

Raiffeisen VPOS Fejlesztői Segédlet



**Raiffeisen
Bank**

Tartalomjegyzék

1	Bevezetés.....	5
2	Fogalmak, rövidítésjegyzék.....	6
3	Implementációs megoldások.....	8
3.1	Kötelezően implementálandó megoldások.....	10
3.1.1	Notification API / URL.....	10
3.1.1.1	A Kártyabirtokos átirányítása a Notification API-tól kapott válasz alapján....	13
3.1.2	Payment page segítségével történő fizetés.....	14
3.1.2.1	Fizetés folyamata.....	14
3.1.2.2	Általános leírás.....	16
3.1.2.2.1	Aláírás.....	19
3.1.2.2.2	Kulcsok generálása.....	19
3.1.2.2.3	Aláírás generálása (SHA512withRSA http).....	20
3.1.2.2.4	Teszt kulcs a bank által küldött üzenetek ellenőrzéséhez.....	22
3.1.2.2.5	Éles kulcs a bank által küldött üzenetek ellenőrzéséhez.....	22
3.1.2.3	Payment Page-en történő fizetés indítása.....	23
3.1.2.3.1	Emv 3DSecure tranzakció feldolgozása (opcionálisan implementálható)..	26
3.1.3	Sztornó (reversal) tranzakció.....	34
3.1.4	Tranzakció státuszának lekérdezése.....	37
3.1.4.1	HTML formátum segítségével.....	37
3.1.4.2	JSON formátum segítségével.....	39
3.2	Opcionálisan implementálható megoldások.....	44
3.2.1	Visszatérítés (Refund) tranzakció.....	44
3.2.2	Előengedélyezés / Előengedélyezés befejezése.....	44
3.2.2.1	Előengedélyezés befejezése POST hívás segítségével.....	45
3.2.3	Webes fizetés + JSON API.....	48
3.2.3.1	Fizetési folyamat.....	49
3.2.3.2	Kommunikáció.....	49
3.2.3.3	Általános leírás.....	50
3.2.3.3.1	Header.....	50
3.2.3.3.2	Payload.....	50

3.2.3.3	Signature	50
3.2.3.4	Ismétlődő fizetés (MIT - Merchant-Initiated Transaction & CIT - Customer-Initiated Transaction)	51
3.2.3.5	CVV kód megadása meghatározott összeghatár fölött CIT-es ismétlődő fizetés során.....	55
3.2.3.6	Kártya tokenizálása 0 Forinttal (Account verification) – MIT-es ismétlődő fizetéshez	58
4	Kereskedő portál szolgáltatásainak ismertetése	61
4.1	Alap ismertetés.....	61
4.2	Visszatérítés	62
4.3	Előengedélyezés és annak befejezése.....	63
4.4	Fizetési link generálása.....	64
5	Integrációs tesztelés	66
5.1	Tesztesetek.....	66
5.1.1	Kötelezően implementálandó tranzakciótípusok.....	66
5.1.1.1	Normál fizetés	66
5.1.1.2	Sztornó	67
5.1.2	Opcionálisan igényelhető tranzakciótípusok.....	67
5.1.2.1	Normál fizetés kártya regisztrációval	67
5.1.2.2	Mentett kártyás fizetés (CIT).....	67
5.1.2.3	Ismétlődő fizetés - MIT.....	68
5.1.2.4	Visszatérítés	68
5.1.2.5	Előengedélyezés / Előengedélyezés befejezése	68
5.1.3	Sikertelen tranzakció feldolgozása	69
5.1.4	JSON API – tranzakció állapotának lekérdezése	69
5.2	Teszteléshez használandó kártyaadatok.....	69
6	Függelékjegyzék.....	70
6.1	Formátum kódok.....	70
6.2	TranCode értékei.....	70
6.3	HostCode értékei.....	73
6.4	Deviza kódok	76
6.5	Interface nyelvi (helyi) kódok.....	76

Változáskezelés

Verzió	Változás	Módosítás dátuma
1.01	„3.1.2.2 Általános leírás” fejezet kiegészítése a SUCCES_URL és a FAILURE_URL-re megküldött tranzakcióadatokkal.	2024. október 15.

1 Bevezetés

Ezen dokumentum a Raiffeisen Bank (továbbiakban: Bank) online fizetési megoldásának Kereskedő oldali integrációjához készített fejlesztői segédlete.

A segédlet bemutatja a Bank által biztosított virtuális bankkártyaelfogadói megoldáson keresztül nyújtott lehetőségeket és azok implementálási módjait. Az integráció bármely programnyelven elvégezhető. Az integráció minden esetben a Kereskedő feladata, melyhez a Bank technikai támogatást igen, SDK-t nem biztosít.

Amennyiben a fejlesztés során bármilyen kérdés merülne fel, kérjük vegye fel velünk a kapcsolatot

- technikai kérdések miatt a vpos_devsupport@raiffeisen.hu,
- üzleti kérdések miatt pedig a vpos@raiffeisen.hu

e-mail címen.

2 Fogalmak, rövidítésjegyzék

Fogalom	Leírás
SDK	Software Development Kit
Tanúsítvány	<p>Tanúsítványt a biztonságos webhelyek használnak a webszerver és a böngésző közötti biztonságos kapcsolat létrehozására. A biztonságos weboldalak lehetővé teszik az adatátvitel, a bejelentkezés, a fizetési kártyás tranzakciók biztonságossá tételét, valamint a biztonságos böngészést az oldalon.</p> <p>Ha biztonságos webhelyet nyit meg, a címsorban egy „zár” ikon látható. Ha rákattint, megtekintheti a telepített tanúsítvány részleteit.</p>
.crt file	A CRT fájlok ASCII formátumúak, és bármely szövegszerkesztőben megnyithatók a tanúsítványfájl tartalmának megtekintéséhez. Az X.509 tanúsítási szabványt követi, amely meghatározza a tanúsítvány szerkezetét. Meghatározza azokat az adatmezőket, amelyeket az SSL-tanúsítványnak tartalmaznia kell. A CRT azon tanúsítványok PEM formátumába tartozik, amelyek Base64 ASCII kódolású fájlok.
Publikus kulcs (public key) és privát kulcs (private key)	A nyílt/nyilvános kulcsú rejtjelezés vagy titkosítás, más néven aszimmetrikus kulcsú titkosítás egy olyan kriptográfiai eljárás neve, ahol a felhasználó egy kulcspárral – egy nyilvános és egy titkos kulccsal rendelkezik. A titkos kulcs titokban tartandó, míg a nyilvános kulcs széles körben terjeszthető. A kulcsok matematikailag összefüggenek, ám a titkos kulcsot gyakorlatilag nem lehet meghatározni a nyilvános kulcs ismeretében. Egy, a nyilvános kulccsal kódolt üzenetet csak a kulcspár másik darabjával, a titkos kulccsal lehet visszafejteni.
SHA512with RSA	Az SHA512withRSA egy hibrid kriptográfiai algoritmus, amely az SHA-512hash algoritmust és az RSA digitális aláírási sémát használja. Az SHA-512 segítségével létrehoz egy hash értéket az adatokhoz, majd aláírja a hash-t RSA segítségével egy privát kulccsal. Az így kapott aláírás a megfelelő nyilvános kulccsal ellenőrizhető, biztosítva az adatok sértetlenségét és hitelességét.
OpenSSL	Az OpenSSL egy szoftverkönyvtár olyan alkalmazásokhoz, amelyek biztonságos kommunikációt biztosítanak számítógépes hálózatokon keresztül a lehallgatás ellen, és azonosítják a felet a másik végén. Az internetes szerverek széles körben használják, beleértve a HTTPS-webhelyek többségét

Base64	A Base64 kódolás 64 karakterből álló ábécén alapuló tartalomkódolási forma, melynek segítségével bináris, illetve speciális karaktereket tartalmazó adatokból ASCII karaktersorozat állítható elő. Az ily módon kódolt adatok akár a karaktereket 7 biten ábrázoló rendszereken is könnyen átvihetők.
Payment gateway	Szolgáltatás végpont
Token	A Kártyabirtokos kártyaadatainak helyettesítésére szolgál. Segítségével a Kereskedő terhelést kezdeményezhet a kártyaadatok megadása és a kártya tulajdonosának bevonása nélkül. Továbbá a Kártyabirtokosnak is lehetősége van fizetés indítására a kártyaadatainak újbóli megadása nélkül.
Success URL	A Kereskedő webhelyének egy oldala, amelyre a kereskedő Notify URL-ének helytelen működése esetén a sikeres tranzakciót követően átirányítja a felhasználó böngészőjét.
Failure URL	A Kereskedő webhelyének egy oldala, amelyre a kereskedő Notify URL-ének helytelen működése esetén átirányítja a felhasználó böngészőjét sikertelen tranzakciót követően.
Notify URL	Egy külön URL, a Kereskedő úgynevezett visszahívási címe, amelyet fizetés esetén meghív a Bank BE szolgáltatása. A fizetéssel kapcsolatos információk feldolgozásához szükséges.
PCI DSS	A Payment Card Industry Data Security Standard (PCI DSS) egy információbiztonsági szabvány, amelyet a főbb kártyamárkák bankkártyáinak kezelésére használnak. A szabványt a Payment Card Industry Security Standards Council adminisztrálja, használatát pedig a kártyamárkák írják elő. A szabványt a Kártyabirtokosok adatainak jobb ellenőrzése és a bankkártya-csalás csökkentése érdekében hozták létre.
JSON	JavaScript Object Notation egy egyszerű adatsere-formátum.
BE	Backend
FE	Frontend
TranCode	A Bank irányába indított kérésekre kapott válaszban megtalálható eredménykód Értékei .
HostCode	A HostCode a szolgáltató által adott ISO8583 válasz kód. Ennek a kódnak a segítségével jobban beazonosítható és kielemezhető miért lett a tranzakció elutasítva, ezért kiemelten fontos ennek letárolása a TranCode mellett. Ez a kód kizárólag a Banktól kapott válasz üzenetben található meg. Értékei .

ISO 8583	Az ISO 8583 egy nemzetközi szabvány a bankkártyás tranzakciókból származó bankközi üzenet küldéséhez.
3D Secure	Az 3D Secure egy továbbfejlesztett kétlépcsős azonosítási módszer a bankkártya tranzakciókhoz. Általában a "VISA Secure" vagy a "Mastercard ID Check" néven ismert. Az ügyfélnek egy jelszót vagy egyedi kódot kell megadnia a tranzakció jóváhagyásához, amelyet a Kibocsátó Bank küld a Kártyabirtokos részére.
CVC	Card Validation Code – bankkártya ellenőrző kód
CVV	Card Verification Value – bankkártya ellenőrző érték
Payment Page	A Bank által biztosított fizetési felület, ahol a Kártyabirtokos megadja a fizetéshez használni kívánt bankkártya számát, lejárat dátumát, CVV számát és a kártyabirtokos nevét.
MerchantID (MID)	Kereskedő azonosító
TerminalID (TID)	Terminál azonosítója
Napzárás	A Banknál a nap zárása 20 órakor automatikusan megtörténik. Ekkor a két napzárás közötti időszakban sikeresen engedélyezett tranzakciók a kártyatársaságok irányába megküldésre kerülnek.

3 Implementációs megoldások

A Raiffeisen Bank egy összetett integrációs megoldást kínál, melyet a Kereskedő implementálhat.

A "Checkout by the payment page" során -, melyet a [Payment page segítségével történő fizetés](#) alfejezetben részletezünk - a Kereskedő a saját webes felületéről HTTPS hívásban adja át a fizetés adatait (MID, TID, összeg, megrendelés azonosítója, stb.) a Banknak, aki átirányítja a Kártyabirtokost a Raiffeisen Bank biztonságos fizetési felületére, ahol a fizetéshez a Kártyabirtokos megadja a bankkártyája adatait. A fizetés eredményéről még a böngészőben azonnal visszajelzést kap a Kártyabirtokos. A tranzakciót követően a Payment Pageről lehetőség van visszairányítani a felhasználót a Kereskedő weboldalára.

A Kereskedőnek ki kell alakítania a szolgáltató és közte történő backend-backend üzenetváltás lehetőségét ([Notification API](#)), mely során a Bank a fizetés eredményéről tájékoztatást küld a Kereskedő részére, így biztosítva a rendellenes működésből (böngésző bezárása, időtúllépés, kapcsolatvesztés stb.) származó visszaigazolás megtörténtét. Ezen kérésre a kereskedőnek szinkron választ kell adnia, melyben lezárja a tranzakciót.

A "Checkout by web + JSON API" alfejezetben taglalt megoldás segítségével a Kereskedő backend alkalmazása egy speciális token (Token) segítségével tud fizetést kezdeményezni. Ennek előfeltétele a Kártyabirtokos által indított biztonságos fizetési oldalon történő sikeres fizetés és a tokenizáció – kártyabirtokos általi – engedélyezése. Ezen fizetés során a megadott kártyához a fizetési rendszer egy tokent rendel, melyet a fent említett Notification API-n keresztül kap meg a Kereskedő backend-je.

A két implementációs megoldásnál eltérő tranzakció típusok érhetőek el, ezeket az alábbi táblázat foglalja össze.

Tranzakció típusa	HTML	JSON
Fizetés	X	
Tokenizált fizetés (CIT)	X	X
Ismétlődő fizetés (MIT)		X
Tranzakció állapota	X	X
Sztornó / Visszatérítés	X	
Előengedélyezés / előengedélyezés befejezése	X	
Account verification	X	
ApplePay	X	
GooglePay	X	

A Bank megkülönböztet alap és igényelhető szolgáltatásokat a vPOS-t használó Kereskedők számára, azonban egyes igényelhető szolgáltatások előzetes banki bírálat alapján kerülhetnek csak aktiválásra. A lenti táblázat szemlélteti mely alapszolgáltatások és mely igényelhető szolgáltatásokat nyújtja a Bank. Amennyiben igényelhető szolgáltatást szeretne a Kereskedő igénybe venni, kérjük igényét a Kereskedő Portálon keresztül adja le.

	Alapszolgáltatások	Igyényelhető szolgáltatások
Normál fizetés + sztornó	X	
GooglePay/ApplePay fizetés	X	
Mentett kártyás fizetés (CIT)		X
Kereskedő által indított ismétlődő fizetés (MIT) Account verification-nel		X (Külön MID és TID szükséges hozzá, AV esetén további MID / TID kerül kiosztásra)
Visszatérítés (Refund)		X
Előengedélyezés / Előengedélyezés befejezése		X (Külön MID és TID szükséges hozzá)
Fizetési link (Pay by link)		X (Külön MID és TID szükséges hozzá)

3.1 Kötelezően implementálandó megoldások

3.1.1 Notification API / URL

A Notification API a Kereskedő szerver oldalán implementált API szolgáltatás, amely biztosítja számára, hogy a tranzakcióról azonnali információt kapjon, és azt lezárja. A szolgáltatás URL címének nyilvánosan elérhetőnek kell lenni.

A fizetési szolgáltatás értesítést küld a Kereskedő részére a sikeres / sikertelen tranzakciókról. Az API használata a tranzakció lezárásán túl még az alábbi esetekben lehet kiemelten hasznos:

1. böngésző kifagyása;
2. felhasználói hibából fellépő probléma (pl.: böngésző ablak bezárása);
3. internetkapcsolatban fellépő probléma;
4. böngészőbe telepített Plug-in nem megfelelő működése, mely hatással lehet annak működésére;

Összegezve:

- a fizetési szolgáltató a Kereskedő részére a tranzakció feldolgozásának eredményét HTTP/HTTPS POST metódus segítségével adja át;
- a Kereskedőnek szükséges a szolgáltatásában implementálnia ezt az API-t;
- a Notify URL-nek nyilvános internetről elérhetőnek kell lenni;
- Teszt payment gateway IP címei:
 - o 18.196.61.127
 - o 3.120.143.246
 - o 18.197.170.36
- Éles payment gateway IP címe:
 - o 217.13.180.171

Notification API URL nem tartalmazhat port számot (csak a 80/443 pontok használhatók), ezáltal ngrok nem használható ennek tesztelésére.

Bank irányából érkező kérés paramétere:

Paraméter	Formátum	Leírás	Megjegyzés
MerchantID	AN(15)	Kereskedő egyedi azonosítója	Értéke megegyezik az eredeti autorizációs kérés értékével
TerminalID	AN(8)	Terminál egyedi azonosítója	Értéke megegyezik az eredeti autorizációs kérés értékével

TotalAmount	N(1..12)	Összeg	Értéke megegyezik az eredeti autorizációs kérés értékével
Currency	N(3)	Deviza kód	Értéke megegyezik az eredeti autorizációs kérés értékével. Értékei.
PurchaseTime	N(12)	Eredeti kérés pontos dátuma és ideje (YYMMDDhhmmss)	Értéke megegyezik az eredeti autorizációs kérés értékével
OrderID	ANS(1..20)	Rendelés azonosítója	Értéke megegyezik az eredeti autorizációs kérés értékével
Delay	N(1)	Payment ID Pre-authorization	Értéke megegyezik az eredeti autorizációs kérés értékével
XID	ANS(1..28)	Tranzakció azonosítója	Tranzakció azonosítója
ApprovalCode	AN(6)	Authorizációs kód	A Kibocsátó Bank által visszaadott autorizációs kód vagy jóváhagyó kód.
Rrn	N(12)	Retrieval Reference Number	A kártyás tranzakció egyedi azonosítója az ISO 8583 szabvány alapján.
ProxyPan	ANS(13..19)	Maszkolt PAN értéke	Maszkolt PAN értéke.
TranCode	N(3)	Tranzakció eredményének kódja	Minden kérés tartalmazza az annak sikerességére vagy sikertelenségére vonatkozó kódot. Értékei.
Signature	AN(1..40)	Aláírás értéke	A paraméter karakterszáma függ a választott generálási metódustól
UPCToken	ANS(32)	Az első sikeres tranzakciót követően a payment gateway által megküldött TOKEN.	A Kártyabirtokos kártyaadatának helyettesítésére szolgál. Segítségével a Kereskedő terhelést kezdeményezhet a kártyaadatok megadása és a kártya tulajdonosának bevonása nélkül.

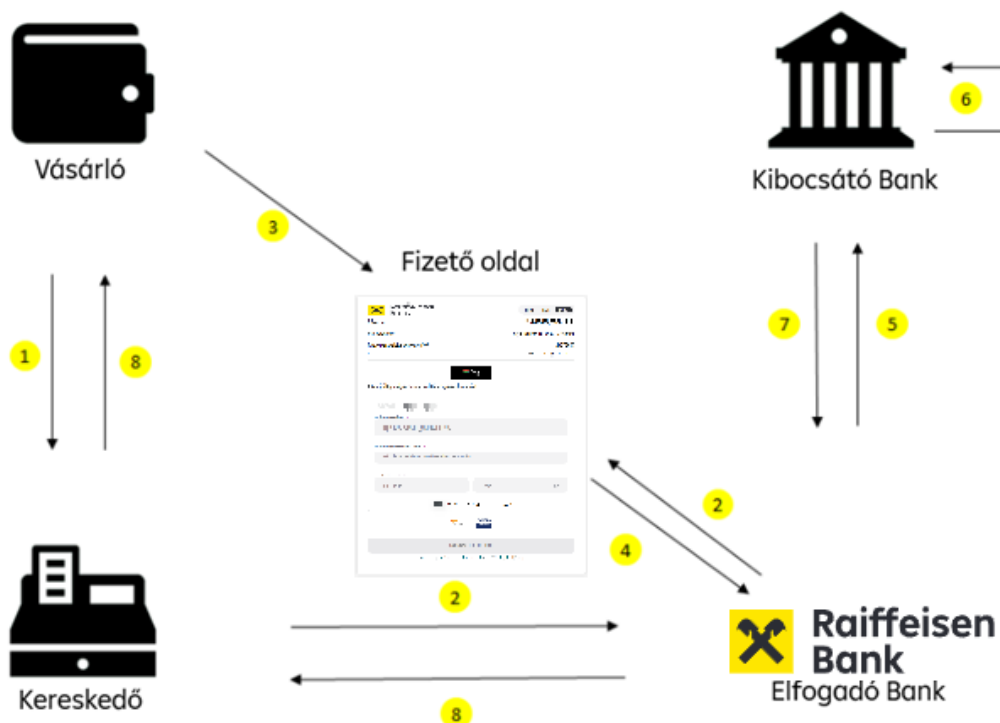
3.1.2 Payment page segítségével történő fizetés

A Bank által biztosított fizetési felület, mely a Kereskedő részéről történő implementációt követően biztosítja az ügyfél általi kártyaadatok bevitelét és az ezt követő elektronikus fizetés teljes mértékű végrehajtását. Sikeres fizetés esetén a Kereskedő részére a [Notification API](#) segítségével megküldésre kerül a tranzakció részletei, melyet a kereskedőnek le kell zárni a bank felé küldött válasz üzenettel, melynek tartalmaznia kell a forwardURL-t, melyre a kártyabirtokos átirányításra kerül, ahol a kereskedő megjeleníti a tranzakció részleteit.

A nem, vagy helytelenül működő Notification API esetén a tranzakció sikertelen állapotba kerül és a kártyabirtokos a Kereskedő által megadott Failure URL-re kerül átirányításra. Ebben az esetben a kereskedőnek szükséges lekérdeznie a tranzakció státuszát és azt megjeleníteni a kártyabirtokos részére.

FONTOS, hogy a fizetési felület megnyitását követően, a kártyabirtokosnak 15 perc áll rendelkezésre a kártyaadatainak megadására, amennyiben szükséges az erős ügyfélhitelesítés lefolytatására, valamint a tranzakció befejezésére.

3.1.2.1 Fizetés folyamata



A fizetés lépései:

1. A Kártyabirtokos rendelést ad le a Kereskedő weboldalán, majd továbblép annak kifizetésére.
2. A Kereskedő átirányítja a Kártyabirtokost a Bank által biztosított fizetési felületre a kártyaadatok megadásának érdekében. Ennek pontos leírását a [Payment page segítségével történő fizetés](#) fejezet tartalmazza.
3. A Kártyabirtokos megadhatja a kártyaadatokat, vagy pedig mobiltárca alapú fizetést választhat.
4. Ezt követően elküldésre kerül a fizetési kérelem a Kibocsátó Bank irányába;
5. 3DS erős ügyfélhitelesítés használata esetén a Kártyabirtokosnak további adatok megadására van szükség a tranzakció jóváhagyásához (pl. egyszer használatos jelszó).
6. A Kártyabirtokos hitelesíti a tranzakciót.
7. A Kibocsátó Bank feldolgozza a tranzakciót és annak eredményét visszaadja.
8. A kártyabirtokos visszairányításra kerül a kereskedő weboldalára.
 - a) Sikeres fizetés esetén a Kereskedő részére a [Notification API](#) segítségével megküldésre kerül a tranzakció részletei, melyet a kereskedőnek le kell zárni a bank felé küldött válasz üzenettel, melynek tartalmaznia kell a forwardURL-t, melyre a kártyabirtokos átirányításra kerül., ahol a kereskedő megjeleníti a tranzakció részleteit.
 - b) A nem, vagy helytelenül működő Notification API esetén a tranzakció sikertelen állapotba kerül és a kártyabirtokos a Kereskedő által megadott Failure URL-re kerül átirányításra. Ebben az esetben a kereskedőnek szükséges lekérdeznie a tranzakció státuszát és azt megjeleníteni a kártyabirtokos részére
9. A Kereskedőnek a tranzakció adatait szükséges megjelenítenie a weboldalán a vásárló részére.
 - 9.1. Sikeres fizetés esetén:
 - Fizetés módja -> Bankkártyás fizetés
 - TranCode és szövege
 - ApprovalCode
 - Összeg és devizanem
 - OrderID
 - 9.2. Sikertelen fizetés esetén:
 - Fizetés módja -> Bankkártyás fizetés
 - TranCode és szövege
 - Összeg és devizanem
 - OrderID

3.1.2.2 Általános leírás

Amennyiben a webáruházban a Kártyabirtokos a kártyával történő fizetési lehetőség mellett döntött, a Kereskedő rendszere átirányítja őt a fizetési felületre (a tranzakcióhoz szükséges paraméterek megadásával), ahol a kártyaadatok megadása és ellenőrzése zajlik.

A fizetési felületre történő átirányítást követően a Kártyabirtokossal történő kommunikáció HTTPS protokoll használatával történik.

A Kereskedő rendszerének 3 weboldalt / szolgáltatást kell biztosítani a fizetési szolgáltatással történő interakció érdekében, melyek lehetnek ugyan azok is:

1. **NOTIFY_URL** -> ezen API segítségével a fizetési szolgáltatótól szinkron hívás segítségével a Kereskedő részére kerül elküldésre a tranzakció eredménye, melyet a sikeres tranzakció esetébenle kell zárnia.
2. **SUCCESS_URL** -> a Notify URL nem, vagy helytelen működése esetén a sikeres tranzakciót követően erre a linkre / oldalra kerül átirányításra a Kártyabirtokos.
3. **FAILURE_URL** -> a Notify URL nem, vagy helytelen működése esetén a sikertelen tranzakciót követően erre a linkre / oldalra kerül átirányításra a Kártyabirtokos. Ez a két cím lehet azonos is.

Amennyiben a kereskedő a bank által a Notify URL-jére küldött üzenetre technikai probléma miatt nem tud válaszolni, úgy a kártyabirtokos a kereskedő által korábban megadott SUCCESS_URL vagy pedig a FAILURE_URL kerül átirányításra. Továbbá a bank ezen esetben a tranzakció adatait POST metódussal átadja a kereskedőnek. Ennek okán kérjük a rendszerük ezen adatok fogadására történő felkészítését.

A bank által a SUCCESS vagy a FAILURE URL-re átadott adatok a következők:

Paraméter	Formátum	Leírás	Megjegyzés
MerchantID	AN(15)	Kereskedő egyedi azonosítója	Értéke megegyezik az eredeti authorizációs kérés értékével
TerminalID	AN(8)	Terminál egyedi azonosítója	Értéke megegyezik az eredeti authorizációs kérés értékével
TranCode	N(3)	Tranzakció eredményének kódja	Minden kérés tartalmazza az annak sikerességére vagy sikertelenségére vonatkozó kódot. Értékei.
AltCurrency	N(3)	NEM HASZNÁLT Deviza kód	Értéke megegyezik az eredeti authorizációs kérés értékével. Értékei.

ApprovalCode	AN(6)	Authorizációs kód	A Kibocsátó Bank által visszaadott authorizációs kód vagy jóváhagyó kód.
OrderID	ANS(1..20)	Rendelés azonosítója	Értéke megegyezik az eredeti authorizációs kérés értékével
Signature	AN(1..40)	Aláírás értéke	A paraméter karakterszáma függ a választott generálási módszertől
PurchaseTime	N(12)	Eredeti kérés pontos dátuma és ideje (YYMMDDhhmmss)	Értéke megegyezik az eredeti authorizációs kérés értékével
TotalAmount	N(1..12)	Összeg	Értéke megegyezik az eredeti authorizációs kérés értékével
AltTotalAmount	N(1..12)	NEM HASZNÁLT Összeg	Értéke megegyezik az eredeti authorizációs kérés értékével
ProxyPan	ANS(13..19)	Maszkolt PAN értéke	Maszkolt PAN értéke.
SD			Nem használt
XID	ANS(1..28)	Tranzakció azonosítója	Tranzakció azonosítója
Rrn	N(12)	Retrieval Reference Number	A kártyás tranzakció egyedi azonosítója az ISO 8583 szabvány alapján.
Delay	N(1)	Payment ID Pre-authorization	Értéke megegyezik az eredeti authorizációs kérés értékével
locale	A(2)	Interface nyelve (hu, de, en)	A fizetési felület nyelve. Amennyiben nem kerül megadásra, úgy alapértelmezetten magyar nyelven jelenik meg a fizetői oldal. Értékei.
Email			Nem használt

UPCToken	ANS(32)	Az első sikeres tranzakciót követően a payment gateway által megküldött TOKEN.	A Kártyabirtokos kártyaadatának helyettesítésére szolgál. Segítségével a Kereskedő terhelést kezdeményezhet a kártyaadatok megadása és a kártya tulajdonosának bevonása nélkül.
UPCTokenExp		A kártya lejáratának dátuma.	Formátuma MMYYYY. A token érvényességi ideje megegyezik a kártya lejárat dátumával. A Token – ahogyan a kártya - érvényessége a visszakapott év és hónap utolsó napjáig szól.

Tranzakció adatainak átadására példa:

MerchantID: 111111
 TerminalID: E222222
 TranCode: 000
 Currency: 348
 AltCurrency:
 ApprovalCode:
 OrderID: 3333333
 Signature:
 PurchaseTime: 230329113000
 TotalAmount: 10000
 AltTotalAmount: 0
 ProxyPan: 499999*****0011
 SD:
 XID: 24092716-6666666
 Rrn:
 Delay:
 locale: hu
 Email:
 UPCToken:
 UPCTokenExp:

3.1.2.2.1 Aláírás

FONTOS: a TID és a MID értékei teszt és az éles használat során, valamint Kereskedő weboldalanként IS eltérnek. 730 nap a tanúsítvány érvényessége.

Minden üzenetet digitális - *SHA512with RSA http* - aláírással kell ellátni, mely a privát és a nyilvános kulcsokon alapul és az üzenet signature változójában kell elhelyezni.

3.1.2.2.2 Kulcsok generálása

Előfeltételek:

1. OpenSSL letöltése és telepítése (1.1.1h verzióval tesztelve);
2. OpenSSL bin mappájának a rendszer környezeti változói között történő elhelyezése;

A Kereskedő általi kulcsok generálásának előfeltétele a Bank által kötött szerződés megléte, majd a Bank által történő regisztrálása. Csak ezt követően kaphatja meg a Kereskedő a MerchantID -t.

Szükséges létrehozni egy **config.dat** fület, melynek a Kereskedőre vonatkozó adatokat kell tartalmaznia ékezet nélkül.

```
[ req ]  
prompt = nem  
distinguished_name = req_distinguished_name
```

```
[ req_distinguished_name ]  
# Ország  
C = HU
```

```
# Megye  
ST = Pest  
# City  
L = Budapest
```

```
# Szervezet megnevezese  
O = Kereskedo halozat
```

```
# Agazat megnevezese  
OU = Bolt 23
```

```
# Tanusitvany neve  
CN = Test Kereskedo Bolt 23
```

```
# Szervezet e-mail cime  
emailAddress=teszt@kereskedo.hu
```

Az itt megadott adatok csak a tanúsítvány és a kapcsolódás azonosítására szolgálnak, ebből kifolyólag minimális eltérés lehet a Kereskedő regisztrációja során megadott adatokkal, azonban törekedni kell az adatok minél pontosabb megadására.

A kulcsok generálása az alábbi módon végezhető el. Kérjük cserélje le a %1 paramétert a parancsokban a Bank által megadott MerchantID-ra!

```
openssl genrsa -out %1.pem 4096
openssl req -new -key %1.pem -x509 -days 730 -config config.dat -out %1.crt
openssl x509 -in %1.crt -noout -pubkey -out %1.pub
```

A MerchantID előtaggal 3 file generálása szükséges:

- MerchantID.pem – private key
- MerchantID.pub - public key
- MerchantID.crt – certificate

A Kereskedő által generált **.crt file tömörített és jelszóval védett állományban** kerüljön elküldésre a vpos@raiffeisen.hu e-mail címre.

A generált .pem file kerüljön elhelyezésre a Kereskedő szerverének security mappájába.

3.1.2.2.3 Aláírás generálása (SHA512withRSA http)

A paraméterek sorrendje nem felcserélhető!

Az aláírást Base64 kódolással kell ellátni.

Amennyiben a Ref3 mező értéke is átadásra kerül a Payment Page részére, akkor az aláírásnak az alábbi formában kell felépülnie:

```
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;Ref3;
```

A ';' száma állandó, így, ha bármely mező értéke hiányzik, vagy nem kerül átadásra, akkor abban az esetben két pontosvessző kerül megadásra egymást követően: ';;'.

Mivel az aláírás utolsó paramétere nem kerül használatra, így az *Amount*-ot követő két karaktere minden esetben ';;'.

```
MerchantId;TerminalId;PurchaseTime;OrderId,Delay;CurrencyId;Amount;;
```

Amennyiben a Delay mező hiányzik, úgy az azt megelőző ';' elhagyása szükséges.

```
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;
MerchantId;TerminalId;PurchaseTime;OrderId,Delay;CurrencyId;Amount;;
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;
```

Az aláírás felépítése refund/reversal vonatkozásában:

A refund vagy reversal üzenetek során a következő adatok szükségesek: ApprovalCode, RRN. Ha a kérés tartalmazott RefundAmount és / vagy Ref3 mezőket, akkor azokat az aláírásban is szerepeltetni kell. A következő példa minden adatot tartalmaz:

Mivel a fizetési tranzakció aláírásának utolsó paramétere nem kerül használatra, így a refund és reversal aláírásában az *Amount*-ot követő és *ApprovalCore*-ot megelőző két karakter minden esetben ';' .

```
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;ApprovalCode;RRN  
;RefundAmount;Ref3;
```

Amennyiben nem kerül megadásra opcionálisan megadható mező (RefundAmount or Ref3), akkor az azokhoz tartozó ';' megadása sem szükséges.

```
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;ApprovalCode;RRN  
;Ref3;  
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;ApprovalCode;RRN  
;RefundAmount;  
MerchantId;TerminalId;PurchaseTime;OrderId;CurrencyId;Amount;;ApprovalCode;RRN  
;
```

A Banktól kapott üzenetek aláírásának validálása:

Az aláírás ellenőrzéséhez az adatoknak az alábbi sorrendben kell szerepelnie:

```
MerchantId;TerminalId;PurchaseTime;OrderId,Delay;Xid;CurrencyId;Amount;;TranCo  
de;ApprovalCode;
```

A tokennel ellátott aláírás ellenőrzéséhez az adatoknak az alábbi sorrendben kell szerepelnie:

```
MerchantId;TerminalId;PurchaseTime;OrderId,Delay;Xid;CurrencyId;Amount;;TranCode;ApprovalCode;UPCT  
oken,UPCTokenExp;
```

Az aláírás ellenőrzéséhez a Bank által kiállított tanúsítvány szükséges, mely a teszt és az éles környezet tekintetében eltérő.

Az üzenet aláírásának előállításához SHA512withRSA algoritmus szükséges.

3.1.2.2.4 Teszt kulcs a bank által küldött üzenetek ellenőrzéséhez

A fejlesztés során a teszt rendszerben a bank által küldött üzenetek az alábbi tanúsítvánnyal kerülnek aláírásra. Az üzenetek validálásához kérjük az alábbi kulcsot használnia.

```
-----BEGIN CERTIFICATE-----
MIICChDCCAe0CASowDQYJKoZIhvcNAQEFBQAwgYgxCzAJBgNVBAYTAIVBMQ0wCwYD
VQQIEwRLWUIWMQ0wCwYDVQQHEwRLWUIWMQwwCgYDVQQKEwNVUEMxEzARBgNVBAsT
CkUtQ09NTUUVSQ0UxGTAxBgNVBAMTEFVQYy5FQ09NTUUVSQ0UuQ0ExHTAbBgkqhkiG
9w0BCQEWDmVjLmhlbHBAdXBjLnVhMB4XDTA2MDMxNDE0MDIxNVVoXDTA5MDEwMTE0
MDIxNVowgYsxCzAJBgNVBAYTAIVBMRMwEQYDVQQIEwptb21lLVN0YXRIMQ0wCwYD
VQQHEwRLeWI2MQwwCgYDVQQKEwNVUEMxZzAVBgNVBAsTDmVDb21tZXJjZSBVbml0
MRIwEAYDVQQDEwItaWduYXR1cmUxHTAbBgkqhkiG9w0BCQEWDmVjLmhlbHBAdXBj
LnVhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzloeW9btImJ1X/u1DofZY
1lGEAdDqmBKljFIARpwyNjUb70RkZPzq1TB3SuNNJQ+1Wms2sKGu5uozoy9a2AR
rJOsR+QJSwEcQo/th+NhhTTBNh/rPshlCX6R2Hm1yoMTvTrloxAXpDtkeyMQdBe
SZ991wX/EhX0zMaRG2dDSQIDAQABMA0GCSqGSIb3DQEEBBQUAA4GBAMwpbjWXzoNQ
wQcxAYaoL7uFhNDub8QnCJJjC3HvGz2Kz250hyWc3KVRSEGG4I9sNZ11PrHUg6OP
i4dPF01D5Nd36YlcMj5wsu3L4J77NvuLAj36ZZTPTsp0UmFdPaBa99GaeZgyfRxB
NNNZ4iNswLcXmGStimAC/32TO4SsPn91
-----END CERTIFICATE-----
```

3.1.2.2.5 Éles kulcs a bank által küldött üzenetek ellenőrzéséhez

A kereskedő általi integrációt és a Bank általi ellenőrzést követően az éles rendszerben a bank által küldött üzenetek az alábbi tanúsítvánnyal kerülnek aláírásra. Az üzenetek validálásához kérjük az alábbi kulcsot használnia.

```
-----BEGIN CERTIFICATE-----
MIICfTCCAeYCAQkwDQYJKoZIhvcNAQEFBQAwgYgxCzAJBgNVBAYTAIVBMQ0wCwYD
VQQIEwRLWUIWMQ0wCwYDVQQHEwRLWUIWMQwwCgYDVQQKEwNVUEMxEzARBgNVBAsT
CkUtQ09NTUUVSQ0UxGTAxBgNVBAMTEFVQYy5FQ09NTUUVSQ0UuQ0ExHTAbBgkqhkiG
9w0BCQEWDmVjLmhlbHBAdXBjLnVhMB4XDTA1MDgwMzEzNTk0MFoXDTA4MDUyMzEz
NTk0MfowgYQxCzAJBgNVBAYTAIVBMQ0wCwYDVQQIEwRLeWI2MQ0wCwYDVQQHEwRL
eWI2MQwwCgYDVQQKEwNVUEMxGTAxBgNVBAsTEEUtQ29tbWVvY2UgRGVwdC4xZDZAN
BgNVBAMTBnNlcnciZicjEdMBSGCSqGSIb3DQEJARYOZWZMUAoGVscEB1cGMudWEwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANNcize8kS8kblb3mV9tT54S3LaseLlb
hsnMlxVwVK3Zvpnug/OAn7H0dd3z0QKH9KbX/LXpC2I0uf6TJcpRkkp9XBedlwhS
OvAFqqvCam5K7EgpLQhm2WN7CU8G/yeHypRrk2zyR8djpHQJOGlyMqcccn0CeFos
jUu3Ju/e9bnAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEACanXJ0K2838tRW49Jl0N
NrLFR3GWFJTevs3H952TM7TN2neuEAYAB9XQ2Gk9MBrHgw4Wc2A89VK1M8rd7Mzo
Qvz3ABE7+zRa2r/Fgg0wO219ixEajBw5Q2PNrzEwqe810Mz8CPCbvOQd/eH4BDm6
J2vxcUsUDwW7zXITB4mdW6l=
-----END CERTIFICATE-----
```

Ezen tanúsítvány nem rendelkezik lejáratával.

3.1.2.3 Payment Page-en történő fizetés indítása

A Kereskedő weboldaláról történő Payment Page meghívása során kötelező a meghatározott paraméterek átadása, külön ehhez a szolgáltatáshoz biztosított kereskedő (MID) és terminál azonosító (TID) segítségével. Ezen paramétereket és azok leírását az alább található „Kérés paramétereit” táblázat tartalmazza.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/rbhu/enter	Teszt payment gateway cím
POST	https://secure-ecom.raiffeisen.hu/rbhu/enter	Éles payment gateway cím

Kérés paramétereit:

Paraméter	Kötelező	Formátum	Leírás	Megjegyzés
Version	igen	N(1)	Interface verziója	Kommunikációs protokoll verziószáma. Jelenlegi értéke '1'. Ezen paraméter szolgál referenciálul a gateway számára az input feldolgozásához.
MerchantID	igen	AN(15)	Kereskedő egyedi azonosítója	Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	igen	AN(8)	Terminál egyedi azonosítója	Egyedi azonosító, mely a Bank által kerül kiállításra
TotalAmount	igen	N(1..12)	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
Currency	igen	N(3) 348	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.

PurchaseTime	igen	N(12..17)	Megadható dátum és idő formátumok yyMMddHHmmss	<ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
Local	igen	A(2)	Interface nyelve (hu, de, en)	A fizetési felület nyelve. Amennyiben nem kerül megadásra, úgy alapértelmezetten magyar nyelven jelenik meg a fizetői oldal. Értékei.
OrderID	igen	ANS(1..20)	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.
PurchaseDesc	nem	ANS(0..125)	A vásárlás rövid leírása	A kereskedő részéről tetszőlegesen megadható leírás a vásárló tájékoztatása érdekében. A Kereskedői portálon, Payment Page-n kerül megjelenítésre.
Signature	igen	SHA512withRSA	Aláírás értéke	A paraméter karakterszáma függ a választott generálási metódustól
Delay	nem	N(1)	Előengedélyezés jelzésének paramétere	Amennyiben a kereskedő ilyen funkcióval nem rendelkezik, úgy elhagyható. Előengedélyezés indításához a paraméter értéke „1”, máskülönben „0” vagy nem is kerül átadásra

Ref3	igen	ANS(0..150)	Egyedi rendelésazonosító	<p>Megadható jegyszám vagy egyéb azonosító, mint teljes név, telefonszám, stb.</p> <p>Amennyiben nem szeretne külön azonosítót használni, úgy ennek értékeként az OrderID megadása szükséges.</p> <p>Ezen érték kerül megjelenítésre az analitikában.</p>
------	------	-------------	-----------------------------	---

A paraméterek átadása HTTPS / POST metódus segítségével történik egy előre definiált HTML formátumban a Payment Page részére, ahol a Vevő megadhatja a kártya adatait.

Adatátadásra példa:

```
<form action="https://ecg.test.upc.ua/rbhu/enter" method="POST">
  <input name="Version" type="hidden" value="1" />
  <input name="MerchantID" type="hidden" value="1111111" />
  <input name="TerminalID" type="hidden" value="E1111111" />
  <input name="TotalAmount" type="hidden" value="100000" />
  <input name="Currency" type="hidden" value="348" />
  <input name="Local" type="hidden" value="hu" />
  <input name="PurchaseTime" type="hidden" value="230329113000"/>
  <input name="OrderID" type="hidden" value="RENDELES_123" />
  <input name="PurchaseDesc" type="hidden" value="tran test" />
  <input name="Ref3" type="hidden" value="RefAzon" />
  <input name="Signature" type="hidden" value="" />
  <input type="submit"/>
</form>
```

3.1.2.3.1 Emv 3DSecure tranzakció feldolgozása *(opcionálisan implementálható)*

Az Emv 3DS tranzakció feldolgozáshoz szükséges kiegészítő adatok - Kereskedő részéről történő – átadása a Payment Page meghívásakor történik. Ezen adatok átadása a kérés 3DSv2Data mezőjében történik JSON formátumban. Ezt követően a megadott adatok alapján a Kibocsátó Bank és az Elfogadó Bank döntést hoz a további hitelesítés szükségességéről.

Ezt követően a Kártyabirtokos a Payment Page-en adhatja meg a fizetéshez szükséges kártya adatokat.

3DS megfelelően működik 3DSv2Data paraméterek megadása nélkül is, ezek kiegészítő információk.

Átadandó paraméterek:

Elem neve	Mező neve	Leírás	Elfogadott értékei- / formátuma
acctInfo	chAccAgeInd	Mennyi ideje rendelkezik a kártyabirtokos fiókkal a kereskedőnél	01 = Nem rendelkezik (vendégként vásárol) 02 = A tranzakció során regisztrált 03 = Kevesebb mint 30 nap 04 = 30–60 nap 05 = Több mint 60 nap
	chAccChange	Adatok legutolsó módosításának dátuma. Pl.: számlázási cím, szállítási cím, fizetési mód vagy regisztráció dátuma.	YYYYMMDD
	chAccChangeInd	Adatok legutolsó módosításának hossza. Pl.: számlázási cím, szállítási cím, fizetési mód vagy regisztráció dátuma.	01 = Tranzakció során módosított 02 = Kevesebb mint 30 napja 03 = 30–60 napja 04 = Több mint 60 napja
	chAccDate	Regisztráció dátuma.	YYYYMMDD
	chAccPwChange	Utolsó jelszó módosítás, vagy fiók visszaállítás dátuma.	YYYYMMDD

chAccPwChangeInd	Utolsó jelszó módosítás, vagy fiók visszaállítás hossza.	01 = Nem változott 02 = Tranzakció során módosított 03 = Kevesebb mint 30 napja 04 = 30–60 napja 05 = Több mint 60 napja
nbPurchaseAccoun	Az elmúlt 6 hónapban a kártyabirtokos fiókjával történt vásárlások darabszáma.	
paymentAccAge	Az a dátum, amikor a fizetési számlát a kártyabirtokos 3DS kérelmező-fiókjában regisztrálták.	YYYYMMDD
paymentAcclnd	Az időtartam, ami óta a Kártyabirtokos regisztrációval rendelkezik a 3DS kérelmezőnél.	01 = Nem rendelkezik (vendégként vásárol) 02 = A tranzakció során regisztrált 03 = Kevesebb mint 30 nap 04 = 30–60 nap 05 = Több mint 60 nap
provisionAttemptsDay	Kártyaregisztrációs kísérletek száma az elmúlt 24 órában.	
shipAddressUsage	Az a dátum, amikor a tranzakcióhoz használt szállítási címet először használták	YYYYMMDD
shipAddressUsageInd	Annak intervalluma, amikor a tranzakcióhoz használt szállítási címet először használták	01 = Ezen tranzakció során 02 = Kevesebb mint 30 napja 03 = 30–60 napja 04 = Több mint 60 napja
shipNameIndicator	A számlán szereplő Kártyabirtokos nevének és a tranzakcióhoz használt szállítási név azonosságának ellenőrzése.	01 = Megegyező 02 = eltérő

	suspiciousAccActivity	Kereskedő tapasztalt-e gyanús tevékenységet (beleértve a korábbi csalást is) a kártyabirtokos számláján.	01 = Nem tapasztalt gyanús tevékenységet 02 = Tapasztalt gyanús tevékenységet
	txnActivityDay	Tranzakciók (sikeres és felhagyott) száma ehhez a kártyabirtokos számlához a 3DS Kérelmező szolgáltatással az összes fizetési számlán az elmúlt 24 órában.	
	txnActivityYear	Tranzakciók száma (sikeres és félbehagyott) ehhez a kártyabirtokos számlához a 3DS Kérelmező szolgáltatással az összes fizetési számlán az előző évben.	
	acctNumber	Számlaszám, a fizetési tranzakciók engedélyezési kérelméhez. PAN, token képviselheti.	
	acctType	A kártya típusát jelzi	01 = Nem alkalmazható 02 = Credit 03 = Debit
	cardExpiryDate	PAN / token lejárat dátuma	
cardHolderInfo	billAddrCity	A Kártyabirtokos számlázási címének városa. (kötelező (ha rendelkezésre áll), kivéve, ha a piaci vagy regionális rendelkezések korlátozza ezen információ küldését)	
	billAddrCountry	A Kártyabirtokos számlázási címének országa.	

billAddrLine1	A kártyabirtokos számlázási címének első sora.	
billAddrLine2	A kártyabirtokos számlázási címének második sora.	
billAddrLine3	A kártyabirtokos számlázási címének harmadik sora.	
billAddrPostCode	A számlázási cím irányítószáma.	
billAddrState	A számlázási címhez tartozó megye.	
cardholderName	Kártyabirtokos neve.	
email	A kártyabirtokos által a vásárlás során, vagy pedig a 3DS Requestor-nál a regisztráció során megadott e-mail címe.	
homePhone	A kártyabirtokos által megadott otthoni telefonszáma.	Példa 'homePhone': {'Cc':'044','Subscriber':'55555555'} <i>Országkód (Cc), 1-3 hosszán;</i>
mobilePhone	A kártyabirtokos által megadott mobiltelefon száma.	Példa 'mobilePhone': {'Cc':'044','Subscriber':'55555555'} <i>Országkód (Cc), 1-3 hosszán;</i>
shipAddrCity	A kártyabirtokos által megadott szállítási cím városa.	
shipAddrCountry	A kártyabirtokos által megadott szállítási cím országa.	
shipAddrLine1		

	shipAddrLine2		
	shipAddrLine3		
	shipAddrPostCode	A kártyabírtokos által megadott szállítási cím irányítószáma.	
	shipAddrState	A kártyabírtokos által megadott szállítási cím megyéje.	
	workPhone		
	merchantId	Az Elfogadó Bank által a kereskedő részére kiadott azono-sítója.	
merchantRiskIndicator	deliveryEmailAddresses		
	deliveryTimeframe	Az áru szállítási időintervalluma.	01 = Elektronikus módon 02 = Azonos napi szállítás 03 = Következő napi szállítás 04 = Kettő vagy több napi szállítás
	giftCardAmount		
	giftCardCount		
	giftCardCurr		
	preOrderDate		
	preOrderPurchaseInId		
	reorderItemsInId		

	shipIndicator	A tranzakcióhoz választott szállítási módot jelöli. A kereskedőknek azt a Szállítási mutatót kell kiválasztaniuk, amely a legpontosabban írja le a kártyabirtokos konkrét tranzakcióját, nem pedig az általános üzleti tevékenységét. Ha egy vagy több cikk is szerepel a vásárlásban, akkor a fizikai áruhoz használja a Szállítási mutatót, vagy ha kizárólag digitális áruról van szó, akkor használja a legdrágább termékre vonatkozó Szállítási mutatót.	<p>01 = A kártyabirtokos számlázási címére kerül kiszállításra</p> <p>02 = Egyéb, kereskedőnél már megadott címre kerül kiszállításra</p> <p>03 = A kártyabirtokos számlázási címétől eltérő címre kerül kiszállításra</p> <p>04 = "Bolton átétel" / Átvétel helyi üzletben (A Kereskedő címét a szállítási cím mezőknek kell tartalmaznia)</p> <p>05 = Digitális javak (például online szolgáltatásokat, elektronikus ajándék kártyákat tartalmaz)</p> <p>06 = Utazási és rendezvényre szóló jegyek, nincs szállítás</p> <p>07 = Egyéb (például játékok, digitális szolgáltatások melyek nem kerülnek kiszállításra, valamint különböző digitális előfizetések stb.)</p>
priorTransl D		A3DS Server tranzakció ID a kártyabirtokos előzetesen hitelesített tranzakciójához.	Példa: 59ae264e-b0f4-43c7-870e-4d14bd52806e
threeRIInd		3RI kérés típusa	<p>01 = Ismétlődő tranzakció</p> <p>02 = Részletfizetés</p> <p>03 = Add card</p> <p>04 = Kártya információk frissítése</p> <p>05 = Kártya tokenizálása (Account verification)</p>

Példa:

```
<form action="https://ecg.test.upc.ua/rbhu/enter" method="POST">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <input name="Version" type="hidden" value="1">
  <input name="MerchantID" type="hidden" value="1111111">
  <input name="TerminalID" type="hidden" value="E1111111">
  <input name="TotalAmount" type="hidden" value="1000">
  <input name="Currency" type="hidden" value="348">
  <input name="Local" type="hidden" value="hu">
  <input type="HIDDEN" name="PurchaseTime" value="230329113000">
  <input name="OrderID" type="hidden" value="121sdsds2sd">
  <input name="PurchaseDesc" type="hidden" value="tran test">
  <input name="Signature" type="hidden" value="">
  <input name="3DSv2Data" type="hidden" value="
    {
      "acctInfo":{
        "chAccAgeInd":"03",
        "chAccChange":"20160712",
        "chAccChangeInd":"04",
        "chAccDate":"20140328",
        "chAccPwChange":"20170328",
        "chAccPwChangeInd":"02",
        "nbPurchaseAccount":"11",
        "paymentAccAge":"20160917",
        "paymentAcclnd":"02",
        "provisionAttemptsDay":"3",
        "shipAddressUsage":"20160714",
        "shipAddressUsageInd":"02",
        "shipNameIndicator":"02",
        "suspiciousAccActivity":"02",
        "txnActivityDay":"1",
        "txnActivityYear":"21"
      },
      "acctType":"03",
      "authenticationInd":"01",
      "authenticationInfo":{
        "threeDSReqAuthData":"login GP",
        "threeDSReqAuthMethod":"02",
        "threeDSReqAuthTimestamp":"201711071307"
      },
      "cardHolderInfo":{
        "billAddrCity":"Sydney",
        "billAddrCountry":"036",
        "billAddrLine1":"Unit 1",
        "billAddrLine2":"123 Street Suburb",
        "billAddrLine3":"abc Line 3",
        "billAddrPostCode":"2000",
        "billAddrState":"NSW",
```



```
"cardholderName":"Suda Ichiro",
"email":"abc@123.com",
"homePhone":{
  "cc":"61",
  "subscriber":"90123917131"
},
"mobilePhone":{
  "cc":"61",
  "subscriber":"0421522329"
},
"workPhone":{
  "cc":"61",
  "subscriber":"89102183192"
},
"shipAddrCity":"Sydney",
"shipAddrCountry":"036",
"shipAddrLine1":"Unit 1",
"shipAddrLine2":"123 Street",
"shipAddrLine3":"abc Line 3",
"shipAddrPostCode":"2000",
"shipAddrState":"NSW"
},
"challengeInd":"01",
"eventCallbackUrl":"http://localhost:8082/3ds-notify",
"merchantId":"123456789012345",
"merchantRiskIndicator":{
  "deliveryEmailAddress":"test@123.com",
  "deliveryTimeframe":"02",
  "giftCardAmount":"123",
  "giftCardCount":"02",
  "giftCardCurr":"840",
  "preOrderDate":"20170519",
  "preOrderPurchaseInd":"02",
  "reorderItemsInd":"01",
  "shipIndicator":"01"
},
"purchaseAmount":"200",
"purchaseCurrency":"036",
"purchaseDate":"20190521104643",
"purchaseInstalData":"24",
"transType":"03"
}
">
<input type="submit">
</form>
```

3.1.3 Sztornó (reversal) tranzakció

Sztornó (reversal) csak a tranzakció napján kezdeményezhető, teljes összeggel, amennyiben a napzárás még nem történt meg.

Ez POST hívás segítségével lehetséges az alábbi táblázatokban található végpont és paraméterek segítségével.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/rbhu/repayment	Teszt payment gateway cím
POST	https://secure-ecom.raiffeisen.hu/rbhu/repayment	Éles payment gateway cím

Kérés paramétere:

Paraméter	Kötelező	Formátum	Leírás	Megjegyzés
MerchantID	igen	AN(15)	Kereskedő azonosítója egyedi	Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	igen	AN(8)	Terminál azonosítója egyedi	Egyedi azonosító, mely a Bank által kerül kiállításra
TotalAmount	igen	N(1..12)	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
Currency	igen	N(3)	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.

PurchaseTime	igen	N(12..17)	Megadható dátum és idő formátumok yyMMddHHmmss	<ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
OrderID	igen	ANS(1...20)	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.
ApprovalCode	igen	AN(6)	Authorizációs kód	A kibocsájtó bank által visszaadott authorizációs kód vagy jóváhagyó kód.
Rrn	igen	N(12)	Retrieval Reference Number	A kártyás tranzakció egyedi azonosítója az ISO 8583 szabvány alapján.
Signature		Depends on the scheme	Aláírás értéke	A paraméter karakterszáma függ a választott generálási metódustól
Ref3	igen	ANS(0..150)	Egyedi rendelésazonosító	<p>Megadható jegyszám vagy egyéb azonosító, mint teljes név, telefonszám, stb.</p> <p>Amennyiben nem szeretne külön azonosítót használni, úgy ennek értékeként az OrderID megadása szükséges.</p> <p>Ezen érték kerül megjelenítésre az analitikában.</p>
RefundAmount	igen	N(1..12)	Visszatérítés értéke	Visszatérítés értéke

Példa kérés:

```

<html>
  <body>
    <form method='POST' action="https://ecg.test.upc.ua/rbhu/repayment">
      <input type='hidden' name='MerchantID' value='1111111' />
      <input type='hidden' name='TerminalID' value=' E2222222' />
      <input type='hidden' name='OrderID' value= RENDELES_123/>
      <input type='hidden' name='Currency' value='348' />
      <input type='hidden' name='TotalAmount' value='12550' />
      <input type='hidden' name='PurchaseTime' value='230329113000' />
      <input type='hidden' name='ApprovalCode' value='123456' />
      <input type='hidden' name='RRN' value='5555555555' />
      <input type='hidden' name='RefundAmount' value='12000' />
      <input type='hidden' name='Signature' value='45F345Fafde4455445Gvb550'
    />
    <input type='submit' value='go'>
  </form>
</body>
</html>

```

A kérésre kapott válasz az alábbi paramétereket tartalmazza:

Paraméter	Formátum	Leírás	Megjegyzés
TranCode	N(3)	Tranzakció eredményének kódja	Minden kérés tartalmazza az annak sikerességére vagy sikertelenségére vonatkozó kódot. Értékei.
MerchantID	AN(15)	Kereskedő egyedi azonosítója	
TerminalID	AN(8)	Terminál egyedi azonosítója	
CardScheme	AN(4)	Kártya típusa	<ul style="list-style-type: none"> • VISA – Visa • MAST – MasterCard • MAES - Maestro
ERROR	ANS	Hiba rövid leírása	Csak hiba esetén tartalmazza.

Példa válasz:

```
<html>
<body>
  <form>
    <input name="MerchantID" type="hidden" value="1111111"/>
    <input name="TerminalID" type="hidden" value="E2222222"/>
    <input name="CardScheme" type="hidden" value="VISA" />
    <input name="TranCode" type="hidden" value="000" />
  </form>
</body>
</html>
```

3.1.4 Tranzakció státuszának lekérdezése

3.1.4.1 HTML formátum segítségével

A Kereskedő részére biztosított az adott fizetési tranzakció állapotának lekérdezése.

Ez POST hívás segítségével lehetséges az alábbi táblázatokban található végpont és paraméterek segítségével.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/rbhu/service/01	Teszt payment gateway cím
POST	https://secure-ecom.raiffeisen.hu/rbhu/service/01	Éles payment gateway cím

Kérés paramétere:

Paraméter	Kötelező	Formátum	Leírás	Megjegyzés
MerchantID	igen	AN(15)	Kereskedő azonosítója	egyedi Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	igen	AN(8)	Terminál azonosítója	egyedi Egyedi azonosító, mely a Bank által kerül kiállításra

TotalAmount	igen	N(1..12)	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 10000 megadása szükséges.
Currency	igen	N(3)	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.
PurchaseTime	igen	N(12..17)	Megadható dátum és idő formátumok yyMMddHHmmss	Az értékének meg kell egyeznie a lekérdezni kívánt tranzakció PurchaseTime paraméterével. <ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
OrderID	igen	ANS(1..20)	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.

Példa kérés:

```

<html>
<body>
  <form method='POST' action="https://ecg.test.upc.ua/rbhu/service/01">
    <input type='hidden' name='MerchantID' value='1111111'>
    <input type='hidden' name='TerminalID' value='E2222222'>
    <input type='hidden' name='TotalAmount' value='12550'>
    <input type='hidden' name='Currency' value='348'>
    <input type='hidden' name='PurchaseTime' value='230329113000'>
    <input type='hidden' name='OrderID' value='RENDELES_123'>
  </form>
</body>
</html>

```

A kérésre a választ szöveggént kapja meg a Kereskedő az alábbi hozzáadott paraméterekkel:

- XID
- TranCode
- ApprovalCode

Válaszra példa:

```
<html>
<body>
  <pre style="word-wrap: break-word; white-space: pre-wrap;">XID=00023092017-112376-1
  TranCode=000
  Currency=348
  TerminalID=E2222222
  MerchantID=1111111
  OrderID= RENDELES_123
  ApprovalCode=502222
  ProxyPan=555949*****0015
  RRN=326317227596
  </pre>
</body>
</html>
```

Ennek a megoldásnak a használata opcionális. használata javasolt pl. arra az esetre, ha a Vásárló böngészőjében nem jelent meg megfelelően a tranzakcióra kapott válasz.

3.1.4.2 JSON formátum segítségével

A JSON típusú hívások leírását a [Általános leírás](#) fejezet tartalmazza.

A Kereskedő ezen API segítségével tudja az előzetes fizetési tranzakció állapotát lekérdezni.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/rbhu/service/01	Teszt payment gateway cím -JSON
POST	https://secure-ecom.raiffeisen.hu/rbhu/service/01	Éles payment gateway cím -JSON

Kötelezően beállítandó mezők a státusz kéréshez:

Paraméter	JSON adattípus	Formátum	Kötelező	Name	Leírás
MerchantID	string	AN(15)	igen	Kereskedő azonosítója	egyedi Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	string	AN(8)	igen	Terminál azonosítója	egyedi Egyedi azonosító, mely a Bank által kerül kiállításra
TotalAmount	number	N(1..12)	igen	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
Currency	number	N(3)	igen	Deviza kód	Egyedi azonosító, mely a Bank által kerül kiállításra. Értékei.
PurchaseTime	string	N(12..17)	igen	Megadható dátum és idő formátumok yyMMddHHmmss	Az értékének meg kell egyeznie a lekérdezni kívánt tranzakció PurchaseTime paraméterével. <ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc

A válaszban megtalálható lesz a „result” tömb, mely a keresés eredményét tartalmazza. Amennyiben a keresés találatot eredményez, úgy a válasz az alábbi táblázatban található értékekkel tér vissza.

Paraméter	JSON adattípus	Formátum	Name	Leírás
tranCode	string	N(3)	Tranzakció eredményének kódja	Result code of the transaction
approvalCode	string	AN(6)	Authorizációs kód	A Kibocsátó Bank által visszaadott authorizációs kód vagy jóváhagyó kód.
rrn	string	N(12)	Retrieval Reference Number	A kártyás tranzakció egyedi azonosítója az ISO 8583 szabvány alapján.
comment	string	ANS(0..64)	Result comment	Result of transaction
cardNumMasked	string	N(13..19)	A kártya első 6 és utolsó 4 karakterét tartalmazza.	Maszkolt PAN értéke.
tranTime	string	ANS(..20)	Tranzakció időpontja	Tranzakció időpontja
amount	number	N(1..12)	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
currency	number	N(3)	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.
operType	string	ANS	Tranzakció típusa	Tranzakció típusának leírása
actionCode	string	N(3)	Szolgáltató válaszkódja	Az értéke az elutasított tranzakció további elemzésének segítségével szolgálhat.

3.2 Opcionálisan implementálható megoldások

3.2.1 Visszatérítés (Refund) tranzakció

A visszatérítés engedélyezéséhez lépjen kapcsolatba a dedikált kapcsolattartójával.

Visszatérítés (refund) indítására csak a tranzakció elszámolását követően van lehetőség teljes vagy részleges összegben.

Ezen funkciót a [Sztornó \(reversal\) tranzakció](#) fejezetben leírtaknak megegyezően lehet implementálni. A Bank dönti el az adott - *rbhu/repayment* végpontra küldött - kérésről, hogy az sztornó vagy visszatérítés lesz.

3.2.2 Előengedélyezés / Előengedélyezés befejezése

A lehetőség engedélyezéséhez lépjen kapcsolatba a dedikált kapcsolattartójával.

Ezen típusú fizetési tranzakció használata olyan esetekben célszerű, mely során első körben a kártyán egy bizonyos összeg kerül zárolásra, azonban VISA bankkártyával történő tranzakció esetén a végleges fizetés akár nagyobb összeggel is történhet, maximum az eredeti összeg 115%-val. Mastercard és Maestro esetén csak az eredeti összeg 100%-val zárható le az előengedélyezett tranzakció.

Használata során a fizetési kérés kiegészítése szükséges egy Delay mezővel melynek értéke "1".

Fizetési folyamat:

1. A Kereskedő a kérést kiegészíti **Delay=1** paraméterrel.
2. A Kártyabirtokos (Vevő) végig megy a már ismert fizetési folyamaton.
3. Ha a tranzakció sikeres, akkor az adott összeg zárolásra kerül a kártyabirtokos számláján, továbbá a tranzakción feltüntetésre kerül, hogy „előengedélyezés”.
4. Ez a tranzakció nem kerül automatikusan elszámolás alá. A fizetés véglegesítését és elszámolását a Kereskedő a Kereskedő Portálon tudja elvégezni az [Előengedélyezés és annak befejezése](#) fejezetben részletezett módon.
5. Az előengedélyezés befejezésére a Kereskedő Portálon van lehetőség az adott tranzakció részletező felületén maximum 30 napig. A 31. napon az előengedélyezett tranzakció már nem zárható le, valamint a kártyabirtokos számláján korábban zárolt összeg feloldásra kerül.
6. Sikeres fizetést követően az „Előengedélyezés” típusú tranzakció „Előengedélyezés befejezése” típusú tranzakcióra változik, mely a fizetés tényét bizonyítja.

3.2.2.1 Előengedélyezés befejezése POST hívás segítségével

Az eredeti tranzakció adatainak megadása szükséges a megfelelő paraméterek beállításához. Ezen adatokat a Kereskedő a sikeres előengedélyezés tranzakciót követően, az általa kialakított Notification URL-re megküldött válaszból tudja megadni.

Ez POST hívás segítségével lehetséges az alábbi táblázatokban található végpont és paraméterek segítségével.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/go/capture	Teszt payment gateway cím
POST	https://secure-ecom.raiffeisen.hu/go/capture	Éles payment gateway cím

Kérés paraméterei:

Paraméter	Kötelező	Formátum	Leírás	Megjegyzés
MerchantID	igen	AN(15)	Kereskedő egyedi azonosítója	Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	igen	AN(8)	Terminál egyedi azonosítója	Egyedi azonosító, mely a Bank által kerül kiállításra
TotalAmount	igen	N(1..12)	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
Currency	igen	N(3)	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.

PurchaseTime	igen	N(12..17)	Megadható dátum és idő formátumok yyMMddHHmmss	<ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
OrderID	igen	ANS(1...20)	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.
ApprovalCode	igen	AN(6)	Authorizációs kód	A kibocsájtó bank által visszaadott authorizációs kód vagy jóváhagyó kód.
Rrn	igen	N(12)	Retrieval Reference Number	A kártyás tranzakció egyedi azonosítója az ISO 8583 szabvány alapján.
PostauthorizationAmount	igen	N(1..12)	Előengedélyezés befejezésének összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges. A rendelés eredeti összegétől nem lehet több.
Signature		Depends on the scheme	Aláírás értéke	A paraméter karakterszáma függ a választott generálási metódustól

Példa kérés:

```
<html>
<body>
<form method='POST' action="https://ecg.test.upc.ua/go/capture">
  <input type='hidden' name='MerchantID' value='1111111' />
  <input type='hidden' name='TerminalID' value='E1111111' />
  <input type='hidden' name='OrderID' value='RENDELES_123' />
  <input type='hidden' name='Currency' value='348' />
  <input type='hidden' name='TotalAmount' value='1200000' />
  <input type='hidden' name='PurchaseTime' value='230329113000' />
  <input type='hidden' name='ApprovalCode' value='123456' />
  <input type='hidden' name='RRN' value='E222222222' />
  <input type='hidden' name='PostauthorizationAmount' value='1200000' />
  <input type='hidden' name='Signature' value="" />
  <input type='submit' value='go'>
</form>
</body>
</html>
```

Példa válasz:

```
<html>
<head></head>
<body>
<p>TranCode=000
TerminalID=E7885614
MerchantID=1757764
</p>
</body>
</html>
```

Amennyiben az előengedélyezés befejezése sikeresen megtörtént, a hívásra kapott válaszban a TranCode=000 értékkel szerepel. Hiba esetén az alábbi táblázatban található kódok egyike található meg a TranCode értékeként.

Hibakódok:

Tran code	Leírás
506	Az előengedélyezés befejezésének határideje lejárt. (több mint 30 nap)
507	Az előengedélyezés befejezése már sikeresen megtörtént. (újbóli próbálkozás esetén)
508	Az előengedélyezés befejezése során a fizetendő összeg nem megfelelően lett megadva. (rossz összeg, vagy annak értéke Mastercard esetén több mint az eredeti összeg, VISA esetén pedig több mint az eredeti összeg 115%-a)

3.2.3 Webes fizetés + JSON API

A Kereskedőnek fel kell vennie a kapcsolatot a dedikált kapcsolattartójával és kérvényeznie kell a tokenizálási szolgáltatás aktiválását, amennyiben ez a kiegészítő szolgáltatás nem a szerződéskötéskor került megigénylésre.

A kártyaadatok helyettesítésére egy tokenizálási eljárás került kialakításra, mely lehetővé teszi a fizetési kérelmek küldését JSON backend-backend API kommunikáció segítségével. A kártya tokenizálásához elengedhetetlen egy, a fizetési felületen (Webes fizetés) a Kártyabirtokos által indított és végrehajtott sikeres fizetési tranzakció, mely során a Kártyabirtokos a kártyája tokenizálásához hozzájárult. Mivel a JSON API segítségével történő fizetés során kártyaadatok megadása nem lehetséges, így az ilyen típusú fizetés előfeltétele a fizetési felület implementálása.

CIT-es fizetésre csak bizonyos összeghatárig van lehetőség CVC / CVV kód megadása nélkül. Ha a fizetés összege meghaladja a Bank által meghatározott maximálisan engedélyezett összeget, akkor HTML alapú, Payment Page-en történő fizetést kell indítania a kereskedőnek.

Bankkártya tokenizációja:

1. Kártyabirtokos a fizetői felületen megadja a kártyaadatokat és hozzájárulását adja a kártyaadatának tokenizálására.
2. A sikeres tranzakciót követően a Kereskedő a [NOTIFY_URL](#)-ére küldött üzenetben megkapja a tranzakció során használt kártya tokenizált változatát.
3. A megkapott TOKEN-t és az ahhoz tartozó adatokat (mint pl. a token érvényességi ideje) a Kereskedőnek szükséges elmentenie, hogy a későbbi tranzakciókat ezek segítségével tudja kezdeményezni.

3.2.3.1 Fizetési folyamat

Tokenizált CIT-es fizetés esetén a Kártyabirtokos a Kereskedő weboldalán a kiválasztott termékeket a kosárba helyezi. A pénztárnál a fizetési lehetőségek megjelenítésekor a Kereskedő ellenőrzi, hogy a Kártyabirtokos rendelkezik e már tokenizált bankkártyával és amennyiben igen, azt maszkolt módon a kártya utolsó 4 számjegyét, a bankkártya típusát (Visa, Maestro, MasterCard) logójával együtt megjeleníti. A Kártyabirtokos kiválaszthatja a fizetés indításához használni kívánt kártyát és a kereskedő annak TOKEN-ével tudja a fizetést lefolytatni.

Amennyiben nincs rendelkezésre álló mentett kártya a Kereskedő rendszerében, úgy egy fizetői felületen történő tranzakció indítása szükséges. Sikeres fizetési tranzakció esetén a Bank tájékoztatja a Kereskedőt a tranzakció sikerességéről a Notification API segítségével. Az üzenet tartalmazza a bankkártya TOKEN-t, a maszkolt kártyaszámot és a tranzakció adatait. A Kereskedőnek a Notification API-n keresztül kapott kérésre jóváhagyó választ kell küldenie. Ezt követően a további fizetések JSON hívások segítségével történhetnek a Kereskedő és a Bank között, a fizetési felületre történő átirányításra csak a CVC / CVV limit meghaladása esetén van szükség, mely a [CVV kód megadása meghatározott összeghatár fölött CIT-es ismétlődő fizetés során](#) fejezetben kerül kifejtésre.

A fizetést követően a rendszer átirányítja a Kártyabirtokost a Kereskedő által Notify API válaszában megküldött forwardURL-re. Amennyiben ez valamilyen oknál fogva nem lehetséges, úgy a sikertelen URL címére.

A token érvényességi ideje válaszüzenetben megküldött UPCTokenExp dátuma. A tokenizált kártya törlésére a Kereskedőnek kell lehetőséget biztosítania a saját rendszerében.

3.2.3.2 Kommunikáció

FIGYELEM, JSON alapú fizetés vagy státusz lekérdezés során a Kereskedő Notification URL-jére semmilyen üzenet nem kerül megküldésre, mivel a kérésre azonnali választ kap.

3.2.3.3 Általános leírás

A kommunikáció JSON formátumon alapul. A kéréseket "Content-Type=application/json" header-el kell küldeni.

Minden kérésnek és válasznak az alábbi schemat kell követnie:

```
{  
  "header": "...base64 encoded data...",  
  "payload": "...base64 encoded data...",  
  "signature": "...generated signature..."  
}
```

3.2.3.3.1 Header

A "header" értéke minden esetben {"alg":"RS256"}, vagyis "eyJhbGciOiJSUzI1NiJ9" Base64 kódolással.

3.2.3.3.2 Payload

A "payload" mező értéke Base64 kódolással ellátott JSON objektum.

3.2.3.3.3 Signature

A "signature" az alábbiak alapján kerül generálásra:

1. a Base64 kódolású header, egy '.' (pont) karakter és a Base64 kódolású payload összefűzése,
2. majd a RS512 aláíró algoritmussal történő aláírása és annak a Base64es kódolása.

Felépítése:

```
signature = base64(sign_rs512(base64(header)+'.'+base64(payload),private_key))
```

(a „+” jel csak az összefűzés megjelenítése miatt szerepel a példában, az aláírásban az NEM szerepel, ellentétben a ‘.’-al, amit kötelező szerepeltetni benne)

Aláírás generálása OpenSSL-el:

```
openssl dgst -sha512 -sign .\private_key.pem .\datafile.txt > signature.bin
```

Aláírás generálása PHP nyelven:

```
$pkeyid = openssl_get_privatekey($priv_key);
openssl_sign($datafile, $signature, $pkeyid);
openssl_free_key($pkeyid);
```

3.2.3.4 Ismétlődő fizetés (MIT - Merchant-Initiated Transaction & CIT - Customer-Initiated Transaction)

A Kártyabirtokos által kezdeményezett (CIT-es) tranzakció során a Kártyabirtokos első, fizetési felületen történő vásárlása során az ahhoz használt kártya adatai tokenizálásra kerülnek. Ez biztosítja a továbbiakban azt, hogy a későbbi vásárlások során – a korábban tokenizált kártyát szeretné használni a Kártyabirtokos - nem szükséges megadnia a kártyaadatait. Így a tranzakció lebonyolítása gyorsabbá és zökkenőmentesebbé válik.

A Kereskedő által kezdeményezett (MIT) tranzakció az a fizetési forma, mely a Kereskedő és a Kártyabirtokos között létrejött megegyezés / szerződés alapján a Kártyabirtokos engedélyezi a Kereskedő számára, hogy Kártyabirtokos nevében és a jelenléte nélkül fizetést kezdeményezzen.

Például, ha a Kereskedő előfizetéses szolgáltatást nyújt és a Kártyabirtokos hozzájárult a szolgáltatás ellenértékének Kereskedő általi rendszeres és automatikus levonásához.

Ahhoz, hogy egy fizetést Kereskedő által kezdeményezett tranzakció kategóriába soroljuk,

- a Kártyabirtokos részéről beleegyezés szükséges a későbbi Kereskedő által indított fizetés kezdeményezéséhez;
- kizárólagosan a Kártyabirtokos által korábban jóváhagyott árukkal vagy szolgáltatásokkal kapcsolatos díjakra vonatkozóan indíthat fizetési kérelmet;

Ismétlődő fizetés engedélyezése érdekében kérjük, vegye fel a kapcsolatot a dedikált kapcsolattartójával.

Kérés paramétere:

Paraméter	JSON adattípus	Formátum	Kötelező	Leírás	Megjegyzés
MerchantID	string	AN(15)	igen	merchant ID	Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	string	AN(8)	igen	terminal ID	Egyedi azonosító, mely a Bank által kerül kiállításra

TotalAmount	number	N(1..12)	igen	Rendelés vásárlás összege /	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
Currency	number	N(3)	igen	Deviza kód	Egyedi azonosító, mely a Bank által kerül kiállításra. Értékei.
PurchaseTime	string	N(12..17)	igen	Megadható dátum és idő formátumok yyMMddHHmmss	<ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
OrderID	string	ANS(1..20)	igen	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.
PurchaseDesc	string	ANS(0..125)	nem	A vásárlás rövid leírása	A kereskedő részéről tetszőlegesen megadható leírás a vásárló tájékoztatása érdekében. A Kereskedői portálon, Payment Page-n, valamint a bizonylaton kerül megjelenítésre.

Token	string	ANS(32)	igen	Az első sikeres tranzakciót követően a payment gateway által megküldött TOKEN.	A Kártyabirtokos kártyaadatainak heyyətesítésére szolgál. Segítségével a Kereskedő a terhelést kezdeményezhet a kártyaadatok megadása és a kártya tulajdonosának bevonása nélkül.
RecurrentDesc	number	N(12)	igen	ismétlődő fizetés típusának azonosítója	CIT tranzakció esetén az értéke: 761000000000 Tokenizált Visa (4-es kezdetű PAN) kártyával történő tranzakció esetén ezen paraméter küldését mellőzni kell. MIT tranzakció esetén az értéke: 761040000000

Válasz paramétereit:

Paraméter	JSON adattípus	Formátum	Name	Leírás
MerchantID	string	AN(15)	Kereskedő egyedi azonosítója	Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	string	AN(8)	Terminál egyedi azonosítója	Egyedi azonosító, mely a Bank által kerül kiállításra

ApprovalCode	string	AN(1..6)	Bank authorization code	A Kibocsátó Bank által visszaadott autorizációs kód vagy jóváhagyó kód.
Rrn	string	N(12)	Reference Retrieval Number	A kártyás tranzakció egyedi azonosítója az ISO 8583 szabvány alapján.
TranCode	string	N(3)	Tranzakció kód	Minden kérés tartalmazza az annak sikerességére vagy sikertelenségére vonatkozó kódot. Értékei.
HostCode	string	N(3)	Az autorizációs host által adott tranzakció kód	További információs mező az engedélyben szereplő tranzakciós kód értékéből Értékei.
Comment	string	ANS(0..64)	Comment	

Példa hívásra:

```
{
  "MerchantID":"1111111",
  "TerminalID":"E222222",
  "OrderID":"RENDELES_123",
  "UPCToken":"76E7F59A0ADFEF9A330FC0D33B56DC03",
  "TotalAmount":"10000",
  "Currency":"348",
  "PurchaseTime":"230329113000",
  "PurchaseDesc":" MIT / CIT transaction",
  "RecurrentDesc":"761000000000"
}
```

Példa válaszra:

```
{
  "MerchantID":"1111111",
  "TerminalID":"E222222",
  "ApprovalCode":"341186",
  "Rrn":"234814642291",
  "HostCode":"000",
  "TranCode":"000",
  "Comment":"Approved"
}
```

3.2.3.5 CVV kód megadása meghatározott összeghatár fölött CIT-es ismétlődő fizetés során

FONTOS, hogy CVV2 megadása nélküli fizetésre kizárólag a Bank által meghatározott összeghatárig van lehetőség.

Amennyiben a vásárlás összege átlépné a meghatározott maximális összeget, úgy a Kereskedőnek fizetői felületre szükséges átirányítania a Kártyabirtokost. JSON API-n keresztül történő fizetés során az összeghatárt meghaladva, vagy pedig átlépbe „{“TranCode”:“414”,“Comment”:“Tran is prohibited. CVC required”}” hibaüzenetet kap a kereskedő.

Ilyen esetben a [Payment Page-en történő fizetés indítása](#) fejezetben leírtakhoz hasonlóan egy HTML POST hívás összeállítása szükséges, azonban az itt összeállított hívásnak már tartalmaznia kell a kártyabirtokos korábbi vásárlása során visszakapott TOKEN-ét, amelynek köszönhetően a fizetői felületre történő navigációt követően a kártyabirtokosnak már csak a kártyájához tartozó CVV számot kell megadnia.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/rbhu/enter	Teszt payment gateway cím
POST	https://secure-ecom.raiffeisen.hu/rbhu/enter	Éles payment gateway cím

Kérés paramétere:

Paraméter	Kötelező	Formátum	Leírás	Megjegyzés
Version	igen	N(1)	Interface verziója	Kommunikációs protokoll verziószáma. Jelenlegi értéke '1'. Ezen paraméter szolgál referenciálul a gateway számára az input feldolgozásához.
MerchantID	igen	AN(15)	Kereskedő azonosítója egyedi	Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	igen	AN(8)	Terminál azonosítója egyedi	Egyedi azonosító, mely a Bank által kerül kiállításra

TotalAmount	igen	N(1..12)	Rendelés / vásárlás összege	Megadása százados jegy pontossággal szükséges. Pl.: 1000 Forint esetén 100000 megadása szükséges.
Currency	igen	N(3) 348	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.
PurchaseTime	igen	N(12..17)	Megadható dátum és idő formátumok yyMMddHHmmss	<ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
Local	igen	A(2)	Interface nyelve (hu, de, en)	A fizetési felület nyelve. (jelen esetben magyar) Értékei.
OrderID	igen	ANS(1..20)	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.
PurchaseDesc	nem	ANS(0..125)	A vásárlás rövid leírása	A kereskedő részéről tetszőlegesen megadható leírás a vásárló tájékoztatása érdekében. A Kereskedői portálon, Payment Page-n, valamint a bizonylaton kerül megjelenítésre.
Signature	igen	SHA512withRSA	Aláírás értéke	A paraméter karakterszáma függ a választott generálási metódustól

Ref3	igen	ANS(0..150)	Egyedi rendelésazonosító	<p>Megadható jegyszám vagy egyéb azonosító, mint teljes név, telefonszám, stb.</p> <p>Amennyiben nem szeretne külön azonosítót használni, úgy ennek értékeként az OrderID megadása szükséges.</p> <p>Ezen érték kerül megjelenítésre az analitikában.</p>
UPCToken	igen	ANS(32)	Az első sikeres tranzakciót követően a payment gateway által megküldött TOKEN.	<p>A Kártyabirtokos kártyaadatainak helyettesítésére szolgál. Segítségével a Kereskedő terhelést kezdeményezhet a kártyaadatok megadása és a kártya tulajdonosának bevonása nélkül.</p>

A paraméterek átadása HTTPS / POST metódus segítségével történik egy előre definiált HTML formátumban a Payment Page részére, ahol a Vevő megadhatja a kártya adatait.

Adatátadásra példa:

```
<form action="https://ecg.test.upc.ua/rbhu/enter" method="POST">
  <input name="Version" type="hidden" value="1" />
  <input name="MerchantID" type="hidden" value="1111111" />
  <input name="TerminalID" type="hidden" value="E222222" />
  <input name="TotalAmount" type="hidden" value="100000" />
  <input name="Currency" type="hidden" value="348" />
  <input name="Local" type="hidden" value="en" />
  <input name="PurchaseTime" type="hidden" value="230329113000"/>
  <input name="OrderID" type="hidden" value="RENDELES_123" />
  <input name="Ref3" type="hidden" value="812812812812" />
  <input name="UPCToken" type="hidden" value=" F75F13380BC898EFC" />
  <input name="PurchaseDesc" type="hidden" value="CVV / CVC2 enter" />
  <input name="Signature" type="hidden" value=""/>
  <input type="submit"/>
</form>
```

3.2.3.6 Kártya tokenizálása 0 Forinttal (Account verification) – MIT-es ismétlődő fizetéshez

Lehetőség van a kártyaadatok 0 Ft-os összeggel történő ellenőrzésére, illetve tokenizálására, amennyiben engedélyezésre és beállításra került a Bank részéről. Külön AV-re dedikált kereskedő (MID) és terminál azonosító (TID) segítségével történhet meg a kártyaadatok tokenizálása egy lépésben, terhelés nélkül, melyet követően a token a Kereskedő részére NOTIFY URL-en keresztül kerül megküldésre.

A kártya token használata kizárólag a MIT-es tranzakciókra dedikált kereskedő (MID) és terminálon (TID) azonosítóval történhet.

Terminál regisztrációja és ismétlődő fizetés engedélyezése érdekében kérjük, vegye fel a kapcsolatot a dedikált kapcsolattartójával.

A Kereskedő weboldaláról történő Payment Page meghívása során kötelező meghatározott paraméterek átadása. Ezen paramétereket és azok leírását az alább található „Kérés paramétereit” táblázat tartalmazza.

Szolgáltatás végpontok:

HTTP method	URL	Leírás
POST	https://ecg.test.upc.ua/rbhu/enter	Teszt payment gateway cím
POST	https://secure-ecom.raiffeisen.hu/rbhu/enter	Éles payment gateway cím

Kérés paramétereit:

Paraméter	Kötelező	Formátum	Leírás	Megjegyzés
Version	igen	N(1)	Interface verziója	Kommunikációs protokoll verziószáma. Jelenlegi értéke '1'. Ezen paraméter szolgál referenciául a gateway számára az input feldolgozásához.
MerchantID	igen	AN(15)	Kereskedő azonosítója	egyedi Egyedi azonosító, mely a Bank által kerül kiállításra
TerminalID	igen	AN(8)	Terminál azonosítója	egyedi Egyedi azonosító, mely a Bank által kerül kiállításra

TotalAmount	igen	N(1..12)	Rendelés / vásárlás összege	AV esetén 000, azaz 0 Forint..
Currency	igen	N(3) 348	Deviza kód	A Bank és a Kereskedő között megkötött szerződésbe foglalt devizanem. Jelen esetben Forint, vagyis 348. Értékei.
PurchaseTime	igen	N(12..17)	Megadható dátum és idő formátumok yyMMddHHmmss	<ul style="list-style-type: none"> • yy - év • MM - hónap • d - nap • HH - óra (0-23) • mm - perc • ss - másodperc
Local	igen	A(2)	Interface nyelve (hu, de, en)	A fizetési felület nyelve. (jelen esetben magyar) Értékei.
OrderID	igen	ANS(1..20)	Rendelés azonosítója maximum 20 byte	Minden egyes fizetésnél egyedinek kell lennie.
PurchaseDesc	nem	ANS(0..125)	A vásárlás rövid leírása	A kereskedő részéről tetszőlegesen megadható leírás a vásárló tájékoztatása érdekében. A Kereskedői portálon, Payment Page-n, valamint a bizonylaton kerül megjelenítésre.
Signature	igen	SHA512withRSA	Aláírás értéke	A paraméter karakterszáma függ a választott generálási metódustól

A kártya regisztrációja során a TotalAmount 0 forint lesz.

A paraméterek átadása HTTPS / POST metódot segítségével történik egy előre definiált HTML formátumban a Payment Page részére, ahol a Vevő megadhatja a kártya adatait.

Adatátadásra példa:

```
<form action="https://ecg.test.upc.ua/rbhu/enter" method="POST">
  <input name="Version" type="hidden" value="1" />
  <input name="MerchantID" type="hidden" value="1111111" />
  <input name="TerminalID" type="hidden" value="E1111111" />
  <input name="TotalAmount" type="hidden" value="000" />
  <input name="Currency" type="hidden" value="348" />
  <input name="Local" type="hidden" value="en" />
  <input name="PurchaseTime" type="hidden" value="230329113000"/>
  <input name="OrderID" type="hidden" value="RENDELES_123" />
  <input name="PurchaseDesc" type="hidden" value="Card registration" />
  <input name="Signature" type="hidden" value="" />
  <input type="submit"/>
</form>
```

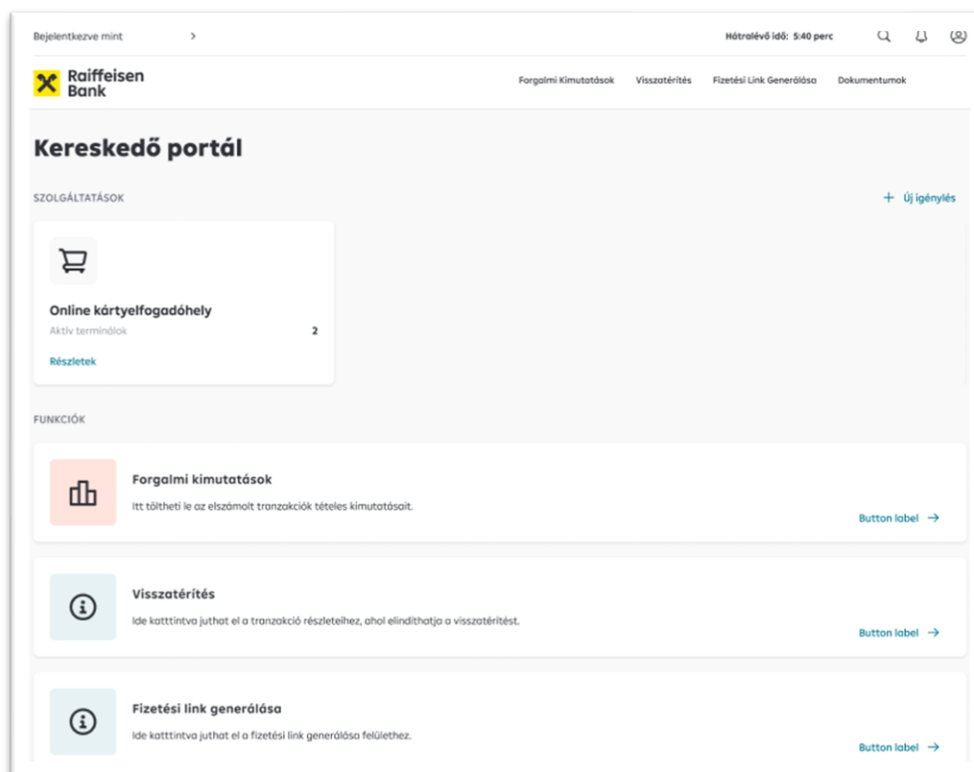
A regisztráció adatai a Kereskedő Notification URL-re kerülnek megküldésre, mely tartalmazza a további tranzakciókhoz használandó TOKEN-t is. A TOKEN kizárólag a Kereskedő MIT-es terminálján használható.

4 Kereskedő portál szolgáltatásainak ismertetése

4.1 Alap ismertetés

A Raiffeisen Bank Kereskedő fizetési megoldásait, köztük a VPOS szolgáltatást a saját fejlesztésű Kereskedő Portálon keresztül van lehetőség igényelni. Aktivált VPOS szolgáltatást követően ezen a felületen van lehetőség az elszámolt tranzakciókról történő tételes forgalmi kimutatások elérésére. A felület a www.raiffeisen.hu oldalról, vagy közvetlenül is elérhető

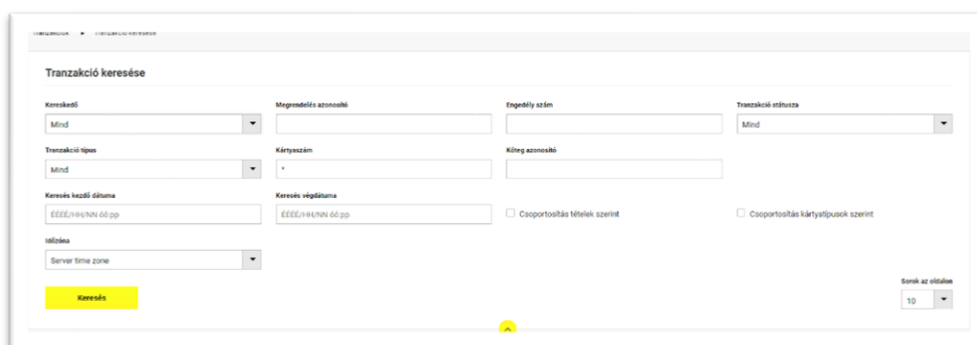
A Kereskedő Portálon az alábbi tranzakció típusok kezdeményezhetőek:



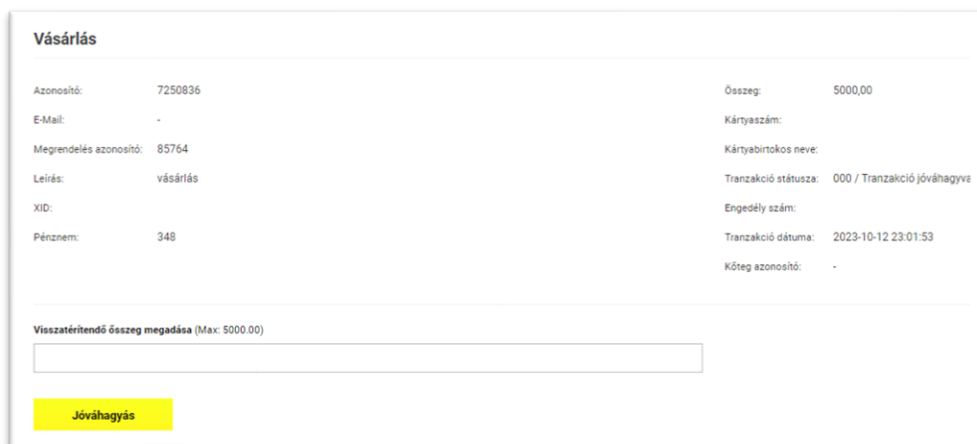
4.2 Visszatérítés

A Kereskedő - Banki engedélyt követően - az alábbi menüben tudja kezdeményezni a sikeres tranzakció részleges vagy teljes összegű visszatérítését. Napzárást megelőzően csak teljes összegű visszatérítésre, sztoróra van lehetőség. A Bank fenntartja a jogot a részleges visszatérítések maximum darabszámának a meghatározására. A rész összegek viszont nem haladhatják meg az eredeti vásárlási összeget, tehát maximum csak 100% téríthető vissza.

Első lépésben szükséges a visszatérítendő tranzakció kikeresése:



A visszatérítendő tranzakciót megnyitva, az alábbi képernyőn van lehetőség a visszatérítés indítására. A visszatérítendő összeget tizedesvesszővel, százados értékig kell megadni. Ami 1000 Forint esetén 1000.00 értéket jelent.



4.3 Előengedélyezés és annak befejezése

Ezt a tranzakció típust csak speciális tevékenységek esetén engedélyezi a Bank. Ezen kétlépcsős fizetési mód esetén először foglalásra kerül a Kártyabirtokos számláján a vásárlás összegével. Második lépésként a Kereskedőnek a Kereskedő Portál használatával lehetősége van a foglalás teljes összegű törlésére, vagy befejezésére. A hatályos kártyatársasági szabályok értelmében a lezárás során megadott összeg - Mastercard típusú kártyák esetén - nem lehet magasabb, mint az előengedélyezés összege. Visa kártyák esetén a lezárás során megadott összeg maximum +15%-kal lehet magasabb az eredeti, előengedélyezett összegnél. Az összeget tizedesvesszővel, százados értékig kell megadni. Ami 1000 Forint esetén 1000.00 értéket jelent. Egy foglalás / előengedélyezés befejezésére maximum 30 napig áll rendelkezésre, azt követően a Kártyabirtokos számláján a terhelés feloldásra kerül.

Az előengedélyezés indításáról az Előengedélyezés / Előengedélyezés befejezése pontban olvashat részletesen.

Az előengedélyezés befejezéséhez az előző pontban részletezett módon szükséges a tranzakciót kiválasztani, majd az alábbi képernyőn van lehetőség a tranzakció törlésére, vagy véglegesítésére.

Előengedélyezés

Azonosító:	7250835	Összeg:	10000,00
E-Mail:	-	Kártyaszám:	
Megrendelés azonosító:	96301	Kártyabirtokos neve:	
Leírás:	Előengedélyezés	Tranzakció státusza:	000 / Tranzakció jóváhagyva
XID:		Engedély szám:	888746
Pénznem:	348	Tranzakció dátuma:	2023-10-12 22:59:25
		Köteg azonosító:	-

Visszatérítendő összeg megadása (Máx: 10000.00)

Jóváhagyás

Előengedélyezett tranzakció befejezése

Információ:

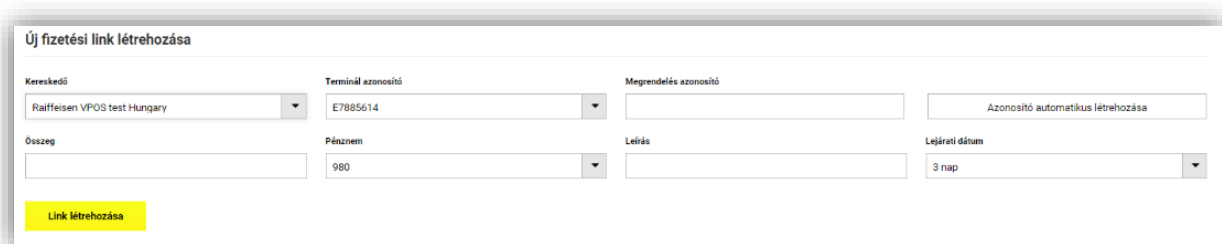
- A megengedett legnagyobb különbség - MC 0%, VISA +15%
- 30 napig lehet előengedélyezett tranzakciót lezárni

Jóváhagyás

4.4 Fizetési link generálása

Azon Kereskedők számára, akik a fizetési kötelezettség felmerüléséről a Kártyabirtokost nem klasszikus webáruházban (vásárlói kosár összeállításával), hanem egyéb csatornán, jellemzően e-mail-ben eljuttatott levél vagy számla megküldésével tájékoztatja, és az összeg bankkártyával történő kiegyenlítését a link-re kattintva kezdeményezheti a kártyabirtokos. Ebben az esetben a Kártyabirtokos a fizetési linkre kattintva átirányításra kerül a banki fizetőoldalra, ahol teljesítheti az adott fizetést.


Ilyen fizetési linket az alábbi menüben generálhat. Az összeget tizedes vesszővel, százados értékig kell megadni. Ami 1 000 Forint esetén 1000.00 értéket jelent.

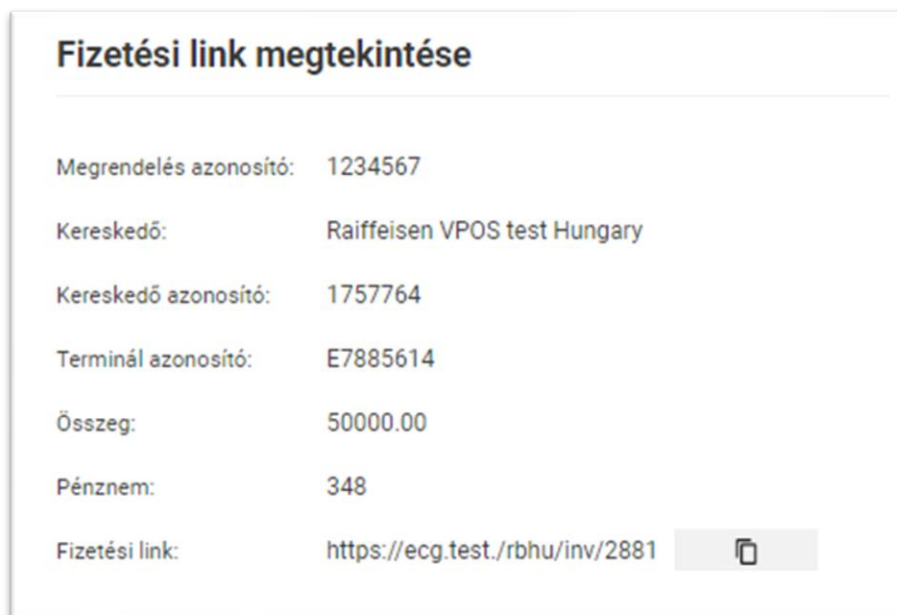


Új fizetési link létrehozása

Kereskedő	Terminál azonosító	Megrendelés azonosító	Azonosító automatikus létrehozása
Raiffeisen VPOS test Hungary	E7885614		
Összeg	Pénznem	Leírás	Lejárat dátum
	980		3 nap

Link létrehozása

A generálást követően lehetőség van az elkészült egyedi fizetési link kimásolására ezen gomb megnyomásával: 



Fizetési link megtekintése

Megrendelés azonosító:	1234567
Kereskedő:	Raiffeisen VPOS test Hungary
Kereskedő azonosító:	1757764
Terminál azonosító:	E7885614
Összeg:	50000.00
Pénznem:	348
Fizetési link:	https://ecg.test./rbhu/inv/2881 

Lehetőség van a korábban elkészített linkek visszakeresésére is:

Fizetési link keresése

Kereskedő	Megrendelés azonosító	Fizetési link státusza
<input type="text" value="Raiffeisen VPOS test Hungary"/>	<input type="text"/>	<input type="text" value="Létrehozás dátuma"/>
Keresés kezdő dátuma	Keresés végdátuma	
<input type="text" value="ÉÉÉÉ/HH/NN óó:pp"/>	<input type="text" value="ÉÉÉÉ/HH/NN óó:pp"/>	
<input type="button" value="Keresés"/>		

5 Integrációs tesztelés

A fejezet a Kereskedő részéről, a fejlesztés során végrehajtandó tesztesetek leírását, valamint a teszteléshez használható TESZT kártyák adatait tartalmazza.

5.1 Tesztesetek

A Bank az alábbi táblázatban „Kötelezően implementálandó tranzakciótípusok” jelöléssel ellátott teszteseteket várja el a szolgáltatás élesbe állítása előtt. Amennyiben a Kereskedő engedélyt kért és kapott az „Opcionálisan igényelhető” jelölésű tranzakciótípusok bármelyikére, akkor azon tesztesetek elvégzése is kötelező.

	Kötelezően implementálandó tranzakciótípusok	Opcionálisan igényelhető tranzakciótípusok
Normál fizetés+sztorató	x	
Mentett kártyás fizetés (CIT)		x
Kereskedő által indított ismétlődő fizetés (MIT)		x
Account verification		x
Visszatérítés (Refund)		x
Előengedélyezés / Előengedélyezés befejezése		x
Fizetési link		x

5.1.1 Kötelezően implementálandó tranzakciótípusok

5.1.1.1 Normál fizetés

Az a fizetési forma, amely során a vásárlás végén a pénztárnál a Kártyabirtokos a Bank által biztosított VPOS segítségével egyenlíti ki a vásárlás összegét.

1. a Kereskedő weboldalán a megvásárolni kívánt termék(ek), vagy szolgáltatás(ok) kosárba helyezése;
2. fizetés kezdeményezése;
 - 2.1. az [Payment Page-en történő fizetés indítása](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez szükséges link összeállítása;
 - 2.2. a fizetési felület meghívása a beállított paraméterekkel;
3. a megjelenő fizetési felületen a kártyaadatok megadása;
4. fizetés sikerességének vagy sikertelenségének ellenőrzése;
 - 4.1. a [Notification API](#) megküldött információk segítségével;
 - 4.2. státuszlekérdezés segítségével;
 - 4.3. tranzakció eredményének a webáruházban történő megjelenítésével

5.1.1.2 Sztornó

1. előfeltétele egy már előzőleg sikeresen lebonyolított fizetés;
2. sztornó kezdeményezése
 - 2.1. a [Sztornó \(reversal\) tranzakció](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez szükséges link összeállítása RefoundAmount és RRN értékekkel;
3. a tranzakció sikerességének vagy sikertelenségének ellenőrzése;
 - 3.1. a html válaszban kapott TranCode érték alapján;
 - 3.2. Kereskedő Portál-ban a tranzakciók menüpontban;

5.1.2 Opcionálisan igényelhető tranzakciótípusok

5.1.2.1 Normál fizetés kártya regisztrációval

Az a fizetési forma, amely során a vásárlás végén a pénztárnál a Kártyabirtokos a Bank által biztosított VPOS segítségével úgy egyenlíti ki a vásárlás összegét, hogy a kártyáját tokenizálja, ezáltal lehetővé téve azt, hogy a későbbiekben a kártya adatainak megadására ne legyen szükség.

1. a Kereskedő weboldalán a megvásárolni kívánt termék(ek), vagy szolgáltatás(ok) kosárba helyezése;
2. fizetés kezdeményezése
 - 2.1. az [Payment Page-en történő fizetés indítása](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez szükséges link összeállítása;
 - 2.2. a fizetési felület meghívása a beállított paraméterekkel;
3. a megjelenő fizetési felületen a kártyaadatok megadása és a „Tokenizálja a kártyát” checkbox bejelölése;
4. fizetés sikerességének vagy sikertelenségének ellenőrzése;
 - 4.1. a [Notification API](#) megküldött információk segítségével. Az üzenetnek tartalmaznia kell a tranzakció során létrejött TOKEN-t.
 - 4.2. tranzakció eredményének a webáruházban történő megjelenítésével

5.1.2.2 Mentett kártyás fizetés (CIT)

A Kártyabirtokosnak - az adott Kereskedőnél a [Normál fizetés kártya regisztrációval](#) fejezetben leírt vásárlását követően – lehetősége van a már elmentett kártyájával újabb fizetést lebonyolítani anélkül, hogy a kártyadatait újból meg kelljen adnia.

1. a Kereskedő weboldalán a megvásárolni kívánt termék(ek), vagy szolgáltatás(ok) kosárba helyezése;
2. fizetés kezdeményezése
 - 2.1. a vásárláshoz használni kívánt elmentett kártyát a Kártyabirtokos kiválasztja;

- 2.2. a [JSON alapú fizetés](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez JSON összeállítása és a megfelelő végpontra történő elküldése;
3. a fizetés sikerességének vagy sikertelenségének ellenőrzése;
 - 3.1. a Banktól kapott szinkron válaszban található információk segítségével.
 - 3.2. tranzakció eredményének a webáruházban történő megjelenítésével

5.1.2.3 Ismétlődő fizetés - MIT

Például rendszeres vagy előfizetéses szolgáltatás esetében a Kereskedőnek - a Kártyabirtokossal történő szerződéskötést vagy egyezséget és a Kártyabirtokos kártyájának regisztrációját követően - lehetősége van saját maga által, a Kártyabirtokos beavatkozása nélkül fizetési tranzakció indítására.

1. előfeltétele a kártyaregisztráció megléte;
2. az [Ismétlődő fizetés \(MIT - Merchant-Initiated Transaction & CIT - Customer-Initiated Transaction\)](#) fejezetben leírtak alapján;
3. a tranzakció ellenőrzése a Banktól kapott szinkron válaszségítségével;

5.1.2.4 Visszatérítés

1. előfeltétele egy már előzőleg sikeresen lebonyolított fizetés;
2. visszatérítéskezdeményezése
 - 2.1. a [Visszatérítés \(Refund\) tranzakció](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez szükséges link összeállítása RefoundAmount és RRN értékekkel;
3. a tranzakció sikerességének vagy sikertelenségének ellenőrzése;
 - 3.1. a html válaszban kapott TranCode érték alapján;
 - 3.2. Kereskedő Portál-ban a tranzakciók menüpontban;

5.1.2.5 Előengedélyezés / Előengedélyezés befejezése

1. a Kereskedő weboldalán a megvásárolni kívánt termék(ek), vagy szolgáltatás(ok) kosárba helyezése;
2. előengedélyezéssel indított fizetés kezdeményezése
 - 2.1. az [Előengedélyezés / Előengedélyezés befejezése](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez szükséges link összeállítása;
 - 2.2. a fizetési felület meghívása a beállított paraméterekkel;
3. a megjelenő fizetési felületen a kártyaadatok megadása;
4. fizetés sikerességének vagy sikertelenségének ellenőrzése;
 - 4.1. a [Notification API](#) megküldött információk segítségével;
 - 4.2. tranzakció eredményének a webáruházban történő megjelenítésével
 - 4.3. a Kereskedő Portál-ban az Előengedélyezett tranzakció meglétének ellenőrzése;
5. Kereskedő Portál-ban Előengedélyezés befejezése teljes, vagy részösszeggel a [Előengedélyezés és annak befejezése](#) fejezetben leírtak alapján.

5.1.3 Sikertelen tranzakció feldolgozása

1. a Kereskedő weboldalán a megvásárolni kívánt termék(ek), vagy szolgáltatás(ok) kosárba helyezése;
2. fizetés kezdeményezése;
 - 2.1. az [Payment page segítségével történő fizetés](#) fejezetben leírtak alapján a fizetés kezdeményezéséhez szükséges link összeállítása;
 - 2.2. a fizetési felület meghívása a beállított paraméterekkel;
3. a megjelenő fizetési felületen olyan kártyaadatok megadása mely TranCode-ja nem '000';
4. fizetés sikertelenségének ellenőrzése;
 - 4.1. a [Notification API](#) megküldött információk segítségével;
 - 4.2. tranzakció eredményének a webáruházban történő megjelenítésével

5.1.4 JSON API – tranzakció állapotának lekérdezése

1. Előfeltétele egy már előzőleg lebonyolított sikeres vagy sikertelen tranzakció.
2. A JSON alapú lekérdezés [Tranzakció állapotának lekérdezése](#) fejezetben található leírás alapján lehetséges.

5.2 Teszteléshez használandó kártyaadatok

Hibakód	Leírás	Kártyaszám
		
000	Sikeres tranzakció	4999999999990011
105	Tranzakciót a Kibocsátó Bank elutasította	4999999999990029
		
000	Sikeres tranzakció	5559490000000007
105	Tranzakciót a Kibocsátó Bank elutasította	5559490000000106
		
000	Sikeres tranzakció	6258148147036936

- kártyán szereplő név -> tetszőleges;
- kártya lejáratási dátuma -> tetszőleges, de a tesztelés időpontjától későbbi;
- CVV2 -> tetszőleges 3 szám;

6 Függelékjegyzék

6.1 Formátum kódok

Kód	Megnevezés	Leírás
N	Numerikus	Csak számokból állhat.
AN	Alfanumerikus	Csak számokból és karakterekből állhat.
ANS	Alfanumerikus / Speciális karakterek	Számokból, karakterekből és speciális karakterekből állhat.

6.2 TranCode értékei

A Kereskedő által a Bank irányába indított minden egyes kérésre kapott válaszban található TranCode értékeit az alábbi lista tartalmazza. Ez a kód mutatja a kérés feldolgozásának sikerességét (000), vagy a bármilyen okból fellépő hiba / probléma beazonosításához elengedhetetlen kódot.

TranCode	Description	Leírás
000	Transaction successful	A tranzakció jóváhagyva
002	Approved partial authorization	Megerősített részleges engedély
101	Invalid card parameters	A megadott kártyaparaméterek érvénytelenek
105	Not approved by the issuer	A kibocsátó bank elutasította
108	Lost / stolen card	Elveszett / elloptott kártya
111	Non-existent card	Nem létező kártya
116	Insufficient funds	Fedezethiány
130	Limit is exceeded	Limit túllépése
131	Additional customer authentication required	További ügyfélhitelesítés szükséges
290	Issuer unavailable	A kibocsátó nem érhető el
291	Technical / communication problems	Technikai / kommunikációs probléma
401	Wrong format	Érvénytelen paraméterek
402	Invalid acquirer / seller details	Érvénytelen elfogadói / kereskedői adatok
403	Component communication failure	Komponens kommunikációs hiba
404	Authentication error	Engedélyezési hiba
405	Signature is invalid	Alírási hiba
406	Transaction quota exceeded	Túllépte a tranzakciós kvótát

407	Seller is not active	A kereskedő nem aktív
408	Transaction not found	A tranzakció nem található
409	Too many transactions detected	Túl sok tranzakciót rögzítettek
410	Order paid (repeat possible)	A rendelést már kifizették
411	Order request time outdated	A rendelési kérelem ideje elavult
412	Replay order condition	Megrendelés ismételt végrehajtásának állapota
413	Unknown card type	Ismeretlen kártyatípus
414	CVC required	CVC szükséges
415	Installment plan was not found	Részletfizetési terv nem található
420	The total number of successful transactions per day is limited	A napi sikeres tranzakciók száma korlátozott
421	Limit transaction amount (without full 3-D Secure authentication)	Tranzakció összegének korlátozása (teljes 3-D Secure hitelesítés nélkül)
430	Transaction denied by gateway	Az átjáró megtagadta a tranzakciót (A fizetési művelet tilos)
431	Attempt 3D-Secure is not accepted	A 3D-Secure kísérletet nem fogadják el (A fizetési művelet tilos)
432	Card in the stop list	A Kártya tiltólistán szerepel (A fizetési művelet tilos)
433	The number of transactions has exceeded the limit	A kártyával végrehajtott tranzakciók száma túllépte a korlátot
434	The store does not accept cards from the country	A kereskedő csak a hazai bankok által kibocsátott kártyákat fogadja el
435	Client IP address in the stop list	Az ügyfél IP-címe a tiltólistán (A fizetési művelet tilos)
436	The amount of transactions has exceeded the limit	A kártyával végrehajtott tranzakciók teljes összege meghaladta a korlátot
437	The limit for entering the number of cards has been exceeded	Túllépte a kártya számának megadására vonatkozó korlátot
438	Invalid currency code	Érvénytelen valutakód
439	Time limit from request to authorization exceeded	A kéréstől az engedélyezésig eltelt idő túllépte a határt
440	Authorization time limit exceeded	Az engedélyezési időkorlát túllépése
441	MPI interoperability problem	MPI interoperabilitási probléma (3D-biztonságos tranzakciófeldolgozási probléma)

442	ACS communication problem	ACS kommunikációs probléma (3D-biztonságos tranzakciófeldolgozási probléma)
443	ActiveServer communication problem	ActiveServer kommunikációs probléma
444	Parameter NameOnCard is invalid or empty	A NameOnCard paraméter érvénytelen vagy üres
450	Recurring payments are prohibited	Az ismétlődő fizetések tiltottak (A fizetési művelet tilos)
451	MPI service not enabled	Az MPI szolgáltatás nincs engedélyezve
452	Payment from card to card is not included	KÁRTYA-KÁRTYA Fizetési szolgáltatás nincs engedélyezve
460	Token service not included	A token szolgáltatás nincs engedélyezve
501	Canceled by user	Felhasználó által törölt tranzakció
502	The web session has expired	A webes munkamenet lejárt
503	The transaction was canceled by the seller	A kereskedő törölte a fizetési műveletet
504	Transaction was canceled by the cancellation gateway	A tranzakciót a törlési átjáró törölte
505	Incorrect sequence of operations	Helytelen műveletsorozat
506	Pre-authorization has expired	Az előengedélyezés lejárt
507	Pre-authorized transaction already processed with payment	Az előengedélyezett tranzakciót már feldolgozták a fizetéssel együtt
508	Invalid amount to pay for a pre-authorized transaction	Érvénytelen összeg az előre engedélyezett tranzakció kifizetéséhez
509	Not able to trace back to original transaction	Nem lehet visszavezetni az eredeti tranzakcióra
510	Refund is expired	A visszatérítés lejárt
511	Transaction canceled by settlement action	A tranzakciót elszámolási intézkedéssel törölték
512	Repeated cancellation or refund	Ismételt törlés vagy visszatérítés
513	Invoice expiration date is finish	A számla lejárat dátuma lejárt
601	Not completed	A tranzakció feldolgozás alatt áll
602	Waiting for confirmation of payment	A fizetés visszaigazolására vár
603	Wait customer auth required	Várakozás, ügyfélengedélyre van szükség

701	Unable to process transaction/declined by the authorization	Nem lehet feldolgozni a tranzakciót / elutasított engedélyezés
902	Unable to process transaction	Nem lehet feldolgozni a tranzakciót
909	Unable to process transaction	Nem lehet feldolgozni a tranzakciót
999	Transaction in progress .. (intermediate status, you must send a request for payment status before the final status.)	Tranzakció folyamatban .. (köztes státusz, a végső állapot előtt fizetési státuszra vonatkozó kérelmet kell küldenie)

6.3 HostCode értékei

A HostCode a szolgáltató által adott ISO8583 válasz kód. Ennek a kódnak a segítségével jobban beazonosítható és kielemezhető miért lett a tranzakció elutasítva, ezért kiemelten fontos ennek letárolása a TranCode mellett. Ez a kód kizárólag a szolgáltatótól kapott válasz üzenetben található meg.

HostCode	Description	Leírás
000	Successful transaction	Sikeres tranzakció
001	Approve with Identification	Megerősített részleges engedély
002	Approved For Partial Amount	Részösszegre jóváhagyva
010	Additional customer authentication required (chip and PIN or SCA)	További ügyfélhitelesítés szükséges (chip és PIN vagy SCA)
011	PIN required	PIN-kód szükséges
100	Do not honor transaction	Tranzakció nem teljesíthető
101	Expired Card	Lejárt kártya
102	Fraud is suspected	Csalás gyanúja merül fel
103	Call Issuer.	Vegye fel a kapcsolatot a Kibocsátóval
104	Card is restricted	A kártya korlátozva van
106	Excessive pin failures	Túl sok pin hiba
107	Call Card Issuer – Used only for signature-based transactions.	Hívja a kártyakibocsátót - Csak aláíráson alapuló tranzakciók esetén használatos
108	Call issuer, special condition	Hívja a kibocsátót, különleges feltétel
109	Invalid Merchant ID	Érvénytelen kereskedői azonosító
110	Cannot process amount	Nem lehet feldolgozni az összeget
111	Invalid account – retry	Érvénytelen számla - újbóli próbálkozás

114	Invalid account or Failed Currency Conversion	Érvénytelen számla vagy Sikertelen valutaváltás
116	Insufficient funds - retry	Nincs elegendő fedezet - újbóli próbálkozás
117	Incorrect Pin	Hibás PIN-kód
119	Transaction not permitted by law	Törvény által nem engedélyezett tranzakció
120	Not permitted or EMV Error	Nem engedélyezett vagy EMV hiba
121	Withdrawal limit exceeded - retry	Készpénzfelvételi limit túllépése - újbóli próbálkozás
122	Cannot process transaction - Security violation	Tranzakciót nem lehet feldolgozni - biztonsági szabálysértés
123	Limit reached for total number of transactions In cycle	A tranzakciók teljes számának korlátja elérve a ciklusban
124	Transaction not permitted by law.	Törvény által nem engedélyezett tranzakció
125	Bad Issue/Expiration Date	Rossz kibocsátási/lejárati dátum
126	Pin processing error (PVV Check Failed or PIN Response Code Undefined)	PIN-kód feldolgozási hiba (PVV-ellenőrzés sikertelen vagy PIN-válaszkód nem meghatározott)
127	Pin processing error	PIN-kód feldolgozási hiba
128	Pin processing error	PIN-kód feldolgozási hiba
129	Incorrect CVV or CVV2 code	Helytelen CVV vagy CVV2 kód
130	Cash-in limit exceeded	Befizetési limit túllépése
200	Invalid card	Érvénytelen kártya
201	Card expired	A kártya lejárt
202	Invalid card	Érvénytelen kártya
204	Account restricted	Bankszámla korlátozás
205	Call security	Biztonsági hívás
206	Invalid Pin	Érvénytelen PIN-kód
207	Capture, Special Condition	Lekérdezés, különleges feltétel
208	Lost Card	Elveszett kártya
209	Stolen Card	Lopott kártya
306	File Update Error	Fájlfrissítési hiba
800	This code is used only in the Network Management Response message (1814) for indicating "Successful Sign On/Off".	Ezt a kódot csak a hálózatirányítási válaszüzenetben (1814) használják a "Sikeres be-/kikapcsolás" jelzésére
902	Invalid transaction - retry	Érvénytelen tranzakció - újbóli próbálkozás

903	Transaction needs to be entered again	A tranzakciót újra be kell adni
904	The message received was not within standards	A kapott üzenet nem felelt meg a szabványoknak
907	The Issuer is Inoperative	A kibocsátó nem elérhető
908	Issuing institution is unknown or invalid	A kibocsátó intézmény ismeretlen vagy érvénytelen
909	System malfunction	Rendszerhiba
910	The Issuer is Inoperative	A kibocsátó nem elérhető
911	UPC Authorization System has no knowledge of attempt to either authorize or deny the transaction.	A UPC engedélyező rendszernek nincs tudomása a tranzakció engedélyezésére vagy elutasítására tett kísérletről
912	Time out waiting for response	A válaszra várakozás ideje lejárt
913	Duplicate transaction received	Duplikált tranzakció érkezett
914	Could not find the original transaction	Nem található az eredeti tranzakció
915	Amount being reversed is greater than original, or no amount being reversed.	A visszavont összeg nagyobb, mint az eredeti, vagy nincs visszavont összeg
920	Pin processing error/Unable To Verify PIN	PIN-kód feldolgozási hiba/nem sikerült ellenőrizni a PIN-kódot
921	PIN not changed	A PIN kód nem változott
922	Unacceptable PIN—Transaction Declined—Retry	Elfogadhatatlan PIN-ügylet elutasítva-visszatérítés
923	Request in progress	Folyamatban lévő kérés
936	Payment Scheme does not response	A fizetési rendszer nem válaszol
940	Pick up card, special condition	Kártya felvétele, különleges feltétel

6.4 Deviza kódok

Az ISO 4217 szabvány a valuták és az egyes pénznemek jelölésének 3-karakteres kódjait tartalmazza. A lenti táblázatban látható mely pénzben melyik országban használt.

Pénznem	Betű kódja	Deviza kód	Tizedesjegy
Forint	HUF	348	2
Euró	EUR	978	2
US Dollár	USD	840	2

6.5 Interface nyelvi (helyi) kódok

ISO 639-1 alpha-2 standardnak megfelelő nyelvi kódok az alábbiak lehetnek.

Kód	Nyelv
hu	Magyar
de	Német
en	Angol