Kapitel 3 Anwendung und Zusammenfassung der Ergebnisse

§ 11 Anwendung der Ergebnisse auf verschiedene Account-Typen

Nachfolgend wird die entwickelte Lösung über die allgemeine Rechtsscheinhaftung[1] zu den Beweiserleichterungen[2] auf die unterschiedlichen Accounts angewandt. Die verschiedenen Account-Typen sind nach der Sicherheit ihrer verwendeten Authentisierungsmethode geordnet. **830**

I. Internetanschluss, IP-Adresse

1. Rechtsscheinhaftung

Es ist zwar davon auszugehen, dass bei einem Internetanschluss die Identität des Anschlussinhabers vor Vertragsschluss zuverlässig überprüft wird,[3] was eine der Voraussetzungen für die Anerkennung des Rechtsscheintatbestandes ist.[4] Ein Rechtsschein dafür, dass der Account-Inhaber gehandelt hat, kann aufgrund einer Verbindung, bei der der Rechner sich mit seiner IP-Adresse ausgewiesen hat, jedoch aus zwei Gründen nicht erfolgen. Zum einen kann an der korrekten Zuordnung von IP-Adresse zum Anschluss gezweifelt werden,[5] sodass die Sicherheit der Authentisierungsmethode[6] den zuverlässigen Rückschluss auf den Account-Inhaber nicht zulässt. Ferner werden Internetanschlüsse regelmäßig von mehreren Benutzer verwendet, sodass selbst bei einer zuverlässigen Zuordnung von einer IP-Adresse zum Anschluss kein Rückschluss auf die handelnde Person möglich ist.[7] Eine Rechtsscheinhaftung für den missbräuchlichen Abschluss von Verträgen über einen Internetanschluss scheidet somit aus. Für einen Missbrauch, der **831**

1 Oben Rn. 489 ff.
2 Oben Rn. 772 ff.
3 Oben Rn. 39.
4 Oben Rn. 595 ff.
5 Oben Rn. 45.
6 Oben Rn. 534 ff.
7 Oben Rn. 47.

Verbindungsentgelte zur Folge hat, haftet der Anschlussinhaber jedoch nach § 45i Abs. 4 S. 1 TKG.[8]

2. Beweiserleichterungen

832 Beim Internetanschluss[9] stellt sich die Frage, ob anhand einer IP-Adresse mit anschließend ermitteltem Anschlussinhaber eine Beweiserleichterung in Betracht kommt. Eine Beweislastumkehr[10] kommt nicht in Betracht, weil der Geschäftsgegner zahlreiche andere Möglichkeiten hat, eine mögliche Beweisnot zu vermeiden.[11] Tatsächliche Vermutung[12] und Anscheinsbeweis[13] scheiden aus, weil es der Lebenserfahrung widerspricht, dass der Anschlussinhaber alleiniger Verwender eines häuslichen Internetanschlusses ist. Die Beweiserleichterungen beim Bildschirmtext[14] lassen sich nicht auf Internetanschlüsse übertragen, weil Bildschirmtext einen viel stärkeren Fokus auf den Abschluss von Rechtsgeschäften hatte, wohingegen das Internet primär ein allgemeines Informations- und Teilnahmebedürfnis befriedigt.

833 Die Beweiserleichterungen bei deliktischen Ansprüchen zeigen, dass solche auch bei der rechtsgeschäftlichen Haftung in Betracht kommen. Bei Urheberrechtsverletzungen besteht eine tatsächliche Vermutung dafür, dass der Anschlussinhaber verantwortlich ist.[15] Die tatsächliche Vermutung wird – anders als hier[16] – zur Begründung einer sekundären Darlegungslast[17] ver-

8 Ausführlich oben Rn. 521.
9 Oben Rn. 39.
10 Oben Rn. 776.
11 Oben Rn. 657 ff.
12 Oben Rn. 781.
13 Oben Rn. 785.
14 Oben Rn. 808.
15 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 12; Urteil v. 15. 11. 2012, I ZR 74/12 (Morpheus) – NJW 2013, 1441, Rn. 33; Urteil v. 8. 1. 2014, I ZR 169/12 (BearShare), Rn. 15; *OLG Hamm*, Urteil v. 27. 10. 2011, 22 W 82/11 – MMR 2012, 40, 40 f.; *OLG Köln*, Urteil v. 11. 9. 2009, 6 W 95/09 – MMR 2010, 44, 45; Urteil v. 23. 12. 2009, 6 U 101/09 – MMR 2010, 281; Beschluss v. 24. 3. 2011, 6 W 42/11 – MMR 2011, 396, 397; *LG Düsseldorf*, Urteil v. 21. 3. 2012, 12 O 579/10 – NJW 2012, 3663, 3663 f.
16 Oben Rn. 781.
17 Oben Rn. 792.

wendet.[18] Der Gedanke, der hinter dieser Beweiserleichterung steht, lässt sich übertragen. Der Internetanschluss befindet sich in der räumlichen Sphäre des Anschlussinhabers, sodass er den Zugang zu diesem kontrollieren kann. Eine sekundäre Darlegungslast kommt somit in Betracht. In deren Rahmen hat der Anschlussinhaber darzulegen, dass er nicht der Einzige ist, der den Internetanschluss benutzt. Bei einem Mehrpersonenhaushalt reicht dafür bereits die Tatsache, dass der Anschlussinhaber nicht alleine in dem Haushalt wohnt. Ferner kann der Anschlussinhaber durch Ortsabwesenheit zur fraglichen Zeit eventuell sogar den vollen Negativbeweis erbringen, dass er eine gewisse Handlung mit einem Rechner nicht vorgenommen hat.

II. E-Mails

1. Rechtsscheinhaftung

Bei dem Versand von E-Mails[19] fehlt es an beiden Voraussetzungen für die Anerkennung eines Rechtsscheintatbestandes. Die notwendige Sicherheit des Authentisierungsverfahrens[20] ist nicht gegeben. Zum einen kann eine E-Mail auch ohne Authentisierung beim SMTP-Server versendet werden.[21] Zum anderen ist die Absender-Angabe einer E-Mail nur eine Header-Information, die beliebig gesetzt werden kann.[22] Ebenso wie auf einen Brief ein beliebiger Absender geschrieben werden kann, kann der Versender einer Mail frei gewählt werden. Eine zuverlässige Überprüfung der Identität des Account-Inhabers findet nicht statt,[23] sodass die zweite Voraussetzung des Rechtsscheintatbestandes, eine zuverlässige Identifikationsfunktion,[24] nicht erfüllt ist. Der Empfang einer E-Mail begründet daher keinen Rechtsschein dafür, dass der Inhaber des E-Mail-Accounts gehandelt hat.[25] **834**

18 *BGH*, Urteil v. 12. 5. 2010, I ZR 121/08 (Sommer unseres Lebens) – BGHZ 185, 322, Rn. 12.
19 Oben Rn. 48.
20 Oben Rn. 534 ff.
21 Oben Rn. 49.
22 Zu diesem sog. Mail-Spoofing oben Rn. 212.
23 Oben Rn. 51 ff.
24 Oben Rn. 595 ff.
25 Im Ergebnis ebenso *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 257; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger/Wiebe*, 21, 34; *Reese*, S. 52; *Ultsch*, DZWir 1997, 466, 470.

2. Beweiserleichterungen

835 Bei der Frage, ob bei E-Mails[26] eine Beweiserleichterung in Betracht kommt, soll zunächst die in der Literatur diskutierte Frage des Anscheinsbeweises aufgegriffen werden.[27] Ob ein Beweis des ersten Anscheins[28] dafür spricht, dass eine E-Mail tatsächlich vom angegebenen Absender versendet wurde,[29] ist umstritten. Teilweise wird dieser Anscheinsbeweis hauptsächlich unter Berufung auf rechtsökonomische Erwägungen bejaht.[30] Herrschend wird hingegen angenommen, dass ein solcher Anscheinsbeweis nicht besteht und der Anspruchsteller die Urheberschaft der E-Mail voll beweisen muss.[31]

836 Für einen Anscheinsbeweis wird die rechtsökonomische Erwägung herangezogen, dass ansonsten der Absender der Erklärung ein „Widerrufsrecht kraft Beweislastverteilung" habe.[32] Dem Rechtsverkehr solle nicht zugemutet werden, dass er in einer Papierwirtschaft mit Rückbestätigungen per E-Mail geschlossener Verträge operiert.[33] Die effektive Durchsetzung von Ansprüchen solcher Verträge würde ohne den Anscheinsbeweis erheblich beeinträchtigt werden.[34] Dagegen ist jedoch einzuwenden, dass das reine Vertrauen auf ein unsicheres Medium nicht deren rechtliche Schutzbedürftigkeit begründet. Wenn sich Vertragspartner einen einfachen, kostengünstigen, aber unsicheren Kommunikationskanal aussuchen, was ihnen mög-

---

26 Oben Rn. 48.

27 Zum Beweiswert von E-Mails siehe *Sander*, CR 2014, 292, 293 ff.

28 Oben Rn. 785.

29 Zur Frage der Beweiserleichterungen für den Zugang von E-Mails *Willems*, MMR 2013, 551.

30 *Mankowski*, NJW 2002, 2822; *ders.*, CR 2003, 44; *ders.*, MMR 2004, 181; *Winter*, JurPC Web-Dok., 71/2002, Rn. 14; wohl auch *Haug*[2], Rn. 726; ohne Begründung *AG Hannover*, Urteil v. 20. 12. 1999, 518 C 13916/99 – WuM 2000, 412.

31 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *AG Bonn*, Urteil v. 25. 10. 2001, 3 C 193/01 – CR 2002, 301; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128; *Bergfelder*, S. 346; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 309 f.; *Ernst*, Vertragsgestaltung, Rn. 24; *ders.*, MDR 2003, 1091, 1092; *Jandach*, in: FS Kilian, 443, 451; *Kitz*, in: *Hoeren*/*Sieber*/*Holznagel*, Kap. 13.1 Rn. 69; *F. A. Koch*, Internet-Recht[2], S. 116; *Redeker*, IT-Recht[5], Rn. 906; *Roßnagel*, K&R 2003, 84, 85; *Roßnagel*/*Pfitzmann*, NJW 2003, 1209; *Wiebe*, MMR 2002, 128; *ders.*, MMR 2002, 257, 258.

32 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181.

33 *Mankowski*, MMR 2004, 181, 182.

34 Ebd.

lich bleiben muss,[35] verzichten sie bewusst auf den erhöhten Schutz durch die Rechtsordnung. Sie müssen ihrem Vertragspartner ein entsprechendes Vertrauen entgegenbringen oder sich über alternative Möglichkeiten,[36] wie eine Vorleistungspflicht der Gegenseite, absichern. Ferner wird argumentiert, dass die Verneinung eines Anscheinsbeweises eine Beweislastumkehr zu seinen Lasten darstelle,[37] weil der Empfänger keine Möglichkeit hat, das Absenden der E-Mail zu beweisen. Dies verkennt die grundsätzliche Beweislastverteilung.[38] Mit dem Anscheinsbeweis muss vielmehr eine von dem Normalfall abweichende Beweiserleichterung gerechtfertigt werden.

Dogmatisch wird der Anscheinsbeweis mit einem aus der Lebenserfahrung stammenden Erfahrungssatz begründet, dass E-Mails regelmäßig vom behaupteten Aussteller stammen.[39] Diese Erfahrung stammt aus der eigenen Wahrnehmung von *Mankowski*,[40] was jedoch wegen der Vielseitigkeit des Einsatzes von E-Mails nicht als ausreichende Erfahrungsgrundlage angesehen werden kann.[41] Selbst der empirische Nachweis, dass die Mehrzahl von E-Mails vom behaupteten Empfänger stammen,[42] begründet nur eine überwiegende Wahrscheinlichkeit, keine Typizität. Eine kausale Verbindung zwischen der Vermutungsbasis und der vermuteten Tatsache lässt sich daraus nicht herleiten.[43] Zu einem solchen Erfahrungssatz führt nur die selektive Wahrnehmung der zugestellten E-Mails. Bei Berücksichtigung der zahlreichen Spam- und Phishing-Mails, die häufig von entsprechenden Filtern aussortiert werden und nicht in den Posteingang des E-Mail-Kontos gelangen, lässt sich sogar an der empirischen Grundlage zweifeln.[44] Bei diesen Mails ist es üblich, dass falsche Absender verwendet werden, um den dadurch getäuschten Nutzer zu einer Interaktion zu motivieren. **837**

Für das Vorliegen des Erfahrungssatzes, der behauptete Absender stimme mit dem tatsächlichen Verfasser überein, wird ferner vorgebracht, dass **838**

35 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1214.
36 Dazu oben Rn. 657 ff.
37 *Haug*[2], Rn. 726.
38 Oben Rn. 772.
39 *Mankowski*, CR 2003, 44, 45.
40 *Mankowski*, NJW 2002, 2822, 2824.
41 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
42 Siehe *Ernst*, MDR 2003, 1091, 1092.
43 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211 f.; *Roßnagel*, K&R 2003, 84, 85.
44 *F. A. Koch*, Internet-Recht[2], S. 116, was ohne den daraus folgenden Schluss erkannt wird von *Mankowski*, NJW 2002, 2822, 2823.

die Wahrscheinlichkeit von Eingriffen gering sei.[45] Der bloße Verweis auf die Unsicherheit des Internets reiche nicht aus.[46] Eine Manipulation stelle eine absolute Ausnahme dar.[47] Die vielfältigen Möglichkeiten E-Mails zu fälschen sprechen bereits dagegen, dass Verfälschungen eine Ausnahme seien.[48] Die Behauptung, dass es an einer einfach umzusetzenden technischen Möglichkeit der Verfälschung von E-Mails fehle,[49] kann leicht widerlegt werden. Der Absender einer E-Mail ist eine Header-Information, die beliebig gewählt werden kann.[50] Ein Dritter kann daher problemlos über einen fremden Namen E-Mails über einen beliebigen SMTP-Server verschicken. Diese Möglichkeit solle dem Anscheinsbeweis nicht entgegen stehen, weil dieser Maskerade-Angriff durch den Zustellungsweg im Mail-Header, der nicht vom üblichen SMTP-Server initiiert ist, nachvollziehbar sei. Ein Maskerade-Angriff, der nicht aufdeckbar ist, sei nur schwer zu bewerkstelligen.[51] Dagegen ist jedoch einzuwenden, dass durch die mangelnde Authentisierung bei SMTP-Servern häufig auch das Senden über den vom Account-Inhaber benutzten SMTP-Server möglich ist.[52] Darüber hinaus kann es durchaus vorkommen, dass der Dritte eigene Zugangsdaten zum SMTP-Server besitzt, mit denen er sich authentisieren kann. Ein Mitarbeiter kann beispielsweise eine scheinbar von seinem Arbeitskollegen stammende E-Mail absetzen oder der Kunde eines Freemail-Anbieters kann E-Mails mit der Absenderangabe anderer Kunden verschicken. Ferner kann der Dritte die Zugangsdaten des Account-Inhabers zum E-Mail-Konto ausspähen[53] oder ein E-Mail-Konto unter fremdem Namen anlegen.[54] Wegen der weltweiten Nutzbarkeit der E-Mail lässt sich kein Rückschluss auf eine Person oder einen Personenkreis herleiten, von dem die E-Mail stammen könnte.[55] Der Blick auf anerkannte Beweiserleichterungen hat gezeigt, dass ein so unsicheres System wie der E-Mail-Versand keine hinreichende Grundlage

45 *Mankowski*, CR 2003, 44, 45.
46 *Winter*, JurPC Web-Dok., 71/2002, Rn. 17.
47 *Mankowski*, NJW 2002, 2822, 2824.
48 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
49 *Mankowski*, CR 2003, 44, 45.
50 Oben Rn. 212.
51 *Sosnitza/Gey*, K&R 2004, 465, 468; *Mankowski*, NJW 2002, 2822, 2823.
52 *Roßnagel*, K&R 2003, 84; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1211.
53 Oben Rn. 124 ff.
54 Oben Rn. 210.
55 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.

für einen Anscheinsbeweis ist.[56] Beim Absenden einer E-Mail ist daher der Schluss auf den Account-Inhaber nicht möglich.[57]

839 Hinzu kommt, dass die Manipulation nicht beim Versenden der E-Mail erfolgen muss. E-Mails sind lediglich Text-Dateien, deren Schriftzeichen wie bei jeder anderen Datei verändert werden können. Bei jeder Station, die eine E-Mail vom Absender zum Empfänger macht, kann ihr Inhalt verändert werden.[58] Der Empfänger kann den Mail-Header nachträglich ändern,[59] oder den Inhalt der E-Mail auf eine für ihn bessere Version ändern. Sämtliche nachträgliche Veränderungen der E-Mail sind nicht nachweisbar.[60] Eine E-Mail hat daher noch nicht einmal den Beweiswert einer nicht unterzeichneten mit Bleistift in Druckbuchstaben geschriebenen Postkarte.[61] Diese Möglichkeit die E-Mail nachträglich zu verändern, schließt die Anerkennung eines Anscheinsbeweises aus.[62]

840 Für den Anscheinsbeweis solle sprechen, dass es an Motiven und Anreizen fehle, E-Mails unter fremdem Namen zu versenden.[63] Dagegen spricht zunächst, dass sich in der Rechtsprechung Fälle finden lassen, bei denen scheinbar grundlos die Zugangsdaten eines Account-Inhabers missbraucht wurden.[64] Ferner zeigen die zahlreichen Phishing-Mails, dass Kriminelle sich materielle Vorteile davon versprechen, E-Mails unter falscher Absenderangabe zu versenden. Darüber hinaus gibt es durchaus zahlreiche Anwendungsbeispiele, bei denen ein rational nachvollziehbares Motiv für eine gefälschte Absender-Adresse vorhanden ist. Ein Angreifer bei einem Social-Engineering-Angriff[65] kann beispielsweise vor seinem Anruf als vermeintlicher technischer Ansprechpartner eine E-Mail, die scheinbar vom Vorgesetzten des Opfers stammt, in der er den Anruf ankündigt und um Zusammenarbeit bittet, verschicken.

---

56 Oben Rn. 826.
57 *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.
58 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1210.
59 Ebd., 1210.
60 *Ernst*, MDR 2003, 1091, 1092.
61 *Roßnagel*, K&R 2003, 84.
62 *AG Bonn*, Urteil v. 25. 10. 2001, 3 C 193/01 – CR 2002, 301; *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1210.
63 *Mankowski*, CR 2003, 44, 45; *ders.*, MMR 2004, 181, 182.
64 Oben Rn. 634.
65 Dazu oben Rn. 162.

841 Darüber hinaus sollen die strafrechtlichen Konsequenzen eines Missbrauchs, der nachträglichen Veränderung oder eines Prozess-Betruges ausreichend vor diesen schützen.[66] Strafrechtliche Konsequenzen schrecken jedoch insbesondere nur ab, wenn die Möglichkeit der Aufdeckung besteht. Da nachträgliche Veränderungen nicht bewiesen werden können und es zahlreiche Wege gibt, wie eine E-Mail ohne Absenden durch den behaupteten Absender zum Empfänger gelangen kann, ist dem möglichen Straftäter die Straftat nur schwer nachzuweisen. Ferner kommen Täuschungshandlungen wie der Prozessbetrug häufig vor.[67] Die strafrechtlichen Konsequenzen halten die im Zivilprozess streitenden Parteien anscheinend nicht davon ab, die Unwahrheit zu behaupten. Wer behauptet, dass die strafrechtlichen Konsequenzen eines Prozessbetrugs einen Anscheinsbeweis für die Echtheit einer E-Mail begründen, muss sich fragen lassen, ob mit diesem Argument, nicht auch ein Anscheinsbeweis dahingehend besteht, dass alles, was Prozessparteien vortragen, der Wahrheit entspricht. Die Absurdität eines solchen Anscheinsbeweises zeigt, dass das Argument der drohenden Strafbarkeit nicht für einen Anscheinsbeweis der Echtheit von E-Mails spricht.

842 Ferner solle die Erschütterung des Anscheinsbeweises, beispielsweise durch Zeugenbeweis, einfach möglich sein, sodass der Anscheinsbeweis den Absender nicht übermäßig belaste.[68] Der Absender könne beispielsweise Einblicke in sein System gewähren, um zu zeigen, dass die E-Mail sich nicht in seinem Postausgang oder Papierkorb befinde.[69] Diese Behauptung verkennt jedoch zwei entscheidende Merkmale. Zum einen können E-Mails so gelöscht werden, dass keine Spuren mehr von ihnen auf dem eigenen Mail-Server zu finden sind. Ebenso wie einen normalen Papierkorb kann man auch die elektronischen Papierkörbe leeren.[70] Zum anderen könnte das Fehlen der E-Mail im System des Account-Inhabers zahlreiche Gründe haben. Die E-Mail könnte von einem anderen Rechner versendet worden sein, sodass sie im Postausgang des einen Rechners nicht auftaucht, wenn sie nicht auf allen Endgeräten per IMAP synchron gehalten werden. Zum anderen ist der Beweis der negativen Tatsache, dass der Account-Inhaber die E-Mail nicht versendet hat, nur schwer zu führen. Dem Account-Inhaber wird

66 *Mankowski*, NJW 2002, 2822, 2825; *ders.*, MMR 2004, 181, 182; *Winter*, JurPC Web-Dok., 71/2002, Rn. 14.
67 Siehe *Krell*, JR 2012, 102.
68 *Mankowski*, MMR 2004, 181, 182 f.
69 *Mankowski*, CR 2003, 44, 49.
70 Was ebd., 49 anscheinend verkennt.

es schwer fallen, die Vermutungsbasis zu erschüttern.[71] Es wird behauptet, dass der Anspruchsteller die Urheberschaft der E-Mail nur beweisen müsse, wenn sich der Missbrauch aufdränge.[72] Dies verkennt die zahlreichen Möglichkeiten, die zur Verfälschung eines E-Mail-Absenders oder einer E-Mail bestehen. Häufig ist unaufklärbar, wie ein Dritter den Missbrauch bewerkstelligt hat. Der Account-Inhaber würde damit durch die allgemeine Systemrisiken belastet, die er ebenso wenig wie der Erklärungsempfänger kontrollieren kann. Dies wäre unbillig.

Für den Anscheinsbeweis soll darüber hinaus sprechen, dass E-Mail-Adressen auf einer einmaligen, exklusiven Zuordnung zu einem Inhaber beruhen.[73] Dies verkennt jedoch, dass zahlreiche E-Mail-Adressen nicht einem Inhaber in Form einer natürlich Person zugeordnet sind, sondern eine Gruppe von Empfängern oder eine funktionale Einheit erreicht.[74] E-Mail-Adressen wie info@firma.de, no-reply@newsletter-versender.de oder vorstand@verein.de sind gerade nicht einem Inhaber zugeordnet. **843**

Darüber hinaus sprechen systematische Argumente gegen die Anerkennung des Anscheinsbeweises. Im Umkehrschluss zu § 371a Abs. 1 S. 2 ZPO, der Nachfolgeregelung zu § 292a ZPO,[75] soll ein Anscheinsbeweis bei E-Mails gerade nicht bestehen.[76] Der Wortlaut des § 371a Abs. 1 S. 2 ZPO sperrt keine anderweitigen Anscheinsbeweise.[77] Ferner zeigt der Vergleich mit den Schrifturkunden, dass die Anerkennung eines Anscheinsbeweises in systematischem Widerspruch zu der Wertung des § 440 Abs. 1 ZPO steht. Weil bei diesen der sich auf die Urkunde Berufende deren Echtheit zu beweisen hat, muss dies erst recht für die Echtheit von E-Mails gelten.[78] Der Blick auf anerkannte Beweiserleichterungen in vergleichbaren Situationen hat gezeigt, dass für den Anscheinsbeweis eine hinreichend sichere Authentisierungsmethode sowie eine zuverlässige Identifizierung des Account-Inhabers beim Anlegen des Accounts erforderlich ist.[79] Beides fehlt bei der **844**

71 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213.
72 *Winter*, JurPC Web-Dok., 71/2002, Rn. 17.
73 *Mankowski*, MMR 2004, 181, 183.
74 Oben Rn. 57.
75 Dazu oben Rn. 801 ff.
76 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213; *Roßnagel*, K&R 2003, 84, 86; *Wiebe*, MMR 2002, 257, 258.
77 *Mankowski*, NJW 2002, 2822, 2827; *ders.*, CR 2003, 44, 47; *Sosnitza/Gey*, K&R 2004, 465, 466; *Winter*, JurPC Web-Dok., 71/2002, Rn. 12.
78 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1212; *Roßnagel*, K&R 2003, 84, 85.
79 Oben Rn. 826.

E-Mail, sodass die Annahme eines Anscheinsbeweises gängigen Wertungen widersprechen würde.

845 Ferner würde die Anerkennung eines Anscheinsbeweises falsche Anreize setzen.[80] Die Behauptung, dass eine missbräuchliche Berufung auf den Anscheinsbeweis kaum vorstellbar sei,[81] kann leicht widerlegt werden. Wenn einfach zu fälschende E-Mails als rechtssicherer Beweis anerkannt werden, könnte ein Krimineller in betrügerischer Absicht, eine E-Mail von jeder Person fälschen, deren E-Mail-Adresse und ladungsfähige Anschrift er kennt, und diese mit Zahlungsansprüchen konfrontieren. Durch die Anerkennung eines Anscheinsbeweises würde ein starker Anreiz zur Fälschung von E-Mails geschaffen werden.[82] Ein Anscheinsbeweis für E-Mails ist somit abzulehnen.

846 Eine tatsächliche Vermutung[83] dafür, dass eine E-Mail vom Account-Inhaber stammt scheidet somit erst recht aus. Eine sekundäre Darlegungslast[84] sowie eine Umkehr der Beweislast[85] scheitern daran, dass einige Missbrauchsmöglichkeiten, wie das Mail-Spoofing,[86] außerhalb der Sphäre des Account-Inhabers stammen.

III. Benutzerkonten auf Internetseiten

1. Rechtsscheinhaftung

a) Informationsportale und Online-Shops

847 Bei Benutzerkonten auf Internetseiten muss bezüglich der Rechtsscheinhaftung wegen der Vielfalt der unterschiedlichen Arten differenziert werden. Bei einem Account auf einem Informationsportal, bei dem Personendaten zur Registrierung nicht erforderlich sind,[87] scheitert der Rechtsscheintatbestand bereits an einer irgendwie gearteten Identifikationsfunktion.[88] Selbst

80 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213.
81 *Mankowski*, CR 2003, 44, 48.
82 *Roßnagel/Pfitzmann*, NJW 2003, 1209, 1213.
83 Oben Rn. 781.
84 Oben Rn. 792.
85 Oben Rn. 776.
86 Oben Rn. 212.
87 Siehe dazu oben Rn. 60.
88 Oben Rn. 595 ff.

bei Online-Shops, die mutmaßlich ein starkes Interesse an der Solvenz ihrer Vertragspartner haben, ist keine hinreichend zuverlässige Identifikationsfunktion vorhanden.[89] Ein Rechtsscheintatbestand scheidet bei diesen Accounts somit regelmäßig aus.

b) Internet-Auktionsplattformen

Benutzerkonten auf Internetseiten mit Reputationssystem hingegen wird häufig eine Identifikationsfunktion bezüglich einer numerischen Identität zugesprochen.[90] Diese wird häufig pauschal behauptet,[91] wobei die Ausführungen darauf hindeuten, dass der Account den Account-Inhaber identifizieren soll. Zur Begründung der Identifikationsfunktion werden zwei Argumente genannt: die Geheimhaltungspflicht des Passworts sowie die Überprüfung der Angaben bei der Registrierung. **848**

Die Geheimhaltungspflicht des Passworts kann eine Identifikationsfunktion bezüglich des Account-Inhabers nicht überzeugend begründen.[92] Zum einen erfolgt die Begründung von Identifikationsfunktion und Geheimhaltungspflicht häufig zirkulär.[93] Zum anderen betrifft die Geheimhaltungspflicht lediglich die Sicherheit der verwendeten Authentisierungsmethode.[94] Die Identifikationsfunktion sowie deren Zuverlässigkeit muss jedoch durch die Art des Accounts sowie die Überprüfung der angegebenen Personendaten bei der Registrierung erfolgen.[95] **849**

Die Angabe der Daten bei der Registrierung und deren Plausibilitätskontrolle durch die Internet-Auktionsplattform kann keine Identifikationsfunktion bezüglich des Account-Inhabers überzeugend begründen. Zwar muss **850**

89 Oben Rn. 62.

90 *BGH*, Urteil v. 11. 3. 2009, I ZR 114/06 (Halzband) – BGHZ 180, 134, Rn. 18; Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *Genius*, jurisPR-BGHZivilR 12/2011, Anm. 1, C; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger*/*Wiebe*, 21, 34; *J. Hoffmann*, in: *Leible*/*Sosnitza*, Rn. 174; *Klein*, MMR 2011, 450; *Mankowski*, CR 2007, 606; *Stöber*, JR 2012, 225, 228.

91 Vgl. etwa *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18.

92 So aber *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *Herresthal*, K&R 2008, 705, 708; *ders.*, in: *Taeger*/*Wiebe*, 21, 34.

93 Oben Rn. 558.

94 Dazu allgemein oben Rn. 534 ff.

95 Oben Rn. 595 ff.

ein Nutzer seinen Namen und seine Adresse bei der Registrierung angeben.[96] Einer Person können diese Daten jedoch nur zuverlässig zugeordnet werden, wenn diese Daten auch überprüft werden. Die Überprüfung der E-Mail-Adresse reicht zur Identifizierung des Account-Inhabers nicht aus.[97] Die E-Mail-Adresse hat keinerlei Identifikationsfunktion bezüglich einer numerischen Identität einer Person,[98] sodass aus ihrer Überprüfung keine Identifikationsfunktion für einen Account abgeleitet werden kann. Auch die Plausibilitätskontrolle der Daten durch einen Abgleich mit der Schufa kann keine Identifikationsfunktion bezüglich der numerischen Identität des Namensträgers begründen.[99]

851 Als Zwischenergebnis lässt sich festhalten, dass die Registrierung bei einer Internet-Auktionsplattform keine Identifikationsfunktion bezüglich der numerischen Identität des Account-Inhabers herstellt. Ein Account bei einer Internet-Auktionsplattform mit Reputationssystem identifiziert daher nur die virtuelle Identität des Erstellers und nicht die numerische Identität des Account-Inhabers. Die überwiegende Zahl der Accounts bei solchen Plattformen sind vom jeweiligen Account-Inhaber erstellt. Wegen der zahlreichen Möglichkeiten einen Account unter falschem Namen zu eröffnen und erfolgreich zu betreiben, kann jedoch keine zuverlässige Identifikationsfunktion angenommen werden. Darüber hinaus kann angenommen werden, dass zahlreiche Accounts unter falschem Namen angelegt wurden, wenn sich ein betroffener Namensträger sogar durch den gesamten Instanzenzug klagen muss, um sich gegen falsche Accounts auf seinen Namen zu wehren.[100]

852 Man kann jedoch überlegen, ob eine zuverlässige Identifizierung des Account-Inhabers später durch das Reputationssystem[101] geschaffen wird. Doch selbst ein Reputationssystem begründet keine hinreichend zuverlässige Überprüfung der Zuordnung des Accounts zum Account-Inhaber.[102] Die Voraussetzung der zuverlässigen Identifikation[103] zur Anerkennung eines

96 *Gurmann*, S. 18 f.; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 174.

97 *Gurmann*, S. 19; **a.A.** *Stöber*, JR 2012, 225, 228. Dazu bereits oben Rn. 598.

98 Oben Rn. 48. Für die E-Mail-Adresse erkennt *Stöber*, dass ohne Identitätsüberprüfung keine Identifikationsfunktion bestehen kann, ebd., 229.

99 Oben Rn. 608.

100 Vgl. *BGH*, Urteil v. 10. 4. 2008, I ZR 227/05 (Namensklau im Internet) – NJW 2008, 3714.

101 Wie beispielsweise eBay es betreibt, dazu oben Rn. 66.

102 Oben Rn. 620.

103 Oben Rn. 595 ff.

Rechtsscheintatbestandes ist somit bei Benutzerkonten auf Internetseiten regelmäßig nicht gegeben. Die in der Regel anzutreffende rein wissensbasierte Authentisierung bietet darüber hinaus keine hinreichende Gewähr dafür, dass der Account-Inhaber handelt, sodass die Anerkennung des Rechtsscheintatbestandes auch daran scheitert.[104] Ein Rechtsscheintatbestand dafür, dass der Account-Inhaber eines passwortgeschützten Benutzerkontos auf einer Internetseite selbst gehandelt hat, besteht somit nicht.[105]

c) Accounts mit Zwei-Faktor-Authentisierung

Setzen Benutzerkonten im Internet eine Zwei-Faktor-Authentisierung[106] ein, verwenden sie eine hinreichend sichere Authentisierungsmethode für die Anerkennung eines Rechtsscheintatbestandes.[107] Zahlreiche Anbieter setzen mittlerweile zur Absicherung eine Zwei-Faktor-Authentisierung ein.[108] Eine Rechtsscheinhaftung bei Missbrauch dieser Accounts kommt jedoch nur in Betracht, wenn der Account-Inhaber bei der Registrierung oder später zuverlässig identifiziert wurde,[109] was bei den genannten Beispielen nicht gegeben ist. Eine Rechtsscheinhaftung kann bei diesen Beispielen somit nur in Einzelfällen in Betracht kommen, wenn der Account-Inhaber gegenüber dem Geschäftsgegner das Zutreffen der Identitätsbehauptung des Accounts bestätigt hat.[110] **853**

2. Beweiserleichterungen

Bei Benutzerkonten auf Internetseiten werden unterschiedliche Formen der Beweiserleichterung diskutiert. Zunächst soll untersucht werden, ob ein An- **854**

104 Zur Unsicherheit der rein wissensbasierten Authentisierung oben Rn. 544 ff.

105 Im Ergebnis auch *BGH*, Urteil v. 11. 5. 2011, VIII ZR 289/09 (VIP-Bareinrichtung) – BGHZ 189, 346, Rn. 18; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 57; *M. Wolf/Neuner*[10], § 50 Rn. 108; **a.A.** *Borges*, NJW 2011, 2400, 2402; *Herresthal*, K&R 2008, 705, 708 f.; *ders.*, in: *Taeger/Wiebe*, 21, 34 f.; *Stöber*, JR 2012, 225, 229 f.

106 Dazu oben Rn. 117 ff.

107 Oben Rn. 578 ff.

108 Beispielsweise bieten Google und Facebook dies an, dazu *J. Schmidt*, heise online v. 11. 2. 2011; *ders.*, heise online v. 13. 5. 2011.

109 Oben Rn. 595 ff.

110 Oben Rn. 623.

scheinsbeweis bei Benutzerkonten auf Internet-Auktionsplattformen in Betracht kommt und anschließend, ob für sämtliche Formen der Benutzerkonten auf Internetseiten eine sekundäre Darlegungslast des Account-Inhabers begründet ist.

a) Anscheinsbeweis

855 Die Frage, ob ein Anscheinsbeweis[111] dafür spricht, dass der Account-Inhaber eine vorliegende Erklärung über den Account abgegeben hat, ist umstritten. Dies wird zum Teil aus rechtsökonomischen Erwägungen und wegen der zahlreichen problemlos verlaufenden Fälle angenommen.[112] Überwiegend wird ein Anscheinsbeweis jedoch unter Verweis auf den Sicherheitsstandard im Internet abgelehnt.[113]

856 Für den Anscheinsbeweis wird insbesondere die teleologische Erwägung angeführt, dass der Account-Inhaber nicht die Möglichkeit haben darf, sich von einem ungewollten Vertrag zu lösen.[114] Das Vertrauen in den elektroni-

111 Oben Rn. 785.

112 *Ernst*, Vertragsgestaltung, Rn. 26 ff.; *ders.*, MDR 2003, 1091, 1093; *Härting/Golz*, ITRB 2005, 137, 138; *Härting*[4], Rn. 584; *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 42 ff.; *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 183; *M. Köhler/Arndt/Fetzer*[7], Rn. 324; *Mankowski*, EWiR 2001, 1123, 1124; *ders.*, CR 2007, 606; *ders.*, CR 2011, 458.

113 *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, 594; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611; Urteil v. 20. 7. 2009, 2 U 50/09, I-2 U 50/09, Rn. 24; *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814; Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676; *OLG Naumburg*, Urteil v. 2. 3. 2004, 9 U 145/03 – OLG-NL 2005, 51; *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259; *LG Konstanz*, Urteil v. 19. 4. 2002, 2 O 141/01 A – CR 2002, 609; *LG Magdeburg*, Urteil v. 21. 10. 2003, 6 O 1721/03 (321) – CR 2005, 466, 467; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128; *AG Bremen*, Urteil v. 20. 10. 2005, 16 C 168/05 – NJW 2006, 518, 519; *Biallaß*, ZUM 2007, 397; *Borges*, in: Internet-Auktion, 214, 223; *Borges/Schwenk/Stuckenberg/Wegener*, S. 311; *Hanau*, Handeln unter fremder Nummer, S. 215; *Kitz*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.1 Rn. 67; *F. A. Koch*, Internet-Recht[2], S. 115; *Noack/Kremer*, AnwBl 2004, 602, 604; *Oechsler*, AcP 208 (2008), 565, 578; *ders.*, MMR 2011, 631, 632; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45b; *Wiebe*, Elektronische Willenserklärung, S. 435; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 58; *Dennis Werner*, K&R 2011, 499, 500.

114 *Mankowski*, CR 2011, 458; *Winter*, CR 2004, 219, 221.

schen Handel solle gestärkt werden, damit er nicht zum Erliegen komme.[115] Dieses Vertrauen stützte sich bei der rein wissensbasierten Authentisierung sogar auf drei vertrauensbegründende Momente: den Benutzernamen, das Passwort sowie deren Zusammenpassen.[116] Dagegen lässt sich jedoch einwenden, dass eine rein wissensbasierte Authentisierung unter den Nachteilen leidet, dass die Information des Geheimnisses unendlich teilbar ist und eine Kontrolle über die Verbreitung des Wissens nicht stattfinden kann.[117] Häufig beträgt die Kombination aus Benutzername und Passwort um die dreißig Zeichen,[118] wovon nur das Passwort geheim ist. Die Vertrauensbasis ist daher recht gering.

Die Lebenserfahrung hat ferner gezeigt, dass auch ohne einen starken **857**
rechtlichen Schutz dieses Vertrauens, der Handel über Internetplattformen unverändert fortbesteht.[119] Häufig liegen der Annahme des Anscheinsbeweises leicht zu widerlegende Grundannahmen bezüglich passwortgeschützter Accounts zu Grunde. Der Behauptung, dass Passwörter die Antwort auf die unsichere E-Mail seien,[120] ist zu widersprechen. Passwortgeschützte Accounts dienen dem Nutzer primär dazu, eine virtuelle Identität bei einem Authentisierungsnehmer zu erstellen. Daraus entstehen dem Nutzer beispielsweise die Vorteile, dass er auf der Seite wiedererkannt wird und Einblick in seine vorangegangen Aktionen, wie Bestellungen, nehmen kann oder seine Daten oder Präferenzen wegen der gespeicherten Informationen nicht erneut eingeben muss. Aus dem gleichen Grund ist der Behauptung, dass Passwörter zur Vermeidung von Kaufreue dienen sollen,[121] zu widersprechen. Mit diesen Behauptungen wird versucht, den passwortgeschützten Accounts eine nicht vorhandene Bedeutung zuzusprechen, die den Anscheinsbeweis mit der nicht vorhandenen Zweckrichtung rechtfertige. Vielmehr ist jedoch darauf einzugehen, ob die sich auf zahlreichen praktischen Vorteilen entwickelten Accounts die rechtlichen Anforderungen an den Anscheinsbeweis erfüllen.

115 *Mankowski*, EWiR 2001, 1123.
116 *Mankowski*, CR 2007, 606, 607; *ders.*, CR 2011, 458.
117 Oben Rn. 111.
118 Der Benutzername „max.mustermann@web.de“ sowie ein acht Zeichen langes Passwort ergeben zusammen 29 Zeichen.
119 Oben Rn. 385.
120 *Mankowski*, CR 2007, 606, 607; *ders.*, CR 2011, 458.
121 *Ernst*, MDR 2003, 1091, 1093.

858 Die angemessene Verteilung der Risiken beim Online-Handel solle ebenfalls einen Anscheinsbeweis rechtfertigen. Der Anspruchsteller solle eine reelle Chance haben, den Anspruch durchzusetzen.[122] Das Risiko des Missbrauchs dürfe nicht allein dem Erklärungsempfänger auferlegt werden,[123] weil sich beide Parteien diesem Risiko gleichermaßen aussetzen.[124] Dagegen ist jedoch einzuwenden, dass demjenigen, der sich auf ein Rechtsgeschäft einlässt, ohne sich durch unterschiedliche Möglichkeiten abzusichern[125] oder ohne sichere Beweismittel zu schaffen, das Risiko billigerweise aufgebürdet werden kann.[126] Im Offline-Bereich ist anerkannt, dass der Anbieter das Risiko missbräuchlicher Bestellung zu tragen hat.[127] Ein unberechtigtes Vertrauen in einen Vertragspartner muss nicht durch die Rechtsordnung geschützt werden. Der mündliche Vertragsschluss beispielsweise ist auch schwer zu beweisen, zum Beispiel unter Vertragspartnern, die sich kennen und vertrauen, jedoch auch ohne Schutz durch die Rechtsordnung üblich. Eine angemessene Risikoverteilung muss daher nicht zu einem Anerkennen des Anscheinsbeweises führen.

859 Sodann soll überprüft werden, ob die Voraussetzung des Anscheinsbeweises, dass ein Erfahrungssatz nach der allgemeinen Lebenserfahrung gegeben sein muss, vorliegt. Vielfach wird für den Anscheinsbeweis ins Felde geführt, dass die große Anzahl an problemlos verlaufenden Transaktionen sowie der prozentual geringe Anteil an Missbrauchsfällen einen für einen Anscheinsbeweis tauglichen Erfahrungssatz begründen.[128] Eine behauptete Seltenheit der Angriffe[129] sowie die unzutreffend[130] behauptete geringe Wahrscheinlichkeit einer Manipulation[131] sollen einen Anscheinsbeweis rechtfertigen. Die zahlreichen korrekt abgewickelten Geschäfte können den

122 *Winter*, CR 2004, 219, 221.
123 *Ernst*, MDR 2003, 1091, 1093.
124 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *Biallaß*, ZUM 2007, 397.
125 Zu den Möglichkeiten oben Rn. 657.
126 *Kuhn*, S. 257.
127 *F. A. Koch*, Internet-Recht[2], S. 115.
128 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44; *Wiebe/Neubauer*, in: *Hoeren/Sieber/Holznagel*, Kap. 15 Rn. 58; *M. Köhler/Arndt/Fetzer*[7], Rn. 324; *Winter*, CR 2004, 219, 221.
129 *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 184.
130 Oben Rn. 127.
131 *Mankowski*, EWiR 2001, 1123, 1124.

Anscheinsbeweis nicht begründen.[132] Eine empirische Statistik reicht nicht aus, weil diese nur eine Aussage bezüglich der statistischen Masse, nicht bezüglich des Einzelfalls trifft.[133]

Es ist daher entscheidend, ob ein Erfahrungssatz nach der Lebenser- **860**
fahrung vorliegt, dass über einen Account abgegebene Erklärungen vom Account-Inhaber stammen. Dafür ist entscheidend, wie die Zugangsdaten missbraucht werden können und wie wahrscheinlich dies ist. Der Anscheinsbeweis verlangt dafür keine absolute Sicherheit,[134] sondern nur eine Typizität. Ein Erfahrungssatz lässt sich wegen der Missbrauchsmöglichkeiten nur schwer annehmen.[135] Ferner liegen kaum Erkenntnisse darüber vor, wie wahrscheinlich verschiedene Geschehensabläufe sind. Neben dem Handeln des Account-Inhabers selbst, kann er die Zugangsdaten einem Dritten weitergeben,[136] der sie befugt oder unbefugt nutzt. Der Account-Inhaber könnte die Zugangsdaten jedoch auch notiert oder in der Schlüsselbund-Verwaltung gespeichert haben.[137] Beobachtungen dazu entstehen nur durch singuläre Betrachtungen, aus denen sich kein Erfahrungssatz ableiten lässt.[138] Die erforderliche Typizität lässt sich aus der Lebenserfahrung daher nicht feststellen.[139]

Ein Anscheinsbeweis kann daher nur als „Anscheinsbeweis ohne ersten **861**
Anschein“[140] über den Ausschluss alternativer Geschehensabläufe begründet werden.[141] Es kommt daher auf die Wahrscheinlichkeit der verschiedenen Geschehensabläufe an. Der Geschehensablauf, dass der Account-Inhaber mit seinen Zugangsdaten die Erklärung abgibt, muss zur Anerkennung des Anscheinsbeweises hoch wahrscheinlich sein. Für diese Wahrscheinlichkeit muss die rein wissensbasierte Authentisierung einen gewissen Si-

---

132 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.

133 Oben Rn. 787 sowie *BGH*, Urteil v. 27. 5. 1957, II ZR 132/56 (Einschreibbrief) – BGHZ 24, 308, 312.

134 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44.

135 *Oechsler*, AcP 208 (2008), 565, 578; *ders.*, MMR 2011, 631, 632.

136 Zur Weitergabe oben Rn. 125.

137 Oben Rn. 132 ff.

138 *BGH*, Urteil v. 4. 7. 1989, VI ZR 309/88 – NJW 1989, 2947. Dies ist bei der ec-Karte ähnlich *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 345.

139 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *LG Köln*, Urteil v. 27. 10. 2005, 8 O 15/05 – BeckRS 2006, 07259.

140 *Jungmann*, ZZP 120 (2007), 459.

141 Dazu oben Rn. 788.

cherheitsstandard aufweisen. Brute-Force-Attacken[142] müssen vom Authentisierungsnehmer erschwert werden und der Authentisierungsnehmer muss durch Vorgaben wie eine Mindestpasswortlänge sichere Passwörter erzwingen.[143] Dabei sind die Sicherungsmaßnahmen des Authentisierungsnehmers im Einzelfall zu untersuchen, weil es keinen gesetzlichen Standard für Passwörter gibt.[144]

862 Dabei besteht ferner das Problem, dass zur abschließenden Beurteilung der Wahrscheinlichkeit die Sicherheitsinfrastruktur des Authentisierungsnehmers detailliert bewertet werden muss. Denn wenn diese Schwachstellen aufweist, ist ein Missbrauch auch ohne Zutun des Account-Inhabers möglich.[145] Beim Missbrauch einer ec-Karte besteht dieses Problem in ähnlicher, aber schwächerer Form.[146] Der Authentisierungsnehmer wird regelmäßig keinen Einblick in seine Sicherheitsinfrastruktur geben, weil er die Sicherheit dadurch gefährden könnte.[147] Bei Zwei-Personen-Konstellationen, wie sie auch bei ec-Karten vorhanden sind, besteht die prozessuale Möglichkeit den Authentisierungsnehmer durch eine sekundäre Darlegungslast[148] im Rahmen des Zumutbaren zur Preisgabe der Informationen zu bewegen.[149] Da die Preisgabe von Informationen über die Sicherheitsinfrastruktur des Authentisierungsnehmers die Sicherheit gefährdet, ist ihm eine vollständige Offenlegung jedoch nicht zumutbar. Bei einer Drei-Personen-Konstellation, wie sie bei Internetauktions-Plattformen besteht, ist der Authentisierungsnehmer jedoch nicht Prozesspartei, sodass es im Prozess keine prozessuale Möglichkeit gibt, ihn zu Angaben über die Sicherheitsinfrastruktur zu bewegen. Ob die Sicherheit bei einem gewissen Authentisierungsnehmer eine hinreichende Wahrscheinlichkeit begründet, lässt sich daher mangels notwendiger Informationen nicht abschließend bestimmen.

863 Zwar ist zur positiven Entscheidung, ob ein Anscheinsbeweis vorliegt, die Sicherheitsinfrastruktur des jeweiligen Authentisierungsnehmers erforderlich. Die negative Entscheidung, dass er nicht gegeben ist, kann jedoch durch die Wahrscheinlichkeit alternativer Geschehensabläufe begrün-

142 Oben Rn. 181.
143 *Ernst*, Vertragsgestaltung, Rn. 30; *ders.*, MDR 2003, 1091, 1094.
144 Siehe *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.
145 Oben Rn. 215.
146 Oben Rn. 816.
147 Vgl. zur ec-Karte *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 349 f.
148 Oben Rn. 792.
149 Siehe *Jungmann*, in: Jahrbuch Junger Zivilrechtswissenschaftlicher 2007, 329, 350.

det werden. Die pauschale Ablehnung des Anscheinsbeweises mit der Begründung, dass der Sicherheitsstandard nicht ausreichend sei,[150] soll folgend überprüft werden. Dazu soll untersucht werden, ob die zahlreichen Missbrauchsmöglichkeiten gegen einen Anscheinsbeweis sprechen. Einem Angreifer stehen zahlreiche Möglichkeiten offen, das Passwort auszuspähen.[151] Die große Anzahl an Zugangsdaten, die in einer Dropzone erworben werden können, deutet auf eine nicht zu vernachlässigende Wahrscheinlichkeit gestohlener Zugangsdaten hin.[152]

Neben dem Diebstahl kommt auch in Betracht, dass ein Nutzer die Zu- **864**
gangsdaten aufgeschrieben oder in der Schlüsselbund-Verwaltung verwahrt hat.[153] Die Wahrscheinlichkeit dieses Geschehensablaufs ist keinesfalls gering. Die Komplexität der Passwörter hat die paradoxe Wirkung, dass sichere Passwörter schwer zu merken sind und daher notiert werden, was die Authentisierungsmethode unsicher werden lässt.[154] Beim Online-Banking ist sogar anerkannt, dass dem Kunden die Notiz der Zugangsdaten möglich sein muss und nicht per AGB ausgeschlossen werden kann.[155] Es ist daher wahrscheinlich, dass ein Account-Inhaber die Zugangsdaten aufgeschrieben hat und nicht unwahrscheinlich, dass er diese Notiz oder Speicherung nicht sorgfältig schützt. Ferner wäre es dem Account-Inhaber in der Praxis unmöglich, die Behauptung, er habe seine Zugangsdaten aufgeschrieben, zu widerlegen. Diese alternativen Geschehensabläufe verhindern die Anerkennung eines Anscheinsbeweises.[156]

Gegen die Wahrscheinlichkeit dieser alternativen Geschehensabläufe **865**
wird häufig eingewendet, dass Dritten bei vielen Accounts eine Motivation fehle, die Zugangsdaten zu missbrauchen.[157] Selbst wenn es an einem rationalen Grund fehlen sollte, lassen sich Fälle finden, bei denen anschei-

150 *OLG Bremen*, Beschluss v. 21. 6. 2012, 3 U 1/12 – MMR 2012, 593, 594; *OLG Hamm*, Urteil v. 16. 11. 2006, 28 U 84/06 – NJW 2007, 611; *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180.

151 Oben Rn. 126 ff.

152 *BSI*, Lagebericht 2011, S. 22: Im Jahr 2010 standen Zugangsdaten zu über 350.00 Accounts auf Handelsplattformen und Online-Shops in Dropzones zum Verkauf.

153 Oben Rn. 132 ff.

154 Oben Rn. 562.

155 Oben Rn. 563.

156 So ausdrücklich auch *OLG Köln*, Urteil v. 6. 9. 2002, 19 U 16/02 – MMR 2002, 813, 814.

157 *M. Köhler/Arndt/Fetzer*[7], Rn. 324.

nend grundlos die Zugangsdaten missbraucht wurden.[158] Ein mangelndes rationales Interesse eines Dritten an einem Missbrauch der Zugangsdaten spricht somit nicht für einen Anscheinsbeweis.[159] Die Strafbarkeit des Dritten beim Missbrauch der Zugangsdaten[160] spricht wegen der geringen Wahrscheinlichkeit der Aufdeckung ebenso wie bei der E-Mail[161] nicht für den Anscheinsbeweis.

866 Die erste Voraussetzung, die sich aus der Analyse von Anscheinsbeweisen in vergleichbaren Konstellationen ergeben hat,[162] dass eine sichere Authentisierungsmethode mit hoher Wahrscheinlichkeit dafür spricht, dass der Account-Inhaber gehandelt hat, liegt nicht vor. Die zweite Voraussetzung der zuverlässigen Identifizierung des Account-Inhabers ist ebenfalls nicht gegeben. Bei Accounts zu Informationsportalen oder Online-Shops ist diese Voraussetzung mangels Überprüfung der Identitätsbehauptung nicht gegeben.[163] Auch bei Benutzerkonten, bei denen eine Plausibilitätskontrolle stattfindet und ein Reputationssystem vorhanden ist, besteht keine zuverlässige Identifikationsfunktion.[164] Accounts werden häufig unter fremden oder falschen Namen angelegt.[165] Ein Anscheinsbeweis kommt daher für die Echtheit des Kontos nicht in Betracht. Diese Echtheit, also das Zutreffen der Identitätsbehauptung, ist stets voll zu beweisen.[166]

867 Die dritte Voraussetzung zur Anerkennung des Anscheinsbeweises ist die Wahrscheinlichkeit der Unverfälschtheit der Erklärung. Da die Erklärungen, die über einen Account abgegeben wurden, ebenso wie E-Mails[167] nur als Dateien auf einem Rechner liegen, sind sie ebenso manipulierbar und nachträglich nicht nachweisbar. Im Zwei-Personen-Verhältnis kann eine Prozesspartei durch die Manipulation der Erklärung einen Vorteil erlangen. Sie hat damit einen rationalen Grund die Erklärung nachträglich zu verfälschen, was gegen die Wahrscheinlichkeit der Unverfälschtheit spricht. Im Drei-Personen-Verhältnis, wie bei einer Internet-Auktionsplattform, hat der

158 Oben Rn. 634.
159 *LG Bonn*, Urteil v. 19. 12. 2003, 2 O 472/03 – MMR 2004, 179, 180; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.
160 Dazu *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44.
161 Oben Rn. 841.
162 Oben Rn. 826.
163 Oben Rn. 847.
164 Oben Rn. 848 ff.
165 *F. A. Koch*, Internet-Recht[2], S. 201.
166 *Kitz*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.1 Rn. 67.
167 Zur nachträglichen Manipulierbarkeit von E-Mails oben Rn. 839.

Authentisierungsnehmer die Erklärungen entgegen genommen und gespeichert. Zwar kann eine Prozesspartei ihre Belege der Erklärungen, wie die Benachrichtigungs-E-Mails oder Kopien von der Bestätigungsseite, manipulieren. Durch eine Rückfrage bei der Handelsplattform, deren Geschäftsmodell in dem Abschluss der Rechtsgeschäfte liegt, wodurch eine Herausgabe der Informationen zu erwarten ist, lassen sich solche Manipulationen jedoch aufdecken. Die nachträgliche Manipulation beim Dritten ist zwar ebenso möglich, jedoch wegen des mangelnden Eigeninteresses an der Manipulation und dem hohen Eigeninteresse an der Unverfälschtheit der Daten, unwahrscheinlich.[168]

Die aus anerkannten Beweiserleichterungen herausgearbeiteten Voraus- **868**
setzungen sprechen somit gegen einen Anscheinsbeweis. Folgend soll kurz auf Versuche eingegangen werden, einzelne anerkannte Beweiserleichterungen auf Benutzerkonten im Internet zu übertragen. Zwar entfaltet der gesetzlich kodifizierte Anscheinsbeweis bei der elektronischen Signatur in § 371a Abs. 1 S. 2 ZPO[169] systematisch betrachtet keine Sperrwirkung für andere Anscheinsbeweise.[170] Die Vorschrift spreche somit nicht gegen die Anerkennung eines Anscheinsbeweises.[171] Dagegen lässt sich jedoch einwenden, dass sich aus der Wertung des § 371a Abs. 1 ZPO entnehmen lässt, dass eine vergleichbar sichere Authentisierungsmethode gewählt werden muss. Im Umkehrschluss dazu ergibt sich, dass ein Anscheinsbeweis bei einer rein wissensbasierten Authentisierungsmethode nicht in Betracht kommt.[172] Die Beweiserleichterung beim Bildschirmtext[173] lässt sich nicht übertragen, weil der Missbrauch dort nur in der räumlichen Sphäre des Account-Inhabers stattfinden kann.[174] Die rein wissensbasierte Authentisierung ist durch die allerorts mögliche Authentisierung größeren Gefahren ausgesetzt.[175] Ebenso kann einer Übertragung des Anscheinsbeweises bei

168 Ähnlich *Borges*, Verträge, S. 485.
169 Oben Rn. 801.
170 *Biallaß*, ZUM 2007, 397, 397 f.; vgl. zur Sperrwirkung bezüglich der E-Mail oben Rn. 844.
171 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 45; *Ernst*, MDR 2003, 1091, 1093.
172 *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.
173 Oben Rn. 808.
174 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *LG Münster*, Urteil v. 20. 3. 2006, 12 O 645/05, Rn. 15.
175 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256.

der ec-Karte[176] nicht zugestimmt werden. Durch die Besitz-Komponente ist auch sie geringeren Angriffsmöglichkeiten ausgesetzt.[177]

869 Teilweise wird versucht mit der Möglichkeit des Erschütterns[178] den Anscheinsbeweis dennoch zu rechtfertigen. Der Anscheinsbeweis sei anzuerkennen, weil der Anscheinsbeweis leicht zu erschüttern sei.[179] Dem kann nicht zugestimmt werden. Das Erschüttern kann dem Account-Inhaber erhebliche Probleme bereiten.[180] Einzelne Gerichte behaupten, ein Phishing-Angriff beispielsweise sei mittels der Verlaufsprotokolle und des Caches eines Internetbrowsers „noch relativ lange" nachweisbar, weil anhand dessen die besuchten Internetseiten nachvollziehbar sind.[181] Zwar speichert beispielsweise der Browser Firefox das Verlaufsprotokoll in den Standardeinstellungen ohne zeitliche Beschränkungen. Der Browser Safari löscht standardmäßig alle Einträge aus diesem Verlauf, die älter als zwei Wochen sind. Selbst bei Nutzern, die mit den Standardeinstellungen surfen, ist der Verlauf somit eher nur eine kurze Zeit lang gespeichert. Darüber hinaus kann der Nutzer im Browser den Verlauf jederzeit manuell löschen. Ein Nutzer, dem Datenschutz wichtig ist, konfiguriert seinen Browser ohnehin so, dass der Verlauf gar nicht erst aufgezeichnet oder nach dem Schließen des Browsers gelöscht wird. Der Browser-Cache liefert ebenfalls keine hinreichende Grundlage für einen Beweis über längere Zeit hinweg. Er wird bei entsprechender Einstellungen des Nutzers nach dem Schließen des Browsers gelöscht, sodass er auch keine über längere Zeit zuverlässige Quelle von Beweisen ist. Ferner existieren Missbrauchsmöglichkeiten, die sich nicht in der Sphäre des Account-Inhabers abspielen, sodass der Account-Inhaber den Anscheinsbeweis nicht durch die konkrete Möglichkeit eines solchen Missbrauchs erschüttern kann. Deswegen sollte auch der Anscheinsbeweis nicht wegen Anreizfunktion für den Account-Inhaber, den handelnden Dritten zu offenbaren,[182] anerkannt werden. Dies setzt voraus, dass der Dritte stets bekannt ist, was jedoch nicht der Fall ist.

---

176 Dafür *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 44; *Härting*[4], Rn. 584.

177 *LG Bonn*, Urteil v. 7. 8. 2001, 2 O 450/00 – MMR 2002, 255, 256; *AG Erfurt*, Urteil v. 14. 9. 2001, 28 C 2354/01 – MMR 2002, 127, 128.

178 Oben Rn. 790.

179 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 45; *Winter*, CR 2004, 219, 221.

180 *Ernst*, MDR 2003, 1091, 1093.

181 *LG Köln*, Urteil v. 5. 12. 2007, 9 S 195/07 – MMR 2008, 259, 261.

182 So *J. Hoffmann*, in: *Leible/Sosnitza*, Rn. 185.

Wird entgegen der hier vertretenen Meinung der Anscheinsbeweis aner- **870**
kannt, muss er durch eine konkrete und nicht nur abstrakte Möglichkeit eines abweichenden Geschehensablaufs erschüttert werden.[183] Die pauschale Behauptung der Unsicherheit reiche dafür nicht aus.[184] Eine zeitnahe Sperrung des Legitimationszeichens erfülle diese Anforderungen hingegen.[185] Eine Betrachtung der Gesamtumstände kann ebenfalls den Anscheinsbeweis erschüttern, beispielsweise beim Kauf eines Luxusgutes, was sich der Account-Inhaber nicht leisten kann.[186] Ein Befall des Rechners mit einem Trojaner[187] reicht ebenfalls aus, um einen möglichen Anscheinsbeweis zu erschüttern. Dieser ist stets als konkrete Möglichkeit in Betracht zu ziehen.[188]

Ein Anscheinsbeweis dafür, dass eine Erklärung über einen Account von **871**
dessen Inhaber abgegeben wurde, besteht somit nicht. Teilweise wird für einen Sonderfall ein Anscheinsbeweis angenommen. Wenn der Account-Inhaber einen Missbrauch durch eine Person behauptet, die nicht in der Lage ist, die Zugangsdaten professionell auszuspähen, spreche ein Anscheinsbeweis für die Weitergabe.[189] Gegen diesen Anscheinsbeweis lässt sich einwenden, dass er nicht notwendig ist, um eine Beweisnot zu überwinden. Der Richter kann über die freie Beweiswürdigung (§ 286 Abs. 1 S. 1 ZPO) bei solchen konkreten Vorträgen Schutzbehauptungen erkennen.[190] Ein Bedürfnis für den Anscheinsbeweis besteht daher nicht.

Eine tatsächliche Vermutung[191] kommt wegen der fehlenden Voraussetz- **872**
zungen für einen Anscheinsbeweis erst recht nicht in Betracht. Der Missbrauch liegt häufig, aber nicht immer in der Sphäre des Account-Inhabers, sodass dieser ihn nicht unbedingt beweisen kann.[192] Eine Beweislastumkehr ohne tatsächliche Vermutung[193] kommt daher auch nicht in Betracht.

183 *Mankowski*, CR 2011, 458.
184 *Winter*, MMR 2002, 836, 17.
185 *Herresthal*, K&R 2008, 705, 710; *ders.*, in: *Taeger/Wiebe*, 21, 45.
186 *Ernst*, MDR 2003, 1091, 1093.
187 Oben Rn. 193.
188 Unten Rn. 903.
189 *Sonnentag*, WM 2012, 1614, 1618; *Oechsler*, MMR 2011, 631, 632; *ders.*, AcP 208 (2008), 565, 580.
190 Oben Rn. 795.
191 Oben Rn. 781.
192 *Kuhn*, S. 255.
193 Oben Rn. 776.

b) Sekundäre Darlegungslast

873 Nach der Ablehnung der Beweiserleichterung über den Anscheinsbeweis stellt sich die Frage, ob den Account-Inhaber eine sekundäre Darlegungslast[194] beim Missbrauch eines seiner Benutzerkonten auf einer Internetseite trifft. Teilweise wird diese sekundäre Darlegungslast angenommen, weil es sich um Vorgänge in der Sphäre des Account-Inhabers handele.[195] Durch diese Beweiserleichterung werde die als „Widerrufsrecht kraft Beweislastverteilung"[196] bezeichnete Situation verhindert.[197] Ein Missbrauch, etwa mittels eines Trojaners,[198] sei stets mit konkreten Anhaltspunkten im Einzelfall zu belegen.[199]

874 Gegen diese Beweiserleichterung in Form der sekundären Darlegungslast wird eingewandt, dass die Voraussetzungen einer sekundären Darlegungslast nicht vorlägen.[200] Zunächst muss die beweisbelastete Partei die Informationen haben oder sie müssten leicht zu beschaffen sein.[201] Dies sei nicht der Fall, wenn beispielsweise nach einem Trojaner-Angriff, bei dem die Zugangsdaten ausgespäht wurden, dieser sich nicht mehr nachweisen lässt, weil der Computer neu formatiert wurde.[202] Dabei wird jedoch die Natur der sekundären Darlegungslast verkannt. In deren Rahmen muss der Belastete nur die Tatsachen substantiiert darlegen, nicht beweisen.[203] Der Account-Inhaber muss daher nur aus seiner eigenen Kenntnis darlegen, dass er Opfer eines Angriffs wurde, bei dem sein Computer infiziert wurde und er ihn deswegen formatiert hat. Der Geschäftsgegner muss dann anhand dieser substantiierten Darlegung beweisen, dass dies nicht der Fall war. Dieser Einwand spricht somit nicht gegen die sekundäre Darlegungslast.

194 Oben Rn. 792.
195 *Ellenberger*, in: *Palandt*[73], § 172 BGB Rn. 18; *Kremer*, in: NK-BGB[2], Anh zu § 156 Rn. 29; *Noack/Kremer*, AnwBl 2004, 602, 604; *Schramm*, in: MüKo-BGB[6], § 164 Rn. 45b; wohl auch *Teuber/Melber*, MDR 2004, 185, 186; *Wenn*, CR 2006, 137, 138; **a.A.** *Biallaß*, ZUM 2007, 397, 398.
196 *Mankowski*, CR 2003, 44; *ders.*, MMR 2004, 181; dazu oben Rn. 773.
197 *Kremer*, in: NK-BGB[2], Anh zu § 156 Rn. 29.
198 Zu Trojanern oben Rn. 193.
199 *Teuber/Melber*, MDR 2004, 185, 186.
200 *Biallaß*, ZUM 2007, 397, 398.
201 Oben Rn. 793.
202 *Biallaß*, ZUM 2007, 397, 398.
203 Oben Rn. 794 sowie *Leipold*, in: *Stein/Jonas*[22], § 138 ZPO Rn. 38.

Gegen die sekundäre Darlegungslast lässt sich jedoch einwenden, dass dem Account-Inhaber die Substantiierung teilweise nicht möglich sein wird. Ein intelligent programmierter Trojaner wird sich nach einer gezielten Manipulation selbst löschen,[204] um die Spuren zu verwischen. Teilweise werden auch bei der Aktualisierung des Virenschutzes Schadprogramme vernichtet, ohne dass dessen Funktionsweise protokolliert wurde.[205] Es sind daher Angriffsszenarien möglich, bei denen der Account-Inhaber keine Informationen über den Angriff hat und diese auch nicht leicht beschaffen kann. Somit liegen die Voraussetzungen der sekundären Darlegungslast bezüglich Informationen aus der Sphäre des Account-Inhabers nicht vor. Ferner muss berücksichtigt werden, dass es zahlreiche Möglichkeiten des Missbrauchs gibt, die sich außerhalb der Sphäre des Account-Inhabers abspielen. Das Ausprobieren der Zugangsdaten mittels Brute-Force-Attacke[206] oder Schwachstellen beim Authentisierungsnehmer[207] spielen sich außerhalb der Sphäre des Account-Inhabers ab. Die Grundvoraussetzungen, dass der Account-Inhaber somit wegen seiner Sachnähe zu seiner eigenen Sphäre die Darlegung zugemutet wird, liegt somit nicht vor. 875

Es kann zwar vom Account-Inhaber verlangt werden, dass er substantierte Behauptungen zu den Tatsachen aus seiner Sphäre macht. Reichen diese jedoch nicht aus, um einen Missbrauch plausibel erscheinen zu lassen, kann ihm daraus kein Nachteil entstehen. Unterlässt der Account-Inhaber solche Behauptungen ist nach der Lebenserfahrung davon auszugehen, dass ihm solche Darlegungen nicht möglich oder zumutbar sind.[208] Bei Benutzerkonten auf Internetseiten müssen somit Schutzbehauptungen durch die freie richterliche Beweiswürdigung (§ 286 Abs. 1 S. 1 ZPO)[209] verhindert werden. 876

IV. Online-Banking

Beim Online-Banking kommt eine Rechtsscheinhaftung nur in Betracht, wenn der Ansicht gefolgt wird, dass diese nicht durch § 675u S. 1 BGB 877

204 *Armgardt/Spalka*, K&R 2007, 26, 31 f.
205 *Borges*, Elektronischer Identitätsnachweis, S. 252.
206 Oben Rn. 181.
207 Oben Rn. 215.
208 Vgl. *Musielak*, Grundkurs[11], Rn. 403.
209 Oben Rn. 795.

ausgeschlossen ist.[210] Bei einem einfachen TAN-Verfahren[211] sowie beim iTAN-Verfahren[212], die eine rein wissensbasierte Authentisierungsmethode verwenden,[213] kommt wegen der Unsicherheit der Authentisierungsmethode eine Rechtsscheinhaftung nicht in Betracht.[214]

878 Das mTAN-Verfahren hingegen setzt auf eine Zwei-Faktor-Authentisierung[215] und bietet somit grundsätzlich eine ausreichende Grundlage für die Anerkennung eines Rechtsscheintatbestandes. Die Identität des Bank-Kunden wird vor Abschluss des Vertrags ausreichend sicher überprüft.[216] Der Bankkunde ist zur Geheimhaltung der Zugangsdaten ebenso verpflichtet (§ 675l S. 1 BGB) wie die Bank (§ 675m Abs. 1 S. 1 BGB). Die Bank muss eine Sperrmöglichkeit zur Verfügung stellen (§ 675m Abs. 1 S. 1 Nr. 3 BGB), der Kunde sie nutzen (§ 675l S. 2 BGB).[217] Das mTAN-Verfahren ist somit ausreichend sicher für die Anerkennung eines Rechtsscheintatbestandes.

879 Bezüglich der Beweiserleichterungen beim Online-Banking ist auf die Wiedergabe der ausführlichen Diskussion in der Literatur zu verweisen.[218]

V. Online-Bezahldienste

880 Bei einem anonymen Online-Bezahldienst[219] kommt ein Rechtsscheintatbestand mangels Identifikationsfunktion nicht in Betracht. Bei einem Bezahldienst, der mittels einer Überprüfung von Bankkonto oder Kreditkarte an der Identitätsüberprüfung während der Kontoeröffnung partizipiert, ist zwar die Zuverlässigkeit der Identifikationsfunktion[220] gewährleistet. Setzt ein Online-Bezahldienst wie PayPal jedoch auf eine rein wissensbasierte Au-

210 Dazu oben Rn. 512.
211 Dazu *van Look*, in: *Claussen*[4], § 4 Rn. 41; *Schwintowski*[3], § 9 Rn. 34 ff.
212 Dazu *Hansen*, S. 9.
213 Oben Rn. 545.
214 Oben Rn. 544 ff.
215 Oben Rn. 118.
216 Dazu oben Rn. 67.
217 Dazu *Maihold*, in: *Schimansky/Bunte/Lwowski*[4], § 55 Rn. 50.
218 Oben Rn. 819.
219 Zu Online-Bezahldiensten oben Rn. 71.
220 Zu der Notwendigkeit oben Rn. 595 ff.

thentisierung scheitert die Anerkennung des Rechtsscheintatbestandes daran.[221]

Bei nicht-anonymen Online-Bezahldiensten ergeben sich bei den Beweiserleichterungen beim Einsatz einer rein wissensbasierten Authentisierungsmethode keine Unterschiede zu Benutzerkonten auf Internetseiten. Wie bei den Benutzerkonten[222] kommt somit keine Beweiserleichterung in Betracht, weder in Form von Beweislastumkehr mit oder ohne tatsächlicher Vermutung, noch in Form von Anscheinsbeweis oder sekundärer Darlegungslast.[223] 881

VI. Elektronische Signatur

1. Rechtsscheinhaftung

Für die unterschiedlichen Formen der elektronischen Signatur soll im Folgenden überprüft werden, ob sie die Voraussetzungen für die Anerkennung eines Rechtsscheintatbestandes erfüllen. 882

a) Sicherheit der Authentisierungsmethode

Zunächst müsste die elektronische Signatur eine hinreichend sichere Authentisierungemethode verwenden.[224] Die einfache elektronische Signatur (§ 2 Nr. 1 SigG)[225] verwendet keine Authentisierungsmethode. Bei der fortgeschrittenen elektronischen Signatur (§ 2 Nr. 2 SigG) beschränkt sich die Authentisierung auf das Wissen des geheimen Schlüssels, sodass diese rein wissensbasierte Authentisierung keine hinreichende Grundlage für einen Rechtsscheintatbestand ist.[226] Die qualifizierte elektronische Signatur (§ 2 Nr. 2 SigG) hingegen setzt eine Zwei-Faktor-Authentisierung ein. Der geheime Schlüssel darf nur auf der sicheren Signaturerstellungseinheit (§ 2 883

221 Oben Rn. 544 ff. Auf die Unsicherheit der Authentisierung bei PayPal weisen auch hin *Jehle*, S. 353; *Meder/Grabe*, BKR 2005, 467, 474.
222 Oben Rn. 854.
223 Zu den Formen der Beweiserleichterung oben Rn. 774 ff.
224 Dazu oben Rn. 534 ff.
225 Zu den Formen der elektronischen Signatur oben Rn. 74.
226 Oben Rn. 544 ff.

Nr. 10 SigG) gespeichert werden (§ 5 Abs. 4 S. 3 SigG).[227] Dadurch wird eine Besitzkomponente für die Authentisierung verwendet. Auf den darauf gespeicherten geheimen Schlüssel darf nur nach der Abfrage einer PIN[228] zugegriffen werden (vgl. § 15 Abs. 1 S. 1 SigV). Für die qualifizierte elektronische Signatur ist die Verwendung einer sicheren Signaturerstellungseinheit (§ 2 Nr. 10 SigG) erforderlich,[229] was die Sicherheit der Authentisierungsmethode erhöht. Die verwendete Zwei-Faktor-Authentisierung bei der qualifizierten elektronischen Signatur bietet grundsätzlich hinreichende Sicherheit für die Anerkennung eines Rechtsscheintatbestandes.[230]

884 Die Sicherheit der Authentisierungsmethode muss jedoch nicht nur technisch angelegt sein, sondern auch durch den Account-Inhaber unterstützt werden.[231] Bei der qualifizierten elektronischen Signatur betrifft dies insbesondere die Geheimhaltung der PIN sowie die sichere Verwahrung der Chip-Karte. Die Geheimhaltung der PIN ist dem Signaturschlüssel-Inhaber nicht gesetzlich auferlegt. Durch die Pflicht der Zertifizierungsdiensteanbieter die Geheimhaltung des privaten Schlüssels sicherzustellen (§ 5 Abs. 4 S. 2 SigG), haben diese den Signaturschlüssel-Inhaber über die Geheimhaltung der PIN im Rahmen der Belehrung nach § 6 Abs. 1 SigG zu informieren (§ 6 S. 1 Nr. 2 SigG).[232] Darüber hinaus kann angenommen werden, dass die Zertifizierungsdiensteanbieter den Signaturschlüssel-Inhabern eine Geheimhaltungspflicht vertraglich auferlegen.[233] Seitens des Accounts-Inhabers kann somit die notwendige Sorgfalt mit dem Umgang der Zugangsdaten erwartet werden

885 Der Zertifizierungsdiensteanbieter muss ebenfalls dafür sorgen, dass der Authentisierungsvorgang sicher ist.[234] Gesetzlich werden ihm zahlreiche Vorgaben bezüglich der Sicherheit gemacht, beispielsweise § 5 Abs. 5 SigG. Er muss die Sicherheit jedoch nicht nur technisch gewährleisten, sondern auch eine Möglichkeit bieten, die Zugangsdaten zu sperren. Dies muss der Zertifizierungsdiensteanbieter bei qualifizierten elektronischen Signaturen nach § 8 Abs. 1 S. 1 SigG ermöglichen. Die qualifizierte elektronische Si-

227 Dazu *Sanner*, S. 22.
228 Zum Erfordernis der PIN *F. A. Koch*, Internet-Recht[2], S. 145; *Sanner*, S. 22.
229 Dazu im Einzelnen *Bergfelder*, S. 199.
230 Oben Rn. 117 ff.
231 Oben Rn. 586.
232 Dazu *Gramlich*, in: *Spindler/F. Schuster*[2], § 6 SigG Rn. 5; *B. E. Brisch/K. M. Brisch*, in: *Hoeren/Sieber/Holznagel*, Kap. 13.3 Rn. 167.
233 Vgl. *Reese*, S. 26.
234 Oben Rn. 588.

gnatur verwendet also eine hinreichend sichere Authentisierungsmethode.

b) Zuverlässigkeit der Identifikationsfunktion

Ferner muss die Verwendung einer elektronischen Signatur den Account-Inhaber zuverlässig identifizieren.[235] Bei der einfachen und der fortgeschrittenen elektronischen Signatur wird die Identität des Account-Inhabers nicht überprüft, sodass ein Rechtsscheintatbestand an der Unzuverlässigkeit der Identifikationsfunktion scheitert. Bei der qualifizierten elektronischen Signatur hingegen wird die Zuverlässigkeit der Identifikationsfunktion durch die Überprüfung der Identität des Signaturschlüssel-Inhabers (§ 5 Abs. 1 S. 1 SigG) sichergestellt. Die Identifizierung muss mittels Personalausweis oder Reisepass oder eines anderen hoheitlichen Ausweispapiers erfolgen.[236] Die Überprüfung hoheitlicher Ausweisdokumente bietet eine hinreichende Sicherheit zur Identifizierung des Account-Inhabers.[237] **886**

Diese strengen Anforderungen wurden durch das 1. SigÄndG[238] deutlich abgeschwächt. Nach § 5 Abs. 1 S. 2 SigG n.F. kann nunmehr die Identifizierung anhand vorhandener personenbezogener Daten erfolgen. Ferner ist durch die Neuregelung ein persönlicher Kontakt zwischen Zertifizierungsdiensteanbieter und Signaturschlüssel-Inhaber nicht mehr erforderlich. Nach § 5 Abs. 2 SigV 2001 musste die Signaturkarte persönlich übergeben werden und nach § 6 Abs. 3 S. 1 SigG 2001 war die schriftliche Belehrung über Rechts- und Sicherheitsfragen schriftlich zu bestätigen. Diese beiden Regelungen stellten einen persönlichen Kontakt sicher.[239] Die Zuverlässigkeit der Identifikationsfunktion ist durch die Änderungen des 1. SigÄndG empfindlich betroffen. Ein Ehemann kurz vor der Trennung oder der Pfleger einer älteren Dame kann nun – wenn er Zugang zum Online-Banking- und E-Mail-Account hat – mit ein paar Mausklicks eine qualifizierte elektronische Signatur über das Online-Banking beantragen, den privaten Schlüssel auf die Bank-Karte laden, den Brief mit der PIN abfangen und notwendige **887**

235 Oben Rn. 595 ff.

236 *Gramlich*, in: *Spindler/F. Schuster*[2], § 5 SigG Rn. 5.

237 Siehe oben Rn. 612.

238 Erstes Gesetz zur Änderung des Signaturgesetzes vom 4. 1. 2005, BGBl I, S. 2. Siehe dazu Begr. 1. SigÄndG, BT-Drucks. 15/3417; *Roßnagel*, NJW 2005, 385.

239 *Roßnagel*, NJW 2005, 385, 386.

Erklärungen mit dem fremden E-Mail-Account bestätigen.[240] Es gibt daher nach der neuen Fassung des SigG Wege sich ein qualifiziertes Zertifikat auf einen fremden Namen auszustellen. Durch die Übersendung der Zugangsdaten mittels eines Medienbruchs besteht wenigstens ein geringes Maß an Überprüfung der Identität.[241] Diese Absenkung der Sicherheitsanforderungen durch den Gesetzgeber führen jedoch nicht dazu, dass der Rechtsschein nicht mehr besteht.[242] Eine Zurechnung des Rechtsscheins scheidet jedoch aus, wo die elektronische Signatur nicht vom Signaturschlüssel-Inhaber beantragt wurde.[243]

888 Die Zuverlässigkeit der Identifikationsfunktion kommt jedoch nur in Betracht, wenn ein Account einmalig ist. Bei der elektronischen Signatur bedeutet dies, dass der geheime Schlüssel nur eimal vergeben werden darf.[244] Gesetzlich ist dies nach § 2 Nr. 2 lit. b SigG vorgeschrieben, sodass die Identifizierung des Signaturschlüssel-Inhabers ermöglicht wird.[245] Der Gesetzgeber schätzt die Zuverlässigkeit der Identitätsfeststellung bei der elektronischen Signatur als sicher ein, dass andere Dienste auf diese vertrauen dürfen, wenn sie die Identität eines Nutzers überprüfen wollen. Nach § 3 Abs. 3 S. 1 Nr. 1 a.E. DeMailG darf die Identität bei Erstellung eines De-Mail-Kontos mittels qualifizierter elektronischer Signatur überprüft werden. Die qualifizierte elektronische Signatur besitzt somit eine zuverlässige Identifikationsfunktion. Ein Rechtsscheintatbestand, dass der Account-Inhaber der qualifizierten elektronischen Signatur gehandelt hat, besteht somit.[246]

c) Zwischenergebnis

889 Bei der qualifizierten Signatur besteht somit ein Rechtsscheintatbestand dahin gehend, dass der Schlüssel-Inhaber die Erklärung verfasst hat.[247] Bei

240 Die Beispiele stammen von *Roßnagel*, NJW 2005, 385, 386.
241 Zur Überprüfung mittels Medienbruch oben Rn. 617.
242 *Spiegelhalder*, S. 137.
243 Zum Erstellen von Accounts durch Dritte oben Rn. 718.
244 *Borges*, Verträge, S. 51.
245 *Bösing*, S. 24.
246 Im Ergebnis auch *Rieder*, S. 261 ff.; *Reese*, S. 51 ff.; *Spiegelhalder*, S. 126 ff.; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 10; *Sonnentag*, WM 2012, 1614, 1616; *Ultsch*, DZWir 1997, 466, 473; *M. Wolf/Neuner*[10], § 50 Rn. 108.
247 So auch *Ultsch*, in: Vernetzte Welt – gloables Recht, 127, 136 f.; *ders.*, DZWir 1997, 466, 473; *Rieder*, S. 281; *Spiegelhalder*, S. 162; *Reese*, S. 123; *Dörner*, AcP 202

der Zurechnung ergeben sich keine Unterschiede zu anderen Accounts.[248] Der Account-Inhaber haftet jedenfalls bei Weitergabe auf das positive Interesse des Geschäftsgegners.

2. *Beweiserleichterungen*

Bei der qualifizierten elektronischen Signatur (§ 2 Nr. 3 SigG)[249] existiert mit § 371a Abs. 1 S. 2 ZPO ein gesetzlich normierter Anscheinsbeweis,[250] sodass die Frage der Beweiserleichterungen gesetzlich vorgegeben ist. Bei den schwächeren Formen der elektronischen Signatur stellt sich jedoch die Frage, inwiefern Beweiserleichterungen in Betracht kommen. Eine einfache elektronische Signatur (§ 2 Nr. 1 SigG) verwendet keine Authentisierungsmethode. Sie kann einfach kopiert und nachgeahmt werden. Vom Sicherheitsniveau ist sie damit deutlich unterhalb der E-Mail angesiedelt, bei der keine Beweiserleichterungen in Betracht kommen.[251] Somit kommt bei der einfachen elektronischen Signatur erst recht keine Beweiserleichterung in Betracht. **890**

Bei der fortgeschrittenen elektronischen Signatur (§ 2 Nr. 2 SigG) ist technisch ein breites Spektrum an Sicherheit möglich. Je nach konkreter Ausgestaltung kann eine Beweiserleichterung in Betracht kommen.[252] Eine fortgeschrittene elektronische Signatur, die mit der Software Pretty Good Privacy (PGP) erstellt wurde, basiert auf einer rein wissensbasierten Authentisierung. Insofern lassen sich die Ergebnisse zu Benutzerkonten im Internet[253] übertragen, sodass eine Beweiserleichterung nicht in Betracht kommt. Nähert sich eine fortgeschrittene elektronische Signatur dem Sicherheitsstandard der qualifizierten elektronischen Signatur, können jedoch Beweiserleichterungen im Einzelfall begründet sein. **891**

(2002), 363, 388; *Redeker*, IT-Recht[5], Rn. 878; *M. Köhler/Arndt/Fetzer*[7], Rn. 227; einschränkend *Schnell*, S. 267.

248 Zur Zurechnung oben Rn. 671 ff.

249 Zu den Formen der elektronischen Signatur oben Rn. 74.

250 Oben Rn. 801.

251 Oben Rn. 835.

252 *Ernst*, MDR 2003, 1091, 1092.

253 Oben Rn. 854.

VII. Elektronischer Identitätsnachweis

1. Rechtsscheinhaftung

892 Beim elektronischen Identitätsnachweis[254] soll ebenfalls untersucht werden, ob dessen Einsatz hinreichende Grundlage für eine Rechtsscheinhaftung ist. Dazu müsste neben dem Einsatz einer ausreichend sicheren Authentisierungsmethode, die Zuordnung des Accounts zur numerischen Identität des Inhabers zuverlässig erfolgen.

a) Sicherheit der Authentisierungsmethode

893 Zunächst müsste der neue Personalausweis (nPA) eine hinreichend sichere Authentisierungemethode verwenden.[255] Der elektronische Identitätsnachweis im neuen Personalausweis setzt auf eine Authentisierung mittels Besitz und Wissen.[256] Der Zugriff auf den Token in der Chip-Karte des neuen Personalausweises ist durch eine sechsstellige PIN geschützt.[257] Bei der Eingabe der PIN besteht je nach Einsatz des Kartenlesegeräts eine Schwachstelle. Werden Kartenleser der Klasse 1[258] verwendet, der lediglich die Karte lesen kann und bei dem die PIN über die Tastatur des Rechners eingegeben wird, kann die PIN auf einem infizierten Rechner durch einen Trojaner[259] ausgespäht werden.[260] Der Grund für den Einsatz von Klasse-1-Kartenleser ist der günstigere Preis im Vergleich zu Klasse-2- und Klasse-3-Kartenlesern, was eine weite Verbreitung hindern könnte.[261] Ist die PIN einem Dritten bekannt, würde die Authentisierung mittels Wissen und Besitz, praktisch auf eine reine Authentisierung des Besitzes zurückgefahren werden.[262] Um die

254 Dazu oben Rn. 88.
255 Dazu oben Rn. 534 ff.
256 *Borges*, NJW 2010, 3334, 3336; *ders.*, Elektronischer Identitätsnachweis, S. 30; *Engel*, DuD 2006, 207, 209; *W. Müller/Redlich/Jeschke*, DuD 2011, 465, 466; *Roßnagel/Hornung/Schnabel*, DuD 2008, 168, 169.
257 *Borges*, NJW 2010, 3334, 3336; *Roßnagel/Hornung/Schnabel*, DuD 2008, 168; *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173; *Eckert*[8], S. 580.
258 Zur Einteilung der Kartenleser in Klassen *Eckert*[8], S. 592 f.; *Borges/Schwenk/Stuckenberg/Wegener*, S. 157 f.
259 Dazu oben Rn. 193.
260 *Borges*, NJW 2010, 3334, 3337; *Eckert*[8], S. 593, 599.
261 *Borges*, NJW 2010, 3334, 3338.
262 *Borges/Schwenk/Stuckenberg/Wegener*, S. 161.

Identität des Ausweisinhabers zu missbrauchen, müsste der Dritte in diesem Fall noch in den Besitz des Ausweises gelangen[263] und der Ausweis dürfte noch nicht gesperrt sein.

Ein Man-in-the-Middle-Angriff,[264] der den Datenverkehr durch eine Manipulation von DNS-Einträgen auf den Angreifer umleitet, kann durch das Zurückweisen eines vertrauensunwürdigen SSL-Zertifikats durch die Ausweis-App verhindert werden.[265] Man-in-the-Middle-Angriffe, die hingegen darauf setzen, mittels Echtzeitveränderungen eine Diskrepanz zwischen den übermittelten Daten und der Anzeige beim Account-Inhaber herzustellen, indem die übermittelnden Daten durch einen Trojaner[266] verändert werden, sind jedoch möglich.[267] Diese Zwei-Faktor-Methode bietet trotz der Angriffsmöglichkeiten grundsätzlich eine hinreichende Sicherheit für die Anerkennung als Rechtsscheintatbestand.[268] **894**

Auf Seiten des Account-Inhabers, der ausgebenden Stelle sowie des Authentisierungsnehmers werden zahlreiche Vorkehrungen getroffen, den Authentisierungsvorgang abzusichern. Der Authentisierungsvorgang kann nur durchgeführt werden, wenn der Authentisierungsnehmer ein Berechtigungszertifikat besitzt (§ 18 Abs. 4 S. 1 PAuswG). Dieses Prinzip der doppelten Authentisierung,[269] dass sich nicht nur der Account-Inhaber, sondern auch der Authentisierungsnehmer authentisieren muss, schützt vor Phishing.[270] **895**

Bereits bei der Ausgabe des Personalausweises und der Übermittelung der geheimen PIN werden auf Seiten der ausgebenden Behörde Sicherheitsvorkehrungen getroffen. Die PIN wird gemeinsam mit der Aufforderung den Personalausweis abzuholen vom Ausweishersteller an den Namensträger per Post verschickt (§ 13 PAuswG).[271] Der Namensträger muss sich den Ausweis anschließend persönlich bei der Behörde abholen.[272] In der Authentisierungsinfrastruktur ist eine Sperrmöglichkeit vorgesehen (vgl. § 24 Abs. 2 S. 1 PAuswV). **896**

263 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 191.
264 Dazu oben Rn. 168.
265 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 174.
266 Dazu oben Rn. 193.
267 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 192.
268 Oben Rn. 117 ff.
269 *Borges*, Elektronischer Identitätsnachweis, S. 30.
270 *Roßnagel*/*Hornung*/*Schnabel*, DuD 2008, 168, 170.
271 Dazu ebd., 169.
272 *Borges*, NJW 2010, 3334, 3337; *ders.*, Elektronischer Identitätsnachweis, S. 38.

897 Die Mitwirkung des Ausweisinhabers, die zur Sicherheit des Authentisierungsvorgangs notwendig ist,[273] ist ebenfalls gesetzlich verlangt. Sobald der Ausweisinhaber die Authentisierungsmittel erhalten hat, treffen ihn Pflichten zur Sicherung der Zuverlässigkeit des Authentisierungsvorgangs. Er hat zum einen die PIN geheim zu halten und darf sie nicht notieren (§ 27 Abs. 2 PAuswG). Zum anderen muss er durch technische und organisatorische Maßnahmen den Rechner, den er zum Authentisierungsvorgang nutzt, ausreichend sichern (§ 27 Abs. 3 PAuswG). Die Besitzkomponente des Authentisierungsvorgangs, der Personalausweis selbst, kann abhandenkommen oder gestohlen werden. In diesen Fall kann er gesperrt werden,[274] sodass ein Missbrauch nur zwischen Abhandenkommen und Sperranzeige möglich ist. Der Ausweisinhaber ist sogar zur Sperrung verpflichtet (§ 27 Abs. 1 Nr. 3 PAuswG).[275] Der Authentisierungsvorgang ist somit für die Anerkennung als Rechtsscheingrundlage ausreichend sicher.

b) Zuverlässigkeit der Identifikationsfunktion

898 Ferner muss der Ausweisinhaber bei Ausstellung des Ausweises zuverlässig identifiziert werden.[276] Rechtlich stellt sich jedoch die Frage, wie zuverlässig und nachvollziehbar diese Identifikationsfunktion erfüllt wird. Zuverlässig ist die Identifikationsfunktion des Personalausweises, wenn bei der Ausstellung des Ausweises die Angaben des Antragstellers überprüft werden. Die Angaben zur Person entnimmt die ausstellende Behörde entweder dem Melderegister oder der Antragsteller hat sie mit Nachweisen zu belegen (§ 9 Abs. 3 S. 3 PAuswG). Die Zuverlässigkeit der Zuordnung wird ferner dadurch sichergestellt, dass der Ausweis regelmäßig persönlich beantragt werden muss (§ 9 Abs. 1 S. 6 PAuswG) und bei Zweifeln seine Identität überprüft wird (§ 9 Abs. 4 PAuswG). Es gibt jedoch ein „Ungewissheitsdelta“, das die Identitätswahrscheinlichkeit und deren Zweifelsfreiheit ausdrückt.[277] Trotz verbleibender Unsicherheiten ist der Personalausweis das „klassische und universelle Authentisierungsmedium.“[278] Einige gesetz-

273 Oben Rn. 586.
274 *Polenz*, MMR 2010, 671, 675; *Eckert*[8], S. 580.
275 Dazu *Borges*, Elektronischer Identitätsnachweis, S. 39.
276 Oben Rn. 595 ff.
277 *Bohrer*, MittBayNot 2005, 460, 461.
278 *Borges*, Elektronischer Identitätsnachweis, S. 29.

liche Regelungen, die erlauben, dass mittels des neuen Personalausweises eine Identitätsüberprüfung online ebenso möglich ist wie bei Inaugenscheinnahme des Ausweisdokuments, zeigen, dass der Gesetzgeber die Identifikationsfunktion als ausreichend zuverlässig wertet. Bei Erstellen eines De-Mail-Kontos (§ 3 Abs. 3 S. 1 Nr. 1 a.E. DeMailG), eines Bank-Kontos (§ 6 Abs. 2 Nr. 2 lit. c GwG) sowie eines qualifizierten Zertifikats für eine elektronische Signatur (§ 3 Abs. 1 S. 2 SigG) darf der elektronische Identitätsnachweis im neuen Personalausweis zur Überprüfung der Identität des Account-Inhabers verwendet werden. Die Identität des Ausweisinhabers bei Ausstellung des Ausweises wird somit ausreichend sicher überprüft. Die Verwendung des neuen Personalausweises setzt somit einen Rechtsschein bezüglich des Handelns des Ausweisinhabers.[279] Bezüglich der Zurechnung[280] ergeben sich keine Besonderheiten bei der elektronischen Signatur.

2. *Beweiserleichterungen*

Bei den Beweiserleichterungen für die Verwendung des elektronischen Iden- **899**
titätsnachweises[281] soll zunächst auf die diskutierte Möglichkeit eines Anscheinsbeweises[282] eingegangen werden. Beim Anscheinsbeweis ist zwischen der Authentisierung und der Urheberschaft einer Erklärung zu unterscheiden.[283] Für einen Anscheinsbeweis, dass der Ausweisinhaber die Authentisierung vorgenommen hat, fehlt es zunächst mangels praktischer Erfahrungen an einem Erfahrungssatz.[284] Nach der Ausschlussmethode kann jedoch ein Anscheinsbeweis ohne ersten Anschein[285] durch die Unwahrscheinlichkeit alternativer Möglichkeiten begründet werden. Die Voraussetzung, dass die Identität des Ausweisinhabers zuverlässig überprüft wird,[286]

279 Im Ergebnis auch *Borges*, NJW 2010, 3334, 3338; *ders.*, Elektronischer Identitätsnachweis, S. 134 f.
280 Oben Rn. 671 ff.
281 Oben Rn. 88.
282 Oben Rn. 785.
283 *Borges*, Elektronischer Identitätsnachweis, S. 242; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
284 *Borges*, Elektronischer Identitätsnachweis, S. 243; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 313.
285 Oben Rn. 788.
286 Oben Rn. 826.

liegt beim elektronischen Identitätsnachweis vor.[287] Wenn die Ergebnisse der Autorisierung bei einem unabhängigen Dritten gespeichert werden, ist auch die nachträgliche Manipulation der Daten unwahrscheinlich, sodass die dritte Voraussetzungen auch vorliegt. Die eingesetzte Zwei-Faktor-Authentisierung[288] im elektronischen Identitätsnachweis bietet eine hohe Sicherheit.[289] Diese wird in vergleichbaren Konstellationen als ausreichend zur Anerkennung und erste Voraussetzung eines Anscheinsbeweises anerkannt.[290] Ein Angriff durch einen Trojaner[291] als alternativer Geschehensablauf ist bei unsicheren Kartenlesegeräten[292] jedoch möglich. Ein Anscheinsbeweis für die Authentisierung durch den Erklärenden komme daher nur in Betracht, wenn ein Trojaner-Angriff ausgeschlossen werden kann.[293] Das bedeutet, dass ein Anscheinsbeweis für die Authentisierung des Ausweisinhabers in Betracht kommt, wenn dieser ein sicheres Lesegerät der Klasse 2 oder aufwärts verwendet hat.

900 Teilweise wird behauptet, dass der Anscheinsbeweis der ec-Karte[294] zu übertragen sei.[295] Diese Begründung überzeugt nicht. Zwar lässt sich aus dem Anscheinsbeweis bei der ec-Karte entnehmen, dass die Zwei-Faktor-Authentisierung eine hinreichende Grundlage für einen Anscheinsbeweis darstellt. Der Anscheinsbeweis bei der ec-Karte ist jedoch aus zwei Gründen ungeeignet für eine Übertragung auf den elektronischen Identitätsnachweis. Zum einen ist das Beweisobjekt bei der ec-Karte ein anderes. Der Anscheinsbeweis bezieht sich bei der ec-Karte zunächst auf das Handeln des Bankkunden. Steht wie häufig der Fall fest, dass dieser nicht gehandelt hat, bezieht sich der Anscheinsbeweis auf das Vorliegen einer haftungsbegründenden Pflichtverletzung.[296] In dieser zweiten Ausformung der Pflichtverletzung hat der Anscheinsbeweis seine hauptsächliche praktische Bedeutung. Beim Einsatz des elektronischen Identitätsnachweises geht es jedoch

287 Oben Rn. 898.
288 Oben Rn. 117.
289 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
290 Oben Rn. 826.
291 Oben Rn. 193.
292 Oben Rn. 893.
293 *Borges*, Elektronischer Identitätsnachweis, S. 243 f.; *ders.*, NJW 2010, 3334, 3338; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
294 Oben Rn. 812.
295 *Roßnagel*/*Hornung*, DÖV 2009, 301, 305; *Borges*, Elektronischer Identitätsnachweis, S. 244; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 314.
296 Oben Rn. 813.

primär darum, einen Anscheinsbeweis dafür zu begründen, dass der Ausweisinhaber selbst gehandelt hat. Wegen dieser unterschiedlichen Beweisobjekte eignet sich der Anscheinsbeweis der ec-Karte schlecht zur Übertragung auf den elektronischen Identitätsnachweis. Zum anderen existiert ein sachnäherer Anscheinsbeweis, der sich zur Übertragung anbietet. Wenn jedoch ein Anscheinsbeweis im Wege eines Einzelvergleichs übertragen werden soll, ist die elektronische Signatur aus zwei Gründen zu wählen. Zum einen handelt es sich bei der Regelung des § 371a Abs. 1 S. 2 ZPO um eine gesetzlich ausgeformte Beweiserleichterung, der eine größere demokratische Legitimation als einem sich stetig fortentwickelnden Richterrecht zuzusprechen ist. Zum anderen ist die elektronische Signatur dem elektronischen Identitätsnachweis deutlich sachnäher, weil es sich bei beiden um Zugangsdaten im Internet handelt, die über ein Karten-Lesegerät in Verbindung mit einem eigenen Rechner zum Einsatz kommen.

Ob von dem Anschein, dass der Account-Inhaber die Authentisierung **901**
vorgenommen hat, auch auf einen Anschein seiner Urheberschaft einer später abgegebenen Erklärung geschlossen werden kann, ist beim derzeitigen Kenntnisstand schwer zu beurteilen.[297] Mangels eines vorhandenen Erfahrungssatzes ist somit nach der Ausschlussmethode ein Anscheinsbeweis ohne ersten Anschein[298] zu erwägen. Ein Man-in-the-Browser-Angriff[299] auf eine Plattform mit der Folge, dass eine Erklärung nach Authentisierung gefälscht werden kann, erscheint möglich.[300] Ein Anscheinsbeweis für die Urheberschaft einer anschließenden Erklärung kommt jedoch nicht erst in Betracht, wenn Angriffe nicht plausibel erscheinen.[301] Er ist grundsätzlich anzuerkennen. Wenn ein Angriff jedoch plausibel erscheint, ist das Erschüttern des Anscheinsbeweises möglich.

Erschüttern[302] kann der Ausweisinhaber den Anscheinsbeweis beispiels- **902**
weise durch den Nachweis der Weitergabe des Ausweises oder dessen Abhandenkommen.[303] Dann spricht jedoch wie bei der ec-Karte ein weiterer Anscheinsbeweis dafür, dass der Ausweisinhaber Karte und PIN pflichtwid-

297 *Borges*, Elektronischer Identitätsnachweis, S. 248.
298 Oben Rn. 788.
299 Oben Rn. 172.
300 *Borges*, Elektronischer Identitätsnachweis, S. 249.
301 So ebd., S. 250.
302 Oben Rn. 790.
303 *Borges*, Elektronischer Identitätsnachweis, S. 244, 251.

rig zusammen verwahrt hat.[304] Ein Angriff mittels eines Trojaners[305] kann den Anscheinsbeweis erschüttern. Fraglich ist, wie hohe Anforderungen an das Erschüttern zu stellen sind. Eine strenge Anforderung wäre, dass der Account-Inhaber darlegen muss, dass sein Rechner mittels eines Trojaners befallen war und dass dieser konkrete Trojaner zu Missbräuchen der Art des Einzelfalls fähig ist.[306] Weniger streng wäre die Anforderung, dass der Account-Inhaber nur darlegen muss, dass sein Rechner infiziert war.[307]

903 Sehr leicht wäre der Anscheinsbeweis zu erschüttern, wenn der Befall des Rechners des Account-Inhabers mit einem Trojaner stets als konkrete Möglichkeit in Betracht kommt.[308] Antiviren-Programme bieten keinen Schutz gegen neuartige Bedrohungen, weil sie hauptsächlich über die Wiederkennung bekannter Schadsoftware funktionieren.[309] Ferner haben sie erhebliche Probleme, Trojaner zu erkennen. Antiviren-Programme mindern zwar das Infektionsrisiko, schließen es aber nicht aus.[310] Auch eine Firewall verhindert die Infektion des Rechners mit Malware nicht.[311] Erschwerend kommt hinzu, dass Antiviren-Programme teilweise Schadprogramme vernichten, ohne deren genaue Funktionsweise zu protokollieren.[312] Es ist daher dem Ausweisinhaber eventuell trotz erfolgtem Missbrauch über einen Trojaner nicht möglich, substantiiert zur Infektion vorzutragen. Dem Ausweisinhaber kann somit nicht zugemutet werden, genaue Angaben zur Infektion seines Rechners zu machen. Der Ausweisinhaber kann mithin den Anscheinsbeweis stets dadurch erschüttern, dass er die Infektion seines Rechners mit Malware vorträgt.

904 Gelingt dem Account-Inhaber die Erschütterung des Anscheinsbeweises, kommt je nach konkretem Vortrag zum Erschüttern eine Rechtsscheinhaf-

304 *Borges*, Elektronischer Identitätsnachweis, S. 246; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 315.
305 Oben Rn. 193.
306 Dagegen *AG Wiesloch*, Urteil v. 20. 6. 2008, 4 C 57/08 – MMR 2008, 626, 627. Dazu auch *Borges*, Elektronischer Identitätsnachweis, S. 251 m.w.N.
307 In diese Richtung *Teuber*/*Melber*, MDR 2004, 185, 186.
308 So *Borges*, Elektronischer Identitätsnachweis, S. 251; in die gleiche Richtung *Armgardt*/*Spalka*, K&R 2007, 26, 31 f.
309 Oben Rn. 203.
310 Oben Rn. 206.
311 Oben Rn. 209.
312 *Borges*, Elektronischer Identitätsnachweis, S. 251.

tung des Ausweisinhabers[313] in Betracht. Wegen der Anerkennung des Anscheinsbeweises bedarf es keiner weiteren Beweiserleichterungen.

VIII. De-Mail

1. Rechtsscheinhaftung

Bei der De-Mail[314] stellt sich bezüglich der Rechtsscheinhaftung ebenso die Frage, ob die verwendete Authentisierungsmethode ausreichend sicher ist.[315] Im Regelfall erfolgt eine sichere Anmeldung, ausnahmsweise kann auch eine einfache Anmeldung erfolgen (§ 4 Abs. 1 S. 1 DeMailG).[316] Als sichere Authentisierungsmethode wird dabei die Zwei-Faktor-Authentisierung vorgesehen (§ 4 Abs. 1 S. 2 DeMailG).[317] Die einfache, unsicherere Authentisierung ist eine, die lediglich auf einer Wissenskomponente basiert (§ 4 Abs. 1 S. 3 DeMailG).[318] Grund für die Wahl der Zwei-Faktor-Authentisierung ist die Rechtsprechung, die bei einer rein wissensbasierten Authentisierung einen Anscheinsbeweis verneint.[319] Diese Zwei-Faktor-Authentisierung kann nur mittels eines aktiven und in Echtzeit arbeitenden Man-in-the-Middle-Angriffs[320] überwunden werden.[321] Nach § 10 Abs. 1 S. 1 Nr. 1 DeMailG besteht für den Nutzer die Möglichkeit ein Konto zu sperren, sodass der Nutzer die Möglichkeit hat, zur Sicherheit des Authentisierungsvorgangs beizutragen, wenn die Zugangsdaten abhandengekommen sind. Mit der Zwei-Faktor-Authentisierung setzt die De-Mail eine ausreichend sichere Authentisierungsmethode ein[322] und erfüllt somit die erste Voraussetzung zur Anerkennung eines Rechtsscheintatbestandes. **905**

313 Oben Rn. 892 ff.
314 Dazu oben Rn. 92.
315 Zu den Anforderungen daran oben Rn. 534 ff.
316 Dazu *Roßnagel*, NJW 2011, 1473, 1475; *Spindler*, CR 2011, 309, 312.
317 Dazu *Roßnagel*, NJW 2011, 1473, 1475; *ders.*, CR 2011, 23, 26; *Spindler*, CR 2011, 309, 312; *Rose*, K&R 2011, 439, 442.
318 Dazu *Roßnagel*, CR 2011, 23, 26.
319 Begr. DeMailG, BT-Drucks. 17/3630, S. 27 f.; Begr. BPG, BT-Drucks. 16/12598, S. 21.
320 Dazu oben Rn. 168.
321 *Dennis Werner/Wegener*, CR 2009, 310, 311.
322 Oben Rn. 117 ff.

906 Ferner muss der Account-Inhaber bei Erstellung des Accounts zuverlässig identifiziert werden.[323] Kritisch wurde im Gesetzgebungsvorgang insbesondere vom Bundesrat betrachtet, dass den Nutzer keine Pflicht trifft, dem Diensteanbieter Änderungen seiner persönlichen Daten wie der Anschrift mitzuteilen.[324] Abgelehnt wurde diese Forderung des Bundesrates von der Bundesregierung mit der Begründung, dass das DeMailG nur Pflichten für Diensteanbieter statuiere und eine Pflicht für Nutzer somit nicht in das Konzept des Gesetzes passe.[325] Die Diensteanbieter können jedoch durch eine entsprechende Klausel in ihren AGB eine Pflicht zur Mitteilung von Änderungen dem Nutzer auferlegen.[326] Für die zuverlässige Identifizierung des Account-Inhabers bei Registrierung des Accounts spielt eine nachträgliche Adressänderung jedoch keine Rolle. Zwar hat der Geschäftsgegner dadurch womöglich ohne weitere Recherchen keine ladungsfähige Adresse des Account-Inhabers. Dieses Problem unterliegt jedoch dem allgemeinen Geschäftsrisiko.

907 Die Zuverlässigkeit der Identifikation des Account-Inhabers stellt das DeMailG dadurch sicher, dass bei der Anmeldung dessen Identität zuverlässig überprüft werden muss (§ 3 Abs. 2 DeMailG).[327] Bei natürlichen Personen wird dafür z.B. ein amtlicher Ausweis kontrolliert (§ 3 Abs. 3 DeMailG). Die Überprüfung erfolgt über das PostIdent-Verfahren, den neuen Personalausweis[328] oder einen Besuch in einer Geschäftsstelle.[329] Diese Überprüfung ist zentral für die Nutzung von De-Mail,[330] eine Nutzung des Accounts darf der Anbieter vorher nicht zulassen (§ 3 Abs. 4 DeMailG). Die Identität des Account-Inhabers wird somit bei Registrierung des Accounts ausreichend sicher überprüft. Bei Verwendung von De-Mail besteht somit ein Rechtsschein dahingehend, dass der Account-Inhaber die Mail verschickt hat. Für die Zurechnung des Rechtsscheintatbestandes kann auf

323 Oben Rn. 595 ff.
324 BT-Drucks. 17/4145, S. 4.
325 Ebd., S. 10.
326 *Spindler*, CR 2011, 309, 312; *Rose*, K&R 2011, 439, 440.
327 Dazu *Roßnagel*, NJW 2011, 1473, 1474; *ders.*, CR 2011, 23, 26; *Spindler*, CR 2011, 309, 311 f.; *Rose*, K&R 2011, 439, 441.
328 *Dennis Werner/Wegener*, CR 2009, 310, 312; *J. Dietrich/Keller-Herder*, DuD 2010, 299, 300.
329 *Stach*, DuD 2008, 184, 185.
330 Begr. DeMailG, BT-Drucks. 17/3630, S. 27.

die allgemeinen Ausführungen verwiesen werden, weil diese sich nicht von den anderen Accounts unterscheidet.[331]

2. *Beweiserleichterungen*

Bei der De-Mail[332] soll zunächst auf die diskutierte Beweiserleichterung des Anscheinsbeweises eingegangen werden. Bei ihr liegen zwar mangels praktischer Verbreitung keine Erfahrungssätze vor, die einen Anscheinsbeweis begründen können. Dafür kann jedoch wiederum die Figur des Anscheinsbeweises ohne ersten Anschein durch Ausschluss alternativer Geschehensabläufe bemüht werden.[333] Wegen der Sicherheit der Zwei-Faktor-Authentisierung[334] sind Geschehensabläufe, bei denen nicht der Account-Inhaber oder ein Berechtigter gehandelt hat, unwahrscheinlich.[335] Die Grundsätze zum Anscheinsbeweis der ec-Karte[336] zu übertragen,[337] überzeugt jedoch ebenso wenig wie beim elektronischen Identitätsnachweis.[338] Bei einer Einzelübertragung ist vielmehr der sachnähere § 371a Abs. 1 S. 1 ZPO heranzuziehen. Am überzeugendsten lässt sich der Anscheinsbeweis jedoch durch die Analyse anerkannter Beweiserleichterungen in vergleichbaren Situationen begründen. Die Analyse anerkannter Beweiserleichterungen hat ergeben, dass eine Zwei-Faktor-Authentisierung eine ausreichende Grundlage zur Anerkennung des Anscheinsbeweises ist. Neben der sicheren Zwei-Faktor-Authentisierung findet bei der De-Mail eine zuverlässige Identitätsüberprüfung statt[339] und durch die Lagerung der Daten bei einem Dritten ist die nachträgliche Manipulation unwahrscheinlich. **908**

331 Dazu oben Rn. 671 ff.
332 Oben Rn. 92.
333 Oben Rn. 788.
334 Oben Rn. 117.
335 Oben Rn. 826. So auch *Roßnagel*, NJW 2011, 1473, 1477.
336 Oben Rn. 812.
337 So *Roßnagel*, NJW 2011, 1473, 1477.
338 Oben Rn. 900.
339 Oben Rn. 906.

909 Bei der Verwendung der De-Mail spricht daher ein Anscheinsbeweis dafür, dass die Mail vom Account-Inhaber abgesendet wurde.[340] Diese betrifft jedoch nur die Identität des Handelnden, nicht den Inhalt der Nachricht.[341] Erschüttern[342] kann der Account-Inhaber den Anscheinsbeweis dadurch, dass er beispielsweise die Weitergabe der Zugangsdaten oder das Abhandenkommen der Chip-Karte darlegt. Eine Infektion des Rechners des Account-Inhabers mit einem Trojaner[343] ist bei Privatpersonen stets als konkrete Möglichkeit anzusehen,[344] sodass dadurch der Anscheinsbeweis leicht erschüttert werden kann. Ist der Anscheinsbeweis erschüttert, kommt eine Haftung nach Rechtsscheingrundsätzen[345] in Betracht. Wegen der Anerkennung des Anscheinsbeweises kommt es auf weitere Beweiserleichterungen nicht an.

340 Begr. DeMailG, BT-Drucks. 17/3630, S. 19; Begr. BPG, BT-Drucks. 16/12598, S. 21; *Roßnagel*, NJW 2011, 1473, 1477; *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728, 733. Wohl auch *Fechner*[14], Kap. 12 Rn. 190; *Wien*[3], S. 99. Offen gelassen von *Redeker*, IT-Recht[5], Rn. 906.

341 *Spindler*, CR 2011, 309, 315; *Roßnagel*, NJW 2011, 1473, 1477.

342 Oben Rn. 790.

343 Oben Rn. 193.

344 Oben Rn. 903. Vgl. auch *Armgardt/Spalka*, K&R 2007, 26, 31 f.; *Borges*, Elektronischer Identitätsnachweis, S. 251.

345 Oben Rn. 905.