# Elektronikus Kártyatranzakciók az Interneten

## A CIB Bank Zrt.

eCommerce

## Internetes kártyaelfogadás szolgáltatás

## technikai dokumentációja

## Gyakran Feltett Kérdések

# Tartalomjegyzék

# Hálózattal kapcsolatos kérdések

**K:** A banki szerver miért nem válaszol?

**V:** A bank szervere az áruházzal nem a hagyományosan erre a célra szánt 80-as vagy 443-as TCP porton keresztül kommunikál, ezért amennyiben az áruházi szerver és az internet között található bármely hálózati szűrő (switch, router, tűzfal) nincs felkészítve az ezeken a portokon keresztül történő kommunikációra, a kérés nem juthat el a bankhoz A kapcsolat az áruházi szerverről parancssori alkalmazások segítségével ellenőrizhető (pl. cUrl vagy wget segítségével).

**K:** A vásárlók xxx szolgáltatótól/országból miért nem jutnak el a fizetőoldalra?

**V:** A banki szerver ip címét a vásárló internetszolgáltatója oldja fel. Elképzelhető, hogy a vásárló internetszolgáltatója szinkronizációs problémákkal küzd, vagy egyéb okból nem sikerült megállapítania a bank szerverének pontos címét. Ilyen esetekben javasoljuk, hogy a vásárló jelentse be a hibát az internetszolgáltatónak, illetve ha teheti, próbálkozzon meg a vásárlással egy másik internetszolgáltatón keresztül.

**K:** A bank válasza miért csak „500 Server error” vagy „403 Forbidden”?

**V:** A bank válasza minden esetben az oldal forrásában (content) érkezik text/plain mime kódolással. Sikeres feldolgozás esetén a http státusz 200, hiba esetén azonban vagy 403 (titkosítási hiba) vagy 500 (feldolgozási hiba). Léteznek olyan kapcsolatkezelők (alkalmazások vagy függvénykönyvtárak/osztályok) melyen ilyenkor azonnal megszakítják a kapcsolatot, így a hibaüzenet elvész. Célszerű olyan eszközt használni, amely hiba esetén is kiolvassa a teljes tartalmat.

**K:** Minden kérésre RC=D04 hibaüzenetet kapok, miért?

**V:** A bank adott idő alatt csak bizonyos számú kérést szolgál ki, az e számosság feletti üzenetekre RC=D04 hibaüzenetet ad.

**K:** Mik a banki szerver elérhetőségei?

**V:** A teszt szerver az ekit.cib.hu, az éles az eki.cib.hu címeken érhető el. A kereskedői url minden esetben https://<szervernév>/market.saki, a vásárló url minden esetben https://<szervernév>/customer.saki

CIB BANK
Intesa Sanpaolo Group

# Titkosítással kapcsolatos kérdések

**K:** A teszt szerveren tökéletesen működött a titkosítás/kititkosítás. Az éles szerveren miért nem?
**V:** A teszt és éles működéshez a bank két külön kulcsot biztosít. Ezek nevei azonosak, tartalmuk azonban kötelezően eltérő. A webáruházat üzemeltető felelőssége, hogy a kulcsok a megfelelő helyükre kerüljenek.

**K:** Használható-e az IEB0001 azonosító a hozzá kapott titkosítókulccsal?
**V:** Nem. Minden kereskedő egyedi azonosítót kap melyek egyike sem lehet IEBXXXX. A titkosítókulcs, melyet a dokumentációhoz és az ekiCrypt titkosítómodulhoz csatoltunk, pusztán a csatolt alkalmazás működésének tesztelésére alkalmas, a banki kommunikációra nem.

**K:** A,B és C üzenet tökéletesen működik a banki kapcsolatban, de X és Y nem, ez miért lehet?
**V:** Kérjük győződjön meg arról, hogy minden kérést ugyanazzal a kulccsal titkosítanak. A teszt és éles kulcsok azonos nevei elvileg kiküszöbölik az azonos forrásból származó üzenetek különböző kulccsal történő titkosítását, elosztott rendszereknél (pl felhő alapú szolgáltatások) azonban elképzelhető, hogy a szerverpark némely elemeire nem sikerült a kulcsok telepítése.

**K:** Áttértünk Windows operációs rendszerű kiszolgálóról Unix alapúra. Miért nem működik a titkosítás?
**V:** A Unix alapú rendszerek a file neveknél különbséget tesznek a kis és nagybetűk között. Amennyiben a titkosító alkalmazás UER_NOFILE hibakóddal tér vissza, célszerű ellenőrizni a file nevét. A file webszerver számára elérhetetlensége is okozhat problémát. A telepítés során a webszerver technikai felhasználójának (és csak annak!) olvasási jogot kell biztosítani a kulcsfilera és az azt tartalmazó könyvtárra.

**K:** A vásárlóval együtt visszaérkező üzenet (MSGT21) időnként miért kititkosíthatatlan?
**V:** Az ekiCrypt függvénykönyvtár és az arra épülő sakide alkalmazás alapértelmezés szerint urlkódolt üzeneteket képes kezelni. A visszatérő üzenetet a webszerverek urldekódolhatják, emiatt az üzenetben szereplő + és / jelek miatt a nevezett alkalmazáscsomag hibát adhat. Javasoljuk a beérkező üzenet automatikus urlkódolását, mivel ez az urldekódolt üzenetet „kijavítja”, az eleve urlkódolt üzeneten pedig nem változtat.

**K:** A titkosító algoritmus egyaránt használható 32 és 64 bites rendszereknél?
**V:** A virtuális gépeket használó technológiák illetve a hardver sajátosságait „eltakaró” nyelvek esetén igen. Hardver-specifikus binárisok esetén mellékeltünk mind 32, mind 64 bites verziót.

**K:** A sakide alkalmazás az operációs rendszer frissítése óta hibát jelez, mit tegyek?
**V:** Előfordulhat, hogy az operációs rendszerrel együtt módosultak olyan (jellemzően string és memóriakezelő) rendszerfüggvények, melyek az eltérő hivatkozások miatt hibát eredményezhetnek. Ebben az esetben kérjük vegye fel a kapcsolatot a bank ügyintézőjével, megadva a hiba reprodukálásának lépéseit, a régi és az új operációs rendszer valamint a futtatásukhoz használt hardver pontos paramétereit.

**K:** Hogyan lehet ellenőrizni a CIB Bank fizetőoldalának hitelességét?
**V:** Elsődlegesen a böngésző címsorában található zöld lakatra kattintva. A böngésző ekkor minden elérhető információt közöl a kapcsolat titkosságáról, valamint lehetőséget ad az ún certificate-lánc (certificate chain) megtekintésére is (bővebb információ itt található). A CIB Bank a titkosításhoz szükséges certificate-et a Symantec Corp.-tól vásárolja, ezt a fizetőoldal jobb felső sarkában található „Norton-secured" logóra kattintva ellenőrizheti. Amennyiben a fizetőoldal a böngésző szerint nem biztonságos, kérjük győződjön meg arról, hogy a böngésző legfrissebb verzióját használja-e (régebbi verziók hiányos listával rendelkezhetnek az ún top level root CA certificate-kről), és amennyiben igen, kérjük haladéktalanul tájékoztasson minket.

**K:** A sakide alkalmazás miért nem ad semmilyen kimenetet?
**V:** Sikeres futás esetén az alkalmazás a standard kimenetre írja az eredményt, hiba esetén viszont nem lehet kimenet. A pontosabb hibakereséshez az alkalmazást verbose módban célszerű indítani (-v), ekkor a hibaüzenet a standard error csatornára kerül.

**K:** A sakide program UER_BADURL hibakóddal tér vissza, mi a probléma?
**V:** Kérjük ellenőrizze, hogy helyes irányban próbálta meg a titkosítást alkalmazni. A –e paraméter segítségével titkosít, a –d paraméterrel kititkosít. Fordított esetben az alkalmazás UER_BADURL hibát ad.

**K:** A sakide program (vagy a saját rendszerben implementált alkalmazás) a titkosítás eredményeként a következő titkosított értéket adta: PID=<kereskedőazonosító>&CRYPTO=1&DATA=AwMD, amire a bank hibaüzenetet adott. Mi a gond az üzenettel?
**V:** Az AwMD az üres üzenet titkosítása, tehát a bolti algoritmus bemenő értéke sérült a feldolgozás során.

**K:** A bank szervere támogatja az SSL kapcsolatot?
**V:** Az SSL titkosításban rejlő hiba (lásd POODLE attack) miatt a bank nem támogatja az SSL titkosítást. Helyette a TLS titkosítást ajánljuk, annak minden elérhető verziójával.

**K:** A kereskedői url-t hívva miért fut hibára a TLS kapcsolat?
**V:** A kereskedői url csak http protokollon keresztül érhető el.

CIB BANK
Intesa Sanpaolo Group

# Fizetési folyamattal kapcsolatos kérdések

**K:** Mikor tekinthető egy tranzakció sikeresen befejezettnek?

**V:** Csak akkor, ha a bank a lezáró üzenetre (MSGT32) adott válaszában (MSGT31) az authorizációt sikeresnek jelöli (RC=00). Önmagában a lekérdező üzenetre (MSGT33) adott válaszban (MSGT31) szereplő válasz (RC=00) nem elég.

**K:** A tranzakciók rendre időtúllépés miatt meghiúsulnak, mit lehet ez ellen tenni?

**V:** A lezáráshoz szükséges üzenet (MSGT32) a bank szempontjából csak abban az esetben fogadható el, ha az authorizáció már megtörtént (tetszőleges eredménnyel). Az authorizáció megtörténtét az áruház a vásárló visszaérkezésekor (MSGT21) nyugtázhatja, illetve ennek elmaradása esetén (pl. a vásárló bezárja a böngésző ablakot ezzel meghiúsítva a visszairányítást) az erre a célra fenn tartott üzenet (MSGT33) segítségével ellenőrizheti a tranzakció állapotát, és az authorizáció befejeztével a vásárló visszaérkezése nélkül is megerősítheti azt.
Javasolt a következő algoritmus szerint eljárni:

1. A kereskedő inicializálja a tranzakciót (MSGT10) egy új TrID azonosítóval
2. A kereskedő feldolgozza az inicializálás eredményét (MSGT11) és amennyiben nem engedélyezett (RC!=00), a folyamatot az első lépéstől újrakezdi, maximum 3x. A 3. próbálkozás után a folyamatot hibaüzenettel megszakítja
3. A kereskedő a vásárlót a banki fizetőoldalra irányítja (MSGT20)
4. A kereskedő fogadja a banktól visszatérő vásárlót (MSGT21)
5. A kereskedő ellenőrzi, hogy a tranzakció lezárható állapotban van-e (MSGT33)
6. Ha lezárható (fenti felsorolás 2. és 4. esete, vagyis RC=00 illetve RC=<bármi más>), lezárja (MSGT32), a válaszüzenetben (MSGT31) található adatokat megjeleníti, és a folyamatot befejezi
7. Ha nem zárható le (fenti felsorolás 3. esete, vagyik RC=TO), akkor a MSGT33 üzenetre adott bank válasz MSGT31 üzenetben található adatokat megjeleníti és a folyamatot befejezi

A bank válasza (MSGT31) MSGT33-ra, értelmezése és a lehetséges követő lépések:

| RC érték | Magyarázat | Megerősítés | Újabb MSGT33 |
|---|---|---|---|
| **PR** | Az authorizáció még folyamatban van | nem lehetséges | szükséges |
| **TO** | Az authorizáció időtúllépés miatt meghiúsult | nem lehetséges | nem szükséges |
| **00** | Az authorizáció lezárult, a foglalás sikerült | szükséges | nem szükséges |
| **Bármi egyéb** | Az authorizáció lezárult, a foglalás nem sikerült | nem szükséges | nem szükséges |

**K:** Mi történik az időtúllépés miatt meghiúsult tranzakciókkal?

**V:** A bank minden ilyen esetben ún. reverzálást kezdeményez, melynek lényege, hogy a vásárló számláján lefoglalt összeget ismét a vásárló szabad rendelkezésére bocsátjuk. A tranzakciót ezután megerősíteni már nem lehet, a státusz lekérdező üzenetre (MSGT33) RC=TO érték lesz a válasz.

**K:** A vásárló üres oldalt kap a Fizetés gomb megnyomása után, ez mi miatt lehet?

**V:** A fizetés több lépésből áll, ennek során a vásárló böngészője több érintett társaság (CIB Bank, MasterCard, VISA illetve a kártyát kibocsátó bank) weboldalán is megfordulhat. Az utolsó érintett oldal a böngésző címsorában (Location bar) szerepel, ez alapján határolható be, hogy a feltételezett hiba melyik társaság webszerverén fordult elő. Kérjük minden ilyen esetet haladéktalanul jelezzenek felénk, a Location bar-ban található szervernévvel együtt (ha paraméter is szerepel benne, azt kérjük takarják

ki), a minél gyorsabb hibaelhárítás érdekében. A biztonság kedvéért kérjük a Vásárlót, hogy hiba jelentése előtt győződjön meg internetkapcsolata megfelelő működéséről.

**K:** Miért kapok RC=NT értéket a bank válaszában (MSGT31)?
**V:** NT értéket a banki szerver akkor ad, ha nem talált a kérésnek megfelelő tranzakciót. Kérjük ellenőrizze, hogy a kérésben helyes kereskedő azonosítót, tranzakció azonosítót és összeget használt.

**K:** Miért kapok RC=X0 értéket a bank válaszában (MSGT31)?
**V:** Amennyiben a vásárláshoz használt kártya rendelkezik 3D Secure védelemmel (bővebben itt és itt olvashat róla), a CIB bank a vásárlót minden esetben a kibocsátó bankhoz irányítja authentikációra. Amennyiben az authentikáció sikertelenül zárul, a CIB bank a tranzakciót X0 válaszkóddal elutasítja.

**K:** Mennyi idő után tekinthető az authorizáció időtúllépés miatt meghiúsultnak? Változtatható-e ez az időtartam? Letiltható-e?
**V:** Az authorizáció alapértelmezés szerint 10 perc után minősül időtúllépés miatt meghiúsultnak. Letiltani nem lehet, de a megfelelő üzenetek kombinációjával a sikeres authorizációt meg lehet erősíteni (MSGT33 és MSGT32 üzenetek), az időtúllépés bekövetkezte előtt.

**K:** Az átirányítás megtörténhet az inicializációs üzenettel (MSGT10)?
**V:** Nem, mert a vásárló böngészője nem képes a bank titkosított válaszát (MSGT11) értelmezni, így a fizetési folyamat ennél a lépésnél meg fog szakadni. Átirányítani csak az arra a célra szánt üzenettel (MSGT20) szabad a vásárlót.

**K:** Átirányítás nélkül, a vásárló helyett letöltve is megjeleníthető a fizetőoldal?
**V:** Sikeres inicializációt követően minden esetben át kell irányítani a vásárlót a bank fizetőoldalára.

**K:** Lehetséges előre inicializálni tranzakciót és csak valamennyi idő elteltével a fizetőoldalra irányítani a vásárlót?
**V:** A tranzakciót a bank az előre definiált időtúllépés után lezárja.

**K:** Lehetséges többször megerősíteni (MSGT32) authorizációt?
**V:** Az első megerősítéssel a bank az authorizációt lezárja, azon módosítani többször nem lehet. Minden, ezután küldött megerősítő üzenet hibát eredményez.

**K:** A vásárlót a fizetés után vissza lehet irányíttatni nem standard portra is?
**V:** Igen, az inicializáló üzenetben (MSGT10) az URL értékénél a szervernév után kell megadni a portszámot, kettősponttal elválasztva (http://server.dom:<port>/). Ügyelni kell azonban arra, hogy a vásárlók többségénél a hálózati szabályok ezt a kapcsolatot nem engedélyezik.

**K:** A vásárló jelezte, hogy sokáig (10-60 másodperc) tart, amíg a kártyaadatok beírása és a Fizetés gomb megnyomása után visszajut a webáruházba. Mi történik ilyenkor?
**V:** Miután a vásárló megadta a kártyainformációkat, a bank a vásárlót továbbirányítja a kártyatársaságok, rajtuk keresztül pedig (amennyiben szükséges) a kibocsátó bankhoz, hogy a tranzakcióhoz tartozó

megerősítő kódot (ez lehet általános vagy egyszer használatos jelszó) megadhassa (3D Secure). MasterCard és Maestro típusú kártyák esetében az átirányítás mindenképp megtörténik, ez átlagosan 5-10 másodperccel növeli meg az authorizáció idejét. A kód megadását követően a bank authorizálja a tranzakciót (ez további szintén 5-10 de maximum 40 másodperc), majd ezt követően irányítja vissza a vásárló böngészőjét a webáruházba.

CIB BANK
Intesa Sanpaolo Group

# Egyéb kérdések

**K:** A bank válaszüzenete miért csak RC=SXX vagy RC=DXX kódot tartalmaz?

**V:** A bank szervere akkor tud titkosított válaszüzenetet küldeni, ha sikerült a kereskedő üzenetét feldolgoznia. Hiba esetén a hiba típusának megfelelő hibakódot ad, ezeknek a listája a Reference guide-ban érhető el. Ilyen esetekben célszerű meggyőződni arról, hogy az üzenet a megfelelő paraméterek felhasználásával készült, a folyamat megfelelő lépéseként lett-e elküldve, a megfelelő titkosítókulcs felhasználásával. Kiemelendő, hogy jelen dokumentációhoz csatolt titkosítókulcs egyik banki szerverrel való kommunikációra sem alkalmas, pusztán az alkalmazás működésének tesztelésére való.

**K:** Az inicializáló üzenetben (MSGT10) milyen URL értéket lehet alkalmazni?

**V:** Teljes értékű domain nevet (FQDN), ami nincs felparaméterezve. A teljesség igénye nélkül néhány példa:

| URL | Elfogadható |
|---|---|
| server1 | Nem |
| http://server1 | Nem |
| http://server1.hu | Nem |
| http://server1/ | Nem |
| http://server1.hu/ | Igen |
| https://server1.hu/ | Igen |
| ftp://server1.hu/ | Nem |
| http://127.0.0.1/ | Igen |
| http://server1.hu/path/script.ext | Igen |
| http://server1.hu/path/script.ext?param=value | Nem |
| http://http://server1.hu/ | Nem |

**K:** A tranzakció azonosítóba miért került a banki válaszban + jel?

**V:** Az azonosító kötelezően 16 karakter hosszú kell legyen. Amennyiben a kereskedő szoftvere ennél rövidebbet küld, a bank szervere automatikusan 16 karakter hosszúra egészíti ki, szóközökkel, melyek urlkódolt formája a + jel.

**K:** Miért kapok az MSGT11 üzenetben RC=02 értéket?

**V:** Az inicializáló üzenetben (MSGT10) küldött tranzakció azonosító már foglalt. Az azonosítót minden fizetés megkezdése előtt pszeudovéletlen értékként szükséges előállítani. A modern programnyelvi verziók minden véletlenszám-generálás előtt végrehajtanak ún reseed lépést (a véletlenszám-képzés alapjául szolgáló érték újragenerálása), célszerű azonban ezt explicit módon, kényszerítve is végrehajtani az azonosító számítása előtt.

**K:** A fizetendő összeget milyen formában kell megadni?

**V:** Magyar forint esetén egész számként, Euró esetében pedig két tizedesjegy pontossággal. Utóbbi esetben a két tizedesjegy minden esetben kötelező. Az egészrészt a törtrésztől pont választja el.

**K:** A tranzakció adatait el kell tárolni?
**V:** Igen, ez egyrészt előfeltétele a tranzakciók sikerességének, másrészt nagyban segít az esetleges későbbi vásárlói tájékoztatásban.

**K:** Milyen formában kell átadni a bank számára a tranzakcióhoz tartozó kosár adatait?
**V:** A bank nem fogad és nem tárol kosár adatot, csak a fizetéshez szükséges információkat (MSGT10)

**K:** Milyen formában kell átadni a bank számára a vásárló személyes adatait?
**K:** Amennyiben a vásárló előzetesen, explicit jóváhagyta (GDPR), a vásárló neve, számlázási címe és e-mail címe átadható a bank számára, a PSD2-re épülő EMV 3DS authentikáció gyorsításának érdekében. A mezők típusát és megengedett értékkészletüket a Technikai dokumentáció tartalmazza.

**K:** Célszerű-e a vásárlónak e-mailt küldeni a tranzakció eredményéről?
**V:** Igen. Előfordulhat, hogy a vásárló nem várja meg az authorizáció eredményét és becsukja a böngészőjét, emiatt az azonnali tájékoztatás lehetetlenné válik. Az e-mailben ugyanazokat az adatokat szükséges küldeni, melyeket a visszaigazoló weblapon is láthat a vásárló (tranzakció azonosító, összeg, devizanem, válaszkód leírással és engedélyszám).

**K:** A vásárlót a fizetés megkezdése előtt azonosítani kell?
**V:** Igen, ez előfeltétele a sikeres banki tesztnek. Az azonosítás tetszőleges, általánosan elfogadott módon (egyszeri vagy állandó jelszó megadásával, illetve biometrikus adatok ellenőrzésével) történhet.

**K:** A vásárlóazonosító (UID) tartalmazhat e-mail címet?
**V:** Az UID mező csak a specifikációban megengedett karaktereket tartalmazhat (kis és nagybetű, szám, kötőjel, aláhúzás illetve szóköz).

**K:** A kommunikációnál használt paraméterek escape-elhetőek-e, illetve tartalmazhatnak-e extra karaktereket (pl sortörés)?
**V:** Sem a titkosítatlan sem a titkosított paraméterek nem escape-elhetőek (az urlkódolás miatt egyébként sincs rá szükség) és nem is tartalmazhatnak ún whitespace karaktereket (pl sortörés vagy tabulátor).

**K:** A vásárló tájékoztatásakor furcsán jelennek meg a karakterek, ez mitől lehet?
**V:** A bank szervere az üzeneteket, így az authorizáció eredményét (MSGT31, RT paraméter) is ISO-8859-2 kódolással küldi. Amennyiben a bolt ettől eltérő kódolást (pl UTF-8) használ, az értékeket explicit konvertálni kell megjelenítés előtt.