EBA/GL/2014/12_Rev1

19. detsember 2014

Lõplikud suunised

Internetimaksete turvalisus

Sisukord

Internetimaksete turvalisuse suunised

Käesolevate suuniste staatus

Käesolev dokument hõlmab suuniseid, mis antakse välja Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määruse (EL) nr 1093/2010 (millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ) (EBA määrus) artikli 16 alusel. Kooskõlas EBA määruse artikli 16 lõikega 3 peavad pädevad asutused ja finantseerimisasutused võtma mis tahes meetmeid, et kõnealuseid suuniseid järgida.

Käesolevates suunistes kirjeldatakse järelevalvetavasid, mis Euroopa Pangandusjärelevalve hinnangul on asjakohased Euroopa Finantsjärelevalve Süsteemis rakendamiseks, ehk teisisõnu, kuidas tuleks liidu õigust konkreetses valdkonnas kohaldada. Seega Euroopa Pangandusjärelevalve eeldab, et käesolevaid suuniseid järgivad kõik pädevad asutused ja finantseerimisasutused, kellele nimetatud suunised on mõeldud. Suuniste adressaadiks olevad pädevad asutused peaksid suuniseid järgima, lisades need sobival viisil oma järelevalvetavadesse (nt muutes oma õigusraamistikku või järelevalvemenetlusi), kaasa arvatud juhul, kui suunised on mõeldud eelkõige finantseerimisasutustele.

Aruandlusnõuded

5. maiks 2015 peavad pädevad asutused kooskõlas EBA määruse artikli 16 lõikega 3 Euroopa Pangandusjärelevalvele teatama, kas nad järgivad või kavatsevad kõnealuseid suuniseid järgida, ning kui neid ei järgita või järgida ei kavatseta, siis tuleb seda otsust põhjendada. Kui pädevad asutused jätavad nimetatud tähtpäevaks vastava teate saatmata, käsitab Euroopa Pangandusjärelevalve seda nii, et kõnealustes asutustes suuniseid ei järgita. Teated tuleks saata jaotises 5 esitatud vormil aadressil compliance@eba.europa.eu, märkides viite „EBA/GL/2014/12”. Teated peaksid esitama isikud, kellel on vajalikud volitused oma pädeva asutuse nimel aru anda sellest, kas suuniseid järgitakse või ei järgita.

Kooskõlas EBA määruse artikli 16 lõikega 3 avaldatakse teated Euroopa Pangandusjärelevalve veebilehel.

I jaotis. Reguleerimisala ja mõisted

Reguleerimisala

1. Käesolevate suunistega sätestatakse internetimaksete turvalisuse miinimumnõuded. Suunised tuginevad direktiivi 2007/64/EÜ[1] (edaspidi „makseteenuste direktiiv") eeskirjadele, mis käsitlevad makseteenuste teabele esitatavaid nõudeid ja makseteenuste pakkujate kohustusi seoses makseteenuste osutamisega. Lisaks sellele nõutakse direktiivi artikli 10 lõikes 4, et makseasutused võtaksid kasutusele kindla juhtimiskorralduse ja piisavad sisekontrolli mehhanismid.

2. Käesolevaid suuniseid kohaldavad makseteenuse pakkujad interneti kaudu pakutavate makseteenuste osutamisele, nagu on määratletud direktiivi artiklis 1.

3. Käesolevad suunised on suunatud määruse (EL) nr 1093/2010 artikli 4 lõikes 1 määratletud finantseerimisasutustele ja määruse (EL) nr 1093/2010 artikli 4 lõikes 2 määratletud pädevatele asutustele. Euroopa Liidu 28 liikmesriigi pädevad asutused peaksid tagama, et nende järelevalve alla kuuluvad makseteenuste direktiivi artiklis 1 määratletud makseteenuse pakkujad kohaldavad neid suuniseid.

4. Lisaks sellele võivad pädevad asutused otsustada, et nõuavad makseteenuse pakkujatelt pädevale asutusele suuniste järgimise teatamist.

5. Käesolevad suunised ei mõjuta Euroopa Keskpanga internetimaksete turvalisuse soovituste (edaspidi „aruanne")[2] kehtivust. Aruanne jääb dokumendiks, mille alusel keskpangad peaksid oma maksesüsteemide ja -viiside järelevalve funktsiooni täites hindama vastavust internetimaksete turvalisuse nõuetele.

6. Käesolevates suunistes on sätestatud miinimumnõuded. Nendega ei piirata makseteenuse pakkujate vastutust jälgida ja hinnata maksetoimingute riske, koostada oma üksikasjalikud turbepoliitikad ja rakendada nõuetekohaseid turvalisuse, hädaolukorra lahendamise, vahejuhtumite lahendamise ja toimepidevuse meetmeid, mis on samaulatuslikud osutatud makseteenustele olemuslike riskidega.

7. Suuniste eesmärk on määratleda ühised miinimumnõuded alljärgnevatele internetimakseteenustele, olenemata kasutatavast seadmest:

    - [kaardid] internetis kaardimaksete tegemine, sealhulgas virtuaalkaardimaksed ning kaardi makseandmete registreerimine nn rahakotilahenduste jaoks kasutamiseks;

[1] Euroopa Parlamendi ja nõukogu direktiiv 2007/64/EÜ, 13. november 2007, makseteenuste kohta siseturul ning direktiivide 97/7/EÜ, 2002/65/EÜ, 2005/60/EÜ ja 2006/48/EÜ muutmise ning direktiivi 97/5/EÜ kehtetuks tunnistamise kohta (ELT L 319, 5.12.2007).

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

- [krediidikorraldused] internetis krediidikorralduste tegemine;

- [e-volitus] otsedebiteerimise elektrooniliste volituste väljastamine ja muutmine;

- [e-raha] kahe e-raha konto vahel interneti kaudu elektroonilise rahaülekannete tegemine.

8. Kui suunistes on märgitud tulemus, võib tulemuse saavutada mitmel viisil. Käesolevates suunistes esitatakse lisaks allpool märgitud nõuetele ka parimate tavade näited (1. lisas), mida makseteenuse pakkujaid kutsutakse üles järgima, aga mille järgimine ei ole kohustuslik.

9. Kui makseteenuste ja -viiside osutamine toimub maksekava kaudu (näiteks kaardimaksekavad, krediidikorralduste kavad, otsedebiteerimise kavad jne), peaksid makseviiside järelevalve funktsiooni täitev asjaomane keskpank ja pädevad asutused tegema koostööd, et tagada, et kava toimimise eest vastutavad tegutsejad rakendavad käesolevaid suuniseid järjepidevalt.

10. Kaardimaksete algatamise teenuseid pakkuvaid maksete integreerijaid [3] peetakse kas internetimakseteenuste omandajateks (ja seega makseteenuse pakkujateks) või asjakohaste kavade või makseteenuse pakkujate asutusevälisteks tehniliste teenuste osutajateks. Viimasel juhul peaksid maksete integreerijad olema lepinguga kohustatud suuniseid järgima.

11. Suuniste reguleerimisalast jäävad välja

- muud internetiteenused, mida makseteenuse pakkujad osutavad oma makseveebikoha kaudu (nt e-vahendamine, veebilepingud);

- maksed, mille juhised esitatakse posti, telefonitellimuse, kõneposti või SMS-põhise tehnoloogia abil;

- mobiiltelefonimaksed, välja arvatud brauseripõhised maksed;

- krediidikorraldused, kus kolmas isik saab juurdepääsu kliendi maksekontole;

- ettevõtja poolt erivõrkude kaudu tehtavad maksetehingud;

- anonüümsete ja füüsiliste või virtuaalsete vahendite lisamist mittevõimaldavate ettemaksekaartide abil tehtud kaardimaksed, kui puudub väljastaja ja kaardiomaniku pidev suhe;

- maksetehingute kliiring ja arveldus.

[3] Maksete integreerijad pakuvad makse saajale (st e-kauplejale) standardiseeritud liidese makseteenuse pakkuja osutatud makse algatamise teenustele.

Mõisted

12. Käesolevates suunistes ja täiendusena makseteenuste direktiivi mõistetele kasutatakse järgmisi mõisteid:

- „Autentimine" – menetlus, mis võimaldab makseteenuse pakkujal kontrollida kliendi identiteeti.

- „Tugev autentimissüsteem" – käesolevates suunistes menetlus, milles kasutatakse vähemalt kaht järgmist elementi, mis kuuluvad teadmise, omamise või tunnuse kategooriasse: i) midagi, mida teab ainult kasutaja, näiteks püsiparool, kood, PIN-kood; ii) midagi, mis on ainult kasutajal, näiteks autentimistõend, kiipkaart, mobiiltelefon; iii) kasutaja mingi omadus, näiteks biomeetrilised omadused (nt sõrmejälg). Lisaks sellele peavad valitud elemendid olema üksteisest sõltumatud, st ühe rikkumine ei ohusta teist/teisi. Vähemalt üks nendest elementidest ei tohiks olla korduvkasutatav ega korratav (v.a tunnus) ja seda ei tohiks olla võimalik interneti kaudu varjatult varastada. Tugev autentimismenetlus tuleks koostada nii, et autentimisandmete konfidentsiaalsus oleks kaitstud.

- „Volitamine" – menetlus, millega kontrollitakse, kas kliendil või makseteenuse pakkujal on õigus teha teatud toiming, näiteks rahaülekande õigus või saada juurdepääs tundlikele andmetele.

- „Volitused" – enamasti konfidentsiaalne teave, mille esitab klient või makseteenuse pakkuja autentimise eesmärgil. Volitused võivad tähendada ka teavet sisaldava füüsilise vahendi omamist (nt ühekorraparoolide generaator, kiipkaart) või midagi, mille kasutaja jätab meelde, või tema mingit omadust (nt biomeetrilised omadused).

- „Oluline makseturvaintsident" – vahejuhtum, mis oluliselt mõjutab või võib oluliselt mõjutada makseteenuse pakkuja maksesüsteemide turvalisust, usaldusväärsust või jätkuvust ja/või tundlike andmete või vahendite turvalisust. Olulisuse hindamisel tuleks arvestada võimalike mõjutatud klientide arvu, ohustatud summat ja mõju teistele makseteenuse pakkujatele või maksetaristutele.

- „Tehingu riskianalüüs" – konkreetse tehingu riski hindamine, arvestades selliseid kriteeriume nagu kliendi maksemustrid (käitumine), seonduva tehingu väärtus, toote tüüp ja makse saaja profiil.

- „Virtuaalkaardid" – kaardipõhine makselahendus, milles luuakse internetiostude jaoks kasutatav alternatiivne ajutine kaardinumber, millel on piiratud kehtivusperiood, piiratud kasutus ja eelmääratud kasutuslimiit.

- „Rahakotilahendused" – lahendused, millega klient saab registreerida ühe või mitme maksevahendi andmed, et teha makseid mitmele e-kauplejale.

II jaotis. Internetimaksete turvalisuse suunised

Üldine kontrolli ja turvalisuse keskkond

Üldjuhtimine

1. Makseteenuse pakkujad peaksid rakendama internetimakseteenuste jaoks ametlikku turvapoliitikat ja seda regulaarselt läbi vaatama.

   1.1 Turvapoliitika peaks olema nõuetekohaselt dokumenteeritud, korrapäraselt läbi vaadatud (kooskõlas suunisega 2.4) ning heaks kiidetud kõrgema juhtkonna poolt. Turvapoliitika peaks määratlema turvaeesmärgid ja riskivalmidus.

   1.2 Turvapoliitikas tuleks määratleda rollid ja vastutusvaldkonnad, sealhulgas riskijuhtimise funktsiooni täitmine koos otsese aruandlusahelaga juhtkonnatasandile ja aruandlusahelatega osutatavate internetimakseteenuste kohta, sealhulgas tundlike makseandmete haldamine seoses riskihindamise, riskikontrolli ja riskide maandamisega.

Riskihindamine

2. Makseteenuse pakkujad peaksid internetimaksete ja nendega seotud teenuste turvalisuse osas tegema ja dokumenteerima põhjalikke riskihindamisi nii enne teenus(t)e kasutuselevõttu kui ka korrapäraselt pärast seda.

   2.1 Makseteenuse pakkujad peaksid oma riskijuhtimise funktsiooni kaudu tegema ja dokumenteerima internetimaksete ja seonduvate teenuste detailseid riskihindamisi. Makseteenuse pakkujad peaksid arvestama nende poolt osutatavate või planeeritavate internetimakseteenustega seotud turvaohtude pideva seire tulemusi, arvestades i) nende kasutatavaid tehnoloogilisi lahendusi, ii) asutusevälistele teenuseosutajatele edasi antud teenuseid ja iii) klientide tehnilist keskkonda. Makseteenuse pakkujad peaksid arvestama valitud tehnoloogiaplatvormide, rakendusarhitektuuri, programmeerimistehnikate ning rutiinide riske nii enda poolel[4] kui ka klientide poolel[5] ning samuti turvaintsidentide järelevalve menetluse tulemusi (vt suunis 3).

   2.2 Eeltoodu alusel peaksid makseteenuse pakkujad määrama, kas ja mis ulatuses võib olla vaja muuta olemasolevaid turvameetmeid, kasutatavaid tehnoloogiaid, menetlusi või osutatavaid teenuseid. Makseteenuse pakkujad peaksid arvestama muudatuste rakendamiseks (sealhulgas klientide jaoks kasutuselevõtuks) vajalikku aega ning võtma

[4] Näiteks süsteemi vastuvõtlikkus makseseansi ülevõtmise, SQL-injektsiooni, murdskriptimise, puhvri ületäitumise suhtes jne.

[5] Näiteks multimeediarakenduste, brauseri pistikprogrammide, raamide, välislinkide jne riskid.

vahemeetmeid turvaintsidentide ja pettuste ning võimaliku takistava mõju minimeerimiseks.

2.3 Riskide hindamise raames tuleks käsitleda vajadust kaitsta ja turvata tundlikke makseandmeid.

2.4 Makseteenuse pakkujad peaksid vaatama läbi riskistsenaariumid ja olemasolevad turvameetmed pärast nende teenuseid mõjutavaid olulisi intsidente, enne taristu või menetluse olulist muudatust ning kui riskide seire tegevuste käigus tuvastatakse uusi ohte. Lisaks sellele tuleks vähemalt kord aastas teha riskihindamise üldine läbivaatamine. Riskihindamiste ja läbivaatamiste tulemused tuleks esitada kinnitamiseks kõrgemale juhtkonnale.

Intsidentide järelevalve ja aruandlus

3. Makseteenuse pakkujad peaksid tagama turvaintsidentide järjepideva ja integreeritud seire, käsitlemise ning järelmeetmed, sealhulgas klientide turvateemaliste kaebuste korral. Makseteenuse pakkuja peaks kehtestama turvaintsidentidest juhatusele ja oluliste makseturvaintsidentide korral pädevatele asutustele teatamise menetluse.

3.1 Makseteenuse pakkujatel peaks olema kasutusel turvaintsidentide ja turvalisusega seotud kliendikaebuste seire, käsitlemise ja järelmeetmete võtmise ning intsidentidest juhatusele teatamise menetlus.

3.2 Makseteenuse pakkujatel peaks olema kasutusel menetlus, millega tagatakse pädevatele asutustele – järelevalveasutustele ja andmekaitseasutustele (kui on olemas), viivitamatu teatamine, kui on toimunud osutatud makseteenustega seotud oluline makseturvaintsident.

3.3 Makseteenuse pakkujatel peaks olema kasutusel menetlus koostööks asjaomaste õiguskaitseasutustega oluliste makseturvaintsidentide, sealhulgas andmeturvalisuse rikkumiste korral.

3.4 Vastuvõtvad makseteenuse pakkujad peaksid lepinguga nõudma, et e-kauplejad säilitaksid, töötleksid või edastaksid tundlikke andmeid oluliste makseturvaintsidentide, sealhulgas andmeturvalisuse rikkumiste teemal nii nendega kui ka asjaomaste õiguskaitseasutusega toimuva koostöö jaoks. Kui makseteenuse pakkuja saab teada, et e-kaupleja ei tee lepingu nõuete kohaselt koostööd, peaks ta võtma meetmeid selle lepingukohustuse jõustamiseks või lepingu lõpetamiseks.

Riskikontroll ja riskide maandamine

4. Makseteenuse pakkujad peaksid rakendama oma turvapoliitika kohaselt turvameetmeid tuvastatud riskide maandamiseks. Meetmed peaksid hõlmama turvalisuse kaitse mitut

kihti, millest ühe läbimise korral tagatakse kaitse järgmise kihiga (edaspidi „mitmekihiline kaitse").

4.1 Internetimakseteenuste kavandamisel, arendamisel ja haldamisel peaksid makseteenuse pakkujad pöörama eritähelepanu infotehnoloogiakeskkondade (nt arendus-, katse- ja tootmiskeskkond) piisavale lahususele ning identiteedi ja juurdepääsu juhtimise alusena n-ö vähimate õiguste põhimõtte rakendamisele.[6]

4.2 Makseteenuse pakkujatel peaksid võrkude, veebikohtade, serverite ja sidelinkide kuritarvitamise või rünnakute eest kaitseks olema kasutusel asjakohased turvalahendused. Makseteenuse pakkujad peaksid kõrvaldama serveritest nende kaitsmiseks (tugevdamiseks) kõik liigsed funktsioonid ning kõrvaldama riskialdiste rakenduste haavatavused või neid vähendama. Eri rakenduste juurdepääs andmetele ja ressurssidele tuleks hoida vähimate õiguste põhimõtte kohaselt minimaalsena. Makseteenuse pakkuja tegelikke veebikohti matkivate võltsveebikohtade kasutamise piiramiseks tuleks internetimakseteenuseid pakkuvad tehingute veebikohad tuvastada makseteenuse pakkuja nimel koostatud laiendatud valideerimissertifikaatide või muu sarnase autentimismeetodi abil.

4.3 Makseteenuse pakkujatel peaksid olema kasutusel asjakohased järgmistele elementidele juurdepääsu seire, jälgimise ja piiramise menetlused: i) tundlikud makseandmed ning ii) loogilised ja füüsilised kriitilised vahendid, näiteks võrgud, süsteemid, andmebaasid, turvamoodulid jne. Makseteenuse pakkujad peaksid koostama, säilitama ja analüüsima asjakohaseid logisid ja kontrolljälgi.

4.4 Makseteenuse pakkujad peaksid internetimakseteenuste kavandamisel[7], arendamisel ja haldamisel tagama, et andmete minimeerimine[8] on põhifunktsioonide oluline osa: tundlike makseandmete kogumine, marsruutimine, töötlemine, salvestamine ja/või arhiivimine ning visualiseerimine tuleks hoida kõige minimaalsemal võimalikul tasemel.

4.5 Internetimakseteenuste turvameetmeid tuleks katsetada riskijuhtimise funktsiooni järelevalve all, et tagada nende stabiilsus ja tõhusus. Kõigile muudatustele tuleks kohaldada ametlikku muudatushalduse menetlust, millega tagatakse, et kõiki muudatusi kavandatakse, katsetatakse, dokumenteeritakse ja volitatakse nõuetekohaselt. Katseid tuleks tehtud muudatuste ja täheldatud turvaohtude alusel regulaarselt korrata ning need peaksid sisaldama asjakohaste ja teadaolevate võimalike rünnakute stsenaariume.

[6] „Süsteemi iga programm ja iga õigustega kasutaja peaks tegutsema ülesande täitmiseks vähimaid võimalikke õigusi kasutades." Vt Saltzer, J.H. (1974), „Protection and the Control of Information Sharing in Multics", Communications of the ACM, 17. aastakäik, nr 7, lk 388.

[7] Lõimitud eraelukaitse.

[8] Andmete minimeerimine tähendab põhimõtet, et konkreetse funktsiooni täitmiseks kogutakse isikuandmeid võimalikult vähe.

4.6 Makseteenuse pakkuja internetimakseteenuste turvameetmeid tuleks regulaarselt auditeerida, et tagada nende stabiilsus ja tõhusus. Auditeerida tuleks ka internetimakseteenuste rakendamist ja toimimist. Auditite sagedus ja rõhuasetus peaks arvestama asjakohaseid turvariske ning auditid peaksid olema nendega proportsionaalsed. Auditeerima peaksid usaldusväärsed ja sõltumatud (asutusesisesed või -välised) eksperdid. Nad ei tohiks olla mingil viisil seotud osutatavate internetimakseteenuste arendamise, rakendamise või haldamisega.

4.7 Alati, kui makseteenuse pakkuja kasutab internetimakseteenuste turvalisusega seotud funktsioonide jaoks allhanget, peaks leping sisaldama sätteid, millega nõutakse käesolevate suuniste põhimõtete ja juhiste järgimist.

4.8 Makseteenuse pakkujad, kes pakuvad vastuvõtmise teenuseid, peaksid tundlikke makseandmeid käitlevatelt (salvestavatelt, töötlevatelt või edastavatelt) e-kauplejatelt lepinguga nõudma nende IT-taristus turvameetmete rakendamist kooskõlas suunistega 4.1–4.7, et vältida tundlike makseandmete vargust e-kauplejate süsteemide kaudu. Kui makseteenuse pakkuja saab teada, et e-kaupleja ei kasuta nõutavaid turvameetmeid, peaks ta võtma meetmeid selle lepingukohustuse jõustamiseks või lepingu lõpetamiseks.

Jälgitavus

5. Makseteenuse pakkujatel peaksid olema rakendatud menetlused, millega tagatakse kõigi tehingute, sealhulgas e-volituse menetlusvoo asjakohane jälgimine.

5.1 Makseteenuse pakkujad peaksid tagama, et nende teenus sisaldab turvamehhanisme, millega üksikasjalikult logitakse tehingu ja e-volituse andmed, sealhulgas tehingu järjekorranumber, tehinguandmete ajatemplid, parameetrite muudatused ning samuti juurdepääs tehingu ja e-volituse andmetele.

5.2 Makseteenuse pakkujad peaksid kasutama logifaile, millega saab jälgida tehingu ja e-volituse andmete mis tahes täiendusi, muudatusi või kustutusi.

5.3 Makseteenuse pakkujad peaksid tegema ja analüüsima tehingu ja e-volituse andmete päringuid, et tagada logifailide hindamisvahendite olemasolu. Asjakohased rakendused peaksid olema kättesaadavad ainult volitatud isikutele.

Internetimaksete konkreetsed kontrolli- ja turvameetmed

Kliendi esialgne tuvastamine, teave

6. Kliendid tuleks kooskõlas Euroopa rahapesuvastaste õigusaktidega [9] nõuetekohaselt tuvastada ja nad peaksid kinnitama oma valmidust teha teenuste abil internetimakseid, enne kui neile antakse teenustele juurdepääs. Makseteenuse pakkujad peaksid esitama kliendile nõuetekohase eelneva, korrapärase või erakorralise teabe turvaliste internetimaksetehingute nõuete (nt seadmed, menetlused) ja nende olemuslike riskide kohta.

6.1 Makseteenuse pakkujad peaksid tagama, et klient on läbinud kliendi suhtes rakendatavad hoolsusmenetlused ja on esitanud nõuetekohased isikut tõendavad dokumendid [10] ning seonduva teabe, enne kui talle antakse juurdepääs internetimakseteenustele.[11]

6.2 Makseteenuse pakkujad peaksid tagama, et kliendile esitatud eelteave[12] sisaldab internetimakseteenuste üksikasjalikku teavet, muu hulgas järgmist:

- kliendi seadmetele, tarkvarale või muudele vajalikele vahenditele (nt viirustõrjetarkvara, tulemüürid) kehtivate mis tahes nõuete selge teave;
- individuaalsete turvavolituste nõuetekohase ja turvalise kasutamise suunised;
- kliendi poolt maksetehingu esitamise ja volitamise ning/või teabe saamise menetluse üksikasjalik kirjeldus koos iga toimingu tulemustega;
- kogu kliendile pakutava riistvara ja tarkvara nõuetekohase ning turvalise kasutamise suunised;
- sisselogimiseks või tehingute tegemiseks vajalike isiklike turvavolituste või kliendi riistvara või tarkvara kaotamise või varguse korral kohaldatav menetlus;
- tuvastatud või oletatava kuritarvitamise korral kohaldatav menetlus;
- internetimakseteenuse kasutamisel makseteenuse pakkuja ja kliendi vastutuse ja kohustuste kirjeldus.

[9] Näiteks Euroopa Parlamendi ja nõukogu 26. oktoobri 2005. aasta direktiiv 2005/60/EÜ rahandussüsteemi rahapesu ja terrorismi rahastamise eesmärgil kasutamise vältimise kohta. ELT L 309, 25.11.2005, lk 15–36. Vt ka komisjoni 1. augusti 2006. aasta direktiiv 2006/70/EÜ Euroopa Parlamendi ja nõukogu direktiivi 2005/60/EÜ rakendusmeetmete kehtestamise kohta seoses mõistega „riikliku taustaga isik" ning kliendi suhtes lihtsustatud nõuetekohaste hoolsuse menetluste ja harva või väga piiratud mahus teostatud finantstegevuse alusel tehtud erandite tehniliste kriteeriumite kohta. ELT L 214, 4.8.2006, lk 29–34.

[10] Näiteks pass, riiklik ID-kaart või täiustatud e-allkiri.

[11] Kliendi tuvastamise menetlus ei välista mis tahes erandite kohaldamist, mis on sätestatud kehtivates rahapesuvastastes õigusaktides. Makseteenuse pakkujad ei pea internetimakseteenuste korral tuvastama klienti eraldi menetlusega, kui klient on juba tuvastatud, näiteks seoses teiste olemasolevate makseteenustega või konto avamiseks.

[12] See teave täiendab teavet, mida nõutakse makseteenuste direktiivi artikli 42 kohaselt, kus on sätestatud, mis teavet peab makseteenuse pakkuja esitama makseteenuse kasutajale enne makseteenuste osutamise lepingu sõlmimist.

6.3 Makseteenuse pakkuja peaks tagama, et kliendiga sõlmitud raamlepingus on sätestatud, et makseteenuse pakkuja võib turvakaalutlustel blokeerida konkreetse tehingu või makseviisi[13]. Selles tuleks sätestada kliendile teatamise meetod ja tingimused ning viis, kuidas klient saab makseteenuse pakkuja poole pöörduda internetimakse tehingu või teenuse blokeeringu kõrvaldamiseks kooskõlas makseteenuste direktiiviga.

[13] Vt makseteenuste direktiivi artikkel 55 makseviisi kasutamise piirangute kohta.

Tugev klientide autentimise süsteem

7. Internetimaksete algatamist ja juurdepääsu tundlikele makseandmetele tuleks kaitsta tugeva autentimissüsteemi abil. Makseteenuse pakkujad peaksid kasutama tugeva autentimissüsteemi menetlust kooskõlas käesolevates suunistes esitatud määratlusega.

7.1 [krediidikorraldus/e-volitus/e-raha] Makseteenuse pakkujad peaksid tagama kliendi poolt internetimaksete tehingute (sh liitkrediidikorralduste) ning otsedebiteerimise elektrooniliste volituste väljastamise või muutmise korral kliendi volitamise tugeva autentimissüsteemi. Samas võivad makseteenuse pakkujad kaaluda alternatiivsete kliendi autentimise meetmete rakendamist järgmistel juhtudel:

- selle kliendi jaoks olemasolevate valgetesse nimekirjadesse kantud usaldatud saajatele suunatud maksed;
- sama kliendi sama makseteenuse pakkuja juures oleva kahe konto vahelised tehingud;
- sama makseteenuse pakkuja piires tehtud tehingud, kui see on õigustatud tehingu riskianalüüsi alusel;
- madala väärtusega maksed, nagu on osutatud maksteenuste direktiivis.[14]

7.2 Tundlikele makseandmetele juurdepääsu saamiseks või nende muutmiseks (sh valgete nimekirjade koostamiseks ja muutmiseks) on vaja tugevat autentimissüsteemi. Kui makseteenuse pakkuja pakub ainult nõustamisteenuseid ilma tundlike kliendi- või makseandmete (nt maksekaardi andmed) esitamiseta, mida saab pettuse toimepanemiseks kergesti väärkasutada, võib makseteenuse pakkuja autentimisnõudeid riskihindamise alusel kohandada.

7.3 [kaardid] Kaarditehingute korral peaksid kõik kaarte väljastavad makseteenuse pakkujad toetama kaardiomaniku tugeva autentimise süsteemi. Kõik väljastatud kaardid peavad olema tehniliselt valmis (registreeritud) tugeva autentimise süsteemiga kasutamiseks.

7.4 [kaardid] Vastuvõtmisteenuseid pakkuvad makseteenuse pakkujad peaksid toetama tehnoloogiaid, millega väljastaja saab kasutada kaardiomaniku suhtes turvalise autentimise süsteemi nende kaardimaksekavade korral, milles vastuvõtja osaleb.

7.5 [kaardid] Vastuvõtmisteenuseid pakkuvad makseteenuse pakkujad peaksid nõudma, et nende e-kaupleja toetaks väljastajal kaardiomaniku poolt internetis tehtavate kaarditehingute jaoks tugeva autentimise süsteemi kasutamist. Madala riskiga tehingute eelnevalt tuvastatud kategooriate korral võib kaaluda alternatiivseid

[14] Vt madala väärtusega makseviisi määratlus makseteenuste direktiivi artikli 34 lõikes 1 ja artikli 53 lõikes 1.

autentimismeetmeid, näiteks tehingu riskianalüüsi alusel või kui maksed on madala väärtusega, nagu on osutatud makseteenuste direktiivis.

7.6 [kaardid] Teenuse poolt lubatud kaardimakse kavade korral peaksid rahakotilahenduste pakkujad nõudma väljastaja poolt tugeva autentimise süsteemi kasutamist, kui seaduslik hoidja registreerib esimest korda kaardi andmed.

7.7 Rahakotilahenduste pakkujad peaksid toetama tugeva autentimise süsteemi, kui kliendid logivad rahakoti makseteenustesse sisse või teevad interneti kaudu kaarditehinguid. Madala riskiga tehingute eelnevalt tuvastatud kategooriate korral võib kaaluda alternatiivseid autentimismeetmeid, näiteks tehingu riskianalüüsi alusel või kui maksed on madala väärtusega, nagu on osutatud makseteenuste direktiivis.

7.8 [kaardid] Virtuaalkaartide korral peaks esialgne registreerimine toimuma ohutus ja usaldusväärses keskkonnas.[15] Virtuaalkaardi andmete koostamisel tuleks nõuda kliendi tugeva autentimise süsteemi, kui kaart väljastatakse internetikeskkonnas.

7.9 Makseteenuse pakkujad peaksid tagama nõuetekohase kahepoolse autentimise, kui nad suhtlevad e-kauplejatega internetimaksete algatamiseks ja tundlikele makseandmetele juurdepääsu saamiseks.

Kliendi lisamine, autentimisvahendite ja/või tarkvara edastamine

8. Makseteenuse pakkujad peaksid tagama, et kliendi internetimakseteenuse kasutajate hulka lisamine ja teenuse kasutamiseks vajalike autentimisvahendite ja/või vastava maksetarkvara edastamine toimub turvaliselt.

8.1 Kliendi kasutajate hulka lisamine ja autentimisvahendite ja/või maksetarkvara edastamine peaks vastama järgmistele nõuetele.

- Asjakohased menetlused tuleks korraldada ohutus ja usaldusväärses keskkonnas, arvestades makseteenuse pakkuja kontrolli alla mittekuuluvatest seadmetest tekkivaid võimalikke riske.

- Isiklike turvavolituste, maksetarkvara ja kõigi internetimaksetega seotud isikustatud seadmete edastamiseks peaksid kehtima tõhusad ja turvalised menetlused. Makseteenuse pakkuja peaks interneti teel esitatava tarkvara samuti digitaalselt allkirjastama, et klient saaks kontrollida selle autentsust ja veenduda, et seda ei ole rikutud.

[15] Makseteenuse pakkuja vastutuse alla kuuluvad keskkonnad, kus tuleb tagada kliendi ja teenust pakkuva makseteenuse pakkuja nõuetekohane autentimine ning konfidentsiaalse/tundliku teabe kaitse, hõlmavad järgmist: i) makseteenuse pakkuja ruumid; ii) internetipanga või muu turvaline veebikoht, näiteks kui haldusasutus pakub võrreldavaid turvafunktsioone muu hulgas suunises 4 määratletu kohaselt, või iii) pangaautomaatide teenused. (Pangaautomaatide korral nõutakse kliendi tugevat autentimist, tüüpiliselt kiibi ja PIN-koodi või kiibi ja biomeetria abil.)

- [kaardid] Kaarditehingute korral peaks kliendil olema võimalik registreeruda tugeva autentimissüsteemi kasutamiseks olenemata konkreetsest internetiostust. Kui pakutakse veebipoes ostmise ajal aktiveerimise võimalust, tuleks selleks klient suunata ohutusse ja usaldusväärsesse keskkonda.

8.2 [kaardid] Väljastajad peaksid aktiivselt julgustama kaardiomanikke osalema tugeva autentimise süsteemis ja võimaldama kaardiomanikel osalemisest loobuda ainult erandlikel ja vähestel juhtudel, kui seda õigustab konkreetse kaarditehingu risk.

Sisselogimise katsed, seansi aegumine, autentimise kehtivus

9. Makseteenuse pakkujad peaksid piirama sisselogimise või autentimise katsete arvu, määratlema internetimakseteenuste seansi aegumise eeskirjad ja määrama autentimise kehtivuse ajalised piirangud.

9.1 Autentimiseks ühekorraparooli kasutamisel peaksid makseteenuse pakkujad tagama, et paroolide kehtivusaeg piirneb rangelt minimaalse vajaliku ajaga.

9.2 Makseteenuse pakkujad peaksid määrama maksimaalse ebaõnnestunud sisselogimise või autentimise katsete arvu, pärast mida blokeeritakse (ajutiselt või püsivalt) juurdepääs internetimakseteenusele. Makseteenuse pakkujatel peaks olema kehtestatud blokeeritud internetimakseteenuste taasaktiveerimise turvaline menetlus.

9.3 Makseteenuse pakkujad peaksid kehtestama maksimaalse ajavahemiku, pärast mida lõpetatakse automaatselt mitteaktiivsed internetimakseteenuste seansid.

Tehingute seire

10. Enne makseteenuse pakkuja poolset lõplikku volitamist tuleks kasutada tehingute järelevalve mehhanisme, mis on projekteeritud pettuslike maksetehingute ennetamiseks, tuvastamiseks ja blokeerimiseks; kahtlased või suure riskiga tehinguid tuleks eraldi kontrollida ja hinnata. E-volituste väljastamiseks tuleb kasutada samaväärseid turvalisuse järelevalve ja volitamise mehhanisme.

10.1 Makseteenuse pakkujad peaksid pettuste tuvastamise ja ennetamise süsteemide abil tuvastama kahtlased tehingud enne seda, kui makseteenuse pakkuja tehingud või e-volitused lõplikult volitab. Need süsteemid peaksid põhinema näiteks parameetripõhistel eeskirjadel (nt kompromiteeritud või varastatud kaardiandmete mustad nimekirjad) ning jälgima kliendi või kliendi juurdepääsuseadme ebatavalisi käitumismustreid (nt internetiprotokolli (IP) aadressi[16] või IP-vahemiku muutumine internetimakseteenuste seansi ajal, mis mõnikord leitakse IP geograafilise asukoha määramise kontrollidega [17], konkreetse kliendi korral ebatavaliste e-kaupleja

[16] IP-aadress on ainulaadne numberkood, mille alusel tuvastatakse iga internetti ühendatud arvuti.

[17] Geo-IP-kontrolliga kontrollitakse, kas väljastav riik vastab IP-aadressile, kust kasutaja tehingu algatab.

kategooriate või ebatavaliste tehinguandmete alusel jne). Need süsteemid peaksid samuti suutma seansil tuvastada pahavara nakkuse tundemärke (nt skript inimese poolt valideerimise asemel) ja teadaolevaid pettuste stsenaariume. Seirelahenduste ulatus, keerukus ja kohandatavus asjakohaste andmekaitseõigusaktide nõuete täitmisel peaks olema samaulatuslik riskihindamise tulemusega.

10.2 Vastuvõtvatel makseteenuse pakkujatel peaksid olema rakendatud e-kaupleja tegevuse seireks pettuste tuvastamise ja ennetamise süsteemid.

10.3 Makseteenuse pakkujad peaksid kontrollima ja hindama mis tahes tehinguid sobiva ajavahemiku jooksul, et mitte liiga palju viivitada makseteenuse algatamist ja/või teostamist.

10.4 Kui makseteenuse pakkuja otsustab oma riskipoliitika kohaselt blokeerida maksetehingu, mis on tuvastatud võimaliku pettustehinguna, peaks makseteenuse pakkuja säilitama blokeeringut võimalikult lühikese aja jooksul, kuni kõik turvaprobleemid on lahendatud.

Tundlike makseandmete kaitse

11. Tundlikke makseandmeid tuleks kaitsta nende salvestamise, töötlemise ja edastamise ajal.

11.1 Kõiki andmeid, millega tuvastatakse ja autenditakse kliente (nt sisselogimisel, internetimaksete algatamisel ja e-volituste väljastamisel, muutmisel või tühistamisel) ning ka kliendi liidest (makseteenuse pakkuja või e-kaupleja veebikoht), tuleks nõuetekohaselt kaitsta varguse ja volitamata juurdepääsu või muutmise eest.

11.2 Makseteenuse pakkujad peaksid tagama, et tundlike makseandmete interneti kaudu vahetamise ajal kasutatakse teabevahetuse poolte vahel turvalist otspunktkrüptimist[18] kogu asjakohase sideseansi ajal, et kaitsta andmete konfidentsiaalsust ja usaldusväärsust tugevate ja üldtunnustatud krüptimistehnikate abil.

11.3 Vastuvõtmisteenuseid pakkuv makseteenuse pakkuja peaks julgustama oma e-kauplejaid mitte salvestama tundlikke makseandmeid. Kui e-kaupleja käitleb (salvestab, töötleb või edastab) tundlikke makseandmeid, peaksid makseteenuse pakkujad nõudma e-kauplejatelt lepinguga selliste andmete kaitsmiseks vajalike meetmete võtmist. Makseteenuse pakkujad peaksid tegema regulaarseid kontrolle ja kui makseteenuse pakkuja saab teada, et tundlikke makseandmeid käitlev e-kaupleja ei kasuta nõutavaid turvameetmeid, peaks ta võtma meetmeid selle lepingukohustuse jõustamiseks või lepingu lõpetamiseks.

[18] Otspunktkrüptimine tähendab krüptimist lähtepunktis või selle lähedal nii, et vastav dekrüptimine toimub ainult sihtpunktis või selle lähedal. ETSI EN 302 109 V1.1.1. (2003-06).

Klientide teadlikkus ning selgitused ja teave klientidele

Selgitused ja teave klientidele

12. Makseteenuse pakkujad peaksid vajaduse korral kliente internetimakseteenuste turvalise kasutamise osas abistama ja juhendama. Makseteenuse pakkujad peaksid suhtlema oma klientidega nii, et kliendid saaksid veenduda saadud sõnumite autentsuses.

12.1 Makseteenuse pakkujad peaksid tagama vähemalt ühe turvalise kanali[19] pidevaks suhtluseks klientidega internetimakseteenuse nõuetekohase ja turvalise kasutamise teemal. Makseteenuse pakkujad peaksid teatama klientidele sellest kanalist ja selgitama, et makseteenuse pakkujalt mis tahes muul viisil, näiteks e-postiga saadetud sõnum internetimakseteenuse nõuetekohase ja turvalise kasutamise teemal ei ole usaldusväärne. Makseteenuse pakkuja peaks selgitama järgmist:

- menetlus, kuidas kliendid saavad teatada makseteenuse pakkujale (eeldatavatest) pettusmaksetest, kahtlastest juhtumitest või ebatavalistest olukordadest internetimakseteenuste seansi ajal ja/või võimalikest sotsiaalse manipuleerimise[20] katsetest;

- järgmised sammud (st kuidas makseteenuse pakkuja kliendile vastab);

- kuidas makseteenuse pakkuja teatab kliendile (võimalikest) pettustehingutest või nende algatamata jätmisest või hoiatab klienti rünnakute toimumisest (nt andmepüügi e-kirjad).

12.2 Makseteenuse pakkuja peaks teatama klientidele internetimakseteenusega seotud turvamenetluste uuendustest turvalise kanali kaudu. Mis tahes hoiatused oluliste tekkivate riskide kohta (nt sotsiaalse manipuleerimise hoiatused) tuleks samuti esitada turvalise kanali kaudu.

12.3 Makseteenuse pakkuja peaks korraldama klienditoe, millele saab esitada küsimusi ja kaebusi, millelt saab paluda abi ja millele saab teatada ebatavalistest olukordadest või intsidentidest, mis on seotud internetimaksete ja asjakohaste teenustega, ning klientidele tuleks nõuetekohaselt teatada, kuidas sellist tuge saada.

12.4 Makseteenuse pakkujad peaksid algatama klientidele selgituste ja teabe levitamise programmid, mille eesmärk on tagada, et kliendid mõistavad vähemalt järgmiste asjaolude vajadust:

[19] Näiteks konkreetne postkast makseteenuse pakkuja veebikohas või turvalises veebikohas.

[20] Sotsiaalne manipuleerimine tähendab selles kontekstis inimeste manipuleerimise tehnikaid teabe saamiseks (nt e-posti või telefoni teel) või suhtlusvõrgustikest teabe saamiseks pettuse sooritamiseks või arvutile või võrgule volitamata juurdepääsu saamiseks.

- oma paroolide, autentimistõendite, isikuandmete ja muude konfidentsiaalsete andmete kaitse;

- isikliku seadme (nt arvuti) turvalisuse nõuetekohane haldamine turvakomponente (viirustõrje, tulemüürid, turvapaigad) paigaldades ja uuendades;

- interneti kaudu tarkvara alla laadimisega seotud oluliste ohtude ja riskide arvestamine, kui klient ei saa olla mõistlikult kindel, et tarkvara on originaalne ja rikkumata;

- makseteenuse pakkuja tegeliku internetimaksete veebikoha kasutamine.

12.5 Vastuvõtvad makseteenuse pakkujad peaksid nõudma, et e-kauplejad eraldaksid maksetega seotud protsessid selgesti veebipoest, et klientidel oleks lihtsam eristada, millal nad suhtlevad makseteenuse pakkujaga ja mitte makse saajaga (näiteks suunates kliendi mujale ja avades eraldi brauseri akna, et makseprotsessi ei kuvataks samas e-kaupleja aknas).

Teated ja piirangud

13. Makseteenuse pakkujad peaksid kehtestama internetimakseteenuste piirangud ja nad võivad anda oma klientidele võimaluse nende piirangute ulatuses riski veelgi vähendada. Nad võivad samuti pakkuda hoiatuse ja kliendiprofiili haldamise teenuseid.

13.1 Makseteenuse pakkuja peaks enne kliendile internetimakseteenuste osutamist kehtestama teenuste piirangud [21] (näiteks iga üksikmakse maksimumsumma või ajavahemiku kumulatiivne summa) ning nad peaksid sellest teatama klientidele. Makseteenuse pakkujad peaksid võimaldama klientidele internetimaksete funktsiooni sulgemist.

Kliendi juurdepääs makse algatamise ja sooritamise oleku teabele

14. Makseteenuse pakkujad peaksid kinnitama klientidele makse algatamist ja esitama neile sobiva aja jooksul teabe, millega kontrollida maksetehingu nõuetekohast algatamist ja/või sooritamist.

14.1 [krediidikorraldus/e-volitus] Makseteenuse pakkuja peaks tagama klientidele peaaegu reaalajas võimaluse kontrollida tehingute sooritamise olekut ja millal tahes kontojääki[22] ohutus ja usaldusväärses keskkonnas.

14.2 Mis tahes üksikasjalikud elektroonilised aruanded tuleks avaldada ohutus ja usaldusväärses keskkonnas. Kui makseteenuse pakkuja teatab klientidele elektrooniliste aruannete kättesaadavusest (näiteks regulaarselt, kui väljastatakse

[21] Piirangud võivad kehtida kas üldiselt (st kõigile internetimakseid võimaldavatele makseviisidele) või individuaalselt.

[22] Välja arvatud vahendi erandlik kättesaadavuse puudumine tehnilise hoolduse tõttu või oluliste intsidentide tagajärjel.

perioodiline e-aruanne, või erakorraliselt pärast tehingu sooritamist) alternatiivse kanali kaudu, näiteks SMS-i, e-kirja või kirja kaudu, ei tohiks teatesse lisada tundlikke makseandmeid, või nende lisamisel peaksid need olema varjatud.

III jaotis. Lõppsätted ja rakendamine

15. Käesolevaid suuniseid kohaldatakse alates 01.08.2015.

1. lisa. Parimate tavade näited

Lisaks eespool sätestatud nõuetele kirjeldatakse käesolevates suunistes mõningaid parimaid tavasid, mida makseteenuse pakkujaid julgustatakse järgima, aga mille järgimine ei ole kohustuslik. Ülevaatlikkuse huvides on märgitud ka peatükid, millele parimat tava kohaldatakse.

Üldine kontrolli ja turvalisuse keskkond

Üldjuhtimine

PT 1 Turvapoliitika tuleks sätestada eraldi dokumendis.

Riskikontroll ja riskide maandamine

PT 2 Makseteenuse pakkujad võiksid pakkuda turvavahendeid (nt nõuetekohaselt turvatud seadmeid ja/või kohandatud brausereid), et kaitsta kliendi liidest ebaseadusliku kasutamise või rünnakute eest (nt brauserist teabe varastamise eest).

Jälgitavus

PT 3 Vastuvõtmise teenuseid pakkuvad makseteenuse pakkujad võiksid lepinguga nõuda, et makseteavet salvestavad e-kauplejad rakendaksid jälgitavuse tagamiseks asjakohaseid menetlusi.

Internetimaksete konkreetsed kontrolli- ja turvameetmed

Kliendi esialgne tuvastamine, teave

PT 4 Klient võib sõlmida internetimaksetehingute jaoks eraldi teenuslepingu selle asemel, et tingimused lisatakse makseteenuse pakkujaga sõlmitud üldisemasse teenuslepingusse.

PT 5 Makseteenuse pakkujad võivad samuti tagada, et klientidele tagatakse pidevalt või erakorraliselt ning asjakohase meetodi abil (nt infolehed, veebilehed) selged ja üheselt mõistetavad juhised, mis selgitavad nende vastutust teenuse turvalisel kasutamisel.

Tugev klientide autentimise süsteem

PT 6 [kaardid] e-kauplejad peaksid toetama internetikaudsete kaarditehingute korral väljastaja poolt kaardiomaniku tugeva autentimise süsteemi kasutamist.

PT 7 Kliendi mugavuse huvides võivad makseteenuse pakkujad kaaluda kõigi internetimakseteenuste jaoks üheainsa tugeva autentimise süsteemi kasutamist. See võib suurendada lahenduse heakskiitu klientide hulgas ja lihtsustada nõuetekohast kasutamist.

PT 8 Tugeva autentimise süsteemid võivad sisaldada elemente, mis seostavad autentimise konkreetse summa ja makse saajaga. See võib anda klientidele maksete volitamisel suurema kindlustunde. Tugeva autentimise andmete ja tehingu andmete seostamist võimaldav tehnoloogiline lahendus peaks olema rikkumiskindel.

Tundlike makseandmete kaitse

PT 9 On soovitatav, et tundlikke makseandmeid käitlevad e-kauplejad koolitaksid oma pettuste haldamise töötajaid nõuetekohaselt ja ajakohastaksid koolitust korrapäraselt, et tagada sisu vastavus muutuvale turvakeskkonnale.

Selgitused ja teave klientidele

PT 10 On soovitatav, et vastuvõtmise teenuseid pakkuvad makseteenuse pakkujad korraldaksid oma e-kauplejatele pettuste ennetamise teemal õppeprogramme.

Teated ja piirangud

PT 11 Makseteenuse pakkujad võivad pakkuda klientidele kehtivate nõuete raames vahendi, millega kliendid saavad hallata internetimakseteenuste piiranguid ohutus ja turvalises keskkonnas.

PT 12 Makseteenuse pakkujad võivad esitada klientidele nende riskihindamispoliitikate alusel hoiatusi (nt telefoni või SMS-i teel) kahtlaste või suure riskiga maksetehingute kohta.

PT 13 Makseteenuse pakkujad võivad lubada klientidel määrata üldisi ja isiklikke eeskirju, mida kasutatakse nende internetimaksetega ja muude teenustega seotud käitumise parameetritena – näiteks et nad algatavad makseid ainult teatud riikidest ja mujalt algatatud maksed tuleks blokeerida või et nad võivad lisada konkreetseid makse saajaid valgetesse või mustadesse nimekirjadesse.