►B

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2018/389

av den 27 november 2017

om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för stränga kundautentisering och gemensamma och säkra öppna kommunikationsstandarder

(Text av betydelse för EES)

(EUT L 69, 13.3.2018, s. 23)

Ändrad genom:

		Officiella tidningen		
		nr	sida	datum
►M1	Kommissionens delegerade förordning (EU) 2022/2360 av den 3 augusti 2022	L 312	1	5.12.2022
►M2	Kommissionens delegerade förordning (EU) 2023/1650 av den 15 maj 2023	L 208	1	23.8.2023

▼B

KOMMISSIONENS DELEGERADE FÖRORDNING (EU) 2018/389

av den 27 november 2017

om komplettering av Europaparlamentets och rådets direktiv (EU) 2015/2366 vad gäller tekniska tillsynsstandarder för sträng kundautentisering och gemensamma och säkra öppna kommunikationsstandarder

(Text av betydelse för EES)

KAPITEL 1

ALLMÄNA BESTÄMMELSER

Artikel 1

Syfte

Denna förordning fastställer de krav som betaltjänstleverantörer ska efterleva i fråga om att genomföra säkerhetsåtgärder, så att det blir möjligt för dem att göra följande:

a) Tillämpa förfarandet för sträng kundautentisering i enlighet med artikel 97 i direktiv (EU) 2015/2366.

b) Göra undantag från tillämpningen av säkerhetskraven för sträng kundautentisering, om särskilda och begränsade villkor uppfylls som baseras på betalningstransaktionens risk, belopp och upprepning och vilken betalningskanal som används vid genomförandet av transaktionen.

c) Skydda betaltjänstanvändarens personliga säkerhetsbehörighetsuppgifters konfidentialitet och integritet.

d) Upprätta gemensamma och säkra öppna standarder för kommunikation mellan kontoförvaltande betaltjänstleverantörer, leverantörer av betalningsinitieringstjänster, leverantörer av kontoinformationstjänster, betalare, betalningsmottagare och andra leverantörer av betaltjänster med avseende på tillhandahållande och användning av betaltjänster vid tillämpningen av avdelning IV i direktiv (EU) 2015/2366.

Artikel 2

Allmänna autentiseringskrav

1. Betaltjänstleverantörerna ska ha inrättat transaktionsövervakningsmekanismer som gör det möjligt för dem att upptäcka icke auktoriserade eller bedrägliga betalningstransaktioner vid genomförande av de säkerhetsåtgärder som avses i artikel 1 a och b.

Dessa mekanismer ska baseras på en analys av betalningstransaktioner som beaktar element som är typiska för betaltjänstanvändaren vid normal användning av personliga säkerhetsbehörighetsuppgifter.

▼B

2. Betaltjänstleverantörerna ska säkerställa att transaktionsövervakningsmekanismerna åtminstone beaktar alla följande riskbaserade faktorer:

a) Förteckningar över element som komprometterats eller stulits.

b) Transaktionsbeloppet för varje betalning.

c) Kända bedrägeriscenarier i samband med tillhandahållande av betaltjänster.

d) Tecken på infektion av sabotageprogram i något skede av autentiseringsförfarandet.

e) Om inloggningsutrustningen eller programvaran tillhandahålls av betaltjänstleverantören, en loggfil över användningen av den inloggningsutrustning eller programvara som tillhandahålls betaltjänstanvändaren samt avvikande användning av inloggningsutrustningen eller programvaran.

Artikel 3

Granskning av säkerhetsåtgärder

1. Genomförande av de säkerhetsåtgärder som avses i artikel 1 ska dokumenteras, regelbundet testas, utvärderas och, i enlighet med betaltjänstleverantörens tillämpliga rättsliga ram, revideras av revisorer med expertis inom IT-säkerhet och betalningar som är operativt oberoende inom betaltjänstleverantören eller i förhållande till denna.

2. Perioden mellan de revisioner som avses i punkt 1 ska fastställas med beaktande av de relevanta bokförings- och lagstadgade revisionsregler som betaltjänstleverantören omfattas av.

Betaltjänstleverantörer som utnyttjar det undantag som avses i artikel 18 ska dock genomgå en revision av sina metoder, sin modell och de rapporterade bedrägerifrekvenserna minst en gång per år. Den revisor som genomför denna revision ska ha expertis inom IT-säkerhet och betalningar och vara operativt oberoende inom betaltjänstleverantören eller i förhållande till denna. Under det första år som undantaget i artikel 18 tillämpas, och minst vart tredje år därefter, eller oftare på den behöriga myndighetens begäran, ska revisionen genomföras av en oberoende och kvalificerad extern revisor.

3. Inom ramen för denna revision ska en utvärdering och rapport läggas fram om huruvida betaltjänstleverantörens säkerhetsåtgärder uppfyller kraven i denna förordning.

Behöriga myndigheterna ska på begäran få tillgång till hela rapporten.

▼B

KAPITEL II

SÄKERHETSÅTGÄRDER FÖR TILLÄMPNING AV STRÄNG KUNDAUTENTISERING

Artikel 4

Autentiseringskod

1. Om betaltjänstleverantörerna tillämpar sträng kundautentisering i enlighet med artikel 97.1 i direktiv (EU) 2015/2366 ska autentiseringen grundas på minst två element som kategoriseras som kunskap, innehav och unik egenskap och leda till att en autentiseringskod genereras.

Autentiseringskoden ska endast godtas en gång av betaltjänstleverantören när betalaren använder autentiseringskoden för att få tillgång till sina betalkonton online, för att initiera en elektronisk betalningstransaktion eller för att genomföra någon åtgärd, på distans, som kan innebära en risk för betalningsbedrägeri eller andra missbruk.

2. Vid tillämpning av punkt 1 ska betaltjänstleverantörerna anta säkerhetsåtgärder som säkerställer att alla följande krav uppfylls:

a) Ingen information om något av de element som avses i punkt 1 kan inhämtas från den autentiseringskod som lämnats ut.

b) Det är inte möjligt att generera en ny autentiseringskod på grundval av kännedom om någon annan autentiseringskod som genererats i ett tidigare skede.

c) Autentiseringskoden kan inte förfalskas.

3. Betaltjänstleverantörerna ska säkerställa att autentisering genom generering av en autentiseringskod innehåller alla följande åtgärder:

a) Om generering av en autentiseringskod för tillämpning av punkt 1 – vid autentisering för fjärråtkomst, elektroniska betalningar på distans eller någon annan åtgärd, på distans, som kan innebära en risk för betalningsbedrägeri – misslyckas, ska det inte vara möjligt att avgöra vilket av de element som avses i den punkten som var felaktigt.

b) Högst fem misslyckade autentiseringsförsök i rad under en fastställd tidsperiod får ske innan de åtgärder som avses i artikel 97.1 i direktiv (EU) 2015/2366 tillfälligt blockeras.

c) Under kommunikationssessionerna finns ett skydd, i enlighet med kraven i kapitel V, mot att uppgifter som överförs under autentiseringen kapas eller manipuleras av icke auktoriserade parter.

▼B

d) Betalaren får vara inaktiv i högst fem minuter från det att denne autentiserats och fått tillgång till sitt betalkonto online.

4. Om den blockering som avses i punkt 3 b är tillfällig ska blockeringsperiodens längd och antalet nya försök fastställas på grundval av egenskaperna hos den betaltjänst som tillhandahålls användaren och alla relevanta anknutna risker, med beaktande av, åtminstone, de faktorer som avses i artikel 2.2.

Betalaren ska förvarnas innan blockeringen blir permanent.

Om blockeringen har gjorts permanent ska ett säkert förfarande upprättas genom vilket betalaren åter kan börja använda de blockerade elektroniska betalningsinstrumenten.

Artikel 5

Dynamiska kopplingar

1. Betaltjänstleverantörer som tillämpar stränг kundautentisering i enlighet med artikel 97.2 i direktiv (EU) 2015/2366 ska, utöver kraven i artikel 4 i denna förordning, anta säkerhetsåtgärder som uppfyller alla följande krav:

a) Betalaren informeras om betalningstransaktionens belopp och betalningsmottagaren.

b) Den autentiseringskod som genereras är specifik för betalningstransaktionens belopp och den betalningsmottagare som betalaren godkände då transaktionen initierades.

c) Den autentiseringskod som betaltjänstleverantören godkänner motsvarar det ursprungliga specifika betalningstransaktionsbelopp och betalningsmottagarens identitet, som godkänts av betalaren.

d) Eventuella ändringar av belopp eller betalningsmottagare leder till att den genererade autentiseringskoden ogiltigförklaras.

2. Vid tillämpning av punkt 1 ska betaltjänstleverantörerna anta säkerhetsåtgärder som ska säkerställa konfidentialiteten, autenticiteten och integriteten hos följande:

a) Transaktionsbeloppet och betalningsmottagaren under alla autentiseringsfaser.

b) Den information som visas för betalaren under alla autentiseringsfaser, inbegripet generering, överföring och användning av autentiseringskoden.

3. Vid tillämpning av punkt 1 b och om betaltjänstleverantörerna tillämpar stränг kundautentisering i enlighet med artikel 97.2 i direktiv (EU) 2015/2366 ska följande autentiseringskrav gälla:

▼B

a) Vad gäller kortbaserade betalningstransaktioner där betalaren har godkänt ett exakt belopp av de medel som ska blockeras i enlighet med artikel 75.1 i det direktivet, ska autentiseringskoden vara specifik för det belopp som betalaren har godkänt för blockering och som godkändes av betalaren när transaktionen initierades.

b) För betalningstransaktioner där betalaren har godkänt att en uppsättning elektroniska betalningstransaktioner på distans genomförs till en eller flera betalningsmottagare ska autentiseringskoden vara specifik för betalningstransaktionernas totalbelopp och för de specificerade betalningsmottagarna.

Artikel 6

Krav beträffande de element som kategoriseras som kunskap

1. Betaltjänstleverantörerna ska anta åtgärder för att minska risken för att de element för sträng kundautentisering som kategoriseras som kunskap röjs av eller lämnas ut till icke auktoriserade parter.

2. Betalarens användning av dessa element ska vara föremål för begränsningsåtgärder i syfte att förhindra att de lämnas ut till icke auktoriserade parter.

Artikel 7

Krav beträffande de element som kategoriseras som innehav

1. Betaltjänstleverantörerna ska anta åtgärder för att minska risken för att de element för sträng kundautentisering som kategoriseras som innehav används av icke auktoriserade parter.

2. Betalarens användning av dessa element ska vara föremål för åtgärder som syftar till att förhindra reproducering av dessa element.

Artikel 8

Krav beträffande utrustning och programvara kopplad till element som kategoriseras som unik egenskap

1. Betaltjänstleverantörerna ska anta åtgärder för att minska risken för att de autentiseringselement som kategoriseras som unik egenskap och som läses av inloggningsutrustning och programvara som tillhandahålls betalaren röjs av icke auktoriserade parter. Betaltjänstleverantörerna ska minst säkerställa att det föreligger mycket låg sannolikhet att en icke auktoriserad part autentiseras som betalare med hjälp av denna inloggningsutrustning och programvara.

2. Betalarens användning av dessa element ska vara föremål för åtgärder som säkerställer att denna utrustning och programvara garanterar skydd mot icke auktoriserad användning av elementen genom tillgång till utrustning och programvara.

▼B

Artikel 9

Elementens oberoende

1. Betaltjänstleverantörerna ska säkerställa att användning av de element för sträng kundautentisering som avses i artiklarna 6, 7 och 8 omfattas av åtgärder som säkerställer att röjande, med avseende på teknik, algoritmer och parametrar, av ett av elementen inte äventyrar de andra elementens tillförlitlighet.

2. Betaltjänstleverantörer ska anta säkerhetsåtgärder om något av elementen för sträng kundautentisering eller autentiseringskoden används med hjälp av en anordning med flera funktioner, för att minska risken som skulle uppkomma om säkerheten i anordningen med flera funktioner skulle äventyras.

3. Vid tillämpning av punkt 2 ska de riskreducerande åtgärderna innehålla följande:

a) Användning av separerade säkra exekveringsmiljöer med hjälp av den programvara som finns installerad i anordningen med flera funktioner.

b) Mekanismer för att säkerställa att programvaran eller utrustningen inte har ändrats av betalaren eller av en tredjepart.

c) Om ändringar har gjorts, mekanismer för att begränsa konsekvenserna av dem.

KAPITEL III

UNDANTAG FRÅN STRÄNG KUNDAUTENTISERING

▼M1

Artikel 10

Tillgång till betalkontoinformation direkt hos den kontoförvaltande betaltjänstleverantören

1. Betaltjänstleverantörer ska ha möjlighet att inte tillämpa stark kundautentisering under förutsättning att kraven i artikel 2 är uppfyllda, om en betaltjänstanvändare har direkt online-tillgång till sitt betalkonto och om tillgången är begränsad till någon av följande uppgifter online utan att känsliga betalningsuppgifter lämnas ut:

a) Saldot för ett eller flera specifika betalkonton.

b) Betalningstransaktionerna de senaste 90 dagarna till och från ett eller flera specifika betalkonton.

2. Med avvikelse från punkt 1 ska betaltjänstleverantörer inte undantas från tillämpning av stark kundautentisering om något av följande villkor uppfylls:

▼M1

a) Det är första gången betaltjänstanvändaren får online-tillgång till de uppgifter som anges i punkt 1.

b) Det har gått mer än 180 dagar sedan betaltjänstanvändaren senaste gången hade online-tillgång till de uppgifter som anges i punkt 1 och stark kundautentisering tillämpades.

Artikel 10a

Tillgång till betalkontoinformation via en leverantör av kontoinformationstjänster

1. Betaltjänstleverantörer ska inte tillämpa stark kundautentisering om en betaltjänstanvändare har online-tillgång till sitt betalkonto via en leverantör av kontoinformationstjänster, förutsatt att tillgången är begränsad till någon av följande uppgifter online utan att känsliga betalningsuppgifter lämnas ut:

a) Saldot för ett eller flera specifika betalkonton.

b) Betalningstransaktionerna de senaste 90 dagarna till och från ett eller flera specifika betalkonton.

2. Med avvikelse från punkt 1 ska betaltjänstleverantörer tillämpa stark kundautentisering om något av följande villkor uppfylls:

a) Det är första gången betaltjänstanvändaren får online-tillgång till de uppgifter som anges i punkt 1 via leverantören av kontoinformationstjänster.

b) Det har gått mer än 180 dagar sedan betaltjänstanvändaren senaste gången hade online-tillgång till de uppgifter som anges i punkt 1 via leverantören av kontoinformationstjänster och stark kundautentisering tillämpades.

3. Med avvikelse från punkt 1 ska betaltjänstleverantörer ha möjlighet att tillämpa stark kundautentisering om en betaltjänstanvändare har online-tillgång till sitt betalkonto via en leverantör av kontoinformationstjänster och betaltjänstleverantören har objektivt motiverade och vederbörligen styrkta skäl som rör icke auktoriserad eller bedräglig tillgång till betalkontot. I sådana fall ska betaltjänstleverantören dokumentera och vederbörligen motivera skälen för att tillämpa stark kundautentisering för sin behöriga nationella myndighet på dess begäran.

▼M1

4. Kontoförvaltande betaltjänstleverantörer som erbjuder ett särskilt gränssnitt enligt artikel 31 ska inte vara skyldiga att tillämpa det undantag som fastställs i punkt 1 i den här artikeln med avseende på den beredskapsmekanism som avses i artikel 33.4, om de inte tillämpar det undantag som fastställs i artikel 10 i det direkta gränssnitt som används för autentisering och kommunikation med betaltjänstanvändarna.

▼B

Artikel 11

Kontaktfria betalningar vid försäljningsställe

Förutsatt att kraven i artikel 2 uppfylls behöver betaltjänstleverantörerna inte tillämpa sträng kundautentisering om betalaren initierar en kontaktfri elektronisk betalningstransaktion, under förutsättning att följande villkor uppfylls:

a) Värdet på den enskilda kontaktfria elektroniska betalningstransaktionen är högst 50 euro.

b) Det ackumulerade värdet av tidigare kontakfria elektroniska betalningstransaktioner som initierats med hjälp av betalningsinstrument med kontaktfri funktion sedan dagen då sträng kundautentisering senast tillämpades är högst 150 euro.

c) Högst fem på varandra följande kontaktfria elektroniska betalningstransaktioner har initierats via betalningsinstrument med kontaktfri funktion sedan dagen då sträng kundautentisering senast tillämpades.

Artikel 12

Obemannade terminaler för transport- och parkeringsavgifter

Förutsatt att kraven i artikel 2 uppfylls behöver betaltjänstleverantörerna inte tillämpa sträng kundautentisering om betalaren initierar en elektronisk betalningstransaktion vid en obemannad betalningsterminal för att betala en transport- eller parkeringsavgift.

Artikel 13

Betrodda betalningsmottagare

1. Betaltjänstleverantörer ska tillämpa sträng kundautentisering om en betalare upprättar eller ändrar en förteckning över betrodda betalningsmottagare genom betalarens kontoförvaltande betaltjänstleverantör.

2. Förutsatt att de allmänna autentiseringskraven uppfylls behöver betaltjänstleverantörer inte tillämpa sträng kundautentisering om betalaren initierar en betalningstransaktion och betalningsmottagaren finns med på den förteckning över betrodda betalningsmottagare som tidigare upprättats av betalaren.

▼B

Artikel 14

Återkommande transaktioner

1. Betaltjänstleverantörer ska tillämpa sträng kundautentisering när en betalare för första gången upprättar, ändrar eller för första gången initierar en serie återkommande transaktioner av samma värde och till samma betalningsmottagare.

2. Förutsatt att de allmänna autentiseringskraven uppfylls behöver betaltjänstleverantörer inte tillämpa sträng kundautentisering vid initiering av alla följande betalningstransaktioner som ingår i den serie av betalningstransaktioner som avses i punkt 1.

Artikel 15

Kreditöverföringar mellan konton som innehas av samma fysiska eller juridiska person

Förutsatt att kraven i artikel 2 uppfylls behöver betaltjänstleverantörer inte tillämpa sträng kundautentisering om betalaren initierar en kreditöverföring under omständigheter då betalaren och betalningsmottagaren är samma fysiska eller juridiska person och båda betalkontona innehas av samma kontoförvaltande betaltjänstleverantör.

Artikel 16

Transaktioner av begränsat värde

Förutsatt att de allmänna autentiseringskraven uppfylls behöver betaltjänstleverantörerna inte tillämpa sträng kundautentisering om betalaren initierar en elektronisk betalningstransaktion på distans, under förutsättning att följande villkor uppfylls:

a) Värdet av den elektroniska betalningstransaktionen på distans är högst 30 euro.

b) Det ackumulerade värdet av tidigare elektroniska betalningstransaktioner på distans som initierats av betalaren sedan den senaste tillämpningen av sträng kundautentisering är högst 100 euro.

c) Högst fem på varandra följande enskilda elektroniska betalningstransaktioner på distans har initierats av betalaren sedan den senaste tillämpningen av sträng kundautentisering.

Artikel 17

Säkra processer och protokoll för företagsbetalningar

Betaltjänstleverantörer behöver inte tillämpa sträng kundautentisering när det gäller juridiska personer som initierar elektroniska betalningstransaktioner genom användning av specifika betalningsprocesser eller

▼B

protokoll som endast görs tillgängliga för betalare som inte är konsumenter, om de behöriga myndigheterna har förvissat sig om att dessa förfaranden eller protokoll garanterar åtminstone samma säkerhetsnivå som den som föreskrivs i direktiv (EU) 2015/2366.

Artikel 18

Transaktionsriskanalys

1. Betaltjänstleverantörer behöver inte tillämpa sträng kundautentisering om betalaren initierar en elektronisk betalningstransaktion, på distans, som betaltjänstleverantören bedömer utgöra en låg risk enligt den transaktionsövervakningsmekanism som avses i artikel 2 och i punkt 2 c i denna artikel.

2. En sådan elektronisk betalningstransaktion som avses i punkt 1 ska anses utgöra en lågrisktransaktion om samtliga följande villkor uppfylls:

a) Bedrägerifrekvensen, för den aktuella typen av transaktion, som rapporterats av betaltjänstleverantören och som beräknats i enlighet med artikel 19 är lika med eller lägre än de bedrägerifrekvenser som fastställts som referens i tabellen i bilagan, för ”elektroniska kortbaserade betalningar på distans” respektive ”kreditöverföringar på distans”.

b) Transaktionsbeloppet överskrider inte det relevanta tröskelvärde för undantag som anges i tabellen i bilagan.

c) Betaltjänstleverantörerna har efter att ha genomfört en riskanalys i realtid inte konstaterat

   i) avvikande betalnings- eller beteendemönster hos betalaren,

   ii) avvikande uppgifter avseende betalarens inloggningsutrustning/-programvara,

   iii) infektion av sabotageprogram i något av autentiseringsskedena,

   iv) kända bedrägeriscenarier i samband med tillhandahållandet av betaltjänster,

   v) att betalarens lokalisering avviker från det normala,

   vi) att betalningsmottageren befinner sig på en plats som anses innebära hög risk.

3. Betaltjänstleverantörer som avser att undanta elektroniska betalningstransaktioner på distans från sträng kundautentisering med hänvisning till att de utgör lågrisktransaktioner, ska minst beakta följande riskbaserade faktorer:

a) Den enskilda betaltjänstanvändarens tidigare utgiftsmönster.

b) Betalningstransaktionshistoriken hos var och en av betaltjänstleverantörens betaltjänstanvändare.

▼B

c) Var betalaren och betalningsmottagaren befinner sig vid tidpunkten för betalningstransaktionen om inloggningsutrustningen eller programvaran tillhandahålls av betaltjänstleverantören.

d) Avvikande betalningsmönster konstateras hos betaltjänstanvändaren i förhållande till dennes betalningstransaktionshistorik.

Betaltjänstleverantörens bedömning ska kombinera alla dessa riskbaserade faktorer för att få fram ett riskvärde för varje enskild transaktion som avgör om en specifik betalning ska tillåtas utan sträng kundautentisering.

Artikel 19

Beräkning av bedrägerifrekvens

1. Betaltjänstleverantören ska för varje typ av transaktion som avses i tabellen i bilagan säkerställa att den övergripande bedrägerifrekvensen – som omfattar såväl betalningstransaktioner som autentiseras genom sträng kundautentisering som sådana som genomförs enligt något av de undantag som avses i artiklarna 13–18 – är lika med eller lägre än de bedrägerifrekvenser för samma typ av betalningstransaktion och som fastställs som referens i tabellen i bilagan.

Den övergripande bedrägerifrekvensen för varje typ av transaktion ska beräknas som det totala värdet av icke auktoriserade eller bedrägliga transaktioner på distans, oavsett om medlen har återvunnits eller ej, dividerat med det totala värdet av alla transaktioner på distans inom respektive transaktionstyp, oavsett om de är autentiserade med tillämpning av sträng kundautentisering eller genomförda enligt de undantag som avses i artiklarna 13–18, på löpande basis en gång i kvartalet (90 dagar).

2. Beräkningen av bedrägerifrekvenserna och de tal som blir resultatet ska bedömas genom den revisorsgranskning som avses i artikel 3.2 vilken ska säkerställa att de är fullständiga och korrekta.

3. Metoden och eventuella modeller som används av betaltjänstleverantören för att räkna ut bedrägerifrekvensen, samt bedrägerifrekvensen i sig ska dokumenteras på lämpligt sätt och vara tillgängliga i sin helhet för behöriga myndigheter och EBA, med förhandsanmälan till relevant behörig myndighet på deras begäran.

Artikel 20

Upphävande av undantag som baseras på transaktionsriskanalys

1. Betaltjänstleverantörer som utnyttjar undantagen i artikel 18 ska omedelbart rapportera till de behöriga myndigheterna om en av de bedrägerifrekvenser som de övervakar, för alla typer av betalningstransaktioner som anges i tabellen i bilagan, överskrider den tillämpliga bedrägerifrekvens som fastställts som referens och ska till behöriga myndigheter lämna en redogörelse för de åtgärder som de avser att anta för att deras övervakade bedrägerifrekvens återigen ska överensstämma med tillämpliga bedrägerifrekvenser som fastställts som referens.

▼B

2. Betaltjänstleverantörer ska omedelbart upphöra att tillämpa undantaget i artikel 18 för alla typer av betalningstransaktioner som anges i tabellen i bilagan inom det specifika tröskelvärdesintervallet om deras övervakade bedrägerifrekvenser under två på varandra följande kvartal överskrider den tillämpliga bedrägerifrekvens som fastställts som referens för det betalningsinstrumentet eller för den typen av betalningstransaktion inom tröskelvärdesintervallet för det undantaget.

3. Efter upphävandet av det undantaget i artikel 18 i enlighet med punkt 2 i denna artikel får betaltjänstleverantörerna inte tillämpa detta undantag igen förrän deras beräknade bedrägerifrekvenser under ett kvartal är lika med eller lägre än de bedrägerifrekvenser som fastställts som referens som är tillämpliga för den typen av betalningstransaktion inom det tröskelvärdesintervallet för undantag.

4. Betaltjänstleverantörer som avser att ånyo utnyttja undantaget i artikel 18 ska anmäla detta till behöriga myndigheter i god tid och ska innan de åter utnyttjar undantaget lägga fram uppgifter som styrker att deras övervakade bedrägerifrekvens återigen efterlever den tillämpliga bedrägerifrekvens som fastställts som referens för tröskelvärdesintervallet för undantag, i enlighet med punkt 3 i denna artikel.

Artikel 21

Övervakning

1. För att utnyttja undantagen i artiklarna 10–18 ska betaltjänstleverantörerna minst en gång i kvartalet dokumentera och övervaka följande uppgifter för varje typ av transaktion fördelat på betalningstransaktioner på distans och övriga betalningstransaktioner:

a) Det totala värdet av icke auktoriserade eller bedrägliga betalningstransaktioner i enlighet med artikel 64.2 i direktiv (EU) 2015/2366, det totala värdet av alla betalningstransaktioner och de bedrägerifrekvenser som följer av dem, inbegripet en uppdelning av betalningstransaktioner som initierats genom sträng kundautentisering och enligt vart och ett av undantagen.

b) Det genomsnittliga transaktionsvärdet, inbegripet en uppdelning av betalningstransaktioner som initierats genom sträng kundautentisering och enligt vart och ett av undantagen.

c) Antalet betalningstransaktioner där något av undantagen tillämpats och deras andel i förhållande till det totala antalet betalningstransaktioner.

2. Betaltjänstleverantörer ska göra resultaten av övervakningen i enlighet med punkt 1 tillgängliga för behöriga myndigheter och EBA, med förhandsanmälan till relevanta behöriga myndigheter på deras begäran.

▼B

KAPITEL IV

BETALTJÄNSTANVÄNDARES PERSONLIGA SÄKERHETSBEHÖRIGHETSUPPGIFTERS KONFIDENTIALITET OCH INTEGRITET

Artikel 22

Allmänna krav

1. Betaltjänstleverantörerna ska säkerställa konfidentialiteten och integriteten hos betaltjänstanvändarnas personliga säkerhetsbehörighetsuppgifter, inbegripet autentiseringskoder, under alla autentiseringsfaser.

2. Vid tillämpning av punkt 1 ska betaltjänstleverantörerna säkerställa att alla följande krav uppfylls:

a) Personliga säkerhetsbehörighetsuppgifter maskeras när de visas och kan inte läsas i sin helhet när de anges av betaltjänstanvändaren under autentiseringen.

b) Personliga säkerhetsbehörighetsuppgifter i dataformat, samt kryptografiskt material som avser kryptering av de personliga säkerhetsbehörighetsuppgifterna, lagras inte i klartext.

c) Skydd finns mot icke auktoriserat utlämnande av hemligt kryptografiskt material.

3. Betaltjänstleverantörerna ska fullt ut dokumentera det förfarande som avser hantering av kryptografiskt material för kryptering eller för att på annat sätt göra de personliga säkerhetsbehörighetsuppgifterna oläsbara.

4. Betaltjänstleverantörerna ska säkerställa att hantering och dirigering (*routing*) av personliga säkerhetsbehörighetsuppgifter och av de autentiseringskoder som genererats i enlighet med kapitel II sker i säkra miljöer i enlighet med strikta och allmänt erkända branschstandarder.

Artikel 23

Skapande och överföring av säkerhetsbehörighetsuppgifter

Betaltjänstleverantörerna ska säkerställa att skapandet av personliga säkerhetsbehörighetsuppgifter sker i en säker miljö.

De ska minska riskerna för icke auktoriserad användning av personliga säkerhetsbehörighetsuppgifter och därpå följande användning av autentiseringsutrustning och programvara, stöld eller kopiering, innan de levereras till betalaren.

Artikel 24

Anknytning till betaltjänstanvändaren

1. Betaltjänstleverantörerna ska på ett säkert sätt säkerställa att endast betaltjänstanvändaren har anknytning till de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen och programvaran.

▼B

2. Vid tillämpning av punkt 1 ska betaltjänstleverantörerna säkerställa att alla följande krav uppfylls:

a) Anknytningen mellan betaltjänstanvändarens identitet och de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen och programvaran sker i en säker miljö på betaltjänstleverantörens ansvar, som minst ska omfatta betaltjänstanvändarens lokaler, den internetmiljö som betaltjänstleverantören tillhandahåller eller liknande säkra webbplatser som betaltjänstleverantören använder samt dess bankomattjänster, med beaktande av de risker som förknippas med sådan utrustning och sådana underliggande komponenter som använts under associeringsförfarandet som inte faller under betaltjänstleverantörens ansvar.

b) Anknytning på distans mellan betaltjänstanvändarens identitet och de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen och programvaran sker med hjälp av sträng kundautentisering.

Artikel 25

Leverans av säkerhetsbehörighetsuppgifter, autentiseringsutrustning och programvara

1. Betaltjänstleverantörerna ska säkerställa att leveransen av personliga säkerhetsbehörighetsuppgifter, autentiseringsutrustning och programvara till betaltjänstanvändaren sker på ett säkert sätt som är utformat för att hantera risker avseende icke auktoriserad användning till följd av att de förlorats, stulits eller kopierats.

2. Vid tillämpning av punkt 1 ska betaltjänstleverantörerna åtminstone tillämpa alla följande åtgärder:

a) Effektiva och säkra leveransmekanismer som säkerställer att de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen och programvaran levereras till rätt betaltjänstanvändare.

b) Mekanismer som gör det möjligt för betaltjänstleverantören att kontrollera autenticiteten på den autentiseringsprogramvara som levereras till betaltjänstanvändaren via internet.

c) Om leveransen av de personliga säkerhetsbehörighetsuppgifterna genomförs utanför betaltjänstleverantörens lokaler eller på distans, arrangemang som säkerställer att

   i) ingen icke auktoriserad part kan få tillgång till mer än en komponent av de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen eller programvaran, om dessa levereras via samma kanal,

   ii) aktivering av de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen eller programvaran krävs innan de kan börja användas.

▼B

d) Arrangemang som säkerställer att aktiveringen sker i en säker miljö i enlighethet med de associeringsförfaranden som avses i artikel 24 i fall då de personliga säkerhetsbehörighetsuppgifterna, autentiseringsutrustningen eller programvaran måste aktiveras innan de används för första gången.

Artikel 26

Förnyelse av personliga säkerhetsbehörighetsuppgifter

Betaltjänstleverantörerna ska säkerställa att förnyelse eller återaktivering av personliga säkerhetsbehörighetsuppgifter följer förfarandena för upprättande, anknytning och leverans av säkerhetsbehörighetsuppgifter och autentiseringsutrustning i enlighet med artiklarna 23, 24 och 25.

Artikel 27

Radering, avaktivering och återkallande

Betaltjänstleverantörerna ska säkerställa att de har effektiva förfaranden för att kunna genomföra alla följande säkerhetsåtgärder:

a) Säker radering, avaktivering eller återkallande av personliga säkerhetsbehörighetsuppgifter, autentiseringsutrustning och programvara.

b) Om betaltjänstleverantören distribuerar återanvändbar autentiseringsutrustning och programvara ska säker återanvändning av utrustning eller programvara vara inrättad, dokumenterad och genomförd innan den görs tillgänglig för andra betaltjänstanvändare.

c) Avaktivering eller återkallande av information som avser personliga säkerhetsbehörighetsuppgifter som lagras i betaltjänstleverantörens system och databaser och, i tillämpliga fall i offentliga transaktionsregister.

KAPITEL V

GEMENSAMMA OCH SÄKRA ÖPPNA KOMMUNIKATIONSSTANDARDER

Avsnitt 1

Allmänna krav beträffande kommunikation

Artikel 28

Krav för identifiering

1. Betaltjänstleverantörerna ska säkerställa säker identifiering vid kommunikation mellan betalarens utrustning och betalningsmottagarens godkännandeutrustning för elektroniska betalningar, inbegripet, men inte begränsat till, betalterminaler.

2. Betaltjänstleverantörerna ska säkerställa att risken att kommunikation felaktigt riktas till icke auktoriserade parter i mobilapplikationer och andra betaltjänstanvändargränssnitt som erbjuder elektronisk betalning effektivt minskas.

▼B

Artikel 29

Spårbarhet

1. Betaltjänstleverantörerna ska ha förfaranden för att säkerställa att alla betalningstransaktioner och annan interaktion med betaltjänstanvändaren, andra betaltjänstleverantörer och andra företag, inbegripet säljföretag, i fråga om tillhandahållande av betaltjänster är spårbara, och säkerställa att kunskap inhämtas i efterhand om alla relevanta händelser i alla skeden av den elektroniska transaktionen.

2. Vid tillämpning av punkt 1 ska betaltjänstleverantörerna säkerställa att alla kommunikationssessioner som upprättas med betaltjänstanvändaren, andra betaltjänstleverantörer och andra företag, inbegripet säljföretag, bygger på följande:

a) En unik identifieringskod för sessionen.

b) Säkerhetsmekanismer för detaljerad loggning av transaktionen, inbegripet transaktionsnummer, tidsstämplar och all relevant transaktionsdata.

c) Tidsstämplar som ska baseras på ett enhetligt tidsreferenssystem och som ska synkroniseras efter en officiell tidssignal.

Avsnitt 2

Särskilda krav för den gemensamma och säkra öppna kommunikationsstandarden

Artikel 30

Allmänna krav beträffande inloggningsgränssnitt

1. Kontoförvaltande betaltjänstleverantörer som erbjuder en betalare ett betakonto som finns tillgängligt online ska ha minst ett gränssnitt som uppfyller följande krav:

a) Leverantörer av kontoinformationstjänster, leverantörer av betalningsinitieringstjänster och betaltjänstleverantörer som ger ut kortbaserade betalningsinstrument har möjlighet att identifiera sig för den kontoförvaltande betaltjänstleverantören.

▼M2

b) Leverantörer av kontoinformationstjänster har möjlighet att på ett säkert sätt kommunicera för att begära och erhålla information om en eller flera specifika betalkonton och tillhörande betalningstransaktioner.

▼B

c) Leverantörer av betalningsinitieringstjänster har möjlighet att på ett säkert sätt kommunicera för att initiera ett betalningsuppdrag från betalarens betalkonto och erhålla all information om initieringen av betaltransaktioner och all information som finns tillgänglig för de kontoförvaltande betaltjänstleverantörerna avseende utförandet av betalningstransaktionen.

▼B

2. Vid autentisering av betaltjänstanvändaren ska leverantörerna av kontoinformationstjänster och leverantörerna av betalningsinitieringstjänster, med hjälp av det gränssnitt som avses i punkt 1, kunna förlita sig på alla de autentiseringsförfaranden som den kontoförvaltande betaltjänstleverantören tillhandahåller betaltjänstanvändaren.

Gränssnittet ska minst uppfylla samtliga följande krav:

a) En leverantör av betalningsinitieringstjänster eller en leverantör av kontoinformationstjänster ska kunna ge den kontoförvaltande betaltjänstleverantören instruktioner om att inleda autentiseringen på grundval av betaltjänstanvändarens godkännande.

b) Kommunikationssessioner mellan den berörda kontoförvaltande betaltjänstleverantören, leverantören av kontoinformationstjänster, leverantören av betalningsinitieringstjänster och betaltjänstanvändaren ska upprättas och underhållas genom autentiseringen.

c) Integriteten och konfidentialiteten hos de personliga säkerhetsbehörighetsuppgifter och autentiseringskoder som överförs av eller genom leverantören av betalningsinitieringstjänster eller leverantören av kontoinformationstjänster ska säkerställas.

3. De kontoförvaltande betaltjänstleverantörerna ska säkerställa att deras gränssnitt uppfyller de kommunikationsstandarder som utfärdats av internationella eller europeiska standardiseringsorganisationer.

De kontoförvaltande betaltjänstleverantörerna ska också säkerställa att de tekniska specifikationerna för alla gränssnitt dokumenteras och närmare beskriva en uppsättning rutiner, protokoll och verktyg som leverantörerna av betalningsinitieringstjänster, leverantörerna av kontoinformationstjänster och betaltjänstleverantörerna som ger ut kortbaserade betalningsinstrument behöver för att deras programvara och applikationer ska vara driftskompatibla med den kontoförvaltande betaltjänstleverantörens system.

De kontoförvaltande betaltjänstleverantörerna ska åtminstone – och senast sex månader före den tillämpningsdag som avses i artikel 38.2, eller före måldatumet för marknadslansering av inloggningsgränssnittet om lanseringen äger rum efter den dag som avses i artikel 38.2 – kostnadsfritt göra dokumentationen tillgänglig på begäran av auktoriserade leverantörer av betalningsinitieringstjänster, leverantörer av kontoinformationstjänster och betaltjänstleverantörer som ger ut kortbaserade betalningsinstrument eller leverantörer av betaltjänster som hos sina behöriga myndigheter har ansökt om relevant auktorisation, och ska göra en sammanfattning av dokumentationen allmänt tillgänglig på sina webbplatser.

▼B

4. ►M2 Utöver vad som anges i punkt 3 ska de kontoförvaltande betaltjänstleverantörerna – förutom i krissituationer – säkerställa att ändringar av de tekniska specifikationerna för deras gränssnitt, på förhand snarast möjligt och senast tre månader innan de genomförs, görs tillgängliga för auktoriserade leverantörer av betalningsinitieringstjänster, leverantörer av kontoinformationstjänster och betaltjänstleverantörer som ger ut kortbaserade betalningsinstrument, eller betaltjänstleverantörer som har ansökt hos sina behöriga myndigheter om relevant auktorisation. ◄

Betaltjänstleverantörerna ska dokumentera krissituationer då ändringar genomförts och på begäran ge behöriga myndigheter tillgång till denna dokumentation.

▼M1

4a. Med avvikelse från punkt 4 ska kontoförvaltande betaltjänstleverantörer ge de betaltjänstleverantörer som avses i denna artikel tillgång till de ändringar av de tekniska specifikationerna för deras gränssnitt som gjorts för att uppfylla kraven i artikel 10a minst 2 månader innan sådana ändringar genomförs.

▼B

5. De kontoförvaltande betaltjänstleverantörerna ska tillhandahålla en testfunktion, inklusive supporttjänster, för testning av förbindelser och funktioner, så att de auktoriserade leverantörerna av betalningsinitieringstjänster, betaltjänstleverantörer som ger ut kortbaserade betalningsinstrument och leverantörer av kontoinformationstjänster, eller betaltjänstleverantörer som har ansökt om relevant auktorisering, ska kunna testa den programvara och de applikationer som används för att erbjuda användarna en betaltjänst. Testfunktionen ska erbjudas senast sex månader före den tillämpningsdag som avses i artikel 38.2 eller före det måldatum för marknadslansering av inloggningsgränssnittet om lanseringen äger rum före den dag som avses i artikel 38.2.

Inga känsliga uppgifter får emellertid delas genom testfunktionen.

6. Behöriga myndigheter ska säkerställa att de kontoförvaltande betaltjänstleverantörerna alltid lever upp till de krav som ingår i dessa standarder i fråga om de gränssnitt som de inrättat. ►M2 Om en kontoförvaltande betaltjänstleverantör inte uppfyller de krav beträffande gränssnitt som fastställs i dessa standarder ska de behöriga myndigheterna säkerställa att tillhandahållandet av betalningsinitieringstjänster och kontoinformationstjänster inte hindras eller störs, i den utsträckning som respektive leverantör av sådana tjänster uppfyller villkoren i artikel 33.5. ◄

Artikel 31

Valmöjlighet beträffande inloggningsgränssnittet

▼M2

De kontoförvaltande betaltjänstleverantörerna ska fastställa de gränssnitt som avses i artikel 30 genom att antingen använda ett särskilt gränssnitt eller genom att låta de betaltjänstleverantörer som avses i artikel 30.1 använda sig av gränssnitten för autentisering av och kommunikation med den kontoförvaltande betaltjänstleverantörens betaltjänstanvändare.

▼B

Artikel 32

Skyldigheter beträffande särskilda gränssnitt

1. Under förutsättning att artiklarna 30 och 31 efterlevs ska kontoförvaltande betaltjänstleverantörer som infört ett särskilt gränssnitt säkerställa att detta särskilda gränssnitt alltid erbjuder likvärdig tillgänglighet och funktion, inklusive supporttjänster, som de gränssnitt som tillhandahålls betaltjänstanvändaren för direkt tillgång till dennes betalkonto online.

2. Kontoförvaltande betaltjänstleverantörer som har infört ett särskilt gränssnitt ska fastställa transparenta resultatindikatorer och servicenivåmål som är minst lika strikta som de som fastställts för det gränssnitt som används av deras betaltjänstanvändare, både när det gäller tillgänglighet och tillhandahållande av data i enlighet med artikel 36. Dessa gränssnitt, indikatorer och mål ska övervakas av de behöriga myndigheterna och stresstestas.

3. De kontoförvaltande betaltjänstleverantörer som har infört ett särskilt gränssnitt ska säkerställa att detta gränssnitt inte hindrar tillhandahållandet av betalningsinitierings- och kontoinformationstjänster. Sådana hinder kan bland annat vara att de betaltjänstleverantörer som avses i artikel 30.1 inte kan använda de säkerhetsbehörighetsuppgifter som de kontoförvaltande betaltjänstleverantörerna utfärdat för sina kunder, införande av omdirigeringar till den kontoförvaltande betaltjänstleverantörens autentisering eller andra funktioner, begäranden om ytterligare auktorisering och registrering utöver den som föreskriv i artiklarna 11, 14 och 15 i direktiv (EU) 2015/2366 eller begäranden av extrakontroller av det godkännande som betaltjänstanvändarna lämnat till leverantörer av betalningsinitierings- eller kontoinformationstjänster.

4. Vid tillämpning av punkterna 1 och 2 ska den kontoförvaltande betaltjänstleverantören övervaka det särskilda gränssnittets tillgänglighetet och prestanda. De kontoförvaltande betaltjänstleverantörerna ska på sina webbplatser publicera kvartalsstatistik över det särskilda gränssnittets tillgänglighet och prestanda och över det gränssnitt som används av deras betaltjänstanvändare.

Artikel 33

Beredskapsåtgärder för särskilda gränssnitt

1. De kontoförvaltande betaltjänstleverantörerna ska i det särskilda gränssnittet bygga in en strategi och planer för beredskapsåtgärder i händelse av att gränssnittets funktion inte uppfyller kraven i artikel 32, om gränssnittet utsätts för ett oplanerat driftsstopp eller om det inträffar en systemkollaps. Ett oplanerat driftsstopp eller en systemkollaps kan antas ha inträffat när fem på varandra följande begäranden om tillgång till information i syfte att tillhandahålla en betalningsinitieringstjänst eller kontoinformationstjänst inte besvaras inom 30 sekunder.

▼B

2. Beredskapsåtgärderna ska innehålla kommunikationsplaner för att informera betaltjänstleverantörer som använder sig av särskilda gränssnitt om åtgärder för att återställa systemet och en redogörelse för de omedelbart tillgängliga handlingsalternativ som betaltjänstleverantörerna har i ett sådant läge.

3. Såväl den kontoförvaltande betaltjänstleverantören som de betaltjänstleverantörer som avses i artikel 30.1 ska i enlighet med punkt 1 rapportera problem med särskilda gränssnitt till sina respektive behöriga myndigheter utan onödigt dröjsmål.

4. Som en del av beredskapsmekanismen ska de betaltjänstleverantörer som avses i artikel 30.1 ha möjlighet att använda de gränssnitt som tillhandahålls betaltjänstanvändaren för autentisering och kommunikation med deras kontoförvaltande betaltjänstleverantör, till dess att det särskilda gränssnittet är återställt till den grad av tillgänglighet och prestanda som föreskrivs i artikel 32.

5. I detta syfte ska de kontoförvaltande betaltjänstleverantörerna säkerställa att de betaltjänstleverantörer som avses i artikel 30.1 kan identifieras och att de kan förlita sig på de autentiseringsförfaranden som den kontoförvaltande betaltjänstleverantören tillhandahåller betaltjänstanvändaren. Om de betaltjänstleverantörer som avses i artikel 30.1 använder sig av det gränssnitt som avses i punkt 4 ska de

a) vidta nödvändiga åtgärder för att säkerställa att de inte kommer åt, lagrar eller använder uppgifter för andra syften än tillhandahållande av den tjänst som betaltjänstanvändaren efterfrågat,

b) fortsätta att efterleva skyldigheterna i artiklarna 66.3 respektive 67.2 i direktiv (EU) 2015/2366,

c) logga de uppgifter som de fått tillgång till genom det gränssnitt som den kontoförvaltande betaltjänstleverantören tillhandahåller betaltjänstanvändarna och, på begäran och utan onödigt dröjsmål, lämna loggfilerna till sina behöriga myndigheter,

d) för sina behöriga nationella myndigheter, på begäran och utan onödigt dröjsmål, vederbörligen motivera användningen av det gränssnitt som gjorts tillgängligt för betaltjänstanvändarna så att dessa ska kunna komma åt sina betalkonton online direkt,

e) vederbörligen informera den kontoförvaltande betaltjänstleverantören.

6. De behöriga myndigheterna ska, efter samråd med EBA för att säkerställa enhetlig tillämpning av följande villkor, undanta de kontoförvaltande betaltjänstleverantörer som har valt att använda ett särskilt gränssnitt, från skyldigheten att upprätta den beredskapsmekanism som beskrivs i punkt 4, förutsatt att det särskilda gränssnittet uppfyller alla följande villkor:

a) Det efterlever alla skyldigheter beträffande särskilda gränssnitt som fastställs i artikel 32.

▼B

b) Det har utformats och testats i enlighet med artikel 30.5 på ett tillfredsställande sätt för de betaltjänstleverantörer som avses däri.

c) Det har använts i stor utsträckning under minst tre månader av betaltjänstleverantörerna för kontoinformationstjänster, betalningsinitieringstjänster och för att bekräfta tillgängliga medel vid kortbaserade betalningar.

d) Eventuella problem som rör det särskilda gränssnittet har lösts utan onödigt dröjsmål.

7. Behöriga myndigheter ska återkalla det undantag som avses i punkt 6 om den kontoförvaltande betaltjänstleverantören inte uppfyller villkoren i a och d under mer en två på varandra följande kalenderveckor. Behöriga myndigheter ska informera EBA om detta återkallande och säkerställa att den kontoförvaltande betaltjänstleverantören, så snart som möjligt, dock senast inom två månader, inrättar den beredskapsmekanism som avses i punkt 4.

Artikel 34

Certifikat

1. För den identifiering som avses i artikel 30.1 a ska betaltjänstleverantörerna använda sig av kvalificerade certifikat för elektroniska stämplar, som avses i artikel 3.30 i förordning (EU) nr 910/2014 eller för autentisering av webbplatser, som avses i artikel 3.39 i den förordningen.

2. I den här förordningen ska det registreringsnummer som det hänvisas till i offentliga handlingar i enlighet med led c i bilaga III eller led c i bilaga IV till förordning (EU) nr 910/2014, vara auktoriseringsnumret för betaltjänstleverantören som ger ut kortbaserade betalningsinstrument, leverantörerna av kontoinformationstjänster, leverantörerna av betalningsinitieringstjänster, inbegripet kontoförvaltande betaltjänstleverantörer som tillhandahåller sådana tjänster, vilket finns tillgängligt i respektive medlemsstats offentliga register enligt artikel 14 i direktiv (EU) 2015/2366 eller som blir tillgängligt genom anmälan av varje auktorisation enligt artikel 8 i Europaparlamentets och rådets direktiv 2013/36/EU ([1]) i enlighet med artikel 20 i det direktivet.

3. I den här förordningen ska de kvalificerade certifikat för elektroniska stämplar eller för autentisering av webbplatser som avses i punkt 1, på ett språk som är brukligt i internationella finanskretsar, innefatta ytterligare särskilda egenskaper med avseende på följande:

([1]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

▼B

a) Betaltjänstleverantörens roll, som kan innefatta något av eller allt följande:

i) Kontoförvaltning.

ii) Betalningsinitiering.

iii) Kontoinformation.

iv) Utfärdande av kortbaserade betalningsinstrument.

b) Namnet på den behöriga myndighet hos vilken betaltjänstleverantören är registrerad.

4. De egenskaper som avses i punkt 3 ska inte påverka driftskompatibiliteten och erkännandet av kvalificerade certifikat för elektroniska stämplar eller för autentisering av webbplatser.

Artikel 35

Säkra kommunikationssessioner

1. I syfte att säkerställa uppgifternas konfidentialitet och integritet ska de kontoförvaltande betaltjänstleverantörerna, betaltjänstleverantörerna som ger ut kortbaserade betalningsinstrument, leverantörerna av kontoinformationstjänster och leverantörerna av betalningsinitieringstjänster, med hjälp av effektiva och allmänt erkända krypteringstekniker, säkerställa att säker kryptering tillämpas mellan de kommunicerande parterna under hela respektive kommunikationssession.

2. Betaltjänstleverantörerna som ger ut kortbaserade instrument, leverantörer av kontoinformationstjänster och leverantörerna av betalningsinitieringstjänster ska se till att den tillgång de får av de kontoförvaltande betaltjänstleverantörerna är så kortvarig som möjligt, och de ska aktivt avbryta sådan tillgång så snart den begärda åtgärden har slutförts.

3. Leverantörerna av kontoinformationstjänster och leverantörerna av betalningsinitieringstjänster ska under parallella nätverkssessioner med den kontoförvaltande betaltjänstleverantören säkerställa att dessa sessioner på ett säkert sätt är kopplade till relevanta sessioner med betaltjänstanvändaren, i syfte att förhindra att eventuella meddelanden eller uppgifter som överförs mellan dem skulle kunna feldirigeras.

4. Om leverantörer av kontoinformationstjänster, leverantörer av betalningsinitieringstjänster och betaltjänstleverantörer ger ut kortbaserade betalningsinstrument tillsammans med den kontoförvaltande betaltjänstleverantören ska otvetydiga hänvisningar till följande finnas:

a) Betaltjänstanvändaren eller betaltjänstanvändarna och tillhörande kommunikationssessioner, så att åtskillnad kan göras mellan flera begäranden från samma betaltjänstanvändare.

b) För betalningsinitieringstjänster, den unikt identifierade betalningstransaktion som initierats.

▼B

c) För bekräftelse av tillgängliga medel, den unikt identifierade begäran avseende det belopp som krävs för att den kortbaserade transaktionen ska kunna utföras.

5. De kontoförvaltande betaltjänstleverantörerna, leverantörerna av kontoinformationstjänster, leverantörerna av betalningsinitieringstjänster och de betaltjänstleverantörer som ger ut kortbaserade betalningsinstrument ska om de överför personliga säkerhetsbehörighetsuppgifter och autentiseringskoder, säkerställa att dessa vid ingen tidpunkt är läsbara, varken direkt eller indirekt eller för personalen.

Om de personliga säkerhetsbehörighetsuppgifterna förlorar sin konfidentialitet under dessa leverantörers ansvar ska de utan onödigt dröjsmål informera de betaltjänstanvändare som de är associerade med samt den som har utfärdat de personliga säkerhetsbehörighetsuppgifterna.

Artikel 36

Utbyte av uppgifter

1. De kontoförvaltande betaltjänstleverantörerna ska uppfylla följande krav:

a) De ska förse leverantörerna av kontoinformationstjänster med samma information från specifika betalkonton och tillhörande betalningstransaktioner som tillhandahållits betaltjänstanvändaren vid direkt begäran om tillgång till kontoinformation, under förutsättning att denna information inte innehåller känsliga uppgifter.

b) De ska omedelbart efter mottagande av betalningsuppdraget förse leverantörer av betalningsinitieringstjänster med samma information om initiering och utförande av betalningstransaktionen som lämnats eller tillgängliggjorts för betaltjänstanvändaren när denne direkt initierat transaktionen.

c) De ska på begäran omedelbart förse betaltjänstleverantörerna med en bekräftelse i ett enkelt ja eller nej-format om huruvida det belopp som krävs för att utföra betalningstransaktionen är tillgängligt på betalarens betalkonto.

2. Om en oväntad händelse eller ett fel inträffar under identifierings-, eller autentiseringsprocessen, eller vid utbyte av dataelement, ska den kontoförvaltande betaltjänstleverantören sända ett meddelande till leverantören av betalningsinitieringstjänster eller leverantören av kontoinformationstjänster och den betaltjänstleverantör som ger ut kortbaserade instrument där orsakerna till den oväntade händelsen eller felet förklaras.

▼M2

Om den kontoförvaltande betaltjänstleverantören erbjuder ett särskilt gränssnitt i enlighet med artikel 32 ska gränssnittet se till att meddelanden om oförutsedda händelser eller fel kan kommuniceras av alla betaltjänstleverantörer som upptäcker händelsen eller felet till andra betaltjänstleverantörer som deltar i kommunikationssessionen.

▼B

3. Leverantörerna av kontoinformationstjänster ska ha inrättat lämpliga och ändamålsenliga mekanismer för att förhindra åtkomst till annan information än från specifika betalkonton och tillhörande betalningstransaktioner, i enlighet med användarens uttryckliga godkännande.

4. Leverantörer av betalningsinitieringstjänster ska förse kontoförvaltande betaltjänstleverantörer med samma information som begärs från betaltjänstanvändaren vid direkt initiering av betalningstransaktionen.

5. Leverantörer av kontoinformationstjänster ska ha tillgång till information från specifika betalkonton och tillhörande betalningstransaktioner som innehas av kontoförvaltande betaltjänstleverantörer i syfte att utföra kontoinformationstjänsten under någon av följande omständigheter:

a) När betaltjänstanvändaren aktivt begär sådan information.

▼M2

b) Om betaltjänstanvändaren inte aktivt begär informationen, högst fyra gånger under en 24-timmarsperiod, såvida inte fler tillfällen överenskommits mellan leverantören av kontoinformationstjänster och den kontoförvaltande betaltjänstleverantören, med betaltjänstanvändarens godkännande.

▼B

KAPITEL VI

SLUTBESTÄMMELSER

Artikel 37

Översyn

Utan att det påverkar tillämpningen av artikel 98.5 i direktiv (EU) 2015/2366 ska EBA senast 14 mars 2021 se över de bedrägerifrekvenser som avses i bilagan till denna förordning samt de undantag som beviljats enligt artikel 33.6 avseende särskilda gränssnitt och, om så är lämpligt, lägga fram förslag till uppdateringar av dessa för kommissionen i enlighet med artikel 10 i förordning (EU) nr 1093/2010.

Artikel 38

Ikraftträdande

1. Denna förordning träder i kraft dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Denna förordning ska tillämpas från och med 14 september 2019.

3. Artikel 30.3 och 30.5 ska dock tillämpas 14 mars 2019.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

▼B

BILAGA

	Bedrägerifrekvens som fastställts som referens (%) för:	
Tröskelvärde för undantag	Elektroniska kortbaserade betalningar på distans	Elektronisk kreditöverföring på distans
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015