

Financial Risk&Regulation

**Az MNB új ajánlása a pénzforgalmi szolgáltatások,
a nyílt bankolás kapcsán**

Hírlevél – 2021. augusztus

Az MNB elkötelezett a nyílt bankolás hazai elterjedésének elősegítésében, ezért 2020-ban vezetői körlevélben fordult az érintett piaci szereplőkhöz a fizetés-kezdemenyezési és számlainformációs szolgáltatásokhoz kapcsolódó biztonságos kommunikációval kapcsolatos egyes kérdésekről. Ezt követően 2021-ben vizsgálatot indított a 10 legnagyobb magyar bank nyílt API megoldásának technikai fókuszú felmérésére, továbbá a jogszabályok egységes alkalmazásának elősegítése céljából júliusban kiadta a nyílt bankolás akadályozásáról szóló ajánlást. Augusztusi hírlevelünk ebből az ajánlásból mutat be számos – a fogyasztóvédelem szempontjából különösen lényeges – témakört, hogy szemléltessük az MNB milyen gyakorlatokat tekint akadályozásnak, valamint követendő piaci megoldásnak.

A PSD2 teljeskörű hatályba lépésének elteltével, 2019. szeptember 14 óta a számlavezető pénzforgalmi szolgáltatóknak (továbbiakban: számlavezetők vagy bankok) hozzáférést kell biztosítaniuk alkalmazásprogramozási felületeikhez a számlainformációs és fizetés-kezdemenyezési pénzforgalmi szolgáltatók, azaz harmadik fél szolgáltatók részére. Ennek ellenére a hazai és EU piacon egyaránt megfigyelhető, hogy a „PSD2 nagy újítása, a nyílt bankolás egyelőre csak korlátozottan tudott elterjedni, mivel egyrészt a nemzetközi szabályozás nem elég specifikus a megvalósítandó hozzáférési interfészek vonatkozásában, másrészt pedig a bankok sokféle módon akadályozhatják az új szerepelőket.” – írja az MNB által a napokban publikált [Fizetési Rendszer Jelentés](#). Az „akadályozás” nem feltétlenül szándékos a bankok részéről, hiszen ez fakadhat a szabályozás téves értelmezéséből vagy a minimális megfelelésre való törekvésből is. Az ajánlás ismeretében azonban a bankoknak érdemes áttekinteniük meglévő hozzáférési felületeiket,

mert a jövőben az akadályozónak minősülő megoldások felügyeleti bírságot vonhatnak maguk után.

A nyílt bankolás lehetővé teszi a feltörekvő fintech szereplők számára, hogy a robotsztus banki adatkészlethez való szabályozott hozzáférés lévén új ügyféligényt kielégítő szolgáltatásokkal rukkoljanak elő. [A koronavírus által kialakult megváltozott élethelyzet](#) pedig fogékony környezetet teremtett az előremutató online szolgáltatások iránt. A folyamat a bankok számára is előnyné fordítható, amennyiben a fintech-ekre rivális helyett partnerként tekintenek és felismerik a kisebb, agilis szervezetekkel való együttműködés előnyeit. Amellett, hogy a nyílt bankolás új lehetőségeket tár fel a bankok számára, úgy számtalan bizonytalansággal is együtt járhat. Hogyan kezelendő egy harmadik félen keresztül indított tranzakcióval kapcsolatos ügyfélpanasz? Miként biztosítható a rendszerek nyíltsága amellet, hogy az IT biztonság ne sérüljön? Ilyen és ehhez hasonló kérdésekben nyújthatnak segítséget [PSD2-vel kapcsolatos szolgáltatásaink](#).

Mi az API?

Application Programming Interface magyarul alkalmazásprogramozási felület és annak dokumentációja, amely egy program számára hozzáférést biztosít egy másik rendszer – esetünkben internetbank – utasításkészletéhez anélkül, hogy annak belső működését ismernie kellene a programozónak. A hétköznapi életben leggyakrabban akkor találkozhatunk API-kkal, amikor telefonunkra új alkalmazást telepítünk, és az engedélyt kér pl. az eszköz kamerájának használatához. Ilyenekor az újonnan telepített app a kamera API-ján keresztül kommunikál az azt kezelő szoftverrel.

A harmadik fél szolgáltatók pénzforgalmi szolgáltatásának akadályozása

Az SCAr.¹ 31. cikkre hivatkozva az MNB emlékezteti a pénzforgalmi szolgáltatókat, hogy az API hozzáférést két módon biztosíthatják. Vagy engedélyezik azon interfészeik igénybevételét, amelyeket a pénzforgalmi szolgáltatást igénybe vevők hitelesítésére használnak, vagy célra rendelt interfészt hoznak létre erre a célra. Azok a bankok, amelyek az utóbbi megoldást választották kötelesek biztosítani, hogy ez az interfész ne akadályozza a harmadik fél által nyújtott szolgáltatások igénybevételét.

Többszörös erős ügyfél-hitelesítés

A pénzforgalmi szolgáltató erős ügyfél-hitelesítést köteles alkalmazni, amikor a fizető fél (akár csalásra is alkalmat adó csatornán) távoli/online műveletet hajt végre. A számlavezető pénzforgalmi szolgáltató ezért harmadik fél szolgáltató számára is köteles biztosítani azokat a hitelesítési eljárási módjait, amelyeket saját ügyfelei számára is lehetővé tesz. Ennek értelmében harmadik fél szolgáltatók pénzforgalmi szolgáltatásainak igénybevétele során a számlavezető pénzforgalmi szolgáltató bonyolítja le az erős ügyfél-hitelesítést. Az MNB elvárja, hogy a hitelesítés

- ne álljon a szükségesnél több lépésből,
- ne kérjen szükségtelen vagy felesleges adatokat, valamint
- ne okozzon egyéb módon indokolatlan kellemetlenséget

a harmadik fél szolgáltató pénzforgalmi szolgáltatásait igénybe vevő ügyfélnek, mint amikor közvetlenül fér hozzá a fizetési számlájához (a továbbiakban: többszörös erős ügyfél-hitelesítés).

Az ajánlás szerint többszörös erős ügyfél-hitelesítésnek minősülnek az alábbi esetek:

- a számlainformációs szolgáltatás igénybevétele során a számlavezető által lebonyolított erős ügyfél-hitelesítés több lépésből áll vagy egyéb kellemetlenséget okoz a felhasználónak, mint amikor közvetlenül kérdezi le a számlainformációit,

- a számlavezető nem egyetlen erős ügyfél-hitelesítést alkalmaz a fizetés-kezdeménnyezési szolgáltatás igénybevétele során, holott a harmadik fél szolgáltató minden szükséges fizetési adatot megadott,
- a számlavezető több erős ügyfél-hitelesítést ír elő a fizetés-kezdeménnyezési szolgáltatást nyújtó pénzforgalmi szolgáltatón keresztül kezdeménnyezett fizetési műveletek esetében arra való hivatkozással, hogy az általa biztosított megoldás két különálló erős ügyfél-hitelesítést alkalmaz.

Nem minősül akadályozásnak, ha kellően megalapozott oknál fogva kér többszörös erős ügyfél-hitelesítést a számlavezető (pl. csalásra gyanakszik), ugyanakkor ilyen irányú gyanúját kellően megalapozva alá kell támasztania. Szintén nem meríti ki az akadályozás fogalmát, ha a számlavezető hiányzó adatokra hivatkozva kéri a felhasználót többszöri hitelesítésre. Ilyen esetben ugyanis hitelesítéshez kötött először a hiányos információ lekérése, majd a fizetési megbízás végrehajtása is. Ugyancsak nem minősül akadályozásnak, amennyiben a számlainformációs és a fizetés-kezdeménnyezési szolgáltatás együttes igénybevétele esetén külön két erős ügyfél-hitelesítés szükséges a számlaadatokhoz történő hozzáféréshez majd pedig a fizetési művelet kezdeménnyezéséhez is.


90 napon belüli újra-hitelesítés

A pénzforgalmi szolgáltató saját belátása szerint eltekinthet az erős ügyfél-hitelesítés alkalmazásától, ha teljesíti az SCAr. 2. és 10 cikk (2) bekezdésében foglalt feltételeket és az ügyfél érzékeny fizetési adatok közzététele nélkül fér hozzá:

- egy vagy több megjelölt fizetési számla egyenlegéhez;
- az elmúlt 90 napban egy vagy több megjelölt fizetési számlán keresztül végrehajtott fizetési műveletekhez.

Az MNB követendő gyakorlatnak tartja, ha a számlavezető pénzforgalmi szolgáltató él a kivétellel, ugyanakkor nem számít akadályozásnak, ha nem

¹ A Bizottság (EU) 2018/389 felhatalmazáson alapuló rendelete (2017. november 27.) az (EU) 2015/2366 európai parlamenti és tanácsi irányelvnek az erős ügyfél-hitelesítésre, valamint a közös és biztonságos nyílt kommunikációs standardokra vonatkozó szabályozástechnikai standardok tekintetében történő kiegészítéséről



alkalmazza ezt a lehetőséget. Mindazonáltal, ha saját ügyfelei számára hitelesítés nélkül hozzáférhetővé teszi a fenti információkat, akkor azt megkülönböztetés nélkül minden harmadik fél szolgáltatóval szemben alkalmaznia kell. A számlavezető minezektől csakis csalás, vagy visszaélés alapos gyanúja esetén térhet el.

A fizetési számla ügyfél általi megadásának kikényszerítése

Az MNB jó gyakorlatnak tartja a célra rendelt interfészt létrehozó számlavezető szolgáltatók esetén, ha a harmadik fél szolgáltatásának onboarding folyamata esetén az ügyfél-azonosításhoz kizárólag személyes hitelesítési adatait (pl. internetbanki azonosítót) szükséges manuálisan megadni és elvárja, hogy ne követeljék meg harmadik fél ügyfeleitől a fizetési számlájuk azonosítójának manuális megadását, mert az a Felügyelet értelmezésében akadályozásnak minősül. A számlavezető részéről az MNB jó gyakorlatnak tartja, ha az ügyfél hozzájárulása alapján lehetővé teszi a számlainformációs szolgáltatást nyújtó szolgáltatók számára, hogy az interfészen keresztül lekérjék az ügyfél összes fizetési számlájának listáját. Fizetés-kezdemenyvezési szolgáltatás esetében pedig az ügyfél legördülő lista segítségével választhassa ki a terhelendő fizetési számlát.

További ügyfél-hozzájárulás megkövetelése

Fizetés-kezdemenyvezési és számlainformációs szolgáltatás nyújtásának feltétele az ügyfél kifejezett hozzájárulása, amelyet közvetlenül a harmadik fél számára ad meg. További ügyfél-hozzájárulás megkövetelése a számlavezető részéről már akadályozásnak minősül. Annak ellenére, hogy a számlavezető banknak nincs rálátása a harmadik fél számára megadott hozzájárulásra, nem kötheti ezt az interfész igénybevételeinek feltételévé sem.

Az MNB jó gyakorlatnak tartja, ha a számlavezető internet- vagy mobilbanki felületén lehetőséget biztosít a felhasználó számára, hogy a számladataihoz való hozzáférést letilthassa az általa választott harmadik fél szolgáltatók esetében. Ugyanakkor felszólítja a számlavezető szolgáltatót, hogy kerülje azt a fajta megoldást, amikor a harmadik felek tiltása alapbeállításként általánosan fennáll és azt az ügyfélnek előzetesen engedélyeznie kell, mielőtt harmadik fél szolgáltatását venné igénybe.

Egyéb akadályozó eljárások

Az ajánlás leszögezi, hogy számlainformációs és fizetés-kezdemenyvezési szolgáltatás igénybevételeinek nem lehet feltétele, hogy szerződéses jogviszony álljon fenn a harmadik fél szolgáltató és a számlavezető között. Ugyancsak

nem számíthatnak fel díjat a bankok a célra rendelt hozzáférési interfész használatáért cserébe kivéve, ha a felek az interfész használatán túl egyéb szolgáltatásokra vonatkozóan kívánnak megállapodást kötni.

A bankoknak biztosítaniuk kell az ügyfél számára, hogy harmadik fél szolgáltató igénybevétele során ugyanazokat az erős hitelesítési eljárásokat (pl. biometrikus azonosítást) használhassa, amelyeket olyankor is lehetővé tesz számára, amikor az ügyfél közvetlenül fér hozzá a fizetési számlájához. Technikailag ez azt követeli meg, hogy a bankok

interfészei lehetővé tegyék harmadik fél szolgáltatók számára az általuk végzett erős ügyfél-hitelesítésre történő hagyatkozást. A hitelesítés során az „MNB elvárja a számlavezető pénzforgalmi szolgáltatóktól, hogy azok ne alkalmazzanak szükségtelen vagy felesleges lépéseket és homályos vagy elbátortalanító nyelvezetet” és (pl. telefonos hitelesítés során) az ügyfélnek küldött SMS-ért sem számolhatnak fel magasabb díjat.

Az ajánlás alkalmazása 2021.augusztus 1-jétől elvárt az érintett pénzügyi szervezetektől és ezzel együtt a 2020-ban kiadott vezetői körlevél hatályát veszti.

A nemzetközi szabályozói környezet és a hazai gyakorlat mentén az MNB folyamatosan bővíti és pontosítja elvárásait, mely jelentősen érinti a pénzügyi piac szereplőit, és azok törvényi előírásoknak történő megfelelését. A KPMG szakértői készséggel állnak rendelkezésre a felügyeleti elvárások értelmezésben, implementálásában, és releváns szakmai tanácsokat nyújtanak a megfelelő gyakorlatok kialakításához.

A hírlevél készítésében részt vettek: Szvetlik Kitti, Wieder Gergő.

Kapcsolat:



Rakó Ágnes
partner
M: +36 70 370 1792
E: agnes.rako@kpmg.hu



Szalai Péter
igazgató
M: +36 70 370 1739
E: peter.szalai@kpmg.hu



Wieder Gergő
senior menedzser
M: +36 70 333 1471
E: gergo.wieder@kpmg.hu



Soltész József
menedzser
M: +36 70 370 1766
E: jozsef.soltesz@kpmg.hu

[KPMG.hu](https://www.kpmg.hu)



Az itt megjelölt információk tájékoztató jellegűek, és nem vonatkoznak valamely meghatározott természetes vagy jogi személy, illetve jogi személyiség nélküli szervezet körülményeire. Társaságunk ugyan törekszik pontos és időszere információkat közölni, ennek ellenére nem vállal felelősséget a közölt információk jelenlegi vagy jövőbeli hatályosságáért. Társaságunk nem vállal felelősséget az olyan tevékenységből eredő károkért, amelyek az itt közölt információk felhasználásából erednek, és nélkülözik társaságunknak az adott esetre vonatkozó teljes körű vizsgálatát és azon alapuló megfelelő szaktanácsadást.

A KPMG név, a KPMG logó a KPMG International lajstromozott védjegye.

© 2021 A KPMG Tanácsadó Kft., a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a KPMG International Limited („KPMG International”) angol „private company limited by guarantee” társasághoz kapcsolódó független tagtársaságból álló KPMG globális szervezet tagtársasága. Minden jog fenntartva.