Sorge

III.

Praxisaspekte

4 In der praktischen Umsetzung stellt sich bislang noch eine Reihe von Problemen beim Einsatz der qualifizierten elektronischen Signatur durch Gerichte. Dies betrifft zunächst die benötigte Ausstattung mit jeweils einem **Kartenlesegerät**, einer **Signaturkarte** und der zum Signieren benötigten Software. Insbesondere bei

678

Einbeziehung der ehrenamtlichen Richter und der Möglichkeit, Urteile auch außerhalb des Gerichts zu unterzeichnen, können hier ein erheblicher Kostenaufwand und auch ein nicht zu unterschätzendes Fehlerpotential entstehen [1] . Die Möglichkeit der Signatur mit dem **elektronischen Personalausweis** als Signaturkarte schien das Potential zu haben, diesen Aufwand zu reduzieren. Dazu müsste aber ein Dienstleister (qualifizierter Vertrauensdiensteanbieter, Art. 3 Nr. 19 eIDAS-Verordnung) ein qualifiziertes Zertifikat zum Nachladen auf den Personalausweis anbieten, was aktuell nicht mehr der Fall ist. Alternativ wird die Möglichkeit einer **Fernsignatur**, bei der die Signaturerstellungsdaten beim Vertrauensdiensteanbieter verbleiben, durch die eIDAS-Verordnung [2] eröffnet. Der Unterzeichner muss auch für die Fernsignatur seine Identität gegenüber dem Vertrauensdiensteanbieter mit einem sicheren Verfahren nachweisen. Hierfür eignet sich etwa die eID-Funktion des elektronischen Personalausweises. Die AusweisApp in Verbindung mit der NFC-Funktion der meisten modernen Smartphones ermöglicht deren Verwendung als Kartenlesegerät für den Ausweis. Nach der erstmaligen sicheren Anmeldung beim Vertrauensdiensteanbieter kann die Identität bei der Erstellung einzelner Signaturen grundsätzlich auch mit einem anderen Verfahren nachgewiesen werden, etwa in Anlehnung an die Freigabe von Überweisungen im Online-Banking. Auch wenn die Signatur beim Vertrauensdiensteanbieter erstellt wird, kann die Vertraulichkeit des unterzeichneten Dokuments grundsätzlich gewahrt werden, da für die Signaturerstellung lediglich ein kryptographischer Hashwert („digitaler Fingerabdruck“) des Dokuments an den Anbieter übermittelt werden muss. Wenn viele qualifizierte elektronische Signaturen erstellt werden müssen, dürfte statt der Fernsignatur die Anschaffung von Kartenlesegerät und Signaturkarte aber effizienter sein. Eine weitere Alternative wird künftig mit der europäischen Brieftasche für die Digitale Identität (Art. 3 Nr. 42, 5a—5f eIDAS-VO) bereitstehen. Zudem könnte die Verwendung **qualifizierter elektronischer Siegel** (Art. 3 Nr. 27 eIDAS-VO) zukünftig zu einer Vereinfachung in Fällen beitragen, in denen es nicht auf die (natürliche) Person des Unterzeichners ankommt; sie ist aber in § 46d nicht vorgesehen.

Ob die Voraussetzung der qualifizierten elektronischen Signatur erfüllt ist, bestimmt sich lediglich nach der (objektiv durch Anwendung eines mathematischen Verfahrens in Verbindung mit der Widerrufsprüfung des verwendeten Zertifikats feststellbaren) Gültigkeit der Signatur, nicht nach deren Anzeige in einem E-Akten-System. [3]

5 Das Hinzufügen des Namens des Unterzeichners ist aus rein technischer Sicht idR redundant, da das bei einer qualifizierten Signatur verwendete qualifizierte Zertifikat den Namen des Unterzeichners oder ein Pseudonym enthält (Anhang I lit. b eIDAS-VO), wobei das Pseudonym in der Praxis den Ausnahmefall darstellt. Der Name ist dennoch zwingend hinzuzufügen. Das ermöglicht auch eine **schnelle Identifikation der Verantwortlichen**, ohne dass dazu die Signaturen und zugehörigen Zertifikate geprüft werden müssen. Es ist aber denkbar, dass der hinzugefügte Name nicht mit dem Ersteller der qualifizierten elektronischen Signatur übereinstimmt. Die Form ist dann nicht gewahrt [4] . Auch ist darauf hinzuweisen, dass eine einfache elektronische Signatur nicht mit dem Hinzufügen des Namens gleichgesetzt werden kann; zwar ist das Hinzufügen des Namens die gängigste und prozessrechtlich teils auch von der Rspr. [5] geforderte Form der einfachen elektronischen Signatur. Aus der Legaldefinition der elektronischen Signatur in Art. 3 Nr. 10 eIDAS-VO und dem Regelungszusammenhang in der Verordnung ergibt sich jedoch klar, dass eine elektronische Signatur weder den Namen des Unterzeichners enthalten noch aus sich heraus seine Identifizierbarkeit ermöglichen muss. [6] § 46d Satz 1 fordert aber explizit das Hinzufügen des Namens. Die Rechtsfolgen nicht gewahrter Form bei elektronischen gerichtlichen Dokumenten richten sich nach den gleichen Grundsätzen wie bei der nicht gewahrten Schriftform [7] .

679

In der Lit. wird auf das Problem der **Mehrfachsignatur** zB bei Kammer- bzw. Senatsentscheidungen hingewiesen. Technisch besteht hier zunächst keine Besonderheit; ein Dokument kann unproblematisch mehrfach signiert werden — mit oder (bevorzugt) ohne Einbeziehung bestehender Signaturen. Werden nach der ersten Signatur noch Änderungen (einschließlich kleinster Rechtschreibkorrekturen) vorgenommen, passen die vor diesen Änderungen erstellten Signaturen aber nicht mehr zum Dokument [8] . Gegenebenfalls muss der Zeichnungsprozess dann erneut begonnen werden. Daher empfiehlt es sich, erst nach Abstimmung und eventuellen Korrekturen qualifiziert elektronisch zu signieren [9] . Durch § 46e Abs. 2 wird eine Umgehung des Problems vorgezeichnet. Sie besteht im handschriftlichen Unterzeichnen und der anschließenden Übertragung in ein elektronisches Dokument. Die Anwendbarkeit ist aber nicht auf Schriftstücke beschränkt, die von mehreren Personen unterschrieben werden müssen. § 46d Satz 2 stellt nun klar, dass das Formerfordernis auch durch das somit entstandene elektronische Dokument erfüllt wird, wenn die Anforderungen des § 46e Abs. 2 erfüllt sind.

6 Eine besondere Herausforderung für die Gerichte dürfte die **langfristige Erhaltung der Authentizitäts- und Integritätsfunktion** der elektronischen Signatur sein [10] . Die kryptographischen Verfahren, die für qualifizierte elektronische Signaturen eingesetzt

werden — sogenannte kryptographische Hashfunktionen sowie digitale Signaturverfahren — können ihre Sicherheitsfunktion durch Fortschritte der Mathematik sowie (in geringerem Ausmaß) durch steigende Rechenleistung im Laufe der Jahre einbüßen. Reduzierte oder wegfallende Sicherheit muss nicht in jedem Fall problematisch sein [11] , doch kann eine einmal verlorene Sicherheitsgarantie nicht im Nachhinein wieder hergestellt werden. Daher sollten im Zweifelsfall Maßnahmen für deren Erhalt getroffen werden. Eine technische Lösung besteht in der sogenannten **Übersignatur**: Hierbei wird das Dokument einschließlich seiner ursprünglichen Signatur und einer Zeitangabe durch einen Vertrauensdiensteanbieter mit einem neuen Verfahren qualifiziert signiert oder mit einem qualifizierten elektronischen Siegel versehen, solange die ursprüngliche Signatur noch als sicher gilt [12] . Es entsteht ein sog. qualifizierter Zeitstempel (Art. 42 eIDAS-VO). Der Dienstleister bestätigt somit, dass die ursprüngliche Signatur zu einem Zeitpunkt vorlag, als sie noch sicher war. Aus der Sicht des Gerichts lässt sich ein solcher Prozess automatisieren bzw. zumindest teilweise an einen Anbieter eines sog. Bewahrungsdienstes (Art. 34 eIDAS-VO) auslagern, doch sollte die Thematik bei der Einführung elektronischer Aktenführung jedenfalls bedacht werden.

---

1 1 Auf die Problematik weist *Bader*, NZA 2016, 16 (18) hin. [Im Print: Fußnote 1 auf Seite 678]

2 2 Vgl. Erwägungsgrund 52 der Verordnung. [Im Print: Fußnote 2 auf Seite 678]

3 3 *Müller*, RDi 2023, 352 (354). Der besprochenen Entscheidung (LG Köln v. 4.5.2023 — 14 O 297/22) lag die Verwendung eines E-Akten-Systems zugrunde, das die drei Status „grün“ (endgültig positives Ergebnis), „rot“ (endgültig negatives Ergebnis) und „gelb“ (kein eindeutiges Ergebnis), vgl. S. 356 der Quelle. Technisch plausibel ist ein „nicht eindeutiges“ Ergebnis nur, wenn sich das bei der qualifizierten elektronischen Signatur verwendete Zertifikat, etwa wegen einer gestörten Internetverbindung oder einer Fehlfunktion beim Vertrauensdiensteanbieter, vorübergehend nicht auf Widerruf prüfen lässt. [Im Print: Fußnote 3 auf Seite 678]

4 4 So zur inhaltlich identischen Vorschrift der ZPO MünchKommZPO/*Fritsche*, § 130b ZPO Rz. 4. [Im Print: Fußnote 4 auf Seite 678]

5 5 So ließ etwa das BAG zutreffend den Namenszug „Rechtsanwalt“ in seinem Beschluss, BAG v. 25.8.2022 — 2 AZN 234/22, zur Erfüllung des Signaturerfordernisses nach § 46c Abs. 4 ArbGG ausreichen, weil der Unterzeichner anderweitig identifizierbar war; der BGH versteht aber in seiner Rspr. zu § 130a ZPO anscheinend (etwa BGH v. 11.10.2024 — V ZR 261/23) die Identifizierbarkeit des Unterzeichners entgegen der klaren europarechtlichen Regelung als Voraussetzung der einfachen elektronischen Signatur. [Im Print: Fußnote 5 auf Seite 678]

6 6 Dazu ausführlich jurisPK-ERV Band 1/*Sorge*, Kapitel 3 Rz. 18 f. [Im Print: Fußnote 6 auf Seite 678]

7 7 jurisPK-ERV Band 2/*Natter*, § 46d ArbGG Rz. 12. [Im Print: Fußnote 7 auf Seite 678]

8 1 *Viefhues*, Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, NJW 2005, 1009 (1012). [Im Print: Fußnote 1 auf Seite 679]

9 2 jurisPK-ERV Band 2/*Natter*, § 46d ArbGG Rz. 13. [Im Print: Fußnote 2 auf Seite 679]

10 3 Ausführlicher dazu jurisPK-ERV Band 1/*Sorge*, Kapitel 3 Rz. 33 ff. [Im Print: Fußnote 3 auf Seite 679]

11 4 *Hansen*, Eine überflüssige Übersignatur signierter Urteile — JurPC-Web-Dok. 0100/2014. [Im Print: Fußnote 4 auf Seite 679]

12 5 Nach bis 28.7.2017 geltendem Recht (§ 17 SigV a.F.) wurde hierfür ein qualifizierter Zeitstempel (§ 9 SigG a.F.) benötigt, der von einem Zertifizierungsdiensteanbieter ausgestellt wurde. Die eIDAS-VO (Art. 34) führt die Rolle eines qualifizierten Bewahrungsdienstes ein. Es besteht jedoch kein Zwang, einen solchen einzusetzen. § 15 des Vertrauensdienstegesetzes (VDG, als nationales Durchführungsgesetz zur eIDAS-VO) fordert lediglich, die Daten rechtzeitig „durch geeignete Maßnahmen neu zu schützen“. Wie hierbei nach dem Stand der Technik vorgegangen wird, ist in der Technischen Richtlinie 03125 („TR-ESOR“) des BSI dargestellt. Das Vorgehen nach § 17 SigV a.F. entspricht diesem Stand der Technik immer noch. [Im Print: Fußnote 5 auf Seite 679]