K&H Pénzforgalmi Szolgáltató Kft.

vPOS / Payment Gateway

Illesztési dokumentáció

v1.2

Tartalom

A rendszer célja

A rendszer lehetővé teszi a K&H Pénzforgalmi Szolgáltató Kft. szerződött kereskedő partnereinél működő Internetes alkalmazások számára az on-line bankkártyás fizetést.

a virtuális POS szolgáltatás jellemzői

- forint, euró és amerikai dollár (HUF, EUR, USD) alapú elszámolás,
- több nyelven elérhető, felhasználóbarát fizetőoldal,
- magas szintű, biztonságos tranzakció végrehajtása a K&H Pénzforgalmi Szolgáltató Kft. titkosított fizetőoldalán történik,
- automatikusan ellenőrzésre kerül, hogy a fizetésre felkínált bankkártya nincs-e tiltólistán, érvényes-e, van-e megfelelő fedezet, ezzel minimálisra csökkentve a bankkártyával történő visszaélések arányát,
- magas szintű, szabványos biztonsági megoldások
  a rendszer egyes elemei egymás közötti kommunikációjukban a PKI szabványos infrastruktúrára alapozott, magas védelmi szintű authentikációs titkosítási módszereket használnak (strong encryption, SSL, digitális aláírás),
- tiszta architektúra, biztonságos működés
  a rendszer egyszerű interfészei, állapotvezérelt működése, belső felépítése garantálja a bizonytalan kommunikációs közeg ellenére a tranzakciók biztonságos végrehajtását és a folyamatos működőképességet,
- többlet szolgáltatások
  a vásárlás tranzakciótípus mellett refund (jóváírás) típusú tranzakciók is elérhetőek,

a K&H Payment Gateway rendszeréhez történő illesztés lépései

1. A K&H PSZ kereskedőazonosítót (Shop MID) és vPOS azonosítót rendel a bolthoz és megküldi Önnek. Mindkét környezetben (teszt/éles) a megadott Shop MID azonosítót kell használni az URL-ekben!
2. Ön az internetes áruház programjában – szükség esetén szakember bevonásával - megvalósítja a leírásban szereplő protokollt a tesztrendszerben (Sandbox).
3. Elküldi a tesztkörnyezethez a visszatérési URL-eket a vpos_khpos@kh.hu címre!
   1, eset: sikeres banki tranzakció eredményének megjelenése után
   2, eset (opcionális): sikertelen vagy megszakított tranzakció esetén
4. Ön kulcspárt generál a K&H PSZ által biztosított alkalmazás segítségével, amely publikus része automatikusan hozzá rendelődik az Ön Vpos azonosítójához
5. Ön aláírással együtt teszteli az alkalmazást és annak befejezésekor a teszteléshez szükséges információkat jelzi a K&H PSZ felé. Ön ekkor lehetővé teszi a társaság számára az előírt honlaptartalom ellenőrzését is.
6. K&H PSZ elvégzi a bankkártyás vásárlás funkcionális tesztelését és az előírt honlaptartalom ellenőrzését.
7. Megfelelés esetén a fizetési átjáró éles környezetben engedélyezésre kerül, melyről email-ben értesítjük.
8. Ön kulcspárt generál a K&H PSZ által biztosított alkalmazás segítségével az éles környezethez, mely aktiválása után, az URL átírásával elérheti az éles K&H PSZ payment gateway felületet.

elvárások az elkészült alkalmazással szemben

- kezelje a Sikertelen fizetés, a Mégsem, a Megszakadt kommunikáció, a Kártyabirtokos nem tér vissza a boltba eseteket is
- a jóváírás (refund) tranzakció kezelése, kialakítása
- az összes sikeres tranzakció (fizetés, jóváírás) esetében állítson ki e-mail-ben a kártyabirtokos számára egy igazolást
- a kiállított igazolásnak kötelezően tartalmazni kell az alábbi adatokat:
- tranzakció azonosító (txid)
- összeg (amount)
- valutanem (ccy)
- banki engedélyszám – ez a PGResult oldal hívására kapott eredménylap negyedik sorában található
- kereskedő (elfogadó) cégszerű neve
- kereskedő (elfogadó) internet címe
- áru/szolgáltatás megnevezése

előírt honlap tartalom

https://khpos.hu/sw/static/file/eloirt_honlap_tartalom.pdf

a fizetés folyamata

1. A kártyabirtokos a kereskedő Web-es alkalmazásában eljut ahhoz a ponthoz, ahol a kiválasztott áru, szolgáltatás ellenértékét ki kell fizetnie. Ekkor a "Fizetem" nyomógombra rakott URL-en keresztül elindít egy szerver oldali kódot (pl. CGI script, ASP vagy servlet). Ez a kereskedői alkalmazás részét képező kód olyan 302-es típusú HTTP válasz üzenetet generál, amely redirekciót tartalmaz **URL1**-re, a következő paraméterekkel:

- egyedi tranzakcióazonosító (txid-max.10 hosszú numerikus karakter), melyet a kereskedő definiál és meggátolja ugyanazon vásárlás többszöri kifizetését,
- tranzakciótípus (eladás),
- kereskedőazonosító Shop MID (mid=12345678),
- a fizetendő összeg (fillérben kell megadni, HUF valuta esetén egész forintra kerekítve),
- valutakód,
- aláírás,
- nyelvkód.

A kereskedőazonosító a K&H PSZ által szerződéskötést követően adott kód. Az aláírást a kereskedői alkalmazás készíti a kereskedő által generált saját kulcs felhasználásával, amely a tranzakcióazonosítót, tranzakciótípust, a kereskedőazonosítót, a fizetendő összeget és a valutakódot védi.

2. A redirekció hatására a böngésző meghívja **URL1**-et a kapott paraméterekkel, a következő (a tesztrendszerben értelmezhető) példához hasonlóan:

https://pay.sandbox.khpos.hu/pay/v1/PGPayment?txid=3141592653&type=PU&mid=10234506&amount=1234000&ccy=HUF&sign=a1154ffeb7…535cfc88cfd784&lang=HU

Az **URL1** által indított servlet a paraméterként kapott tranzakcióazonosító alapján ellenőrzi a kért tranzakció egyediségét, valamint az aláírás hitelességét. Ha az ellenőrzés mindent rendben talált, a nyelvkódnak megfelelő válaszlap generálódik, mely kiírja a fizetési tranzakció paramétereit (összeg, valutakód, kereskedő teljes neve) és bekéri a kártyaszámot, lejárati dátumot, CVV2-t. A kártyabirtokos a "fizetés" gomb lenyomásával indítja a kért tranzakciót.

3. A tranzakció feldolgozását követően a fizetési felület visszairányítja a kártyabirtokost a megadott visszatérési URL-re, melyet a rendszer kiegészít a txid= paraméterrel.

4. A bolti alkalmazás a visszatéréstől függetlenül URL2 hívásával kérdezheti le a tranzakció eredményét. A hívás szintaktikája:

https://pay.sandbox.khpos.hu/pay/v1/PGResult?mid=10234506&txid=3141592653

A trx lekérdezést TLS 1.2 vagy magasabb protokollon kell megvalósítani!

Az eredménylap plain text típusú, fix szerkezetű rekordokkal, mely tartalmazza a tranzakció állapotára vonatkozó kódot (1. sor), az authorizáció megtörténte után az authorizációs válaszkódot (2. sor), a válaszkódhoz tartozó szöveges üzenetet (3. sor), a banki engedélyszámot (4. sor)

```
ACK
0
ELFOGADVA / ENGEDELYEZVE
08304J
```

A tranzakciós állapotkódok a következők lehetnek:

- "NAK" - a fizetés eredménytelen (pl. nincs a számlán pénz),
- "UTX" - ismeretlen tranzakcióazonosító,
- "PEN" - még nincs eredmény, ismételt hívás szükséges,
- "ERR" - hiba (pl. nem hiteles aláírás),
- "CAN" - a kártyabirtokos „Mégsem” gombot nyomott,
- "EXP" - lejárt fizetési kísérlet (letelt a 25-30 perc),
- "ACK" - sikeres tranzakció.

a jóváírás folyamata

1. A kereskedő Web-es alkalmazása dönthet úgy, hogy egy adott, sikeresen megtörtént tranzakció teljes, vagy részösszegét jóvá kell írni a kártyabirtokos számára. **Jóváírás tranzakció következő naptól indítható!** Ekkor a kereskedői alkalmazás meghívja **URL1**-et a következő paraméterekkel:

- a jóváírni kívánt tranzakció azonosítója, melyet a kereskedő definiált,
- tranzakciótípus (jóváírás) **type=RE**,
- kereskedőazonosító,
- a jóváírandó összeg (fillérben forintra kerekítve) [mely lehet kevesebb is, mint az eredeti tranzakcióban szereplő összeg,]
- valutakód,
- aláírás.

Az aláírást a kereskedői alkalmazás készíti a kereskedő által generált saját kulcs felhasználásával, amely a tranzakcióazonosítót, tranzakciótípust, a kereskedőazonosítót, a fizetendő összeget és a valutakódot védi.

https://pay.sandbox.khpos.hu/pay/v1/PGPayment?txid=3141592653&type=RE&mid=10234506&amount=1234000&ccy=HUF&sign=a1154ffeb7…535cfc88cfd784

2. Az **URL1** által indított servlet a paraméterként kapott tranzakcióazonosító alapján ellenőrzi a kért tranzakció létezését, „ACK” státuszát, a megadott összeget, a valutakód egyezését valamint az aláírás hitelességét. Ha az ellenőrzés mindent rendben talált, az adott paraméterekkel (tranzakcióazonosító, összeg, valutakód, kereskedőazonosító) Payment Gateway banki üzenetet generál.

3. **URL2** hívásával kérdezheti le a jóváírás eredményét. A hívás szintaktikája:

https://pay.sandbox.khpos.hu/pay/v1/PGResult?mid=10234506&txid=3141592653

Az eredménylap plain text típusú. Ennek lehetséges tartalma a következő:

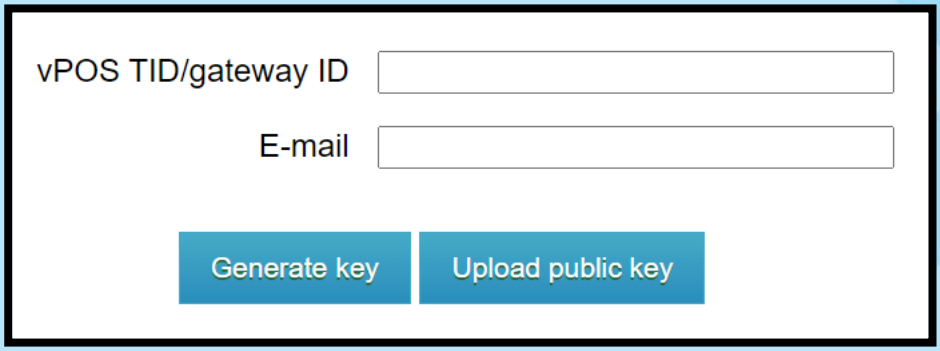
- "UTX" - ismeretlen tranzakcióazonosító,
- "PE2" - jóváírás folyamatban, ismételt lekérdezés szükséges,
- "ERR" hiba, (pl.: aznapi refund indítás)
- "VOI" . jóváírt.

A bolti interfész leírása

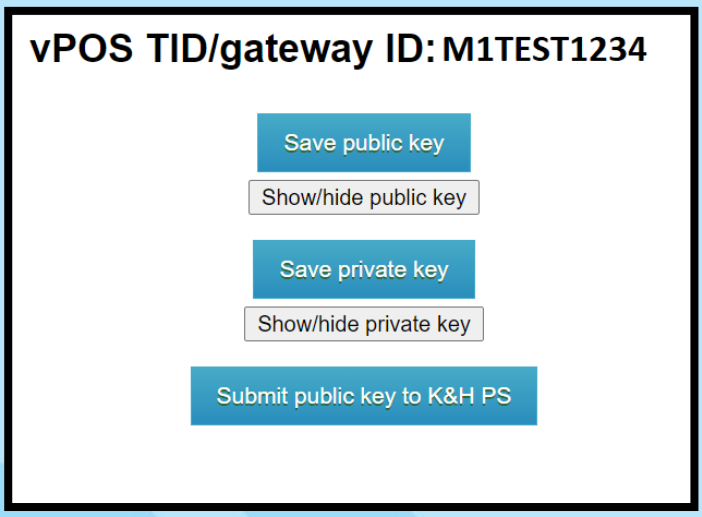
a, kulcs generálás

A teszt és az éles környezetben eltérő kulcspárokat kell használni, melyet egy egyszerű, online applikáción keresztül kell generálni, az alábbi elérhetőségen:

Teszt környezet: https://sandbox.khpos.hu/keygen
Éles környezet: https://pay.khpos.hu/keygen



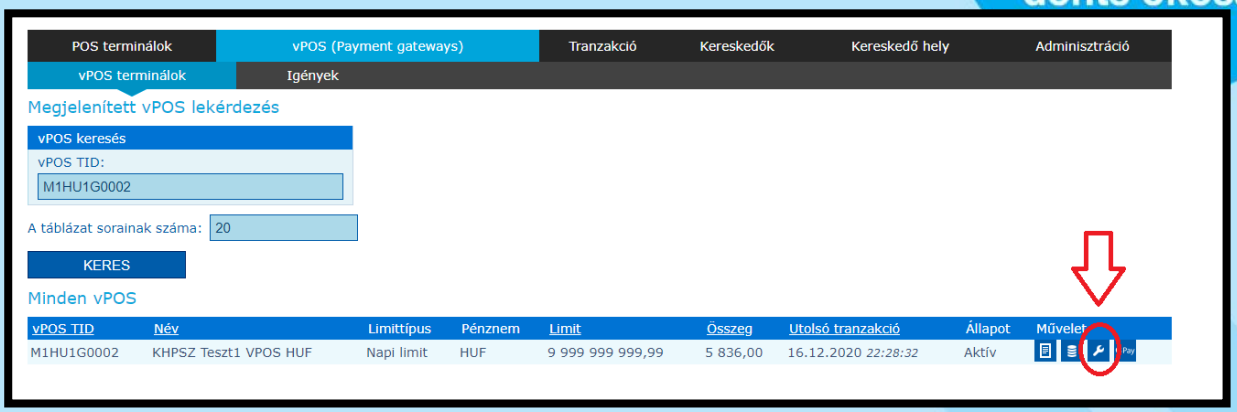
- adja meg a vPOS TID azonosítót (gateway ID) és a **szerződésben rögzített technikai e-mail** címet
- generálja le a kulcspárt (Generate key)

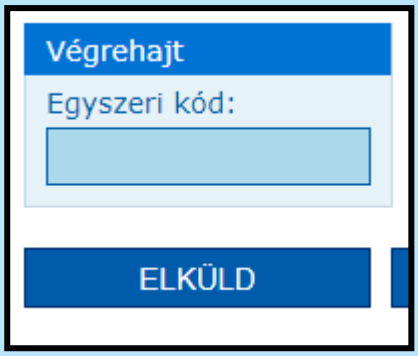


- a privát és publikus kulcsot töltse le (Save private key, Save public key)
- a publikus kulcsot töltse fel a rendszerbe (Submit public key to K&H PS)

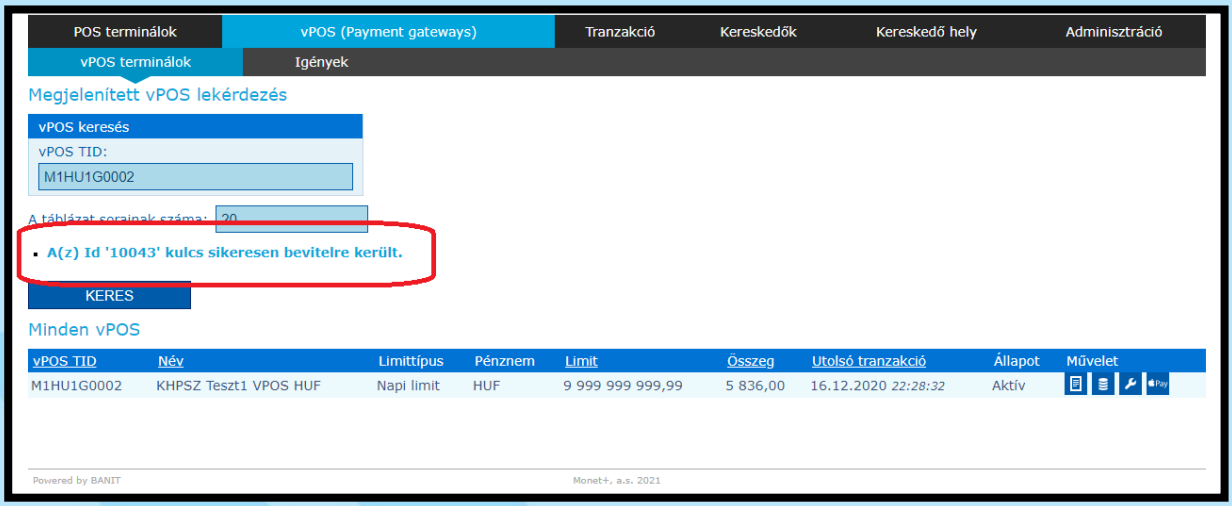
a tesztkörnyezeteben (Sandbox) a feltöltött kulcs azonnal használható!

Éles környezet esetén a generált kulcspához egy automatikus üzenet érkezik a megadott tech. email címre, amely tartalmaz egy egyszeri aktiváló kódot.
A POS24 alkalmazásban a megadott kóddal **aktiválnia kell** a generált kulcspárt!
(vPOS (Payment gateways) / vPOS terminálok)





Sikeres aktiválás esetén az alábbi üzenet jelenik meg, mely után a kulcs azonnal használható az éles környezetben.



b. aláírásképzés:

```
$ java -classpath <lásd lent> RSASign sign
"mid=1&txid=100&type=PU&amount=1&ccy=HUF" test_private_key
"test_password"
```

`data_to_sign` : **az aláírandó szöveg: a PGPayment hívás paraméterei GET-stílusban (nyelv paraméter nélkül): `mid,txid,type,amount,ccy` sorrendben. Tehát például: `mid=1&txid=100&type=PU&amount=1000&ccy=HUF`). Az aláírásban a paraméterek sorrendje kötött!**

`test_private_key` : a privát kulcsot tartalmazó file.
Az output maga az aláírás hexadump formában, ahogy a `sign` paramétert mint URL-paramétert meg kell adni.

Aláírás openssl segítségével is lehetséges:

openssl dgst -sign private_key.pem -hex -sha1 <file_containing_the_stuff_to_sign >sign.hex

Ebben a példában a file_containing_the_stuff_to_sign fájl tartalma a fentiek szerinti aláírandó szöveg sor- és fájlvég karakterek nélkül.

A parancssori elérésen kívül hogyha egy script-nyelvből elérhetőek az openssl szolgáltatásai, akkor értelemszerűen onnan is lehetséges aláírás, például:

PHP:

```
#!/usr/bin/php
<?php

$data = "mid=1&txid=100&type=PU&amount=1000&ccy=HUF";

$fp = fopen("./private_key.pem", "r");
$priv_key = fread($fp, 8192);
fclose($fp);
$pkeyid = openssl_get_privatekey($priv_key);

// compute signature
openssl_sign($data, $signature, $pkeyid);

// free the key from memory
openssl_free_key($pkeyid);

echo bin2hex($signature);

?>
```

Megjegyzések:

Az eszközök 1.4-as verziótól kezdve működnek SUN-féle Java virtuális géppel. A `classpath` paraméterben a szeparáló karakter a platformnak megfelelő, tehát Windows-on:

```
bcprov-jdk15-146.jar;khb_sign_util.jar
```

Unix-on (beleértve a Linux-ot):

```
bcprov-jdk15-146.jar:khb_sign_util.jar
```

A `bcprov-*.jar` a megfelelő verziójú Bouncy Castle-féle kriptográfiai csomag. Esetleges frissítésekor ügyeljünk arra, hogy a JDK verzióhoz megfelelő csomagot válasszuk.

http://www.bouncycastle.org/

http://www.bouncycastle.org/latest_releases.html

Példák 1.5-ös illetve 1.6-os Jávával:

1.5-össel:

```
java15 -classpath bcprov-jdk15-146.jar;khb_sign_util.jar RSASign
keygen test_private_key "test_password" test_public_key
```

1.6-ossal:

```
java16 -classpath bcprov-jdk16-146.jar;khb_sign_util.jar RSASign
keygen test_private_key "test_password" test_public_key
```

ahol java15 illetve java16 a megfelelő java futtatót jelenti, de előbb ezt kell telepíteni:
Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files
Itt található:

http://java.sun.com/javase/downloads/index.jsp
http://www.oracle.com/technetwork/java/javase/downloads/index.html

Ha nem telepítettük, ilyen hibába ütközünk: `java.lang.SecurityException`

A `bcprov-jdk*.jar`-ok elérhetősége:
`http://www.bouncycastle.org/latest_releases.html`

Minden aláírási funkció elérhető java-ból közvetlenül is az RSASign osztály metódusainak hívásával:

```
import java.security.PrivateKey;
import java.security.interfaces.RSAPublicKey;
public static void writeKey(
          PrivateKey key,
          String private_key_file_name,
          String password ) throws Exception;

public static void generateKey(
          String private_key_file_name,
          String public_key_file_name,
```

```
            String password ) throws Exception;

public static PrivateKey readKey(
            String private_key_file_name,
            String password ) throws Exception;

public static void writePublicKey(
            RSAPublicKey key,
            PrivateKey priKey,
            String public_key_file_name ) throws Exception;

public static RSAPublicKey readPublicKey(
            String public_key_file_name ) throws Exception;

public static final byte[] sign(
            PrivateKey key,
            byte data[] ) throws Exception;

public static final boolean verify(
            PublicKey key,
            byte data[],
                        byte sigBytes[] ) throws Exception;
```

a bolti alkalmazás által hívandó URL-ek

A bolti alkalmazás a következő URL-eket hívhatja meg (a HTTP protokoll GET vagy POST műveletével is).
Biztonsági okokból a POST művelet használata ajánlatos.

Az URL-ek a Payment Gateway rendszer alapeléréséhez képest értendőek, amelyik
https://pay.sandbox.khpos.hu/pay/v1 a tesztrendszerre, illetve
https://pay.khpos.hu/pay/v1 az éles rendszer.

Eladás tranzakció esetén:

URL	funkció	kötelező paraméte-rek	opcionális paraméte-rek	válasz
/PGPayment (**URL1**)	új tranzakció indítása	mid, txid, type=PU, amount, ccy, sign	lang,	text/html típusú válaszlap a felhasználó számára

/PGResult (**URL2**)	tranzakció eredményének lekérdezése: https://pay.sandbox.khpos.hu/pay/v1/PGResult?mid=12345678&txid=1234567890	mid, txid		text/plain típusú válaszlap fix hosszú szerkezettel:
				PEN - még nincs eredmény, ismételt hívás szükséges.
				CAN - „Mégsem” gombot nyomtak.
				EXP - lejárt fizetési kísérlet (25-30 perc eltelt).
				NAK - a fizetés eredménytelen (pl. ha nincs a számlán elegendő pénz).
				UTX - ismeretlen tranzakcióazonosító.
				ERR - hiba.
				ACK - sikeres tranzakció.
				`ACK`
				`0`
				`ELFOGADVA / ENGEDELYEZVE`
				`08304J`
				3 char státusz,
				3 num válaszkód,
				48 char szöveges üzenet,
				8 char engedélyszám,

Jóváírás tranzakció esetén:

URL	funkció	kötelező paraméte-rek	opcionális paraméte-rek	válasz
/PGPayment (**URL1**)	tranzakció jóváírása	mid, txid, type=RE, amount, ccy, sign		text/plain típusú válaszlap fix hosszú szerkezettel: **PE2** - kérés elfogadva. **UTX** - ismeretlen tranzakcióazonosító. **ERR** - hiba (pl. hibás aláírás, nem egyező tranzakciós adatok).
/PGResult (**URL2**)	tranzakció státuszának lekérdezése	mid, txid		text/plain típusú válaszlap fix hosszú szerkezettel: **PE2** - jóváírás folyamatban. **UTX** - ismeretlen tranzakcióazonosító. **ERR** - hiba **VOI** - jóváírt. 3 char státusz, 3 num válaszkód, 48 char szöveges üzenet, 6 char (eredetihez képest megváltozott) engedélyszám.

adatszótár: a paraméterek magyarázata

Név	Típus	
Tranzakcióazonosító (txid)	(maximum) 10 num karakter	Kereskedő adja, nem kezdőthet nullával!
Tranzakciótípus (type)	(maximum) 2 char	Kereskedő adja PU - eladás RE – jóváírás
Kereskedőazonosító (mid)	(maximum) 10 num	Bank adja
Tranzakció összege fillérben (amount)	num (00)	Maximum érték: 4294967200 csak ‘00’ val végződhet
Valutakód (ccy)	3 char	HUF, EUR, USD
Aláírás (sign)	256 char	Aláírás, melyet a kereskedő képez
Nyelv (lang)	2 char	HU, EN, DE, ES, IT, PL stb.

egyebek

A bolti alkalmazásról nyilvántartott paraméterek:

- Kereskedőazonosító (mid),
- kereskedő megnevezése, elérhetősége, címe
- kereskedő által adott (teszt/éles) visszahívási URL sikeres tranzakció (ACK) esetén,
- kereskedő által adott (teszt/éles) visszahívási URL sikertelen vagy megszakított tranzakció esetén.

A rendszer állapotkezelésének stabilitását a következő szabályok biztosítják:

- új tranzakció kérését csak akkor fogadja el a PG, ha a **txid_mid** egyedi. Ezzel megakadályozható, hogy egy futó fizetési tranzakció bármilyen ok miatt (pl. back gomb használata a böngészőben) vissza próbáljon lépni az állapot gráfban
- egy tranzakció bármilyen állapotában megszakadhat, ennek semmilyen következménye nincs a PG működőképességére
- a kereskedő egy új fizetési tranzakció kérés indítása után a **txid**-re hivatkozva bármikor lekérdezheti a tranzakció aktuális állapotát
- jóváírásra vonatkozó kérést csak "ACK" állapotú tranzakcióra fogad el a rendszer

nyelvkódok

A lang opcionális paraméter szabályozza, hogy milyen nyelvű válaszlapot ad a rendszer.

A paraméter értéke a ISO 639-1 szabvány (kétbetűs nyelvkódok) szerinti.

A támogatott nyelvkódok listája:

HU	magyar
DE	német
ES	spanyol
EN	angol
FR	francia
IT	olasz
PL	lengyel
PT	portugál
RO	román
SK	szlovák

A fizetési felületen további nyelvválasztási lehetőség található.

(Magyar, Horvát, Cseh, Angol, Francia, Német, Olasz, Japán, Lengyel, Portugál, Román, Orosz, Szlovák, Szlovén, Spanyol, Török, Vietnámi)

tesztelés

általánosan ellenőrzendő

- A banki fizető felület nem jelenhet meg keretben (iframe) a kereskedő oldalán vagy TopUp ablakban.
- A banki fizető felületen helyes összeg jelenjen meg.
- A tranzakcióazonosító legfeljebb 10 karakter hosszú lehet.

A fizetési felületen megjelenitődik a Webáruház neve, címe, elérhetősége. Kérjük az adatok helyességét ellenőrizni!

Az integráció kialakítása után hajtsák végre az alábbi teszteseteket:

Sikeres fizetés (státusz ACK)

Kérjük, a fizetési oldalra irányítás után használja az alábbi kártya adatokat!
Kártyaszám: 4154610001000209
Lejárat: 10/23
CVC: 100
Várja meg, amíg az automatikus visszairányítás megtörténik a kereskedői weboldalra.

elvárt működés: a kereskedő alkalmazása jelenítse meg a banki tranzakció sikerességét és adjon tranzakció igazolást e-mail formájában
ellenőrizni kell:
- fizetendő összeg,
- tranzakció eredményének megjelenése a kereskedő oldalán
- e-mail megérkezése a vásárlóhoz,
- e-mail tartalma (tranzakció azonosító [txid], összeg (amount), valutanem (ccy), banki engedélyszám, kereskedő (elfogadó) cégszerű neve, kereskedő (elfogadó) internet címe, áru/szolgáltatás megnevezése)

Elutasított tranzakció (NAK)

Kérjük, a fizetési oldalra irányítás után használja az alábbi kártya adatokat!
Kártyaszám: 5542860001000224
Lejárat: 06/23
CVC: 200
Az elutasítás után a visszatérés gombra kattintva a visszairányítás megtörténik a kereskedői weboldalra.
A NAK üzenet eredményként a 25-30 perces pending időtartam letelte után jelenik meg a lekérdezésre.

elvárt működés: a kereskedő alkalmazása jelenítse meg a banki tranzakció sikertelenségét.
ellenőrizni kell:
- tranzakció eredményének megjelenése a kereskedő oldalán.

Fizetés nélküli visszatérés a kereskedői oldalra (státusz CAN)

A fizetési oldalra irányítás után kártyaadatok megadása nélkül a visszatérés gombra kattintva a visszairányítás megtörténik a kereskedői weboldalra.

Elvárt működés: a kereskedő alkalmazása jelenítse meg a banki tranzakció sikertelenségét.
Ellenőrzendő:
- tranzakció eredményének megjelenése a kereskedő oldalán

Jóváírás (státusz VOI)

Visszafizetés indítása a sikeres fizetésről.
(jóváírás (refund) egy adott trx-re **másnaptól lehetséges**!!!)

elvárt működés: a kereskedő alkalmazása sikeres jóváírás esetén (VOI) küldjön tranzakció igazoló emailt a kártyabirtokosnak.
ellenőrizni kell:
- e-mail megérkezése a vásárlóhoz
- e-mail tartalma (tranzakció azonosító [txid], összeg (amount), valutanem (ccy), a jóváíráshoz tartozó [módosult] banki engedélyszám, kereskedő (elfogadó) cégszerű neve, kereskedő (elfogadó) internet címe, áru/szolgáltatás megnevezése).

kapcsolat, értesítés:

Amennyiben a tesztkörnyezetben a fenti tesztesetek sikeresen végrehajtásra kerültek kérjük, jelezze azt a vpos_khpos@kh.hu email címen, a levél tárgyában a VPOS kereskedői azonosító (**MID**) és a **szerződött webáruház webcím** megjelenítésével.
Amennyiben a visszatérési URL-ek eltérnek a teszt és az éles környezetben egymástól, kérjük az email-ben adja meg az éles visszatérési URL-eket is!

Felhívjuk figyelmét, hogy az előírt honlaptartalom a tesztelés alkalmával ellenőrzésre kerül! (Előírt honlap tartalom) Ezért kérjük, végezze el a tartalmi feltöltést is!

Az értesítést követően válasz emailben fogjuk tájékoztatni az élesbe állás menetéről.

éles rendszer elérés:

Az éles rendszer engedélyezése után a tesztrendszerben használt URL-ek elejéből a sandbox részt ki kell venni!
A teszteseteknél megadott tesztkártya adatok az éles környezetben nem érvényesek!

példa:

https://pay.sandbox.khpos.hu/pay/v1 a tesztrendszer elérhetőség
https://pay.khpos.hu/pay/v1 az éles rendszer elérhetőség