EBA/GL/2014/12_Rev1

19. joulukuuta 2014

Ohjeet

internet-maksujen turvallisuudesta

Sisällysluettelo

Ohjeet internet-maksujen turvallisuudesta

Näiden ohjeiden asema

Tämä asiakirja sisältää ohjeet, jotka on laadittu Euroopan valvontaviranomaisen (Euroopan pankkiviranomaisen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/78/EY kumoamisesta 24 päivänä marraskuuta 2010 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1093/2010 (EPV-asetus) 16 artiklassa säädetyllä tavalla. EPV-asetuksen 16 artiklan 3 kohdan mukaisesti toimivaltaisten viranomaisten ja finanssilaitosten on kaikin tavoin pyrittävä noudattamaan ohjeita.

Ohjeissa esitetään Euroopan pankkiviranomaisen näkemys Euroopan finanssivalvojien järjestelmässä toteutettavista asianmukaisista valvontakäytännöistä tai siitä, miten unionin lainsäädäntöä on sovellettava tietyllä alalla. Näin ollen Euroopan pankkiviranomainen odottaa kaikkien toimivaltaisten viranomaisten ja finanssilaitosten, joille ohjeet on osoitettu, noudattavan niitä. Toimivaltaisten viranomaisten, joita nämä ohjeet koskevat, on noudatettava ohjeita sisällyttämällä ne valvontakäytäntöihinsä asianmukaisesti (esimerkiksi muuttamalla lainsäädäntöään tai valvontasääntöjään ja/tai ohjeitaan tai valvontamenettelyjään), mukaan luettuina tietyt, ensisijaisesti laitoksille osoitetut ohjeet.

Raportointivaatimukset

EPV-asetuksen 16 artiklan 3 kohdan mukaan toimivaltaisten viranomaisten on ilmoitettava EPV:lle 5. toukokuuta 2015 mennessä, noudattavatko tai aikovatko ne noudattaa näitä ohjeita, sekä esitettävä perustelunsa, mikäli ne eivät noudata näitä ohjeita. Jos ilmoitusta ei toimiteta tähän määräaikaan mennessä, EPV katsoo, että toimivaltaiset viranomaiset eivät noudata ohjeita. Ilmoitukset on toimitettava lähettämällä jaksossa 5 oleva lomake osoitteeseen compliance@eba.europa.eu. Viitteeksi on merkittävä EBA/GL/2014/12. Ilmoituksen lähettäjällä on oltava asianmukaiset valtuudet ilmoittaa ohjeiden noudattamisesta kyseisen toimivaltaisen viranomaisen puolesta.

Ilmoitukset julkaistaan EPV:n verkkosivustolla 16 artiklan 3 kohdan mukaisesti.

I – Soveltamisala ja määritelmät

Soveltamisala

1. Näissä ohjeissa vahvistetaan verkkomaksujen turvallisuutta koskevat vähimmäisvaatimukset. Ohjeet perustuvat direktiivin 2007/64/EY[1] (jäljempänä 'maksupalveludirektiivi') sääntöihin maksupalveluja koskevista tiedonantovaatimuksista ja maksupalveluntarjoajien velvollisuuksista niiden tarjotessa maksupalveluja. Direktiivin 10 artiklan 4 kohdassa vaaditaan lisäksi, että maksulaitoksilla on käytössään toimivat päätöksenteko-, ohjaus- ja valvontajärjestelyt ja riittävät sisäisen valvonnan menetelmät.

2. Ohjeita sovelletaan maksupalveluihin, joita direktiivin 1 artiklassa määritellyt maksupalveluntarjoajat tarjoavat internetin välityksellä.

3. Ohjeet osoitetaan asetuksen (EU) N:o 1093/2010 4 artiklan 1 kohdassa määritellyille rahoituslaitoksille ja asetuksen (EU) N:o 1093/2010 4 artiklan 2 kohdassa määritellyille toimivaltaisille viranomaisille. Euroopan unionin 28 jäsenvaltion toimivaltaisten viranomaisten tulisi varmistaa valvonnassaan, että maksupalveludirektiivin 1 artiklassa määritellyt maksupalveluntarjoajat soveltavat näitä ohjeita.

4. Toimivaltaiset viranomaiset voivat myös päättää vaatia, että maksupalveluntarjoajien on ilmoitettava toimivaltaiselle viranomaiselle noudattavansa ohjeita.

5. Nämä ohjeet eivät heikennä suosituksia, joita Euroopan keskuspankki on antanut internet-maksujen turvallisuudesta ("Recommendations for the security of internet payments", jäljempänä 'raportti')[2], vaan ne ovat edelleen pätevät. Kyseinen raportti on vastedeskin asiakirja, jonka perusteella keskuspankkien tulisi maksujärjestelmien ja -välineiden yleisvalvonnassa arvioida internet-maksujen turvallisuusvaatimusten noudattamista.

6. Ohjeet ovat vähimmäisvaatimuksia. Ne eivät vaikuta maksupalveluntarjoajien velvollisuuteen seurata ja arvioida maksutoimintoihinsa liittyviä riskejä, laatia omat yksityiskohtaiset turvallisuuspolitiikkansa ja toteuttaa riittäviä turvallisuutta, varautumista, häiriönhallintaa ja toiminnan jatkuvuutta koskevia toimenpiteitä, jotka ovat yhteismitallisia tarjottaviin maksupalveluihin liittyvien riskien kanssa.

7. Ohjeiden tarkoituksena on määritellä yhteiset vähimmäisvaatimukset alla luetelluille internet-maksupalveluille riippumatta siitä, millaisella laitteella niitä käytetään:

    - [kortit] virtuaalisten ja muiden korttimaksujen suorittaminen internetissä sekä korttimaksutietojen rekisteröinti käytettäväksi ns. lompakkoratkaisuissa;

[1] Euroopan parlamentin ja neuvoston direktiivi 2007/64/EY, annettu 13 päivänä marraskuuta 2007, maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta (EUVL L 319, 5.12.2007).

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [tilisiirrot] tilisiirtojen suorittaminen verkossa;

- [sähköinen valtakirja] sähköisten suoraveloitusvaltakirjojen antaminen ja muuttaminen;

- [sähköinen raha] sähköisen rahan siirrot kahden sähköisen rahan tilin välillä internetissä.

8. Ohjeessa esitetyt vaatimukset ja suositukset voidaan saavuttaa erilaisin keinoin. Näissä ohjeissa on jäljempänä esitettävien vaatimusten lisäksi (liitteessä 1) hyviä käytännön esimerkkejä, joita maksupalveluntarjoajia on hyvä mutta ei pakko noudattaa.

9. Maksupalvelujen ja -välineiden (esim. maksukortti, tilisiirto- ja suoraveloitusjärjestelmät) valvonnasta vastaavien toimivaltaisten viranomaisten ja keskuspankkien tulisi tehdä yhteistyötä varmistaakseen, että järjestelmän toiminnasta vastaavat toimijat soveltavat ohjeita yhdenmukaisesti.

10. Maksupalveluja tarjoavien ns. maksuintegroijien (*payment integrators*) [3] katsotaan olevan joko verkkomaksupalvelujen välittäjiä (ja siten maksupalveluntarjoajia) tai asiaankuuluvien järjestelmien tai maksupalveluntarjoajien ulkopuolisten teknisten palvelujen tuottajia. Jälkimmäisessä tapauksessa maksuintegroijat tulisi velvoittaa sopimusteitse noudattamaan ohjeita.

11. Ohjeiden soveltamisalaan eivät kuulu:

- muut verkkopalvelut, joita maksupalveluntarjoaja tarjoaa maksusivustonsa välityksellä (esim. sähköiset arvopaperinvälityspalvelut, online-sopimukset);

- maksut, joissa toimeksianto annetaan postitse, puhelimitse, puhepostin välityksellä tai käyttäen tekstiviestejä;

- muut kuin selainpohjaiset mobiilimaksut;

- tilisiirrot, joissa kolmannella osapuolella on pääsy asiakkaan maksutilille;

- maksutapahtumat, jotka yritys toteuttaa erillisverkkojen välityksellä;

- korttimaksut anonyymeilla fyysisillä tai virtuaalisilla maksukorteilla (prepaid-korteilla), joille ei voi uudelleen ladata rahaa; kortin liikkeeseenlaskijan ja kortinhaltijan välillä ei ole myöskään jatkuvaa kanssakäymistä;

- maksutapahtumien selvitys ja katteensiirto.

[3] Maksuintegroijat tarjoavat maksunsaajalle (eli verkkokauppiaalle) standardoidun rajapinnan maksupalveluntarjoajien tuottamiin maksutoimeksiantopalveluihin.

Määritelmät

12. Näissä ohjeissa käytetään maksupalveludirektiivissä annettujen määritelmien lisäksi seuraavia määritelmiä:

- *Todentaminen* tarkoittaa menettelytapaa, jolla maksupalveluntarjoajan on mahdollista todentaa asiakkaan henkilöllisyys.

- *Asiakkaan vahva tunnistaminen* tarkoittaa näissä ohjeissa menettelytapaa, joka perustuu kahden tai useamman seuraavan tekijän käyttöön – tekijät ryhmitellään tiedoksi, hallussapidoksi ja henkilökohtaiseksi ominaisuudeksi: i) jokin, jonka ainoastaan käyttäjä tietää, esim. kiinteä salasana, tunnus, henkilökohtainen tunnusluku; ii) jokin, joka on ainoastaan käyttäjän hallussa, esim. tunniste, toimikortti, matkapuhelin; iii) jokin, jota käyttäjä on (ominaisuuksiltaan), esim. sormenjälki tai muu biometrinen ominaisuus. Näiden valittujen tekijöiden on oltava lisäksi toisistaan riippumattomia, eli yhden tekijän paljastuminen ei vaaranna toista tekijää tai toisia tekijöitä. Vähintään yhden tekijöistä tulisi olla sellainen, ettei sitä voida käyttää uudelleen eikä jäljentää (lukuun ottamatta henkilökohtainen ominaisuus) eikä henkilön tietämättä varastaa internetin välityksellä. Asiakkaan vahvan tunnistamisen menettely olisi suunniteltava sellaiseksi, että se takaa tunnistamistietojen luottamuksellisuuden.

- *Valtuuttaminen* tarkoittaa menettelytapaa, jossa tarkastetaan, onko asiakkaalla tai maksupalveluntarjoajalla oikeus toteuttaa jokin toimenpide, esim. oikeus siirtää varoja tai oikeus päästä luottamuksellisiin tietoihin.

- *Tunn*isteet tarkoittavat – yleensä luottamuksellisia – tietoja, joita asiakas tai maksupalveluntarjoaja toimittaa tunnistautumista varten. Tunnisteet voivat tarkoittaa myös fyysistä välinettä, johon tiedot sisältyvät (esim. kertasalasanan generaattori, toimikortti), tai jotakin, jonka käyttäjä muistaa tai joka on ominaista vain hänelle (esim. biometriset ominaisuudet).

- *Merkittävä häiriö* maksamisen turvallisuudessa tarkoittaa häiriötä, joka vaikuttaa tai saattaa vaikuttaa olennaisesti maksamiseen liittyvien maksupalveluntarjoajan järjestelmien turvallisuuteen, eheyteen tai jatkuvuuteen ja/tai luottamuksellisten maksutietojen tai varojen turvallisuuteen. Olennaisuutta arvioitaessa tulisi ottaa huomioon vaikutukselle mahdollisesti altistuvien asiakkaiden lukumäärä, vaarassa oleva rahamäärä sekä laajempi vaikutus muihin maksupalveluntarjoajiin tai muihin maksuinfrastruktuureihin.

- *Maksutapahtuman riskianalyysi* tarkoittaa tiettyyn maksutapahtumaan liittyvän riskin arvioimista siten, että otetaan huomioon muun muassa asiakkaan maksamistavat (toiminta), kyseessä olevan maksutapahtuman arvo, tuotetyyppi sekä maksunsaajan profiili.

- *Virtuaalikortti* tarkoittaa korttipohjaista maksuratkaisua, jossa luodaan vaihtoehtoinen, väliaikainen ja rajallisen ajan voimassa oleva korttinumero, jonka käyttö on rajoitettu verkko-ostoksiin ja jossa on ennalta määritelty käyttöraja.

- *Lompakkoratkaisut* tarkoittavat ratkaisuja, joilla asiakas voi rekisteröidä yhteen tai useampaan maksuvälineeseen liittyviä tietoja suorittaakseen maksuja usealle verkkokauppiaalle.

II – Ohjeet internet-maksujen turvallisuudesta

Yleinen valvonta- ja turvallisuusympäristö

Hallinto ja ohjaus

1. Maksupalveluntarjoajan tulisi laatia verkkomaksupalvelujen turvallisuuspolitiikka ja arvioida se säännöllisin väliajoin.

   1.1 Turvallisuuspolitiikka tulisi dokumentoida asianmukaisesti ja arvioida säännöllisin väliajoin (ohjeen 2.4 mukaisesti). Sen tulee olla toimivan johdon hyväksymä. Turvallisuuspolitiikassa tulisi määritellä turvallisuustavoitteet ja riskinottohalukkuus.

   1.2 Turvallisuuspolitiikassa tulisi määritellä tehtävät ja vastuut, riskienhallinnan raportointi johdolle, internet-maksupalveluja koskevat raportointikanavat, sekä riskiarvioon perustuva luottamuksellisten maksutietojen hallinta.

Riskien arviointi

2. Maksupalveluntarjoajan tulisi laatia yksityiskohtaiset riskinarviot, jotka koskevat verkkomaksujen ja niihin liittyvien palvelujen turvallisuutta sekä ennen palvelun tai palvelujen käyttöönottoa että myöhemmin säännöllisesti..

   2.1 Maksupalveluntarjoajan riskienhallinnan tulisi laatia yksityiskohtaiset riskiarviot internet-maksuista ja niihin liittyvistä palveluista. Maksupalveluntarjoajan tulisi huomioida nykyisiin tai suunniteltuihin maksupalveluihinsa kohdistuvat turvallisuusuhat seuraamalla näitä palveluja jatkuvasti ja ottaa tällöin huomioon i) palveluissa käytetyt tekniset ratkaisut, ii) ulkopuolisille palveluntarjoajille ulkoistetut palvelut ja iii) asiakkaan tekninen toimintaympäristö. Maksupalveluntarjoajan tulisi huomioida valittuihin järjestelmäalustoihin liittyvät riskit, sovellusarkkitehtuuri, ohjelmointitekniikat ja -käytännöt niin omalla tahollaan[4] kuin asiakkaiden taholla[5] sekä turvallisuuteen liittyvien häiriöiden seurantaprosessin tulokset (ks. ohje 3).

   2.2 Maksupalveluntarjoajan tulisi tämän perusteella päättää, onko nykyisiin turvatoimenpiteisiin tehtävä muutoksia ja kuinka laajoja ne ovat, mitä teknologioita käytetään ja mitä menettelytapoja tai palveluja tarjotaan. Maksupalveluntarjoajan tulisi ottaa huomioon muutosten vaatima aika (kuten niiden saattaminen asiakkaiden käyttöön) ja toteutettava tarvittavat väliaikaiset toimenpiteet turvallisuushäiriöiden ja petosten sekä mahdollisten häiriövaikutusten minimoimiseksi.

[4] Kuten alttius istunnon kaappaukselle maksun suorittamisen aikana, SQL-injektioille, XSS-haavoittuvuuksille (Cross-Site Scripting), puskurin ylivuotovirheille jne.

[5] Kuten riskit, jotka liittyvät mm. multimediasovellusten, selaimen liitännäisten, kehysten ja ulkoisten linkkien käyttöön.

2.3 Riskejä arvioitaessa tulisi kiinnittää huomiota luottamuksellisten maksutietojen suojaamis- ja turvaamistarpeeseen.

2.4 Maksupalveluntarjoajan tulisi tarkistaa riskiskenaariot ja nykyiset turvatoimenpiteet palveluihinsa vaikuttavien merkittävien häiriöiden jälkeen, ennen infrastruktuuriin tai menettelytapoihin tehtävää huomattavaa muutosta ja kun riskien seurannassa havaitaan uusia uhkia. Lisäksi tulisi vähintään kerran vuodessa tarkistaa riskiarviot. Riskiarviot ja niiden tarkistusten tulokset tulisi toimittaa hyväksyttäviksi toimivalle johdolle.

Häiriöseuranta ja -raportointi

3. Maksupalveluntarjoajan tulisi varmistaa turvallisuushäiriöiden sekä turvallisuuteen liittyvien asiakasvalitusten yhdenmukainen seuranta, käsittely ja jatkotoimet. Maksupalveluntarjoajan tulisi laatia menettelytapa, jolla tällaisista häiriöistä raportoidaan johdolle ja – jos kyse on maksuturvallisuutta koskevista merkittävistä häiriöistä – toimivaltaisille viranomaisille.

3.1 Maksupalveluntarjoajalla tulisi olla käytössään prosessi turvallisuuteen liittyvien häiriöiden ja asiakasvalitusten seurantaa, käsittelyä ja jatkotoimia sekä johdolle raportointia varten.

3.2 Maksupalveluntarjoajalla tulisi olla menettely, jolla toimivaltaisille viranomaisille (eli valvonta- ja tietosuojaviranomaisille) ilmoitetaan välittömästi, jos maksupalveluissa ilmenee merkittäviä häiriöitä maksamisen turvallisuudessa..

3.3 Maksupalveluntarjoajalla tulisi olla menettely, joka mahdollistaa yhteistyön asiaankuuluvien lainvalvontaviranomaisten kanssa merkittävissä tietoturvaloukkauksissa ja merkittävissä maksamisen turvallisuushäiriöissä.

3.4 Maksutapahtumia hyvittävän tai välittävän maksupalveluntarjoajan tulisi vaatia sopimusteitse, että verkkokauppiaat, jotka tallentavat, käsittelevät tai välittävät luottamuksellisia maksutietoja, tekevät tietoturvaloukkauksissa ja merkittävissä maksuturvallisuutta koskevissa muissa häiriöissä yhteistyötä sekä maksupalveluntarjoajan että asiaankuuluvien lainvalvontaviranomaisten kanssa. Jos maksupalveluntarjoaja saa tietää, ettei verkkokauppias tee sopimuksessa vaadittua yhteistyötä, sen tulisi ryhtyä toimiin tämän sopimusvelvoitteen täytäntöön panemiseksi tai irtisanoa sopimus.

Riskien hallinta

4. Maksupalveluntarjoajan tulisi toteuttaa turvallisuuspolitiikkansa mukaisia turvallisuustoimenpiteitä tunnistettujen riskien vähentämiseksi. Näihin toimenpiteisiin tulisi sisällyttää useita turvakerroksia, jotka mahdollistavat sen, että epäonnistuminen yhdellä turvatasolla korjataan seuraavalla turvatasolla.

4.1 Suunnitellessaan, kehittäessään ja ylläpitäessään internet-maksupalveluja maksupalveluntarjoajan tulisi kiinnittää erityistä huomiota tietoteknisissä toimintaympäristöissä (esim. kehitys-, testaus- ja tuotantoympäristöissä) hoidettavien tehtävien eriyttämiseen. Lisäksi käyttäjille tulee myöntää vain välttämättömät käyttövaltuudet työtehtäviin nähden.

4.2 Maksupalveluntarjoajalla tulisi olla käytössään asianmukaiset turvallisuusratkaisut verkkojen, verkkosivustojen, palvelimien ja viestintäyhteyksien suojaamiseksi väärinkäytöltä tai hyökkäyksiltä. Maksupalveluntarjoajan tulisi karsia palvelimilta kaikki tarpeettomat toiminnot suojatakseen (vahvistaakseen) niitä ja poistaakseen tai vähentääkseen vaaralle alttiiden sovellusten haavoittuvuutta. Eri sovellusten pääsy vaadittuihin tietoihin ja resursseihin tulisi pitää ehdottomassa minimissä. Jotta voitaisiin rajoittaa (maksupalveluntarjoajien laillisia sivustoja jäljittelevien) ”huijaussivustojen” käyttöä, internet-maksupalveluja tarjoavat sivustot, joilla toteutetaan maksutapahtumia, tulisi tunnistaa maksupalveluntarjoajan nimissä laadituilla sertifikaateilla tai vastaavanlaisilla todentamismenetelmillä.

4.3 Maksupalveluntarjoajalla tulisi olla käytössään asianmukaiset prosessit, joilla seurataan, jäljitetään ja rajoitetaan pääsyä i) luottamuksellisiin maksutietoihin ja ii) kriittisiin loogisiin ja fyysisiin resursseihin, kuten verkkoon, järjestelmiin, tietokantoihin, turvamoduuleihin jne. Maksupalveluntarjoajan tulisi luoda, tallentaa ja analysoida asianmukaisia lokeja ja kirjausketjuja.

4.4 Suunnitellessaan, kehittäessään ja pitäessään yllä internet-maksupalveluja maksupalveluntarjoajan tulisi varmistaa, että luottamuksellisten maksutietojen kerääminen, reitittäminen, käsittely, tallentaminen ja/tai arkistointi sekä näkyvyys pidetään ehdottomalla minimitasolla.

4.5 Internet-maksupalvelujen turvatoimenpiteitä tulisi testata riskienhallintatoiminnon valvonnassa niiden tehokkuuden ja vaikuttavuuden varmistamiseksi. Kaikki muutokset olisi tehtävä virallisessa muutoksenhallintaprosessissa, jolla varmistetaan, että muutokset suunnitellaan, testataan, dokumentoidaan ja hyväksytään asianmukaisesti. Testit olisi toistettava säännöllisin väliajoin jo tehtyjen muutosten ja havaittujen turvallisuusuhkien perusteella, ja niihin tulisi sisällyttää skenaarioita relevanteista ja tiedossa olevista mahdollisista hyökkäyksistä.

4.6 Maksupalveluntarjoajan internet-maksupalvelujen turvatoimenpiteet tulisi ajoittain tarkastaa niiden tehokkuudenvarmistamiseksi. Myös internet-maksupalvelujen käyttöönotto ja toimivuus tulisi tarkastaa. Tällaisten tarkastusten tiheydessä ja painopisteissä tulisi ottaa huomioon kyseessä olevat turvallisuusriskit, ja tarkastukset tulisi suhteuttaa oikein tällaisiin riskeihin. Tarkastusten tekijöiden tulisi olla luotettuja ja riippumattomia (sisäisiä tai ulkopuolisia) asiantuntijoita. Heidän ei pitäisi olla millään tavalla mukana verkkomaksupalvelujen kehittämisessä, toteuttamisessa tai toimintojen ohjauksessa.

4.7 Kun maksupalveluntarjoaja ulkoistaa verkkomaksupalvelujen turvallisuuteen liittyviä toimintoja, sopimukseen tulisi sisällyttää ehtoja, jotka edellyttävät näissä ohjeissa esitettyjen periaatteiden ja suositusten noudattamista.

4.8 Maksutapahtumien hyvitys- tai välityspalveluita tuottavan maksupalveluntarjoajan tulisi vaatia sopimusteitse, että verkkokauppiaat, jotka käsittelevät (eli tallentavat, prosessoivat tai välittävät) luottamuksellisia maksutietoja, toteuttavat tietojärjestelmäinfrastruktuurissaan turvatoimenpiteitä ohjeiden 4.1–4.7 mukaisesti, jotta luottamuksellisia maksutietoja ei anastettaisi niiden omien järjestelmien kautta. Jos maksupalveluntarjoaja saa tietää, ettei verkkokauppiaalla ole vaadittuja turvatoimenpiteitä, sen tulisi ryhtyä toimiin tämän sopimusvelvoitteen täytäntöön panemiseksi tai irtisanoa sopimus.

Jäljitettävyys

5. Maksupalveluntarjoajalla tulisi olla käytössään prosessit, joilla varmistetaan, että kaikki maksutapahtumat sekä sähköistä valtakirjaa koskevan prosessin kulku voidaan asianmukaisesti jäljittää.

5.1 Maksupalveluntarjoajan tulisi varmistaa, että sen palveluun sisältyy turvallisuusmekanismeja, joilla rekisteröidään yksityiskohtaisesti maksutapahtumia ja sähköisiä valtakirjoja koskevat tiedot, kuten maksutapahtuman juokseva numero, maksutapahtumatietojen aikaleimat, parametroinnin muutokset sekä maksutapahtumia ja sähköisiä valtakirjoja koskevien tietojen käyttöoikeudet.

5.2 Maksupalveluntarjoajan tulisi käyttää lokitiedostoja, joiden avulla voidaan jäljittää kaikki maksutapahtumia ja sähköisiä valtakirjoja koskevien tietojen lisäykset, muutokset tai poistot.

5.3 Maksupalveluntarjoajan tulisi analysoida maksutapahtumia ja sähköisiä valtakirjoja koskevat tiedot ja varmistaa, että sillä on keinot arvioida lokitiedostoja. Tällaisten sovellusten tulisi olla ainoastaan valtuutetun henkilöstön käytettävissä.

Internet-maksuja koskevat erityiset valvonta- ja turvatoimenpiteet

Asiakaan ensitunnistaminen ja tunnistamistiedot

6. Ennen kuin asiakkaalle annetaan oikeus käyttää internet-maksupalveluja, hänet tulisi tunnistaa asianmukaisesti rahanpesun estämisen eurooppalaisen lainsäädännön [6] mukaisesti ja vahvistaa, että hän on halukas suorittamaan internetmaksuja tällaisia

[6] Esimerkiksi Euroopan parlamentin ja neuvoston direktiivi 2005/60/EY, annettu 26 päivänä lokakuuta 2005, rahoitusjärjestelmän käytön estämisestä rahanpesutarkoituksiin sekä terrorismin rahoitukseen. EUVL L 309, 25.11.2005, s. 15–36. Ks. myös komission direktiivi 2006/70/EY, annettu 1 päivänä elokuuta 2006, täytäntöönpanotoimenpiteistä ”poliittisesti vaikutusvaltaisen henkilön” määritelmän sekä yksinkertaistettuja asiakkaan tuntemismenettelyjä sekä satunnaisesti tai hyvin rajoitetusti harjoitetun rahoitustoiminnan perusteella myönnettyjä poikkeuksia koskevien teknisten perusteiden osalta. EUVL L 214, 4.8.2006, s. 29–34.

palveluja käyttäen. Maksupalveluntarjoajan tulisi antaa asiakkaalle riittävästi ”ennakkotietoja” tai ”varsinaisia tietoja” tai tarvittaessa ”tapauskohtaisia tietoja” niistä vaatimuksista (esim. laitteisto, menettelyt), jotka on täytettävä turvallisten internet-maksutapahtumien toteuttamiseksi, sekä niihin sisältyvistä riskeistä.

6.1 Ennen kuin maksupalveluntarjoaja myöntää asiakkaalle verkkomaksupalvelujen käyttöoikeuden, sen tulisi varmistaa, että asiakas on tunnistettu ja että asiakas on toimittanut riittävät henkilöllisyysasiakirjat[7] ja niihin liittyvät tiedot.[8]

6.2 Maksupalveluntarjoajan tulisi varmistaa, että asiakkaalle annettavat ennakkotiedot[9] sisältävät yksityiskohtaiset tiedot internet-maksupalveluista. Lisätietojen tulisi sisältää tarvittaessa seuraavat:

- selkeät tiedot vaatimuksista, jotka koskevat asiakkaan laitteistoa, ohjelmistoa tai muita tarvittavia välineitä (esim. virustorjuntaohjelma, palomuurit);
- suosituksia henkilökohtaisten tunnisteiden asianmukaisesta ja turvallisesta käytöstä;
- vaiheittainen kuvaus menettelystä, jossa asiakas tekee ja hyväksyy maksutoimeksiannon ja/tai saa tietoa muun muassa kunkin toimen seurauksista;
- ohjeita kaikkien asiakkaalle toimitettujen laitteistojen ja ohjelmistojen asianmukaisesta ja turvallisesta käytöstä;
- menettelyt, joita noudatetaan, kun henkilökohtaiset tunnisteet tai sisäänkirjautumisessa tai maksutapahtumien toteuttamisessa käytettävä asiakkaan laitteisto tai ohjelmisto katoaa tai ne anastetaan;
- menettelyt, joita noudatetaan, jos havaitaan tai epäillään, että kyseessä on laiton käyttö;
- kuvaus internet-maksupalvelun käyttöä koskevista maksupalveluntarjoajan ja asiakkaan velvollisuuksista ja vastuista.

6.3 Maksupalveluntarjoajan tulisi varmistaa, että asiakkaan kanssa tehdyssä puitesopimuksessa määritellään maksupalveluntarjoajan mahdollisuus estää tietty

[7] Esimerkiksi passi, kansallinen henkilötodistus tai kehittynyt sähköinen allekirjoitus.

[8] Asiakkaan tuntemisprosessi ei estä soveltamasta voimassa olevassa rahanpesun estämisen lainsäädännössä säädettyjä poikkeuksia. Maksupalveluntarjoajien ei tarvitse suorittaa erillistä asiakkaan tuntemisprosessia verkkomaksupalveluja varten, mikäli tällainen prosessi on jo suoritettu esim. muiden olemassa olevien maksuihin liittyvien palvelujen tai tilin avaamisen yhteydessä.

[9] Tällaiset tiedot täydentävät maksupalveludirektiivin 42 artiklaa, jossa säädetään, mitä tietoja maksupalveluntarjoajan on annettava maksupalvelun käyttäjälle ennen kuin tämän kanssa tehdään sopimus maksupalvelujen tarjoamisesta.

maksutapahtuma tai tietyn maksuvälineen käyttö[10] turvallisuusongelmien perusteella. Sopimuksessa tulisi määritellä menetelmät ja ehdot, joilla asiakkaalle ilmoitetaan tästä, sekä siitä, miten asiakas voi ottaa yhteyttä maksupalveluntarjoajaan internet-maksutapahtuman tai -palvelun eston poistamiseksi maksupalveludirektiivin mukaisesti.

Asiakkaan vahva tunnistaminen

7. Internet-maksutoimeksiannon antaminen sekä luottamuksellisiin maksutietoihin pääsy tulisi suojata asiakkaan vahvalla tunnistamisella. Maksupalveluntarjoajalla tulisi olla vahva ja näissä ohjeissa annetun määritelmän mukainen asiakkaan tunnistamismenettely.

7.1 [tilisiirto/sähköinen valtakirja/sähköinen raha] Maksupalveluntarjoajan tulisi tunnistaa asiakas vahvasti asiakkaan hyväksyessä internet-maksutoimeksiantoja (myös yhdessä erässä suoritettavia tilisiirtoja) sekä sähköisten suoraveloitusvaltakirjojen antamista tai muuttamista varten. Maksupalveluntarjoaja voi kuitenkin myös harkita ottavansa käyttöön vaihtoehtoisia asiakkaan tunnistamismenetelmiä seuraavia varten

- kyseistä asiakasta varten aiemmin laadittuihin niin sanottuihin valkoisiin listoihin sisältyville luotettaville maksunsaajille lähtevät maksut;
- saman asiakkaan kahden tilin väliset maksutapahtumat, kun molempia tilejä pitää sama maksupalveluntarjoaja;
- saman maksupalveluntarjoajan sisäiset siirrot maksutapahtuman riskianalyysin perusteella;
- maksupalveludirektiivissä tarkoitetut pienet maksut.[11]

7.2 Luottamuksellisten maksutietojen käyttömahdollisuus tai muuttaminen (mukaan lukien valkoisten listojen laatiminen ja muuttaminen) edellyttää asiakkaan vahvaa tunnistamista. Jos maksupalveluntarjoaja tarjoaa yksinomaan neuvontapalveluita, joissa ei luottamuksellisia asiakas- tai maksutietoja, esimerkiksi maksukorttitietoja, joita voitaisiin helposti käyttää väärin petostarkoituksessa, maksupalveluntarjoaja voi muuttaa tunnistamisvaatimuksiaan riskiarvionsa perusteella.

7.3 [kortit] Kaikkien kortteja liikkeeseen laskevien maksupalveluntarjoajien tulisi tukea kortinhaltijan vahvaa tunnistamista korttimaksutapahtumissa. Kaikkien liikkeeseen laskettujen korttien on oltava teknisesti valmiita (rekisteröityjä) käytettäviksi vahvan tunnistamisen kanssa.

[10] Ks. maksupalveludirektiivin 55 artikla maksuvälineen käyttörajoista.

[11] Ks. pienmaksuvälineiden määritelmä maksupalveludirektiivin 34 artiklan 1 kohdassa ja 53 artiklan 1 kohdassa.

7.4 [kortit] Maksutapahtumien hyvitys- tai välityspalveluita tarjoavan maksupalveluntarjoajan tulisi tukea teknologioita, joilla kortin liikkeeseenlaskijan on mahdollista suorittaa kortinhaltijan vahva tunnistaminen.

7.5 [kortit] Maksutapahtumien hyvitys- tai välityspalveluja tarjoavan maksupalveluntarjoajan tulisi vaatia verkkokauppiasta tukemaan ratkaisuja, joilla kortin liikkeeseenlaskijan on mahdollista tunnistaa kortinhaltija vahvasti internetissä toteutettavissa korttimaksutapahtumissa. Vaihtoehtoisten tunnistamismenetelmien käyttöä voidaan harkita ennalta määritetyissä vähäriskisissä maksutapahtumissa; tällaiset maksutapahtumat voivat esimerkiksi perustua maksutapahtuman riskianalyysiin tai sisältää maksupalveludirektiivissä tarkoitettuja pieniä maksuja.

7.6 [kortit] Lompakkoratkaisujen tarjoajien tulisi edellyttää, että kortin liikkeeseenlaskija suorittaa vahvan tunnistamisen kortin laillisen haltijan rekisteröidessä kortin tiedot.

7.7 Lompakkoratkaisujen tarjoajien tulisi tukea asiakkaan vahvaa tunnistamista asiakkaiden kirjautuessa sisään lompakkomaksupalveluihin tai toteutettaessa korttimaksutapahtumia internetin välityksellä. Vaihtoehtoisten tunnistamistoimenpiteiden käyttöä voidaan harkita ennalta määritetyissä vähäriskisissä maksutapahtumissa; tällaiset maksutapahtumat voivat olla maksupalveludirektiivissä tarkoitettuja pieniä maksuja tai perustua maksutapahtuman riskianalyysiin.

7.8 [kortit] Virtuaalikorttien ensirekisteröinnin tulisi tapahtua turvallisessa ja luotettavassa ympäristössä.[12] Virtuaalikortin tietoja luotaessa tulisi käyttää asiakkaan vahvaa tunnistamista, jos kortti lasketaan liikkeeseen verkossa.

7.9 Maksupalveluntarjoajan tulisi varmistaa asianmukainen molemminpuolinen tunnistaminen ollessaan yhteydessä verkkokauppiaisiin, kun tarkoituksena on käynnistää verkkomaksutapahtumia ja päästä käyttämään luottamuksellisia maksutietoja.

Asiakkaalle toimitettaviin tunnistusvälineisiin ja/tai -ohjelmistoihin rekisteröityminen ja hankinta

8. Maksupalveluntarjoajan tulisi varmistaa, että internet-maksupalvelun käyttämiseksi vaadittavien tunnistusvälineiden, toimittaminen asiakkaille toteutetaan turvallisella tavalla (mukaan lukien maksamiseen liittyvät ohjelmistot).

[12] Maksupalveluntarjoajan vastuulla oleva ympäristö, jossa taataan asiakkaan ja palvelun tarjoavan maksupalveluntarjoajan asiaankuuluva tunnistaminen sekä luottamuksellisten tai arkaluonteisten tietojen suojaaminen. Tällaisia ympäristöjä ovat muun muassa i) maksupalveluntarjoajan toimitilat, ii) verkkopankkisivusto tai muu turvallinen sivusto, jossa esimerkiksi valtion virasto tarjoaa muun muassa ohjeessa 4 määriteltyjen kaltaiset vastaavat turvaominaisuudet, tai iii) pankkiautomaattipalvelut. (Pankkiautomaattien tapauksessa edellytyksenä on asiakkaan vahva tunnistaminen. Tällainen tunnistaminen tapahtuu yleensä mikrosirun ja henkilökohtaisen tunnusluvun tai mikrosirun ja biometrisen tunnisteen avulla.

8.1 Asiakkaalle toimitettavien tunnistusvälineiden ja/tai maksamiseen liittyvän ohjelmiston hankinnan tulisi täyttää seuraavat vaatimukset:

- Niihin liittyvät menettelyt tulisi toteuttaa turvallisessa ja luotettavassa ympäristössä, ja tällöin tulisi ottaa huomioon riskit, joita saattaa aiheutua laitteista, jotka eivät ole maksupalveluntarjoajan valvonnassa.

- Henkilökohtaisten tunnisteiden, maksamiseen liittyvien ohjelmistojen ja kaikkien verkkomaksamiseen liittyvien henkilökohtaisten laitteiden toimittamista varten tulisi olla käytössä tehokkaat ja turvalliset menettelyt. Internetin välityksellä toimitettavissa ohjelmistoissa tulisi olla myös maksupalveluntarjoajan digitaalinen allekirjoitus, jotta asiakas voi varmistaa ohjelmiston aitouden ja väärentämättömyyden.

- [kortit] Korttimaksutapahtumissa asiakkaalla tulisi olla mahdollisuus käyttää vahvaa tunnistamista yksittäisen verkko-ostoksen luonteesta riippumatta. Jos aktivointimahdollisuus tarjotaan verkko-ostoksen aikana, tämä tulisi tehdä ohjaamalla asiakas edelleen turvalliseen ja luotettavaan ympäristöön.

8.2 [kortit] Korttien liikkeeseenlaskijoiden tulisi kannustaa aktiivisesti kortinhaltijaa käyttämään vahvaa tunnistautumista ja sallia kortinhaltijoiden ohittaa vahva tunnistautuminen vain poikkeuksellisissa ja harvoissa tapauksissa, kun se on yksittäiseen korttimaksutapahtumaan liittyvän riskin kannalta perusteltua.

Sisäänkirjautumisyritykset, istunnon aikakatkaisu, tunnistamisen voimassaolo

9. Maksupalveluntarjoajan tulisi asettaa tietty raja sisäänkirjautumis- tai tunnistautumisyritysten lukumäärälle, määritellä säännöt internet-maksupalvelun aikakatkaisulle (time out) ja asettaa aikarajat tunnistamisen voimassaololle.

9.1 Kun tunnistamisessa käytetään kertakäyttösalasanoja, maksupalveluntarjoajan tulisi varmistaa, että salasanat ovat voimassa ainoastaan välttämättömän minimiajan.

9.2 Maksupalveluntarjoajan tulisi asettaa epäonnistuneille sisäänkirjautumis- tai tunnistautumisyrityksille enimmäismäärä, jonka jälkeen internet-maksupalvelun käyttö estetään (tilapäisesti tai pysyvästi). maksupalveluntarjoajilla tulisi olla käytössään turvallinen menettely, jolla internet-maksupalvelu aktivoidaan uudelleen eston jälkeen.

9.3 Maksupalveluntarjoajan tulisi asettaa internet-maksupalveluistunnoille enimmäisaika, jonka jälkeen istunnot keskeytetään automaattisesti, jos niitä ei käytetä.

Maksutapahtumien seuranta

10. Maksupalveluntarjoajan tulisi käyttää vilpillisten maksutapahtumien ennaltaehkäisyyn, tunnistamiseen ja torjuntaan tarkoitettuja seurantamekanismeja ennen maksutapahtuman lopullista hyväksyntää; epäilyttävät tai suuririskiset maksutapahtumat tulisi asettaa erityiseen seulonta- ja arviointimenettelyyn. Vastaavia tietoturvaseuranta- ja hyväksymismekanismeja tulisi käyttää myös sähköisten valtakirjojen antamista varten.

    10.1 Ennen maksutapahtumien tai sähköisten valtakirjojen lopullista hyväksyntää maksupalveluntarjoajan tulisi käyttää väärinkäytösten havaitsemiseen ja ennaltaehkäisyyn tarkoitettuja järjestelmiä tunnistaakseen epäilyttävät maksutapahtumat. Tällaisten järjestelmien tulisi perustua esimerkiksi parametroituihin sääntöihin (kuten vaarantuneita tai varastettuja korttitietoja koskeviin mustiin listoihin), ja niillä tulisi seurata asiakkaan tai asiakkaan laitteen epätavallisia toimintatapoja (kuten IP-osoitteen [13] tai IP-osoitealueen muutos verkkomaksupalveluistunnon aikana, joka havaitaan toisinaan Geolocation IP -tarkistuksissa, [14] sekä tietyn asiakkaan käyttämät epätyypilliset verkkokauppiasryhmät tai epätavalliset maksutapahtumatiedot jne.). Tällaisten järjestelmien tulisi myös kyetä havaitsemaan merkkejä haittaohjelman saastuttamasta istunnosta (esim. tekeekö validoinnin komentosarja vai ihminen) sekä tunnetut väärinkäytösskenaariot. Seurantaratkaisujen laajuus, monimutkaisuus ja mukautettavuus tulisi suhteuttaa riskinarvion tulokseen. Tällöin tulisi kuitenkin noudattaa asiaa koskevaa tietosuojalainsäädäntöä.

    10.2 Maksutapahtumia hyvittävän tai välittävän maksupalveluntarjoajan tulisi käyttää petosten havaitsemiseen ja ennaltaehkäisyyn tarkoitettuja järjestelmiä verkkokauppiaiden toimintojen seurantaa varten.

    10.3 Maksupalveluntarjoajan tulisi toteuttaa kaikki maksutapahtumien seulonta- ja arviointimenettelyt kohtuullisessa ajassa, jotta niistä ei aiheudu kohtuutonta viivästystä kyseessä olevan maksupalvelun aloittamiselle ja/tai toteutukselle.

    10.4 Mikäli maksupalveluntarjoaja päättää riskipolitiikkansa perusteella estää sellaisen maksutapahtuman, jossa on havaittu mahdollinen väärinkäytös, sen tulisi säilyttää esto voimassa mahdollisimman lyhyen ajan, kunnes turvallisuusongelma on ratkaistu.

Luottamuksellisten maksutietojen suojaaminen

11. Luottamukselliset maksutiedot tulisi suojata niiden tallennuksen, käsittelyn tai välityksen yhteydessä.

    11.1 Kaikki tiedot, joita käytetään asiakkaiden tunnistamisessa ja todentamisessa (esim. sisäänkirjautumisen, internet-maksutoimeksiantojen antamisen ja sähköisten

[13] IP-osoite on internetiin kytketyn tietokoneen yksilöivä numerotunnus.

[14] ”Geo-IP”-tarkistuksessa tarkistetaan, onko myöntäjämaa sama kuin IP-osoitteessa, josta käyttäjä käynnistää maksutapahtuman.

valtakirjojen antamisen, muuttamisen tai peruuttamisen yhteydessä), sekä asiakaskäyttöliittymä (maksupalveluntarjoajan tai verkkokauppiaan verkkosivusto) tulisi turvata asianmukaisin toimin luvattomalta pääsyltä tai muutoksilta.

11.2 Maksupalveluntarjoajan tulisi varmistaa tehokkaita ja laajasti tunnustettuja salaustekniikoita käyttämällä, että kun luottamuksellisia maksutietoja vaihdetaan internetin välityksellä, osapuolet käyttävät turvallista päästä-päähän-salausta[15] koko istunnon ajan tietoaineiston luottamuksellisuuden ja eheyden turvaamiseksi.

11.3 Maksutapahtumien hyvitys- tai välityspalveluita tuottavan maksupalveluntarjoajan tulisi ohjeistaa verkkokauppiaitaan jättämään luottamukselliset maksutiedot tallentamatta. Mikäli verkkokauppiaat käsittelevät (eli tallentavat, prosessoivat tai välittävät) luottamuksellisia maksutietoja, maksupalveluntarjoajan tulisi vaatia sopimusteitse, että näillä on käytössään tarvittavat toimenpiteet tällaisten tietojen suojaamiseksi. Maksupalveluntarjoajan tulisi tarkistaa säännöllisin väliajoin luottamuksellisten tietojen käsittely, ja jos se saa tietää, ettei luottamuksellisia maksutietoja käsittelevällä verkkokauppiaalla ole vaadittuja turvatoimenpiteitä, sen tulisi ryhtyä toimiin tämän sopimusvelvoitteen täytäntöön panemiseksi tai irtisanoa sopimus.

[15] Päästä-päähän -salauksella tarkoitetaan, että salaus tapahtuu lähettävän pään järjestelmässä tai sen piirissä ja purkaus vastaavasti ainoastaan vastaanottavan pään järjestelmässä tai sen piirissä. ETSI EN 302 109 V1.1.1. (2003-06).

Asiakastietoisuus, -koulutus ja -viestintä

Asiakaskoulutus ja -viestintä

12. Maksupalveluntarjoajan tulisi tarjota asiakkaille tarvittaessa neuvontaa ja ohjeistusta verkkomaksupalvelujen turvallisesta käytöstä. Maksupalveluntarjoajan tulisi viestiä asiakkaidensa kanssa siten, että asiakas voi olla vakuuttunut vastaanottamiensa viestien aitoudesta.

12.1 Maksupalveluntarjoajan tulisi tarjota ainakin yksi turvallinen kanava[16] asiakkaiden kanssa tapahtuvaan jatkuvaan viestintään, joka koskee internet-maksupalvelun oikeaa ja turvallista käyttöä. Maksupalveluntarjoajan tulisi ilmoittaa asiakkailleen tästä kanavasta ja kertoa, että kaikki maksupalveluntarjoajan puolesta muilla tavoin lähetetyt sähköpostit tai muut viestit, jotka koskevat internet-maksupalvelun oikeaa ja turvallista käyttöä, ovat epäluotettavia. Maksupalveluntarjoajan tulisi kertoa

- miten asiakkaiden on meneteltävä ilmoittaakseen maksupalveluntarjoajalle (epäillyt) vilpilliset maksut, internet-maksupalveluistunnon aikana ilmenevät epäilyttävät tapahtumat tai poikkeamat ja/tai mahdolliset käyttäjän manipulointiyritykset[17];

- seuraavista vaiheista eli siitä, miten maksupalveluntarjoaja vastaa asiakkaalle;

- miten maksupalveluntarjoaja ilmoittaa asiakkaalle (mahdollisista) vilpillisistä tai toteuttamattomista maksutapahtumista tai varoittaa asiakasta ilmenneistä hyökkäyksistä (esim. tietoja kalastelevista sähköpostiviesteistä).

12.2 Maksupalveluntarjoajan tulisi pitää asiakkaat ajan tasalla verkkomaksupalvelujen turvallisuusmenettelyjen päivityksistä turvallisen kanavan välityksellä. Kaikki varoitukset huomattavista kasvavista uusista riskeistä tulisi niin ikään lähettää turvallisen kanavan välityksellä.

12.3 Maksupalveluntarjoajan tulisi tarjota asiakkaalle neuvontaa kaikissa kysymyksissä, valituksissa, tukipyynnöissä ja poikkeamien tai häiriöiden ilmoituksissa, jotka koskevat internet-maksamista ja siihen liittyviä palveluja, ja asiakkaiden tulisi saada asianmukaisesti tieto siitä, miten tällaista neuvoa voi saada.

12.4 Maksupalveluntarjoajan tulisi käynnistää asiakaskoulutus ja -tietoisuusohjelmia, joilla varmistetaan, että asiakkaat ymmärtävät ainakin tarpeen

- suojata salasanat, tunnisteet, henkilötiedot ja muu luottamuksellinen tieto

[16] Esim. erillinen sähköpostilaatikko maksupalveluntarjoajan verkkosivustolla tai turvallinen verkkosivusto.

[17] Käyttäjän manipuloinnilla (social engineering) tarkoitetaan tässä yhteydessä ihmisten manipulointitekniikkaa, jonka tarkoituksena on saada tietoja (esim. sähköpostitse tai puhelimitse) tai napata tietoja verkkoyhteisöistä petollisiin tarkoituksiin tai tietokoneen tai verkon luvattoman käytön mahdollistamiseksi.

- hoitaa kunnolla henkilökohtaisen laitteen (esim. tietokoneen) tietoturva asentamalla ja päivittämällä tietoturvakomponentteja (virustorjunta, palomuurit ja tietoturvakorjaukset);

- ottaa huomioon huomattavat uhat ja riskit, joita liittyy ohjelmistojen lataamiseen internetistä, jos asiakas ei voi riittävästi varmistua siitä, että ohjelmisto on aito eikä väärennetty;

- käyttää maksupalveluntarjoajan aitoa internet-maksusivustoa.

12.5 Maksutapahtumia hyvittävän tai välittävän maksupalveluntarjoajan tulisi vaatia verkkokauppiaita pitämään maksamiseen liittyvät prosessit selvästi erillään verkkokaupasta, jotta asiakkaiden olisi helpompi havaita, milloin he ovat yhteydessä maksupalveluntarjoajaan eivätkä maksunsaajaan (esim. ohjaamalla asiakas uuteen osoitteeseen ja avaamalla erillinen ikkuna, jotta maksamisprosessia ei näytetä verkkokauppiaan sivulla).

Ilmoitukset, käyttörajojen asettaminen

13. Maksupalveluntarjoajan tulisi asettaa internet-maksupalveluille käyttörajoja ja sen olisi hyvä tarjota asiakkailleen mahdollisuuksia vähentää riskejä näiden rajojen sisällä. Se voi myös tarjota varoituspalveluja ja asiakasprofiilin hallintapalveluja.

13.1 Ennen internet-maksupalvelujen tarjoamista asiakkaalle maksupalveluntarjoajan tulisi asettaa palveluihin sovellettavia käyttörajoja [18] (esim. yksittäisen maksun enimmäismäärä tai tiettynä ajanjaksona suoritettavien maksujen yhteismäärä). Maksupalveluntarjoajan tulisi tarjota asiakkaille mahdollisuus poistaa internet-maksutoiminto käytöstä.

Asiakkaan pääsy maksutapahtumaa koskeviin tietoihin

14. Maksupalveluntarjoajan tulisi vahvistaa asiakkailleen, että maksutapahtuma on toteutettu, ja tarjota asiakkaille hyvissä ajoin tiedot, joita nämä tarvitsevat tarkistaakseen, että maksutapahtuma on annettu ja/tai toteutettu oikein.

14.1 [tilisiirto/sähköinen valtakirja] Maksupalveluntarjoajan tulisi tarjota asiakkaille lähes reaaliaikainen mahdollisuus tarkistaa milloin tahansa[19] maksutapahtumien tilanne ja tilien saldot turvallisessa ja luotettavassa ympäristössä.

14.2 Kaikkien yksityiskohtaisten sähköisten tiliotteiden tulisi olla saatavilla turvallisessa ja luotettavassa ympäristössä. Jos maksupalveluntarjoaja ilmoittaa asiakkaille sähköisten

[18] Tällaisia rajoja voidaan soveltaa joko yleisesti (eli kaikkiin verkkomaksut mahdollistaviin maksuvälineisiin) tai yksittäistapauksissa.

[19] Paitsi poikkeustilanteissa, joissa mahdollisuus ei ole käytettävissä teknisen huollon tai huomattavien häiriöiden vuoksi.

tiliotteiden saatavuudesta (esim. säännöllisin väliajoin, kun tiettyä jaksoa koskeva sähköinen tiliote on saatavilla, tai tapauskohtaisesti maksutapahtuman toteuttamisen jälkeen) tekstiviestillä, sähköpostilla, kirjeellä tai muun vaihtoehtoisen kanavan kautta, tällaisiin viesteihin ei tulisi sisällyttää luottamuksellisia maksutietoja tai ne tulisi ainakin suojata.

III – Loppumääräykset ja täytäntöönpano

15. Nämä ohjeet tulevat voimaan 01.08.2015.

Liite 1: Hyviä käytännön esimerkkejä

Edellä esitettyjen vaatimusten lisäksi näissä ohjeissa esitetään joitakin hyviä käytännön esimerkkejä, joita maksupalveluntarjoajien ja asiaankuuluvien markkinaosapuolten olisi hyvä mutta ei pakko ottaa käyttöön. Jotta esimerkkitapaukset olisi helppo sijoittaa oikeaan kontekstiin, niiden yhteydessä mainitaan luku, johon ne liittyvät.

Yleinen valvonta- ja turvallisuusympäristö

Hallinta ja ohjaus

Esimerkki 1: Turvallisuuspolitiikka on hyvä laatia erilliseksi asiakirjaksi.

Riskien valvonta ja vähentäminen

Esimerkki 2: Maksupalveluntarjoajan olisi hyvä tarjota asiakkaalle turvavälineitä (esim. laitteita ja/tai asianmukaisesti turvattuja asiakkaiden tarpeisiin muokattuja selaimia), joilla asiakkaan käyttöliittymä suojataan oikeudettomalta käytöltä tai hyökkäyksiltä (kuten ns. man-in-the-browser-hyökkäyksiltä).

Jäljitettävyys

Esimerkki 3: Maksutapahtumien hyvitys- tai välityspalveluja tuottavan maksupalveluntarjoajan olisi hyvä vaatia sopimusteitse, että maksutietoja tallentavilla verkkokauppiailla on käytössään asianmukaiset jäljitettävyyttä tukevat prosessit.

Internetmaksuja koskevat erityiset valvonta- ja turvatoimenpiteet

Asiakaan ensitunnistaminen ja tunnistamistiedot

Esimerkki 4: Asiakkaan olisi hyvä allekirjoittaa erillinen palvelusopimus internet-maksutapahtumien tekemisestä. Tämä on parempi ratkaisu kuin se, että palvelun ehdot sisällytetään maksupalveluntarjoajan kanssa tehtävään laajempaan yleisluonteiseen sopimukseen.

Esimerkki 5: Maksupalveluntarjoajan olisi hyvä myös varmistaa, että asiakkaille tarjotaan säännöllisesti tai tarvittaessa tapauskohtaisesti ja asianmukaisin keinoin (esim. esittein tai verkkosivujen välityksellä) selkeät ja helppotajuiset ohjeet, joissa tuodaan esiin asiakkaiden velvollisuudet, jotka liittyvät palvelun turvalliseen käyttämiseen.

Asiakkaan vahva tunnistaminen

Esimerkki 6: [kortit] Verkkokauppiaiden olisi hyvä tukea sitä, että kortin liikkeeseenlaskija tunnistaa kortinhaltijan vahvasti internetin välityksellä suoritettavissa korttimaksutapahtumissa.

Esimerkki 7: Maksupalveluntarjoajan olisi hyvä harkita käyttävänsä vain yhtä asiakkaan vahvan tunnistamisen välinettä kaikissa internet-maksupalveluissa, jotta asiakkaiden olisi helpompi käyttää palveluja. Näin asiakkaat hyväksyvät palvelun helpommin, mikä edistää palvelun asianmukaista käyttöä.

Esimerkki 8: Asiakkaan vahvaan tunnistamiseen voisi sisällyttää elementtejä, jotka liittävät tunnistamisen tiettyyn rahamäärään ja maksunsaajaan. Tämä toisi asiakkaille lisävarmuutta maksuja hyväksyttäessä.. Teknisen ratkaisun, joka mahdollistaa vahvaa tunnistamista koskevien tietojen ja maksutapahtumatietojen yhdistämisen, tulisi olla suojattu väärinkäytöksiltä.

Luottamuksellisten maksutietojen suojaaminen

Esimerkki 9: Luottamuksellisia maksutietoja käsittelevien verkkokauppiaiden olisi hyvä tarjota väärinkäytösten estämisestä vastaavalle henkilöstölleen asiaankuuluvaa koulutusta säännöllisin väliajoin, jotta sen sisältö kulloinkin vastaa muuttuvaa tietoturvaympäristöä.

Asiakaskoulutus ja -viestintä

Esimerkki 10: Maksutapahtumien hyvitys- tai välityspalveluja tuottavan maksupalveluntarjoajan olisi hyvä järjestää verkkokauppiailleen väärinkäytösten estämiseen liittyvää koulutusta.

Ilmoitukset, rajoitusten asettaminen

Esimerkki 11: Maksupalveluntarjoajan olisi hyvä tarjota asiakkailleen ennalta määriteltyjen rajojen puitteissa mahdollisuus asettaa ja hallita internet-maksupalveluihin liittyviä käyttörajoja turvallisessa ja luotettavassa ympäristössä.

Esimerkki 12: Maksupalveluntarjoajan olisi hyvä varoittaa asiakkaita esimerkiksi puhelimitse tai tekstiviestillä epäilyttävistä tai suuririskisistä maksutapahtumista riskienhallintapolitiikkansa mukaisesti.

Esimerkki 13: Maksupalveluntarjoajan tulisi tarjota asiakkaille mahdollisuus määrittää omia yleisiä sääntöjä, joilla rajoitetaan heidän toimintaansa internetmaksuissa ja niihin liittyvissä palveluissa. Asiakkaat voivat esimerkiksi määrätä, että he antavat maksutoimeksiantoja ainoastaan tietyistä maista käsin ja että muualta annetut maksutoimeksiannot on estettävä. He voivat myös sisällyttää tiettyjä maksunsaajia valkoisille tai mustille listoille.