KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2018/389

27. november 2017,

millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 regulatiivsete tehniliste standarditega, mis käsitlevad kliendi tugevat autentimist ning ühiseid ja turvalisi teabevahetuse avatud standardeid

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 25. novembri 2015. aasta direktiivi (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta, ([1]) eriti selle artikli 98 lõike 4 teist lõiku,

ning arvestades järgmist:

(1) Elektrooniliselt pakutavad makseteenused tuleks teostada turvaliselt, võttes kasutusele tehnoloogia, mis suudab tagada kasutaja turvalise autentimise ja vähendada maksimaalselt pettuse ohtu. Autentimismenetlus peaks üldiselt hõlmama mehhanisme tehingute seireks, et tuvastada katseid kasutada makseteenuse kasutaja isikustatud turvavolitusi, mis on kaotatud või varastatud või mida on väärkasutatud; samuti tuleks sellega tagada, et makseteenuse kasutaja on seaduslik kasutaja ja annab seega isikustatud turvavolitusi tavapärasel viisil kasutades oma nõusoleku rahaliste vahendite ülekandmiseks ja oma kontoandmetele juurdepääsuks. Lisaks tuleb kindlaks määrata nõuded seoses kliendi tugeva autentimisega, mida tuleks kasutada iga kord, kui maksja siseneb interneti kaudu oma maksekontole, algatab elektroonilise maksetehingu või teeb kaugejuurdepääsu teel mis tahes muu toimingu, mille puhul võib esineda maksepettuse või muu kuritarvitamise oht, nõudes selliste autentimiskoodide genereerimist, mille puhul ei ole ohtu, et neid saaks kas tervikuna või mõne nende genereerimiseks kasutatud elemendi avalikustamise läbi võltsida.

(2) Kuna pettuste skeemid muutuvad pidevalt, peaksid nõuded kliendi tugevale autentimisele võimaldama tehnoloogiliste lahenduste uuendamist, et reageerida elektrooniliste maksete turvalisust ähvardavate uute ohtude tekkele. Sätestatud nõuete pideva tulemusliku rakendamise tagamiseks on samuti asjakohane nõuda, et kliendi tugeva autentimise ja selle erandite juures kasutatavad turvameetmed, isikustatud turvavolituste konfidentsiaalsuse ja tervikluse kaitsemeetmed ning meetmed, millega kehtestatakse ühised ja turvalised teabevahetuse avatud standardid, oleksid dokumenteeritud, et neid korrapäraselt testitaks ja hinnataks ning et neid auditeeriksid audiitorid, kellel on IT-turvalisuse ja elektrooniliste maksete alane pädevus ning kes on oma tegevuses sõltumatud. Selleks et pädevatel asutustel oleks võimalik teha järelevalvet nimetatud meetmete läbivaatamise kvaliteedi üle, tuleks läbivaatamise tulemused neile kättesaadavaks teha, kui nad seda taotlevad.

(3) Kuna elektrooniliste kaugmaksetehingute puhul on suurem pettuseoht, tuleb selliste tehingute puhul kehtestada täiendavad nõuded kliendi tugeva autentimise kohta, millega tagatakse, et elemendid loovad dünaamilise lingi tehingu ning maksja poolt enne makse algatamist kindlaks määratud summa ja makse saaja vahel.

(4) Dünaamilise lingi loomine on võimalik autentimiskoodide genereerimisega, millele kehtivad ranged turvanõuded. Tehnoloogilise neutraalsuse säilitamise eesmärgil ei tohiks nõuda autentimiskoodide töölerakendamiseks teatava tehnoloogia kasutamist. Kui turvanõuded on täidetud, peaksid autentimiskoodid niisiis põhinema sellistel lahendustel nagu ühekordsete salasõnade genereerimine ja valideerimine, digiallkirjad või muud krüptimispõhised kehtivuse kinnitused, mille juures kasutatakse võtmeid või krüptitud materjali, mis on salvestatud autentimiselementidesse.

([1]) ELT L 337, 23.12.2015, lk 35.

(5) On vaja sätestada erinõuded puhuks, kui maksja poolt elektroonilise kaugmaksetehingu algatamise hetkel ei ole teada selle tehingu lõplik summa, tagamaks, et vastavalt direktiivile (EL) 2015/2366 on kliendi tugev autentimine konkreetselt seotud maksimumsummaga, millega seoses maksja on oma nõusoleku andnud.

(6) Kliendi tugeva autentimise kohaldamise tagamiseks tuleb samuti nõuda asjakohaste turvaelementide olemasolu selliste kliendi tugeva autentimise elementide puhul, mis kuuluvad teadmise kategooriasse (miski, mida teab üksnes kasutaja), nagu pikkus või keerukus, omamise kategooriasse (miski, mida omab üksnes kasutaja), nagu algoritmi spetsifikaadid, võtme pikkus ja entroopia, või olemuse kategooriasse (miski, mis on kasutajale omane), nagu algoritmi spetsifikaadid ning elemendid biomeetrilise anduri ja biomeetrilise malli kaitsmiseks, ennekõike leevendamaks riski, et nimetatud elemendid tuvastatakse ja kõrvalistele isikutele avaldatakse ning et sellised isikud neid kasutavad. Samuti tuleb sätestada nõuded, millega tagatakse, et need elemendid on sõltumatud, nii et neist ühe rikkumine ei ohustaks teiste usaldusväärsust, ennekõike siis, kui mõnda neist elementidest kasutatakse mitmeotstarbelises seadmes, st sellises seadmes nagu tahvelarvuti või mobiiltelefon, mida saab kasutada nii makse tegemise korralduse andmiseks kui ka autentimisprotsessiks.

(7) Nõuded kliendi tugevale autentimisele kehtivad maksja algatatud maksetele sõltumata sellest, kas maksja on füüsiline või juriidiline isik.

(8) Anonüümsete makseinstrumentide vahendusel sooritatud maksetele ei kehti nende olemusest tulenevalt kliendi tugeva autentimise nõue. Kui selliste instrumentide anonüümsus lepingutest või õigusnormidest tulenevatel põhjustel tühistatakse, kehtivad maksetele turvanõuded, mis tulenevad direktiivist (EL) 2015/2366 ja käesolevast regulatiivsest tehnilisest standardist.

(9) Kooskõlas direktiiviga (EL) 2015/2366 on erandid kliendi tugevast autentimisest määratletud vastavalt maksetehingu riski tasemele, summale, korduvusele ja selle täitmiseks kasutatud maksekanalile.

(10) Tegevus, mis eeldab juurdepääsu maksekonto kontoseisule ja viimastele tehingutele tundlikke makseandmeid avalikustamata, korduvad maksed sellistele makse saajatele, kelle maksja on kliendi tugevat autentimist kasutades eelnevalt salvestanud või kinnitanud, ning maksed sama makseteenuse pakkuja juures kontot omavale samale füüsilisele või juriidilisele isikule või selliselt isikult kujutavad enesest väikest riski ja võimaldavad seega makseteenuse pakkujal mitte kohaldada kliendi tugevat autentimist. Ent siiski tuleb rõhutada, et vastavalt direktiivi (EL) 2015/2366 artiklitele 65, 66 ja 67 peaksid makse algatamise teenuse pakkujad, kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad ja kontoteabe teenuse pakkujad taotlema ja saama vajalikku ja olulist teavet kontot haldavalt makseteenuse pakkujalt konkreetse makseteenuse pakkumise eesmärgil ainult makseteenuse kasutaja nõusolekul. Selline nõusolek võidakse anda eraldi iga teabenõude või iga algatatava makse kohta või kontoteabe teenuse pakkujate puhul volitusena määratud maksekontode ja nendega seotud maksetehingute kohta vastavalt makseteenuse kasutajaga sõlmitud lepingule.

(11) Müügipunktis tehtavate väikese väärtusega viipemaksete suhtes tuleks näha ette erandid, mille juures võetakse arvesse ka üksteisele järgnevate tehingute maksimaalset arvu või üksteisele järgnevate tehingute teatavat kindlat maksimumväärtust kliendi tugevat autentimist kohaldamata, kuna need võimaldavad kasutajasõbralike ja väikese riskiga makseteenuste väljatöötamist. Samuti on asjakohane kehtestada erand sellistele elektroonilistele maksetehingutele, mis algatatakse personalita terminalides, kuna sel juhul ei pruugi kliendi tugeva autentimise kohaldamine praktilistel põhjustel alati lihtne olla (näiteks vältimaks järjekordi ja võimalikke õnnetusi enne teemaksuväravaid või muid turva- või julgeolekuriske).

(12) Sarnaselt müügipunktis sooritatavatele väikese väärtusega viipemaksetele tehtava erandiga tuleb leida sobilik tasakaal soovi vahel suurendada kaugmaksetehingute turvalisust ning vajaduse vahel tagada e-kaubanduse valdkonna maksete kasutajasõbralikkus ja kättesaadavus. Nende põhimõtetega kooskõlas tuleks piirmäärad, millest allpool ei ole vaja kliendi tugevat autentimist kohaldada, kehtestada läbimõeldult, et need hõlmaksid ainult väikese väärtusega veebioste. Veebiostude puhul kehtivad piirmäärad tuleks kehtestada läbimõeldumalt, kuna asjaolu, et isik ei ole ostu sooritamise ajal füüsiliselt kohal, kujutab enesest pisut suuremat turvariski.

(13) Nõuded kliendi tugevale autentimisele kehtivad maksja algatatud maksetele sõltumata sellest, kas maksja on füüsiline või juriidiline isik. Paljud äriühingute maksed algatatakse sihtotstarbeliste protsesside või protokollide vahendusel, mis tagavad samasuguse maksete kõrgetasemelise turvalisuse, mida direktiiv (EL) 2015/2366 tahab saavutada kliendi tugeva autentimisega. Kui pädevad asutused teevad kindlaks, et nimetatud makseprotsesside ja -protokollidega (mis on kättesaadavad ainult sellistele maksjatele, kes ei ole tarbijad) on saavutatud direktiivi (EL) 2015/2366 eesmärgid, mis käsitlevad turvalisust, võivad makseteenuse pakkujad nende protsesside või protokollidega seoses saada vabastuse kliendi tugeva autentimise nõuete täitmisest.

(14) Kui reaalajas toimuv tehingu riskianalüüs liigitab makse väikese riskiga tehingute hulka, tuleks samuti ette näha erand sellisele maksteenuse pakkujale, kes kavatseb mitte kohaldada kliendi tugevat autentimist, võttes vastu tulemuslikud ja riskipõhised nõuded, millega on tagatud makseteenuse kasutaja rahaliste vahendite ja isikuandmete turvalisus. Need riskipõhised nõuded peaksid omavahel kombineerima riskianalüüsi tulemused, mis kinnitavad, et ei ole tuvastatud maksja tavapäratuid kulutusi või tavapäratut käitumist, ja mille juures võetakse arvesse muid riskitegureid, nagu teave maksja ja makse saaja asukoha kohta, ning kaugmaksete jaoks välja arvutatud pettuste viitemääral põhinevad rahalised piirmäärad. Kui reaalajas toimuva tehingute riskianalüüsi põhjal ei saa makset liigitada väikese riskiga tehinguks, peaks makseteenuse pakkuja uuesti kasutusele võtma kliendi tugeva autentimise. Sellise riskipõhise erandi maksimumväärtus tuleks kehtestada selliselt, et sellele vastav pettuste määr oleks väga madal isegi võrreldes teatava perioodi kestel ja jooksvalt arvutatud pettuste määraga makseteenuse pakkuja kõigi maksetehingute, sealhulgas kliendi tugevat autentimist kasutades autenditud tehingute puhul.

(15) Tulemusliku rakendamise tagamiseks peaksid need makseteenuse pakkujad, kes soovivad kasutada erandit kliendi tugeva autentimise nõudest, korrapäraselt jälgima ning tegema pädevatele asutustele ja Euroopa Pangandusjärelevalvele (EBA) nende taotluse alusel kättesaadavaks pettuse teel tehtud või autoriseerimata maksetehingute väärtuse maksetehingu liikide kaupa ja pettuste määrad kõigi nende kaudu tehtud maksetehingute kohta nii nende tehingute puhul, mis on autenditud kliendi tugeva autentimise kaudu, kui ka nende puhul, mis on täidetud asjakohast erandit kasutades.

(16) Samuti aitab uute ajalooliste andmete kogumine elektrooniliste maksetehingute pettuste määra kohta EBA-l tulemuslikult läbi vaadata kliendi tugeva autentimise piirmäärad, mis põhinevad reaalajas toimuval tehingute riskianalüüsil. EBA peaks käesolevad regulatiivsed tehnilised standardid läbi vaatama ja esitama komisjonile vajaduse korral nende ajakohastamise kavandid, esitades uued kavandatavad piirmäärad ja neile vastavad pettuste määrad, et suurendada elektrooniliste kaugmaksete turvalisust kooskõlas direktiivi (EL) 2015/2366 artikli 98 lõikega 5 ning Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1093/2010 ([1]) artikliga 10.

(17) Makseteenuse pakkujatel, kes kasutavad mõnda kehtestatavatest eranditest, peaks alati olema lubatud rakendada omal valikul kliendi tugevat autentimist neile tegevustele ja maksetehingutele, millele on osutatud erandeid kehtestavates sätetes.

(18) Meetmed, millega kaitstakse isikustatud turvavolituste, samuti autentimisseadmete ja -tarkvara konfidentsiaalsust ja terviklust, peaksid piirama riske, mis on seotud makseinstrumentide autoriseerimata või pettuse teel kasutamisega ja maksekontole loata juurdepääsuga. Sel eesmärgil tuleb kehtestada nõuded, mis käsitlevad isikustatud turvavolituste turvalist andmist ja kättetoimetamist ning volituste sidumist makseteenuse kasutajaga, ning luua tingimused selliste volituste uuendamiseks ja deaktiveerimiseks.

(19) Selleks et tagada kontoteabe teenuste kontekstis tõhus ja turvaline teabevahetus asjaomaste osalejate vahel, tuleks kindlaks määrata teabevahetuse ühiste ja turvaliste avatud standardite nõuded, mida peavad rakendama kõik asjaomased makseteenuse pakkujad. Direktiiviga (EL) 2015/2366 on ette nähtud, et kontoteabe teenuse pakkujatel on juurdepääs maksekonto teabele ja et nad võivad seda kasutada. Käesoleva määrusega ei muudeta seega juurdepääsueeskirju selliste kontode puhul, mis ei ole maksekontod.

([1]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12).

(20) Kõik kontot haldavad makseteenuse pakkujad, kelle maksekontod on interneti kaudu juurdepääsetavad, peaksid pakkuma vähemalt üht juurdepääsuliidest, mis võimaldavad turvalist teabevahetust kontoteabe teenuse pakkujate, makse algatamise teenuse pakkujate ja kaardipõhiseid makseinstrumente väljastavate makseteenuse pakkujatega. Liidese kaudu peaks kontoteabe teenuse pakkujatel, makse algatamise teenuse pakkujatel ja kaardipõhiseid makseinstrumente väljastavatel makseteenuse pakkujatel olema võimalik ennast kontot haldavale makseteenuse pakkujale identifitseerida. Samuti peaks kontoteabe teenuse pakkujatel ja makse algatamise teenuse pakkujatel olema võimalik liidese kaudu kasutada kontot haldava makseteenuse pakkuja poolt makseteenuse kasutajale pakutavaid autentimismenetlusi. Tehnoloogia ja ärimudeli neutraalsuse tagamiseks peaks kontot haldavatel makseteenuse pakkujatel olema vabadus otsustada, kas nad võtavad kasutusele spetsiaalse liidese teabevahetuseks kontoteabe teenuse pakkujate, makse algatamise teenuse pakkujate ja kaardipõhiseid makseinstrumente väljastavatel makseteenuse pakkujatega, või lubavad nad sellise teabevahetuse eesmärgil kasutada liidest, mida kasutatakse kontot haldavate makseteenuse pakkujate makseteenuse kasutajate identifitseerimiseks ja nendega teabe vahetamiseks.

(21) Selleks et kontoteabe teenuse pakkujad, makse algatamise teenuse pakkujad ja kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad saaksid välja töötada oma tehnilised lahendused, peaks liidese tehnilise kirjelduse kohta olema piisav dokumentatsioon ja see peaks olema avalikult kättesaadav. Vähemalt kuus kuud enne käesolevate regulatiivsete standardite kohaldamiskuupäeva või siis enne liidese turul kasutusele võtmise kuupäeva (kui kasutusele võtmine toimub enne standardite kohaldamiskuupäeva) peaks kontot haldav makseteenuse pakkuja lisaks sellele sisse seadma süsteemi, mille kaudu saavad makseteenuse pakkujad testida tehnilisi lahendusi. Selleks et tagada erinevate teabevahetuseks kasutatavate tehnoloogiliste lahenduste koostalitlusvõime, tuleks liidese juures kasutada rahvusvaheliste või Euroopa standardiorganisatsioonide välja töötatud teabevahetusstandardeid.

(22) Kontoteabe teenuse pakkujate ja makse algatamise teenuse pakkujate pakutavate teenuste kvaliteet sõltub nende liideste nõuetekohasest toimimisest, mille kontot haldavad makseteenuse pakkujad on kasutusele võtnud või kohandanud. Seega on oluline võtta nimetatud teenuste kasutajate huvides meetmed talitluspidevuse tagamiseks juhul, kui need liidesed ei vasta käesolevate standardite sätetele. Riiklikud pädevad asutused vastutavad selle eest, et kontoteabe teenuse pakkujatel ja makse algatamise teenuse pakkujatel ei tehtaks võimatuks nende teenuste osutamist või neid seejuures ei takistataks.

(23) Kui juurdepääsu maksekontodele pakutakse spetsiaalse liidese vahendusel, siis selleks, et tagada makseteenuse kasutajatele direktiivis (EL) 2015/2366 sätestatud õigus kasutada makse algatamise teenuse pakkujaid ja teenuseid, mis võimaldavad juurdepääsu kontoteabele, tuleb spetsiaalsete liideste puhul nõuda, et nende kättesaadavus ja sooritusvõime oleksid samal tasemel nagu makseteenuse kasutaja kasutataval liidesel. Samuti peaksid kontot haldavad maksteenuse pakkujad kindlaks määrama spetsiaalsete liideste kättesaadavuse ja sooritusvõime läbipaistvad peamised tulemusnäitajad ja teenustaseme eesmärgid, mis on vähemalt niisama ranged nagu selle liidese puhul, mida kasutavad nende makseteenuse kasutajad. Neid liideseid peaksid katsetama makseteenuse pakkujad, kes neid kasutama hakkavad, ning seejärel peaksid neid stressitestis kontrollima ja nende toimimist jälgima pädevad asutused.

(24) Tagamaks, et spetsiaalset liidest kasutavad makseteenuse pakkujad saavad jätkata oma teenuste osutamist juhul, kui spetsiaalne liides ei ole kättesaadav või ei tööta nõuetekohaselt, tuleb rangetel tingimustel ette näha varumehhanism, mis võimaldab sellistel teenuseosutajatel kasutada liidest, mida kontot haldav makseteenuse pakkuja omab omaenese makseteenuse kasutajate identifitseerimiseks ja nendega teabe vahetamiseks. Teatavad kontot haldavad maksteenuse pakkujad vabastatakse kohustusest näha oma kasutajatele mõeldud liidese kaudu ette selline varumehhanism, kui nende pädevad asutused teevad kindlaks, et spetsiaalsed liidesed vastavad konkreetsetele tingimustele, mis tagavad takistamatu konkurentsi. Juhul kui nõuetest vabastatud spetsiaalsed liidesed ei suuda nõutud tingimusi täita, tühistavad asjaomased pädevad asutused antud vabastused.

(25) Selleks et pädevatel asutustel oleks võimalik teha teabevahetusliideste kasutuselevõtmise ja haldamise üle tulemuslikku järelevalvet ja kontrolli, peaks kontot haldav makseteenuse pakkuja tegema oma veebisaidil kokkuvõtte asjaomasest dokumentatsioonist ja esitama pädevatele asutustele taotluse korral dokumentatsiooni lahenduste kohta hädaolukorra puhuks. Samuti peaksid kontot haldavad makseteenuse pakkujad tegema avalikkusele kättesaadavaks statistika selle liidese kättesaadavuse ja sooritusvõime kohta.

(26) Andmete konfidentsiaalsuse ja tervikluse kaitseks tuleb tagada kontot haldavate makseteenuse pakkujate, kontoteabe teenuse pakkujate, makse algatamise teenuse pakkujate ja kaardipõhiseid makseinstrumente väljastavate makseteenuse pakkujate vaheliste teabevahetusseansside turvalisus. Eriti oluline on nõuda, et kontot

haldavad makseteenuse pakkujad, kontoteabe teenuse pakkujad, makse algatamise teenuse pakkujad ja kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad kasutaksid omavahel andmeid vahetades turvalist krüptimist.

(27) Selleks, et suurendada kasutajate usaldust ja tagada klientide tugev autentimine, tuleks arvesse võtta Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 ([1]) kohast e-identimise vahendite ja usaldusteenuste kasutamist, eriti seoses teavitatud e-identimise süsteemidega.

(28) Selleks et tagada kohaldamiskuupäevade omavaheline kooskõla, peaks käesolev määrus olema kohaldatav samast kuupäevast, millest alates liikmesriigid peavad tagama direktiivi (EL) 2015/2366 artiklites 65, 66, 67 ja 97 osutatud turvameetmete kohaldamise.

(29) Käesolev määrus põhineb regulatiivsete tehniliste standardite eelnõul, mille Euroopa Pangandusjärelevalve (EBA) esitas komisjonile.

(30) EBA on viinud läbi avalikud konsultatsioonid käesoleva määruse aluseks olevate regulatiivsete tehniliste standardite eelnõu kohta, analüüsinud võimalikku seonduvat kulu ja kasu ning küsinud arvamust määruse (EL) nr 1093/2010 artikli 37 kohaselt loodud pangandussektori sidusrühmade kogult,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

Käesoleva määrusega kehtestatakse nõuded, mida makseteenuse pakkujad peavad täitma, kui nad rakendavad turvameetmeid, mis võimaldavad neil teha järgmist:

a) kasutada kooskõlas direktiivi (EL) 2015/2366 artikliga 97 kliendi tugeva autentimise menetlust;

b) teha erand kliendi tugeva autentimise turvanõuete kohaldamisest, kui täidetud on kindlad ja piiratud tingimused, mis põhinevad riski tasemel, maksetehingu summal ja korduvusel ning selle täitmiseks kasutatud maksekanalil;

c) kaitsta makseteenuse kasutaja isikustatud turvavolituste konfidentsiaalsust ja terviklust;

d) kehtestada ühised ja turvalised teabevahetuse avatud standardid teabevahetuseks kontot haldavate makseteenuse pakkujate, makse algatamise teenuse pakkujate, kontoteabe teenuse pakkujate, maksjate, makse saajate ja muude makseteenuse pakkujate vahel seoses makseteenuste pakkumise ja kasutamisega, kohaldades direktiivi (EL) 2015/2366 IV jaotist.

Artikkel 2

Autentimise üldnõuded

1. Artikli 1 punktides a ja b osutatud turvameetmete rakendamise eesmärgil peavad makseteenuse pakkujatel olema tehinguseiremehhanismid, mis võimaldavad neil avastada autoriseerimata või pettuse teel tehtud maksetehinguid.

([1]) Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 53).

Need mehhanismid peavad tuginema maksetehingute analüüsile, mille juures võetakse arvesse elemente, mis on makseteenuse kasutajale iseloomulikud isikustatud turvavolituste tavapärase kasutamise puhul.

2. Makseteenuse pakkujad tagavad, et tehinguseiremehhanismid võtavad arvesse vähemalt kõiki järgmisi riskipõhiseid tegureid:

a) murtud või varastatud autentimisvahendite loetelu;

b) iga maksetehingu summa;

c) makseteenuste osutamisega seoses teada olevad petuskeemid;

d) märgid pahavaraga nakatumise kohta autentimismenetluse mis tahes seansi kestel;

e) juhul kui juurdepääsuseadme või -tarkvara annab kasutaja käsutusse makseteenuse pakkuja, logid sellise juurdepääsuseadme või -tarkvara kasutamise ning juurdepääsuseadme või -tarkvara tavapäratu kasutamise kohta.

Artikkel 3

Turvameetmete läbivaatamine

1. Artiklis 1 osutatud turvameetmete rakendamist tuleb kooskõlas makseteenuse pakkujale kohaldatava õigusraamistikuga dokumenteerida, korrapäraselt testida ja hinnata ning seda peavad auditeerima audiitorid, kellel on IT-turvalisuse ja elektronmaksete alane pädevus ning kes tegutsevad makseteenuse pakkujast sõltumatult või tema juures autonoomselt.

2. Lõikes 1 osutatud auditite vahelise perioodi kindlaksmääramisel võetakse arvesse asjaomast kohustusliku auditi ja raamatupidamisraamistikku, mida kohaldatakse makseteenuse pakkuja suhtes.

Siiski tuleb artiklis 18 osutatud erandit kasutavate makseteenuse pakkujate puhul vähemalt kord aastas auditeerida nende metoodikat, mudelit ja teatatud pettuste määra. Auditit tegeval audiitoril peab olema IT-turvalisuse ja elektrooniliste maksete alane pädevus ning ta peab tegutsema makseteenuse pakkujast sõltumatult või tema juures autonoomselt. Artikli 18 kohase erandi kasutamise esimese aasta jooksul ja seejärel vähemalt kord kolme aasta jooksul või sagedamini, kui pädev asutus seda nõuab, teeb auditit sõltumatu ja kvalifitseeritud välisaudiitor.

3. Kõnealuses auditis esitatakse hinnang ja aruanne selle kohta, kas makseteenuse pakkuja turvameetmed vastavad käesolevas määruses sätestatud nõuetele.

Kogu aruanne tuleb pädevatele asutustele nende taotluse alusel kättesaadavaks teha.

II PEATÜKK

TURVAMEETMED KLIENDI TUGEVA AUTENTIMISE KOHALDAMISEL

Artikkel 4

Autentimiskood

1. Kui makseteenuse pakkujad kohaldavad vastavalt direktiivi (EL) 2015/2366 artikli 97 lõikele 1 kliendi tugevat autentimist, peab autentimine põhinema kahel või enamal elemendil, mis kuuluvad teadmise, omamise ja tunnuse kategooriasse ning mille tulemusena genereeritakse autentimiskood.

Kui maksja kasutab autentimiskoodi selleks, et siseneda interneti kaudu oma maksekontole, algatada elektrooniline maksetehing või teha kaugejuurdepääsu teel mis tahes muu toiming, mille puhul võib esineda maksepettuse või muu kuritarvitamise oht, aktsepteerib makseteenuse pakkuja autentimiskoodi ainult ühel korral.

2. Lõike 1 kohaldamisel võtavad makseteenuse pakkujad kasutusele turvameetmeid, millega on tagatud, et täidetud on kõik järgmised tingimused:

a) avalikustatud autentimiskoodi põhjal ei ole võimalik tuletada mitte mingisugust teavet lõikes 1 osutatud elementide kohta;

b) mõnda muud varem genereeritud autentimiskoodi teades ei ole võimalik genereerida uut autentimiskoodi;

c) autentimiskoodi ei ole võimalik võltsida.

3. Makseteenuse pakkujad tagavad, et autentimine autentimiskoodi genereerimise kaudu hõlmab kõiki järgmisi meetmeid:

a) kui autentimise korral, mille eesmärk on kaugjuurdepääs, elektroonilise maksetehingu tegemine või kaugejuurdepääsu teel mis tahes muu sellise toimingu tegemine, mille puhul võib esineda maksepettuse või muu kuritarvitamise riski oht, nurjub lõike 1 kohase autentimiskoodi genereerimine, ei tohi olla võimalik kindlaks teha, milline kõnealuses lõikes osutatud elementidest oli väär;

b) üksteisele järgnevate nurjunud autentimiskatsete arv, mille järel direktiivi (EL) 2015/2366 artikli 97 lõikes 1 osutatud tegevused ajutiselt või alaliselt blokeeritakse, ei tohi teatava ajavahemiku jooksul olla üle viie;

c) vastavalt V peatüki nõuetele on teabevahetusseansid kaitstud autentimise käigus edastatud autentimisandmete hõive ja kõrvaliste isikute poolse manipuleerimise vastu;

d) pärast seda, kui maksja on interneti kaudu maksekontole sisenemiseks autenditud, ei tohi ta olla passiivne rohkem kui viis minutit.

4. Kui lõike 3 punktis b osutatud blokeering on ajutine, tuleb selle blokeeringu kestuse ja uute katsete arvu kehtestamisel tugineda maksjale osutatavate teenuste omadustele ja kõigile sellega kaasnevatele riskidele, võttes arvesse vähemalt artikli 2 lõikes 2 osutatud tegureid.

Enne alalise blokeeringu rakendamist teavitatakse maksjat.

Kui blokeering on muudetud alaliseks, tuleb kehtestada turvaline menetlus, mida kasutades maksja saab blokeeritud elektroonilised makseinstrumendid blokeeringust vabastada.

Artikkel 5

Dünaamilise lingi loomine

1. Kui makseteenuse pakkujad kohaldavad vastavalt direktiivi (EL) 2015/2366 artikli 97 lõikele 2 kliendi tugevat autentimist, peavad nad lisaks käesoleva määruse artikli 4 nõuete täitmisele kehtestama kõik järgmised turvameetmed:

a) maksjale teatatakse maksetehingu summa ja makse saaja;

b) genereeritud autentimiskood on konkreetselt seotud maksja poolt enne makse algatamist kinnitatud maksetehingu summa ja makse saajaga;

c) autentimiskood, mille makseteenuse pakkuja on aktsepteerinud, vastab maksetehingu algsele konkreetsele summale ja maksja poolt kinnitatud makse saajale;

d) summa või makse saaja mis tahes muudatus tingib genereeritud autentimiskoodi kehtetustamise.

2. Lõike 1 kohaldamisel võtavad makseteenuse pakkujad kasutusele turvameetmed, mis tagavad kõikide järgmiste andmete konfidentsiaalsuse, autentsuse ja tervikluse:

a) tehingu summa ja makse saaja kõigis autentimise etappides;

b) maksjale kuvatav teave kõigis autentimise etappides, sealhulgas autentimiskoodi genereerimise, edastamise ja kasutamise kestel.

3. Lõike 1 punkti b kohaldamisel ja kui makseteenuse pakkujad kohaldavad vastavalt direktiivi (EL) 2015/2366 artikli 97 lõikele 2 kliendi tugevat autentimist, kehtivad autentimiskoodile järgmised nõuded:

a) kui tegu on kaardipõhise maksetehinguga, mille puhul maksja on andnud oma nõusoleku täpse summa rahaliste vahendite blokeerimiseks vastavalt kõnealuse direktiivi artikli 75 lõikele 1, on autentimiskood konkreetselt seotud summaga, mille blokeerimiseks maksja on nõusoleku andnud ja millega ta on enne tehingu algatamist nõustunud;

b) kui tegu on maksetehingutega, mille puhul maksja on andnud oma nõusoleku ühele või mitmele makse saajale suunatud elektrooniliste kaugmaksetehingute seeria täitmiseks, on autentimiskood konkreetselt seotud erinevate tehingute kogusumma ja maksete kindlaksmääratud saajatega.

Artikkel 6

Nõuded teadmise kategooriasse kuuluvatele elementidele

1. Makseteenuse pakkujad võtavad kasutusele meetmed leevendamaks riski, et kõrvalised isikud saavad teada kliendi tugeva autentimise elemendid, mis kuuluvad teadmise kategooriasse, või et sellised elemendid neile isikutele avaldatakse.

2. Kui maksja kasutab neid elemente, tuleb kohaldada leevendusmeetmeid, et vältida elementide avalikustamist kõrvalistele isikutele.

Artikkel 7

Nõuded omamise kategooriasse kuuluvatele elementidele

1. Makseteenuse pakkujad võtavad kasutusele meetmed leevendamaks riski, et kõrvalised isikud kasutavad kliendi tugeva autentimise elemente, mis kuuluvad omamise kategooriasse.

2. Kui maksja kasutab neid elemente, tuleb kohaldada meetmeid elementide kopeerimise vältimiseks.

Artikkel 8

Nõuded seadmetele ja tarkvarale seoses olemuse kategooriasse kuuluvate elementidega

1. Makseteenuse pakkujad võtavad kasutusele meetmed leevendamaks riski, et kõrvalised isikud avastavad kliendi tugeva autentimise elemendid, mis kuuluvad olemuse kategooriasse ning mida loetakse maksja käsutusse antud juurdepääsuseadmete ja -tarkvara abil. Makseteenuse pakkujad tagavad vähemalt selle, et nende juurdepääsuseadmete ja -tarkvara puhul on väga väike tõenäosus, et kõrvaline isik autenditaks maksjana.

2. Kui maksja kasutab neid elemente, tuleb kohaldada meetmeid, millega tagatakse, et seadmeid ja tarkvara ei saa autoriseerimata kasutada juhul, kui olemas on juurdepääs seadmetele ja tarkvarale.

Artikkel 9

Elementide sõltumatus

1. Makseteenuse pakkujad tagavad, et nende kliendi tugeva autentimise elementide kasutamise suhtes, mille osutatakse artiklites 6, 7 ja 8, kohaldatakse meetmeid, mis tagavad tehnoloogia, algoritmide ja parameetrite puhul, et ühe elemendi rikkumine ei ohusta teiste usaldusväärsust.

2. Kui mõnda kliendi tugeva autentimise elementi või autentimiskoodi kasutatakse mitmeotstarbelises seadmes, võtavad makseteenuse pakkujad kasutusele turvameetmed, et leevendada selle mitmeotstarbelise seadme võimalikust murdmisest tulenevat riski.

3. Lõike 2 kohased leevendusmeetmed peavad sisaldama kõike järgmist:

a) mitmeotstarbelisse seadmesse paigaldatud tarkvara vahendusel kasutatakse üksteisest eraldatud turvalisi täitmiskeskkondi;

b) olemas on mehhanismid, millega tagatakse, et maksja või kolmas isik ei ole teinud muudatusi tarkvaras või seadme juures;

c) kui on tehtud muudatusi, on olemas mehhanismid nende tagajärgede leevendamiseks.

III PEATÜKK

ERANDID KLIENDI TUGEVAST AUTENTIMISEST

Artikkel 10

Maksekonto teave

1. Tingimusel, et täidetud on artiklis 2 ja käesoleva artikli lõikes 2 sätestatud nõuded, antakse makseteenuse pakkujatele luba mitte kohaldada kliendi tugevat autentimist juhul, kui maksjal on tundlikke makseandmeid avaldamata piiratud juurdepääs interneti kaudu ühele või mõlemale järgmistest elementidest:

a) ühe või mitme määratud maksekonto saldo;

b) viimase 90 päeva jooksul ühe või mitme määratud maksekonto kaudu täidetud tehingud.

2. Lõike 1 kohaldamisel ei ole makseteenuse pakkujad kliendi tugeva autentimise kohaldamisest vabastatud juhul, kui täidetud on üks järgmistest tingimustest:

a) makseteenuse kasutaja kasutab interneti kaudu juurdepääsu lõikes 1 osutatud teabele esimest korda;

b) on möödunud rohkem kui 90 päeva viimasest korrast, kui makseteenuse kasutaja kasutas internetipõhist juurdepääsu lõike 1 punktis b nimetatud teabele ja kui kohaldati kliendi tugevat autentimist.

Artikkel 11

Viipemaksed müügipunktis

Tingimusel, et täidetud on artiklis 2 sätestatud nõuded, antakse makseteenuse pakkujatele luba mitte kohaldada kliendi tugevat autentimist juhul, kui maksja algatab elektroonilise viipemaksetehingu, eeldusel, et täidetud on järgmised tingimused:

a) elektroonilise viipemaksetehingu üksiksumma ei ole suurem kui 50 eurot ja

b) maksja poolt viipemakseid võimaldava makseinstrumendiga algatatud elektrooniliste viipemaksetehingute kogusumma pärast kuupäeva, kui viimati kohaldati kliendi tugevat autentimist, ei ületa 150 eurot või

c) viipemakseid võimaldava makseinstrumendiga algatatud elektrooniliste viipemaksetehingute arv pärast viimast korda, kui kohaldati kliendi tugevat autentimist, ei ole suurem kui viis.

Artikkel 12

Personalita terminalid transpordi- ja parkimistasude maksmiseks

Tingimusel, et täidetud on artiklis 2 sätestatud nõuded, antakse makseteenuse pakkujatele luba mitte kohaldada kliendi tugevat autentimist juhul, kui maksja algatab personalita makseterminalis elektroonilise maksetehingu transpordi- või parkimistasu maksmise eesmärgil.

Artikkel 13

Usaldatavad makse saajad

1. Makseteenuse pakkujad kohaldavad kliendi tugevat autentimist juhul, kui maksja koostab oma kontot haldava makseteenuse pakkuja vahendusel usaldatavate makse saajate loetelu või muudab seda loetelu.

2. Tingimusel, et täidetud on autentimisele esitatavad üldnõuded, antakse makseteenuse pakkujatele luba mitte kohaldada kliendi tugevat autentimist juhul, kui maksja algatab maksetehingu ja makse saaja on kantud usaldatavate makse saajate loetellu, mille maksja on eelnevalt loonud.

Artikkel 14

Korduvad tehingud

1. Makseteenuse pakkujad kohaldavad kliendi tugevat autentimist juhul, kui maksja loob korduvate tehingute seeria, mille summa ja makse saaja on sama, seda seeriat muudab või selle esmakordselt algatab.

2. Tingimusel, et täidetud on autentimisele esitatavad üldnõuded, antakse makseteenuse pakkujatele luba mitte kohaldada kliendi tugevat autentimist kõikide hilisemate maksetehingute puhul, mis kuuluvad lõikes 1 osutatud maksetehingute seeriasse.

Artikkel 15

Kreeditkorraldused samale füüsilisele või juriidilisele isikule kuuluvate kontode vahel

Tingimusel, et täidetud on artiklis 2 sätestatud nõuded, antakse makseteenuse pakkujatele luba mitte kohaldada kliendi tugevat autentimist juhul, kui maksja teeb kreeditkorralduse ning maksja ja makse saaja on üks ja sama füüsiline või juriidiline isik ja mõlemat maksekontot haldab üks ja sama kontot haldav makseteenuse pakkuja.

Artikkel 16

Väikese väärtusega tehingud

Makseteenuse pakkujatele antakse luba mitte kohaldada kliendi tugevat autentimist juhul, kui maksja algatab elektroonilise kaugmaksetehingu ja täidetud on järgmised tingimused:

a) elektroonilise kaugmaksetehingu summa ei ole suurem kui 30 eurot ja

b) maksja poolt algatatud elektrooniliste kaugmaksetehingute kogusumma pärast eelmist korda, kui kohaldati kliendi tugevat autentimist, ei ületa 100 eurot või

c) maksja poolt algatatud elektroonilisi kaugmaksetehinguid pärast eelmist korda, kui kohaldati kliendi tugevat autentimist, ei ole rohkem kui viis üksteisele järgnevat individuaalset elektroonilist kaugmaksetehingut.

Artikkel 17

Äriühingute turvalised makseprotsessid ja -protokollid

Makseteenuse pakkujatele antakse luba mitte kasutada kliendi tugevat autentimist juriidiliste isikute puhul, kes algatavad elektroonilisi maksetehinguid selliseid sihtotstarbelisi makseprotsesse või -protokolle kasutades, mis tehakse kättesaadavaks ainult maksjatele, kes ei ole eratarbijad, kui pädevad asutused on veendunud, et sellised protsessid või protokollid tagavad vähemalt samaväärse turvalisuse taseme kui see, mis on sätestatud direktiivis (EL) 2015/2366.

Artikkel 18

Tehingu riskianalüüs

1. Makseteenuse pakkujatele antakse luba mitte kasutada kliendi tugevat autentimist juhul, kui maksja algatab elektroonilise kaugmaksetehingu, mille makseteenuse pakkuja on artiklis 2 ja käesoleva artikli lõike 2 punktis c osutatud tehinguseiremehhanismide alusel lugenud väikese riskiga tehinguks.

2. Lõikes 1 osutatud elektrooniline maksetehingut käsitletakse väikese riskiga tehinguna, kui täidetud on kõik järgmised tingimused:

a) seda liiki tehingutega seotud pettuste määr, mille teenusepakkuja on teatanud ja mis on arvutatud vastavalt artiklile 19, on sama suur või väiksem kui pettuste viitemäärad vastavalt „elektrooniliste kaardipõhiste kaugmaksete“ ja „elektrooniliste kreeditkorralduste“ puhul, mis on esitatud lisas toodud tabelis;

b) tehingu summa ei ületa asjakohast erandi tegemise piirmäära, mis on esitatud lisas toodud tabelis;

c) makseteenuse pakkujad ei ole reaalajas toimuva riskianalüüsi tulemusena avastanud ühtegi järgmistest asjaoludest:

   i) maksja tavapäratud kulutused või käitumismuster;

   ii) ebatavaline teave maksja seadme/tarkvara kasutamise kohta;

   iii) pahavaraga nakatumine autentimismenetluse mis tahes seansi kestel;

   iv) makseteenuste osutamisega seoses teadaolev petuskeem;

   v) maksja tavapäratu asukoht;

   vi) makse saaja kõrge riskitasemega asukoht.

3. Need makseteenuse pakkujad, kes kavatsevad vabastada elektroonilised maksetehingud kliendi tugevast autentimisest põhjusel, et need kujutavad enesest väikest riski, peavad arvesse võtma vähemalt järgmisi riskipõhiseid tegureid:

a) konkreetse kasutaja eelnevate kulutuste muster;

b) maksetehingute ajalugu makseteenuse pakkuja iga makseteenuse kasutaja puhul;

c) juhul kui juurdepääsuseadme või -tarkvara on kasutaja käsutusse andnud makseteenuse pakkuja, maksja ja makse saaja asukoht maksetehingu hetkel;

d) makseteenuse kasutaja maksekäitumine, mis on kasutaja maksetehingute ajalooga võrreldes tavapäratu.

Makseteenuse pakkuja antavas hinnangus koondatakse kõik need riskipõhised tegurid iga konkreetse tehingu riskiskooriks, et teha kindlaks, kas teatavat makset tohiks lubada ilma kliendi tugeva autentimiseta.

Artikkel 19

Pettuste määra arvutamine

1. Lisas toodud tabelis esitatud iga tehingute liigi puhul peab makseteenuse pakkuja tagama, et üldised pettuste määrad, mis on seotud nii nende tehingutega, mis autenditakse kliendi tugevat autentimist kasutades, kui ka nende tehingutega, mille täitmisel on kasutatud mõnda artiklites 13–18 osutatud eranditest, on sama suured või väiksemad, kui lisas toodud tabelis esitatud pettuste viitemäärad sama liiki maksetehingute puhul.

Üldise pettuste määra arvutamisel iga tehingute liigi kohta korrapäraselt kord kvartalis (90 päeva jooksul) jagatakse autoriseerimata või pettuse teel tehtud kaugtehingute koguväärtus sõltumata sellest, kas rahalised vahendid on tagasi saadud või mitte, kõigi sama liiki kaugtehingute koguväärtusega sõltumata sellest, kas need tehingud, on autenditud kliendi tugevat autentimist kasutades või on nende täitmisel kasutatud mõnda artiklites 13–18 osutatud eranditest.

2. Pettuste määra arvutamist ja sellest tulenevaid arvandmeid hinnatakse artikli 3 lõikes 2 osutatud auditi käigus, mis tagab, et need on täielikud ja täpsed.

3. Makseteenuse pakkuja poolt pettuste määra arvutamisel kasutatavat metoodikat ja mis tahes mudelit, samuti pettuste määrasid tuleb piisavalt dokumenteerida ning need tuleb taotluse alusel täies ulatuses kättesaadavaks teha pädevatele asutustele ja tingimusel, et asjaomast pädevat asutust/asjaomaseid pädevaid asutusi eelnevalt teavitatakse, EBA-le.

Artikkel 20

Erandite kasutamise lõpetamine tehingu riskianalüüsi alusel

1. Makseteenuse pakkujad, kes kasutavad artiklis 18 osutatud erandit, teatavad pädevatele asutustele viivitamata sellest, kui mõni nende jälgitavatest pettuste määradest ükskõik millise lisas toodud tabelis esitatud liiki maksetehingu puhul ületab kohaldatavat pettuste viitemäära, ja esitavad pädevatele asutustele selliste meetmete kirjelduse, mida nad kavatsevad võtta, et viia nende seiratav pettuste määr taas kooskõlla pettuste kohaldatavate viitemääradega.

2. Makseteenuse pakkujad lõpetavad viivitamata artiklis 18 osutatud erandi kasutamise ükskõik millist lisas toodud tabelis esitatud liiki maksetehingu puhul konkreetses erandi kohaldamise vahemikus, kui nende jälgitav pettuste määra ületab kahe järjestikuse kvartali kestel pettuste viitemäära, mida kohaldatakse selle makseinstrumendi või seda liiki maksetehingu suhtes selles erandi kohaldamise vahemikus.

3. Pärast artiklis 18 osutatud erandi lõpetamist kooskõlas käesoleva artikli lõikega 2 ei kasuta makseteenuse pakkujad seda erandit uuesti seni, kuni nende arvutustel põhinev pettuste määr on ühe kvartali kestel sama suur või väiksem kui pettuste viitemäär, mida kohaldatakse seda liiki maksetehingute suhtes selles erandi kohaldamise vahemikus.

4. Kui makseteenuse pakkujad kavatsevad uuesti kasutada artiklis 18 osutatud erandit, teatavad nad sellest pädevatele asutustele mõistliku aja jooksul ja esitavad enne erandi uuesti kasutamist tõendid selle kohta, et nende jälgitav pettuste määr on taas kooskõlla viidud pettuste viitemääradega, mida kohaldatakse selles erandi kohaldamise vahemikus vastavalt käesoleva artikli lõikele 3.

Artikkel 21

Tehinguseire

1. Artiklites 10–18 sätestatud erandite kasutamiseks peavad makseteenuse pakkujad vähemalt kvartalipõhiselt salvestama ja seirama järgmisi andmeid igat liiki maksetehingute kohta, esitades tehingute jaotuse eraldi nii kaugmaksetehingute kui ka muude kui kaugmaksetehingute puhul:

a) autoriseerimata või pettuse teel tehtud tehingute koguväärtus vastavalt direktiivi (EL) 2015/2366 artikli 64 lõikele 2, kõigi maksetehingute koguväärtus ja sellest tulenev pettuste määr, sealhulgas maksetehingute jaotus kliendi tugevat autentimist kasutades algatatud tehingute puhul ja erandit kasutades algatatud tehingute puhul iga erandi kohta eraldi;

b) tehingu keskmine väärtus, sealhulgas maksetehingute jaotus kliendi tugevat autentimist kasutades algatatud tehingute puhul ja erandit kasutades algatatud tehingute puhul iga erandi kohta eraldi;

c) selliste tehingute arv, mille puhul igat erandit kohaldati, ja nende osakaal maksetehingute koguarvust.

2. Makseteenuse pakkujad teevad lõike 1 kohase jälgimise tulemused taotluse alusel kättesaadavaks pädevatele asutustele ja tingimusel, et asjaomast pädevat asutust/asjaomaseid pädevaid asutusi eelnevalt teavitatakse, EBA-le.

IV PEATÜKK

MAKSETEENUSE KASUTAJA ISIKUSTATUD TURVAVOLITUSTE KONFIDENTSIAALSUS JA TERVIKLUS

Artikkel 22

Üldnõuded

1. Makseteenuse pakkujad tagavad makseteenuse kasutaja isikustatud turvavolituste, sealhulgas autentimiskoodide konfidentsiaalsuse ja tervikluse kõigis autentimise etappides.

2. Lõike 1 kohaldamisel tagavad makseteenuse pakkujad, et täidetud on kõik järgmised tingimused:

a) kui isikustatud turvavolitusi kuvatakse, on need varjatud, ja kui makseteenuse kasutaja neid autentimise jooksul sisestab, ei ole neid võimalik täies ulatuses lugeda;

b) andmeformaadis isikustatud turvavolitusi, samuti isikustatud turvavolituste krüpteerimisega seotud krüptitud materjali ei säilitata vorminguvaba teksti kujul;

c) salastatud krüptitud materjal on kaitstud loata avalikustamise eest.

3. Makseteenuse pakkujad dokumenteerivad täies ulatuses protsessi, mis on seotud isikustatud turvavolituste krüpteerimiseks või muul viisil loetamatuks muutmiseks kasutatava krüptitud materjali haldamisega.

4. Makseteenuse pakkujad tagavad, et isikustatud turvavolituste ja II peatüki kohaselt genereeritud autentimiskoodide töötlemine ja marsruutimine toimub turvalistes keskkondades kooskõlas rangete ja laialdaselt tunnustatud valdkonnastandarditega.

Artikkel 23

Turvavolituste loomine ja edastamine

Makseteenuse pakkujad tagavad, et isikustatud turvavolitused luuakse turvalises keskkonnas.

Nad leevendavad isikustatud turvavolituste, autentimisseadmete ja -tarkvara autoriseerimata kasutamise riski, mis tuleneb nende kaotamisest, vargusest või kopeerimisest enne maksjale üleandmist.

Artikkel 24

Seostamine makseteenuse kasutajaga

1. Makseteenuse pakkujad tagavad, et isikustatud turvavolituste, autentimisseadmete ja -tarkvaraga on turvalisel viisil seostatud ainult makseteenuse kasutaja.

2. Lõike 1 kohaldamisel tagavad makseteenuse pakkujad, et täidetud on kõik järgmised tingimused:

a) makseteenuse kasutaja isikusamasuse seostamine isikustatud turvavolituste, autentimisseadmete ja -tarkvaraga toimub turvalistes keskkondades, mille eest vastutab makseteenuse pakkuja ja mis hõlmab vähemalt makseteenuse pakkuja ruume, makseteenuse pakkuja poolt ette nähtud internetikeskkonda või muid sarnaseid turvalisi veebisaite, mida makseteenuse kasutaja kasutab, ja tema pangaautomaaditeenuseid, ning võttes arvesse riske, mis tulenevad seostamisprotsessi jooksul seadmetest ja nende koosteelementidest, mille eest ei vastuta makseteenuse pakkuja;

b) makseteenuse kasutaja isikusamasuse seostamine isikustatud turvavolituste ning autentimisseadmete või -tarkvaraga kaugjuurdepääsu teel toimub kliendi tugevat autentimist kasutades.

Artikkel 25

Volituste, autentimisseadmete ja -tarkvara kättetoimetamine

1. Makseteenuse pakkujad tagavad, et isikustatud turvavolituste, autentimisseadmete ja -tarkvara kättetoimetamine toimub turvalisel viisil, mis on töötatud välja riskide käsitlemiseks seoses nende kaotamisest, vargusest või kopeerimisest tuleneva autoriseerimata kasutamisega.

2. Lõike 1 kohaldamisel rakendavad makseteenuse pakkujad vähemalt kõiki järgmisi meetmeid:

a) tulemuslikud ja turvalised kättetoimetamismehhanismid, millega on tagatud, et isikustatud turvavolitused, autentimisseadmed ja -tarkvara toimetatakse makseteenuse seadusliku kasutaja kätte;

b) mehhanismid, mis võimaldavad makseteenuse pakkujal kontrollida makseteenuse kasutajale interneti teel kätte toimetatud autentimistarkvara autentsust;

c) kord, millega tagatakse, et kui isikustatud turvavolitused toimetatakse kätte väljapool makseteenuse pakkuja ruume või kaugjuurdepääsu teel, siis:

   i) ei ole kõrvalistel isikutel võimalik enese kätte saada enam kui üht isikustatud turvavolituste, autentimisseadme või -tarkvara elementidest, kui need toimetatakse kätte sama kanali kaudu;

   ii) tuleb kättetoimetatud isikustatud turvavolitused, autentimisseadmed või -tarkvara enne nende kasutamist aktiveerida;

d) kord, millega tagatakse, et kui isikustatud turvavolitused, autentimisseadmed või -tarkvara tuleb enne nende esmakordset kasutamist aktiveerida, siis toimub aktiveerimine turvalises keskkonnas kooskõlas artiklis 24 osutatud seostamismenetlusega.

Artikkel 26

Isikustatud turvavolituste uuendamine

Makseteenuse pakkujad tagavad, et isikustatud turvavolituste uuendamise või uuesti aktiveerimise korral peetakse kinni turvavolituste ja autentimisseadmete artiklite 23, 24 ja 25 kohasest loomise, kasutajaga seostamise või kättetoimetamise menetlusest.

Artikkel 27

Hävitamine, deaktiveerimine ja tühistamine

Makseteenuse pakkujad tagavad, et neil on olemas tulemuslikud menetlused kõigi järgmiste turvameetmete rakendamiseks:

a) isikustatud turvavolituste, autentimisseadmete ja -tarkvara turvaline hävitamine, deaktiveerimine või tühistamine;

b) kui makseteenuse pakkuja poolt jagatavad autentimisseadmed ja -tarkvara on taaskasutatavad, on enne seadme või tarkvara teisele makseteenuse kasutajale kättesaadavaks tegemist ette nähtud, dokumenteeritud ja rakendatud selle turvaline taaskasutus;

c) makseteenuse pakkuja süsteemides ja andmebaasides ning vajaduse korral avalikes andmehoidlates säilitatava ja isikustatud turvavolitustega seotud teabe deaktiveerimine või tühistamine.

V PEATÜKK

ÜHISED JA TURVALISED TEABEVAHETUSE AVATUD STANDARDID

1. jagu

Üldnõuded teabevahetusele

Artikkel 28

Nõuded identifitseerimisele

1. Makseteenuse pakkujad tagavad turvalise identifitseerimise maksja seadme ja makse saaja elektrooniliste maksete vastuvõtmisseadmete, sealhulgas, kuid mitte ainult, makseterminalide vahelise teabevahetuse käigus.

2. Makseteenuse pakkujad tagavad, et mobiilirakendusi ja muid makseteenuse pakkuja elektrooniliste maksete teenuste kasutajaliideseid kasutades leevendatakse tulemuslikult teabevahetuse kõrvalistele isikutele ümbersuunamise riski.

Artikkel 29

Jälgitavus

1. Makseteenuse pakkujad peavad olema kehtestanud korra, millega tagatakse, et kõik maksetehingud ja muu suhtlus makseteenuse kasutaja, muude teenusepakkujate ja muude üksuste, sealhulgas kaupade vahendajatega makseteenuste osutamise kontekstis on jälgitavad, nii et kõik elektronilise tehinguga seotud sündmused kõigis erinevates etappides oleksid tagantjärele teada.

2. Lõike 1 kohaldamisel tagavad makseteenuse pakkujad, et kõigi makseteenuse kasutaja, muude teenusepakkujate ja muude üksuste, sealhulgas kaupade vahendajatega loodud teabevahetusseansside juures kasutatakse kõiki järgmisi elemente:

a) seansi unikaalne tunnuskood;

b) turvamehhanismid tehingu, sealhulgas tehingu numbri, ajatemplite ja kõigi asjaomaste tehinguandmete üksikasjalikuks logimiseks;

c) ajatemplid, mis põhinevad ühtlustatud ajaviidete süsteemil ja mis sünkroniseeritakse ametliku ajasignaaliga.

2. jagu

Erinõuded ühiste ja turvaliste teabevahetuse avatud standardite kohta

Artikkel 30

Üldised kohustused seoses juurdepääsuliidestega

1. Kontot haldavad makseteenuse pakkujad, kes pakuvad maksjale interneti kaudu juurdepääsetavat maksekontot, peavad sisse seadma vähemalt ühe liidese, mis vastab kõigile järgmistele nõuetele:

a) kontoteabe teenuse pakkujad, makse algatamise teenuse pakkujad ja kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad saavad ennast kontot haldavale makseteenuse pakkujale identifitseerida;

b) kontoteabe teenuse pakkujatel on võimalus turvaliseks teabevahetuseks, et nõutada ja saada teavet ühe või enama määratud maksekonto ja sellega seotud maksetehingute kohta;

c) makse algatamise teenuse pakkujatel on võimalus turvaliseks teabevahetuseks, et algatada maksja kontol maksekorraldus ning saada kogu teave maksetehingu algatamise kohta ja kogu teave, mis on kontot haldavale makseteenuse pakkujale kättesaadav maksetehingu täitmise kohta.

2. Makseteenuse kasutaja autentimise eesmärgil peab lõikes 1 osutatud liides samuti võimaldama kontoteabe teenuse pakkujatel ja makse algatamise teenuse pakkujatel kasutada kõiki kontot haldava makseteenuse pakkuja poolt makseteenuse kasutajale pakutavaid autentimismenetlusi.

Liides peab vastama vähemalt kõikidele järgmistele nõuetele:

a) makse algatamise teenuse pakkujal või kontoteabe teenuse pakkujal peab olema võimalik anda kontot haldavale makseteenuse pakkujale makseteenuse kasutaja nõusoleku alusel juhised alustada autentimist;

b) kogu autentimise kestel alustatakse ja säilitatakse teabevahetusseansse kontot haldava makseteenuse pakkuja, kontoteabe teenuse pakkuja, makse algatamise teenuse pakkuja ja asjaomase makseteenuse pakkuja vahel;

c) isikustatud turvavolituste ning kontoteabe teenuse pakkuja või makse algatamise teenuse pakkuja poolt või tema kaudu edastatud autentimiskoodide terviklus ja konfidentsiaalsus on tagatud.

3. Kontot haldavad makseteenuse pakkujad tagavad, et nende liidesed vastavad rahvusvaheliste või Euroopa standardiorganisatsioonide poolt välja antud teabevahetuse standarditele.

Samuti tagavad kontot haldavad makseteenuse pakkujad selle, et kõigi liideste tehnilise kirjelduse dokumenteerimisel määratakse kindlaks rutiinid, protokollid ja vahendid, mida makse algatamise teenuse pakkujad, kontoteabe teenuse pakkujad ja kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad vajavad selleks, et nende tarkvara ja rakendused oleksid kontot haldavate makseteenuse pakkujate süsteemidega koostalitlusvõimelised.

Kontot haldavad makseteenuse pakkujad teevad hiljemalt ja mitte vähem kui kuus kuud enne artikli 38 lõikes 2 osutatud kohaldamiskuupäeva või enne juurdepääsuliidese kasutuselevõtmise sihtkuupäeva, kui kasutuselevõtmine toimub pärast artikli 38 lõike 2 osutatud kuupäeva, dokumentatsiooni tasuta kättesaadavaks selleks taotluse esitanud tegevusluba omavatele makse algatamise teenuse pakkujatele, kontoteabe teenuse pakkujatele ja kaardipõhiseid makseinstrumente väljastavatele makseteenuse pakkujatele või sellistele makseteenuse pakkujatele, kes on taotlenud oma pädevatelt asutustelt vastava tegevusloa saamist, ning teevad dokumentatsiooni kokkuvõtte oma veebisaitidel avalikkusele kättesaadavaks.

4. Lisaks lõikele 3 tagavad kontot haldavad makseteenuse pakkujad selle, et igasugune muudatus nende liidese tehnilises kirjelduses tehakse makse algatamise teenuse pakkujatele, kontoteabe teenuse pakkujatele ja kaardipõhiseid makseinstrumente väljastavatele makseteenuse pakkujatele või sellistele makseteenuse pakkujatele, kes on taotlenud oma pädevatelt asutustelt vastava tegevusloa saamist, eelnevalt kättesaadavaks nii vara kui võimalik ja mitte hiljem kui kolm kuud enne muudatuse kasutusele võtmist, välja arvatud eriolukorras.

Makseteenuse pakkujad dokumenteerivad eriolukorrad, milles muudatused on kasutusele võetud, ja esitavad dokumentatsiooni taotluse alusel pädevatele asutustele.

5. Kontot haldavad makseteenuse pakkujad teevad ühenduse ja funktsioonide katsetamiseks kättesaadavaks testimissüsteemi, mis hõlmab kasutajatuge, et makse algatamise teenuse pakkujatel, kontoteabe teenuse pakkujatel ja kaardipõhiseid makseinstrumente väljastavatel makseteenuse pakkujatel või sellistel makseteenuse pakkujatel, kes on taotlenud oma pädevatelt asutustelt vastava tegevusloa saamist, oleks võimalik testida oma tarkvara ja rakendusi, mida kasutatakse kasutajatele makseteenuse pakkumiseks. See testimissüsteem tuleks teha kättesaadavaks mitte vähem kui kuus kuud enne artikli 38 lõikes 2 osutatud kohaldamiskuupäeva või enne juurdepääsuliidese kasutuselevõtmise sihtkuupäeva, kui kasutuselevõtmine toimub pärast artikli 38 lõike 2 osutatud kuupäeva.

Siiski ei jagata testimissüsteemi kaudu tundlikku teavet.

6. Pädevad asutused tagavad, et kontot haldavad makseteenuse pakkujad täidavad igal ajal kohustusi, mis on käesolevates standardites ette nähtud nende poolt loodava(te) liides(t)e puhul. Juhul kui kontot haldav makseteenuse pakkuja jätab täitmata käesolevates standardites sätestatud liideste kohta käivad nõuded, tagavad pädevad asutused, et makse algatamise teenuste ja kontoteabe teenuste osutamist ei takistata ega häirita, kui selliste teenuste osutajad vastavad artikli 33 lõikes 5 kehtestatud tingimustele.

Artikkel 31

Võimalused seoses juurdepääsuliidesega

Kontot haldavad makseteenuse pakkujad loovad artiklis 30 osutatud liides(ed) kas kasutades spetsiaalset liidest või siis võimaldades artikli 30 lõikes 1 osutatud makseteenuse pakkujatel kasutada liideseid, mida kasutatakse autentimiseks ja teabevahetuseks kontot haldava makseteenuse pakkuja makseteenuste kasutajatega.

Artikkel 32

Spetsiaalse liidesega seotud kohustused

1. Vastavalt artiklitele 30 ja 31 tagavad sellised kontot haldavad makseteenuse pakkujad, kes on loonud spetsiaalse liidese, et spetsiaalne liides võimaldab igal ajal samal tasemel kättesaadavust ja sooritusvõimet nagu nende liideste puhul, mis on tehtud kättesaadavaks makseteenuse kasutajale maksekontole otse sisenemiseks interneti kaudu.

2. Kontot haldavad makseteenuse pakkujad, kes on loonud spetsiaalse liidese, määravad kindlaks läbipaistvad peamised tulemusnäitajad ja teenustaseme eesmärgid, mis on nii kättesaadavuse kui ka artikliga 36 kooskõlas edastatavate andmete seisukohast vähemalt niisama ranged nagu selle liidese puhul, mida kasutavad nende makseteenuste kasutajad. Pädevad asutused jälgivad neid liideseid, näitajaid ja eesmärkide saavutamist ning korraldavad stressiteste.

3. Kontot haldavad makseteenuse pakkujad, kes on loonud spetsiaalse liidese, tagavad, et selline liides ei takista makse algatamise ja kontoteabe teenuste osutamist. Takistamine võib muu hulgas hõlmata seda, et artikli 30 lõikes 1 osutatud makseteenuse pakkujatel takistatakse selliste volituste kasutamist, mille kontot haldavad makseteenuse pakkujad on andnud oma klientidele, neid suunatakse sunniviisiliselt kasutama kontot haldava makseteenuse pakkuja autentimist või muid funktsioone, neilt nõutakse täiendavaid autoriseerimisi ja registreerimisi lisaks neile, mis on sätestatud direktiivi (EL) 2015/2366 artiklites 11, 14 ja 15, või nõutakse, et nad täiendavalt kontrolliks nõusolekut, mille makseteenuse kasutaja on andnud kontoteabe ja makse algatamise teenuste osutajatele.

4. Lõigete 1 ja 2 kohaldamisel jälgivad kontot haldavad makseteenuse pakkujad spetsiaalse liidese kättesaadavust ja sooritusvõimet. Kontot haldavad makseteenuse pakkujad avaldavad oma veebisaidil kvartalistatistika spetsiaalse liidese ja makseteenuse kasutajate poolt kasutatava liidese kättesaadavuse ja sooritusvõime kohta.

Artikkel 33

Eriolukorra meetmed spetsiaalse liidese jaoks

1. Kontot haldavad makseteenuse pakkujad peavad spetsiaalse liidese ülesehituse juures ette nägema strateegia ja kava eriolukorra meetmete võtmiseks juhul, kui sihtotstarbeline liides ei toimi artikli 32 kohaselt, kui liides on plaaniväliselt mittekasutatav ja kui süsteemi töö on katkenud. Seda, et liides on plaaniväliselt mittekasutatav või et süsteemi töö on katkenud, võib eeldada, kui viiele järjestikusele teabele juurdepääsu taotlusele, mis on esitatud makse algatamise teenuse või kontoteabe teenuse osutamise eesmärgil, ei laeku vastust 30 sekundi jooksul.

2. Eriolukorra meetmete hulka peavad kuuluma teavituskavad, et teavitada spetsiaalset liidest kasutavaid makseteenuse pakkujaid meetmetest süsteemi taastamiseks, ja kirjeldus olemasolevate alternatiivsete võimaluste kohta, mida makseteenuse pakkujad selle aja jooksul saavad kasutada.

3. Nii kontot haldavad makseteenuse pakkujad kui ka artikli 30 lõikes 1 osutatud makseteenuse pakkujad teatavad spetsiaalse liidese probleemidest lõikes 1 kirjeldatud viisil viivitamata vastavatele riiklikele pädevatele asutustele.

4. Osana eriolukorra mehhanismist on artikli 30 lõikes 1 osutatud makseteenuse pakkujatel lubatud seni, kuni on taastatud spetsiaalse liidese kättesaadavuse ja sooritusvõime artikliga 32 ette nähtud tase, kasutada neid liideseid, mis on autentimise ja kontot haldava makseteenuse pakkujaga teabe vahetamise eesmärgil kättesaadavaks tehtud makseteenuse kasutajale.

5. Sel eesmärgil tagavad kontot haldavad makseteenuse pakkujad, et artikli 30 lõikes 1 osutatud makseteenuse pakkujaid on võimalik identifitseerida ja et nad saavad kasutada autentimismenetlusi, mille kontot haldav makseteenuse pakkuja on ette näinud makseteenuse kasutajale. Kui artikli 30 lõikes 1 osutatud makseteenuse pakkujad kasutavad lõikes 4 osutatud liidest, siis nad:

a) võtavad vajalikud meetmed tagamaks, et nad ei kasuta, püüa saada ega säilita mingeid andmeid muul eesmärgil kui maksja poolt taotletud teenuse osutamine;

b) jätkavad direktiivi (EL) 2015/2366 artikli 66 lõikest 3 ja artikli 67 lõikest 2 tulenevate kohustuste täitmist;

c) koostavad logi andmete kohta, millele saadi juurdepääs liidese kaudu, mida kontot haldav makseteenuse pakkuja haldab oma makseteenuse kasutajate jaoks, ja esitavad logifailid oma riiklikule pädevale asutusele taotluse alusel ja põhjendamatu viivituseta;

d) esitavad oma riiklikule pädevale asutusele taotluse alusel ja põhjendamatu viivituseta nõuetekohase põhjenduse sellise liidese kasutamise kohta, mida kontot haldav makseteenuse pakkuja haldab oma makseteenuse kasutajate jaoks;

e) teavitavad sellest kontot haldavat makseteenuse pakkujat.

6. Pädevad asutused, kes on järgmiste tingimuste järjepideva kohaldamise tagamiseks eelnevalt EBAga konsulteerinud, vabastavad spetsiaalse liidese kasuks otsustanud kontot haldavad makseteenuse pakkujad kohustusest luua lõikes 4 kirjeldatud eriolukorra mehhanism, kui sihtotstarbeline liides vastab kõikidele järgmistele tingimustele:

a) see täidab kõiki artiklis 32 spetsiaalsetele liidestele seatud tingimusi;

b) see on kavandatud ja seda on testitud kooskõlas artikli 30 lõikega 5 ning kõnealuses sättes osutatud makseteenuse pakkujaid rahuldaval viisil;

c) makseteenuse pakkujad on seda vähemalt kolm kuud laialdaselt kasutatud kontoteabe teenuste ja makse algatamise teenuste osutamiseks ning rahaliste vahendite olemasolu kinnitamiseks kaardipõhiste maksete puhul;

d) kõik spetsiaalse liidesega seotud probleemid on lahendatud põhjendamatu viivituseta.

7. Pädevad asutused tühistavad lõikes 6 osutatud vabastuse, kui kontot haldavad makseteenuse pakkuja ei vasta rohkem kui kahe järjestikuse kalendrinädala jooksul tingimustele a ja d. Pädevad asutused teatavad tühistamisest EBA-le ning tagavad, et kontot haldav makseteenuse pakkuja loob võimalikult lühikese aja jooksul ja hiljemalt kahe kuu möödudes lõikes 4 osutatud eriolukorra mehhanismi.

Artikkel 34

Sertifikaadid

1. Artikli 30 lõike 1 punktis a osutatud identifitseerimise eesmärgil kasutavad makseteenuse pakkujad määruse (EL) nr 910/2014 artikli 3 lõikes 30 osutatud e-templi kvalifitseeritud sertifikaate või kõnealuse määruse artikli 3 lõikes 39 osutatud veebisaidi autentimist.

2. Käesoleva määruse kohaldamisel tähendab määruse (EL) nr 910/2014 III lisa punkti c või IV lisa punkti c kohane registrinumber, nagu see on esitatud ametlikes dokumentides, kaardipõhiseid makseinstrumente väljastava makseteenuse pakkuja, kontoteabe teenuse pakkuja ja makse algatamise teenuse pakkuja, sealhulgas selliseid teenuseid pakkuva kontot haldavate makseteenuse pakkuja, tegevusloa numbrit, mis on kättesaadav päritoluliikmesriigi avaliku registri kaudu vastavalt direktiivi (EL) 2015/2366 artiklile 14 või mis tuleneb teadetest, mis esitatakse kooskõlas Euroopa Parlamendi ja nõukogu direktiivi 2013/36/EL ([1]) artikliga 20 iga kõnealuse direktiivi artikli 8 kohaselt antud tegevusloa kohta.

3. Käesoleva määruse kohaldamisel peavad lõikes 1 osutatud e-templi kvalifitseeritud sertifikaadid sisaldama rahvusvahelises rahanduses tavapäraselt kasutatavas keeles esitatud täiendavaid eritunnuseid kõige järgmise kohta:

a) makseteenuse pakkuja roll, mis võib seisneda ühes või mitmes järgmises tegevuses:

   i) konto haldamine;

   ii) maksete algatamine;

   iii) maksekonto teabe andmine;

   iv) kaardipõhiste makseinstrumentide väljastamine;

b) makseteenuse pakkuja registrijärgse asukoha pädevate asutuste nimed.

4. Lõikes 3 osutatud tunnused ei tohi mõjutada e-templi või veebisaidi autentimise kvalifitseeritud sertifikaatide koostalitlusvõimet ja tunnustamist.

([1]) Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338).

Artikkel 35

Teabevahetusseansi turvalisus

1. Kontot haldavad makseteenuse pakkujad, kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad, kontoteabe teenuse pakkujad ja makse algatamise teenuse pakkujad tagavad, et internetipõhise teabevahetuse käigus kohaldavad teabevahetuse pooled andmete konfidentsiaalsuse ja tervikluse kaitsmiseks kogu asjakohase sideseansi kestel turvalist krüptimist, kasutades tugevaid ja üldtunnustatud krüptimismeetodeid.

2. Kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad, kontoteabe teenuse pakkujad ja makse algatamise teenuse pakkujad tagavad, et kontot haldava makseteenuse pakkuja poolt pakutavad juurdepääsuseansid on võimalikult lühikesed, ning lõpetavad aktiivselt kõik sellised sessioonid kohe, kui soovitud tegevus on sooritatud.

3. Paralleelsete veebiseansside korral kontot haldava makseteenuse pakkujaga tagavad kontoteabe teenuse pakkujad ja makse algatamise teenuse pakkujad, et sellised seansid on turvaliselt seotud makseteenuse kasutajaga loodud vastavate seanssidega, vältimaks võimalust, et mis tahes nende vahel vahetatud sõnumit või teavet võidakse valesti marsruutida.

4. Kontoteabe teenuse pakkujad, makse algatamise teenuse pakkujad ja kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad esitavad kontot haldava makseteenuse pakkujaga teavet vahetades üheselt mõistatavad viited kõigile järgmistele elementidele:

a) makseteenuse kasutaja või kasutajad ning vastav teabevahetusseanss, et eristada üksteisest sama kasutaja või samade kasutajate esitatud päringud;

b) makse algatamise teenuste puhul algatatud maksetehing, mis on üheselt identifitseeritud;

c) rahaliste vahendite kättesaadavuse kinnituse puhul üheselt identifitseeritud taotlus seoses kaardipõhise maksetehingu täitmiseks vajaliku summaga.

5. Kontot haldavad makseteenuse pakkujad, kontoteabe teenuse pakkujad, makse algatamise teenuse pakkujad ja kaardipõhiseid makseinstrumente väljastavad makseteenuse pakkujad tagavad, et kui nad edastavad isikustatud turvavolitusi ja autentimiskoode, siis ei ole need ühegi töötaja jaoks ühelgi hetkel ei otseselt ega kaudselt loetavad.

Juhul kui isikustatud turvavolitused kaotavad konfidentsiaalsuse nende teenusepakkujate pädevuse piires, teatavad nad põhjendamatu viivituseta nendega seotud makseteenuse kasutajat ja isikustatud turvavolituste väljaandjat.

Artikkel 36

Andmevahetus

1. Kontot haldavad makseteenuse pakkujad peavad täitma kõiki järgmisi nõudeid:

a) nad esitavad kontoteabe teenuse pakkujatele sama kontoteabe määratud maksekontode ja nendega seotud maksetehingute kohta, nagu tehakse kättesaadavaks makseteenuse kasutajale, kui ta taotleb kontoteabele vahetut juurdepääsu, tingimusel et see teave ei sisalda tundlikke makseandmeid;

b) nad esitavad makse algatamise teenuse pakkujatele kohe pärast maksekorralduse laekumist maksetehingu algatamise ja täitmise kohta sama teabe, mis esitatakse või tehakse kättesaadavaks makseteenuse kasutajale maksetehingu vahetu algatamise korral;

c) taotluse alusel annavad nad makseteenuse pakkujale kohe lihtsa „jah“ või „ei“ kujul kinnituse selle kohta, kas maksetehingu täitmiseks vajalik summa on maksja maksekontol olemas.

2. Kui identifitseerimis- või autentimismenetluse või andmeelementide vahetamise kestel toimub ootamatu sündmus või tekib viga, saadab kontot haldav makseteenuse pakkuja selle kohta makse algatamise teenuse pakkujale või kontoteabe teenuse pakkujale ja kaardipõhiseid makseinstrumente väljastavale makseteenuse pakkujale teavituse, kus on selgitatud ootamatu sündmuse või vea põhjuseid.

Kui kontot haldav makseteenuse pakkuja pakub kooskõlas artikliga 32 spetsiaalset liidest, peab liides olema seadistatud selliselt, et makseteenuse pakkuja, kes ootamatu sündmuse või vea avastab, saab sündmusest või veast teatada teistele sideseansis osalevatele makseteenuse pakkujatele.

3. Kontoteabe teenuse pakkujatel peavad olema sobilikud ja tulemuslikud mehhanismid, millega takistatakse juurdepääs muule teabele kui see, mis pärineb kasutaja sõnaselgel nõusolekul määratud maksekontodelt ja nendega seotud maksetehingutest.

4. Makse algatamise teenuse pakkujad esitavad maksetehingu vahetu algatamise korral kontot haldavatele makseteenuse pakkujatele sama teabe nagu see, mida nõutakse makseteenuse kasutajalt.

5. Kontoteabe teenuse osutamise eesmärgil on kontoteabe teenuse pakkujatel võimalik pääseda juurde kontot haldava makseteenuse pakkuja valduses olevale teabele, mis pärineb määratud maksekontodelt ja nendega seotud maksetehingutest, ühel järgmistest juhtudest:

a) kui makseteenuse kasutaja sellist teavet aktiivselt taotleb;

b) kui makseteenuse kasutaja sellist teavet aktiivselt ei taotle, mitte sagedamini kui neli korda 24 tunni pikkuse perioodi jooksul, välja arvatud juhul, kui kontoteabe teenuse osutaja ja kontot haldav makseteenuse pakkuja on makseteenuse kasutaja nõusolekul kokku leppinud selles, et see toimub sagedamini.

VI PEATÜKK

LÕPPSÄTTED

Artikkel 37

Läbivaatamine

Ilma et see piiraks direktiivi (EL) 2015/2366 artikli 98 lõike 5 kohaldamist, vaatab EBA hiljemalt 14. märtsiks 2021 läbi käesoleva määruse lisas osutatud pettuste määrad, samuti artikli 33 lõike 6 kohased vabastused spetsiaalsetele liidestele, ja esitab vajaduse korral komisjonile kooskõlas määruse (EL) nr 1093/2010 artikliga 10 nende ajakohastamise eelnõud.

Artikkel 38

Jõustumine

1. Käesolev määrus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

2. Käesolevat määrust kohaldatakse alates 14. septembrist 2019.

3. Artikli 30 lõikeid 3 ja 5 kohaldatakse aga alates 14. märtsist 2019.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 27. november 2017

Komisjoni nimel

president

Jean-Claude JUNCKER

LISA

	Pettuste viitemäär (protsentides):	
Erandi tegemise piirmäär	Elektroonilised kaardipõhised kaugmaksed	Elektroonilised kreeditkorraldused
500 eurot	0,01	0,005
250 eurot	0,06	0,01
100 eurot	0,13	0,015