EBA/GL/2014/12_Rev1

19 ta' Diċembru 2014

Linji Gwida finali

dwar is-sigurtà tal-pagamenti bl-internet

Werrej

Linji Gwida dwar is-sigurtà tal-pagamenti bl-internet

Status ta' dawn il-Linji gwida

Dan id-dokument fih linji gwida maħruġa skont l-Artikolu 16 tar-Regolament (UE) Nru 1093/2010 tal-Parlament Ewropew u tal-Kunsill tal-24 ta' Novembru 2010 li jistabbilixxi Awtorità Superviżorja Ewropea (Awtorità Bankarja Ewropea) u li jemenda d-Deċiżjoni Nru 716/2009/KE u jħassar id-Deċiżjoni tal-Kummissjoni 2009/78/KE ('ir-Regolament tal-EBA'). Skont l-Artikolu 16(3) tar-Regolament tal-EBA, l-awtoritajiet kompetenti u l-istituzzjonijiet finanzjarji għandhom jagħmlu kull sforz biex jikkonformaw mal-linji gwida.

Il-linji gwida jistabbilixxu l-opinjoni tal-EBA dwar il-prattiki superviżorji xierqa fis-Sistema Ewropea tas-Superviżuri Finanzjarji jew dwar kif il-liġi tal-Unjoni għandha tiġi applikata f'qasam partikolari. L-EBA għalhekk tistenna li l-awtoritajiet kompetenti u l-istituzzjonijiet finanzjarji kollha li lejhom huma indirizzati l-linji gwida jikkonformaw mal-linji gwida. L-awtoritajiet kompetenti li għalihom japplikaw il-linji gwida għandhom jikkonformaw billi jinkorporawhom fil-prattiki superviżorji tagħhom kif xieraq (eż. billi jemendaw il-qafas legali tagħhom jew il-proċessi superviżorji tagħhom), inkluż fejn il-linji gwida huma indirizzati primarjament lejn l-istituzzjonijiet.

Rekwiżiti tar-rapportar

Skont l-Artikolu 16(3) tar-Regolament tal-EBA, l-awtoritajiet kompetenti għandhom jinnotifikaw lill-EBA jekk jikkonformawx jew jekk ikunux biħsiebhom jikkonformaw ma' dawn il-linji gwida, jew inkella jagħtu r-raġunijiet għan-nuqqas ta' konformità, sas-5.05.2015. Fin-nuqqas ta' kwalunkwe notifika sa din l-iskadenza, l-awtoritajiet kompetenti jitqiesu mill-EBA li mhumiex konformi. In-notifiki għandhom jintbagħtu billi tiġi sottomessa l-formola pprovduta fit-Taqsima 5 lil compliance@eba.europa.eu bir-referenza 'EBA/GL/2014/12'. In-notifiki għandhom jiġu sottomessi minn persuni b'awtorità xierqa li jirrapportaw il-konformità f'isem l-awtoritajiet kompetenti tagħhom.

In-notifiki se jiġu ppubblikati fuq il-websajt tal-EBA, f'konformità mal-Artikolu 16(3).

Titolu I – Ambitu u definizzjonijiet

Ambitu

1. Dawn il-linji gwida jistabbilixxu sett ta' rekwiżiti minimi fil-qasam tas-sigurtà tal-pagamenti bl-internet. Il-linji gwida jibnu fuq ir-regoli tad-Direttiva 2007/64/KE [1] ("id-Direttiva dwar is-Servizzi ta' Ħlas", PSD) rigward rekwiżiti ta' informazzjoni għal servizzi ta' ħlas u obbligi ta' fornituri ta' servizzi ta' ħlas (PSPs) fir-rigward tal-forniment ta' servizzi ta' ħlas. Barra minn hekk, l-Artikolu 10(4) tad-Direttiva jeħtieġ lill-istituzzjonijiet tal-ħlas ikollhom fis-seħħ arranġamenti ta' governanza robusti u mekkaniżmi interni ta' kontroll adegwati.

2. Il-linji gwida japplikaw għall-forniment ta' servizzi ta' ħlas offruti permezz tal-internet minn PSPs kif definit fl-Artikolu 1 tad-Direttiva.

3. Il-linji gwida jindirizzaw lill-istituzzjonijiet finanzjarji kif definit fl-Artikolu 4(1) tar-Regolament (UE) Nru 1093/2010 u lill-awtoritajiet kompetenti kif definit fl-Artikolu 4(2) tar-Regolament (UE) Nru 1093/2010. L-awtoritajiet kompetenti fit-28 Stat Membru tal-Unjoni Ewropea għandhom jiżguraw l-applikazzjoni ta' dawn il-linji gwida mill-PSPs kif definit fl-Artikolu 1 tal-PSD taħt is-superviżjoni tagħhom.

4. Barra minn hekk, l-awtoritajiet kompetenti jistgħu jiddeċiedu li jeħtieġu lill-PSPs jirrapportaw lill-awtorità kompetenti li jkunu qed jikkonformaw mal-linji gwida.

5. Dawn il-linji gwida ma jaffettwawx il-validità tal-Bank Ċentrali Ewropew "Rakkomandazzjonijiet għas-sigurtà ta' pagamenti bl-internet" (ir-"Rapport"). [2] Ir-Rapport b'mod partikolari jkompli jirrappreżenta d-dokument li l-banek ċentrali fil-funzjoni ta' sorveljanza tagħhom għal sistemi u strumenti ta' ħlas għandhom jivvalutaw il-konformità rigward is-sigurtà tal-pagamenti bl-internet kontra tiegħu.

6. Il-linji gwida jikkostitwixxu aspettattivi minimi. Dawn huma mingħajr preġudizzju għar-responsabbiltà tal-PSPs li jimmonitorjaw u jivvalutaw ir-riskji involuti fl-operazzjonijiet ta' pagament tagħhom, jiżviluppaw il-politiki tas-sigurtà dettaljati tagħhom stess u jimplimentaw miżuri adegwati ta' sigurtà, kontinġenza, ġestjoni ta' inċidenti u kontinwità tan-negozju li jkunu proporzjonali mar-riskji inerenti fis-servizzi ta' ħlas ipprovduti.

7. L-għan tal-linji gwida huwa li jiddefinixxu r-rekwiżiti minimi komuni għas-servizzi ta' pagament bl-internet elenkati hawn taħt, irrispettivament mill-apparat ta' aċċess użat:

[1] Id-Direttiva 2007/64/KE tal-Parlament Ewropew u tal-Kunsill tat-13 ta' Novembru 2007 dwar is-servizzi ta' ħlas fis-suq intern li temenda d-Direttivi 97/7/KE, 2002/65/KE, 2005/60/KE u 2006/48/KE u li tħassar id-Direttiva 97/5/KE, ĠU L 319, 05.12.2007,

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

- [kards] l-eżekuzzjoni tal-ħlasijiet bil-kard fuq l-internet, inklużi ħlasijiet virtwali bil-kard, kif ukoll ir-reġistrazzjoni ta' data ta' ħlas bil-kard għall-użu f'"soluzzjonijiet kartiera";

- [trasferimenti ta' kreditu] l-eżekuzzjoni ta' trasferimenti ta' kreditu (CTs) fuq l-internet;

- [mandat elettroniku] il-ħruġ u l-emenda ta' mandati elettroniċi ta' debitu dirett;

- [flus elettroniċi] trasferimenti ta' flus elettroniċi bejn żewġ kontijiet ta' flus elettroniċi permezz tal-internet.

8. Meta l-linji gwida jindikaw eżitu, l-eżitu jista' jintlaħaq permezz ta' mezzi differenti. Dawn il-linji gwida, minbarra r-rekwiżiti stabbiliti kif ġej, jipprovdu wkoll eżempji tal-aħjar prattiki (fl-Anness 1), li l-PSPs huma mħeġġa, iżda mhux meħtieġa, li jsegwu.

9. Meta l-provvista tas-servizzi u ta' strumenti ta' ħlas tiġi offruta permezz ta' skema ta' pagament (eż. skemi ta' ħlasijiet bil-kard, skemi ta' trasferiment ta' kreditu, skemi ta' debiti diretti, eċċ), l-awtoritajiet kompetenti u l-bank ċentrali rilevanti b'funzjoni ta' sorveljanza fuq l-istrumenti ta' ħlas għandhom jikkollaboraw biex jiżguraw applikazzjoni konsistenti tal-linji gwida mill-atturi responsabbli mill-funzjonament tal-iskema.

10. L-integraturi tal-pagamenti [3] li joffru servizzi ta' bidu ta' ħlasijiet huma kkunsidrati jew bħala akkwirenti ta' servizzi ta' pagamenti bl-internet (u għalhekk bħala PSPs) jew inkella bħala fornituri esterni ta' servizz tekniku tal-skemi rilevanti jew PSPs. Fl-aħħar każ, l-integraturi tal-pagamenti għandhom jkunu meħtieġa permezz ta' kuntratt biex jikkonformaw mal-linji gwida.

11. Eskludi mill-ambitu tal-linji gwida huma:

- servizzi oħra tal-internet ipprovduti minn PSP permezz tas-sit elettroniku ta' ħlas tiegħu (eż. senserija elettronika, kuntratti onlajn);

- ħlasijiet fejn l-istruzzjoni tingħata bil-posta, ordni telefonika, voice mail jew permezz ta' teknoloġija bbażata fuq SMS;

- ħlasijiet bil-mowbajl ħlief ħlasijiet ibbażati fuq brawżer;

- CTs fejn parti terza taċċessa l-kont ta'pagament tal-klijent;

- tranżazzjonijiet ta' ħlas magħmulin minn intrapriża permezz ta' netwerks iddedikati;

[3] L-integraturi tal-ħlas jipprovdu lill-prenditur (jiġifieri l-kummerċjant elettroniku) interfaċċa standardizzat għal servizzi ta' bidu ta' pagament ipprovdut mill-PSPs.

- ħlasijiet bil-kard permezz ta' kards anonimi u mhux rikarikabbli fiżiċi jew virtwali mħallsa minn qabel fejn ma jkun hemm l-ebda relazzjoni kontinwa bejn l-emittent u d-detentur tal-kard;

- ikklerjar u ħlas ta' tranżazzjonijiet ta' ħlas.

Definizzjonijiet

12. Għall-finijiet ta' dawn il-linji gwida, u minbarra d-definizzjonijiet ipprovduti fil-PSD, japplikaw id-definizzjonijiet li ġejjin:

- *Awtentifikazzjoni* tfisser proċedura li tippermetti lill-PSP jivverifika l-identità ta' klijent.

- *Awtentifikazzjoni b'saħħitha tal-konsumaturi*, għall-iskop ta' dawn il-linji gwida, hija proċedura bbażata fuq l-użu ta' tnejn mill-elementi li ġejjin jew iktar – kategorizzati bħala għarfien, sjieda u inerenza: i) xi ħaġa li jkun jaf l-utent biss, pereżempju password statika, kodiċi, numru ta' identifikazzjoni personali; ii) xi ħaġa li l-utent biss jippossjedi, eż token, smart card, telefown ċellulari; iii) xi ħaġa li huwa l-utent, eż. karatteristika bijometrika, bħall-marka tas-swaba'. Barra minn hekk, l-elementi magħżula għandhom ikunu reċiprokament indipendenti, jiġifieri l-ksur ta' wieħed minnhom ma jikkompromettix lill-ieħor/l-oħrajn. Mill-inqas wieħed mill-elementi m'għandux ikun jista' jerġa' jintuża u ma jkunx replikabbli (ħlief għall-inerenza), u ma jkunx kapaċi li jinsteraq bil-moħbi permezz tal-internet. Il-proċedura ta' awtentifikazzjoni b'saħħitha għandha tkun iddisinjata b'tali mod li tipproteġi l-kunfidenzjalità tad-data ta' awtentifikazzjoni.

- *Awtorizzazzjoni* tfisser proċedura li tiċċekkja jekk klijent jew PSP għandux id-dritt li jwettaq ċerta azzjoni, pereżempju id-dritt li jittrasferixxi fondi, jew li jkollu aċċess għal data sensittiva.

- *Kredenzjali* tfisser l-informazzjoni — ġeneralment kunfidenzjali — ipprovduta minn klijent jew PSP għall-finijiet ta' awtentifikazzjoni. Kredenzjali tista' tfisser ukoll il-pussess ta' għodda fiżika li jkun fiha l-informazzjoni (eż. ġeneratur ta' password ta' darba, smart card), jew xi ħaġa li l-utent jimmemorizza jew jirrappreżenta (bħal karatteristiċi bijometriċi).

- *Inċident ewlieni ta' sigurtà ta' ħlas* tfisser inċident li għandu jew li jista' jkollu impatt materjali fuq is-sigurtà, l-integrità jew il-kontinwità tas-sistemi tal-PSP relatati mal-ħlas u/jew is-sigurtà ta' data jew fondi ta' pagament sensittivi. Il-valutazzjoni tal-materjalità għandha tikkunsidra n-numru ta' klijenti potenzjalment affettwati, l-ammont f'riskju u l-impatt fuq PSPs oħra jew infrastrutturi oħra ta' ħlas.

- *Analiżi ta' tranżazzjoni tar-riskju* tfisser evalwazzjoni tar-riskju relatata ma' tranżazzjoni speċifika b'kunsiderazzjoni ta' kriterji bħal, pereżempju, mudelli ta' ħlas tal-klijenti (imġiba), valur tat-tranżazzjoni relatata, tip ta' prodott u profil tal-prenditur.

- *Kards virtwali* tfisser soluzzjoni ta' ħlas ibbażata fuq kard fejn numru ta' kard temporanju, alternattiv b'perjodu ta' validità mnaqqas, użu limitat u limitu ta' nfiq definit minn qabel jiġi ġġenerat li jista' jintuża għal xiri fuq l-internet.

- *Soluzzjonijiet kartiera* tfisser soluzzjonijiet li jippermettu lil klijent jirreġistra data relatata ma' strument tal-ħlas wieħed jew aktar sabiex jagħmlu ħlasijiet ma' diversi kummerċjanti elettroniċi.

Titolu II – Linji gwida dwar is-sigurtà ta' pagamenti bl-internet

Ambjent ġenerali ta' kontroll u sigurtà

Governanza

1. Il-PSPs għandhom jimplimentaw u jirrieżaminaw regolarment politika ta' sigurtà formali għal servizzi ta' pagament bl-internet.

   1.0 Il-politika ta' sigurtà għandha tkun iddokumentata tajjeb, u rieżaminata regolarment (b'mod konformi mal-linja gwida 2.4) u approvata mill-maniġment superjuri. Hija għandha tiddefinixxi l-objettivi ta' sigurtà u l-aptit tar-riskju.

   1.1 Il-politika ta' sigurtà għandha tiddefinixxi r-rwoli u r-responsabbiltajiet, inkluża l-funzjoni tal-ġestjoni tar-riskju b'linja ta' rappurtar diretta għal-livell ta' bord, u l-linji ta' rappurtar għas-servizzi ta' pagamenti bl-internet pprovduti, inkluż il-ġestjoni ta' data ta' pagament sensittiv fir-rigward tal-valutazzjoni, il-kontroll u l-mitigazzjoni tar-riskju.

Valutazzjoni tar-riskju

2. Il-PSPs għandhom iwettqu u jiddokumentaw valutazzjonijiet tar-riskju bir-reqqa fir-rigward tas-sigurtà tal-pagamenti bl-internet u servizzi relatati, kemm qabel l-istabbiliment tas-servizz(i) kif ukoll regolarment wara dan.

   2.1 Il-PSPs, permezz tal-funzjoni tal-ġestjoni tar-riskji tagħhom, għandhom iwettqu u jiddokumentaw valutazzjonijiet tar-riskju dettaljati għal pagamenti bl-internet u servizzi relatati. Il-PSPs għandhom jikkunsidraw ir-riżultati tal-monitoraġġ kontinwu tat-theddid għas-sigurtà relatat mas-servizzi ta' pagament bl-internet li joffru jew li jippjanaw li joffru, filwaqt li jikkunsidraw: i) is-soluzzjonijiet tat-teknoloġija użati minnhom, ii) is-servizzi esternalizzati lil fornituri esterni u, iii) l-ambjent tekniku tal-klijenti. Il-PSPs għandhom jikkunsidraw ir-riskji assoċjati mal-pjattaformi teknoloġiċi magħżulin, l-arkitettura ta' applikazzjoni, it-tekniki u rutini ta' programmazzjoni kemm min-naħa tagħhom [4] kif ukoll min-naħa tal-klijenti tagħhom, [5] kif ukoll ir-riżultati tal-proċess ta' monitoraġġ tal-inċidenti ta' sigurtà (ara l-linja gwida 3).

   2.2 Fuq din il-bażi, il-PSPs għandhom jiddeterminaw jekk u sa liema punt jistgħu jkunu meħtieġa bidliet għall-miżuri ta' sigurtà eżistenti, it-teknoloġiji użati u l-proċeduri jew is-servizzi offruti. Il-PSPs għandhom jikkunsidraw il-ħin meħtieġ biex jimplimentaw il-bidliet (inkluża l-introduzzjoni tal-klijenti) u jieħdu l-miżuri interim xierqa biex jimminimizzaw inċidenti tas-sigurtà u l-frodi, kif ukoll effetti ta' tfixkil potenzjali.

[4] Bħas-suxxettibbiltà tas-sistema għall-inħajġakkjar tas-sessjoni ta' ħlas, l-injezzjoni SQL, skripts bejn is-siti, *buffer overflows*, eċċ.

[5] Bħar-riskji assoċjati mal-użu ta' applikazzjonijiet multimedia, plug-ins tal-brawżer, frejms, links esterni, eċċ.

2.3 Il-valutazzjoni tar-riskji għandha tindirizza l-ħtieġa li d-data ta' pagamenti sensittivi tiġi protetta u żgurata.

2.4 Il-PSPs għandhom iwettqu rieżami tax-xenarji tar-riskji u l-miżuri ta' sigurtà eżistenti wara li inċidenti maġġuri affettwaw is-servizzi tagħhom, qabel bidla kbira fl-infrastruttura jew il-proċeduri u meta theddidiet ġodda jiġu identifikati permezz ta' attivitajiet ta' monitoraġġ tar-riskju. Barra minn hekk, rieżami ġenerali tal-valutazzjoni tar-riskju għandha titwettaq mill-inqas darba fis-sena. Ir-riżultati tal-valutazzjonijiet tar-riskju u r-rieżamijiet għandhom jiġu sottomessi lill-maniġment superjuri għal approvazzjoni.

Monitoraġġ u rappurtar tal-inċidenti

3. Il-PSPs għandhom jiżguraw il-monitoraġġ konsistenti u integrat, it-trattament u s-segwitu ta' inċidenti ta' sigurtà, inklużi lmenti ta' klijenti relatati mas-sigurtà. Il-PSPs għandhom jistabbilixxu proċedura għar-rappurtar ta' tali inċidenti lill-maniġment u, fil-każ ta' inċidenti maġġuri ta' sigurtà ta' ħlas, lill-awtoritajiet kompetenti.

3.1 Il-PSPs għandu jkollhom proċess fis-seħħ biex jimmonitorjaw, jittrattaw u jsegwu inċidenti ta' sigurtà u lmenti ta' klijenti relatati mas-sigurtà u jirrapportaw tali inċidenti lill-maniġment.

3.2 Il-PSPs għandu jkollhom proċedura biex jinnotifikaw immedjatament lill-awtoritajiet kompetenti (jiġifieri l-awtoritajiet superviżorji, u l-awtoritajiet ta' protezzjoni tad-data), meta dawn ikunu jeżistu, fil-każ ta' inċidenti ewlenin tas-sigurtà tal-ħlas rigward is-servizzi ta' ħlas ipprovduti.

3.3 Il-PSPs għandu jkollhom proċedura biex jikkooperaw dwar inċidenti ewlenin tas-sigurtà tal-ħlas, inkluż ksur tad-data, mal-aġenziji rilevanti ta' infurzar tal-liġi.

3.4 L-akkwist tal-PSPs għandu kuntrattwalment jeħtieġ lil kummerċjanti elettroniċi li jaħżnu, jipproċessaw jew jittrażmettu data ta' ħlas sensittiva biex jikkooperaw dwar inċidenti maġġuri tas-sigurtà ta' ħlas, inkluż ksur tad-data, kemm magħhom kif ukoll mal-aġenziji rilevanti ta' infurzar tal-liġi. Jekk PSP isir konxju li kummerċjant elettroniku ma jkunx qed jikkoopera kif meħtieġ skont il-kuntratt, għandu jieħu passi biex jinfurza dan l-obbligu kuntrattwali, jew itemm il-kuntratt.

Kontroll u mitigazzjoni tar-riskju

4. Il-PSPs għandhom jimplimentaw miżuri ta' sigurtà b'mod konformi mal-politiki ta' sigurtà rispettivi tagħhom sabiex jimmitigaw ir-riskji identifikati. Dawn il-miżuri għandhom jinkorporaw saffi multipli ta' difiżi ta' sigurtà, fejn il-falliment ta' linja waħda ta' difiża jinqabad bil-linja li jmiss ta' difiża ("difiża fil-fond").

4.1 Fit-tfassil, l-iżvilupp u ż-żamma tas-servizzi ta' pagament bl-internet, il-PSPs għandhom jagħtu attenzjoni speċjali lis-segregazzjoni adegwata tad-dmirijiet fl-ambjenti tat-teknoloġija informatika (IT) (eż. l-ambjenti ta' żvilupp, ittestjar u produzzjoni) u l-implimentazzjoni xierqa tal-prinċipju "tal-inqas privileġġ" bħala l-bażi għal identità u ġestjoni soda ta' aċċess. [6]

4.2 Il-PSPs għandu jkollhom soluzzjonijiet ta' sigurtà xierqa fis-seħħ sabiex jipproteġu netwerks, siti elettroniċi, servers u links ta' komunikazzjoni kontra abbuż jew attakki. Il-PSPs għandhom ineħħu l-funzjonijiet superfluwi kollha tas-servers sabiex jipproteġuhom (isaħħuhom) u jeliminaw jew inaqqsu l-vulnerabbiltajiet tal-applikazzjonijiet f'riskju. L-aċċess mill-applikazzjonijiet varji għad-data u r-riżorsi meħtieġa għandu jinżamm bħala minimu strett skont il-prinċipju "tal-inqas privileġġ". Sabiex jirrestrinġu l-użu ta' siti elettroniċi "foloz" (li jimitaw siti ta' PSPs leġittimi), is-siti elettroniċi transazzjonali li joffru servizzi ta' pagament bl-internet għandhom jiġu identifikati permezz ta' ċertifikati ta' validazzjoni estiżi mfassla f'isem il-PSP jew permezz ta' metodi oħrajn ta' awtentifikazzjoni simili.

4.3 Il-PSPs għandu jkollhom proċessi xierqa fis-seħħ sabiex jimmonitorjaw, jintraċċaw u jirrestrinġu l-aċċess għal: i) data ta' ħlas sensittiva, u ii) riżorsi kritiċi loġiċi u fiżiċi, bħal netwerks, sistemi, databases, moduli ta' sigurtà, eċċ. Il-PSPs għandhom joħolqu, jaħżnu u janalizzaw logs u rekords tal-awditjar xierqa.

4.4 Fit-tfassil, [7] l-iżvilupp u ż-żamma tas-servizzi ta' pagament bl-internet, il-PSPs għandhom jiżguraw li l-minimizzazzjoni tad-data [8] tkun komponent essenzjali tal-funzjonalità ewlenija: il-ġbir, ir-rotot, l-ipproċessar, il-ħżin u/jew l-arkivjar, u l-viżwalizzazzjoni ta' data ta' ħlas sensittiva għandhom jinżammu fil-livell minimu assolut.

4.5 Il-miżuri ta' sigurtà għas-servizzi ta' pagament bl-internet għandhom jiġu ttestjati taħt is-superviżjoni tal-funzjoni tal-ġestjoni tar-riskju biex tiġi żgurata r-robustezza u l-effikaċja tagħhom. Il-bidliet kollha għandhom ikunu soġġetti għal proċess formali ta' ġestjoni ta' bidla li jiżgura li l-bidliet ikunu ppjanati, ittestjati, dokumentati u awtorizzati kif xieraq. Fuq il-bażi tal-bidliet magħmula u t-theddid tas-sigurtà osservati, it-testijiet għandhom jiġu ripetuti regolarment u għandhom jinkludu xenarji ta' attakki potenzjali rilevanti u magħrufin.

[6] 'Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.' ["Kull programm u kull utent privileġġjat tas-sistema għandu jopera permezz tal-użu tal-inqas ammont ta' privileġġ possibbli neċessarju biex isir ix-xogħol."] Ara Saltzer, J.H. (1974), '*Protection and the Control of Information Sharing in Multics*', Komunikazzjonijiet tal-ACM, Vol. 17, Nru 7, p. 388.

[7] Kunsiderazzjoni tal-privatezza fit-tfassil (*privacy by design*).

[8] Minimizzazzjoni tad-data tirreferi għall-politika tal-ġbir tal-inqas ammont ta' informazzjoni personali meħtieġ biex titwettaq funzjoni partikolari.

4.6 Il-miżuri ta' sigurtà tal-PSP għal servizzi ta' pagament bl-internet għandhom jiġu awditjati perjodikament biex tiġi żgurata r-robustezza u l-effikaċja tagħhom. L-implimentazzjoni u l-funzjonament tas-servizzi ta' pagament bl-internet għandhom jiġu awditjati wkoll. Il-frekwenza u l-iffukar ta' tali awditjar għandhom jieħdu in kunsiderazzjoni, u jkunu proporzjonati għar, riskji tas-sigurtà involuti. Esperti (interni jew esterni) fdati u indipendenti għandhom iwettqu l-awditjar. Dawn m'għandhomx ikunu involuti bi kwalunkwe mod fl-iżvilupp, l-implimentazzjoni jew il-ġestjoni operattiva tas-servizzi ta' pagament bl-internet ipprovduti.

4.7 Kull meta l-PSPs jesternalizzaw funzjonijiet relatati mas-sigurtà tas-servizzi ta' pagament bl-internet, il-kuntratt għandu jinkludi dispożizzjonijiet li jeħtieġu konformità mal-prinċipji u l-linji gwida stabbiliti f'dawn il-linji gwida.

4.8 Il-PSPs li joffru servizzi ta' akkwist għandhom kuntrattwalment jeħtieġu lill-kummerċjanti elettroniċi li jittrattaw (jiġifieri jaħżnu, jipproċessaw jew jittrażmettu) data ta' ħlas sensittiva biex jimplimentaw miżuri ta' sigurtà fl-infrastruttura tal-IT tagħhom, b'mod konformi mal-linji gwida 4.1 sa 4.7, sabiex jiġi evitat is-serq ta' dik id-data ta' ħlas sensittiva permezz tas-sistemi tagħhom. Jekk PSP isir konxju li kummerċjant elettroniku ma jkollux il-miżuri meħtieġa ta' sigurtà fis-seħħ, għandu jieħu miżuri biex jinforza dan l-obbligu kuntrattwali, jew itemm il-kuntratt.

Traċċabbiltà

5. Il-PSPs għandu jkollhom proċessi fis-seħħ li jiżguraw li t-tranżazzjonijiet kollha, kif ukoll il-fluss tal-proċess ta' mandat elettroniku, jiġu traċċati kif xieraq.

5.1 Il-PSPs għandhom jiżguraw li s-servizz tagħhom jinkorpora mekkaniżmi ta' sigurtà għall-illoggjar dettaljat ta' data ta' tranżazzjoni u mandat elettroniku, inkluż in-numru sekwenzjali ta' tranżazzjoni, kronogrammi għal data tat-tranżazzjoni, il-bidliet ta' parameterizzazzjoni kif ukoll aċċess għal data ta' tranżazzjoni u mandat elettroniku.

5.2 Il-PSPs għandhom jimplimentaw log fajls li jippermettu li kwalunkwe żieda, bidla jew tħassir ta' data ta' tranżazzjoni u mandat elettroniku jiġu traċċati.

5.3 Il-PSPs għandhom jinvestigaw u janalizzaw id-data tat-tranżazzjoni u tal-mandat elettroniku u għandhom jiżguraw li jkollhom l-għodod biex jevalwaw il-log fajls. L-applikazzjonijiet rispettivi għandhom ikunu disponibbli għall-persunal awtorizzat biss.

Miżuri speċifiċi ta' kontroll u sigurtà għall-pagamenti bl-internet

Identifikazzjoni, informazzjoni inizjali tal-klijent

6. Il-klijenti għandhom ikunu identifikati kif jixraq b'mod konformi mal-leġiżlazzjoni [9] Ewropea kontra l-ħasil tal-flus u għandhom jikkonfermaw ir-rieda tagħhom li jagħmlu pagamenti bl-internet permezz tas-servizzi qabel jingħataw aċċess għal tali servizzi. Il-PSPs għandhom jipprovdu informazzjoni adegwata "minn qabel", "regolari" jew, fejn applikabbli, "ad hoc" lill-klijent dwar ir-rekwiżiti meħtieġa (pereżempju tagħmir, proċeduri) għat-twettiq ta' tranżazzjonijiet siguri ta' pagamenti bl-internet u r-riskji inerenti.

6.1 Il-PSPs għandhom jiżguraw li l-klijent ikun għamel il-proċeduri ta' diliġenza dovuta mal-klijenti, u pprovda dokumenti ta' identità xierqa [10] u informazzjoni relatata qabel ma jingħata aċċess għas-servizzi ta' pagament bl-internet. [11]

6.2 Il-PSPs għandhom jiżguraw li l-informazzjoni minn qabel [12] ipprovduta lill-klijent tinkludi dettalji speċifiċi relatati mas-servizzi ta' pagament bl-internet. Dawn għandhom jinkludu, kif xieraq:

- informazzjoni ċara dwar kwalunkwe rekwiżit f'termini ta' tagħmir tal-klijent, softwer jew għodda oħra neċessarji (eż. softwer antivirus, firewalls);
- linji gwida għall-użu xieraq u sigur ta' kredenzjali ta' sigurtà personalizzati;
- deskrizzjoni pass, pass tal-proċedura għall-klijent biex jissottometti u jawtorizza tranżazzjoni ta' ħlas u/jew jikseb informazzjoni, inklużi l-konsegwenzi ta' kull azzjoni;
- linji gwida għall-użu xieraq u sigur tal-ħardwer u s-softwer kollha pprovduti lill-klijent;
- il-proċeduri li għandhom jiġu segwiti fil-każ ta' telf jew serq tal-kredenzjali ta' sigurtà personalizzati jew il-ħardwer jew softwer tal-klijent għall-illoggjar jew it-twettiq ta' tranżazzjonijiet;

[9] Pereżempju, id-Direttiva 2005/60/KE tal-Parlament Ewropew u tal-Kunsill tas-26 ta' Ottubru 2005 dwar il-prevenzjoni tal-użu tas-sistema finanzjarja għall-iskop tal-ħasil tal-flus u l-finanzjament tat-terroriżmu. ĠU L 309, 25.11.2005, pp. 15-36. Ara wkoll id-Direttiva tal-Kummissjoni 2006/70/KE tal-1 ta' Awwissu 2006 li tistabbilixxi miżuri implimentattivi għad-Direttiva 2005/60/KE tal-Parlament Ewropew u tal-Kunsill dwar id-definizzjoni ta' "persuni esposti politikament" u l-kriterji tekniċi għal proċeduri ssimplifikati tad-diliġenza dovuta mal-klijent u għal eżenzjoni għal raġunijiet ta' attività finanzjarja mwettqa fuq bażi okkażjonali jew limitata ħafna. ĠU L 214, 4.8.2006, p. 29-34.

[10] Pereżempju, passaport, karta tal-identità nazzjonali jew firma elettronika avvanzata.

[11] Il-proċess ta' identifikazzjoni tal-klijent huwa mingħajr preġudizzju għal kwalunkwe eżenzjonijiet ipprovduti fil-leġiżlazzjoni eżistenti kontra l-ħasil tal-flus. Il-PSPs m'għandhomx għalfejn iwettqu proċess separat ta' identifikazzjoni tal-klijent għas-servizzi ta' pagament bl-internet, bil-kundizzjoni li tali identifikazzjoni tal-klijent tkun diġà twettqet, eż. għal servizzi relatati mal-ħlas eżistenti oħra jew għall-ftuħ ta' kont.

[12] Din l-informazzjoni tissupplimenta l-Artikolu 42 tal-PSD li jispeċifika l-informazzjoni li l-PSP għandu jipprovdi lill-utent tas-servizz ta' ħlas qabel jidħol f'kuntratt għall-forniment ta' servizzi ta' ħlas.

- il-proċeduri li għandhom jiġu segwiti jekk ikun skopert jew suspettat abbuż;

- deskrizzjoni tar-responsabbiltajiet u l-obbligi tal-PSP u l-klijent rispettivament rigward l-użu tas-servizz ta' pagament bl-internet.

6.3 Il-PSPs għandhom jiżguraw li l-kuntratt qafas mal-klijent jispeċifika li l-PSP jista' jimblokka tranżazzjoni speċifika jew l-istrument ta' ħlas [13] fuq il-bażi ta' tħassib dwar is-sigurtà. Dan għandu jistabbilixxi l-metodu u t-termini tan-notifika tal-klijenti u kif il-klijent jista' jikkuntattja lill-PSP biex ikollu t-tranżazzjoni jew servizz ta' pagament bl-internet "żblukkat", b'mod konformi mal-PSD.

Awtentifikazzjoni b'saħħitha tal-konsumaturi

7. Il-bidu tal-pagamenti bl-internet, kif ukoll l-aċċess għal data ta' ħlas sensittiva, għandhom ikunu protetti minn awtentifikazzjoni b'saħħitha tal-konsumaturi. Il-PSPs għandu jkollhom proċedura ta' awtentifikazzjoni b'saħħitha tal-konsumaturi b'mod konformi mad-definizzjoni pprovduta f'dawn il-linji gwida.

7.1 [CT/mandat elettroniku/flus elettroniċi] Il-PSPs għandhom iwettqu awtentifikazzjoni b'saħħitha tal-konsumaturi għall-awtorizzazzjoni tal-klijent ta' tranżazzjonijiet ta' pagamenti bl-internet (inklużi CTs ragruppati) u l-ħruġ jew l-emenda ta' mandati elettroniċi ta' debitu dirett. Madankollu, il-PSPs jistgħu jikkunsidraw li jadottaw miżuri alternattivi ta' awtentifikazzjoni tal-konsumaturi għal:

- pagamenti 'il barra lil benefiċjarji fdati inklużi fil-listi bojod stabbiliti preċedentament għal dak il-klijent;

- tranżazzjonijiet bejn żewġ kontijiet tal-istess konsumatur miżmuma fl-istess PSP;

- trasferimenti fi ħdan l-istess PSP iġġustifikati minn analiżi tar-riskju ta' tranżazzjoni;

- ħlasijiet ta' valur baxx, kif imsemmi fil-PSD. [14]

7.2 Il-kisba ta' aċċess jew l-emenda ta' data ta' ħlas sensittiva (inkluż il-ħolqien u l-emendar ta' listi bojod) jeħtieġu awtentifikazzjoni b'saħħitha tal-konsumaturi. Meta PSP joffri servizzi purament konsultattivi, mingħajr ebda informazzjoni sensittiva dwar il-konsumaturi jew il-ħlas, bħal data dwar il-ħlas bil-kard, li jistgħu faċilment jintużaw ħażin biex isir frodi, il-PSP jista' jadatta r-rekwiżiti ta' awtentifikazzjoni tiegħu fuq il-bażi tal-valutazzjoni tar-riskju tiegħu.

[13] Ara l-Artikolu 55 tal-PSD dwar il-limiti tal-użu tal-istrument ta' ħlas.

[14] Ara d-definizzjoni ta' strumenti ta' ħlas ta' valur baxx fl- Artikoli 34(1) u 53(1) tal-PSD.

7.3 [kards] Għal tranżazzjonijiet bil-kards, il-PSPs kollha li joħorġu kards għandhom jappoġġjaw l-awtentifikazzjoni b'saħħitha tad-detentur tal-kards. Il-kards kollha maħruġa għandhom ikunu teknikament lesti (reġistrati) biex jintużaw b'awtentifikazzjoni b'saħħitha.

7.4 [kards] Il-PSPs li joffru servizzi ta' akkwist għandhom jappoġġjaw it-teknoloġiji li jippermettu lill-emittent iwettaq awtentifikazzjoni b'saħħitha tad-detentur tal-kard għall-iskemi ta' ħlas bil-kards li jipparteċipa fihom l-akkwirent.

7.5 [kards] Il-PSPs li joffru servizzi ta' akkwist għandhom jeħtieġu lill-kummerċjant elettroniku tagħhom jappoġġja soluzzjonijiet li jippermettu lill-emittent iwettaq awtentifikazzjoni b'saħħitha tad-detentur tal-kard għal tranżazzjonijiet bil-kards permezz tal-internet. L-użu ta' miżuri alternattivi ta' awtentifikazzjoni jista' jitqies għal kategoriji identifikati minn qabel ta' tranżazzjonijiet ta' riskju baxx, eż. fuq il-bażi ta' analiżi tar-riskju ta' tranżazzjoni, jew li jinvolvi pagamenti ta' valur baxx, kif imsemmi fil-PSD.

7.6 [kards] Għall-iskemi ta' ħlas bil-kard aċċettati mis-servizz, il-fornituri tas-soluzzjonijiet kartiera għandhom jeħtieġu awtentifikazzjoni b'saħħitha mill-emittent meta d-detentur leġittimu jirreġistra d-data tal-kard għall-ewwel darba.

7.7 Il-fornituri tas-soluzzjonijiet kartiera għandhom jappoġġjaw l-awtentifikazzjoni b'saħħitha tal-konsumaturi meta l-konsumaturi jilloggjaw fis-servizzi tal-ħlas kartiera jew iwettqu tranżazzjonijiet bil-kard permezz tal-internet. L-użu ta' miżuri alternattivi ta' awtentifikazzjoni jista' jiġi kkunsidrat għal kategoriji identifikati minn qabel ta' tranżazzjonijiet b'riskju baxx, eż. ibbażati fuq analiżi tar-riskju ta' tranżazzjoni, jew li jinvolvu ħlasijiet ta' valur baxx, kif imsemmi fil-PSD.

7.8 [kards] Għal kards virtwali, ir-reġistrazzjoni inizjali għandha ssir f'ambjent sigur u fdat. [15] L-awtentifikazzjoni b'saħħitha tal-konsumaturi għandha tkun meħtieġa għall-proċess virtwali ta' ġenerazzjoni tad-data tal-kard jekk il-kard tinħareġ fl-ambjent tal-internet.

7.9 Il-PSPs għandhom jiżguraw l-awtentifikazzjoni bilaterali xierqa meta jikkomunikaw mal-kummerċjanti elettroniċi għall-iskop li jagħtu bidu lil pagamenti bl-internet u jaċċessaw data ta' ħlas sensittiva.

[15] Ambjenti taħt ir-responsabbiltà tal-PSP fejn l-awtentikazzjoni adegwata tal-klijent u tal-PSP li joffri s-servizz u l-protezzjoni ta' informazzjoni kunfidenzjali/sensittiva tkun assigurata jinkludu: i) il-bini tal-PSP; ii) is-servizzi bankarji bl-internet jew sit elettroniku ieħor sigur, eż fejn il-GA joffri karatteristiċi tas-sigurtà paragunabbli inter alia oħra kif definit fil-Linja Gwida 4; jew iii) servizzi tal-magna teller awtomatika (ATM). (Fil-każ ta' ATMs, l-awtentikazzjoni b'saħħitha tal-konsumatur hija meħtieġa. Din l-awtentikazzjoni hija tipikament pprovduta minn ċippa u PIN, jew ċippa u biometrija).

Reġistrazzjoni u provvista ta' għodod ta' awtentifikazzjoni u/jew softwer mogħtija lill-konsumatur

8. Il-PSPs għandhom jiżguraw li r-reġistrazzjoni tal-klijent u l-provvista inizjali tal-għodod ta' awtentifikazzjoni meħtieġa biex jintuża s-servizz ta' pagament bl-internet u/jew il-kunsinna ta' softwer relatat mal-pagamenti lill-klijenti jiġu mwettqa b'mod sigur.

    8.1 Ir-reġistrazzjoni u l-provvista ta' għodod ta' awtentifikazzjoni u/jew softwer relatat mal-pagament mogħtija lill-klijent għandhom jissodisfaw ir-rekwiżiti li ġejjin.

        - Il-proċeduri relatati għandhom jitwettqu f'ambjent sigur u fdat filwaqt li jitqiesu r-riskji possibbli li jirriżultaw minn apparati li mhumiex taħt il-kontroll tal-PSP.

        - Proċeduri effettivi u siguri għandhom ikunu fis-seħħ għall-kunsinna ta' kredenzjali tas-sigurtà personalizzati, softwer relatat mal-pagament u l-apparati personalizzati kollha relatati mal-pagament bl-internet. Softwer mogħti permezz tal-internet għandu jiġi wkoll iffirmat diġitalment mill-PSP biex jippermetti lill-klijent jivverifika l-awtenticità tiegħu u li dan ma jkunx ġie mbagħbas.

        - [kards] Għal tranżazzjonijiet bil-kard, il-klijent għandu jkollu l-għażla li jirreġistra għall-awtentifikazzjoni b'saħħitha indipendentement minn xirja speċifika bl-internet. Meta tkun offruta attivazzjoni matul xiri online, din tista' ssir billi l-konsumatur jiġi dirett lura lejn ambjent sigur u fdat.

    8.2 [kards] L-emittenti għandhom jinkoraġġixxu b'mod attiv ir-reġistrazzjoni tad-detentur tal-kards għal awtentifikazzjoni b'saħħitha u jippermettu lid-detenturi tal-kards tagħhom jaqbżu r-reġistrazzjoni biss f'numru eċċezzjonali u limitat ta' każijiet fejn dan ikun ġustifikat mir-riskju relatat mat-tranżazzjoni speċifika tal-kard.

Tentattivi ta' lloggjar, skadenza tas-sessjoni, validità ta' awtentifikazzjoni

9. Il-PSPs għandhom jillimitaw in-numru ta' tentattivi ta' lloggjar jew tentattivi ta' awtentifikazzjoni, jiddefinixxu regoli għal 'skadenza' ('time-out') tas-sessjoni ta' servizzi ta' pagament bl-internet u jistabbilixxu limiti ta' żmien għall-validità ta' awtentifikazzjoni.

    9.1 Meta tintuża password ta' darba (OTP) għal skopijiet ta' awtentifikazzjoni, il-PSPs għandhom jiżguraw li l-perjodu ta' validità ta' tali passwords ikun limitat għall-minimu strett meħtieġ.

    9.2 Il-PSPs għandhom jistabbilixxu in-numru massimu ta' tentattivi falluti ta' lloggjar u ta' awtentifikazzjoni u wara dan l-aċċess għas-servizz ta' pagament bl-internet ikun (temporanjament jew permanentement) imblukkat. Dawn għandu jkollhom proċedura sigura fis-seħħ biex jerġgħu jiġu attivati s-servizzi ta' ħlas bl-internet imblukkati.

    9.3 Il-PSPs għandhom jistabbilixxu l-perjodu massimu li wara li jgħaddi, sessjonijiet inattivi ta' servizzi ta' pagament bl-internet jintemmu awtomatikament.

Monitoraġġ tat-tranżazzjonijiet

10. Il-mekkaniżmi ta' monitoraġġ tat-tranżazzjonijiet imfassla biex jipprevjenu, jidentifikaw u jimblukkaw tranżazzjonijiet ta' ħlas frodulenti għandhom jiġu operati qabel l-awtorizzazzjoni finali tal-PSP; tranżazzjonijiet suspettużi jew b'riskju għoli għandhom ikunu soġġetti għal skrinjar speċifiku u proċedura ta' evalwazzjoni. Mekkaniżmi ta' monitoraġġ tas-sigurtà ekwivalenti u ta' awtorizzazzjoni għandhom ikunu fis-seħħ ukoll għall-ħruġ tal-mandati elettroniċi.

10.1 Il-PSPs għandhom jużaw sistemi ta' sejbien u ta' prevenzjoni ta' frodi biex jidentifikaw tranżazzjonijiet suspettużi qabel il-PSP finalment jawtorizza tranżazzjonijiet jew mandati elettroniċi. Sistemi bħal dawn għandhom ikunu bbażati, pereżempju, fuq regoli parametrizzati (bħal listi suwed ta' data tal-kards kompromessi jew misruqa), u jimmonitorjaw mudelli ta' mġiba anormali tal-klijent jew apparat ta' aċċess tal-klijent (bħal bidla ta' indirizz ta' Protokoll ta' Internet (IP) [16] jew firxa tal-IP matul is-sessjoni tas-servizzi ta' pagament bl-internet, xi kultant identifikati permezz ta' kontrolli tal-IP ta' lokazzjoni ġeografika, [17] kategoriji atipiċi ta' kummerċjanti elettroniċi għal klijent speċifiku jew data ta' tranżazzjoni anomali, eċċ). Dawn is-sistemi għandhom ikunu kapaċi wkoll isibu sinjali ta' infezzjoni ta' malware fis-sessjoni (eż. permezz ta' skript versus validazzjoni umana) u xenarji ta' frodi magħrufin. Il-firxa, il-kumplessità u l-adattabbiltà tas-soluzzjonijiet ta' monitoraġġ, filwaqt li jkunu konformi mal-leġiżlazzjoni rilevanti tal-protezzjoni tad-data, għandhom ikunu proporzjonati mal-eżitu tal-valutazzjoni tar-riskju.

10.2 Il-PSPs ta' akkwist għandu jkollhom sistemi ta' skoperta u ta' prevenzjoni tal-frodi fis-seħħ sabiex jimmonitorjaw l-attivitajiet ta' kummerċjanti elettroniċi.

10.3 Il-PSPs għandhom iwettqu kwalunkwe skrinjar ta' tranżazzjonijiet u proċeduri ta' evalwazzjoni f'perjodu ta' żmien xieraq, sabiex ma jkunx hemm dewmien bla bżonn tal-bidu u/jew tal-eżekuzzjoni tas-servizz ta' ħlas ikkonċernat.

10.4 Meta l-PSP, skont il-politika tar-riskju tiegħu, jiddeċiedi li jimblokka tranżazzjoni ta' ħlas li tkun ġiet identifikata bħala potenzjalment frodulenti, il-PSP għandu jżomm l-imblokk għall-iqsar żmien possibbli sakemm il-kwistjonijiet ta' sigurtà jkunu ġew solvuti.

Protezzjoni ta' data ta' ħlas sensittiva

11. Id-data ta' ħlas sensittiva għandha tiġi protetta meta tiġi maħżuna, ipproċessata jew trażmessa.

[16] Indirizz tal-IP huwa kodiċi numeriku uniku li jidentifika kull kompjuter imqabbad mal-internet.

[17] Verifika ta' "Geo-IP" tivverifika jekk il-pajjiż emittenti jikkorrispondix mal-indirizz tal-IP minn fejn l-utent qed jibda t-tranżazzjoni.

11.1 Id-data kollha użata biex tidentifika u tawtentifika l-klijenti (eż. fl-illoggjar, fil-bidu ta' pagamenti bl-internet, u fil-ħruġ, l-emenda jew il-kanċellazzjoni ta' mandati elettroniċi), kif ukoll l-interface tal-klijent (PSP jew sit elettroniku ta' kummerċjanti elettroniċi), għandha tkun żgurata b'mod adegwat kontra s-serq u l-aċċess jew emenda mhux awtorizzati.

11.2 Il-PSPs għandhom jiżguraw li meta jiskambjaw data ta' ħlas sensittiva permezz tal-internet, kriptaġġ ta' sigurtà "end-to-end" [18] jiġi applikat bejn il-partijiet li jikkomunikaw matul is-sessjoni ta' komunikazzjoni rispettiva, sabiex jissalvagwardjaw il-kunfidenzjalità u l-integrità tad-data, bl-użu ta' tekniki ta' kriptaġġ b'saħħithom u rikonoxxuti b'mod wiesa'.

11.3 Il-PSPs li joffru servizzi ta' akkwist għandhom jinkoraġġixxu lill-kummerċjanti elettroniċi biex ma jaħżnu ebda data ta' ħlas sensittiva. Fil-każ li l-kummerċjanti elettroniċi jittrattaw, jiġifieri jaħżnu, jipproċessaw jew jittrażmettu data ta' ħlas sensittiva, tali PSPs għandhom jeħtieġu kuntrattwalment lill-kummerċjanti elettroniċi jkollhom il-miżuri neċessarji fis-seħħ biex jipproteġu din id-data. Il-PSPs għandhom iwettqu kontrolli regolari u jekk PSP isir konxju li kummerċjant elettroniku li jittratta data ta' ħlas sensittiva ma jkollux il-miżuri ta' sigurtà meħtieġa fis-seħħ, għandu jieħu passi biex jinforza dan l-obbligu kuntrattwali, jew itemm il-kuntratt.

Sensibilizzazzjoni, edukazzjoni u komunikazzjoni tal-konsumaturi

Edukazzjoni u komunikazzjoni tal-konsumaturi

12. Il-PSPs għandhom jipprovdu assistenza u gwida lill-klijenti, fejn meħtieġ, fir-rigward tal-użu sigur tas-servizzi ta' pagament bl-internet. Il-PSPs għandhom jikkomunikaw mal-klijenti tagħhom b'tali mod biex jassigurawhom dwar l-awtenticità tal-messaġġi riċevuti.

12.1 Il-PSPs għandhom jipprovdu mill-inqas kanal wieħed sigur [19] għall-komunikazzjoni kontinwa mal-klijenti rigward l-użu korrett u sigur tas-servizz ta' pagament bl-internet. Il-PSPs għandhom jinfurmaw lill-klijenti dwar dan il-kanal u jispjegaw li kwalunkwe messaġġ f'isem il-PSP permezz ta' kwalunkwe mezz ieħor, bħall-eimail, li jikkonċerna l-użu korrett u sigur tas-servizz ta' pagament bl-internet, mhuwiex affidabbli. Il-PSP għandu jispjega:

[18] Kriptaġġ "end-to-end" tirreferi għal kriptaġġ ġewwa jew fis-sistema "end" tas-sors, fejn id-deċifrar korrispondenti jseħħ biss fi ħdan jew fis-sistema "end" ta' destinazzjoni. ETSI EN 302 109 V1.1.1. (2003-06)).

[19] Bħal mailbox iddedikata fuq is-sit elettroniku tal-PSP jew sit elettroniku sigur.

- il-proċedura għall-klijenti biex jirrappurtaw lill-PSP ħlasijiet frodulenti (suspettati), inċidenti suspettużi jew anomaliji matul is-sessjoni tas-servizzi ta' pagament bl-internet u/jew tentattivi ta' inġinerija [20] soċjali possibbli;

- il-passi li jmiss, jiġifieri kif il-PSP se jirrispondi lill-klijent;

- kif il-PSP se jinnotifika lill-klijent dwar tranżazzjonijiet frodulenti (potenzjali) jew in-nuqqas ta' bidu tagħhom, jew iwissi lill-klijent dwar l-okkorrenza ta' attakki (eż. e-mails ta' phishing).

12.2 Permezz tal-kanal sigur, il-PSPs għandhom iżommu lill-klijenti infurmati dwar aġġornamenti fil-proċeduri tas-sigurtà li jirrigwardaw is-servizzi ta' pagament bl-internet. Kwalunkwe allert dwar riskji sinifikanti emerġenti (eż. twissijiet dwar l-inġinerija soċjali) għandhom jiġu pprovduti wkoll permezz tal-kanal sigur.

12.3 L-assistenza tal-konsumatur għandha ssir disponibbli mill-PSPs għall-mistoqsijiet, l-ilmenti, it-talbiet kollha għal appoġġ u notifiki ta' anomaliji jew inċidenti rigward pagamenti bl-internet u servizzi relatati, u l-klijenti għandhom jiġu infurmati kif xieraq dwar kif assistenza bħal din tista' tinkiseb.

12.4 Il-PSPs għandhom jibdew programmi ta' edukazzjoni u sensibilizzazzjoni tal-klijenti maħsuba biex jiżguraw li l-klijenti jifhmu, bħala minimu, il-ħtieġa:

- li jipproteġu l-passwords, tokens ta' sigurtà, dettalji personali u data kunfidenzjali oħra tagħhom;

- li jiġġestixxu b'mod xieraq is-sigurtà tal-apparat personali (eż. kompjuter), permezz tal-installazzjoni u l-aġġornament ta' komponenti ta' sigurtà (antivirus, firewalls, irqajja' ta' sigurtà);

- li jikkunsidraw it-theddid u r-riskji sinifikanti relatati mat-tniżżil ta' softwer permezz tal-internet jekk il-klijent ma jkunx jista' jkun ċert b'mod raġonevoli li s-softwer huwa ġenwin u li ma ġiex imbagħbas;

- li jużaw is-sit elettroniku ġenwin tal-pagament bl-internet tal-PSP.

12.5 Il-PSPs ta' akkwist għandu jeħtieġ li l-kummerċjanti elettroniċi jisseparaw b'mod ċar proċessi relatati ma' pagamenti mill-ħanut online sabiex jagħmluha iktar faċli għall-klijenti biex jidentifikaw meta jkunu qed jikkomunikaw mal-PSP u mhux il-prenditur (pereżempju billi jerġgħu jidderieġu lill-klijent u l-ftuħ ta' window separata sabiex il-proċess ta' ħlas ma jkunx jidher fi fejm tal-kummerċjant elettroniku).

[20] Inġinerija soċjali f'dan il-kuntest tfisser tekniki ta' manipulazzjoni tan-nies biex tinkiseb informazzjoni (eż permezz ta' e-mails jew telefonati), jew irkupru ta' informazzjoni minn netwerks soċjali, għall-finijiet ta' frodi jew il-kisba ta' aċċess mhux awtorizzat għal kompjuter jew netwerk.

Notifiki, issettjar ta' limiti

13. Il-PSPs għandhom jistabbilixxu limiti għal servizzi ta' pagament bl-internet u jistgħu jipprovdu lill-klijenti tagħhom għażliet għal aktar limitazzjoni tar-riskju f'dawn il-limiti. Huma jistgħu jipprovdu wkoll servizzi ta' ġestjoni ta' twissija u tal-profil tal-klijent.

    13.1 Qabel ma jipprovdu servizzi ta' pagament bl-internet lil klijent, il-PSPs għandhom jistabbilixxu limiti [21] li japplikaw għal dawk is-servizzi, (eż. ammont massimu għal kull ħlas individwali jew ammont kumulattiv tul ċertu perjodu ta' żmien) u għandhom jinfurmaw lill-klijenti tagħhom kif xieraq. Il-PSPs għandhom jippermettu lill-klijenti jiskonnettjaw il-funzjonalità ta' pagament bl-internet.

Aċċess tal-konsumatur għal informazzjoni dwar l-istatus tal-bidu u l-eżekuzzjoni tal-pagament

14. Il-PSPs għandhom jikkonfermaw mal-klijenti tagħhom il-bidu tal-pagament u jipprovdu lill-klijenti fi żmien dovut l-informazzjoni meħtieġa biex jiċċekkjaw li tranżazzjoni ta' ħlas tkun inbdiet u/jew ġiet eżegwita b'mod korrett.

    14.1 [CT/mandat elettroniku] Il-PSPs għandhom jipprovdu lill-klijenti faċilità qrib il-ħin reali biex jiċċekkjaw l-istatus tal-eżekuzzjoni tat-tranżazzjonijiet kif ukoll il-bilanċi tal-kontijiet fi kwalunkwe ħin [22] f'ambjent sigur u fdat.

    14.2 Kull dikjarazzjoni elettronika dettaljata għandha tkun disponibbli f'ambjent sigur u fdat. Meta l-PSPs jinfurmaw lill-klijenti dwar id-disponibbiltà tad-dikjarazzjonijiet elettroniċi (eż. regolarment meta tkun inħarġet dikjarazzjoni elettronika perjodika, jew fuq bażi ad hoc wara l-eżekuzzjoni ta' tranżazzjoni) permezz ta' kanal alternattiv, bħal SMS, e-mail jew ittra, id-data tal-ħlas sensittiva m'għandhiex tiġi inkluża f'tali komunikazzjonijiet jew, jekk tiġi inkluża, għandha tkun mgħottija.

Titolu III – Dispożizzjonijiet finali u implimentazzjoni

15. Dawn il-Linji Gwida japplikaw mill-01.08.2015.

[21] Dawn il-limiti jistgħu jew japplikaw globalment (jiġifieri għall-istrumenti kollha ta' pagament li jippermettu pagamenti bl-internet) jew individwalment.

[22] Eskluż in-nuqqas ta' disponibbiltà eċċezzjonali tal-faċilità għal finijiet ta' manutenzjoni teknika, jew bħala riżultat ta' inċidenti maġġuri.

Anness 1: Eżempji tal-aħjar prattika

Minbarra r-rekwiżiti stipulati hawn fuq, dawn il-linji gwida jiddeskrivu uħud mill-aħjar prattiki li l-PSPs u l-parteċipanti tas-suq rilevanti huma mħeġġin, iżda mhux meħtieġa, li jadottaw. Għall-faċilità ta' referenza, il-kapitoli li għandhom japplikaw għalihom dawn l-aħjar prattiki huma ddikjarati b'mod espliċitu.

Ambjent ta' kontroll u sigurtà ġenerali

Governanza

BP 1: Il-politika ta' sigurtà tista' tiġi stipulata f'dokument iddedikat.

Kontroll u mitigazzjoni tar-riskju

BP 2: Il-PSPs jistgħu jipprovdu għodod ta' sigurtà (eż apparati u/jew brawżers adattati għall-użijiet u l-utenti speċifiċi, żgurati sew) biex jipproteġu l-interfaċċa tal-klijent kontra l-użu illegali jew attakki (eż. attakki "man in the browser").

Traċċabbiltà

BP 3: Il-PSPs li joffru servizzi ta' akkwist jistgħu kuntrattwalment jeħtieġu lill-kummerċjanti elettroniċi li jaħżnu l-informazzjoni ta' pagament biex ikollhom proċessi adegwati fis-seħħ li jappoġġjaw it-traċċabbiltà.

Miżuri speċifiċi ta' kontroll u sigurtà għal pagamenti bl-internet

Identifikazzjoni inizjali tal-konsumatur, informazzjoni

BP4: Il-klijent jista' jiffirma kuntratt ta' servizz iddedikat għat-twettiq ta' tranżazzjonijiet ta' pagamenti bl-internet, pjuttost milli t-termini jiġu inklużi f'kuntratt usa' ta' servizz ġenerali mal-PSP.

BP5: Il-PSPs jistgħu jiżguraw ukoll li l-klijenti huma pprovduti, fuq bażi kontinwa jew, fejn applikabbli, fuq bażi ad hoc, u permezz ta' mezzi xierqa (eż. fuljetti, paġni tas-sit elettroniku), struzzjonijiet ċari u sempliċi li jispjegaw ir-responsabbiltajiet tagħhom rigward l-użu sigur tas-servizz.

Awtentifikazzjoni b'saħħitha mal-klijenti

BP6: [kards] Il-kummerċjanti elettroniċi jistgħu jappoġġjaw awtentifikazzjoni b'saħħitha tad-detentur tal-kards mill-emittent f'tranżazzjonijiet bil-kards permezz tal-internet.

BP7: Għall-finijiet tal-konvenjenza tal-klijent, il-PSPs jistgħu jikkunsidraw li jużaw għodda ta' awtentifikazzjoni b'saħħitha għall-klijenti unika għas-servizzi kollha ta' pagament bl-internet. Dan jista' jżid l-aċċettazzjoni tas-soluzzjoni fost il-klijenti u jiffaċilita l-użu xieraq.

BP8: Awtentifikazzjoni b'saħħitha tal-konsumaturi tista' tinkludi elementi li jgħaqqdu l-awtentifikazzjoni ma' ammont u prenditur speċifiku. Dan jista' jipprovdi lill-klijenti żieda

fiċ-ċertezza meta jawtorizzaw l-pagamenti. Is-soluzzjoni tat-teknoloġija li tippermetti li d-data ta' awtentifikazzjoni b'saħħitha u d-data dwar tranżazzjonijiet ikunu marbutin għandha tkun reżistenti għat-tbagħbis.

Protezzjoni ta' data ta' ħlas sensittiva

BP 9: Huwa mixtieq li l-kummerċjanti elettroniċi li jittrattaw id-data sensittiva ta' ħlas iħarrġu sew lill-persunal tal-ġestjoni tal-frodi tagħhom u jaġġornaw dan it-taħriġ regolarment biex jiżguraw li l-kontenut jibqa' rilevanti għal ambjent ta' sigurtà dinamiku.

Edukazzjoni u komunikazzjoni tal-klijent

BP 10: Huwa mixtieq li l-PSPs li joffru servizzi ta' akkwist jirranġaw programmi edukattivi għall-kummerċjanti elettroniċi tagħhom dwar il-prevenzjoni tal-frodi.

Notifiki, issettjar ta' limiti

BP 11: Fil-limiti stabbiliti, il-PSPs jistgħu jipprovdu lill-klijenti tagħhom il-faċilità li jiġġestixxu l-limiti għal servizzi ta' pagament bl-internet f'ambjent sigur u fdat.

BP 12: Il-PSPs jistgħu jimplimentaw allerti għall-klijenti, bħal permezz ta' telefonati jew SMS, għal tranżazzjonijiet ta' ħlas ta' riskju għoli jew suspettużi bbażati fuq il-politiki tal-ġestjoni tar-riskju tagħhom.

BP 13: Il-PSPs jistgħu jippermettu lill-klijenti jispeċifikaw regoli ġenerali u personalizzati bħala parametri għall-imġiba tagħhom rigward pagamenti bl-internet u servizzi relatati, eż. li huma se jibdew biss ħlasijiet minn ċerti pajjiżi speċifiċi u li l-ħlasijiet mibdija minn x'imkien ieħor għandhom jiġu mblukkati, jew li huma jistgħu jinkludu prendituri speċifiċi fil-listi bojod jew suwed.