Der Beweis im Zivilprozess

von
Prof. Dr. Hans-Jürgen Ahrens

1. Auflage

Dr. Otto Schmidt Köln 2015

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 504 47140 8

Leseprobe zu

Ahrens

Der Beweis im Zivilprozess

2015, ca. 1376 Seiten, Handbuch, 16 x 24cm
ISBN 978-3-504-47140-8
179,00 €

Kapitel 23:
Beweis mittels elektronischer Dokumente

Schrifttum:

Abel, Urkundenbeweis durch digitale Dokumente, MMR 1998, 644; *Bacher*, Elektronisch eingereichte Schriftsätze im Zivilprozess, NJW 2009, 1548; *Chr. Berger*, Beweisführung mit elektronischen Dokumenten, NJW 2005, 1016; *Chr. Berger*, Elektronische Dokumente in Gerichtsverfahren, in: Bär u.a. (Hrsg.), Rechtskonformes eGovernment – eGovernment-konformes Recht, 2005, S. 141; *Bergfelder*, Der Beweis im elektronischen Rechtsverkehr, 2006; *Bergmann*, Beweisprobleme bei rechtsgeschäftlichem Handeln im Internet, Gedächtnis-

schrift Meurer (2002), S. 643; *Bertsch/Fleisch/Michels*, Rechtliche Rahmenbedingungen des Einsatzes digitaler Signaturen, DuD 2002, 69; *Binder*, Pflichten zur Offenlegung elektronisch gespeicherter Informationen im deutschen Zivilprozess am Beispiel der Unternehmensdokumentation, ZZP 122 (2009), 187; *Bieser*, Das neue Signaturgesetz, DStR 2001, 27; *Bitzer/Brisch*, Digitale Signatur, Berlin 1999; *Bizer*, Beweissicherheit im elektronischen Rechtsverkehr, in: Herausforderung an das Recht der Informationsgesellschaft, 1996; *Bizer/Hammer*, Elektronisch signierte Argumente als Beweismittel, DuD 1993, 619; *Blaurock/Adam*, Elektronische Signatur und europäisches Privatrecht, ZEuP 2001, 93; *Borges*, Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, 3334; *Borges*, Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, 3334; *Brenn*, Das österreichische Signaturgesetz – Unterschriftenersatz in elektronischen Netzwerken, ÖJZ 1999, 587; *Brenn*, Signaturgesetz, Wien 1999; *Brenn/Posch*, Signaturverordnung, Wien 2000; *Brisch/Brisch*, Elektronische Signatur und Signaturgesetz, in: Hoeren/Sieber, Handbuch Multimediarecht, Stand August 2005; *Britz*, Beschränkung der freien Beweiswürdigung durch gesetzliche Beweisregel?, ZZP 110 (1997), 61; *Czeguhn*, Beweiswert und Beweiskraft digitaler Dokumente im Zivilprozeß, JuS 2004, 124; *Ebbing*, Schriftform und E-Mail, CR 1996, 271; *Engel/Flechsig/Tettenborn*, Das neue Informations- und Kommunikationsdienste-Gesetz, NJW 1997, 2981; *Susanne Englisch*, Elektronisch geführte Beweisführung im Zivilprozeß, Diss. Bielefeld 1999; *Erber-Faller*, Gesetzgebungsvorschläge der Bundesnotarkammer zur Einführung elektronischer Unterschriften, CR 1996, 375; *Fina*, Die rechtliche Gleichstellung von elektronischen Signaturen mit handschriftlichen Unterschriften im europäischen Gemeinschaftsrecht und US-amerikanischen Bundesrecht, ZfRV 2001, 1; *Fischer-Dieskau*, Der Referentenentwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts, MMR 2003, 701; *Fischer-Dieskau*, Das elektronisch signierte Dokument als Mittel zur Beweissicherung, 2006; *Fischer/Dieskau/Hornung*, Erste höchstrichterliche Entscheidung zur elektronischen Signatur, NJW 2007, 2897; *Fischer-Dieskau-Steidle*, Die Herstellererklärung für Signaturanwendungskomponenten, MMR 2006, 68; *Fischer-Dieskau/Gitter/Paul/Steidle*, Elektronisch signierte Dokumente als Beweismittel im Zivilprozeß, MMR 2002, 709; *Fischer-Dieskau/Roßnagel/Steidle*, Beweisführung am seidenen BIT-String? Die Langzeitaufbewahrung elektronischer Signaturen auf dem Prüfstand, MMR 2004, 451; *Dominik Gassen*, Digitale Signaturen in der Praxis – Grundlagen, Sicherheitsfragen und normativer Rahmen, Diss. Köln 2002; *Geis*, Die digitale Signatur, NJW 1997, 3000; *Geis*, Europäische Aspekte der digitalen Signatur und Verschlüsselung, MMR 1998, 236; *Geis*, Zivilprozeßrechtliche Aspekte des elektronischen Dokumentenmanagements, CR 1993, 653; *Geis*, Das DE-Mail-Gesetz, NJW 2011, 1473; *Geis*, Rechtsregeln für einen sicheren elektronischen Rechtsverkehr, CR 2011, 23; *Gottwald*, Auswirkungen des elektronischen Rechtsverkehrs auf Parteivortrag und richterliche Sachbearbeitung im Zivilprozess, Festschrift Vollkommer (2006), S. 259; *Gravsen/Dumortier/van Eecke*, Die europäische Signaturrichtlinie – Regulative Fiktion und Bedeutung der Rechtswirkung, MMR 1999, 577; *Hähnchen*, Das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, NJW 2001, 2831; *Hammer/Bizer*, Beweiswert elektronisch signierte Dokumente, DuD 1993, 689; *Hoffmann/Borchers*, Das besondere elektronische Anwaltspostfach, CR 2014, 62; *Jandt*, Die Mitwirkung Dritter bei der Signaturerzeugung, K&R 2009, 548; *Jandt/Wilke*, Gesetzliche Anforderungen an das ersetzende Scannen von Papierdokumenten, K&R 2009, 96; *Jeep/Wiedemann*, Die Praxis der elektronischen Registeranmeldung, NJW 2007, 2439; *Jungermann*, Der Beweiswert elektronische Signaturen. Eine Studie zur Verläßlichkeit elektronischer Signaturen und zu den Voraussetzungen und Rechtsfolgen des § 292a ZPO, Frankfurt 2002; *Kuner*, Das Signaturgesetz aus internationaler Sicht, CR 1997, 643; *Malzer*, Zivilrechtliche Form und prozessuale Qualität der digitalen Signatur nach dem Signaturgesetz, DNotZ 1998, 96; *Malzer*, Elektronische Beglaubigung und Medientransfer durch den Notar, DNotZ 2006, 9; *Mankowski*, Für einen Augenscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mail, CR 2002, 44; *Mankowski*, Wie problematisch ist die Identität des Erklärenden bei E-Mails wirklich?, NJW 2002, 2822; *Mankowski*, Zum Nachweis des Zugangs bei elektronischen Erklärungen, NJW 2004, 1901; *Mankowski*, Zum Nachweis des Zugangs bei elektronischen Erklärungen, NJE 2004, 1901; *Melullis*, Zum Regelungsbedarf bei der elektronischen Willenserklärung, MDR 1994, 109; *Miedbrodt/Mayer*, E-Commerce – Digitale Signaturen in der Praxis, MDR 2001, 432; *Morgenstern*, Zuverlässigkeit von IP-Adressen-Ermittlungssoftware CR 2011, 203; *Müglich*, Neue Formvorschriften für den E-Commerce. Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht, MMR 2000, 7; *Müller*, Die Container-Signatur zur Wahrung

der Schriftform, NJW 2013, 3758; *Müller-Teckhof*, Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten, MMR 2014, 95; *Nöcker*, Urkunden und EDI-Dokumente, CR 2000, 176; *Nowak*, Der elektronische Vertrag – Zustandekommen und Wirksamkeit unter Berücksichtigung des neuen Formvorschriftenanpassungsgesetzes", MDR 2001, 841; *Oertel*, Elektronische Form und notarielle Aufgaben im elektronischen Rechtsverkehr, MMR 2001, 419; *Patti*, Die Beweiskraft des elektronischen Dokuments im italienischen Recht, Festschrift Manfred Rehbinder (2002), S. 707; *Polenz*, Der neue elektronische Personalausweis, MMR 2010, 671; *Pordesch*, Die elektronische Form und das Präsentationsproblem, 2002; *Preuß*, Verfahrensrechtliche Grundlagen für den „Elektronischen Schriftverkehr" im Zivilprozess, ZZP 125 (2012), 135; *Rechberger/McGuire*, Die elektronische Urkunde und das Beweismittelsystem der ZPO, in: Rechberger, Die elektronische Revolution im Rechtsverkehr, Wien 2006, S. 1 ff.; *Reese*, Vertrauenshaftung und Risikoverteilung bei Verwendung qualifizierter elektronischer Signaturen, 2007 (zugleich Diss. Osnabrück 2006); *Riehm*, E-Mail als Beweismittel im Zivilgerichtsverfahren, SJZ 96 (2000), 497; *Roßnagel*, Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, 3312; *Roßnagel*, Anerkennung von Prüf- und Bestätigungsstellen nach dem Signaturgesetz, MMR 1999, 342; *Roßnagel*, Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, MMR 1999, 261; *Roßnagel*, Signaturgesetz nach 2 Jahren, NJW 1999, 1591; *Roßnagel*, Auf dem Weg zu neuen Signaturregelungen, MMR 2000, 451; *Roßnagel*, Das neue Recht elektronischer Signaturen, NJW 2001, 1817; *Roßnagel*, Die neue Signaturverordnung, BB 2002, 261; *Roßnagel*, Die fortgeschrittene elektronische Signatur, MMR 2003, 164; *Roßnagel*, Elektronische Signaturen mit der Bankkarte?, NJW 2005, 385; *Roßnagel*, Die Ausgabe sicherer Signaturerstellungseinheiten, MMR 2006, 441; *Roßnagel*, Fremderzeugung von qualifizierten Signaturen?, MMR 2008, 22; *Roßnagel*, Das DE-Mail-Gesetz, NJW 2011, 1473; *Roßnagel*, Rechtsregeln für einen sicheren elektronischen Rechtsverkehr, CR 2011, 23; *Roßnagel*, Auf dem Weg zur elektronischen Verwaltung – Das E-Government-Gesetz, NJW 2013, 2710; *Roßnagel/Fischer-Dieskau*, Automatisiert erzeugte elektronische Signaturen, MMR 2004, 133; *Roßnagel/Fischer-Dieskau*, Elektronische Dokumente als Beweismittel, NJW 2006, 806; *Roßnagel/Pfitzmann*, Der Beweiswert von E-Mail, NJW 2003, 1209; *Roßnagel/Nebel*, Beweisführung mittels ersetzend gescannter Dokumente, NJW 2014, 886; *Rott*, Die Auswirkungen des Signaturgesetzes auf die rechtliche Behandlung von elektronischem Datenmanagement und Datenaustausch – Eine Prognose, NJW-CoR 1998, 420; *Scheffler/Dresser*, Vorschläge zur Änderung zivilrechtlicher Formvorschriften und ihre Bedeutung für den Wirtschaftszweig E-Commerce, CR 2000, 378; *Schemmann*, Die Beweiswirkung elektronischer Signaturen und die Kodifizierung des Anscheinsbeweises in § 371a Abs. 1 Satz 2 ZPO, ZZP 118 (2005), 161; *Schippel*, Die elektronische Form, Festschrift Odersky (1996), S. 657; *Schmiedl*, Die elektronische Signatur, CR 2002, 508; *Schnell*, Signaturmißbrauch und Rechtsscheinhaftung, 2007; *Schnell*, Daniel, Signaturmißbrauch und Rechtsscheinhaftung, 2007; *Schriewer*, Das spanische Gesetz für elektronische Signaturen, RIW 2005, 833; *Schuppenhauer*, Beleg und Urkunde – ganz ohne Papier? – Welche Beweiskraft bietet das elektronische Dokument an sich?, DB 1994, 2041; *Schwoerer*, Die elektronische Justiz, 2005; *Seidel*, Das Recht des elektronischen Geschäftsverkehrs – Rahmenbedingungen, technische Infrastruktur und Signaturgesetzgebung, Wiesbaden 1997; *Spickhoff/Bleckwenn*, Zum Beweiswert digitaler Aufklärungsbögen bei Verwendung elektronischer Signaturen, VersR 2013, 1350; *Spindler*, Das DE-Mail-Gesetz – ein weiterer Schritt zum sicheren E-Commerce, CR 2011, 309; *Spindler/Rockenbauch*, Die elektronische Identifizierung, MMR 2013, 139; *Stadler*, Der Zivilprozeß und neue Formen der Informationstechnik, ZZP 115 (2002), 413; *Thomale*, Die Haftungsregelung nach § 11 SigG, MMR 2004, 80; *Troiano*, Die elektronische Signatur – Angleichung und Diversifizierung der Vorschriften auf EG-Ebene, im italienischen und im deutschen Recht, ZEuP 2005, 43; *Viefhues*, Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, NJW 2005, 1009; *Wiebe*, Die elektronische Willenserklärung. Kommunikationstheoretische und rechtsdogmatische Grundlagen des elektronischen Geschäftsverkehrs, Tübingen 2002; *Wiebe*, Die elektronische Willenserklärung, 2002; *Yonemaru/Roßnagel*, Japanische Signaturgesetzgebung – Auf dem Weg zu „e-japan", MMR 2002, 798.

§ 81 Grundlagen: Rechtsentwicklung, technische Rahmenbedingungen

I. Gesetzesgeschichte des § 371a, ergänzende Normen

1. Zusammenwirken von Beweisrecht und Technikrecht

1 Die erste gesetzliche Äußerung zur Behandlung elektronischer Dokumente erfolgte 2001 mit der Regelung des **§ 371 Abs. 1 S. 2**. Damit war deren Qualifizierung als **Gegenstand des Augenscheinsbeweises** festgelegt (dazu Kap. 22 Rz. 44 ff.). Eigenständige beweisrechtliche Regelungen für elektronische Dokumente sind später mit § 371a, § 371b und 416a erzeugt worden.

2 **Vorläufervorschrift des § 371a** war – mit anderem Wortlaut – **§ 292a**. § 292a umfasste nur den Inhalts des § 371a Abs. 1 S. 2 und sprach zudem von „Willenserklärung" statt „Erklärung". Die Verschiebung und Erweiterung der Norm erfolgte durch das JustizkommunikationsG (JKomG) vom 22.3.2005.[1] Geregelt sind **Beweisfolgen** der **Verwendung elektronischer Signaturen**.

3 Die **technischen Rahmenbedingungen** elektronischer Signaturen sind erstmals am 1.7.1997 durch das Gesetz zur digitalen Signatur (SigG 1997)[2] festgelegt worden; das SigG 1997 war Teil des Informations- und KommunikationsdiensteG (IuKDG). Als Reaktion auf einen dazu erstellten Evaluierungsbericht der Bundesregierung und auf die **Richtlinie 1999/93/EG** vom 13.12.1999[3] ist das **SigG vom 16.5.2001** entstanden,[4] das von der **Signaturverordnung** (SigV) vom 16.11.2001 flankiert wird.[5] Modifiziert bzw. ergänzt worden ist das SigG durch das FormvorschriftenanpassungsG (FormVAnpG) vom 13.7.2001,[6] das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften (VwVfÄndG) vom 21.8.2002[7] und das Erste SigÄndG vom 4.1.2005.[8] Partiell überholt werden diese Regelungen durch die Möglichkeiten zum Einsatz des **elektronischen Personalausweises** und des **DE-Mail-Dienstes** (dazu Kap. 22 § 84).

2. Beweisvorgaben des Unionsrechts

4 Art. 5 Abs. 1 lit. b der Signaturrichtlinie 1999/93/EG ordnet an, dass qualifizierte Signaturen in Gerichtsverfahren **als Beweismittel zuzulassen** sind. Art. 5 Abs. 2 regelt zusätzlich, dass elektronische Signaturen die Wirksamkeit und die Zulässigkeit als Beweismittel im Gerichtsverfahren nicht allein deshalb abgesprochen werden darf, weil sie in elektronischer Form vorliegt, nicht auf einem qualifizierten Zertifikat beruht, der Zertifizierungsdiensteanbieter nicht akkreditiert ist oder die Signatur nicht von einer sicheren Signaturerstellungseinheit erstellt worden ist. Nach Erwägungsgrund 21 berührt die Richtlinie nicht die mitgliedstaatlichen Vorschriften über die **freie gerichtliche Würdigung** von Beweismitteln.

5 Der Beweis wird durch die Richtlinienregelung nicht klassifiziert (Strengbeweis, Beweismittelart, Freibeweis). Auch wird dem nationalen Recht **kein bestimmter Beweiswert** vorgeschrieben. Art. 5 Abs. 2 gestattet es, auf die technischen Eigenarten

1 BGBl. I 2005, 827 und S. 2022; RegE v. 13.8.2004, BT-Drucks. 15/4067.
2 BGBl. I 1997, 1872.
3 Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. EG Nr. L 13 v. 19.1.2000, S. 12.
4 BGBl. I 2001, 876.
5 BGBl. I 2001, 3074; Ermächtigungsgrundlage: § 24 SigG.
6 BGBl. I 2001, 1542.
7 BGBl. I 2002, 3322.
8 BGBl. I 2005, 2.

der jeweils verwendeten Signatur Rücksicht zu nehmen und Differenzierungen zu treffen.[1]

3. Förderung des elektronischen Geschäftsverkehrs

Der Gesetzgeber hat den **Empfänger** qualifiziert signierter Erklärungen **vor** unbegründeten **Einwendungen des Verwenders schützen** wollen[2] und ist davon ausgegangen, dass ihm bei einem Streit um die Echtheit ein größerer Schutz als bei Vorlage einer privaten Schrifturkunde zuteil werde.[3] Eine eigenständige Regelung wurde für erforderlich gehalten, weil der Erklärungsempfänger so gut wie nie **Klarheit über die tatsächlichen Umstände der Signaturerstellung** erlangen kann, also nicht weiß, wie der Signaturverwender organisiert ist und welches **Sicherheitsniveau** er beim Umgang mit elektronischen Signaturen beachtet hat, und weil generell das **Vertrauen in die Signaturtechnik** und die **Verkehrsfähigkeit der elektronischen Erklärung gestärkt** werden sollten, um den elektronischen Geschäftsverkehr zu fördern.[4] Der Gesetzgeber greift mit dem Förderungsgedanken Erwägungsgrund 16 der Signaturrichtlinie auf, wonach die Richtlinie einen Beitrag zur Verwendung und rechtlichen Anerkennung elektronischer Signaturen in der Gemeinschaft leisten will.[5] 6

4. Technische Sicherheitsvermutung

Das SigG soll den Rahmen für die Verwendung der elektronischen Signatur schaffen. Seine Regelungen bilden die Grundlage für die **Sicherheitsinfrastruktur** „qualifizierter Signaturen". Unter welchen Voraussetzungen eine elektronische Signatur mit einer eigenhändigen Unterschrift gleichgestellt wird, hat das FormVAnpG geregelt, dessen Art. 1 die §§ 126 ff. BGB geändert hat. 7

Für die Beweisregelung des § 371a Abs. 1 S. 2 ist u.a. die **Sicherheitsvermutung des § 15 Abs. 1 S. 4 SigG** bedeutsam. Diese Norm lautet: 8

„Mit diesen [sc.: Gütezeichen der zuständigen Behörde für akkreditierte Zertifizierungsdiensteanbieter] wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung zum Ausdruck gebracht."

§ 15 Abs. 1 S. 4 SigG enthält eine objektive Beschreibung der Sicherheit. Danach kann beim **Gebrauch akkreditierter Signaturen** sicher davon ausgegangen werden, dass die Signatur mit dem zugrunde liegenden Signaturschlüssel erzeugt wurde und die **signierten Daten** danach **nicht verändert** wurden.[6] 9

§ 15 Abs. 1 S. 4 SigG ist eine **technische Basis** der Beweisregelung des § 371a Abs. 1 S. 2. Die Beweiswirkung des **§ 371a Abs. 1 S. 2** beschränkt sich allerdings nicht auf diesen Anwendungsbereich, sondern gilt auch für qualifizierte Signaturen ohne Anbieter-Akkreditierung (zur Terminologie unten Rz. 13 ff.). 10

§ 15 Abs. 1 S. 4 SigG ist **Nachfolgeregelung zu § 1 Abs. 1 SigG 1997**. Die Interpretation des § 1 Abs. 1 SigG 1997 war streitig. Das ist darauf zurückzuführen, dass das SigG 1997 ausschließlich technische Rahmenbedingungen der digitalen Signatur regelte, während deren Rechtswirkungen einem gesonderten Gesetzgebungsverfahren vor- 11

1 *Blaurock/Adam* ZEuP 2001, 93, 100.
2 RegE FormVAnpG, BT-Drucks. 14/4987, S. 13, 17 und 25.
3 BT-Drucks. 14/4987, S. 13 und 17.
4 BT-Drucks. 14/4987, S. 13, 17 und 44.
5 Der Bericht der EG-Kommission vom 15.3.2006 über die Anwendung der Richtlinie [KOM (2006) 120 endg.] bedauert die mangelnde Benutzung qualifizierter elektronischer Signaturen.
6 RegE zum SigG 2000, BT-Drucks. 14/4662, S. 28.

behalten bleiben sollten.[1] Der E**valuierungsbericht** der Bundesregierung nahm an, dass die Sicherheitsvermutung zu einer Beweiserleichterung führe.[2] *Roßnagel* vertrat die Auffassung, es handele sich um eine Art „vorgezogener Anscheinsbeweis".[3] Einige Autoren sprachen der Norm jegliche Beweiswirkung ab.[4] Andere Autoren sahen in der Norm eine gesetzliche Vermutungsregel[5] oder eine tatsächliche Vermutung.[6] Kein Streit bestand darüber, dass das Prüfungsergebnis widerlegt werden darf, es sich also **nicht** um eine **absolute Verkehrsschutzregelung** handelt. Diese Auffassung ist auf § 15 Abs. 1 S. 4 SigG zu übertragen. Es handelt sich bei § 15 Abs. 1 S. 4 SigG um eine **widerlegbare technisch-organisatorische Sicherheitsvermutung**.[7]

II. Begriffsbildungen des SigG

1. Digitale Signatur, elektronische Signatur

12 § 2 Abs. 1 SigG 1997 benutzte den Begriff der „digitalen Signatur". Er ist im SigG 2001 durch den **technologieoffeneren Begriff** der **elektronischen Signatur** ersetzt worden.[8] **Sicherheit**, wie sie mit der digitalen Signatur verbunden sein sollte, ist nach neuer Terminologie **nur** bei Verwendung **qualifizierter** elektronischer Signaturen gegeben.[9] § 2 SigG 2001 unterscheidet elektronische Signaturen, fortgeschrittene elektronische Signaturen und qualifizierte elektronische Signaturen.[10] Hinzu kommen qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung gem. § 15 SigG.

2. Fortgeschrittene, qualifizierte und akkreditierte Signaturen

13 § 2 Nr. 2c SigG verlangt für eine **fortgeschrittene elektronische Signatur** u.a., dass die Signatur mit Mitteln erzeugt wird, die unter alleiniger Kontrolle des Signaturschlüsselinhabers gehalten werden. Diese Signaturen sollen die **Identifizierung des Schlüsselinhabers** ermöglichen, setzen aber nicht die Erfüllung organisatorischer oder technischer Sicherheitsanforderungen voraus. Rechtswirkungen werden daran nicht geknüpft, also auch nicht die Wirkungen des § 371a Abs. 1 S. 2 oder des § 15 Abs. 1 S. 4 SigG.

14 Die **Beweiswirkungen** des § 371a Abs. 1 S. 2 und Abs. 2 S. 2 treten erst bei Verwendung **qualifizierter Signaturen** (§ 2 Nr. 3 SigG) ein, die zusätzlich auf einem zum Zeitpunkt der Erzeugung gültigen **qualifizierten Zertifikat** beruhen und mittels einer sicheren Signaturerstellungseinheit erzeugt wurden. Zertifikate sind nach § 2 Nr. 6 SigG elektronische Bescheinigungen, mit denen **Signaturprüfschlüssel** einer Person zugeordnet werden und die Identität dieser Person bestätigt wird. **Ausgestellt** werden

1 *Schemmann* ZZP 118 (2005), 161, 164. S. auch *Roßnagel* NJW 1998, 3312, 3315: Sicherstellung hoher faktischer Sicherheit.
2 BT-Drucks. 14/1191, S. 17.
3 *Roßnagel* NJW 1998, 3312, 3315 f.; *Roßnagel* Kommentar zum Multimediarecht (Stand: November 2000), 5. Teil: SigG § 1, Rz. 42.
4 *Geis* NJW 1997, 3000, 3001; *Mertes* CR 1996, 769, 775.
5 *Abel* MMR 1998, 644, 647.
6 Mit Einschränkungen *Bitzer*, Beweissicherheit S. 160 f.; *Roßnagel* NJW 1998, 3312, 3317 ff.; unentschlossen *Bitzer/Brisch*, Digitale Signatur S. 129 f.; zur Vertiefung *Miedbrodt*, Signaturregulierung im Rechtsvergleich, Diss. Frankfurt am Main 2000, S. 66 f.; *Brückner*, Online Banking, Diss. München 1999, S. 139 ff.
7 *Schemmann* ZZP (2005), 161, 178. S. auch RegE zum SigG 2000, BT-Drucks. 14/4662, S. 28 (Sicherheitsvermutung mit besonders hohem Beweiswert).
8 RegE zum SigG v. 16.11.2000, BT-Drucks. 14/4662, S. 18.
9 Zu den Signaturverfahren und den daran Beteiligten *Brisch/Brisch* in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 13.3 (Stand 2012) Rz. 64 ff.
10 Zur Differenzierung *Roßnagel* MMR 2003, 164 ff.

die Zertifikate von vertrauenswürdigen Dritten, den Zertifizierungsdiensteanbietern (**Trust-Center**).

Akkreditierte Signaturen werden von einem **Zertifizierungsdiensteanbieter** ausgestellt (vgl. § 15 SigG), der sich einer Vorabprüfung durch die zuständige Kontroll- und Prüfbehörde (§ 3 SigG i.V.m. § 66 TKG), nämlich die **Bundesnetzagentur** für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, unterzogen hat. Akkreditierte Signaturen haben ein **höheres Sicherheitsniveau** als normale qualifizierte elektronische Signaturen. Diese Sicherheitsstufe muss nach § 1 Abs. 3 SigG[1] für öffentliche elektronische Dokumente nur eingehalten werden, wenn **für öffentlich-rechtliche Verwaltungstätigkeiten** eine entsprechende gesetzliche Anordnung getroffen worden ist; davon hat der Gesetzgeber **im VwVfÄndG** (oben Rz. 3) **und** im **JKomG** (oben Rz. 2) Gebrauch gemacht.[2] 15

3. Zertifizierungsdiensteanbieter

Zertifizierungsdiensteanbieter sind die natürlichen oder juristischen Personen, die qualifizierte Zertifikate und qualifizierte Zeitstempel ausstellen (§ 2 Nr. 8 SigG). In der Zertifikatausstellung erschöpft sich ihre Aufgabe allerdings nicht (unten Rz. 5). Sie fungieren als **unabhängige vertrauenswürdige Dritte**, die mit dem der signierten Erklärung beigefügten Zertifikat für die Zuordnung von Identität und Prüfschlüssel sorgen. Notwendig ist die Einschaltung von Zertifizierungsdiensteanbietern, weil die Verschlüsselung durch ein Zusammenspiel eines privaten und eines öffentlichen Schlüssels erfolgt (unten Rz. 51); der öffentliche Schlüssel erspart dem Empfänger der signierten Erklärung, denselben Schlüssel wie der Absender in Händen halten zu müssen.[3] Damit eine **Nachprüfung von Zertifikaten** möglich ist, müssen die Zertifizierungsdiensteanbieter gem. § 5 Abs. 1 S. 2 SigG einen **Verzeichnisdienst** anbieten, der jederzeit über öffentlich erreichbare Kommunikationsverbindungen abrufbar sein muss. Dort müssen alle vom Zertifizierungsdiensteanbieter ausgestellten Zertifikate verzeichnet sein. Das Verzeichnis ist durch Zertifikatssperrungen (§ 8 Abs. 1 Satz 1 SigG), die ein Signaturschlüsselinhaber verlangen kann, **jederzeit aktuell** zu halten. 16

Die vertrauensbildende Infrastruktur der Zertifizierung ist nicht hoheitlich ausgestaltet, sondern **marktwirtschaftlich organisiert**. Zertifizierungsdiensteanbieter stehen untereinander im wirtschaftlichen Wettbewerb.[4] Sie bedürfen für ihre Tätigkeit zwar keiner Genehmigung. Ihre Zuverlässigkeit, Fachkunde und die Einhaltung des Sicherheitskonzepts wird aber **durch** die **Bundesnetzagentur überwacht** (§ 4 SigG). Die Bundesnetzagentur bildet in der Infrastruktur die oberste Instanz. 17

Der Zertifizierungsdiensteanbieter hat die Aufgabe einer **Registrierungsstelle und** einer **Zertifizierungsstelle**. Als Registrierungsstelle **identifiziert** er den Antragsteller als künftigen Teilnehmer des Signierverfahrens, registriert ihn und händigt ihm die Signaturkarte (Chipkarte) aus. Als Zertifizierungsstelle ist er für fünf wesentliche Verfahrensschritte des Schlüsselmanagements zuständig, nämlich die **Generierung** des Schlüsselpaares als Unikat in abstrahlsicheren Räumen, die **Zertifizierung** des Signaturschlüsselpaares durch elektronische Versiegelung der Verknüpfung von Schlüssel und Benutzeridentität, die **Personalisierung** des geheimen Schlüssels durch Über- 18

1 Norm eingefügt durch den BT-Ausschuss für Wirtschaft und Technologie, BT-Drucks. 14/5324.
2 *Reese* Vertrauenshaftung S. 18. Zum Erfordernis einer qualifizierten Signatur als Wirksamkeitsvoraussetzung einer in elektronischer Form (§ 130a Abs. 1 S. 2 ZPO) eingereichten Berufungsbegründung BGH NJW 2010, 2134 Rz. 22.
3 Näher zu den sog. asymmetrischen Verfahren *Jungermann* Beweiswert S. 9 ff.
4 Zur vergleichenden Werbung eines Anbieters OLG Köln NJWE-WettbR 1998, 56, 57.

tragung auf ein Speichermedium (in der Regel die Signaturkarte), das Verwalten der **Verzeichnisdienste** mit den Listen der gültigen und gesperrten Zertifikate und das Betreiben des die Nutzung eines Zeitstempels ermöglichenden **Zeitstempeldienstes**. Biometrische Merkmale enthält das Speichermedium nicht.[1]

4. Prüf- und Bestätigungsstellen

19 Vom Zertifizierungsdiensteanbieter zu unterscheiden sind Prüf- und Bestätigungsstellen, die gem. §§ 18 SigG, 16 SigV von der Bundesnetzagentur anzuerkennen sind. Sie prüfen als **unparteiische Dritte** gem. §§ 15 Abs. 2 SigG, 2 SigV umfassend die **Sicherheitskonzepte** akkreditierter Zertifizierungsdiensteanbieter und bestätigen die Übereinstimmung **technischer** Komponenten bzw. **Produkte** mit den Sicherheitsanforderungen nach dem Stand von Wissenschaft und Technik (§§ 15 Abs. 7 S. 1, 17 Abs. 4 SigG, 15 SigV).

III. Verweisungen auf den Urkundenbeweis

1. Entbehrliche Analogiebildung, formelle Beweisregeln

20 Die Verweisungen des § 371a Abs. 1 S. 1 und des § 371a Abs. 2 S. 1 machen frühere Überlegungen entbehrlich, unter welchen Voraussetzungen und in welchem Umfang formelle Beweisregeln des Urkundenbeweisrechts auf elektronische Dokumente analog anzuwenden sind. Zugleich hat der Gesetzgeber – ebenso bereits durch § 371 Abs. 1 S. 2 – mit der Regelung anerkannt, dass **elektronische Dokumente** keine Urkunden sondern **Augenscheinsobjekte** sind. Der Beweis mit Hilfe elektronischer Dokumente ist ein Augenscheinsbeweis.[2]

21 § 371a ist im **Zusammenwirken mit § 371 Abs. 1 S. 2** zu lesen, der Regelungen für alle elektronischen Dokumente enthält, ohne dass es auf die Verwendung einer qualifizierten Signatur ankommt. Die Vorschriften des Urkundenbeweises über den **Editionsanspruch** des Beweisführers (§§ 422 ff.) sind kraft der Verweisung in § 371 Abs. 2 S. 2 anzuwenden. Der **Beweisantritt** ist eigenständig nach dem Vorbild des § 420 in § 371 Abs. 1 S. 2 geregelt. Ebenfalls eigenständig geregelt ist in § 371 Abs. 3 die **Beweisvereitelung**, für die das Urkundenbeweisrecht in § 427, § 441 Abs. 3 S. 3 und § 444 Spezialnormen enthält (allgemein zur Beweisvereitelung Kap. 8 § 30).

22 Verwiesen wird sowohl für **private** als auch für **öffentliche elektronische Dokumente** mit qualifizierter Signatur auf die Vorschriften über die Beweiskraft von Urkunden. Dabei handelt es sich um die speziellen **formellen Beweisregeln**, die in ihrem Anwendungsbereich den Grundsatz freier Beweiswürdigung (§ 286) verdrängen. Auf private elektronische Dokumente ist **§ 416** anzuwenden, auf öffentliche elektronische Dokumente sind es die **§§ 415, 417 und 418**.

2. Private elektronische Dokumente

a) Verweisung auf § 416

23 Für Privaturkunden bedeutet die Verweisung, dass die richterlichen **Rechtsfortbildungen zu § 416** ebenfalls in Bezug genommen werden. Dementsprechend gilt die formelle Beweisregel auch für den **Beweis der willentlichen Inverkehrgabe** (näher: Kap. 26

1 *Preuß* ZZP 125 (2012), 135, 146.
2 RegE FormVAnpG, BT-Drucks. 14/4987, S. 23.

Rz. 56) einer qualifiziert elektronisch signierten Erklärung. Im Beweis der Inverkehrgabe mit Willen des Ausstellers liegt die eigentliche Bedeutung des § 416.

24 § 416 enthält keine Regelung über die Widerlegung des Ergebnisses der Beweisregelanwendung. Sie ist durch **analoge Anwendung des § 415 Abs. 2** in § 416 hineinzulesen (näher: Kap. 26 Rz. 78). Der Beweisgegner kann also den **Gegenteilsbeweis** führen, dass die elektronische Erklärung **abhanden gekommen** ist, also nicht mit Willen ihres vermeintlichen Ausstellers in den Verkehr gelangt ist (zum Bezugsgegenstand der Feststellung willentlicher Inverkehrgabe bzw. umgekehrt des Abhandenkommens s. unten Rz. 27).

25 Der Beweis der willentlichen Inverkehrgabe einer qualifiziert signierten elektronischen Willenserklärung gegen den **Einwand des Abhandenkommens** kann aus **materiell-rechtlichen** Gründen **überflüssig** sein, wenn die Verwendung der Signaturmedien bzw. Identifizierungsmittel (Smartcard etc.) der als Aussteller erscheinenden Person zuzurechnen ist.[1]

b) Gesonderte Echtheitsprüfung

26 Die Bedeutung des **§ 416** ist gering, weil die **Echtheit einer Urkunde** von der Beweisregel **nicht umfasst** wird. Für die Echtheitsbeurteilung gelten die Regelungen der §§ 439 und 440. Die Echtheit einer Urkunde ist mit allen normalen Beweismitteln zu beweisen. Steht bei einer unterschriebenen Urkunde die Echtheit der Namensunterschrift fest, wird nach **§ 440 Abs. 2** vermutet, dass der über der Urkunde stehende Text vom Aussteller herrührt, also ebenfalls echt ist. Auf diese Regelung verweist § 371a Abs. 1 nicht. Für die Beurteilung der Echtheit einer privaten elektronischen Erklärung mit qualifizierter Signatur gilt die **Sonderregelung** des **§ 371a Abs. 1 S. 2** (dazu unten Rz. 44).

27 Der für § 416 zu führende Gegenteilsbeweis des Abhandenkommens einer Erklärung überschneidet sich mit der Erschütterung des Anscheins der Echtheit der qualifizierten Signatur (dazu unten Rz. 66). Der **Echtheitsbeweis** gem. § 371a Abs. 1 S. 2 kann durch den Beweis **widerlegt** werden, dass die signierte Erklärung nicht vom Signaturschlüsselinhaber abgegeben wurde, weil ihm die **Signaturerstellungseinheit** (Signaturkarte) **abhanden gekommen** war und die zusätzlich benötigte PIN ausgespäht wurde.[2] Das bewiesene Abhandenkommen der Signaturkarte, also des privaten Schlüsselträgers, **zerstört** die Basis des **Echtheitsanscheins** der elektronischen Erklärung. Dann stammt selbstverständlich auch die Erklärung nicht vom Schlüsselinhaber.

28 **Gelingt** diese **Erschütterung nicht**, ist die Erzeugung der Erklärung durch den Schlüsselinhaber persönlich oder einen von ihm autorisierten Dritten in Anwendung des § 371a Abs. 1 S. 2 bewiesen. Er kann dann aber noch **zusätzlich** den gegen die Anwendung der formellen Beweisregel der §§ 371a Abs. 1 S. 1, 416 gerichteten Beweis führen, dass die signierte **echte Erklärung** deshalb **nicht mit** seinem **Willen in den Verkehr gelangt** ist, weil es sich z.B. um einen verwechselten Entwurf handelte, weil die E-Mail-Absendefunktion versehentlich angeklickt wurde,[3] oder weil das Absenden unter Zwang oder Drohung einer dritten Person erfolgte.

---

1 Dazu eingehend *Reese* Vertrauenshaftung und Risikoverteilung bei Verwendung qualifizierter elektronischer Signaturen, S. 120 ff.; s. ferner *Schemmann* ZZP 118 (2005), 161, 174.

2 *Oertel* MMR 2001, 419, 420; *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 713; *Roßnagel/Fischer-Dieskau* MMR 2004, 134, 138; *Schemmann* ZZP 118 (2005), 161, 171 und 173; so auch RegE FormVAnpG, BT-Drucks. 14/4987, S. 24 f.

3 *Schemmann* ZZP 118 (2005), 161, 177.

29 Der Einwand des **Abhandenkommens des Signiermediums** richtet sich gegen die Echtheit des Dokuments, der Einwand des **Abhandenkommens der Erklärung** i.S.d. § 416 gegen deren willentliche Inverkehrgabe aus sonstigen Gründen jenseits der Signaturkartenverwendung.[1] Für die Verweisung des § 371a Abs. 1 S. 1 auf § 416 und den damit verbundenen formellen Beweis der willentlichen Inverkehrgabe bleibt demgemäß fast kein Anwendungsbereich. Zu beachten ist überdies, dass **materiellrechtliche Zurechnungen** den Gegenteilsbeweis zur Ausschaltung des § 416 vielfach irrelevant machen.

c) Elektronisches Originaldokument

30 Die Beweisregelungen des § 371a Abs. 1 gelten nur für **elektronische Originaldokumente**. Die **Transformation einer Papierurkunde** in ein elektronisches Dokument durch **nachträgliches Einscannen** lässt im elektronischen Dokument die Sicherheitsmerkmale des Papierdokuments verloren gehen.[2] Auf ursprünglich papiergebundene Privaturkunden, die in ein elektronisches Dokument überführt worden sind, ist die Beweisregel des § 416 grundsätzlich nicht kraft der Verweisung des § 371a Abs. 1 S. 1 anzuwenden.[3] § 371b, der seit dem 17.10.2013 gilt, findet nur auf **gescannte öffentliche Urkunden** Anwendung.

31 Eine eingescannte Privaturkunde kann allerdings unter denselben Voraussetzungen **wie** eine **Urkundenfotokopie**, die hinsichtlich Echtheit und Fehlerfreiheit der Urschrift und hinsichtlich der Übereinstimmung mit der Urschrift nicht umstritten ist, Grundlage der Anwendung des § 416 sein[4] (näher dazu Kap. 28 Rz. 39). Das wird insbesondere in Betracht kommen, wenn die Papierurkunde durch das **Einscannen als Bilddatei** gespeichert, also nicht in ein digitales Textdokument umgewandelt wird. Soweit § 416 nicht anzuwenden ist, ist das durch Scannen hergestellte Dokument ein Augenscheinsobjekt, das das Gericht im Rahmen freier Beweiswürdigung zu bewerten hat. Auf **Papierausdrucke rücktransformierter** privater elektronischer **Dokumente**, die durch Einscannen von Papieroriginalen entstanden sind, ist das **Urkundenbeweisrecht nicht** anzuwenden. Insbesondere ist § 435 nicht analog anzuwenden;[5] dem steht die Beschränkung des § 416a entgegen.

32 Wird das **gescannte Papierdokument** mit einer **qualifiziert signierten Erklärung** der scannenden Stelle versehen, dass das Ausgangsdokument mit dem von ihr erzeugten elektronischen Dokument übereinstimmt, wird diese Erklärung von § 371a Abs. 1 S. 1 erfasst.[6] Die Echtheit der **elektronischen Übereinstimmungserklärung** wiederum ist in Anwendung des § 371a Abs. 1 S. 2 zu beurteilen.[7] Zur Transformation von Papierurkunden in elektronische Dokumente durch einen Notar s. unten Rz. 34. § 298a Abs. 2 ordnet für den mit **elektronischen Akten** geführten Zivilprozess an, dass dem Gericht eingereichte papiergebundene Unterlagen durch Einscannen zu transformieren sind, die **Papierversion** aber bis zum Verfahrensabschluss **aufzubewahren** ist. Das ist wegen des Beweisantritts durch Vorlage der Originalurkunde (§ 420) erforderlich.[8] Der Anspruch auf effektiven Rechtsschutz (Art. 19 Abs. 4, 20 Abs. 3 GG) verbietet

1 Unklar ist der Standpunkt von *Schemmann* ZZP 118 (2005), 161, 177. Fehlende Differenzierung bei *Jungermann* Beweiswert S. 121 ff.
2 *Roßnagel/Wilke* NJW 2006, 2145.
3 *Roßnagel/Nebel* NJW 2014, 886, 887.
4 Unberücksichtigt geblieben bei *Roßnagel/Wilke* NJW 2006, 2145, 2148.
5 Für mikroverfilmte Dokumente unzutreffend a.A. *Bütter/Aicher* WM 2005, 1729, 1737 f.
6 Zur Verpflichtung, elektronische Akten ordnungsgemäß zu führen und dafür in Übereinstimmung mit der Verpflichtung zur Wahrung optischer Identität (§ 7 EGovG) farbige Ursprungsdokumente auch farbig einzuscannen, VG Wiesbaden NJW 2014, 2060, 2061.
7 *Roßnagel/Wilke* NJW 2006, 2145, 2148.
8 *Viefhues* NJW 2005, 1009, 1013.

ebenfalls die Vernichtung, wenn es auf die Originaleigenschaft des Dokuments ankommt.[1]

Ist ein gescanntes Dokument im Rahmen **freier Beweiswürdigung** nach § 286 zu beurteilen, können **technische Sicherungen** den Beweiswert erhöhen. Dazu gehören qualifizierte Zeitstempel gem. § 2 Nr. 14 SigG und ein Dokumentenmanagementsystem.[2] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Stand der Technik in der **Technischen Richtlinie 03138** (TR-RESISCAN) zusammengefasst. 33

3. Öffentliche elektronische Dokumente

Öffentliche elektronische Dokumente können von einer **Behörde** oder einer mit öffentlichem Glauben versehenen Person, in der Regel einem **Notar**, herrühren. § 371a Abs. 2 S. 1 greift die **Legaldefinition** des § 415 Abs. 1 S. 1 für öffentlichen Urkunden auf. Die dortigen Ausführungen gelten entsprechend. 34

Anzuwenden sind nach § 371a Abs. 2 S. 1 die **formellen Beweisregeln** des Urkundenbeweises gem. **§§ 415, 417 und 418**. Anders als für private elektronische Dokumente wird für öffentliche Dokumente von § 371a nicht verlangt, dass sie mit einer Signatur versehen sind. **Verzichtet** wird **schlechthin auf** eine **Signierung**, nicht nur auf die Anwendung eines besonderen Signierschlüssels. Es bleibt der Behörde oder Urkundsperson überlassen, durch interne Vorkehrungen für Authentizität des Dokuments zu sorgen. Insoweit gilt nichts anderes als bei der Errichtung öffentlicher Urkunden, etwa hinsichtlich der Verwendung von Dienstsiegeln. 35

Durch **öffentlich-rechtliche Spezialregelungen** (vgl. § 1 Abs. 3 SigG) wird für praktisch wichtige elektronische Kommunikationen angeordnet, dass öffentliche elektronische Dokumente **qualifiziert signiert** werden müssen (§ 3a VwVfG, § 36a SGB I, § 33 Abs. 3 SGB X, § 87a AO).[3] Teilweise ist die elektronische Form sogar ganz ausgeschlossen worden (z.B. in § 38a StAngG). 36

Das JKomG schreibt für **gerichtliche elektronische Dokumente** ebenfalls die qualifizierte Signatur vor (§ 130b ZPO, § 46 ArbGG, § 41a Abs. 1 S. 1 StPO, § 110 Abs. 1 S. 1 OWiG, § 55a Abs. 1 S. 3 VwGO, § 52a Abs. 1 S. 3 FGO, § 65a Abs. 1 S. 3 SGG).[4] Deren Missachtung führt zum **Rechtsmittelverlust**.[5] 37

Anwälte können gem. § 130a Abs. 1 ZPO **Schriftsätze in elektronischer Form** einreichen, sofern dies für das betreffende Gericht zugelassen worden ist (§ 130a Abs. 2). Benutzt werden muss dafür eine qualifizierte elektronische Signatur. Da die qualifizierte elektronische Signatur an die Stelle der eigenhändigen Anwaltsunterschrift tritt, muss die **Signatur** nach Auffassung des BGH **durch** einen zur Vertretung berechtigten **Anwalt** erfolgen,[6] der bestimmende Schriftsätze wegen der darin enthaltenen unmittelbar wirkenden Parteierklärung als Urheber ihres Inhalts verantworten soll. 38

1 Vgl. *Müller-Terpitz/Rauchhaus* MMR 2013, 10, 13; *Roßnagel* NJW 2013, 2710, 2709/2710.
2 Dazu *Roßnagel/Nebel* NJW 2014, 886, 889.
3 Zur Versäumung der Form beim Widerspruch gegen einen Beitragsbescheid VGH Kassel MMR 2006, 257. Zur Beweiserleichterung *Roßnagel/Fischer-Dieskau* NJW 2006, 806, 807 f.
4 Für ein übertriebenes Sicherheitsdenken hält dies *Schwoerer* Die elektronische Justiz, S. 78 ff., 148 ff.; kritisch auch *Viefhues* NJW 2005, 1009, 1001. Zur formgerechten Signierung einer Klageschrift bei monetärer Beschränkung der Signaturverwendungsmöglichkeit BFH DStRE 2007, 515 m. Bespr. *Fischer-Dieskau/Hornung* NJW 2007, 2897.
5 So in BGH NJW 2010, 2134 m. Bespr. *Hadidi/Mödl* NJW 2010, 2097; BFH NJW 2012, 334 Rz. 22 u. 26, stellt wesentlich auf die landesrechtliche Durchführungsverordnung (HbgERVV 2008) ab, deren Auslegung revisionsrechtlich nur beschränkt überprüfbar war.
6 BGH NJW 2011, 1294 m. Anm. *Hamm*. Zur Zulässigkeit sog. Container-Signaturen BGH NJW 2013, 2034 Rz. 10 m. krit. Bespr. *Müller* NJW 2013, 3758 f.

Es ist allerdings zweifelhaft, ob die möglicherweise **delegierte Signierung** als Problem der Formwirksamkeit erfasst werden sollte.[1]

39 **Ausdrucke öffentlicher** elektronischer Dokumente sind unter den Voraussetzungen des **§ 416a** als Urkunden zu behandeln (dazu Kap. 23 § 83). Der umgekehrte Vorgang des **Scannens öffentlicher Urkun**den, also der Überführung in ein elektronisches Dokument betrifft § 371b. § 371b stellt seit dem 17.10.2013 eingescannte öffentliche Urkunden i.V.m. einer Identitätsbestätigung der **Originalurkunde gleich**. § 437 ist jedoch nur anwendbar, wenn zusätzlich eine qualifizierte elektronische Signatur angebracht worden ist.

40 § 39a BeurkG, der durch das JKomG geschaffen wurde, lässt **elektronische notarielle Vermerkurkunden** zu. Notare können daher **öffentliche Beglaubigungen** in elektronischer Form durch eigene Signierung vornehmen, die in einem Attribut-Zertifikat den Schlüsselinhaber als Notar ausweist.[2] Die Einreichung einer Gesellschafterliste erfolgt durch Zeugnisurkunde, die neben der qualifizierten Signatur keiner zusätzlichen Beglaubigung bedarf.[3] Für eine qualifizierte Signatur steht dem Notar keine Gebühr gem. § 55 Abs. 1 KostO (= Nr. 25100 KV zum GNotKG von 2013) zu.[4]

41 **Abschriftsbeglaubigungen** können sowohl bei der Umwandlung elektronischer Dokumente in Papierabschriften als auch bei Herstellung elektronischer Dokumente von papiergebundenen Erklärungen anfallen.[5] Die **Transformation** qualifiziert signierter elektronischer Dokumente in Papierausdrucke regelt **§ 42 Abs. 4 BeurkG**.[6] Der Notar hat eine Signaturprüfung vorzunehmen und ihr Ergebnis in der Beglaubigung zu dokumentieren.

42 Die **Beurkundung von Willenserklärungen** und sonstiger Niederschriften in unmittelbarer elektronischer Form ist **nicht** gestattet. Von der papiergebundenen Urkundenurschrift dürfen beglaubigte Abschriften gefertigt werden, nicht aber elektronische Ausfertigungen.[7] Die **Verwahrung privater** elektronischer Dokumente **durch** einen **Notar** erspart bei Langzeitaufbewahrung Vorkehrungen gegen den Verfall des Signaturbeweiswertes.

4. Abgrenzung: Materielle Beweiskraft

43 Auch bei elektronischen Dokumenten besagt eine formelle Beweiskraft nichts über den materiellen Beweiswert des Dokumenteninhalts. **Ungesicherte EDV-Dokumentationen** sind gegen **nachträgliche Veränderungen** nicht geschützt. Anders als bei papiergebundenen (eventuell sogar handschriftlich verfassten) Urkunden lassen sich spätere Ergänzungen oder Manipulationen kaum nachvollziehen.[8]

1 Eingehend dazu *Preuß* ZZP 125 (2012), 135, 151, 156 ff. (mit Hinweisen auf die Rspr. des BFH zur eingescannten Unterschrift).
2 Näher *Oertel* MMR 2001, 419, 422; *Malzer* DNotZ 2006, 9, 11 ff., 18 ff., *Jeep/Wiedemann* NJW 2007, 2439, 2441 f.
3 OLG Schleswig DNotZ 2008, 709, 711; KG DNotZ 2011, 911, 912; a.A. OLG Jena ZIP 2010, 1939 = DNotZ 2010, 793 m. Anm. *Bettendorf/Mödl*.
4 OLG Düsseldorf MDR 2010, 595.
5 *Oertel* MMR 2001, 419, 422; *Malzer* DNotZ 2006, 9, 13.
6 *Malzer* DNotZ 2006, 9, 16 ff.
7 *Malzer* DNotZ 2006, 9, 12.
8 Zur Verwendung in der ärztlichen Dokumentation eingehend *Spickhoff/Bleckwenn* VersR 2013, 1350, 1358 ff.

§ 82 Echtheitsbeweis

I. Echtheitsbeweis für private elektronische Dokumente

1. Normqualifizierung, Beweisgegenstand

§ 371a Abs. 1 S. 2 ist vom Gesetzgeber als ein gesetzlich geregelter Fall des **Anscheinsbeweises** angesehen worden.[1] Zur Erzeugung des Anscheins ist die Einhaltung von **Vorgaben des Signaturgesetzes** erforderlich. Bei der Verwendung einer qualifizierten elektronischen Signatur soll es sich um einen typischen Ablauf handeln, der eine Beweiserleichterung im Prozess rechtfertigt. Dem ist in der Literatur entgegengehalten worden, es handle sich um eine **gesetzliche Vermutung**, weil der Anscheinsbeweis auf **Erfahrungsannahmen des Gesetzgebers** beruhe, nicht aber auf richterlich festgestellten Erfahrungssätzen.[2] 44

Im Gesetzgebungsverfahren hat der Bundesrat in seiner Stellungnahme zum RegE des § 292a ZPO a.F. die **Existenz** entsprechenden **Erfahrungswissens** in Abrede genommen, weil dieses Wissen erst im Umgang mit der elektronischen Signatur erworben werden könne.[3] Richtig ist zwar, dass die Basis des Anscheinsbeweises grundsätzlich (zu Einschränkungen unten Rz. 66) vom Gesetzgeber vorgegeben ist; der Gesetzgeber wollte unterschiedliche richterliche Bewertungen in Bezug auf die bestehenden Erfahrungssätze ausschließen.[4] Die gesetzliche Regelung beruht gleichwohl auf Erfahrungswissen mathematischer und informationstechnischer Experten;[5] es darf von den Gerichten nicht generell in Zweifel gezogen werden.[6] 45

Von einem richterlich formulierten Anscheinsbeweis (dazu Kap. 16 Rz. 1 ff.) unterscheidet sich § 371a Abs. 1 S. 2 nicht in Bezug auf die **Einschränkung der freien Beweiswürdigung**. Richterliche Erfahrungssätze sind revisibel; über einen vom BGH akzeptierten Erfahrungssatz und einen darauf gestützten Anscheinsbeweis darf sich die Instanzrechtsprechung nicht unter Berufung auf § 286 hinwegsetzen. Gleiches gilt für § 371a Abs. 1 S. 2. 46

Die eintretende **Rechtsfolge** ist der Erfolg eines **Echtheitsbeweises**.[7] Mit der Begründung des Anscheins der Echtheit wird der **Nachweis** der **Integrität, Authentizität** und **korrekten Autorisierung** des Dokuments geführt.[8] Wie jeder Hauptbeweis kann der Echtheitsbeweis durch gegenläufige Indizien widerlegt werden. Die Qualifizierung als „Anscheinsbeweis" besagt also nur, dass die **Annahme der Echtheit** bei Vorliegen bestimmter technischer Rahmenbedingungen des SigG **gerechtfertigt** und geboten ist, dass sie aber durch bewiesene „Erschütterungstatsachen" widerlegt wird. Die „Erschütterung" bedeutet nicht die Führung eines Hauptbeweises des Gegenteils (zur Unterscheidung von Gegenbeweis und Gegenteilsbeweis Kap. 3 Rz. 5). 47

Ob § 371a Abs. 1 S. 2 wirklich nur eine Beweiserleichterung bewirkt, ist in Zweifel gezogen worden, weil die vom SigG vorgesehenen technisch-organisatorischen 48

1 RegE zum FormVAnpG BT-Drucks. 14/4987, S. 22 und 44 („kein Fremdkörper innerhalb des zivilprozessualen Beweisrechts"). Dem folgend *Roßnagel* NJW 2001, 1817, 1826; *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 710; *Hähnchen* JuS 2001, 2831, 2833; *Tettenborn* CR 2000, 683, 689; *Jandt* K&R 2009, 548, 554.
2 *Schemmann* ZZP 118 (2005), 161, 182; ihm im Grundsatz folgend *Musielak*, Festschrift Vollkommer (2006), S. 237, 251.
3 RegE BT-Drucks. 14/4987, S. 37.
4 RegE BT-Drucks. 14/4987, S. 44.
5 RegE BT-Drucks. 14/4987, S. 44 (Gegenäußerung der BReg).
6 *Schemmann* ZZP 118 (2005), 161, 172.
7 *Schemmann* ZZP 118 (2005), 161, 165.
8 *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 710.

Grundlagen der Feststellung des Echtheitsbeweises so **streng** seien, dass mit ihrer Feststellung **mehr als** ein bloßer **Anschein** bewiesen sei und es somit auf eine Anwendung des § 371a Abs. 1 S. 2 nicht mehr ankomme.[1] **Bezweifelt wird** also, dass der **Anscheinsbeweis** angesichts der Grundlagen des Anscheins **faktisch erschüttert** werden kann. Letztlich hängt dies davon ab, was man als Feststellungsvoraussetzungen für den Echtheitsanschein ausreichen lässt; sie müssen im Rahmen richterrechtlicher Feinarbeit erst noch herausgearbeitet werden.

2. Geltung für signierte Erklärungen

49 Während § 292a nur für eine signierte „Willenserklärung" galt, ist dieser Begriff in § 371a Abs. 1 S. 2 auf „Erklärung" erweitert worden. Damit erfasst die Norm **auch Wissenserklärungen** wie z.B. Quittungen.[2] Auf diese Weise lassen sich digitalisierte Fotos mit einer signierten Erklärung über die Entstehung der Fotos verbinden und als Kombination von schriftlicher Zeugenaussage (§ 377) und Augenscheinssubstitution (Kap. 22 Rz. 19) zu Beweiszwecken verwenden.[3] Anwendbar ist die Neuregelung ferner auf **rechtsgeschäftsähnliche Erklärungen** wie z.B. Mahnungen, Fristsetzungen oder Anzeigen.[4]

50 **Weggefallen** ist in § 371a Abs. 1 S. 2 die vorherige **Bezugnahme auf § 126a BGB**. Daher ist belanglos, ob mit der zu beweisenden signierten Erklärung eine vorgeschriebene gesetzliche Schriftform ersetzt werden soll.[5]

3. Das Verschlüsselungsverfahren

51 Qualifizierte elektronische Signaturen beruhen auf einem mathematisch-wissenschaftlichen Verschlüsselungsverfahren.[6] Es handelt sich um ein **Public Key Kryptoverfahren**, das zwei einander komplementär zugeordnete mathematische Schlüssel benutzt. Verwendet werden ein geheimer **privater Schlüssel** und ein **öffentlich zugänglicher Schlüssel**, der Signaturprüfschlüssel. Die Schlüsselinhalte lassen sich bei Einhaltung des Standes von Wissenschaft und Technik **nicht wechselseitig errechnen**. Eine Entschlüsselung ist immer nur unter Einsatz des Komplementärschlüssels eines Schlüsselpaares möglich. Der öffentliche Signaturprüfschlüssel ist aus dem Verzeichnis des Zertifizierungsdiensteanbieters jederzeit für jedermann abrufbar.

52 Aus dem Klartext, dem die Signatur als ein Siegel beigefügt wird, wird ein **Hashwert** errechnet, in den Anzahl und Art der Zeichen sowie deren Reihenfolge eingerechnet werden. Der Hashwert wird mit dem privaten Schlüssel **verschlüsselt** (signiert), der sich auf einer **nicht auslesbaren Chipkarte** (Signaturkarte = **Smartcard**) befindet. Eingefügt wird der auf der Karte befindliche Schlüssel über ein an den Computer angeschlossenes Lesegerät. Zusätzlich muss eine mindestens **sechsstellige PIN** eingegeben (Kombination von Kartenbesitz und wissensbasierter Identifikation) oder ein biometrisches Verfahren benutzt werden. Als Ergebnis des Verschlüsselungsverfahrens steht die **digitale Signatur** zur Verfügung, die an die elektronische Datei **angehängt** und mit ihr übermittelt wird.

---

1 So zu § 292a ZPO a.F. *Roßnagel* NJW 2001, 1817, 1826; *Roßnagel* MMR 2000, 451, 459; *Oertel* MMR 2001, 419, 420.
2 RegE BR-Drucks. 609/04 S. 79; *Schemmann* ZZP 118 (2005), 161, 166.
3 Das Foto selbst ist nicht zu signieren, *Knopp* ZRP 2008, 156, 158.
4 *Schemmann* ZZP 118 (2005), 161, 166.
5 *Schemmann* ZZP 118 (2005), 161, 166.
6 Eingehend zur Technik *Bitzer/Brisch* Digitale Signatur, 1999; *Jungermann* Beweiswert S. 9 ff. (zur Methode der asymmetrischen Algorithmen).

Die zu signierende **Datei selbst** wird **nicht verschlüsselt**. Digitale Signaturverfahren verschleiern die zu versendende Erklärung bzw. Information nicht. Soweit Zertifizierungsdiensteanbieter anbieten, die Chipkarte **zusätzlich** mit einem **Textverschlüsselungsschlüsselpaar** auszustatten und die Verschlüsselungsschlüssel zertifizieren, damit die Datenübertragung in verlässlich verschlüsselter Form stattfinden kann, ist dieses Schlüsselpaar **von** dem **Signaturschlüsselpaar nach** dem **SigG** technisch und organisatorisch **getrennt**; die rechtlichen Vorgaben des Echtheitsbeweises gem. § 371a Abs. 1 S. 2 beziehen sich darauf nicht. 53

Zur **Feststellung der Identität des Verwenders** wird der **öffentliche Signaturprüfschlüssel** benutzt, der – einem Ausweis vergleichbar – von einem Zertifizierungsdiensteanbieter **garantiert** wird (**qualifiziertes Zertifikat**); das Zertifikat gibt Auskunft über die Echtheit des verwendeten öffentlichen Schlüssels des Absenders.[1] Der Empfänger der Datei muss die Echtheit des Schlüssels überprüfen. Die notwendigen Angaben erhält er durch das qualifizierte Zertifikat, das der eigentlichen Nachricht als Anhang beigefügt wird. Zusätzlich wird der **öffentliche Schlüssel des Zertifizierungsdiensteanbieters** benötigt, den die **Bundesnetzagentur ausgestellt** hat; er muss zu dem geheimen Schlüssel passen, mit dem der Zertifizierungsdiensteanbieter das Zertifikat signiert hat. Auf dessen Überprüfung ist der erste Prüfungsschritt gerichtet. Wenn die Echtheit des öffentlichen Schlüssels des Absenders feststeht (Feststellung der **Authentizität**), hat der Empfänger zu prüfen, ob die gesendeten Daten mit dem Hashwert des Originaltextes übereinstimmen, oder ob dieser Text während des Versendens verändert wurde (Feststellung der **Integrität**). 54

4. Voraussetzungen des Anscheinsbeweises

a) Positive Anforderungsbestimmung

Der Gesetzeswortlaut des § 371a Abs. 1 S. 2 stellt **nicht** die **Grundlagen des Anscheins** in den Vordergrund, **sondern** dessen **Erschütterung**, also den Gegenbeweis.[2] Voraussetzung des Anscheins ist „eine **Prüfung nach dem Signaturgesetz**". Diese Prüfung soll ermitteln, ob das elektronische Dokument mit einer (zumindest) qualifizierten Signatur i.S.d. SigG versehen ist.[3] Das ist der Fall, wenn die Signierung mit dem geheimen Schlüssel des Inhabers des den Schlüssel speichernden Signaturmediums erfolgt ist und der Schlüsselinhaber identifiziert worden ist. Die **Einzelanforderungen** der **Sicherheitsbewertung** ergeben sich aus **§ 2 Nr. 2a–d und Nr. 3a und b SigG**. In der signaturrechtlichen Literatur wird die Ansicht vertreten, auch die Einhaltung der Voraussetzungen des § 17 SigG sei Voraussetzung der Anwendung des Anscheinsbeweises.[4] 55

So wie beim Urkundenbeweis unter Geltung der Verhandlungsmaxime einzelne Voraussetzungen der Anwendung formeller Beweisregeln nach der Rechtsprechungspraxis von den Parteien unstreitig gestellt werden können (Kap. 28 Rz. 38), ist es auch bei der Prüfung einer elektronischen Signatur grundsätzlich möglich, **einzelne tatbestandliche Voraussetzungen** einer qualifizierten Signatur **unstreitig** werden zu lassen. Allerdings sind **zentrale** gesetzliche **Signaturanforderungen immer** zu **überprüfen**, 56

1 Zur Organisation des Vertrauens *Jungermann*, Beweiswert S. 27 ff.
2 *Bergmann*, Gedächtnisschrift Meurer (2002) S. 643, 649 (zu § 292a ZPO a.F.); *Musielak*, Festschrift Vollkommer (2006), S. 237, 250 f. A.A. wohl *Knopp* Anm. zu LG München I MMR 2008, 622, 624, der einen Umkehrschluss gegen einen Anscheinsbeweis aus dem Nichtvorliegen des § 371a ZPO zieht.
3 *Bergmann*, Gedächtnisschrift Meurer S. 643, 649.
4 *Fischer-Dieskau/Roßnagel/Steidle* MMR 2004, 451, 452; *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 712.

wenn die Signaturechtheit bestritten wird.[1] Dazu wird man jedenfalls die Verwendung eines privaten und eines öffentlichen Schlüssels und die Einschaltung eines Zertifizierungsdiensteanbieters rechnen müssen, die überhaupt erst die Einordnung als qualifizierte elektronische Signatur erlauben.

b) Unterscheidung qualifizierter und akkreditierter Signaturen

57 Der Anscheinsbeweis der Echtheit kann **nur mit qualifizierten Signaturen** oder höherwertigeren qualifizierten Signaturen mit Anbieter-Akkreditierung geführt werden (zu den Sicherheitsstufen oben Kap. 23 Rz. 12). Einzelne Einwendungen gegen die Signatur sind leichter zu überwinden, wenn der Signaturschlüssel von einem **durch** die **Bundesnetzagentur akkreditierten** Zertifizierungsdiensteanbieter ausgegeben worden ist und es sich daher um eine akkreditierte Signatur handelt.

c) Ausschließliche Signatur

58 Voraussetzung höherstufiger Signaturen ist die **ausschließliche Zuordnung** der Signatur zum Signaturschlüsselinhaber;[2] Signaturschlüsselinhaber ist eine natürliche Person (§ 2 Nr. 9 SigG). Die Ausschließlichkeit hat der Zertifizierungsdiensteanbieter zu prüfen. Er prüft auch die Verwendung von Komponenten, die für die Erzeugung von Signaturschlüsseln zugelassen sind, damit die **Einmaligkeit des privaten Schlüssels** gewährleistet ist.[3] Damit wird nachgewiesen, dass das Dokument **mit** dem **privaten Schlüssel** des Signaturverwenders **signiert** worden sein muss. Für die gerichtliche Überprüfung ist auf die Dokumentation des Zertifizierungsdiensteanbieters zurückzugreifen.

d) Identifizierung des Signaturschlüsselinhabers

59 Der Schlüsselinhaber wird mittels des Zertifikats identifiziert. Das setzt wiederum die **Gültigkeit des Zertifikats** voraus. Dessen langfristige Überprüfung ist nur bei Verwendung der Zertifikate akkreditierter Zertifikatdiensteanbieter gewährleistet.[4]

e) Signaturerzeugung

60 Die Signatur muss mittels einer **Signaturerstellungseinheit** erfolgt sein, die der Signaturschlüsselinhaber **unter** seiner **alleinigen Kontrolle** halten kann, in der Regel einer Signaturkarte (Smartcard). Der Signaturschlüssel muss dafür auf einem Datenträger gespeichert sein, der nur einmal vorhanden ist und aus dem nicht kopiert werden kann.[5] Darüber hinaus ist ein **Schutzmechanismus gegen** Finder, Diebe und andere **Unberechtigte** erforderlich, etwa die Verwendung einer PIN oder biometrischer Merkmale.[6] Der Zertifizierungsdiensteanbieter muss sich davon überzeugt haben, dass der Schlüsselinhaber eine sichere Signaturerstellungseinheit besitzt.[7]

1 *Schemmann* ZZP 118 (2005), 161, 167 m.w.N. (kein pauschaler Verzicht).
2 *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 711.
3 Vgl. *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 711; *Roßnagel* MMR 2003, 164, 165.
4 *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 711.
5 *Roßnagel* MMR 2003, 164, 165.
6 *Roßnagel* MMR 2003, 164, 166.
7 *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 711.

f) Unverfälschtheit der Daten

Die Signatur muss mit den signierten Daten in einer Weise verknüpft sein, dass nachträgliche Datenveränderungen erkannt werden können. Die Verknüpfung geschieht durch **sichere Hash- und Signaturverfahren**. Deren Sicherheitseignung hängt von der Verwendung von **Algorithmen** ab, die nach publizierter Einschätzung der Bundesnetzagentur, der das Bundesamt für Sicherheit in der Informationstechnik[1] zuarbeitet, sicher sind. Sie dürfen im Zeitpunkt der Sicherheitsbewertung **nicht älter als sechs Jahre** sein. Die Zeitschranke trägt dem Umstand Rechnung, dass die zur Verschlüsselung benutzten Algorithmen aufgrund technischen Fortschritts entschlüsselt werden können[2] und daher der **Signaturbeweiswert im Zeitablauf sinken** kann.[3] Digitale Signaturen haben also ein „Verfallsdatum"; das SigG gewährt ihnen keine zeitlich unbegrenzte Vermutung der Echtheit. 61

Eine archivierende Aktualisierung (Konservierung) kann entweder durch eine erneute Signierung (**Übersignierung**, §§ 6 Abs. 1 S. 1 SigG, 17 SigV) erfolgen, die dann allerdings in der Regel nicht der Aussteller der Erstsignatur vornehmen wird, oder – vorzugswürdig – durch automatische **Zufügung eines** qualifizierten **Zeitstempels** (§ 9 SigG).[4] Die Prüfung von Zeitstempeln ist nicht dem Prüfverfahren nach § 17 Abs. 2 S. 2 SigG unterworfen.[5] 62

g) Sicherheit der Signaturerstellungseinheit

Zur Sicherung der **Geheimhaltung und Einmaligkeit der Signaturerstellungseinheit** (Smartcard) ist erforderlich, dass der Zertifizierungsdiensteanbieter die Signaturerstellungseinheit vor Ausstellung des Zertifikats überprüft und das Ergebnis dokumentiert.[6] 63

h) Gültigkeit des Zertifikats

Die Signatur muss auf einem qualifizierten Zertifikat beruhen, das im Zeitpunkt ihrer Erstellung gültig ist. Ausgestellt werden kann ein qualifiziertes Zertifikat nur von einem **Diensteanbieter, der** die gesetzlich vorgeschriebenen **technisch-organisatorischen Sicherheitsanforderungen erfüllt**. Ist der Diensteanbieter bei der Bundesnetzagentur **akkreditiert**, bedarf es dafür keiner weiteren Beweismittel.[7] Ohne Akkreditierung muss ein gerichtlicher Sachverständiger auf die Dokumentation des Diensteanbieters zurückgreifen. 64

Die Echtheitsvermutung des **§ 15 Abs. 1 S. 4 SigG** erleichtert bei Verwendung akkreditierter Signaturen die Feststellung des Echtheitsanscheins (oben Kap. 23 Rz. 10). Sie umfasst aber nur die technischen und organisatorischen Prozesse des Zertifizierungsdiensteanbieters.[8] 65

1 www.bsi.de.
2 Dazu *Jungermann* Beweiswert S. 20 ff., 45 f.
3 Vgl. *Schemmann* ZZP 118 (2005), 161, 168.
4 *Schemmann* ZZP 118 (2005), 161, 168; s. ferner *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 712; *Fischer-Dieskau/Roßnagel/Steidle* MMR 2004, 451, 452.
5 Zur Kritik daran *Schemmann* ZZP 118 (2005), 161, 168 f.
6 Zum Auseinanderfallen von Zertifizierungsdiensteanbieter und Ausgeber der sicheren Signaturerstellungseinheit *Roßnagel* MMR 2006, 441 ff.
7 *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 712.
8 *Schemmann* ZZP 118 (2005), 161, 178.

5. Erschütterung des Echtheitsanscheins

66 Der Beweisgegner, der sich an der signierten Erklärung nicht festhalten lassen will, muss Erschütterungstatsachen vorbringen, wenn die Echtheit vorläufig feststeht. Ungeklärt ist, **welche Tatsachenbehauptungen** der Parteien **zur Führung des Anscheinsbeweises** gehören und welche der **Erschütterung** des vorläufigen Echtheitsbeweises zuzuordnen sind. Dies gilt insbesondere für die Detailanforderungen an die Organisationssicherheit der Zertifizierungsstellen als Vertrauensinstanz.[1] Das bedarf noch näherer technischer und rechtlicher Untersuchungen. Beeinflusst wird die Fixierung der technischen Standards auch von Einzelfallerkenntnissen, die aus zivilprozessualen Beweisverfahren gewonnen werden; sie können Grundlage für eine Anpassung technischer Standards sein. Zieht man den Umfang der Prüfungserfordernisse für die Ermittlung der Anscheinsechtheit zu weit, geht der Charakter einer Beweiserleichterung verloren; der gesetzgeberische Zweck (dazu oben Rz. 6) wird dann vereitelt. In der Rechtsanwendungspraxis muss der **Inhalt einer technischen Standardprüfung, die** die widerlegbare **Echtheitsvermutung trägt**, näher herausgearbeitet werden.

67 **Unklar** ist z.B., ob die Verwendung eines Schlüssels, der vom Zertifizierungsdiensteanbieter auf einer auslesbaren Diskette ausgeliefert wurde, so dass zum Signieren nicht eine sichere Signaturerstellungseinheit verwendet wurde, eine Erschütterung des vorläufig geführten Echtheitsanscheins bedeutet,[2] oder ob ein derartiges Fehlverhalten bereits in Form ein Negativbeweises Gegenstand der die Anscheinsechtheit tragenden Feststellungen des gerichtlichen Sachverständigen sein muss und ohne dazu getroffene Feststellungen schon die vorläufige beweismäßige Feststellung der Echtheit scheitert.

68 Erschütterungstatsache ist das Vorbringen des Beweisgegners, die für das Signieren benutzte **Smartcard samt PIN** sei von einem Dritten **unautorisiert verwendet** worden, etwa weil sie gestohlen oder anderweitig abhanden gekommen und die PIN ausgespäht worden ist (oben Rz. 27). Einwenden können soll der Beweisgegner auch, dass die **Daten** beim Signieren **fehlerhaft oder unvollständig angezeigt** worden sind, weil die dafür verwendeten Anwendungskomponenten fehlerhaft gearbeitet haben,[3] dass vom Zertifizierungsdiensteanbieter das Zertifikat und damit die Schlüssel einer falschen Person zugeordnet worden sind,[4] dass § 5 Abs. 1 S. 1 SigG zuwider eine **fehlerhafte Personenidentifizierung** stattgefunden hat,[5] dass ein Zertifikat **nicht** weisungsgemäß **gesperrt** worden ist (§ 8 Abs. 1 S. 1 SigG),[6] dass die verwendeten Signaturalgorithmen nicht mehr als sicher gelten,[7] oder dass der **Identifizierungs- und Übergabeprozess** des Zertifizierungsdiensteanbieters systematische **Defizite** aufweist.[8]

69 **Streitige Erschütterungstatsachen** müssen vom Beweisgegner ihrerseits bewiesen werden, ehe sie die Anscheinsechtheit erschüttern können.[9]

1 Unklar ist die von *Jungermann*, Beweiswert S. 113, vorgeschlagene Reduzierung der Anscheinsvoraussetzungen auf die positive Überprüfung der qualifizierten elektronischen Signatur nach dem SigG.
2 So wohl *Schemmann* ZZP 118 (2005), 161, 167.
3 *Fischer-Dieskau/Gitter/Paul/Steidle* MMR 2002, 709, 713. zur Anzeige der zu signierenden Daten auch *Roßnagel/Fischer-Dieskau* MMR 2004, 134, 136; *Jungermann*, Beweiswert S. 127.
4 *Schemmann* ZZP 118 (2005), 161, 172.
5 *Schemmann* ZZP 118 (2005), 161, 172.
6 *Schemmann* ZZP 118 (2005), 161, 172.
7 *Schemmann* ZZP 118 (2005), 161, 175.
8 *Roßnagel* NJW 2005, 385, 388.
9 *Malzer* DNotZ 2006, 9, 30. Unzutreffend a.A. *Schröter* WM 2000, 2134 („nur plausibel dartun"); *Jungermann* Beweiswert S. 127.

6. Hilfsweise: Beweiswürdigung nach § 286

Sofern es nicht gelingt, den Echtheitsanschein mittels § 372a Abs. 1 S. 2 zu beweisen, können die festgestellten Sicherheitsmerkmale gleichwohl beweiserhebliche Bedeutung im Rahmen **freier Beweiswürdigung** erlangen.[1] Es kommt dann auf **zusätzliche Beweisindizien** an. Dazu gehört z.B., ob ein Fälschungsinteresse erkennbar ist.[2] Zum Beweis der Absendung von E-Mails, deren Papierausdruck als Beweismittel verwendet werden soll, s. Kap. 16 Rz. 73 und Kap. 26 Rz. 55. 70

7. Ausländische elektronische Signaturen

Ausländische Signaturen sind inländischen qualifizierten Signaturen mit und ohne Anbieter-Akkreditierung unter den Voraussetzungen des § 23 Abs. 1 und 2 SigG **gleichgestellt**. Formelle Voraussetzung ist gem. § 18 Abs. 2 SigV die **Feststellung gleichwertiger Sicherheit** durch die Bundesnetzagentur.[3] Sichere Signierungen aus anderen EU-Staaten dürfen gegenüber inländischen Signaturen nicht benachteiligt werden.[4] 71

Für **andere ausländische** elektronische **Dokumente** und das ihnen zugrunde liegende Sicherheitssystem gilt § 286.[5] 72

II. Echtheit öffentlicher elektronischer Dokumente

Öffentliche Dokumente erlangen ihren **erhöhten Beweiswert** wegen der Mitwirkung einer **Amtsperson**. Für sie verlangt § 371a Abs. 2 S. 1 grundsätzlich nicht die Verwendung einer qualifizierten Signatur, damit die formellen Beweisregeln anzuwenden sind. Die Verwendung einer **qualifizierten Signatur** ist aber durch **Spezialvorschriften** für in der Praxis wichtige Dokumente vorgeschrieben. 73

Die **Echtheitsvermutung des § 437** für **inländische** öffentliche Urkunden ist auf öffentliche elektronische Signaturen nur anzuwenden, wenn das Dokument qualifiziert signiert worden ist (§ 371a Abs. 2 S. 2; ab 1.7.2014: § 371a Abs. 3 S. 1). Für **ausländische** öffentliche **elektronische Dokumente** gilt die Echtheitsvermutung nicht, auch wenn § 23 Abs. 1 SigG unter dort bezeichneten Voraussetzungen ausländische und inländische Signaturen mit qualifiziertem Zertifikat innerhalb der EU und des Europäischen Wirtschaftsraums gleichstellt. Grenzen setzt dieser Ungleichbehandlung nur das unionsrechtliche Diskriminierungsverbot. 74

§ 83 Umwandlung öffentlicher elektronischer Dokumente in Papierdokumente, § 416a ZPO

I. Entstehung des § 416a

§ 416a ist durch das Justizkommunikationsgesetz (JKomG) vom 22.3.2005[6] geschaffen worden. Die Norm steht in engem **Zusammenhang mit § 371a**, der in dieser Fas- 75

1 Vgl. RegE zum SigG 2000, BT-Drucks. 14/4662, S. 28: Beweiswert im Rahmen von § 292a ZPO(a.F.) „und im Rahmen der freien Beweiswürdigung"; *Roßnagel* NJW 2005, 385, 388.
2 Vgl. *Fischer-Dieskau/Roßnagel/Steidle* MMR 2004, 451, 454.
3 Nach *Jungermann*, Beweiswert S. 131, nicht Voraussetzung des Echtheitsanscheinsbeweises.
4 *Blaurock/Adam* ZEuP 2001, 93, 98.
5 Zum elektronischen Konnossement „Bolero – bill of lading" im Seefrachtverkehr *v. Bernstorff* RIW 2001, 504, 509 f.
6 BGBl. I 2005, 827 und S. 2022; RegE v. 13.8.2004, BT-Drucks. 15/4067.

sung ebenfalls auf das JKomG zurückgeht. Ihr **Wortlaut** ist in doppelter Hinsicht **misslungen** und bedarf der teleologischen Korrektur. Weitere Regelungen zu öffentlichen elektronischen Dokumenten hat Art. 1 des Gesetzes zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013[1] eingeführt.

II. Transformation elektronischer Dokumente

1. Grundsätzlich kein Urkundenbeweis

76 Elektronische Dokumente sind Augenscheinsobjekte und damit Gegenstand des **Augenscheinsbeweises** (Kap. 22 Rz. 31, Kap. 23 Rz. 20). Durch § 371, § 371a und § 371b werden allerdings Regelungen des Urkundenbeweisrechts in Bezug genommen oder es wird auf sie verwiesen. Werden elektronische Dokumente ausgedruckt und damit in ein Papierdokument überführt, kommt dem Ausdruck grundsätzlich **keine Urkundenqualität** zu. Insbesondere sind auf die Ausdrucke ohne Sonderregelung nicht die formellen Beweisregeln der §§ 415–418 anzuwenden. Derartige Ausdrucke haben selbst bei notarieller Beglaubigung des Ergebnisses der Medientransformation nicht den Charakter einer Urkunde. Sie sind Beweismittel, deren Wert im Rahmen **freier Beweiswürdigung** (§ 286) beurteilt werden muss.

2. Sonderregelung für öffentliche elektronische Dokumente

77 Wird ein **öffentliches** elektronisches Dokument ausgedruckt und mit einem Beglaubigungsvermerk versehen, entsteht dadurch ein Dokument, das der **beglaubigten Abschrift** einer öffentlichen Urkunde gleichgestellt ist. Sie reicht für einen Beweisantritt nach §§ 420, 435 aus. Damit **vertritt** der beglaubigte **Papierausdruck das** elektronische **Originaldokument** als Urkunde, soweit auf das Originaldokument nach § 371a Abs. 2 S. 1 die formellen Urkundenbeweisregeln anzuwenden sind, also die Normen der **§§ 415, 417 und 418**.

78 Für **gerichtliche** elektronische **Dokumente** (§ 130b) gelten die **§§ 165, 314**. Bei ihnen tritt ein **Transfervermerk** an die Stelle einer Beglaubigung. Ein vollständiger Transfer von Aufzeichnungen einer im elektronischen Dokument eventuell enthaltenen Videosequenz (vgl. § 128a) kommt nicht in Betracht.[2]

III. Anforderungen an das elektronische Dokument

1. Elektronisches Originaldokument

79 Das elektronische Dokument muss als solches errichtet worden sein.[3] § 416a gilt **nicht** für ein elektronisches Dokument, das **durch Einscannen** eines ursprünglichen Papierdokumentes **entstanden** ist (zum Einscannen s. auch Rz. 30).

2. Öffentliches Dokument

80 Die Sonderregelung des § 416a gilt nur für öffentliche, **nicht** hingegen **für private** elektronische Dokumente. Weiterreichenden privaten Gesetzgebungsvorschlägen[4] ist der Gesetzgeber zu Recht nicht gefolgt.

1 BGBl. I 2013, 3786.
2 *Berger* Elektronische Dokumente S. 141, 146.
3 Zöller/*Geimer*[30] § 416a Rz. 1.
4 *Geis* CR 1993, 653 ff.; dazu *Britz* ZZP 110 (1997) 61, 86.

Für öffentliche Dokumente von Behörden oder Notaren stellt der Wortlaut des § 416a keinen personellen **Zusammenhang** zwischen der **Errichtung** des elektronischen Dokuments **und** der **Beglaubigung** des Papierausdrucks her. Gestattet man es einer Behörde oder einem Notar, eine Beglaubigung des Ausdrucks eines **fremden** elektronischen **Dokuments** zu erteilen, ist die Wahrscheinlichkeit der Authentizität und Integrität des Originaldokuments insbesondere in den Fällen nicht gesichert, in denen das Originaldokument nicht qualifiziert signiert worden ist. Der **Wortlaut des § 416a** ist daher **einzuschränken**: Die Beglaubigung der Medientransformation muss von der Behörde oder Urkundsperson vorgenommen werden, die das elektronische Originaldokument errichtet hat. Wird diese Korrektur nicht vorgenommen, ist jedenfalls regelmäßig gem. §§ 371a Abs. 2 S. 1, 435 S. 1 von Amts wegen die Vorlage des Originaldokuments anzuordnen. 81

Für den Ausdruck eines **gerichtlichen Dokuments** mit Transfervermerk gem. § 298 Abs. 2 entsteht das Problem ungesicherter Authentizität und Integrität des Textes nicht. § 416a verlangt insoweit, dass der Vermerk vom **zuständigen Gericht** erteilt worden sein muss. Überdies schreibt § 130b eine qualifizierte elektronische Signatur vor. 82

3. Signaturerfordernis

Das elektronische Dokument muss **nicht signiert** oder gar qualifiziert signiert worden sein.[1] § 416a verweist generell auf § 371a Abs. 2, der in S. 2 eine qualifizierte Signatur nur für den Echtheitsbeweis nach § 437 fordert. Auf öffentliche elektronische Dokumente sind die formellen Beweisregeln des Urkundenbeweisrechts nach § 371a Abs. 2 S. 1 schlechthin anzuwenden. Allerdings existieren für die wichtigsten Anwendungsbereiche **Sonderregelungen** (vgl. Rz. 36 ff.), die die Beifügung einer qualifizierten Signatur verlangen. Dann kann dem Ausdruck eines in eine Papierform transformierten elektronischen Dokuments auch nur unter dieser Voraussetzung der Beweiswert der Abschrift einer öffentlichen Urkunde zukommen. **Beglaubigte Abschriften** öffentlicher elektronischer Dokumente **ohne qualifizierte Signatur** sind in derartigen Fällen nicht zur Beweisführung nach §§ 415, 417 oder 418 zuzulassen. 83

§ 84 Sonstige elektronische Beweise

I. Elektronischer Identitätsnachweis mittels maschinenlesbaren Personalausweises

Das am 1.11.2010 in Kraft getretene Personalausweisgesetz (PAuswG) sieht vor, dass ein in den Ausweis **integrierter Chip** die Personaldaten enthält und die Verwendung des Ausweises als **Signaturkarte** ermöglicht. Als Signaturerstellungseinheit unterliegt der Ausweis den Vorgaben des SigG. Nach § 22 PAuswG gilt der Ausweis als sichere Signaturerstellungseinheit. 84

Elektronisch nachgewiesen wird mittels der Chipdaten die **Identität der Person**, die als Urheber einer Handlung, insbesondere einer Willenserklärung festzustellen ist. Die **Authentisierung** unter Verwendung des Ausweises und der zugehörigen PIN ist als solche Gegenstand eines **Anscheinsbeweises**, der durch konkrete Anhaltspunkte für einen Trojanerangriff zu erschüttern ist[2] oder durch die ernsthafte Möglichkeit 85

1 A.A. Thomas/Putzo/*Reichold*[33] § 416a Rz. 2; MünchKommZPO/*Schreiber*[4] § 416a Rz. 4.
2 Abweichend *Borges* NJW 2010, 3334, 3338: Führung des Anscheinsbeweises nur bei Ausschluss eines Trojanerangriffs.

der Weitergabe oder des Abhandenkommens des Ausweises.[1] Eine etwaige **Rechtsscheinhaftung** bleibt davon **unberührt**.

86 Aufgrund bewiesener Authentisierung ist die Vornahme der **Handlung durch** den **Ausweisinhaber** im Wege des **Anscheinsbeweises** bewiesen. Für die Beurteilung der **Echtheit** einer damit verbundenen Erklärung gilt dann **§ 440 Abs. 2**. Erschüttert wird der Anschein durch konkrete Anhaltspunkte für eine Infizierung des Rechners durch einen Trojaner.[2]

87 Die EU hat einen Verordnungsvorschlag vorgelegt (Kom [2012] 238/2), der die elektronische Identifizierung **unionsrechtlich** regeln soll.[3]

II. Elektronische Post im DE-Mail-Dienst

88 Das DE-Mail-Gesetz vom 28.4.2011 soll nach seinem § 1 Abs. 1 einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr im Internet ermöglichen. Beweisrechtlich von Bedeutung sind der **Postfach- und Versanddienst** gem. § 5 und der **Identitätsbestätigungsdienst** gem. § 6. Um die Zielsetzungen des E-Government-Gesetzes (EGovG) vom 25.7.2013[4] zur Förderung der elektronischen Verwaltung zu unterstützen, ist zugleich das De-Mail-Gesetz geändert worden. Ermöglicht werden soll die elektronische Kommunikation mit den Verwaltungsbehörden.[5] De-Mail-Dienste sollen für die Bundesverwaltung angeboten werden.[6] Ab 2020 soll eine elektronische Aktenführung für Bundesbehörden eingerichtet werden.

89 Die Eröffnung eines **De-Mail-Kontos** setzt eine **Identifizierung des Nutzers** voraus. Die Voraussetzungen werden in Orientierung an § 3 Abs. 1 SigV durch § 3 Abs. 3 S. 1 Nr. 4 De-Mail-G geregelt.

90 Nach § 7 De-Mail-G kann der Nutzer erklären, dass er sein Konto für den Zugang von Behördennachrichten öffnet. Das Senden einer De-Mail kann **als konkludente Zugangseröffnung** angesehen werden.[7]

91 § 5 Abs. 7 regelt die **Versandbestätigung**, Abs. 8 die **Bestätigung des Eingangs** einer Nachricht im DE-Mail-Postfach des Empfängers und Abs. 9 die **Abholbestätigung** bei förmlichen Zustellungen durch eine öffentliche Stelle nach den Vorschriften der Prozessordnungen.

92 Mit dem DE-Mail-Dienst darf der **ungesicherte E-Postbrief** der Deutschen Post AG nicht verwechselt werden. Bei derartigen Diensten trägt der Empfänger ein Risiko in zeitlicher Hinsicht, weil es für den **Zugangszeitpunkt** auf die bloße Wahrnehmbarkeit im Empfangsbereich ankommt.

93 Die **Identitätsdaten** werden übermittelt, wenn sich der Nutzer dieser Möglichkeit bedient und der akkreditierte Diensteanbieter die Nachricht mit einer qualifizierten elektronischen Signatur versieht. Dafür gilt dann § 371a. Diese Authentisierungsmöglichkeit tritt in **Konkurrenz** zu derjenigen nach **§ 18 PAuswG**.[8]

1 *Borges* NJW 2010, 3334, 3338.
2 *Borges* NJW 2010, 3334, 3337.
3 Kritisch dazu *Spindler/Rockenbauch* MMR 2013, 139 ff.
4 BGBl. I 2013, 2749.
5 *Roßnagel* NJW 2013, 2710, 2711.
6 *Roßnagel* NJW 2013, 2710, 2712.
7 *Roßnagel* NJW 2013, 2710, 2715.
8 *Roßnagel* NJW 2011, 1473, 1476.

Da die **Abholbestätigung** nach § 5 Abs. 9 S. 5 De-Mail-G mit einer qualifizierten elektronischen Signatur zu versehen ist, gelten dafür §§ 371a Abs. 2, 415 und 437 ZPO.[1] Die **Versandbestätigung** und die **Eingangsbestätigung** sind nach § 5 Abs. 7 S. 3 bzw. nach § 5 Abs. 8 S. 4 mit einer qualifizierten elektronischen Signatur zu versehen. Dafür gilt dann § 371a Abs. 1 ZPO. Da es sich um **private Dokumente** handelt, ist § 416 ZPO anzuwenden.[2] Ebenfalls einen **Anschein der Echtheit** begründet gem. § 371a Abs. 2[3] eine elektronische Nachricht, die von einer natürlichen Person versandt worden ist, wenn das De-Mail-Konto gem. § 4 Abs. 1 S. 2 De-Mail-G sicher angemeldet und dem Anmelder allein zugeordnet ist. Für qualifiziert signierte **öffentliche Dokumente** gilt gem. § 371a Abs. 3 S. 1 die Echtheitsvermutung des § 437. Dieselbe Regelung greift nach § 371a Abs. 3 S. 2 ein, wenn eine nach § 5 Abs. 5 De-Mail-G absenderbestätigte De-Mail mit sicherer Anmeldung von einer öffentlichen Behörde oder einer mit öffentlichem Glauben versehenen Person versandt wurde.[4] 94

III. Elektronisches Anwaltspostfach

Zur Förderung des elektronischen **Rechtsverkehrs mit den Gerichten** hat der Gesetzgeber durch Gesetz vom 10.10.2013[5] mit § 130a Abs. 4 Nr. 1–4 ZPO sichere **elektronische Übermittlungswege** benannt, die den Nachweis der Zustellung elektronischer Dokumente durch **elektronisches Empfangsbekenntnis** ermöglichen sollen (§ 174 Abs. 4).[6] 95

Alternativ zur DE-Mail-Infrastruktur kann die Übermittlung nach § 130a Abs. 4 Nr. 2 zwischen einem **besonderen elektronischen Anwaltspostfach** und der elektronischen Poststelle des Gerichts erfolgen. Standardmäßig werden die Nachrichten Ende-zu-Ende verschlüsselt.[7] Einzurichten hat das besondere elektronische Anwaltspostfach die Bundesrechtsanwaltskammer (§ 31a BRAO). Dieser Teil der Neuregelung tritt am 1. Januar 2018 in Kraft. Die damit ermöglichten elektronischen Zustellungen bergen für den Zustellungsempfänger die Gefahr der Versäumung von Fristen, wenn er nicht beachtet, dass die Erlangung der elektronischen Verfügungsmacht den Zugangszeitpunkt markiert.[8] Die Rechtsprechung zur „physischen" Zustellung ist nicht übertragbar. 96

IV. Ausländische elektronische Signaturen

Das Gesetz über Rahmenbedingungen für elektronische Signaturen v. 16.5.2001 (BGBl. I 2001, 876) stellt in § 23 Abs. 1 unter den dort bezeichneten Voraussetzungen die elektronischen Signaturen mit einem **ausländischen qualifizierten Zertifikat** aus einem anderen Mitgliedstaat der EU oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum gleich. Durch dieses Gesetz ist die Richtlinie 1999/93/EG des Europäischen Parlamentes und des Rates v. 13.12.1999 (ABl. EG Nr. L 13 2000, S. 2) in nationales Recht transformiert worden. 97

1 *Roßnagel* NJW 2011, 1473, 1477.
2 Dazu auch *Spindler* CR 2011, 309, 315; *Preuß* ZZP 125 (2012), 135, 167.
3 Geltung ab 1.7.2014.
4 Geltung am 1.7.2014.
5 BGBl. I 2013, 3786.
6 Dazu *Hoffmann/Borchers* CR 2014, 62, 64.
7 *Hoffmann/Borchers* CR 2014, 62, 65.
8 Vgl. dazu den Fall österr. OGH ÖJZ 2014, 471.