GEDELEGEERDE VERORDENING (EU) 2018/389 VAN DE COMMISSIE

van 27 november 2017

tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt en tot wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG, 2013/36/EU en Verordening (EU) nr. 1093/2010 en tot intrekking van Richtlijn 2007/64/EG [1], en met name artikel 98, lid 4, tweede alinea,

Overwegende hetgeen volgt:

(1) Elektronische betaaldiensten dienen op een beveiligde wijze te worden uitgevoerd, met gebruikmaking van technologieën die de veilige authenticatie van de gebruiker kunnen garanderen en het risico op fraude zo veel mogelijk kunnen beperken. De authenticatieprocedure dient in de regel transactiemonitoringmechanismen te bevatten, met het oog op het opsporen van pogingen om gebruik te maken van persoonlijke beveiligingsgegevens (credentials) van een betaaldienstgebruiker die verloren, gestolen of ontvreemd zijn, en dient ook te garanderen dat de betaaldienstgebruiker de rechtmatige gebruiker is en dus instemt met de overdracht van middelen en de toegang tot zijn rekeninginformatie via een normaal gebruik van persoonlijke beveiligingsgegevens. Voorts dient nadere invulling te worden gegeven aan de vereisten van de sterke cliëntauthenticatie die dienen te worden toegepast telkens als een betaler zich online toegang verschaft tot zijn betaalrekening, een elektronische betalingstransactie initieert of via een communicatiemiddel op afstand een handeling uitvoert die een risico op betalingsfraude of andere vormen van misbruik kan meebrengen, door te eisen dat een authenticatiecode wordt gegenereerd die bestand is tegen het risico dat deze wordt vervalst, hetzij volledig, hetzij door onthulling van elementen op basis waarvan de code is gegenereerd.

(2) Aangezien fraudemethoden voortdurend veranderen, dienen de eisen inzake strenge cliëntauthenticatie ruimte te laten voor innovatie bij de technische oplossingen die een antwoord moeten bieden voor de opkomst van nieuwe bedreigingen voor de veiligheid van elektronische betalingen. Teneinde te garanderen dat de vastgestelde eisen daadwerkelijk doorlopend worden toegepast, dient ook te worden verplicht dat de beveiligingsmaatregelen voor de toepassing van strenge cliëntauthenticatie en vrijstellingen daarvan, de maatregelen om vertrouwelijkheid en integriteit van de persoonlijke beveiligingsgegevens en de maatregelen voor het vaststellen van gemeenschappelijke en veilige open communicatiestandaarden, worden gedocumenteerd, op gezette tijden getest, geëvalueerd en gecontroleerd door auditors met deskundigheid op het gebied van IT-beveiliging en betalingen en die operationeel onafhankelijk zijn. Om bevoegde autoriteiten in staat te stellen de kwaliteit van de toetsing van deze maatregelen te monitoren, dienen die toetsingen hun, op verzoek, beschikbaar te worden gesteld.

(3) Aangezien transacties voor elektronisch betalen op afstand fraudegevoeliger zijn, dienen aanvullende voorwaarden te worden ingevoerd voor de sterke cliëntauthenticatie van dergelijke transacties, hetgeen ervoor moet zorgen dat de elementen de transactie dynamisch koppelen aan een bedrag en een door de betaler bij het initiëren van de transactie nader aangegeven betalingsbegunstigde.

(4) Dynamische koppeling wordt mogelijk dankzij het genereren van authenticatiecodes waaraan een reeks strenge beveiligingseisen wordt gesteld. Om technologisch neutraal te blijven, mag voor de implementatie van authenticatiecodes geen specifieke technologie worden voorgeschreven. Daarom dienen authenticatiecodes te zijn gebaseerd op oplossingen zoals het genereren en valideren van eenmalige wachtwoorden, digitale handtekeningen of andere validiteitsbeweringen die cryptografisch zijn onderbouwd aan de hand van sleutels of andere in de authenticatie-elementen besloten cryptografisch materiaal, zolang de beveiligingsvereisten zijn vervuld.

[1] PB L 337 van 23.12.2015, blz. 35.

(5) Specifieke eisen dienen te worden vastgesteld voor de situatie waarin het eindbedrag niet bekend is op het tijdstip dat de betaler een elektronische betalingstransactie op afstand initieert, om ervoor te zorgen dat de sterke cliëntauthenticatie specifiek is voor het maximumbedrag waarvoor de betaler zijn instemming heeft gegeven als bedoeld in Richtlijn (EU) 2015/2366.

(6) Om de toepassing van sterke cliëntauthenticatie te verzekeren, dienen ook adequate beveiligingskenmerken te worden geëist voor de elementen van sterke cliëntauthenticatie die zijn gekwalificeerd als kennis (iets dat alleen de gebruiker kent), zoals lengte of complexiteit, voor de elementen die als bezit worden gekwalificeerd (iets dat alleen de gebruiker bezit), zoals algoritmespecificaties, lengte van de sleutel en informatie-entropie, en voor de apparatuur en software die elementen lezen die worden gekwalificeerd als inherentie (iets wat de gebruiker is), zoals algoritmespecificaties, biometrische sensor- en template protection-kenmerken, met name om het risico te mitigeren dat die elementen worden onthuld aan, vrijgegeven aan en gebruikt door onbevoegde partijen. Ook dienen de vereisten te worden vastgesteld die ervoor moeten zorgen dat die elementen onderling onafhankelijk zijn, zodat het kraken van een van die elementen de betrouwbaarheid van de overige elementen niet in gevaar brengt, met name wanneer een van die elementen wordt gebruikt via een multipurpose-apparaat, met name een apparaat zoals een tablet of een mobiele telefoon dat kan worden gebruikt voor zowel het doorgeven van de instructie om de betaling uit te voeren als bij de authenticatieprocedure.

(7) De vereisten voor sterke cliëntauthenticatie gelden voor betalingen die worden geïnitieerd door de betaler, ongeacht of de betaler een natuurlijke persoon is of een rechtspersoon.

(8) Voor betalingen die via anonieme betaalinstrumenten verlopen, geldt, naar hun aard, geen verplichting van strenge cliëntauthenticatie. Wanneer het anonieme karakter van die instrumenten op contractuele gronden of op grond van wetgeving wordt opgeheven, gelden voor die betalingen de beveiligingseisen die voortvloeien uit Richtlijn (EU) 2015/2366 en uit deze technische reguleringsnorm.

(9) Overeenkomstig Richtlijn (EU) 2015/2366 zijn de vrijstellingen van het beginsel van sterke cliëntauthenticatie vastgesteld op basis van de omvang van het risico, het bedrag, de recurrentie en het voor de uitvoering van de betalingstransactie gebruikte betalingskanaal.

(10) Handelingen waarvoor toegang tot het saldo en de recente transacties van een betaalrekening nodig zijn zonder dat gevoelige betalingsgegevens worden vrijgegeven, recurrente betalingen aan dezelfde betalingsbegunstigden die vooraf zijn ingesteld of bevestigd door de betaler met gebruikmaking van sterke cliëntauthenticatie, en betalingen aan en van dezelfde natuurlijke persoon of rechtspersoon met rekeningen bij dezelfde betaaldienstverlener, houden een laag risico in, zodat betaaldienstverleners geen sterke cliëntauthenticatie hoeven toe te passen. Een en ander laat onverlet dat betaalinitiatiedienstverleners, betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven en rekeninginformatiedienstverleners, overeenkomstig de artikelen 65, 66 en 67 van Richtlijn (EU) 2015/2366, met de instemming van de gebruiker van de betaaldienst, van de rekeninghoudende betaaldienstverlener alleen de informatie dienen te vragen en te verkrijgen die noodzakelijk en van essentieel belang is om een bepaalde betaaldienst te verrichten. Deze instemming kan afzonderlijk worden gegeven voor ieder verzoek om informatie of voor iedere te initiëren betaling of, in het geval van rekeninginformatiedienstverleners, als mandaat voor welbepaalde betaalrekeningen en daarmee samenhangende betalingstransacties zoals bepaald in de contractuele overeenkomst met de betaaldienstgebruiker.

(11) Vrijstellingen voor contactloze betalingen van kleine bedragen in verkooppunten, waarbij ook rekening wordt gehouden met een maximumaantal opeenvolgende transacties of een bepaald vast maximumbedrag van opeenvolgende transacties zonder dat sterke cliëntauthenticatie wordt toegepast, helpen de ontwikkeling mogelijk te maken van gebruiksvriendelijke betaaldiensten met laag risico, zodat in dergelijke vrijstellingen dient te worden voorzien. Ook is het passend om een vrijstelling te bepalen voor het geval van elektronische betalingstransacties die worden geïnitieerd vanaf onbemande betaalautomaten waar het gebruik van sterke cliëntauthenticatie om operationele redenen niet steeds gemakkelijk is toe te passen (bijv. om wachtrijen en de kans op ongevallen bij tolpoortjes te vermijden of wegens andere veiligheids- of beveiligingsrisico's).

(12) Evenals bij de vrijstelling voor het contactloos betalen van kleine bedragen in verkooppunten dient een goed evenwicht te worden gevonden tussen het belang van versterkte beveiliging bij betalingen op afstand en de behoeften van gebruiksvriendelijkheid en toegankelijkheid van betalingen in de e-commercesector. In lijn met die beginselen dienen de drempels waaronder geen sterke cliëntauthenticatie hoeft te worden toegepast, behoedzaam te worden vastgesteld, zodat hiermee alleen onlineaankopen voor een laag bedrag worden gedekt. De drempels voor onlineaankopen dienen behoedzamer te worden vastgesteld, omdat het feit dat de persoon niet fysiek aanwezig is bij het doen van de aankoop, een iets hoger veiligheidsrisico oplevert.

(13) De vereisten voor sterke cliëntauthenticatie gelden voor betalingen die worden geïnitieerd door de betaler, ongeacht of de betaler een natuurlijke persoon is of een rechtspersoon. Talrijke zakelijke betalingen worden geïnitieerd via specifieke procedures of protocollen die de hoge niveaus van betalingsbeveiliging garanderen die Richtlijn (EU) 2015/2366 via sterke cliëntauthenticatie tracht te bereiken. Wanneer de bevoegde autoriteiten vaststellen dat met die betalingsprocedures en -protocollen die alleen beschikbaar worden gesteld aan betalers niet zijnde consumenten, de doelstellingen van Richtlijn (EU) 2015/2366 in termen van beveiliging worden verwezenlijkt, kunnen betaaldienstverleners, met betrekking tot die procedures of protocollen, vrijstelling krijgen van de voorwaarden voor sterke cliëntauthenticatie.

(14) In het geval van realtimeanalyse van transactierisico's die een betalingstransactie kenmerken als een transactie met laag risico, is het ook passend om een vrijstelling in te voeren voor de betaaldienstverlener die voornemens is geen sterke cliëntauthenticatie toe te passen door de vaststelling van effectieve en risicoafhankelijke eisen die de veiligheid van de middelen en persoonsgegevens van de betaaldienstgebruiker verzekeren. Die risicoafhankelijke vereisten dienen de scores te combineren van de risicoanalyse en zo te bevestigen dat geen abnormaal uitgave- of gedragspatroon van de betaler is geconstateerd, rekening houdende met andere risicofactoren zoals informatie over de locatie van de betaler en de betalingsbegunstigde, met financiële drempels die zijn gebaseerd op fraudepercentages die voor betalingen op afstand zijn berekend. Wanneer op basis van de realtimeanalyse van transactierisico's een betaling niet kan worden gekwalificeerd als een transactie met een laag risico, dient de betaaldienstverlener terug te keren naar sterke cliëntauthenticatie. Het maximumbedrag van dit soort risicoafhankelijke vrijstelling dient zodanig te worden vastgesteld dat dit correspondeert met een zeer laag fraudepercentage, ook vergeleken met de fraudepercentages van alle betalingstransacties van de betaaldienstverlener, met inbegrip van die welke zijn geauthenticeerd via sterke cliëntauthenticatie, binnen een bepaalde tijdspanne en op voortschrijdende basis.

(15) Met het oog op een doeltreffende handhaving dienen betaaldienstverleners die aanspraak willen maken op de vrijstellingen van sterke cliëntauthenticatie, regelmatig voor elk type betalingstransactie de waarde van frauduleuze of ongeoorloofde betalingstransacties en de waargenomen fraudepercentages voor al hun betalingstransacties, ongeacht of deze zijn geauthenticeerd met sterke cliëntauthenticatie of zijn uitgevoerd op grond van een desbetreffende vrijstelling, te monitoren en beschikbaar te stellen aan bevoegde autoriteiten en de Europese Bankautoriteit (hierna „de EBA" genoemd), op hun verzoek.

(16) Het verzamelen van dit nieuwe historische bewijsmateriaal over de fraudepercentages bij elektronische betalingstransacties zal ook bijdragen aan een effectieve herziening door de EBA van de drempels voor vrijstelling van sterke cliëntauthenticatie op basis van een realtimeanalyse van transactierisico's. De EBA dient deze technologische reguleringsnormen te evalueren en, in voorkomend geval, ontwerpactualiseringen voor te leggen aan de Commissie, door het voorleggen van nieuwe ontwerpdrempels en daarmee samenhangende fraudepercentages, met het oog op het versterken van de veiligheid van elektronische betalingen op afstand, in overeenstemming met artikel 98, lid 5, van Richtlijn (EU) 2015/2366 en artikel 10 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([1]).

(17) Betaaldienstverleners die van de vast te stellen vrijstellingen gebruikmaken, dienen de mogelijkheid te krijgen om te allen tijde ervoor te kiezen sterke cliëntauthenticatie toe te passen op de in die bepalingen bedoelde handelingen en betalingstransacties.

(18) De maatregelen die de vertrouwelijkheid en integriteit beschermen van persoonlijke beveiligingsgegevens, alsmede van authenticatieapparatuur en -software, dienen de risico's te beperken met betrekking tot fraude door ongeoorloofd of frauduleus gebruik van betaalinstrumenten en ongeoorloofde toegang tot betaalrekeningen. Met het oog daarop dienen voorwaarden te worden ingevoerd betreffende het veilig aanmaken en aanleveren van de persoonlijke beveiligingsgegevens en de koppeling daarvan aan de betaaldienstgebruiker, en dienen voorwaarden te worden bepaald voor het verlengen en deactiveren van die beveiligingsgegevens.

(19) Teneinde doeltreffende en veilige communicatie te waarborgen tussen de betrokken actoren in het kader van rekeninginformatiediensten, betaalinitiatiediensten en de bevestiging betreffende de beschikbaarheid van middelen, dienen de vereisten nader te worden bepaald voor gemeenschappelijke en veilige open communicatiestandaarden waaraan alle betrokken betaaldienstverleners dienen te voldoen. Door Richtlijn (EU) 2015/2366 wordt voorzien in de toegang en het gebruik van betaalrekeninginformatie door rekeninginformatiedienstverleners. Met deze verordening worden de regels inzake de toegang tot rekeningen niet zijnde betaalrekeningen dus niet gewijzigd.

([1]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12).

(20) Iedere rekeninghoudende betaaldienstverlener met betaalrekeningen die online toegankelijk zijn, dient ten minste één toegangsinterface aan te bieden die veilige communicatie mogelijk maakt met rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven. Met de interface dienen rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, zichzelf te kunnen identificeren bij de rekeninghoudende betaaldienstverlener. Ook dient het daarmee mogelijk te zijn dat rekeninginformatiedienstverleners en betaalinitiatiedienstverleners een beroep kunnen doen op de authenticatieprocedures die de rekeninghoudende betaaldienstverlener aan de betaaldienstgebruiker heeft aangeboden. Met het oog op technologie- en bedrijfsmodelneutraliteit dienen de rekeninghoudende betaaldienstverleners vrij te kunnen kiezen of zij een interface aanbieden die specifiek bestemd is voor de communicatie met rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, dan wel, ten behoeve van die communicatie, het gebruik van de interface toestaan voor de identificatie van en de communicatie met de betaaldienstgebruikers van de rekeninghoudende betaaldienstverlener.

(21) Teneinde rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, in staat te stellen hun technische oplossingen te ontwikkelen, dienen de technische specificaties van de interface adequaat te worden gedocumenteerd en publiek beschikbaar te worden gesteld. Bovendien dient de rekeninginformatiedienstverlener een voorziening aan te bieden waarmee betaaldienstverleners de technische oplossingen kunnen testen ten minste zes maanden vóór de datum van toepassing van deze reguleringsnormen of, indien de lancering plaatsvindt na de datum van toepassing van deze normen, vóór de datum waarop de interface op de markt wordt gebracht. Om de interoperabiliteit van verschillende technologische communicatieoplossingen te garanderen, dient de interface communicatiestandaarden te gebruiken die zijn ontwikkeld door internationale of Europese standaardisatieorganisaties.

(22) De kwaliteit van de door de rekeninginformatiedienstverleners en betaalinitiatiedienstverleners verleende diensten zal afhankelijk zijn van het correct functioneren van de interfaces die beschikbaar worden gesteld of die worden aangepast door de rekeninghoudende betaaldienstverleners. Daarom is het van belang dat, wanneer die interfaces niet voldoen aan de in deze normen vervatte bepalingen, maatregelen worden genomen om de bedrijfscontinuïteit te garanderen ten behoeve van de gebruikers van die diensten. Het is de taak van nationale bevoegde autoriteiten ervoor te zorgen dat rekeninginformatiedienstverleners en betaalinitiatiedienstverleners niet geblokkeerd of gehinderd worden bij het verlenen van hun diensten.

(23) Wanneer door middel van een speciale interface tot betaalrekeningen toegang wordt geboden, dienen, om het recht van betaaldienstgebruikers te garanderen om gebruik te maken van betaalinitiatiedienstverleners en van diensten waarmee toegang kan worden verkregen tot rekeninginformatie, zoals bepaald in Richtlijn (EU) 2015/2366, die speciale interfaces dezelfde mate van beschikbaarheid en hetzelfde prestatieniveau te hebben als de interface die voor de betaaldienstgebruiker beschikbaar is. Rekeninghoudende betaaldienstverleners dienen ook transparante kritische prestatie-indicatoren (KPI's) en serviceniveaudoelstellingen vast te leggen voor de beschikbaarheid en de prestaties van speciale interfaces die ten minste even streng zijn als die welke gelden voor de interface die voor hun betaaldienstgebruikers wordt gebruikt. Die interfaces dienen te worden getest door de betaaldienstverleners die deze zullen gaan gebruiken, en bevoegde autoriteiten dienen op die interfaces stresstests uit te voeren en deze te monitoren.

(24) Om te garanderen dat betaaldienstverleners die van de speciale interface gebruikmaken, hun diensten kunnen blijven verlenen bij problemen inzake beschikbaarheid of bij ontoereikende prestaties, dient, onder strikte voorwaarden, te worden voorzien in een terugvalmechanisme waardoor die dienstverleners kunnen gebruikmaken van de interface die de rekeninghoudende betaaldienstverlener onderhoudt voor de identificatie van en de communicatie met zijn eigen betaaldienstgebruikers. Bepaalde rekeninghoudende betaaldienstverleners zullen worden vrijgesteld van de verplichting om dit soort terugvalmechanisme aan te bieden via hun customer facing interfaces wanneer hun bevoegde autoriteiten vaststellen dat de speciale interfaces voldoen aan specifieke voorwaarden die onbelemmerde concurrentie garanderen. Ingeval de vrijgestelde speciale interfaces niet aan de vereiste voorwaarden voldoen, dient de toegekende vrijstelling te worden ingetrokken door de betrokken bevoegde autoriteiten.

(25) Om bevoegde autoriteiten in staat te stellen doeltreffend toezicht te houden op de implementatie en het beheer van de communicatie-interfaces en een en ander te monitoren, dienen rekeninghoudende betaaldienstverleners een overzicht te maken van de desbetreffende documentatie die op hun website beschikbaar is, en dienen zij, op verzoek, de bevoegde autoriteiten documentatie te verschaffen over de oplossingen bij noodsituaties. De rekeninghoudende betaaldienstverleners dienen ook de statistische gegevens over de beschikbaarheid en de prestaties van die interface publiek beschikbaar te maken.

(26) Om de vertrouwelijkheid en de integriteit van gegevens te garanderen, moet de veiligheid worden verzekerd van communicatiesessies tussen rekeninghoudende betaaldienstverleners, rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven. Het is met

name noodzakelijk dat bij het uitwisselen van gegevens tussen rekeninginformatiedienstverleners, betaalinitiatiedienstverleners, betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, en rekeninghoudende betaaldienstverleners veilige versleuteling wordt toegepast.

(27) Om het vertrouwen van gebruikers te versterken en om sterke cliëntauthenticatie te verzekeren, dient het gebruik van elektronische identificatiemiddelen en vertrouwensdiensten als uiteengezet in Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad ([1]), in aanmerking te worden genomen, met name wat betreft aangemelde stelsels voor elektronische identificatie.

(28) Om te zorgen voor onderling afgestemde toepassingsdata, dient deze verordening van toepassing te zijn vanaf dezelfde datum als die waarop de lidstaten moeten zorgen voor de toepassing van de in de artikelen 65, 66, 67 en 97 van Richtlijn (EU) 2015/2366 bedoelde beveiligingsmaatregelen.

(29) Deze verordening is gebaseerd op de ontwerpen van technische reguleringsnormen die de Europese Bankautoriteit (EBA) aan de Commissie heeft voorgelegd.

(30) De EBA heeft open en transparante publieksraadplegingen gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, heeft de mogelijke kosten en baten geanalyseerd en heeft het advies van de in overeenstemming met artikel 37 van Verordening (EU) nr. 1093/2010 opgerichte Stakeholdergroep Bankwezen ingewonnen,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

Door deze verordening worden de vereisten vastgesteld die betaaldienstverleners in acht moeten nemen ten behoeve van de uitvoering van beveiligingsmaatregelen die hen in staat stellen het volgende te doen:

a) toepassen van de procedure voor sterke cliëntauthenticatie in overeenstemming met artikel 97 van Richtlijn (EU) 2015/2366;

b) vrijstellen van de toepassing van de beveiligingsvereisten voor sterke cliëntauthenticatie, afhankelijk van nader omschreven en beperkte voorwaarden op basis van de omvang van het risico, het bedrag en de recurrentie van de betalingstransactie en het voor de uitvoering van de betalingstransactie gebruikte betalingskanaal;

c) beschermen van de vertrouwelijkheid en de integriteit van de persoonlijke beveiligingsgegevens (credentials) van de betaaldienstgebruiker;

d) vaststellen van gemeenschappelijke en veilige open standaarden voor de communicatie tussen rekeninghoudende betaaldienstverleners, betaalinitiatiedienstverleners, rekeninginformatiedienstverleners, betalers, betalingsbegunstigden en andere betaaldienstverleners met betrekking tot het verlenen en het gebruik van betaaldiensten uit hoofde van titel IV van Richtlijn (EU) 2015/2366.

Artikel 2

Algemene authenticatievereisten

1. Betaaldienstverleners beschikken over mechanismen voor het monitoren van transacties waarmee zij ongeoorloofde of frauduleuze betalingstransacties voor de toepassing van de onder a) en b) van artikel 1 genoemde veiligheidsmaatregelen kunnen implementeren.

([1]) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 53).

Die mechanismen zijn gebaseerd op de analyse van betalingstransacties, waarbij rekening wordt gehouden met elementen die typisch zijn voor de betaaldienstgebruiker in omstandigheden van normaal gebruik van de persoonlijke beveiligingsgegevens.

2. Betaaldienstverleners zorgen ervoor dat de mechanismen voor het monitoren van transacties ten minste met elk van de volgende risicofactoren rekening houden:

a) lijsten van gecompromitteerde of gestolen authenticatie-elementen;

b) het bedrag van elke betalingstransactie;

c) bekende fraudescenario's bij het verlenen van betaaldiensten;

d) tekenen van malwarebesmetting tijdens sessies van de authenticatieprocedure;

e) ingeval de toegangsapparatuur of -software door de betaaldienstverlener wordt verstrekt, een gebruikslog van de aan de betalingsgebruiker verstrekte toegangsapparatuur of -software en het abnormale gebruik van de toegangsapparatuur of -software.

Artikel 3

Evaluatie van de beveiligingsmaatregelen

1. De implementatie van de in artikel 1 bedoelde beveiligingsmaatregelen wordt in overeenstemming met het toepasselijke juridische kader van de betaaldienstverlener gedocumenteerd, op gezette tijden getest, geëvalueerd en gecontroleerd door auditors met deskundigheid op het gebied van IT-beveiliging en betalingen, en die operationeel onafhankelijk zijn binnen of ten opzichte van de betaaldienstverlener.

2. De tijdsspanne tussen de in lid 1 bedoelde audits wordt vastgesteld rekening houdende met het desbetreffende boekhoudkundige en wettelijke auditkader dat op de betaaldienstverlener van toepassing is.

Betaaldienstverleners kunnen evenwel gebruikmaken van de in artikel 18 bedoelde afwijking op voorwaarde dat ten minste eenmaal per jaar een audit van de methodologie, het model en de gemelde fraudepercentages plaatsvindt. De auditor die deze audit uitvoert, beschikt over deskundigheid op het gebied van IT-beveiliging en betalingen, en is operationeel onafhankelijk binnen of ten opzichte van de betaaldienstverlener. In het eerste jaar dat van de afwijking op grond van artikel 18 wordt gebruikgemaakt en vervolgens ten minste om de drie jaar, of vaker op verzoek van de bevoegde autoriteit, wordt deze audit uitgevoerd door een onafhankelijke en gekwalificeerde externe auditor.

3. Deze audit maakt een evaluatie van en doet verslag over de inachtneming van de in deze verordening vastgestelde vereisten door de beveiligingsmaatregelen van de betaaldienstverlener.

Het volledige verslag wordt aan bevoegde autoriteiten op hun verzoek ter beschikking gesteld.

HOOFDSTUK II

BEVEILIGINGSMAATREGELEN VOOR DE TOEPASSING VAN STERKE CLIËNTAUTHENTICATIE

Artikel 4

Authenticatiecode

1. Wanneer betaaldienstverleners in overeenstemming met artikel 97, lid 1, van Richtlijn (EU) 2015/2366 sterke cliëntauthenticatie toepassen, is deze authenticatie gebaseerd op twee of meer elementen die als kennis, bezit en inherentie worden gekwalificeerd en die resulteren in het genereren van een authenticatiecode.

De authenticatie wordt pas door de betaaldienstverlener geaccepteerd wanneer de betaler de authenticatiecode gebruikt om online toegang te krijgen tot zijn betaalrekening, om een elektronische betalingstransactie te initiëren of om via een communicatiemiddel op afstand een handeling uit te voeren die een risico op betalingsfraude of andere vormen van misbruik kan meebrengen.

2. Voor de toepassing van lid 1 nemen betaaldienstverleners beveiligingsmaatregelen waarmee aan elk van de volgende voorwaarden kan worden voldaan:

a) informatie over een van de in lid 1 bedoelde elementen kan niet worden afgeleid uit de openbaarmaking van de authenticatiecode;

b) het is niet mogelijk een nieuwe authenticatiecode te genereren op basis van de kennis van andere, voordien gegenereerde authenticatiecodes;

c) de authenticatiecode kan niet worden vervalst.

3. Betaaldienstverleners zorgen ervoor dat de authenticatie door middel van het genereren van een authenticatiecode elk van de volgende elementen omvat:

a) wanneer de authenticatie voor toegang op afstand, elektronische betalingen op afstand of andere handelingen via een communicatiemiddel op afstand die een risico op betalingsfraude of andere vormen van misbruik kunnen meebrengen, geen authenticatiecode voor de toepassing van lid 1 heeft gegenereerd, is het niet mogelijk om te identificeren welke van de in dat lid bedoelde elementen niet correct was;

b) het aantal mislukte authenticatiepogingen dat opeenvolgend kan plaatsvinden voordat de in artikel 97, lid 1, van Richtlijn (EU) 2015/2366 genoemde handelingen tijdelijk of permanent worden geblokkeerd, bedraagt binnen een bepaalde tijdsspanne maximaal vijf;

c) de communicatiesessies zijn overeenkomstig de vereisten van hoofdstuk V beschermd tegen onderschepping van authenticatiegegevens die tijdens de authenticatie worden doorgegeven, en tegen manipulatie door onbevoegde partijen;

d) de maximumtijd zonder activiteit van de betaler nadat deze zich heeft geauthenticeerd om online toegang te krijgen tot zijn betaalrekening, bedraagt niet meer dan vijf minuten.

4. Wanneer de in lid 3, onder b), bedoelde blokkering tijdelijk is, wordt de duur van die blokkering en het aantal nieuwe pogingen bepaald op basis van de kenmerken van de aan de betaler geleverde dienst en alle daaraan verbonden betrokken risico's, rekening houdende met ten minste de in artikel 2, lid 2, bedoelde factoren.

De betaler wordt gewaarschuwd voordat de blokkering permanent wordt.

Wanneer de blokkering permanent is geworden, wordt een veilige procedure ingesteld waardoor de betaler opnieuw kan gebruikmaken van de geblokkeerde elektronische betaalinstrumenten.

Artikel 5

Dynamische koppeling

1. Wanneer betaaldienstverleners sterke cliëntauthenticatie toepassen in overeenstemming met artikel 97, lid 2, van Richtlijn (EU) 2015/2366, stellen zij, afgezien van de vereisten van artikel 4 van deze verordening, ook beveiligingsmaatregelen vast die aan elk van de volgende voorwaarden voldoen:

a) de betaler wordt in kennis gesteld van het bedrag van de betalingstransactie en van de betalingsbegunstigde;

b) de gegenereerde authenticatiecode is specifiek voor het bedrag van de betalingstransactie en de betalingsbegunstigde waarmee de betaler bij het initiëren van de transactie akkoord is gegaan;

c) de door de betaaldienstverlener geaccepteerde authenticatiecode stemt overeen met het oorspronkelijke specifieke bedrag van de betalingstransactie en de identiteit van de betalingsbegunstigde waarmee de betaler akkoord is gegaan;

d) wijzigingen van het bedrag of de betalingsbegunstigde maken de gegenereerde authenticatiecode ongeldig.

2. Voor de toepassing van lid 1 nemen betaaldienstverleners beveiligingsmaatregelen die de vertrouwelijkheid, authenticiteit en integriteit van elk van de volgende elementen garanderen:

a) het transactiebedrag en de betalingsbegunstigde tijdens alle fasen van de authenticatie;

b) de informatie die de betaler te zien krijgt tijdens alle fasen van de authenticatie, daaronder begrepen het genereren, doorzenden en gebruiken van de authenticatiecode.

3. Voor de toepassing van lid 1, onder b), en wanneer betaaldienstverleners in overeenstemming met artikel 97, lid 2, van Richtlijn (EU) 2015/2366 sterke cliëntauthenticatie toepassen, gelden voor de authenticatiecode de volgende vereisten:

a) wat betreft een op kaarten gebaseerde betalingstransactie waarvoor de betaler heeft ingestemd met het exacte bedrag dat mag worden geblokkeerd overeenkomstig artikel 75, lid 1, van die richtlijn, is de authenticatiecode specifiek voor het bedrag dat met instemming van de betaler is geblokkeerd en waarmee deze akkoord is gegaan bij het initiëren van de transactie;

b) wat betreft betalingstransacties waarvoor de betaler heeft ingestemd met de uitvoering van een batch van elektronische betalingstransacties op afstand aan een of meerdere betalingsbegunstigden, is de authenticatiecode specifiek voor het volledige bedrag van de batch betalingstransacties en de vermelde betalingsbegunstigden.

Artikel 6

Vereisten voor de als kennis gekwalificeerde elementen

1. Betaaldienstverleners nemen maatregelen om het risico te mitigeren dat de als kennis gekwalificeerde elementen van sterke cliëntauthenticatie worden ontdekt door of onthuld aan onbevoegde partijen.

2. Het gebruik van die elementen door de betaler is onderworpen aan risicobeperkende maatregelen die de onthulling ervan aan onbevoegde partijen moeten voorkomen.

Artikel 7

Vereisten voor de als bezit gekwalificeerde elementen

1. Betaaldienstverleners nemen maatregelen om het risico te mitigeren dat de als bezit gekwalificeerde elementen van sterke cliëntauthenticatie worden gebruikt door onbevoegde partijen.

2. Het gebruik van die elementen door de betaler is onderworpen aan maatregelen die replicatie van die elementen moeten voorkomen.

Artikel 8

Vereisten voor aan als inherentie gekwalificeerde elementen gekoppelde apparatuur en software

1. Betaaldienstverleners nemen maatregelen om het risico te mitigeren dat de elementen van sterke cliëntauthenticatie die als inherentie worden gekwalificeerd en worden gelezen door aan de betaler verstrekte toegangsapparatuur en -software, worden ontdekt door onbevoegde partijen. De betaaldienstverleners zorgen er ten minste voor dat bij die toegangsapparatuur en -software de kans zeer klein is dat een onbevoegde partij als de betaler wordt geauthenticeerd.

2. Het gebruik van die elementen door de betaler is onderworpen aan maatregelen die ervoor moeten zorgen dat gegarandeerd is dat die apparatuur en de software bestand zijn tegen ongeoorloofd gebruik van de elementen door toegang tot de apparatuur en de software.

Artikel 9

Onafhankelijkheid van de elementen

1. Betaaldienstverleners zorgen ervoor dat het gebruik van de in de artikelen 6, 7 en 8 bedoelde elementen van sterke cliëntauthenticatie onderworpen is aan maatregelen die ervoor zorgen dat, in termen van technologie, algoritmen en parameters, het kraken van een van die elementen de betrouwbaarheid van de overige elementen niet in gevaar brengt.

2. Betaaldienstverleners nemen beveiligingsmaatregelen wanneer een of meer van de elementen van sterke cliëntauthenticatie of de authenticatiecode zelf worden gebruikt op een multipurposeapparaat, om het risico te mitigeren dat zou voortvloeien uit het feit dat het multipurposeapparaat is gecompromitteerd.

3. Voor de toepassing van lid 2 omvatten de risicobeperkende maatregelen elk van de volgende elementen:

a) het gebruik van gescheiden, beveiligde uitvoeringsomgevingen via de software die op het multipurposeapparaat is geïnstalleerd;

b) mechanismen om ervoor te zorgen dat de software of het apparaat niet wordt gewijzigd door de betaler of door een derde partij;

c) wanneer wijzigingen hebben plaatsgevonden, mechanismen om de gevolgen daarvan te dempen.

HOOFDSTUK III

VRIJSTELLINGEN VAN STERKE CLIËNTAUTHENTICATIE

Artikel 10

Betaalrekeninginformatie

1. Het is betaaldienstverleners toegestaan om sterke cliëntauthenticatie niet toe passen, mits de voorwaarden van artikel 2 en lid 2 van dit artikel in acht worden genomen en wanneer een betaaldienstgebruiker beperkt wordt in zijn onlinetoegang tot een of beide van de volgende elementen zonder dat gevoelige betalingsgegevens worden vrijgegeven:

a) het saldo van een of meer aangewezen betaalrekeningen;

b) de betalingstransacties die de laatste negentig dagen zijn uitgevoerd via een of meer aangewezen betaalrekeningen.

2. Voor de toepassing van lid 1 zijn betaaldienstverleners niet vrijgesteld van het toepassen van sterke cliëntauthenticatie wanneer een van de beide volgende voorwaarden is vervuld:

a) de betaaldienstgebruiker krijgt voor het eerst online toegang tot de in lid 1 genoemde informatie;

b) meer dan negentig dagen zijn verstreken sinds de betaaldienstgebruiker toegang heeft gehad tot de in lid 1, onder b), genoemde informatie en sterke cliëntauthenticatie is toegepast.

Artikel 11

Contactloze betalingen in verkooppunten

Het is betaaldienstverleners toegestaan om, mits de voorwaarden van artikel 2 in acht worden genomen, sterke cliëntauthenticatie niet toe passen wanneer de betaler een contactloze elektronische betalingstransactie initieert indien de volgende voorwaarden zijn vervuld:

a) het individuele bedrag van de contactloze elektronische betalingstransactie bedraagt niet meer dan 50 EUR, en

b) het totale bedrag van voorafgaande contactloze elektronische betalingstransacties die zijn geïnitieerd door middel van een betaalinstrument met een contactloze functionaliteit, beloopt sinds de datum van de laatste toepassing van sterke cliëntauthenticatie niet meer dan 150 EUR, of

c) het aantal opeenvolgende contactloze elektronische betalingstransacties die zijn geïnitieerd via het betaalinstrument dat een contactloze functionaliteit biedt, bedraagt sinds de datum van de laatste toepassing van sterke cliëntauthenticatie niet meer dan vijf.

Artikel 12

Onbemande betaalautomaten voor vervoerbewijzen en parkeergelden

Het is betaaldienstverleners toegestaan om, mits de voorwaarden van artikel 2 in acht worden genomen, sterke cliëntauthenticatie niet toe passen wanneer de betaler een elektronische betalingstransactie initieert op een onbemande betaalautomaat met het oog op de betaling van vervoerbewijzen of parkeergelden.

Artikel 13

Betrouwbare betalingsbegunstigden

1. Betaaldienstverleners passen sterke cliëntauthenticatie toe wanneer een betaler een lijst van betrouwbare betalingsbegunstigden aanmaakt of aanpast via de rekeninghoudende betaaldienstverlener van de betaler.

2. Het is betaaldienstverleners toegestaan om, mits de algemene authenticatievereisten in acht worden genomen, sterke cliëntauthenticatie niet toe te passen wanneer de betaler een betalingstransactie initieert en de betalingsbegunstigde is opgenomen in een voordien door de betaler aangemaakte lijst van betrouwbare betalingsbegunstigden.

Artikel 14

Recurrente transacties

1. Betaaldienstverleners passen sterke cliëntauthenticatie toe wanneer een betaler een reeks recurrente transacties met hetzelfde bedrag en dezelfde betalingsbegunstigde aanmaakt, aanpast of voor het eerst initieert.

2. Het is betaaldienstverleners toegestaan om, mits de algemene authenticatievereisten in acht worden genomen, sterke cliëntauthenticatie niet toe te passen voor het initiëren van alle volgende betalingstransacties uit de in lid 1 bedoelde reeks transacties.

Artikel 15

Overmakingen tussen door dezelfde natuurlijke persoon of rechtspersoon aangehouden rekeningen

Het is betaaldienstverleners toegestaan om, mits de voorwaarden van artikel 2 in acht worden genomen, sterke cliëntauthenticatie niet toe passen wanneer de betaler een overmaking initieert wanneer de betaler en de betalingsbegunstigde dezelfde natuurlijke persoon of rechtspersoon zijn en beide betaalrekeningen worden aangehouden bij dezelfde rekeninghoudende betaaldienstverlener.

Artikel 16

Transacties voor kleine bedragen

Het is betaaldienstverleners toegestaan om sterke cliëntauthenticatie niet toe passen wanneer de betaler een elektronische betalingstransactie op afstand initieert, mits de volgende voorwaarden zijn vervuld:

a) het bedrag van de elektronische betalingstransactie op afstand bedraagt niet meer dan 30 EUR, en

b) het totale bedrag van voorafgaande elektronische betalingstransacties op afstand die zijn geïnitieerd sinds de laatste toepassing van sterke cliëntauthenticatie, beloopt niet meer dan 100 EUR, of

c) het aantal voorafgaande elektronische betalingstransacties op afstand die zijn geïnitieerd sinds de laatste toepassing van sterke cliëntauthenticatie, beloopt niet meer dan vijf opeenvolgende individuele elektronische betalingstransacties op afstand.

Artikel 17

Veilige zakelijke betalingsprocedures en -protocollen

Het is betaaldienstverleners toegestaan om sterke cliëntauthenticatie niet toe te passen ten aanzien van rechtspersonen die elektronische betalingstransacties initiëren via het gebruik van speciale betalingsprocedures of -protocollen die alleen beschikbaar worden gesteld aan betalers niet zijnde consumenten wanneer de bevoegde autoriteiten zich ervan hebben vergewist dat die processen of protocollen beveiligingsniveaus garanderen die ten minste gelijkwaardig zijn aan die waarin door Richtlijn (EU) 2015/2366 wordt voorzien.

Artikel 18

Analyse van transactierisico's

1. Het is betaaldienstverleners toegestaan om sterke cliëntauthenticatie niet toe te passen wanneer de betaler een elektronische betalingstransactie op afstand initieert die door de betaaldienstverleners volgens de in artikel 2 en in lid 2, onder c), van dit artikel bedoelde mechanismen voor transactiemonitoring is geïdentificeerd als een transactie die weinig risico oplevert.

2. Een in lid 1 bedoelde elektronische betalingstransactie wordt beschouwd als een transactie die weinig risico oplevert, wanneer elk van de volgende voorwaarden is vervuld:

a) het fraudepercentage voor dat type transactie, zoals gemeld door de betaaldienstverlener en berekend in overeenstemming met artikel 19, is gelijkwaardig aan of ligt lager dan de referentiefraudepercentages die in de tabel in de bijlage worden genoemd voor, onderscheidenlijk, „elektronische op kaarten gebaseerde betalingen op afstand" en „elektronische overmakingen op afstand";

b) het transactiebedrag ligt niet hoger dan de betrokken drempelwaarde voor vrijstelling die in de tabel in de bijlage wordt genoemd;

c) betaaldienstverleners hebben als gevolg van het uitvoeren van een realtimerisicoanalyse niet een van de volgende elementen geïdentificeerd:

   i) een abnormaal uitgave- of gedragspatroon van de betaler;

   ii) ongewone informatie over de toegangsapparatuur of -software van de betaler;

   iii) een malwarebesmetting tijdens sessies van de authenticatieprocedure;

   iv) bekende fraudescenario's bij het verlenen van betaaldiensten;

   v) een ongebruikelijke locatie van de betaler;

   vi) een hoogrisicolocatie van de betalingsbegunstigde.

3. Betaaldienstverleners die voornemens zijn elektronische betalingstransacties op afstand vrij te stellen van sterke cliëntauthenticatie op grond van het feit dat deze een laag risico inhouden, nemen ten minste de volgende risicofactoren in aanmerking:

a) de vroegere uitgavepatronen van de individuele betaaldienstgebruiker;

b) de betalingstransactiegeschiedenis van elk van de betaaldienstgebruikers van de betaaldienstverlener;

c) de locatie van de betaler en de betalingsbegunstigde op het tijdstip van de betalingstransactie in gevallen dat de toegangsapparatuur of -software door de betaaldienstverleners wordt verstrekt;

d) de identificatie van ongebruikelijke betalingspatronen van de betaaldienstgebruiker ten opzichte van de betalingstransactiegeschiedenis van de gebruiker.

In de beoordeling die een betaaldienstverlener maakt, worden al die risicofactoren gecombineerd tot een risicoscore voor elke individuele transactie om te bepalen of een specifieke betaling kan worden toegestaan zonder sterke cliëntauthenticatie.

Artikel 19

Berekening van fraudepercentages

1. Voor elk in de tabel in de bijlage genoemd type transactie zorgt de betaaldienstverlener ervoor dat de totale fraudepercentages voor zowel via sterke cliëntauthenticatie geauthenticeerde betalingstransacties als voor transacties die worden uitgevoerd op grond van een van de in de artikelen 13 tot en met 18 bedoelde vrijstellingen, gelijkwaardig zijn aan of lager dan het referentiefraudepercentage voor hetzelfde type betalingstransactie dat in de tabel in de bijlage is vermeld.

Het totale fraudepercentage voor elk type transactie wordt berekend als de totale waarde van ongeoorloofde of frauduleuze transacties op afstand, ongeacht of de middelen zijn teruggevorderd of niet, gedeeld door de totale waarde van alle transacties op afstand voor hetzelfde type transactie, ongeacht of deze zijn geauthenticeerd met sterke cliëntauthenticatie dan wel zijn uitgevoerd op grond van een van de in de artikelen 13 tot en met 18 bedoelde vrijstellingen, op voortschrijdende kwartaalbasis (negentig dagen).

2. De berekening van de fraudepercentages en de daaruit resulterende cijfers worden beoordeeld tijdens de in artikel 3, lid 2, bedoelde audit, hetgeen ervoor zorgt dat deze volledig en nauwkeurig zijn.

3. De methodologie en eventuele modellen die de betaaldienstverlener gebruikt om de fraudepercentages te berekenen, alsmede de fraudepercentages zelf worden adequaat gedocumenteerd en worden, op hun verzoek, volledig ter beschikking gesteld aan bevoegde autoriteiten en, na voorafgaande kennisgeving aan de betrokken bevoegde autoriteit of autoriteiten, aan de EBA.

Artikel 20

Stopzetting van vrijstellingen op basis van analyse van transactierisico's

1. Betaaldienstverleners die van de in artikel 18 bedoelde vrijstelling gebruikmaken, doen onverwijld melding aan de bevoegde autoriteiten wanneer een van hun gemonitorde fraudepercentages, voor een van de types betalingstransacties uit de tabel in de bijlage, het toepasselijke referentiefraudepercentage overschrijdt en verschaffen de bevoegde autoriteiten een beschrijving van de maatregelen die zij voornemens zijn te nemen zodat hun gemonitorde fraudepercentage opnieuw aan de toepasselijke referentiefraudepercentages voldoet.

2. Betaaldienstverleners zetten onverwijld het gebruik stop van de in artikel 18 bedoelde vrijstelling voor een van de types betalingstransacties die is vermeld in de tabel in de bijlage met de specifieke vrijstellingsbandbreedte, wanneer hun gemonitorde fraudepercentage voor twee opeenvolgende kwartalen het toepasselijke referentiefraudepercentage voor dat betaalinstrument of dat type betalingstransactie overschrijdt binnen die vrijstellingsbandbreedte.

3. Na de stopzetting van de in artikel 18 bedoelde vrijstelling overeenkomstig lid 2 van dit artikel maken betaaldienstverleners pas opnieuw gebruik van die vrijstelling wanneer hun berekende fraudepercentage gelijk is aan of lager ligt dan de referentiefraudepercentages over één kwartaal voor dat type betalingstransactie binnen die vrijstellingsbandbreedte.

4. Wanneer betaaldienstverleners opnieuw willen gebruikmaken van de in artikel 18 bedoelde vrijstelling, stellen zij de bevoegde autoriteiten binnen een redelijk tijdsbestek daarvan in kennis en verschaffen zij, voordat zij opnieuw van die vrijstelling gebruikmaken, bewijsmateriaal voor het feit dat hun gemonitorde fraudepercentage, in overeenstemming met lid 3 van dit artikel, opnieuw binnen het toepasselijke fraudepercentage is gebracht voor die vrijstellingsbandbreedte.

Artikel 21

Monitoring

1. Om gebruik te kunnen maken van de in de artikelen 10 tot en met 18 bepaalde vrijstellingen, leggen betaaldienstverleners voor elk type betalingstransactie de volgende gegevens vast en monitoren ze deze, met een uitsplitsing in betalingstransacties op afstand en betalingstransacties niet op afstand, ten minste op kwartaalbasis:

a) de totale waarde van ongeoorloofde of frauduleuze betalingstransacties overeenkomstig artikel 64, lid 2, van Richtlijn (EU) 2015/2366, de totale waarde van alle betalingstransacties en het daaruit resulterende fraudepercentage, met inbegrip van een uitsplitsing van via sterke cliëntauthenticatie geïnitieerde betalingstransacties en volgens elk van de vrijstellingen;

b) de gemiddelde transactiewaarde, met inbegrip van een uitsplitsing van via sterke cliëntauthenticatie geïnitieerde betalingstransacties en volgens elk van de vrijstellingen;

c) het aantal betalingstransacties waar elk van de vrijstellingen is toegepast en hun aandeel in het totale aantal betalingstransacties.

2. Betaaldienstverleners stellen de uitkomsten van de monitoring overeenkomstig lid 1 ter beschikking van bevoegde autoriteiten en, na voorafgaande kennisgeving aan de betrokken bevoegde autoriteit of autoriteiten, van de EBA.

HOOFDSTUK IV

VERTROUWELIJKHEID EN INTEGRITEIT VAN PERSOONLIJKE BEVEILIGINGSGEGEVENS VAN BETAALDIENSTGEBRUIKERS

Artikel 22

Algemene vereisten

1. Betaaldienstverleners verzekeren de vertrouwelijkheid en integriteit van de persoonlijke beveiligingsgegevens van de betaaldienstgebruiker, daaronder begrepen authenticatiecodes, tijdens alle fasen van de authenticatie.

2. Voor de toepassing van lid 1 zorgen betaaldienstverleners ervoor dat aan elk van de volgende voorwaarden wordt voldaan:

a) persoonlijke beveiligingsgegevens worden afgeschermd wanneer ze verschijnen en zijn niet volledig leesbaar wanneer ze door de betaaldienstgebruiker tijdens de authenticatie worden ingegeven;

b) persoonlijke beveiligingsgegevens in gegevensformaat, alsmede cryptografisch materiaal met betrekking tot de versleuteling van de persoonlijke beveiligingsgegevens worden niet opgeslagen als niet-gecodeerde tekst;

c) geheim cryptografisch materiaal wordt beschermd tegen ongeoorloofde bekendmaking.

3. Betaaldienstverleners documenteren het proces met betrekking tot het beheer van cryptografisch materiaal dat wordt gebruikt voor het versleutelen of anderszins onleesbaar maken van de persoonlijke beveiligingsgegevens, volledig.

4. Betaaldienstverleners zorgen ervoor dat de verwerking en het routeren van persoonlijke beveiligingsgegevens en van de in overeenstemming met hoofdstuk II gegenereerde authenticatiecodes plaatsvinden in een beveiligde omgeving volgens sterke en algemeen erkende sectorale standaarden.

Artikel 23

Aanmaken en doorgeven van beveiligingsgegevens

Betaaldienstverleners zorgen ervoor dat het aanmaken van persoonlijke beveiligingsgegevens in een veilige omgeving plaatsvindt.

Zij beperken het risico van ongeoorloofd gebruik van de persoonlijke beveiligingsgegevens en van de authenticatieapparatuur en -software als gevolg van verlies, diefstal of kopiëren vóór de levering ervan aan de betaler.

Artikel 24

Koppeling aan de betaaldienstgebruiker

1. Betaaldienstverleners zorgen ervoor dat alleen de betaaldienstgebruiker veilig wordt gekoppeld aan de persoonlijke beveiligingsgegevens en de authenticatieapparatuur en -software.

2. Voor de toepassing van lid 1 zorgen betaaldienstverleners ervoor dat aan elk van de volgende voorwaarden wordt voldaan:

a) de koppeling van de identiteit van de betaaldienstgebruiker aan persoonlijke beveiligingsgegevens en authenticatieapparatuur en -software vindt plaats in veilige omgevingen onder de verantwoordelijkheid van de betaaldienstverlener. Die omgevingen omvatten ten minste de bedrijfsgebouwen van de betaaldienstverlener, de door de betaaldienstverlener verschafte internetomgeving of andere vergelijkbare veilige websites die door de betaaldienstverlener worden gebruikt, en zijn geldautomaatdiensten, rekening houdende met risico's die verbonden zijn aan apparaten en onderliggende onderdelen die worden gebruikt tijdens de koppelingsprocedure maar die niet onder de verantwoordelijkheid van de betaaldienstverlener vallen;

b) de koppeling via een communicatiemiddel op afstand van de identiteit van de betaaldienstgebruiker aan de persoonlijke beveiligingsgegevens en aan authenticatieapparatuur of -software vindt plaats door middel van sterke cliëntauthenticatie.

Artikel 25

Levering van beveiligingsgegevens en authenticatieapparatuur en -software

1. Betaaldienstverleners zorgen ervoor dat de levering van persoonlijke beveiligingsgegevens en authenticatieapparatuur en -software aan de betaaldienstgebruiker op een veilige manier verloopt die de risico's helpt te voorkomen die zijn verbonden aan het ongeoorloofde gebruik ervan als gevolg van verlies, diefstal of kopiëren.

2. Voor de toepassing van lid 1 passen betaaldienstverleners ten minste elk van de volgende maatregelen toe:

a) doeltreffende en veilige leveringsmechanismen die garanderen dat de persoonlijke beveiligingsgegevens en authenticatieapparatuur en -software aan de rechtmatige betaaldienstgebruiker worden geleverd;

b) mechanismen waarmee de betaaldienstverlener de authenticiteit kan nagaan van de authenticatiesoftware die aan de betaaldienstgebruiker via het internet wordt geleverd;

c) regelingen die ervoor zorgen dat, wanneer de levering van persoonlijke beveiligingsgegevens plaatsvindt buiten de bedrijfsruimten van de betaaldienstverlener of via een communicatiemiddel op afstand:

   i) geen onbevoegde partij meer dan één element van de persoonlijke beveiligingsgegevens en de authenticatieapparatuur of -software kan krijgen wanneer die via hetzelfde kanaal worden geleverd;

   ii) de geleverde persoonlijke beveiligingsgegevens en authenticatieapparatuur of -software moeten worden geactiveerd voordat ze kunnen worden gebruikt;

d) regelingen die ervoor zorgen dat, in gevallen waarin de persoonlijke beveiligingsgegevens en de authenticatieapparatuur of -software moeten worden geactiveerd vóór het eerste gebruik ervan, de authenticatie in een veilige omgeving plaatsvindt in overeenstemming met de in artikel 24 bedoelde koppelingsprocedures.

Artikel 26

Vernieuwing van persoonlijke beveiligingsgegevens

Betaaldienstverleners zorgen ervoor dat de vernieuwing of het opnieuw activeren van persoonlijke beveiligingsgegevens verloopt volgens de procedures voor het aanmaken, koppelen en leveren van de beveiligingsgegevens en de authenticatieapparatuur in overeenstemming met de artikelen 23, 24 en 25.

Artikel 27

Vernietiging, deactivering en herroeping

Betaaldienstverleners zorgen ervoor dat zij beschikken over effectieve procedures om elk van de volgende beveiligingsmaatregelen toe te passen:

a) de veilige vernietiging, deactivering of herroeping van de persoonlijke beveiligingsgegevens en authenticatieapparatuur en -software;

b) wanneer de betaaldienstverlener herbruikbare authenticatieapparatuur en -software distribueert, wordt het veilige hergebruik van een apparaat of van software vastgelegd, gedocumenteerd en geïmplementeerd voordat deze aan een andere betaaldienstgebruiker beschikbaar worden gesteld;

c) het deactiveren of herroepen van informatie met betrekking tot persoonlijke beveiligingsgegevens die zijn opgeslagen in de systemen en databases van de betaaldienstverlener, en, in voorkomend geval, in publieke registers.

HOOFDSTUK V

GEMEENSCHAPPELIJKE EN VEILIGE OPEN COMMUNICATIESTANDAARDEN

Afdeling 1

Algemene vereisten voor communicatie

Artikel 28

Identificatievereisten

1. Betaaldienstverleners zorgen voor veilige identificatie bij de communicatie tussen de apparatuur van de betaler en de apparatuur van de betalingsbegunstigde voor het accepteren van elektronische betalingen, met inbegrip van, maar niet beperkt tot betaalterminals.

2. Betaaldienstverleners zorgen ervoor dat de risico's dat communicatie wordt afgeleid naar onbevoegde partijen in mobiele applicaties en andere interfaces voor betaaldienstgebruikers die elektronische betaaldiensten verlenen, daadwerkelijk worden beperkt.

Artikel 29

Traceerbaarheid

1. Betaaldienstverleners beschikken over procedures die borgen dat alle betalingstransacties en andere interacties met de betaaldienstgebruiker, met andere betaaldienstverleners en met andere entiteiten, daaronder begrepen handelaren, in het kader van het verrichten van de betaaldienst traceerbaar zijn, zodat achteraf alle gebeurtenissen die relevant zijn voor de elektronische transactie in alle verschillende fasen, bekend zijn.

2. Voor de toepassing van lid 1 zorgen betaaldienstverleners ervoor dat communicatiesessies die tot stand komen met de betaaldienstgebruiker, andere betaaldienstverleners en andere entiteiten, daaronder begrepen handelaren, gebruikmaken van elk van de volgende elementen:

a) een unieke identificator van de sessie;

b) beveiligingsmechanismen voor een gedetailleerde logging van de transactie, met onder meer een transactienummer, tijdstempel en alle relevante transactiegegevens;

c) tijdstempels die zijn gebaseerd op een eengemaakt tijdsreferentiesysteem en die zijn gesynchroniseerd met een officieel tijdsignaal.

Afdeling 2

Specifieke vereisten voor de gemeenschappelijke en veilige open standaarden voor communicatie

Artikel 30

Algemene verplichtingen voor toegangsinterfaces

1. Rekeninghoudende betaaldienstverleners die een betaler een betaalrekening aanbieden die online toegankelijk is, beschikken over ten minste één interface die voldoet aan elk van de volgende vereisten:

a) rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, zijn in staat om zichzelf te identificeren bij de rekeninghoudende betaaldienstverlener;

b) rekeninginformatiedienstverleners zijn in staat om veilig te communiceren bij het verzoeken om en ontvangen van informatie over een of meer aangewezen betaalrekeningen en daarmee samenhangende betalingstransacties;

c) betaalinitiatiedienstverleners zijn in staat om veilig te communiceren bij het initiëren van een betalingsopdracht van de betaalrekening van de betaler en om alle informatie te ontvangen over de initiëring van de betalingstransactie en alle informatie die toegankelijk is voor de rekeninghoudende betaaldienstverleners met betrekking tot de uitvoering van de betalingstransactie.

2. Voor de authenticatie van de betaaldienstgebruiker kunnen rekeninginformatiedienstverleners en betaalinitiatiedienstverleners dankzij de in lid 1 bedoelde interface een beroep doen op alle authenticatieprocedures die de rekeninghoudende betaaldienstverlener aan de betaaldienstgebruiker heeft aangeboden.

De interface voldoet ten minste aan elk van de volgende vereisten:

a) een betaalinitiatiedienstverlener of een rekeninginformatiedienstverlener is in staat de rekeninghoudende betaaldienstverlener te instrueren om de authenticatie te starten op basis van de instemming van de betaaldienstgebruiker;

b) communicatiesessies tussen de rekeninghoudende betaaldienstverlener, de rekeninginformatiedienstverlener, de betaalinitiatiedienstverlener en betaaldienstgebruikers komt tot stand en wordt aangehouden via de authenticatie;

c) de integriteit en de vertrouwelijkheid van de persoonlijke beveiligingsgegevens en van door of via de betaalinitiatiedienstverlener of de rekeninginformatiedienstverlener doorgezonden authenticatiecodes worden gewaarborgd.

3. Rekeninghoudende betaaldienstverleners zorgen ervoor dat hun interfaces communicatiestandaarden volgen die zijn uitgevaardigd door internationale of Europese standaardisatieorganisaties.

Rekeninghoudende betaaldienstverleners zorgen er ook voor dat de technische specificaties van de interfaces worden gedocumenteerd, waarbij een stel routines, protocollen en tools wordt aangegeven die betaalinitiatiedienstverleners, rekeninginformatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, nodig hebben om hun software en toepassingen interoperabel te maken met de systemen van de rekeninghoudende betaaldienstverleners.

Rekeninghoudende betaaldienstverleners stellen ten minste, en zeker zes maanden vóór de in artikel 38, lid 2, genoemde toepassingsdatum, of vóór de beoogde datum voor de marktlancering van de toegangsinterface wanneer de lancering plaatsvindt na de in artikel 38, lid 2, genoemde datum, de documentatie kosteloos beschikbaar op verzoek van vergunninghoudende betaalinitiatiedienstverleners, rekeninginformatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven of betaaldienstverleners die bij hun bevoegde autoriteiten de desbetreffende vergunning hebben aangevraagd, en stellen een overzicht van de documentatie publiek beschikbaar op hun website.

4. Naast het bepaalde in lid 3 zorgen rekeninghoudende betaaldienstverleners ervoor dat, afgezien van noodsituaties, aanpassingen aan de technische specificaties van hun interface aan vergunninghoudende betaalinitiatiedienstverleners, rekeninginformatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven of betaaldienstverleners die bij hun bevoegde autoriteiten de desbetreffende vergunning hebben aangevraagd, zo snel mogelijk vooraf en ten minste drie maanden voordat de aanpassing wordt geïmplementeerd, beschikbaar worden gesteld.

Betaaldienstverleners documenteren noodsituaties waarin aanpassingen zijn geïmplementeerd en stellen de documentatie op verzoek aan bevoegde autoriteiten beschikbaar.

5. Betaaldienstverleners stellen een testvoorziening beschikbaar, met inbegrip van ondersteuning, voor het testen van verbindingen en functionaliteiten zodat vergunninghoudende betaalinitiatiedienstverleners, rekeninginformatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven of betaaldienstverleners die bij hun bevoegde autoriteiten de desbetreffende vergunning hebben aangevraagd, de software en toepassingen kunnen testen die zij gebruiken om een betaaldienst aan gebruikers aan te bieden. Deze testvoorziening dient beschikbaar te worden gesteld uiterlijk zes maanden vóór de in artikel 38, lid 2, genoemde toepassingsdatum of vóór de beoogde datum voor de marktlancering van de toegangsinterface, wanneer de lancering plaatsvindt na de in artikel 38, lid 2, genoemde datum,

Via de testvoorziening mag evenwel geen gevoelige informatie worden gedeeld.

6. Bevoegde autoriteiten zien erop toe dat rekeninghoudende betaaldienstverleners te allen tijde aan de in deze normen opgenomen verplichtingen voldoen wat betreft de interface of interfaces die zij beschikbaar stellen. Ingeval een rekeninghoudende betaaldienstverlener niet aan de in deze normen voor interfaces vastgestelde vereisten voldoet, zorgen bevoegde autoriteiten ervoor dat het verlenen van betaalinitiatiediensten en rekeninginformatiediensten niet wordt belet of verstoord, voor zover de betrokken verleners van die diensten aan de in artikel 33, lid 5, bepaalde voorwaarden voldoen.

Artikel 31

Opties voor toegangsinterfaces

Rekeninghoudende betaaldienstverleners zetten de in artikel 30 bedoelde interface of interfaces op via een speciale interface of door toe te staan dat de in artikel 30, lid 1, genoemde betaaldienstverleners gebruikmaken van de interfaces die worden gebruikt voor authenticatie van en communicatie met de betaaldienstgebruikers van de rekeninghoudende betaaldienstverlener.

Artikel 32

Voor een speciale interface geldende verplichtingen

1. Op voorwaarde dat het bepaalde in de artikelen 30 en 31 in acht wordt genomen, zorgen rekeninghoudende betaaldienstverleners die een speciale interface hebben opgezet, ervoor dat die speciale interface te allen tijde hetzelfde niveau van beschikbaarheid en prestaties, met inbegrip van ondersteuning, aanbiedt als de interfaces die aan de betaaldienstgebruiker beschikbaar worden gesteld om direct onlinetoegang te krijgen tot zijn betaalrekening.

2. Rekeninghoudende betaaldienstverleners die een speciale interface hebben opgezet, leggen transparante kritische prestatie-indicatoren (KPI's) en serviceniveaudoelstellingen vast, die ten minste even streng zijn als die voor de interface die voor hun betaaldienstgebruikers wordt gebruikt, zowel in termen van beschikbaarheid als in termen van gegevens die zijn verschaft in overeenstemming met artikel 36. Die interfaces, indicatoren en doelstellingen worden door de bevoegde autoriteiten gemonitord en aan stresstests onderworpen.

3. Rekeninghoudende betaaldienstverleners die een speciale interface hebben opgezet, zorgen ervoor dat deze interface geen obstakels opwerpt voor het verlenen van betaalinitiatiediensten en rekeninginformatiediensten. Bij dergelijke obstakels kan het onder meer gaan om het beletten van het gebruik door de in artikel 30, lid 1, genoemde betaaldienstverleners van de door rekeninghoudende betaaldienstverleners aan hun cliënten afgegeven beveiligingsgegevens, het opleggen van omleiding naar de authenticatie of andere functies van de rekeninghoudende betaaldienstverlener, het eisen van bijkomende vergunningen en registraties boven op die welke zijn bepaald in de artikelen 11, 14 en 15 van Richtlijn (EU) 2015/2366, of het eisen van extra controles op de door betaaldienstgebruikers aan betaalinitiatiedienstverleners en rekeninginformatiedienstverleners verleende toestemming.

4. Voor de toepassing van de leden 1 en 2 monitoren rekeninghoudende betaaldienstverleners de beschikbaarheid en prestaties van de speciale interface. Rekeninghoudende betaaldienstverleners maken op hun website per kwartaal statistische gegevens bekend over de beschikbaarheid en prestaties van de speciale interface en van de door hun betaaldienstgebruikers gebruikte interface.

Artikel 33

Uitwijkvoorzieningen voor een speciale interface

1. Rekeninghoudende betaaldienstverleners nemen, bij het vormgeven van de speciale interface, een strategie en plannen voor uitwijkvoorzieningen op voor het geval de interface niet presteert in overeenstemming met artikel 32, de interface ongepland onbeschikbaar is en het systeem uitvalt. Ongeplande onbeschikbaarheid of een systeemuitval kan worden geacht te hebben plaatsgevonden wanneer op vijf opeenvolgende verzoeken om toegang tot informatie voor het verlenen van betaalinitiatiediensten of rekeninginformatiediensten niet binnen dertig seconden een antwoord is gekomen.

2. Uitwijkvoorzieningen omvatten communicatieplannen om betaaldienstverleners die van de speciale interface gebruikmaken, te informeren over maatregelen om het systeem te herstellen en een beschrijving van de meteen beschikbare alternatieve opties waarover betaaldienstverleners in de tussentijd kunnen beschikken.

3. Zowel de rekeninghoudende betaaldienstverlener als de betaaldienstverleners genoemd in artikel 30, lid 1, melden problemen met in lid 1 beschreven speciale interfaces onverwijld bij hun respectieve bevoegde nationale autoriteiten.

4. Als onderdeel van een uitwijkvoorziening mogen in artikel 30, lid 1, genoemde betaaldienstverleners gebruikmaken van de interfaces die aan de betaaldienstgebruiker beschikbaar worden gesteld voor de authenticatie door en communicatie met hun rekeninghoudende betaaldienstverlener, totdat de speciale interface is hersteld tot het in artikel 32 bepaalde niveau van betrouwbaarheid en prestaties.

5. Met het oog daarop zorgen rekeninghoudende betaaldienstverleners ervoor dat de in artikel 30, lid 1, genoemde betaaldienstverleners kunnen worden geïdentificeerd en een beroep kunnen doen op de door de rekeninghoudende betaaldienstverlener voor de betaaldienstgebruiker vastgestelde authenticatieprocedures. Wanneer de in artikel 30, lid 1, bedoelde betaaldienstverleners gebruikmaken van de in lid 4 bedoelde interface, doen zij het volgende:

a) zij nemen de nodige maatregelen om ervoor te zorgen dat zij zich geen toegang verschaffen tot gegevens of deze opslaan of verwerken voor andere doelstellingen dan het verlenen van de door de betaaldienstgebruiker gevraagde dienst;

b) zij blijven voldoen aan de verplichtingen uit hoofde van, onderscheidenlijk, artikel 66, lid 3, en artikel 67, lid 2, van Richtlijn (EU) 2015/2366;

c) zij loggen de gegevens waartoe zij toegang hadden via de interface die door de rekeninghoudende betaaldienstverlener wordt geëxploiteerd ten behoeve van zijn betaaldienstgebruikers, en verschaffen, op verzoek en onverwijld, de logboekbestanden aan hun bevoegde nationale autoriteit;

d) zij verantwoorden tegenover hun bevoegde nationale autoriteit, op verzoek en onverwijld, deugdelijk het gebruik van de interface die aan de betaaldienstgebruiker beschikbaar is gesteld met het oog op rechtstreekse onlinetoegang tot zijn betaalrekening;

e) zij informeren de rekeninghoudende betaaldienstverlener in die zin.

6. Bevoegde autoriteiten verlenen, na overleg met de EBA met het oog op een coherente toepassing van de onderstaande voorwaarden, aan de rekeninghoudende betaaldienstverleners die voor een speciale interface hebben geopteerd, ontheffing van de verplichting om de in lid 4 beschreven uitwijkvoorziening op te zetten wanneer de speciale interface aan elk van de volgende voorwaarden voldoet:

a) hij voldoet aan alle in artikel 32 uiteengezette verplichtingen voor speciale interfaces;

b) hij is ontworpen en getest in overeenstemming met artikel 30, lid 5, tot tevredenheid van de daarin genoemde betaaldienstverleners;

c) hij is ten minste drie maanden door betaaldienstverleners breed gebruikt voor het verlenen van rekeninginformatiediensten en betaalinitiatiediensten en voor het bevestigen van de beschikbaarheid van middelen voor op kaarten gebaseerde betalingen;

d) problemen met betrekking tot de speciale interface zijn onverwijld opgelost.

7. Bevoegde autoriteiten herroepen de in lid 6 bedoelde ontheffing wanneer de rekeninghoudende betaaldienstverleners voor meer dan twee opeenvolgende kalenderweken niet aan de voorwaarden van de punten a) en d) voldoen. Bevoegde autoriteiten stellen de EBA van deze herroeping in kennis en zorgen ervoor dat de rekeninghoudende betaaldienstverlener, binnen de kortst mogelijke tijd en uiterlijk binnen twee maanden, de in lid 4 bedoelde uitwijkvoorziening opzet.

Artikel 34

Certificaten

1. Met het oog op identificatie als bedoeld in artikel 30, lid 1, onder a), doen betaaldienstverleners een beroep op gekwalificeerde certificaten voor elektronische zegels als bedoeld in artikel 3, punt 30, van Verordening (EU) nr. 910/2014 voor websiteauthenticatie als bedoeld in artikel 3, punt 39, van die verordening.

2. Voor de toepassing van deze verordening is het registratienummer als vermeld in de officiële registers, in overeenstemming met bijlage III, onder c), of bijlage IV, onder c), bij Verordening (EU) nr. 910/2014, het vergunningnummer van de betaaldienstverlener die op kaarten gebaseerde betaalinstrumenten uitgeeft, en het vergunningnummer van de rekeninginformatiedienstverleners en betaalinitiatiedienstverleners, met inbegrip van rekeninghoudende betaaldienstverleners die dergelijke diensten verlenen, dat beschikbaar is in het openbare register van de lidstaat van herkomst overeenkomstig artikel 14 van Richtlijn (EU) 2015/2366, of dat voortvloeit uit de kennisgevingen overeenkomstig artikel 20 van Richtlijn 2013/36/EU van het Europees Parlement en de Raad [1] van elke op grond van artikel 8 van die richtlijn afgegeven vergunning.

3. Voor de toepassing van deze verordening bevatten gekwalificeerde certificaten voor elektronische zegels of voor websiteauthenticatie als bedoeld in lid 1, in een in internationale financiële kringen gangbare taal, bijkomende specifieke attributen voor elk van de volgende elementen:

a) de rol van de betaaldienstverlener, die een of meer van de volgende kan zijn:

   i) dienstverlening op het gebied van het beheer van bankrekeningen;

   ii) betaalinitiatie;

   iii) rekeninginformatie;

   iv) uitgifte van op kaarten gebaseerde betaalinstrumenten;

b) de naam van de bevoegde autoriteiten waar de betaaldienstverlener is geregistreerd.

4. De in lid 3 genoemde attributen zijn niet van invloed op de interoperabiliteit en erkenning van gekwalificeerde certificaten voor elektronische zegels of websiteauthenticatie.

---

[1] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).

Artikel 35

Beveiliging van communicatiesessies

1. Rekeninghoudende betaaldienstverleners, betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, rekeninginformatiedienstverleners en betaalinitiatiedienstverleners zorgen ervoor dat bij gegevensuitwisseling via het internet tussen de communicerende partijen gedurende de hele betrokken communicatiesessie veilige versleuteling wordt toegepast om de vertrouwelijkheid en de integriteit van gegevens te garanderen, door gebruik te maken van sterke en algemeen erkende versleutelingstechnieken.

2. Betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, rekeninginformatiedienstverleners en betaalinitiatiedienstverleners houden de door rekeninghoudende betaaldienstverleners aangeboden toegangssessies zo kort mogelijk en beëindigen actief dergelijke sessies zodra de gevraagde actie is uitgevoerd.

3. Wanneer zij parallelle netwerksessies met de rekeninghoudende betaaldienstverlener in stand houden, zorgen rekeninginformatiedienstverleners en betaalinitiatiedienstverleners ervoor dat die sessies veilig worden gekoppeld aan de betrokken sessies die tot stand worden gebracht met de betaaldienstgebruiker of betaaldienstgebruikers, om het risico te voorkomen dat onderling tussen hen gecommuniceerde berichten of informatie wordt afgeleid.

4. Rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten bij de rekeninghoudende betaaldienstverlener uitgeven, vermelden ondubbelzinnige referenties naar elk van de volgende items:

a) de betaaldienstgebruiker of betaaldienstgebruikers en de overeenkomstige communicatiesessie zodat verschillende verzoeken van dezelfde betaaldienstgebruiker of betaaldienstgebruikers kunnen worden onderscheiden;

b) voor betaalinitiatiediensten: de uniek geïdentificeerde geïnitieerde betalingstransactie:

c) voor de bevestiging van de beschikbaarheid van middelen: het uniek geïdentificeerde verzoek met betrekking tot het voor de uitvoering van de op kaarten gebaseerde betalingstransactie.

5. Rekeninghoudende betaaldienstverleners, rekeninginformatiedienstverleners, betaalinitiatiedienstverleners en betaaldienstverleners die op kaarten gebaseerde betaalinstrumenten uitgeven, zorgen ervoor dat, wanneer zij persoonlijke beveiligingsgegevens en authenticatiecodes communiceren, deze niet — rechtstreeks of indirect — op enig tijdstip leesbaar zijn voor personeelsleden.

In geval van verlies van vertrouwelijkheid van persoonlijke beveiligingsgegevens binnen hun bevoegdheid stellen die dienstverleners de daaraan gekoppelde betaaldienstgebruiker en de uitgever van de persoonlijke beveiligingsgegevens daarvan onverwijld in kennis.

Artikel 36

Gegevensuitwisseling

1. Rekeninghoudende betaaldienstverleners voldoen aan elk van de volgende voorwaarden:

a) zij verstrekken rekeninginformatiedienstverleners dezelfde informatie van aangewezen betaalrekeningen en daarmee samenhangende transacties die aan de betaaldienstgebruiker beschikbaar worden gesteld, wanneer rechtstreeks om toegang tot de rekeninginformatie wordt gevraagd, op voorwaarde dat deze informatie geen gevoelige betalingsgegevens bevat;

b) zij verstrekken onmiddellijk na ontvangst van de betalingsopdracht aan betaalinitiatiedienstverleners dezelfde informatie over de initiëring en uitvoering van de betalingstransactie die is verschaft of beschikbaar is gesteld aan de betaaldienstgebruiker, wanneer deze laatste de transactie rechtstreeks heeft geïnitieerd;

c) zij verschaffen, op verzoek, aan betaaldienstverleners een bevestiging, in de vorm van een eenvoudig „ja" of „neen", op de vraag of het voor de uitvoering van een betaaltransactie vereiste bedrag op de betaalrekening van de betaler beschikbaar is.

2. In geval van een onverwachte gebeurtenis of een fout tijdens de identificatie- of authenticatieprocedure of bij de uitwisseling van de gegevensbestanddelen zendt de rekeninghoudende betaaldienstverlener een kennisgevingsbericht aan de betaalinitiatiedienstverlener of de rekeninginformatiedienstverlener en aan de betaaldienstverlener die op kaarten gebaseerde betaalinstrumenten uitgeeft, waarin de reden voor die onverwachte gebeurtenis of die fout wordt toegelicht.

Wanneer de rekeninghoudende betaaldienstverlener overeenkomstig artikel 32 een speciale interface aanbiedt, wordt bij die interface voorzien in kennisgevingsberichten betreffende onverwachte gebeurtenissen of fouten, die door betaaldienstverleners die de gebeurtenis of fout ontdekken, moeten worden meegedeeld aan de overige aan de communicatiesessie deelnemende betaaldienstverleners.

3. Rekeninginformatiedienstverleners beschikken over geschikte en doeltreffende mechanismen om ervoor te zorgen dat alleen toegang tot informatie wordt gegeven vanaf aangewezen betaalrekeningen en daarmee samenhangende betalingstransacties, in overeenstemming met de uitdrukkelijke toestemming van de gebruiker.

4. Betaalinitiatiedienstverleners verschaffen rekeninghoudende betaaldienstverleners dezelfde informatie als die welke van de betaaldienstgebruiker wordt gevraagd bij het rechtstreeks initiëren van de betalingstransactie.

5. Rekeninginformatiedienstverleners zijn in staat toegang te krijgen tot informatie van aangewezen betaalrekeningen en daarmee samenhangende betalingstransacties waarover rekeninghoudende betaaldienstverleners beschikken, om de rekeninginformatiedienst in een van de beide volgende omstandigheden te kunnen uitvoeren:

a) telkens als de betaaldienstgebruiker actief om die informatie verzoekt;

b) telkens als de betaaldienstgebruiker niet actief om die informatie verzoekt, niet minder dan viermaal over een periode van 24 uur, tenzij een hogere frequentie is overeengekomen tussen de betaalinitiatiedienstverlener en de rekeninghoudende betaaldienstverlener, met de toestemming van de betaaldienstgebruiker.

HOOFDSTUK VI

SLOTBEPALINGEN

Artikel 37

Evaluatie

Onverminderd het bepaalde in artikel 98, lid 5, van Richtlijn (EU) 2015/2366 evalueert de EBA tegen 14 maart 2021 de in de bijlage bij deze verordening genoemde fraudepercentages, alsmede de op grond van artikel 33, lid 6, verleende vrijstellingen met betrekking tot speciale interfaces, en legt zij ontwerpactualiseringen hiervan, overeenkomstig artikel 10 van Verordening (EU) nr. 1093/2010, aan de Commissie voor.

Artikel 38

Inwerkingtreding

1. Deze verordening treedt in werking op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

2. Deze verordening is van toepassing met ingang van 14 september 2019.

3. De leden 3 en 5 van artikel 30 zijn evenwel van toepassing met ingang van 14 maart 2019.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 27 november 2017.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE

	Referentiefraudepercentage (%) voor:	
Drempelwaarde voor vrijstelling	Elektronische op kaarten gebaseerde betalingen op afstand	Elektronische overmakingen op afstand
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015