
OTP Webshop migráció a SimplePay rendszerre

Technikai dokumentáció

2020.09.06.



Tartalom

1	Bevezetés	5
1.1	PSD2, SCA, EMV 3D Secure	5
1.2	3DS megvalósítás a SimplePay rendszerében Webshop szolgáltatáshoz.....	5
1.3	Kompatibilitás	6
1.4	Nem támogatott funkciók	6
1.5	SimplePay rendszer dokumentációk.....	6
2	SimplePay rendszerek	7
2.1	Sandbox, teszt rendszer OTP Webshop használata esetén	7
2.1.1	URL-ek a SOAP hívások esetére	7
2.1.2	URL-ek fizetőoldali redirect esetére.....	7
2.1.3	Teszt VPOS kulcs.....	7
2.1.4	VPOS neve	7
2.2	Éles fizetési rendszer OTP Webshop használata esetén.....	8
2.2.1	URL-ek a SOAP hívások esetére	8
2.2.2	URL-ek fizetőoldali redirect esetére.....	8
2.2.3	VPOS kulcs tartalma.....	8
2.2.4	VPOS neve	8
3	Tranzakció típusok	9
3.1	Háromszereplős fizetések	9
3.2	Háromszereplős fizetések erős ügyfélhitelesítéssel, (SCA, 3DS).....	9
3.2.1	A sikeres 3DS folyamathoz minimálisan szükséges adatok	9
3.2.2	A sikeres 3DS folyamathoz ajánlott adatok	10
3.2.3	További opcionális adatok	11
3.2.4	Adattovábbítási nyilatkozat.....	11
3.2.5	Nem ismert vásárlói adatok esete	11
3.3	3DS challenge éles és sandbox rendszeren.....	12
3.4	Kétszereplős fizetések kártyaregisztráció esetére.....	12
3.5	Háromszereplős fizetés recurring kártyaregisztrációval.	12
3.5.1	isRecurringNeeded	13
3.6	Kétszereplős recurring fizetés	13
3.6.1	isAreq	13
3.6.2	isType.....	13
3.6.3	isRecurringNeeded	13
3.7	Háromszereplős fizetés oneclick kártyaregisztrációval.....	14
3.8	Kétszereplős oneclick fizetés.....	14
3.8.1	isAreq	14
3.8.2	isType.....	14

3.8.3	isBrowser	15
3.8.4	redirectUrl	15
3.8.5	challenge	16
3.8.6	isBackUrl	16
3.9	Kétszereplős fizetések kártyaadatok küldésével	16
3.9.1	isAreq	16
3.9.2	isType.....	17
3.9.3	isBrowser	17
3.9.4	redirectUrl	18
3.9.5	challenge	18
3.9.6	isBackUrl	18
4	Elszámolások	19
4.1	Tranzakciós analitika fájl formátum.....	19
4.2	Új CSV tranzakciós analitika formátum.....	19
4.3	Tranzakciós analitika küldési módja	19
5	Tesztelés és élesítés.....	20
5.1	Háromszereplős fizetések	20
5.2	Kétszereplős fizetések kártyaregisztráció esetére.....	20
5.3	Kétszereplős fizetések kártyaadatok küldésével	20
6	Ajánlott módosítások	21
6.1	Tranzakció azonosítók megjelenítése	21
6.2	Tájékoztatások megjelenítése	21
6.3	Adattovábbítási nyilatkozat elfogadtatása	21
6.4	Kártyatárolási nyilatkozat elfogadtatása	21
6.5	Fizetés mobil eszközön	22
7	SimplePay API v2	22
7.1	OTP rendszerében korábban regisztrált kártyák terhelése API v2 használatával	22
8	Támogatás	23
9	Mellékletek	24
I.	EMV 3D Secure	24

Dokumentum történet

Dátum	Verzió	Változás
2019. 05. 29.	190529	Eredeti kiadás
2019. 06. 04.	190604	Analitika formátumok bővítése
2019. 08. 08.	190808	OTP-nél korábban regisztrált kártyák terhelése API v2 esetén
2019. 08. 28.	190828	Szolgáltatási környezetek megnevezésének javítása
2019. 09. 16.	190916	Pontosítások - Bevezetés További ajánlott módosítás - Fizetés mobil eszközön
2020. 05. 13.	200513	VPOS kulcs generálás lehetősége a kereskedői admin felületen
2020. 06. 24.	200624	3DS folyamat háromszereplős fizetésekhez Új CSV analitika formátum bevezetése
2020. 08. 15.	200815	3DS folyamat kétszereplős fizetésekhez
2020. 09. 06.	200906	Sandbox fizetőoldali 3DS Challenge kártya teszteléshez

1 Bevezetés

Az OTP Mobil rendszere az OTP Bank 2017-től elérhető, aszinkron működésű Webshop 5.0 interface (<http://simplepartner.hu/download.php?target=webshop5>) használatának lehetőségét is biztosítja a SimplePay rendszeréhez.

Az OTP Bank „Webshop” (Middleware, MW) szolgáltatásával megegyező interface megadja a lehetőséget arra, hogy a korábban az OTP Bank rendszerének használatához implementált technikai megoldással a SimplePay rendszerén keresztül is lehessen tranzakciókat indítani. A SimplePay rendszeréhez csatlakozás azok számára, akik korábban a banki rendszert használták így néhány módosítással megoldható.

A migráció esetén feltételezzük, hogy a kereskedői weboldalon a Webshop 5.0 alapján működő bankkártyás fizetés működik.

Jelen dokumentáció ahhoz nyújt segítséget, hogy azon kereskedők, akik a „Webshop” szolgáltatást használják egyszerűen válthassanak a SimplePay szolgáltatásra. A dokumentáció a VPOS-okra, a szolgáltatás elérhetőségére (teszt és éles), elszámolásokra, tesztelési és élesítési folyamatokra fókuszál.

Jelen dokumentáció nem tárgyalja sem a Webshop technikai működését, sem a SimplePay szolgáltatás technikai működését.

Az OTP Bank Webshop 5.0 dokumentációja és mintakódja az alábbi URL-en érhető el.
<http://simplepartner.hu/download.php?target=webshop5>

1.1 PSD2, SCA, EMV 3D Secure

A PSD2 az Európai Unió második pénzforgalmi irányelve a digitális pénzügyi szolgáltatásokról, amely szerint kétfaktoros hitelesítést, vagy erős ügyfélhitelesítést (Strong Customer Authentication, SCA) szükséges alkalmazni a bankkártyás fizetéseknél.

Az EMV 3D Secure (3DS) pedig a kártyatársasági szabvány az erős ügyfélhitelesítés (SCA) technikai megvalósítására. **A 3DS alkalmazásának hazai határideje 2020 szeptember 30.**

Az erős ügyfélhitelesítés törvényi háttéréről az **I. mellékletben** olvasható további információ.

Az erős ügyfélhitelesítés technikai megoldása aktív fejlesztés alatt áll a SimplePay rendszerben, emiatt ez a dokumentáció gyakran változhat! Ennek a dokumentációnak az aktuális, friss verziója mindig letölthető az alábbi URL-ről:

<http://simplepartner.hu/download.php?target=otpvposhu>

1.2 3DS megvalósítás a SimplePay rendszerében Webshop szolgáltatáshoz

A 2020 szeptember 30-án érvénybe lépő erős ügyfél hitelesítés megköveteli a kibővített tranzakciós adatok küldését a bankkártyás fizetés indításakor. Az erős ügyfélhitelesítés megvalósítását az OTP Bank Webshop szolgáltatásában a Webshop 5.1 verzió dokumentációja írja le, mely az alábbi URL-en érhető el.

<http://simplepartner.hu/download.php?target=webshop51dochu>

Az 5.1 verzió az implementálása már csak a SimplePay rendszerében lesz elérhető, így az csak az OTP Bank Webshop szolgáltatásáról az OTP Mobil SimplePay szolgáltatására váltó kereskedők számára érhető el.

A kibővített adattartalommal történő tranzakciók indítása jelen dokumentáció „**Tranzakció típusok**” c. fejezetben található meg.

Fontos!

A fentebb említett szabvány a 3DS **2.x** verziójának bevezetéséről szól. Ugyanakkor a SimplePay rendszerében jelenleg is működik a 3DS **1.0** szerinti ügyfélhitelesítés, azonban ez nem követel meg semmilyen kereskedőt is érintő változtatást.

A jelenleg működő 3DS 1.0-ról 2.x verzióra a szeptemberi határidőig átvált a SimplePay rendszere.

1.3 Kompatibilitás

Kompatibilitási problémák miatt a tranzakciók indítása meghiúsulhat az alábbi esetekben:

- a kereskedői rendszer az OTP Bank Webshop 5.0 előtti technikai kritériumoknak megfelelően módon működik
- tranzakció indítás "startWorkflow" metódust alkalmaz

1.4 Nem támogatott funkciók

- Ügyfél regisztrációs adatok karbantartó felülete
- SZÉP kártya elfogadás

1.5 SimplePay rendszer dokumentációk

Az OTP Mobil SimplePay rendszerének dokumentációja és mintakódja az alábbi URL-eken érhető el. Minden olyan technikai részletben, amit jelen dokumentáció nem tárgyal, az ebben leírtak a mérvadók.

Háromszereplős fizetés

Mintakód: <http://simplepartner.hu/download.php?target=v21sdk>

Dokumentáció:

Magyar: <http://simplepartner.hu/download.php?target=v21dochu>

Angol: <http://simplepartner.hu/download.php?target=v21docen>

Kétszereplős fizetés tárolt kártyával:

Mintakód: <http://simplepartner.hu/download.php?target=v21cardstoragesdk>

Dokumentáció:

Magyar: <http://simplepartner.hu/download.php?target=v21cardstoragedochu>

Angol: <http://simplepartner.hu/download.php?target=v21cardstoragedocen>

Kétszereplős fizetés kártyaadatokkal:

Mintakód: <http://simplepartner.hu/download.php?target=v21autosdk>

Dokumentáció:

Magyar: <http://simplepartner.hu/download.php?target=v2autodochu>

Angol: <http://simplepartner.hu/download.php?target=v2autodocen>

2 SimplePay rendszerek

A SimplePay két egymástól teljesen elkülönülő fizetési rendszerből épül föl. Az egyik rendszer a fejlesztési tranzakciós tesztekhez használható, míg a másik az éles tranzakciókhoz. A két rendszer nincs egymással semmilyen kapcsolatban.

2.1 Sandbox, teszt rendszer OTP Webshop használata esetén

Kizárólag csak teszt tranzakciók indítására alkalmas.
Csak a fizetőoldalon található tesztkártyákkal lehet rajta tranzakciót indítani.

2.1.1 URL-ek a SOAP hívások esetére

Eddig az OTP Bank VPOS szolgáltatási környezetben

<https://www.otpbankdirekt.hu/mwaccesspublic/mwaccess>

SimplePay sandbox üzemű szolgáltatási környezetben:

<https://sandbox.simplepay.hu/mw/mw/pspHU>

2.1.2 URL-ek fizetőoldali redirect esetére

Eddig az OTP Bank VPOS szolgáltatási környezetben

<https://www.otpbankdirekt.hu/webshop/do/webShopVasarlasInditas>

SimplePay sandbox üzemű szolgáltatási környezetben

<https://sandbox.simplepay.hu/pay/pay/webshop/do/webShopVasarlasInditas>

2.1.3 Teszt VPOS kulcs

Az OTP Banki szolgáltatás esetén használt **teszt** VPOS alkalmazásával lehet teszt tranzakciókat indítani.

VPOS kulcs: #02299991

VPOS devizaneme: HUF

VPOS kulcs: #02299992

VPOS devizaneme: EUR

VPOS kulcs: #02299993

VPOS devizaneme: USD

2.1.4 VPOS neve

Megegyezik a kulcs nevével. Ezen a néven lehet használni a továbbiakban POS ID-ként tranzakciók indításakor:

<posid>**#02299991**</posid>

A sandbox rendszeren további beállítások nem szükségesek.

2.2 Éles fizetési rendszer OTP Webshop használata esetén

Kizárólag csak éles tranzakciók indítására alkalmas.

Egy szerződés (kereskedő) alatt több weboldalhoz, illetve több devizanemhez is létrehozható egyedi kereskedői fiók.

Az OTP Bank rendszerében használt VPOS egy-egy ilyen SimplePay kereskedői fiókhoz tartozik.

A kereskedői fiók neve (Kereskedői azonosító, vagy MERCHANT) a kereskedői admin felületen található meg.

A MERCHANT értéke **MWxxxxxx** formátumú. A tranzakciók kezelése során ennek a MW prefix nélküli részét szükséges felhasználni POS ID-ként.

2.2.1 URL-ek a SOAP hívások esetére

OTP Bank VPOS szolgáltatási környezetben

<https://www.otpbankdirekt.hu/mwaccesspublic/mwaccess>

SimplePay éles üzemű szolgáltatási környezetben

<https://securepay.simplepay.hu/mw/mw/pspHU>

2.2.2 URL-ek fizetőoldali redirect esetére

OTP Bank VPOS szolgáltatási környezetben

<https://www.otpbankdirekt.hu/webshop/do/webShopVasarlasInditas>

SimplePay éles üzemű szolgáltatási környezetben

<https://securepay.simplepay.hu/pay/pay/webshop/do/webShopVasarlasInditas>

2.2.3 VPOS kulcs tartalma

Az éles rendszeren használható az OTP Banknál alkalmazott éles kereskedői VPOS kulcs, illetve a SimplePay rendszerében is generálható új kulcs. Kereskedői döntés, hogy melyiket szeretné használni. Technikailag a két megoldás egyenértékű.

OTP VPOS kulcs használata esetén

Ebben az esetben a kereskedő az eddigi VPOS publikus kulcsának (**123456.pubKey**) tartalmát szükséges beállítani a rendszerünkben. A SimplePay kereskedői admin rendszerben (<https://admin.simplepay.hu/admin/>) a „**Fiókkezelő / Technikai adatok**” oldalon a „**Publikus kulcs**” mezőben lehet megadni a publikus kulcs tartalmát.

Új VPOS kulcs használata esetén

Ebben az esetben a SimplePay rendszerében lehet új kulcsot generálni. A kulcs generálás a SimplePay kereskedői admin rendszerben (<https://admin.simplepay.hu/admin/>) a „**Fiókkezelő / Technikai adatok**” oldalon végezhető el.

A „**Kulcsgenerálás**” gombra kattintva lehet generálni az új kulcsot, aminek a privát elemeit le lehet tölteni, a publikus eleme pedig automatikusan beállításra kerül a rendszerbe.

2.2.4 VPOS neve

Megegyezik a SimplePay kereskedői fiók MW prefix nélküli nevével (MERCHANT). Ennek az értékét lehet használni a továbbiakban POS ID-ként.

Például, ha a MERCHANT értéke **MW123456**, akkor annak MW prefix nélküli formáját (**123456**) lehet használni a továbbiakban POS ID-ként: <posid>**123456**</posid>

3 Tranzakció típusok

3.1 Háromszereplős fizetések

A fenti beállításokon kívül nem szükséges további beállítás ahhoz, hogy a jelenlegi módon, tovább üzemeljen a fizetési szolgáltatás a SimplePay rendszerben.

Ugyanakkor fontos figyelmet fordítani arra, hogy a korábbi elvárásokhoz képest a 2020 szeptember 30-án érvénybe lépő erős ügyfél hitelesítés megköveteli a kibővített tranzakciós adatok küldését.

3.2 Háromszereplős fizetések erős ügyfélhitelesítéssel, (SCA, 3DS)

A fentebb említett Webshop 5.1 verzió fogadja és a kártyakibocsátó bank felé továbbítja az erős ügyfélhitelesítéshez szükséges további adatokat.

Az adatokat az „**isAreq**” mezőben szükséges küldeni. Az **isAreq** mező elhelyezése és tartalma egy **JSON** struktúrában leírt adat, amelyik **base64** enkódolva van. A JSON struktúra, illetve a mezők adattartalmának leírása **a fentebb említett Webshop 5.1 dokumentációban az 5.1.1 fejezetben található meg.**

Az isAreq tartalmát a SimplePay rendszere továbbítja az fizetés elindításakor. A bank ezeket figyelembe veszi a tranzakció engedélyezésénél, emiatt a tranzakció sikeressége érdekében kiemelten fontos a küldésük és az adatok valóság!

Az adatot formailag vizsgálja a SimplePay rendszere, de a tartalmát csak a kártyakibocsátó bank validálja. A formai vizsgálat során az alábbi pontokat ellenőrzi a SimplePay rendszere.

Abban az esetben, ha a kereskedői rendszer a hagyományos módon is küld adatot, illetve az **isAreq** is tartalmazza ugyanazt a mezőt, akkor az **isAreq** tartalma kerül tovább küldésre. Ilyen lehet pl. az **isMailAddress** paraméter és az **isAreq**-en belül megtalálható **email** paraméter. Ha mindkettő küldve van, akkor az **isAreq/email** lesz kiértékelve.

Ha van **isAreq** mező, akkor a tartalma base64 enkódolva van-e.
Ha nem, akkor a hibaüzenet **HIBASBASE64FORMATUM**

Ha van **isAreq** mező, akkor a base64 dekódolás utáni tartalom valid JSON string-e.
Ha nem, akkor a hibaüzenet **HIBASJSONFORMATUM**

3.2.1 A sikeres 3DS folyamathoz minimálisan szükséges adatok

Az **isAreq** JSON string-ben felsorolt összes adat nem biztos, hogy minden kereskedőnek a rendelkezésére áll a tranzakció elindításakor, azonban az alábbiak küldése kiemelten fontos a tranzakció sikeressége szempontjából.

billAddrCity: város
billAddrCountry: ország
billAddrLine1: cím
billAddrPostCode: irányítószám
billAddrState: megye
email: a vásárló e-mail címe

Abban az esetben, ha valamelyik mezőhöz nem áll rendelkezésre az adat, akkor az egész mezőt kikell venni a JSON string-ból, azaz a félreértések elkerülése végett csak azt van értelme küldeni a SimplePay felé, aminek valós tartalmat tud adni a kereskedői rendszer.

Arra kiemelt figyelmet kell fordítani, hogy a JSON struktúrában az elküldött adat a megfelelő szinten maradjon, például a „**billAddrCity**” minden esetben a „**cardholder**” alatt kell legyen, függetlenül attól, hogy milyen egyéb elemek lettek eltávolítva a JSON-ból.

A fenti minimálisan szükséges adatokhoz a JSON struktúra az alábbi:

```
{
  "cardholder":{
    "billAddrCity":"billAddrCity",
    "billAddrCountry":"222",
    "billAddrLine1":"billAddrLine1",
    "billAddrPostCode":"billAddrPostCode",
    "billAddrState":"111",
    "email":"aaa-bbb@example.com",
  },
}
```

3.2.2 A sikeres 3DS folyamathoz ajánlott adatok

Az alábbi adatok küldése opcionális, de ha rendelkezésre állnak akkor ajánlott átadni az **isAReq**-ben.

threeDSReqAuthMethod: kártyabirtokos kereskedői oldali regisztrációjának módja
lehetséges értékek:

01: vendég

02: kereskedőnél rögzített azonosító

05: harmadok feles azonosító a kereskedői rendszerben (Facebook, Google account, stb)

billAddrLine2: cím második sora

billAddrLine3: cím harmadik sora

shipAddrCity: szállítási város

shipAddrCountry: szállítási ország

shipAddrLine1: szállítási cím

shipAddrLine2: szállítási cím második sora

shipAddrLine3: szállítási cím harmadik sora

shipAddrPostCode: szállítási irányítószám

shipAddrState: szállítási megye

mobilePhone, vagy homePhone, vagy workPhone: a vásárló valamelyik telefonszáma

cc: (country code) ország hívószám

subscriber: telefonszám

Arra kiemelt figyelmet kell fordítani, hogy a JSON struktúrában az elküldött adat a megfelelő szinten maradjon, például a lenti mintában a „**cc**” a „**cardholder**” / „**mobilePhone**” alatt kell legyen.

Opcionális adatokkal kiegészített JSON struktúra:

```
{
  "threeDSRequestor":{
    "threeDSRequestorAuthenticationInfo":{
      "threeDSReqAuthMethod":"02"
    }
  },
  "cardholder":{
    "billAddrCity":"billAddrCity",
    "billAddrCountry":"222",
    "billAddrLine1":"billAddrLine1",
    "billAddrPostCode":"billAddrPostCode",
    "billAddrState":"111",
    "email":"aaa-bbb@example.com",
    "mobilePhone":{
      "cc":"cc",
      "subscriber":"subs"
    }
  },
  "shipAddrCity":"shipAddrCity",
  "shipAddrCountry":"111",
  "shipAddrLine1":"shipAddrLine1",
  "shipAddrPostCode":"shipAddrPostCode",
  "shipAddrState":"222"
},
}
```

3.2.3 További opcionális adatok

Minden egyéb, a dokumentációban leírt JSON-ben található adat küldése opcionális. A küldésük csak akkor releváns, ha a kereskedő valid adatokkal tudja küldeni.

3.2.4 Adattovábbítási nyilatkozat

Az **isAreq** tartalmában a kereskedő harmadik félnek adja át a megrendelési/vásárlói adatokat, ezért **a vásárlónak az adattovábbítási nyilatkozatot** kifejezetten **el kell fogadnia**.

Az adattovábbítási nyilatkozat és elhelyezésének módja a SimplePay API v2 dokumentációjában található meg az „**Adattovábbítási nyilatkozat**” c. fejezetben.

3.2.5 Nem ismert vásárlói adatok esete

Abban az esetben, **ha a kereskedői rendszerben nem ismertek a vásárló adatai**, akkor az alábbi változók hatására a fizetőoldalon is meg tudja adni ezt a vásárló.

Ezek a változók már a Webshop 5.0 verzióban is elérhetők.

```
<isMailAddressNeeded>true</isMailAddressNeeded>
<isNameNeeded>true</isNameNeeded>
<isCountryNeeded>true</isCountryNeeded>
<isCountyNeeded>true</isCountyNeeded>
<isZipcodeNeeded>true</isZipcodeNeeded>
<isStreetNeeded>true</isStreetNeeded>
```

3.3 3DS challenge éles és sandbox rendszeren

A 3DS challenge során a kártyakibocsátó bank interaktívan szeretné beazonosítani a kártya birtokosát az adott tranzakció során.

A folyamatban éles működés esetén SMS-ben küld a bank a kártyatulajdonosnak egy egyszer használható azonosítót, amit a banki felületen kell megadjon. Ha az azonosító kód megfelelő, akkor folytatódik a fizetési folyamat.

A sandbox fizetőoldalon szimuláva van a 3DS challenge folyamat. Annak érdekében, hogy a tranzakció során 3DS challenge történjen a sandbox legördülő kártyalistájából a 3DS folyamathoz megjelölt kártyát kell kiválasztani a teszt fizetéskor.

Ebben az esetben nem történik meg azonnal a fizetés hanem előbb átírányításra kerülünk a banki kódbekérő oldal szimulációjára. Az **éles** működés esetén itt (vagy ennek megfelelő kártyakibocsátó banki felületen) lehet megadni az SMS-ben kapott kódot.

A **sandbox** 3DS Challenge szimuláció esetén **NEM küld** a rendszer **SMS-ben kódot**, hanem két konstans érték megadására van lehetőség:

- **1234** a sikeres teszt folyamathoz
- **1111** a sikertelen teszt folyamathoz

3.4 Kétszereplős fizetések kártyaregisztráció esetére

A kártyaregisztráció funkció és a regisztrált kártyával fizetés a továbbra is használható a SimplePay rendszerében.

A SimplePay rendszerében ennek az API-nak a használatával továbbra is lehet kártyát tárolni és a tárolt kártyát további tranzakciókhoz fel lehet használni.

Az OTP Bank rendszerében korábban tárolt kártyákhoz tartozó tokeneket továbbra is lehet használni a SimplePay rendszerén keresztül. Ebben az esetben a SimplePay VPOS és a korábbi OTP VPOS unióba lesznek kötve és a korábban regisztrált tokenekkel továbbra is lehet tranzakciót indítani.

A kártya regisztrációja minden esetben egy háromszereplős regisztrációs fizetésben történik meg. Ezután lehet a regisztrált kártyát kétszereplős módon terheli.

3.5 Háromszereplős fizetés recurring kártyaregisztrációval.

A recurring fizetések olyan tranzakciók, amit a kereskedő indít rendszeres időközönként, a vásárló jelenléte nélkül terhelve a regisztrált kártyát. A recurring használható például rendszeresen ismétlődő beszedésekhez, előfizetések kezeléséhez, stb.

A recurring fizetésekhez egy háromszereplős kártyaregisztrációs fizetés (**WEBSHOPFIZETESINDITAS**) szükséges, majd a későbbiekben a regisztráció során megadott kártyát lehet kétszereplősen (**WEBSHOPFIZETESKETSZEREPLÓS**) terhelni.

A jelenlegi interface a **WEBSHOPFIZETESINDITAS** során történő ügyfél regisztráció, vagy kártya regisztráció esetén az alábbi változókat várja.

isConsumerRegistrationNeeded = true

isConsumerRegistrationId = abc123

3.5.1 isRecurringNeeded

Ezen ismert elemek mellett szükséges a továbbiakban küldeni az **isRecurringNeeded** paramétert, aminek hatására a SimplePay rendszere recurring regisztrációként fogja végrehajtani az adott ügyfél regisztrációt, vagy kártya regisztrációt.

isRecurringNeeded = true

3.6 Kétszereplős recurring fizetés

A recurring regisztráció során felhasznált kártyát a továbbiakban a kereskedő rendszere a felhasználó jelenléte nélkül terhelheti például havi, heti, stb. rendszeres beszedések esetén.

Ezekhez a fizetésekhez a jelenlegi **WEBSHOPFIZETESKETSZEREPLŐS** hívásokat lehet továbbra is használni. A hívásokban továbbra is küldeni kell az eddigi módon a regisztrációnál, az **isConsumerRegistrationId** mezőben megadott azonosítót.

Továbbá ki kell egészíteni a hívást az alábbi elemekkel.

3.6.1 isAreq

A háromszereplős fizetéseknél leírt adatokon kívül ebben az esetben a **cardholderName** mező is a minimálisan szükséges adatok közé tartozik, mivel nincs fizetőoldal, ahol ezt a vásárló megadhatná.

```
{
  "cardholder":{
    "billAddrCity":"billAddrCity",
    "billAddrCountry":"222",
    "billAddrLine1":"billAddrLine1",
    "billAddrPostCode":"billAddrPostCode",
    "billAddrState":"111",
    "email":"aaa-bbb@example.com",
    "cardholderName": "",
  },
}
```

3.6.2 isType

A mező annak jelölésére szolgál, hogy a vásárló a tranzakciónál jelen van vagy sem.

Értéke az alábbiak egyike lehet

- **CIT** (Customer Initiated Transaction) a vásárló jelenlétével indított tranzakció
- **MIT** (Merchant Initiated Transaction) a vásárló jelenléte nélkül indított tranzakció
- **REC** (Recurring) a vásárló jelenléte nélkül, **rendszeresen** indított tranzakció

Recurring regisztráció utáni kétszereplős fizetés esetén ez az érték csak **REC** lehet, mivel a tranzakció valamilyen rendszerességgel a kereskedő által van indítva a vásárló jelenléte nélkül.

3.6.3 isRecurringNeeded

Az ismert elemek mellett szükséges a továbbiakban küldeni az alábbi paramétert, aminek hatására a SimplePay rendszere recurring fizetesként fogja a kártyakibocsátó bank felé küldeni a tranzakciót.

isRecurringNeeded = true

3.7 Háromszereplős fizetés oneclick kártyaregisztrációval

Oneclick kártyaregisztráció esetén a regisztrált kártyát a kereskedő kényelmi szolgáltatásként menti el, amit a későbbi fizetéseknél a felhasználó jelenlétével tud terhelni.

A jelenlegi interface a **WEBSHOPFIZETESINDITAS** során történő ügyfél regisztráció, vagy kártya regisztráció esetén az alábbi változókat várja.

isConsumerRegistrationNeeded = true
isConsumerRegistrationId = abc123

A fentiek nem jelentenek különbséget az eddigi regisztrációs lehetőséghez képest. A későbbiekben a regisztráció során megadott kártyát viszont csak a felhasználó jelenlétével lehet terhelni a **WEBSHOPFIZETESKETSZEREPLIS** hívással.

3.8 Kétszereplős oneclick fizetés

A oneclick regisztráció során felhasznált kártyát a továbbiakban a kereskedő rendszere a felhasználó jelenlétével terhelheti.

Ezekhez a fizetésekhöz a jelenlegi **WEBSHOPFIZETESKETSZEREPLIS** hívásokat lehet továbbra is használni. A hívásokban továbbra is küldeni kell az eddigi módon a regisztrációnál, az **isConsumerRegistrationId** mezőben megadott azonosítót.

Továbbá ki kell egészíteni a hívást az alábbi elemekkel.

3.8.1 isAreq

Az **isAreq** részletes leírása fentebb a háromszereplős fizetéseknél található meg. A háromszereplős fizetéseknél leírt adatokon kívül ebben az esetben a **cardholderName** mező is a minimálisan szükséges adatok közé tartozik, mivel nincs fizetőoldal, ahol ezt a vásárló megadhatná.

```
{
  "cardholder":{
    "billAddrCity":"billAddrCity",
    "billAddrCountry":"222",
    "billAddrLine1":"billAddrLine1",
    "billAddrPostCode":"billAddrPostCode",
    "billAddrState":"111",
    "email":"aaa-bbb@example.com",
    "cardholderName": "",
  },
}
```

3.8.2 isType

A mező annak jelölésére szolgál, hogy a vásárló a tranzakciónál jelen van vagy sem. Értéke az alábbiak egyike lehet

- **CIT** (Customer Initiated Transaction) a vásárló jelenlétével indított tranzakció
- **MIT** (Merchant Initiated Transaction) a vásárló jelenléte nélkül indított tranzakció
- **REC** (Recurring) a vásárló jelenléte nélkül, **rendszeresen** indított tranzakció

Onclick regisztráció utáni háromszereplős fizetés esetén ez az érték **CIT**, vagy **MIT** lehet, mivel a tranzakció a kereskedő által van indítva a vásárló jelenlétével, vagy anélkül, azonban nem rendszeres, hanem valamilyen eseti vásárlás kifizetése történik meg.

CIT esetre példa, amikor a jelenlevő vásárló interakciójára, megtörténik azonnal a terhelés indítása. Bár a fizetési tranzakció technikailag a **WEBSHOPFIZETESKETSZEREPLŐS** hívással történik, ami során nincs fizetőoldal, azonban a felhasználó jelenléte miatt valójában ez is háromszereplős fizetesként értelmezhető.

MIT esetre a példa, amikor a vásárló interakciójára csak letárolódnak a fizetés adatai és egy későbbi időpontban indítja azt el a kereskedő, például valamilyen kereskedő számára lényeges ellenőrzés után, vagy éjszakánként kötegelten.

3.8.3 isBrowser

CIT tranzakció esetén a vásárló böngészőjének paraméterei (**browser**). Ez az adat is a **3DS** ellenőrzés része, ami továbbítja van a kártyakibocsátó bank felé.

Az **isBrowser** mező tartalma egy **JSON** struktúrában leírt adat, amelyik **base64** enkódolva van.

browser tömb részletei

- **accept**: Accept http fejléc értéke
- **agent**: User-Agent http fejléc érték
- **ip**: a böngésző forrás IP-je
- **java**: a böngésző támogatja-e a java appleteket; javascriptben: `navigator.javaEnabled()`
- **lang**: a böngésző nyelve; javascriptben: `navigator.language`
- **color**: a böngésző színmélysége; javascriptben: `screen.colorDepth`
- **height** = a böngésző képernyőjének magassága; javascriptben: `screen.height`
- **width** = a böngésző képernyőjének szélessége; javascriptben: `screen.width`
- **tz** = a böngésző időzónája; javascriptben: `new Date().getTimezoneOffset()`

JSON minta

```
{
"accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
"agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36",
"ip": "94.199.53.96",
"java": false,
"lang": "hu-HU",
"color": 24,
"height": 1920,
"width": 1080,
"tz": -120
}
```

3.8.4 redirectUrl

Ha a **banki 3DS** ellenőrzés **sikertelen**, akkor az autorizáció még **nem** történik meg.

A kereskedői rendszernek fel kell készülnie arra, hogy a 3DS folyamat során a kártyakibocsátó bank megkövetelheti, hogy **CIT** tranzakció esetén a kártyabirtokos interaktívan azonosítsa magát (**challenge**). Az azonosításhoz a vásárló interakciójára van szükség. Ebben az esetben a **WEBSHOPFIZETESKETSZEREPLŐS** hívás válaszában a SimplePay rendszere visszaad egy olyan URL-t (**redirectUrl**) a kereskedőnek, amire átirányíthatja a vásárlót.

Mivel a tranzakció során a vásárló jelen van (**isType = CIT**) így a kereskedőnek van lehetősége átirányítani a vásárlót a kapott URL-re.

A fentiekből adódóan a kereskedői rendszernek fel kell készülnön arra, hogy a **redirectUrl** mezőt fogadhassa a **WEBSHOPFIZETESKETSZEREPLÓS** hívás szinkron válaszában.

3.8.5 challenge

Ha a kereskedői rendszer átirányítja a vásárlót a „**redirectUrl**” mezőben kapott URL-re, akkor egy olyan helyre jut, ahol a kártyakibocsátó bank által megkívánt további ügyféllenőrzési folyamat történik meg.

3.8.6 isBackUrl

A challenge folyamat böngészőben történik, aminek a végén a SimplePay rendszere visszairányítja a vásárlót a kereskedői weboldalra.

Annak érdekében, hogy a potenciális challenge folyamat végén megadható legyen, hogy hova kell a vásárlót visszairányítani a **WEBSHOPFIZETESKETSZEREPLÓS** hívásban szükséges megadni az URL-t.

A **WEBSHOPFIZETESKETSZEREPLÓS** hívásban ezért szükséges küldeni az **isBackUrl** mezőt is annak érdekében, hogy egy challenge esetén a visszairányítás a kereskedői weboldalra megtörténhessen.

Ennek a mezőnek a tartalma megegyezik a háromszereplős fizetések **isBackUrl** mezőjével.

Az **isBackUrl** opcionális. Ha nincs küldve, akkor a challenge folyamat és az autorizáció végén a SimplePay oldalán történik meg a tranzakció eredményéről a tájékoztatás.

3.9 Kétszereplős fizetések kártyaadatok küldésével

A funkció használatával továbbra is lehet olyan fizetéseket kezdeményezni, ahol a kereskedő weboldalán lett bekérve a vásárló kártyája.

A SimplePay rendszerének PCI-DSS megfelelése miatt szükséges a kereskedő oldali megfelelés is abban az esetben, ha kártyaadatokat kér be a vásárlótól és tovább küldi kétszereplős módon.

Az éles rendszerben való tranzakció indításnak feltétele, hogy a kereskedő a saját PCI-DSS **AOC**-t (Attestation of Compliance) bemutassa a SimplePay felé.

Ezekhez a fizetésekhöz a jelenlegi **WEBSHOPFIZETESKETSZEREPLÓS** hívásokat lehet továbbra is használni. A hívásokban továbbra is küldeni kell az eddigi módon a kártyaadatokat, továbbá a jelenlegi **WEBSHOPFIZETESKETSZEREPLÓS** hívást ki kell egészíteni az alábbi elemekkel.

3.9.1 isAreq

Az **isAreq** részletes leírása fentebb a háromszereplős fizetéseknél található meg. A háromszereplős fizetéseknél leírt adatokon kívül ebben az esetben a **cardholderName** mező is a minimálisan szükséges adatok közé tartozik, mivel nincs fizetőoldal, ahol ezt a vásárló megadhatná.

```
{  
  "cardholder":{
```



```

    "billAddrCity": "billAddrCity",
    "billAddrCountry": "222",
    "billAddrLine1": "billAddrLine1",
    "billAddrPostCode": "billAddrPostCode",
    "billAddrState": "111",
    "email": "aaa-bbb@example.com",
    "cardholderName": "",
  },
}

```

3.9.2 isType

A mező annak jelölésére szolgál, hogy a vásárló a tranzakciónál jelen van vagy sem.

Értéke az alábbiak egyike lehet

- **CIT** (Customer Initiated Transaction) a vásárló jelenlétével indított tranzakció
- **MIT** (Merchant Initiated Transaction) a vásárló jelenléte nélkül indított tranzakció
- **REC** (Recurring) a vásárló jelenléte nélkül, **rendszeresen** indított tranzakció

Ebben az esetben mindhárom típus előfordulhat.

Ha a kereskedő oldalán a tranzakció indításakor **jelen volt a vásárló**, akkor ez egy **háromszereplős** fizetés, amikor ez az érték csak **CIT** lehet.

Ha a kereskedő oldalán a tranzakció indításakor **nem volt jelen a vásárló**, és ez egy eseti terhelés, akkor ez egy **kétszereplős** fizetés, amikor ez az érték csak **MIT** lehet.

Ha a kereskedő oldalán a tranzakció indításakor **nem volt jelen a vásárló**, és ez egy rendszeres (**recurring**) terhelés, akkor ez egy **kétszereplős** fizetés, amikor ez az érték csak **REC** lehet.

3.9.3 isBrowser

CIT tranzakció esetén a vásárló böngészőjének paraméterei (**browser**). Ez az adat is a **3DS** ellenőrzés része, ami továbbítja van a kártyakibocsátó bank felé.

Az **isBrowser** mező tartalma egy **JSON** struktúrában leírt adat, amelyik **base64** enkódolva van.

browser tömb részletei

- **accept**: Accept http fejléc értéke
- **agent**: User-Agent http fejléc érték
- **ip**: a böngésző forrás IP-je
- **java**: a böngésző támogatja-e a java appleteket; javascriptben: `navigator.javaEnabled()`
- **lang**: a böngésző nyelve; javascriptben: `navigator.language`
- **color**: a böngésző színmélysége; javascriptben: `screen.colorDepth`
- **height** = a böngésző képernyőjének magassága; javascriptben: `screen.height`
- **width** = a böngésző képernyőjének szélessége; javascriptben: `screen.width`
- **tz** = a böngésző időzónája; javascriptben: `new Date().getTimezoneOffset()`

JSON minta

```

{
  "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
  "agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36",
  "ip": "94.199.53.96",
  "java": false,
  "lang": "hu-HU",
}

```

```
"color":24,  
"height":1920,  
"width":1080,  
"tz":-120  
}
```

3.9.4 redirectUrl

Ha a **banki 3DS** ellenőrzés **sikertelen**, akkor az authorizáció még **nem** történik meg.

A kereskedői rendszernek fel kell készülnie arra, hogy a 3DS folyamat során a kártyakibocsátó bank megkövetelheti, hogy **CIT** tranzakció esetén a kártyabirtokos interaktívan azonosítsa magát (**challenge**). Az azonosításhoz a vásárló interakciójára van szükség. Ebben az esetben a **WEBSHOPFIZETESKETSZEREPLIS** hívás válaszában a SimplePay rendszere visszaad egy olyan URL-t (**redirectUrl**) a kereskedőnek, amire átirányíthatja a vásárlót.

Mivel a tranzakció során a vásárló jelen van (isType = CIT) így a kereskedőnek van lehetősége átirányítani a vásárlólót a kapott URL-re.

A fentiekből adódóan a kereskedői rendszernek fel kell készülnjön arra, hogy a **redirectUrl** mezőt fogadhassa a **WEBSHOPFIZETESKETSZEREPLIS** hívás szinkron válaszában.

3.9.5 challenge

Ha a kereskedői rendszer átirányítja a vásárlót a „**redirectUrl**” mezőben kapott URL-re, akkor egy olyan helyre jut, ahol a kártyakibocsátó bank által megkívánt további ügyféllenőrzési folyamat történik meg.

3.9.6 isBackUrl

A challenge folyamat böngészőben történik, aminek a végén a SimplePay rendszere visszairányítja a vásárlót a kereskedői weboldalra.

Annak érdekében, hogy a potenciális challenge folyamat végén megadható legyen, hogy hova kell a vásárlót visszairányítani a **WEBSHOPFIZETESKETSZEREPLIS** hívásban szükséges megadni az URL-t.

A **WEBSHOPFIZETESKETSZEREPLIS** hívásban ezért szükséges felvenni az **isBackUrl** mezőt is, annak érdekében, hogy a visszairányítás a kereskedői weboldalra megtörténhessen.

Ennek a mezőnek a tartalma megegyezik a háromszereplős fizetések **isBackUrl** mezőjével.

Az **isBackUrl** opcionális. Ha nincs küldve, akkor a challenge folyamat és az authorizáció végén a SimplePay oldalán történik meg a tranzakció eredményéről a tájékoztatás.

4 Elszámolások

A SimplePay rendszere az OTP Webshop esetén alkalmazott formátumokat és küldési útvonalakat is tudja szolgáltatni.

4.1 Tranzakciós analitika fájl formátum

Az alábbi OTP elszámolási formátumokat tudja jelenleg szolgáltatni a SimplePay rendszere.

- CSV D (HUF, EUR és USD elfogadás esetén)
- K01D (HUF elfogadás esetén)
- K04D (EUR és USD elfogadás esetén)
- K05D (HUF elfogadás esetén)

Ezeket túlmenően választható a SimplePay saját elszámoló fájl formátuma is (HUF, EUR és USD elfogadás esetén), aminek a mintája az alábbi elszámolásokkal kapcsolatos dokumentáció mellékleteként található meg.

Magyarul: <http://simplepartner.hu/download.php?target=merchantguidehu>

Angolul: <http://simplepartner.hu/download.php?target=merchantguideen>

4.2 Új CSV tranzakciós analitika formátum

2020 második félévben az OTP Bank egységesíteni fogja az elszámoló analitika formátumokat és csak egy, a fentiekől eltérő formátumban fogja az adatokat szolgáltatni. A SimplePay rendszere is fel lesz készítve az új analitika formátumra és a Bankkal párhuzamosan az új formátumban is képes lesz analitika fájlt generálni.

Ugyanakkor a SimplePay rendszerben a régi, fentebb felsorolt formátumok is meg fognak maradni. Azokban az esetekben, ahol a régebbi formátumokra van építve valamilyen kereskedő oldali üzleti logika, vagy automatizált adatfeldolgozás, ott továbbra is változatlan formában szolgáltatja a rendszer a tranzakciós adatokat.

4.3 Tranzakciós analitika küldési módja

Az analitika fájlokat az alábbi módokon tudja küldeni a SimplePay rendszere a kereskedő felé.

- e-mail

- OTP SFTP szerver (remote.otpbank.hu:17626 szerveren egy új mappába)
- SimplePay saját SFTP szerver
- Hypex

5 Tesztelés és élesítés

Mivel a migráció után a kereskedő a SimplePay rendszerében fog tranzakciókat indítani, így az éles rendszer igénybevétele a SimplePay élesítési szabályai alapján történik.

A tesztelési pontokból az alábbiak nem értelmezhetők az OTP Webshop esetén, így ezek tesztelése nem szükséges, vagy nem lehetséges.

- IPN fogadás
- oneclick fizetések és a cardSecret
- recurring fizetések esetén az egyedi tokenek

A kereskedői rendszer sikeres SimplePay oldali tesztjei után az éles rendszer is aktiválásra kerül.

5.1 Háromszereplős fizetések

A **háromszereplős** fizetések élesítés előtti tesztelési szabályai az alábbi SimplePay fejlesztői dokumentációnak a „**Tesztelés**” című fejezetében található meg.

Magyarul: <http://simplepartner.hu/download.php?target=v21dochu>

Angolul: <http://simplepartner.hu/download.php?target=v21docen>

5.2 Kétszereplős fizetések kártyaregisztráció esetére

A **kétszereplős** fizetések kártyaregisztráció esetén további teszteket igényelnek. Az élesítés előtti tesztelési szabályai az alábbi SimplePay fejlesztői dokumentációnak a „**Tesztelés**” című fejezetében található meg.

Magyarul: <http://simplepartner.hu/download.php?target=v21cardstoragedochu>

Angolul: <http://simplepartner.hu/download.php?target=v21cardstoragedocen>

5.3 Kétszereplős fizetések kártyaadatok küldésével

A kártyaadatok küldésével történő kétszereplős fizetések esetén az élesítés előtti tesztelési szabályai az alábbi SimplePay fejlesztői dokumentációnak a „**Tesztelés**” című fejezetében található meg.

Magyarul: <http://simplepartner.hu/download.php?target=v2autodochu>

Angolul: <http://simplepartner.hu/download.php?target=v2autodocen>

6 Ajánlott módosítások

Az OTP Webshop korábbi élesítési feltételeihez képest a SimplePay többlétszolgáltatásai, technikai lehetőségei, vagy a szabályozó környezet változásai miatt az alábbi pontokon ajánlott átgondolni a meglévő fizetési folyamatot.

6.1 Tranzakció azonosítók megjelenítése

Ahol nem látható a tranzakció azonosítója a vásárló számára, ott a vásárlói megkeresések gördülékenyebb kezelése érdekében ajánlott ezt megjelenítve.

6.2 Tájékoztatások megjelenítése

Azoknál a kereskedői rendszereknél, ahol a sikertelen és a megszakított fizetések esetén nincs tájékoztatás a fizetés kimenetéről ajánlott vásárlói tájékoztatást megjeleníteni.

A háromszereplős fizetés alábbi dokumentációjában „**A tranzakció eredményétől függő tájékoztatások**” fejezetben található erről információ.

Magyarul: <http://simplepartner.hu/download.php?target=v21dochu>

Angolul: <http://simplepartner.hu/download.php?target=v21docen>

6.3 Adattovábbítási nyilatkozat elfogadtatása

Vásárlói személyes adat átadása előtt a vásárlóval el kell fogadtatni az adattovábbítási nyilatkozatot. Jelenleg ez ajánlott, azonban a 2020 szeptember 30-án életbe lépő erős ügyfélhitelesítés alkalmazásával adatátadás esetén kötelező lesz.

A nyilatkozat elhelyezése és szövege az „**Adattovábbítási nyilatkozat**” fejezetben található meg a háromszereplős fizetés dokumentációjában.

Magyarul: <http://simplepartner.hu/download.php?target=v21dochu>

Angolul: <http://simplepartner.hu/download.php?target=v21docen>

6.4 Kártyatárolási nyilatkozat elfogadtatása

A kártyaregisztrációs tranzakció előtt a vásárlót tájékoztatni kell, ami során a vásárlónak a kártya regisztrációról szóló nyilatkozatot kifejezetten el kell fogadja. Ez a nyilatkozat nem helyettesíti az adattovábbítási nyilatkozatot, hanem azt kiegészíti a kártyaregisztrációs tranzakció esetén.

A dokumentáció az alábbi URL-en érhető el:

Magyarul: <http://simplepartner.hu/download.php?target=v21cardstoragedochu>

Angolul: <http://simplepartner.hu/download.php?target=v21cardstorage docen>

Oneclick tranzakciók esetére a „**Oneclick kártya regisztrációs nyilatkozat**” fejezetben található meg a nyilatkozat.

Recurring tranzakciók esetére a „**Recurring kártyaregisztrációs nyilatkozat**” fejezetben található meg a nyilatkozat.

6.5 Fizetés mobil eszközön

Abban az esetben, ha a fizetés mobil applikációban webview használatával van megvalósítva ajánlott az alábbi dokumentáció **1. sz. melléklet** javaslatait figyelembe venni.

Az itt leírtak a Google és Facebook által biztonsági okokból letiltott, bizonyos (régebbi) webview komponenseken keresztül social login kérdését tárgyalják.

Ugyanakkor számos további problémának is kiinduló oka lehet az elavult komponens, emiatt ajánlott a mellékletben leírt más komponensek használata.

Magyarul: <http://simplepartner.hu/download.php?target=v21dochu>

Angolul: <http://simplepartner.hu/download.php?target=v21docen>

7 SimplePay API v2

A migráció megvalósítható a SimplePay API v2 használatával is.

Eben az esetben a kereskedő technikailag nem az OTP Webshop interface használatával fog tranzakciókat indítani a SimplePay rendszerében, hanem a SimplePay saját API-ja segítségével. Ennek előnye, hogy a közeljövőben életbelépő PSD2 előírásainak, valamint az aktuális kártyatársasági szabályoknak, illetve a PCI-DSS által támasztott minden követelménynek megfelel.

Ezzel ellentétesen az OTP Bank Webshop szolgáltatásán további fejlesztések nem lesznek végezve, így technikailag és szolgáltatásaiban is a jelenlegi szinten fog üzemelni.

A SimplePay API v2 összes dokumentációja és mintakódja az első fejezetben található címen érhető el.

7.1 OTP rendszerében korábban regisztrált kártyák terhelése API v2 használatával

Az OTP VPOS szolgáltatásában korábban elmentett kártyák felhasználhatók a API v2-vel is.

A technikai megvalósításról az alábbi dokumentáció „**OTP Webshop szolgáltatásban tárolt kártyák terhelése**” című fejezetben található meg.

Ilyen esetben a SimplePay admin rendszerében **össze kell kötni** a kereskedő **aktuális SimplePay** fiókját a kereskedő **korábbi OTP VPOS** szolgáltatásával. Ennek során válik aktívvá az átjárás a két szolgáltatás között és lesz elérhető a jelenlegi rendszerben a korábban tárolt kártya. Annak érdekében, hogy ez megtörténjen már a szerződés megkötésekor jelezze ezirányú igényét!

Ez a megoldás a **sandboxon nem tesztelhető**, mert kell hozzá egy már létező, valós OTP bankos kártyaregisztráció, ami csak az éles rendszerükön keresztül érhető el.

Magyarul: <http://simplepartner.hu/download.php?target=v21cardstorage dochu>

Angolul: <http://simplepartner.hu/download.php?target=v21cardstorage docen>

8 Támogatás

További információért, technikai támogatásért kérjük lépjen kapcsolatba velünk az itsupport@otpmobil.com címen.

Kérjük, a gyorsabb ügyintézés végett minden esetben írja meg nekünk azt az adatot, ami alapján be tudjuk azonosítani a problémát, vagy a kérdését.

Tranzakció

Tranzakcióval kapcsolatos kérdés esetén a fizetés **SimplePay** azonosítóját adja meg nekünk. Az azonosító kilenc számjegyű.

Kereskedői fiók

Kereskedői technikai beállításokkal kapcsolatban a SimplePay rendszeren belüli kereskedői fiók azonosítót. Az azonosító a fiók MERCHANT értéke.

Fizetési rendszer

Melyik rendszerrel kapcsolatos a kérdése. A **sandbox rendszer** csak tesztek esetén, az **éles rendszer** a valós fizetési tranzakciók esetén.

Élesítés

Élesítési tesztek esetén kérjük, hogy írja meg nekünk az itsupport@otpmobil.com címre, hogy

- melyik szerződött domain névhez készült a tesztelhető fizetés
- melyik fiókot használják (MERCHANT)
- hol érjük el a tesztelhető rendszert

9 Mellékletek

I. EMV 3D Secure

Az Európai Unió, illetve a tagországi törvényhozó és felügyeleti szervek, a vonatkozó Európai Uniósi direktíva (Az Európai Parlament és a Tanács 2015. november 25-i (EU) 2015/2366 irányelve; **PSD2**), illetve ennek tagországi jogszabályi adaptálásalapján ún. kötelező erős ügyfél hitelesítés alkalmazását (**Strong Customer Authentication - SCA**) írják elő, **2019. szeptember 14-i** hatályba lépéssel, minden Európai Gazdasági Térségen belül kibocsátott készpénz-helyettesítő fizetőeszköz elfogadás során.

Az MNB a piaci szereplőkkel történt egyeztetések hatására 12 hónapos meghosszabbított átállási időszakot biztosít a hazai szereplők részére a fenti dátumhoz képest, így az új határidő 2020 szeptember 30.

Hazai jogszabályi háttér

Az Európai Parlament és a Tanács 2015. november 25-i (EU) 2015/2366 irányelve az alábbi jogszabályokba került adaptálásra:

- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
- 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról
- 2013. évi CCXXXV. törvény az egyes fizetési szolgáltatókról

A PSD2-es módosításokat tartalmazza többek között a 2017. évi 184. Magyar Közlönyben szereplő 2017. évi CXLV. salátatörvény is, továbbá az Európai Bizottság 2018/389 felhatalmazáson alapuló rendelete.

A bankkártya elfogadás tekintetében a szabályozás kiterjed az internetes (ügynevezett VPOS) elfogadásra is. A PSD2 megfelelés értelmében és az internetes kártyaelfogadás biztonságosabbá tétele érdekében, 2020. szeptember 14-ig be kell vezetni és teljeskörűen meg kell valósítani a kártyabirtokos fokozott biztonságú ellenőrzését, az ügynevezett EMV 3D Secure 2.0 szolgáltatást.

3D Secure a gyakorlatban

A renDELETEH kapcsolódó technológia bevezetését teljes mértékben elvégzi az OTP Mobil Kft. Abban az esetben, **ha jelen dokumentáció alapján** ún. háromszereplős módon **van igénybe véve a bankkártyás fizetés**, tehát a kereskedői rendszer nem használ kártyatárolásra épülő extra szolgáltatási elemeket, **akkor a kereskedőnek ezzel kapcsolatban nincs további teendője**.

A 3D Secure megvalósulásához ugyanakkor elengedhetetlen a kereskedői rendszerből történő, az EMV 3D Secure 2.0 szabvány által előírt adatok szolgáltatása. A kereskedői rendszernek ehhez jelen dokumentációban a „start” hívás leírásában megjelölt adatokkal szükséges minden elindított tranzakciót paraméterezni.

Az EMV 3D Secure szabvány követelményéről az alábbi linken tájékozódhat:

<https://www.emvco.com/emv-technologies/3d-secure/>

Mi az EMV 3D Secure 2.0 szolgáltatás és miért van szükség rá?

Az utóbbi években széles körben elterjedtek az elektronikus úton történő, kényelmes, akár mobil eszközről kezdeményezett internetes vásárlások. Ezzel együtt megnőtt a csalások, a számítógépes vagy internetes visszaélések, az adatlopások száma és volumene is.

A bankkártyás fizetések biztonságos és megbízható lebonyolítása érdekében nemcsak a szabályozó szervek, hanem a kártyatársaságok és a bankok is folyamatosan dolgoznak újabb, hatékonyabb megoldásokon. Az internetes vásárlásoknál jelenleg is működő 3D Secure 1.0 a böngészőből indított internetes vásárlások során teszi lehetővé a fizető fél azonosítását. Ez a lehetőség okos eszközről indított vásárlás esetén nem elérhető, mobiltelefonról pedig csak abban az esetben érhető el, ha böngészőn keresztül (nem alkalmazásból) történik a fizetés kezdeményezése.

Az EMV 3D Secure 2.0 egy még biztonságosabb ügyfél hitelesítést tesz lehetővé, és alkalmazható nemcsak a böngésző által vezérelt felületekről indított vásárláskor, hanem az alkalmazásokon belüli (in app) vásárlások, mobiltelefonon és más okos eszközökön bonyolított fizetések során. Az EMV 3D Secure 2.0 olyan ügyfélhitelesítésre alkalmas azonosítási módszerekre támaszkodik, mint a biometria (pl. ujjlenyomatok vagy arcfelismerés), vagy egyszeri jelszavak. A tranzakció során a jelenleginél több adat kerül átadásra a kibocsátó bankok felé, ezzel téve lehetővé az ügyfél megalapozottabb minősítését, az esetleges csalások és visszaélések gyors és hatékony kiszűrését.

Milyen technikai felkészülést igényel a 3D Secure 2.0 bevezetése?

A jogszabály értelmében a 3D Secure 2.0 során az Európai Gazdasági Térségen belül kibocsátott bankkártyákkal az Európai Gazdasági Térségen belül működő elfogadóhelyen végrehajtott tranzakcióknál a kártyabirtokost –néhány kivételtől eltekintve– erős ügyfél hitelesítéssel kell azonosítani. A megfelelő hitelesítés érdekében mind a kibocsátó banknak, mind az elfogadó banknak (vagy az elfogadónak) rendelkeznie kell 3D Secure megoldással (a 3D Secure 1.0-ban az elfogadói megoldás MPI vagy Merchant Plug-in-ként ismert), amely segítségével a vásárlást kezdeményező fél azonosítható.

A jelen dokumentáció alapján fejlesztett és üzemeltetett internetes kártyaelfogadási folyamat a standard háromszereplős modell, amely azt jelenti, hogy az internetes vásárlások során a kártyabirtokos a webáruházi felületről átirányításra kerül az OTP Mobil Kft. által biztosított SimplePay internetes felületre. Ezen a fizetőoldalon adja meg a szükséges kártyaadatokat, a tranzakció ezen a felületen megy végbe, majd ezt követően a vásárló visszairányításra kerül a webshopba.

Ezen fizetési mód alkalmazásakor a bankkártya adatok biztonságos kezeléséért és a továbbításáért (a fizetőfelület és a bank között) a bank felel. Kereskedői oldalon ezzel nincs technikai teendő, ha a 3D Secure folyamathoz szükséges vásárlási adatokat küldi a kereskedő.