KOMISSION DELEGOITU ASETUS (EU) 2018/389,

annettu 27 päivänä marraskuuta 2017,

Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 täydentämisestä asiakkaan vahvaa tunnistamista sekä yhteisiä ja turvallisia avoimia viestintästandardeja koskevilla teknisillä sääntelystandardeilla

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta 25 päivänä marraskuuta 2015 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 ([1]) ja erityisesti sen 98 artiklan 4 kohdan toisen alakohdan,

sekä katsoo seuraavaa:

(1) Sähköisesti tarjotut maksupalvelut olisi toteutettava suojatulla tavalla ottamalla käyttöön teknologioita, joilla voidaan taata käyttäjän turvallinen tunnistaminen ja vähentää mahdollisimman paljon petoksen riskiä. Tunnistamismenettelyn olisi pääsääntöisesti sisällettävä maksutapahtumien valvontamekanismeja, joilla havaitaan yritykset käyttää maksupalvelunkäyttäjän henkilökohtaisia turvatunnuksia, jotka ovat kadonneet, varastettu tai joutuneet väärin käsiin, minkä lisäksi tunnistamismenettelyllä olisi varmistettava, että maksupalvelunkäyttäjä on laillinen käyttäjä, joka hyväksyy varojen siirron ja tilitietoihinsa pääsyn käyttämällä henkilökohtaisia turvatunnuksiaan normaalilla tavalla. Lisäksi on tarpeen täsmentää asiakkaan vahvaa tunnistamista koskevat vaatimukset, joita olisi sovellettava aina, kun maksaja käyttää maksutiliään verkon kautta, käynnistää sähköisen maksutapahtuman tai toteuttaa minkä tahansa toimen etäkanavan kautta, johon voi liittyä maksupetoksen tai muunlaisen väärinkäytöksen riski, vaatimalla sellaisen tunnistamiskoodin tuottamista, joka kestää sen riskin, että koodi väärennetään kokonaan tai että jokin niistä tekijöistä, joista se on tuotettu, paljastuu.

(2) Koska petosmenetelmät muuttuvat jatkuvasti, asiakkaan vahvaa tunnistamista koskevien vaatimusten olisi mahdollistettava sellaisten teknisten ratkaisujen innovoiminen, joilla voidaan vastata uusiin sähköisten maksujen turvallisuuteen kohdistuviin uhkiin. Sen varmistamiseksi, että vahvistettavien vaatimusten täytäntöönpano on tosiasiallista ja jatkuvaa, on myös asianmukaista edellyttää, että turvatoimenpiteet, jotka koskevat asiakkaan vahvan tunnistamisen soveltamista ja sen poikkeuksia, toimenpiteet, joilla suojataan henkilökohtaisten turvatunnusten luottamuksellisuutta ja eheyttä, ja toimenpiteet, joilla laaditaan yhteiset ja turvalliset avoimet viestintästandardit, dokumentoidaan ja että ne ovat säännöllisesti testattavina, arvioitavina ja sellaisten toiminnallisesti riippumattomien tarkastajien tarkastettavina, joilla on tietoturvaan ja maksuihin liittyvää asiantuntemusta. Jotta toimivaltaiset viranomaiset voisivat valvoa näiden toimenpiteiden uudelleentarkastelujen laatua, uudelleentarkastelut olisi annettava pyynnöstä niiden saataville.

(3) Koska sähköisiin etämaksutapahtumiin kohdistuu tavanomaista suurempi petosriski, on tarpeen ottaa käyttöön lisävaatimuksia, jotka koskevat asiakkaan vahvaa tunnistamista tällaisissa maksutapahtumissa, jotta voidaan varmistaa, että maksutapahtuman tekijät yhdistävät tapahtuman dynaamisesti määrään ja maksunsaajaan, jotka maksaja on ilmoittanut tapahtumaa käynnistäessään.

(4) Dynaamisen yhdistämisen mahdollistaa tunnistamiskoodien tuottaminen, jonka on täytettävä tiukat turvallisuusvaatimukset. Teknologianeutraaliuden säilyttämiseksi ei saisi vaatia, että tunnistamiskoodit toteutetaan tietyllä teknologialla. Sen vuoksi tunnistamiskoodien olisi perustuttava sellaisiin ratkaisuihin kuin kertakäyttösalasanojen tai digitaalisten allekirjoitusten tuottaminen ja validointi tai muut salaukseen perustuvat validiuden vahvistamiset, joissa käytetään tunnistamisen tekijöihin tallennettuja avaimia tai salausteknistä aineistoa, edellyttäen, että turvallisuusvaatimukset täytetään.

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

(5) On tarpeen vahvistaa erityiset vaatimukset sellaisten tilanteiden varalta, joissa lopullinen määrä ei ole tiedossa sillä hetkellä, kun maksaja käynnistää sähköisen etämaksutapahtuman, jotta varmistetaan, että asiakkaan vahva tunnistaminen koskee direktiivin (EU) 2015/2366 mukaisesti nimenomaan sitä enimmäismäärää, jonka maksaja on hyväksynyt.

(6) Asiakkaan vahvan tunnistamisen soveltamiseksi on myös tarpeen vaatia riittäviä turvaominaisuuksia asiakkaan vahvan tunnistamisen tekijöiltä, jotka kuuluvat ryhmään ”tieto” (jotain, minkä vain käyttäjä tietää), kuten pituus tai monimutkaisuus, ja ryhmään ”hallussapito” (jotain, mitä vain käyttäjällä on hallussaan), kuten algoritmien eritelmät, avaimenpituus ja entropia, ja vaatia riittäviä turvaominaisuuksia sellaisia tekijöitä lukevilta laitteilta ja ohjelmistoilta, jotka kuuluvat ryhmään ”erityinen ominaisuus” (jotain, mitä käyttäjä on), kuten algoritmien eritelmät sekä biometristen tunnistimen ja mallien suojaominaisuudet, jotta voidaan vähentää erityisesti sitä riskiä, että oikeudettomat tahot ottavat tai saavat nämä tekijät selville ja käyttävät niitä. Lisäksi on tarpeen vahvistaa vaatimukset, joilla varmistetaan, että nämä tekijät ovat toisistaan riippumattomia siten, että yhden rikkominen ei aseta kyseenalaiseksi muiden luotettavuutta, etenkin, jos näitä tekijöitä käytetään monikäyttölaitteella, kuten taulutietokoneella tai matkapuhelimella, jota voidaan käyttää sekä maksun suorittamista koskevien ohjeiden antamiseen että tunnistamismenettelyssä.

(7) Asiakkaan vahvaa tunnistamista koskevia vaatimuksia sovelletaan maksajan käynnistämiin maksuihin riippumatta siitä, onko maksaja luonnollinen henkilö vai oikeushenkilö.

(8) Maksut, jotka suoritetaan käyttämällä anonyymejä maksuvälineitä, eivät luonteensa vuoksi kuulu asiakkaan vahvaa tunnistamista koskevan velvollisuuden piiriin. Jos tällaisten maksuvälineiden anonyymius poistetaan sopimuksen tai lainsäädännön perusteella, maksuihin sovelletaan direktiivistä (EU) 2015/2366 ja näistä teknisistä sääntelystandardeista johtuvia turvallisuusvaatimuksia.

(9) Poikkeukset asiakkaan vahvaa tunnistamista koskevasta periaatteesta on määritelty direktiivin (EU) 2015/2366 mukaisesti maksutapahtuman riskitason, määrän ja toistuvuuden ja sen toteuttamiseen käytetyn maksukanavan perusteella.

(10) Riskitaso on alhainen toimissa, jotka edellyttävät pääsyä maksutilin saldoon ja viimeaikaisiin tapahtumiin ilman arkaluonteisten maksutietojen ilmoittamista, toistuvissa maksuissa samoille maksunsaajille, jotka maksaja on aiemmin luonut tai vahvistanut käyttämällä asiakkaan vahvaa tunnistamista, sekä maksuissa samalle luonnolliselle henkilölle tai oikeushenkilölle taikka samalta luonnolliselta henkilöltä tai oikeushenkilöltä, minkä vuoksi maksupalveluntarjoajien ei tarvitse soveltaa niissä asiakkaan vahvaa tunnistamista. Tässä ei oteta huomioon sitä, että maksutoimeksiantopalvelun tarjoajien, korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien ja tilitietopalvelun tarjoajien on direktiivin (EU) 2015/2366 65, 66 ja 67 artiklan mukaan pyydettävä ja saatava tiliä ylläpitävältä maksupalveluntarjoajalta ainoastaan ne olennaiset tiedot, jotka tarvitaan tietyn maksupalvelun tarjoamiseen maksupalvelunkäyttäjän hyväksynnällä. Hyväksyntä voidaan antaa erikseen kuhunkin tietopyyntöön tai kutakin käynnistettävää maksua varten tai, tilitietopalvelun tarjoajien osalta, nimettyjä maksutilejä ja niihin liittyviä maksutapahtumia koskevana toimeksiantona maksupalvelunkäyttäjän kanssa tehdyn sopimuksen mukaisesti.

(11) Myyntipaikassa tapahtuvia kontaktittomia pienmaksuja koskevat poikkeukset, joissa otetaan huomioon myös peräkkäisten maksutapahtumien enimmäislukumäärä tai niiden tietty kiinteä enimmäisarvo soveltamatta asiakkaan vahvaa tunnistamista, antavat mahdollisuuden kehittää käyttäjäystävällisiä ja vähäriskisiä maksupalveluja, minkä vuoksi niistä olisi annettava säännökset. Asianmukaista on myös vahvistaa poikkeus miehittämättömillä päätteillä käynnistettäviä maksutapahtumia varten, joissa asiakkaan vahvaa tunnistamista ei ole aina helppo soveltaa toiminnallisten syiden vuoksi (joita ovat esimerkiksi jonojen ja mahdollisten onnettomuuksien välttäminen tiemaksuporteilla tai muut turvallisuusriskit).

(12) Vastaavasti kuin poikkeuksessa, joka koskee myyntipaikassa tapahtuvia kontaktittomia pienmaksuja, on pyrittävä tasapainottamaan sopivalla tavalla hyöty, joka saadaan lisäämällä etämaksujen turvallisuutta, ja maksujen käyttäjäystävällisyyteen ja käyttömahdollisuuteen liittyvät tarpeet sähköisen kaupankäynnin alalla. Kynnysarvot, joiden alittuessa asiakkaan vahvaa tunnistamista ei tarvitse soveltaa, olisi näitä periaatteita ja varovaisuutta noudattaen vahvistettava koskemaan ainoastaan sellaisia verkko-ostoksia, joiden arvo ei ole suuri. Verkko-ostoksia koskevat kynnysarvot olisi vahvistettava varovaisemmin ottaen huomioon, ettei henkilö ole ostosta tehdessään fyysisesti läsnä, mikä aiheuttaa hieman suuremman turvallisuusriskin.

(13) Asiakkaan vahvaa tunnistamista koskevia vaatimuksia sovelletaan maksajan käynnistämiin maksuihin riippumatta siitä, onko maksaja luonnollinen henkilö vai oikeushenkilö. Monet yritysten suorittamat maksut käynnistetään käyttämällä erityisprosesseja tai -protokollia, joilla varmistetaan, että maksujen turvallisuus on yhtä korkealla tasolla kuin direktiivissä (EU) 2015/2366 pyritään saavuttamaan asiakkaan vahvan tunnistamisen avulla. Jos toimivaltaiset viranomaiset toteavat, että maksuprosesseilla ja -protokollilla, jotka ovat ainoastaan sellaisten maksajien käytettävissä, jotka eivät ole kuluttajia, saavutetaan direktiivissä (EU) 2015/2366 asetetut turvallisuustavoitteet, maksupalveluntarjoajat voidaan vapauttaa asiakkaan vahvaa tunnistamista koskevista vaatimuksista näiden prosessien ja protokollien osalta.

(14) Jos maksutapahtuma luokitellaan vähäriskiseksi maksutapahtumien reaaliaikaisessa riskianalyysissä, on myös aiheellista ottaa käyttöön sellaista maksupalveluntarjoajaa koskeva poikkeus, joka ei aio soveltaa asiakkaan vahvaa tunnistamista, vahvistamalla tehokkaat ja riskiperusteiset vaatimukset, joilla varmistetaan varojen ja henkilötietojen suoja. Riskiperusteisissa vaatimuksissa olisi yhdistettävä riskianalyysin pisteytykset, jotta voidaan varmistaa, ettei maksajan rahankäyttö- tai käyttäytymistavoissa ole havaittu mitään poikkeavaa, ja ottaa huomioon muut riskitekijät, maksajan ja maksunsaajan sijaintipaikkaa koskevat tiedot mukaan luettuina, yhdessä rahamääräisten kynnysarvojen kanssa, jotka perustuvat etämaksuja varten laskettuihin petososuuksiin. Jos maksua ei voida luokitella vähäriskiseksi maksutapahtumien reaaliaikaisen riskianalyysin perusteella, maksupalveluntarjoajan olisi ryhdyttävä käyttämään uudelleen asiakkaan vahvaa tunnistamista. Riskiperusteiselle poikkeukselle olisi vahvistettava enimmäisarvo, jolla varmistetaan, että vastaava petososuus jää hyvin pieneksi tiettynä ajanjaksoa ja jatkuvasti verrattuna myös maksupalveluntarjoajan kaikkien maksutapahtumien petososuuksiin, mukaan luettuina maksutapahtumat, joissa käytetään asiakkaan vahvaa tunnistamista.

(15) Tehokkaan täytäntöönpanon varmistamiseksi maksupalveluntarjoajien, jotka haluavat hyödyntää asiakkaan vahvaa tunnistamista koskevia poikkeuksia, olisi seurattava säännöllisesti jokaisen maksutapahtumatyypin osalta petollisten tai oikeudettomien maksutapahtumien arvoa ja kaikkien maksutapahtumiensa havaittuja petososuuksia riippumatta siitä, onko niissä käytetty asiakkaan vahvaa tunnistamista vai onko ne suoritettu asiaankuuluvan poikkeuksen nojalla, ja annettava nämä tiedot toimivaltaisten viranomaisten ja Euroopan pankkiviranomaisen, jäljempänä ’EPV’, pyynnöstä niiden saataville.

(16) Näiden uusien historiallisten tietojen kerääminen sähköisten maksutapahtumien petososuuksista hyödyttää myös tehokasta uudelleentarkastelua, jonka EPV suorittaa kynnysarvoista, joita sovelletaan maksutapahtumien reaaliaikaiseen riskianalyysiin perustuvaan, asiakkaan vahvaa tunnistamista koskevaan poikkeukseen. EPV:n olisi direktiivin (EU) 2015/2366 98 artiklan 5 kohdan ja Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1093/2010 ([1]) 10 artiklan mukaisesti tarkasteltava näitä teknisiä sääntelystandardeja uudelleen ja toimitettava komissiolle päivitysluonnokset, joissa ehdotetaan tarvittaessa uusia kynnysarvoja ja vastaavia petososuuksia sähköisten etämaksujen turvallisuuden parantamiseksi.

(17) Maksupalveluntarjoajien, jotka hyödyntävät jotakin säädettävää poikkeusta, olisi milloin tahansa voitava soveltaa asiakkaan vahvaa tunnistamista kyseisissä säännöksissä tarkoitettuihin toimiin ja maksutapahtumiin.

(18) Toimenpiteillä, joilla suojataan henkilökohtaisten turvatunnusten luottamuksellisuutta ja eheyttä, sekä tunnistamislaitteilla ja -ohjelmistoilla olisi rajoitettava sellaisiin petoksiin liittyviä riskejä, joka tehdään käyttämällä maksuvälineitä oikeudettomasti tai petollisesti tai pääsemällä oikeudettomasti maksutileille. Tätä varten olisi otettava käyttöön vaatimukset, jotka koskevat henkilökohtaisten turvatunnusten turvallista luomista ja toimittamista sekä niiden yhdistämistä maksupalvelunkäyttäjään, ja säätää tällaisten turvatunnusten uusimista ja deaktivointia koskevista edellytyksistä.

(19) Jotta voidaan varmistaa tehokas ja turvallinen viestintä asiaankuuluvien toimijoiden välillä tilitietopalvelujen, maksutoimeksiantopalvelujen ja varojen käytettävissä olon vahvistamisen yhteydessä, on tarpeen täsmentää yhteisiä ja turvallisia avoimia viestintästandardeja koskevat vaatimukset, jotka kaikkien asianomaisten maksupalveluntarjoajien on täytettävä. Direktiivissä (EU) 2015/2366 annetaan tilitietopalvelun tarjoajia koskevat säännökset maksutilitietoihin pääsystä ja näiden tietojen käytöstä. Sen vuoksi tässä asetuksessa ei muuteta sääntöjä, jotka koskevat muille tileille kuin maksutileille pääsyä.

([1]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1093/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan pankkiviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/78/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 12).

(20) Jokaisen tiliä ylläpitävän maksupalveluntarjoajan, jonka ylläpitämille maksutileille pääsee verkon kautta, olisi tarjottava ainakin yhtä pääsyn mahdollistavaa rajapintaa, joka mahdollistaa turvallisen viestinnän tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien kanssa. Rajapinnan olisi annettava tilitietopalvelun tarjoajille, maksutoimeksiantopalvelun tarjoajille ja korttipohjaisia maksuvälineitä liikkeeseen laskeville maksupalveluntarjoajille mahdollisuus varmentaa itsensä tiliä ylläpitävälle maksupalveluntarjoajalle. Sen olisi myös annettava tilitietopalvelun tarjoajille ja maksutoimeksiantopalvelun tarjoajille mahdollisuus käyttää tunnistamismenettelyjä, joita tiliä ylläpitävä maksupalveluntarjoaja tarjoaa maksupalvelunkäyttäjälle. Jotta varmistettaisiin teknologianeutraalius ja liiketoimintamallia koskeva neutraalius, tiliä ylläpitävien maksupalveluntarjoajien olisi voitava vapaasti päättää, tarjoavatko ne rajapintaa, joka on tarkoitettu tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien kanssa käytävään viestintään, vai sallivatko ne sen, että tähän viestintään käytetään rajapintaa, joka on tarkoitettu tiliä ylläpitävien maksupalveluntarjoajien maksupalvelunkäyttäjien varmentamiseen ja niiden kanssa käytävään viestintään.

(21) Jotta tilitietopalvelun tarjoajat, maksutoimeksiantopalvelun tarjoajat ja korttipohjaisia maksuvälineitä liikkeeseen laskevat maksupalveluntarjoajat voisivat kehittää teknisiä ratkaisujaan, rajapintaa koskevat tekniset eritelmät olisi dokumentoitava asianmukaisesti ja julkistettava. Tiliä ylläpitävän maksupalveluntarjoajan olisi myös tarjottava järjestelmä, jonka avulla maksupalveluntarjoajat voivat testata teknisiä ratkaisuja vähintään kuusi kuukautta ennen näiden sääntelystandardien soveltamispäivää tai, jos käyttöönotto tapahtuu näiden standardien soveltamispäivän jälkeen, ennen päivää, jona rajapinta tuodaan markkinoille. Erilaisten teknisten viestintäratkaisujen yhteentoimivuuden varmistamiseksi rajapinnassa olisi käytettävä kansainvälisten tai eurooppalaisten standardointiorganisaatioiden kehittämiä viestintästandardeja.

(22) Tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien tarjoamien palvelujen laatu riippuu tiliä ylläpitävien maksupalveluntarjoajien käyttöön ottamien tai mukauttamien rajapintojen asianmukaisesta toiminnasta. Sen vuoksi on tärkeää, että jos tällaiset rajapinnat eivät ole näiden standardien säännösten mukaisia, toteutetaan toimenpiteitä, joilla varmistetaan liiketoiminnan jatkuvuus näiden palvelujen käyttäjien hyödyksi. Kansallisten toimivaltaisten viranomaisten velvollisuutena on varmistaa, ettei tilitietopalvelun tarjoajien eikä maksutoimeksiantopalvelun tarjoajien harjoittamaa palveluntarjontaa estetä tai vaikeuteta.

(23) Jos maksutileille pääsyä tarjotaan eritysrajapinnan välityksellä, sen varmistamiseksi, että maksupalvelunkäyttäjillä on direktiivin (EU) 2015/2366 mukaisesti oikeus käyttää maksutoimeksiantopalvelun tarjoajia ja palveluja, jotka mahdollistavat pääsyn tilitietoihin, on tarpeen edellyttää, että erityisrajapinnat ovat käytettävyydeltään ja suorituskyvyltään samaa tasoa kuin rajapinta, joka on maksupalvelunkäyttäjän käytettävissä. Tiliä ylläpitävien maksupalveluntarjoajien olisi myös määriteltävä eritysrajapintojen käytettävyyttä ja suorituskykyä varten läpinäkyvät keskeiset suoritusindikaattorit ja palvelutasotavoitteet, jotka ovat vähintään yhtä tiukat kuin ne, jotka koskevat niiden maksupalvelujenkäyttäjien käyttämää rajapintaa. Maksupalveluntarjoajien, jotka tulevat käyttämään näitä rajapintoja, olisi testattava ne, niille olisi tehtävä stressitestejä, ja toimivaltaisten viranomaisten olisi valvottava niitä.

(24) Sen varmistamiseksi, että erityisrajapintaa käyttävät maksupalveluntarjoajat voivat jatkaa palvelujensa tarjoamista, vaikka rajapinnan käytettävyydessä esiintyisi ongelmia tai sen suorituskyky olisi riittämätön, on tarpeen säätää tiukoilla edellytyksillä varajärjestelmästä, joka antaa näille palveluntarjoajille mahdollisuuden käyttää rajapintaa, jota tiliä ylläpitävä maksupalveluntarjoaja ylläpitää omien maksupalvelunkäyttäjiensä varmentamista ja niiden kanssa käytävää viestintää varten. Tietyt tiliä ylläpitävät maksupalveluntarjoajat vapautetaan velvollisuudesta tarjota varajärjestelmää asiakaspuolen rajapintojensa välityksellä, jos niiden toimivaltaiset viranomaiset toteavat, että eritysrajapinnat täyttävät tietyt edellytykset, joilla varmistetaan esteetön kilpailu. Jos poikkeusten piiriin kuuluvat erityisrajapinnat eivät täytä vaadittuja edellytyksiä, asianomaisten toimivaltaisten viranomaisten on peruutettava myönnetyt poikkeukset.

(25) Jotta toimivaltaiset viranomaiset voisivat tehokkaasti valvoa ja seurata viestintärajapintojen toteuttamista ja hallinnointia, tiliä ylläpitävien maksupalveluntarjoajien olisi annettava verkkosivustollaan saataville tiivistelmä asiaankuuluvista asiakirjoista ja toimitettava toimivaltaisille viranomaisille pyynnöstä asiakirjat erityisen kiireellisiä tilanteita koskevista ratkaisuista. Tiliä ylläpitävien maksupalveluntarjoajien olisi myös julkistettava tilastot kyseisen rajapinnan käytettävyydestä ja suorituskyvystä.

(26) Tietojen luottamuksellisuuden ja eheyden turvaamiseksi on tarpeen varmistaa tiliä ylläpitävien maksupalveluntarjoajien, tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien välisten viestintäistuntojen turvallisuus. Erityisesti on tarpeen vaatia

turvallisen salauksen käyttöä tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien, korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien ja tiliä ylläpitävien maksupalveluntarjoajien välisessä tietojenvaihdossa.

(27) Jotta voitaisiin parantaa käyttäjien luottamusta ja varmistaa asiakkaan vahva tunnistaminen, olisi otettava huomioon Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) mukaisten sähköisen tunnistamisen menetelmien ja luottamuspalvelujen käyttö erityisesti ilmoitettujen sähköisen tunnistamisen järjestelmien osalta.

(28) Soveltamispäivien yhteen sovittamiseksi tätä asetusta olisi sovellettava samasta päivästä, josta alkaen jäsenvaltioiden on varmistettava direktiivin (EU) 2015/2366 65, 66, 67 and 97 artiklassa tarkoitettujen turvallisuustoimenpiteiden soveltaminen.

(29) Tämä asetus perustuu teknisten sääntelystandardien luonnoksiin, jotka EPV on toimittanut komissiolle.

(30) EPV on järjestänyt avoimet ja läpinäkyvät julkiset kuulemiset teknisten sääntelystandardien luonnoksista, joihin tämä asetus perustuu, analysoinut niihin mahdollisesti liittyviä kustannuksia ja hyötyjä sekä pyytänyt lausunnon asetuksen (EU) N:o 1093/2010 37 artiklan mukaisesti perustetulta pankkialan osallisryhmältä,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

Tässä asetuksessa vahvistetaan vaatimukset, jotka maksupalveluntarjoajien on täytettävä sellaisten turvatoimenpiteiden täytäntöön panemiseksi, joiden avulla ne voivat toteuttaa seuraavat toimet:

a) soveltaa asiakkaan vahvaa tunnistamista koskevaa menettelyä direktiivin (EU) 2015/2366 97 artiklan mukaisesti;

b) myöntää poikkeus asiakkaan vahvaa tunnistamista koskevien turvallisuusvaatimusten soveltamisesta erityisillä ja rajoitetuilla edellytyksillä, jotka perustuvat maksutapahtuman riskitasoon, määrään ja toistuvuuteen sekä maksutapahtuman toteuttamisessa käytettävään maksukanavaan;

c) suojata maksupalvelunkäyttäjän henkilökohtaisten turvatunnusten luottamuksellisuutta ja eheyttä;

d) vahvistaa tiliä ylläpitävien maksupalveluntarjoajien, maksutoimeksiantopalvelun tarjoajien, tilitietopalvelun tarjoajien, maksajien, maksunsaajien ja muiden maksupalveluntarjoajien välistä viestintää varten yhteiset ja turvalliset avoimet standardit, jotka koskevat maksupalvelujen tarjoamista ja käyttöä direktiivin (EU) 2015/2366 IV osastoa sovellettaessa.

2 artikla

Yleiset tunnistamisvaatimukset

1. Maksupalveluntarjoajilla on oltava käytössään maksutapahtumien valvontamekanismit, joiden avulla ne voivat havaita oikeudettomat tai petolliset maksutapahtumat 1 artiklan a ja b alakohdassa tarkoitettujen turvatoimenpiteiden täytäntöön panemiseksi.

([1]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (EUVL L 257, 28.8.2014, s. 53).

Näiden mekanismien on perustuttava maksutapahtumien analysointiin, jossa otetaan huomioon tekijät, jotka ovat ominaisia maksupalvelunkäyttäjälle henkilökohtaisten turvatunnusten normaaleissa käyttöolosuhteissa.

2. Maksupalveluntarjoajien on varmistettava, että maksutapahtumien valvontamekanismeissa otetaan huomioon ainakin kaikki seuraavat riskiperusteiset tekijät:

a) luettelot väärinkäytetyistä tai varastetuista tunnistamistekijöistä;

b) kunkin maksutapahtuman määrä;

c) tunnetut petosskenaariot maksupalvelujen tarjoamisessa;

d) merkit haittaohjelmatartunnasta tunnistamismenettelyn istuntojen aikana;

e) jos maksupalveluntarjoaja toimittaa pääsyn mahdollistavan laitteen tai ohjelmiston, maksupalvelunkäyttäjälle toimitetun, pääsyn mahdollistavan laitteen tai ohjelmiston käyttöloki ja kyseisen laitteen tai ohjelmiston poikkeava käyttö.

3 artikla

Turvatoimenpiteiden uudelleentarkastelu

1. Edellä 1 artiklassa tarkoitettujen turvatoimenpiteiden täytäntöönpano on dokumentoitava ja sitä on testattava ja arvioitava säännöllisesti, ja tarkastajien, joilla on tietoturvaan ja maksuihin liittyvää asiantuntemusta ja jotka ovat toiminnallisesti riippumattomia maksunpalveluntarjoajassa tai maksupalveluntarjoajasta, on säännöllisesti tarkastettava niiden täytäntöönpano maksupalveluntarjoajaan sovellettavan oikeudellisen kehyksen mukaisesti.

2. Edellä 1 kohdassa tarkoitettujen tarkastusten toteuttamistiheys määritetään ottaen huomioon maksupalveluntarjoajaan sovellettava merkityksellinen tilinpäätössäännöstö ja lakisääteistä tilitarkastusta koskeva kehys.

Maksupalveluntarjoajille, jotka käyttävät 18 artiklassa tarkoitettua poikkeusta, on kuitenkin tehtävä menetelmiä, mallia ja ilmoitettuja petososuuksia koskeva tarkastus ainakin kerran vuodessa. Tarkastajalla, joka suorittaa tämän tarkastuksen, on oltava tietoturvaan ja maksuihin liittyvää asiantuntemusta, ja tarkastajan on oltava toiminnallisesti riippumaton maksunpalveluntarjoajassa tai maksupalveluntarjoajasta. Riippumattoman ja pätevän ulkopuolisen tarkastajan on suoritettava tämä tarkastus ensimmäisen vuoden aikana, jona poikkeusta käytetään 18 artiklan nojalla, ja vähintään joka kolmas vuosi sen jälkeen tai useammin toimivaltaisen viranomaisen pyynnöstä.

3. Tarkastuksessa on esitettävä arviointi ja kertomus siitä, ovatko maksupalveluntarjoajan turvatoimenpiteet tässä asetuksessa vahvistettujen vaatimusten mukaisia.

Koko kertomus on annettava toimivaltaisten viranomaisten pyynnöstä niiden saataville.

II LUKU

ASIAKKAAN VAHVAN TUNNISTAMISEN SOVELTAMISTA KOSKEVAT TURVATOIMENPITEET

4 artikla

Tunnistamiskoodi

1. Jos maksupalveluntarjoajat soveltavat asiakkaan vahvaa tunnistamista direktiivin (EU) 2015/2366 97 artiklan 1 kohdan mukaisesti, tunnistamisen on perustuttava kahteen tai useampaan tekijään, jotka kuuluvat ryhmiin ”tieto”, ”hallussapito” ja ”erityinen ominaisuus”, ja sen on johdettava tunnistamiskoodin tuottamiseen.

Maksupalveluntarjoajan on hyväksyttävä tunnistamiskoodi ainoastaan kerran, kun maksaja käyttää sitä päästäkseen maksutililleen verkon kautta, käynnistääkseen sähköisen maksutapahtuman tai toteuttaakseen etäkanavan kautta minkä tahansa toimen, joka voi aiheuttaa maksupetoksen tai muunlaisen väärinkäytöksen riskin.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on toteutettava turvatoimenpiteet, joilla varmistetaan kaikkien seuraavien vaatimusten täyttyminen:

a) tunnistamiskoodin ilmoittamisesta ei ole mahdollista johtaa mitään tietoja 1 kohdassa tarkoitetuista tekijöistä;

b) uutta tunnistamiskoodia ei ole mahdollista tuottaa mihinkään muuhun, aiemmin tuotettuun tunnistamiskoodiin liittyvien tietojen perusteella;

c) tunnistamiskoodin väärentäminen ei ole mahdollista.

3. Maksupalveluntarjoajien on varmistettava, että tunnistamiseen, joka perustuu tunnistamiskoodin tuottamiseen, kuuluvat kaikki seuraavat toimenpiteet:

a) jos tunnistamisessa, joka suoritetaan etäkäyttöä, sähköisiä etämaksuja ja muita toimia varten etäkanavan kautta, johon voi liittyä maksupetoksen tai muunlaisen väärinkäytöksen riski, ei ole kyetty tuottamaan tunnistamiskoodia 1 kohdan tarkoituksia varten, ei ole mahdollista määrittää, mikä mainitussa kohdassa tarkoitetuista tekijöistä on ollut virheellinen;

b) tunnistamisyrityksiä, jotka voidaan tehdä peräkkäin, minkä jälkeen direktiivin (EU) 2015/2366 97 artiklan 1 kohdassa tarkoitetut toimet estetään väliaikaisesti tai pysyvästi, saa olla enintään viisi tietyn ajanjakson aikana;

c) viestintäistunnot suojataan tunnistamisen aikana lähetettävien tunnistamistietojen sieppaamiselta ja oikeudettomien tahojen suorittamalta manipuloinnilta V luvun vaatimusten mukaisesti;

d) enimmäisaika, jonka maksaja voi olla passiivinen sen jälkeen, kun se on tunnistettu verkon kautta tapahtuvaa maksutilin käyttöä varten, on viisi minuuttia.

4. Jos 3 kohdan b alakohdassa tarkoitettu esto on väliaikainen, sen kesto ja uudelleenyritysten lukumäärää on vahvistettava maksajalle tarjotun palvelun ominaisuuksien ja kaikkien siihen liittyvien merkityksellisten riskien perusteella ottaen huomioon ainakin 2 artiklan 2 kohdassa tarkoitetut tekijät.

Maksajaa on varoitettava ennen kuin estosta tehdään pysyvä.

Jos estosta on tehty pysyvä, on otettava käyttöön suojattu menettely, jonka avulla maksaja saa estetyt sähköiset maksuvälineet uudelleen käyttöönsä.

5 artikla

Dynaaminen yhdistäminen

1. Jos maksupalveluntarjoajat soveltavat asiakkaan vahvaa tunnistamista direktiivin (EU) 2015/2366 97 artiklan 2 kohdan mukaisesti, niiden on tämän asetuksen 4 artiklan vaatimusten lisäksi toteutettava turvatoimenpiteet, jotka täyttävät kaikki seuraavat vaatimukset:

a) maksajalle ilmoitetaan maksutapahtuman määrä ja maksunsaaja;

b) tunnistamiskoodi tuotetaan tiettyä maksutapahtuman määrää ja tiettyä maksunsaajaa varten, jotka maksajan on hyväksynyt käynnistäessään tapahtuman;

c) maksupalveluntarjoajan hyväksymä tunnistamiskoodi vastaa alkuperäistä maksutapahtuman määrää ja maksunsaajan henkilöllisyyttä, jotka maksaja on hyväksynyt;

d) määrän tai maksunsaajan muutokset johtavat tuotetun tunnistamiskoodin mitätöintiin.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on toteutettava turvatoimenpiteet, joilla varmistetaan kaikkien seuraavien tietojen luottamuksellisuus, aitous ja eheys:

a) maksutapahtuman määrä ja maksunsaaja kaikissa tunnistamisen vaiheissa;

b) maksajalle näytetyt tiedot kaikissa tunnistamisen vaiheissa, tunnistamiskoodin tuottaminen, lähettäminen ja käyttö mukaan luettuina.

3. Sovellettaessa 1 kohdan b alakohtaa sovelletaan seuraavia tunnistamiskoodia koskevia vaatimuksia, jos maksupalveluntarjoajat soveltavat asiakkaan vahvaa tunnistamista direktiivin (EU) 2015/2366 97 artiklan 2 kohdan mukaisesti:

a) korttipohjaisessa maksutapahtumassa, jota varten maksaja on mainitun direktiivin 75 artiklan 1 kohdan mukaisesti hyväksynyt täsmällisen määrän varaamisen, tunnistamiskoodi on ainoastaan sitä määrää varten, jonka varaamiseen maksaja on antanut hyväksynnän ja jonka se on hyväksynyt käynnistäessään tapahtuman;

b) maksutapahtumissa, joita varten maksaja on antanut hyväksynnän siihen, että yhdelle tai useammalle maksunsaajalle suoritetaan erä sähköisiä etämaksutapahtumia, tunnistamiskoodi on ainoastaan kyseisen maksutapahtumaerän kokonaismäärää ja yksilöityjä maksunsaajia varten.

6 artikla

Ryhmään ”tieto” kuuluvia tekijöitä koskevat vaatimukset

1. Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot ottavat tai saavat ryhmään ”tieto” kuuluvat asiakkaan vahvan tunnistamisen tekijät selville.

2. Maksajan käyttäessä näitä tekijöitä niiden käyttöön sovelletaan riskinhallintatoimenpiteitä, joiden tavoitteena on estää kyseisten tekijöiden paljastuminen oikeudettomille tahoille.

7 artikla

Ryhmään ”hallussapito” kuuluvia tekijöitä koskevat vaatimukset

1. Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot käyttävät ryhmään ”hallussapito” kuuluvia asiakkaan vahvan tunnistamisen tekijöitä.

2. Maksajan käyttäessä näitä tekijöitä niiden käyttöön sovelletaan toimenpiteitä, joiden tavoitteena on estää kyseisten tekijöiden kopioituminen.

8 artikla

Ryhmään ”erityinen ominaisuus” kuuluviin tekijöihin liittyviä laitteita ja ohjelmistoja koskevat vaatimukset

1. Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot ottavat selville ryhmään ”erityinen ominaisuus” kuuluvia tekijöitä, joita maksajalle toimitetut pääsyn mahdollistavat laitteet ja ohjelmistot lukevat. Maksupalveluntarjoajien on varmistettava ainakin, että oikeudettoman tahon tunnistaminen maksajaksi on hyvin epätodennäköistä pääsyn mahdollistavien laitteiden ja ohjelmistojen käytön yhteydessä.

2. Kun maksaja käyttää näitä tekijöitä, niiden käyttöön sovelletaan toimenpiteitä, joilla varmistetaan, että laitteet ja ohjelmistot tarjoavat suojan niiden oikeudettomasta käytöstä johtuvalta kyseisten tekijöiden oikeudettomalta käytöltä.

9 artikla

Tekijöiden riippumattomuus toisistaan

1. Maksupalveluntarjoajien on varmistettava, että 6, 7 ja 8 artiklassa tarkoitettuihin asiakkaan vahvan tunnistamisen tekijöihin sovelletaan toimenpiteitä, joilla varmistetaan teknologian, algoritmien ja parametrien osalta, ettei yhden tekijän rikkominen aseta kyseenalaiseksi muiden tekijöiden luotettavuutta.

2. Maksupalvelujen tarjoajien on toteutettava turvatoimenpiteitä, joita sovelletaan silloin, kun jotakin asiakkaan vahvan tunnistamisen tekijää tai itse tunnistamiskoodia käytetään monikäyttölaitteella, ja joilla vähennetään monikäyttölaitteen vaarantumisesta aiheutuvaa riskiä.

3. Sovellettaessa 2 kohtaa riskinhallintatoimenpiteiden on sisällettävä kaikki seuraavat osatekijät:

a) erillisten suojattujen toteuttamisympäristöjen käyttö monikäyttölaitteeseen asennetun ohjelmiston välityksellä;

b) mekanismit, joilla varmistetaan, ettei maksaja tai kolmas osapuoli ole muuttanut ohjelmistoa tai laitetta;

c) jos muutoksia on tapahtunut, mekanismit, joilla lievennetään niiden seurauksia.

III LUKU

ASIAKKAAN VAHVAA TUNNISTAMISTA KOSKEVAT POIKKEUKSET

10 artikla

Maksutilitiedot

1. Edellä 2 artiklassa ja tämän artiklan 2 kohdassa säädettyjen vaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksupalvelunkäyttäjän pääsyä jompaankumpaan tai kumpaankin seuraavista tiedoista rajoitetaan siten, ettei arkaluonteisia maksutietoja ilmoiteta:

a) yhden tai useamman nimetyn maksutilin saldo;

b) maksutapahtumat, jotka on toteutettu edeltävien 90 päivän aikana yhden tai useamman nimetyn maksutilin välityksellä.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajia ei saa vapauttaa asiakkaan vahvan tunnistamisen soveltamisesta, jos jompikumpi seuraavista perusteista täyttyy:

a) maksupalvelunkäyttäjä käyttää 1 kohdassa tarkoitettuja tietoja ensimmäisen kerran verkossa;

b) on kulunut yli 90 päivää siitä, kun maksupalvelunkäyttäjä edellisen kerran käytti 1 kohdan b alakohdassa tarkoitettuja tietoja verkossa ja asiakkaan vahvaa tunnistamista sovellettiin.

11 artikla

Myyntipaikassa tapahtuvat kontaktittomat maksut

Edellä 2 artiklassa säädettyjen vaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksaja käynnistää kontaktittoman sähköisen maksutapahtuman ja seuraavat edellytykset täyttyvät:

a) yksittäinen kontaktittoman sähköisen maksutapahtuman määrä on enintään 50 euroa; ja

b) sellaisten aiempien kontaktittomien sähköisten maksutapahtumien kumulatiivinen määrä, jotka on käynnistetty maksuvälineellä, jossa on kontaktiton toiminto, on enintään 150 euroa asiakkaan vahvan tunnistamisen viimeisestä soveltamispäivästä laskettuna; tai

c) sellaisten peräkkäisten kontaktittomien sähköisten maksutapahtumien lukumäärä, jotka on käynnistetty maksuvälineellä, jossa on kontaktiton toiminto, on enintään viisi asiakkaan vahvan tunnistamisen viimeisen soveltamiskerran jälkeen.

12 artikla

Miehittämättömät päätteet liikennemaksuja ja pysäköintimaksuja varten

Edellä 2 artiklassa säädettyjen vaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksaja käynnistää sähköisen maksutapahtuman miehittämättömällä päätteellä maksaakseen liikennemaksun tai pysäköintimaksun.

13 artikla

Luotettavat maksunsaajat

1. Maksupalveluntarjoajien on sovellettava asiakkaan vahvaa tunnistamista, kun maksaja luo tiliä ylläpitävän maksupalveluntarjoajansa välityksellä luettelon luotettavista maksunsaajista tai muuttaa tällaista luetteloa.

2. Yleisten tunnistamisvaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksaja käynnistää maksutapahtuman ja maksunsaaja sisältyy maksajan luotettavista maksunsaajista aiemmin luomaan luetteloon.

14 artikla

Toistuvat maksutapahtumat

1. Maksupalveluntarjoajien on sovellettava asiakkaan vahvaa tunnistamista, kun maksaja ensimmäisen kerran luo sarjan toistuvia maksutapahtumia, joissa on sama määrä ja sama maksunsaaja, tai muuttaa tällaista sarjaa tai käynnistää sen.

2. Yleisten tunnistamisvaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista käynnistettäessä kaikkia myöhempiä maksutapahtumia, jotka kuuluvat 1 kohdassa tarkoitettuun maksutapahtumien sarjaan.

15 artikla

Saman luonnollisen henkilön tai oikeushenkilön hallussa olevien tilien väliset tilisiirrot

Edellä 2 artiklassa säädettyjen vaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksaja käynnistää tilisiirron, jossa maksaja ja maksunsaaja ovat sama luonnollinen henkilö tai oikeushenkilö ja molempia maksutilejä ylläpitää sama tiliä ylläpitävä maksupalveluntarjoaja.

16 artikla

Vähäarvoiset maksutapahtumat

Edellä 2 artiklassa säädettyjen vaatimusten täyttyessä on sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksaja käynnistää sähköisen etämaksutapahtuman ja seuraavat edellytykset täyttyvät:

a) sähköisen etämaksutapahtuman määrä on enintään 30 euroa; ja

b) sellaisten aiempien sähköisten etämaksutapahtumien kumulatiivinen määrä, jotka maksaja on käynnistänyt vahvan tunnistamisen viimeisen soveltamisen jälkeen, on enintään 100 euroa; tai

c) sellaisten aiempien sähköisten etämaksutapahtumien lukumäärä, jotka maksaja on käynnistänyt vahvan tunnistamisen viimeisen soveltamisen jälkeen, on enintään viisi peräkkäistä yksittäistä sähköistä etämaksutapahtumaa.

17 artikla

Yritysten käyttämät suojatut maksuprosessit ja -protokollat

On sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun on kyse oikeushenkilöistä, jotka käynnistävät sähköisiä maksutapahtumia käyttämällä erityisiä maksuprosesseja tai -protokollia, jotka ovat ainoastaan sellaisten maksajien käytettävissä, jotka eivät ole kuluttajia, ja kun toimivaltaiset viranomaiset ovat vakuuttuneita siitä, että näillä prosesseilla ja protokollilla varmistetaan vähintään vastaavat turvallisuustasot kuin direktiivissä (EU) 2015/2366 säädetään.

18 artikla

Maksutapahtumien riskianalyysi

1. On sallittava, että maksupalveluntarjoajat eivät sovella asiakkaan vahvaa tunnistamista, kun maksaja käynnistää sähköisen etämaksutapahtuman, jota maksupalveluntarjoaja pitää vähäriskisenä 2 artiklassa ja tämän artiklan 2 kohdan c alakohdassa tarkoitettujen maksutapahtumia koskevien valvontamekanismien mukaisesti.

2. Edellä 1 kohdassa tarkoitettua sähköistä maksutapahtumaa on pidettävä vähäriskisenä, kun kaikki seuraavat edellytykset täyttyvät:

a) maksunpalveluntarjoajan ilmoittama ja 19 artiklan mukaisesti laskettu maksutapahtumatyypin petososuus on sama tai pienempi kuin liitteessä olevassa taulukossa esitetyt petosten viiteosuudet, jotka koskevat ”sähköisiä korttipohjaisia etämaksuja” ja ”sähköisiä etätilisiirtoja”;

b) maksutapahtuman määrä ei ylitä liitteessä olevassa taulukossa esitettyä vastaavaa poikkeuksen kynnysarvoa;

c) maksupalveluntarjoajat eivät ole havainneet mitään seuraavista seikoista suorittaessaan reaaliaikaista riskianalyysiä:

   i) maksajan poikkeavat rahankäyttö- tai käyttäytymistavat;

   ii) epätavalliset tiedot maksajan pääsystä, joka tapahtuu laitteen tai ohjelmiston avulla;

   iii) haittaohjelmatartunta tunnistamismenettelyn istunnon aikana;

   iv) tunnetut petosskenaariot maksupalvelujen tarjoamisessa;

   v) maksajan poikkeava sijaintipaikka;

   vi) maksunsaajan suuririskinen sijaintipaikka.

3. Maksupalveluntarjoajien, jotka aikovat vapauttaa sähköiset etämaksutapahtumat asiakkaan vahvasta tunnistamisesta niiden vähäriskisyyden perusteella, on otettava huomioon ainakin seuraavat riskiperusteiset tekijät:

a) yksittäisen maksupalvelunkäyttäjän aiemmat rahankäyttötavat;

b) historiatiedot maksupalveluntarjoajan kunkin maksupalvelunkäyttäjän maksutapahtumista;

c) maksajan ja maksunsaajan sijaintipaikat maksutapahtuman ajankohtana tapauksissa, joissa maksupalveluntarjoaja toimittaa pääsyn mahdollistavan laitteen tai ohjelmiston;

d) maksupalvelunkäyttäjän sellaisten maksamistapojen havaitseminen, jotka ovat käyttäjän maksutapahtumia koskevien historiatietojen perusteella poikkeavia.

Maksupalveluntarjoajan tekemässä arvioinnissa kaikki nämä riskiperusteiset tekijät on yhdistettävä kunkin yksittäisen maksutapahtuman osalta riskipisteytykseksi, jonka avulla määritetään, onko tietty maksu sallittava ilman asiakkaan vahvaa tunnistamista.

19 artikla

Petososuuksien laskeminen

1. Maksupalveluntarjoajan on varmistettava kummankin liitteessä olevassa taulukossa esitetyn maksutapahtumatyypin osalta, että petosten kokonaisosuudet, jotka käsittävät sekä asiakkaan vahvan tunnistamisen avulla tunnistetut maksutapahtumat että jonkin 13–18 artiklassa tarkoitetun poikkeuksen nojalla toteutetut maksutapahtumat, vastaavat kyseisessä taulukossa esitettyä samaan maksutapahtumatyyppiin liittyvien petosten viiteosuutta tai alittavat sen.

Petosten kokonaisosuus lasketaan kunkin maksutapahtumatyypin osalta jatkuvaluonteisesti neljännesvuosittain (90 päivän ajalta) määrittämällä ensin oikeudettomien tai petollisten etämaksutapahtumien kokonaisarvo riippumatta siitä, onko varat saatu takaisin vai ei, ja jakamalla näin saatu arvo kaikkien samaa maksutapahtumatyyppiä olevien etämaksutapahtumien kokonaisarvolla riippumatta siitä, onko ne tunnistettu soveltamalla asiakkaan vahvaa tunnistamista vai toteutettu jonkin 13–18 artiklassa tarkoitetun poikkeuksen nojalla.

2. Petososuuksien laskemista ja tulokseksi saatuja lukuja on arvioitava 3 artiklan 2 kohdassa tarkoitetussa tarkastuksessa, jolla on varmistettava niiden täydellisyys ja oikeellisuus.

3. Maksupalveluntarjoajan petososuuksien laskemiseen käyttämät menetelmät ja mallit sekä itse petososuudet on dokumentoitava asianmukaisesti ja annettava toimivaltaisten viranomaisten ja EPV:n pyynnöstä kokonaisuudessaan niiden saataville, jolloin asiasta on annettava ennakkoilmoitus asianomaiselle tai asianomaisille toimivaltaisille viranomaisille.

20 artikla

Maksutapahtumien riskianalyysiin perustuvien poikkeusten lakkauttaminen

1. Jos maksupalveluntarjoaja hyödyntää 18 artiklassa tarkoitettua poikkeusta ja yksi sen valvotuista petososuuksista ylittää sovellettavan petosten viiteosuuden jommankumman liitteessä olevassa taulukossa esitetyn maksutapahtumatyypin osalta, maksupalveluntarjoajan on välittömästi ilmoitettava asiasta toimivaltaisille viranomaisille ja toimitettava niille kuvaus toimenpiteistä, jotka se aikoo toteuttaa, jotta sen valvottu petososuus saadaan jälleen vastaamaan sovellettavia petosten viiteosuuksia.

2. Maksupalveluntarjoajien on välittömästi lakattava hyödyntämästä 18 artiklassa tarkoitettua poikkeusta kumpaankin liitteessä olevassa taulukossa esitettyyn maksutapahtumatyyppiin vastaavalla poikkeuksen kynnysarvon määräämällä välillä, jos niiden valvotut petososuudet ylittävät kahden peräkkäisen neljännesvuoden aikana petosten viiteosuuden, jota sovelletaan kyseiseen maksuvälineeseen tai maksutapahtumatyyppiin vastaavalla poikkeuksen kynnysarvon määräämällä välillä.

3. Sen jälkeen, kun 18 artiklassa tarkoitettu poikkeus on lakkautettu tämän artiklan 2 kohdan mukaisesti, maksupalveluntarjoajat eivät saa käyttää sitä ennen kuin niiden laskettu petososuus on neljännesvuoden aikana sama tai pienempi kuin petosten viiteosuudet, joita sovelletaan kyseiseen maksutapahtumatyyppiin poikkeuksen kynnysarvon määräämällä välillä.

4. Jos maksupalveluntarjoajat aikovat hyödyntää 18 artiklassa tarkoitettua poikkeusta uudelleen, niiden on ilmoitettava asiasta toimivaltaisille viranomaisille kohtuullisen ajan kuluessa, ja ennen kuin ne alkavat hyödyntää sitä uudelleen, niiden on osoitettava, että niiden valvottu petososuus on saatu vastaamaan sovellettavaa petosten viiteosuutta poikkeuksen kynnysarvon määräämällä välillä tämän artiklan 3 kohdan mukaisesti.

21 artikla

Seuranta

1. Voidakseen hyödyntää 10–18 artiklassa säädettyjä poikkeuksia maksupalveluntarjoajien on vähintään neljännesvuosittain kirjattava kunkin maksutapahtumatyypin osalta seuraavat tiedot eriteltyinä etämaksutapahtumiin ja muihin maksutapahtumiin ja seurattava niitä:

a) oikeudettomien tai petollisten maksutapahtumien kokonaisarvo direktiivin (EU) 2015/2366 64 artiklan 2 kohdan mukaisesti, kaikkien maksutapahtumien kokonaisarvo ja vastaava petososuus, mukaan luettuna asiakkaan vahvaa tunnistamista soveltamalla käynnistettyjen maksutapahtumien ja kunkin poikkeuksen nojalla käynnistettyjen maksutapahtumien erittely;

b) maksutapahtumien keskimääräinen arvo, mukaan luettuna asiakkaan vahvaa tunnistamista soveltamalla käynnistettyjen maksutapahtumien ja kunkin poikkeuksen nojalla käynnistettyjen maksutapahtumien erittely;

c) sellaisten maksutapahtumien lukumäärä, joissa on sovellettu kutakin poikkeusta, ja niiden prosenttiosuus maksutapahtumien kokonaislukumäärästä.

2. Maksupalveluntarjoajien on annettava 1 kohdan mukaisen seurannan tulokset toimivaltaisten viranomaisten ja EPV:n pyynnöstä niiden saataville, jolloin asiasta on annettava ennakkoilmoitus asianomaiselle tai asianomaisille toimivaltaisille viranomaisille.

IV LUKU

MAKSUPALVELUNKÄYTTÄJÄN HENKILÖKOHTAISTEN TURVATUNNUSTEN LUOTTAMUKSELLISUUS JA EHEYS

22 artikla

Yleiset vaatimukset

1. Maksupalvelujen tarjoajien on kaikissa tunnistamisen vaiheissa varmistettava maksupalvelunkäyttäjän henkilökohtaisten turvatunnusten luottamuksellisuus ja eheys, tunnistamiskoodit mukaan luettuina.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on varmistettava, että kaikki seuraavat vaatimukset täyttyvät:

a) henkilökohtaiset turvatunnukset näytetään peitettyinä eivätkä ole kokonaan luettavissa, kun maksupalvelunkäyttäjä syöttää niitä tunnistamisen aikana;

b) tiedontallennusmuodossa olevia henkilökohtaisia turvatunnuksia ja henkilökohtaisten turvatunnusten salaukseen liittyviä salausteknisiä aineistoja ei tallennetta ilmitekstinä;

c) salaista salausteknistä aineistoa suojataan oikeudettomalta paljastamiselta.

3. Maksupalveluntarjoajien on dokumentoitava kokonaan sellaisen salausteknisen aineiston hallintaprosessi, jonka avulla henkilökohtaiset turvatunnukset salataan tai tehdään muulla tavoin lukukelvottomiksi.

4. Maksupalveluntarjoajien on varmistettava, että maksupalvelunkäyttäjän henkilökohtaiset turvatunnukset ja II luvun mukaisesti tuotetut tunnistamiskoodit käsitellään ja reititetään suojatuissa ympäristöissä vahvojen ja yleisesti tunnustettujen toimialastandardien mukaisesti.

23 artikla

Tunnusten luominen ja lähettäminen

Maksupalveluntarjoajien on varmistettava, että henkilökohtaiset turvatunnukset luodaan suojatussa ympäristössä.

Niiden on vähennettävä henkilökohtaisten turvatunnusten ja tunnistamislaitteiden ja -ohjelmistojen oikeudettoman käytön riskejä, joita aiheutuu, kun tunnukset, laitteet tai ohjelmistot kadotetaan, varastetaan tai kopioidaan ennen niiden toimittamista maksajalle.

24 artikla

Yhdistäminen maksupalvelunkäyttäjään

1. Maksupalveluntarjoajien on varmistettava, että henkilökohtaiset turvatunnukset, tunnistamislaitteet ja -ohjelmistot yhdistetään suojatulla tavalla ainoastaan maksupalvelunkäyttäjään.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on varmistettava, että kaikki seuraavat vaatimukset täyttyvät:

a) maksupalvelunkäyttäjän henkilöllisyyden yhdistäminen henkilökohtaisiin turvatunnuksiin, tunnistamislaitteisiin ja -ohjelmistoihin toteutetaan maksupalveluntarjoajan vastuulla suojatuissa ympäristöissä, jotka käsittävät ainakin maksupalveluntarjoajan toimitilat, sen tarjoaman internetympäristön tai muut vastaavat sen käyttämät suojatut verkkosivustot ja sen pankkiautomaattipalvelut, ottaen huomioon riskit, jotka liittyvät yhdistämisprosessin aikana käytettäviin laitteisiin ja peruskomponentteihin, jotka eivät ole maksupalveluntarjoajan vastuulla;

b) maksupalvelunkäyttäjän henkilöllisyyden yhdistäminen henkilökohtaisiin turvatunnuksiin ja tunnistamislaitteisiin ja -ohjelmistoihin etäkanavan välityksellä suoritetaan käyttämällä asiakkaan vahvaa tunnistamista.

25 artikla

Tunnusten, tunnistamislaitteiden ja -ohjelmistojen toimittaminen

1. Maksupalveluntarjoajien on varmistettava, että henkilökohtaiset turvatunnukset ja tunnistamislaitteet ja -ohjelmistot toimitetaan maksupalvelunkäyttäjälle suojatulla tavalla, jolla käsitellään niiden katoamisesta, varastamisesta tai kopioimisesta johtuvaan oikeudettomaan käyttöön liittyviä riskejä.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on toteutettava ainakin kaikki seuraavat toimenpiteet:

a) tehokkaat ja turvalliset toimitusmekanismit, joilla varmistetaan, että henkilökohtaiset turvatunnukset ja tunnistamislaitteet ja -ohjelmistot toimitetaan lailliselle maksupalvelunkäyttäjälle;

b) mekanismit, joiden avulla maksupalveluntarjoaja voi tarkistaa maksupalvelunkäyttäjälle internetin välityksellä toimitettujen tunnistamisohjelmistojen aitouden;

c) järjestelyt, joilla varmistetaan silloin, kun henkilökohtaiset turvatunnukset toimitetaan maksupalveluntarjoajan toimitilojen ulkopuolella tai etäkanavan välityksellä, että

   i) mikään oikeudeton taho ei voi saada henkilökohtaisista turvatunnuksista eikä tunnistamislaitteista tai -ohjelmistoista enempää kuin yhden ominaisuuden, kun ne toimitetaan saman kanavan välityksellä;

   ii) henkilökohtaiset turvatunnukset ja tunnistamislaitteet tai -ohjelmistot on aktivoitava ennen niiden käyttöä;

d) järjestelyt, joilla varmistetaan, että aktivointi tapahtuu suojatussa ympäristössä 24 artiklassa tarkoitettujen yhdistämismenettelyjen mukaisesti silloin, kun henkilökohtaiset turvatunnukset ja tunnistamislaitteet tai -ohjelmistot on aktivoitava ennen niiden ensimmäistä käyttöä,

26 artikla

Henkilökohtaisten turvatunnusten uusiminen

Maksupalveluntarjoajien on varmistettava, että henkilökohtaisten turvatunnusten uusimisessa tai uudelleenaktivoinnissa noudatetaan turvatunnusten ja tunnistamislaitteiden luomisessa, yhdistämisessä ja toimittamisessa noudatettavia menettelyjä 23, 24 ja 25 artiklan mukaisesti.

27 artikla

Hävittäminen, deaktivoiminen ja mitätöiminen

Maksupalveluntarjoajien on varmistettava, että niillä on käytössään tehokkaat prosessit seuraavien turvatoimenpiteiden toteuttamiseksi:

a) henkilökohtaiset turvatunnukset ja tunnistamislaitteet ja -ohjelmistot hävitetään, deaktivoidaan tai mitätöidään turvallisesti;

b) jos maksupalveluntarjoaja jakaa uudelleenkäytettäviä tunnistamislaitteita ja -ohjelmistoja, laitteen tai ohjelmiston turvallinen uudelleenkäyttö vahvistetaan, dokumentoidaan ja toteutetaan ennen sen antamista toisen maksupalvelunkäyttäjän käyttöön;

c) henkilökohtaisia turvatunnuksia koskevat tiedot, jotka on tallennettu maksupalveluntarjoajan järjestelmiin ja tietokantoihin sekä tapauksen mukaan julkisiin rekistereihin, deaktivoidaan tai mitätöidään.

V LUKU

YHTEISET JA TURVALLISET AVOIMET VIESTINTÄSTANDARDIT

1 jakso

Yleiset viestintävaatimukset

28 artikla

Varmentamisvaatimukset

1. Maksupalveluntarjoajien on varmistettava suojattu varmentaminen maksajan laitteen ja sähköisten maksujen hyväksymiseen tarkoitettujen maksunsaajan laitteiden välisessä viestinnässä, mikä koskee muun muassa maksupäätteitä.

2. Maksupalveluntarjoajien on varmistettava sellaisten riskien tehokas vähentäminen, joita aiheutuu siitä, että viestintä virheellisesti ohjautuu oikeudettomille tahoille mobiilisovelluksissa ja muissa maksupalvelunkäyttäjien rajapinnoissa, jotka tarjoavat sähköisiä maksupalveluja.

29 artikla

Jäljitettävyys

1. Maksupalveluntarjoajilla on oltava käytössään prosessit, joilla varmistetaan, että kaikki maksutapahtumat ja muut vuorovaikutukset maksupalvelunkäyttäjän, muiden maksupalveluntarjoajien ja muiden yhteisöjen kanssa, kauppiaat mukaan luettuina, maksupalvelun tarjoamisen yhteydessä ovat jäljitettävissä sen varmistamiseksi, että kaikki tapahtumat, jotka ovat sähköisen maksutapahtuman kannalta merkityksellisiä sen eri vaiheissa, tiedetään jälkikäteen.

2. Sovellettaessa 1 kohtaa maksupalveluntarjoajien on varmistettava, että kaikki viestintäistunnot maksupalvelunkäyttäjän, muiden maksupalveluntarjoajien ja muiden yhteisöjen kanssa, kauppiaat mukaan luettuina, perustuvat kaikkiin seuraaviin tekijöihin:

a) viestintäistunnon yksilöllinen tunniste;

b) turvamekanismit maksutapahtuman yksityiskohtaista kirjaamista varten, maksutapahtuman numero, aikaleimat ja kaikki maksutapahtumaa koskevat merkitykselliset tiedot mukaan luettuina;

c) aikaleimat, jotka perustuvat yhdenmukaiseen aikareferenssijärjestelmään ja jotka synkronoidaan virallisen aikamerkin mukaisesti.

2 jakso

Yhteisiä ja turvallisia avoimia viestintästandardeja koskevat erityisvaatimukset

30 artikla

Pääsyn mahdollistavia laitteita koskevat yleiset velvollisuudet

1. Tiliä ylläpitävien maksupalveluntarjoajien, jotka tarjoavat maksajalle verkossa käytettävissä olevan maksutilin, on otettava käyttöön ainakin yksi rajapinta, joka täyttää kaikki seuraavat vaatimukset:

a) tilitietopalvelun tarjoajat, maksutoimeksiantopalvelun tarjoajat ja korttipohjaisia maksuvälineitä liikkeeseen laskevat maksupalveluntarjoajat voivat varmentaa itsensä tiliä ylläpitävälle maksupalveluntarjoajalle;

b) tilitietopalvelun tarjoajat voivat kommunikoida turvallisesti pyytääkseen ja saadakseen tietoja yhdestä tai useammasta nimetystä maksutilistä ja niihin liittyvistä maksutapahtumista;

c) maksutoimeksiantopalvelun tarjoajat voivat kommunikoida turvallisesti käynnistääkseen maksutoimeksiannon maksajan maksutililtä ja saadakseen kaikki tiliä ylläpitävän maksupalveluntarjoajan saatavilla olevat tiedot maksutapahtuman toteuttamisesta.

2. Edellä 1 kohdassa tarkoitetun rajapinnan on maksupalvelunkäyttäjän tunnistamiseksi annettava tilitietopalvelun tarjoajille ja maksutoimeksiantopalvelun tarjoajille mahdollisuus käyttää kaikkia tunnistamismenettelyjä, joita tiliä ylläpitävä maksupalveluntarjoaja tarjoaa maksupalvelunkäyttäjälle.

Rajapinnan on täytettävä ainakin kaikki seuraavat vaatimukset:

a) maksutoimeksiantopalvelun tarjoajalla tai tilitietopalvelun tarjoajalla on oltava mahdollisuus kehottaa tiliä ylläpitävää maksupalveluntarjoajaa aloittamaan tunnistamisen maksupalvelunkäyttäjän hyväksynnällä;

b) tunnistamista on käytettävä, kun luodaan ja ylläpidetään tiliä ylläpitävän maksupalveluntarjoajan, tilitietopalvelun tarjoajan, maksutoimeksiantopalvelun tarjoajan ja minkä tahansa maksupalvelunkäyttäjän välisiä viestintäistuntoja;

c) maksutoimeksiantopalvelun tarjoajan tai tilitietopalvelun tarjoajan toimittamien tai sen välityksellä toimitettavien henkilökohtaisten turvatunnusten luottamuksellisuus ja eheys on varmistettava.

3. Tiliä ylläpitävien maksupalveluntarjoajien on varmistettava, että niiden rajapinnat ovat kansainvälisten tai eurooppalaisten standardointiorganisaatioiden antamien viestintästandardien mukaisia.

Tiliä ylläpitävien maksupalveluntarjoajien on varmistettava myös, että rajapintojen tekniset eritelmät dokumentoidaan ja niissä esitetään maksutoimeksiantopalvelun tarjoajien, tilitietopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien rutiinit, protokollat ja välineet, jotka mahdollistavat niiden ohjelmistojen ja sovellusten yhteentoimivuuden tiliä ylläpitävien maksupalveluntarjoajien järjestelmien kanssa.

Vähintään kuusi kuukautta ennen 38 artiklan 2 kohdassa tarkoitettua soveltamispäivää tai ennen pääsyn mahdollistavan rajapinnan markkinoille saattamisen tavoitepäivää, jos se saatetaan markkinoille 38 artiklan 2 kohdassa tarkoitetun päivän jälkeen, tiliä ylläpitävien maksupalveluntarjoajien on ainakin annettava edellä tarkoitetut asiakirjat maksutta saataville toimiluvan saaneiden maksutoimeksiantopalvelun tarjoajien, tilitietopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien tai sellaisten maksupalveluntarjoajien pyynnöstä, jotka ovat hakeneet asiaankuuluvaa toimilupaa toimivaltaisilta viranomaisiltaan, ja julkistettava kyseisistä asiakirjoista tiivistelmä verkkosivustollaan.

4. Edellä olevan 3 kohdan lisäksi maksupalveluntarjoajien on varmistettava, että erityisen kiireellisiä tilanteita lukuun ottamatta kaikki muutokset niiden rajapinnan teknisiin eritelmiin annetaan ennakolta mahdollisimman pian ja vähintään kolme kuukautta ennen muutoksen täytäntöönpanoa toimiluvan saaneiden maksutoimeksiantopalvelun tarjoajien, tilitietopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien tai sellaisten maksupalveluntarjoajien saataville, jotka ovat hakeneet asiaankuuluvaa toimilupaa toimivaltaisilta viranomaisiltaan.

Maksupalveluntarjoajien on dokumentoitava erityisen kiireelliset tilanteet, joissa muutoksia on pantu täytäntöön, ja annettava nämä asiakirjat pyynnöstä toimivaltaisten viranomaisten saataville.

5. Tiliä ylläpitävien maksupalveluntarjoajien on annettava käyttöön testausjärjestelmä liitännän ja toiminnan testausta varten, tuki mukaan luettuna, jotta toimiluvan saaneet maksutoimeksiantopalvelun tarjoajat, korttipohjaisia maksuvälineitä liikkeeseen laskevat maksupalveluntarjoajat ja tilitietopalvelun tarjoajat tai sellaiset maksupalveluntarjoajat, jotka ovat hakeneet asiaankuuluvaa toimilupaa, voivat testata ohjelmistojaan ja sovelluksiaan, joita käytetään maksupalvelun tarjoamiseen käyttäjille. Testausjärjestelmä olisi annettava saataville vähintään kuusi kuukautta ennen 38 artiklan 2 kohdassa tarkoitettua soveltamispäivää tai ennen pääsyn mahdollistavan rajapinnan markkinoille saattamisen tavoitepäivää, jos se saatetaan markkinoille 38 artiklan 2 kohdassa tarkoitetun päivän jälkeen.

Testausjärjestelmän kautta ei saa kuitenkaan jakaa arkaluonteisia tietoja.

6. Toimivaltaisten viranomaisten on varmistettava, että tiliä ylläpitävät maksupalveluntarjoajat täyttävät aina näissä standardeissa asetetut velvollisuudet käyttöön ottamiensa rajapintojen osalta. Siinä tapauksessa, että tiliä ylläpitävä maksupalveluntarjoaja ei noudata rajapintoja koskevia vaatimuksia, jotka vahvistetaan näissä standardeissa, toimivaltaisten viranomaisten on varmistettava, ettei maksutoimeksiantopalvelujen ja tilitietopalvelujen tarjoaminen esty tai häiriinny, jos näiden palvelujen asianomaiset tarjoajat täyttävät 33 artiklan 5 kohdassa säädetyt edellytykset.

31 artikla

Pääsyn mahdollistavia rajapintoja koskevat vaihtoehdot

Tiliä ylläpitävien maksupalveluntarjoajien on luotava 30 artiklassa tarkoitettu rajapinta (tarkoitetut rajapinnat) ottamalla käyttöön erityisrajapinta tai sallimalla, että 30 artiklan 1 kohdassa tarkoitetut maksupalveluntarjoajat käyttävät rajapintoja, joita käytetään tunnistamiseen ja viestintään tiliä ylläpitävän maksupalveluntarjoajan maksupalvelunkäyttäjien kanssa.

32 artikla

Erityisrajapintaa koskevat velvollisuudet

1. Jollei 31 ja 30 artiklasta muuta johdu, tiliä ylläpitävien maksupalveluntarjoajien, jotka ovat ottaneet erityisrajapinnan käyttöön, on varmistettava, että eritysrajapinta on käytettävyydeltään ja suorituskyvyltään, tuki mukaan luettuna, aina samaa tasoa kuin rajapinnat, jotka annetaan maksupalvelunkäyttäjän käyttöön, jotta maksupalvelunkäyttäjä voi käyttää maksutiliään suoraan verkon kautta.

2. Tiliä ylläpitävien maksupalveluntarjoajien, jotka ovat ottaneet erityisrajapinnan käyttöön, on määriteltävä läpinäkyvät keskeiset suoritusindikaattorit ja palvelutasotavoitteet, jotka ovat käytettävyyden ja 36 artiklan mukaisesti toimitettavien tietojen osalta vähintään yhtä tiukat kuin ne, jotka on vahvistettu kyseisten palveluntarjoajien maksupalvelunkäyttäjien käyttämää rajapintaa varten. Toimivaltaisten viranomaisten on valvottava näitä rajapintoja, indikaattoreita ja tavoitteita, ja niille on tehtävä stressitestejä.

3. Tiliä ylläpitävien maksupalveluntarjoajien, jotka ovat ottaneet erityisrajapinnan käyttöön, on varmistettava, ettei erityisrajapinta luo esteitä maksutoimeksiantopalvelujen ja tilitietopalvelujen tarjoamiselle. Tällaisiin esteisiin voivat muun muassa kuulua tekijät, jotka estävät 30 artiklan 1 kohdassa tarkoitettuja maksupalveluntarjoajia käyttämästä tiliä ylläpitävien maksupalveluntarjoajien asiakkailleen antamia tunnuksia; jotka pakosta ohjaavat tiliä ylläpitävän maksupalveluntarjoajan tunnistamis- ja muihin toimintoihin; jotka vaativat ylimääräisiä toimilupia ja rekisteröintejä direktiivin (EU) 2015/2366 11, 14 ja 15 artiklassa säädettyjen lisäksi tai jotka vaativat tekemään lisätarkastuksia hyväksynnöille, jotka maksupalvelunkäyttäjät ovat antaneet maksutoimeksiantopalvelun tarjoajille ja tilitietopalvelun tarjoajille.

4. Tiliä ylläpitävien maksupalveluntarjoajien on 1 ja 2 kohtaa sovellettaessa valvottava erityisrajapinnan käytettävyyttä ja suorituskykyä. Niiden on julkaistava verkkosivustollaan neljännesvuosittaiset tilastot erityisrajapinnan ja maksupalvelunkäyttäjiensä käyttämän rajapinnan käytettävyydestä ja suorituskyvystä.

33 artikla

Erityisrajapintaa koskevat varotoimenpiteet

1. Tiliä ylläpitävien maksupalveluntarjoajien on sisällytettävä eritysrajapinnan suunnitteluun varotoimenpiteitä koskeva strategia ja suunnitelmat siltä varalta, ettei rajapinta toimi 32 artiklan mukaisesti, että se on ennakoimattomasti poissa käytöstä ja että järjestelmä kaatuu. Voidaan olettaa, että erityisrajapinta on ennakoimattomasti poissa käytöstä tai järjestelmä on kaatunut, jos viiteen peräkkäiseen pyyntöön saada tietoja maksutoimeksiantopalvelujen tai tilitietopalvelujen tarjoamista varten ei saada vastausta 30 sekunnin kuluessa.

2. Varotoimenpiteisiin on sisällyttävä viestintäsuunnitelmat, joiden mukaisesti erityisrajapintaa käyttäville maksupalveluntarjoajille ilmoitetaan toimenpiteistä, joilla järjestelmä palautetaan käyttöön, ja kuvaus välittömästi saatavilla olevista vaihtoehdoista, joita maksupalveluntarjoajat voivat käyttää tänä aikana.

3. Sekä tiliä ylläpitävän maksupalveluntarjoajan että 30 artiklan 1 kohdassa tarkoitettujen maksupalveluntarjoajien on ilmoitettava 1 kohdassa kuvatuista erityisrajapintoihin liittyvistä ongelmista viipymättä toimivaltaisille kansallisille viranomaisilleen.

4. Varomekanismin osana on sallittava, että 30 artiklan 1 kohdassa tarkoitetut maksupalveluntarjoajat käyttävät rajapintoja, jotka on annettu maksupalvelunkäyttäjien käyttöön niiden tunnistamista ja tiliä ylläpitävän maksupalveluntarjoajan kanssa käymää viestintää varten, kunnes erityisrajapinnan käytettävyys ja suorituskyky on palautettu 32 artiklan mukaiselle tasolle.

5. Tiliä ylläpitävien maksupalveluntarjoajien on tätä varten varmistettava, että 30 artiklan 1 kohdassa tarkoitetut maksunpalveluntarjoajat voidaan varmentaa ja että ne voivat käyttää tiliä ylläpitävän maksupalveluntarjoajan maksupalvelunkäyttäjälle tarjoamia tunnistamismenettelyjä. Jos 30 artiklan 1 kohdassa tarkoitetut maksupalveluntarjoajat käyttävät 4 kohdassa tarkoitettua rajapintaa, niiden on

a) toteutettava tarvittavat toimenpiteet sen varmistamiseksi, etteivät ne hanki, säilytä tai käsittele tietoja muihin tarkoituksiin kuin maksupalvelunkäyttäjän pyytämän palvelun tarjoamiseen;

b) täytettävä edelleen direktiivin (EU) 2015/2366 66 artiklan 3 kohdasta ja 67 artiklan 2 kohdasta johtuvat velvollisuudet;

c) rekisteröitävä tiedot, jotka hankitaan tiliä ylläpitävän maksupalveluntarjoajan maksupalvelunkäyttäjiään varten hoitaman rajapinnan välityksellä, ja toimitettava lokitiedostot pyynnöstä ja ilman aiheetonta viivytystä kansalliselle toimivaltaiselle viranomaiselleen;

d) asianmukaisesti perusteltava kansalliselle toimivaltaiselle viranomaiselle pyynnöstä ja ilman aiheetonta viivytystä sellaisen rajapinnan käyttö, joka on annettu maksupalvelunkäyttäjien käyttöön, jotta ne voivat käyttää maksutiliään suoraan verkon kautta;

e) ilmoitettava asiasta tiliä ylläpitävälle maksupalveluntarjoajalle.

6. Kuultuaan EPV:tä seuraavien edellytysten johdonmukaisen soveltamisen varmistamiseksi toimivaltaisten viranomaisten on vapautettava tiliä ylläpitävät maksupalveluntarjoajat, jotka ovat valinneet erityisrajapinnan, velvollisuudesta ottaa käyttöön 4 kohdassa kuvattu varomekanismi, jos erityisrajapinta täyttää kaikki seuraavat edellytykset:

a) se täyttää kaikki erityisrajapintoihin 32 artiklan mukaisesti sovellettavat velvollisuudet;

b) se on suunniteltu ja sitä on testattu 30 artiklan 5 kohdan mukaisesti kyseisessä kohdassa tarkoitettuja maksupalveluntarjoajia tyydyttävällä tavalla;

c) maksunpalveluntarjoajat ovat käyttäneet sitä laajasti vähintään kolmen kuukauden ajan tilitietopalvelujen ja maksutoimeksiantopalvelujen tarjoamiseen ja varojen saatavuuden vahvistamiseen korttipohjaisia maksuja varten;

d) kaikki erityisrajapintaan liittyvät ongelmat on ratkaistu ilman aiheetonta viivytystä.

7. Toimivaltaisten viranomaisten on peruutettava 6 kohdassa tarkoitettu poikkeus, jos tiliä ylläpitävät maksupalveluntarjoajat eivät täytä a ja d alakohdassa säädettyjä edellytyksiä yli kahden peräkkäisen kalenteriviikon ajan. Toimivaltaisten viranomaisten on ilmoitettava peruutuksesta EPV:lle ja varmistettava, että tiliä ylläpitävä maksupalveluntarjoaja ottaa 4 kohdassa tarkoitetun varomekanismin käyttöön mahdollisimman pian ja viimeistään kahden kuukauden kuluessa.

34 artikla

Varmenteet

1. Maksupalveluntarjoajien on käytettävä 30 artiklan 1 kohdan a alakohdassa tarkoitettuun varmentamiseen asetuksen (EU) N:o 910/2014 3 artiklan 30 kohdassa tarkoitettua sähköisen leiman hyväksyttyä varmennetta tai mainitun asetuksen 3 artiklan 39 kohdassa tarkoitettua verkkosivustojen todentamisen hyväksyttyä varmennetta.

2. Sovellettaessa tätä asetusta asetuksen (EU) N:o 910/2014 liitteessä III olevan c alakohdan tai liitteessä IV olevan c alakohdan mukaisella virallisissa rekistereissä olevassa muodossa olevalla rekisterinumerolla tarkoitetaan korttipohjaisia maksuvälineitä liikkeeseen laskevan maksupalveluntarjoajan, tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien, myös näitä palveluja tarjoavien tiliä ylläpitävien maksupalveluntarjoajien, toimiluvan numeroa, joka on saatavissa kotijäsenvaltion julkisesta rekisteristä direktiivin (EU) 2015/2366 14 artiklan nojalla tai joka on tuloksena jokaista Euroopan parlamentin ja neuvoston direktiivin 2013/36/EU ([1]) 8 artiklan nojalla myönnettyä toimilupaa koskevista ilmoituksista, jotka annetaan mainitun direktiivin 20 artiklan mukaisesti.

3. Edellä 1 kohdassa tarkoitettuihin sähköisten leimojen tai verkkosivustojen todentamisen hyväksyttyihin varmenteisiin sisältyy tätä asetusta sovellettaessa rahoitusalalla tavanomaisesti käytettävällä kielellä ilmaistuja erityisiä valinnaisia lisäattribuutteja kunkin seuraavan seikan osalta:

a) maksupalveluntarjoajan rooli, joka voi olla yksi tai useampi seuraavista toiminnoista:

   i) tilien ylläpito;

   ii) maksutoimeksiannot;

   iii) tilitiedot;

   iv) korttipohjaisten maksuvälineiden liikkeeseenlasku;

b) niiden toimivaltaisten viranomaisten nimi, joissa maksupalvelujentarjoaja on rekisteröity.

4. Edellä 3 kohdassa tarkoitetut attribuutit eivät vaikuta sähköisten leimojen tai verkkosivustojen todentamisen hyväksyttyjen varmenteiden yhteentoimivuuteen eikä tunnustamiseen.

([1]) Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU, annettu 26 päivänä kesäkuuta 2013, oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta (EUVL L 176, 27.6.2013, s. 338).

35 artikla

Viestintäistuntojen turvallisuus

1. Tiliä ylläpitävien maksupalveluntarjoajien, korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien, tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on varmistettava, että vaihdettaessa tietoja internetissä viestinnän osapuolten välillä sovelletaan turvallista salausta koko viestintäistunnon ajan käyttämällä vahvoja ja yleisesti tunnustettuja salaustekniikoita, jotta turvataan tietojen luottamuksellisuus ja eheys.

2. Korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien, tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on pidettävä tiliä ylläpitävien maksupalveluntarjoajien tarjoamat pääsyistunnot mahdollisimman lyhyinä, ja niiden on aktiivisesti lopetettava nämä istunnot heti, kun pyydetty toimi on saatu päätökseen.

3. Ylläpitäessään rinnakkaisia verkkoistuntoja tiliä ylläpitävän maksupalveluntarjoajan kanssa tilitietopalvelun tarjoajien ja maksutoimeksiantopalvelun tarjoajien on varmistettava, että nämä istunnot liitetään turvallisesti maksupalvelunkäyttäjän (maksupalvelunkäyttäjien) kanssa käynnistettyihin istuntoihin, jotta estetään niiden välillä vaihdettujen viestien tai tietojen ohjaaminen väärille tahoille.

4. Tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien tarjoajien on kommunikoidessaan tiliä ylläpitävän maksupalveluntarjoajan kanssa viitattava yksiselitteisesti kaikkiin seuraaviin seikkoihin:

a) maksupalvelunkäyttäjä tai maksupalvelunkäyttäjät ja vastaava viestintäistunto, jotta samalta maksupalvelunkäyttäjältä tai samoilta maksupalvelunkäyttäjiltä tulevat pyynnöt voidaan erottaa toisistaan;

b) kun on kyse maksutoimeksiantopalveluista, käynnistetty maksutapahtuma, joka on varmennettu yksilöllisesti;

c) kun on kyse varojen saatavuuden vahvistamisesta, yksilöllisesti varmennettu pyyntö, joka koskee korttipohjaisen maksutapahtuman toteuttamiseen tarvittavaa määrää.

5. Tiliä ylläpitävien maksupalveluntarjoajien, tilitietopalvelun tarjoajien, maksutoimeksiantopalvelun tarjoajien ja korttipohjaisia maksuvälineitä liikkeeseen laskevien maksupalveluntarjoajien on varmistettava, että niiden lähettäessä henkilökohtaisia turvatunnuksia ja tunnistamiskoodeja kukaan henkilöstön jäsen ei pysty lukemaan niitä suoraan tai välillisesti.

Jos palveluntarjoajien toimivaltaan kuuluvien henkilökohtaisten turvatunnusten luottamuksellisuus menetetään, palveluntarjoajien on ilman aiheetonta viivytystä ilmoitettava asiasta sille maksupalvelunkäyttäjälle, johon henkilökohtaiset turvatunnukset liittyvät, sekä kyseisten tunnusten antajalle.

36 artikla

Tietojenvaihdot

1. Tiliä ylläpitävien maksupalveluntarjoajien on täytettävä kaikki seuraavat vaatimukset:

a) niiden on annettava tilitietopalvelun tarjoajille samat tiedot nimetyiltä maksutileiltä ja niihin liittyvistä maksutapahtumista, jotka annetaan maksupalvelunkäyttäjän saataville, jos tilitietoihin pääsyä pyydetään suoraan ja kyseiset tiedot eivät sisällä arkaluonteisia maksutietoja;

b) niiden on välittömästi maksutoimeksiannon vastaanottamisen jälkeen annettava maksutoimeksiantopalvelun tarjoajille samat tiedot maksutapahtuman käynnistämisestä ja toteuttamisesta, jotka annetaan maksupalvelunkäyttäjälle tai sen saataville, kun kyseinen käyttäjä käynnistää maksutapahtuman suoraan;

c) niiden on pyynnöstä annettava välittömästi maksupalveluntarjoajille vahvistus yksinkertaisessa ”kyllä”- tai ”ei”-muodossa sen mukaan, onko maksutapahtuman toteuttamiseen tarvittava määrä käytettävissä maksajan maksutilillä.

2. Jos varmentamis- tai tunnistamisprosessin tai tietoelementtien vaihdon aikana sattuu odottamaton tapahtuma tai virhe, tiliä ylläpitävän maksupalveluntarjoajan on lähetettävä maksutoimeksiantopalvelun tarjoajalle tai tilitietopalvelun tarjoajalle ja korttipohjaisia maksuvälineitä liikkeeseen laskevalle maksupalveluntarjoajalle ilmoitusviesti, jossa selitetään odottamattoman tapahtuman tai virheen syy.

Jos tiliä ylläpitävä maksupalveluntarjoaja tarjoaa erityisrajapinnan 32 artiklan mukaisesti, rajapinnan on oltava sellainen, että jokainen maksunpalveluntarjoaja, joka havaitsee odottamattoman tapahtuman tai virheen, lähettää siitä ilmoitusviestit muille viestintäistuntoon osallistuville maksupalveluntarjoajille.

3. Tilitietopalvelun tarjoajilla on oltava käytössään asianmukaiset ja tehokkaat mekanismit, joilla estetään pääsy muihin kuin nimetyiltä maksutileiltä ja niihin liittyvistä maksutapahtumista oleviin tietoihin käyttäjän nimenomaisen hyväksynnän mukaisesti.

4. Maksutoimeksiantopalvelun tarjoajien on annettava tiliä ylläpitäville maksupalveluntarjoajille samat tiedot, jotka on pyydetty maksupalvelunkäyttäjältä maksutapahtumaa käynnistettäessä.

5. Tilitietopalvelun tarjoajilla on oltava mahdollisuus saada nimetyiltä maksutileiltä ja niihin liittyvistä maksutapahtumista olevat tiedot, jotka ovat tiliä ylläpitävien maksupalveluntarjoajien hallussa, jommassakummassa seuraavista tilanteista:

a) aina, kun maksupalvelunkäyttäjä pyytää aktiivisesti tällaisia tietoja;

b) kun maksupalvelunkäyttäjä ei pyydä tällaista tietoa aktiivisesti, enintään neljä kertaa 24 tunnin aikana, jos tilitietopalvelun tarjoaja ja tiliä ylläpitävä maksupalveluntarjoaja eivät ole sopineet keskenään tietojen tiheämmästä saannista, maksupalvelunkäyttäjän hyväksynnällä.

VI LUKU

LOPPUSÄÄNNÖKSET

37 artikla

Uudelleentarkastelu

Rajoittamatta direktiivin (EU) 2015/2366 98 artiklan 5 kohdan soveltamista EPV tarkastelee viimeistään 14 päivänä maaliskuuta 2021 tämän asetuksen liitteessä tarkoitettuja petososuuksia ja 33 artiklan 6 kohdan nojalla myönnettyjä, erityisrajapintoja koskevia poikkeuksia ja toimittaa tarvittaessa komissiolle päivitysluonnokset asetuksen (EU) N:o 1093/2010 10 artiklan mukaisesti.

38 artikla

Voimaantulo

1. Tämä asetus tulee voimaan seuraavana päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

2. Tätä asetusta sovelletaan 14 päivästä syyskuuta 2019.

3. Edellä olevan 30 artiklan 3 ja 5 kohtaa sovelletaan kuitenkin 14 päivästä maaliskuuta 2019.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 27 päivänä marraskuuta 2017.

Komission puolesta

Puheenjohtaja

Jean-Claude JUNCKER

LIITE

	Petosten viiteosuus (%):	
Poikkeuksen kynnysarvo	Sähköiset korttipohjaiset etämaksut	Sähköiset etätilisiirrot
500 euroa	0,01	0,005
250 euroa	0,06	0,01
100 euroa	0,13	0,015