RAIFFEISEN PAY
INNOVATÍV FIZETÉSI SZOLGÁLTATÁS

Egységes Adatbeviteli Megoldások
QR/NFC/Deeplink

verzió 1.5

Tartalomjegyzék

1. Azonnali Fizetési Rendszer 2.0

1.1. Bevezetés

Az Azonnali Fizetési Rendszert szabályozó MNB rendelet értelmében a pénzforgalmi szolgáltatóknak kötelező a mobilbanki alkalmazásokban a QR-kód, NFC és deeplinkes fizetés (továbbiakban Egységes Adatbeviteli Megoldások – EAM) lehetőségének megteremtése egy egységes, kötelezően alkalmazandó szabvány alapján.

A Raiffeisen Bank ezen fizetési szolgáltatásokra építve egy kereskedő oldali megoldást dolgozott ki a vállalati szegmens részére, mely lehetővé teszi az elfogadók számára kártya-helyettesítő, azonnali fizetési megoldás lebonyolítását szabványos internetes API kapcsolaton keresztül.

Jelen dokumentum célja az egységes adatbeviteli megoldások (EAM) gyakorlati alkalmazásához szükséges technikai követelmények összefoglalása.

Az Aggregátor (Innopay Zrt.) a GIRO Zrt-vel kötött kiszervezési szerződés alapján végzi az egységes adatbeviteli kódok létrehozását, valamint a fizetési megbízások teljesüléséről szóló státuszinformáció továbbítását, és ehhez kapcsolódóan, de ezen túlmutatóan egyeztetési és egyéb szolgáltatásokat nyújt.

A Sub-Aggregátorok (jelen esetben Raiffeisen Bank) szerződött partnereik számára lehetőséget adnak azonnali mobilfizetési megbízások a tranzakcióra és a Kedvezményezettre vonatkozó adatainak egységes adatbeviteli kódok formájában a fizető felek mobileszközére, mint készpénzhelyettesítő fizetési eszközre történő átadásához.

1.2. Azonnali átutalási megbízás benyújtásához alkalmazható egységes adatbeviteli megoldások

1. **QR-kódos vásárlás két fajtája:** mobilbanki alkalmazáson belül történik a QR-kód beolvasása vagy a többfunkciós eszköz (mobiltelefon, tablet stb.) gyári kamerájának szoftvere olvassa be a QR-kódot, ami az előre telepített mobilfizetési alkalmazást elindítja. QR-kód az ISO/IEC 18004 szabvány szerint meghatározott kód.

   A QR-kód alapú adatbeviteli megoldást az alábbi technikai tartalommal kell kialakítani:

   - a kód maximális mérete 24-es, azaz 113 × 113 egység, valamint körülötte 4 egység üres helyet ki kell hagyni;
   - a QR-kód hibajavítási képessége minimum M szintű (15 százalékos veszteség visszaállítási képesség).

2. **Deeplinkkel kezdeményezett azonnali fizetés:** nem szükséges kamerás leolvasás, mert a deeplink (mélyhivatkozás alapú adatbeviteli eljárás) elindítja a mobilfizetési alkalmazást és az előkészített fizetési kezdeményezési űrlapot kell csak jóváhagynia a fizető félnek. A deeplink technológia leírását az MNB 35/2017. (XII.14.) MNB (MNB rendelet) rendeletének 5. számú melléklete tartalmazza.

3. **NFC-n kezdeményezett azonnali fizetés:** Az RFID (Radio Frequency Identification) szabványokra épülő, 13,56 MHz-en kommunikáló ISO/IEC 14443 technológiai szabványban ismertetett rövid hatótávú kommunikációs technológia. Azonnali átutalási megbízás benyújtását támogató kód kibocsátására a szabványban rögzített aktív kommunikációs mód alkalmazható.

A fizetési séma három féle adatbeviteli, adatátadási módszerére a továbbiakban, mint **egységes adatbeviteli megoldás** hivatkozik a dokumentum. Az egységes adatbeviteli megoldás alatt minden esetben egyszerre mindhárom adatbeviteli módot (QR-kód, NFC, deeplink) kell érteni.

1.3. A szolgáltatás új szereplői

Aggregátor

A GIRO egyetlen Aggregátorral szerződött, amely az egységes adatbeviteli megoldás útján kezdeményezett fizetési tranzakciók esetében biztosítja az átutaláshoz szükséges QR-kód zárt rendszerben történő előállítását és ellenőrzését. Továbbá gondoskodik a fizetésforgalmi státuszok továbbításáról a fizetési kezdeményező felé. Ennek megvalósításához a GIRO-nak nyilván kell tartania a regisztrált Aggregátort és számára továbbítania kell a fizető fél pénzforgalmi szolgáltatója által indított visszajelző üzenetet Az Aggregátor ezt az üzenetet fogja továbbítani a tranzakcióhoz tartozó sub-aggregátor részére.

Sub-aggregátor

Az Aggregátor nem közvetlenül szerződik a kereskedővel vagy szolgáltatóval, hanem úgynevezett sub-aggregátor szolgáltatóval állapodik meg. Ekkor a kereskedők a sub-aggregátorral szerződnek, aki garantálja a kereskedők kérései alapján a kereskedők felé az egységes adatbeviteli megoldás létrehozását és továbbítja a kereskedők számára a visszajelző üzeneteket, továbbá a kereskedők felé az elszámolást is végezheti. **Jelen esetben a Raiffeisen Bank veszi fel ezt a szerepet.**

2. Az egységes adatbeviteli megoldás működésének bemutatása

Az egységes adatbeviteli megoldás – tágabb értelemben – olyan fizetési kérelem, ami a kedvezményezett és a fizető eszközei közötti közvetlen adatátadás útján kerül közlésre és csak a kedvezményezettre és a műveletre vonatkozó adatokat tartalmazza, tehát a fizetőre vonatkozóan adatot nem tartalmaz (az MNB rendelet a fizetési kérelem fogalmát szűkebben értelmezi, mert csak a belföldi fizetési rendszerben szabványosított és az átutalás megadásához szükséges minden adatot tartalmazó, a pénzforgalmi szolgáltatók által közvetített üzeneteket tekinti annak).

A fizető fél az EAM útján beolvasott adatok alapján mobileszközén egy átutalási megbízást hoz létre azzal, hogy meghatározza a megterhelendő fizetési számláját és az adatok ellenőrzése után a neki felkínált lehetőségek keretei között a megbízás adatainak módosításával, illetve kiegészítésével vagy anélkül jóváhagyja az átutalási megbízást.

A belföldi fizetési rendszerben alkalmazott speciális eljárás megköveteli az EAM kód hitelesítését, ami garantálja, hogy a kedvezményezett az EAM kód előállítását pénzforgalmi szolgáltató közreműködésével végzi, valós gazdasági tevékenységet folytat és a kifizetett összeg a megfelelő fizetési számlára kerül, illetve vita esetén a fogyasztói jogok érvényesítését megfelelő eljárásrend és kötelezettségvállalások is támogatják.

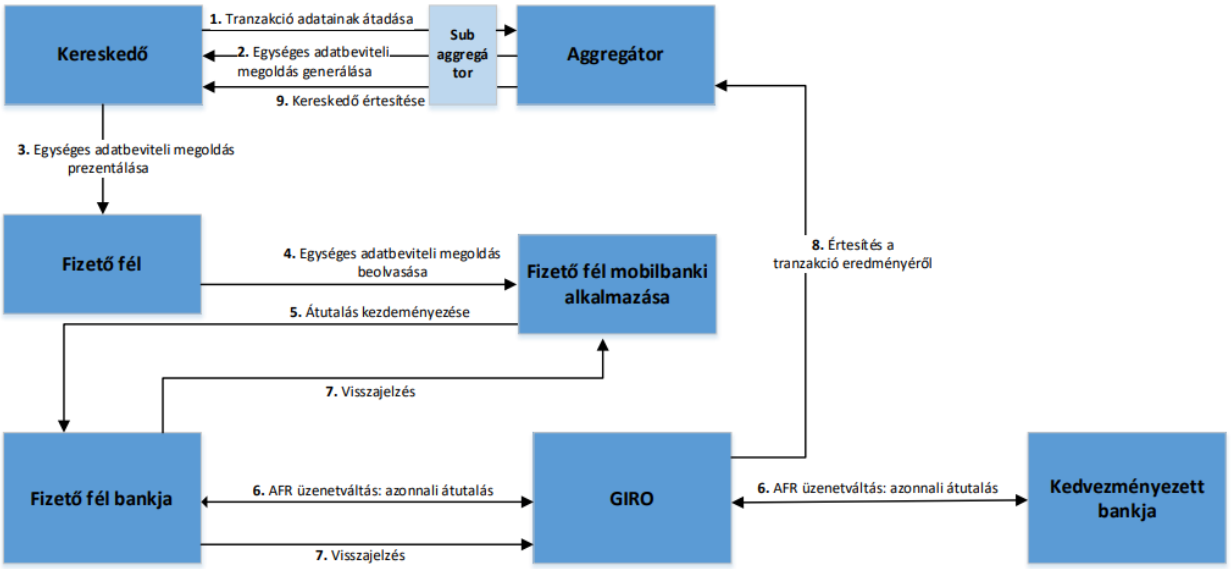
Az EAM fizetés biztonságos, hiszen a fizető félnek nem kell személyes adatait megadni az adatbevitelhez. Csak hiteles kód alapján olvashatók be a mobileszközbe, illetve az azon futó, pénzforgalmi szolgáltató által biztosított mobilalkalmazásba a megbízás adatok, és a hitelesítő kód eredetiségét és megfelelőségét a fizető fél számlavezető pénzforgalmi szolgáltatója is ellenőrzi.

Az EAM fizetés gyorsaságát az elfogadói végpont számára történő – a teljesítés megtörténtét igazoló –, azonnali visszajelzés garantálja, amit a fizető fél bankja állít össze és amit az Aggregátor a végponti értesítés céljából átalakít; tehát a fizetés kezdeményezése és a végpontok értesítése között csak néhány másodperc különbség lehet. A fizető fél számlavezető pénzforgalmi szolgáltatója a művelet bármi okból történő meghiúsulása esetén is küld értesítést az elfogadói végpont számára.

Az EAM-mal beolvasott átutalási megbízás specialitása, hogy a fizetés kedvezményezettje nem csak az áru vagy szolgálatás értékesítője, hanem elfogadó, illetve elszámoló fél (Sub-Aggregátor vagy más közvetítő) is lehet, amely a befolyt összeget tételesen, vagy gyűjtve továbbítja a tényleges kedvezményezett számára.

Az EAM előállítása történhet tételenkénti (egyenkénti) igénylés alapján valós időben, vagy kötegelt formában – nem valós időben – is.

2.1. Sikeres, a séma alapján kezdeményezett azonnali átutalás



1. ábra – A séma alapján kezdeményezett többfunkciós eszközön indított azonnali átutalás – Sikeres üzenetáramlás logikai folyamatábrája

A folyamat lépései:

1. Tranzakció adatainak átadása: A kereskedő rendszere az aktuális vásárlás adatait a sub-aggregátor számára elektronikus csatornán átadja, aki továbbítja az Aggregátornak.

2. Az Aggregátor létrehozza az egységes adatbeviteli megoldást a rendeletben meghatározott szabvány szerint, ami a tranzakció és a kedvezményezett adatait is tartalmazza és az adatokat hitelesítő kóddal látja el.

3. A kereskedő megjeleníti, elérhetővé teszi a kasszarendszerén az előállt egységes adatbeviteli megoldást. Számlás fizetés esetén kinyomtatja a számlára a QR-kódot. Webshop vásárlás esetén egy link (deeplink) generálása történik, amire kattintva nyílik meg a mobilbanki alkalmazás. NFC esetében a kereskedő eszköze sugározza az adatokat.

4. A Fizető fél beolvassa többfunkciós eszköze segítségével az egységes adatbeviteli megoldást. Az egységes adatbeviteli megoldás beolvasása elindítja az előre telepített mobilbanki alkalmazást a többfunkciós eszközén, ugyanis az egységes adatbeviteli megoldásban lévő domain-en tárolva vannak azon mobilbanki alkalmazások nevei, amiket fel tud éleszteni az egységes adatbeviteli megoldás beolvasása az adott többfunkciós eszközön. Egyéb esetben a fizető fél már előre belép a mobilbanki alkalmazásba és ott olvassa be az egységes adatbeviteli megoldást.

5. Fizető fél alkalmazása megvizsgálja a fizetési kezdeményezés előtt az egységes adatbeviteli megoldásra vonatkozó formai követelményeket, annak érvényességi idejét és a hitelesítő kódot, hogy nem történt-e változtatás az egységes adatbeviteli

megoldásban található információkban. A hitelesítő kód vizsgálata a Tanúsítványkezelési Útmutatóban részletezett eljárás szerint történik. Ezután, ha az erős ügyfélhitelesítés is megtörtént, akkor elindítja az azonnali átutalás kezdeményezést a Fizető fél bankja irányába az alkalmazás. Amennyiben a fizető fél bankja és a kedvezményezett bankja megegyezik, bankon belüli átutalás történik. A fizető fél bankjának lehetősége van letárolni az egységes adatbeviteli megoldást későbbi jóváhagyásra. A jóváhagyás megtörténtekor minden szükséges ellenőrzést el kell végezni.

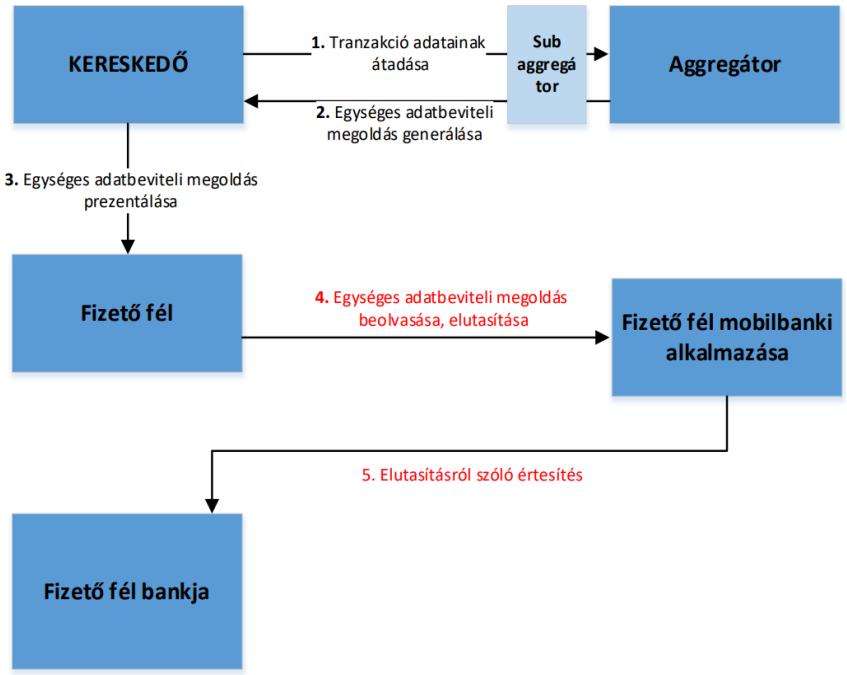
6. A fizető fél bankja – üzleti feltételek és a fedezet ellenőrzése után – azonnali átutalást küld a Kedvezményezett bankjának a GIROInstant platformon keresztül. Az elszámolt bankközi tranzakcióról végső státuszriportban kap értesítést. Az üzenetváltás lépései megegyeznek az azonnali átutalás sémájára vonatkozó üzenetváltással (pacs.008: átutalás, pacs.002: kedvezményezett visszajelzése pacs.002: végső státusz riport). Bankon belüli átutalás esetén értelemszerűen a tranzakció nem halad át a GIROInstant-on, ezért végső státuszriport sem áll elő. Olyan eset is előfordulhat, hogy a tranzakció ellenértéke egy korlátozott rendeltetésű gyűjtőszámlára érkezik, ahonnan a sub-aggregátor juttatja el tranzakció összegét a kereskedőnek.

7. A fizető fél bankja a GIROInstant platformon keresztül visszajelző üzenetet küld a sikeres terhelésről pain.002 visszajelző üzenet formátumban. Az üzenet címzettje minden esetben az Aggregátor. Az Aggregátor feladata -minden esetben- továbbítani a visszajelző üzenetet a sub-aggregátor számára, aki értesíti a kereskedőt. Ezzel egyidőben a bank értesíti a fizető felet is a többfunkciós eszközén a terhelés megtörténtéről, aki ezáltal meggyőződik a tranzakció végállapotáról.

8. A GIROInstant eljuttatja az Aggregátornak a visszajelző üzenetet.

9. A visszajelző üzenet alapján az Aggregátor a sub-aggregátoron keresztül értesíti a kereskedőjét az elszámolás megtörténtéről. Erről abban az esetben tudja a Raiffeisen Bank értesíteni a kereskedőt, ha a kereskedő bekérdez (pollozás szükséges).

2.2. Hibaág 1: A fizető fél által elutasított fizetési kezdeményezés



2.ábra – A séma alapján kezdeményezett, többfunkciós eszközön indított azonnali átutalás: a mobilalkalmazás negatív visszajelzése

A folyamat lépései:

1. Tranzakció adatainak átadása: A kereskedő rendszere az aktuális vásárlás adatait a sub-aggregátor számára elektronikus csatornán átadja, aki továbbítja azt az Aggregátor felé.

2. Az Aggregátor létrehozza az egységes adatbeviteli megoldást a rendeletben meghatározott szabvány szerint, ami a tranzakció és a kedvezményezett adatait is tartalmazza. Az adatokat hitelesítési kóddal látja el a generáló algoritmus a visszaélések megakadályozása érdekében.

3. A kereskedő megjeleníti, elérhetővé teszi a kasszarendszerén az egységes adatbeviteli megoldást. Számlás fizetés esetén kinyomtatja a számlára a QR-kódot. Webshop vásárlás esetén egy link 9 Egységes Adatbeviteli Megoldás alapján kezdeményezett azonnali átutalások (deeplink) generálása történik, amire kattintva nyílik meg a mobilbanki alkalmazás. NFC esetében a kereskedő eszköze sugározza az adatokat.

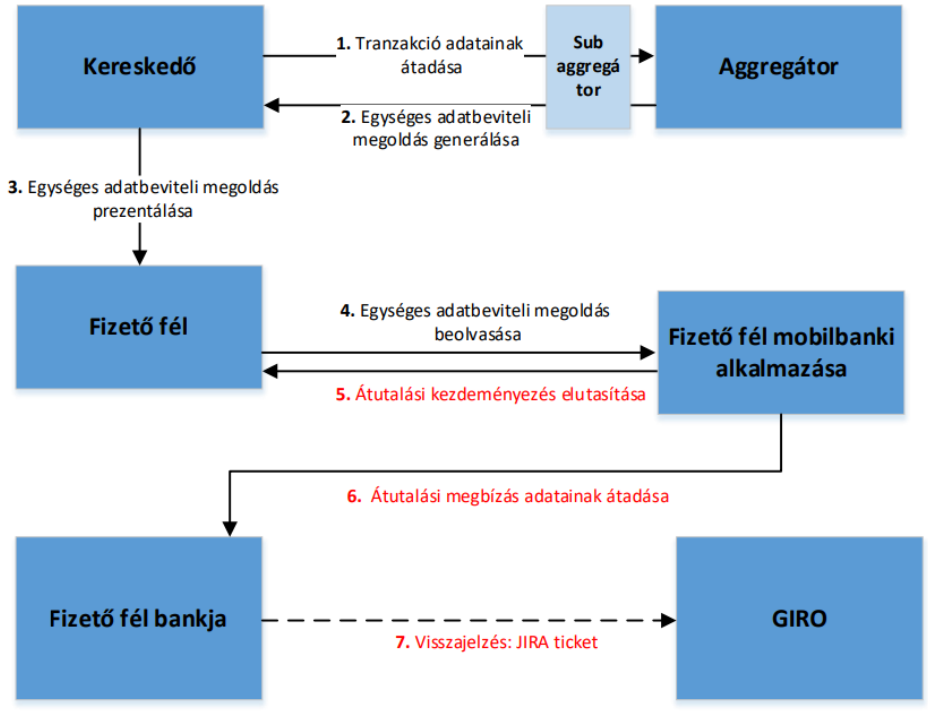
4. A Fizető fél beolvassa többfunkciós eszköze segítségével az egységes adatbeviteli megoldást. Az egységes adatbeviteli megoldás beolvasása elindítja az előre telepített mobilbanki alkalmazást a többfunkciós eszközön, ugyanis az egységes adatbeviteli megoldásban tárolva vannak azon mobilbanki alkalmazások nevei, amiket fel tud éleszteni az egységes adatbeviteli megoldás beolvasása az adott operációs rendszeren. Egyéb esetben a fizető fél már előre belép a mobilbanki alkalmazásba és

ott olvassa be az egységes adatbeviteli megoldást. A fizető fél a beolvasást követően dönthet úgy is, hogy az adott egységes adatbeviteli megoldással létrehozott azonnali átutalásra vonatkozó kezdeményezést mégsem kívánja benyújtani a bankjához. Ebben az esetben elutasítja az egységes adatbeviteli megoldással kezdeményezett azonnali átutalást. Ilyen eset lehet például, hogy a fizetési folyamat közben a fizető fél úgy dönt, hogy a megnyitott alkalmazástól eltérő (másik) mobilbanki alkalmazással kívánja lebonyolítani a fizetést.

5. A fizető fél bankja értesül a mobilbanki alkalmazástól a beolvasott egységes adatbeviteli megoldással kezdeményezett azonnali átutalás elutasításáról. A fizető fél bankján kívül más szereplő a folyamatban (Aggregátor, sub-aggregátor, kereskedő) közvetlenül nem értesül a fizető fél általi elutasításról, azaz visszajelző üzenetet (pain.002 formában) a fizető fél bankja nem hoz létre és nem küld az Aggregátor irányába. Így a lehetőség adott az egységes adatbeviteli megoldás újbóli felhasználására.

6. Az Aggregátor, sub-aggregátor, kereskedő számára az egységes adatbeviteli megoldás érvényességi idejének lejárata a mérvadó, hiszen addig még kaphatnak pozitív vagy negatív visszajelző üzenetet a tranzakció állapotáról. Az érvényességi idő alapesetben 120 másodpercben lesz minimalizálva.

2.3. Hibaág 2: A fizető fél mobilbanki alkalmazásában meghiúsult fizetési kezdeményezés



3. ábra – A séma alapján kezdeményezett, többfunkciós eszközön indított azonnali átutalás: a mobilalkalmazás negatív visszajelzése

A folyamat lépései:

1. Tranzakció adatainak átadása: A kereskedő rendszere az aktuális vásárlás adatait az Aggregátor számára elektronikus csatornán átadja. Előfordulhat, hogy a kereskedő és az Aggregátor közé subaggregátor is beáll a kezdeményezés és a visszajelzés folyamatába.

2. Az Aggregátor létrehozza az egységes adatbeviteli megoldást a rendeletben meghatározott szabvány szerint, ami a tranzakció és a kedvezményezett adatait is tartalmazza. Az adatokat hitelesítési kóddal látja el a generáló algoritmus a visszaélések megakadályozása érdekében.

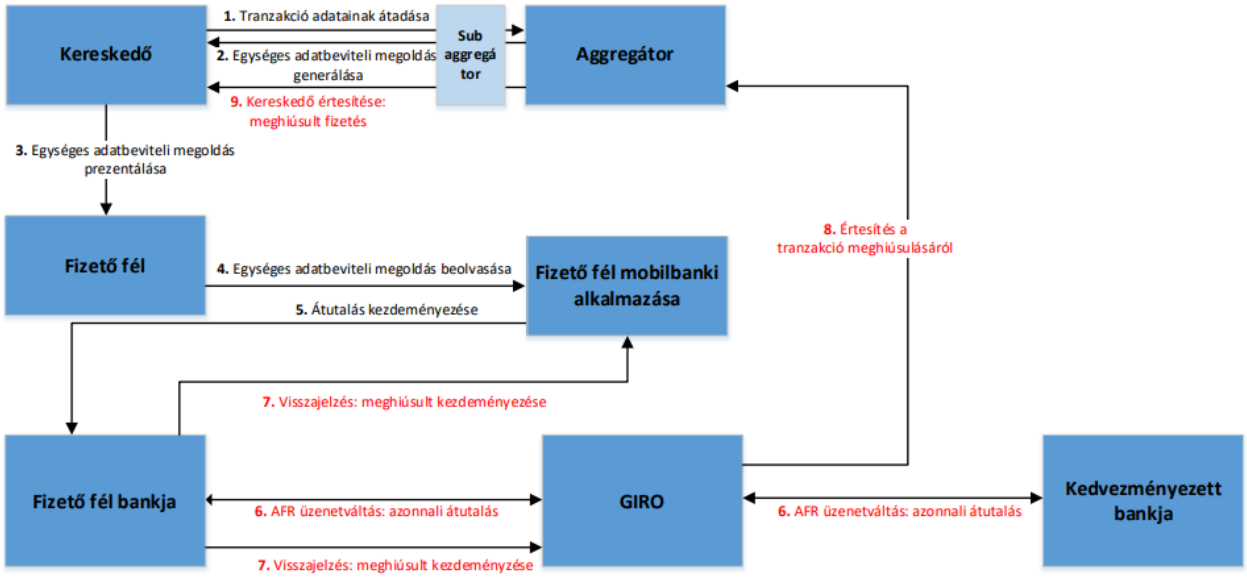
3. A kereskedő megjeleníti, elérhetővé teszi a kasszarendszerén az egységes adatbeviteli megoldást. Számlás fizetés esetén kinyomtatja a számlára a QR-kódot. Webshop vásárlás esetén egy link (deeplink) generálása történik, amire kattintva nyílik meg a mobilbanki alkalmazás. NFC esetében a kereskedő eszköze sugározza az adatokat.

4. A Fizető fél beolvassa többfunkciós eszköze segítségével az egységes adatbeviteli megoldást. Az egységes adatbeviteli megoldás beolvasása elindítja az előre telepített mobilbanki alkalmazást a többfunkciós eszközön, ugyanis az egységes adatbeviteli megoldásban tárolva vannak azon mobilbanki alkalmazások nevei, amiket fel tud éleszteni az egységes adatbeviteli megoldás beolvasása az adott operációs rendszeren. Egyéb esetben a fizető fél már előre belép a mobilbanki alkalmazásba és ott olvassa be az egységes adatbeviteli megoldást. A fizető fél bankja nem képes a GIRO-n keresztül visszajelző üzenetet küldeni a kereskedőnek abban az esetben, ha a mobilalkalmazás az egységes adathordozó megoldás formai ellenőrzésekor olyan hiányosságot talált, ami miatt a visszajelző üzenet létrehozására nem megoldható – például, ha nincs kitöltve egy kötelező mező vagy a kedvezményezett számlaszáma érvénytelen. Ekkor a visszajelző üzenet segítségével történő értesítés nem lehetséges, minden ilyen esetben egyedi kivizsgálási eljárás szükséges. Logikailag ide tartozik a lejárt érvényességi idejű egységes adatbeviteli megoldás esete, amikor is a visszajelző üzenet generálása nem megengedett a rendszer performanciájának veszélyeztetése miatt.

5. A mobilbanki alkalmazás értesíti a fizető felet a kezdeményezés meghiúsulásáról.

6. A fenti értesítéssel egyidőben a mobilbanki alkalmazás értesíti a fizető fél bankját a hibaokról.

2.4. Hibaág 3: Az azonnali átutalásban résztvevő szereplők bármelyikénél elutasított fizetési kezdeményezés



4. ábra A séma alapján kezdeményezett azonnali átutalás: a fizető fél pénzforgalmi szolgáltatójának negatív visszajelzése

A folyamat lépései:

1. Tranzakció adatainak átadása: A kereskedő rendszere az aktuális vásárlás adatait az Aggregátor számára elektronikus csatornán átadja. Előfordulhat, hogy a kereskedő és az Aggregátor közé subaggregátor is beáll a kezdeményezés és a visszajelzés folyamatába.

2. Az Aggregátor létrehozza az egységes adatbeviteli megoldást a rendeletben meghatározott szabvány szerint, ami a tranzakció és a kedvezményezett adatait is tartalmazza. Az adatokat hitelesítési kóddal látja el a generáló algoritmus a visszaélések megakadályozása érdekében.

3. A kereskedő megjeleníti, elérhetővé teszi a kasszarendszerén az egységes adatbeviteli megoldást. Számlás fizetés esetén kinyomtatja a számlára a QR-kódot. Webshop vásárlás esetén egy link (deeplink) generálása történik, amire kattintva nyílik meg a mobilbanki alkalmazás. NFC esetében a kereskedő eszköze sugározza az adatokat.

4. A Fizető fél beolvassa többfunkciós eszköze segítségével az egységes adatbeviteli megoldást. Az egységes adatbeviteli megoldás beolvasása elindítja az előre telepített mobilbanki alkalmazást a többfunkciós eszközön, ugyanis az egységes adatbeviteli megoldásban tárolva vannak azon mobilbanki alkalmazások nevei, amiket fel tud éleszteni az egységes adatbeviteli megoldás beolvasása az adott operációs rendszeren. Egyéb esetben a fizető fél már előre belép a mobilbanki alkalmazásba és ott olvassa be az egységes adatbeviteli megoldást.

5. Ha a mobilbanki alkalmazás a formai ellenőrzéseket elvégezte, akkor továbbítja a fizetési kezdeményezést a fizető bankja számára. A fizetési kezdeményezéssel kapcsolatban a fizető fél bankja a következő ellenőrzéseket hajtja végre: • fizető fél fedezetének ellenőrzése: fedezetlenség esetén kötelezően az MS03 hibakóddal kell a visszajelző üzenetet küldeni. • hitelesítő kód ellenőrzése: ha az ellenőrzésen elbukik, akkor a vonatkozó hibakóddal kell a visszajelző üzenetet küldeni. • minden, a tranzakció átutalására vonatkozó egyéb formai és üzleti követelmény: ha az ellenőrzésen elbukik, akkor a vonatkozó hibakóddal kell a visszajelző üzenetet küldeni. Ebben a lépésben történik az egységes adatbeviteli megoldás esetleges korábbi felhasználásának ellenőrzése is a többszörös küldés elkerülése céljából. Ez az ellenőrzés a Kedvezményezett belső tranzakcióazonosítója mező vizsgálatával történhet. Ez a mező globálisan egyedi azonosító. Ha egy egységes adatbeviteli megoldás alapján korábban már kezdeményeztek azonnali átutalást, akkor a fizető fél bankja az AM05 hibakóddal tölti ki az esetleges további visszajelző üzenetet a duplikált kezdeményezés jelzésére. A fizető fél bankjának 180 napra visszamenően kell ellenőrizni az egységes adatbeviteli megoldás esetleges korábbi felhasználását. Ha az aggregátor a fentiek ellenére is több azonnali átutalást kapna egyazon egységes adatbeviteli megoldás alapján, akkor a Chargeback dokumentációban (címe: Egységes adatbeviteli megoldással kezdeményezett azonnali fizetések hiba- 13 Egységes Adatbeviteli Megoldás alapján kezdeményezett azonnali átutalások és reklamációkezelése) ismertetett eljárást kell kövesse a visszautaláshoz. Az aggregátor kezelni tudja a hibás, többszörösen elküldött ugyanazon visszajelző üzenetek esetét is, mert a GIRO rendszere átengedi a többszörösen küldött visszajelzéseket.

6. A fizető fél bankja azonnali átutalással elindítja a fenti ellenőrzések után a tranzakciót. Amennyiben az azonnali átutalást nem sikerül végrehajtani, a fizető fél bankja visszajelzést küld a frontend számára és az Aggregátornak. Az üzenet összeállítására és kiküldésére vonatkozó végrehajtási időre vonatkozó követelményt lásd a következő fejezetben.

7. A fizető fél bankja a GIROInstant platformon keresztül visszajelző üzenetet küld a sikertelen átutalásról pain.002 visszajelző üzenet formátumban. Az üzenet címzettje az Aggregátor. Ezzel egyidőben a bank értesíti a fizető felet is a többfunkciós eszközön a terhelés meghiúsulásáról.

8. A GIROInstant továbbítja a negatív visszajelző üzenetet az Aggregátornak.

9. A visszajelző üzenet alapján az Aggregátor (esetenként sub-aggregátoron keresztül) értesíti a kereskedőjét a fizetési művelet meghiúsulásáról.

3. Fizetési helyzetek ismertetése, mezőkitöltöttség biztosítása

Egységes adatbeviteli megoldással történő fizetés során jelenleg kizárólag dinamikus (eseti fizetésre szolgáló egyedi) kódok képzése lehetséges. A tapasztalatok és az üzleti igények függvényében kerülhet sor a (több fizetés teljesítésére alkalmas) statikus kódok használatának lehetővé tételére.

Jelenleg szűk körben van lehetőség mezők módosítására. A tapasztalatok birtokában a mezővédelmi korlátozások fokozatosan enyhíthetők lesznek.

A mezővédelem, és az alkalmazható érvényességi időhossz (offset) értékeket a kötelezően feltüntetendő fizetési helyzet kódok (purpose code) határozzák meg.

3.1. Meghatározott fizetési helyzetek

1. Vásárlás fizikai, kereskedelmi eladóhelyen (1. PoS terminál, 2. pénztárgép periféria (képernyő, NFC jeladó), 3. PDA/telefon/tablet segítségével történő kód prezentálással)
2. Loyalty App-pal indított fizikai vásárlás (PoS terminál, pénztárgép periféria, telefon/tablet/PDA)
3. Webes vásárlás során prezentált kód (1. QR, 2. elküldött deeplink)
4. Közszolgáltatási (államigazgatás, biztosítás, posta, távközlés is) számla (kötegelt kód előállítás, QR kód prezentálása tartós adathordozón, pl. papíron; pdf fájl, vagy deeplink bemutatása, webes felület, fizikai pont)
5. Kereskedelmi számla (QR prezentálás tartós adathordozón, képernyőn, deeplink küldése)
6. Önkiszolgáló automatán történő vásárlás

1. táblázat – Fizetési helyzetek, adatbeviteli módok

	Megnevezés	QR	NFC	Deeplink
a	Vásárlás fizikai eladóhelyen	X	X	--
b	Loyalty App-pal indított fizikai vásárlás	X	X	--
c	Webes vásárlás során prezentált kód	X	--	X
d	Közszolgáltatási számla (államigazgatás, biztosítás, Magyar Posta, távközlés, útdíj is)	X	X	X

	Megnevezés	QR	NFC	Deeplink
e	Kereskedelmi számla, egyéb eseti fizetendők eseti kód alapján	X	X	X
f	Önkiszolgáló automatánál történő vásárlás	X	X	--

2. táblázat – Fizetési helyzetek, adatbeviteli eszközök

	Eszköz			
Fizetési helyzet	**pénztár gép**	**tel/tablet/ PDA**	**Böngésző**	**Üzenő App[1]**
Vásárlás fizikai eladóhelyen	x	x		
Loyalty App-pal indított fizikai vásárlás	x	x		
Webes vásárlás során prezentált kód			x	x
Közszolgáltatási számla (államigazgatás, biztosítás, Magyar Posta, távközlés, útdíj is)			x	x
Kereskedelmi számla, egyéb eseti fizetendők eseti kód alapján			x	x
Önkiszolgáló automatánál történő vásárlás				

[1] Üzeneteket kezelő mobilalkalmazás (Messaging Application)

3. táblázat - Adatbeviteli módok és eszközök

	Eszköz			
Adatbeviteli mód	**pénztárgép**	**tel/tablet /PDA**	**böngésző**	**Üzenő App**
QR	x	x	x	--
NFC	x	x	--	--
Deeplink	--	x	x	x

Egyes fizetési helyzetekben a kódigénylés (create payment) üzenetet eltérően kell kitölteni.

Minden fizetési helyzetben fizetési helyzetazonosítót (purpose code) kell alkalmazni, ezek a kódok a fizetési helyzethez rendelten meghatározottak. A helyzetazonosító kitöltése kötelező, melynek oka, hogy a speciális ellenőrzéseket ez a kód határozza meg.

A Sub-Aggregátor felelőssége, hogy csak az adott fizetési helyzetre értelmezhető, helyes helyzetazonosító kódokat töltsék a Kedvezményezettek az üzenetbe, mert az Aggregátor ezeket a kódokat az üzenet validálása során nem vizsgálja. A Sub-Aggregátoroktól elvárt, hogy szerződéseikben rögzítsék a kedvezményezett által használható fizetési helyzet kódokat, szem előtt tartva a fizető felek részére készülő számlainformáció egyértelműségének igényét is.

A fizetési helyzetazonosító kódok korrekt használata azért is fontos, hogy a fizető felek és a kedvezményezettek pénzforgalmi szolgáltatói, vagy az igénybe vett számlainformációs szolgáltatók pontos kimutatást tudjanak adni a fizetőknek vásárlási forgalmukról. A kereskedelmi számlák, díjbekérők esetén a közlemény rovat fizető fél általi kitöltését a kedvezményezett lehetővé teheti megfelelő mezővédelmi beállítás alkalmazásával.

A közlemény és az összeg felülírása lehetséges lesz személyek közötti (P2P) fizetések körében, de az összeg adat csak a fejlesztések későbbi fázisában. Egyelőre nem teszi lehetővé a rendszer a P2P fizetések (és csak azok) esetében egy meggenerált kódra több fizetés teljesítését (illetve ezt dupla fizetésként, tehát hibaként jelzi), ennek megvalósítására is csak a rendszer éles indulását követő fejlesztési fázisokban lesz lehetőség.

A használatra előírt kódok szerepelnek az ISO 20022 szabvány külső kódlistáján, tehát nem került meghatározásra „proprietary", tehát sajátságos kód. Amennyiben új kódokra merül fel igény, azokat az erre jogosult intézménynek fel kell vetetni az ISO 20022 külső kódok listájára.

3.2. Fizetési helyzet kódok

3.2.1. Fizetési helyzet kódok alkalmazása

A fizikai üzletben történő vásárlás esetén az IPPS fizetési helyzet kódot lehet alkalmazni, webes értékesítési, vagy fizetési felületen IPEW kódot kell használni.

A közüzemi számlák QR kódjában az alábbi kódok elhelyezését kezdeményezheti a kedvezményezett: UBIL, COMT, TBIL, GOVT, INSU.

Az eseti kereskedelmi számlák és díjbekérők elvárt fizetési helyzetkódja: IVPT. Ezt a kódot lehet alkalmazni akkor is, ha egyébként legfeljebb 10 percen belül lejáró fizetési helyzet kódot kellene alkalmazni, de a Kedvezményezett 10 percnél hosszabb lejárati időt kíván meghatározni ezen fizetési helyzethez rendelt (60 napos) időintervallumon belül. Ebben az esetben a közleményt lehetőleg védett mezőként kell kezelni.

Webes értékesítési, vagy fizetési felületen IPEW kódot kell használni.

3.2.2. Adatbeviteli kód érvényességi ideje

Az Aggregátor öt érvényességi paramétert (maximum értéket) alkalmaz a különféle fizetési helyzetekben, percekben meghatározva azokat. A kedvezményezett az intervallumon belül dönthet az offset paraméter, vagyis az érvényességi idő mértékéről, tekintettel az adatbeolvasás és a megbízás kiegészítésének és jóváhagyásának fizető fél oldali időigényére is.

Az 1. sz. táblázat a)-c). fizetési helyzetek (bolt, webshop) esetében 10 perc, a d) helyzetben (tömeges számlakibocsátás) 180 nap, az e) helyzetben (kereskedelmi számla, díjbekérő) maximum 60 nap, a f)-g) helyzetekben (önkiszolgáló automata, ATM) 3 perc, a h) helyzetben (természetes személy kedvezményezett) maximum 5 nap. Habár a rendszer később alkalmassá tehető a lejárati idő árnyaltabb meghatározására ennek különösebb üzleti szükségessége még nem merült fel, ezért célszerűbb ezzel az egységes, és az Aggregátor által beállított paraméterezéssel elindítani a rendszer működését.

Az „Offset" értékek használatát a Sub-Aggregátor szabályozza és ellenőrzi.

4. táblázat – Fizetési helyzetek, kitöltési követelmények

Fizetési helyzet	Fizetési helyzet kód (Purpose code)	Lejárati idő	Védelem alól kivehető
Vásárlás fizikai eladóhelyen	IPPS – Instant Payments at POS	Max. 10perc	ügyfélazonosító
Webes vásárlás	IPEW - InstantPaymentsInECommerce	Max. 10perc	ügyfélazonosító
Közszolgáltatási számla (államigazgatás, pénzügy, távközlés is)	TBIL - TelecommunicationBill UBIL - Utilities (Villany, Víz-csatorna, Hulladékkezelés, Gáz) COMT - ConsumerThirdPartyConsolidatedPayment (díjbeszedő) GOVT - GovernmentPayment (Magyar Posta Zrt., útdíj is) INSU - InsurancePremium (biztosítási díj	Max. 180 nap	nincs
Kereskedelmi számla, díjbekérő eseti kód alapján	IVPT - InvoicePayment	Max. 60 nap	Közlemény, ügyfélazonosító

4. EAM műveletekhez kapcsolódó API leírások magyarázata

4.1. Biztonság és authentikáció

Az API a kommunikáció során standard REST HTTPS hívásokat használ, amelyek http headerjében vezérlőinformációk közlekednek, a fizetési információ (payload) formátuma pedig JSON.

A Raiffeisen PAY API-k által használt megoldás:

Kliens – Szerver kapcsolati protokoll: HTTPS

Kliens authentikáció:

API Key alapú, tehát Hívó fél a regisztráció során kap a banktól, melyet a hívások http headerjében szerepeltetni szükséges, a következők szerint:

- X-API-KEY (értékét a pay portálon a regisztrációt követően kapja meg a Banktól)

Digitális aláírás alkalmazása a magas biztonság érdekében:

Az OpenBanking Security Profile Implementer's Draft iránymutatása szerint http headerben küldött base64 encoded, detached típusú JWS/JWT tokenek formájában várjuk hívó fél authentikációjához használható aláírást.

4.2. EAM payload adattartalom


```
{
 "paymentInfo": {
  "transactionReference": " EAMID1062605",
  "transactionAmount": 10,
  "transactionCurrency": "HUF",
  "expiryDateTimeOffset": 5,
  "allowedModes": {
   "qrAllowed": true,
   "nfcAllowed": true,
   "deeplAllowed": false
  },
  "remittanceInfo": "Teszt EAM generate",
  "purposeCode": "IPPS",
  "deviceType" : "CASHREGISTER",
```

```
   "editableFields": {
     "isAmountEditable": false,
     "isRemittanceInformationEditable": false,
     "isCustomerIdEditable": false
    },
    "invoiceReference": "invoiceReference001",
    "customerReference": "customerReference001"
  },
  "payeeInfo": {
    "accountNumber": " HU92130995970058055050103045",
    "terminalReference": "TESTEAM01"
  }
}
```


4.3. Create EAM mezőmagyarázatok

Kérés törzse

Mező név	**Tartalom**	**Leírás**	**Szabály**
paymentIno	EAM adatok		
transactionReference	Tranzakció azonosító	A tranzakció azonosító a fizetési kérelem küldője és subaggregátor között az adott egyedi tranzakció azonosítására szolgáló ponttól pontig hivatkozás. A megbízás azonosító a megbízással kapcsolatos több üzenetben is szerepeltethető.	Egyediséget kell biztosítani.
transactionAmount	Kérelem összege	A kért összeg, a fizetési kérelem küldője által megadott pénznemben.	
transactionCurrency	Devizanem	A devizakódot az ISO 4217 szabvány szerint.	Csak 'HUF' lehet.
expiryDateTimeOffset	Érvényességi időhossza	Adatbeviteli kód érvényességi ideje határozza meg a létrehozáshoz képest.	A fizetési helyzetekhez köthetően meg van határozva a maximum.
allowedModes	Adatbeviteli mód	Adatbeviteli módot kell megadni.	
qrAllowed	QR adatbeviteli mód	Az EAM QR formában is megjeleníthető.	
nfcAllowed	NFC adatbeviteli mód	Az EAM NFC eszközzel is beolvasható.	
deeplAllowed	Deeplink adatbeviteli mód	Az EAM deeplink formájában is közétehető.	

remittanceInfo	Strukturálatlan közlemény	Ha a közlemény nem módosíthatónak van megjelölve, akkor az adatmezőben adható meg az átutaló és a kedvezményezett közötti megállapodás szerinti információ. A beérkező átutalás és az azzal rendezni kívánt tétel, pl. a vevő folyószámlán nyilvántartott kereskedelmi számla egyeztetését/rekonsziliálását lehetővé tevő, strukturálatlan formában megadott információ.	
purposeCode	Jogcím/Fizetési helyzet azonosító	A jogcím segítségével a végponti szereplők: kezdeményező fél, átutaló/(tényleges) fizető, illetve a (tényleges) jogosult információt közölhetnek az adott átutalás jellegére vonatkozóan. Lehetséges értékei: IPEW: Webes vásárlás IPPS: Vásárlás fizikai eladóhelyen	Csak 'IPEW' vagy 'IPPS' lehet
deviceType	Eszköz típusa	Az eszköz típusa, lehetséges értékei: CASHREGISTER: pénztárgép SMARTDEVICE: Okos eszköz (telefon, tablet, PDA) BROWSER: böngésző MESSAGINGAPP: Üzenő App	Csak 'CASHREGISTER', 'SMARTDEVICE', 'BROWSER' vagy 'MESSAGINGAPP' lehet
editableFields	Módosítható mezők		
isAmountEditable	Összeg módosíthatóság	A EAM kérés küldője jelölheti, hogy az összeg a fizetőfél által módosítható-e vagy sem. Ha az összeg módosítható, akkor az eredeti összegtől eltérő – alacsonyabb vagy magasabb – összeggel is teljesíthető maximum az azonnali átutalás értékhatáráig.	
isRemittanceInformationEditable	Közlemény módosíthatóság	A EAM kérés küldője jelölheti, hogy a közlemény a fizetőfél által módosítható-e vagy sem. Ha módosítható, akkor az eredeti közlemény átírható.	

isCustomerIdEditable	Ügyfélazonosító módosíthatóság	A EAM kérés küldője jelölheti, hogy az ügyfélazonosító módosítható-e vagy sem. Ha módosítható, akkor az ügyfélazonosítót egy fizeti láncolatban például egy Loyalty App módosíthatja.	
invoiceReference	Számla vagy nyugta azonosító	Számla vagy nyugta azonosítót szükséges lehet megadni – például közüzemi számlafizetések esetében – a befizetendő számla azonosítóját, mivel ez segítheti a későbbi visszakereshetőséget mind a fizető fél, mind pedig a kedvezményezett oldalán. Ennek mintájára kiskereskedelmi tranzakciók esetén hasznos lehet a nyugta azonosító megadása.	
customerReference	Ügyfélazonosító	Ügyfélazonosító elsősorban közüzemi számlafizetéseknél fordulhat elő, hogy a szolgáltató ügyfeleit speciális, csak az adott szolgáltató által alkalmazott azonosítóval azonosítja. Ebben az esetben szükséges ennek a szerepeltetése is az átutalási üzenetben, mivel mind a fizető fél, mind pedig a kedvezményezett oldalán segíti a teljesítések egyértelmű nyomon követését.	
payeeInfo	Kedvezményezett		
accountNumber	Kedvezményezett számlája IBAN formátumban	Kedvezményezett nemzetközi pénzforgalmi jelzőszáma	Magyarország esetében 28 karakter hosszúságú számsor és mindig HU megjelöléssel kezdődik, továbbá az utolsó 24 karakter megegyezik a pénzforgalmi jelzőszámmal, amennyiben

			az 3×8 karakterű, a 2×8 karakterű pénzforgalmi jelzőszám esetén az IBAN utolsó nyolc számjegye nulla.
terminalReference	Terminál azonosító	Kedvezményezetti eszköz azonosítója	
shopId	Boltazonosító	Kedvezményezetti bolt sorszáma	

Válasz törzse

Sikeres API hívás esetén (HTTP 200)

Mezőnév	**Megjegyzés**
paymentReference	Aggregátor által generált EAM egyedi azonosítója
creationDateTime	Az Aggregátor időbélyege. A formátum kezelés részleteit külön pont tartalmazza.
expiryDateTimeOffset	Fizetési helyzetenként meghatározott kereten belüli érték percben, amelyet a Kedvezményezett határoz meg a fizetési helyzetre megadott értéken belül.
paymentUrl	Egységes adatbeviteli kód

Hiba esetén

HTTP 400 – Általános (üzleti validációs) hiba, a hiba okait a válaszban visszakapja a hívó fél. A paymentReference adat alatt az „errorCode" és a „description" mezőpárok ismétlődnek.

Mezőnév	**Megjegyzés**
errorCode	Egyedi hibakód azonosító (bővebben a hibakód táblázatban)
errorId	x-request-id mezőben küldött érték
description	Hibakódhoz tartozó rövid magyarázat.

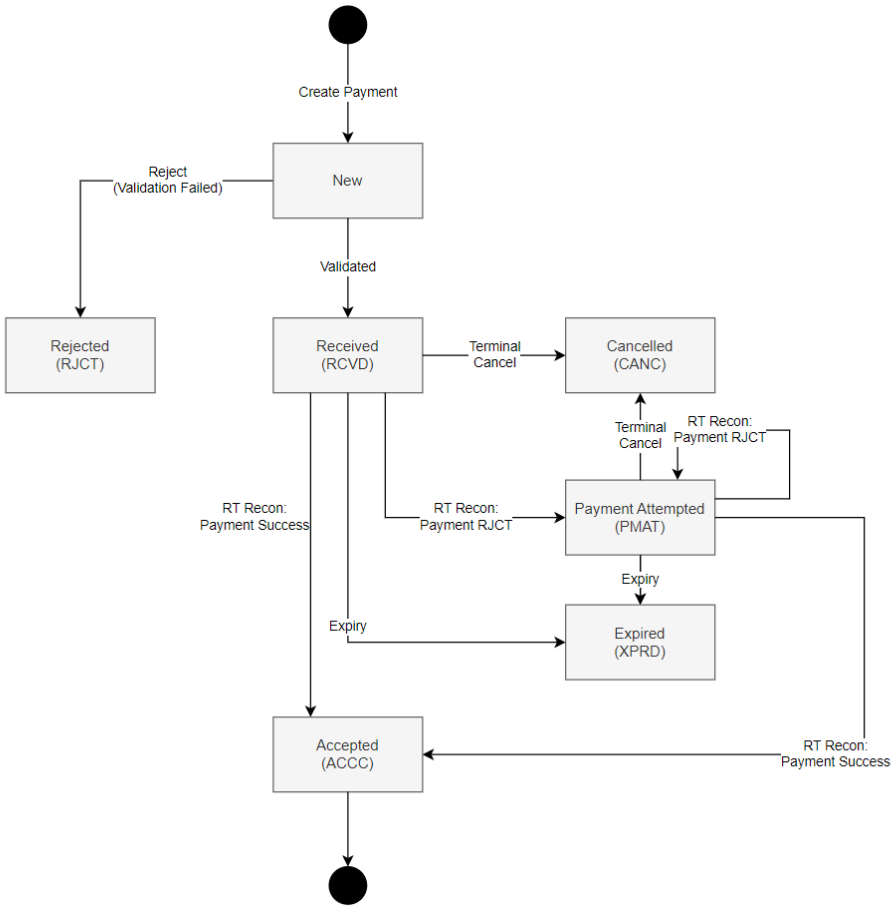
Error kód	Error leírás
E0001	Érvénytelen pénznem
E0003	Érvénytelen fizetési helyzet kód
E0004	Érvénytelen érvényességi idő
E0005	QR aláírási szolgáltatás szünetel, ismételje meg a hívást!
E0006	Érvénytelen Sub-Aggregátor vagy Technikai Aggregátor azonosító
E0007	Technikai Aggregátor azonosítója és a tanúsítvány szervezetazonosító nem párosítható
E0008	A beérkező hívásban nem volt tanúsítvány
E0009	A beérkező hívásban nem volt érvényes tanúsítvány
E0100	Végstátuszú fizetés nem vonható vissza
E0200	Hiányzó mező(k)
E0300	Érvénytelen mezőtípus
E0400	Érvénytelen összeg
E0600	Érvénytelen mezőhossz
E0601	Olyan szám érték, ami a megadott határértékeken kívül esik
E0602	Olyan dátum, mely megszabott időintervallumon kívülre esik
E0700	Érvénytelen karakter
E9999	Nem várt hiba

HTTP 403 – Forbidden

A hívó félnek nincs joga az adott API hívás kezdeményezésére, ez akkor fordulhat elő, ha az x-api-key nem megfelelő.

4.4. EAM státusz üzenetek és jelentésük

státusz	**leírás**
RECEIVED	A beérkezett validált hibamentes kérés RECEIVED státuszt kap, RECEIVED: egy új payment (URL) létrehozása esetén keletkezik ez az induló státusz
CANCELLED	A kedvezményezett visszavonta a EAM-ot. Visszavonni csak olyan EAM-ot lehet amire még nem érkezett be pain.002 státusz üzenet a GIRO rendszeréből.
PAYMENT_ATTEMPTED	pain002-es elutasítása (reject) ellenére a fizetési kezdeményezés megismételhető, de a státusz megváltozott státusz azt mutatja, hogy korábban már volt fizetési próbálkozás. (A QR kód banki alkalmazásba történő beolvasása még nem minősül próbálkozásnak.)
ACCEPTED	Az azonnali átutalás sikeresen megtörtént, a kért összeg megérkezett a kedvezményezett számlájára és erről pain.002 üzenet érkezett be (ACCC az Aggregátor rendszerében).
EXPIRED	Nem történt státuszváltozás a megadott lejárati időn belül, így a payment státusza EXPIRED-re vált.



5.ábra - „Payment" állapotgép státuszváltozásának logikai folyamata

4.5. Visszautasítási kódok

A Fizető fél pénzforgalmi szolgáltatója a következő táblázatban felsorolt okokat megadva kommunikálhatja egy adott tranzakció visszautasításának okát az Aggregátor számára.

A táblázat első blokkja tartalmazza a végső státuszriportban (FSR-ben) érkező partnerbanki és GIROInstant hibaokokat. A második blokk tartalmazza a séma alapján végrehajtott vásárlásra specifikus hibakódokat. A harmadik blokk egyetlen gyűjtő hibaok kódot tartalmaz, ami minden egyéb, az előzőekben nem felsorolt visszautasítási esetre használatos. Ide tartoznak azok a szenzitív visszautasítási okok, amik harmadik fél számára nem megjeleníthetők.

Kód	Üzleti eset	Visszautasító	Csak az FSR-ből másolva	Csak a tranz. végrehajtása előtti ellenőrzésből
AB05	Kedvezményezett banknál történő időtúllépés	GIRO	x	
AB06	Fizető fél bankjánál történő időtúllépés	GIRO	x	
AB07	Pillanatnyilag nem elérhető rendszerrésztvevő	Kedvezményezett bankja	x	
AG01	A tranzakciótípus nem engedélyezett az adott számla típuson	Bármelyik bank		
AM06	Az adott számlához megállapított minimum összegnél kisebb összegű tranzakció	Bármelyik bank		
AM05	Duplikált üzenet	Fizető fél bankja		x
NOOR	Kivizsgálási üzenetre: az eredeti megbízás nem található	GIRO	x	
Séma specifikus hibakódok				
DS0D	Az aláíró tanúsítványt visszavonták, nem felel meg az ellenőrzésnek	Fizető fél bankja		x
DS17	Az egységes adathordozó megoldás hitelesítő kódja nem megfelelő (aláírás hiba)	Fizető fél bankja		x
DS0E	Tanúsítvány nem áll rendelkezésre	Fizető fél bankja		x
Gyűjtő hibakód				
MS03	Nem meghatározott hibaok	Bármelyik szereplő		

WAF_BLOCK error:

Az API hívás során tapasztalt WAF (Web Application Firewall) error általában akkor fordul elő, amikor a rendszerünk tartalmi vagy formai validáció során gyanús, hiányos, vagy nem megfelelő adatot észlel. Ez a védelem célja, hogy megóvja a rendszert az esetleges támadásoktól és hibás adatbevitelektől.

Annak érdekében, hogy technikai csapatunk a lehető leggyorsabban és legpontosabban kivizsgálhassa az esetet, kérjük, hogy küldje el a hívás részleteit tartalmazó logokat a support részére. A logokban kérjük feltüntetni:

- A hívás pontos időpontját,
- Az alkalmazott végpontot (API endpoint),
- A hívás során használt HTTP metódust (pl. GET, POST),
- Az elküldött adatok részleteit (headers, request body),
- Az esetleges hibaüzeneteket vagy hibakódokat.

A fenti információk segítenek a kollégáknak a probléma mielőbbi beazonosításában és megoldásában.

4.6. HTTP headerek

x-api-key
Az x-api-key a TECHUSER-hez van kötve (tehát ha egy cég a RaiffeisenPay Portálon több technikai felhasználót is létrehoz, akkor neki több TECHUSER-e és több x-api-key értéke is lesz

user-agent
Kötelező továbbá a User-Agent HTTP header küldése, minden híváshoz. A tartalma mindegy, csak legyen benne valami.
Például:
User-Agent: xyz

x-request-id és x-correlation-id
Az x-request-id és x-correlation-id headerekbe Version 4 UUID-t kérünk, de az is jó nekünk, ha csak simán egy-egy random sztringet kapunk. Csak a logolás során van használatban, így tudunk könnyen keresni a logokban.

x-jws-signature
A requestben a http bodyban küldött üzleti adattartalomra, mint payloadra egy Detached JWT típusú aláírást kérünk.

minta programkód jwt generáláshoz (JavaScript)
...

```
var header={"kid":keyID,"typ":"JWT","alg":"RS512","iat": epoch(), "jti": uuid4()}
var stringHeader = JSON.stringify(header);
var stringPayload = JSON.stringify(JSON.parse(request.data));
var stringJWT = JWS.sign(header.alg, stringHeader, stringPayload, privateKey);
var jwtArray=stringJWT.split(".");
var jwtDetached=jwtArray[0]+".."+jwtArray[2];
...
```

teljes jwt példa

ezt generálja a library

eyJraWQiOiIvU049MTUzNDk3MDAxNTU4NDI0MDQwNjMvQz1lVS9MPUJ1ZGFwZXN0L09VPW9u
bHlfZm9yX2RldmVsb3BtZW50X3VzZS9DTj1wMTkwMjZfb3BlbmJhbmtpbmdfLV9hcGlfdXNlcl9j
ZXJ0aWZpY2F0ZXMiLCJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiIsImlhdCI6MTU4Nzk4NDkzNSwian
RpIjoiMWM4MDNlYWYtOTEwNS00NWZhLWE5YTEtODIwOGUzOGVmYTNmIn0.eyJvcmRlcklEIjo
iZG9uXzA0MjdfMTI1NTM1IiwiY3JlZGl0b3JBY2NvdW50IjoiSFU5NjEyMDEwNjU5MDE2MzUyMDAw
MDEwMDAwMCIsInRyYW5zYWN0aW9uQW1vdW50IjoxMjMsInRyYW5zYWN0aW9uQ3VycmVuY
3kiOiJIVUYiLCJ0cmFuc2FjdGlvbkRhdGVUaW1lIjoiMjAyMC0wNC0yN1QxMDo1NTozNS4zNDhaIiw
iZXhwaXJ5RGF0ZVRpbWUiOiIyMDIwLTA0LTI3VDEzOjU1OjM1LjM0OFoiLCJyZW1pdHRhbmNlSW
5mb3JtYXRpb24iOiJyw7Z2aWQiLCJwdXJwb3NlIjoiQ0lDQSIsInNob3BJRCI6IjEyMzQ1IiwibWVyY
2hEZXZJRCI6IjEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nzg5MDEyMzQ1IiwiaW52b2ljZUlEIj
oiMTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDUiLCJjdXN0b21lcklEIjoiMTIzNDU
2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDUiLCJsb3lhbHR5SUQiOiIxMjM0NTY3ODkw
MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NSIsIk5BVkNoZWNrSUQiOiIxMjM0NTY3ODkwMTIzN
DU2Nzg5MDEyMzQ1Njc4OTAxMjM0NSJ9.a5A3a9RxejRJxtjfD4lCb1J8GanxRXVwOH74XlWmbin
WvcY_qbZWK_MnpL8F7NsNsQ8L6JNC5DbYMwgUM1d2hl_msGouRAN4huKCoz5gb5W3btagES
mjShca3COWGCLlk48r0r3DIXNtcnDMgYcXI7ZBjYG_o0e4GYC30HTFtgl1Vv1zBxuhJgFI6xdCOAIo
9Pxz6kbDd9ry27llyxbap1CDHQjriQUSOkX_E1DqvJqXk-
SPWSJRjPeeLkX43tMx3VxD478nZDNTJFJcIWiGnOWGwvBuFR7RlQACPcg-
gMAzchpDzJoWnJbW4DMLQl-k8NCwLOlx9MxPpSTrtTuksw

detached jwt példa

ugyanaz, mint az előző, csak a két pont közötti rész ki van vágva

eyJraWQiOiIvU049MTUzNDk3MDAxNTU4NDI0MDQwNjMvQz1lVS9MPUJ1ZGFwZXN0L09VPW9u
bHlfZm9yX2RldmVsb3BtZW50X3VzZS9DTj1wMTkwMjZfb3BlbmJhbmtpbmdfLV9hcGlfdXNlcl9j
ZXJ0aWZpY2F0ZXMiLCJ0eXAiOiJKV1QiLCJhbGciOiJSUzUxMiIsImlhdCI6MTU4Nzk4NDkzNSwian
RpIjoiMWM4MDNlYWYtOTEwNS00NWZhLWE5YTEtODIwOGUzOGVmYTNmIn0..a5A3a9RxejRJx
tjfD4lCb1J8GanxRXVwOH74XlWmbinWvcY_qbZWK_MnpL8F7NsNsQ8L6JNC5DbYMwgUM1d2hl
_msGouRAN4huKCoz5gb5W3btagESmjShca3COWGCLlk48r0r3DIXNtcnDMgYcXI7ZBjYG_o0e4
GYC30HTFtgl1Vv1zBxuhJgFI6xdCOAIo9Pxz6kbDd9ry27llyxbap1CDHQjriQUSOkX_E1DqvJqXk-
SPWSJRjPeeLkX43tMx3VxD478nZDNTJFJcIWiGnOWGwvBuFR7RlQACPcg-
gMAzchpDzJoWnJbW4DMLQl-k8NCwLOlx9MxPpSTrtTuksw

4.7. JWT header

jwt header	érték	megjegyzés
"kid"	a generáláshoz használt kulcs azonosítója	a kid http headerből vett érték
"typ"	"JWT"	konstans
"alg"	"RS512" vagy "ES256"	az alkalmazott algoritmustól függően
"iat"	unix timestamp (integer)	sysdate() kell bele
"jti"	generált random UUID4	egyedi kell legyen

{
 "kid": "/SN=15349700155842404063/C=HU/L=Budapest/OU=only_for_development_use/CN=p19026_openbanking_-_api_user_certificates",
 "typ": "JWT",
 "alg": "RS512",
 "iat": 1585563716,
 "jti": "e395cf5e-0fc4-430b-9f7e-bee20855b475"
}

https://jwt.io/#debugger-io

4.8. Base Url

A base url az éles és teszt környezet esetén eltér.

Teszt környezet: https://pay-api-int.raiffeisen.hu

Éles környezet: https://pay-api.raiffeisen.hu

Fontos, hogy teszt környezetes apikey-ek a teszt környezeten fognak működni, valamint teszt környezeten lesz jogosultságuk az adott műveletekre, ugyanígy éles környezeten lévő apikey-k az éles környezeten fognak működni. Éles környezeten teszt apikey beküldése INVALID_APIKEY hibához fog vezetni.

Éles környezeten is be kell állítani a felhasználóhoz tartozó jogosultságokat (lásd később Raiffeisen PAY Portál beállítás) ugyanúgy, mint teszt környezeten. Ha adott éles környezeten lévő felhasználónál nincs beállítva az adott jog - például nincs bepipálva a PAY portálos felhasználójánál az EAM jogosultság, és így hívja az eam műveleteket - szintén INVALID_APIKEY hiba fog a válaszban érkezni.

4.9. Minta hívások

4.9.1. EAM Init minta hívás

Az alábbi minta hívás példák teszt környezeten történtek.
(https://pay-api-int.raiffeisen.hu)

/qr-v1/rafipay-eam-v1/eam-init

request

```
curl --location 'https://pay-api-int.raiffeisen.hu/qr-v1/rafipay-eam-v1/eam-init' \
--header 'accept:  application/json' \
--header 'content-type:  application/json' \
--header 'x-correlation-id: 54133eca-85dd-4855-ad83-da0056b06e13' \
--header 'x-request-id: dd6931fc-56b5-44d5-8e80-e7ac4abcf7d7' \
--header 'x-jws-signature:
eyJraWQiOiIvU049Mjc0MjgyOTU3Mzg1NDc5NDk2ODEwNDU0NzYyMDcwMjUxMzE3MD
A0L0M9SFUvTD1CdWRhcGVzdC9PVT1vbmx5X2Zvcl9kZXZlbG9wbWVudF91c2UvQ049c
DE5MDI2X29wZW5iYW5raW5nXy1fYXBpX3VzZXJfY2VydGlmaWNhdGVzIiwidHlwIjoiSld
UIiwiaWF0IjoxNzI0MzM3MTExLCJqdGkiOiI1YTc3YjkxZC04NWI3LTRhZDQtYjk0NS0wNT
EwZWVlZTM3YWUiLCJhbGciOiJSUzUxMiJ9..PUVbWCggzp31wgN_uUBkSaurA_KHR9CD
p21vAAbGr5xaAuTgGPz-
ZKZ7m26JbAoHAP4UKzZ8urKGkAg6wAklpVM0ONQopDZ7m56r26ExK0S0bMKYpLiSzik
RkD4glsYtXx7hUzymOwWZAuSWx5n_h9glEgrTrC4XTtlf3dLPK5N62xVLmEQzc3ktxZjXF
Le015knUbZyCFX-
boqw6nT3MaqfbubcoqMOyxk2WcEMC5DKxyd7Q35WkF1fjde8tj99N3vNimHESfqbSbKf
OpM1-
BxVgY2bPqmu4ibI7qVLHqSi2cCMtpTnoPxDgexQVOePJBrtoLR5WUS9gUSGhlZ_Yw' \
--header 'x-api-key: **********' \
--data
'{"payeeInfo":{"terminalReference":"TESTEAM01","shopId":"0123456789","accountNumb
er":"HU91120113510184523800100006"},"paymentInfo":{"deviceType":"CASHREGISTER","
allowedModes":{"nfcAllowed":false,"qrAllowed":true,"deeplAllowed":false},"transactio
nCurrency":"HUF","expiryDateTimeOffset":5,"transactionReference":"ID885949135","inv
oiceReference":"invoiceReference001","transactionAmount":10,"purposeCode":"IPPS","c
ustomerReference":"customerReference001","remittanceInfo":"EAM
generate","editableFields":{"isRemittanceInformationEditable":false,"isCustomerIdEdi
table":false,"isAmountEditable":false}}}'
```

response

```
{
   "paymentReference": "IN240822d1oMKheZ9",
   "creationDateTime": "2024-08-22T14:31:53.854Z",
   "expiryDateTimeOffset": 5,
```

```
  "paymentUrl": "https://teszt-
azonnalifizetes.hu/HCT/3/1/UBRTHUHBXXX/Teszt/Teszt/HU91120113510184523800100
006/HUF10/20240822163153%2B2-
0000005/IPPS/EAM%20generate/0123456789.UBR2.1.12345678.INNOHUH0/TESTEAM01
/invoiceReference001/customerReference001/ID885949135_IN240822d1oMKheZ9/htt
ps%3A%2F%2Fwww.afr.com%2F/___/15.mw0wBCecaVTdDnNQkV9U6wQUEG9-
O8wVQ6M79fzXEPe9F-
ebta9wwOQVOw7hoVXTreq0GZXCR138fi3CKPt6zchiMfkRuhX6yd7l_WMm79G5DO52u
DizSrr352Zlslk-"
}
```


4.9.2. EAM query minta hívás

/qr-v1/rafipay-eam-v1/query-by-payment-reference

request


```
curl --location 'https://pay-api-int.raiffeisen.hu/qr-v1/rafipay-eam-v1/query-by-
payment-reference' \
--header 'accept:  application/json' \
--header 'content-type:  application/json' \
--header 'x-correlation-id: ceb7817c-eed4-4e98-b4d4-a378240bac7f' \
--header 'x-request-id: 632e1a32-3d62-4764-88f0-7a136539a0cc' \
--header 'x-jws-signature:
eyJraWQiOiIvU049MTM4NjIvQz1IVS9MPUJ1ZGFwZXN0L09VPW9ubHlfZm9yX2RldmVsb
3BtZW50X3VzZS9DTj1wMTkwMjZfb3BlbmJhbmtpbmdfLV9hcGlfdXNlcl9jZXJ0aWZpY2
F0ZXMiLCJ0eXAiOiJKV1QiLCJpYXQiOjE3MjQzMzk0MjUsImp0aSI6IjE1NWRmYmVmLTE3
MWEtNDFlYy1hMmQ3LTkzMGJkNGNkYTdjMCIsImFsZyI6IlJTNTEyIn0..FPqxfL-
CQMK4xX6wF2RAI8fwaNDDyABKSXhczAsvQ7BL83q6W0wNhYqJg2DcCi3Ir5q95nPtPF
MGFwhKVxvYyezahtIXddUi5M6MOwjz6f9J4TqxWtRTyykPzgCn6vYbL6qdI5BIr0WRK2Ii
67X2YoGNLGCho_CM2SglCR0eq5Q0wCQ9sgLI0VW9jnsV0-
ZqxD1lPHy7rABfQcuR9WR4TMDHDvqLytfpqI7Cz853bnHJ5NvAQ7I1vtwcWuoBYEbMgA
mrmsDky6MJOZHU_dT-
NoqbUSEXBj4BtpULZZ0ie9jIV6gMNJYXUILhQYbXjlr0JUNaAdHJsZ2RO_ZsYXmVgg' \
--header 'x-api-key: ************' \
--data '{"paymentReference":"IN240822d1oMKheZ9"}'
```


response


```
{
  "paymentStatus": "RECEIVED"
}
```


/qr-v1/rafipay-eam-v1/query-by-payment-reference

request

```
curl --location 'https://pay-api-int.raiffeisen.hu/qr-v1/rafipay-eam-v1/query-by-transaction-reference' \
--header 'accept:  application/json' \
--header 'content-type:  application/json' \
--header 'x-correlation-id: ff2cbbc9-82c5-4713-a07d-f308a14da8bf' \
--header 'x-request-id: d561e4c0-2155-4efa-9ba4-06c4d0953e70' \
--header 'x-jws-signature: eyJraWQiOiIvU049MTM4NjIvQz1IVS9MPUJ1ZGFwZXN0L09VPW9ubHlfZm9yX2RldmVsb3BtZW50X3VzZS9DTj1wMTkwMjZfb3BlbmJhbmtpbmdfLV9hcGlfdXNlcl9jZXJ0aWZpY2F0ZXMiLCJ0eXAiOiJKV1QiLCJpYXQiOjE3MjQzMzk3MTksImp0aSI6ImQyODc1NzliLWQzMzItNGQwMC1hMzY4LTViYTY4NzMyNDZiMCIsImFsZyI6IlJTNTEyIn0..bEdRpDG7eWb9wGPqM1j8J4cC5ykrj6meAuX85L9aj67i8sEHdI-tmpkMjIkmCpVQjF-02UqpRI5ThNV6sowv30bZY79QZeFfAqg-95p4zhW0RGD9Mt1-59pskVFO3gIUzyxZ7DCo21jA5L88aBh1HxvbmKefuJnS7TmGA0P0SyCS1QxAwtu_IFrm_LNXwx4LjwkhteUjF_bPMep1VH0YGcR9AHnLi-mxGsAtCblmrWo9flztWkyiaqDrzRNsLL8P7CPpB2Y8ii5ksmcpTFktcyqI6LxVBleyHuUNQowgThRGtJyP_ZFNbvZH6DpSMybjrafMxSKF6YZXsFI60GoLHg' \
--header 'x-api-key: ********** \
--data '{"transactionReference":"ID885949135"}'
```

response

```
{
   "paymentStatus": "RECEIVED"
}
```

4.9.3. Cancel EAM mintahívás

/qr-v1/rafipay-eam-v1/eam-cancel

request

```
curl --location 'https://pay-api-int.raiffeisen.hu/qr-v1/rafipay-eam-v1/eam-cancel' \
--header 'accept:  application/json' \
--header 'content-type:  application/json' \
--header 'x-correlation-id: 00fda037-b6f0-488f-8ed2-a1bde0060cfa' \
--header 'x-request-id: 5bd95f04-ed06-4dce-b881-95b0e8c44ab6' \
--header 'x-jws-signature: eyJraWQiOiIvU049MTM4NjIvQz1IVS9MPUJ1ZGFwZXN0L09VPW9ubHlfZm9yX2RldmVsb3BtZW50X3VzZS9DTj1wMTkwMjZfb3BlbmJhbmtpbmdfLV9hcGlfdXNlcl9jZXJ0aWZpY2F0ZXMiLCJ0eXAiOiJKV1QiLCJpYXQiOjE3MjQzMzk4NzAsImp0aSI6ImVjNjBiNmFhLWJjMWQtNDQ3Yi04MjE4LTVhOGRjNzQyM2U3MCIsImFsZyI6IlJTNTEyIn0..QuUy_l4qm
```

LXI3nfriy5ePxZaJi7q99gTqt923-0FAcnbj_4zvfYFHJx2hsVM3KtSnqHsqlU_WqU-6NErnNBkqYGkhSZFZuOnZ2xRwm4K0j4ZX8D_IqgLMVft88GVQSgJkxatOi9PnBoPOZJDHGV9V3BHaRmKOlVnvMzuBtUmvziK_BYN1DGGnViUI3JMzFSsXioffEI0dbcjjlphnk-oLyrA1ri0MHcKF-DH_q2hJyxcDcr7vkONyWkQiNpLvnq9H01bPOrKtIObDaDWZ78AN1pV_tel8k_QUiN9Hu12Lscd_qcjLJ0Qtw2j9ZyLCbEMD9PBCyNSYJbqbUQ_-Z-mXw' \ --header 'x-api-key: ********** \ --data '{"paymentReference":"IN240822ZIjmXRxBR"}'
response
Status 204

4.10. Karakterhasználat korlátozása

Az UTF-8 szerinti összes alapkarakteren (a 32-126 közötti tartományban) felül kizárólag a 128 fölötti „extended" ASCII tartományban található magyar ékezetes karakter használható.

Tételes felsorolás:

ASCII 32 – 126:

szóköz, ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~

ASCII 128 fölött:

á Á é É í Í ó Ó ö Ö ő Ő ú Ú ü Ü ű Ű

Az EAM igénylése során a Transaction reference és a Payment Reference mezőben nem szerepelhet alsó kötőjel (_). Az üzenetekben megadott mezőhosszok és a QR képgenerálásra alkalmas mérethatár betartása URL Safe (%-os) kódolás után értendők.

A fordított törtvonal (\) reprezentálása kizárólag a karakter duplikálásával (\\) történhet, mert egyébként a rendszer hibaüzenetet ad.

A fizetési kezdeményezésben nem szerepelhet xml üzenet validációját megakadályozó karaktersor (pl. xml-ben nem engedélyezett HTML entitás)

4.11. Egyéb hivatkozások

A **kedvezményezett (belső) tranzakció** azonosítója (transactionReference) végig kíséri az üzenet életútját. Ezt az adatot a kedvezményezett, vagy a kedvezményezett rendelkezésére bocsátott végpont képezi. Az azonosító célja, hogy a kedvezményezett minden üzenetben

nyomon követhesse a megbízásának feldolgozását, hiszen az adat a számlakivonaton és a státuszinformáció üzenetben is megjelenik. A kedvezményezett azonosítója a bankközi térben nem az end-to-end Id rovatba kerül, mert azt a GIRO szabványalkalmazás a fizető fél bankja számára meghatározott módon rendeli kitölteni. A kedvezményezett belső tranzakcióazonosítója az EAM-ban egy rovaton (credTranId) osztozik az Aggregátor egyedi azonosítójával, ezáltal a kedvezményezett bank is egy adattá összefűzve kapja meg a két azonosítót a bankközi átutalás üzenetben (vagy az EAM kódban).

Az ***Aggregátor egyedi műveleti azonosítója (paymentReference)*** szintén végig kíséri az EAM életútját. Az Aggregátor ezt az azonosítót az EAM igénylés válaszüzenetében, az URL kódban adja meg. A paymentReference azonosítót kell használni a státusz lekérdezésekhez, illetve az EAM visszavonása során is. Az Aggregátor egyedi azonosítója a kedvezményezett (belső) tranzakcióazonosítójával egybefűzve kerül az URL-be és a kedvezményezett bankja a CredTranId rovatban alsó kötő jel összefűzéssel a két azonosítót egy rovatban ('tag') kapja meg és bocsátja ügyfele rendelkezésére. Megjegyzendő, hogy az Aggregátor (statisztikai célból) az általános üzleti validációs hibákkal visszautasított createPayment kezdeményezésekhez is hozzárendel egy ilyen azonosítót.

4.12. Callback URL

A Callback URL használata azokban az esetekben értelmezett, amikor a fizetési folyamatot a fizető fél eszközén lévő, a mobilbanki alkalmazástól eltérő alkalmazásból kezdeményezik. A CallBack URL segítségével a fizetés végén a fizető fél visszatérhet arra a felületre, ahonnan a vásárlást kezdeményezte. Ilyen felületek lehetnek: online áruház fizetés státusz oldala, alkalmazáson belüli vásárlás esetén az adott alkalmazás fizetés státusz oldala, vagy loyalty alkalmazás fizetés utáni landing oldala. A felület önmagában is jelzi a fizetés sikerességét, vagy elutasítását.

Az Aggregátor által megképzett EAM-ba internetes vásárlás esetén URL, alkalmazáson belüli vagy loyalty alkalmazásos vásárlás esetén pedig Deeplink igényelhető.

Abban az aesetben, ha IPEW kódot kívánnak használni a callback url megadása kötelező előzetesen a szerződéskötés alkalmával, API hívás során nem kell adni a callback urt-t.

5. Azonnali fizetés arculati elemeinek megjelenítése

Az MNB célja a piaci gyakorlat egységesítése az Azonnali Fizetési Szolgáltatáshoz kapcsolódó arculati elemek megjelenítésére vonatkozóan. Az MNB elvárja, hogy minden piaci szereplő maradéktalanul betartsa az Arculat kézikönyvben foglalt alapvető tájékoztatási szabályokat, melynek értelmében meg kell jeleníteni az Azonnali Fizetés logóját minden az Azonnali Fizetés szabályai szerint feldolgozott tranzakciók esetében.

Az MNB nemrég döntést hozott arról, hogy az Azonnali Fizetésre épülő szolgáltatások a jövőben a ***qvik*** összefoglaló márkanév alatt jelennek majd meg. A qvik kialakítása során az MNB célja egy könnyen kimondható, más fizetési módoktól egyértelműen megkülönböztethető és a fizetés gyorsaságára utaló márkanév bevezetése volt.

A qvik bevezetésével az MNB kiadta a hozzá kapcsolódó Arculati kézikönyvet, amely szabályozza a piaci szereplőket, hogy hogyan jelenítsék meg az Azonnali Fizetésre épülő szolgáltatások egyedi logóit és piktogramjait. A kézikönyv emellett iránymutatásokat fog tartalmazni arra vonatkozóan is, hogy a pénzforgalmi szolgáltatók hogyan segítsék és várják el üzleti partnereiktől az Azonnali Fizetésre épülő elfogadói szolgáltatások nyújtása során az Azonnali Fizetéshez kapcsolódó marketing elemek megjelenítését.

A mindenkor hatályban lévő arculati kézikönyv itt érhető el:

https://www.mnb.hu/penzforgalom/azonnalifizetes/gyakori-kerdesek-valaszok/arculati-elemek

6. Raiffeisen PAY Portál beállítás

6.1. Raiffeisen PAY Portál

A Raiffeisen PAY Portál az API-hoz kapcsolódó adminisztratív feladatok ellátását szolgálja.

Elérhetőség: https://pay-portal.raiffeisen.hu

A Portál használatának feltételei:

- Raiffeisen Banknál vezetett folyószámla
- Raiffeisen PAY szerződés és a folyószámlára vonatkozó admin jogosultság
- Raiffeisen PAY admin felhasználónév és aktiválókód

A következő beállításokat szükséges elvégezni a portálon az API kapcsolat létrehozásához:

1. Rendszeradminisztrátor aktiválása
2. Új Felhasználók létrehozása
3. Jogosultság beállítása a jogosultságok szerkesztése képernyőn
4. PKCS#10 RSA2048-SHA512 algoritmussal készített CSR (Certificate Signing Request) kérelem feltöltése a Tanúsítványok fülön (A CSR állományokban custom attribútumként szerepeltetni kell az API felhasználónak, mint kliensnek és alkalmazottainak bank által ismert azonosítóit)
5. a Bank által aláírt Certificate letöltése

A Raiffeisen PAY Portál tesztkörnyezetben nem elérhető, az alábbi beállításokat a Raiffeisen Bank végzi el az ügyfél helyett a tesztelés során.

6.2. Rendszeradminisztrátor aktiválása

A Raiffeisen Pay hozzáférés létrehozását követően a rendszer adminsztrátor szerepkörben megadott személy a telefonszámára (a Banknak megadott és beállított telefonszámára) sms aktiváló kódot kap, amelyet aktiválni kell. A https://pay-portal.raiffeisen.hu oldalon aktiválás menüre kell kattintani, beírni a Direkt azonosítót és az SMS-ben kapott aktiváló kódot. Az aktiválás után lehet megadni a bejelentkezési jelszót.

Az aláírási jelszó 365 napig érvényes, utána meg kell változtatni. Amennyiben rendelkezik Direktnet hozzáféréssel meg tudja változtatni az ügyintézés\beállítások\jelszóváltoztatás menüpontban.

6.3. Belépés

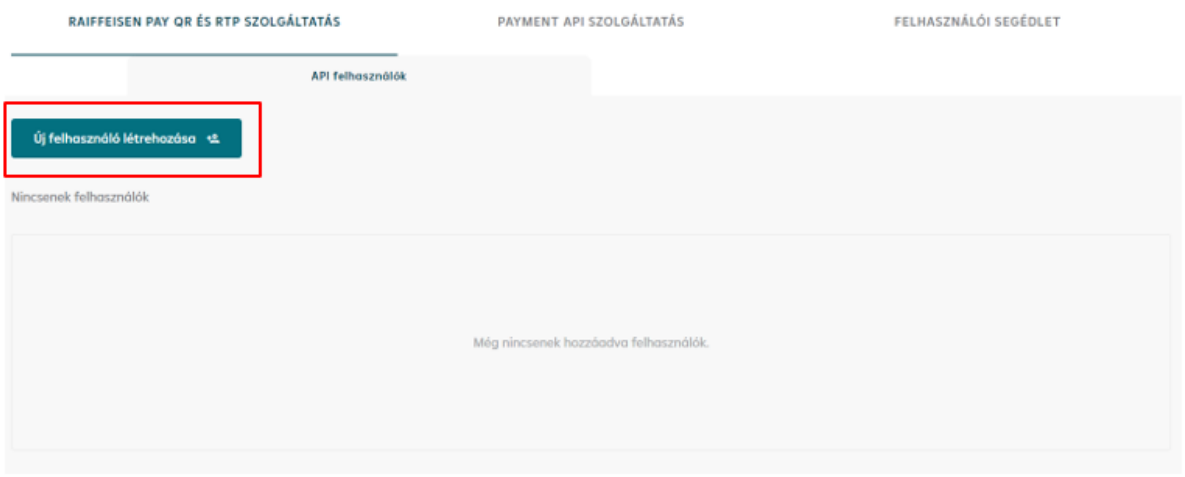
Belépés menüre kell kattintani, beírni a Direkt azonosítót és a jelszót, majd az SMS-ben kapott aktiváló kódot.

6.4. Sapka váltás

Amennyiben több Raiffeisen Pay felhasználóval is rendelkezik, mert több céget is hozzárendelt a szolgáltatáshoz a cégek között a fejlécben található felhasználónév melletti ikonra kattintva lehetséges a váltás.

6.5. Új felhasználó létrehozása

A portálon az Új felhasználó létrehozása gombra kell kattintani ahhoz, hogy az API kapcsolatot létre lehessen hozni.



Először meg kell adni a felhasználó nevét. A névben ékezetes karakter és szóköz nem szerepelhet. A felhasználónév a tranzakciók esetében megjelenhet a különböző banki alkalmazások esetében, ezért ennek megadásakor érdemes körültekintően eljárni.

Az alkalmazható karakterek:

AÁBCDEÉFGHIÍJKLMNOÓÖŐPQRSTUÚÜŰVWXYZ

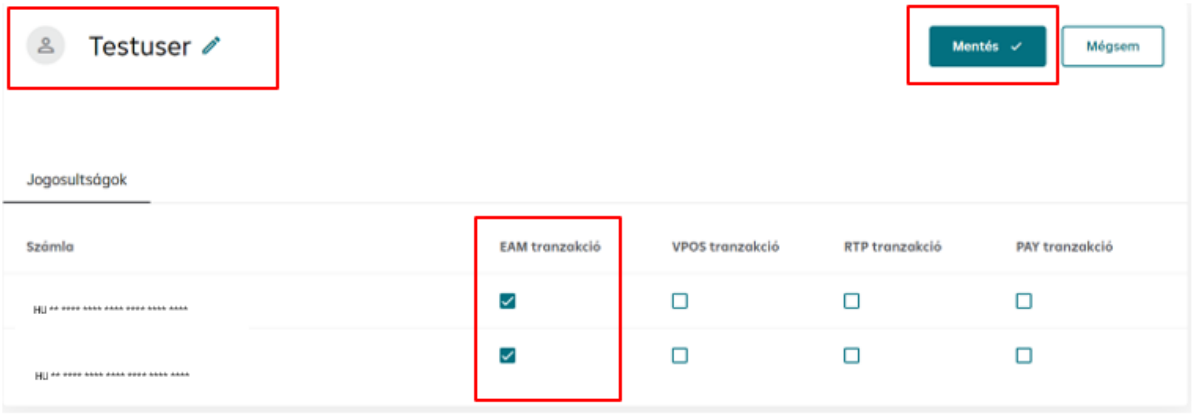
aábcdeéfghiíjklmnoóöőpqrstuúüűvwxyz

1234567890

]#$%&()+,-./;:?@_{}!

Szóköz

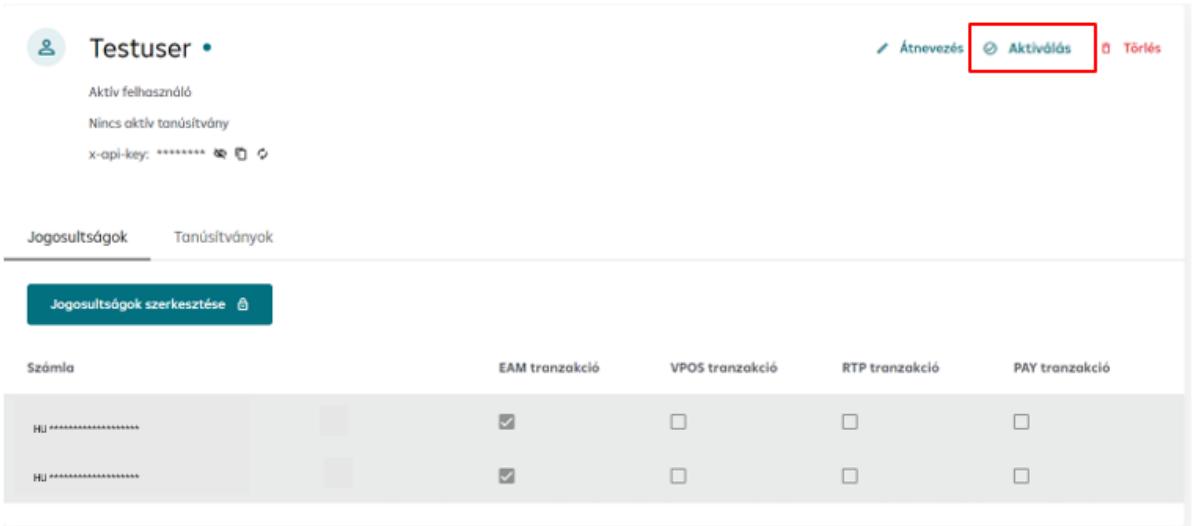
Ezután ki kell választani a számlát és be kell jelölni az EAM tranzakció jogosultságokat, majd Mentés gombra kell kattintani.



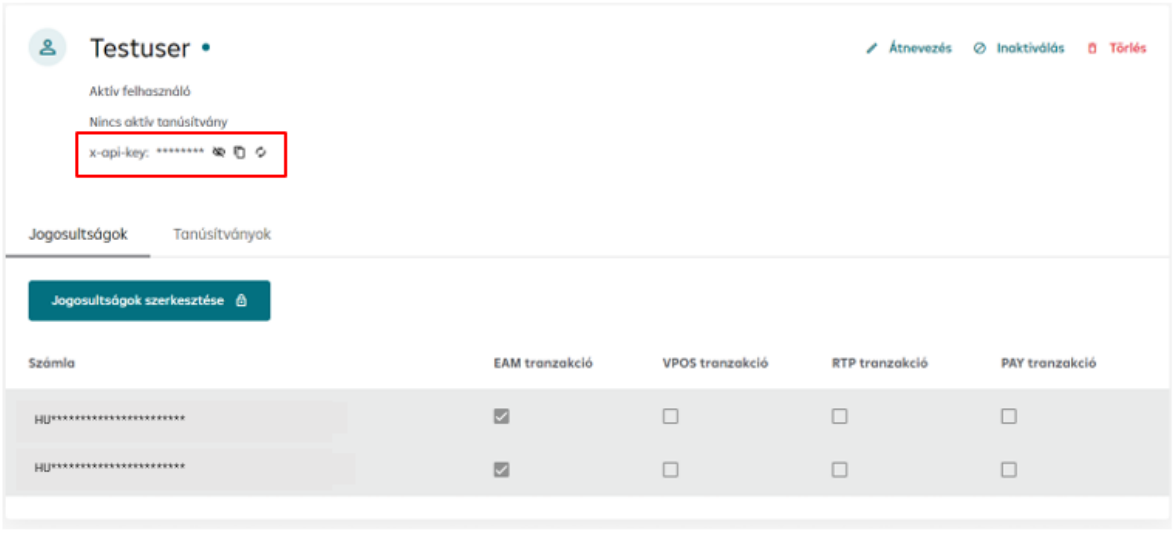
Alá kell írni a megbízást, jelszó+SMS kombinációval. Figyelni kell arra, hogy amennyiben sapkát vált, tehát másik azonosítóval használja a szolgáltatást, akkor ahhoz a szolgáltatáshoz tartozó belépési jelszót kell megadni a felhasználó létrehozása során.

Amennyiben háromszor rossz jelszót ad meg, akkor a rendszer kitiltja. Ahhoz, hogy tudja használni a szolgáltatást új aktiváló kódot kell kérni a banki kapcsolattartójától.

A rögzítés után aktiválni kell a felhasználót az Aktiválás gombra kattintva. Az aktiválás is ugyanúgy aláírás köteles, mint a felhasználó létrehozása.



A kliens authentikációhoz szükséges API key itt érhető el:



7. Hitelesítési folyamat beállítása

7.1. Konfigurációs file előállítása

A cég adatai és a törzsszám felhasználásával az alábbi minta szerint kell előállítani a konfigurációs fájlt:

 csr_details_minta_v02.txt	**csr_details_minta_v02.txt**

```
oid_section = oids

[req ]
default_bits = 2048
prompt = no
default_md = sha512
distinguished_name = dn
req_extensions = req_ext

[ oids ]
apiUserType = 1.2.3.45

[ dn ]
C=HU
ST= Budapest
L= Budapest
O=APIUser
OU=APIUser_OU
emailAddress=admin@domainnev.hu
CN = apiuser@domainnev.hu

[ req_ext ]
subjectAltName = @alt_names
basicConstraints = critical, CA:FALSE
keyUsage = digitalSignature, keyEncipherment
apiUserType = ASN1:UTF8String:PaymentHUB
2.5.4.97 = ASN1:UTF8String:AB1234

[ alt_names ]
DNS.1 = domainnev.hu
```

A CSR formai kellékeként elvárjuk, hogy custom extensionben szerepeljen a vállalat Raiffeisen Banknál nyilvántartott törzsszáma (basicnumber), például AB1234 (csak szám is lehet, 123456)

Ez a rövid (13 jegyű) számlaszám középső részében található: példaként 6700- AB1234-001

A kiemelt mezőértékek példák a kitöltésre. Értelemszerűen a valós adatokkal töltse ki!

Megnevezés	**Magyarázat**
ST	a megyét írja be, ahonnan igénybe veszik szolgáltatást
L	a várost írja be, ahonnan igénybe veszik szolgáltatást
emailAddress	az rendszergazda felhasználó email címe, aki az „API felhasználót" is létrehozta a Raiffeisen Pay Portálon
CN	A kiállítandó tanúsítványban a Common Name mező értéke. Konvenció szerint: apiuser@domainnev.hu, ahol a domainnev.hu a vállalkozás saját webhelye (de lehet egyéb emailcím is)
2.5.4.97	Reserved OID, a szervezet azonosítására. Ide a ASN1:UTF8String:AB1234 példában az utolsó kiemelt 6 jegy cserélendő a vállalat törzsszáma (basic number, fontos, hogy ne legyen szóköz a 6 karakter és a kettőspont között).
DNS.1	A vállalat webhelyének nevét kérjük ide másolni (a SAN – subject alternative name blokk képzéséhez)

7.2. Privát kulcs és CSR fájl generálása

A hitelesítési token aláírásához szükséges privát-publikus kulcspár és a certificate signing request (CSR) fájl létrehozása nélkülözhetetlen.

Az előállított konfigurációs fájlt felhasználva az openssl használatával elő kell állítani a privát kulcsot és a CSR állományt, az alábbi minta szerint:

openssl
openssl genrsa -out **key.pem** 2048
openssl req -new -key **key.pem** -out **csr.pem** -config < **csr_details.txt**

Kulcsgenerálás és -kezelés kereskedő által biztosított eszközön (POS, Kassza, SoftPOS):
A Sub-Aggregátor vagy Technikai Aggregátor által megvalósított kulcsgenerálási és kulcskezelési folyamatnak a következő követelményeknek kell megfelelnie:

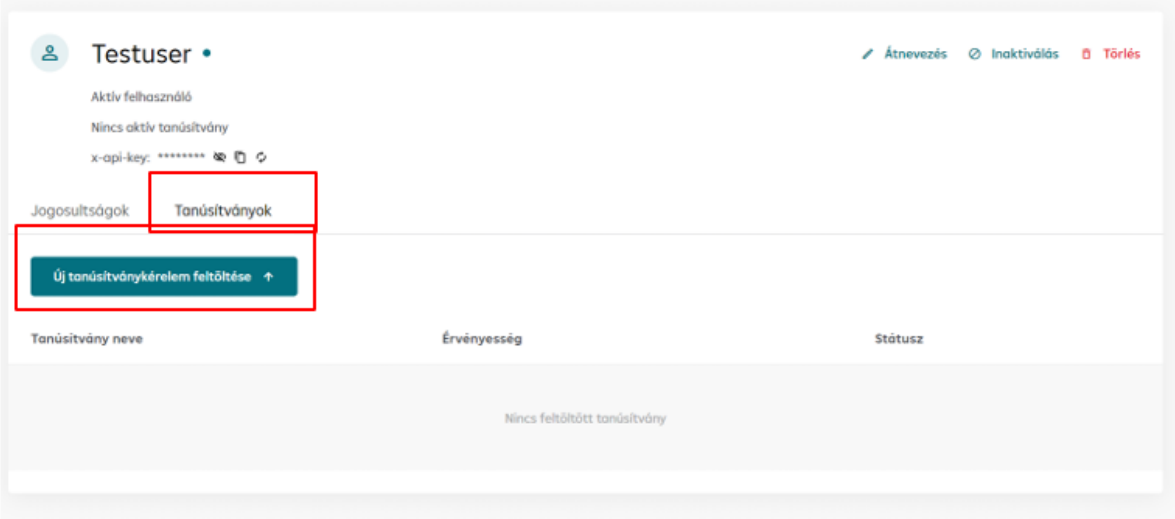
A Végponti Szoftver kulcspárokat generál és azokat a Végponti Szoftvert futtató rendszer biztonságos tárhelyére menti. Biztonságos tárhelynek minősül:

- Legalább FIPS 140-2 certifikációval rendelkező Hardware Security Module
- Android Keystore system
- Microsoft CNG key isolation architecture
- Apple Secure Enclave

7.3. CSR fájl feltöltése és CERT letöltése a Raiffeisen PAY Portálon

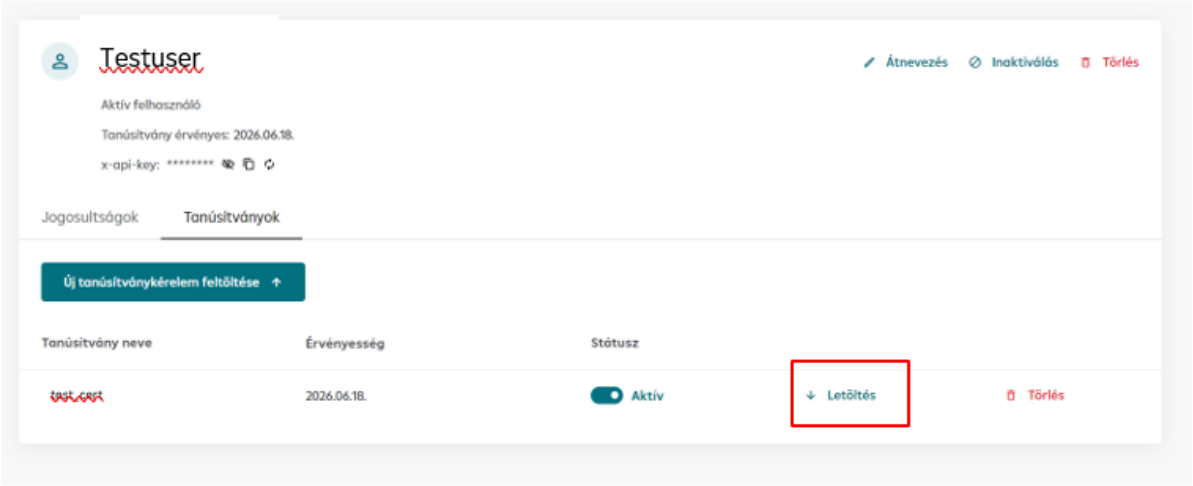
A Tanúsítványkérelem (CSR fájl) feltöltésének és az API-ban használható Tanúsítvány (CERT fájl) letöltésének folyamata:

A Tanúsítványok fülön elérhető új tanúsítványkérelem feltöltése gombra kell kattintani.



Majd ki kell választani a CSR fájlt, fel kell tölteni és el kell nevezni, majd a szokásos módon alá kell írni a megbízást.

Az API használatához a tanúsítványt le kell tölteni a letöltés gombbal.



7.4. KID generálása a cert fájlból

A Raiffeisen Pay Onboarding Portálról letöltött cert.pem fájlból ki kell olvasni néhány adatot:

openssl
openssl x509 -in **cert.pem** -text –noout

Ezeket az alábbiak szerint kell összeállítani, hogy megkapjuk a KID-et:

cert mező		**érték (minta)**
Serial Number		12345678 (0xBC614E, BC:61:4E) **ez módosul az új folyamatban, sokkal hosszabb lesz, ezt érdemes megvizsgálni**
Issuer	C	HU
	L	Budapest
	OU	raiffeisen_bank_zrt
	CN	openbanking_-_api_user_certificates
összeállított kid		
/SN=12345678/C=HU/L=Budapest/OU=raiffeisen_bank_zrt/CN=openbanking_-_api_user_certificates		

A saját webshop alkalmazásba a key.pem fájlt és a KID-et kell betölteni.

8. Tesztelés

Minden partnernek egyedi teszt felhasználói adatokat biztosít a Bank.

9. Kapcsolat és hibabejelentés

Raiffeisen PAY szolgáltatással kapcsolatos kérdése esetén kérjük forduljon a Raiffeisen Bank Ügyfélszolgálatához, mely munkanapokon 8 és 17 óra között teljes, munkaidőn kívül pedig csökkentett kapacitással áll rendelkezésére, az alábbi elérhetőségeken:

Telefonon: +3680488588 (RaiffeisenDirekt 3.1, E-csatornák menüpont)

E-mail: raiffeisenpay@raiffeisen.hu

Az API csatlakozással kapcsolatos technikai kérdések kapcsán az alábbi e-mail címen keressen minket: premiumapi_support@raiffeisen.hu