I. A leggyakoribb felhasználói hibákról röviden

A bankszámla-szinkronizáció során előforduló esetleges hibajelenségeket az esetek nagy részében jellemzően végfelhasználói hibák okozzák. A négy leggyakoribb végfelhasználói hiba:

- **Elrontott azonosítás:** nem megfelelően megadott felhasználónév, jelszó vagy második faktor (pl. SMS).
- **Nem megfelelő jogosultságokkal indított lekérdezés:** az adott felhasználónak nincs jogosultsága lekérdezni a kívánt számlainformációkat.
- **Consent felülírás:** több Aggreg8 felhasználónál használták ugyanazokat a netbanki azonosítási adatokat, így csak az utolsóként szinkronizált felhasználónál lesz élő banki oldali meghatalmazás.
- **Elmaradt ISC adás:** a felhasználó a szinkronizációs folyamatot idő előtt megszakította és nem adott hozzájárulást számlainformációinak megosztására az Aggreg8-tól az Aggreg8 Partnere irányába.

A felsorolt hibákról, illetve a könnyen azonosítható, banki oldalról eredő problémákról, valamint az azok elkerülésére vonatkozó javaslatokról lentebb olvasható részletes leírás.

II. A jellemző felhasználói hibákról bővebben

1. Elrontott azonosítás

A felhasználó a banki autentikációs felületre való átirányítást követően helytelen netbanki azonosítót, jelszót vagy második faktoros azonosítót adott meg, vagy nem végezte el a második faktoros azonosítást. Mindig érdemes felhívni a felhasználók figyelmét, hogy a folyamat során az összes szükséges autentikációs lépést végezzék el.

Amennyiben a szinkronizáció végén az Aggreg8 SyncUI felületén az alábbi hibaüzenetek valamelyike jelenik meg, nagy valószínűséggel elrontott azonosítás miatt fut hibára a szinkronizáció:

- *A bank oldalán adott felhatalmazás nem sikeres. Kérjük próbálja újra!*
- *A bank oldalán megadott második faktoros azonosító (pl. SMS) nem volt megfelelő. Kérjük próbálja újra!*

Többszörös 2FA azonosítás

A következő bankoknál különösen érdemes figyelni, hogy a teljes azonosítási folyamaton menjen végig a felhasználó, miután több második faktoros autentikációs lépcső is szükséges a szinkronizációs folyamat sikeres elvégzéséhez:

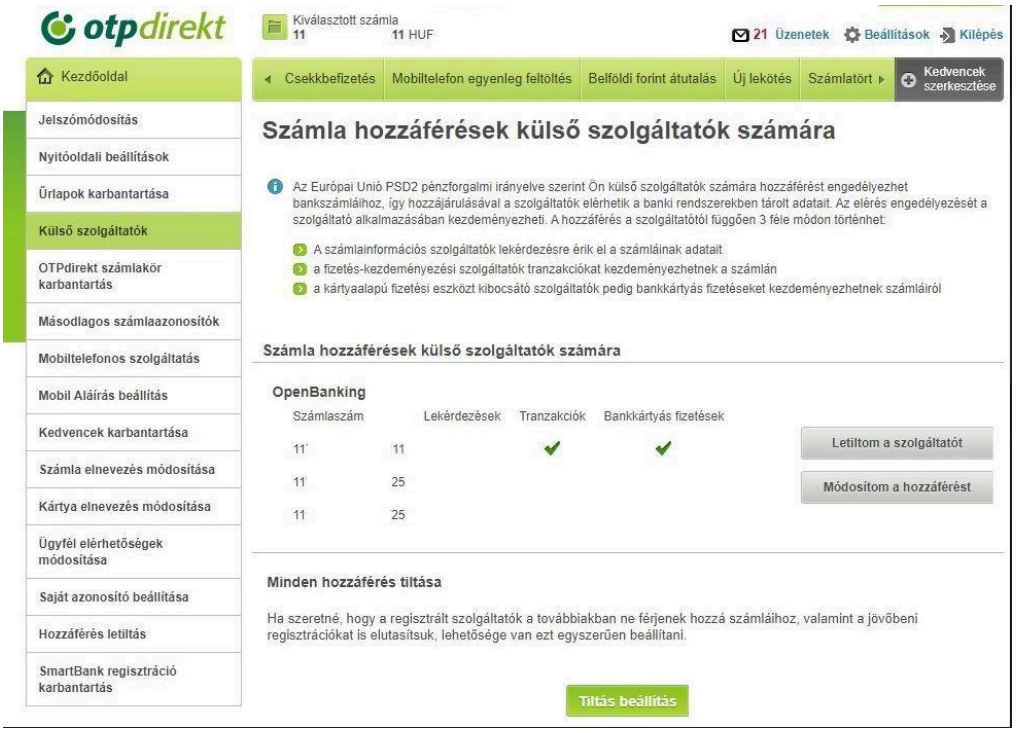
- **K&H Bank**
- **Erste Bank**
- **CIB Bank**
- **MBH (ex-BB)** – (megj: mobiltokenes azonosítás esetén egy 2FA van a folyamatban, de internetbanki azonosítás esetén az MBH (ex-BB) netbanki belépéshez, illetve a számlainformációk megosztásának jóváhagyásához is szükséges második faktor megadása.)

Nem átjárható banki API ágak

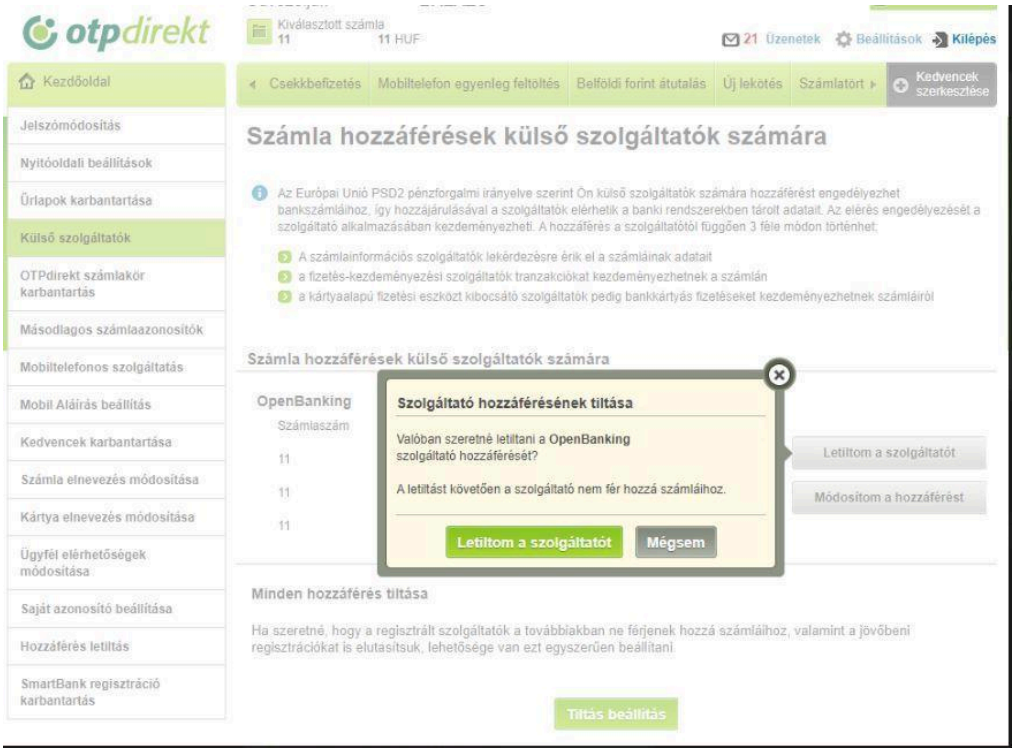
Bizonyos bankoknál előfordulhat, hogy ugyanazon felhasználói csoport (pl. lakossági felhasználók) számára többféle azonosítási mód is elérhető a PSD2 alapú számlainformáció-lekérdezéshez, amelyeket a bank különálló, nem átjárható API ágakon kezel. Ilyen esetben az adott bank által egyedileg elvárt módon kezelhetők a hozzáférések, amelyekről az adott bank saját felületén ad tájékoztatást. Jelenleg az alábbi bank(ok) esetében ismert hasonló működés:

- **OTP**
    - Az OTP Banknál egyaránt lehetőség van az OTP Direkt és Új OTP InternetBank felületeken használt azonosítással meghatalmazást adni a bankszámlainformációk lekérdezésére, a külső szolgáltatók, mint az Aggreg8 számára.
    - Amennyiben egy adott felhasználó már sikeresen adott meghatalmazást külső szolgáltató részére a két azonosítási forma valamelyikével és a következő alkalommal a másik azonosítási móddal szeretne meghatalmazást adni, először a megfelelő internetbanki felületre ellátogatva vissza kell vonnia **minden, külső szolgáltatók számára a korábban adott jóváhagyást.** Ebben az esetben tehát ha él az Aggreg8-en kívül más külső szolgáltató felé adott jóváhagyás is, azt is vissza kell vonni a megfelelő netbanki felületen.
    - Példa: ha először OTP Direkt ágon történt az autentikáció a számlainformációk lekérdezése során, és a felhasználó a következő alkalommal már az Új OTP InternetBanki azonosítási formával szeretne meghatalmazást adni az Aggreg8 számára, először be kell lépnie az OTP Direkt felületére, és visszavonni az Aggreg8, és minden más külső szolgáltató számára korábban adott meghatalmazást. Csak ezt követően tud majd az Új OTP InternetBanki autentikációval sikeres szinkronizációt végezni (illetve igény szerint új meghatalmazásokat kiosztani más külső szolgáltatók felé).

    - A meghatalmazás visszavonásának lépései az **OTP Direkt netbankban:**
        - A bejelentkezést követően a beállítások menüpont alatt a felhasználó kiválasztja a *Külső szolgáltatók* almenüt.

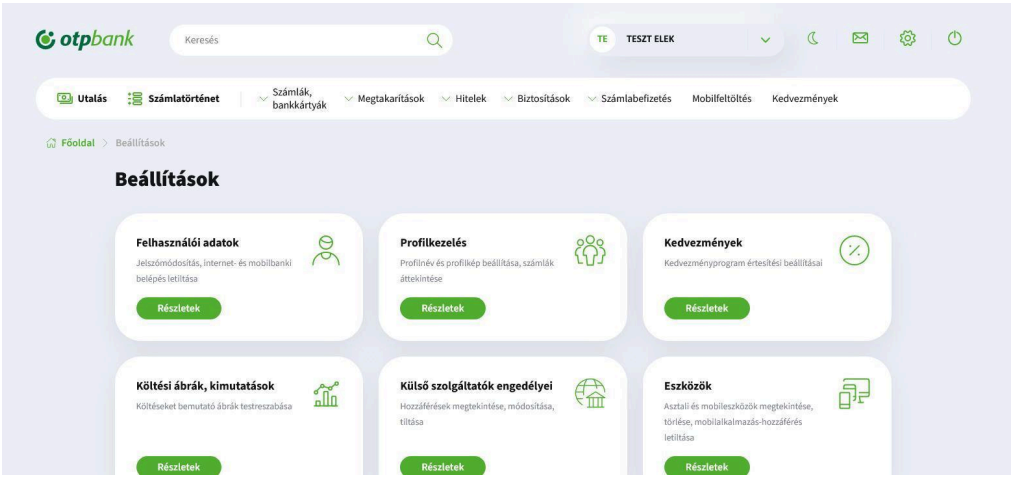


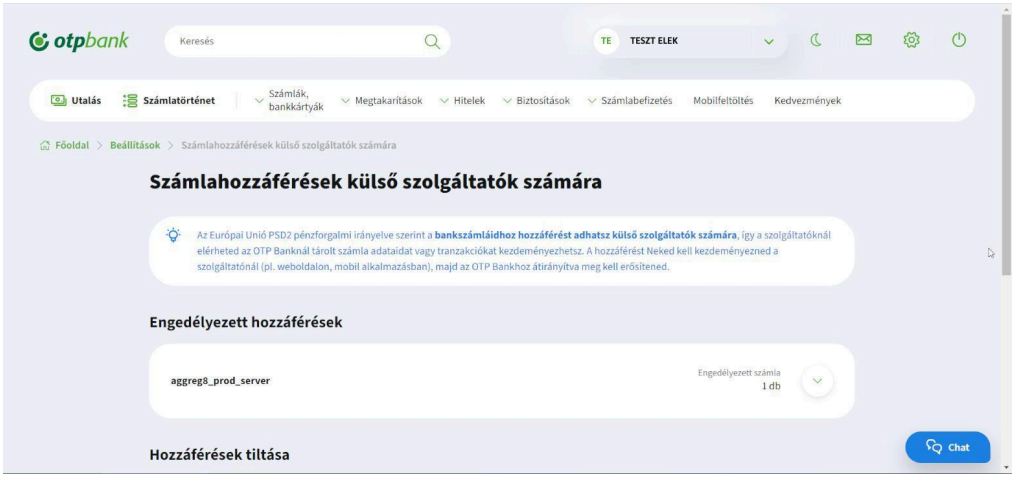
- Itt a felhasználó minden, a listában szereplő szolgáltató esetében a *Letiltom a szolgáltatót* gombra kattint, majd a felugró ablakban ismét a *Letiltom a szolgáltatót* lehetőséget választja (a képernyőképen látható példán egy fiktív „OpenBanking” szolgáltató szerepel).



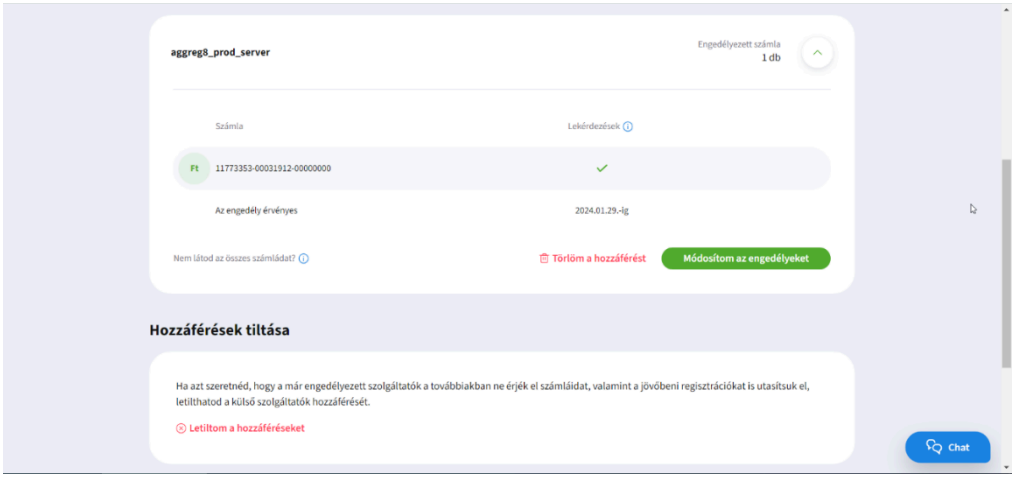
- Ezt követően az OTP Direkt ágon adott meghatalmazás megszűnik, és lehetőség van az Új OTP InternetBank ágon történő autentikációra egy új szinkronizáció során.

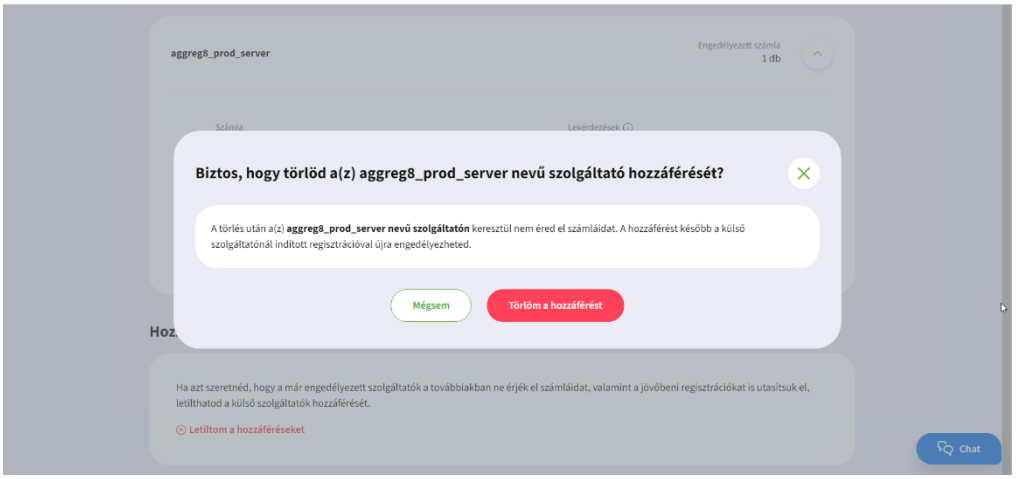
- A meghatalmazás visszavonásának lépései az **Új OTP InternetBankban:**
  - A bejelentkezést követően a beállítások menüpont alatt a felhasználó kiválasztja a *Külső szolgáltatók engedélyei* almenüt.





- Itt a felhasználó minden, a listában szereplő szolgáltató esetében szolgáltató kiválasztása után, a *Törlöm a hozzáférést* gombra kattint, majd a felugró ablakban ismét a *Törlöm a hozzáférést* lehetőséget választja.





- Ezt követően az Új OTP InternetBank ágon adott meghatalmazás megszűnik, és lehetőség van az OTP Direkt ágon történő autentikációra egy új szinkronizáció során.

- **Fontos:**
  - Amennyiben a felhasználó azonosítási formát vált, a szinkronizáció során a még Aggreg8 oldalon bekért internetbanki azonosító esetében is az új azonosítási ághoz/formához tartozó értéket kell megadnia (OTP Direkt esetében OTP Direkt azonosító, Új OTP InternetBank esetében email cím).
  - Amennyiben a felhasználó azonosítási formát vált, az Aggreg8 oldalon új banki kapcsolatként jelenik majd meg, azaz a korábban használt azonosítási formával lekérdezett számlatörténetet a rendszer nem pontozza össze az új azonosítási formával végzett szinkronizáció során kapott adatokkal, ez Aggreg8 üzleti partnerének oldalán a tranzakciók multiplikálódásának észlelését eredményezheti, amit az ISC objektum consentedAccount mezőjét figyelembe véve tudnak kiszűrni (amennyiben ugyanaz az IBAN tartozik több accountID-hez akkor érdemes ilyen típusú tranzakció multiplikálódásra gyanakodni).

2. Nem megfelelő jogosultságokkal indított lekérdezés

„Alacsony" netbanki felhasználói jogosultsági szint

Tapasztalataink alapján az API-n történő adatátadás engedélyezését több bank is „tranzakciónak" tekinti, ezért annak ellenére, hogy nem zajlik valós pénzügyi tranzakció, ezeknél a bankoknál a PSD2 API csatornán keresztül történő számlainformáció lekérdezésre jogosító felhatalmazás megadásához is a tranzakció indításához szükséges jogosultság szükséges.

Bizonyos bankok esetében ez a gyakorlat mind a lakossági és mind a vállalati számlák számlainformációinak elérését "korlátozza", utóbbi esetben pedig a legtöbbször ez azt feltételezi, hogy egy, a számlainformációk lekérdezésére szóló felhatalmazás jóváhagyásához "10 pontos" banki aláírási jogosultság szükséges.

A következő táblázatban bemutatjuk, hogy (2024. 07. 30-i állapot szerint) az egyes bankoknál a korábbi tapasztalataink alapján a felhasználóknak milyen banki jogosultsággal kell rendelkeznie a PSD2 alapú számlainformációs szolgáltatás használatához. Fontos kiemelni, hogy az alábbi lista a részben a saját, részben a szerződött üzleti partnereink tapasztalatai alapján került elkészítésre. (Megj: A dokumentum továbbá tartalmaz további, banki autentikációhoz kapcsolódó bankspecifikus információkat is.)

Megj.: ez a működés az Aggerg8 megítélése szerint szembe megy az EU-s PSD2 direktívában foglaltakkal, a bankoknak ugyanis a PSD2 API-kon is az internetbankival azonos adattartalmat, az internetbankival azonos feltételekkel és autentikációval kell biztosítaniuk a felhasználók számára. Ebben az esetben ugyanakkor, bár egy megtekintői jogkörrel rendelkező netbanki felhasználó az internetbanki felületeken láthatja a számla- és tranzakcióadatokat, PSD2 API-n keresztül nem fér hozzá ugyanehhez az információhoz. Az Aggreg8 ebben az ügyben (is) aktívan presszionálja a bankokat a törvényi elvárásokhoz igazodó működés irányába.

Amennyiben a szinkronizáció végén az Aggreg8 SyncUI felületén az alábbi hibaüzenet jelenik meg, nagy valószínűséggel jogosultsági probléma miatt fut hibára a szinkronizáció:

- *A felhatalmazás megerősítéséhez teljes banki aláírási jogosultság szükséges. Kérjük új próbálkozás esetén ilyen jogosultsággal rendelkező felhasználóval erősítsék meg a felhatalmazást.*

I. Magyar bankok

Bank neve	PSD2 API csatorna használatához szükséges minimum banki jogosultság	Egyéb azonosításhoz kapcsolódó információk
CIB Business online	Tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	Vica azonosítás a tapasztalatunk alapján nem támogatott
CIB Internetbank	Tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	-
Erste George	Tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	-
Gránit	Megtekintői jogosultság	-
K&H	Tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	-
Magnet	Megtekintői jogosultság	-
MBH(ex-BB) lakossági	Tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	A felhatalmazást (decoupled módon) az internetbanki felületen / vagy a banki mobilalkalmazásban kell megkeresni és aláírni
MBH(ex-BB) vállalati	Az MBH (exBB) vállalati API ág megszűnt, a számlák innen az MBH (exMKB) számlavezető rendszerbe kerültek átköltöztetésre. MKB vállalati API ágon kérdezhető le	
MBH(ex-MKB) lakossági	Megtekintői jogosultság	Amennyiben az adott számla csak az asztali Direct Bank kliensből érhető el, ahhoz a bank nem biztosít PSD2 API kapcsolatot. Utóbbi használatához ebben az esetben netbanki jogosultság igénylése szükséges a banktól.
MBH(ex-MKB) vállalati	A bank tájékoztatása alapján rögzítői jogosultság szükséges, viszont a tapasztalatok alapján úgy látjuk elegendő megtekintési jogosultság is	
MBH(ex-Takarék)	Megtekintői jogosultság	Vica azonosítás nem támogatott

OTP	Jelenleg megtekintői jogosultság is elég (azonban a bank kommunikációja alapján ez a jövőben megváltozhat)	Vállalati számlákat csak az OTPdirekt ágon lehet lekérdezni
Raiffeisen	Valószínűleg tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	Vállalati számláknál jellemzően külön engedélyeztetni kell a PSD2 csatorna használatát a bankfiókban
UniCredit	Valószínűleg rögzítői jogosultság	Amennyiben az adott számla csak az asztali Spectra kliensből érhető el, ahhoz a bank nem biztosít PSD2 API kapcsolatot. Utóbbi használatához Spectranet netbanki jogosultság igénylése szükséges a banktól.
UniCredit SpectraNet	Megtekintői jogosultság	-

II. Szlovák bankok

Bank neve	Jelenlegi információink alapján	Egyéb
CSOB Banka	tranzakció indításához szükséges jogosultság (10 pontos aláírási jogosultság)	-
Fio Banka	Megtekintői jogosultság	-
Slovenská Sporiteľna	Megtekintői jogosultság	-
Tatra Banka	Megtekintői jogosultság	-
UniCredit	Megtekintői jogosultság	-
VÚB Banka	Megtekintői jogosultság	

III. Román bankok

Bank neve	Jelenlegi információink alapján	Egyéb
Banca Transilvania	Megtekintői jogosultság	-
UniCredit	Megtekintői jogosultság	-
BCR	Megtekintői jogosultság	-
Raiffeisen	Megtekintői jogosultság	-
ING	Megtekintői jogosultság	-

Asztali kliensprogramra korlátozott hozzáférés

Bizonyos bankoknál előfordulhat, hogy nem biztosítanak PSD2 API hozzáférést abban az esetben, ha az adott bankszámlához a felhasználó nem rendelkezik netbanki hozzáféréssel, csak asztali szoftverből (vastagkliensből) tudja azt kezelni. Jelenleg az alábbi bank(ok) esetében ismert hasonló működés:

- **UniCredit Bank**: az UniCredit bank esetében, amennyiben az adott számla csak az asztali Spectra kliensből érhető el, ahhoz a bank nem biztosít PSD2 API kapcsolatot. Utóbbi használatához Spectranet netbanki jogosultság igénylése szükséges a banktól.
- **MBH (ex-MKB):** az MBH (ex-MKB) API ág esetében, amennyiben az adott számla csak az asztali Direct Bank kliensből érhető el, ahhoz a bank nem biztosít PSD2 API kapcsolatot. Utóbbi használatához netbanki jogosultság igénylése szükséges a banktól.

„Opt-in" PSD2 API csatorna

Bizonyos bankoknál előfordulhat, hogy a PSD2 API csatornát az első használat előtt külön engedélyeztetni kell a felhasználó banki kapcsolattartójával. A kezdeti bekapcsolást követően a csatorna aztán az engedély visszavonásáig zavartalanul használható. Jelenleg az alábbi bank(ok) esetében ismert hasonló működés:

- **Raiffeisen Bank (vállalati számlák esetében)**

  Megj.: ez a működés az Aggerg8 megítélése szerint szembe megy az EU-s PSD2 direktívában foglaltakkal, a bankoknak ugyanis a PSD2 API-kon is az internetbankival azonos adattartalmat, az internetbankival azonos feltételekkel és autentikációval kell biztosítaniuk a felhasználók számára. Ebben az esetben ugyanakkor, bár az adott felhasználónak egyébként van online hozzáférése a számla- és tranzakcióadatokhoz, PSD2 API-n keresztül alapértelmezetten nem fér hozzá ugyanehhez az információhoz, „opt-in" jelleggel tudja hozzá megszerezni a hozzáférést. Az Aggreg8 ebben az ügyben (is) aktívan presszionálja a bankokat a törvényi elvárásokhoz igazodó működés irányába.

3. Consent felülírás

Banki oldalon jellemzően egy külső szolgáltató (pl. az Aggreg8) felé, egy netbanki felhasználó, egyszerre egy darab „élő" banki oldali számlainformáció-lekérdezési meghatalmazást (consentet) tarthat fenn párhuzamosan.

Consent felülírás több Aggreg8 felhasználóval

Ennek megfelelően, ha két különálló Aggreg8 felhasználóval, ugyanannak a netbanki felhasználónak az adataival (netbanki azonosító + jelszó + második faktor) azonosítva történik egymást követően két szinkronizáció, csak a banki oldalon utoljára kiadott consent lesz érvényes, az elsőként szinkronizáló Aggreg8 felhasználó banki oldali consentje felülíródik és érvénytelen lesz. A felhatalmazás felülírása azt eredményezi, hogy az adott banki kapcsolat vonatkozásában az Aggreg8 (bár még a felhatalmazásadástól kezdődően nem múlt el a consent eredeti érvényességi idejét jelentő 180 nap) nem lesz képes passzív lekérdezések keretében a számlainformációk napi 4x történő lekérdezésére (csak egy újabb felhasználó által banki átirányítás keretében adott új felhatalmazás alapján).

Mindig érdemes tehát figyelni, hogy egy netbanki felhasználó adatait használva csak egy Aggreg8 felhasználóval történjen szinkronizáció, ellenkező esetben fennáll a consent felülírás veszélye. Ennél a „korlátozásnál" figyelembe kell venni az összes Aggreg8 által biztosított környezeten adott párhuzamos felhatalmazásokat is (azaz például ugyanarra a netbanki felhasználóra Aggreg8 SANDBOX környezetén indított szinkronizálás felül fogja írni a korábban Aggreg8 PROD környezeten az adott felhasználóra vonatkozóan adott felhatalmazást.)

Consent felülírás Aggreg8 oldalon hibásan megadott netbanki azonosítóval

Előfordulhat, hogy egy adott Aggreg8 felhasználó új add-bank flowt indít (új banki kapcsolatot hoz létre), amelynek során egy korábban már szinkronizált bankszámla adatait kérdezi le ismét, ugyanazon netbanki felhasználó adatait használva a banki oldali azonosításhoz.

Amennyiben a folyamat során a felhasználó az Aggreg8 és a bank oldalán is helyesen ad meg minden adatot, a végeredmény egyenértékű lesz egy consent-extend flow (azaz consent/meghatalmazás hosszabbítás) eredményével, vagyis az adott banki kapcsolatra újabb 180 napon keresztül lesz élő consent banki oldalon.

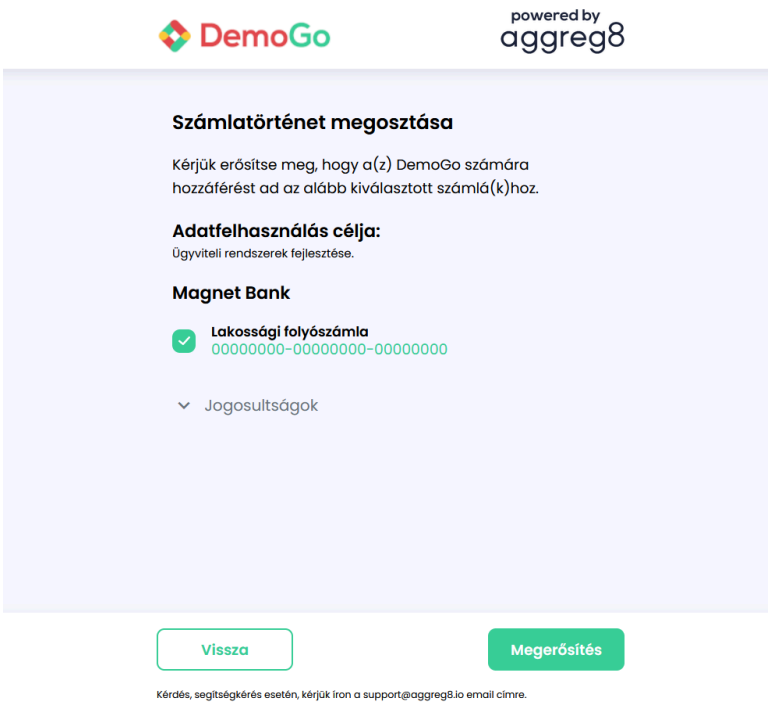
Ha viszont a felhasználó a folyamat során még az Aggreg8 felületén hibásan, vagy legalábbis a korábban alkalmazottól eltérő módon adja meg netbanki azonosítóját (olyan bankok esetén, amelyeknél azt előre megadni szükséges), a folyamat végén egy új banki kapcsolat fog létrejönni. Ehhez az új kapcsolathoz tartozik majd az élő banki oldali consent, a korábbi kapcsolathoz tartozó számlatörténet pedig nem fog frissülni.

4. Elmaradt ISC adás

Új banki kapcsolat létrehozásakor mindig figyelni kell rá, hogy a felhasználó a teljes szinkronizációs és információmegosztási folyamaton haladjon végig. Ezen folyamat utolsó lépése az ISC (Information Sharing Consent), azaz az információmegosztási hozzájárulás megadása, amelynek keretében a felhasználó hozzájárul, hogy az Aggreg8-nél tárolt banki adatait az Aggreg8 Partnerével megossza.

Amennyiben a megosztás nem történik meg, a szinkronizáció maga hiába volt sikeres, a lekérdezett számlainformációk azonban csak az Aggreg8 adatbázisában lesznek jelen, azokra az Aggreg8 Partnere a GDPR consent hiányában nem fog tudni bekérdezni.

Az ISC adás lépése az alábbi képernyőképen látható:



III. Nem felhasználói oldalról eredő hibák

1. Hálózati probléma

Hálózati probléma a bank, a felhasználó, az Aggreg8, vagy az Aggreg8 Partnere oldalán is előfordulhat, az internetszolgáltató, vagy egyéb az adott fél közvetlen hatáskörén kívül eső hálózati infrastruktúrában adódó ideiglenes hiba miatt.

Amennyiben a szinkronizáció során az Aggreg8 SyncUI felületén az alábbi hibaüzenetek valamelyike jelenik meg, nagy valószínűséggel hálózati probléma miatt fut hibára a szinkronizáció:

- *A kapcsolat megszakadt. Kérjük próbálja újra!*
- *Időtúllépés miatt a kapcsolat megszakadt. Kérjük próbálja újra!*
  (Megj.: ez utóbbi hibaüzenet nem csak hálózati hibára utalhat, előfordulhat például, hogy az adott banki szerverektől nem érkezett válasz időben az Aggreg8 által indított hívásra, valamilyen belső, banki probléma miatt).

2. Banki oldalon megváltozó, korábban könyveltként átadott tranzakcióadatok

Előfordulhat, hogy egy-egy bank bizonyos idő után megváltozott adattartalommal kezd átadni korábban már sikeresen lekérdezett, könyvelt tranzakciókat. Az Aggreg8 számos különböző logikával rendelkezik, amely ilyen esetekben, adott mintázatok és információtartalom alapján a hasonló banki oldali jelenségeket is ki tudja szűrni, és összepárosítani a megváltozott tranzakciót annak eredeti variánsával (elkerülve a potenciális duplikációkat).

Vannak ugyanakkor esetek, mikor egy-egy könyvelt tranzakció korábban Aggreg8 oldalon még nem tapasztalt módon változik meg, így az aktuálisan létező/működő logikák nem tudják elvégezni az összepárosítást. Amennyiben az Aggreg8 ilyen banki oldali anomáliát tapasztal, automatikusan hibára futtatja a szinkronizációt, így biztosítva, hogy nem keletkeznek duplikációk, fals adatok az adatbázisban.

Ilyen esetekben az addig nem ismert adatváltozási mintázatot az Aggreg8 megvizsgálja, majd új logikát fejleszt, amellyel az újonnan megismert banki oldali jelenség is kiküszöbölhető.

Amennyiben a szinkronizáció végén az Aggreg8 SyncUI felületén az alábbi hibaüzenet jelenik meg, banki oldalon megváltozó, könyvelt tranzakcióadatok miatt fut hibára a szinkronizáció:

- *A banktól frissen kapott és korábban lekérdezett információk között eltérést tapasztalunk, ezért a szinkronizálás sikertelen.*