KOMMISSIONENS DELEGEREDE FORORDNING (EU) 2018/389

af 27. november 2017

om supplerende regler til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 for så vidt angår reguleringsmæssige tekniske standarder for stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF ([1]), særlig artikel 98, stk. 4, og

ud fra følgende betragtninger:

(1) Betalingstjenester, der udbydes elektronisk, bør gennemføres på sikker vis ved hjælp af teknologier, der garanterer sikker autentifikation af brugeren og begrænser risikoen for svig mest muligt. Autentifikationsproceduren bør generelt omfatte transaktionsovervågningsmekanismer, som kan afsløre forsøg på at gøre brug af en betalingstjenestebrugers tabte, stjålne eller uberettiget tilegnede personaliserede sikkerhedsoplysninger, og bør også sikre, at betalingstjenestebrugeren er den retmæssige bruger, som derfor giver sit samtykke til overførslen af midler og adgang til sine kontooplysninger ved normal brug af de personaliserede sikkerhedsoplysninger. Det er endvidere nødvendigt at præcisere de krav om stærk kundeautentifikation, der bør stilles, hver gang en betaler tilgår sin betalingskonto online, initierer en elektronisk betalingstransaktion eller udfører en handling gennem en fjernkanal, der kan indebære risiko for betalingssvig eller andre former for misbrug, og som indebærer generering af en autentifikationskode, der bør være modstandsdygtig over for risikoen for at blive forfalsket i sin helhed eller for visning af de elementer, som ligger til grund for kodens generering.

(2) De metoder, der anvendes til at begå svig, ændrer sig konstant, og derfor bør kravene om stærk kundeautentifikation give mulighed for innovation for så vidt angår de tekniske løsninger, der tager højde for nye trusler mod sikre elektroniske betalinger. For at sikre, at de krav, der skal indføres, til stadighed opfyldes effektivt, bør det endvidere påkræves, at sikkerhedsforanstaltningerne ved anvendelse af stærk kundeautentifikation og undtagelserne i forhold hertil, foranstaltningerne til beskyttelse af de personaliserede sikkerhedsoplysningers fortrolighed og integritet og foranstaltningerne til indførelse af fælles og sikre åbne standarder for kommunikation dokumenteres, regelmæssigt testes, evalueres og revideres af revisorer med speciale i IT-sikkerhed og -betalinger, som er operationelt uafhængige. For at give kompetente myndigheder mulighed for at overvåge kvaliteten af den revision, som foretages af disse foranstaltninger, bør sådanne revisioner stilles til rådighed for dem efter anmodning.

(3) Elektroniske fjernbetalingstransaktioner indebærer en større risiko for svig, og derfor er det nødvendigt at stille yderligere krav om stærk kundeautentifikation i forbindelse med sådanne transaktioner og sikre, at elementerne dynamisk knytter transaktionen til et beløb og en betalingsmodtager, som betaleren specificerer, når transaktionen initieres.

(4) Dynamisk tilknytning sker ved generering af autentifikationskoder, som skal opfylde et sæt strenge sikkerhedskrav. For at sikre teknologisk neutralitet bør der ikke stilles krav om en specifik teknologi til gennemførelse af autentifikationskoder. Derfor bør autentifikationskoder baseres på løsninger som f. eks. generering og validering af engangsadgangskoder, digitale underskrifter eller andre kryptografisk underbyggede validitetsudsagn, som bruger nøgler eller kryptografisk materiale lagret i autentifikationselementerne, forudsat at sikkerhedskravene opfyldes.

([1]) EUT L 337 af 23.12.2015, s. 35.

(5) Det er nødvendigt at stille specifikke krav med henblik på den situation, hvor det endelige beløb ikke er kendt på det tidspunkt, hvor betaleren initierer en elektronisk fjernbetalingstransaktion, for at sikre, at den stærke kundeautentifikation er specifik for det maksimumsbeløb, som betaleren har givet sit samtykke til, jf. direktiv (EU) 2015/2366.

(6) For at sikre anvendelsen af stærk kundeautentifikation er det også nødvendigt at stille passende sikkerhedskrav til de elementer af stærk kundeautentifikation, der karakteriseres som viden (noget, som kun brugeren ved), f.eks. længde eller kompleksitet, til de elementer, der karakteriseres som besiddelse (noget, som kun brugeren besidder), f.eks. algoritmespecifikationer, nøglelængde og entropi, og til anordninger og software, som læser elementer, der karakteriseres som iboende egenskab (noget, som brugeren er), f.eks. algoritmespecifikationer, biometrisk sensor og modelbeskyttelse, navnlig med henblik på at afbøde risikoen for, at nævnte elementer afdækkes af, vises til eller bruges af uautoriserede parter. Det er også nødvendigt at stille krav, som skal sikre, at nævnte elementer er uafhængige, således at brud på et af dem ikke svækker de andres pålidelighed, navnlig hvis disse elementer anvendes gennem en multifunktionel anordning, dvs. en anordning som f.eks. en tablet eller en mobiltelefon, der både kan anvendes til at give instruks om at foretage betalingen og i forbindelse med autentifikationsprocessen.

(7) Kravene om stærk kundeautentifikation finder anvendelse på betalinger, som betaleren initierer, uanset om betaleren er en fysisk eller en juridisk person.

(8) Betalinger, som foretages gennem anonyme betalingsinstrumenter, er i sagens natur ikke omfattet af kravet om stærk kundeautentifikation. Hvis sådanne instrumenters anonymitet fjernes af kontraktmæssige eller juriske grunde, er betalingerne omfattet af de sikkerhedskrav, som følger af direktiv (EU) 2015/2366 og denne reguleringsmæssige tekniske standard.

(9) Undtagelserne fra princippet om stærk kundeautentifikation er i overensstemmelse med direktiv (EU) 2015/2366 blevet defineret på grundlag af risikoniveauet, beløbet, den tilbagevendende karakter og den betalingskanal, der anvendes til at gennemføre betalingstransaktionen.

(10) Handlinger, som indebærer adgang til saldoen eller de seneste transaktioner på en betalingskonto uden visning af følsomme betalingsdata, tilbagevendende betalinger, som tidligere er oprettet og bekræftet af betaleren ved brug af stærk kundeautentifikation, til de samme betalingsmodtagere, og betalinger til og fra den samme fysiske eller juridiske person med konti hos den samme betalingstjenesteudbyder, udgør en begrænset risiko og giver således betalingstjenesteudbydere mulighed for at undlade at anvende stærk kundeautentifikation. Her ses der bort fra, at i henhold til artikel 65, 66 og 67 i direktiv (EU) 2015/2366 bør betalingsinitieringstjenesteudbydere, betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, og kontooplysningstjenesteudbydere kun anmode om og indhente de oplysninger fra den kontoførende betalingstjenesteudbyder, som er nødvendige og væsentlige for at kunne levere en given betalingstjeneste med betalingstjenestebrugerens samtykke. Et sådant samtykke kan gives individuelt for hver anmodning om oplysninger og for hver betaling, der skal initieres, eller til kontooplysningstjenesteudbydere som et mandat i forbindelse med angivne betalingskonti og dertil knyttede betalingstransaktioner som fastlagt i den kontraktmæssige aftale med betalingstjenestebrugeren.

(11) Undtagelser for mindre kontaktløse betalinger på salgssteder, hvor der også tages højde for et maksimalt antal konsekutive transaktioner eller et bestemt fast maksimumsbeløb for konsekutive transaktioner uden anvendelse af stærk kundeautentifikation, giver mulighed for at udvikle brugervenlige betalingstjenester, som indebærer en lav risiko, og bør derfor også tages i betragtning. Der bør også indføres en undtagelse for elektroniske betalingstransaktioner, der initieres i ubemandede betalingsterminaler, hvor det af operationelle grunde muligvis ikke altid er let at anvende stærk kundeautentifikation (f.eks. for at undgå køer og potentielle uheld ved betalingsstationer eller andre risici for sikkerheden).

(12) Her er det ligesom i forbindelse med undtagelsen for mindre kontaktløse betalinger på salgsstedet nødvendigt at finde en passende balance mellem interessen i øget sikkerhed for fjernbetalinger og behovet for brugervenlighed og adgang til betalinger inden for e-handel. I overensstemmelse med nævnte principper bør de tærskelværdier, hvorunder det ikke er nødvendigt at anvende stærk kundeautentifikation, fastsættes på forsigtig vis, således at de kun omfatter mindre onlinekøb. Tærskelværdierne for onlinekøb bør fastsættes på mere forsigtig vis, idet personen ikke er fysisk til stede, når købet foretages, hvilket indebærer en lidt større risiko for sikkerheden.

(13) Kravene om stærk kundeautentifikation finder anvendelse på betalinger, som betaleren initierer, uanset om betaleren er en fysisk eller en juridisk person. Mange erhvervsrelaterede betalinger initieres gennem dedikerede processer eller protokoller, som garanterer de høje grader af sikkerhed for betalinger, som direktiv (EU) 2015/2366 tager sigte på at opnå gennem stærk kundeautentifikation. Hvis de kompetente myndigheder konstaterer, at nævnte betalingsprocesser og -protokoller, der kun stilles til rådighed for betalere, som ikke er forbrugere, er i overensstemmelse med målsætningerne i direktiv (EU) 2015/2366 for så vidt angår sikkerhed, kan betalingstjenesteudbydere indrømmes undtagelse fra kravene om stærk kundeautentifikation i forhold til nævnte processer eller protokoller.

(14) Der bør også indføres en undtagelse for betalingstjenesteudbydere, som ikke har til hensigt at anvende stærk kundeautentifikation, hvis en realtidsanalyse af transaktionsrisici kategoriserer en betalingstransaktion som en transaktion, der indebærer en lav risiko, idet der stilles effektive og risikobaserede krav, som sikrer betalingstjenestebrugerens midler og personoplysninger. Nævnte risikobaserede krav bør kombinere resultaterne af risikoanalysen, idet det bekræftes, at der ikke er konstateret unormale udgifts- eller adfærdsmønstre for betaleren under hensyntagen til andre risikofaktorer, herunder oplysninger om betalerens og betalingsmodtagerens opholdssted, med beløbsmæssige tærskelværdier baseret på de procentsatser for svig, der er beregnet for fjernbetalinger. Hvis en betaling på grundlag af realtidsanalysen af transaktionsrisici ikke kan kategoriseres som en transaktion, der indebærer en lav risiko, bør betalingstjenesteudbyderen på ny anvende stærk kundeautentifikation. Maksimumsbeløbet for en sådan risikobaseret undtagelse bør fastsættes således, at det sikrer en meget lav tilsvarende procentsats for svig, også set i forhold til procentsatserne for svig for alle betalingstjenesteudbyderens betalingstransaktioner, herunder dem, der er autentificeret gennem stærk kundeautentifikation, inden for en bestemt tidsperiode og på rullende basis.

(15) Betalingstjenesteudbydere, som ønsker at drage fordel af undtagelserne fra stærk kundeautentifikation, bør med henblik på effektiv håndhævelse regelmæssigt for hver betalingstransaktionstype overvåge værdien af svigagtige eller uautoriserede betalingstransaktioner og de konstaterede procentsatser for svig for alle deres betalingstransaktioner, uanset om de er autentificeret gennem stærk kundeautentifikation eller gennemført i henhold til en relevant undtagelse, og efter anmodning stille disse oplysninger til rådighed for de kompetente myndigheder og for Den Europæiske Banktilsynsmyndighed (EBA).

(16) Indsamlingen af dette nye historiske belæg for procentsatserne for svig i forbindelse med elektroniske betalingstransaktioner vil også bidrage til EBA's effektive gennemgang af tærskelværdierne for en undtagelse fra stærk kundeautentifikation baseret på en realtidsanalyse af transaktionsrisici. EBA bør gennemgå disse reguleringsmæssige tekniske standarder og om nødvendigt forelægge udkast til ajourføringer heraf for Kommissionen med nye udkast til tærskelværdier og tilsvarende procentsatser for svig med henblik på at øge sikkerheden for elektroniske fjernbetalinger i overensstemmelse med artikel 98, stk. 5, i direktiv (EU) 2015/2366 og artikel 10 i Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([1]).

(17) Betalingstjenesteudbydere, som gør brug af de undtagelser, der skal tages i betragtning, bør til enhver tid have mulighed for at anvende stærk kundeautentifikation i forbindelse med de handlinger og de betalingstransaktioner, der er omhandlet i nævnte bestemmelser.

(18) De foranstaltninger, der beskytter personaliserede sikkerhedsoplysningers fortrolighed og integritet, samt autentifikationsanordninger og software bør begrænse risici for svig i forbindelse med uautoriseret eller svigagtig brug af betalingsinstrumenter og uautoriseret adgang til betalingskonti. Derfor er det nødvendigt at stille krav om sikker oprettelse og levering af personaliserede sikkerhedsoplysninger og sammenkædning heraf med betalingstjenestebrugeren og at stille betingelser om fornyelse og deaktivering af nævnte oplysninger.

(19) For at garantere effektiv og sikker kommunikation mellem de relevante aktører i forbindelse med kontooplysningstjenester, betalingsinitieringstjenester og bekræftelse af midlers tilgængelighed er det nødvendigt at præcisere de krav til fælles og åbne kommunikationsstandarder, som alle relevante betalingstjenesteudbydere skal opfylde. Direktiv (EU) 2015/2366 omhandler kontooplysningstjenesteudbyderes adgang til og brug af betalingskontooplysninger. Denne forordning indebærer derfor ikke ændringer af reglerne om adgang til andre konti end betalingskonti.

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

(20) Kontoførende betalingstjenesteudbydere med betalingskonti, som er tilgængelige online, bør mindst stille et adgangsinterface til rådighed, som muliggør sikker kommunikation med kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter. Interfacet bør gøre det muligt for kontooplysningstjenesteudbyderne, betalingsinitieringstjenesteudbyderne og de betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, at identificere sig over for den kontoførende betalingstjenesteudbyder. Det bør også gøre det muligt for kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere at anvende de autentifikationsprocedurer, som den kontoførende betalingstjenesteudbyder stiller til rådighed for betalingstjenestebrugeren. For at sikre teknologi- og forretningsmodelneutralitet bør det stå de kontoførende betalingstjenesteudbydere frit at bestemme, om de vil stille et interface til rådighed, som er dedikeret til kommunikation med kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, eller om de for så vidt angår nævnte kommunikation vil give mulighed for, at interfacet anvendes til identifikation og kommunikation med de kontoførende betalingstjenesteudbyderes betalingstjenestebrugere.

(21) For gøre det muligt for kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, at videreudvikle deres tekniske løsninger bør den tekniske specifikation for interfacet dokumenteres behørigt og offentliggøres. Endvidere bør den kontoførende betalingstjenesteudbyder stille en facilitet til rådighed, som gør det muligt for betalingstjenesteudbyderne at teste de tekniske løsninger mindst seks måneder forud for disse reguleringsmæssige standarders anvendelsesdato, eller, hvis lanceringen finder sted efter disse standarders anvendelsesdato, forud for den dato, hvor interfacet lanceres på markedet. For at sikre interoperabilitet mellem forskellige teknologiske kommunikationsløsninger bør interfacet anvende kommunikationsstandarder, som er udviklet af internationale eller europæiske standardiseringsorganer.

(22) Kvaliteten af de tjenester, som kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere leverer, afhænger af, om de interface, som er taget i brug eller tilpasset af kontoførende betalingstjenesteudbydere, fungerer korrekt. Det er derfor vigtigt, at der træffes foranstaltninger med henblik på tilfælde, hvor sådanne interface ikke er i overensstemmelse med bestemmelserne i disse standarder, for at sikre forretningskontinuitet for brugerne af nævnte tjenester. Det påhviler de nationale kompetente myndigheder at sikre, at kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere hverken udsættes for blokering eller hindringer i forbindelse med leveringen af deres tjenester.

(23) Hvis der tilbydes adgang til betalingskonti gennem et dedikeret interface, er det nødvendigt at stille krav om, at dedikerede interface har samme tilgængelighed og ydeevne som det interface, der stilles til rådighed for betalingstjenestebrugeren, for at sikre betalingstjenestebrugeres ret til at gøre brug af betalingsinitieringsudbydere og tjenester, som giver adgang til kontooplysninger, jf. direktiv (EU) 2015/2366. Kontoførende betalingstjenesteudbydere bør også definere gennemsigtige nøgleresultatindikatorer og serviceniveaumål for dedikerede interfaces tilgængelighed og ydeevne, som er mindst lige så omfattende som dem, der er fastsat for det interface, som deres betalingstjenestebrugere anvender. De nævnte interface bør testes af de betalingstjenesteudbyderne, som har til hensigt at anvende dem, og bør gøres til genstand for stresstest og overvåges af kompetente myndigheder.

(24) For at sikre, at betalingstjenesteudbydere, som anvender et dedikeret interface, fortsat kan levere deres tjenester i tilfælde af problemer med tilgængelighed eller utilstrækkelig ydeevne, er det nødvendigt på strenge betingelser at stille en alternativ mekanisme til rådighed, som gør det muligt for sådanne udbydere at anvende det interface, som den kontoførende betalingstjenesteudbyder opretholder til at identificere og kommunikere med sine egne betalingstjenestebrugere. Visse kontoførende betalingstjenesteudbydere vil blive indrømmet undtagelse fra bestemmelsen om at skulle stille en sådan alternativ mekanisme til rådighed gennem deres kunderelaterede interface, hvis de kompetente myndigheder konstaterer, at de dedikerede interface opfylder særlige betingelser, som sikrer uhindret konkurrence. Hvis de dedikerede interface, som er omfattet af undtagelsen, ikke opfylder de krævede betingelser, tilbagekalder de relevante kompetente myndigheder de indrømmede undtagelser.

(25) For at gøre det muligt for de kompetente myndigheder effektivt at føre tilsyn med og overvåge kommunikationsinterfacenes gennemførelse og forvaltning bør de kontoførende betalingstjenesteudbydere offentliggøre et sammendrag af den relevante dokumentation på deres websted og efter anmodning stille dokumentation om nødløsninger til rådighed for de kompetente myndigheder. De kontoførende betalingstjenesteudbydere bør også offentliggøre statistikker om nævnte interfaces tilgængelighed og ydeevne.

(26) For at sikre dataenes fortrolighed og integritet er det nødvendigt at garantere sikre kommunikationssessioner mellem kontoførende betalingstjenesteudbydere, kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter. Det er navnlig

nødvendigt at kræve, at der anvendes sikker kryptering mellem kontooplysningstjenesteudbydere, betalingsinitieringsudbydere, betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, og kontoførende betalingstjenesteudbydere ved udveksling af data.

(27) For at styrke brugernes tillid og sikre stærk kundeautentifikation bør der tages hensyn til brug af elektroniske identifikationsmidler og tillidstjenester som omhandlet i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([1]), navnlig for så vidt angår anmeldte elektroniske identifikationsordninger.

(28) For at sikre indbyrdes afstemte anvendelsesdatoer bør denne forordning anvendes fra den samme dato som den dato, hvorfra medlemsstaterne skal sikre, at de i artikel 65, 66, 67 og 97 i direktiv (EU) 2015/2366 omhandlede sikkerhedsforanstaltninger finder anvendelse.

(29) Denne forordning er baseret på det udkast til reguleringsmæssige tekniske standarder, som Den Europæiske Banktilsynsmyndighed (EBA) har forelagt Kommissionen.

(30) EBA har afholdt åbne og gennemsigtige offentlige høringer om det udkast til reguleringsmæssige tekniske standarder, som ligger til grund for denne forordning, analyseret de potentielle omkostninger og fordele samt anmodet interessentgruppen for banker, der er nedsat i henhold artikel 37 i forordning (EU) nr. 1093/2010, om en udtalelse —

VEDTAGET DENNE FORORDNING:

KAPITEL I

GENERELLE BESTEMMELSER

Artikel 1

Genstand

Ved denne forordning indføres der krav, som betalingstjenesteudbydere skal opfylde med henblik på at gennemføre sikkerhedsforanstaltninger, som sætter dem i stand til at:

a) anvende proceduren for stærk kundeautentifikation i overensstemmelse med artikel 97 i direktiv (EU) 2015/2366

b) undlade at anvende sikkerhedskravene om stærk kundeautentifikation på særlige og begrænsede betingelser, der er baseret på risikoniveauet, betalingstransaktionens beløb og tilbagevendende karakter samt den betalingskanal, der anvendes til at gennemføre transaktionen

c) beskytte fortroligheden og integriteten af betalingstjenestebrugeres personaliserede sikkerhedsoplysninger

d) indføre fælles og sikre åbne standarder for kommunikation mellem kontoførende betalingstjenesteudbydere, betalingsinitieringstjenesteudbydere, kontooplysningstjenesteudbydere, betalere, betalingsmodtagere og andre betalingstjenesteudbydere i forbindelse med levering og brug af betalingstjenester, jf. afsnit IV i direktiv (EU) 2015/2366.

Artikel 2

Generelle autentifikationskrav

1. Betalingstjenesteudbydere skal råde over transaktionsovervågningsmekanismer, som sætter dem i stand til at afsløre uautoriserede eller svigagtige betalingstransaktioner med henblik på at gennemføre de sikkerhedsforanstaltninger, der er omhandlet i artikel 1, litra a) og b).

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 53).

Disse mekanismer skal være baseret på en analyse af betalingstransaktioner under hensyntagen til elementer, som er typiske for betalingstjenestebrugere i forbindelse med normal brug af personaliserede sikkerhedsoplysninger.

2. Betalingstjenesteudbydere skal sikre, at transaktionsovervågningsmekanismen som et minimum tager højde for hver af følgende risikobaserede faktorer:

a) lister over svækkede eller stjålne autentifikationselementer

b) de enkelte betalingstransaktionsbeløb

c) kendte scenarier for svig i forbindelse med udbud af betalingstjenester

d) tegn på malware-infektion i autentifikationsprocedurens sessioner

e) hvis betalingstjenesteudbyderen stiller adgangsanordning eller software til rådighed, en log over brugen af den adgangsanordning eller det software, som er stillet til rådighed for betalingstjenestebrugeren, og unormal brug af adgangsanordning eller software.

Artikel 3

Gennemgang af sikkerhedsforanstaltningerne

1. Gennemførelsen af de sikkerhedsforanstaltninger, der er omhandlet i artikel 1, skal dokumenteres, regelmæssigt testes, evalueres og revideres i overensstemmelse med de gældende rammebestemmelser for betalingstjenesteudbyderen af revisorer med ekspertise inden for IT-sikkerhed og -betalinger, som er operationelt uafhængige inden for eller af betalingstjenesteudbyderen.

2. Perioden mellem de revisioner, der er omhandlet i stk. 1, fastsættes under hensyntagen til de relevante rammebestemmelser om regnskaber og lovpligtig revision, der finder anvendelse på betalingstjenesteudbyderen.

Betalingstjenesteudbydere, som benytter den undtagelse, der er omhandlet i artikel 18, gøres dog som et minimum på årsbasis til genstand for en revision af metode, model og indberettede procentsatser for svig. De revisorer, som foretager denne revision, skal have ekspertise inden for IT-sikkerhed og -betalinger og være operationelt uafhængige inden for eller af betalingstjenesteudbyderen. I det første år, hvor der gøres brug af den undtagelse, der er omhandlet i artikel 18, og mindst hver tredje år derefter, eller oftere efter den kompetente myndigheds anmodning, skal denne revision foretages af en uafhængig og kvalificeret ekstern revisor.

3. Denne revision skal føre til en evaluering af og en rapport om, hvorvidt betalingstjenesteudbyderens sikkerhedsforanstaltninger opfylder de krav, der er omhandlet i denne forordning.

Hele rapporten stilles efter anmodning til rådighed for de kompetente myndigheder.

KAPITEL II

SIKKERHEDSFORANSTALTNINGER I FORBINDELSE MED ANVENDELSE AF STÆRK KUNDEAUTENTIFIKATION

Artikel 4

Autentifikationskode

1. Hvis betalingstjenesteudbydere anvender stærk kundeautentifikation i overensstemmelse med artikel 97, stk. 1, i direktiv (EU) 2015/2366, skal autentifikationen være baseret på to eller flere elementer, der karakteriseres som viden, besiddelse og iboende egenskab, og skal føre til generering af en autentifikationskode.

Autentifikationskoden accepteres kun én gang af betalingstjenesteudbyderen, når betaleren anvender autentifikationskoden til at tilgå sin betalingskonto online, til at initiere en elektronisk betalingstransaktion eller til at udføre en handling gennem en fjernkanal, der kan indebære risiko for betalingssvig eller andre former for misbrug.

2. Betalingstjenesteudbydere træffer med henblik på stk. 1 sikkerhedsforanstaltninger, som garanterer, at følgende krav opfyldes:

a) oplysninger om de elementer, der er omhandlet i stk. 1, kan ikke udledes ved visning af autentifikationskoden

b) en ny autentifikationskode kan ikke genereres baseret på kendskab til andre tidligere genererede autentifikationskoder

c) autentifikationskoden kan ikke forfalskes.

3. Betalingstjenesteudbydere sikrer, at autentifikation ved generering af en autentifikationskode omfatter følgende foranstaltninger:

a) hvis autentifikation med henblik på fjernadgang, elektroniske fjernbetalinger og andre handlinger gennem en fjernkanal, der kan indebære risiko for betalingssvig eller andre former for misbrug, ikke har genereret en autentifikationskode med henblik på stk. 1, må det ikke være muligt at identificere, hvilket af de i stk. 1 omhandlede elementer der ikke var korrekt

b) det antal mislykkede forsøg på autentifikation, der kan finde sted konsekutivt, inden de handlinger, der er omhandlet i artikel 97, stk. 1, i direktiv (EU) 2015/2366, blokeres midlertidigt eller permanent, må ikke overstige fem i en given tidsperiode

c) kommunikationssessioner beskyttes mod fangst af autentifikationsdata fremsendt i forbindelse med autentifikation og mod uautoriserede parters manipulation i overensstemmelse med kravene i kapitel V

d) det tidsrum uden aktivitet fra betalerens side, der højst må forløbe, efter at betaleren er autentificeret med henblik tilgang til sin betalingskonto online, er på fem minutter.

4. Hvis den blokering, der er omhandlet i stk. 3, litra b), er midlertidig, fastsættes varigheden af nævnte blokering og antallet af nye forsøg på grundlag af kendetegnene ved den tjeneste, der ydes betaleren, og alle de relevante involverede risici under hensyntagen til som et minimum de faktorer, der er omhandlet i artikel 2, stk. 2.

Betaleren advares, inden blokeringen gøres permanent.

Hvis blokeringen er blevet gjort permanent, indføres der en sikker procedure, som giver betaleren mulighed for på ny at anvende de blokerede elektroniske betalingsinstrumenter.

Artikel 5

Dynamisk tilknytning

1. Hvis betalingstjenesteudbydere anvender stærk kundeautentifikation i overensstemmelse med artikel 97, stk. 2, i direktiv (EU) 2015/2366, træffer de i tillæg til de krav, der er omhandlet i denne forordnings artikel 4, også sikkerhedsforanstaltninger, som opfylder følgende krav:

a) betaleren gøres opmærksom på betalingstransaktionsbeløbet og på betalingsmodtageren

b) den genererede autentifikationskode er specifik for det betalingstransaktionsbeløb og den modtager, som betaleren godkendte, da transaktionen blev initieret

c) den autentifikationskode, som betalingstjenesteudbyderen har godkendt, svarer til det oprindelige specifikke betalingstransaktionsbeløb og til identiteten af den betalingsmodtager, som betaleren har godkendt

d) enhver ændring af beløbet eller betalingsmodtageren medfører, at den genererede autentifikationskode bliver ugyldig.

2. Betalingstjenesteudbydere træffer med henblik på stk. 1 sikkerhedsforanstaltninger, som garanterer fortroligheden, ægtheden og integriteten af hvert af følgende:

a) transaktionsbeløbet og betalingsmodtageren i alle autentifikationsfaserne

b) de oplysninger, som vises betaleren i alle autentifikationsfaserne, herunder generering, fremsendelse og brug af autentifikationskoden.

3. Hvis betalingstjenesteudbydere anvender stærk kundeautentifikation i overensstemmelse med artikel 97, stk. 2, i direktiv (EU) 2015/2366, stilles der med henblik på stk. 1, litra b), følgende krav til autentifikationskoden:

a) hvis betaleren i forbindelse med en kortbaseret betalingstransaktion har givet sit samtykke til det præcise beløb, der skal blokeres i henhold til nævnte direktivs artikel 75, stk. 1, skal autentifikationskoden være specifik for det beløb, som betaleren har givet sit samtykke til at blokere, og som betaleren godkendte, da transaktionen blev initieret

b) hvis betaleren i forbindelse med betalingstransaktioner har givet sit samtykke til gennemførelse af en batch af elektroniske fjernbetalingstransaktioner til en eller flere betalingsmodtagere, skal autentifikationskoden være specifik for det samlede beløb af betalingstransaktionsbatchen og for de specificerede betalingsmodtagere.

Artikel 6

Krav til de elementer, der karakteriseres som viden

1. Betalingstjenesteudbydere træffer foranstaltninger med henblik på at afbøde risikoen for, at de elementer af stærk kundeidentifikation, der karakteriseres som viden, afdækkes af eller vises til uautoriserede parter.

2. Betalerens brug af disse elementer er genstand for afbødende foranstaltninger for at forhindre, at de vises til uautoriserede parter.

Artikel 7

Krav til de elementer, der karakteriseres som besiddelse

1. Betalingstjenesteudbydere træffer foranstaltninger med henblik på at afbøde risikoen for, at de elementer af stærk kundeidentifikation, der karakteriseres som besiddelse, bruges af uautoriserede parter.

2. Betalerens brug af disse elementer er genstand for foranstaltninger, som er udformet med henblik på at forhindre genskabelse heraf.

Artikel 8

Krav til anordninger og software knyttet til elementer karakteriseret som iboende egenskab

1. Betalingstjenesteudbydere træffer foranstaltninger med henblik på at afbøde risikoen for, at de autentifikationselementer, der karakteriseres som iboende egenskab og læses af adgangsanordninger og software stillet til rådighed for betaleren, afdækkes af uautoriserede parter. Betalingstjenesteudbydere skal som et minimum sikre, at der er yderst ringe sandsynlighed for, at nævnte adgangsanordninger og software giver anledning til, at en uautoriseret part autentificeres som betaleren.

2. Betalerens brug af disse elementer gøres til genstand for foranstaltninger, som sikrer, at nævnte anordninger og software garanterer modstandsdygtighed over for uautoriseret brug af elementerne gennem adgang til anordninger og software.

Artikel 9

Elementernes uafhængighed

1. Betalingstjenesteudbydere påser, at brugen af de elementer af stærk kundeautentifikation, som er omhandlet i artikel 6, 7 og 8, gøres til genstand for foranstaltninger, der — for så vidt angår teknologi, algoritmer og parametre — sikrer, at brud på et af elementerne ikke svækker de andre elementers pålidelighed.

2. Betalingstjenesteudbydere træffer sikkerhedsforanstaltninger, hvis elementer af stærk kundeautentifikation eller selve autentifikationskoden anvendes gennem en multifunktionel anordning, for at afbøde den risiko, som ville opstå, hvis nævnte multifunktionelle anordning blev svækket.

3. De afbødende foranstaltninger skal med henblik på stk. 2 omfatte følgende:

a) brug af adskilte sikre gennemførelsesmiljøer gennem det software, som er installeret i den multifunktionelle anordning

b) mekanismer til at sikre, at hverken software eller anordning er blevet ændret af betaleren eller af tredjemand

c) mekanismer til at afbøde følgerne af eventuelle ændringer.

KAPITEL III

UNDTAGELSER FRA STÆRK KUNDEAUTENTIFIKATION

Artikel 10

Betalingskontooplysninger

1. Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, jf. dog de krav, der skal opfyldes i henhold til artikel 2 og stk. 2 i denne artikel, hvis en betalingstjenestebruger kun kan tilgå den ene eller begge af følgende poster online uden visning af følsomme betalingsdata:

a) saldoen på en eller flere angivne betalingskonti

b) de betalingstransaktioner, der er gennemført i de seneste 90 dage, over en eller flere angivne betalingskonti.

2. Betalingstjenesteudbydere indrømmes med henblik på stk. 1 ikke undtagelse fra anvendelse af stærk kundeautentifikation, hvis en af følgende betingelser er opfyldt:

a) betalingstjenestebrugeren har adgang online til de oplysninger, der er omhandlet i stk. 1, for første gang

b) der er gået mere end 90 dage, siden betalingstjenestebrugeren sidst havde adgang online til de oplysninger, der er omhandlet i stk. 1, litra b), og siden der blev anvendt stærk kundeautentifikation.

Artikel 11

Kontaktløse betalinger på salgsstedet

Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, jf. dog de krav, der skal opfyldes i henhold til artikel 2, hvis betaleren initierer en kontaktløs elektronisk betalingstransaktion, forudsat at følgende betingelser er opfyldt:

a) værdien af hver enkelt kontaktløs elektronisk betalingstransaktion overstiger ikke 50 EUR, og

b) den samlede værdi af tidligere kontaktløse elektroniske betalingstransaktioner initieret ved hjælp af et betalingsinstrument med en kontaktløs funktionalitet siden den seneste anvendelse af stærk kundeautentifikation overstiger ikke 150 EUR, eller

c) antallet af konsekutive kontaktløse elektroniske betalingstransaktioner initieret ved hjælp af et betalingsinstrument med en kontaktløs funktionalitet siden den seneste anvendelse af stærk kundeautentifikation overstiger ikke fem.

Artikel 12

Ubemandede terminaler til betaling af befordringsbilletter og parkeringsgebyrer

Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, jf. dog de krav, der skal opfyldes i henhold til artikel 2, hvis betaleren initierer en elektronisk betalingstransaktion i en ubemandet betalingsterminal med det formål at betale en befordringsbillet eller et parkeringsgebyr.

Artikel 13

Troværdige begunstigede

1. Betalingstjenesteudbydere skal anvende stærk kundeautentifikation, hvis en betaler opretter eller ændrer en liste over troværdige begunstigede gennem betalerens kontoførende betalingstjenesteudbyder.

2. Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, jf. dog de generelle autentifikationskrav, hvis betaleren initierer en betalingstransaktion, og betalingsmodtageren er opført på en liste over troværdige begunstigede, som betaleren tidligere har opstillet.

Artikel 14

Tilbagevendende transaktioner

1. Betalingstjenesteudbydere skal anvende stærk kundeidentifikation, hvis en betaler for første gang opretter, ændrer eller initierer en række tilbagevendende transaktioner med det samme beløb og den samme betalingsmodtager.

2. Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, jf. dog de generelle autentifikationskrav, ved initieringen af alle efterfølgende betalingstransaktioner, som indgår i den række af betalingstransaktioner, der er omhandlet i stk. 1.

Artikel 15

Kreditoverførsler mellem den samme fysiske eller juridiske persons konti

Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, jf. dog de krav, der skal opfyldes i henhold til artikel 2, hvis betaleren initierer en kreditoverførsel, og det forholder sig sådan, at betaleren og betalingsmodtageren er den samme fysiske eller juridiske person, og at begge betalingskonti føres af den samme kontoførende betalingstjenesteudbyder.

Artikel 16

Mindre transaktioner

Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, hvis betaleren initierer en elektronisk fjernbetalingstransaktion, forudsat at følgende betingelser er opfyldt:

a) værdien af den elektroniske fjernbetalingstransaktion overstiger ikke 30 EUR, og

b) den samlede værdi af tidligere elektroniske fjernbetalingstransaktioner initieret af betaleren siden den seneste anvendelse af stærk kundeautentifikation overstiger ikke 100 EUR, eller

c) antallet af tidligere elektroniske fjernbetalingstransaktioner initieret af betaleren siden den seneste anvendelse af stærk kundeautentifikation overstiger ikke fem konsekutive enkeltstående elektroniske fjernbetalingstransaktioner.

Artikel 17

Sikre erhvervsrelaterede betalingsprocesser og -protokoller

Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation i forbindelse med juridiske personer, som initierer elektroniske betalingstransaktioner ved brug af dedikerede betalingsprocesser eller -protokoller, der udelukkende stilles til rådighed for betalere, som ikke er forbrugere, hvis de kompetente myndigheder finder det godtgjort, at nævnte processer eller protokoller mindst sikrer samme grader af sikkerhed som dem, der er omhandlet i direktiv (EU) 2015/2366.

Artikel 18

Transaktionsrisikoanalyse

1. Betalingstjenesteudbydere har mulighed for at undlade at anvende stærk kundeautentifikation, hvis betaleren initierer en elektronisk fjernbetalingstransaktion, som betalingstjenesteudbyderen anser for at indebære en lav risiko i henhold til de transaktionsovervågningsmekanismer, der er omhandlet i artikel 2 og i stk. 2, litra c), i denne artikel.

2. En elektronisk betalingstransaktion som omhandlet i stk. 1 anses for at indebære en lav risiko, hvis følgende betingelser er opfyldt:

a) procentsatsen for svig for nævnte type transaktioner, som indberettet af betalingstjenesteudbyderen og beregnet i overensstemmelse med artikel 19, svarer til eller er mindre end de referencesatser for svig, der er angivet i tabellen i bilaget for henholdsvis »elektroniske kortbaserede fjernbetalinger« og »elektroniske fjernkreditoverførsler«

b) transaktionsbeløbet overstiger ikke den relevante tærskelværdi for undtagelser (Exemption Threshold Value (»ETV«)), der er angivet i tabellen i bilaget

c) betalingstjenesteudbydere har ved en realtidsanalyse af risici ikke konstateret følgende:

   i) unormale udgifts- eller adfærdsmønstre hos betaleren

   ii) usædvanlige oplysninger om betalerens adgang til anordninger og software

   iii) malware-infektion i autentifikationsprocedurens sessioner

   iv) kendte scenarier for svig i forbindelse med udbud af betalingstjenester

   v) unormalt opholdssted for betaleren

   vi) højrisikoopholdssted for betalingsmodtageren.

3. Betalingstjenesteudbydere, som har til hensigt at undtage elektroniske fjernbetalingstransaktioner fra stærk kundeautentifikation, fordi de indebærer en lav risiko, tager som et minimum højde for følgende risikobaserede faktorer:

a) den enkelte betalingstjenestebrugers tidligere udgiftsmønstre

b) betalingstransaktionshistorikken for hver af betalingstjenesteudbyderens betalingstjenestebrugere

c) betalerens og betalingsmodtagerens opholdssted på det tidpunkt, hvor betalingstransaktionen finder sted, hvis betalingstjenesteudbyderen stiller adgangsanordning og software til rådighed

d) unormale betalingsmønstre hos betalingstjenestebrugeren i forhold til brugerens betalingstransaktionshistorik.

Betalingstjenesteudbyderens vurdering indebærer, at alle nævnte risikobaserede faktorer kombineres til en risikoberegning for hver enkelt transaktion med henblik på at fastlægge, hvorvidt en bestemt betaling bør godkendes uden stærk kundeautentifikation.

Artikel 19

Beregning af procentsatser for svig

1. Betalingstjenesteudbyderen sikrer for hver type transaktion, der er angivet i tabellen i bilaget, at de samlede procentsatser for svig, som både omfatter betalingstransaktioner, der er autentificeret gennem stærk kundeautentifikation, og betalingstransaktioner, der er gennemført i henhold til en af de undtagelser, der er omhandlet i artikel 13-18, svarer til eller er mindre end referencesatsen for svig for den samme type betalingstransaktion, der er angivet i tabellen i bilaget.

Den samlede procentsats for svig for hver type transaktion beregnes som den samlede værdi af uautoriserede eller svigagtige fjerntransaktioner, uanset om midlerne er inddrevet, divideret med den samlede værdi af alle fjerntransaktioner for den samme type transaktioner, uanset om de er autentificeret ved brug af stærk kundeautentifikation eller gennemført i henhold til en af de undtagelser, der er omhandlet i artikel 13-18, på rullende kvartalsbasis (90 dage).

2. Beregningen af procentsatserne for svig og de deraf følgende værdier vurderes ved den revision, der er omhandlet i artikel 3, stk. 2, hvorved det sikres, at de er fuldstændige og præcise.

3. Den metode og de modeller, som betalingstjenesteudbyderen anvender til at beregne procentsatserne for svig, samt selve procentsatserne for svig, dokumenteres behørigt og stilles, uden forudgående underretning af den eller de relevante kompetente myndigheder, efter anmodning i fuldt omfang til rådighed for de kompetente myndigheder og for EBA.

Artikel 20

Ophør med brug af undtagelser baseret på transaktionsrisikoanalyse

1. Betalingstjenesteudbydere, som gør brug af den undtagelse, der er omhandlet i artikel 18, underretter omgående de kompetente myndigheder, hvis en af deres overvågede procentsatser for svig for de typer betalingstransaktioner, der er angivet i tabellen i bilaget, overstiger den gældende referencesats for svig, og fremsender en beskrivelse til de kompetente myndigheder af de foranstaltninger, de har til hensigt at træffe for at sikre, at deres overvågede procentsats for svig på ny er i overensstemmelse med de gældende referencesatser for svig.

2. Betalingstjenesteudbydere ophører omgående med at gøre brug af den undtagelse, der er omhandlet i artikel 18, for de typer betalingstransaktioner, der er angivet i tabellen i bilaget i det særlige tærskelinterval for undtagelser, hvis deres overvågede procentsats for svig i to på hinanden følgende kvartaler overstiger den gældende referencesats for svig for det pågældende betalingsinstrument eller den pågældende type betalingstransaktion i nævnte tærskelinterval for undtagelser.

3. Hvis betalingstjenesteudbydere i overensstemmelse med stk. 2 i denne artikel ophører med at gøre brug af den undtagelse, der er omhandlet i artikel 18, gør betalingstjenesteudbyderne først på ny brug af nævnte undtagelse, når deres beregnede procentsats for svig i et kvartal svarer til eller er lavere end de gældende referencesatser for svig for den pågældende type betalingstransaktion i nævnte tærskelinterval for undtagelser.

4. Hvis betalingstjenesteudbydere har til hensigt på ny at gøre brug af den undtagelse, der er omhandlet i artikel 18, underretter de inden for et rimeligt tidsrum de kompetente myndigheder herom og fremlægger, inden de på ny gør brug af undtagelsen, belæg for, at deres overvågede procentsats for svig på ny er i overensstemmelse med den gældende referencesats for svig for nævnte tærskelinterval for undtagelser i overensstemmelse med stk. 3 i denne artikel.

Artikel 21

Overvågning

1. Betalingstjenesteudbydere skal for at kunne gøre brug af de undtagelser, der er omhandlet i artikel 10-18, som et minimum på kvartalsbasis registrere og overvåge følgende data for hver type betalingstransaktion med en opdeling i både fjern- og ikkefjernbetalingstransaktioner:

a) den samlede værdi af uautoriserede eller svigagtige betalingstransaktioner i henhold til artikel 64, stk. 2, i direktiv (EU) 2015/2366, den samlede værdi af alle betalingstransaktioner og den deraf følgende procentsats for svig med en opdeling i betalingstransaktioner initieret gennem stærk kundeautentifikation og omfattet af hver af undtagelserne

b) den gennemsnitlige transaktionsværdi med en opdeling i betalingstransaktioner initieret gennem stærk kundeautentifikation og omfattet af hver af undtagelserne

c) det antal betalingstransaktioner, som er omfattet af hver af undtagelserne, og den procentdel, som de udgør i forhold til det samlede antal betalingstransaktioner.

2. Betalingstjenesteudbyderne stiller, uden forudgående underretning af den eller de relevante kompetente myndigheder, efter anmodning resultaterne af overvågningen i henhold til stk. 1 til rådighed for de kompetente myndigheder og for EBA.

KAPITEL IV

FORTROLIGHEDEN OG INTEGRITETEN AF BETALINGSTJENESTEBRUGERNES PERSONALISEREDE SIKKERHEDSOPLYSNINGER

Artikel 22

Generelle krav

1. Betalingstjenesteudbydere sikrer fortroligheden og integriteten af betalingstjenestebrugerens personaliserede sikkerhedsoplysninger, herunder autentifikationskoder, i alle autentifikationsfaserne.

2. Betalingstjenesteudbydere sikrer med henblik på stk. 1, at følgende krav opfyldes:

a) personaliserede sikkerhedsoplysninger maskeres, når de vises, og kan ikke i fuldt omfang læses, når betalingstjenestebrugeren indgiver dem i forbindelse med autentifikation

b) personaliserede sikkerhedsoplysninger i dataformat samt kryptografisk materiale med tilknytning til krypteringen af de personaliserede sikkerhedsoplysninger lagres ikke i klartekst

c) hemmeligt kryptografisk materiale er beskyttet mod uautoriseret visning.

3. Betalingstjenesteudbydere dokumenterer i fuldt omfang den proces, der er knyttet til forvaltningen af det kryptografiske materiale, som anvendes til kryptering, eller sikrer i modsat fald, at de personaliserede sikkerhedsoplysninger gøres ulæselige.

4. Betalingstjenesteudbydere sikrer, at behandling og routing af personaliserede sikkerhedsoplysninger og af autentifikationskoder genereret i overensstemmelse med kapitel II foregår i et sikkert miljø i overensstemmelse med robuste and almindeligt anerkendte industristandarder.

Artikel 23

Oprettelse og fremsendelse af sikkerhedsoplysninger

Betalingstjenesteudbydere sikrer, at personaliserede sikkerhedsoplysninger oprettes i et sikkert miljø.

De afbøder risikoen for uautoriseret brug af de personaliserede sikkerhedsoplysninger og af autentifikationsanordninger og software som følge af tab, tyveri eller kopiering heraf, før de leveres til betaleren.

Artikel 24

Sammenkædning med betalingstjenestebrugeren

1. Betalingstjenesteudbydere sikrer, at kun betalingstjenestebrugeren sammenkædes, på en sikker måde, med personaliserede sikkerhedsoplysninger, autentifikationsanordninger og software.

2. Betalingstjenesteudbydere sikrer med henblik på stk. 1, at følgende krav opfyldes:

a) sammenkædningen af betalingstjenestebrugerens identitet med personaliserede sikkerhedsoplysninger, autentifikationsanordninger og software gennemføres på betalingstjenesteudbyderens ansvar i et sikkert miljø, der som et minimum omfatter betalingstjenesteudbyderens forretningslokaler, det internetmiljø, som betalingstjenesteudbyderen stiller til rådighed, eller andre lignende sikre websteder, som betalingstjenesteudbyderen anvender, samt dennes automatiserede pengeautomattjenester, idet der tages hensyn til de risici, der er forbundet med anordninger og underliggende komponenter, som anvendes under sammenkædningsprocessen, og som betalingstjenesteudbyderen ikke er ansvarlig for

b) sammenkædning gennem en fjernkanal af betalingstjenestebrugerens identitet med de personaliserede sikkerhedsoplysninger og autentifikationsanordninger eller software gennemføres ved brug af stærk kundeautentifikation.

Artikel 25

Levering af sikkerhedsoplysninger, autentifikationsanordninger og software

1. Betalingstjenesteudbydere sikrer, at personaliserede sikkerhedsoplysninger, autentifikationsanordninger og software leveres til betalingstjenestebrugeren på en sikker måde, der er udformet med henblik på at afbøde de risici, der er forbundet med uautoriseret brug heraf som følge af tab, tyveri eller kopiering.

2. Betalingstjenesteudbydere træffer med henblik på stk. 1 som et minimum følgende foranstaltninger:

a) effektive og sikre leveringsmekanismer, som garanterer, at de personaliserede sikkerhedsoplysninger, autentifikationsanordninger og software leveres til den retmæssige betalingstjenestebruger

b) mekanismer, som gør det muligt for betalingstjenesteudbyderen at verificere ægtheden af det autentifikationssoftware, der er leveret til betalingstjenestebrugeren gennem internettet

c) ordninger, som i forbindelse med levering af personaliserede sikkerhedsoplysninger uden for betalingstjenesteudbyderens forretningslokaler eller gennem en fjerkanal, sikrer, at:

   i) uautoriserede parter ikke kan indhente mere end et enkelt element af de personaliserede sikkerhedsoplysninger, autentifikationsanordningerne eller softwaret ved levering gennem samme kanal

   ii) personaliserede sikkerhedsoplysninger, autentifikationsanordninger eller software, der er leveret, skal aktiveres før brug

d) ordninger, som i forbindelse med personaliserede sikkerhedsoplysninger, autentifikationsanordninger eller software, der er blevet aktiveret før brug første gang, sikrer, at aktiveringen finder sted i et sikkert miljø i overensstemmelse med de sammenkædningsprocedurer, der er omhandlet i artikel 24.

Artikel 26

Fornyelse af personaliserede sikkerhedsoplysninger

Betalingstjenesteudbydere sikrer, at fornyelse eller genaktivering af personaliserede sikkerhedsoplysninger foretages i overensstemmelse med de procedurer for oprettelse, sammenkædning og levering af sikkerhedsoplysninger og autentifikationsanordninger, der er omhandlet i artikel 23, 24 og 25.

Artikel 27

Destruktion, deaktivering og tilbagekaldelse

Betalingstjenesteudbydere sikrer, at de råder over effektive processer, som gør muligt at træffe følgende sikkerhedsforanstaltninger:

a) sikker destruktion, deaktivering eller tilbagekaldelse af personaliserede sikkerhedsoplysninger, autentifikationsanordninger og software

b) hvis betalingstjenesteudbyderen distribuerer autentifikationsanordninger og software, der kan genanvendes, sikker genanvendelse af anordninger eller software konstateres, dokumenteres og gennemføres, før anordningerne eller softwaret stilles til rådighed for en anden betalingstjenestebruger

c) deaktivering eller tilbagekaldelse af oplysninger med tilknytning til personaliserede sikkerhedsoplysninger lagret i betalingstjenesteudbyderens systemer og databaser og, hvis det er relevant, offentlige registre.

KAPITEL V

FÆLLES OG SIKRE ÅBNE STANDARDER FOR KOMMUNIKATION

Afdeling 1

Generelle krav til kommunikation

Artikel 28

Krav til identifikation

1. Betalingstjenesteudbydere garanterer sikker identifikation ved kommunikation mellem betalerens anordning og betalingsmodtagerens anordninger til accept af elektroniske betalinger, herunder (men ikke begrænset til) betalingsterminaler.

2. Betalingstjenesteudbydere sikrer, at risikoen for fejldirigering af kommunikation til uautoriserede parter i mobile applikationer og betalingstjenestebrugeres andre interface med elektroniske betalingstjenester, afbødes effektivt.

Artikel 29

Sporbarhed

1. Betalingstjenesteudbydere råder over processer, som sikrer, at alle betalingstransaktioner og andre former for interaktion med betalingstjenestebrugeren, med andre betalingstjenesteudbydere og med andre enheder, herunder forretningsdrivende, i forbindelse med levering af betalingstjenesten er sporbare, således at der sikres efterfølgende kendskab til alle hændelser, som er relevante for den elektroniske transaktion på alle de forskellige stadier.

2. Betalingstjenesteudbydere skal med henblik på stk. 1 sikre, at der ved alle kommunikationssessioner med betalingstjenestebrugeren, andre betalingstjenesteudbydere og andre enheder, herunder forretningsdrivende, anvendes følgende:

a) en entydig identifikator for sessionen

b) sikkerhedsmekanismer til detaljeret registrering af transaktionen, herunder transaktionsnummer, tidsstempler og alle relevante transaktionsdata

c) tidsstempler, som er baseret på et fælles tidsreferencesystem, og som er synkroniseret i overensstemmelse med et officielt tidssignal.

Afdeling 2

Særlige krav til fælles og sikre åbne standarder for kommunikation

Artikel 30

Generelle forpligtelser i forhold til adgangsinterface

1. Kontoførende betalingstjenesteudbydere, som tilbyder betaleren en betalingskonto, der kan tilgås online, skal som et minimum have et interface til rådighed, som opfylder følgende krav:

a) kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, kan identificere sig over for den kontoførende betalingstjenesteudbyder

b) kontooplysningstjenesteudbydere kan kommunikere sikkert med det formål at anmode om og modtage oplysninger om en eller flere angivne betalingskonti og dertil knyttede betalingstransaktioner

c) betalingsinitieringstjenesteudbydere kan kommunikere sikkert med det formål at initiere en betalingsordre fra betalerens betalingskonto og modtage alle oplysninger om betalingstransaktionens initiering og alle oplysninger, som er tilgængelige for de kontoførende betalingstjenesteudbydere, vedrørende betalingstransaktionens gennemførelse.

2. Det interface, der er omhandlet i stk. 1, skal med henblik på autentifikation af betalingstjenestebrugeren gøre det muligt for kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere at anvende alle de autentifikationsprocedurer, som den kontoførende betalingstjenesteudbyder stiller til rådighed for betalingstjenestebrugeren.

Interfacet skal som et minimum opfylde følgende krav:

a) en betalingsinitieringstjenesteudbyder eller kontooplysningstjenesteudbyder har mulighed for at pålægge den kontoførende betalingstjenesteudbyder at påbegynde autentifikation baseret på betalingstjenestebrugerens samtykke

b) kommunikationssessioner mellem den kontoførende betalingstjenesteudbyder, kontooplysningstjenesteudbyderen, betalingsinitieringstjenesteudbyderen og berørte betalingstjenestebrugere oprettes og videreføres under hele autentifikationen

c) integritet og fortrolighed sikres for personaliserede sikkerhedsoplysninger og autentifikationskoder fremsendt af eller gennem betalingsinitieringstjenesteudbyderen eller kontooplysningstjenesteudbyderen.

3. Kontoførende betalingstjenesteudbydere sikrer, at deres interface følger de standarder for kommunikation, som udstedes af internationale og europæiske standardiseringsorganer.

Kontoførende betalingstjenesteudbydere sikrer også, at den tekniske specifikation for interface er dokumenteret med nærmere angivelse af en række rutiner, protokoller og værktøjer, som betalingsinitieringstjenesteudbydere, kontooplysningstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, har for brug, således at deres software og applikationer kan fungere sammen med de kontoførende betalingstjenesteudbyderes systemer.

Kontoførende betalingstjenesteudbydere skal som et minimum og senest seks måneder før den anvendelsesdato, der er omhandlet i artikel 38, stk. 2, eller når markedsføringen finder sted efter den dato, der er omhandlet i artikel 38, stk. 2, før måldatoen for adgangsinterfacets markedsføring, stille dokumentationen gratis til rådighed efter anmodning fra godkendte betalingsinitieringstjenesteudbydere, kontooplysningstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, eller betalingstjenesteudbydere, som har anmodet deres kompetente myndigheder om meddelelse af den relevante tilladelse, og stille et resumé af dokumentationen til rådighed for offentligheden på deres websted.

4. Kontoførende betalingstjenesteudbydere skal i tillæg til stk. 3, undtagen i kritiske situationer, sikre, at ændringer af den tekniske specifikation for deres interface, hurtigst muligt og senest tre måneder før ændringen gennemføres, stilles til rådighed for godkendte betalingsinitieringstjenesteudbydere, kontooplysningstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, eller betalingstjenesteudbydere, som har anmodet deres kompetente myndigheder om meddelelse af den relevante tilladelse.

Betalingstjenesteudbydere skal dokumentere kritiske situationer, hvor der blev gennemført ændringer, og efter anmodning stille dokumentationen til rådighed for de kompetente myndigheder.

5. Kontoførende betalingstjenesteudbydere stiller en testfacilitet til afprøvning af tilslutning og funktion, herunder support, til rådighed for godkendte betalingsinitieringstjenesteudbydere, betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, og kontooplysningstjenesteudbydere eller betalingstjenesteudbydere, som har anmodet om meddelelse af den relevante tilladelse, for at gøre det muligt at afprøve software og applikationer, som anvendes til at udbyde betalingstjenester til brugere. Denne testfacilitet bør stilles til rådighed senest seks måneder før den anvendelsesdato, der er omhandlet i artikel 38, stk. 2, eller når markedsføringen finder sted efter den dato, der er omhandlet i artikel 38, stk. 2, før måldatoen for adgangsinterfacets markedsføring.

Følsomme oplysninger udveksles dog ikke gennem denne testfacilitet.

6. De kompetente myndigheder sikrer, at kontoførende betalingstjenesteudbydere til enhver tid opfylder de forpligtelser, der indgår i disse standarder, i forhold til det eller de interface, som tages i brug. De kompetente myndigheder skal, hvis en kontoførende betalingstjenesteudbyder ikke opfylder de krav, der stilles til interface i disse standarder, sikre, at leveringen af betalingsinitieringstjenester og kontooplysningstjenester hverken forhindres eller afbrydes, under forudsætning af at de respektive udbydere af sådanne tjenester opfylder de betingelser, der er omhandlet i artikel 33, stk. 5.

Artikel 31

Optioner med hensyn til adgangsinterface

Kontoførende betalingstjenesteudbydere opretter det eller de interface, der er omhandlet i artikel 30, ved hjælp af et dedikeret interface eller ved at give de betalingstjenesteudbydere, der er omhandlet i artikel 30, stk. 1, mulighed for at gøre brug af de interface, der anvendes til autentifikation og kommunikation med den kontoførende betalingstjenesteudbyders betalingstjenestebrugere.

Artikel 32

Forpligtelser i forhold til et dedikeret interface

1. Kontoførende betalingstjenesteudbydere, som har taget et dedikeret interface i brug, påser, at det dedikerede interface til enhver tid sikrer samme tilgængelighed og ydeevne, herunder support, som de interface, der stilles til rådighed for betalingstjenestebrugere ved direkte adgang til betalingskonti online, jf. dog de krav, der skal opfyldes i henhold til artikel 30 og 31.

2. Kontoførende betalingstjenesteudbydere, som har taget et dedikeret interface i brug, definerer gennemsigtige nøgleresultatindikatorer og serviceniveaumål, som er mindst lige så omfattende som dem, der er fastsat for det interface, som deres betalingstjenestebrugere anvender, både for så vidt angår tilgængelighed og de data, der leveres i overensstemmelse med artikel 36. Nævnte interface, indikatorer og mål overvåges af de kompetente myndigheder og gøres til genstand for stresstest.

3. Kontoførende betalingstjenesteudbydere, som har taget et dedikeret interface i brug, sikrer, at dette interface ikke skaber hindringer for levering af betalingsinitierings- og kontooplysningstjenester. Sådanne hindringer kan bl.a. bevirke, at de betalingstjenesteudbydere, der er omhandlet i artikel 30, stk. 1, ikke kan gøre brug af de sikkerhedsoplysninger, som kontoførende betalingstjenesteudbydere har givet til deres kunder, påtvinge omdirigering til den kontoførende betalingstjenesteudbyders autentifikation eller andre funktioner, nødvendiggøre yderligere tilladelser og registreringer i tillæg til dem, der er omhandlet i artikel 11, 14 og 15 i direktiv (EU) 2015/2366, eller nødvendiggøre yderligere kontroller af det samtykke, som betalingstjenestebrugere har givet til betalingsinitierings- og kontooplysningstjenesteudbydere.

4. Kontoførende betalingstjenesteudbydere overvåger med henblik på stk. 1 og 2, tilgængelighed og ydeevne for så vidt angår det dedikerede interface. Kontoførende betalingstjenesteudbydere offentliggør hvert kvartal statistikker på deres websted med oplysninger om tilgængelighed og ydeevne for så vidt angår det dedikerede interface og det interface, som deres betalingstjenestebrugere anvender.

Artikel 33

Beredskabsforanstaltninger i forhold til et dedikeret interface

1. Kontoførende betalingstjenesteudbydere indarbejder ved udformningen af det dedikerede interface en strategi og planer for beredskabsforanstaltninger for det tilfældes skyld, at interfacet ikke fungerer i overensstemmelse med artikel 32, interfacet uforudset ikke er tilgængeligt, eller systemet svigter. Hvis fem konsekutive anmodninger om adgang til oplysninger med henblik på levering af betalingsinitieringstjenester eller kontooplysningstjenester ikke besvares inden for 30 sekunder, må der formodes at være tale om utilsigtet manglende tilgængelighed eller systemsvigt.

2. Beredskabsforanstaltninger omfatter kommunikationsplaner, som skal sikre, at betalingstjenesteudbydere, som gør brug af det dedikerede interface, informeres om foranstaltninger, som tager sigte på at genetablere systemet, og en beskrivelse af alternative, øjeblikkeligt tilgængelige, løsninger, som betalingstjenesteudbydere kan gøre brug af i dette tidsrum.

3. Kontoførende betalingstjenesteudbydere skal såvel som de betalingstjenesteudbydere, der er omhandlet i artikel 30, stk. 1, omgående indberette problemer med dedikerede interface som beskrevet i stk. 1 til deres respektive kompetente nationale myndigheder.

4. De betalingstjenesteudbydere, som er omhandlet i artikel 30, stk. 1, skal som led i en beredskabsmekanisme have mulighed for at gøre brug af de interface, der er stillet til rådighed for betalingstjenestebrugerne til autentifikation og kommunikation med deres kontoførende betalingstjenesteudbyder, indtil det dedikerede interface på ny sikrer den tilgængelighed og ydeevne, der er omhandlet i artikel 32.

5. Kontoførende betalingstjenesteudbydere skal med henblik herpå sikre, at de betalingstjenesteudbydere, der er omhandlet i artikel 30, stk. 1, kan identificeres og kan anvende de autentifikationsprocedurer, som den kontoførende betalingstjenesteudbyder har stillet til rådighed for betalingstjenestebrugeren. Hvis de betalingstjenesteudbydere, der er omhandlet i artikel 30, stk. 1, gør brug af det interface, der er omhandlet i stk. 4, skal de:

a) træffe de nødvendige foranstaltninger med henblik på at sikre, at de ikke tilgår, lagrer eller behandler data med andre formål end at levere den tjeneste, som betalingstjenestebrugeren har anmodet om

b) fortsat opfylde de betingelser, der er omhandlet i henholdsvis artikel 66, stk. 3, og artikel 67, stk. 2, i direktiv (EU) 2015/2366

c) logge de data, der tilgås gennem det interface, som den kontoførende betalingstjenesteudbyder stiller til rådighed for sine betalingstjenestebrugere, og efter anmodning og uden unødig forsinkelse indgive logfilerne til deres kompetente nationale myndighed

d) behørigt, efter anmodning og uden unødig forsinkelse, over for deres kompetente nationale myndighed godtgøre brugen af det interface, der er stillet til rådighed for betalingstjenestebrugerne med henblik på direkte tilgang til deres betalingskonto online

e) informere den kontoførende betalingstjenesteudbyder herom.

6. De kompetente myndigheder indrømmer, efter høring af EBA med henblik på at sikre konsekvent anvendelse af nedenstående betingelser, de kontoførende betalingstjenesteudbydere, som har valgt et dedikeret interface, undtagelse fra forpligtelsen til at oprette den beredskabsmekanisme, der er omhandlet i stk. 4, hvis det dedikerede interface opfylder følgende betingelser:

a) det opfylder alle betingelserne for dedikerede interface som omhandlet i artikel 32

b) det er udformet og testet i overensstemmelse med artikel 30, stk. 5, og de deri nævnte betalingstjenesteudbydere er tilfredse hermed

c) det har af betalingstjenesteudbydere i mindst tre måneder i vidt omfang været anvendt til at udbyde kontooplysningstjenester og betalingsinitieringstjenester samt til at bekræfte, at midler er tilgængelige for kortbaserede betalinger

d) eventuelle problemer i forbindelse med det dedikerede interface er blevet løst uden unødig forsinkelse.

7. De kompetente myndigheder tilbagekalder den undtagelse, der er omhandlet i stk. 6, hvis de kontoførende betalingstjenesteudbydere i mere end to på hinanden følgende kalenderuger ikke har opfyldt betingelse a) og d). De kompetente myndigheder underretter EBA om denne tilbagekaldelse og sikrer, at den kontoførende betalingstjenesteudbyder hurtigst muligt og senest efter to måneder opretter den beredskabsmekanisme, der er omhandlet i stk. 4.

Artikel 34

Certifikater

1. Betalingstjenesteudbydere skal med henblik på identifikation som omhandlet i artikel 30, stk. 1, litra a), gøre brug af kvalificerede certifikater for elektroniske segl som omhandlet i artikel 3, nr. 30), i forordning (EU) nr. 910/2014 eller for webstedsautentifikation som omhandlet i nævnte forordnings artikel 3, nr. 39).

2. Det registreringsnummer, som fremgår af det officielle register i overensstemmelse med bilag III, litra c), eller bilag IV, litra c), i forordning (EU) nr. 910/2014, er med henblik på denne forordning nummeret på den tilladelse, der er meddelt den betalingstjenesteudbyder, der udsteder kortbaserede betalingsinstrumenter, kontooplysningstjenesteudbyderne og betalingsinitieringstjenesteudbyderne, herunder kontoførende betalingstjenesteudbydere, som udbyder sådanne tjenester, og som er opført i hjemlandets offentlige register i henhold til artikel 14 i direktiv (EU) 2015/2366 eller følger af underretningerne om enhver tilladelse meddelt i henhold til artikel 8 i Europa-Parlamentets og Rådets direktiv 2013/36/EU ([1]) i overensstemmelse med nævnte direktivs artikel 20.

3. De kvalificerede certifikater for elektroniske segl eller for webstedsautentifikation, der omhandlet i stk. 1, skal med henblik på denne forordning, på et sprog, der sædvanligvis anvendes på det finansielle område, omfatte supplerende særlige kendetegn i forhold til følgende:

a) betalingstjenesteudbyderens rolle, som kan være en eller flere af følgende:

   i) kontoføring

   ii) betalingsinitiering

   iii) kontooplysning

   iv) udstedelse af kortbaserede betalingsinstrumenter

b) navnet på de kompetente myndigheder, hvor betalingstjenesteudbyderen er registreret.

4. De kendetegn, der er omhandlet i stk. 3, må ikke påvirke interoperabilitet og genkendelse for så vidt angår kvalificerede certifikater for elektroniske segl eller for webstedsautentifikation.

([1]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

Artikel 35

Sikre kommunikationssessioner

1. Kontoførende betalingstjenesteudbydere, betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere skal ved udveksling af data gennem internettet påse, at der gøres brug af sikker kryptering mellem de kommunikerende parter under hele kommunikationssessionen med anvendelse af stærke og almindeligt anerkendte krypteringsteknikker til at sikre dataenes fortrolighed og integritet.

2. Betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere sikrer, at de adgangssessioner, som kontoførende betalingstjenesteudbydere stiller til rådighed, bliver så korte som muligt, og de afslutter aktivt sådanne sessioner så snart den handling, der er anmodet om, er fuldført.

3. Kontooplysningstjenesteudbydere og betalingsinitieringstjenesteudbydere skal, hvis de opretholder parallelle netværkssessioner med den kontoførende betalingstjenesteudbyder, påse, at nævnte sessioner på en sikker måde er knyttet til relevante sessioner, der er oprettet med betalingstjenestebrugeren eller -brugerne, for at forhindre, at meddelelser eller oplysninger, som kommunikeres dem imellem, eventuelt fejldirigeres.

4. Kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, som udsteder kortbaserede betalingsinstrumenter med den kontoførende betalingstjenesteudbyder, sikrer utvetydige henvisninger:

a) til betalingstjenestebrugeren eller -brugerne og den tilsvarende kommunikationssession for at skelne mellem flere anmodninger fra den eller de samme betalingstjenestebrugere

b) for betalingsinitieringstjenester, til den entydigt identificerede initierede betalingstransaktion

c) for bekræftelse af midlers tilgængelighed, til den entydigt identificerede anmodning, der er knyttet til det beløb, som er nødvendigt for at gennemføre den kortbaserede betalingstransaktion.

5. Kontoførende betalingstjenesteudbydere, kontooplysningstjenesteudbydere, betalingsinitieringstjenesteudbydere og betalingstjenesteudbydere, der udsteder kortbaserede betalingsinstrumenter, skal, hvis de fremsender personaliserede sikkerhedsoplysninger og autentifikationskoder, sikre, at disse ikke på noget tidspunkt kan læses direkte eller indirekte af personale.

Udbydere skal i tilfælde af tab af fortrolige personaliserede sikkerhedsoplysninger inden for deres kompetenceområde uden unødig forsinkelse underrette den betalingstjenestebruger, som er kædet sammen med dem, og udstederen af de personaliserede sikkerhedsoplysninger herom.

Artikel 36

Dataudvekslinger

1. Kontoførende betalingstjenesteudbydere skal opfylde følgende krav:

a) de giver kontooplysningstjenesteudbydere de samme oplysninger fra angivne betalingskonti og dertil knyttede betalingstransaktioner, som gøres tilgængelige for betalingstjenestebrugeren ved direkte anmodning om adgang til kontooplysninger, forudsat at disse oplysninger ikke omfatter følsomme betalingsdata

b) de giver umiddelbart efter modtagelse af betalingsordren betalingsinitieringstjenesteudbydere de samme oplysninger om initieringen og gennemførelsen af betalingstransaktionen, som gives eller gøres tilgængelige for betalingstjenestebrugeren, forudsat at transaktionen initieres direkte af sidstnævnte

c) de bekræfter efter anmodning straks over for betalingstjenesteudbydere med blot et »ja« eller et »nej«, om det beløb, der er nødvendigt for at gennemføre betalingstransaktionen, er tilgængeligt på betalerens betalingskonto.

2. Den kontoførende betalingstjenesteudbyder skal ved en uforudset hændelse eller fejl under identifikations- og autentifikationsprocessen eller dataelementernes udveksling, sende en underretningsmeddelelse til betalingsinitieringstjenesteudbyderen eller den kontoførende betalingstjenesteudbyder og den betalingstjenesteudbyder, der udsteder kortbaserede betalingsinstrumenter, med en forklaring om grunden til den uforudsete hændelse eller fejl.

Hvis den kontoførende betalingstjenesteudbyder stiller et dedikeret interface til rådighed i overensstemmelse med artikel 32, skal interfacet indebære, at underretningsmeddelelser om uforudsete hændelser eller fejl fremsendes af enhver betalingstjenesteudbyder, som konstaterer en hændelse eller en fejl, til de andre betalingstjenesteudbydere, som deltager i kommunikationssessionen.

3. Kontooplysningstjenesteudbydere skal råde over passende og effektive mekanismer, som med betalingstjenestebrugerens udtrykkelige samtykke forhindrer adgang til andre oplysninger end oplysninger fra angivne betalingskonti og dertil knyttede betalingstransaktioner.

4. Betalingsinitieringstjenesteudbydere giver kontoførende betalingstjenesteudbydere de samme oplysninger som dem, betalingstjenestebrugeren anmodes om ved direkte initiering af betalingstransaktionen.

5. Kontooplysningstjenesteudbydere har mulighed for at få adgang til oplysninger fra angivne betalingskonti og dertil knyttede betalingstransaktioner, som kontoførende betalingstjenesteudbydere er i besiddelse af, med henblik på at gennemføre kontooplysningstjenester under en følgende omstændigheder:

a) når betalingstjenestebrugeren aktivt anmoder om sådanne oplysninger

b) hvis betalingstjenestebrugeren ikke aktivt anmoder om sådanne oplysninger, højt fire gange inden for en periode på 24 timer, medmindre en større hyppighed er aftalt mellem kontooplysningstjenesteudbyderen og den kontoførende betalingstjenesteudbyder, med betalingstjenestebrugerens samtykke.

KAPITEL VI

AFSLUTTENDE BESTEMMELSER

Artikel 37

Gennemgang

EBA gennemgår senest den 14. marts 2021 de procentsatser for svig, der er omhandlet i bilaget til denne forordning, samt de undtagelser, der er indrømmet i henhold til artikel 33, stk. 6, i forhold til dedikerede interface, og forelægger om nødvendigt udkast til ajourføringer heraf for Kommissionen i overensstemmelse med artikel 10 i forordning (EU) nr. 1093/2010, jf. dog artikel 98, stk. 5, i direktiv (EU) 2015/2366.

Artikel 38

Ikrafttræden

1. Denne forordning træder i kraft dagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

2. Denne forordning anvendes fra den 14. september 2019.

3. Artikel 30, stk. 3 og 5, anvendes dog fra den 14. marts 2019.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 27. november 2017.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

BILAG

	Referencesats for svig (%) for:	
ETV	Elektroniske kortbaserede fjernbetalinger	Elektroniske fjernkreditoverførsler
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015