Arretz (Hrsg.)

Digitale Authentifizierung

Finanz Colloquium Heidelberg, 2022

Zitiervorschlag:
Autor in: Arretz (Hrsg.), Digitale Authentifizierung, S. XX.

ISBN: 978-3-95725-972-1

Finanz Colloquium Heidelberg GmbH
Im Bosseldorn 30, 69126 Heidelberg
www.FCH-Gruppe.de
info@FCH-Gruppe.de
Satz: Finanz Colloquium Heidelberg GmbH
Druck: VDS-VERLAGSDRUCKEREI SCHMIDT, Neustadt an der Aisch

Arretz (Hrsg.)

Digitale Authentifizierung

Frank Arretz (Hrsg.)
Partner, Bank- und Kapitalmarktrecht
Schalast & Partner Rechtsanwälte mbB, Frankfurt am Main

Hartje Bruns
Director Products
Governikus GmbH & Co. KG, Bremen

Tobias Eiss
Geschäftsführer
ClariLab, Frankfurt am Main

Markus Hertlein
Geschäftsführender Gesellschafter, Geschäftsführung
XignSys GmbH, Gelsenkirchen

Michael R. Kissler
Rechtsanwalt & Compliance-Manager
Unleashed Capital GmbH

Alexander Stöhr
Vice President of Operations
XignSys GmbH, Gelsenkirchen

Petra Waldmüller-Schantz
Director Communications
Governikus GmbH & Co. KG, Bremen

Finanz Colloquium Heidelberg, 2022

Digitale Authentifizierung 7

Digitale Authentifizierung

Vorwort

Liebe Leserinnen, liebe Leser,

Gleich, ob persönlich, digital oder hybrid – jede Wirtschaftstätigkeit setzt vielfältiges Vertrauen in die beteiligten Personen und Produkte voraus. Das Vertrauen wiederum bildet sich insbesondere durch Authentifizierung.

Kaufen Sie eine Ware, möchten Sie sicher sein, dass es sich nicht um eine Fälschung handelt. Und wenn Sie die Ware mit Karte bezahlen, soll der Zahlungsbetrag beim Verkäufer ankommen.

Woher wissen Sie als Kunde, ob es sich beispielsweise bei dem Ihnen angepriesenen Käse tatsächlich um Original Sura Kees aus dem Montafon handelt?

Hier greift das erprobte System der Authentifizierung von Lebensmitteln ein. Mittels chemisch-analytischer Methoden werden Verfälschungen des Originals nachgewiesen. Ihr Vertrauen als Kunde speist sich aus der entsprechenden Authentifizierung des Produkts.

Auch für den anschließenden Zahlungsvorgang ist die Unverfälschtheit zentral. Bei Ihnen soll der Kaufpreis abgebucht werden, dem Konto des Verkäufers und nicht etwa einem Dritten soll er gutgeschrieben werden.

Welche Methoden der Authentifizierung im Finanzsektor eingesetzt werden, um Verfälschungen möglichst auszuschließen, bildet den Gegenstand dieser Studie.

Im Mittelpunkt steht dabei die digitale Ausprägung der Authentifizierung. Sämtliche Autoren beschäftigen sich seit Jahren aus verschiedenen Richtungen mit der Identitätsprüfung und ihren Herausforderungen durch die Digitalisierung.

Nach einem Überblick über die rechtlichen Vorgaben, für den der Herausgeber verantwortlich zeichnet, erläutert Michael Kissler von der Unleashed Capital GmbH die aktuellen Verfahren zur Prüfung der digitalen Identität und wirft einen Blick in die Zukunft.

Einen wichtigen Blickwinkel bringen Petra Waldmüller-Schantz und Hartje Bruns von der Governikus GmbH & Co. KG ein: Sie untersuchen insbesondere Synergieeffekte zwischen der öffentlichen Verwaltung und dem Finanzsektor bei den eingesetzten Verfahren der Identitätsprüfung.

Markus Hertlein und Alexander Stöhr von der XignSys GmbH zeigen heutige und zukünftige Anwendungsformen und -bereiche der Authentifizierung auf, wobei sie diese vor allem auf ihren Widerstand gegen Angriffe prüfen.

Tobias Eiss von der ClariLab GmbH & Co. KG beschäftigt sich in seinem Beitrag mit der Herausforderung komplexer „Know-Your-Customer"-Prozesse. Er legt die Möglichkeiten der Automatisierung der erforderlichen Identitätsprüfung dar.

Der Band gewährt im Ergebnis zum einen den Einblick in die aktuelle Praxis der Authentifizierung und trägt zum anderen zur Diskussion über zukünftige Projekte bei. Genießen Sie ihn – gegebenenfalls mit einem geprüften und echten Sura Kees aus dem Montafon.

Frank Arretz, Schalast & Partner

Hinweis: Zur besseren Lesbarkeit und Unterstützung des Leseflusses wurde im nachfolgenden Buch auf die Verwendung des generischen Maskulinums zurückgegriffen. Selbstverständlich schließen jedoch alle Formulierungen und Personenbezeichnungen alle Geschlechter gleichermaßen ein.

A. Gesetzliche Anforderungen an die digitale Authentifizierung

I. Authentifizierung als Herzstück der gesetzlichen Regeln

Sie bildet das „Herzstück“[1] der PSD II[2]: Die digitale Authentifizierung in der Form der sogenannten starken Kundenauthentifizierung.

Die Authentifizierung des Kunden steht im Mittelpunkt der gesetzgeberischen Initiativen zur Gewährleistung des Zahlungsverkehrs. Es geht um technische Verfahren, um das Risiko krimineller Handlungen zu minimieren. Dabei wiederum handelt es sich um eine Grundvoraussetzung für die „Entwicklung eines soliden Umfelds für den elektronischen Geschäftsverkehr“[3].

1. Der gesetzliche Rahmen

Die zentrale gesetzliche Vorschrift zur Regelung der starken Kundenauthentifizierung ist § 55 ZAG. Die Vorschrift dient der Umsetzung des Artikel 97 PSD II.

Gemäß Artikel 115 Abs. 4 PSD II tritt sie 18 Monate nach Inkrafttreten der sog. technischen Regulierungsstandards, wie sie in Artikel 98 PSD II erwähnt sind, in Kraft.

Die im Rahmen der PSD II vorgesehenen technischen Regulierungsstandards sind am 14. März 2018 in Kraft getreten.[4] Dies bedeutet, dass § 55 ZAG seit dem 14. September 2019 gilt.

Die Regelung tritt damit an die Stelle der bisherigen EBA-Leitlinien zur Sicherheit von Internetzahlungen vom 19. Dezember 2014[5].

2. Die „technischen Regulierungsstandards“

Um was handelt es sich bei den technischen Regulierungsstandards? Immerhin wird das Inkrafttreten einer der zentralen Normen für die Kundenauthentifizierung an ihr Inkrafttreten gekoppelt.

Da Artikel 97 PSD II und folglich auch der ihn umsetzende § 55 ZAG mit offenen Rechtsbegriffen arbeiten, hat Artikel 98 PSD II vorgesehen, dass technische Regulierungsstandards den Inhalt der Vorschrift konkretisieren.

Das Verfahren zum Erlass technischer Regulierungsstandards beruht auf der Verordnung (EU) Nr. 1093/2010 vom 24. November 2010.

---

[1] So die Formulierung bei *Dietze*, in: Ellenberger/Findeisen/Nobbe/Böger (Hrsg.), Kommentar zum Zahlungsverkehrsrecht, 3. Auflage 2020, § 55 ZAG RdNr. 749.

[2] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienst im Binnenmarkt; im Folgenden als „PSD II“ bezeichnet.

[3] *Casper/Terlau/Zahrte*, ZAG, 2. Auflage 2020, § 55 RdNr. 1 unter Hinweis auf *Zahrte*, NJW 2018, 337.

[4] Konkret handelt es sich um die delegierte Verordnung (EU) 2018/389 der Kommission vom 27. November 2017 zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation. Zu diesen RTS und ihrer Entstehung vgl. *Brian/Arretz*, BP 10/2017, 351.

[5] Diese hatte die BaFin mit Rundschreiben 4/2015 (BA) – Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSi) vom 05. Mai 2015 übernommen.

Gemäß § 10 dieser Verordnung erarbeitet die Europäische Bankenaufsicht[6] in einem ersten Schritt die Entwürfe derartiger technischer Regulierungsstandards.

Von entscheidender Bedeutung ist, dass sie nach dem Wortlaut der Verordnung lediglich technischer Art sind. Sie dürfen keine strategischen oder politischen Entscheidungen enthalten und sind durch den entsprechenden Gesetzgebungsakt begrenzt.

Die Reaktion der Kommission, ob sie den Entwurf technischer Regulierungsstandards billigt oder nicht, hat innerhalb von drei Monaten zu erfolgen.

Bei einer fehlenden Billigung sieht das weitere Verfahren im Kern eine „Abstimmung" zwischen der EBA und der Kommission, die formal die technischen Regulierungsstandards erlässt, vor. Hat die Kommission die technischen Regulierungsstandards erlassen, können das Europäische Parlament oder der Rat innerhalb einer dreimonatigen Frist Einwände erheben. Erhebt auch nur eines der beiden Organe derartige Einwände, treten die Regulierungsstandards nicht in Kraft.

Im Ergebnis handelt es sich um ein Verfahren mit diversen Konsultationen und Abstimmungen zwischen den beteiligten Kreisen mit einem „Schlusswort" des Europäischen Parlaments bzw. des Rates. Dabei darf der Ausdruck „technische Regulierungsstandards" nicht darüber hinwegtäuschen, dass mit diesem Mittel sehr konkrete Anforderungen aufgestellt werden, die für die Praxis eine immense Rolle spielen.

II. Die Authentifizierung

1. Der Begriff der Authentifizierung und seine Abgrenzungen

§ 55 Abs. 1 ZAG verlangt eine starke Kundenauthentifizierung durch den Zahlungsdienstleister, wenn der Zahler online auf sein Zahlungskonto zugreift, einen elektronischen Zahlungsvorgang auslöst oder über einen Fernzugang einer Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs beinhaltet.

Weiter verlangt § 55 Abs. 1 ZAG von dem Zahlungsdienstleister angemessene Sicherheitsvorkehrungen, um die Vertraulichkeit und die Integrität personalisierter Sicherheitsmerkmale der Zahlungsdienstenutzer zu schützen.

In einem ersten Schritt ist der Begriff der Authentifizierung von der Autorisierung und der Authentisierung abzugrenzen[7].

Vom Gesetz definiert ist der Ausdruck „Autorisierung". Gemäß § 675j Abs. 1 BGB ist ein Zahlungsvorgang gegenüber dem Zahler nur wirksam, wenn er diesem zustimmt. Diese Zustimmung bezeichnet das Gesetz als Autorisierung. Es handelt sich dabei mit anderen Worten um die Einwilligung oder die Genehmigung des Zahlers, damit der Zahlungsvorgang wirksam wird.

Anders als die legaldefinierte „Autorisierung" kennt das Gesetz den Begriff der Authentisierung dagegen nicht.

[6] Es handelt sich um die European Banking Authority; hier im Folgenden, wie üblich, mit „EBA" abgekürzt.

[7] So zu Recht *Casper/Terlau/Zahrte*, a.a.O., RdNr. 2.

Nach dem allgemeinen Sprachgebrauch handelt es sich dabei um die von einer Person behauptete Identität. Sie weist ihre Identität durch die Eingabe eines Passwortes (z. B. PIN), die Vorlage eines entsprechenden Dokuments (z. B. Personalausweis) oder biometrische Merkmale (z. B. Fingerabdruck) nach.

Wie die Autorisierung ist auch die Authentifizierung im Gesetz definiert. Die Definition findet sich in § 1 Abs. 23 ZAG. Er setzt Artikel 4 Nr. 29 PSD II um.

Danach handelt es sich um ein Verfahren, mit dessen Hilfe der Zahlungsdienstleister die Identität des Zahlungsdienstenutzers oder die berechtigte Verwendung eines bestimmten Zahlungsinstruments überprüfen kann. Bei diesem Vorgang wird auch die Verwendung der personalisierten Sicherheitsmerkmale des Nutzers überprüft.

Die personalisierten Sicherheitsmerkmale sind gemäß § 1 Abs. 25 ZAG personalisierte Merkmale, die der Zahlungsdienstleister einem Zahlungsdienstenutzer zum Zwecke der Authentifizierung bereitgestellt. Dazu gehören beispielsweise eine persönliche Identifikationsnummer (PIN), eine einmal verwendbare Transaktionsnummer (TAN) oder auch der Nutzungscode für die elektronische Signatur.

2. Die starke Kundenauthentifizierung

§ 55 ZAG setzt den Begriff der „starken Kundenauthentifizierung“ voraus. Seine Definition findet sich nicht in § 55 ZAG, sondern in § 1 Abs. 24 ZAG.

Danach handelt es sich bei ihr um eine Authentifizierung, die so ausgestaltet ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist.

Sie erfolgt unter Heranziehung von mindestens zwei voneinander unabhängigen Elementen. Dabei stellt die Nichterfüllung eines Kriteriums die Zuverlässigkeit des anderen nicht infrage.

Das Gesetz sieht insoweit die Kategorien Wissen, also etwas, das nur der Nutzer weiß, Besitz, also etwas, das nur er besitzt, und Inhärenz, also etwas, das der Nutzer ist, vor.

Die Kategorie Wissen erfasst beispielsweise Passwörter und PIN; die Kategorie Besitz den Token oder das Smartphone, während sich die Inhärenz auf biometrische Charakteristika wie z. B. den Fingerabdruck bezieht.

Die legal definierte (starke) Kundenauthentifizierung war schon Thema des von der EU-Kommission im Jahre 2012 vorgelegten Grünbuchs „Ein integrierter europäischer Markt für Karten-, Internet- und mobile Zahlungen“.[8]

So wird in dem Grünbuch unter Ziffer 26 die Frage aufgeworfen, ob es zusätzlicher Sicherheitsanforderungen, wie z. B. der Zwei-Faktoren-Authentifizierung bei Fernzahlungen bedürfe.

Konkrete Anforderungen an die Gestaltung lassen sich dem Grünbuch allerdings nicht entnehmen. Es bleibt bei der aufgeworfenen Frage.

[8] KOM(2011) 941 endgültig; https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52011DC0941&from=DE

Die 2-Faktor-Authentifizierung findet sich in dem im Jahre 2014 durch die Europäische Zentralbank veröffentlichten Leitlinien zur Sicherheit von Internetzahlungen durch die Europäische Zentralbank[9].

Wie oben bereits erörtert, erfolgt bei der starken Kundenauthentifizierung der Schutz durch zwei der drei Elemente aus den Kategorien Wissen, Besitz und Inhärenz.

Erforderlich ist eine solche starke Kundenauthentifizierung nach der gesetzlichen Regelung des § 55 Abs. 1 Satz 1 Nr. 1 ZAG zunächst bei einem Online-Zugriff des Zahlers auf sein Zahlungskonto.

Nicht erforderlich ist eine Eignung des Geräts, den Zahlungsvorgang auszulösen. Daher sind hier auch Bankautomaten erfasst. Die telefonische Abfrage ist dagegen ausweislich des Erwägungsgrundes 95 zur PSD II ausdrücklich ausgenommen[10].

Gemäß § 55 Abs. 1 Satz 1 Nr. 2 ZAG ist auch beim Auslösen eines elektronischen Zahlungsvorgangs eine starke Kundenauthentifizierung vorgesehen.

„Auslösen" bedeutet eine Handlung des Zahlers, die zu einem Vorgang beim kontoführenden Zahlungsdienstleister führt. Da Lastschriften nicht vom Zahler, sondern vom Zahlungsempfänger ausgelöst werden, sind sie von der Vorschrift nicht umfasst. Bei der beleghaften eingereichten Überweisung löst erst der Zahlungsdienstleister den Vorgang aus. Daher fallen derartige Handlungen nicht unter den Begriff des „Auslösens"[11].

§ 55 Abs. 1 S. 1 Nr. 3 ZAG umfasst schließlich als Auffangtatbestand jede risikobehaftete Handlung über einen Fernzugang.

Beispiele sind hier die Änderungen des Passwortes für das Online-Banking, aber auch Änderungen von Limiten[12].

3. Die Einzelheiten nach den technischen Regulierungsstandards

§ 55 Abs. 5 ZAG enthält eine umfassende Verweisung auf den „delegierten Rechtsakt nach Artikel 98 der Richtlinie (EU) 2015/2366".

Gemeint sind damit die technischen Regulierungsstandards gemäß der bereits oben zitieren Delegierten Verordnung vom 27. November 2017. Sie regelt die näheren Einzelheiten zu den Erfordernissen und Verfahren zur starken Kundenauthentifizierung einschließlich etwaiger Ausnahmen.

Die Delegierte Verordnung enthält mit Kapitel III ein eigenes Kapitel zu den „Ausnahmen von der starken Kundenauthentifizierung". Einschlägige Parameter sind die Risikohöhe, der gegenständ-

[9] https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf?1cb42bdb72f4c5ef75ec637e-59a0bfda; die entsprechenden Vorarbeiten hatte das von der EZB ins Leben gerufene „European Forum on the Security of Retail Payments, SecuRe Pay, geleistet.

[10] *Casper/Terlau/Zahrte*, a.a.O., RdNr. 36 ff.

[11] Dazu und zu weiteren Beispielen ausführlich *Casper/Terlau/Zahrte*, a.a.O., RdNr. 41 ff.

[12] Die Schwierigkeiten liegen in der weiten Formulierung des Tatbestands; vgl. dazu und den Beispielen *Casper/Terlau/Zahrte*, a.a.O., RdNr. 45.

liche Betrag, die Häufigkeit des Vorgangs sowie der Weg der Zahlung.

Im Einzelnen:

Artikel 10 Abs. 1 RTS[13] sieht Ausnahmen bei den Informationen zu den Zahlungskonten vor. Es geht dabei um den Abruf des Kontostands einer oder mehrerer Zahlungskosten bzw. um den Abruf von Zahlungsvorgängen der letzten 90 Tage.

Ruft der Nutzer eine oder beide dieser Informationen ab, ist eine starke Kundenauthentifizierung nur dann erforderlich, wenn der Nutzer zum ersten Mal zugreift oder mehr als 90 Tage seit dem letztmaligen Zugriff verstrichen sind.

Nach Artikel 11 RTS kann unter bestimmten Voraussetzungen beim kontaktlosen Zahlen an der Verkaufsstelle von der starken Kundenauthentifizierung abgesehen werden.

Voraussetzung ist, dass der Einzelbetrag nicht über 50 EUR hinausgeht und frühere kontaktlose elektronische Zahlungsvorgänge insgesamt nicht über 150 EUR hinausgehen; alternativ ist eine starke Kundenauthentifizierung dann wieder erforderlich, wenn die Anzahl der aufeinanderfolgenden kontaktlosen elektronischen Zahlungsvorgänge mehr als fünf beträgt

Ohne weitere Voraussetzungen kann gemäß Artikel 12 RTS von einer starken Kundenauthentifizierung abgesehen werden, wenn es sich um ein Verkehrsnutzungsentgelt oder eine Parkgebühr handelt, deren Bezahlung an einem unbeaufsichtigten Terminal erfolgt.

Wird gemäß Artikel 13 RTS eine Liste vertrauenswürdiger Empfänger seitens des Zahlers erstellt oder verändert, muss bei diesem erstmaligen Vorgang eine starke Kundenauthentifizierung verlangt werden.

Befindet sich der Zahlungsempfänger auf der erstellten Liste, kann bei einer entsprechenden Zahlung durch den Zahler von der starken Kundenauthentifizierung abgesehen werden.

Eine vergleichbare Regelung findet sich in Artikel 14 RTS. Auch hier muss bei einer Änderung oder erstmaligen Erstellung einer Serie wiederkehrender Zahlungsvorgänge mit demselben Betrag und demselben Zahlungsempfänger eine starke Kundenauthentifizierung vorgesehen werden. Alle nachfolgenden Zahlungsvorgänge sind dann von dieser Vorgabe befreit.

Ebenfalls befreit sind nach Artikel 15 RTS Überweisungen, bei denen der Zahler und der Zahlungsempfänger dieselbe natürliche oder juristische Person ist und beide Zahlungskonten bei demselben Kontoführer unterhalten werden.

Bei elektronischen Fernzahlungsvorgängen kann nach Artikel 16 RTS von der starken Kundenauthentifizierung abgesehen werden, wenn der Betrag des einzelnen Vorgangs nicht über 30 EUR hinausgeht und die Summe der früheren Vorgänge nicht über 100 EUR hinausgehen oder seit der letzten Durchführung der starken Kundenauthentifizierung nicht mehr als fünf einzelne Vorgänge ausgelöst worden sind.

[13] Im Folgenden werden die Vorschriften der Delegierten Verordnung mit der üblichen Bezeichnung „RTS" – Regulatory Technical Standards – versehen.

Artikel 17 RTS sieht eine Ausnahme bei dedizierten Zahlungsprozessen vor, die juristische Personen auslösen. Bei dem Zahler darf es sich nicht um Verbraucher handeln. Wird zusätzlich ein vergleichbares Sicherheitsniveau wie bei der starken Kundenauthentifizierung erreicht, kann von dieser abgesehen werden.

Eine besondere Regel hält Artikel 18 RTS mit der Transaktionsrisikoanalyse bereit. Danach kann bei einem elektronischen Fernzahlungsvorgang von einer starken Kundenauthentifizierung abgesehen werden, wenn die Transaktion mit einem niedrigen Risiko verbunden ist.

Als mit einem niedrigen Risiko verbunden gilt ein solcher Vorgang, bei dem die Betrugsrate maximal so hoch ist wie die Referenzbetrugsrate. Darüber hinaus sind Schwellenwerte hinsichtlich des Zahlungsbetrages einzuhalten.

Entsprechend dem Anhang zur Delegierten Verordnung bestehen Schwellenwerte bei 100 EUR, 250 EUR und 500 EUR.

Bei der Referenzbetrugsrate wird zwischen kartengebundenen Fernzahlungsvorgängen und elektronischen Überweisungen differenziert. Für erstere liegt die jeweilige Referenzbetrugsrate bei 0,13 % (100 EUR), 0,06 % (250 EUR) und 0,01 % (500 EUR); bei letzteren liegt sie bei 0,015 % (100 EUR), 0,01 % (250 EUR) und 0,005 % (500 EUR).

Neben diesem formalen Ansatz dürfen bei der Risikoanalyse in Echtzeit keine besonderen Szenarien zum Vorschein kommen.

Dazu gehören ungewöhnliches Ausgabe- oder Verhaltensmuster des Zahlers, ungewöhnliche Information über den Zugriff auf das Zugangsgerät, eine Malware-Infektion, ein bekanntes Betrugsszenario, ein ungewöhnlicher Ort des Zahlers oder ein Ort des Zahlers mit hohem Risiko.

Artikel 19 RTS legt die Regeln für die Ermittlung der Gesamtbetrugsrate fest. Für jede der oben beschriebenen Zahlungsvorgangsart aus dem Anhang zur Delegierten Verordnung hat der Zahlungsdienstleister sicherzustellen, dass die Gesamtbetrugsrate die entsprechende Referenzbetrugsrate nicht überschreitet. Diese Verpflichtung gilt sowohl bei Vorgängen mit starker Kundenauthentifizierung als auch bei Vorgängen, die gemäß einer der hier besprochenen Ausnahmetatbestände durchgeführt werden.

Die Gesamtbetrugsrate ergibt sich nach Artikel 19 RTS als Gesamtwert der nicht autorisierten oder betrügerisch Fernzahlungsvorgänge dividiert durch den Gesamtwert aller Fernzahlungsvorgänge für dieselbe Zahlungsvorgangsart. Eine Aktualisierung ist alle 90 Tage vorgesehen.

Zur Überwachung der beschriebenen Ausnahmen sind die Zahlungsdienstleister nach Artikel 21 RTS verpflichtet, für jede Zahlungsart verschiedene Daten jedenfalls quartalsweise zu erfassen.

Diese Daten sind danach zu differenzieren, ob es sich um Fernzahlungsvorgänge oder Nicht-Fernzahlungsvorgänge handelt. Konkret ist der Gesamtwert der nicht autorisierten oder betrügerischen Zahlungsvorgänge, der Gesamtwert aller Zahlungsvorgänge sowie die entsprechende Betrugsrate zu erfassen. Dabei ist danach zu differenzieren, ob sie unter Durchführung einer starken Kundenauthentifizierung ausgelöst worden sind und welche Zahlungsvorgänge im Rahmen der vorgenannten Ausnahmen durchgeführt würden.

Darüber hinaus haben die Zahlungsdienstleister den durchschnittlichen Betrag der einzelnen Zahlungen zu erfassen. Auch hier ist wiederum auszuführen, ob sie mit einer starken Kundenauthentifizierung verbunden waren oder nicht.

Schließlich ist die Anzahl der Zahlungsvorgänge, für welche die einzelnen Ausnahmen genutzt wurden, sowie deren prozentualer Anteil im Verhältnis zur Gesamtzahl der Zahlungsvorgänge zu erfassen und überwachen.

Überschreitet die konkrete Betrugsrate die Referenzbetrugsrate in zwei aufeinanderfolgenden Quartalen, ist der Zahlungsdienstleister nach Artikel 20 RTS verpflichtet, die Nutzung der Ausnahme aufgrund der Transaktionsanalyse unverzüglich einzustellen. Eine Wiederaufnahme setzt voraus, dass die Betrugsrate in einem Quartal die Referenzbetrugsrate nicht mehr überschreitet.

4. Angemessene Sicherheitsvorkehrungen

Während § 55 Abs. 1 Satz 1 ZAG in Zusammenhang mit den soeben erläuterten Regeln der Delegierten Verordnung die Tatbestände festlegt, bei denen eine starke Kundenauthentifizierung zu verlangen ist, verlangt § 55 Abs. 1 Satz 2 ZAG angemessene Sicherheitsvorkehrungen des Zahlungsdienstleisters, um die Vertraulichkeit und die Integrität der Sicherheitsmerkmale des Nutzers zu schützen.

Die konkrete Umsetzung dieser Vorgabe findet sich in den Artikeln 22 bis 27 RTS.

Sie verlangen zunächst allgemein, in jeder Phase der Authentifizierung die Sicherheitsmerkmale zu schützen.

Um diesen Schutz zu erreichen, müssen die personalisierten Sicherheitsmerkmale bei der Anzeige verschleiert sein. Das kryptografische Material zur Verschlüsselung der personalisierten Sicherheitsmerkmale ist vor unbefugter Offenlegung zu schützen.

Die Erstellung und Übertragung der Sicherheitsmerkmale haben in einer sicheren Umgebung zu erfolgen. Gleiches gilt für die Identitätsprüfung des Zahlungsdienstnutzers mittels personalisierter Sicherheitsmerkmale. Das Risiko einer unbefugten Nutzung der Authentifizierungsgeräte und der Software ist zu „mindern".

Erfolgt die Identitätsprüfung über einen Fernzugang, ist eine starke Kundenauthentifizierung vorzunehmen.

Diese Regeln gelten entsprechend bei einer Verlängerung oder der erneuten Aktivierung der personalisierten Sicherheitsmerkmale.

Schließlich schreibt Artikel 27 RTS Sicherheitsmaßnahmen bei der Vernichtung, der Deaktivierung und dem Widerruf personalisierter Sicherungsmaßnahmen, der dazugehörigen Authentifizierungsgeräte und der Software vor.

5. Besonderheiten bei elektronischen Fernzahlungsvorgängen

Gemäß § 55 Abs. 2 ZAG ist bei einem elektronischen Fernzahlungsvorgang eine starke Kundenauthentifizierung zu verlangen.

Sie muss nach der gesetzlichen Regelung Elemente umfassen, die den Zahlungsvorgang dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger ver-

knüpfen. Hintergrund ist, dass insoweit ein höheres Betrugsrisiko besteht.

Im Mittelpunkt stehen der Begriff des „Fernzahlungsvorgangs" sowie die „dynamische Verweisung".

Der Fernzahlungsvorgang wird in § 1 Abs. 19 ZAG, der Artikel 4 Nr. 6 PSD II umsetzt, definiert.

Danach handelt es sich um einen Zahlungsvorgang, der über das Internet oder mittels eines Geräts, das für die Fernkommunikation verwendet werden kann, ausgelöst wird. Beispiele sind der Einsatz der Kreditkarte im Internet sowie die Überweisung im Online-Banking.

Kein Fernzahlungsvorgang im Sinne dieser Vorschrift ist eine Zahlung innerhalb eines geschlossenen und besonders gesicherten Netzwerks. Dies trifft beispielsweise auf Selbstbedienungsterminals und Geldausgabeautomaten zu.

Wie die dynamische Verknüpfung zu erfolgen hat, regelt insbesondere Artikel 5 RTS.

Dem Zahler müssen danach der Zahlungsbetrag und der Zahlungsempfänger angezeigt werden. Der generierte Authentifizierungscode gilt speziell für diesen Zahlungsbetrag und diesen Zahlungsempfänger. Gleiches gilt für den vom Zahlungsdienstleister akzeptierten Code[14].

6. Die Skepsis der zivilen Gerichtsbarkeit

Der Bundesgerichtshof hat sich mit Urteil vom 26. Januar 2016 grundlegend mit der Beweislastverteilung im Online-Banking beschäftigt[15]. Danach lässt er einen Anscheinsbeweis bei einem Authentifizierungsverfahren im Online-Banking zu, wenn auf Grundlage aktueller Erkenntnisse die praktische Unüberwindbarkeit des eingesetzten Sicherungssystems gegeben ist. Die Authentifizierung dürfe von einer Kompromittierung der eingesetzten Geräte nicht berührt werden.

Jedenfalls in dem konkreten smsTAN-Verfahren, das dem Bundesgerichtshof vorlag, sind diese Voraussetzungen nicht erfüllt.

Der Gerichtshof führt insbesondere unter Bezug auf Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik aus, es sei fraglich, ob das smsTAN-Verfahren allgemein das erforderliche Sicherheitsniveau aufweise.

Dies ist insoweit bemerkenswert, als die BaFin in ihren „Fragen und Antworten zu den Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)" vom 24. Juni 2016 unter Ziffer 4a) die Frage, ob die heutigen kreditwirtschaftlichen Authentifizierungsverfahren die Anforderungen an eine starke Kundenauthentifizierung erfüllen, zwar auf den Einzelfall bezogen hat. Gleichzeit hat sie aber betont, die eingesetzten Verfahren beruhten auf den geforderten Elementen Wissen und Besitz.

Im Ergebnis zeigt sich hier exemplarisch ein mögliches Auseinanderfallen der aufsichtsrechtlichen Vorgaben einerseits sowie der zivilrechtlichen Haftungstatbestände andererseits. Die zivilrechtliche Haftung wird grundsätzlich autonom, d. h. unabhängig von aufsichtsrechtlichen Regelungen bestimmt.

[14] Die hier geforderte Verknüpfung zwischen Betrag, Empfänger und Code erfüllen die früher gebräuchlichen TAN-Listen nicht.

[15] BGH vom 26. Januar 2016 – XI ZR 91/14.