TUCA ZBARCEA
ASOCIATII

NOI ACTORI PE PIAȚA SERVICIILOR FINANCIARE
OPEN BANKING - PSD 2

Data: 30 martie 2018

Autor: Gabriela ANTON, Partener al Țuca Zbârcea & Asociații

PSD 2 – OPEN BANKING

- Directiva UE 2015/2366 privind serviciile de plată în cadrul pieței interne (PSD2) a intrat în vigoare pe 13 ianuarie 2018, dată până la care statele membre aveau obligația să transpună PSD 2 în dreptul intern
- România nu a transpus PSD2 în dreptul intern și nici nu există o inițiativă legislativă până la acest moment
- Parte din conceptul de „open banking”, PSD2 va modifica fundamental modul de realizare a operațiunilor de plată, de accesare a informațiilor cu privire la conturi, prin deschiderea pieței serviciilor de plată către noi actori denumiți generic “TPP” – terțe părți prestatori
- TPP pot fi instituții nebancare, companii FinTech sau comercianți care se pot autoriza ca instituții de servicii de plată.
- PSD 2 reprezintă o recunoaștere a revoluției „FinTech” pe piața serviciilor de plată și elimină monopolul băncilor asupra datelor bancare ale clienților
- Se estimează că instituțiile FinTech vor juca un rol semnificativ în viitorul mediu financiar. Tot mai mulți investitori sunt disponibili să investească sume semnificative în companiile FinTech.

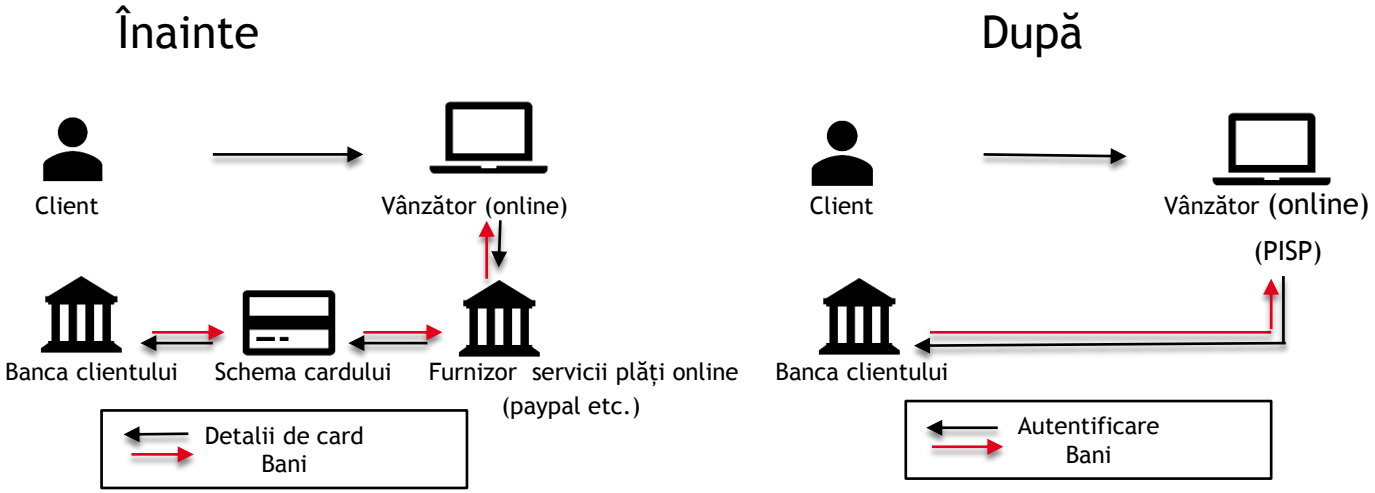
TTP – PSIP și AISP

- Unul din scopurile principale ale PSD 2 este să încurajeze noi actori să intre pe piața serviciilor de plată, și realizează acest lucru prin obligarea băncilor să dea acces la informații privind conturile bancare unor terțe părți
- Băncile sunt obligate să furnizeze acces la infrastructura lor de plăți - *application programming interfaces (APIs)* și la datele clienților către terțe părți - TTP care își pot apoi dezvolta serviciile de informații și plăți, dar și alte servicii financiare către clienții băncilor
- Aceste Terțe Părți Prestatori (TPP) se împart în două grupe:
  - Prestatori de Servicii de Informare cu privire la Cont - AISP (Account Information Service Providers)
  - Prestatori de Servicii de Inițiere a Plății – PISP (Payment Initiation Service Providers)
- Accesul TTP este posibil doar în cazul conturilor de plăți accesibile online
- În acest mod se dorește ca piața serviciilor de plată să asigure drepturi egale tuturor participanților, în timp ce sunt introduse cerințe de securitate a datelor și de protecție a consumatorilor mult mai puternice

PISP – cine sunt

- PISP sunt instituții de plată care pot iniția operațiuni de plată
- Introducerea PISP reprezintă o modificare majoră în această industrie, întrucât În prezent se utilizează transferurile bancare (SEPA) și cardurile de plată, care sunt însă ambele oferite numai de banca la care este deschis contul bancar sau de emitenți de monedă electronică. Astfel, nu sunt foarte multe opțiuni de plată prin care se pot transfera fonduri dintr-un cont de plăți
- Prin autorizarea ca PISP, comercianții (mari retaileri, precum Amazon) vor putea să obțină acces la datele contului cu acordul clientului. În acest mod, cumpărăturile online vor putea fi efectuate direct de comerciant, în calitate de PISP, pe baza permisiunii date de client, fără să mai fie necesară utilizarea unui card și fără a mai utiliza un alt prestator de servicii de plată (precum paypal)

PISP – cum funcționează



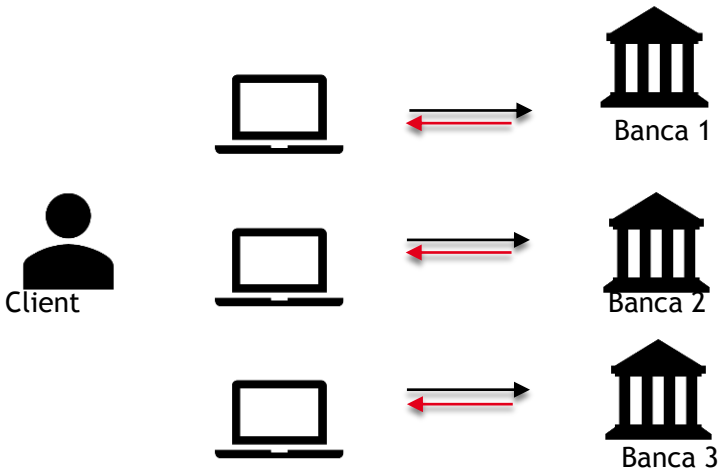
- Clientul – plătitor trebuie să își dea consimțământul explicit pentru executarea unei plăti de către PISP
- PISP nu deține în niciun moment fondurile plătitorului
- PISP se identifică față de bancă și comunică în condiții de securitate ordinul de plată
- Banca furnizează PISP toate informațiile privind inițierea și executarea operațiunii de plată
- Nu este obligatorie existența unei relații contractuale între PISP și bancă

AISP – cine sunt

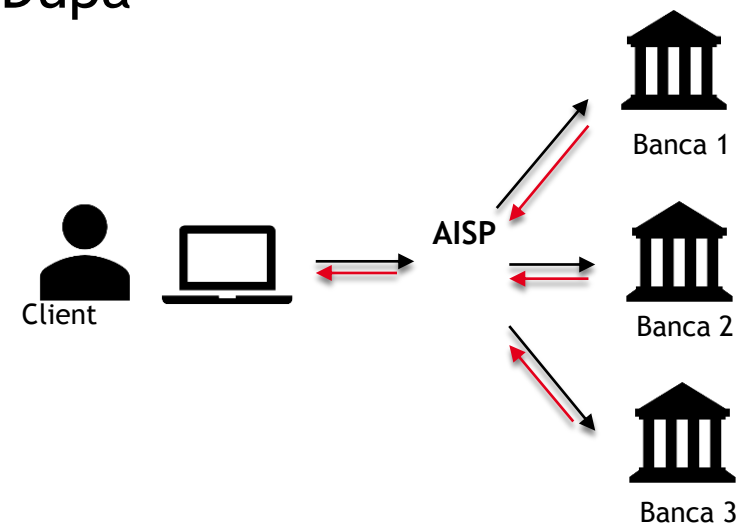
- AISP sunt prestatorii care pot accesa conturile bancare și pot extrage informații cu privire la conturi.
- În cazul clienților care dețin mai multe conturi bancare, aceste schimbări le vor permite să acceseze informațiile cu privire la conturile lor dintr-un singur loc, pe baza serviciilor furnizate de AISP.
- Se are în vedere ca AISP ar putea să analizeze comportamentul clientului și să dea recomandări acestuia pentru a-și eficientiza tranzacțiile: de exemplu în cazul unui client care economisește să recomande contul cu dobânda cea mai avantajoasă
- Cea mai interesantă perspectivă este dată de posibilitatea de a analiza datele și comportamentul clientului în timp real. Momentul când un client face o tranzacție de plată poate fi o oportunitate perfectă pentru marketing direct sau a oferi alte servicii

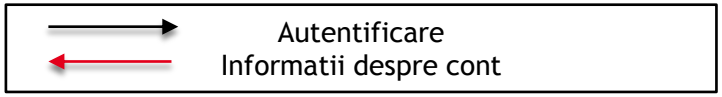
AISP – cum funcționează

Înainte



După





AISP – cum funcționează

- Este necesar ca clientul să-și dea consimțământul explicit pentru ca AISP ca să poata accesa informațiile cu privire la conturile sale
- AISP trebuie să se identifice față de bancă și să comunice în condiții de securitate cu banca și clientul
- AISP nu poate utiliza, accesa sau stoca date în alte scopuri decât pentru prestarea serviciului de informare cu privire la conturi
- Nu este obligatorie existența unei relații contractuale între AISP și bancă

TTP – obligații de reglementare și securitate

- Terții prestatori au obligația să se autorizeze în calitate de prestatori de servicii de plată (PSP). TTP (în calitate de PSP) pot folosi dreptul de stabilire și libertatea de a presta servicii pentru a furniza servicii în alte state membre, pe baza autorizării din statul membru de origine
- PSD2 introduce cerințe sporite cu privire la politica de securitate, măsurile de control a securității și de atenuare a riscurilor în vederea protejării clienților împotriva fraudei și a utilizării ilegale a datelor sensibile și cu caracter personal, pe lângă procedurile de conducere, de gestionare a riscurilor și a procedurilor contabile, precum și mecanismele de control intern
- Aceste cerințe necesită cunoștințe și capacități extinse de gestionare a funcțiilor de management, IT, conformare, risc, juridic și resurse umane. PSD2 nu introduce modificări sub aspectul cerințelor de capital, iar în cazul AISP nu introduce cerințe de capital minim sau fonduri proprii

Plata prin PISP – cine răspunde

- În cazul în care ordinul de plată este inițiat printr-un PISP, banca (în calitate de PSP care oferă servicii de administrare cont) rambursează clientului plătitor, valoarea operațiunii de plată neexecutate sau executate defectuos
- PISP are sarcina de a dovedi că ordinul de plată a fost primit de bancă, precum și că, în limitele competenței sale, operațiunea de plată a fost autentificată, înregistrată corect și nu a fost afectată de o defecțiune tehnică sau de alte deficiențe.
- Dacă PISP este răspunzător pentru neexecutarea sau executarea defectuoasă sau cu întârziere a operațiuni de plată, acesta despăgubește imediat banca pentru pierderile suferite sau sumele plătite în urma rambursării acordate clientului – plătitor.
- Dacă clientul neagă faptul că a autorizat o operațiune de plată executata, PISP sau banca trebuie să furnizeze probe pentru a dovedi frauda sau neglijența gravă din partea clientului
- Dacă PISP sau banca plătitorului nu solicită o autentificare strictă a clienților, plătitorul nu suportă pierderile decât în cazul în care a acționat fraudulos.
- Dacă beneficiarul plății sau banca beneficiarului nu solicită o autentificare strictă a clienților, acesta rambursează prejudiciul către PISP sau banca plătitorului.

Accesul la informații – cine răspunde

- Dat fiind obiectivul de a acorda un acces nerestricționat acestor terțe părți, PSD2 nu impune un cadrul contractual între TTĂ și bănci, astfel încât băncilor nu au control asupra modului în care TTP operează sau se comportă
- Banca poate refuza accesul la un cont de plăți doar dacă are motive justificate în mod obiectiv și susținute de dovezi legate de accesarea neautorizată sau frauduloasă a contului de plăți de către PISP și AISP. Aceste incidente sunt raportate autorității compentente (BNR)
- PSP trebuie să aibă un cadru cu măsuri de atenuare și mecanisme de control adecvate pentru a gestiona riscurile operaționale și de securitate, inclusiv proceduri de gestionare a incidentelor, inclusiv pentru detectarea și clasificarea incidentelor operaționale și de securitate majore
- PSP trebuie sa furnizeze BNR evaluări anuale (cel puțin) cu privire la riscurile operaționale și de securitate și gradul de adecvare al măsurilor și mecanismelor de control la riscuri

GDPR și riscul de securitate

- Accesul la platformele băncilor de către un număr crescând de instituții va crește riscul atacurilor cibernetice
- Referitor la accesul la informațiile cu privire la conturile clienților, noile reglementări europene privind protecția datelor cu caracter personal (GDPR - General Data Privacy Rules) solicită protecția datelor personale precum și obținerea și dovedirea existenței consimțământului dat de client, sub sancțiunea unor amenzi exorbitante
- Astfel, în caz de breșe ale securității platformei sau de atacuri informatice, și băncile pot fi afectate de astfel de incidente, putând fi expuse atât la amenzi cât și unor riscuri reputaționale
- Toți actorii implicați trebuie să se asigure că se aplică măsuri de securitate adecvate pentru a proteja confidențialitate și integritatea datelor sensibile (coduri de acces) și cu caracter personal

PSD 2 și provocările pentru bănci

- Băncile sunt obligate să acord acces la datele clienților și la infrastructura de plăți conform noilor cerințe de reglementare
- Este de așteptat însă ca si băncile să profite de noile reglementări pentru a adăuga aceste servicii în oferta lor de servicii. Această strategie ar trebui să funcționeze dat fiind că băncile au deja know-how-ul pentru efectuarea operațiunilor de plăți
- Se preconizează însă că adăugarea acestui tip nou de servicii să fie doar începutul unei transformări mult mai profunde. Acest lucru se datorează faptului că marjele de pofit din operațiunile de plăți propriu-zise (transferul bancar) devin din ce în ce mai mici

PSD2 – noi oportunități

- Cel mai tipic exemplu de metode de plată care pot deveni populare este conexiunea cu rețelele sociale. Serviciile care permit efectuarea de plăți prin aplicații de mesagerie sunt deja populare în US (precum Venmo)
- Prin deschiderea accesului la conturi, se vor putea crea aplicațiii care să permită plăți instant: vom putea permite whatsapp să se conecteze la contul nostru și cu amprenta noastră să acceptăm o plată de la prieteni. Fără alte complicații, fără IBAN și alte coduri
- Oportunitatea poate consta în transformarea infrastructurii de plăți - *application programming interfaces (APIs)* în platforme (precum facebook) sau market places (precum Amazon)
- În timp ce aceste platforme creează o oportunitate foarte bună de a obține date unice cu privire la comportamentul consumatorilor (și astfel oportunități de vânzare a serviciilor căte clienți prin capturarea metadatelor privind contextul și operațiunilor clienților), GDPR interzice aceste prelucrări fără un consimțământ clar exprimat al consumatorului și limitat atât din punct de vedere al scopului cât și al duratei. În plus, un consumator poate oricând să-și retragă consimțământul și să solicite eliminarea tuturor datelor cu caracter personal în posesia băncii sau al unor terți

PSD 2 – ce va însemna pentru client

- *Operațiuni de plată:* servicii inovative de plată la comercianți, alternative la carduri
- *Noi aplicații:* acces la conturi printr-un singur punct/aplicație
- *Acces la informații:* monitorizarea integrată a conturilor , acces la informații utile precum schimburi valutare, compararea comisioanelor bancare
- *Plăți instant:* acces prin aplicații mobile la mai multe conturi și operatori, plăți de facturi sau transferuri către alți utilizatori (prieteni)

TUCA ZBARCEA
ASOCIATII

Vă mulțumim!

Gabriela ANTON, Partener
gabriela.anton@tuca.ro

Șoseaua Nicolae Titulescu, nr. 4-8
America House, Aripa de Vest, etaj 8
Sector 1, 011141, București, România
T: (40-21) 204 88 90
F: (40-21) 204 88 99
E: office@tuca.ro
www.tuca.ro