



RAIFFEISEN PAY INNOVATÍV FIZETÉSI SZOLGÁLTATÁS

Online Fizető Oldal

verzió 1.3

Tartalom

1.	Azonnali Fizetési Rendszer 2.0	4
1.1.	Bevezetés	4
1.2.	Azonnali átutalási megbízás benyújtásához alkalmazható egységes adatbeviteli megoldások webes vásárlás során	4
1.3.	A szolgáltatás új szereplői	5
2.	Az egységes adatbeviteli megoldás működésének bemutatása	6
2.1.	Sikeres, a séma alapján kezdeményezett azonnali átutalás	7
2.2.	Hibaág 1: A fizető fél által elutasított fizetési kezdeményezés	8
2.3.	Hibaág 2: A fizető fél mobilbanki alkalmazásában megghiúsult fizetési kezdeményezés	10
2.4.	Hibaág 3: Az azonnali átutalásban résztvevő szereplők bármelyikénél elutasított fizetési kezdeményezés	11
3.	Online Fizetési Oldal	14
3.1.	Integrált fizetési folyamat áttekintés	14
4.	Integráció	15
4.1.	Biztonság és autentikáció	15
4.2.	Base URL	15
4.3.	EAM tranzakció indítás az Online Fizetési Oldalon	15
4.3.1.	Payload összeállítása	15
4.3.2.	Payload becsomagolása jsonString-be	17
4.3.3.	HMAC signature generálása	18
4.3.4.	'Payment start' hívás indítása	18
4.3.5.	Vásárló átirányítása az Online Fizetési Oldalra	19
4.4.	Tranzakció eredményének lekérdezése a kereskedő oldalán	19
4.5.	EAM státusz üzenetek és jelentésük	20
4.6.	Callback URL	21
5.	Azonnali fizetés arculati elemeinek megjelenítése	22
6.	Teszteléshez szükséges lépések	23
6.1.	Tesztadatok	23
6.2.	Raiffeisen PAY Portál beállítás	23
6.2.1.	Raiffeisen PAY Portál	23
6.2.2.	Belépés	23
6.2.3.	Új felhasználó létrehozása	26
6.2.4.	API key, HMAC és Technikai felhasználó azonosítója	28

7.	Élesítéshez szükséges lépések.....	29
7.1.	Raiffeisen PAY Portál beállítás.....	29
7.1.1	Raiffeisen PAY Portál.....	29
7.1.2	Rendszeradminisztrátor aktiválása.....	29
7.1.3	Belépés	30
7.1.4	Új felhasználó létrehozása.....	30
7.1.5.	API key, HMAC és Technikai felhasználó azonosítója.....	33
8.	Kapcsolat és hibabejelentés	34

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 mobil eszközére, mint készpénzhelyettesítő fizetési eszközre történő átadásához.

1.2. Azonnali átutalási megbízás benyújtásához alkalmazható egységes adatbeviteli megoldások webes vásárlás során

QR-kódos vásárlás

A 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).

Deeplink

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.

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 garántálja 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 mobil eszközén 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.

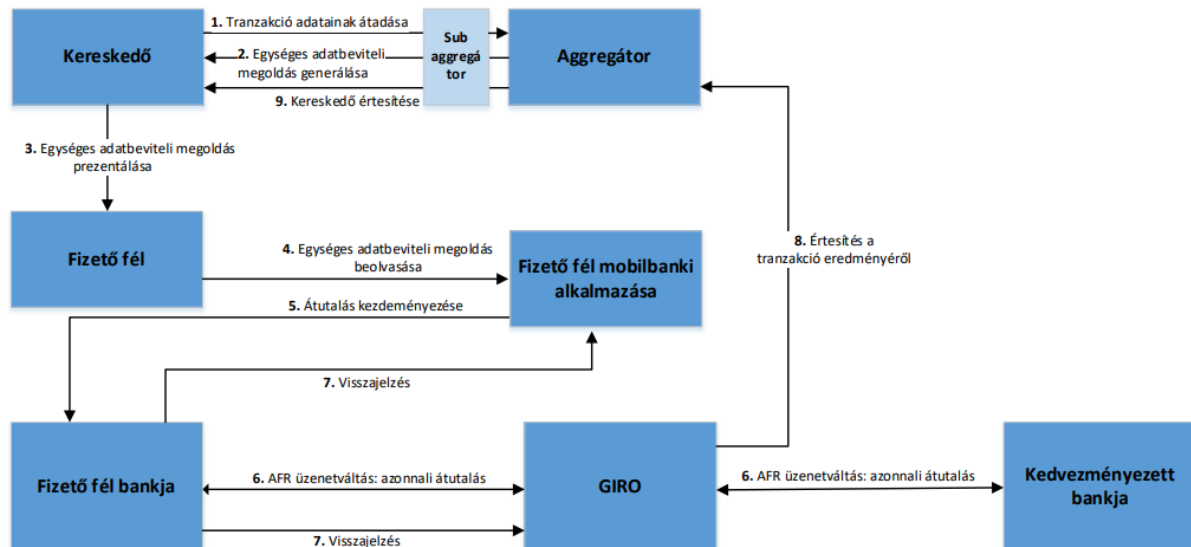
Az EAM fizetés biztonságos, hiszen a fizető félnek nem kell személyes adatait megadni az adatbevitelhez. Csak hiteles kód alapján olvashatók be a mobil eszközbe, illetve az azon futó, pénzforgalmi szolgáltató által biztosított mobilalkalmazásba a megbízás adatok, és a hitelesítő kód eredetiségét és megfelelőségét 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 bármilyen okból történő megghiúsulása esetén is küld értesítést az elfogadói végpont számára.

Az EAM-mal beolvasott átutalási megbízás specialitása, hogy a fizetés kedvezményezettje nem csak az áru vagy szolgáltatás 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 köteget 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

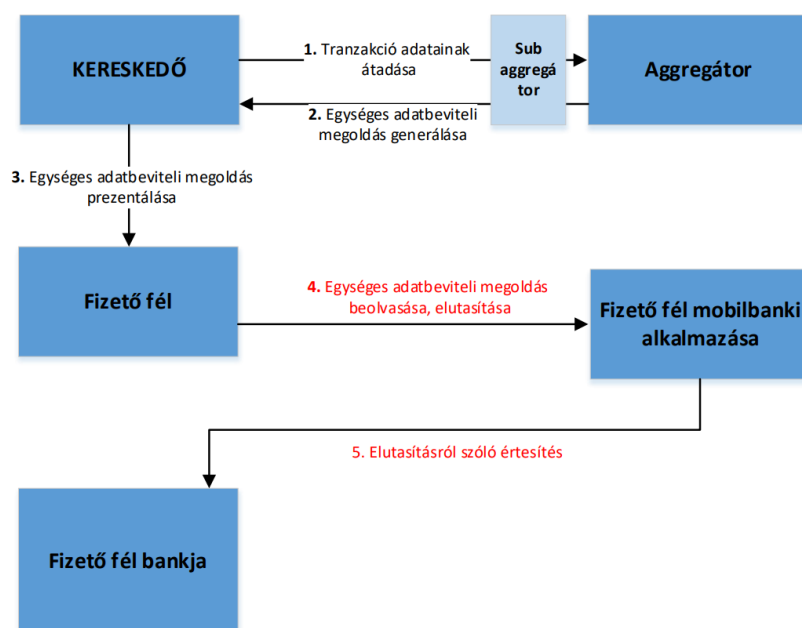
A folyamat lépései:

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

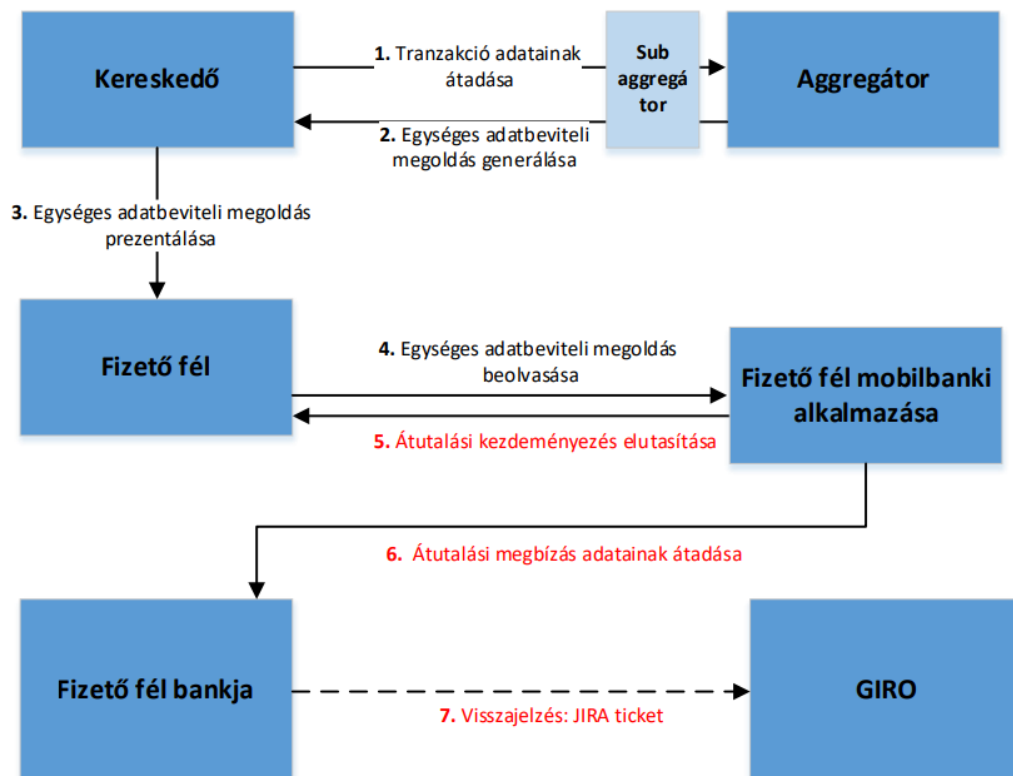


2.ábra – A séma alapján kezdeményezett, többfunkciós eszközön indított azonnali átutalás: a mobilalkalmazás negatív visszajelzése

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 lejáratát 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 megghiúsult fizetési kezdeményezés



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

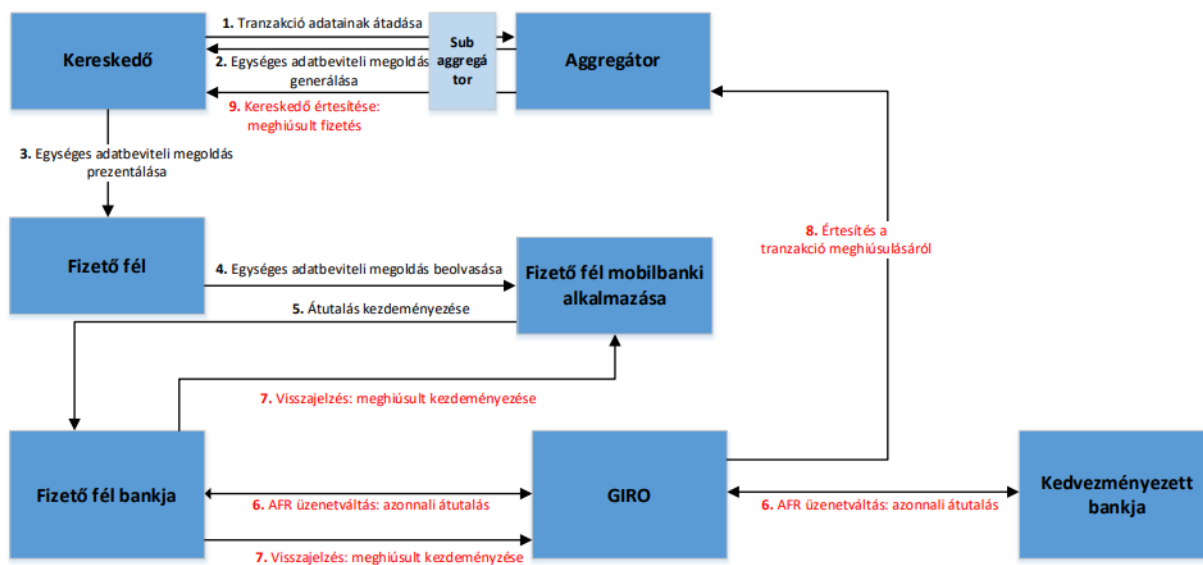
A folyamat lépései:

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 meghíúsulásáról.
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 megíúsulásáról.
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 megghiúsulásáról.

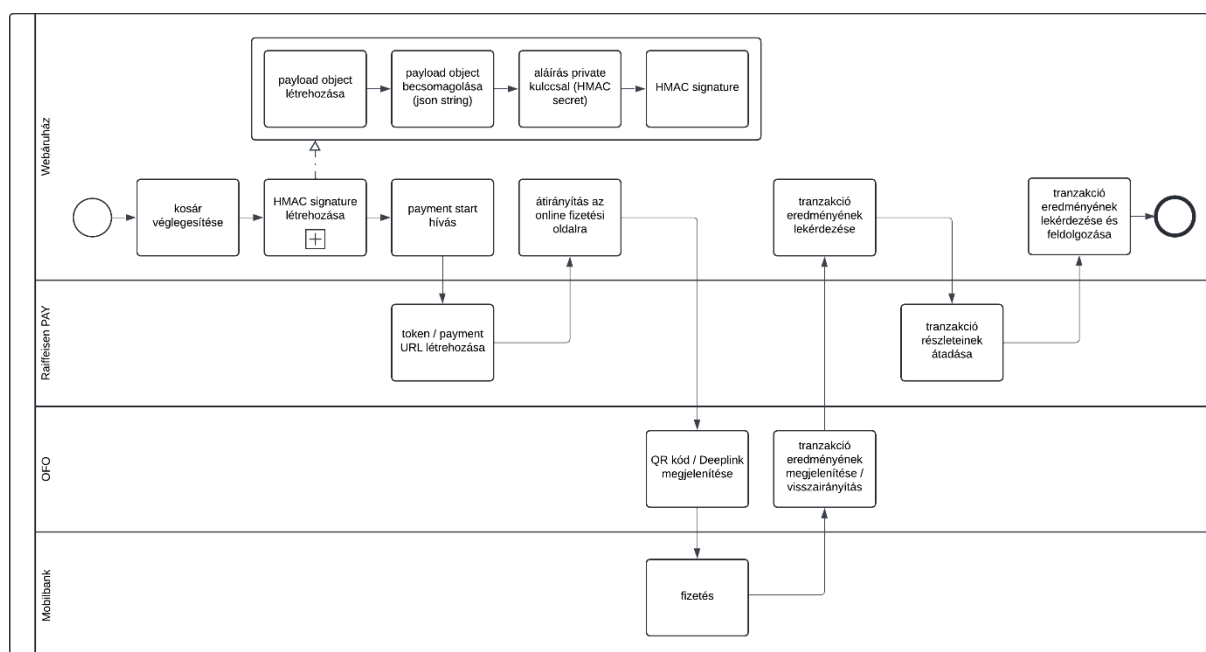
3. Online Fizetési Oldal

Az Online Fizetési Oldal szolgáltatás jelenleg csak az EAM (azonnal fizetés QR kóddal és/vagy Deeplinkkel) fizetési módot támogatja webes vásárlások során. Az Online Fizetési Oldal tehát abban az esetben használható, ha a webes vásárlás során már kiválasztásra került az EAM fizetési mód, vagy a webáruházban csak az EAM fizetési mód érhető el.

Az Online Fizetési Oldal szolgáltatás a Raiffeisen PAY szolgáltatás **weboldalba történő integrációjának** megkönnyítését szolgálja, így az egységes adatbeviteli megoldások közül a **QR kódos fizetés** és a **Deeplinkkel kezdeményezett fizetés** elérhető benne.

A szolgáltatás tartalmazza a Deeplink és QR kód generálást, a fizetési hivatkozás megjelenítésének logikáját (QR és Deeplink), a fizetés indítását és a fizetés eredményének feldolgozását és megjelenítését.

3.1. Integrált fizetési folyamat áttekintés



4. Integráció

4.1. Biztonság és autentikáció

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:

Protokoll: HTTPS

Authentikáció:

- 1) API Key alapú, tehát Hívó fél a regisztráció során kap a banktól, melyet a hívások http headerjében szerepeltetni szükséges
→ X-API-KEY (értékét a pay portálon a regisztrációt követően kapja meg a Banktól)
- 2) Digitális aláírás alkalmazása a magas biztonság érdekében
→ HMAC signature (értékét a pay portálon a regisztrációt követően kapja meg a Banktól)

Éles és teszt környezetben az api-key és a HMAC secret értéke eltérő.

4.2. Base URL

Teszt környezet: <https://pay-api-pc.raiffeisen.hu>

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

4.3. EAM tranzakció indítás az Online Fizetési Oldalon

4.3.1. Payload összeállítása

A kosár véglegesítése után össze kell állítani a payload-ot a Raiffeisen PAY szolgáltatás (rafipay-vpos-service) API sémája alapján. A mezőhosszt url enkódolás után kell figyelembe venni.

Mezők:

Mezőnév	Típus	Mezőhossz	Kötelező	Leírás
technicalUserId	string	5	igen	az API felhasználó technikai azonosítója (pl. 10234) → A technikai azonosítót a Raiffeisen PAY Portálon a Raiffeisen EAM és RTP szolgáltatás fölön az API felhasználó részleteit megnyitva található.
language	string (enum)	2	igen	a fizetési oldal megjelenítésének kezdőnyelve, értéke: "HU"

				→ a megnyitást követően a felületen is állítható a felhasználó által
url	string	max 230	igen	Tartalma egy URL vagy Deeplink, amely a fizetést indító fizetési felület státusz oldalára navigálja vissza a fizető felet. A fizető fél mobil banki applikációjának, a fizetés végén lehetőséget kell biztosítania az ebben a mezőben lévő URL megnyitására.
transactionReference	string	max 17	igen	kereskedő által kiosztott max. 17 karakter hosszú egyedi kód
paymentMethods	object / string (enum)	3	igen	az azonnali fizetési mód megjelenítéséhez az "EAM" értéket kell használni
transactionCurrency	string	3	igen	devizakód ISO 4217 szabvány szerint - csak "HUF" lehet
transactionAmount	integer	15	igen	kosár / fizetési kérelem összege
remittanceInfo	string	max 70	nem	közlemény - max. 70 karakter (UTF8 alapkarakterek + magyar ékezetes karakterek*)
shopId	string	max 10	igen	kereskedő által meghatározott boltazonosító - (UTF8 alapkarakterek + magyar ékezetes karakterek*) <i>pl.: shop0001</i>
terminalReference	string	max 35	igen	kereskedő által meghatározott terminál azonosító - max. 35 karakter (UTF8 alapkarakterek + magyar ékezetes karakterek*) <i>pl.: terminal0001</i>
timestamp	string	-	igen	a payload összeállításának időbélyege datetimeoffset formátumban. ISO 8601 zulu vagy local time format. A timestamp nem lehet a jövőben, illetve nem lehet 5 percnél régebbi a valós

				időhöz képest (pl. 2024-10-04T14:23:45Z)
idempotencyKey	string (uuid)	-	igen	kereskedő által kiosztott UUID formátumú egyedi kód

* 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

Példa:

```
{
  technicalUserId: "10234",
  language: "HU",
  url: "https://demo-webshop.hu",
  transactionReference: "1Ffnhelta3b",
  paymentMethods: [
    "EAM"
  ],
  transactionCurrency: "HUF",
  transactionAmount: 250,
  remittanceInfo: "Teszt vásárlás",
  shopId: "shop0001",
  terminalReference: "terminal0001",
  timestamp: "2024-10-04T14:23:45Z",
  idempotencyKey: "f4e5b92d-60ff-46bd-a26a-8342116cdec5"
}
```

4.3.2. Payload becsomagolása jsonString-be

A payload-ot át kell alakítani jsonString formátumúra, valamint minifyolni kell a JSON-t.

Az ékezetes karaktereket és a / jeleket és egyéb különleges karaktereket nem kell escapelni (pl. url mező tartalma a példában).

Becsomagolt payload (minified jsonString) példa:

```
{"idempotencyKey":"f4e5b92d-60ff-46bd-a26a-8342116cdec5","technicalUserId":"10234","language":"HU","url":"https://demo-webshop.hu","transactionReference":"1Ffnhelta3b","paymentMethods":["EAM"],"transactionCurrency":"HUF","transactionAmount":250,"remittanceInfo":"Teszt vásárlás","shopId":"shop0001","terminalReference":"terminal0001","timestamp":"2024-10-04T14:23:45Z"}
```

A request headernél Content-Type-nak application/json-nak kell lennie.

4.3.3. HMAC signature generálása

A HMAC signature létrehozásához a jsonString formátumúra alakított payloadot kell titkosítani SHA256 algoritmussal, amihez a HMAC secret private kulcsot kell használni aláírásként. **A létrehozott aláírásnak HEX formátumúnak kell lennie.** A secret maga is HEX formátumban van ezt figyelembe kell venni az implementációnál mivel egyes HMAC generáló library-k alpból nem HEX formátumban várják ezt a paramétert (ez library-ként eltérő lehet). A generálás módja a 7. menüpontban kerül bemutatásra.

HMAC signature példa (a korábbi példákban szereplő adatok használatával):

```
66A300848188A93663FB2334A0258DB5DEBA442CA2258033645905F4FD96A7E0
```

4.3.4. 'Payment start' hívás indítása

A 'Payment start' hívást a rafipay-vpos-service API séma alapján kell összeállítani.

Végpont

POST {BaseURL}/qr-v1/onlinefizetes-v1/start

Header

Mezők:

Signature	string (hex)	a fent leírt módon generált HMAC signature
X-Request-ID	string (uuid)	kereskedő által UUID sémában kiosztott egyedi hívásazonosító, mely az adott hívást azonosítja
X-Correlation-ID	string (uuid)	kereskedő által UUID sémában kiosztott egyedi munkamenet-azonosító, mely a teljes munkamenetet azonosítja

Body

A payload meg kell egyezzen a signature létrehozás során összeállított payloaddal.

Response

Sikeres kérés esetén az alábbi kódot adja vissza a szolgáltatás:

- 200: Payment created

A sikeres hívás eredményeképp a Raiffeisen PAY szolgáltatás (rafipay-vpos-service) előállít egy payment URL-t, és visszaadja azt a válaszban.

```
{
  "salt": "string",
  "redirectUrl": "string"
}
```

Sikertelen kérés esetén az alábbi hibakódokat adhatja vissza a szolgáltatás:

- 400: General error response
- 401: Access Denied. There is no access token or the api call was made with an invalid access token

```
{
  "errorId": "string",
  "errorCode": "string",
  "errorDescription": "string",
  "errorDetails": [
    {
      "field": "string",
      "errorDescription": "string"
    }
  ]
}
```

4.3.5. Vásárló átirányítása az Online Fizetési Oldalra

A vásárlót a Payment start hívásra adott válaszban kapott payment URL-re kell irányítani. Az Online Fizetési Oldal megjeleníti az azonnali fizetéshez szükséges QR kódot és/vagy Deeplinket.

A tranzakció befejezése után a fizetési oldalon megjelenik a tranzakció eredménye, valamint a kereskedő oldalára mutató (a payloadban megadott) visszatérési/redirect link.

4.4. Tranzakció eredményének lekérdezése a kereskedő oldalán

A kereskedő a Payment Query by transaction reference vagy a Payment query by payment reference hívások valamelyikének segítségével le tudja kérdezni a tranzakció részleteit a rafipay-vpos-service API-n.

- transaction reference: kereskedői tranzakció azonosító
- payment reference: fizetési szolgáltató (aggregátor) tranzakció azonosító

A következő szakaszban a kereskedői azonosító alapján történő lekérdezést írjuk le részletesen (az aggregátor által kiosztott azonosító alapján történő lekérdezés logikája megegyezik ezzel).

Végpont

POST {BaseURL}/qr-v1/onlinefizetes-v1 /query-by-transaction-reference

Header

Mezők:

Signature	string (hex)	a fent leírt módon generált HMAC signature
X-Request-ID	string (uuid)	kereskedő által UUID sémában kiosztott egyedi hívásazonosító, mely az adott hívást azonosítja

X-Correlation-ID	string (uuid)	kereskedő által UUID sémában kiosztott egyedi munkamenet-azonosító, mely a teljes munkamenetet azonosítja
------------------	---------------	---

Body

Mezők:

idempotencyKey	string (uuid)	kereskedő által kiosztott UUID formátumú egyedi kód
technicalUserId	string	az API felhasználó technikai azonosítója (pl. 10234)
transactionReference	string	a payment start hívásban megadott egyedi tranzakció-azonosító kód
timestamp	string	a kérés összeállításának időbélyege datetimeoffset formátumban (pl. 2024-10-04T14:23:45Z)

Példa:

```
{
  "idempotencyKey": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "technicalUserId": "string",
  "transactionReference": "string",
  "timestamp": "2024-10-15T10:14:26.121Z"
}
```

Response

```
{
  "salt": "TzRxZ+VpvtSv0WAH/OUce6FBjNwhGqIevYXTjEHTv2s=",
  "status": "EXPIRED"
}
```

A **status** értékei az alábbiak lehetnek:

- RECEIVED
- CANCELLED
- PAYMENT_ATTEMPTED
- ACCEPTED
- EXPIRED

4.5. 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 lejáratidőn belül, így a payment státusza EXPIRED-re vált.

4.6. 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 esetben, ha IPEW kódot kívánnak használni a callback url megadása kötelező előzetesen a szerződéskötés alkalmával, API hívás során nem kell adni a callback url-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. Teszteléshez szükséges lépések

A tesztkörnyezetünk performancia tesztre alkalmas, teljes integrációval rendelkezik a tranzakciók teljes életciklusára vonatkozóan beleértve az Aggregátori és GIRO kapcsolatot is, ami lefedi az élessel megegyező folyamatokat.

6.1. Tesztadatok

Minden partnernek egyedi teszt felhasználói adatokat biztosít a Bank, ezt a banki kapcsolattartótól kell kérni. **A teszteléshez szükséges titoktartási megállapodás aláírása.** A tesztkörnyezet csak hétköznapokon érhető el **7:00 és 20:00 óra között.**

6.2. Raiffeisen PAY Portál beállítás

6.2.1. Raiffeisen PAY Portál

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

Elérhetőség: <https://pay-portal-pc.raiffeisen.hu>

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

1. Új Felhasználók létrehozása
2. Jogosultság beállítása a jogosultságok szerkesztése képernyőn
3. API key, HMAC és technikai felhasználó azonosítójának kinyerése az RPP portálról

6.2.2. Belépés

Belépés menüre kell kattintani, beírni a Bank által biztosított **Systemadmin teszt Direkt azonosítót és a jelszót, amit a Bank által biztosított excel táblázat tartalmaz.** Az SMS kód lehívása API-n keresztül történik, a következő lépésben kerül bemutatásra.

Belépés

Aktiválás

Belépés

Kérjük, adja meg SMS kódját, melyet az Ön által megadott telefonszámra szöveges üzenetben kézbesítettünk!

azonosító

jelszó

SMS kód

Bejelentkezés

SMS kód lekérdezése SMS API segítségével:

SMS OTP lekérő API-t a jelszó beírása után kell meghívni, mindig a legutolsó művelethez generált SMS OTP-t fogja visszaadni, legyen az bejelentkezés vagy jóváhagyás.

Az endpoint meghívásához api key (x-api-key) szükséges, illetve két UUID header x-request-id, x-correlation-id. **Az x-api-key-t a Bank által biztosított excel táblázat tartalmazza.**

Method GET

https://testing-tool-sms.huoapi-test.merlinplatform.cloud/smsotp/DIREKT_ID

A path param-ként kell megadni a Systemadmin direkt id-ját, amivel be kíván lépni.

Postman:

Api key header name: x-api-key

GET

https://testing-tool-sms.huoapi-test.merlinplatform.cloud/smsotp/86624407

Params

Authorization

Headers (10)

Body

Scripts

Settings

Auth Type

API Key

The authorization header will be automatically generated when you send the request. [Learn more about API Key](#) authorization.

Key

x-api-key

Value

.....

Add to

Header

kérés:

egyéb headers:

x-request-id

x-correlation-id

GET https://testing-tool-sms.huoapi-test.merlinplatform.cloud/smsotp/86624407

Params Authorization Headers (10) Body Scripts Settings Cookies

Headers 8 hidden

	Key	Value	Description
<input checked="" type="checkbox"/>	x-correlation-id	{{ \$guid }}	
<input checked="" type="checkbox"/>	x-request-id	{{ \$guid }}	
	Key	Value	Description

Body Cookies Headers (11) Test Results

200 OK 1.04 s 599 B

{ } JSON Preview Visualize

```
1 {
2   "response": {
3     "otp": "55381767",
4     "sms": "Your one time password for login is: 55381767 RBHU",
5     "smstimestamp": "2025-07-17 15:17:11.00+00:00"
6   }
7 }
```

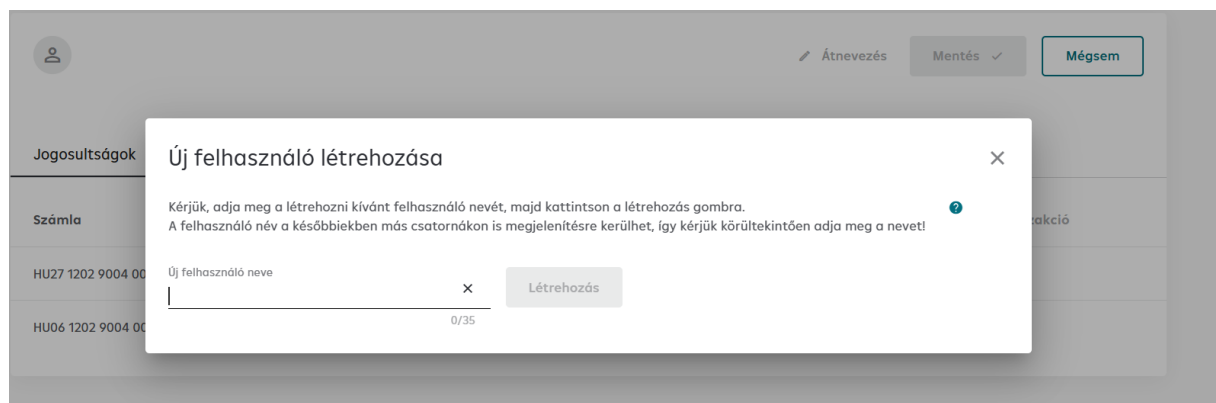
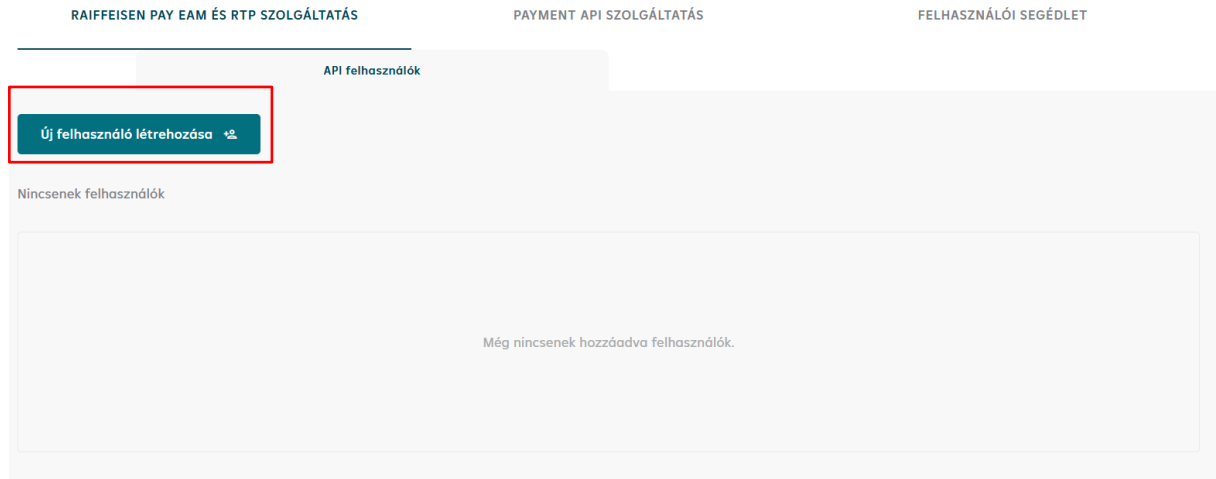
CURL example:

```
curl --location 'https://testing-tool-sms.huoapi-test.merlinplatform.cloud/smsotp/PASTE_DIREKT_ID_HERE' \
--header 'x-api-key: API_KEY_SECRET' \
--header 'x-correlation-id: 8863237b-6207-4117-ba79-0d415ff8d822' \
--header 'x-request-id: e4347b9d-bb06-4bb0-8c25-385b388f1cef'
```

Az OTP mezőben található érték lesz az, amit az SMS code input mezőbe kell másolni az RPP portálon. Az RPP portálon végrehajtott minden műveletet jelszó + SMS kód kombinációval kell aláírni, minden esetben a jelszó beírását követően újra le kell kérdezni az SMS kódot.

6.2.3. Új felhasználó létrehozása

A portálon a Raiffeisen PAY EAM és RTP szolgáltatás fölön az Új felhasználó létrehozása gombra kell kattintani, API teszt felhasználó neve szabadon megadható.



Az alkalmazható karakterek:

AÁBCDEÉFGHIÍJKLMNOÓÖŐPQRSTUÚÜŰVWXYZ

aábcdeéfgghiijklmnoóöőpqrstuúüűvwxyz

1234567890

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

Szóköz

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

Teszt user

Átnevezés

Mentés ✓

Mégsem

Jogosultságok

Számla	Deviza	PAY tranzakció	EAM tranzakció	RTP tranzakció
HUJ ** **** **	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HUJ ** **** **	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Alá kell írni a megbízást, jelszó+SMS kombinációval. Az SMS kódot API-n keresztül kell lekérni, amit az előző pontban bemutatunk.

Kedves Raipay Kriszti Systemadmin!

Felhasználó létrehozás jóváhagyása

Mégsem

Aláírom

Hitelesítés 1/2

Kérjük, először adja meg a Jelszavát, majd kattintson a Tovább gombra!

Jelszó

.....

Megszakítom

Tovább

Hitelesítés 2/2

Kérjük, adja meg az egyszer használatos kódot, amit SMS-ben küldtünk Önnek a 06305565370 telefonszámra!

Egyszer használatos kód

.....

8/8


[Nem kaptam SMS-t.](#)

[Megszakítom](#)

[Tovább](#)

6.2.4. API key, HMAC és Technikai felhasználó azonosítója


A kliens autentikációhoz szükséges API key, a HMAC secret és technikai felhasználó azonosítója itt érhető el:



 **Teszt user** •



[Átnevezés](#) [Inaktiválás](#) [Törlés](#)

Aktív felhasználó


Nincs aktív tanúsítvány

Technikai felhasználó azonosítója: 17648 

x-api-key: *****  

HMAC secret: *****  

[Jogosultságok](#) [Tanúsítványok](#)

[Jogosultságok szerkesztése](#) 

Számla	Deviza	PAY tranzakció	EAM tranzakció	RTP tranzakció
HU ** * * * * *	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HU ** * * * * *	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

7. Élesítéshez szükséges lépések

A qvik szolgáltatás éles használatához Raiffeisen PAY szerződés aláírása szükséges, ezt minden esetben a banki kapcsolattartóval kell egyeztetni.

7.1. Raiffeisen PAY Portál beállítás

7.1.1 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:

- Rendszeradminisztrátor aktiválása
- Új Felhasználók létrehozása
- Jogosultság beállítása a jogosultságok szerkesztése képernyőn
- API key, HMAC és technikai felhasználó azonosítójának kinyerése az RPP portálról

7.1.2 Rendszeradminisztrátor aktiválása

A Raiffeisen Pay hozzáférés létrehozását követően a rendszer adminisztrátor 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.

Belépés

Aktiválás

Direkt Azonosító és Aktiváló PIN kód megadása

Kérjük, adja meg a 8 számjegyű Direkt Azonosítóját és az SMS-ben kapott aktiváló PIN kódot, majd kattintson a TOVÁBB gombra.

Direkt Azonosító

Aktiváló PIN kód

Tovább

Új aktiváló PIN kódot a +36 80 488 588-as telefonszámon a 2-4-es menüpontban (sikeres beazonosítás után), vagy a bankfiókban kérhet. További teendőkről a [Segítségben](#) olvashat.

Ha nincs internetbanki hozzáférése, igényeljen [igénylőlapunk](#) postai beküldésével vagy bankfiókunkban.

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

7.1.3 Belépés

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

Belépés

Aktiválás

Belépés

Kérjük, adja meg SMS kódját, melyet az Ön által megadott telefonszámra szöveges üzenetben kézbesítettünk!

Amennyit

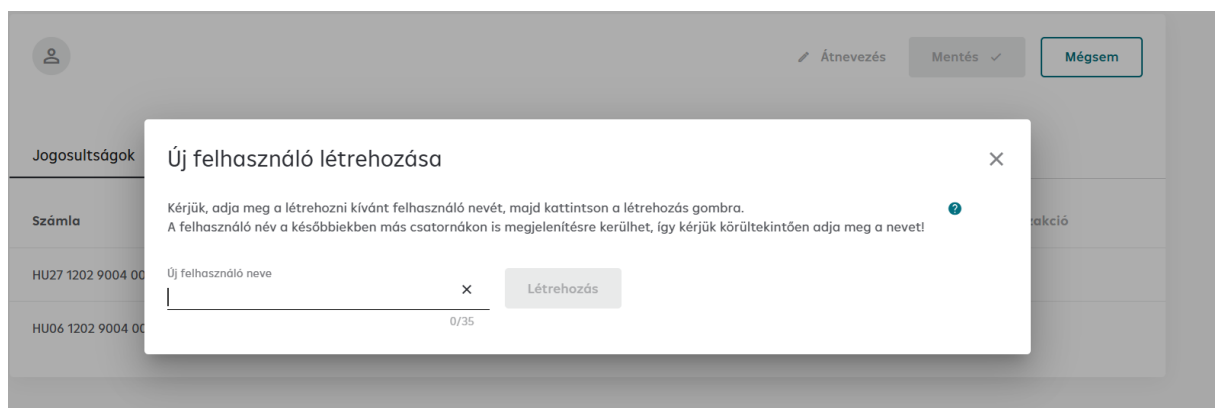
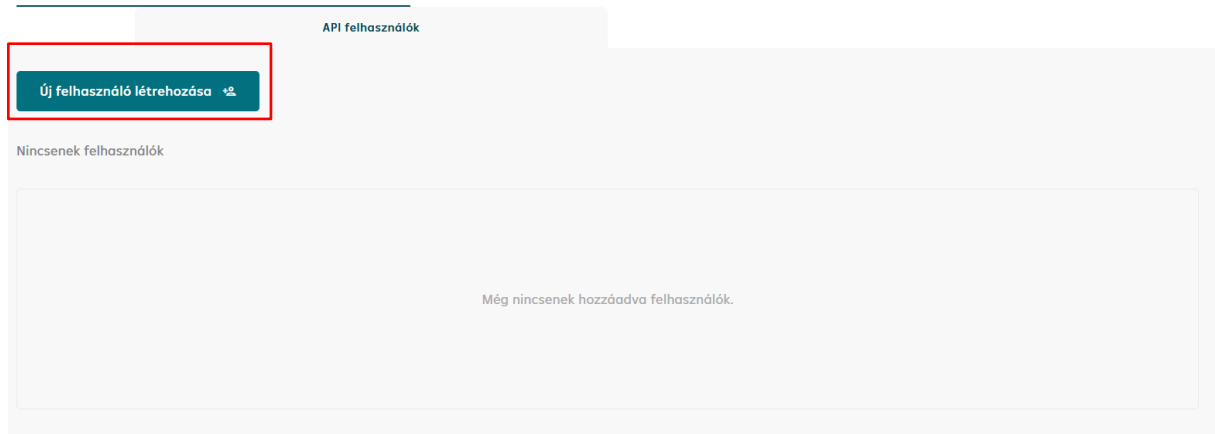
Jelszó

SMS kód

Bejelentkezés

7.1.4 Új felhasználó létrehozása

A portálon a Raiffeisen PAY EAM és RTP Szolgáltatás fölön az Új felhasználó létrehozása gombra kell kattintani.



Először meg kell adni a felhasználó nevét. A felhasználónév a tranzakciók esetében megjelenhet a különböző banki alkalmazásokban, ezért ennek megadásakor érdemes körültekintően eljárni.

Az alkalmazható karakterek:

AÁBCDEÉFGHIÍJKLMNOÓÖŐPQRSTUÚÜŰVWXYZ

aábcdeéfgghiíjklmnoóöőpqrstuúüűvwxyz

1234567890

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

Szóköz

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

Teszt user

Átnevezés

Mentés ✓

Mégsem

Jogosultságok

Számla	Deviza	PAY tranzakció	EAM tranzakció	RTP tranzakció
HU ** **** **	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HU ** **** **	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Kedves Raipay Kriszti Systemadmin!

Felhasználó létrehozás jóváhagyása

Mégsem

Aláírom

Hitelesítés 1/2

Kérjük, először adja meg a Jelszavát, majd kattintson a Tovább gombra!

Jelszó

.....

Megszakítom

Tovább

Hitelesítés 2/2

Kérjük, adja meg az egyszer használatos kódot, amit SMS-ben küldtünk Önnek a 06305565370 telefonszámmal!

Egyszer használatos kód

.....

8/8

Nem kaptam SMS-t.

Megszakítom


Tovább

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.

7.1.5. API key, HMAC és Technikai felhasználó azonosítója


A kliens autentikációhoz szükséges API key, a HMAC secret és technikai felhasználó azonosítója itt érhető el:



 **Teszt user •**



[Átnevezés](#) [Inaktiválás](#) [Törlés](#)

Aktív felhasználó

Nincs aktív tanúsítvány


Technikai felhasználó azonosítója: 17648 

x-api-key: *****  

HMAC secret: *****  

Jogosultságok

Tanúsítványok

Jogosultságok szerkesztése 

Számla	Deviza	PAY tranzakció	EAM tranzakció	RTP tranzakció
HU ** **** * * * * *	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HU ** **** * * * * *	HUF	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

8. 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