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 (Text von Bedeutung für den EWR.)

C/2017/7782

OJ L 69, 13.3.2018, p. 23–43 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

In force: This act has been changed. Current consolidated version: 13/03/2018

ELI: http://data.europa.eu/eli/reg_del/2018/389/oj

Languages, formats and link to OJ

	BG	ES	CS	DA	DE	ET	EL	EN	FR	GA	HR	IT	LV	LT	HU	MT	NL	PL	PT	RO	SK	S
HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTML	HTI
PDF																						
Official Journal																						

Multilingual display

English (en) | Please choose | Please choose | Display

Text

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

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG ([1]), insbesondere Artikel 98 Absatz 4 Unterabsatz 2,

in Erwägung nachstehender Gründe:

(1) Elektronisch angebotene Zahlungsdienste sollten sicher abgewickelt werden, wobei Technologien eingesetzt werden sollten, mit denen eine sichere Authentifizierung des Nutzers gewährleistet und das Betrugsrisiko so weit wie möglich verringert werden kann. Das Authentifizierungsverfahren sollte generell Transaktionsüberwachungsmechanismen enthalten, um Versuche zur Verwendung der personalisierten Sicherheitsmerkmale eines Zahlungsdienstnutzers, die verloren, gestohlen oder missbräuchlich verwendet wurden, zu erkennen; außerdem sollte das Authentifizierungsverfahren sicherstellen, dass es sich bei dem Zahlungsdienstnutzer um den legitimen Nutzer handelt, der somit durch die normale Verwendung der personalisierten Sicherheitsmerkmale seine Zustimmung für den Transfer von Geldbeträgen und den Zugang zu seinen Kontoinformationen erteilt. Des Weiteren ist es notwendig, Erfordernisse des Verfahrens zur starken Kundenauthentifizierung festzulegen, die jedes Mal angewendet werden sollten, wenn ein Zahler online auf sein Zahlungskonto zugreift, einen elektronischen Zahlungsvorgang auslöst oder über einen Fernzugang eine Handlung vornimmt, die insofern das Risiko eines Betrugs im Zahlungsverkehr oder eines anderen Missbrauchs birgt, als die Generierung eines Authentifizierungscodes erforderlich ist; dieser Code sollte gegenüber dem Risiko der Fälschung in seiner Gesamtheit oder durch die Offenlegung der Elemente, auf deren Grundlage er generiert wurde, immun sein.

(2) Angesichts der sich ständig ändernden Betrugsmethoden sollten die Erfordernisse für eine starke Kundenauthentifizierung innovative technische Lösungen ermöglichen, mit denen neu aufkommenden Bedrohungen der Sicherheit elektronischer Zahlungen begegnet werden kann. Zur Gewährleistung einer wirksamen kontinuierlichen Umsetzung der festzulegenden Anforderungen sollte ebenfalls verlangt werden, dass die Sicherheitsmaßnahmen für die Durchführung einer starken Kundenauthentifizierung und ihrer Ausnahmen, die Maßnahmen für den Schutz der Vertraulichkeit und der Integrität der personalisierten Sicherheitsmerkmale und die Maßnahmen für die Einrichtung gemeinsamer und sicherer offener Standards für die Kommunikation dokumentiert, regelmäßig getestet, bewertet und von operativ unabhängigen Prüfern mit Fachwissen auf dem Gebiet der IT-Sicherheit und des Zahlungsverkehrs geprüft werden. Damit die zuständigen Behörden die Qualität der Überprüfung dieser Maßnahmen überwachen können, sollten ihnen diese Überprüfungen auf Verlangen zur Verfügung gestellt werden.

(3) Da elektronische Fernzahlungsvorgänge einem höheren Betrugsrisiko ausgesetzt sind, ist es notwendig, bei solchen Vorgängen zusätzliche Anforderungen für eine

starke Kundenauthentifizierung einzuführen; diese sollten sicherstellen, dass die Elemente den Zahlungsvorgang dynamisch mit einem Betrag und einem Zahlungsempfänger verknüpfen, die vom Zahler beim Auslösen des Zahlungsvorgangs angegeben werden.

(4) Eine dynamische Verknüpfung ist durch Generierung von Authentifizierungscodes möglich, bei der eine Reihe strenger Sicherheitsanforderungen einzuhalten sind. Um Technologieneutralität sicherzustellen, sollte für die Implementierung von Authentifizierungscodes keine bestimmte Technologie vorgegeben werden. Solange die Sicherheitsanforderungen erfüllt sind, sollten Authentifizierungscodes daher auf Lösungen beruhen wie der Generierung und Validierung einmaliger Passwörter, digitalen Signaturen oder anderen kryptografisch basierten Gültigkeitsversicherungen unter Verwendung von Schlüsseln oder kryptografischem Material, die in den Authentifizierungselementen gespeichert werden.

(5) Für den Fall, dass der endgültige Betrag zu dem Zeitpunkt, zu dem der Zahler einen elektronischen Fernzahlungsvorgang auslöst, nicht bekannt ist, müssen besondere Anforderungen festgelegt werden, die sicherstellen, dass die starke Kundenauthentifizierung speziell für den Höchstbetrag gilt, für den der Zahler seine Zustimmung erteilt hat, wie in der Richtlinie (EU) 2015/2366 vorgesehen.

(6) Um die Durchführung einer starken Kundenauthentifizierung zu gewährleisten, müssen ebenfalls angemessene Sicherheitsmerkmale für die Elemente der starken Kundenauthentifizierung verlangt werden: für Elemente der Kategorie Wissen (etwas, das nur der Nutzer weiß), wie Länge oder Komplexität, für Elemente der Kategorie Besitz (etwas, das nur der Nutzer besitzt), wie Algorithmusspezifikationen, Schlüssellänge und Informationsentropie, und für Geräte und Software, die Elemente der Kategorie Inhärenz (etwas, das der Nutzer ist) lesen, wie Algorithmusspezifikationen, biometrischer Sensor und Funktionen für den Schutz biometrischer Templates, insbesondere, um das Risiko zu mindern, dass diese Elemente von Unbefugten aufgedeckt, offengelegt und verwendet werden. Ferner ist die Festlegung von Anforderungen notwendig, um sicherzustellen, dass diese Elemente voneinander unabhängig sind, sodass die Nichterfüllung eines Elements die Zuverlässigkeit der anderen nicht infrage stellt, vor allem, wenn diese Elemente von einem Mehrzweckgerät verwendet werden, d. h. von Geräten wie einem Tablet oder einem Mobiltelefon, die sowohl für die Erteilung der Anweisung zur Ausführung der Zahlung als auch für den Authentifizierungsprozess verwendet werden können.

(7) Die Erfordernisse einer starken Kundenauthentifizierung gelten für vom Zahler ausgelöste Zahlungsvorgänge, unabhängig davon, ob der Zahler eine natürliche oder juristische Person ist.

(8) Aufgrund ihrer speziellen Natur unterliegen Zahlungen, die unter Verwendung eines anonymen Zahlungsinstruments ausgeführt werden, nicht der Pflicht zur starken Kundenauthentifizierung. Wird die Anonymität solcher Instrumente aus vertraglichen oder rechtlichen Gründen aufgehoben, unterliegen Zahlungen den Sicherheitsanforderungen, die sich aus der Richtlinie (EU) 2015/2366 und dem

vorliegenden technischen Regulierungsstandard ergeben.

(9) Gemäß der Richtlinie (EU) 2015/2366 wurden die Ausnahmen vom Grundsatz der starken Kundenauthentifizierung ausgehend vom Risikoniveau, vom Betrag und von der Periodizität des Zahlungsvorgangs und des für seine Ausführung genutzten Zahlungswegs festgelegt.

(10) Handlungen, die Einsicht in den Saldo und die letzten Bewegungen eines Zahlungskontos gewähren, ohne dass sensible Zahlungsdaten offengelegt werden, wiederkehrende Zahlungen an dieselben Zahlungsempfänger, die zuvor vom Zahler unter Verwendung der starken Kundenauthentifizierung eingerichtet oder bestätigt wurden, und Zahlungen an und von derselben natürlichen oder juristischen Person, die ein Konto bei demselben Zahlungsdienstleister unterhält, sind mit einem geringen Risiko verbunden und geben Zahlungsdienstleistern die Möglichkeit, in solchen Fällen von einer starken Kundenauthentifizierung abzusehen. Dessen ungeachtet sollten Zahlungsauslösedienstleister, Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausgeben, und Kontoinformationsdienstleister nach den Artikeln 65, 66 und 67 der Richtlinie (EU) 2015/2366 die für die Bereitstellung eines bestimmten Zahlungsdienstes notwendigen und wesentlichen Informationen nur mit Zustimmung des Zahlungsdienstnutzers vom kontoführenden Zahlungsdienstleister anfordern und erhalten. Diese Zustimmung kann individuell für jede Informationsanforderung oder für jede auszulösende Zahlung oder im Fall von Kontoinformationsdienstleistern als Mandat für die in der vertraglichen Vereinbarung mit dem Zahlungsdienstnutzer bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen erteilt werden.

(11) Ausnahmen für kontaktlose Kleinbetragszahlungen an der Verkaufsstelle, die auch eine maximale Anzahl von aufeinanderfolgenden Vorgängen oder einen bestimmten Höchstbetrag aufeinanderfolgender Vorgänge ohne Durchführung einer starken Kundenauthentifizierung einbeziehen, erlauben die Entwicklung benutzerfreundlicher Zahlungsdienste mit niedrigem Risiko und sollten deshalb vorgesehen werden. Gleichfalls angemessen ist die Festlegung einer Ausnahme für elektronische Zahlungsvorgänge, die an unbeaufsichtigten Terminals ausgelöst werden, an denen eine starke Kundenauthentifizierung aus operativen Gründen nicht immer ohne Weiteres durchführbar ist (z. B. zur Vermeidung von Staus und potenziellen Unfällen an Mautstellen oder aufgrund anderer Sicherheitsrisiken).

(12) Wie bei der Ausnahme für kontaktlose Kleinbetragszahlungen an der Verkaufsstelle sollte auch im elektronischen Geschäftsverkehr ein angemessenes Verhältnis zwischen dem Interesse erhöhter Sicherheit bei Fernzahlungsvorgängen und dem Erfordernis der Benutzerfreundlichkeit und allgemeinen Zugänglichkeit von Zahlungsvorgängen sichergestellt werden. Diesen Grundsätzen entsprechend sollten auf umsichtige Weise Schwellenwerte festgesetzt werden, unterhalb deren ausschließlich bei Online-Kleinbetragskäufen von einer starken Kundenauthentifizierung abgesehen werden kann. Für Online-Käufe sollten die Schwellenwerte noch umsichtiger festgesetzt werden, da der Käufer zum Zeitpunkt des Erwerbs physisch nicht präsent ist und diese Situation mit einem geringfügig

höheren Sicherheitsrisiko einhergeht.

(13) Die Erfordernisse einer starken Kundenauthentifizierung gelten für vom Zahler ausgelöste Zahlungsvorgänge, unabhängig davon, ob der Zahler eine natürliche oder juristische Person ist. Viele Zahlungsvorgänge von Unternehmen werden durch dedizierte Prozesse oder Protokolle ausgelöst, die das hohe Maß an Sicherheit gewährleisten, das die Richtlinie (EU) 2015/2366 mit der starken Kundenauthentifizierung erzielen möchte. Falls die zuständigen Behörden feststellen, dass solche Zahlungsprozesse und -protokolle, die nur für Zahler verfügbar sind, bei denen es sich nicht um Verbraucher handelt, die Zielsetzungen der Richtlinie (EU) 2015/2366 im Hinblick auf die Sicherheit erfüllen, können Zahlungsdienstleister in Bezug auf diese Prozesse oder Protokolle von den Erfordernissen einer starken Kundenauthentifizierung ausgenommen werden.

(14) Wenn ein Zahlungsvorgang mithilfe von Echtzeit-Transaktionsrisikoanalysen als Vorgang mit niedrigem Risiko eingestuft wird, ist es ebenfalls angemessen, durch Festlegung wirksamer, risikobasierter Anforderungen, die die Sicherheit der Gelder und personenbezogenen Daten des Zahlungsdienstnutzers gewährleisten, für Zahlungsdienstleister, die von einer starken Kundenauthentifizierung absehen wollen, eine Ausnahme vorzusehen. Bei solchen risikobasierten Anforderungen sollten die Einstufungen der Risikoanalysen zusammengeführt werden, um zu bestätigen, dass kein ungewöhnliches Ausgabe- oder Verhaltensmuster des Zahlers erkannt wurde; hierbei sind weitere Risikofaktoren zu berücksichtigen, einschließlich Informationen über den Ort des Zahlers und des Zahlungsempfängers, und es sollten monetäre Schwellenwerte auf der Grundlage der für Fernzahlungsvorgänge berechneten Betrugsraten festgesetzt werden. Falls ein Zahlungsvorgang aufgrund der Echtzeit-Transaktionsrisikoanalyse nicht als Vorgang mit niedrigem Risiko eingestuft werden kann, sollte der Zahlungsdienstleister auf eine starke Kundenauthentifizierung zurückgreifen. Als Höchstbetrag für eine solche risikobasierte Ausnahme sollte ein Betrag festgesetzt werden, der eine äußerst niedrige entsprechende Betrugsrate sicherstellt; dabei sollte auch der Vergleich mit den Betrugsraten für alle Zahlungsvorgänge des Zahlungsdienstleisters, darunter auch die durch eine starke Kundenauthentifizierung authentifizierten Vorgänge, innerhalb einer bestimmten Zeitspanne sowie fortlaufend herangezogen werden.

(15) Zur Gewährleistung einer wirksamen Durchsetzung sollten Zahlungsdienstleister, die Ausnahmen von der starken Kundenauthentifizierung in Anspruch nehmen möchten, für jede Art von Zahlungsvorgang den Gesamtwert betrügerischer oder nicht autorisierter Zahlungsvorgänge und die festgestellten Betrugsraten für alle ihre Zahlungsvorgänge — unabhängig davon, ob diese im Zuge einer starken Kundenauthentifizierung authentifiziert oder im Rahmen einer entsprechenden Ausnahme ausgeführt wurden — regelmäßig überwachen und den zuständigen Behörden und der Europäischen Bankenaufsichtsbehörde (EBA) auf Verlangen mitteilen.

(16) Die Erhebung dieser neuen historischen Daten zu Betrugsraten bei elektronischen Zahlungsvorgängen trägt außerdem dazu bei, dass die EBA die Schwellenwerte für

die auf einer Echtzeit-Transaktionsrisikoanalyse beruhenden Ausnahme von einer starken Kundenauthentifizierung wirksam überprüfen kann. Nach Artikel 98 Absatz 5 der Richtlinie (EU) 2015/2366 sowie nach Artikel 10 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([2]) sollte die EBA diese technischen Regulierungsstandards überprüfen und der Kommission, soweit erforderlich, einen Entwurf ihrer Aktualisierungen übermitteln, um neue Vorschläge für Schwellenwerte und entsprechende Betrugsraten vorzulegen, mit dem Ziel, die Sicherheit elektronischer Fernzahlungsvorgänge zu erhöhen.

(17) Die Zahlungsdienstleister, die eine der vorgesehenen Ausnahmen in Anspruch nehmen, sollten sich jederzeit dafür entscheiden dürfen, bei den in den betreffenden Bestimmungen angegebenen Handlungen und Zahlungsvorgängen von einer starken Kundenauthentifizierung Gebrauch zu machen.

(18) Die Maßnahmen zum Schutz der Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale sowie zum Schutz der Authentifizierungsgeräte und der Software sollten die Betrugsrisiken im Zusammenhang mit der unbefugten oder betrügerischen Verwendung von Zahlungsinstrumenten und dem unbefugten Zugriff auf Zahlungskonten begrenzen. Dazu müssen Anforderungen für die sichere Erstellung und Bereitstellung der personalisierten Sicherheitsmerkmale und ihre Verknüpfung mit dem Zahlungsdienstnutzer eingeführt und Bedingungen für die Verlängerung und Deaktivierung dieser Sicherheitsmerkmale vorgesehen werden.

(19) Um eine wirksame und sichere Kommunikation zwischen den beteiligten Akteuren im Zusammenhang mit Kontoinformationsdiensten, Zahlungsauslösediensten und der Bestätigung der Verfügbarkeit eines Geldbetrags sicherzustellen, ist es notwendig, die Anforderungen für gemeinsame und sichere offene Kommunikationsstandards festzulegen, die von allen betroffenen Zahlungsdienstleistern zu erfüllen sind. Die Richtlinie (EU) 2015/2366 sieht den Zugang zu Zahlungskontoinformationen und deren Nutzung durch Kontoinformationsdienstleister vor. Die Regeln für den Zugang zu Konten, die keine Zahlungskonten sind, werden durch die vorliegende Verordnung daher nicht geändert.

(20) Jeder kontoführende Zahlungsdienstleister, auf dessen Zahlungskonten online zugegriffen werden kann, sollte mindestens eine Zugangsschnittstelle bieten, über die die sichere Kommunikation mit Kontoinformationsdienstleistern, Zahlungsauslösedienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, möglich ist. Die Schnittstelle sollte es Kontoinformationsdienstleistern, Zahlungsauslösedienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, ermöglichen, sich gegenüber dem kontoführenden Zahlungsdienstleister zu identifizieren. Sie sollte ebenfalls so gestaltet sein, dass Kontoinformationsdienstleister und Zahlungsauslösedienstleister sich auf die Authentifizierungsverfahren verlassen können, die dem Zahlungsdienstnutzer vom kontoführenden Zahlungsdienstleister bereitgestellt werden. Zur Gewährleistung der Neutralität im Hinblick auf die Technologie und das Geschäftsmodell sollten die

kontoführenden Zahlungsdienstleister frei entscheiden können, ob sie eine Schnittstelle anbieten, die speziell der Kommunikation mit Kontoinformationsdienstleistern, Zahlungsauslösedienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, dient, oder ob sie für diese Kommunikation die Nutzung der für die Identifizierung und die Kommunikation mit den Zahlungsdienstnutzern des kontoführenden Zahlungsdienstleisters dienende Schnittstelle zulassen möchten.

(21) Damit Kontoinformationsdienstleister, Zahlungsauslösedienstleister und Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, eigene technische Lösungen entwickeln können, sollte die technische Spezifikation der Schnittstelle angemessen dokumentiert und öffentlich zur Verfügung gestellt werden. Darüber hinaus sollte der kontoführende Zahlungsdienstleister mindestens sechs Monate vor Geltungsbeginn des vorliegenden Regulierungsstandards eine Einrichtung anbieten, die den Zahlungsdienstleistern einen Test der technischen Lösungen ermöglicht; wenn die Schnittstelle nach Geltungsbeginn des vorliegenden Regulierungsstandards eingeführt wird, sollte die Testeinrichtung mindestens sechs Monate vor dem Datum der Markteinführung der Schnittstelle angeboten werden. Zur Gewährleistung der Interoperabilität der verschiedenen technischen Kommunikationslösungen sollte die Schnittstelle von internationalen oder europäischen Normungsorganisationen entwickelte Kommunikationsstandards verwenden.

(22) Die Qualität der von Kontoinformationsdienstleistern und Zahlungsauslösedienstleistern bereitgestellten Dienste wird vom ordnungsgemäßen Funktionieren der von den kontoführenden Zahlungsdienstleistern eingerichteten oder angepassten Schnittstellen abhängen. Wenn diese Schnittstellen nicht den Bestimmungen des vorliegenden Standards entsprechen, ist es daher wichtig, Maßnahmen zu ergreifen, mit denen die Aufrechterhaltung des Geschäftsbetriebs für die Nutzer der betreffenden Dienste gewährleistet wird. Es obliegt den zuständigen nationalen Behörden, dafür zu sorgen, dass Kontoinformationsdienstleister und Zahlungsauslösedienstleister bei der Bereitstellung ihrer Dienste nicht blockiert oder behindert werden.

(23) Wird der Zugang zu Zahlungskonten über eine dedizierte Schnittstelle angeboten, muss verlangt werden, dass die dedizierten Schnittstellen denselben Grad an Verfügbarkeit und Leistung aufweisen wie die für die Zahlungsdienstnutzer verfügbare Schnittstelle, damit das Recht der Zahlungsdienstnutzer auf die Nutzung von Zahlungsauslösediensten und von Diensten für den Zugang zu Kontoinformationen gemäß der Richtlinie (EU) 2015/2366 gewährleistet ist. Außerdem sollten die kontoführenden Zahlungsdienstleister transparente wesentliche Leistungsindikatoren und Service-Level-Ziele für die Verfügbarkeit und die Leistung der dedizierten Schnittstellen definieren, die mindestens so streng sind wie diejenigen, die für die von ihren Zahlungsdienstnutzern verwendete Schnittstelle gelten. Diese Schnittstellen sollten von den Zahlungsdienstleistern, die sie verwenden werden, getestet sowie von den zuständigen Behörden Stresstests unterzogen und überwacht werden.

(24) Damit Zahlungsdienstleister, die sich auf die dedizierte Schnittstelle verlassen, bei Problemen mit Verfügbarkeit oder unzureichender Leistung der Schnittstelle ihre Dienste auch weiterhin erbringen können, ist unter Einhaltung strenger Bedingungen die Bereitstellung eines Fall-back-Mechanismus notwendig, der den betroffenen Dienstleistern die Nutzung der Schnittstelle ermöglicht, die der kontoführende Zahlungsdienstleister für die Identifizierung seiner eigenen Zahlungsdienstnutzer und für die Kommunikation mit diesen unterhält. Stellen die zuständigen Behörden allerdings fest, dass die dedizierten Schnittstellen bestimmte Bedingungen erfüllen und dadurch ein ungehinderter Wettbewerb sichergestellt ist, werden bestimmte kontoführende Zahlungsdienstleister von der Auflage ausgenommen sein, über ihre Schnittstelle auf Kundenseite einen solchen Fall-back-Mechanismus bereitzustellen. Falls die von dieser Auflage ausgenommenen dedizierten Schnittstellen die erforderlichen Bedingungen nicht erfüllen, sind die gewährten Ausnahmen von den jeweils zuständigen Behörden zu widerrufen.

(25) Damit die zuständigen Behörden die Implementierung und Unterhaltung der Kommunikationsschnittstellen wirksam überwachen können, sollten die kontoführenden Zahlungsdienstleister eine Zusammenfassung der maßgeblichen Dokumentation auf ihrer Website zur Verfügung stellen und den zuständigen Behörden auf Verlangen die Dokumentation der Notfalllösungen vorlegen. Des Weiteren sollten die kontoführenden Zahlungsdienstleister Statistiken über die Verfügbarkeit und die Leistung dieser Schnittstelle veröffentlichen.

(26) Zum Schutz der Vertraulichkeit und der Integrität der Daten muss die Sicherheit von Kommunikationssitzungen zwischen kontoführenden Zahlungsdienstleistern, Kontoinformationsdienstleistern, Zahlungsauslösedienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, gewährleistet werden. Insbesondere ist eine sichere Verschlüsselung beim Datenaustausch zwischen Kontoinformationsdienstleistern, Zahlungsauslösedienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, und kontoführenden Zahlungsdienstleistern zu verlangen.

(27) Um das Vertrauen der Nutzer zu erhöhen und eine starke Kundenauthentifizierung zu gewährleisten, sollte dem Rückgriff auf elektronische Identifizierungsmittel und Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([3]) Rechnung getragen werden, was insbesondere in Bezug auf notifizierte elektronische Identifizierungssysteme gilt.

(28) Um einen einheitlichen Geltungsbeginn zu gewährleisten, sollte die vorliegende Verordnung ab demselben Datum gelten, ab dem die Mitgliedstaaten die Anwendung der in den Artikeln 65, 66, 67 und 97 der Richtlinie (EU) 2015/2366 festgelegten Sicherheitsmaßnahmen gewährleisten müssen.

(29) Die vorliegende Verordnung stützt sich auf den Entwurf der technischen Regulierungsstandards, der der Kommission von der Europäischen Bankenaufsichtsbehörde (EBA) vorgelegt wurde.

(30) Die EBA hat zu diesem Entwurf offene und transparente öffentliche Konsultationen

durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 eingesetzten Interessengruppe Bankensektor eingeholt —

HAT FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

In dieser Verordnung werden die Anforderungen festgelegt, die Zahlungsdienstleister für die Umsetzung von Sicherheitsmaßnahmen erfüllen müssen, die es ihnen ermöglichen,

a) das Verfahren zur starken Kundenauthentifizierung nach Artikel 97 der Richtlinie (EU) 2015/2366 anzuwenden;

b) unter genau festgelegten, eingeschränkten Voraussetzungen, die auf die Höhe des Risikos, den Betrag und die Häufigkeit des Zahlungsvorgangs sowie auf den für dessen Ausführung genutzten Zahlungsweg abstellen, von der Durchführung der aus Sicherheitsgründen vorgeschriebenen starken Kundenauthentifizierung abzusehen;

c) die Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer zu schützen;

d) gemeinsame und sichere offene Standards für die Kommunikation zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahlern, Zahlungsempfängern und anderen Zahlungsdienstleistern im Zusammenhang mit der Erbringung und der Nutzung von Zahlungsdiensten gemäß Titel IV der Richtlinie (EU) 2015/2366 festzulegen.

Artikel 2

Allgemeine Anforderungen an die Authentifizierung

(1) Die Zahlungsdienstleister verfügen über Transaktionsüberwachungsmechanismen, die ihnen für den Zweck der Umsetzung der in Artikel 1 Buchstaben a und b genannten Sicherheitsmaßnahmen die Erkennung nicht autorisierter oder betrügerischer Zahlungsvorgänge ermöglichen.

Diese Mechanismen basieren auf der Analyse von Zahlungsvorgängen unter Berücksichtigung der Elemente, die für den Zahlungsdienstnutzer im Rahmen einer normalen Verwendung der personalisierten Sicherheitsmerkmale typisch sind.

(2) Die Zahlungsdienstleister stellen sicher, dass die Transaktionsüberwachungsmechanismen zumindest alle nachstehend genannten risikobasierten Faktoren einbeziehen:

a) Liste der missbräuchlich verwendeten oder gestohlenen Authentifizierungselemente;

b) Betrag eines jeden Zahlungsvorgangs;

c) bekannte Betrugsszenarien bei der Erbringung von Zahlungsdienstleistungen;

d) Anzeichen für eine Malware-Infektion bei einer Sitzung während des Authentifizierungsverfahrens;

e) falls das Zugangsgerät oder die Zugangssoftware vom Zahlungsdienstleister bereitgestellt wird, ein Protokoll über die Nutzung des Zugangsgeräts oder der Zugangssoftware, die dem Zahlungsdienstnutzer zur Verfügung gestellt werden, sowie über die ungewöhnliche Nutzung dieses Geräts oder der Software.

Artikel 3

Überprüfung der Sicherheitsmaßnahmen

(1) Die Umsetzung der in Artikel 1 genannten Sicherheitsmaßnahmen wird dokumentiert, regelmäßig getestet, bewertet und von Prüfern mit Fachwissen auf dem Gebiet der IT-Sicherheit und des Zahlungsverkehrs, die innerhalb des Zahlungsdienstleisters oder von diesem operativ unabhängig sind, gemäß dem geltenden Rechtsrahmen des Zahlungsdienstleisters geprüft.

(2) Die Zeiträume zwischen den nach Absatz 1 durchzuführenden Prüfungen werden gemäß dem für den Zahlungsdienstleister geltenden maßgeblichen Rechnungslegungs- und Abschlussprüfungsrahmenwerk festgelegt.

Für Zahlungsdienstleister, die die Ausnahme nach Artikel 18 in Anspruch nehmen, wird mindestens einmal jährlich eine Prüfung der Methodik, des Modells und der gemeldeten Betrugsraten durchgeführt. Der diese Prüfung vornehmende Prüfer verfügt über Fachwissen auf dem Gebiet der IT-Sicherheit und des Zahlungsverkehrs und ist innerhalb des Zahlungsdienstleisters oder von diesem operativ unabhängig. Diese Prüfung wird im ersten Jahr der Inanspruchnahme der Ausnahme nach Artikel 18 sowie im Anschluss daran mindestens alle drei Jahre — oder auf Verlangen der zuständigen Behörde häufiger — von einem unabhängigen, qualifizierten externen Prüfer durchgeführt.

(3) Als Ergebnis dieser Prüfung werden eine Bewertung und ein Bericht erstellt, aus denen hervorgeht, ob die Sicherheitsmaßnahmen des Zahlungsdienstleisters die in dieser Verordnung dargelegten Anforderungen erfüllen.

Der Gesamtbericht wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

KAPITEL II

SICHERHEITSMAßNAHMEN FÜR DIE DURCHFÜHRUNG EINER STARKEN KUNDENAUTHENTIFIZIERUNG

Artikel 4

Authentifizierungscode

(1) Wenn Zahlungsdienstleister gemäß Artikel 97 Absatz 1 der Richtlinie (EU) 2015/2366 eine starke Kundenauthentifizierung verlangen, muss die Authentifizierung auf mindestens zwei Elementen der Kategorien Wissen, Besitz und Inhärenz basieren und die Generierung eines Authentifizierungscodes nach sich ziehen.

Der Authentifizierungscode wird vom Zahlungsdienstleister nur einmalig akzeptiert, wenn der Zahler diesen Code für den Online-Zugriff auf sein Zahlungskonto, für die Auslösung eines elektronischen Zahlungsvorgangs oder für die Ausführung einer Handlung über einen Fernzugang, die das Risiko eines Betrugs im Zahlungsverkehr oder eines anderen Missbrauchs in sich birgt, verwendet.

(2) Für die Zwecke des Absatzes 1 ergreifen Zahlungsdienstleister Sicherheitsmaßnahmen, die gewährleisten, dass alle folgenden Anforderungen erfüllt sind:

a) Aus der Offenlegung des Authentifizierungscodes können keine Informationen über eines der in Absatz 1 genannten Elemente abgeleitet werden.

b) Aufgrund der Kenntnis eines zuvor generierten anderen Authentifizierungscodes kann kein neuer Authentifizierungscode generiert werden.

c) Der Authentifizierungscode kann nicht gefälscht werden.

(3) Die Zahlungsdienstleister stellen sicher, dass die Authentifizierung durch Generierung eines Authentifizierungscodes alle folgenden Sicherheitsmaßnahmen umfasst:

a) Wenn bei der Authentifizierung für den Fernzugriff, für elektronische Fernzahlungsvorgänge und für Handlungen über einen Fernzugang, die das Risiko eines Betrugs im Zahlungsverkehr oder eines anderen Missbrauchs in sich bergen, die Generierung eines Authentifizierungscodes für die Zwecke des Absatzes 1 fehlgeschlagen ist, darf nicht ermittelt werden können, welches der in jenem Absatz genannten Elemente falsch war.

b) Die Anzahl der möglichen aufeinanderfolgenden fehlgeschlagenen Authentifizierungsversuche, nach der die in Artikel 97 Absatz 1 der Richtlinie (EU) 2015/2366 aufgeführten Handlungen vorübergehend oder permanent gesperrt werden, darf innerhalb einer bestimmten Zeitspanne nicht mehr als fünf betragen.

c) Die Kommunikationssitzungen sind gegen den Zugriff auf die während der Authentifizierung übertragenen Authentifizierungsdaten und gegen die Manipulation durch Unbefugte entsprechend den Anforderungen in Kapitel V geschützt.

d) Die maximale Zeitspanne ohne Aktivität, nachdem der Zahler für den Online-Zugriff auf sein Zahlungskonto authentifiziert wurde, darf nicht mehr als fünf Minuten betragen.

(4) Wenn die Sperrung nach Absatz 3 Buchstabe b vorübergehend ist, werden die Dauer dieser Sperrung und die Anzahl der erneuten Versuche auf Grundlage der Merkmale des dem Zahler bereitgestellten Dienstes sowie aller damit verbundenen relevanten Risiken festgelegt, wobei mindestens die in Artikel 2 Absatz 2 genannten

Faktoren zu berücksichtigen sind.

Der Zahler erhält eine Warnung, bevor die Sperrung dauerhaft wird.

Bei einer dauerhaften Sperrung wird ein sicheres Verfahren eingerichtet, das es dem Zahler ermöglicht, die Nutzung der gesperrten elektronischen Zahlungsinstrumente wiederzuerlangen.

Artikel 5

Dynamische Verknüpfung

(1) Wenn Zahlungsdienstleister gemäß Artikel 97 Absatz 2 der Richtlinie (EU) 2015/2366 eine starke Kundenauthentifizierung verlangen, müssen sie zusätzlich zu den in Artikel 4 der vorliegenden Verordnung genannten Auflagen Sicherheitsmaßnahmen ergreifen, die alle folgenden Anforderungen erfüllen:

a) Zahlungsbetrag und Zahlungsempfänger werden dem Zahler angezeigt.

b) Der generierte Authentifizierungscode gilt speziell für den Zahlungsbetrag und den Zahlungsempfänger, denen der Zahler beim Auslösen des Vorgangs zugestimmt hat.

c) Der vom Zahlungsdienstleister akzeptierte Authentifizierungscode entspricht dem ursprünglichen spezifischen Zahlungsbetrag und der Identität des Zahlungsempfängers, denen der Zahler zugestimmt hat.

d) Jede Änderung beim Betrag oder Zahlungsempfänger zieht die Ungültigkeit des generierten Authentifizierungscodes nach sich.

(2) Für die Zwecke des Absatzes 1 sehen die Zahlungsdienstleister Sicherheitsmaßnahmen vor, die die Vertraulichkeit, die Authentizität und die Integrität aller folgenden Angaben gewährleisten:

a) Zahlungsbetrag und Zahlungsempfänger in allen Phasen der Authentifizierung;

b) Angaben, die dem Zahler in allen Phasen der Authentifizierung, einschließlich der Generierung, Übertragung und Verwendung des Authentifizierungscodes, angezeigt werden.

(3) Für die Zwecke des Absatzes 1 Buchstabe b sowie wenn Zahlungsdienstleister gemäß Artikel 97 Absatz 2 der Richtlinie (EU) 2015/2366 eine starke Kundenauthentifizierung verlangen, muss der Authentifizierungscode folgende Anforderungen erfüllen:

a) Bei einem kartengebundenen Zahlungsvorgang, für den der Zahler nach Artikel 75 Absatz 1 der oben genannten Richtlinie seine Zustimmung zu der genauen Höhe des zu blockierenden Geldbetrags erteilt hat, gilt der Authentifizierungscode speziell für den Betrag, für dessen Blockierung der Zahler seine Zustimmung erteilt hat und dem er beim Auslösen des Zahlungsvorgangs zugestimmt hat.

b) Bei Zahlungsvorgängen, für die der Zahler der Ausführung eines Satzes elektronischer Fernzahlungsvorgänge zugunsten eines oder mehrerer Zahlungsempfänger zugestimmt hat, gilt der Authentifizierungscode speziell für den Gesamtbetrag des Satzes und für die angegebenen Zahlungsempfänger.

Artikel 6

Anforderungen an die Elemente der Kategorie Wissen

(1) Die Zahlungsdienstleister ergreifen Maßnahmen zur Minderung des Risikos, dass die in die Kategorie Wissen fallenden Elemente der starken Kundenauthentifizierung von Unbefugten aufgedeckt oder diesen gegenüber offengelegt werden.

(2) Für die Verwendung dieser Elemente durch den Zahler sind risikomindernde Maßnahmen zu treffen, um ihre Offenlegung gegenüber Unbefugten zu verhindern.

Artikel 7

Anforderungen an die Elemente der Kategorie Besitz

(1) Die Zahlungsdienstleister ergreifen Maßnahmen zur Minderung des Risikos, dass die in die Kategorie Besitz fallenden Elemente der starken Kundenauthentifizierung von Unbefugten verwendet werden.

(2) Für die Verwendung dieser Elemente durch den Zahler sind Maßnahmen zu treffen, um ihre Nachbildung zu verhindern.

Artikel 8

Anforderungen an Geräte und Software in Verbindung mit Elementen der Kategorie Inhärenz

(1) Die Zahlungsdienstleister ergreifen Maßnahmen zur Minderung des Risikos, dass die in die Kategorie Inhärenz fallenden Authentifizierungselemente, die von den dem Zahler bereitgestellten Zugangsgeräten und der Zugangssoftware gelesen werden, von Unbefugten aufgedeckt werden. Als Mindestanforderung gewährleisten die Zahlungsdienstleister, dass für diese Zugangsgeräte und die Software eine sehr geringe Wahrscheinlichkeit besteht, dass ein Unbefugter als Zahler authentifiziert wird.

(2) Für die Verwendung dieser Elemente durch den Zahler sind Maßnahmen zu treffen, die sicherstellen, dass diese Geräte und die Software bei einem unbefugten Zugriff auf sie die unbefugte Verwendung der Elemente nicht zulassen.

Artikel 9

Unabhängigkeit der Elemente

(1) Die Zahlungsdienstleister gewährleisten, dass für die Verwendung der in den Artikeln 6, 7 und 8 genannten Elemente der starken Kundenauthentifizierung Maßnahmen gelten, die sicherstellen, dass hinsichtlich Technologie, Algorithmen und Parametern bei Verletzung eines der Elemente die Zuverlässigkeit der anderen Elemente nicht beeinträchtigt wird.

(2) Wenn eines der Elemente der starken Kundenauthentifizierung oder der Authentifizierungscode selbst von einem Mehrzweckgerät verwendet wird, sehen die Zahlungsdienstleister Sicherheitsmaßnahmen zur Minderung des Risikos vor, das aus der missbräuchlichen Verwendung eines solchen Mehrzweckgeräts erwachsen würde.

(3) Für die Zwecke des Absatzes 2 beinhalten die Risikominderungsmaßnahmen alle folgenden Komponenten:

a) Nutzung getrennter sicherer Ausführungsumgebungen durch die im Mehrzweckgerät installierte Software;

b) Mechanismen, mit denen sichergestellt wird, dass die Software oder das Gerät vom Zahler oder einem Dritten nicht verändert wurde;

c) sofern Veränderungen stattgefunden haben, Mechanismen zur Eindämmung von deren Folgen.

KAPITEL III
AUSNAHMEN VON DER STARKEN KUNDENAUTHENTIFIZIERUNG

Artikel 10

Zahlungskontoinformationen

(1) Zahlungsdienstleister dürfen unter Einhaltung der in Artikel 2 sowie in Absatz 2 des vorliegenden Artikels festgelegten Anforderungen davon absehen, eine starke Kundenauthentifizierung zu verlangen, wenn ein Zahlungsdienstnutzer nur auf eine oder beide der folgenden Informationen online zugreifen kann, ohne dass dabei sensible Zahlungsdaten offengelegt werden:

a) Kontostand eines oder mehrerer bezeichneter Zahlungskonten;

b) Zahlungsvorgänge, die in den vergangenen 90 Tagen über ein oder mehrere bezeichnete Zahlungskonten ausgeführt wurden.

(2) Für die Zwecke des Absatzes 1 dürfen Zahlungsdienstleister nicht von der Durchführung einer starken Kundenauthentifizierung ausgenommen werden, wenn eine der folgenden Bedingungen erfüllt ist:

a) Der Zahlungsdienstnutzer greift zum ersten Mal online auf die in Absatz 1 genannten Informationen zu.

b) Mehr als 90 Tage sind verstrichen, seitdem der Zahlungsdienstnutzer letztmals auf die in Absatz 1 Buchstabe b genannten Informationen online zugegriffen hat und eine starke Kundenauthentifizierung verlangt wurde.

Artikel 11

Kontaktlose Zahlungen an der Verkaufsstelle

Zahlungsdienstleister dürfen unter Einhaltung der in Artikel 2 festgelegten Anforderungen bei Auslösen eines kontaktlosen elektronischen Zahlungsvorgangs durch den Zahler davon absehen, eine starke Kundenauthentifizierung zu verlangen, wenn dabei die folgenden Bedingungen erfüllt sind:

a) Der Einzelbetrag des kontaktlosen elektronischen Zahlungsvorgangs geht nicht über 50 EUR hinaus, und

b) die früheren kontaktlosen elektronischen Zahlungsvorgänge, die über ein mit einer kontaktlosen Funktion ausgestattetes Zahlungsinstrument ausgelöst wurden, gehen seit der letzten Durchführung einer starken Kundenauthentifizierung zusammengenommen nicht über 150 EUR hinaus, oder

c) die Anzahl der aufeinanderfolgenden kontaktlosen elektronischen Zahlungsvorgänge, die über das mit einer kontaktlosen Funktion ausgestattete Zahlungsinstrument ausgelöst wurden, geht seit der letzten Durchführung einer starken Kundenauthentifizierung nicht über fünf hinaus.

Artikel 12

Unbeaufsichtigte Terminals für Nutzungsentgelte und Parkgebühren

Zahlungsdienstleister dürfen unter Einhaltung der in Artikel 2 festgelegten Anforderungen von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn der Zahler an einem unbeaufsichtigten Terminal einen elektronischen Zahlungsvorgang auslöst, um ein Verkehrsnutzungsentgelt oder eine Parkgebühr zu zahlen.

Artikel 13

Vertrauenswürdige Empfänger

(1) Wenn ein Zahler durch seinen kontoführenden Zahlungsdienstleister eine Liste der vertrauenswürdigen Empfänger erstellt oder ändert, müssen Zahlungsdienstleister eine starke Kundenauthentifizierung verlangen.

(2) Sind die allgemeinen Anforderungen an die Authentifizierung erfüllt, dürfen Zahlungsdienstleister bei Auslösen eines Zahlungsvorgangs durch den Zahler von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn der Zahlungsempfänger auf einer zuvor vom Zahler erstellten Liste der vertrauenswürdigen Empfänger geführt wird.

Artikel 14

Wiederkehrende Zahlungsvorgänge

(1) Zahlungsdienstleister müssen eine starke Kundenauthentifizierung verlangen, wenn ein Zahler eine Serie wiederkehrender Zahlungsvorgänge mit demselben Betrag und demselben Zahlungsempfänger erstellt, ändert oder erstmals auslöst.

(2) Sind die allgemeinen Anforderungen an die Authentifizierung erfüllt, dürfen Zahlungsdienstleister bei Auslösen aller nachfolgenden Zahlungsvorgänge, die in eine Serie von Zahlungsvorgängen gemäß Absatz 1 eingeschlossen sind, von der Vorgabe einer starken Kundenauthentifizierung absehen.

Artikel 15

Überweisungen zwischen Konten, die von derselben natürlichen oder juristischen Person gehalten werden

Zahlungsdienstleister dürfen unter Einhaltung der in Artikel 2 festgelegten Anforderungen von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn der Zahler eine Überweisung auslöst und es sich bei dem Zahler und dem Zahlungsempfänger um dieselbe natürliche oder juristische Person handelt und beide Zahlungskonten von demselben kontoführenden Zahlungsdienstleister unterhalten werden.

Artikel 16

Kleinbetragszahlungen

Bei Auslösen eines elektronischen Fernzahlungsvorgangs durch den Zahler dürfen Zahlungsdienstleister von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn folgende Bedingungen erfüllt sind:

a) Der Betrag des elektronischen Fernzahlungsvorgangs geht nicht über 30 EUR hinaus, und

b) die früheren elektronischen Fernzahlungsvorgänge, die vom Zahler seit der letzten Durchführung einer starken Kundenauthentifizierung ausgelöst wurden, gehen zusammengenommen nicht über 100 EUR hinaus, oder

c) seit der letzten Durchführung einer starken Kundenauthentifizierung hat der Zahler nacheinander nicht mehr als fünf einzelne elektronische Fernzahlungsvorgänge ausgelöst.

Artikel 17

Von Unternehmen genutzte sichere Zahlungsprozesse und -protokolle

Bei juristischen Personen, die elektronische Zahlungsvorgänge über dedizierte Zahlungsprozesse oder -protokolle auslösen, die nur Zahlern zur Verfügung stehen, bei denen es sich nicht um Verbraucher handelt, können Zahlungsdienstleister von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn die zuständigen Behörden der Auffassung sind, dass diese Prozesse oder Protokolle mindestens ein vergleichbares Sicherheitsniveau wie das in der Richtlinie (EU) 2015/2366 vorgesehene gewährleisten.

Artikel 18

Transaktionsrisikoanalyse

(1) Zahlungsdienstleister können von der Vorgabe einer starken Kundenauthentifizierung absehen, wenn der Zahler einen elektronischen Fernzahlungsvorgang auslöst, für den der Zahlungsdienstleister ermittelt hat, dass er gemäß den in Artikel 2 und in Absatz 2 Buchstabe c beschriebenen Transaktionsüberwachungsmechanismen mit einem niedrigen Risiko verbunden ist.

(2) Ein elektronischer Zahlungsvorgang nach Absatz 1 gilt als Vorgang mit niedrigem Risiko, wenn alle nachstehenden Bedingungen erfüllt sind:

a) Die vom Zahlungsdienstleister gemeldete und nach Artikel 19 berechnete Betrugsrate für diese Art von Zahlungsvorgängen ist maximal so hoch wie die Referenzbetrugsrate, die in der Tabelle im Anhang für „kartengebundene elektronische Fernzahlungsvorgänge“ bzw. für „elektronische Überweisungen über einen Fernzugang“ angegeben ist.

b) Der Zahlungsbetrag geht nicht über den in der Tabelle im Anhang angegebenen jeweiligen Ausnahmeschwellenwert hinaus.

c) Die Zahlungsdienstleister haben bei der Echtzeitrisikoanalyse keines der folgenden Szenarien festgestellt:

i) ungewöhnliches Ausgabe- oder Verhaltensmuster des Zahlers;

ii) ungewöhnliche Informationen über den Zugriff auf das Zugangsgerät oder die Zugangssoftware des Zahlers;

iii) eine Malware-Infektion in einer Phase des Authentifizierungsverfahrens;

iv) bekanntes Betrugsszenario bei der Erbringung von Zahlungsdienstleistungen;

v) ungewöhnlicher Ort des Zahlers;

vi) Ort des Zahlers mit hohem Risiko.

(3) Zahlungsdienstleister, die elektronische Fernzahlungsvorgänge aufgrund ihres niedrigen Risikos von der starken Kundenauthentifizierung ausnehmen wollen, müssen mindestens die folgenden risikobasierten Faktoren berücksichtigen:

a) die früheren Ausgabemuster des betreffenden Zahlungsdienstnutzers;

b) Zahlungsvorgangshistorie eines jeden Zahlungsdienstnutzers des Zahlungsdienstleisters;

c) Ort des Zahlers und des Zahlungsempfängers zum Zeitpunkt des Zahlungsvorgangs, falls das Zugangsgerät oder die Software vom Zahlungsdienstleister bereitgestellt wird;

d) Erkennung ungewöhnlicher Zahlungsmuster des Zahlungsdienstnutzers im Vergleich zu seiner Zahlungsvorgangshistorie.

Bei seiner Bewertung erfasst der Zahlungsdienstleister alle genannten risikobasierten Faktoren für jeden einzelnen Zahlungsvorgang in einem Risikopunktesystem, um zu entscheiden, ob bei einem bestimmten Zahlungsvorgang auf eine starke Kundenauthentifizierung verzichtet werden darf.

Artikel 19

Berechnung der Betrugsraten

(1) Der Zahlungsdienstleister hat für jede der in der Tabelle im Anhang aufgeführte Zahlungsvorgangsart sicherzustellen, dass die Gesamtbetrugsraten sowohl für mit einer starken Kundenauthentifizierung ausgeführte Zahlungsvorgänge als auch für Zahlungsvorgänge, die im Rahmen einer der in den Artikeln 13 bis 18 genannten Ausnahmen ausgeführt wurden, die in der Tabelle im Anhang für die jeweilige

Zahlungsvorgangsart angegebene Referenzbetrugsrate nicht überschreiten.

Die Gesamtbetrugsrate für jede Zahlungsvorgangsart errechnet sich als Gesamtwert der nicht autorisierten oder betrügerischen Fernzahlungsvorgänge, unabhängig davon, ob der Betrag wiedererlangt wurde, dividiert durch den Gesamtwert aller Fernzahlungsvorgänge für dieselbe Zahlungsvorgangsart, die sowohl mit einer starken Kundenauthentifizierung als auch im Rahmen einer der in den Artikeln 13 bis 18 genannten Ausnahmen ausgeführt wurden, wobei diese Aufstellung fortlaufend quartalsweise (90 Tage) erfolgt.

(2) Die Berechnung der Betrugsraten und die daraus resultierenden Werte werden im Rahmen der nach Artikel 3 Absatz 2 durchzuführenden Prüfung bewertet, um sicherzustellen, dass diese vollständig und richtig sind.

(3) Die Methodik und jedes Modell, die vom Zahlungsdienstleister für die Berechnung der Betrugsraten verwendet werden, sowie die Betrugsraten selbst werden in angemessener Weise dokumentiert und den zuständigen Behörden und der EBA in vollem Umfang zugänglich gemacht; sie werden der (den) zuständige(n) Behörde(n) auf deren Verlangen vorab angezeigt.

Artikel 20

Aufhebung von Ausnahmen aufgrund der Transaktionsrisikoanalyse

(1) Zahlungsdienstleister, die die in Artikel 18 genannte Ausnahme nutzen, zeigen den zuständigen Behörden unverzüglich an, wenn eine der überwachten Betrugsraten für eine der in der Tabelle im Anhang angegebenen Zahlungsvorgangsarten die geltende Referenzbetrugsrate überschreitet; außerdem legen die Zahlungsdienstleister den zuständigen Behörden eine Beschreibung der von ihnen vorgesehenen Maßnahmen vor, um sicherzustellen, dass die von ihnen überwachten Betrugsraten wieder die geltenden Referenzbetrugsraten einhalten.

(2) Die Zahlungsdienstleister stellen die Nutzung der Ausnahme nach Artikel 18 für jede in der Tabelle im Anhang für den betreffenden Ausnahmeschwellenwert angegebene Zahlungsvorgangsart unverzüglich ein, wenn die von ihnen überwachte Betrugsrate die für das Zahlungsinstrument oder die Zahlungsvorgangsart im entsprechenden Ausnahmeschwellenwertebereich geltende Referenzbetrugsrate in zwei aufeinanderfolgenden Quartalen überschreitet.

(3) Nach Einstellung der in Artikel 18 genannten Ausnahme gemäß Absatz 2 des vorliegenden Artikels dürfen die Zahlungsdienstleister von dieser Ausnahme erst dann wieder Gebrauch machen, wenn die von ihnen berechnete Betrugsrate die für die jeweilige Zahlungsvorgangsart im entsprechenden Ausnahmeschwellenwertebereich geltende Referenzbetrugsrate in einem Quartal nicht mehr überschreitet.

(4) Beabsichtigen die Zahlungsdienstleister die erneute Nutzung der in Artikel 18 genannten Ausnahme, setzen sie die zuständigen Behörden innerhalb einer angemessenen Frist davon in Kenntnis und erbringen vor der erneuten Nutzung der Ausnahme einen Nachweis dafür, dass die von ihnen überwachte Betrugsrate die für den jeweiligen Ausnahmeschwellenwert geltende Referenzbetrugsrate nach Absatz 3 des

vorliegenden Artikels wieder einhält.

Artikel 21

Überwachung

(1) Damit die Zahlungsdienstleister die in den Artikeln 10 bis 18 dargelegten Ausnahmen nutzen können, erfassen und überwachen sie für jede Zahlungsart die folgenden Daten mindestens quartalsweise, wobei eine Aufschlüsselung nach Fernzahlungsvorgängen und Nicht-Fernzahlungsvorgängen vorzunehmen ist:

a) Gesamtwert der nicht autorisierten oder betrügerischen Zahlungsvorgänge nach Artikel 64 Absatz 2 der Richtlinie (EU) 2015/2366, Gesamtwert aller Zahlungsvorgänge und die entsprechende Betrugsrate, einschließlich einer Aufschlüsselung der unter Durchführung einer starken Kundenauthentifizierung ausgelösten und der im Rahmen der einzelnen Ausnahmen ausgeführten Zahlungsvorgänge;

b) durchschnittlicher Betrag der einzelnen Zahlungen, einschließlich einer Aufschlüsselung der unter Durchführung einer starken Kundenauthentifizierung ausgelösten und der im Rahmen der einzelnen Ausnahmen ausgeführten Zahlungsvorgänge;

c) Anzahl der Zahlungsvorgänge, für die die einzelnen Ausnahmen genutzt wurden, und deren prozentualer Anteil im Verhältnis zur Gesamtzahl der Zahlungsvorgänge.

(2) Die Zahlungsdienstleister stellen den zuständigen Behörden und der EBA die Ergebnisse ihrer Überwachung nach Absatz 1 zur Verfügung und zeigen sie der (den) zuständige(n) Behörde(n) auf deren Verlangen vorab an.

KAPITEL IV
VERTRAULICHKEIT UND INTEGRITÄT DER PERSONALISIERTEN SICHERHEITSMERKMALE DER ZAHLUNGSDIENSTNUTZER

Artikel 22

Allgemeine Anforderungen

(1) Die Zahlungsdienstleister gewährleisten die Vertraulichkeit und die Integrität der personalisierten Sicherheitsmerkmale des Zahlungsdienstnutzers, einschließlich Authentifizierungscodes, in jeder Phase der Authentifizierung.

(2) Für die Zwecke des Absatzes 1 gewährleisten die Zahlungsdienstleister, dass alle folgenden Anforderungen erfüllt sind:

a) Die personalisierten Sicherheitsmerkmale werden bei ihrer Anzeige verschleiert und sind nicht in ihrem gesamten Umfang lesbar, wenn sie vom Zahlungsdienstnutzer während der Authentifizierung eingegeben werden.

b) Die personalisierten Sicherheitsmerkmale im Datenformat sowie das kryptografische Material im Zusammenhang mit der Verschlüsselung der personalisierten

Sicherheitsmerkmale werden nicht im Klartext gespeichert.

c) Das geheime kryptografische Material ist vor unbefugter Offenlegung geschützt.

(3) Die Zahlungsdienstleister dokumentieren den Prozess zur Verwaltung des kryptografischen Materials, mit dem die personalisierten Sicherheitsmerkmale verschlüsselt oder auf andere Weise unlesbar gemacht werden, vollständig.

(4) Die Zahlungsdienstleister gewährleisten die Verarbeitung und die Weiterleitung der personalisierten Sicherheitsmerkmale und der gemäß Kapitel II generierten Authentifizierungscodes in sicheren Umgebungen gemäß weithin anerkannten, strengen Branchenstandards.

Artikel 23

Erstellung und Übertragung von Sicherheitsmerkmalen

Die Zahlungsdienstleister gewährleisten die Erstellung der personalisierten Sicherheitsmerkmale in einer sicheren Umgebung.

Sie sorgen dafür, dass die Risiken einer unbefugten Nutzung der personalisierten Sicherheitsmerkmale sowie der Authentifizierungsgeräte und der Software gemindert werden, sollten die personalisierten Sicherheitsmerkmale vor ihrer Bereitstellung verloren gehen oder gestohlen oder kopiert werden.

Artikel 24

Identitätsüberprüfung des Zahlungsdienstnutzers

(1) Die Zahlungsdienstleister stellen sicher, dass nur der Zahlungsdienstnutzer den personalisierten Sicherheitsmerkmalen, den Authentifizierungsgeräten und der Software zugeordnet ist und dabei Sicherheit gewährleistet ist.

(2) Für die Zwecke des Absatzes 1 stellen die Zahlungsdienstleister sicher, dass alle folgenden Anforderungen erfüllt sind:

a) Die Identitätsüberprüfung des Zahlungsdienstnutzers mithilfe von personalisierten Sicherheitsmerkmalen, Authentifizierungsgeräten und Software findet in sicheren Umgebungen statt, die in den Verantwortungsbereich des Zahlungsdienstleisters fallen und zumindest die Geschäftsräume des Zahlungsdienstleisters, die von diesem bereitgestellte Internetumgebung oder ähnliche sichere Websites, die vom Zahlungsdienstleister und seinen Geldautomatendiensten verwendet werden, umfassen, und trägt den Risiken Rechnung, die mit den bei diesem Prozess verwendeten Geräten und zugrunde liegenden Komponenten, die sich der Verantwortung des Zahlungsdienstleisters entziehen, verbunden sind.

b) Bei der Identitätsüberprüfung des Zahlungsdienstnutzers mithilfe von personalisierten Sicherheitsmerkmalen sowie Authentifizierungsgeräten oder Software über einen Fernzugang wird eine starke Kundenauthentifizierung vorgenommen.

Artikel 25

Bereitstellung von Sicherheitsmerkmalen, Authentifizierungsgeräten und Software

(1) Die Zahlungsdienstleister gewährleisten, dass die Bereitstellung der personalisierten Sicherheitsmerkmale, der Authentifizierungsgeräte und der Software an den Zahlungsdienstnutzer auf sichere Weise erfolgt, um dem Risiko ihrer unbefugten Verwendung bei Verlust, Diebstahl oder Kopie Rechnung zu tragen.

(2) Für die Zwecke des Absatzes 1 wenden die Zahlungsdienstleister zumindest alle folgenden Maßnahmen an:

a) wirksame und sichere Bereitstellungsmechanismen, durch die sichergestellt ist, dass die personalisierten Sicherheitsmerkmale, die Authentifizierungsgeräte und die Software für den rechtmäßigen Zahlungsdienstnutzer bereitgestellt werden;

b) Mechanismen, mit denen der Zahlungsdienstleister die Authentizität der über das Internet für den Zahlungsdienstnutzer bereitgestellten Authentifizierungssoftware verifizieren kann;

c) Vorkehrungen, die bei Bereitstellung der personalisierten Sicherheitsmerkmale außerhalb der Geschäftsräume des Zahlungsdienstleisters oder über einen Fernzugang Folgendes gewährleisten:

   i) ein Unbefugter kann nicht mehr als ein Merkmal der personalisierten Sicherheitsmerkmale, der Authentifizierungsgeräte oder der Software erlangen, wenn diese auf demselben Weg bereitgestellt werden;

   ii) die personalisierten Sicherheitsmerkmale, die Authentifizierungsgeräte oder die Software müssen vor der Nutzung aktiviert werden;

d) Vorkehrungen, die gewährleisten, dass im Falle einer Aktivierung der personalisierten Sicherheitsmerkmale, der Authentifizierungsgeräte oder der Software vor der erstmaligen Verwendung die Aktivierung in einer sicheren Umgebung im Einklang mit der in Artikel 24 beschriebenen Identitätsüberprüfung stattfindet.

Artikel 26

Verlängerung der personalisierten Sicherheitsmerkmale

Die Zahlungsdienstleister gewährleisten, dass die Verlängerung oder die erneute Aktivierung der personalisierten Sicherheitsmerkmale gemäß den Verfahren für die in den Artikeln 23, 24 und 25 beschriebene Erstellung, Verknüpfung und Bereitstellung der Sicherheitsmerkmale und der Authentifizierungsgeräte vorgenommen wird.

Artikel 27

Vernichtung, Deaktivierung und Widerruf

Die Zahlungsdienstleister gewährleisten, dass sie über wirksame Prozesse zur Anwendung aller folgenden Sicherheitsmaßnahmen verfügen:

a) sichere Vernichtung, sichere Deaktivierung und sicherer Widerruf der personalisierten Sicherheitsmerkmale, der Authentifizierungsgeräte und der Software;

b) wenn der Zahlungsdienstleister wiederverwendbare Authentifizierungsgeräte und Software ausgibt, wird die sichere Wiederverwendung eines Geräts oder der Software festgelegt, dokumentiert und implementiert, bevor das Gerät oder die Software einem anderen Zahlungsdienstnutzer bereitgestellt wird;

c) Deaktivierung oder Widerruf von Informationen in Bezug auf die personalisierten Sicherheitsmerkmale, die in den Systemen und Datenbanken des Zahlungsdienstleisters oder gegebenenfalls in öffentlichen Datenarchiven gespeichert sind.

KAPITEL V

GEMEINSAME UND SICHERE OFFENE KOMMUNIKATIONSSTANDARDS

Abschnitt 1

Allgemeine Anforderungen an die Kommunikation

Artikel 28

Anforderungen an die Identifizierung

(1) Für die Kommunikation zwischen dem Gerät des Zahlers und den Akzeptanzgeräten des Zahlungsempfängers, wozu unter anderem auch Zahlungsterminals zählen, gewährleisten die Zahlungsdienstleister eine sichere Identifizierung.

(2) Die Zahlungsdienstleister gewährleisten, dass bei mobilen Anwendungen und anderen Schnittstellen von Zahlungsdienstnutzern, die elektronische Zahlungsdienste ermöglichen, die Risiken einer Fehlleitung der Kommunikation an Unbefugte wirksam eingedämmt werden.

Artikel 29

Rückverfolgbarkeit

(1) Die Zahlungsdienstleister verfügen über Prozesse, die sicherstellen, dass alle Zahlungsvorgänge und anderen Interaktionen mit dem Zahlungsdienstnutzer, mit anderen Zahlungsdienstleistern und mit anderen Einrichtungen, einschließlich Händlern, im Zusammenhang mit der Bereitstellung des Zahlungsdienstes zurückverfolgt werden können, wobei sichergestellt sein muss, dass von allen für die elektronische Transaktion maßgeblichen Ereignissen in jedem Stadium nachträglich Kenntnis erlangt werden kann.

(2) Für die Zwecke des Absatzes 1 gewährleisten die Zahlungsdienstleister, dass jede

mit dem Zahlungsdienstnutzer, mit anderen Zahlungsdienstleistern und mit anderen Einrichtungen, einschließlich Händlern, aufgebaute Kommunikationssitzung auf jedem der folgenden Faktoren beruht:

a) eindeutige Kennung der Sitzung;

b) Sicherheitsmechanismen für die ausführliche Protokollierung der Transaktion, einschließlich Transaktionsnummer, Zeitstempel und aller maßgeblichen Transaktionsdaten;

c) Zeitstempel, die auf einem einheitlichen Zeitreferenzsystem basieren und die entsprechend einem offiziellen Zeitsignal synchronisiert werden.

Abschnitt 2

Besondere Anforderungen an gemeinsame und sichere offene Kommunikationsstandards

Artikel 30

Allgemeine Anforderungen an Zugangsschnittstellen

(1) Kontoführende Zahlungsdienstleister, die einem Zahler ein online zugängliches Zahlungskonto bereitstellen, haben mindestens eine Schnittstelle eingerichtet, die alle folgenden Anforderungen erfüllt:

a) Kontoinformationsdienstleister, Zahlungsauslösedienstleister und Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, können sich gegenüber dem kontoführenden Zahlungsdienstleister identifizieren.

b) Kontoinformationsdienstleister können auf sichere Weise kommunizieren, um Informationen über ein oder mehrere bezeichnete Zahlungskonten und damit in Zusammenhang stehende Zahlungsvorgänge anzufordern und zu empfangen.

c) Zahlungsauslösedienstleister können auf sichere Weise kommunizieren, um einen Zahlungsauftrag für das Zahlungskonto des Zahlers auszulösen und alle Informationen über die Auslösung des Zahlungsvorgangs sowie alle den kontoführenden Zahlungsdienstleistern zugänglichen Informationen in Bezug auf die Ausführung des Zahlungsvorgangs zu empfangen.

(2) Zur Authentifizierung des Zahlungsdienstnutzers ermöglicht es die in Absatz 1 genannte Schnittstelle, dass Kontoinformationsdienstleister und Zahlungsauslösedienstleister sich auf alle Authentifizierungsverfahren verlassen können, die dem Zahlungsdienstnutzer vom kontoführenden Zahlungsdienstleister bereitgestellt werden.

Die Schnittstelle muss zumindest alle folgenden Anforderungen erfüllen:

a) Ein Zahlungsauslösedienstleister oder ein Kontoinformationsdienstleister kann den kontoführenden Zahlungsdienstleister ausgehend von der Zustimmung des Zahlungsdienstnutzers anweisen, mit der Authentifizierung zu beginnen.

b) Während der Authentifizierung werden Kommunikationssitzungen zwischen dem kontoführenden Zahlungsdienstleister, dem Kontoinformationsdienstleister, dem Zahlungsauslösedienstleister und dem betreffenden Zahlungsdienstnutzer aufgebaut und aufrechterhalten.

c) Integrität und Vertraulichkeit der personalisierten Sicherheitsmerkmale und der Authentifizierungscodes, die durch oder über den Zahlungsauslösedienstleister oder den Kontoinformationsdienstleister übertragen werden, sind gewährleistet.

(3) Die kontoführenden Zahlungsdienstleister gewährleisten, dass ihre Schnittstellen die von internationalen oder europäischen Standardisierungsorganisationen ausgegebenen Kommunikationsstandards erfüllen.

Die kontoführenden Zahlungsdienstleister gewährleisten zudem, dass die technische Spezifikation einer jeden Schnittstelle dokumentiert ist und die Routinen, Protokolle und Tools angibt, die von Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, benötigt werden, damit die Interoperabilität ihrer Software und ihrer Anwendungen mit den Systemen der kontoführenden Zahlungsdienstleister gegeben ist.

Die kontoführenden Zahlungsdienstleister machen zumindest die auf die Zugangsschnittstelle bezogene Dokumentation spätestens sechs Monate vor dem in Artikel 38 Absatz 2 genannten Geltungsbeginn oder vor dem anvisierten Termin der Markteinführung der Zugangsschnittstelle, wenn die Einführung nach dem in Artikel 38 Absatz 2 angegebenen Datum erfolgt, auf Verlangen der zugelassenen Zahlungsauslösedienstleister, Kontoinformationsdienstleister und Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, oder der Zahlungsdienstleister, die ihre entsprechende Zulassung bei den zuständigen Behörden beantragt haben, kostenfrei zugänglich und veröffentlichen eine Zusammenfassung der Dokumentation auf ihrer Website.

(4) Zusätzlich zu Absatz 3 gewährleisten die kontoführenden Zahlungsdienstleister, dass sie, Notfallsituationen ausgenommen, jegliche Änderung der technischen Spezifikation ihrer Schnittstelle den zugelassenen Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern und Zahlungsdienstleistern, die kartengebundene Zahlungsinstrumente ausstellen, oder Zahlungsdienstleistern, die ihre entsprechende Zulassung bei den zuständigen Behörden beantragt haben, so bald wie möglich und nicht später als drei Monate vor Implementierung der Änderung im Voraus zur Verfügung stellen.

Die Zahlungsdienstleister dokumentieren Notfallsituationen, in denen Änderungen implementiert wurden, und machen die Dokumentation den zuständigen Behörden auf Verlangen zugänglich.

(5) Die kontoführenden Zahlungsdienstleister stellen eine Testumgebung, einschließlich Unterstützung, für den Verbindungsaufbau und für Funktionstests zur Verfügung, damit die zugelassenen Zahlungsauslösedienstleister, Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, Kontoinformationsdienstleister oder Zahlungsdienstleister, die eine entsprechende Zulassung beantragt haben, ihre

Software und ihre Anwendungen testen können, die sie verwenden, um Benutzern einen Zahlungsdienst anzubieten. Diese Testumgebung sollte spätestens sechs Monate vor dem in Artikel 38 Absatz 2 genannten Geltungsbeginn oder vor dem anvisierten Termin der Markteinführung der Zugangsschnittstelle zur Verfügung gestellt werden, wenn die Einführung nach dem in Artikel 38 Absatz 2 angegebenen Datum erfolgt.

Jedoch dürfen über die Testumgebung keine sensiblen Informationen ausgetauscht werden.

(6) Die zuständigen Behörden stellen sicher, dass die kontoführenden Zahlungsdienstleister den in den vorliegenden Standards verankerten Verpflichtungen in Bezug auf für die von ihnen eingerichtete(n) Schnittstelle(n) jederzeit nachkommen. Falls ein kontoführender Zahlungsdienstleister die Anforderungen an Schnittstellen gemäß den vorliegenden Standards nicht erfüllt, stellen die zuständigen Behörden sicher, dass die Erbringung von Zahlungsauslösediensten und Kontoinformationsdiensten nicht verhindert oder unterbrochen wird, soweit die betreffenden Anbieter solcher Dienste die in Artikel 33 Absatz 5 festgelegten Bedingungen erfüllen.

Artikel 31

Zugangsschnittstellenoptionen

Die kontoführenden Zahlungsdienstleister richten die in Artikel 30 genannte(n) Schnittstelle(n) ein, indem sie eine dedizierte Schnittstelle bereitstellen oder den in Artikel 30 Absatz 1 genannten Zahlungsdienstleistern die Nutzung der für die Authentifizierung und die Kommunikation mit den Zahlungsdienstnutzern des kontoführenden Zahlungsdienstleisters verwendeten Schnittstellen erlauben.

Artikel 32

Anforderungen an eine dedizierte Schnittstelle

(1) Sofern die Anforderungen der Artikel 30 und 31 erfüllt sind, gewährleisten die kontoführenden Zahlungsdienstleister, die eine dedizierte Schnittstelle eingerichtet haben, dass diese Schnittstelle jederzeit denselben Grad an Verfügbarkeit und Leistung, einschließlich Unterstützung, aufweist wie die Schnittstellen, die dem Zahlungsdienstnutzer für den direkten Online-Zugriff auf sein Zahlungskonto zur Verfügung stehen.

(2) Kontoführende Zahlungsdienstleister, die eine dedizierte Schnittstelle eingerichtet haben, definieren transparente wesentliche Leistungsindikatoren und Service-Level-Ziele, die im Hinblick auf Verfügbarkeit und die nach Artikel 36 bereitgestellten Daten mindestens so streng sind wie diejenigen, die für die von ihren Zahlungsdienstnutzern verwendete Schnittstelle gelten. Diese Schnittstellen, Indikatoren und Zielvorgaben werden von den zuständigen Behörden überwacht und Stresstests unterzogen.

(3) Kontoführende Zahlungsdienstleister, die eine dedizierte Schnittstelle eingerichtet haben, gewährleisten, dass diese Schnittstelle die Bereitstellung von Zahlungsauslöse- und Kontoinformationsdiensten nicht beeinträchtigt. Solche Beeinträchtigungen könnten

unter anderem darin bestehen, dass die in Artikel 30 Absatz 1 angegebenen Zahlungsdienstleister die von den kontoführenden Zahlungsdienstleistern an ihre Kunden ausgegebenen Sicherheitsmerkmale nicht verwenden können, wodurch sie auf die Authentifizierungs- und anderen Funktionen des kontoführenden Zahlungsdienstleisters zurückgreifen müssten; dadurch könnten weitere Zulassungen und Registrierungen zusätzlich zu den in den Artikeln 11, 14 und 15 der Richtlinie (EU) 2015/2366 vorgesehenen oder eine zusätzliche Prüfung der vom Zahlungsdienstnutzer den Zahlungsauslöse- und den Kontoinformationsdienstleistern erteilten Zustimmung erforderlich sein.

(4) Die kontoführenden Zahlungsdienstleister überwachen die Verfügbarkeit und Leistung der dedizierten Schnittstelle für die Zwecke der Absätze 1 und 2. Die kontoführenden Zahlungsdienstleister veröffentlichen auf ihrer Website vierteljährliche Statistiken über die Verfügbarkeit und die Leistung der dedizierten Schnittstelle und der von ihren Zahlungsdienstnutzern verwendeten Schnittstelle.

Artikel 33

Notfallmaßnahmen für eine dedizierte Schnittstelle

(1) Für den Fall, dass die Schnittstelle die in Artikel 32 vorgesehene Leistung nicht erbringt oder eine unvorhergesehene Nichtverfügbarkeit der Schnittstelle oder ein Systemausfall auftritt, beziehen die kontoführenden Zahlungsdienstleister in die Gestaltung der dedizierten Schnittstelle eine Notfallstrategie und Notfallpläne ein. Von einer unvorhergesehenen Nichtverfügbarkeit oder einem Systemausfall wird ausgegangen, wenn fünf aufeinanderfolgende Anfragen für den Zugang zu Informationen zur Bereitstellung von Zahlungsauslösediensten oder Kontoinformationsdiensten nicht innerhalb von 30 Sekunden beantwortet werden.

(2) Die Notfallmaßnahmen müssen Kommunikationspläne umfassen, um die die dedizierte Schnittstelle nutzenden Zahlungsdienstleister über Maßnahmen zur Wiederherstellung des Systems zu informieren; ferner müssen die Notfallmaßnahmen eine Beschreibung der sofort verfügbaren alternativen Optionen vorsehen, die die Zahlungsdienstleister während dieser Zeit unter Umständen haben.

(3) Der kontoführende Zahlungsdienstleister sowie die in Artikel 30 Absatz 1 genannten Zahlungsdienstleister melden Probleme mit den dedizierten Schnittstellen entsprechend Absatz 1 des vorliegenden Artikels ihren zuständigen nationalen Behörden unverzüglich.

(4) Im Rahmen eines Notfallmechanismus ist den in Artikel 30 Absatz 1 genannten Zahlungsdienstleistern die Nutzung der Schnittstellen, die der kontoführende Zahlungsdienstleister seinen Zahlungsdienstnutzern für die Authentifizierung und Kommunikation bereitstellt, so lange gestattet, bis für die dedizierte Schnittstelle das in Artikel 32 vorgesehene Verfügbarkeits- und Leistungsniveau wiederhergestellt ist.

(5) Zu diesem Zweck gewährleisten die kontoführenden Zahlungsdienstleister, dass die in Artikel 30 Absatz 1 genannten Zahlungsdienstleister identifiziert werden und sich auf die Authentifizierungsverfahren verlassen können, die der kontoführende

Zahlungsdienstleister dem Zahlungsdienstnutzer bereitstellt. Wenn die in Artikel 30 Absatz 1 genannten Zahlungsdienstleister die Schnittstelle gemäß Absatz 4 nutzen,

a) ergreifen sie die notwendigen Maßnahmen, um sicherzustellen, dass sie nur für den Zweck der Bereitstellung des vom Zahlungsdienstnutzer angeforderten Dienstes Daten abrufen, speichern oder verarbeiten;

b) kommen sie weiterhin den Verpflichtungen gemäß Artikel 66 Absatz 3 bzw. Artikel 67 Absatz 2 der Richtlinie (EU) 2015/2366 nach;

c) protokollieren sie die Daten, die über die vom kontoführenden Zahlungsdienstleister für seine Zahlungsdienstnutzer betriebene Schnittstelle abgerufen werden, und stellen ihrer zuständigen nationalen Behörde auf Verlangen die Protokolldateien unverzüglich zur Verfügung;

d) legen sie gegenüber ihrer zuständigen nationalen Behörde auf Verlangen unverzüglich die Gründe für die Nutzung der Schnittstelle dar, die den Zahlungsdienstnutzern für den direkten Online-Zugriff auf ihr Zahlungskonto bereitgestellt wird;

e) informieren sie den kontoführenden Zahlungsdienstleister diesbezüglich.

(6) Die zuständigen Behörden nehmen — nach Konsultation der EBA zur Gewährleistung der einheitlichen Anwendung der nachstehend genannten Bedingungen — die kontoführenden Zahlungsdienstleister, die sich für eine dedizierte Schnittstelle entschieden haben, von der Verpflichtung zur Einrichtung des Notfallmechanismus nach Absatz 4 aus, wenn die dedizierte Schnittstelle alle folgenden Bedingungen erfüllt:

a) Sie erfüllt alle für dedizierte Schnittstellen in Artikel 32 dargelegten Anforderungen.

b) Sie wurde gemäß Artikel 30 Absatz 5 zur Zufriedenheit der darin genannten Zahlungsdienstleister gestaltet und getestet.

c) Sie wurde mindestens drei Monate lang von Zahlungsdienstleistern in breitem Umfang für die Erbringung von Kontoinformationsdiensten, Zahlungsauslösediensten und zur Bestätigung der Verfügbarkeit eines Geldbetrags bei kartenbasierten Zahlungsvorgängen genutzt.

d) Alle Probleme im Zusammenhang mit der dedizierten Schnittstelle wurden unverzüglich behoben.

(7) Wenn die unter a und d genannten Bedingungen von den kontoführenden Zahlungsdienstleistern für einen Zeitraum von mehr als zwei aufeinanderfolgenden Kalenderwochen nicht erfüllt werden, widerrufen die zuständigen Behörden die in Absatz 6 genannte Ausnahme. Die zuständigen Behörden setzen die EBA von diesem Widerruf in Kenntnis und stellen sicher, dass der kontoführende Zahlungsdienstleister schnellstmöglich, spätestens aber innerhalb von zwei Monaten den Notfallmechanismus gemäß Absatz 4 einrichtet.

Artikel 34

Zertifikate

(1) Zur Identifizierung gemäß Artikel 30 Absatz 1 Buchstabe a verlassen sich die Zahlungsdienstleister auf qualifizierte Zertifikate für elektronische Siegel nach Artikel 3 Absatz 30 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates oder für die Website-Authentifizierung nach Artikel 3 Absatz 39 der genannten Verordnung.

(2) Für die Zwecke der vorliegenden Verordnung ist die Registriernummer gemäß der amtlichen Eintragung nach Anhang III Buchstabe c oder nach Anhang IV Buchstabe c der Verordnung (EU) Nr. 910/2014 die Zulassungsnummer des Zahlungsdienstleisters, der kartengebundene Zahlungsinstrumente ausstellt, des Kontoinformationsdienstleisters oder des Zahlungsauslösedienstleisters, einschließlich der kontoführenden Zahlungsdienstleister, die die betreffenden Dienste erbringen, die nach Artikel 14 der Richtlinie (EU) 2015/2366 im öffentlichen Register des Herkunftsmitgliedsstaats eingetragen ist oder die aus der in Artikel 20 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates ([4]) vorgesehenen Anzeige einer jeden nach Artikel 8 dieser Richtlinie erteilten Zulassung hervorgeht.

(3) Für die Zwecke der vorliegenden Verordnung enthalten die in Absatz 1 genannten qualifizierten Zertifikate für elektronische Siegel oder für die Website-Authentifizierung zusätzliche spezifische Attribute bezüglich einer jeden der folgenden Angaben in einer im Finanzsektor gebräuchlichen Sprache:

a) die Rolle des Zahlungsdienstleisters, die eine oder mehrere der folgenden Funktionen umfassen kann:

   i) Kontoführung;

   ii) Zahlungsauslösung;

   iii) Kontoinformation;

   iv) Ausstellung kartenbasierter Zahlungsinstrumente;

b) den Namen der zuständigen Behörden, bei denen der Zahlungsdienstleister eingetragen ist.

(4) Die Interoperabilität und die Anerkennung von qualifizierten Zertifikaten für elektronische Siegel oder für die Website-Authentifizierung bleiben von den in Absatz 3 aufgeführten Attributen unberührt.

Artikel 35

Sicherheit von Kommunikationssitzungen

(1) Kontoführende Zahlungsdienstleister, Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, Kontoinformationsdienstleister und Zahlungsauslösedienstleister gewährleisten, dass beim Datenaustausch über das Internet während der jeweiligen Kommunikationssitzung eine sichere Verschlüsselung unter Einsatz weithin anerkannter Verschlüsselungstechnologien zwischen den kommunizierenden Parteien angewendet wird, damit der Schutz der Vertraulichkeit und

der Integrität der Daten gewährleistet ist.

(2) Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, Kontoinformationsdienstleister und Zahlungsauslösedienstleister halten die von den kontoführenden Zahlungsdienstleistern angebotenen Zugangssitzungen so kurz wie möglich und beenden eine solche Sitzung aktiv schnellstmöglich nach Abschluss der angeforderten Handlung.

(3) Bestehen parallele Netzwerksitzungen mit dem kontoführenden Zahlungsdienstleister, stellen Kontoinformationsdienstleister und Zahlungsauslösedienstleister sicher, dass diese Sitzungen auf sichere Weise mit den zu dem oder den Zahlungsdienstnutzer(n) jeweils aufgebauten Sitzungen verknüpft sind, damit verhindert wird, dass die zwischen ihnen ausgetauschten Nachrichten oder Informationen fehlgeleitet werden können.

(4) Kontoinformationsdienstleister, Zahlungsauslösedienstleister und Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, liefern bei der Kommunikation mit dem kontoführenden Zahlungsdienstleister unmissverständliche Verweise auf jedes der folgenden Elemente:

a) den oder die Zahlungsdienstnutzer und die entsprechende Kommunikationssitzung, damit mehrere Anforderungen von demselben oder denselben Zahlungsdienstnutzer(n) unterschieden werden können;

b) für Zahlungsauslösedienste den eindeutig identifizierten ausgelösten Zahlungsvorgang;

c) zur Bestätigung der Verfügbarkeit eines Geldbetrags die eindeutig identifizierte Anforderung bezüglich des für die Ausführung des kartenbasierten Zahlungsvorgangs erforderlichen Betrags.

(5) Kontoführende Zahlungsdienstleister, Kontoinformationsdienstleister, Zahlungsauslösedienstleister und Zahlungsdienstleister, die kartengebundene Zahlungsinstrumente ausstellen, gewährleisten, dass personalisierte Sicherheitsmerkmale und Authentifizierungscodes bei ihrer Übertragung zu keiner Zeit direkt oder indirekt von Mitarbeitern gelesen werden können.

Falls die Vertraulichkeit der in ihren Verantwortungsbereich fallenden personalisierten Sicherheitsmerkmale nicht mehr gegeben ist, unterrichten die betreffenden Dienstleister den betroffenen Zahlungsdienstnutzer sowie den Aussteller der personalisierten Sicherheitsmerkmale unverzüglich.

Artikel 36

Datenaustausch

(1) Die kontoführenden Zahlungsdienstleister halten jede der folgenden Anforderungen ein:

a) Sie stellen den Kontoinformationsdienstleistern dieselben Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen bereit, die auch dem Zahlungsdienstnutzer bereitgestellt werden,

wenn er den Zugang zu Kontoinformationen direkt anfordert, sofern diese Informationen keine sensiblen Zahlungsdaten enthalten.

b) Sie stellen den Zahlungsauslösedienstleistern sofort nach Eingang des Zahlungsauftrags dieselben Informationen über die Auslösung und die Ausführung des Zahlungsvorgangs bereit, die auch dem Zahlungsdienstnutzer bereitgestellt oder zugänglich gemacht werden, wenn dieser den Zahlungsvorgang direkt auslöst.

c) Sie übermitteln den Zahlungsdienstleistern auf Verlangen eine sofortige Bestätigung in Form eines einfachen „Ja“ oder „Nein“, ob der für die Ausführung eines Zahlungsvorgangs erforderliche Betrag auf dem Zahlungskonto des Zahlers verfügbar ist.

(2) Tritt während der Identifizierung, der Authentifizierung oder des Austauschs von Datenelementen ein unvorhergesehenes Ereignis oder ein unvorhergesehener Fehler auf, sendet der kontoführende Zahlungsdienstleister dem Zahlungsauslösedienstleister oder dem Kontoinformationsdienstleister und dem Zahlungsdienstleister, der kartengebundene Zahlungsinstrumente ausstellt, eine Benachrichtigung, in der der Grund für das unvorhergesehene Ereignis oder den unvorhergesehenen Fehler erläutert wird.

Wenn der kontoführende Zahlungsdienstleister eine dedizierte Schnittstelle nach Artikel 32 bereitstellt, muss die Schnittstelle so gestaltet sein, dass jeder Zahlungsdienstleister, der ein unvorhergesehenes Ereignis oder einen unvorhergesehenen Fehler erkennt, entsprechende Benachrichtigungen an die anderen an der Kommunikationssitzung beteiligten Zahlungsdienstleister senden kann.

(3) Kontoführende Zahlungsdienstleister verfügen über geeignete und wirksame Mechanismen, damit der Zugriff auf andere Informationen als die von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen gemäß der ausdrücklichen Zustimmung des Nutzers verhindert wird.

(4) Zahlungsauslösedienstleister stellen den kontoführenden Zahlungsdienstleistern dieselben Informationen bereit, die vom Zahlungsdienstnutzer beim direkten Auslösen des Zahlungsvorgangs angefordert werden.

(5) Kontoinformationsdienstleister müssen auf Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen, die von kontoführenden Zahlungsdienstleistern zur Bereitstellung des Kontoinformationsdienstes gehalten werden, jeweils unter folgenden Umständen zugreifen können:

a) wann immer der Zahlungsdienstnutzer diese Informationen aktiv anfordert;

b) sofern der Zahlungsdienstnutzer diese Informationen nicht aktiv anfordert, maximal viermal innerhalb von 24 Stunden, wenn keine höhere Häufigkeit zwischen dem Kontoinformationsdienstleister und dem kontoführenden Zahlungsdienstleister vereinbart wird, mit Zustimmung des Zahlungsdienstnutzers.

KAPITEL VI

SCHLUSSBESTIMMUNGEN

Artikel 37

Überprüfung

Unbeschadet des Artikels 98 Absatz 5 der Richtlinie (EU) 2015/2366 überprüft die EBA am 14. März 2021 die im Anhang der vorliegenden Verordnung angegebenen Betrugsraten sowie die nach Artikel 33 Absatz 6 in Bezug auf dedizierte Schnittstellen erteilten Ausnahmen und übermittelt der Kommission gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 gegebenenfalls Entwürfe der Aktualisierung dieser technischen Regulierungsstandards.

Artikel 38

Inkrafttreten

(1) Diese Verordnung tritt am Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Diese Verordnung gilt ab dem 14. September 2019.

(3) Die Absätze 3 und 5 des Artikels 30 gelten jedoch ab dem 14. März 2019.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 27. November 2017

Für die Kommission
Der Präsident
Jean-Claude
JUNCKER

([1]) ABl. L 337 vom 23.12.2015, S. 35.

([2]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

([3]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 53).

([4]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

ANHANG

	Referenzbetrugsrate (%) für:

Ausnahmeschwellenwert	**Kartengebundene elektronische Fernzahlungsvorgänge**	**Elektronische Überweisungen über einen Fernzugang**
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015

Top