EBA/GL/2014/12_Rev1

19 decembrie 2014

Ghid final

privind securitatea plăților pe internet

Sumar

Ghid final privind securitatea plăților pe internet

Statutul ghidului

Prezentul document conține ghiduri emise în temeiul articolului 16 din Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea Bancară Europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (denumit în continuare „Regulamentul ABE"). În conformitate cu articolul 16 alineatul (3) din Regulamentul ABE, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile necesare pentru a respecta ghidurile.

Ghidul prezintă punctul de vedere al ABE privind practicile adecvate în materie de supraveghere în cadrul Sistemului european al supraveghetorilor financiari sau privind modul în care ar trebui aplicat dreptul Uniunii într-un anumit domeniu. Prin urmare, ABE se așteaptă ca toate autoritățile competente și instituțiile financiare cărora li se aplică ghidul să se conformeze. Autoritățile competente cărora li se aplică ghidul trebuie să îl integreze în practicile lor de supraveghere, după caz (de exemplu, prin modificarea cadrului legislativ sau a procedurilor de supraveghere), inclusiv în cazurile în care anumite puncte din cuprinsul documentului sunt adresate în primul rând instituțiilor.

Cerințe de raportare

În conformitate cu articolul 16 alineatul (3) din Regulamentul ABE, autoritățile competente trebuie să notifice ABE dacă se conformează sau intenționează să se conformeze cu prezentul ghid sau să comunice motivele neconformării până la 5 mai 2015. În absența unei notificări până la acest termen, ABE va considera că autoritățile competente nu respectă ghidul. Notificările se trimit prin intermediul formularului din secțiunea 5, la adresa compliance@eba.europa.eu, cu mențiunea „EBA/GL/2014/12". Notificările trebuie trimise de persoane care au autoritatea de a raporta cu privire la respectarea ghidului în numele autorităților competente.

Notificările vor fi publicate pe site-ul ABE, în conformitate cu articolul 16 alineatul (3).

Titlul I - Domeniu de aplicare și definiții

Domeniul de aplicare

1. Prezentul ghid stabilește un set de cerințe minime în domeniul securității plăților pe internet. Ghidul se bazează pe normele din Directiva 2007/64/CE[1] („Directiva privind serviciile de plată", DSP) referitoare la cerințele de informare pentru serviciile de plată și obligațiile prestatorilor de servicii de plată (PSP) în legătură cu prestarea serviciilor de plată. În plus, articolul 10 alineatul (4) din directivă impune instituțiilor de plată să dispună de sisteme de guvernanță solide și de mecanisme de control intern adecvate.

2. Ghidul se aplică prestării de servicii de plată oferite prin intermediul internetului de prestatorii de servicii de plată definiți la articolul 1 din directivă.

3. Ghidul se adresează instituțiilor financiare, astfel cum sunt definite la articolul 4 alineatul (1) din Regulamentul (UE) nr. 1093/2010, și autorităților competente, astfel cum sunt definite la articolul 4 alineatul (2) din Regulamentul (UE) nr. 1093/2010. Autoritățile competente din cele 28 de state membre ale Uniunii Europene trebuie să asigure aplicarea prezentului ghid de prestatorii de servicii de plată, astfel cum sunt definiți la articolul 1 din DSP, aflați sub supravegherea lor.

4. În plus, autoritățile competente pot decide să le solicite prestatorilor de servicii de plată să raporteze autorității competente respectarea ghidului.

5. Prezentul ghid nu afectează validitatea „Recomandărilor pentru securitatea plăților pe internet" emise de Banca Centrală Europeană („raportul")[2]. Raportul continuă, în special, să reprezinte documentul față de care băncile centrale, în funcția lor de supraveghere a sistemelor și instrumentelor de plată, trebuie să evalueze conformitatea cu privire la securitatea plăților pe internet.

6. Ghidul reprezintă așteptările minime și nu aduce atingere responsabilității prestatorului de servicii de plată de a monitoriza și de a evalua riscurile implicate în operațiunile lor de plată, de a dezvolta propriile politici de securitate detaliate și de a pune în aplicare măsuri adecvate de securitate, contingență, gestionare a incidentelor și continuitate a activității, care sunt proporționale cu riscurile inerente serviciilor de plată prestate.

7. Scopul ghidului este de a defini cerințele minime comune pentru serviciile de plată pe internet enumerate mai jos, indiferent de dispozitivul de acces utilizat:

[1] Directiva 2007/64/CE a Parlamentului European și a Consiliului din 13 noiembrie 2007 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 97/7/CE, 2002/65/CE, 2005/60/CE și 2006/48/CE și de abrogare a Directivei 97/5/CE, JO L 319, 5.12.2007.

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

- [carduri] executarea plăților cu cardul pe internet, inclusiv plata cu carduri virtuale, precum și înregistrarea datelor de plată cu cardul pentru utilizarea în „soluții de tip portofel”;

- [transferuri-credit] executarea transferurilor-credit pe internet;

- [e-mandat] emiterea și modificarea mandatelor electronice de debitare directă;

- [monedă electronică] transferurile de bani electronici între două conturi de monedă electronică prin internet.

8. În cazul în care ghidul indică un rezultat, rezultatul poate fi atins prin mijloace diferite. Pe lângă cerințele prevăzute în continuare, prezentul ghid oferă, de asemenea, exemple de bune practici (în anexa 1), pe care prestatorii de servicii de plată sunt încurajați, dar nu obligați, să le urmeze.

9. În cazul în care oferirea de servicii și instrumente de plată este realizată printr-un sistem de plată (de exemplu, sistemele de plăți cu cardul, sistemele transferurilor-credit, sistemele de debitare directă etc.), autoritățile competente și băncile centrale relevante cu funcție de supraveghere a instrumentelor de plată trebuie să colaboreze pentru a asigura o aplicare consecventă a ghidului de părțile responsabile pentru funcționarea sistemului.

10. Integratorii de plăți[3] care oferă servicii de inițiere de plăți sunt considerați procesatori de servicii de plată pe internet (și, prin urmare, prestatori de servicii de plată), prestatori externi de servicii tehnice pentru sistemele relevante sau prestatori de servicii de plată. În acest din urmă caz, integratorii de plăți trebuie să fie obligați prin contract să respecte ghidul.

11. Sunt excluse din domeniul de aplicare al ghidului:

- alte servicii de internet prestate de un prestator de servicii de plată prin intermediul site-ului său de plată (de exemplu, e-brokeraj, contracte online);

- plățile în cazul în care ordinul este dat prin poștă, comandă telefonică, poștă vocală sau folosind tehnologia pe bază de SMS-uri;

- plățile mobile, altele decât plățile prin intermediul browserului;

- transferurile-credit în cazul în care o terță parte accesează contul de plăți al clientului;

- operațiunile de plată efectuate de o întreprindere prin intermediul rețelelor dedicate;

[3] Integratorii de plăți îi furnizează beneficiarului plății (adică e-comerciantului) o interfață standardizată pentru serviciile de inițiere de plată prestate de prestatorul de servicii de plată.

- plățile cu cardul care folosesc carduri preplătite anonime și care nu sunt reîncărcabile, fizice sau virtuale, în cazul în care nu există nicio relație în curs de desfășurare între emitentul și titularul cardului;

- operațiunile de compensare și decontare a operațiunilor de plată.

Definiții

12. În sensul prezentului ghid și pe lângă definițiile prevăzute în DSP se aplică următoarele definiții:

- *Autentificare* înseamnă o procedură care îi permite prestatorului de servicii de plată să verifice identitatea unui client.

- *Autentificarea strictă a clienților* este, în sensul prezentului ghid, o procedură bazată pe utilizarea a două sau mai multe dintre următoarele elemente - clasificate drept cunoștințe, proprietate și inerență: i) ceva ce numai utilizatorul știe, de exemplu parola statică, codul, codul numeric personal; ii) ceva ce numai utilizatorul are, de exemplu un dispozitiv, smart card, telefon mobil; iii) ceva ce utilizatorul este, de exemplu caracteristica biometrică, cum ar fi o amprentă. În plus, elementele selectate trebuie să fie reciproc independente, adică spargerea unuia nu îl (le) va compromite pe celălalt (celelalte). Cel puțin unul dintre elemente trebuie să fie de unică folosință și să nu poată fi replicat (cu excepția inerenței) și să nu poată fi furat clandestin prin intermediul internetului. Procedura de autentificare strictă trebuie proiectată astfel încât să protejeze confidențialitatea datelor de autentificare.

- *Autorizare* înseamnă o procedură care verifică dacă un client sau un prestator de servicii de plată are dreptul de a efectua o anumită acțiune, de exemplu dreptul de a transfera fonduri sau de a avea acces la date sensibile.

- *Acreditări* înseamnă informațiile - în general confidențiale - furnizate de un client sau de un prestator de servicii de plată în scopul autentificării. Acreditările pot reprezenta, de asemenea, deținerea unui instrument fizic care conține informațiile (de exemplu, generator de parolă unică, smart card) sau ceva ce utilizatorul memorează sau reprezintă (cum ar fi caracteristicile biometrice).

- *Incident major de securitate a plății* înseamnă un incident care are sau ar putea avea un impact semnificativ asupra securității, integrității sau continuității sistemelor de plată ale prestatorului de servicii de plată și/sau asupra securității datelor sau fondurilor sensibile privind plățile. Evaluarea semnificației trebuie să țină cont de numărul de clienți care ar putea fi afectați, valoarea la risc și impactul asupra altor prestatori de servicii de plată sau asupra altor infrastructuri de plată.

- *Analiza de risc al operațiunii* înseamnă evaluarea riscului legat de o operațiune specifică, ținând seama de criterii cum ar fi, de exemplu, tiparul de plată (comportamentul) al clientului, valoarea operațiunii aferente, tipul produsului și profilul beneficiarului plății.

- *Carduri virtuale* înseamnă o soluție de plată pe bază de card unde se generează un număr de card temporar, alternativ, cu o perioadă de valabilitate redusă, utilizare limitată și o limită de consum predefinită, care poate fi utilizată pentru achiziții pe internet.

- *Soluții de tip portofel* înseamnă soluții care îi permit unui client să înregistreze date referitoare la unul sau mai multe instrumente de plată, în scopul de a efectua plăți prin mai mulți e-comercianți.

Titlul II - Ghid privind securitatea plăților pe internet

Mediul general de control și securitate

Guvernanța

1. Prestatorii de servicii de plată trebuie să pună în aplicare și să revizuiască periodic o politică de securitate formală pentru serviciile de plată pe internet.

   1.1 Politica de securitate trebuie să fie documentată în mod corespunzător și revizuită periodic (în conformitate cu orientarea 2.4) și aprobată de conducerea superioară. Aceasta trebuie să definească obiectivele de securitate și apetitul de risc.

   1.2 Politica de securitate trebuie să definească rolurile și responsabilitățile, inclusiv funcția de gestionare a riscurilor cu o linie directă de raportare către consiliul de administrație, precum și liniile de raportare pentru serviciile de plată pe internet prestate, inclusiv gestionarea datelor de plată sensibile în ceea ce privește evaluarea, controlul și diminuarea riscurilor.

Evaluarea riscurilor

2. Prestatorii de servicii de plată trebuie să efectueze și să documenteze evaluări detaliate ale riscurilor în ceea ce privește securitatea plăților pe internet și a serviciilor conexe, atât înainte de inițierea serviciului (serviciilor), cât și ulterior.

   2.1 Prestatorii de servicii de plată, prin funcția lor de gestionare a riscurilor, trebuie să efectueze și să documenteze evaluări detaliate ale riscurilor în ceea ce privește plățile pe internet și serviciile conexe. Prestatorii de servicii de plată trebuie să ia în considerare rezultatele monitorizării continue a amenințărilor la adresa securității serviciilor de plată pe internet, pe care le oferă sau intenționează să le ofere, ținând seama de: i) soluțiile tehnologice pe care le folosesc, ii) serviciile externalizate către prestatori externi și iii) mediul tehnic al clienților. Prestatorii de servicii de plată trebuie să ia în considerare riscurile asociate cu platformele tehnologice alese, arhitectura aplicației, tehnicile de programare și rutinele, atât din partea lor[4], cât și din partea clienților[5], precum și rezultatele procesului de monitorizare a incidentelor de securitate (a se vedea orientarea 3).

   2.2 Pe această bază, prestatorii de servicii de plată trebuie să stabilească dacă și în ce măsură pot fi necesare modificări ale măsurilor de securitate existente, ale tehnologiilor utilizate și ale procedurilor sau serviciilor oferite. Prestatorii de servicii de plată trebuie să țină seama de timpul necesar pentru punerea în aplicare a

[4] Cum ar fi susceptibilitatea sistemului la deturnări ale plăților, injecții SQL, cross-site scripting, suprasaturarea bufferului etc.

[5] Cum ar fi riscurile asociate cu utilizarea aplicațiilor multimedia, plug-in-urilor pentru browser, cadrelor, linkurilor externe etc.

modificărilor (inclusiv prezentarea către clienți) și să ia măsurile provizorii adecvate pentru minimizarea incidentelor de securitate și fraudă, precum și a posibilelor efecte perturbatoare.

2.3 Evaluarea riscurilor trebuie să abordeze necesitatea de a proteja și de a securiza datele de plată sensibile.

2.4 Prestatorii de servicii de plată trebuie să efectueze o revizuire a scenariilor de risc și a măsurilor de securitate existente după incidentele majore care le afectează serviciile, înainte de o schimbare majoră a infrastructurii sau a procedurilor și când sunt identificate noi amenințări prin intermediul activităților de monitorizare a riscurilor. În plus, o revizuire generală a evaluării riscurilor trebuie efectuată cel puțin o dată pe an. Rezultatele evaluărilor și revizuirilor riscurilor trebuie prezentate spre aprobare conducerii superioare.

Monitorizarea și raportarea incidentelor

3. Prestatorii de servicii de plată trebuie să asigure monitorizarea, procesarea și urmărirea coerentă și integrată a incidentelor de securitate, inclusiv a reclamațiilor clienților legate de securitate. Prestatorii de servicii de plată trebuie să stabilească o procedură pentru raportarea unor astfel de incidente către conducere și, în cazul unor incidente majore legate de securitatea plăților, către autoritățile competente.

3.1 Prestatorii de servicii de plată trebuie să instituie un proces pentru a monitoriza, a procesa și a urmări incidentele de securitate și reclamațiile clienților legate de securitate și trebuie să raporteze astfel de incidente către conducere.

3.2 Prestatorii de servicii de plată trebuie să aibă o procedură de notificare imediată a autorităților competente (adică a autorităților de supraveghere, precum și a autorităților de protecție a datelor), dacă acestea există, în cazul unor incidente majore legate de securitate plăților, în ceea ce privește serviciile de plată prestate.

3.3 Prestatorii de servicii de plată trebuie să aibă o procedură de cooperare în privința incidentelor majore legate de securitatea plăților, inclusiv încălcări ale securității datelor, cu organele de aplicare a legii competente.

3.4 Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să solicite prin contract ca e-comercianții care stochează, procesează sau transmit date de plată sensibile să coopereze în privința incidentelor majore legate de securitatea plăților, inclusiv încălcări ale securității datelor, atât cu ei, cât și cu organele de aplicare a legii competente. În cazul în care un prestator de servicii de plată devine conștient de faptul că un e-comerciant nu cooperează astfel cum se solicită prin contract, acesta trebuie să ia măsuri pentru a pune în aplicare această obligație contractuală sau pentru a rezilia contractul.

Controlul și reducerea riscurilor

4. Prestatorii de servicii de plată trebuie să pună în aplicare măsuri de securitate în conformitate cu politicile lor respective de securitate, în scopul de a reduce riscurile identificate. Aceste măsuri trebuie să includă mai multe linii de apărare de securitate, astfel încât căderea unei linii de apărare să fie acoperită de următoarea linie de apărare („apărarea în profunzime").

4.1 La proiectarea, dezvoltarea și menținerea serviciilor de plată pe internet, prestatorii de servicii de plată trebuie să acorde o atenție deosebită separării adecvate a sarcinilor în domeniul tehnologiei informației (IT) (de exemplu, medii de dezvoltare, testare și producție), precum și punerii în aplicare adecvate a principiului „privilegiului minim", ca bază pentru o identitate solidă și gestionarea accesului[6].

4.2 Prestatorii de servicii de plată trebuie să aibă soluții de securitate adecvate pentru a proteja rețelele, site-urile, serverele și legăturile de comunicare împotriva abuzului sau atacurilor. Prestatorii de servicii de plată trebuie să elimine de pe servere toate funcțiile inutile pentru a le proteja (întări) și pentru a elimina sau a reduce vulnerabilitățile aplicațiilor aflate în pericol. Accesul diverselor aplicații la datele și resursele necesare trebuie să fie menținut la un minim strict, conform principiului „privilegiului minim". În scopul de a limita utilizarea de site-uri „false" (care imită site-urile legitime ale prestatorului de servicii de plată), site-urile pentru operațiuni care oferă servicii de plăți pe internet trebuie identificate prin certificate de validare extinse, întocmite în numele prestatorului de servicii de plată, sau prin alte metode de autentificare similare.

4.3 Prestatorii de servicii de plată trebuie să aibă proceduri adecvate pentru a monitoriza, a urmări și a restricționa accesul la: i) datele de plată sensibile, și ii) resursele critice logice și fizice, cum ar fi rețelele, sistemele, bazele de date, modulele de securitate etc. Prestatorii de servicii de plată trebuie să creeze, să salveze și să analizeze jurnale corespunzătoare și piste de audit.

4.4 La proiectarea[7], dezvoltarea și menținerea serviciilor de plată pe internet, prestatorii de servicii de plată trebuie să se asigure că minimizarea datelor[8] este o componentă esențială a funcționalității de bază: colectarea, rutarea, prelucrarea, stocarea și/sau arhivarea, precum și vizualizarea datelor de plată sensibile trebuie menținute la nivelul minim absolut.

[6] „Fiecare program și fiecare utilizator privilegiat al sistemului trebuie să opereze utilizând privilegiul minim necesar pentru a finaliza lucrarea". Vezi Saltzer, JH (1974), „Protection and the Control of Information Sharing in Multics" (Protecția și controlul schimbului de informații în Multics), Comunicările ACM, Vol. 17, nr. 7, p. 388.

[7] Principiul confidențialității prin concepție.

[8] Minimizarea datelor se referă la politica de colectare a celui mai mic volum de informații cu caracter personal, necesare pentru a îndeplini o anumită funcție.

4.5 Măsurile de securitate pentru serviciile de plată pe internet trebuie să fie testate sub supravegherea funcției de gestionare a riscurilor pentru a asigura robustețea și eficiența lor. Toate modificările trebuie să facă obiectul unui proces formal de gestionare a modificărilor, pentru asigurarea faptului că modificările sunt planificate, testate, documentate și autorizate în mod corespunzător. Testele trebuie să fie repetate periodic și să includă scenarii de atacuri potențiale relevante și cunoscute, pe baza modificărilor aduse și a amenințărilor la adresa securității observate.

4.6 Măsurile de securitate ale prestatorului de servicii de plată pe internet trebuie să fie auditate periodic pentru a asigura robustețea și eficiența lor. Punerea în aplicare și funcționarea serviciilor de plată pe internet trebuie să fie, de asemenea, auditate. Frecvența și domeniul de concentrare al acestor audituri trebuie să ia în considerare și să fie proporționale cu riscurile de securitate implicate. Auditurile trebuie efectuate de experți de încredere și independenți (interni sau externi). Aceștia nu trebuie să fie în vreun fel implicați în dezvoltarea, punerea în aplicare sau gestionarea operațională a serviciilor de plată pe internet prestate.

4.7 Ori de câte ori prestatorii de servicii de plată externalizează funcții legate de securitatea serviciilor de plată pe internet, contractul trebuie să includă dispoziții care să impună respectarea principiilor și a orientărilor stabilite în prezentul ghid.

4.8 Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să solicite prin contract ca e-comercianții care procesează (adică stochează, procesează sau transmit) date de plată sensibile să pună în aplicare măsuri de securitate în infrastructura lor IT, în conformitate cu orientările 4.1-4.7, pentru a evita furtul acelor date de plată sensibile prin intermediul sistemelor lor. În cazul în care un prestator de servicii de plată devine conștient de faptul că un e-comerciant nu dispune de măsurile de securitate necesare, acesta trebuie să ia măsuri pentru a pune în aplicare această obligație contractuală sau pentru a rezilia contractul.

Trasabilitatea

5. Prestatorii de servicii de plată trebuie să aibă procese care să asigure faptul că toate operațiunile, precum și fluxul procesului e-mandat, sunt urmărite în mod corespunzător.

5.1 Prestatorii de servicii de plată trebuie să se asigure că serviciul lor include mecanisme de securitate pentru înregistrarea detaliată a datelor de operațiune și e-mandat, inclusiv numărul secvențial al operațiunilor, marcajele de timp pentru datele operațiunii, modificările de parametrizare, precum și accesul la datele operațiunii și e-mandat.

5.2 Prestatorii de servicii de plată trebuie să implementeze fișiere jurnal care să permită urmărirea oricăror adăugări, modificări sau ștergeri ale datelor operațiunii și e-mandat.

5.3 Prestatorii de servicii de plată trebuie să interogheze și să analizeze datele operațiunii și e-mandat și să se asigure că dispun de instrumente pentru evaluarea fișierelor jurnal. Aplicațiile respective trebuie să fie disponibile numai pentru personalul autorizat.

Măsuri specifice de control și de securitate pentru plățile pe internet

Informațiile și identificarea inițială a clientului

6. Clienții trebuie să fie identificați în mod corespunzător, în conformitate cu legislația europeană privind combaterea spălării banilor[9], și trebuie să-și confirme disponibilitatea de a efectua plăți pe internet folosind serviciile înainte de a li se fi acordat accesul la astfel de servicii. Prestatorii de servicii de plată trebuie să ofere informații adecvate „înainte", „în mod periodic" sau, după caz, „ad-hoc" clientului cu privire la cerințele necesare (de exemplu, echipament, proceduri) pentru efectuarea operațiunilor de plată securizată pe internet și riscurile inerente.

6.1 Prestatorii de servicii de plată trebuie să se asigure că fiecare client a urmat procedurile de control și a furnizat documentele de identitate adecvate[10] și informațiile corespunzătoare înainte să-i fie acordat accesul la serviciile de plată pe internet[11].

6.2 Prestatorii de servicii de plată trebuie să se asigure că informațiile prealabile[12] furnizate clientului conțin detalii specifice referitoare la serviciile de plată pe internet. Acestea trebuie să includă, după caz:

- informații clare cu privire la toate cerințele în ceea ce privește echipamentul clientului, programul software sau alte instrumente necesare (de exemplu, programe antivirus, firewall);
- orientări pentru utilizarea corectă și securizată a acreditărilor de securitate personalizate;
- o descriere pas cu pas a procedurii pe care clientul trebuie să o urmeze pentru a transmite și a autoriza o operațiune de plată și/sau pentru a obține informații, inclusiv consecințele fiecărei acțiuni;

[9] De exemplu, Directiva 2005/60/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind prevenirea utilizării sistemului financiar în scopul spălării banilor și finanțării terorismului. JO L 309, 25.11.2005, p. 15-36. A se vedea, de asemenea, Directiva 2006/70/CE din 1 august 2006 de stabilire a măsurilor de punere în aplicare a Directivei 2005/60/CE a Parlamentului European și a Consiliului în ceea ce privește definiția „persoanelor expuse politic" și criteriile tehnice de aplicare a procedurilor simplificate de precauție privind clientela, precum și de exonerare pe motivul unei activități financiare desfășurate în mod ocazional sau la scară foarte limitată. JO L 214, 4.8.2006, p. 29-34.

[10] De exemplu, pașaport, carte de identitate națională sau semnătură electronică avansată.

[11] Procesul de identificare a clientului nu aduce atingere exonerărilor prevăzute în legislația existentă privind combaterea spălării banilor. Prestatorii de servicii de plată nu trebuie să urmeze un proces separat de identificare a clienților pentru serviciile de plată pe internet, cu condiția ca o astfel de identificare a clientului să fi fost deja realizată, de exemplu, pentru alte servicii existente legate de plată sau pentru deschiderea unui cont.

[12] Aceste informații completează articolul 42 din DSP care detaliază informațiile pe care prestatorul de servicii de plată trebuie să le ofere utilizatorului serviciilor de plată înainte de a încheia un contract de prestări de servicii de plată.

- orientări referitoare la utilizarea corectă și securizată a tuturor componentele hardware și software furnizate clientului;

- procedurile de urmat în caz de pierdere sau furt al acreditărilor de securitate personalizate sau al hardware-ului sau software-ului clientului de logare sau de efectuare de operațiuni;

- procedurile de urmat în cazul în care este detectat sau suspectat un abuz;

- o descriere a responsabilităților și a obligațiilor prestatorului de servicii de plată și, respectiv, ale clientului cu privire la utilizarea serviciului de plată pe internet.

6.3 Prestatorii de servicii de plată trebuie să se asigure că este specificat în contractul-cadru al clientului faptul că prestatorul de servicii de plată poate bloca o operațiune specifică sau instrumentul de plată[13] ca urmare a unor preocupări legate de securitate. Acesta trebuie să stabilească metoda și condițiile notificării clientului și modul în care clientul poate contacta prestatorul de servicii de plată pentru ca operațiunea de plată pe internet sau serviciul să-i fie„deblocat”, în conformitate cu DSP.

Autentificarea strictă a clientului

7. Inițierea plăților pe internet, precum și accesul la datele sensibile de plată trebuie să fie protejate prin autentificarea strictă a clientului. Prestatorii de servicii de plată trebuie să aibă o procedură strictă de autentificare a clientului, în conformitate cu definiția prevăzută în prezentul ghid.

7.1 [transferuri-credit/e-mandat/monedă electronică] Prestatorii de servicii de plată trebuie să execute autentificarea strictă a clientului pentru autorizarea operațiunilor de plată pe internet ale clientului (inclusiv pachete de transferuri-credit) și emiterea sau modificarea mandatelor electronice de debitare directă. Cu toate acestea, prestatorii de servicii de plată ar putea lua în considerare adoptarea unor măsuri alternative de autentificare a clientului pentru:

- plățile efectuate către beneficiari de încredere incluși pe listele albe stabilite anterior pentru acel client;

- operațiunile între două conturi ale aceluiași client, deținute la același prestator de servicii de plată;

- transferurile în cadrul aceluiași prestator de servicii de plată, justificate printr-o analiză de risc al operațiunii;

[13] A se vedea articolul 55 din DSP privind limitele de utilizare a instrumentului de plată.

- plățile cu valoare redusă, menționate în DSP[14].

7.2 Obținerea accesului la date de plată sensibile sau modificarea acestora (inclusiv crearea și modificarea listelor albe) necesită autentificarea strictă a clientului. În cazul în care un prestator de servicii de plată oferă servicii pur consultative, care nu afișează informațiile sensibile de plată ale clientului, cum ar fi datele cardurilor de plată, care ar putea fi ușor utilizate în mod abuziv pentru a comite fraude, prestatorul de servicii de plată își poate adapta cerințele de autentificare pe baza evaluării riscurilor.

7.3 [carduri] Pentru operațiunile cu carduri, toți prestatorii de servicii de plată emitenți de carduri trebuie să ofere asistență pentru autentificarea strictă a titularului cardului. Toate cardurile emise trebuie să fie pregătite tehnic (înregistrate) pentru a fi utilizate cu autentificare strictă.

7.4 [carduri] Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să ofere asistență pentru tehnologii care să-i permită emitentului să execute autentificarea strictă a titularului cardului, pentru sistemele de plată cu cardul la care participă achizitorul.

7.5 [carduri] Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să le solicite e-comercianților lor să ofere asistență pentru soluții care să-i permită emitentului să execute autentificarea strictă a titularului cardului, pentru operațiunile cu carduri prin intermediul internetului. Utilizarea măsurilor alternative de autentificare ar putea fi luată în considerare pentru categoriile identificate în prealabil ca operațiuni cu risc redus, de exemplu pe baza unei analize de risc al operațiunii sau care implică plăți cu valoare redusă, astfel cum se prevede în DSP.

7.6 [carduri] Pentru sistemele de plată cu cardul acceptate de serviciu, prestatorii de soluții de tip portofel trebuie să solicite autentificarea strictă de către emitent în cazul în care titularul legitim își înregistrează pentru prima dată datele de card.

7.7 Prestatorii de soluții de tip portofel trebuie să ofere asistență pentru autentificarea strictă a clientului atunci când clienții se conectează la serviciile de plată de tip portofel sau efectuează operațiuni cu carduri prin intermediul internetului. Utilizarea măsurilor alternative de autentificare ar putea fi luată în considerare pentru categoriile identificate în prealabil ca operațiuni cu risc redus, de exemplu pe baza unei analize de risc al operațiunii sau care implică plăți cu valoare redusă, astfel cum se prevede în DSP.

7.8 [carduri] Pentru cardurile virtuale, înregistrarea inițială trebuie să aibă loc într-un mediu sigur și de încredere[15]. Autentificarea strictă a clienților trebuie să fie necesară

[14] A se vedea definiția instrumentelor de plată cu valoare redusă de la articolul 34 alineatul (1) și articolul 53 alineatul (1) din DSP.

[15] Mediile aflate sub responsabilitatea prestatorului de servicii de plată, unde se asigură autentificarea adecvată a clientului și a prestatorului de servicii de plată care oferă serviciul și protecția informațiilor confidențiale/sensibile

pentru procesul de generare a datelor cardului virtual, în cazul în care cardul este emis pe internet.

7.9 Prestatorii de servicii de plată trebuie să asigure autentificarea bilaterală adecvată atunci când comunică cu e-comercianții în vederea inițierii plăților pe internet și a accesării datelor de plată sensibile.

Înscrierea pentru instrumente și/sau programe software de autentificare livrate clientului și furnizarea acestora

8. Prestatorii de servicii de plată trebuie să se asigure că înscrierea clientului pentru instrumente de autentificare și furnizarea inițială a acestor instrumente, necesare pentru a utiliza serviciul de plată pe internet și/sau livrarea programelor software pentru plată către clienți se efectuează într-un mod securizat.

8.1 Înscrierea pentru instrumente de autentificare și/sau programe software pentru plată livrate clientului și furnizarea acestora trebuie să îndeplinească următoarele cerințe.

- Procedurile aferente trebuie să se desfășoare într-un mediu sigur și de încredere, luând în calcul riscurile potențiale provenite din dispozitivele care nu se află sub controlul prestatorului de servicii de plată.

- Trebuie să existe proceduri eficiente și securizate pentru livrarea acreditărilor de securizare personalizate, a programelor software pentru plată și a tuturor dispozitivelor personalizate pentru plăți pe internet. Programele software livrate pe internet trebuie să fie, de asemenea, semnate digital de către prestatorul de servicii de plată, pentru a-i permite clientului să verifice autenticitatea și faptul că nu au avut loc modificări neautorizate.

- [carduri] Pentru operațiunile cu carduri, clientul trebuie să aibă posibilitatea de a se înregistra pentru autentificarea strictă, independent de o anumită achiziție specifică pe internet. În cazul în care se oferă opțiunea de activare în timpul cumpărăturilor online, acest lucru trebuie efectuat prin redirecționarea clientului către un mediu sigur și de încredere.

8.2 [carduri] Emitenții trebuie să încurajeze în mod activ înscrierea titularului cardului pentru autentificarea strictă și trebuie să le permită titularilor de carduri să evite înscrierea numai într-un număr excepțional și limitat de cazuri, care să fie justificate de riscul legat de operațiunea specifică cu cardul.

---

include: i) sediul prestatorului de servicii de plată; ii) internet banking sau alte site-uri securizate, de exemplu, în cazul în care GA oferă caracteristici de securitate comparabile, printre altele după cum se definește la orientarea 4 sau iii) servicii bancomat (ATM). (În cazul ATM-urilor, este necesară autentificarea strictă a clientului. O astfel de autentificare este, de obicei, asigurată prin cip și PIN sau cip și elemente biometrice).

Încercările de logare, expirarea sesiunii, valabilitatea autentificării

9. Prestatorii de servicii de plată trebuie să limiteze numărul de încercări de logare sau de autentificare, să definească reguli pentru expirarea sesiunilor serviciilor de plată pe internet și să stabilească limite de timp pentru validitatea autentificării.

   9.1 La utilizarea unei parole unice (OTP) pentru autentificare, prestatorii de servicii de plată trebuie să se asigure că perioada de valabilitate a unor astfel de parole este limitată la strictul minim necesar.

   9.2 Prestatorii de servicii de plată trebuie să stabilească numărul maxim de încercări de logare sau de autentificare eșuate, după care accesul la serviciul de plată pe internet să fie (temporar sau permanent) blocat. Ei trebuie să aibă o procedură securizată de reactivare a serviciilor de plată pe internet blocate.

   9.3 Prestatorii de servicii de plată trebuie să stabilească perioada maximă după care sesiunile de servicii de plată pe internet inactive să fie terminate în mod automat.

Monitorizarea operațiunilor

10. Mecanismele de monitorizare a operațiunilor, care au scopul de a preveni, de a detecta și de a bloca operațiunile de plată frauduloase trebuie să fie rulate înainte de autorizația finală a prestatorului de servicii de plată; operațiunile suspecte sau cu risc ridicat trebuie să facă obiectul unei examinări specifice și al unei proceduri de evaluare. Trebuie să existe, de asemenea, mecanisme echivalente de monitorizare a securității și de autorizare pentru emiterea de e-mandate.

    10.1 Prestatorul de servicii de plată trebuie să utilizeze sisteme de detectare și de prevenire a fraudei pentru a identifica operațiunile suspecte, înainte ca prestatorul de servicii de plată să autorizeze în mod final operațiunile sau e-mandatele. Astfel de sisteme trebuie să se bazeze, de exemplu, pe normele parametrizate (cum ar fi listele negre de date de card compromise sau furate) și să monitorizeze tiparele de comportament anormal al clientului sau dispozitivele de acces ale clientului [cum ar fi o schimbare a adresei protocolului de internet (IP)[16] sau a gamei de IP-uri folosite în timpul sesiunii de servicii de plată pe internet, uneori identificate prin controale de geolocație a IP-ului[17], categoriile e-comerciale atipice pentru un client anume sau datele anormale ale operațiunii etc.]. Astfel de sisteme trebuie să poată, de asemenea, să detecteze semnele de infecție malware din sesiune (de exemplu, prin script versus validare manuală) și scenariile cunoscute de fraudă. Anvergura, complexitatea și adaptabilitatea soluțiilor de monitorizare, pe lângă faptul că trebuie să respecte legislația relevantă privind protecția datelor, trebuie să fie proporționale cu rezultatul evaluării riscurilor.

[16] O adresă IP este un cod numeric unic de identificare a fiecărui calculator conectat la internet.

[17] O verificare „Geo-IP" verifică dacă țara emitentă corespunde cu adresa IP-ului de la care utilizatorul inițiază operațiunea.

10.2 Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să dispună de sisteme de detectare și de prevenire a fraudei pentru a monitoriza activitățile e-comerciale.

10.3 Prestatorii de servicii de plată trebuie să efectueze toate examinările operațiunilor și procedurile de evaluare într-o perioadă de timp adecvată, pentru a nu întârzia în mod nejustificat inițierea și/sau prestarea serviciilor de plată în cauză.

10.4 În cazul în care prestatorul de servicii de plată, în conformitate cu politica sa de risc, decide să blocheze o operațiune de plată care a fost identificată ca potențial frauduloasă, prestatorul de servicii de plată trebuie să mențină blocarea pentru o perioadă cât mai scurtă posibilă, până când au fost rezolvate problemele de securitate.

Protecția datelor de plată sensibile

11. Datele de plată sensibile trebuie să fie protejate atunci când stocate, procesate sau transmise.

11.1 Toate datele utilizate pentru identificarea și autentificarea clienților (de exemplu, la momentul logării, atunci când are loc inițierea plăților pe internet și când sunt emise, modificate sau anulate e-mandatele), precum și interfața de client (site-ul prestatorului de servicii de plată sau al e-comerciantului) trebuie să fie securizate în mod corespunzător împotriva furtului și a accesului sau modificărilor neautorizate.

11.2 Prestatorii de servicii de plată trebuie să se asigure că, atunci când are loc schimbarea datelor de plată sensibile prin internet, este utilizată criptarea securizată de la un capăt la altul[18], aplicată între părțile care comunică pe parcursul sesiunii de comunicare respective, pentru a proteja confidențialitatea și integritatea datelor, folosind tehnici de criptare stricte și recunoscute la scară largă.

11.3 Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să îi încurajeze pe e-comercianții lor să nu stocheze date de plată sensibile. În cazul în care e-comercianții procesează, adică stochează, procesează sau transmit date de plată sensibile, acești prestatori de servicii de plată trebuie să le solicite prin contract e-comercianților să dispună de măsurile necesare pentru a proteja aceste date. Prestatorii de servicii de plată trebuie să efectueze controale periodice și în cazul în care un prestator devine conștient de faptul că un e-comerciant care procesează date de plată sensibile nu dispune de măsurile de securitate necesare, acesta trebuie să ia măsuri pentru a pune în aplicare obligația contractuală sau pentru a rezilia contractul.

[18] Criptarea de la un capăt la altul se referă la criptarea în cadrul sau la sistemul sursă final, cu decriptarea corespunzătoare care apare doar în cadrul sau la sistemul de destinație final. ETSI EN 302 109 V1.1.1. (2003-06).

Conștientizarea din partea clientului, instruirea și comunicarea cu clienții

Instruirea clientului și comunicarea cu clienții

12. Prestatorii de servicii de plată trebuie să ofere asistență și îndrumare clienților, după caz, în ceea ce privește utilizarea securizată a serviciilor de plată pe internet. Prestatorii de servicii de plată trebuie să comunice cu clienții lor în așa fel încât să îi reasigure de autenticitatea mesajelor primite.

12.1 Prestatorii de servicii de plată trebuie să furnizeze cel puțin un canal securizat[19] pentru comunicarea continuă cu clienții în ceea ce privește utilizarea corectă și sigură a serviciului de plată pe internet. Prestatorii de servicii de plată trebuie să îi informeze pe clienți despre acest canal și să le explice faptul că orice mesaj din partea prestatorului de servicii de plată prin orice alte mijloace, cum ar fi e-mailul, care se referă la utilizarea corectă și securizată a serviciului de plată pe internet, nu este de încredere. Prestatorul de servicii de plată trebuie să explice:

- procedura prin care clienții să îi raporteze prestatorului de servicii de plată plățile (suspecte) frauduloase, incidentele suspecte sau anomaliile din timpul sesiunii serviciilor de plată pe internet și/sau posibilele încercări de inginerie socială[20];
- etapele următoare, adică modul în care prestatorul de servicii de plată îi va răspunde unui client;
- modul în care prestatorul de servicii de plată va notifica clientul asupra operațiunilor (potențial) frauduloase sau neinițierii lor sau modul în care îl va avertiza pe client cu privire la apariția atacurilor (de exemplu, e-mailuri de tip phising).

12.2 Prestatorii de servicii de plată trebuie să îi informeze pe clienți, prin intermediul canalului securizat, asupra actualizărilor procedurilor de securitate cu privire la serviciile de plată pe internet. Orice alerte cu privire la riscurile semnificative emergente (de exemplu, avertizări cu privire la ingineria socială) trebuie să fie, de asemenea, trimise prin intermediul canalului securizat.

12.3 Prestatorii de servicii de plată trebuie să pună la dispoziție un serviciu de asistență pentru clienți pentru toate întrebările, reclamațiile, cererile de asistență și notificările asupra anomaliilor sau incidentelor cu privire la plățile pe internet și serviciile conexe, iar clienții trebuie să fie informați în mod corespunzător asupra modului în care poate fi obținută această asistență.

[19] Cum ar fi o cutie poștală dedicată pe site-ul prestatorului de servicii de plată sau un site web securizat.

[20] Ingineria socială în acest context înseamnă tehnicile de manipulare a oamenilor pentru a obține informații (de exemplu, prin e-mail sau apeluri telefonice) sau preluarea informațiilor din rețelele sociale, în scop de fraudă sau de obținere a accesului neautorizat la un calculator sau o rețea.

12.4 Prestatorii de servicii de plată trebuie să inițieze programe de instruire și conștientizare destinate clienților, create pentru a asigura cel puțin înțelegerea din partea clienților a necesității:

- de protejare a parolelor lor, dispozitivelor de securitate, detaliilor personale și a altor date confidențiale;
- de gestionare în mod corespunzător a securității dispozitivului personal (de exemplu, a calculatorului) prin instalarea și actualizarea componentelor de securitate (antivirusurilor, firewallurilor, patch-urilor de securitate);
- de a lua în considerare amenințările și riscurile semnificative legate de descărcarea de programe software prin intermediul internetului, în cazul în care clientul nu poate fi suficient de sigur că programul software este autentic și nu a fost modificat;
- de a utiliza site-ul original de plată pe internet al prestatorului de servicii de plată.

12.5 Prestatorii de servicii de plată prin acceptare a cardurilor trebuie să le solicite e-comercianților să separe în mod clar procesele legate de plată de magazinul online, pentru a facilita identificarea de către clienți a momentelor când comunică cu prestatorul de servicii de plăți, și nu cu beneficiarul plății (de exemplu, prin redirecționarea clientului și deschiderea unei ferestre separate, astfel încât procesul de plată să nu fie prezentat în cadrul e-comerciantului).

Notificări, stabilirea de limite

13. Prestatorii de servicii de plată trebuie să stabilească limite pentru serviciile de plată pe internet și le-ar putea oferi clienților opțiuni de limitare a riscurilor ulterioare în cadrul acestor limite. Ei pot oferi, de asemenea, servicii de alertă și de administrare a profilului clientului.

13.1 Înainte de a-i oferi unui client serviciile de plată pe internet, prestatorii de servicii de plată trebuie să stabilească limite[21] aplicabile acestor servicii (de exemplu, o sumă maximă pentru fiecare plată individuală sau o sumă cumulată pe o anumită perioadă de timp) și trebuie să își informeze clienții în consecință. Prestatorii de servicii de plată trebuie să le permită clienților să dezactiveze funcționalitatea de plată pe internet.

Accesul clienților la informații despre starea de inițiere și execuție a plății

14. Prestatorii de servicii de plată trebuie să le confirme clienților inițierea plății și să le ofere clienților în timp util informațiile necesare pentru a verifica dacă o operațiune de plată a fost inițiată și/sau executată în mod corect.

[21] Aceste limite pot să se aplice fie la nivel global (de exemplu, pentru toate instrumentele de plată care permit plățile pe internet), fie la nivel individual.

14.1 [transferuri-credit/e-mandat] Prestatorii de servicii de plată trebuie să le ofere clienților o funcție în timp aproape real de verificare a stării de executare a operațiunilor, precum și a soldurilor conturilor în orice moment[22], într-un mediu sigur și de încredere.

14.2 Extrasele electronice detaliate trebuie să fie puse la dispoziție într-un mediu sigur și de încredere. În cazul în care prestatorii de servicii de plată îi informează pe clienți cu privire la disponibilitatea extraselor electronice (de exemplu, în mod periodic, atunci când un extras electronic periodic a fost emis sau ad-hoc, după executarea unei operațiuni) printr-un canal alternativ, cum ar fi SMS, e-mail sau scrisoare, datele de plată sensibile nu trebuie să fie incluse în astfel de comunicări sau, în cazul în care sunt incluse, acestea trebuie să fie mascate.

Titlul III – Dispoziții finale și punerea în aplicare

15. Prezentul ghid se aplică de la 01.08.2015.

[22] Cu excepția lipsei de disponibilitate excepționale a funcției în scopuri de întreținere tehnică sau ca urmare a unor incidente majore.

Anexa 1: Exemple de bune practici

În plus față de cerințele stabilite mai sus, prezentul ghid descrie exemple de bune practici, pe care prestatorii de servicii de plată și participanții pe piața în cauză sunt încurajați, dar nu obligați, să le adopte. Pentru a facilita consultarea, capitolele la care se aplică aceste bune practici sunt prezentate în mod explicit.

Mediul general de control și securitate

Guvernanța

BP 1: Politica de securitate ar putea fi stabilită într-un document dedicat.

Controlul și reducerea riscurilor

BP 2: Prestatorii de servicii de plată ar putea oferi instrumente de securitate (de exemplu, dispozitive și/sau browsere personalizate, securizate în mod adecvat), pentru a proteja interfața clientului împotriva utilizării sau atacurilor ilegale (de exemplu, atacurile „omul din browser").

Trasabilitatea

BP 3: Prestatorii de servicii de plată prin acceptare a cardurilor le-ar putea solicita prin contract e-comercianților care stochează informații de plată să dispună de procese adecvate care să suporte trasabilitatea.

Măsuri specifice de control și de securitate pentru plățile pe internet

Informațiile și identificarea inițială a clientului

BP 4: Clientul ar putea semna un contract de servicii dedicat pentru efectuarea operațiunilor de plată pe internet, în loc ca termenii să fie incluși într-un contract mai larg de servicii generale încheiat cu prestatorul de servicii de plată.

BP 5: Prestatorii de servicii de plată ar putea să se asigure, de asemenea, că le sunt oferite clienților în mod continuu sau, după caz, ad-hoc și prin mijloace adecvate (de exemplu, pliante, pagini ale site-ului) instrucțiuni clare și simple care le explică responsabilitățile în ceea ce privește utilizarea securizată a serviciului.

Autentificarea strictă a clientului

BP 6: [carduri] E-comercianții ar putea oferi asistență pentru autentificarea strictă a titularului cardului, din partea emitentului, în cadrul operațiunilor cu carduri pe internet.

BP 7: Din motive de comoditate pentru client, prestatorii de servicii de plată ar putea lua în considerare utilizarea unui singur instrument de autentificare strictă a clientului pentru toate serviciile de plată pe internet. Acest lucru ar putea spori acceptarea soluției în rândul clienților și facilitarea utilizării corecte.

BP 8: Autentificarea strictă a clientului ar putea include elemente care leagă autentificarea de o anumită sumă și un anumit beneficiar. Acest lucru le-ar putea oferi clienților o certitudine sporită la autorizarea plăților. Soluția tehnologică ce permite legarea datelor de autentificare strictă și a datelor operațiunii trebuie să fie rezistentă la sabotaj.

Protecția datelor de plată sensibile

BP 9: Este de dorit ca e-comercianții care procesează date de plată sensibile să își instruiască în mod corespunzător personalul de gestionare a fraudelor și să actualizeze această instruire în mod regulat pentru a se asigura că instruirea rămâne relevantă pentru un mediu de securitate dinamic.

Instruirea clientului și comunicarea cu clienții

BP 10: Este de dorit ca prestatorii de servicii de plată prin acceptare a cardurilor să organizeze programe de instruire referitoare la prevenirea fraudei pentru e-comercianții lor.

Notificări, stabilirea de limite

BP 11: În limitele stabilite, prestatorii de servicii de plată le-ar putea oferi clienților lor facilitatea de a gestiona limitele pentru serviciile de plată pe internet într-un mediu sigur și de încredere.

BP 12: Prestatorii de servicii de plată ar putea să pună în aplicare alerte pentru clienți, cum ar fi cele prin apeluri telefonice sau SMS-uri, referitoare la operațiunile suspecte sau operațiunile de plată cu risc ridicat, în conformitate cu politicile lor de gestionare a riscurilor.

BP 13: Prestatorii de servicii de plată le-ar putea permite clienților să indice norme generale, personalizate ca parametri pentru comportamentul lor în ceea ce privește plățile pe internet și serviciile conexe, de exemplu, că vor iniția plăți numai din anumite țări specifice și că plățile inițiate din altă parte trebuie să fie blocate sau pot include beneficiari specifici pe liste albe sau negre.