



Kereskedői kézikönyv

KERESKEDŐI RENDSZER Referencia kézikönyv „redirect” (átirányítás) fejlesztéshez

Verzió 2.6.1

2022. január

1. Általános információk

1.1 Összegzés

1.	Általános információk.....	2
1.1	Összegzés.....	2
1.2	Sémák táblázata.....	3
1.3	Képek táblázata	3
1.4	Verziók	3
1.5	Szójegyzék.....	4
2	Bevezetés	6
3	Back office SIA VPOS	7
3.1	E-mail üzenetek	7
4	SIA VPOS átirányítás (redirect) integráció.....	8
4.1	Bevezetés és beállítás	8
4.1.1	A logó küldése	9
4.1.2	E-mail üzenetek.....	9
4.2	HTTP üzenetek.....	10
4.2.1	SIA VPOS átirányítás fizetés kezdeményezés	10
4.2.2	Az OPTIONS mező	18
4.2.3	A teljesített fizetés visszaigazolása/eredménye	20
4.2.4	SIA VPOS fizetés átirányítása token kezdeményezéssel	27
5	SIA VPOS Függelékek.....	28
5.1	Hivatkozások	28
5.2	MAC átirányítás (redirect) generálása	29
5.2.1	A MAC generálása REDIRECT üzenetekhez	29
5.2.2	MAC generálása az eredményüzenetek számára	32
5.2.3	A MAC generálása a REDIRECT számára token üzenetekkel	34
5.3	Paraméterek AUTHORMODE, ACCOUNTINGMODE.....	35
5.3.1	AUTHORMODE.....	35
5.3.2	ACCOUNTINGMODE	35
5.4	3DSDData (átirányítás - redirect).....	37
5.5	Kiválasztott API-k használata.....	45

1.2 Sémák táblázata

1.3 Képek táblázata

1.4 Verziók

Dátum	Változtatások	Változat
2021-11-23	<ul style="list-style-type: none">- minden vpos és sia hivatkozás frissítve SIA VPOS-ra.- hozzáadva a TICKLERPLAN opcionális paraméter a 4.2.1, 4.2.4, 5.2.1 és 5.2.3- mentességek a 3DS2 esetében: az OPTION A és a TEnn bevezetése a 4.2.2 és a 4.2.3.- Masterpass hivatkozások eltávolítva a 4.2.1 és a 4.2.3- 4.2.3 és 5.2.2: a MASKEDPAN felülvizsgálata SVAT szolgáltatással; új mezők hozzáadva: INSTALLMENTSNUMBER, CARDHOLDERDATA, THREEDSRESULT, SUBSCRIPTIONCODE.- 4.2.1 és 4.2.4: bevezetve az SVAO és a kötelező e-mailek eltávolítása.- 4.2.1 és 4.2.4: Szerb cirill (SC), albán (AL) és magyar (HU) nyelvek hozzáadva.- 4.2.4: megjegyzéssel egészült ki, hogy a NETWORK 98 a leggyakrabban használt érték.- 5.4: recurringExpiry és recurringFrequency hozzáadása a 3DSData csomag opcionális mezőjéhez- 4.2.1 és 4.2.4: a PRODUCTREF mérete 50 karakterre növelve.- 4.2.1 és 4.2.4: további részleteket adott az URLMSHEADER megszorításokhoz.- 5.2.1: hozzáadott egy mintát a HMAC-számításból	2.5.0
2022-01-17	<ul style="list-style-type: none">- Migráció a Nexi sablonra és a dokumentum elrendezésének általános felülvizsgálata.- 4.1.1: frissítettük azon e-mailek listáját, amelyekre a logót el kell küldeni.	2.6.0

	<ul style="list-style-type: none"> - 4.1 és 4.2.2: megjegyzéssel egészítettük ki, az iframe használatának mellőzését javasoljuk az átirányítási integrációban. - 4.2.1: további korlátozások az ORDERID mezőben a mybank fizetéseknél. - Diners séma mindenhonann eltávolítva. - 4.2.1 és 4.2.4: URLMSHEADER mezőkorlátozás frissítve 	
2023-01-20	Adja hozzá az 5.5 fejezetet. - Kiválasztott API-k használata	2.6.1

1.5 Szójegyzék

Back office	Ez egy SIA VPOS webalkalmazás, amellyel a kereskedők hozzáférhetnek statisztikákhoz, jelentésekhez, listákhoz, vagy jogosult rendeléseket hajthatnak végre (rögzítés, visszatérítés), vagy új engedélyeket kérhetnek.
CC	Bankkártya
Foglalás	Egy korábban engedélyezett tranzakció számviteli hatásait létrehozó tranzakció
Visszatérítés	Számviteli tranzakció pénzösszeg ügyfélnek történő visszafizetésére (Credit-nek is nevezik)
GET	HTTP protokoll-on történő kommunikációs tranzakció
Hash	N darab bit (pl. 128, 160), amelyet egy karakterláncból egy matematikai eljárással kapunk meg oly módon, hogy különböző karakterláncból mindig más eredményt kapunk
HTTP	Weboldalak továbbítására használt alkalmazási protokoll.
MAC	Üzenet hitelesítési kód
Kereskedelmi rendszer	Virtuális üzletkezelő szoftverrendszer. Virtuális bolt
POST	HTTP protokoll-on történő kommunikációs tranzakció
SHA-256	Biztonságos hash algoritmus hash generálásához. Szabványos FIPS 180-2
SSL	A Netscape Communication által létrehozott Secure Socket Layer szabványos szállítási protokoll
Visszatérítés	Tranzakció a megadott felhatalmazás törlésére az összeg kártyabirtokos részére történő visszafizetésével
URL	Univerzális erőforrás-kereső
VBV	Visa Secure, korábban Verified by Visa: Visa biztonsági rendszer a hitelkártya-tulajdonosok online vásárlásaik során történő hitelesítésére

SecureCode	MasterCard ID Check, korábban SecureCode: Mastercard és Maestro biztonsági rendszer a hitelkártya-tulajdonosok hitelesítésére az online vásárlások során
SafeKey	Biztonsági rendszer az AMEX hitelkártya-tulajdonosok online vásárlásaik során történő hitelesítésére (egyenértékű a VBV-vel)

2 Bevezetés

Ez a dokumentum fontos technikai információkat tartalmaz azon virtuális üzletek tervezői számára, akik integrálni szeretnék webhelyüket a SIA VPOS szolgáltatással. Ez a kézikönyv ezért szigorúan a műszaki személyzetnek szól. Nem tartalmazza a SIA VPOS szolgáltatás tényleges leírását, amit a megfelelő dokumentumok biztosítanak.

Ez a dokumentum az **átirányítás leírását tartalmazza** a SIA **VPOS** rendszer és az ehhez kapcsolódó kereskedői oldali rendeléskezelő rendszerekkel való integráció lehetőségét. Az **API internetes felületéhez** lásd a kapcsolódó útmutatót.

A SIA VPOS egy internetes virtuális POS, amelyet közvetlenül az eladók kapnak. Lehetővé teszi a kereskedők számára, hogy bankkártyájukkal online tranzakciókat hajtsanak végre számítógép és internetkapcsolat segítségével. A rendszer egyaránt használható a hagyományos POS fizikai „dobozának” helyettesítésére és a hitelkártya-tranzakciók testre szabható átjárójaként. Funkcióinak általános leírását lásd a kapcsolódó dokumentumban.

A SIA VPOS szolgáltatást egy back office grafikus felület funkcionalitásai egészítik ki.

Ami az internetes kommunikációs útvonal biztonságát illeti, a kínált megbízhatóság mértéke megegyezik a 256 bites titkosítású TLS 1.2 protokolléval.

Az API-integrációval kapcsolatban lásd: „Kereskedői integráció - VPOS API”.

3 Back office SIA VPOS

Ez egy SIA VPOS webes alkalmazás, amellyel a kereskedők böngészőn keresztül hozzáférhetnek statisztikákhoz, jelentésekhez, listákhoz, vagy jogosult rendeléseket hajthatnak végre (rögzítés, visszatérítés), vagy új engedélyeket kérhetnek.

3.1 E-mail üzenetek

Az üzletek üzemeltetői által a BackOffice grafikus felületen keresztül végrehajtott fizetési tranzakciók során a SIA VPOS szerver számos e-mailt generálhat és küldhet a vásárlónak és a kereskedőnek.

Az e-mail üzenetek nem szabhatók testre. A rendszer nem küld e-maileket, ha a kéréseket az API használatával küldik. Az átirányításból történő e-mailek küldéséhez lásd az Átirányítás fejezet megfelelő bekezdését.

Csak akkor küldjük el az e-mailt az ügyfélnek, ha a felhatalmazás kérésekor ez a mező be van írva az engedélyezési kérelem képernyőn.

Az e-mailt minden alkalommal elküldik az üzemeltetőnek. A használt cím az engedélyezési kérelem képernyőn kötelezően megadott cím.

Az e-mailek tartalma, ha vannak, a következő lesz:

- Összeg
- Bolt azonosító
- Rendelésszám
- Engedély szám
- Kártya típus
- A tranzakció dátuma és időpontja

4 SIA VPOS átirányítás (redirect) integráció

4.1 Bevezetés és beállítás

A kereskedői virtuális áruház és a SIA VPOS rendszer közötti kommunikáció egyszerű HTTP üzenetek segítségével történik. Miután a végfelhasználó befejezte a vásárlás fázist a kereskedői áruházban a megvásárolni kívánt áruk vagy szolgáltatások kiválasztásával, a virtuális áruház átirányítja a böngészőt a SIA VPOS rendszerére. A böngésző átirányítható úrlapon, hivatkozásokon vagy hiteles HTTP-átirányításon keresztül. Amikor a böngésző átirányításra kerül, egy sor paraméter kerül bevitelre, amely lehetővé teszi a SIA VPOS rendszer számára, hogy felismerje a kérés eredetét, és előkészítse mindazt, ami szükséges ahhoz, hogy az ügyfél elvégezhesse a fizetési tranzakciót. Ebben a szakaszban a kártyabirtokosnak egy egyszerű űrlapot kell kitöltenie, amely tartalmazza a bankkártya adatait, a kártya típusát (az üzlet által elfogadottak közül), e-mail címét stb. A felhasználó minden esetben lemondhatja a tranzakciót és visszatérhet a vásárláshoz.

A művelet elvégzése után a kártyabirtokos a teljesített fizetés igazolásához szükséges adatokkal „visszaküldésre kerül” az eredeti weboldalra, és ezzel egyidejűleg a SIA VPOS rendszer HTTP-n keresztül értesíti az áruházat.

Annak érdekében, hogy a felhasználó böngészője átirányítható legyen a virtuális áruház megfelelő oldalaira, három speciális mező megadására van szükség a SIA VPOS rendszernek küldött első üzenetben, amely három URL-t tartalmaz:

- Az az URL, amelyre a felhasználót el kell küldeni, ha a fizetési folyamatot megszakítják, és visszatérnek a kosár módosítása oldalra (URLBACK).
- Az az URL, amelyre a felhasználót el kell küldeni a tranzakció sikeres befejezése esetén (URLDONE).
- A SIA VPOS rendszer által használandó URL, amelyen keresztül értesíti az áruházat a befejezett tranzakció eredményéről (URLMS).

Az UTF-8 szabványos szolgáltatáshoz való hozzáférés URL-címei a következők:

- TESZT környezet: <https://virtualposttest.sia.eu/vpos/payments/main?PAGE=LAND>
- ÉLES környezet: <https://virtualpos.sia.eu/vpos/payments/main?PAGE=LAND>

Az UTF-8 token szolgáltatással történő fizetéshez való hozzáférés URL-címei a következők:

- TESZT környezet: <https://virtualposttest.sia.eu/vpos/payments/main?PAGE=TOKEN>
- ÉLES környezet: <https://virtualpos.sia.eu/vpos/payments/main?PAGE=TOKEN>

MEGJEGYZÉS: A felhasználó átirányítása a SIA VPOS fizetési oldalra egy iframe kereten belül nem ajánlott.

4.1.1 A logó küldése

Az üzemeltető személyre szabhatja a grafikus fizetési felületet úgy, hogy kéri logójának vagy márkájának feltüntetését a megrendelés összefoglaló információinak szánt helyre.

A képet e-mailben kell elküldeni a kereskedő országától vagy hivatkozó bankjától függő címre:

- serviziopos@sia.eu (olasz kereskedők)
- ecommerce@otpsrbija.rs (OTP Szerbia kereskedők)
- ecommerce@unicreditgroup.rs (UniCredit Szerbia kereskedők)
- Kartat@bankacredins.com (Credins Albánia kereskedők)
- elfogadas.budapestkartya@unicreditgroup.hu (UniCredit Magyarország kereskedők)
- SIAGRMA_POS@sia.eu (SIA Görögország kereskedők).

A kép megadható GIF, JPG vagy PNG formátumban, nem lehet nagyobb 140x140 képpontnál, és mérete nem haladhatja meg a 100 Kb-ot.

4.1.2 E-mail üzenetek

Amikor egy ügyfél fizetési tranzakciót hajt végre, a SIA VPOS szerver számos e-mailt generálhat és küldhet az ügyfélnek és a kereskedőnek.

Az e-mailek kereskedőhöz történő továbbítása az alábbi lehetőségek valamelyikével konfigurálható, amikor az üzlet előfizet a szolgáltatásra:

1. Soha
2. Mindig
3. Csak pozitív eredmény esetén

Az e-mail cím megváltozása esetén a kereskedő köteles közölni az új címét a SIA VPOS felé.

Az ügyfélnek küldött e-mailek viszont mindig az alábbi két esetben kerülnek kiküldésre:

1. Online felhatalmazás megadva → Sikeres online tranzakció E-mail
2. Online engedélyezés megtagadva → Elutasított online tranzakció E-mail (az elutasítás indoklásával)

Az e-mail üzenetben található információk szabványos, vagy XML formátumúak lehetnek.

Szabványos formátum esetén a tartalom, ha van, a következő lesz:

- A tranzakció dátuma
- Rendelésszám
- Összeg
- Engedély szám
- Üzlet azonosító

Az XML formátum viszont szigorúan a kereskedőnek küldött e-mailekhez szükséges, és megfelel a SIA VPOS API-k Authorization elemének. Az ilyen formátumú e-mailek tárgya a következő lesz: „Engedélyezés: rendelési szám <OrderID>”

A SIA VPOS által küldött üzenetek nem testre szabhatók ¹. A feladó email címe vpos@sia.eu.

¹Az elfogadó bank szintjén testre szabható.

4.2 HTTP üzenetek

4.2.1 SIA VPOS átirányítás fizetés kezdeményezés

Az első lépés, amelyet a kereskedőnek meg kell tennie, az, hogy az ügyfél böngészője fizetési folyamatot indító üzenetet generáljon a SIA VPOS számára. Ez történhet átirányításon vagy hivatkozáson keresztül (HTTP GET módszerrel), vagy rejtett mezőket tartalmazó űrlap elküldésével (amely használhatja a HTTP POST módszert).

A felhasználó böngészője által a SIA VPOS részére küldött fizetési tranzakciót kezdeményező üzenetnek a következő mezőket kell tartalmaznia:

Név	Kötelező	Leírás
AMOUNT	I	A legkisebb pénznemben kifejezett összeg (fillér, cent). Minimális hossz 1, maximális hossz 8. Az ASI-kártya-ellenőrzési tranzakciónál az összeget 0-ra KELL állítani. Valós tranzakciók esetén az összegnek legalább a kereskedő elfogadója által támogatott minimális összegnek kell lennie (általában 10 Ft).
CURRENCY	I	Pénznem: 3 számjegyű ISO 4127 kód (például forint: 348, euró: 978).
ORDERID	I	Rendelés egyedi azonosítója: ennek legfeljebb 50 karakter hosszúságú alfanumerikus kódnak kell lennie. Egyedi jellegére legalább 5 év garanciát kell vállalni. A megengedett karakterek lehetnek betűk, számok, „-” és „_”. (Az [a-zA-Z0-9_-] reguláris kifejezés kerül alkalmazásra.)
SHOPID	I	A kereskedő üzletének SIA VPOS által kijelölt azonosítója.
URLBACK	I	Teljes URL, amelyre a felhasználót át kell irányítani (ez minden szükséges paramétert tartalmazhat), ha a fizetési folyamat megszakad. Maximális hossza 254 karakter.
URLDONE	I	Teljes URL, amelyre az ügyfél böngészőjét át kell irányítani a tranzakció sikeres befejezése után (az összes szükséges paramétert tartalmazhatja). Az eredményparaméterek hozzá lesznek fűzve a kiválasztott URL-hez. Maximális hossza 254 karakter.

Név	Kötelező	Leírás
URLMS	I	Annak a kereskedői rendszernek az URL-címe, amelyhez a SIA VPOS a teljesített fizetést megerősítő GET-et vagy POST-ot végrehajtja (ez az üzlet által beállított bármely paramétert tartalmazhat). Az eredményparaméterek hozzá lesznek fűzve a kiválasztott URL-hez. Maximum hossza 400 karakter.
URLMSHEADER	N	Az urlms fejlécéhez hozzáadandó paraméterek listája, ha a kereskedő kéri. A megengedett karakterek közé tartoznak a betűk, számok, szóközök és néhány speciális karakter. (A teljes alkalmazott reguláris kifejezés a következő: [a-zA-Z0-9\.\-_\=,;/@%()&];.) Maximális hossza 2000 karakter.
ACCOUNTINGMODE	I	A megrendeléshez használandó foglalás típusa, értéke: <ul style="list-style-type: none"> • D (halasztott) • I (azonnali) Lásd még az 5.3.2.
AUTHORMODE	I	A megrendeléshez használandó engedély típusa, értéke: <ul style="list-style-type: none"> • D (halasztott) • I (azonnali) Hacsak nincsenek különleges esetek, mindig I értéket adjunk meg. Lásd még az 5.3.1.
MAC	I	Üzenet hitelesítési kód: megakadályozza, hogy a végfelhasználó módosítsa a rendelési adatokat. A kapcsolódó számítást lásd az 5.2.1.
LANG	N	Az a nyelv, amelyen a végfelhasználóval való interakcióhoz szükséges üzeneteket meg kell jeleníteni. Ez a mező nem kötelező; az alapértelmezett nyelv az angol. Jelenleg a következők állnak rendelkezésre: AL albán EL hellén EN Angol HU magyar

Név	Kötelező	Leírás
		IT vagy ITA olasz SC szerb cirill SK szlovák SR szerb
SHOPEMAIL	N	Azt az e-mail címet tartalmazza, amelyre a tranzakció eredményeit el kell küldeni. Ha nincs megadva, akkor az áruház konfigurációs adataiban szereplő kerül felhasználásra. Minimális hossz 7 alfanumerikus karakter, maximális hossz 50.
OPTIONS	N	Tartalmazza a fizetéshez aktiválandó további opciókat. Az opciók megjelenési sorrendje nem releváns. A mező tartalma nem érzékeny a kis- és nagybetűkre. További részletekért lásd a megfelelő bekezdéseket.
LOCKCARD	N	Opcionális mező az elérhető fizetési módok és sémák listájának korlátozásához. Tartalmazhatja a fizetési eszköz típusának megfelelő hálózati kódot, amellyel a kereskedő a fizetést választotta. Ennek a paraméternek a lehetséges értékei a következők: 01 – VISA 02 – Mastercard 03 – Dina 04 – Maestro 06 – American Express 08 – JCB 80 – IBAN 81 – AmazonPay 82 – EnelX 84 – Satispay 89 – ApplePay 91 – BancomatPay (Jiffy) 92 – Paga con Postepay 94 – Postepay

Név	Kötelező	Leírás
		<p>96 – MyBank</p> <p>97 – Paypal</p> <p>A1 – Google Pay™</p> <p>CC – Bankkártyák</p> <p>NC – Egyéb fizetési eszközök</p> <p>Vegye figyelembe, hogy egyes fizetési módok vagy sémák bizonyos országokban korlátozottak.</p> <p>Ha a jelzett érték egy bankkártya kód (01, 02, 03, 04, 06, 07 vagy 08), a felhasználó a fizető oldalra kerül, ahol a mezők előre kiválasztottak és nem módosíthatók.</p> <p>A 97 – Paypal esetén a felhasználó automatikusan átirányításra kerül a kapcsolódó fizetési eszköz bejelentkezési oldalára, anélkül, hogy megjelenítené az eszközválasztó oldalt.</p> <p>A 80 – IBAN, 81 – AmazonPay, 82 – EnelX, 84 – Satispay, 89 – ApplePay, 96 – MyBank és A1 – Google Pay™ esetén a fizetési oldal csak a választott fizetési módra aktiválódik.</p> <p>A 92 – Paga con Postepay esetében a felhasználó automatikusan a Postepay fizetési rendszerbe kerül.</p> <p>A 91 – BancomatPay esetében csak akkor indul el automatikusan a BPay tranzakció, ha a PHONENUMBER mezőhöz értéket rendeltek. Ellenkező esetben a felhasználó a fizetőoldalra kerül, hogy megadhassa telefonszámát.</p> <p>CC esetén a fizetési eszköz választó oldalon csak a kiválasztandó bankkártyák jelennek meg.</p> <p>NC esetén a fizetési eszköz kiválasztási oldal csak a kiválasztandó bankkártyákon kívüli eseteket tartalmazza. Ha hiba történik a fizetési folyamat során, a felhasználó az URLBACK oldalra kerül átirányításra.</p>
EMAIL	N	<p>Ügyfél e-mail címe.</p> <p>Minimális hossz 7 alfanumerikus karakter, maximális hossz 50.</p> <p>Ha az e-mail nem szerepel a hívásban, akkor azt a fizetési oldalon kéri a felhasználótól. A mező kitöltése kötelező, kivéve, ha az üzletben engedélyezték a SVAO szolgáltatást.</p>

Név	Kötelező	Leírás
ORDDESCR	N	A megrendelés leírása (lásd: OPTIONS: O, vagy V). Maximális hossza 140.
VSID	N	Érvényesítési szolgáltatás azonosítója MyBank tranzakciókhoz. Ha megadásra kerül, a MyBank bankválasztó oldal kimarad, és a felhasználót átirányítja a kapott azonosítóhoz társított home banking szolgáltatásra. Maximális hossza 35.
OPDESCR	N	További opcionális leírás a rögzítési művelethez azonnali foglalás esetén (a halasztottnál nem használt). A mező nem kapcsolódik a megrendeléshez. Lásd helyette ORDDESCR. Maximális hossza 100.
REMAININGDURATION	N	A hitelkártya érvényességének minimális időtartama hónapokban (OPTIONS D esetén).
USERID	N	Felhasználói azonosító. Alfanumerikus, legfeljebb 255 karakter hosszúságú.
PHONENUMBER	N	Telefonszám a BancomatPay rendszeren történő fizetéshez
CAUSATION	N	A BancomatPay rendszeren történő fizetés oka
USER	N	Felhasználó a BancomatPay rendszeren keresztüli fizetésekhez
NAME	N	Ügyfél keresztnéve (csak OPTIONS B esetén)
SURNAME	N	Ügyfél vezetéknéve (csak OPTIONS B esetén)
TAXID	N	Ügyfél adóazonosítója
PRODUCTREF	N	Eladási azonosító Maximális hossz 50.
ANTIFRAUD	N	A csalás elleni ellenőrzésekhez használt további információkat tartalmazó adatok. A mező kitöltése kötelező, ha az SV69 aktív.
3DSDATA	N	A 3D secure 2.0-hoz használt további információkat tartalmazó 3DS adatok.

Név	Kötelező	Leírás
TRECURR	N	Az ismétlődő fizetés típusa. Kötelező ismétlődő fizetés első tranzakciója esetén vagy OPTIONS M esetén (ha az SVA4 nem aktív). Az elfogadott értékek a következők: R – Ütemezett ismétlődő tranzakció első meghívása U – Nem ütemezett ismétlődő tranzakció első meghívása C – File-ban tárolt kártya (pan alias/token) értesítés Engedélyezés esetén az eredményüzenetben a CRECURR visszaküldésre kerül a kereskedőnek, hogy a következő ismétlődő fizetésekhöz fel tudja használni.
INSTALLMENTSNUMBER	N	Részletfizetések száma. Érték 0 és 99 között.
TICKLERPLAN	N	A kapcsolódó tickler-terv azonosítója (csak akkor érhető el, ha a kereskedő számára engedélyezve van a SVAR szolgáltatással történő tickler elérés).

Kötelező: I = igen, N = nem

Kiválasztott Kötelező = N darab elem regionális felhasználástól függ, további részletekért forduljon a Bankhoz.

Kérjük, vegye figyelembe: 3DSDATA mező, ha van, nagyon nagy lehet. Emiatt nem lesz többé lehetséges a http GET metódus használata az URL-ben szereplő paraméterek átadására a SIA VPOS rendszernek. A kereskedő webhelyről a SIA VPOS fizetési átjáróra történő átirányítást a POST http módszerrel kell végrehajtani, rejtett űrlap beküldésével.

Megjegyzés: a fenti táblázatokban szereplő mezők nevei mind nagybetűvel vannak írva, és kis- és nagybetű érzékeny.

A kezdeményező üzenetben a mezők megjelenési sorrendje tetszőleges.

A kereskedő és a SIA VPOS közötti kommunikációs folyamatban fennáll annak a veszélye, hogy egy idegen fél az üzenet lehallgatását követően megkísérli megváltoztatni annak tartalmát, majd később továbbítani a módosított üzenetet a végső címzettnek. Ezt az incidenst csak egy hitelesítési eljárással lehet megakadályozni, amely minden üzenethez egy MAC-et (üzenet hitelesítési kód) rendel.

A MAC generálására alkalmazott módszer a következő: a HMAC-SHA256 hash² kiszámítása a továbbítandó paraméterek sorozatából eredő karakterlánchoz; megosztott titkos kulcsot használnak a HMAC hash számítás kulcsaként³. A titkos kulcs 50 vagy 100 karakterből áll, és a SIA VPOS biztosítja a kezelők számára. Az üzenet címzettje ugyanazon titkos karakterlánc birtokában tudja ellenőrizni a MAC-et, és így azt is, hogy a kapott paraméterek eredetiek-e vagy sem.

²A visszamenőleges kompatibilitás érdekében a SIA VPOS továbbra is támogatja az MD5 vagy SHA-1 hash-eket, de ezek nem ajánlottak.

³MD5 és SHA-1 esetén a titkos kulcs a string-hez kerül hozzáfűzésre

A kereskedőnek két titkos karakterlánc van:

- **Start key (start kulcs):** ez a karakterlánc a MAC kiszámításához szükséges a fent említett fizetési kezdeményezési üzenetekben;
- **API-Result key (API eredménykulcs):** ez a karakterlánc a SIA VPOS által küldött eredményüzenetek MAC-jének ellenőrzéséhez és a SIA VPOS API-k hívásához használatos.

A fizetési kérelmek és a SIA VPOS által közölt eredmények MAC kiszámításának módszereit a 5.2.1 és 5.2.2A titkos karakterláncokat a SIA VPOS biztonságosan továbbítja az üzletnek a szolgáltatás elindításakor.

Az URLDONE, URLBACK, URLMS és URLMSHEADER mezők tartalmát az üzlet saját belátása szerint dönti el. Ami az URLDONE-t és az URLMS-t illeti, meg kell jegyezni, hogy a rendelésazonosító adatokat a SIA VPOS minden esetben e két karakterlánc végéhez rögzíti a következő bekezdésben leírtak szerint. Az URLDONE és URLBACK maximális hossza 254 karakter, míg az URLMS-é 400 karakter. Az URLMSHEADER legfeljebb 640 karakterből állhat.

Ha a kereskedői rendszer URL-jét képviselő eredeti karakterláncok speciális paramétereket vagy karaktereket tartalmaznak, akkor ezeket a MIME application/x-www-form-urlencoded formátumban kell megadni (a speciális karakterek %XX-re alakulnak át). Az űrlap elküldése esetén az átalakítást a böngésző automatikusan végrehajtja; ha viszont átirányítást használunk, akkor az átalakítást a virtuális áruháznak kell végrehajtania.

A felhasználót a böngésző a HTTP GET metódussal átirányítja az URLDONE és URLBACK címekre.

Az URLDONE és URLBACK URL-nek „http://” vagy „https://” karakterrel kell kezdődnie (vagy bármely más érvényes és a böngészők által értelmezhető HTTP-formával).

Az URL URLMS-nek „http://” vagy „https://” karakterrel kell kezdődnie, **csak a szabványos portok használhatók: 80 a http, 443 a https esetén.**

Ha a kereskedőnek el kell helyeznie néhány mezőt az URLMS-üzenet fejlécében, akkor ezeket hozzáadhatja az URLMSHEADER opcionális mezőben.

Az URLMSHEADER mintája három A, B és C mezővel:

```
URLMSHEADER=A=1&B=2&C=3
```

A fenti URLMSHEADER kódolt verziója:

```
URLMSHEADER=A%3D1%26B%3D2%26C%3D3
```

A fent megadott értékeknek minden esetben meg kell felelniük az első utasításnak, azaz MIME application/x-www-form-urlencoded formátumban kell őket továbbítani.

Példa

Az alábbi példa nem működőképes: csak jelzést ad arról, hogyan kell a fizetési folyamatot űrlap segítségével elindítani.

```
<html>
<body>
<br><center>
SIA VPOS

<form action="http://atpostest.ssb.it/atpos/pagamenti/main" method="POST">

    <input type="hidden" name="PAGE" value="LAND">
    <input type="hidden" name="AMOUNT" value="5000">
```



```
<input type="hidden" name="CURRENCY" value="978">
<input type="hidden" name="LANG" value="ENG">
<input type="hidden" name="SHOPID" value="129280000000211">
<input type="hidden" name="ORDERID" value="7893133444445">
<input type="hidden" name="URLDONE"
value="http://demo.demo.net/mimesys/urlok.html?oper=900">
<input type="hidden" name="URLBACK"
value="http://demo.demo.net/demoshop/backfromt1.html?IdShop=00000000000">
<input type="hidden" name="URLMS"
value="http://demo.ssb.net/index.html?EMAILCLI=tryme@demo.net&CART=02">
<input type="hidden" name="ACCOUNTINGMODE" value="D">
<input type="hidden" name="AUTHORMODE" value="I">
<input type="hidden" name="OPTIONS" value="G">
<input type="hidden" name="EMAIL" value="tryme@demo.net">
<input type="hidden" name="SHOPEMAIL" value="tryme2@demo.net">
<input type="hidden" name="MAC" value="376b61c1189ca70ef88e49c5d3631be7">

<input type="submit" value="Go...">
</form>
</body>
</html>
```

A rejtett mezőkben lévő URL-eket a szokásos módon kell megadni, mivel a böngészők automatikusan elvégzik a szükséges kódolást, amikor a felhasználó végrehajtja a beküldést.

4.2.2 Az OPTIONS mező

Az OPTIONS mező lehetővé teszi különféle további beállítások aktiválását a folyamatban lévő fizetéshez. Ezeket az ábécé betűi jelölik. A jelenleg elérhető lehetőségek a következők:

- **A** – 3DS2 mentesség kérése egy tranzakció esetén. Az áruháznak engedélyezve kell lennie az SVE1 szolgáltatásnak, és meg kell felelnie bizonyos követelményeknek.
- **B** – A rendszer két további mezőt fogad el a bejövő üzenetben: NAME és SURNAME. Ezeknek a mezőknek az értéke, ha vannak ilyenek, tárolásra kerül, és a feldolgozás alatt álló megrendeléshez kapcsolódik. A mezőket a vásárló nem módosíthatja, és nem jelennek meg. Annak érdekében, hogy az értékeket ne lehessen módosítani, a mezők a MAC-számítási karakterlánc részévé válnak. A NAME és SURNAME mezők kitöltése azonban nem kötelező.
- **D** – A rendszer elfogadja a RESIDUALDURATION paramétert a hitelkártya minimális érvényességi idejének beállításához.
- **G** – Elfogadott tranzakció esetén a rendszer nem mutatja meg a tranzakció eredményét a vásárlónak, hanem azonnal átirányítja az URLDONE-ra, hogy a virtuális áruház saját testreszabott „nyugtát” mutasson. Ha az engedélyezés sikertelen, ismét megjelenik az „Adja meg kártyáját” képernyő.
- **H** – Kártyás fizetés esetén az ACQUIRERBIN és a MERCHANTID mezők visszaküldésre kerülnek az URLMS-ben és az URLDONE-ban.
- **I** – Elfogadott tranzakció esetén a rendszer hozzáadja a kibocsátó származási országára vonatkozó információkat tartalmazó ISSUERCOUNTRY mezőt az URLMS-ben és az URLDONE-ban már szereplő információkhoz.
- **K** – Csak token-es fizetés esetén (lásd 4.2.4). A rendszer nem jeleníti meg a céloldalt, hanem folytatja az engedélyezést.
- **L** – Dupla rendelés esetén a rendszer URLMS-re továbbít 07-es eredménykóddal.
- **N** – Elutasított tranzakció esetén a rendszer nem mutatja meg a tranzakció eredményét az ügyfélnek, hanem azonnal átirányítja az URLDONE-ra.
- **P** – Kártyás fizetés esetén az AUTHCODE mező, amely az engedélyezési háttérrendszer által visszaadott válaszkódot adja vissza, az URLMS-ben és az URLDONE-ban jelenik meg.
- **R** – A MAC kiszámítása és elküldése az URLMS-nek és az URLDONE-nak akkor is, ha az eredmény sikertelen. A MAC-hozzárendelés szabályai ugyanazok, mint a sikeres esetben.
- **U** – Ha a G vagy N opció be van állítva, a rendszer hozzáadja az URLMS, URLDONE és URLBACK paraméterekhez a CHINFO nevű opcionális paramétert, amely tartalmazza az ACS által a 3DS 2.x hitelesítés során visszaadott kártyatulajdonos információs mező URL kódolt értékét (opcionálisan).
- **V** – Az ORDDDESCR mező tartalma megjelenik a fizetési oldalon és a nyugtán a mobil/siavpos alapértelmezett skin-eknél.

Az opciók megjelenési sorrendje tetszőleges. Több opció alkalmazása esetén azokat össze kell fűzni, például: OPTIONS=GN.

Az opciók nagy- és kisbetűkkel is jelezhetők: *OPTIONS=b* ugyanaz, mint *OPTIONS=B*.

Vegye figyelembe, hogy egyes opciók a regionális elérhetőségtől függenek.

4.2.3 A teljesített fizetés visszaigazolása/eredménye

Az engedély megadása esetén a tranzakció eredményét két különböző eljárás szerint közlik a kereskedői rendszerrel. Az első a felhasználó böngészőjén megy keresztül, a második közvetlenül a SIA VPOS szerverről az áruházba.

Az eredményt az URLDONE és URLMS paraméterekben meghatározott címek használatával közlik a kereskedővel; az elsővel az elfogadó döntése szerint csak az ügylet végén lépnek kapcsolatba; a másodikkal viszont a SIA VPOS szerver felveszi a kapcsolatot, függetlenül az ügyfél intézkedéseitől, amint a jogosultsági kör válaszol a SIA VPOS rendszer által benyújtott kérésre. A második cím használata ésszerű garanciát ad arra, hogy a tranzakció eredményét a vevő intézkedéseitől függetlenül közöljük a kereskedői rendszerrel.

A felhasználó eldöntheti, hogy használja-e az URLMS-t, valamint hogy ezen a mechanizmuson keresztül csak a pozitív kimenetelű tranzakciókról vagy az összes tranzakcióról kapjon értesítést. Az első lehetőség javasolt: csak a pozitív kimenetelű tranzakciókról történjen értesítés.

A második lehetőség választása esetén figyelembe kell venni, hogy a vásárló az első tranzakció sikertelensége esetén több egymást követő fizetési kísérletet hajthat végre ugyanarra a megrendelésre. Ebben az esetben a kereskedői rendszer N darab negatív eredményt kap N darab sikertelen tranzakció esetén, és végül egy pozitív eredményt.

A tranzakciót megerősítő üzenet a következő adatokat tartalmazza:

Név	Leírás
ORDERID	Rendelési szám: az kezdő üzenet ORDERID mezőjéből másolt érték
SHOPID	Boltazonosító kód: a kezdő üzenet ugyanilyen mezőjéből másolt érték
AUTHNUMBER	Azonosító szám. Az érték csak pozitív eredmény esetén kerül visszaadásra. Ha a felhatalmazást nem adják meg, a mező „NULL” értékkel kerül kitöltésre. Kártyás tranzakciók esetén a kártya kibocsátója által megadott maximum 6 karakteres azonosító. EnelPay tranzakciókhoz legfeljebb 13 karakterből álló Enel által hozzárendelt azonosító. SatisPay tranzakciók esetén a SatisPay által hozzárendelt legfeljebb 36 karakteres azonosító. BancomatPay tranzakciók esetén max. 18 karakteres azonosító, amelyet a BancomatPay rendel hozzá. A Paypal-tranzakciókhoz jelenleg nem használt, és „000000”-nel van feltöltve.
AMOUNT	Összeg: a kezdő üzenet ugyanilyen mezőjéből másolt érték.
CURRENCY	Pénznem: a kezdő üzenet ugyanilyen mezőjéből másolt érték
TRANSACTIONID	A tranzakció SIA VPOS rendszer által hozzárendelt azonosítója. Ez egy 25 karakterből álló karakterlánc
MAC	A megerősítő üzenet hitelesítésének értéke. A kapcsolódó számítást lásd az 5.2.2. Ez egy 32, 40, vagy 64 karakterből álló karakterlánc.

Név	Leírás
RESULT	Az ügylet eredménye. Lásd a következő oldalt.
AUTHORMODE	Engedély típusa: I azonnali, D halasztott. Az érték a kezdeményező üzenet ugyanilyen mezőjéből másolva.
ACCOUNTINGMODE	Elszámolás típusa: I azonnali, D halasztott. Az érték a kezdeményező üzenet ugyanilyen mezőjéből másolva.
NETWORK	Az ügyfél által a fizetéshez használt kártya típusa. Lásd a következő oldalt.
TRANSACTIONTYPE	Ez a mező a végrehajtott tranzakció típusát jelzi (lásd a TRANSACTIONTYPE mező értéktáblázatát). Ha a tranzakció nem engedélyezett (RESULT különbözik 00-tól), előfordulhat, hogy a TRANSACTIONTYPE nem szerepel a válaszban (a 04-es és 05-ös eredménynél is jelen kell lennie).
ISSUERCOUNTRY	Ez a mező csak akkor van jelen az URLMS-ben és az URLDONE-ban, ha az (I) opció keresztül kéri, és csak akkor, ha engedélyt kapott; a kártyakibocsátó származási országát jelzi.
AUTHCODE	OPTION P kártyás fizetéssel. Az engedélyezési rendszer által visszaadott válaszkód.
IBAN	MyBank fizetés esetén csak akkor, ha az áruházban engedélyezve van a megfelelő visszaküldési szolgáltatás (SV58) vagy IBAN fizetés.
ACCOUNTHOLDER	MyBank fizetés esetén csak akkor, ha az áruházban engedélyezve van a megfelelő visszaküldési szolgáltatás (SV58)
ALIASSTR	Postepay-jel történő fizetés esetén csak akkor, ha az áruházban engedélyezve van a megfelelő visszaküldési szolgáltatás (SV62)
AHEMAIL	Számlatulajdonos e-mail-címe, csak akkor, ha az üzletben engedélyezve van a megfelelő visszaküldési szolgáltatás (SV84)
AHTAXID	Számlatulajdonos adóazonosítója, csak akkor, ha az üzletben engedélyezve van a megfelelő visszaküldési szolgáltatás (SV84).
PANTAIL	Csak kártyás fizetés esetén, és csak akkor, ha az üzletben engedélyezve van a megfelelő visszaküldési szolgáltatás (SV64)
PANEXPIRYDATE	Csak kártyás fizetés esetén, és csak akkor, ha az üzletben engedélyezve van a megfelelő visszaküldési szolgáltatás (SV64)
PANALIAS	Csak az M opció jelenlétében, és ha az áruház számára engedélyezve van valamelyik Alias Pan szolgáltatás. Tartalmazza az ügyfél által használt kártyához társított „alias”-t. Numerikus, 19 hosszúságú
PANALIASREV	Csak az M opció jelenlétében, és ha az áruház számára engedélyezve van valamelyik Alias Pan szolgáltatás. Ez tartalmazza a visszavont alias-t. Numerikus, 19 hosszúságú
PANALIASEXPDATE	Csak az M opció jelenlétében, és ha az áruház számára engedélyezve van az Alias Pan valamelyik szolgáltatása. Ez tartalmazza az alias lejárat dátumát ÉÉHH formátumban.

Név	Leírás
PANALIASTAIL	Csak az M opció jelenlétében, és ha az áruház számára engedélyezve van az Alias Pan valamelyik szolgáltatása. Numerikus, és a kártyaszám utolsó 4 számjegyét tartalmazza.
MASKEDPAN	Csak az M opció jelenlétében, és ha az üzlet számára engedélyezve van a maszkolt visszaküldési szolgáltatás (SV61), vagy ha az áruház SVAT-engedélyezett az M opció nélkül is. Ez tartalmazza a maszkolt kártyaszámot (az első hat és az utolsó négy karakter).
ACQUIRERBIN	Csak a H opció megléte esetén, és ha az ügyfél kártyával fizetett. Tartalmazza az ügylet elfogadójának nemzetközi kódját.
MERCHANTID	Csak a H opció megléte esetén, és ha az ügyfél kártyával fizetett. Tartalmazza a SIA VPOS kereskedőkódot, vagy az elfogadó kereskedői kódját, ha az áruház SVAH engedélyezett.
CHINFO	Csak az U opció és a G vagy N valamelyikének jelenléte esetén opcionális üzenetet küld a kártyabirtokosnak az ACS a 3DS 2.x hitelesítés eredményéről.
PANCODE	Csak kártyás fizetés esetén és csak akkor, ha az áruházban engedélyezve van a megfelelő visszaküldési szolgáltatás (SV18). A SIA VPOS generál és visszaküld egy kódot, amely a tranzakcióban használt kártyaszámhoz kapcsolódik.
CARDTYPE	C: hitel; D: betéti; P: prepaid (előre fizetett). Csak kártyás fizetés esetén, ha az üzletben engedélyezve van az SV82, valamint rendelkezésre áll az információ.
TRECURR	Az ismétlődő fizetés típusa. Az érték a kezdő üzenet ugyanilyen mezőjéből másolva. Ez a mező nem lesz jelen, ha az áruház számára engedélyezve van az SVAS.
CRECURR	Ismétlődő kód, amelyet egy ismétlődő tranzakció követésére kell használni. Csak pozitív eredmény esetén és az OPTION M vagy a TRECURR jelenlétében. Ez a mező nem lesz jelen, ha az áruház számára engedélyezve van az SVAS.
INSTALLMENTSNUMBER	Csak akkor, ha az áruház számára engedélyezve van az SVAA részletfizetési szolgáltatás, és ha a kezdeti hívás során részletfizetést kezdeményeztünk.
CARDHOLDERDATA	Csak akkor, ha az áruház számára engedélyezve van az SVAD, és a végrehajtott tranzakció 3DS2.
THREEDSRESULT	Csak akkor, ha az áruház számára engedélyezve van az SVAY, és a végrehajtott tranzakció 3DS2.
SUBSCRIPTIONCODE	Csak akkor, ha az áruház számára engedélyezve van az SVAR, és a kezdeti hívásban TICKLERPLAN lett elküldve.

Megjegyzés: A kiválasztott elemek regionális felhasználásra vonatkoznak, további részletekért forduljon a Bankhoz.

A kereskedő rendszer üzenetet kap az URLMS és az URLDONE címeken, amely a következőkből áll:

URLMS:

URLMS&<confirmation>&MAC=<mac>

URL DONE:

URLDONE&<confirmation>&MAC=<mac>

Ahol:

<confirmation>=ORDERID=<orderId>&SHOPID=<shopId>&AUTHNUMBER=<authNumber>&AMOUNT=<amount>& TRANSACTIONID=<transactionId>&CURRENCY=<currency>&AUTHORMODE=<type of authorization>&RESULT=<outcome>& TRANSACTIONTYPE=<type of transaction>& ISSUERCOUNTRY=<country of issuer (if present)>&NETWORK=<type of card>&ACCOUNTINGMODE=<type of booking>

A RESULT mező a következő értékeket tartalmazhatja:

Kód	Leírás
00	Siker
01	A rendszer megtagadta
02	Elutasítva az áruház konfigurációs problémái miatt
03	Elutasítva az engedélyezési központtal való kommunikációs problémák miatt
04	A kártya kibocsájtója utasította el
05	Elutasítva hibás kártyaszám miatt
06	Váratlan hiba a kérelem feldolgozása során
07	Dupla megrendelés
10	Részletfizetésre nem jogosult kártya
50	Részletfizetés nem lehetséges
51	A törlesztőrészlet száma határértéken kívül van

Abban az esetben, ha engedélyezik a szolgáltatásnak az explicit csalás elleni eredmény (SV54) szolgáltatását, a következő eredmények is lehetségesek:

Kód	Leírás
60	Elutasítva sikertelen Riskshield csalás elleni ellenőrzés miatt
61	Megtagadva a sikertelen AmexPan csalás elleni ellenőrzés miatt
62	Elutasítva a sikertelen AmexPanIP csalás elleni ellenőrzés miatt
63	Megtagadva a sikertelen H3GPan csalás elleni ellenőrzés miatt

64	Elutasítva a sikertelen ItaPanCountry csalás elleni ellenőrzés miatt
65	Megtagadva a PaypalCountry csalás elleni ellenőrzésének sikertelensége miatt
66	Megtagadva a CardEnrolledAuthenticate csalás elleni ellenőrzés sikertelensége miatt
67	Elutasítva, mert a PanBlackList csalás elleni ellenőrzés sikertelen volt
68	Megtagadva a sikertelen CountryPan csalás elleni ellenőrzés miatt
69	Megtagadva a PrepaidPan megghiúsult csalás elleni ellenőrzése miatt
70	Elutasítva, mert a DebitPan csalás elleni ellenőrzése sikertelen volt
71	Megtagadva a VirtualPan csalás elleni ellenőrzésének sikertelensége miatt
72	Megtagadva a sikertelen csalás elleni ThresholdAmount ellenőrzés miatt
73	Megtagadva a sikertelen csalás elleni H3GPanLit ellenőrzés miatt
74	Megtagadva a sikertelen csalás elleni AcqrBinTab ellenőrzés miatt
75	Megtagadva a sikertelen csalás elleni ellenőrzés miatt CountryWL
76	Megtagadva a PrepgWLPan csalás elleni ellenőrzés sikertelensége miatt
77	Elutasítva az IllimitPan csalás elleni ellenőrzés sikertelensége miatt
90	Elutasítva, ha nincs kártyahitelesítési módszer az ügyfél számára

Megjegyzés: a jelenlegi megvalósításban az OUTCOME egyetlen értéke az URLDONE-ban 00

A NETWORK mezőnek a következő értékei lehetnek:

Kód	Leírás
01	VISA
02	MasterCard
04	Maestro
06	American Express
08	JCB
80	IBAN
81	AmazonPay
82	EnelX

84	Satispay
91	BancomatPay (Jiffy)
94	Postepay
96	MyBank
97	Paypal

A TRANSACTIONTYPE mezőnek a következő értékei lehetnek:

Kód	Leírás
TT01	SSL
TT06	VBV
TT07	Biztonsági kód
TT08	Kereskedő VBV
TT09	Kereskedői biztonsági kód
TT10	Nem hitelesített tulajdonos VBV
TT11	Mo/To (Mail Order Telephone Order)
TT13	SafeKey
TT14	Kereskedői SafeKey
TT15	Nem hitelesített tulajdonos SafeKey
TT16	ProtectBuy
TT17	Kereskedői ProtectBuy
TT18	Nem hitelesített tulajdonos ProtectBuy

MEGJEGYZÉS az Applepay kártyáival végzett tranzakciók esetén a tranzakció típusa „TAnn”, a Google Pay[™] esetében pedig „TGnn” lesz. A mentességet élvező 3DS-tranzakciók esetén „TEnn” lesz (kivéve, ha az áruház számára az SVE3 aktíválva van). A tranzakció típusának száma és jelentése változatlan marad.

Egy kérdőjel lesz az URLMS és az URLDONE végéhez fűzve kivéve, ha már jelen van.

FONTOS: A mezőnevek mindegyikét nagybetűvel kell írni, mivel a rendszer kis- és nagybetű érzékeny; a paraméterek GET vagy POST HTTP-be történő beírásának sorrendje tetszőleges.

A MAC mező értéke nem kerül kiszámításra, ha a tranzakció eredménye negatív, hacsak nem lett megadva az OPTION R. Ezért a normál értéke a „NULL” karakterlánc.

Ha az engedélyezési kérelem sikertelen, vagy probléma lépett fel a MAC számítása során, vagy ha a tranzakció PAYPAL-lal történik BILLINGAGREEMENT visszaküldése nélkül, a PANALIAS, PANALIASREV, PANALIASEXPDATE és PANALIASTAIL elemek értéke „NULL”.

Váratlan rendszerhiba esetén, ami miatt az alias pan generálása és/vagy tárolása sikertelen, a PANALIAS, PANALIASREV, PANALIASEXPDATE és PANALIASTAIL elemek értéke „ERROR” lesz.

Az eredményüzenetek MAC-jeinek kiszámításával és ellenőrzésével kapcsolatos további információkért lásd a C2 függelékét.

Az üzlet kifejezetten felelős a MAC kiszámításáért a birtokában lévő "API-Result key" titkos karakterlánc segítségével, annak ellenőrzése érdekében, hogy az egyezik-e a kapott üzenetben megadottal. Ha ezt az ellenőrzést elmulasztja, a kereskedői rendszer érvényesnek tekintheti azokat a megerősítő üzeneteket is, amelyeket nem a SIA VPOS, hanem harmadik felek küldtek.

Nem szabad megfeledkezni arról, hogy az integráció során az URLDONE, URLMS és URLBACK címekre küldött HTTP-üzenetek a rendszer fejlesztésének köszönhetően a jövőben olyan további paramétereket is tartalmazhatnak, amelyek eredetileg nem voltak jelen. **Az alkalmazásoknak ezért figyelmen kívül kell hagyniuk minden olyan paramétert, amelyet nem ismernek fel.**

Ha a kereskedői rendszerrel az URLMS-en keresztül történő kommunikáció meghiúsul, az üzenetküldés nem kerül megismétlésre. A webhely lekérdezheti a SIA VPOS rendszert API hívás segítségével, hogy ellenőrizze a „függőben lévő” megrendelések állapotát.

4.2.4 SIA VPOS fizetés átirányítása token kezdeményezéssel

Ezt a kérés típust olyan kereskedők használják, akik valamelyik SIA VPOS pan-alias tokenizációs rendszerrel rendelkeznek.

A hívás az előzőhöz hasonló (lásd 4.2.1), így kérjük annak használatát.

5 SIA VPOS Függelékek

5.1 Hivatkozások

Az alábbiakban felsoroljuk azokat a hasznos forrásokat, amelyekre hivatkozni lehet kereskedői rendszerintegrációs célokra.

A SIA VPOS nem nyújt semmilyen garanciát vagy támogatást az alábbiakban felsorolt harmadik fél termékeihez.

A HMAC-256 kiszámításához a SIA VPOS a `javax.crypto.Mac` osztályt használja a `HmacSHA256` algoritmussal, amelyet a JDK biztosít.

A HMAC-256 szabvány definícióját és a különböző nyelveken történő megvalósítás példáit lásd:

https://en.wikipedia.org/wiki/Hash-based_message_authentication_code

<https://www.supermind.org/blog/1102/generating-hmac-md5-sha1-sha256-etc-in-java>

<https://www.jokecamp.com/blog/examples-of-creating-base64-hashes-using-hmac-sha256-in-different-languages>

A pénznemkódok listájához a hivatkozás az ISO 4217. Lásd:

https://en.wikipedia.org/wiki/ISO_4217

5.2 MAC átirányítás (redirect) generálása

5.2.1 A MAC generálása REDIRECT üzenetekhez

A fizetési folyamatot indító üzenetek között továbbítandó MAC-et az alábbiakban leírt eljárással kapjuk meg.

A MAC generálásához ajánlott hash függvény a HMAC-256 ⁴.

A kereskedő és a SIA VPOS egy 50 vagy 100 karakterből álló titkos karakterláncon osztoznak. A MAC kódolt adatok előállításához az aláírandó szöveg hash-jét hajtják végre, a titkos karakterláncot a HMAC-256 kulcsaként használva ⁵.

A tranzakciót kezdeményező üzeneteknél az aláírandó szövegnek a következő mezőket kell tartalmaznia, ebben a sorrendben:

- URLMS
- URLDONE
- ORDERID
- SHOPID
- AMOUNT
- CURRENCY
- EXPONENT (ha van)
- ACCOUNTINGMODE
- AUTHORMODE
- OPTIONS (ha vannak)
- NAME (ha van, OPTIONS B esetén)
- SURNAME (ha van, OPTIONS B esetén)
- TAXID (ha van)
- COMMIS (ha van)
- BIZOTTSÁG (ha van, OPTIONS F esetén)
- ORDDESCR (ha van, OPTIONS O vagy V esetén)
- VSID (ha van)
- OPDESCR (ha van)
- REMAININGDURATION (ha van, OPTIONS D esetén)
- USERID (ha van)
- PHONENUMBER (ha van, BancomatPay rendszerhez)
- CAUSATION (ha van, BancomatPay rendszerhez)
- USER (ha van, BancomatPay rendszerhez)
- PRODUCTREF (ha van)
- ANTIFRAUD (ha van)
- 3DSDATA (ha van)
- TRECURRE (ha van)
- URLMSHEADER (ha van)
- INSTALLMENTSNUMBER (ha van)

⁴A visszafele kompatibilitás érdekében a SIA VPOS továbbra is támogatja az MD5 vagy SHA-1 hash-eket, de ezek nem ajánlottak. Tekintettel arra, hogy a három algoritmus eltérő számú bitet állít elő (160 SHA-1, 128 MD5 és 256 HMAC-256), a rendszer képes automatikusan felismerni a MAC generálásához használt függvény típusát.

⁵Az SHA-1 és MD5 titkos karakterláncának sorban állása (mac=text&key)

- TICKLERPLAN (ha van)

Példa a MAC HMAC-256 kiszámításához használt karakterláncra ⁶:

```
MAC=Hash(URLMS=<urlms>&URLDONE=<urldone>&ORDERID=<orderid>&SHOPID=<shopid>
&AMOUNT=<Amount>&CURRENCY=<Currency>&ACCOUNTINGMODE=<accountingmode>&A
UTHORMODE=<authormode>, <startsecretstring> )
```

Az OPTIONS használata:

```
MAC=Hash (URLMS=<urlms>&URLDONE=<urldone>&ORDERID=<orderid>&SHOPID=<shopid>&AMOUNT=<Amount
>&CURRENCY=<Currency>&ACCOUNTINGMODE=<accountingmode>&AUTHORMODE=<authormode> &OPTIONS=B&N
AME=<name>&SURNAME=<surname>, <startsecretstring>)
```

A mezők sorrendje fontos! A használandó titkos karakterlánc az úgynevezett „indítókulcs” (start key).

A MAC számításánál az URLMS, URLDONE és URLMSHEADER mezőket nem „kódolt” formában kell használni, még akkor is, ha paramétereket tartalmaznak.

Példa egy ilyen karakterláncra:

```
URLMS=http://www.dominio.it/ok.asp?par=45&nord=23684&URLDONE=http://www.dominio.it/negozi
o.asp?par=45&nord=23684&ORDERID=A4845b2&SHOPID=123456789012345&AMOUNT=100&CURRENCY=978&AC
COUNTINGMODE=D&AUTHORMODE=I
```

A MAC-et, amely egy hash eredménye, megfelelően kódolni kell ahhoz, hogy HTTP-n keresztül továbbítható legyen. Ehhez hexadecimális konverziót kell végrehajtani.

Az átalakítás eredménye egy 64 karakteres karakterlánc a HMAC-256 számára ⁷.

A MAC nem érzékeny a kis- és nagybetűkre.

Példa a HMAC számításra

Minta hívás URL (HTTP GET-ként) a MAC-számítás előtt:

```
https://virtualposttest.sia.eu/vpos/payments/main?PAGE=LAND&URLBACK=https://virtualposttest
.sia.eu/vpos/payments/test/TEST_VPOS_UTF8_EN.html&URLDONE=https://virtualposttest.sia.eu/v
pos/payments/test/result-
it_new.html&URLMS=https://virtualposttest.sia.eu/vpos/payments/main?PAGE=RICEZIONE_ESITO&O
RDERID=test20211123164921878&SHOPID=12928050505050505&AMOUNT=2312&CURRENCY=978&ACCOUNTINGMO
DE=I&AUTHORMODE=I&LANG=EN&SHOPEMAIL=test.appls@ssb.it&EMAIL=test.appls@ssb.it
```

Kapcsolódó MAC STRING

```
URLMS=https://virtualposttest.sia.eu/vpos/payments/main?PAGE=RICEZIONE_ESITO&URLDONE=https
://virtualposttest.sia.eu/vpos/payments/test/result-
it_new.html&ORDERID=test20211123164921878&SHOPID=12928050505050505&AMOUNT=2312&CURRENCY=978
&ACCOUNTINGMODE=I&AUTHORMODE=I
```

⁶ MD5 vagy SHA1 visszamenőleges kompatibilitás esetén a titkos karakterlánc az aláírandó karakterláncához kerül sorba (mac=string&key).

⁷Ha a használt hash függvény az MD5, az eredmény egy 32 karakteres karakterlánc lesz; ha SHA-1-et használunk, az eredmény egy 40 karakteres karakterlánc lesz.

Minta MAC KULCS

MrXw-RcZ5G-8ge-4EAHE--a-jF-Ux49-BXw2qK4gFZM-U9XXqm

A fenti MAC STRING és MAC KEY használatával a következő H MAC-256 kiszámítható

fa5c28419fd0a0ba80e378ebaa9d12e6cc085bdd780126b830b3f82d5b5b91d1

Ha a fenti példa URL-hez hozzáadjuk a mac=

fa5c28419fd0a0ba80e378ebaa9d12e6cc085bdd780126b830b3f82d5b5b91d1-et, megkapjuk a végső hívható minta URL-t.

5.2.2 MAC generálása az eredményüzenetek számára

A MAC, amelyet a SIA VPOS a kereskedői rendszernek szállított eredményüzenetekhez mellékel, az itt leírt eljárással áll elő. A kereskedő és a SIA VPOS egy 50 vagy 100 karakteres titkos karakterláncon osztoznak. Az adatok MAC-jének előállításához a kommunikációs szöveg a titkos karakterlánccal kerül aláírásra. Vegye figyelembe, hogy a SIA VPOS a start kulcstól eltérő titkos karakterláncot használ az eredményüzenetek MAC-értékének kiszámításához; ezt a karakterláncot „API-result” kulcsnak nevezik, mert a SIA VPOS API-hoz való hozzáférésre is használják.

A SIA VPOS által a MAC generálásához használt hash függvény megegyezik azzal, amelyet a kereskedő az indítóüzenet MAC generálásához használt. Ha a MAC indítóüzenet HMAC-256 típusú, akkor ez lesz az eredményüzenet típusa is. A HMAC256 algoritmus 256 hosszú karakterláncot állít elő ⁸.

A megerősítő üzenetknél az aláírt szöveg a következő mezőket fogja tartalmazni:

- ORDERID
- SHOPID
- AUTHNUMBER (ha az engedélyezés nincs meg, a mező értéke „NULL”)
- AMOUNT
- CURRENCY
- TRANSACTIONID
- ACCOUNTINGMODE
- AUTHORMODE
- RESULT
- TRANSACTIONTYPE
- ISSUERCOUNTRY (ha az OPTIONS I használatával kéri)
- AUTHCODE (bankkártyás fizetéskor, ha az OPTIONS P-n keresztül kéri)
- HASHPAN (ha az áruház számára engedélyezve van a szolgáltatás)
- TRECURRE, CRECURRE (ha az áruház számára engedélyezve van az SVA8 szolgáltatás)
- PANTAIL, PANEXPIRYDATE (ha az áruház számára engedélyezve van az SV64 szolgáltatás)
- AHEMAIL, AHTAXID (ha az áruház számára engedélyezve van az SV84 szolgáltatás)
- ACQUIRERBIN, MERCHANTID (bankkártyás fizetéskor, ha az OPTIONS H-n keresztül kéri)
- CARDTYPE (bankkártyás fizetéskor, ha az áruház számára engedélyezve van az SV82 szolgáltatás)
- CHINFO (opcionális, és csak szerepel, ha az OPTIONS U és OPTIONS G vagy N-en keresztül kéri)
- PANCODE (bankkártyás fizetéskor, ha az áruház számára engedélyezve van az SV18 szolgáltatás)
- INSTALLMENTSNUMBER (bankkártyás fizetéskor, ha az üzletben engedélyezve van az SVAA szolgáltatás és részletfizetést használnak)
- CARDHOLDERDATA (3DS2 bankkártyás fizetéskor, ha az áruház számára engedélyezve van a SVAD szolgáltatás)
- THREEDSRESULT (3DS2 bankkártyás fizetéskor, ha az áruház számára engedélyezve van a SVAY szolgáltatás)
- SUBSCRIPTIONCODE (ha az áruház számára engedélyezve van a SVAR szolgáltatás, és a kezdeti hívás során TICKLERPLAN-t küldtek)

Példa a MAC HMAC-256 kiszámításához használt karakterláncra ⁹:

⁸Tekintettel arra, hogy az SHA1, MD5 és HMAC256 algoritmusok változó számú bitet állítanak elő (160 az első, 128 a második és 256 a harmadik), a rendszer képes automatikusan felismerni a start üzenet MAC generálásához használt függvény típusát, és ugyanazt az algoritmust használja a válaszadáshoz.

⁹ Lásd a 11. megjegyzést NOTEREF _Ref87655788 \h


```
MAC=Hash(ORDERID=<orderId>&SHOPID=<shopId>&AUTHNUMBER=<authNumber>&AMOUNT=<Amount>&CURRENCY=<Currency>&TRANSACTIONID=<transactionId>&ACCOUNTINGMODE=<accountingMode>&AUTHORMODE=<authorMode>&RESULT=<Result>&TRANSACTIONTYPE=<transactionType>&ISSUERCOUNTRY=< issuerCountry>, <API-Result key >)
```

A mezők megjelenési sorrendje fontos! A használandó titkos karakterlánc az úgynevezett „API-eredménykulcs” (API-result key).

Példa egy ilyen karakterláncra:

```
ORDERID=A4845b2&SHOPID=123456789012345&AUTHNUMBER=HJ89KR&AMOUNT=100&CURRENCY=978&TRANSACTIONID=HK84HL2G&ACCOUNTINGMODE=I&AUTHORMODE=I&RESULT=00&TRANSACTIONTYPE=TT01&Absd830923fk32&ISSUERCOUNTRY=ITA
```

A MAC-et, amely egy hash eredménye, megfelelően kódolni kell ahhoz, hogy HTTP-n keresztül továbbítható legyen. Ehhez hexadecimális konverziót kell végrehajtani.

Az átalakítás eredménye egy (HMAC-256 típusú) 64 hosszú karakterlánc.

A MAC nem kis-, nagybetű érzékeny. A SIA VPOS szerver nagybetűket használ.

Megjegyzés: Ha a tranzakció eredménye sikertelen, a MAC nem kerül kiszámításra, és értéke „NULL” lesz; hacsak nem OPTIONS R-t kértek.

5.2.3 A MAC generálása a REDIRECT számára token üzenetekkel

Hasonló a normál redirect-hez (jelenleg használata nem javasolt).

5.3 Paraméterek AUTHORMODE, ACCOUNTINGMODE

Az alábbiakban röviden ismertetjük az AUTHORMODE és ACCOUNTINGMODE paraméterek jelentését a SIA VPOS rendszer különféle lehetséges felhasználásaival kapcsolatban.

5.3.1 AUTHORMODE

1.1.1 Azonnali engedély I

Az azonnali engedélyezési eljárás azt írja elő, hogy az online fizetési szakaszban az engedélyezési kérelmet azonnal megküldik a nemzetközi elfogadói hálózatok felé. A tranzakció sikeres lebonyolítása után a kereskedő biztos lehet abban, hogy a vevő oldalán a fizetendő összeg „le van foglalva”.

Hacsak nincsenek különleges kivételek, ezt az értéket kell használni.

1.1.2 Halasztott engedély D

A halasztott engedélyezési eljárás előírja, hogy az online fizetési szakaszban a tranzakciókat elfogadják, de nem továbbítják az elfogadói hálózatok felé (a kártya érvényessége kibocsátói oldalon minden esetben ellenőrzésre kerül).

Az a kereskedő, aki ezt a fizetés-elfogadási eljárást követi egy későbbi időpontban feldolgozhatja a függőben lévő engedélyezési kérelmeket. A SIA VPOS az eredetinel alacsonyabb összegű halasztott engedélyezési kérelmeket kaphat; a kereskedő több halasztott felhatalmazást is továbbíthat, de legfeljebb az eredeti végösszeg erejéig.

Hacsak nincsenek speciális igények, ezt az értéket ne használjuk.

5.3.2 ACCOUNTINGMODE

1.1.3 Azonnali foglalás I

Az azonnali foglalási eljárás lehetővé teszi a kereskedő számára, hogy minden engedélyezett tranzakciót automatikusan elszámolhatóvá tegyen. A kereskedő beavatkozása nélkül a tranzakció lebonyolításának napjának estéjén a front-end processzor automatikusan elvégzi a tranzakciók teljes engedélyezett összegének elszámolását.

Ez az eljárás alkalmazható például abban az esetben, ha az eladott árut/szolgáltatást a vásárló azonnal felhasználhatja (szoftver, zene, online szolgáltatások stb.).

1.1.4 Halasztott foglalás D

A halasztott foglalási eljárás előírja, hogy az engedélyezett tranzakciókat a kereskedő lefoglalhatóvá teszi. A kereskedőnek az engedélyezéstől számítva előre beállított (például 30) számú napja van a tranzakció könyvelésére.

Ez az eljárás a következő tranzakciókat teszi elérhetővé a kereskedő számára:

-
- Teljes foglalás: a tranzakció az engedélyezett összeg teljes összegére foglalható.
 - Részleges foglalás: a tranzakciót az engedélyezett összegnél alacsonyabb összegre teszik lekönnyvelhetővé; a részleges foglalási tranzakció utalhat olyan meghatalmazásra, amelyre már kértek részfoglalást (osztott szállítmányt), feltéve, hogy a végső foglalási határidő még nem járt le.
 - Lemondás: a napközben lebonyolított foglalási tranzakció törlésre kerül, a tranzakció újra lefoglalható.

5.4 3DSDATA (átirányítás - redirect)

A 3DSDATA mezőt AES-titkosítással kell kódolni az összes olyan mező JSON-reprezentációjával, amelyet a kereskedő el szeretne küldeni az engedélyező központ felé. A következő táblázat tartalmazza a 3DSDATA-n belüli összes mezőt.

A titkosítási algoritmusnak AES/CBC/PKCS5Padding formátumúnak kell lennie, titkosító kulcsként az API kulcs első 16 bájtyát kell megadni. A titkosításhoz használt inicializálási vektornak 16 byte hosszúnak kell lennie, csupa 0-val feltöltve. A titkosított tömbnek base64 kódolásúnak kell lennie.

A következő táblázat felsorolja a 3DSDATA JSON-objektumában használható összes mezőt. A JSON-objektum név/érték párok egyszerű, rendezetlen halmaza. Minden karakterlánc UTF-8 kódolású.

Megjegyzés: a táblázatban szereplő mezőleírások és a kapcsolódó hivatkozások közvetlenül a 3DS 2-t meghatározó EMVco szabványból származnak.

Mező neve	Rövid leírás	Leírás	Értékek	Tartalmazás
threeDSRequestorChallengelnd	3DS Requestor Challenge Indicator	Azt jelzi, hogy kéri-e a hívást ehhez a tranzakcióhoz. Például: A 01-PA esetében a 3DS-kérőnek aggályai lehetnek a tranzakcióval kapcsolatban, és kérhetik a hívást. A 02-NPA esetében hívásra lehet szükség, amikor új kártyát adunk a pénztárcához. Helyi/regionális megbízásokhoz vagy egyéb változókhoz.	Hossz: 2 karakter JSON adattípus: String Elfogadott értékek: • 01 = Nincs preferencia • 02 = Nincs hívás kérés • 03 = Hívás kérés: 3DS kérelmező beállítása • 04 = Hívás kérés: Kötelező • 05–79 = fenntartva EMVCo jövőbeni használatra (az értékek érvénytelenek, amíg az EMVCo meg nem határozza őket) • 80-99 = DS használatra fenntartva Megjegyzés: Ha az elem nincs megadva, a várt művelet az, amit az ACS értelmez	O
addrMatch	Címegezési jelző	Azt jelzi, hogy a kártyabirtokos szállítási címe és a kártyabirtokos számlázási címe megegyezik-e.	Y vagy N	Vagy

chAccAgeInd	Kártyabirtokos számla életkorának mutatója	Az az időtartam, ameddig a kártyabirtokos rendelkezik számlával a 3DS Requestor-nál.	<ul style="list-style-type: none"> • 01 = nincs fiók (vendég) • 02 = e tranzakció során jött létre • 03 = kevesebb, mint 30 nap • 04 = 30-60 nap • 05 = Több mint 60 nap 	Vagy
chAccChange	Kártyabirtokos számlamódosítás	Az a dátum, amikor a kártyabirtokos fiókját a 3DS Requestor-nál legutóbb módosították, beleértve a számlázási vagy szállítási címet, az új fizetési fiókot, vagy az új felhasználó(k) hozzáadását.	Dátumformátum = ÉÉÉÉHHNN	Vagy
chAccChangeInd	Kártyabirtokos számlaváltozás jelzője	A kártyabirtokos fiókinformációinak a 3DS Requestornál legutóbbi módosítása óta eltelt idő, beleértve a számlázási vagy szállítási címet, az új fizetési fiókot vagy az új felhasználó(k) hozzáadását.	<ul style="list-style-type: none"> • 01 = a tranzakció során megváltozott • 02 = kevesebb, mint 30 nap • 03 = 30-60 nap • 04 = több mint 60 nap 	O
chAccDate	Kártyabirtokos számla dátuma	Az a dátum, amikor a kártyabirtokos számlát nyitott a 3DS Requestor-nál.	Dátumformátum = ÉÉÉÉHHNN	O
chAccPwChange	Kártyatulajdonos fiók jelszavának megváltoztatása	Az a dátum, amikor a kártyabirtokos 3DS Requestor-fiókjában jelszómódosításra vagy fiók visszaállítására került sor.	Dátumformátum = ÉÉÉÉHHNN	O

chAccPwChangeInd	Kártyabirtokos fiók jelszavának változás jelzője	Azt jelzi, hogy mennyi idő telt el azóta, hogy a kártyabirtokos 3DS Requestor-fiókjában jelszómódosítás vagy fiók visszaállítása történt.	<ul style="list-style-type: none"> • 01 = nincs változás • 02 = változott a tranzakció során • 03 = kevesebb, mint 30 nap • 04 = 30-60 nap • 05 = több mint 60 nap 	O
nbPurchaseAccount	Kártyabirtokos számlájával történt vásárlások száma	Ezzel a számlával történt vásárlások száma az elmúlt hat hónapban.	String, max 4 hosszú	O
txnActivityDay	Napi tranzakciók száma	Ezen a számlán történt tranzakciók száma (sikeres és megszakadt), amelyek a 3DS Requestor segítségével történtek az elmúlt 24 órában.	String, max 3 hosszú	O
txnActivityYear	Évi tranzakciók száma	Ld. előző, csak az elmúlt évre vonatkozóan.	String, max 3 hosszú	O
shipAddressUsage	Szállítási cím használata	Az a dátum, amikor a tranzakcióhoz használt szállítási címet először használták a 3DS Requestor-hoz.	Dátumformátum = ÉÉÉÉHHNN	O
shipAddressUsageInd	Szállítási cím használati jelző	Azt jelzi, hogy a tranzakcióhoz használt szállítási címet mikor használták először a 3DS Requestor-hoz.	<ul style="list-style-type: none"> • 01 = ez a tranzakció • 02 = kevesebb, mint 30 nap • 03 = 30-60 nap • 04 = több mint 60 nap 	O
shipNameIndicator	Szállítási név jelző	Azt jelzi, hogy a kártyabirtokos neve megegyezik-e a tranzakcióhoz használt szállítási névvel.	<ul style="list-style-type: none"> • 01 = megegyezik • 02 = eltér 	O
acctID	Kártyabirtokos		String, max 64 hosszú	O

	számlaazonosítója			
billAddrCity	Kártyabirtokos számlázási címe - város	A kártyabirtokos számlázási címének városa.	String, max 50 hosszú	Vagy
billAddrCountry	Kártyabirtokos számlázási címe - ország	A kártyabirtokos számlázási címének országa.	ISO 3166-1 numerikus háromjegyű országkód, kivéve az A.5. táblázatban felsorolt kivételeket.	Vagy
billAddrLine1	A kártyabirtokos számlázási címének 1. sora	A kártyabirtokos számlázási címének első sora.	String, max 50 hosszú	Vagy
billAddrLine2	A kártyabirtokos számlázási címének 2. sora	A kártyabirtokos számlázási címének második sora.	String, max 50 hosszú	O
billAddrLine3	A kártyabirtokos számlázási címének 3. sora	A kártyabirtokos számlázási címének harmadik sora.	String, max 50 hosszú	O
billAddrPostCode	Kártyabirtokos számlázási címe - irányítószám	A kártyabirtokos számlázási címének irányítószáma.	String, max 16 hosszú	Vagy
billAddrState	A kártyabirtokos számlázási címének állapota	A kártyabirtokos számlázási címének állama vagy tartománya.	Maximum 3 karakter, az ISO 3166-2 szabványban meghatározott országfelosztási kód	Vagy
homePhone	Kártyabirtokos otthoni telefonszáma	A Kártyabirtokos által megadott otthoni telefonszám.	országkód (1-3) - szám (max. 15)	Vagy
mobilePhone	Kártyabirtokos mobiltelefon száma	A Kártyabirtokos által megadott mobiltelefonszám.	országkód (1-3) - szám (max. 15)	Vagy
shipAddrCity	Kártyabirtokos szállítási címe - település	A Kártyabirtokos által kért szállítási cím településnév része. Kötelező,	String, max 50 hosszú	O

		kivéve, ha a szállítási adatok megegyeznek a számlázási adatokkal (addrMatch = Y).		
shipAddrCountry	A kártyabirtokos szállítási címe - ország	A kártyabirtokos által kért szállítási cím ország része. Kötelező, kivéve, ha a szállítási adatok megegyeznek a számlázási adatokkal (addrMatch = Y).	ISO 3166-1 szerinti numerikus háromjegyű országkód, kivéve az A.5. táblázatban felsorolt kivételeketS.	O
shipAddrLine1	A kártyabirtokos szállítási címének 1. sora	A kártyabirtokos által kért szállítási cím első sora. Kötelező, kivéve, ha a szállítási adatok megegyeznek a számlázási adatokkal (addrMatch = Y).	String, max 50 hosszú	O
shipAddrLine2	A kártyabirtokos szállítási címének 2. sora	A kártyabirtokos által kért szállítási cím második sora.	String, max 50 hosszú	O
shipAddrLine3	A kártyabirtokos szállítási címének 3. sora	A kártyabirtokos által kért szállítási cím harmadik sora.	String, max 50 hosszú	O
shipAddrPostCode	Kártyabirtokos szállítási címe - irányítószám	A kártyabirtokos által kért szállítási cím irányítószáma. Kötelező, kivéve ha a szállítási adatok megegyeznek a számlázási adatokkal (addrMatch = Y).	String, max 16 hosszú	O
shipAddrState	A kártyabirtokos szállítási	A szállítási cím állama vagy tartománya. Kötelező, kivéve,	Maximum 3 karakter, az ISO 3166-2 szabványban meghatározott országfelosztási kód	O

	címének állama	ha a szállítási adatok megegyeznek a számlázási adatokkal (addrMatch = Y).		
workPhone	Kártyabirtokos munkahelyi telefonszám	A kártyabirtokos által megadott munkahelyi telefonszám.	országkód (1-3) - szám (max. 15)	O
deliveryEmailAddress	Szállítási e-mail cím	Elektronikus kézbesítés esetén az az e-mail cím, amelyre az árut kézbesítették.	String, max 254 hosszú	Vagy
deliveryTimeframe	Szállítási időkeret	Jelzi az áru szállítási határidejét.	<ul style="list-style-type: none"> • 01 = elektronikus kézbesítés • 02 = aznapi kiszállítás • 03 = éjszakai szállítás • 04 = minimum két napos szállítás 	Vagy
preOrderDate	Előrendelési dátum	Előrendelt vásárlás esetén az áru várható elérhetőségi dátuma.	Dátum formátum = ÉÉÉÉHHNN	Vagy
preOrderPurchaseInd	Előrendelési vásárlás jelzője	Azt jelzi, hogy a kártyabirtokos megrendelést ad-e le jövőbeni elérhetőségi vagy megjelenési dátummal.	<ul style="list-style-type: none"> • 01 = Elérhető áru • 02 = Jövőbeni elérhetőség 	Vagy
reorderItemsInd	Tételek átrendezése jelző	Azt jelzi, hogy a kártyabirtokos újra rendeli-e a korábban vásárolt árut.	Hossz: 2 karakter JSON adattípus: String lehetséges értékek: <ul style="list-style-type: none"> • 01 = első rendelés • 02 = újra rendelés 	Vagy

shipIndicator	Szállítási jelző	A tranzakcióhoz választott szállítási módot jelöli. A kereskedőknek azt a szállítási jelzőkódot kell kiválasztaniuk, amely a legpontosabban leírja a kártyabirtokos konkrét tranzakcióját. Ha egy vagy több tétel is szerepel az eladásban, használja a szállítási jelzőkódot a fizikai áruhoz, vagy ha az összes áru digitális, akkor használja azt a szállítási jelzőkódot, amely a legdrágább terméket írja le.	<ul style="list-style-type: none"> • 01 = szállítás a kártyabirtokos számlázási címére • 02 = szállítás a kereskedőnél nyilvántartott másik ellenőrzött címre • 03 = a kártyabirtokos számlázási címétől eltérő szállítási cím • 04 = átvétel a helyi üzletben (az üzlet címét a szállítási cím mezőkben kell megadni) • 05 = digitális áruk (beleértve az online szolgáltatásokat, az elektronikus ajándékkártyákat és a beváltási kódokat) • 06 = utazási és/ vagy rendezvény jegyek, nincs szükség szállításra • 07 = egyéb (például játék, nem szállítandó digitális szolgáltatások, elektronikus média előfizetések stb.) 	Vagy
recurringExpiry	Ismétlődő lejárat	Az engedélyezés lejárat dátumát jelzi.	Hossz: 8 karakter JSON adattípus: String Elfogadott formátum: ÉÉÉÉHHNN	O
recurringFrequency	Ismétlődő gyakoriság	Az engedélyezések közötti minimális napok számát jelzi.	Hossz: Változó, maximum 4 karakter JSON adattípus: String Példák elfogadott értékekre: <ul style="list-style-type: none"> • 31 • 031 • 0031 	O

Kérjük, vegye figyelembe, hogy:

- Az EMVCo 3DS szabványai szerint a „3DS Requestor” a „Merchant” (kereskedő) rövidítése.
- Minden karakterláncnak UTF-8 karakterkészletet kell tartalmaznia.
- **Tartalmazás** oszlop jelentése:
 - „R” szükséges
 - „Vagy” opcionális, de javasolt
 - „O” opcionális
 - „C” feltételes

SP	0	@	P	`	p
!	1	A	Q	a	q
“	2	B	R	b	r
#	3	C	S	c	s
\$	4	D	T	d	t
%	5	E	U	e	u
&	6	F	V	f	v
‘	7	G	W	g	w
(8	H	X	h	x
)	9	I	Y	i	y
*	:	J	Z	j	z
+	;	K	[k	{
,	<	L	\	l	
-	=	M]	m	}
.	>	N	^	n	~
/	?	O	_	o	

Példa kód

A következő Java kód csak a 3DSDATA mező létrehozásához alkalmazandó titkosítási folyamat tisztázására szolgál.

```
import java.security.InvalidAlgorithmParameterException;
import java.io.UnsupportedEncodingException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class Utility {

    public static String encode3DSdata(String APISecretMerchant, String JSONObject) throws
    Throwable {

        // Inicializálási vektor
        byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 };

        // AES kulcs az API kereskedői kulcsból
        byte[] key = APISecretMerchant.substring(0, 16).getBytes();
        IvParameterSpec ivParameterSpec = new IvParameterSpec(iv);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, "AES");

        // amit titkosítanunk kell
        byte[] toEncrypt = JSONObject.getBytes("UTF-8");
```

```
// titkosítás
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE, secretKeySpec, ivParameterSpec);
byte[] encrypted = cipher.doFinal(toEncrypt);

// base64-re konvertálás
return DatatypeConverter.printBase64Binary(encrypted);
}
}
```

5.5 Kiválasztott API-k használata

A kézikönyvben leírt átirányítási séma használata közben opcionálisan használhat bizonyos API-szolgáltatásokat is. Ez az API-szolgáltatás segíthet a napi üzleti folyamatokban. Használatuk nem kötelező, de ha használni kívánja őket, kérjük:

- erről a szándékról előzetesen tájékoztassa elfogadó bankját, hogy a rendszer beállítása megfelelő legyen,
- hajtsa végre az ezekhez az API-khoz kapcsolódó teszteseteket a tesztforgatókönyv szerint. Ha ezek a tesztesetek nem szerepelnek az Ön tesztforgatókönyveiben, kérjük, érdeklődjön az elfogadó banknál a részletekért.

Az alábbiakban említett API-k részleteiért olvassa el a megfelelő API kézikönyv fejezetet. Itt csak alapvető hivatkozás található ezekre.

A. Opcionális API-k:

- A tranzakciókkal kapcsolatos műveletek listája:
 - o API neve: LISTOPERATION
- A jogosultságok listája:
 - o API neve: LISTAUTHORIZATION
- Rendelések állapotának lekérése:
 - o API neve: ORDERSTATUS

B. Opcionális API-k, amelyeket a CUBO Merchant Portal funkcióinak alternatívájaként kell használni:

Az alábbi API-k alternatívaként használhatók a CUBO kereskedői portál grafikus felhasználói felülete helyett, amely ugyanazokat a funkciókat fedi le.

- Fizetés visszavonási kérelem / Visszatérítés:
 - o API neve: REFUND

Megjegyzés:

 - ha a jóváhagyott azonnali könyvelési tranzakcióval azonos napon hajtják végre, az a tranzakció visszavonását eredményezi (reversal),
 - abban az esetben, ha az azonnali könyvelési tranzakció napja után hajtjuk végre, vagy halasztott elszámolású a tranzakció, akkor visszatérítési (refund) tranzakciót eredményez
- Foglalási kérelem:

- API neve: ACCOUNTING

- Foglalási kérelem törlése

- API neve: REVERSEACCOUNTING

Megjegyzés: vegye figyelembe, hogy ezt a műveletet a már elszámolt halasztott könyvelésű tranzakciók esetén csak 30 napon belül használhatja

- Eladás – MIT Framework (ismétlődő) – következő tranzakció

- API neve: AUTHORIZATION

Megjegyzés:

- az MIT-t (kereskedő által kezdeményezett tranzakció) csak azonnali elszámolású módú tranzakcióként használhatja,
- ezt a tranzakciót a kifejezetten ehhez a funkcióhoz konfigurált 2. Bolt azonosító használatával kell végrehajtania,
- PanAlias NETWORK = 98 első tranzakcióval kapott PAN alias-t kell használnia.

A tranzakció beállításának részleteiért nézze meg a tesztforgatókönyvek részleteit.