) jederzeit rekonstruieren und dessen Echtheit nachweisen lässt.

[Rz 12] *Verbindlichkeit* bedeutet, dass ein Dokumentautor seine Autoreneigenschaft nicht erfolgreich abstreiten kann — jedes Dokument kann eindeutig seinem Autor zugeordnet werden. Für die Akte als Ganzes bedeutet es, dass die Zusammenstellung der Dokumente sich sicher dem Gericht zuordnen lässt.

[Rz 13] *Verfügbarkeit*: Berechtigte Nutzer sollten jederzeit Zugriff auf die (und Dokumente der) Akte haben.

[Rz 14] Die genannten Schutzziele stehen potentiell im Konflikt mit einem anderen Ziel, nämlich dem *Schutz personenbezogener Daten* der Beteiligten. So soll — wie schon in Abschnitt 2 erwähnt — der Dienstvorgesetzte eines Richters die Daten aus elektronischen Akten nicht nutzen können, um dessen Arbeitszeiten zu überwachen. Es sollte also beispielsweise der genaue Zeitpunkt, zu dem ein Dokument vom Richter angelegt und/oder der Akte hinzugefügt wurde, verborgen bleiben.

[Rz 15] Neben den eigentlichen Schutzzielen ist die *Langzeitarchivierung* relevant: Die Ziele müssen von der erstmaligen Anlage der Akte über den rechtskräftigen Abschluss des Verfahrens hinaus erreicht werden. Aufbewahrungsfristen reichen bis zu mehreren Jahrzehnten — in einigen Fällen darüber hinaus.[16] Dies beeinflusst die Auswahl von Sicherheitsverfahren und führt zu organisatorischem Aufwand.

5 Lösungen

[Rz 16] Bevor wir die einzelnen Schutzziele aus Abschnitt 4 diskutieren, müssen wir klären, in welchem (IT-)Umfeld wir uns bewegen und inwieweit Vertrauen in die bereitgestellte IT-Infrastruktur unterstellt werden kann. Unterstellen wir, dass die technische Infrastruktur und alle Mitarbeiter am Gericht voll vertrauenswürdig sind, müssen Sicherheitsmaßnahmen nicht weiter betrachtet werden. Wird jedoch davon ausgegangen, dass einzelne technische Administra-

Akte zwar beigefügt, aber z. B. dem Prozessgegner gegenüber nicht offengelegt.

16 Aufbewahrungsfristen ergeben sich aus Gesetzen des Bundes und der Länder in ihrem jeweiligen Zuständigkeitsbereich, im Saarland beispielsweise aus der Schriftgutaufbewahrungsverordnung der Justiz des Saarlandes (JSchrAVO-Saar), in deren Anlage konkrete Aufbewahrungsfristen festgelegt sind.

toren oder andere Mitarbeiter am Gericht potentiell ein Interesse daran haben könnten, vertrauliche Dokumente aus Akten einzusehen, um diese der Öffentlichkeit zuzuspielen / zu verkaufen, Dokumente gegen Bezahlung zu manipulieren, etc., so muss das E-Akte-System stärksten Sicherheitsanforderungen genügen. Für die im Folgenden vorgestellten technisch-organisatorischen Maßnahmen zur Umsetzung nehmen wir den zweiten Fall an.

[Rz 17] *Vertraulichkeit* kann durch standardisierte und als sicher eingestufte Verschlüsselungsverfahren erreicht werden. Bei der Umsetzung eines *Berechtigungs-Konzepts* lassen sich unterschiedliche Maßnahmen ergreifen. Im einfachsten Fall könnten — etwa durch die Geschäftsstelle — Berechtigungen auf Basis der öffentlichen Schlüssel der jeweiligen Nutzer vergeben werden. Um eine größere Menge zugriffsberechtigter Nutzer zu verwalten und dem Wechsel von Personen zwischen verschiedenen Rollen Rechnung zu tragen, könnten außerdem attributbasierte Verschlüsselungsverfahren (ABE)[17] verwendet werden. Letztere würden es komfortabel erlauben, Zugriffsrechte der Art «ist Richter am Amtsgericht» oder «ist Rechtsanwalt des Beklagten» vergeben zu können. Eine Entschlüsselung der Daten (und der damit einhergehende Zugriff auf diese) wird dann durch das verwendete kryptographische Verfahren nur Personen ermöglicht, die die nötigen Berechtigungen dafür aufweisen.

[Rz 18] *Authentizität und Integrität* von Dokumenten wird in der Praxis häufig mit Hilfe digitaler Signaturen erreicht. Die Arbeitsgruppe «Zukunft» der Bund-Länder-Kommission[18] weist darauf hin, dass der Einsatz qualifizierter elektronischer Signaturen (auf Basis von Chipkarten) zwar den «sicherheitstechnisch höchstmöglichen Maßstäbe[n]» genügt, die Akzeptanz in der öffentlichen Verwaltung, bei Gerichten und Behörden dafür allerdings nicht gegeben sei. Es wird deshalb vorgeschlagen, nur dort auf die qualifizierte elektronische Signatur zu setzen, wo «dies aus Rechtsgründen unerlässlich ist, wie etwa bei der elektronischen Signatur einer gerichtlichen Entscheidung durch den gesetzlichen Richter». Das BMI kommt für die Verwaltung zu einer ähnlichen Einschätzung: Es sei zu überprüfen «ob und in welchen Fällen auf die qualifizierte elektronische Signatur verzichtet werden kann»[19]. Signaturverfahren sind dennoch Mittel der Wahl, um Integrität und Authentizität auch der Akte als Ganzes sicherzustellen: Zugriffskontrollverfahren können zwar sicherstellen, dass nur Befugte Schreibzugriff auf die an einem sicheren Ort gespeicherte Akte erhalten. Signaturen haben aber den Vorteil, dass — bei Einhaltung gewisser organisatorischer Rahmenbedingungen — auch nach langer Zeit und durch Dritte die Authentizität geprüft werden kann. Qualifizierte Signaturen garantieren den höchsten Sicherheitsstandard, doch können auch lediglich fortgeschrittene Signaturen ausreichen, wenn deren Sicherheit durch (dokumentierte) organisatorische Maßnahmen gewährleistet wird[20]. *(Rechts-)Verbindlichkeit* einzelner vom Richter getroffener Entscheidungen hingegen — wie etwa das Einleiten des schriftlichen Vorverfahrens oder der Urteilsverkündung — setzt die Schriftformäquivalenz und somit auch künftig qualifizierte Signaturen voraus.

[Rz 19] Zur Erreichung der *Revisionssicherheit* können Konzepte bestehender Versionsverwal-

---

17 Goyal, Vipul / Pandey, Omkant / Sahai, Amit / Waters, Brent: Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of The 13th ACM Conference on Computer and Communications Security, CCS '06, 2006.

18 Arbeitsgruppe «Zukunft» der Bund-Länder-Kommission. Gemeinsame Strategie zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Aktenführung. Stand 16. März 2011.

19 BMI, Organisationskonzept elektronische Verwaltungsarbeit: Baustein E-Akte, Berlin (2012), Abschnitt 2.3.1.2.

20 An die Stelle der Signaturen können zukünftig auch fortgeschrittene oder qualifizierte elektronische Siegel nach der eIDAS-Verordnung (Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014) treten.

tungssysteme wie Git[21] aufgegriffen werden. Jeder Zustand einer E-Akte im Zeitverlauf muss dazu so archiviert werden, dass er zu jedem späteren Zeitpunkt wiederhergestellt werden kann — d.h. mit jeder Änderung muss die E-Akte um eine neue *Version* erweitert werden. Die Einhaltung der Anforderungen an die Vertraulichkeit der Akte und enthaltener Dokumente muss dabei für jede Version sichergestellt werden.[22] Um ein Löschen älterer Versionen zu verhindern, dürfen bei der Sicherstellung der Integrität nicht nur einzelne Versionen, sondern es muss bei jeder erstellten Version die gesamte E-Akte inkl. aller Vorversionen berücksichtigt werden. Wie in Git könnte eine Version der Akte hierzu durch einen kryptographischen Hashwert repräsentiert werden, der sowohl von den Daten und Metadaten der aktuellen Version der Akte, als auch vom Hashwert der Vorversion abhängt.[23] Eine elektronische Signatur (des Hashwertes) jeder erzeugten Version durch die Geschäftsstelle kann schließlich die Echtheit (aller Versionen) der E-Akte gewährleisten. Wie bereits bei den einzelnen Dokumenten diskutiert, können fortgeschrittene Signaturen hier unter entsprechenden organisatorischen Rahmenbedingungen ebenfalls ausreichen. Einen zweifelsfreien Nachweis über den Zustand der Akte zu einem relevanten vergangenen Zeitpunkt ermöglichen die Signaturen (auch wenn sie Zeitstempel enthalten) jedoch nicht, solange nicht jeder Mitarbeiter der Geschäftsstelle vertrauenswürdig ist: Letztere könnte Versionen nachträglich löschen / manipulieren, indem sie alle späteren Versionen mit gefälschten Zeitstempeln neu signiert. Um dies zu verhindern, sollte jede Version der E-Akte nach ihrer Erstellung *zusätzlich* von einem vertrauenswürdigen, externen Zeitstempel-Dienstleister signiert werden.

[Rz 20] *Verfügbarkeit* der Akte und in ihr enthaltener Dokumente für berechtigte Nutzer könnte konzeptionell erreicht werden, indem die E-Akte als verteiltes System umgesetzt wird — etwa in Form einer Datei / eines Verzeichnisses, die/das zwischen berechtigten Nutzern manuell oder automatisiert über Spezialsoftware ausgetauscht wird. Ein verteilter Ansatz bärge jedoch die Gefahr, die Komplexität der E-Akte hinsichtlich ihrer Umsetzung und hinsichtlich ihrer Nutzung beträchtlich zu erhöhen: Einerseits wäre schon zum reinen Lesezugriff auf ihr Datenformat Spezialsoftware auf den Endgeräten berechtigter Nutzer erforderlich. Andererseits wären zusätzliche organisatorische oder technische Maßnahmen nötig, um die sequentielle Entwicklung *einer* E-Akte sicherzustellen.[24] Ein zentralisierter Ansatz, bei dem die E-Akte etwa von einem Server innerhalb des Gerichts verwaltet und Zugriff über ein Webinterface ermöglicht wird, scheint daher praktikabler. Die Anforderung der Verfügbarkeit wird hierbei jedoch auf die technische Infrastruktur reduziert und daher hier nicht näher betrachtet.

[Rz 21] Hinsichtlich des *Schutzes personenbezogener Daten* sind insbesondere digitale Signaturen problematisch. Sie enthalten, aus Sicherheits-Sicht aus gutem Grund, einen Zeitstempel, der genaue Auskunft über den Zeitpunkt der Signatur-Erstellung gibt. Da auf digitale Signaturen nicht verzichtet werden kann — Verbindlichkeit ist technisch nur durch sie erreichbar — müsste das verwendete Signaturverfahren so angepasst werden, dass zwei Zeitstempel erzeugt werden:

---

21 Git ist ein verbreitetes, verteiltes Open-Source-Versionsverwaltungssystem, erhältlich unter http://git-scm.com/.

22 Eine Diskussion der Herausforderungen bei der Gewährleistung von Vertraulichkeit und Integrität im Kontext von Versionsverwaltung und ein auch für die E-Akte geeignetes Lösungskonzept finden sich in Leibenger, Dominik / Sorge, Christoph. A storage-efficient cryptography-based access control solution for subversion. In: Proceedings of the 18th ACM Symposium on Access Control Models and Technologies, SACMAT '13, 2013.

23 Das von Git implementierte Konzept ist beschrieben in: git-scm.com, 10.2 Git Internals — Git Objects. In: git-scm.com (Hrsg.), Pro Git, Second Edition. http://git-scm.com/book/en/v2/Git-Internals-Git-Objects, aufgerufen 8. Januar 2015.

24 Ohne zusätzliche Maßnahmen könnten aus einer Version der E-Akte bei parallelen Schreibzugriffen mehrere voneinander unabhängige Nachfolgeversionen entstehen, von denen nur eine gültig sein darf.

ein «ungenauer» Zeitstempel, der nur den Tag der Signatur enthält, könnte feststellbar machen, dass der Richter ein Dokument unterschrieben hat. Ein zweiter, genauer Zeitstempel könnte verschlüsselt hinterlegt werden, um bei Bedarf den exakten Zeitpunkt nachvollziehbar zu machen — etwa in Fällen, wo am Tag der Unterschrift unterschiedliche Sachverhalte eintreten. Eine Beschränkung der Herausgabe des zugehörigen Schlüssels auf bestimmte Ausnahmefälle wäre durch organisatorische Maßnahmen umsetzbar.

[Rz 22] Das dauerhafte Erreichen der Ziele auch im Falle einer *Langzeitarchivierung* einer E-Akte erfordert zusätzliche Maßnahmen: Die verwendeten kryptographischen Verfahren können aufgrund der voranschreitenden technischen Entwicklung nur für einen begrenzten Zeitraum als sicher betrachtet werden. Die Bundesnetzagentur veröffentlicht regelmäßig eine Liste der Verfahren, die entsprechend der Anforderungen des Signaturgesetzes als sicher betrachtet werden können, und gibt Prognosen über ihre Haltbarkeit.[25] Für das gängige Signaturverfahren RSA mit einer Schlüssellänge von 2048 Bits und für die kryptographische Hashfunktion SHA-256 etwa wird eine sichere Verwendbarkeit bis Ende 2020 prognostiziert; eine Garantie für die Prognosen kann es indes nicht geben. Wird davon ausgegangen, dass vom Ablauf dieser Haltbarkeit nur Akten betroffen sind, die bereits dem Archiv überstellt wurden, könnte diese Problematik relativ einfach durch organisatorische Maßnahmen gelöst werden: Es müsste lediglich sichergestellt werden, dass archivierte Akten nicht nachträglich verändert werden können. Erstrebenswerter scheint uns jedoch eine technische Lösung, die auch eine Bearbeitung der Akte über einen längeren Zeitraum ermöglicht und — etwa durch redundante Verwendung mehrerer kryptographischer Signatur- und Hashverfahren — auch gegenüber unerwarteter / frühzeitiger Verletzung der Sicherheitseigenschaften einzelner Verfahren robust ist. Hierzu bietet sich die Adaption der *Evidence Record Syntax*[26] an, die durch frühzeitigen Wechsel der Signatur- und Hashverfahren und bedarfsgemäße Erneuerung bestehender kryptographischer Werte Authentizität und Integrität auch über die Haltbarkeit der initial verwendeten Verfahren hinaus garantieren kann.

6 Fazit und Ausblick

[Rz 23] In dieser Arbeit haben wir einen Überblick über die Herausforderungen — insbesondere aus Sicherheits- und Datenschutzsicht — bei der Einführung der E-Akte in der Justiz gegeben und Lösungsansätze aufgezeigt, um diesen zu begegnen. Aus unserer Sicht kann sich durch die Einführung einer — richtig konzipierten und umgesetzten — E-Akte durchaus eine Verbesserung gegenüber dem Status-quo mit Papier-Akten, auch bezüglich Sicherheit und Datenschutz, ergeben. Durch die Umsetzung unter Verwendung starker kryptographischer Verfahren wäre aus technischer Sicht die Verlagerung einer E-Akte-Lösung «in die Cloud» durchaus vorstellbar — ob dies auch seitens der Justiz gewollt ist, wird in Zukunft wohl noch diskutiert werden müssen. Für eine flächendeckende Einführung des elektronischen Rechtsverkehrs sind noch eine Reihe weiterer Fragestellungen, auch nicht-technischer Natur, zu klären. Krüger und Vogelgesang besprechen in diesem Kontext beispielsweise die Folgen des elektronischen Rechtsverkehrs für den

[25] Bundesnetzagentur: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 13. Januar 2014.

[26] IETF, RFC 4998, Evidence Record Syntax (ERS). http://www.ietf.org/rfc/rfc4998.txt, aufgerufen 8. Januar 2015 (2007).

Justizgewährungsanspruch.[27]

7 Literatur

Arbeitsgruppe «Zukunft» der Bund-Länder-Kommission: Gemeinsame Strategie zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Aktenführung. Stand 16. März 2011, http://www.justiz.de/elektronischer_rechtsverkehr/erv_gesamtstrategie.pdf, abgerufen am 26. Januar 2015

Berlit, Uwe: Richterliche Unabhängigkeit und elektronische Akte, JurPC Web-Dok. 77/2012, http://www.jurpc.de/jurpc/show?id=20120077 (2012), abgerufen am 26. Januar 2015

Bundeskanzleramt: ELAK-Konzept Teil A — Funktionsbeschreibung (Version 1.1 vom 30. November 2001). http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19396 abgerufen am 3. Dezember 2014

Bundeskanzleramt: ELAK-Konzept Teil B — Leistungsverzeichnis (Version 1.1 vom 30. November 2001). http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19397 abgerufen am 26. Januar 2015

Bundesministerium des Innern: Organisationskonzept elektronische Verwaltungsarbeit — Baustein E-Akte, Berlin, 2012, http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/e_akte.pdf?__blob=publicationFile&v=2

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 13. Januar 2014. http://www.bundesnetzagentur.de/SharedDocs/Veroeffentlichungen/Algorithmen/2014Algorithmenkatalog.pdf?__blob=publicationFile&v=1, abgerufen am 26. Januar 2015

Deutscher Bundestag: Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten. Drucksache 17/12634, 6. März 2013

Bundesrechenzentrum: ELAK im Bund. https://www.brz.gv.at/leistungen_services/projekte/2013-10-30-ELAK-im-Bund-Factsheet.pdf?4jwluq, abgerufen am 26. Januar 2015

git-scm.com, 10.2 Git Internals — Git Objects. In: git-scm.com (Hrsg.), Pro Git, Second Edition. http://git-scm.com/book/en/v2/Git-Internals-Git-Objects abgerufen am 26. Januar 2015

Gondrom, Tobias / Brandner, Ralf / Pordesch, Ulrich: RFC 4998, Evidence Record Syntax (ERS). http://www.ietf.org/rfc/rfc4998.txt, abgerufen am 26. Januar 2015 (2007)

Goyal, Vipul / Pandey, Omkant / Sahai, Amit / Waters, Brent: Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of The 13th ACM Conference on Computer and Communications Security, CCS '06, 2006

Leibenger, Dominik / Sorge, Christoph: A storage-efficient cryptography-based access control solution for subversion. In: Proceedings of the 18th ACM Symposium on Access Control Models and Technologies, SACMAT '13, 2013

Kelsey, John: Compression and information leakage of plaintext. In: Daemen, J. / Rijmen, V.

[27] Krüger/Vogelgesang: Elektronischer Rechtsverkehr in Verfahren ohne Anwaltszwang — der Justizgewährungsanspruch des Bürgers als praktischer und theoretischer Störfaktor?, in diesem Band.

(Hrsg.), Fast Software Encryption, Lecture Notes in Computer Science Volume 2365, Springer, Berlin, S. 263—276 (2002)

Krüger, Jochen / Vogelgesang, Stephanie: Elektronischer Rechtsverkehr in Verfahren ohne Anwaltszwang — der Justizgewährungsanspruch des Bürgers als praktischer und theoretischer Störfaktor? — Anmerkungen insbesondere aus amtsrichterlicher Sicht. In: Tagungsband des 18. Internationalen Rechtsinformatik Symposions IRIS 2015, 2015

Dominik Leibenger
Ronald Petrlic
Christoph Sorge
Stephanie Vogelgesang
Universität des Saarlandes, juris-Stiftungsprofessur für Rechtsinformatik und CISPA, 66123 Saarbrücken, DE, {dominik.leibenger,ronald.petrlic,christoph.sorge,stephanie.vogelgesang}@uni-saarland.de