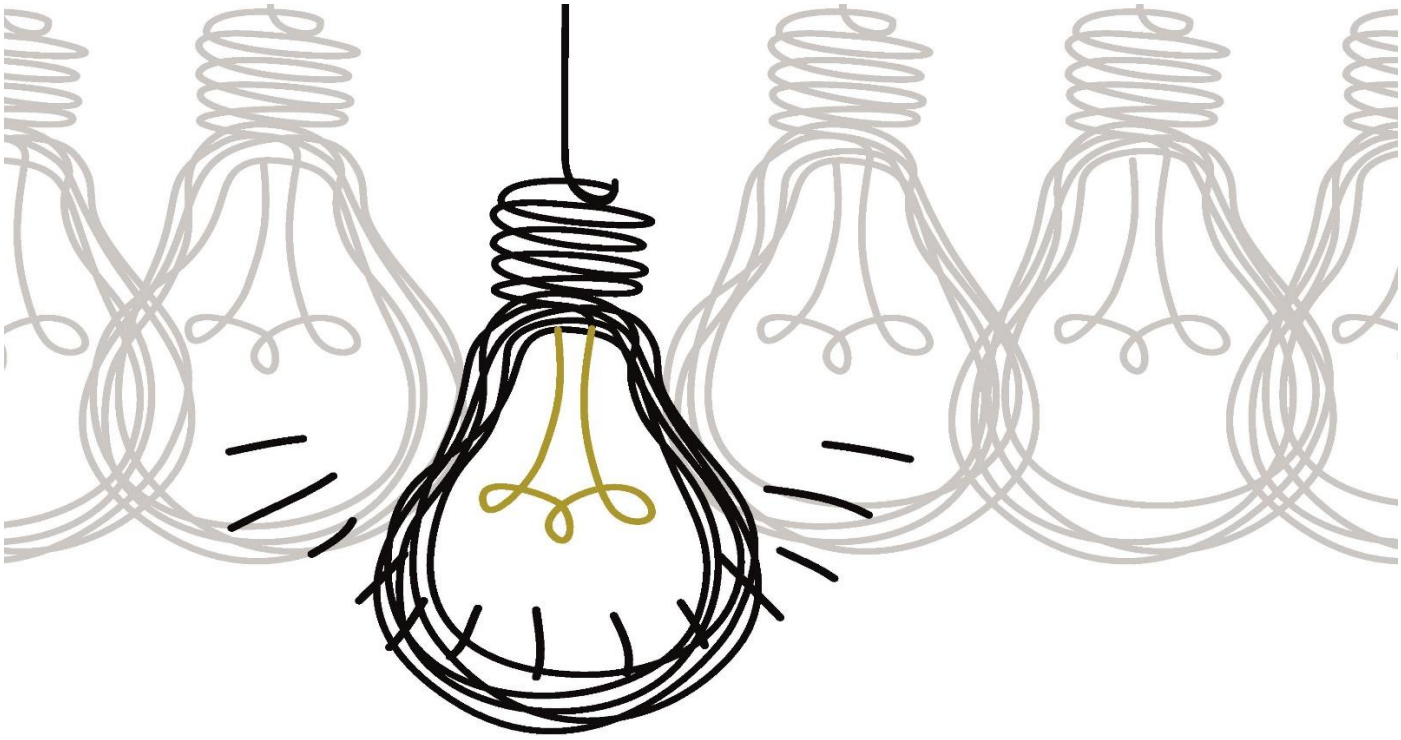


PSD2 és Open Banking

Összefoglaló a 2018. június 22-i PSD2 workshop legfontosabb tanulságairól

2018. június 22-én az ICT Solutions Kft. és az Online Üzleti Informatika Zrt. közös nemzetközi PSD2 workshopot rendezett Visegrádon. A dokumentumban összefoglaljuk a workshop-on elhangzott legérdekesebb információkat és megállapításokat.

Online
BUSINESS TECHNOLOGIES

Bevezetés

A ***PSD2*** és az ún. ***open banking*** manapság a banki konferenciák egyik leggyakrabban tárgyalt témája.

Ez nem véletlen: az információtechnológia fejlődése számos iparágban lehetővé tette új üzleti modellek kialakulását, megváltoztatta a fogyasztói szokásokat, és ezek a változások a FinTech és a BigTech cégeken keresztül beszivárogtak a pénzügyi szolgáltatások piacára is. A PSD2 ezt a folyamatot segíti a szabályozói oldalról, hiszen azért teszi lehetővé FinTech cégek hozzáférését a banki adatbázisokhoz, hogy ezáltal a pénzügyi innováció terjedését segítse elő. Az open banking a jelzett változásokkal összhangban levő együttműködési modell, amelynek keretében a bankok a FinTech cégek bevonásával próbálnak magasabb színvonalú és sokrétűbb szolgáltatásokat nyújtani az ügyfeleiknek.

A 2018. június 22-i PSD2 ***workshop célja*** az volt, hogy a PSD2-höz és az Open Banking-hoz kapcsolódó mélyebb szakmai információkat megosszon, és lehetőséget teremtsen ezen információk megtárgyalására.

A rendezvény a PSD2 és az Open Banking témájában ***360 fokos körképet*** adott, tehát egyaránt foglalkozott a ***PSD2 szabályozási kérdéseivel***, az ***üzleti lehetőségekkel***, és az ***informatikai megvalósítással***. Ezen cél elérése érdekében a téma ismert szakértőit hívtuk meg a rendezvényre: ***Gijs Boudewijn*** az Európai Fizetési Tanács jogi támogatásért felelős tagozatának elnöke ismertette a legfrissebb *szabályozói híreket*, ***Peter Gába*** az Erste csoport open banking kezdeményezésért felelős vezetője adott áttekintést az *open banking üzleti célokra történő felhasználásáról*, míg cégünk részéről ***Németh József*** mutatta be a PSD2 -nek történő megfelelés *informatikai kihívásait*. Az előadásokat *panel beszélgetés* követte, amelynek keretében ***John Basquill*** a Payments Compliance újságírója moderálta a közönség és az előadók közti szakmai párbeszédet.

A rendezvényt megelőzően részletes listát állítottunk össze a bankokat leginkább érdeklő PSD2-es kérdésekről. Ezen témák előzetes feldolgozásába bevontuk a ***Gárdos Mosonyi Tomori Ügyvédi Irodát*** is.

A jelen dokumentumban áttekintjük, hogy mely információkat és megállapításokat tartottuk a legérdekesebbeknek a rendezvényen. Reméljük az összefoglalót hasznosnak találják és találkozunk későbbi rendezvényeinken!

Budapest, 2018.06.28.

Az Online Zrt. csapata

Információk, megállapítások

API sztenderdek

A ***PSD2*** irányelv uniós tagországokban ***történő honosítása késésben van***, így a workshop időpontjában még nem emelte be minden tagország a nemzeti szabályozásába a PSD2 előírásokat. Ez a késlekedés problémát fog okozni az ún. passporting esetében, amikor egy pénzforgalmi szolgáltató egy adott országban megszerzett szolgáltatási engedélyét próbálja honosítani egy másik országban (ld. a PSD2 irányelv 14. cikkét).

Az Európai Bizottság és az Európai Központi Bank 2018 elején olyan ***API értékelő csoport felállítását*** kezdeményezte, amely célja, hogy az öt legnagyobb PSD2 API sztenderd (Open Banking UK, Berlin Group – NextGenPSD2, STET, a szlovák nemzeti API, a lengyel nemzeti API) vizsgálatán keresztül általános iránymutatást adjon a PSD2-höz kapcsolódóan kiadott 2018/389-es számú, erős ügyfél hitelesítéssel és biztonságos kommunikációval foglalkozó szabályozástechnikai sztenderd (RTS SCA) előírásainak való megfelelésre. A csoport megbeszéléseinek emlékeztetői elérhetőek a European Payments Council honlapján (www.europeanpaymentscouncil.eu).

PSD2 API sztenderdek

Az EU a nagy PSD2 API sztenderdeket felülvizsgálja az RTS SCA-nak történő megfelelés szempontjából, de az egységesítés ellenére bankonként különböző API-k kialakítását várhatjuk.

Ennek megfelelően kiemelt szerepük lesz a PSD2 API-k közötti átjárást biztosító technikai szolgáltatóknak.

Ha az európai körképet nézzük, akkor a felsorolt sztenderdek közül a Berlin Group által gondozott ***NextGenPSD2 jelentősége nő***: Németország mellett Olaszország és Hollandia is ezen sztenderd használata felé mozdult el, valamint a francia STET szabványt is harmonizálták a NextGenPSD2-vel.

A felsorolt PSD2 API sztenderdekkel kapcsolatban érdemes megemlíteni, hogy ezek ún. ***API kezdeményezések*** (API initiatives), ami azt jelenti, hogy a sztenderdek ***nem egy konkrét technikai megvalósítást írnak le***, hanem olyan technikai komponenseket határoznak meg, amelyek felhasználásával egy PSD2-es API létrehozható. Ennek logikus következménye, hogy még két NextGenPSD2-nek megfelelő interfész sem lesz technikailag tökéletesen azonos, így várhatóan ***minden PSD2 API*** – még az azonos szabványhoz tartozók is – ***kisebb-nagyobb mértékben különböző lesz***!

Kommunikációs technikai szolgáltatók

Az előző bekezdésekből következően megnő azon cégek jelentősége, amelyek ***átjárást biztosítanak a különböző PSD2 API-k között***. Ezen cégek szolgáltatásának az a lényege, hogy a

PSD2-es tranzakciókat / információ kéréseket küldő pénzforgalmi szolgáltatóknak (angolul Third Party Provider – TPP) csak az ezen szolgáltató által biztosított interfészhez kell kapcsolódniuk, mert a szolgáltatók fogják a banki PSD2 API-khoz történő további illesztéseket elvégezni, ezáltal csillagpontos kommunikációt kialakítva a TPP-k és a bankok között. Felmerül a kérdés, hogy ezen ***technikai szolgáltatóknak minősítteteniük kell-e magukat***, **mint** pénzforgalmi szolgáltató (**TPP**)? Az előzetes elemzésünk szerint ***erre nincs szükség***. A technikai szolgáltatónak és az üzeneteket indító TPP-nek szerződést kell kötnie, amely szerződés szerint a technikai szolgáltató a küldő TPP megbízásából ún. kiszervezett tevékenységet végez a TPP részére. Ennek megfelelően a technikai szolgáltató tevékenységéért harmadik fél irányába a küldő TPP felel, a felelősségi viszonyaikat pedig egymás között létrejött szerződésükben kell rendezniük.

Erős ügyfél-hitelesítés

Erős ügyfél-hitelesítés

A kizárólag átirányításra alapuló erős ügyfél-hitelesítés az EBA 2018. június 13-i véleménye alapján jogszerűen alkalmazható, és nem kötelező egyéb, ügyfél hitelesítési adatok TPP-k részére történő átadására alapuló hitelesítési módszereket alkalmazni.

A PSD2 szolgáltatások egyik sarkalatos eleme az ***erős ügyfél-hitelesítés***. Az RTS SCA végleges változatának 2017. november 27-i publikálásakor felmerült a kérdés, hogy az RTS SCA 32. cikkének 3. bekezdése vajon ***megtiltja-e*** az ***átirányításra alapuló***, az ügyfelek személyi hitelesítési adatainak kiadását nem igénylő hitelesítési módszerek alkalmazását (ilyen pl. az OAuth és az Open ID Connect szabvány)? További kérdésként felmerült, hogy vajon ***kötelező lesz-e*** az ügyfelek személyi hitelesítési adatainak átadásán alapuló ún. ***embedded*** hitelesítés alkalmazása? Az Európai Bankfelügyelet (EBA) 2018. június 13-án kiadott véleménye egyértelműsítette a helyzetet: az ***átirányítás alkalmazása önmagában nem minősül akadályozásnak***, amennyiben nem gátló módon került kialakításra, és az átirányításra alapuló hitelesítés mellett ***nem kötelező más hitelesítési eljárás alkalmazása***.

Sokan gondolják azt, hogy a PSD2 ***erős ügyfél-hitelesítésre*** vonatkozó szabályainak alkalmazása ***csak*** a ***TPP-k API-n keresztüli hozzáférésekor*** kötelező. Ez ***tévedés***. Mivel a PSD2 97. cikke erős ügyfél-hitelesítést ír elő az ügyfél számláinak online elérésekor, ezért az erős ügyfél-hitelesítési szabályok alkalmazása ***kötelező*** az ügyfél által közvetlenül használt ***NetBank és MobilBank megoldásokban is***.

Kivételek az erős ügyfél-hitelesítés alól

Az RTS SCA lehetőséget teremt a bankok számára, hogy az ügyfélélmény javítása érdekében bizonyos ún. ***alacsony kockázatú*** műveletek esetén ***eltekintsenek az erős ügyfél-hitelesítéstől***. Ezen műveletek körét az RTS SCA III. fejezete rögzíti.

A kivételek alkalmazása opcionális a bankok számára és a kivételek alkalmazása komoly változást eredményez a felelősségi viszonyokban, hiszen pl. fizetési műveletek esetében, ha a

fizető fél pénzforgalmi szolgáltatója ***nem alkalmaz erős ügyfél-hitelesítést***, akkor a PSD2 irányelv 74. cikkének 2. pontja szerint ***a fizető fél nem visel semmi fajta veszteséget***, kivéve, ha csalárd módon járt el.

A fenti eljárást és következményeit általában ismerik a bankok, és gyakran találkozunk azzal a véleménnyel, hogy az ***erős-ügyfél hitelesítés alkalmazásáról a bank majd saját hatáskörben***, az ügyfelek előzetes tájékoztatása nélkül, tranzakciónkként, ***egyedileg dönt***. Bár ez alapvetően igaz, de véleményünk szerint a kivételekről tájékoztatni kell az ügyfeleket. Ennek oka, hogy az erős ügyfél-hitelesítés alkalmazása a felelősségi viszonyok változásával jár, amely változásról az ügyfeleket előzetesen tájékoztatni kell, ezért véleményünk szerint a ***kivételkezelés elveit a banki hirdetményekben előzetesen közzé kell tenni***.

A kivételekkel kapcsolatban érdemes megemlíteni, hogy a kivételek között van egy jelenleg mostohán kezelt terület. Az RTS SCA 17. cikke lehetővé teszi a kivételek alkalmazását a ***biztonságos vállalati folyamatok esetében***, akkor, ha az illetékes hatóságok meggyőződtek arról, hogy az alkalmazott eljárások a PSD2 direktívában meghatározott biztonsági szinttel azonos biztonsági szintet tesznek lehetővé. Jelenleg nincs EU-s állásfoglalás arról, hogy ezen felmentést milyen módon és milyen feltételekkel lehet megszerezni, így ezzel kapcsolatban érdemes az illetékes helyi hatóságokhoz fordulni!

Mi számít online módon hozzáférhető számlának?

A PSD2 előírásai szerint a PSD2 API-kon keresztül az ***online módon hozzáférhető számláknak*** kell elérhetőnek lenniük (ld. a PSD2 irányelv 65., 66. és 67. cikkeit). Abban mindenki egyetért, hogy az ügyfelek által a ***netbanki, mobilbanki csatornákon keresztül elérhető számláknak*** ebbe a körbe kell tartozniuk. De mi a helyzet a vállalatoknál használt ún. ***home banki rendszerekkel***, vagy ad abszurdum az ATM-ek szoftvereivel, amelyen keresztül az ügyfél képes távolról hozzáférni a számláihoz? Erre vonatkozóan ***nincs egységes megközelítés***, de pl. a ***brit jogalkotó*** a PSD2 implementálásánál ***a következő megközelítést alkalmazta***: „a technikai megoldástól függetlenül online hozzáférhetőnek minősül minden számla, amelyhez az ügyfél az interneten keresztül hozzáférhet."

API-n keresztül elérhető tranzakciók

Az EBA 2018. június 13-án publikált véleményében egyértelműsítette: minden ügyfél által kezdeményezhető fizetési tranzakciónak (így pl. a csoportos átutalásnak, az értéknapos tranzakcióknak) elérhetőnek kell lennie API-kon keresztül, nem csak az e-commerce hez kapcsolódó egyszeri átutalásoknak.

API-kon keresztül elérhető fizetési tranzakciók köre

A PSD2-es projektek esetében komoly kérdés, hogy a ***PSD2 API-kon keresztül milyen fizetési tranzakciókat*** kell elérhetővé tenni. Ehhez kapcsolódóan ***korábban*** az volt az európai bankok álláspontja, hogy a PSD2 preambulumának 27. és 95. pontjai egyértelműen az e-commerce

támogatására utalnak, így elegendő, ha az ***e-commerce-hez kapcsolódó egyszeri fizetési tranzakciók érhetők*** el a PSD2 API-kon keresztül. Az EBA korábban már említett véleménye erre rácáfolt, mert egyértelműsítette, hogy a PSD2 irányelv definícióinak megfelelően az ügyfél megbízásából indítható ***minden fizetési tranzakció*** (pl. csoportos átutalás, rendszeres átutalás, értéknapos átutalás) elérhető kell legyen a PSD2 API-kon keresztül.

Tartalék megoldások (fallback)

Tartalék megoldások

A screen scraping plus alkalmazása még tartalék (fallback) eljárásként is kockázatos a bankok számára. A megoldás az, hogy a nagy sztenderdek-nek megfelelő jó API-kat kell létrehozni, és felmentést kell szerezni a helyi hatóságoktól a screen scraping plus tartalék megoldásként történő alkalmazása alól.

Az RTS SCA 31. cikke ***két lehetőséget*** kínál a TPP-k hozzáférésének a megoldására. Az egyik lehetőség célra rendelt ún. ***dedikált interfész*** kialakítása, amely a PSD2-es szolgáltatások nyújtására létrehozott, más rendszer-hozzáférési pontoktól elkülönített technikai csatorna. A másik lehetőség az, hogy a bank ugyanazt a hozzáférési csatornát kínálja fel a TPP-knek a PSD2 szolgáltatások elérésére, amely ***csatornát a bank ügyfelei hitelesítésére és a velük történő kommunikációra egyébként használ*** (pl. NetBank, MobilBank). Ha a ***dedikált interfészek nem működnek,*** akkor a netbanki csatornát a bankoknak – a helyi hatóságok felmentésének hiányában – ún. ***fallback*** megoldásként elérhetővé kell tenniük a TPP-k számára.

Ha a TPP-k ez utóbbi csatornát használják a PSD2 szolgáltatások elérésére, akkor a netbanki képernyők funkcióinak használatára és az adatkinyerésre az ún. screen scraping technológiát, pontosabban annak TPP hitelesítéssel kiegészített változatát, a ***screen scraping plus***-t használják.

A ***bankok túlnyomó többsége*** a technikai szempontból biztonságosabb ***dedikált interfészek*** kialakításán gondolkodik, és általában úgy gondolják, hogy az előző bekezdésben említett ***fallback eljárással nincs dolguk***, hiszen a TPP-k ilyenkor önállóan „scrape"-elik a netbankot, és az RTS SCA 33. cikkének 5. pontja szerint ilyenkor ***minden felelősség a TPP-é***. Sajnos ***mindkét pontban tévednek***.

A screen scraping plus alkalmazása során a TPP-ket hitelesíteni kell, így ***a bankoknak módosítani kell a netbankjaikon***, ha fallback eljárásként ezt a csatornát nyitják meg. És bár az RTS SCA 33. cikke valóban megfogalmaz kötelmeket a TPP-k számára, de az alapvető felelősség az ügyfelek felé változatlan, így a ***bankoknak*** elemi ***érdeke***, hogy a ***TPP-k hozzáférését ekkor is szigorúan kontrollálja***.

A megoldás egyszerű. ***Jó PSD2 API-kat kell csinálni*** és a helyi hatóságoknál el kell érni, hogy a bank ***felmentést kapjon*** a screen scraping plus engedélyezése alól (ld. RTS SCA 33. cikkének 6.

pontját). Ha egy bank a korábban említett ***nagy sztenderdek egyikét használja***, akkor ez a felmentés várhatóan egyszerűen megszerezhető lesz.

Üzleti lehetőség - bankok TPP szerepben

A bankok, mint TPP-k

A PSD2 egyik üzleti felhasználási lehetősége, ha a bankok maguk is TPP szolgáltatásokat indítanak. A bankoknak ehhez semmilyen plusz engedély beszerzésére nincs szükségük.

A bankok komolyan foglalkoznak a PSD2 API-k üzleti felhasználásával. Ennek egyik logikus módja, hogy ***a bankok maguk is TPP szolgáltatásokat nyújtanak***. Ezek lehetnek „klasszikus" FinTech szolgáltatások (pl. személyi költségvetés tervezés), de a PSD2 API-kon keresztüli információ kinyerést használhatják a ***hagyományos banki folyamatokban is***, pl. hitel értékesítés során az ügyfél számlakivonatait az ügyfél hozzájárulásával API-n keresztül kérdezik le. Bármely TPP szolgáltatást indításába vágnak is bele, a ***bankok saját jogon nyújthatnak*** online megbízásos átutalási, vagy számlainformációs szolgáltatást, tehát ***semmilyen plusz engedély megszerzésére nincs szükségük***.

Üzleti lehetőség – felhasználhatóak-e más célokra a PSD2-es szolgáltatások során összegyűjtött adatok?

A PSD2 kapcsán szerzett adatokkal kapcsolatos gyakori üzleti kérdés, hogy *a* **megszerzett információkat használhatja-e a bank más célokra**? Szükség van-e a felhasználáshoz az ügyfél hozzájárulására? Ha igen, akkor mennyire konkrét hozzájárulásra van szükség az ügyfelektől? Egyáltalán a GDPR hatályba lépése után lehet-e bármilyen adatközlés/adatfelhasználás ügyfél hozzájárulás nélkül?

A PSD2 irányelv és az RTS SCA ebben a kérdésben egyértelmű: ***ügyfél hozzájárulás hiányában*** az adatokat ***nem szabad felhasználni más szolgáltatások nyújtására***. Ha az ***ügyfél hozzájárul*** az adatai felhasználáshoz, akkor ***már van lehetőség*** az adatok használatára, de a GDPR előírásai szerint a ***hozzájárulás*** kérésének elég ***konkrétnak*** kell lennie, azaz a banknak pontosan meg kell neveznie az ügyfél részére nyújtandó szolgáltatást, valamint azt, hogy a szolgáltatás nyújtásához milyen adatokat fog felhasználni. Ebből következően olyan általános hozzájárulás kérés nem lehetséges, hogy pl. az Ön személyes adatait új termékek kidolgozásához kívánjuk felhasználni. Látni kell ugyanakkor, hogy pl. a termékfejlesztéshez nem szükségesek konkrét személyhez köthető adatok, és az adatállományok ***anonimizálását*** (a személyes adatok elfedését) követően az állományok már felhasználhatóak kutatás fejlesztési célokra.

Ügyfél-hozzájárulás birtokában az is lehetséges, hogy ***több bank közös adatbázist építsen***, de ezen tevékenység folytatása esetén figyelni kell a ***GDPR 26. cikkének*** előírásira és a résztvevő bankoknak adatkezelési szerződést kell kötniük egymással, amelyekben rendezik a feladataikat és felelősségeiket.

Ehhez kapcsolódóan érdemes a figyelmet felhívni arra is, hogy a ***GDPR*** hatályba lépése ***nem azt jelenti***, hogy ettől kezdődően ***minden adatközléshez***, adatfeldolgozáshoz stb. ***az ügyfél hozzájárulása szükséges***. Ez nincs így. Ha pl. ***az adatközlést jogszabály teszi kötelezővé***, akkor az adatközlés ügyfél ***hozzájárulás hiányában is elvégezhető***.

Üzleti lehetőség – Open Banking

Az ***Open Banking*** azt jelenti, hogy egy adott bank a PSD2 előírásain felül szolgáltatások széles körét teszi elérhetővé API-kon keresztül, illetve API-kon keresztül maga is szolgáltatások széles körét veszi igénybe más szolgáltatóknál.

Az Open Banking lehetővé teszi ***szolgáltatási ökoszisztémák*** létrehozását. Ezekben a szolgáltatási ökoszisztémákban az egyes szolgáltatók (pl. biztosítók, kereskedők) az informatikai rendszerek szintjén, ***API-kon keresztül vannak kapcsolatban***, és képesek egymás szolgáltatásainak az elérésére (pl. adott termék értékesítésének a kezdeményezése). Az API-kon keresztül megvalósított kapcsolat segítségével lehetségessé ***válik teljes szolgáltatási értékláncok lefedése***, ahogy a mai nagyvállalatoknál az egyes rendszerek összekapcsolása segítségével lefedhetők teljes vállalati folyamatok. Ezek az ***ökoszisztémák*** azonban ***nem merev struktúrák***, hiszen egy adott szolgáltató a másik ***API-ját*** akár egy ***korábban még nem látott módon***, egy korábban még nem látott szolgáltatás nyújtásához ***használja fel***.

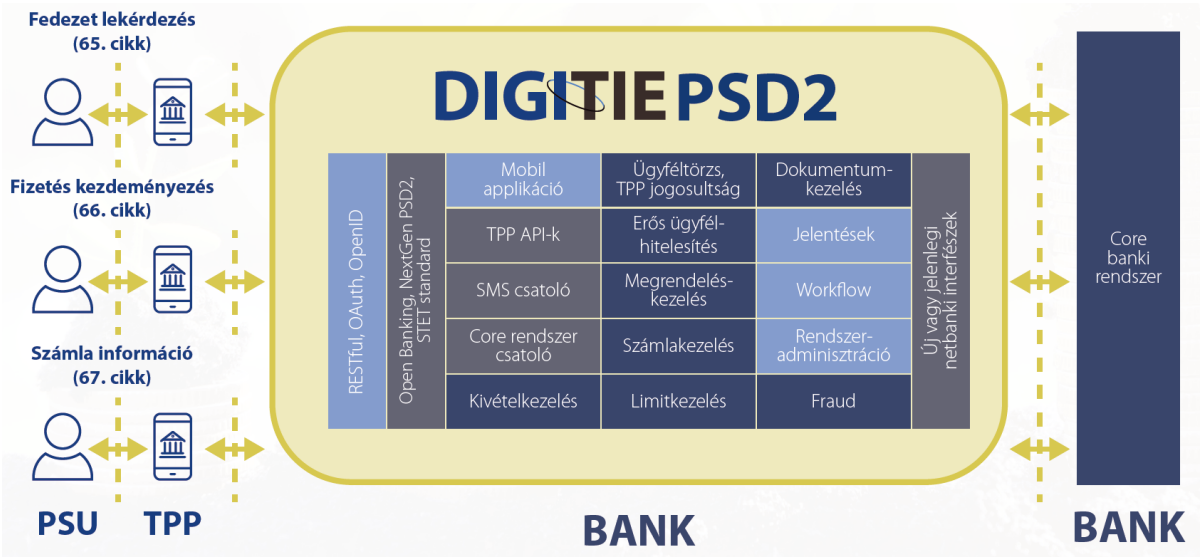
Open Banking

Az Open Banking lehetővé teszi szolgáltatási ökoszisztémák létrehozását. Az ökoszisztéma tagjai az informatikai rendszerek szintjén, API-kon keresztül vannak kapcsolatban, így teljes szolgáltatási értékláncokat lefedhetnek, és képesek egymás szolgáltatásainak az értékesítésére.

Az ökoszisztéma ***üzleti racionalitása*** abban van, hogy az ***API-kat*** megnyitó szervezet szolgáltatásait ***vállalatok széles köre érheti el***, a kapcsolódó vállalatok az elért szolgáltatásokat ***felhasználhatják más szolgáltatások nyújtásához is***, ezáltal a bank a szolgáltatásait ***jóval szélesebb körben „értékesítheti***", mint ahogy arra kizárólag ***saját erőforrásokkal képes lenne***.

Megoldásunk a PSD2-re és az Open Banking-re - DigiTie

Cégünk rendelkezik olyan megoldással, amely választ ad a PSD2 és Open Banking kihívásaira – ez a DigiTie. A ***DigiTie PSD2*** elősegíti a PSD2 előírásainak történő megfelelést.



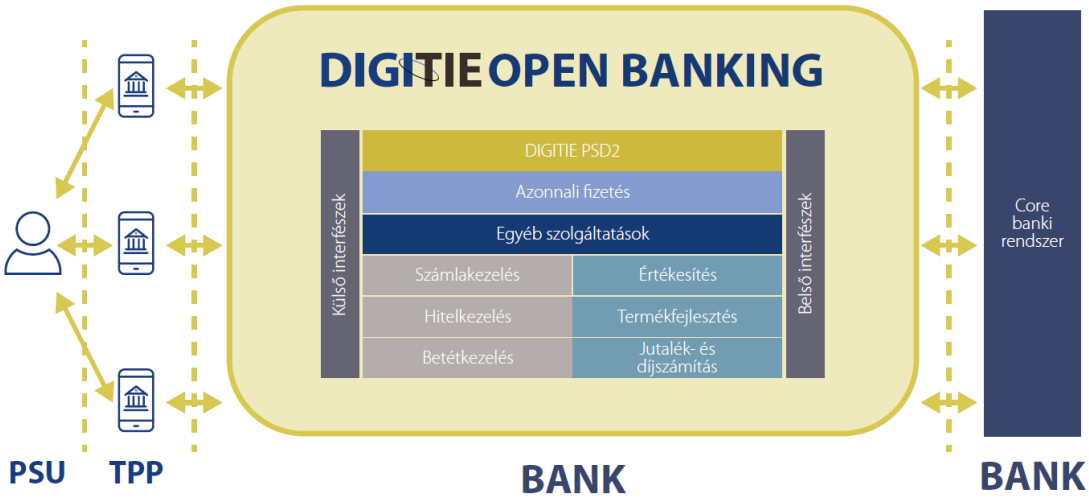
A DigiTie PSD2 a core rendszereket és a FinTech cégeket (TPP, Third Party Provider) összekötő modul, amely 7*24 órában képes a felhasználók (PSU, Payment Service User) megbízásait fogadni, feldolgozni és továbbítani. A modul képes a legelterjedtebb PSD2 szabványok (OpenBankingUK, NextGenPSD2, STET) szerinti kommunikációra. Cégünk a modul fejlesztése során a legkorszerűbb technológiákat alkalmazta: RESTFul interfészek, TLS 1.2 kommunikációs protokoll, OAuth 2.0 és az OpenID Connect 1.0 a hitelesítéshez és engedélyezéshez, X.509 szabvány a tanúsítványokhoz. A modul többféle lehetőséget kínál az erős ügyfél-hitelesítés kezelésére, így például a bankszektorban elterjedt statikus- és SMS-ben elküldött dinamikus jelszavak kombinációját, vagy olyan modern eljárásokat, mint például az ujjlenyomat és a mobilalkalmazás alapú tanúsítás kombinációja. Ezen megoldások iOS és Android platformokon is elérhetőek. A modul ugyanakkor támaszkodhat a bankok által jelenleg használt erős ügyfél-hitelesítési eljárásokra is.

A DigiTie PSD2 a core rendszerekhez többféle módon csatlakozhat: használhatóak a bank meglévő elektronikus csatornáinak (pl. Internet Banking) jelenlegi interfészei, de lehetséges a csatolás új interfészekkel is. Ha a már meglévő interfészeket használjuk, akkor a pénzintézet oldalán csak kisebb fejlesztésekre van szükség.

A modul a törvényi előírásoknak megfelelően képes az erős ügyfél-hitelesítés kihagyására például az alacsony összegű tranzakciók, kisösszegű érintéses fizetések, stb. esetén. A biztonságos működés érdekében a megoldás magában foglalja a limitkezelést, valamint a Fraud komponens részeként az offline megerősítést is. A DigiTie PSD2 célja a törvényi kötelezettségek teljesítése, de később bővíthető.

Míg a DigiTie PSD2 célja a törvényi előírásoknak történő megfelelés biztosítása, addig a ***DigiTie Open Banking*** ezen túlmenően olyan további szolgáltatásokat is kínál, amelyek segítségével a bankok csatlakozhatnak a FinTech ökoszisztémákhoz. A lehetőségek tárháza végtelen: beszélhetünk a FinTech-ektől érkező megbízások alapján 7*24 órában történő hitelezésről, vagy betétszámla nyitásról egy személyi költségvetés tervező szoftver által küldött üzenet alapján.

A DigiTie Open Banking modul, a DigiTie PSD2 összes funkcióját tartalmazza, és lehetőséget teremt új szolgáltatások nyújtására a FinTech-ekkel közösen (lásd a következő képet).



Ezek a funkciók magukban foglalják a testreszabott interfészeket (Open API-kat) a FinTech-ek számára, amelyek különböző technológiákat használhatnak (pl. RESTFUL vagy SOA webszolgáltatás). Míg a DigiTie PSD2 csak néhány szolgáltatás ingyenes nyújtására ad lehetőséget, addig a DigiTie Open Banking segítségével újabb banki szolgáltatások (pl. hitelezés, betétkezelés) üzleti alapokon történő nyújtása válik lehetségessé.

A szolgáltatások 7*24-es támogatása érdekében a DigiTie Open Banking back-office funkciókat nyújt azokra az időszakokra, amikor a core rendszerek offline állapotban vannak, vagyis árnyék-számlavezetést valósít meg. A kiajánlott szolgáltatások üzleti megállapodáson alapuló díjak ellenében érhetőek el, amelyek kezelését a Jutalék- és díjszámítás modul támogatja. Az új csatornák révén lehetőség adódik új termékek értékesítésére is, az Értékesítés és Termékfejlesztés modulok támogatásával.