Elektronikus Kártyatranzakciók az Interneten

A CIB Bank Zrt.

Internetes kártyaelfogadás szolgáltatás technikai dokumentációja

Verziószám: 1.49

A CIB Bank internet technológián alapuló elektronikus kereskedelmi megoldásának dokumentációja.
A jelen dokumentációban leírt módszerek és megoldások a CIB eCommerce szolgáltatásának alapját képezik. A CIB a TLS alapú kártyaelfogadás keretein belül a dokumentumban leírtaktól eltérő módszerekkel nem engedélyezi tranzakciók lebonyolítását.

CIB BANK

TARTALOM

Bevezető

Jelen dokumentum a CIB Bank Zrt által üzemeltetett internetes kártyaelfogadás szolgáltatás fejlesztői leírását tartalmazza.

Gyakori kifejezések

Az alábbiakban a dokumentációban előforduló kifejezések definíciói találhatóak:

Kereskedő	érvényes eCommerce szerződéssel rendelkező természetes vagy jogi személyiség
Webáruház	a Kereskedő (vagy megbízottja) által üzemeltetett informatikai szolgáltatás, melyben termékek és szolgáltatások vásárolhatóak bankkártyával
Vásárló	a kártyás fizetést végrehajtó személy, illetve informatikai értelemben megfeleltetése (pl. webböngésző)
Authorizáció	a vásárló kártyáján a vásárlás összegének elkülönítése
Terhelés	az authorizáció véglegesítése, az elkülönített összeg könyvelése (a kereskedő számláján a jóváírás nem azonnal történik)
Reverzálás	az authorizáció visszavonása, az elkülönített összeg szabad rendelkezésre bocsátása
Visszautalás	a terhelt tranzakció ellentétes irányú könyvelése
Tranzakció	a teljes fizetési folyamat, beleértve a vásárló jelenlétét nem igénylő lépéseket is
3D Secure	a fizetés biztonságát növelő opcionális szolgáltatás, mely a tranzakcióhoz egy egyedi kódot is társít, melyet a vásárló a kártyától függetlenül birtokol (pl sms-ben kap a kibocsátó banktól).
Inicializálás	a webáruház üzenete a banki szerver felé a fizetési igényről
Átirányítás	a vásárló böngészője kapcsolati végpontjának megváltoztatása a bank szerverére
Visszairányítás	a vásárló böngészője kapcsolati végpontjának megváltoztatása a webáruházba
Lekérdezés	a tranzakció és a fizetés pillanatnyi állapotának megismerése
Lezárás	a tranzakció authorizációs részének megerősítése. A bank a lezáratlan tranzakciókat minden esetben reverzálja!
Titkosító kulcs	A Bank által a Kereskedő rendelkezésére bocsátott file(ok), mely(ek) a Kereskedő-Bank kommunikáció során biztosítják a küldött-fogadott üzenetek bizalmasságát
(3)DES	Data Encryption Standard. A Kereskedő-Bank kommunikáció során használt titkosítás algoritmusa
TLS	Transport Layer Security. A Vásárló-Bank kommunikáció során használt titkosítás algoritmusa

CIB BANK

A fizetési folyamat

Authorizáció

Az alábbiakban leírt folyamat a teljes tranzakciós életciklusnak csak a fizetési (authorizáció , más néven blokkolás illetve foglalás) részét fedi le, a tranzakció visszavonását/visszautalást lásd lentebb.

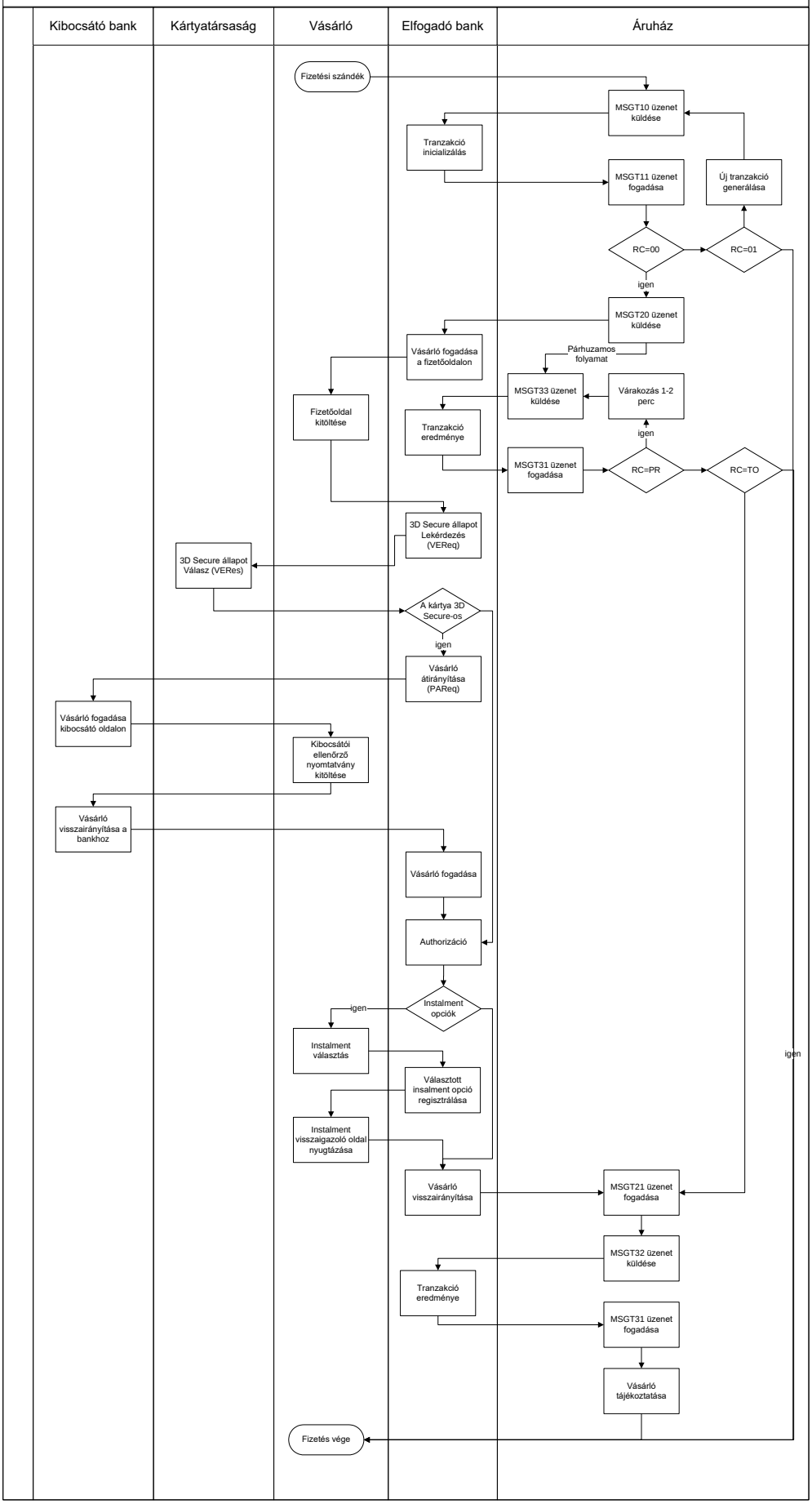
1. A vásárló a kereskedő webáruházában (a továbbiakban „áruház") kiválogatja a szükséges árukat, regisztrálja magát és jelzi a kereskedő felé fizetési szándékát
2. Az áruház eltárolja a fizetéshez szükséges adatokat, majd egyedi azonosítóval ellátva (TRID) elküldi a bank szerverének (MSGT10)
3. A bank ellenőrzi és regisztrálja a kérést, majd ezek eredményéről nyugtázó választ küld (MSGT11)
4. Negatív nyugtázás esetén az áruház a tranzakciót befejezettnek tekinti. Opcionálisan felkínálhatja a lehetőséget új tranzakció indítására
5. Pozitív nyugtázás esetén az áruház átküldi a vásárlót a bank szerverén található fizetőoldalra (MSGT20)
6. A vásárló a fizetőoldalon megadja a fizetéshez szükséges kártyaadatokat
7. A bank kártyatípustól függően továbbküldheti a vásárlót a kártya kibocsátójához további ellenőrzésre. Az ellenőrzés után a vásárló visszakerül a bankhoz
8. A bank a vásárlótól és a kibocsátó banktól kapott információk birtokában foglalást kezdeményez a vásárló kártyáján
9. A foglalás befejeztével a bank a vásárlót visszaküldi az áruházba, az áruház által megadott címre (MSGT21)
10. Az áruház a bank szerverétől információt kér a foglalás sikerességéről (MSGT32)
11. A bank válaszüzenetben elküldi az áruház részére a foglalás adatait (MSGT31)
12. Az áruház közli a vásárlóval a banktól kapott adatokat

Amennyiben az áruház a vásárló visszaküldése (9) után egy előre definiált időn belül (alapértelmezetten 10-15 perc) nem zárja le (MSGT32) a tranzakció eredményét (10), a bank a foglalás feloldását kezdeményezi (reverzálás) a kibocsátó banknál.
Az áruház a sikeres inicializálást követően bármikor lekérdezheti a tranzakció állapotát (MSGT33). Az erre adott banki válasz (MSGT31) struktúrája a CNUM mezőn kívül megegyezik a megerősítés üzenettel, de attól eltérően nem jár a tranzakció lezárásával. Amennyiben az áruházi alkalmazás támogatja, célszerű a vásárló átirányítását követően adott időközönként lekérdezni a tranzakció állapotát. Amennyiben az a bank szerint időtúllépés miatt meghiúsult, az áruház is lezárhatja sikertelen foglalási kísérletként a saját rendszerében.

A fizetési folyamat lépéseit az alábbi ábra szemlélteti:

CIB BANK

3 szereplős fizetési folyamat



CIB BANK

Authorizáció utáni üzenetek

Sikeres authorizáció esetén az áruház a következő kiegészítő üzeneteket alkalmazhatja a tranzakcióra:

- Bármikor lekérdezheti a tranzakció státuszát (MSGT70). A banki válaszban (MSGT71) található STATUS mező értéke jelzi, hogy foglalás alatt van, visszavont, terhelt, vagy visszautalt (lásd 71-es üzenet STATUS mező leírás).
- Visszavonhatja a foglalást (MSGT74). Hatására nem történik terhelés, a vásárló visszakapja a számláján lefoglalt összeget
- Beállíthatja terhelt tranzakció visszautalandó részösszegét (MSGT80)
- Visszautalhat terhelt tranzakciót (MSGT78), ekkor az alapértelmezett, vagy az előre beállított részösszeg kerül visszautalásra

Üzenetek felépítése

A háromszereplős modell megköveteli, hogy a tranzakció (vásárlási folyamat) során a három fél közül egyszerre mindig csak kettő legyen kapcsolatban egymással. Ennek során a vásárló jellemzően egy weboldalon keresztül kommunikál mind a kereskedővel, mind pedig a bankkal, a kereskedő és a bank pedig a későbbiekben részletezett tartalmú, titkosított üzeneteken keresztül kommunikál egymással. Az üzeneteket, amennyiben azok nem a vásárló átirányítására vonatkoznak, HTTP GET vagy POST metódussal küldi a banknak.

Az üzenet általános formája:

`https://server.dom/path/to/script.ext?key1=value1&key2=value2...`

ahol `key<n>` a paraméter neve, `value<n>` pedig a hozzá tartozó érték.

A titkosítás a kereskedő-bank kommunikációban 3DES, a vásárló-bank kommunikációban TLS alapú. A 3DES titkosításhoz a bank ad kulcsot, külön teszt és éles üzemhez. A mellékletek részét képezi a bank által az üzemeltető rendelkezésére bocsátott titkosító modul (sakicrypt), valamint az ennek tesztelésére alkalmas program (sakide). A titkosítás lépései az 5.2 fejezetben olvashatóak.

A banki válasz a kereskedő számára a kérésekre mindig a hívott oldal törzsében (content) érkezik, akkor is, ha a http válaszkód nem 200. Az egyetlen kivétel, amikor a banki üzenet a hívott url paramétereiben érkezik, a vásárló visszairányítása a fizetőoldalról a kereskedőhöz (MSGT21).

CIB BANK

Meződefiníciók

Az egyes üzenetekben előforduló mezők:

Mező jelentése	Azonosító	Hossz
Titkosítás típusa	CRYPTO	1
Titkosított üzenet	DATA	Max 255
Üzenettípus	MSGT	2
Bolt azonosító	PID	7
Tranzakció azonosító	TRID	16
Ügyfél azonosító	UID	11
Összeg	AMO	Max. 16
Pénznem	CUR	3
Időpecsét	TS	14
Válaszkód	RC	2
Válasz szöveg	RT	Max 255
Engedélyszám	ANUM	Max. 6
Kártyaszám	CNUM	Max 19
Authorizáció típusa	AUTH	1
URL	URL	Max. 255
Nyelvkód	LANG	2
Történet	HISTORY	Max. 255
Megjegyzés (Kereskedői)	EXTRA01	Max. 50

A mezők részletes kifejtése:

CRYPTO

Hossz: 1
Reguláris kifejezés: [13]

Leírás: A titkosítás típusa. Csak a titkosított üzenetben jelenik meg, a fogadó számára jelzi, milyen módon titkosított az üzenet. A kereskedő<->bank kommunikációban az értéke mindig 1.

Elfogadott értékek:

1: 3DES (csak kereskedő-bank kommunikáció)
3: TLS (csak vásárló-bank kommunikáció)

DATA

Hossz: max. 255
Reguláris kifejezés: [a-zA-Z0-9/%]{0,255}

Leírás: Az eredeti üzenet titkosítva. Csak a titkosított üzenetben jelenik meg, a PID és CRYPTO értékkel együtt.

MSGT

Hossz: 2
Reguláris kifejezés: [0-9]{2}

Leírás: Az üzenet típusát definiálja. Egyértelműen meghatározza a további paraméterek előfordulását.

PID

Hossz: 7
Reguláris kifejezés: [a-zA-Z]{3}[01][0-9]{3}

Leírás: A kereskedő azonosítója. A bankkal történő kommunikációban szereplő összes üzenet tartalmazza. Az első 3 karakter azonosítja az áruházat (szolgálatót), a további 4 számjegy az áruházon belül az egyes boltokat. A 4 számjegy közül az első azonosítja a virtuális POS terminál elepértelmezett devizanemét is, jelenleg a következő értékek elfogadásával:

0: HUF
1: EUR

A terminálokon jelenleg csak az alapértelmezett devizanemekben történik elfogadás (lásd CUR mező).

TRID

Hossz: 16
Reguláris kifejezés: [0-9]{16}

Leírás: A tranzakció egyedi azonosítója. A tranzakciót annak teljes hosszában (inicializációtól a lezárásig) azonosítja, minden titkosítatlan üzenetben kötelezően szerepel. Az áruház generálja, minden fizetési szándék inicializálása előtt. A generálás során ajánlott pszeudovéletlenszám-generátort alkalmazni. Nem tartalmazhat csak szóközt.

UID

Hossz: 11
Reguláris kifejezés: [a-zA-Z0-9\-_]{11}

Leírás: A vásárló azonosítója a kereskedő rendszerében. Amennyiben az áruházban nem kötelező a regisztráció, használható konstans érték is (pl. CIB12345678). Nem tartalmazhat egymás után több kötőjelet.

AMO

Hossz: max. 16
Reguláris kifejezés: [0-9 \.]{16}

Leírás: A fizetendő összeg. A kötelező tizedesjegyek száma a tranzakció devizanemétől függ (HUF esetén 0, EUR esetén 2). A törtrészt az egészrésztől ponttal kell elválasztani. Egész összeg esetén nincs sem tizedespont, sem törtrész.
Az egyes üzenetekben előfordulhat több összeg is, ezek mindegyike AMO előtaggal rendelkezik.

Példák:

1000 forint: 1000
10 euró: 10.00

CUR

Hossz: 3
Reguláris kifejezés: [a-zA-Z]{3}

Leírás: A tranzakció devizaneme, ISO 3166 szabvány által előírt betű alapú formában.

Elfogadott értékek:

HUF (magyar forint)
EUR (euró)

TS

Hossz: 14
Reguláris kifejezés: [0-9]{14}

Leírás: A tranzakció inicializálásának időpontja a kereskedő oldalán. Az időpontot a következő formában kell megadni: ÉÉÉÉHHNNÓÓPPMM. A rendszer a szökőmásodpercet elfogadja, ekkor a másodperc értéke 60.

Példa:
2012. augusztus 31, 23:59:59: 20120831235959

RC

Hossz: 2
Reguláris kifejezés: [A-Z0-9]{2}

Leírás: Az aktuális kérés végrehajtásának eredménye. A lehetséges értékek pontos értelmezése üzenettípus-függő, ezért ezek részletesen az üzenettípusoknál találhatóak.

Lehetséges értékek:
00: Sikeres végrehajtás
Bármi más: Hiba történt a végrehajtás során

RT

Hossz: max. 255
Reguláris kifejezés: [.]{0,255}

Leírás: Authorizáció esetén a válaszkód szöveges értelmezése a kereskedő és a vásárló számára. Az üzenet nyelve megegyezik a LANG paraméterben megadottal, tartalmazhat url kódolt latin2 (európai nyelvek esetén) és unicode (nem európai nyelvek esetén) karaktereket.

ANUM

Hossz: max 6
Reguláris kifejezés: [a-zA-Z0-9]{0,6}

Leírás: Az authorizáció engedélyezésének azonosítója kibocsátó oldalon. Az ANUM a kibocsátónál sem egyedi azonosító, kérdés esetén célszerű a tranzakció összegével és időpontjával társítani.

AUTH

Hossz: 1
Reguláris kifejezés: [0]

Leírás: Az authorizáció csatornájának típusa. A 0 érték jelöli a webes authorizációt.

URL

Hossz: max 255
Reguláris kifejezés: http[s]?://.+\..+/
Leírás: kereskedői url, melyre a bank a vásárló böngészőjét irányítja a fizetés végeztével. A mező nem tartalmazhat paramétert (`...?param1=value1&param2=value2...`), abszolút elérési utat kell tartalmazzon, és a reguláris kifejezésen felül url-ként kiértékelhető stringet kell képezzen (RFC 2396 és RFC 2732 alapján)

Példa: `http://server.domain.com/path/to/script.ext`

LANG

Hossz: 2
Reguláris kifejezés: [a-zA-Z]{2}

Leírás: A tranzakció során használt nyelv kódja. A vásárló böngészőjében megjelenő fizetőoldal, valamint az authorizáció eredménye ezen a nyelven olvasható.

Elfogadott értékek:

- `HU`: magyar
- `EN`: angol
- `DE`: német
- `IT`: olasz
- `FR`: francia
- `ES`: spanyol
- `PT`: portugál
- `PL`: lengyel
- `CZ`: cseh
- `SK`: szlovák
- `RO`: roman

HISTORY

Hossz: max 255
Reguláris kifejezés: [0-9,]{0,255}

Leírás: A tranzakció során végrehajtott folyamatok egyes állapotainak listája. Az állapotokat kódok jellemzik, a sorrend balról jobbra olvasandó egyes állapotok egymástól vesszővel vannak elválasztva.

Példa: `10,11,20,21,30`

Lehetséges értékek a listában:

- `10`: a vásárló megérkezett a fizetőoldalra
- `11`: a vásárló elküldte a kitöltött fizetőoldalt
- `12`: a vásárló nem engedélyezte a tranzakciót
- `14`: az authorizációs kérést az elfogadó elutasította
- `15`: Sikertelen 3D Secure authentikáció
- `20`: az authorizáció megkezdődött
- `21`: az authorizáció sikerült
- `22`: az authorizációs kérést a kibocsátó elutasította
- `30`: a kereskedő megkapta a tranzakció eredményét
- `55`: a tranzakció időtúllépés miatt kijelölve reverzálásra
- `56`: sikeres reverzálás
- `57`: sikertelen reverzálás

CIB BANK

EXTRA01

Hossz: max 50
Reguláris kifejezés: [0-9a-zA-Z áéíóöőúüűÁÉÍÓÖŐÚÜŰ"\+!\%/\(\)~`<>#\{\},\.\-
>*:_\\|\[łŁ$ß¤\]]{0,50}

Leírás: A tranzakcióra jellemző, opionális extra parameter mely a kereskedői elszámolásban segít azonosítani a trazakciót.

CIB BANK

Üzenettípusok tartalma

A Bank eCommerce szervere az alábbi listában szereplő üzeneteket értelmezi. A felsorolt paraméterek a titkosítatlan üzenetben szerepelnek. A nem kötelező mezők “(opcionális)” utótaggal kerültek megjelölésre.

Tranzakció inicializálás (MSGT10)

- PID
- TRID
- MSGT, értéke 10
- UID
- AMO
- CUR
- TS
- AUTH
- LANG
- URL
- EXTRA01

Tranzakció inicializálás válasz (MSGT11)

- MSGT, értéke 11
- PID
- TRID
- RC, lehetséges értékei:
    - 00: Sikeres inicializálás
    - 01: Az inicializálás egyéb technikai okok miatt nem sikerült
    - 02: A TRID már foglalt

Vásárló átirányítása a fizetőoldalra (MSGT20)

- MSGT, értéke 20
- PID
- TRID

Vásárló visszairányítása a fizetőoldalról a kereskedőhöz (MSGT21)

- MSGT, értéke 21
- PID
- TRID

Tranzakció eredményének lekérdezése megerősítéssel és lezárással (MSGT32)

- MSGT, értéke 32
- PID
- TRID
- AMO

Tranzakció eredményének lekérdezése (MSGT33)

- MSGT, értéke 33
- PID
- TRID
- AMO

Tranzakció eredményének lekérdezése válasz (MSGT31)

A banki szerver mind az MSGT32-es, mind az MSGT33-as kérésre MSGT31 választ ad, az alábbi paraméterekkel:

- MSGT, értéke 31
- PID
- TRID
- AMO
- RC, lehetséges értékek:
    - 00: Sikeres authorizáció
    - PR: Az authorizáció még nem történt meg
    - TO: A tranzakció időtúllépés miatt meghiúsult
    - Bármi más: Sikertelen authorizáció (a hibakódok osztályozása a FAQ-ban található)
- RT
- ANUM
- CNUM (csak 33-as üzenetre válaszként)

Az MSGT33 üzenet RC=00 értéke **tájékoztató jellegű**, amennyiben a bolt nem zárja le MSGT32 üzenet segítségével a tranzakciót, a bank a timeout-ot követően a tranzakciót reverzálja. Ezután a további MSGT33 üzenetekre a bank az MSGT31 válaszüzenetben RC=TO értéket ad. A reverzált üzenetet lezárni nem lehet MSGT32 üzenet segítségével (a bank szervere ekkor hibaüzenetet ad). A lehetséges, illetve kötelező üzenetek küldésének mátrixát a GYFK tartalmazza.

Tranzakció lépéseinek lekérdezése (MSGT37)

- MSGT, értéke 37
- PID

- TRID
- AMO

CIB BANK

Tranzakció lépéseinek lekérdezése válasz (MSGT38)

- MSGT, értéke 38
- PID
- RC, lehetséges értékei:
    - 00: A lekérdezés sikeres volt
    - 01: A lekérdezés meghiúsult (ekkor a HISTORY üres)
- HISTORY

Tranzakció állapotának lekérdezése (MSGT70)

- MSGT, értéke 70
- PID
- TRID
- AMO (az eredetileg foglalt összeg)

Tranzakció állapotának lekérdezése válasz (MSGT71)

- MSGT, értéke 71
- PID
- TRID
- AMO
- RC (az eredeti authorizáció eredménye)
- RT
- STATUS, lehetséges értékei:
    - 10: A tranzakció authorizált, de még nem terhelt
    - 30: A tranzakció automatikusan terhelt
    - 40: A tranzakció reverzálva lett (a 74-es üzenet segítségével)
    - 50: A tranzakció vissza lett utalva
    - 60: A tranzakció le lett zárva
    - 99: Hiba történt a feldolgozás során
- CURAMO2, értéke az aktuálisan visszautalható összeg
- ANUM

Authorizált tranzakció reverzálása (MSGT74)

- MSGT, értéke 74
- PID
- TRID
- AMO

CIB BANK

Authorizált tranzakció reverzálása válasz (MSGT75)

- MSGT, értéke 75
- PID
- TRID
- AMO
- STATUS (lásd MSGT71)

Terhelt tranzakció visszautalása (MSGT78)

- MSGT, értéke 78
- PID
- TRID
- AMO, értéke a terhelt összeg

Terhelt tranzakció visszautalása válasz (MSGT79)

- MSGT, értéke 79
- PID
- TRID
- AMO
- RC (az eredeti authorizáció eredménye)
- RT
- STATUS (lásd MSGT71)
- ANUM

Terhelt tranzakció visszautalandó részösszegének beállítása (MSGT80)

- MSGT, értéke 80
- PID
- TRID
- AMOORIG, értéke az utoljára beállított visszautalható összeg (alapértelmezetten 0)
- AMONEW, értéke a beállítani kívánt visszautalható összeg

Terhelt tranzakció visszautalandó részösszegének beállítása válasz (MSGT81)

- MSGT, értéke 81
- PID
- TRID
- AMO, értéke a beállított visszautalható összeg
- STATUS (lásd MSGT71)

CIB BANK

Egyéb, üzenettípusban definiálatlan hibakódok

Amennyiben a bank szervere nem képes értelmezni a kapott adatokat, a válaszüzenet egy titkosítatlan hibakódot tartalmaz. A hibakódok jelentése a következő:

RC=S01	Hiba a kapott adatok fogadásakor.
RC=S02	Hiba az adatokban.
RC=S03	Értelmezhetetlen kérés.
RC=S04	Adatbázis hiba.
RC=S05	Hiba a feldolgozásban.
RC=S06	Kriptográfiai hiba.
RC=D01	Rossz paraméter.
RC=D02	Értelmezhetetlen kérés.
RC=D03	Hibás sorrend. (Nem a megfelel üzenettípusú kérés jött.)
RC=D04	Üzenettípus nem engedélyezett
RC=D05	Az üzenettípushoz tartozó kérés már ki lett szolgálva
RC=D06	Ismeretlen tranzakció.
RC=D07	Hibás adatformátum.
RC=D08	Hiba az adatokban

Az Sxx üzenetek jellemzően a kititkosítás során észlelt hibákat tartalmazzák, a Dxx üzenetek pedig a sikeres kititkosítás utáni, feldolgozás közben észlelteket (jellemzően a beérkező adatok nem a specifikáció szerinti kitöltését).

CIB BANK

Az üzenetek titkosítása

Az áruház és a bank között minden üzenet kötelezően titkosított formában küldendő. A titkosításhoz/kititkosításhoz használható a bank által jelen dokumentáció mellékleteként átadott ekiCrypt függvénykönyvtár, és az azt felhasználó sakide alkalmazás. Amennyiben egyik megoldás sem lehetséges, a titkosítás a lentebb részletezett módon, natív eszközökkel is megvalósítható.

Titkosító kulcs

A titkosítás 3DES alapú. A bank által rendelkezésre bocsátott titkosító kulcsfile a következő információkat tartalmazza:

Név	Hossz (byte)	Leírás
Kulcsazonosító	4	A file neve (EKI'\0')
Kulcsformátum verziója	2	0x00 0x02
Áruházazonosító	4	Megegyezik a file nevével (pl CIB.des esetén CIB'\0')
Kulcs létrehozásának ideje	4	1970.01.01 óta eltelt másodpercek száma
Első kulcs	8	
Második kulcs	8	
Inicializáló vektor	8	

Natív megoldások esetén csak az utolsó 3 elemet szükséges figyelembe venni. Az áruház a fejlesztési ciklus folyamán 3 kulcsot kap:

- Teszt kulcs: integrációs teszteléshez szükséges, kizárólag a bank tesztszerveréhez érvényes
- Éles kulcs: Sikeres tesztelést követően a bank bocsátja ki, kizárólag a bank éles szerveréhez érvényes

A teszt és az éles kulcs neve azonos, ezért célszerű elkülönítve tárolni (pl. külön könyvtárban).

CIB BANK

Titkosító algoritmus

A titkosításhoz a csomagban található sakide segédprogramot, illetve a sakicrypt függvénykönyvtárat ajánlott használni, de szükség esetén lehetséges a protokoll natív eszközökkel kiváltása is. Az alábbiakban látható egy üzenet titkosítása és annak lépésenkénti részeredménye.

Titkosítatlan üzenet összeállítása

A titkosítatlan üzenet a fenti leírásban található paramétereket kell tartalmazza, tetszőleges sorrendben, paraméternév=érték formában, az egyes paramétereket '&' jelekkel összefűzve (query string). A példa során felhasznált üzenet:

```
PID=IEB0001&TRID=1234567812345678&MSGT=10&UID=IEB00000000&AMO=1000&CUR=HUF&TS=20131
231235959&AUTH=0&LANG=HU&URL=http://dev.bolt.hu/shop/frombank.asp
```

A titkosításhoz használt kulcsfile kulcsrésze (utolsó 24 byte 8-as bontásban):

```
00000000   54 E8 17 70 06 E1 18 77   T..p...w
00000008   51 57 C9 3A E0 0A A3 3D   QW.:...=
00000010   E4 48 CC 19 CD 62 EC 7E   .H...b.~
```

Üzenet URL kódolása

Minden karaktert URL kódolni kell, ez alól kivételt képeznek a '&' és '=' karakterek.

```
00000000   50 49 44 3D 49 45 42 30  30 30 31 26 54 52 49 44   PID=IEB0001&TRID
00000010   3D 31 32 33 34 35 36 37  38 31 32 33 34 35 36 37   =1234567812345678
00000020   38 26 4D 53 47 54 3D 31  30 26 55 49 44 3D 49 45   8&MSGT=10&UID=IE
00000030   42 30 30 30 30 30 30 30  30 26 41 4D 4F 3D 31 30   B00000000&AMO=10
00000040   30 30 26 43 55 52 3D 48  55 46 26 54 53 3D 32 30   00&CUR=HUF&TS=20
00000050   31 33 31 32 33 31 32 33  35 39 35 39 26 41 55 54   131231235959&AUT
00000060   48 3D 30 26 4C 41 4E 47  3D 48 55 26 55 52 4C 3D   H=0&LANG=HU&URL=
00000070   68 74 74 70 25 33 41 25  32 46 25 32 46 64 65 76   http%3A%2F%2Fdev
00000080   2E 62 6F 6C 74 2E 68 75  25 32 46 73 68 6F 70 25   .bolt.hu%2Fshop%
00000090   32 46 66 72 6F 6D 62 61  6E 6B 2E 61 73 70         2Ffrombank.asp
```

CIB BANK

CRC32 számítása és hozzáfűzése

Az URL kódolt stringből CRC32 ellenőrzőösszeget kell számítani, majd annak bináris formáját hozzáfűzni a stringhez.

A fenti üzenet CRC32 értéke: `2CAFE8F8`

Az üzenet végéhez fűzve:

```
00000000   50 49 44 3D 49 45 42 30  30 30 31 26 54 52 49 44   PID=IEB0001&TRID
00000010   3D 31 32 33 34 35 36 37  38 31 32 33 34 35 36 37   =1234567812345678
00000020   38 26 4D 53 47 54 3D 31  30 26 55 49 44 3D 49 45   1&MSGT=10&UID=IE
00000030   42 30 30 30 30 30 30 30  30 26 41 4D 4F 3D 31 30   B00000000&AMO=10
00000040   30 30 26 43 55 52 3D 48  55 46 26 54 53 3D 32 30   00&CUR=HUF&TS=20
00000050   31 33 31 32 33 31 32 33  35 39 35 39 26 41 55 54   1312312359&AUT
00000060   48 3D 30 26 4C 41 4E 47  3D 48 55 26 55 52 4C 3D   H=0&LANG=HU&URL=
00000070   68 74 74 70 25 33 41 25  32 46 25 32 46 64 65 76   http%3A%2F%2Fdev
00000080   2E 62 6F 6C 74 2E 68 75  25 32 46 73 68 6F 70 25   .bolt.hu%2Fshop%
00000090   32 46 66 72 6F 6D 62 61  6E 6B 2E 61 73 70 2C AF   2Ffrombank.asp,.
000000A0   E8 F8                                             ..
```

Pad a titkosításhoz

Amennyiben a kapott string hossza nem 8 egész számú többszöröse, a kiegészítéshez szükséges karakterszám bináris formáját (pl ’6’ esetén 0x06) a string végéhez kell fűzni karakterszám sokszor (`... 0x06 0x06 0x06 0x06 0x06 0x06`).

```
00000000   50 49 44 3D 49 45 42 30  30 30 31 26 54 52 49 44   PID=IEB0001&TRID
00000010   3D 31 32 33 34 35 36 37  38 31 32 33 34 35 36 37   =1234567812345678
00000020   38 26 4D 53 47 54 3D 31  30 26 55 49 44 3D 49 45   1&MSGT=10&UID=IE
00000030   42 30 30 30 30 30 30 30  30 26 41 4D 4F 3D 31 30   B00000000&AMO=10
00000040   30 30 26 43 55 52 3D 48  55 46 26 54 53 3D 32 30   00&CUR=HUF&TS=20
00000050   31 33 31 32 33 31 32 33  35 39 35 39 26 41 55 54   1312312359&AUT
00000060   48 3D 30 26 4C 41 4E 47  3D 48 55 26 55 52 4C 3D   H=0&LANG=HU&URL=
00000070   68 74 74 70 25 33 41 25  32 46 25 32 46 64 65 76   http%3A%2F%2Fdev
00000080   2E 62 6F 6C 74 2E 68 75  25 32 46 73 68 6F 70 25   .bolt.hu%2Fshop%
00000090   32 46 66 72 6F 6D 62 61  6E 6B 2E 61 73 70 2C AF   2Ffrombank.asp,.
000000A0   E8 F8 06 06 06 06 06 06                           ........
```

3DES titkosítás

A paddelt üzenetet a kulcsfileban található kulcsok segítségével kell titkosítani, 3DES CBC módszerrel.

```
00000000   4A 48 7B 6A 81 4A 55 52  52 FC 91 14 D0 4A 6D 8E   JH{j.JURR....Jm.
00000010   28 4D 46 90 CA 99 66 EF  52 2C 14 3E 7F 85 4A BF   (MF...f.R,.>⌂.J.
00000020   C1 84 96 0B 18 D2 83 D2  1E 7F F7 77 E3 C3 1C 7E   .....⌂.w...~
00000030   AF A3 C4 0D 20 EF 8D 02  64 EA 0F 8E 0C BD 35 7F   .... ...d.....5⌂
00000040   FA C9 FA 44 A3 33 41 05  3B E4 19 E9 BF 11 4F E5   ...D.3A.;.....O.
00000050   AA C5 A4 40 A1 49 08 49  D5 CA 6F 70 BE F9 DF 80   ...@.I.I..op....
00000060   83 19 C9 7B 20 F7 FD 4F  CE E8 9E D8 3B 8A 61 62   ...{ ..O....;.ab
00000070   04 23 7F 23 8F 1A 86 76  40 22 D6 70 07 A3 DF FF   .#⌂#...v@".p....
00000080   B4 39 FF 17 ED 73 43 D6  38 DE 2F 8F 83 89 07 71   .9...sC.8./....q
00000090   A3 9E 23 AC 15 63 19 ED  83 C9 CB DE 6C 9F F7 55   ..#..c......l..U
000000A0   88 AD 52 8A 11 40 E4 30                           ..R..@.0
```

CIB BANK

Pad Base64 kódoláshoz

A kapott titkos stringet a fentebb részletezett módon bővíteni kell 3-al osztható hosszra.

```
00000000   4A 48 7B 6A 81 4A 55 52  52 FC 91 14 D0 4A 6D 8E   JH{j.JURR....Jm.
00000010   28 4D 46 90 CA 99 66 EF  52 2C 14 3E 7F 85 4A BF   (MF...f.R,.>⌂.J.
00000020   C1 84 96 0B 18 D2 83 D2  1E 7F F7 77 E3 C3 1C 7E   .........⌂.w...~
00000030   AF A3 C4 0D 20 EF 8D 02  64 EA 0F 8E 0C BD 35 7F   .... ...d.....5⌂
00000040   FA C9 FA 44 A3 33 41 05  3B E4 19 E9 BF 11 4F E5   ...D.3A.;.....O.
00000050   AA C5 A4 40 A1 49 08 49  D5 CA 6F 70 BE F9 DF 80   ...@.I.I..op....
00000060   83 19 C9 7B 20 F7 FD 4F  CE E8 9E D8 3B 8A 61 62   ...{ ..O....;.ab
00000070   04 23 7F 23 8F 1A 86 76  40 22 D6 70 07 A3 DF FF   .#⌂#...v@".p....
00000080   B4 39 FF 17 ED 73 43 D6  38 DE 2F 8F 83 89 07 71   .9...sC.8./....q
00000090   A3 9E 23 AC 15 63 19 ED  83 C9 CB DE 6C 9F F7 55   ..#..c......l..U
000000A0   88 AD 52 8A 11 40 E4 30  03 03 03                  ..R..@.0...
```

Base64 kódolás

A paddelt string Base64 kódolása RFC2045 alapján:

```
00000000   53 6B 68 37 61 6F 46 4B  56 56 4A 53 2F 4A 45 55   Skh7aoFKVVJS/JEU
00000010   30 45 70 74 6A 69 68 4E  52 70 44 4B 6D 57 62 76   0EptjihNRpDKmWbv
00000020   55 69 77 55 50 6E 2B 46  53 72 2F 42 68 4A 59 4C   UiwUPn+FSr/BhJYL
00000030   47 4E 4B 44 30 68 35 2F  39 33 66 6A 77 78 78 2B   GNKD0h5/93fjwxx+
00000040   72 36 50 45 44 53 44 76  6A 51 4A 6B 36 67 2B 4F   r6PEDSDvjQJk6g+O
00000050   44 4C 30 31 66 2F 72 4A  2B 6B 53 6A 4D 30 45 46   DL01f/rJ+kSjM0EF
00000060   4F 2B 51 5A 36 62 38 52  54 2B 57 71 78 61 52 41   O+QZ6b8RT+WqxaRA
00000070   6F 55 6B 49 53 64 58 4B  62 33 43 2B 2B 64 2B 41   oUkISdXKb3C++d+A
00000080   67 78 6E 4A 65 79 44 33  2F 55 2F 4F 36 4A 37 59   gxnJeyD3/U/O6J7Y
00000090   4F 34 70 68 59 67 51 6A  66 79 4F 50 47 6F 5A 32   O4phYgQjfyOPGoZ2
000000A0   51 43 4C 57 63 41 65 6A  33 2F 2B 30 4F 66 38 58   QCLWcAej3/+0Of8X
000000B0   37 58 4E 44 31 6A 6A 65  4C 34 2B 44 69 51 64 78   7XND1jjeL4+DiQdx
000000C0   6F 35 34 6A 72 42 56 6A  47 65 32 44 79 63 76 65   o54jrBVjGe2Dycve
000000D0   62 4A 2F 33 56 59 69 74  55 6F 6F 52 51 4F 51 77   bJ/3VYitUooRQOQw
000000E0   41 77 4D 44                                       AwMD
```

URL kódolás

A Base64 kódolt stringet URL kódolásnak kell alávetni (ezúttal minden karakterét).

```
00000000   53 6B 68 37 61 6F 46 4B  56 56 4A 53 25 32 46 4A   Skh7aoFKVVJS%2FJ
00000010   45 55 30 45 70 74 6A 69  68 4E 52 70 44 4B 6D 57   EU0EptjihNRpDKmW
00000020   62 76 55 69 77 55 50 6E  25 32 42 46 53 72 25 32   bvUiwUPn%2BFSr%2
00000030   46 42 68 4A 59 4C 47 4E  4B 44 30 68 35 25 32 46   FBhJYLGNKD0h5%2F
00000040   39 33 66 6A 77 78 78 25  32 42 72 36 50 45 44 53   93fjwxx%2Br6PEDS
00000050   44 76 6A 51 4A 6B 36 67  25 32 42 4F 44 4C 30 31   DvjQJk6g%2BODL01
00000060   66 25 32 46 72 4A 25 32  42 6B 53 6A 4D 30 45 46   f%2FrJ%2BkSjM0EF
00000070   4F 25 32 42 51 5A 36 62  38 52 54 25 32 42 57 71   O%2BQZ6b8RT%2BWq
00000080   78 61 52 41 6F 55 6B 49  53 64 58 4B 62 33 43 25   xaRAoUkISdXKb3C%
00000090   32 42 25 32 42 64 25 32  42 41 67 78 6E 4A 65 79   2B%2Bd%2BAgxnJey
000000A0   44 33 25 32 46 55 25 32  46 4F 36 4A 37 59 4F 34   D3%2FU%2FO6J7YO4
000000B0   70 68 59 67 51 6A 66 79  4F 50 47 6F 5A 32 51 43   phYgQjfyOPGoZ2QC
000000C0   4C 57 63 41 65 6A 33 25  32 46 25 32 42 30 4F 66   LWcAej3%2F%2B0Of
000000D0   38 58 37 58 4E 44 31 6A  6A 65 4C 34 25 32 42 44   8X7XND1jjeL4%2BD
000000E0   69 51 64 78 6F 35 34 6A  72 42 56 6A 47 65 32 44   iQdxo54jrBVjGe2D
000000F0   79 63 76 65 62 4A 25 32  46 33 56 59 69 74 55 6F   ycvebJ%2F3VYitUo
00000100   6F 52 51 4F 51 77 41 77  4D 44                     oRQOQwAwMD
```

CIB BANK

Üzenet előtaggal bővítése

Az urlkódolt string elé a következő előtagot kell illeszteni:

```
PID=%PID%&CRYPTO=1&DATA=
```

Ahol `%PID%` a bank által az áruház számára biztosított azonosító. A titkosított üzenet tehát az elküldendő üzenet `DATA` értéke lesz.

```
00000000   50 49 44 3D 49 45 42 30  30 30 31 26 43 52 59 50   PID=IEB0001&CRYP
00000010   54 4F 3D 31 26 44 41 54  41 3D 53 6B 68 37 61 6F   TO=1&DATA=Skh7ao
00000020   46 4B 56 56 4A 53 25 32  46 4A 45 55 30 45 70 74   FKVVJS%2FJEU0Ept
00000030   6A 69 68 4E 52 70 44 4B  6D 57 62 76 55 69 77 55   jihNRpDKmWbvUiwU
00000040   50 6E 25 32 42 46 53 72  25 32 46 42 68 4A 59 4C   Pn%2BFSr%2FBhJYL
00000050   47 4E 4B 44 30 68 35 25  32 46 39 33 66 6A 77 78   GNKD0h5%2F93fjwx
00000060   78 25 32 42 72 36 50 45  44 53 44 76 6A 51 4A 6B   x%2Br6PEDSDvjQJk
00000070   36 67 25 32 42 4F 44 4C  30 31 66 25 32 46 72 4A   6g%2BODL01f%2FrJ
00000080   25 32 42 6B 53 6A 4D 30  45 46 4F 25 32 42 51 5A   %2BkSjM0EFO%2BQZ
00000090   36 62 38 52 54 25 32 42  57 71 78 61 52 41 6F 55   6b8RT%2BWqxaRAoU
000000A0   6B 49 53 64 58 4B 62 33  43 25 32 42 25 32 42 64   kISdXKb3C%2B%2Bd
000000B0   25 32 42 41 67 78 6E 4A  65 79 44 33 25 32 46 55   %2BAgxnJeyD3%2FU
000000C0   25 32 46 4F 36 4A 37 59  4F 34 70 68 59 67 51 6A   %2FO6J7YO4phYgQj
000000D0   66 79 4F 50 47 6F 5A 32  51 43 4C 57 63 41 65 6A   fyOPGoZ2QCLWcAej
000000E0   33 25 32 46 25 32 42 30  4F 66 38 58 37 58 4E 44   3%2F%2B0Of8X7XND
000000F0   31 6A 6A 65 4C 34 25 32  42 44 69 51 64 78 6F 35   1jjeL4%2BDiQdxo5
00000100   34 6A 72 42 56 6A 47 65  32 44 79 63 76 65 62 4A   4jrBVjGe2DycvebJ
00000110   25 32 46 33 56 59 69 74  55 6F 6F 52 51 4F 51 77   %2F3VYitUooRQOQw
00000120   41 77 4D 44                                       AwMD
```

Vagyis a banknak küldendő üzenet a következő:

```
PID=IEB0001&CRYPTO=1&DATA=Skh7aoFKVVJS%2FJEU0EptjihNRpDKmWbvUiwUPn%2BFSr%2FBhJYLGNK
D0h5%2F93fjwxx%2Br6PEDSDvjQJk6g%2BODL01f%2FrJ%2BkSjM0EFO%2BQZ6b8RT%2BWqxaRAoUkISdXK
b3C%2B%2Bd%2BAgxnJeyD3%2FU%2FO6J7YO4phYgQjfyOPGoZ2QCLWcAej3%2F%2B0Of8X7XND1jjeL4%2B
DiQdxo54jrBVjGe2DycvebJ%2F3VYitUooRQOQwAwMD
```

A kititkosításhoz az egyes lépések inverz műveleteit (a 3DES-nek önmaga az inverze) kell fordított sorrendben végrehajtani.

CIB BANK

Titkosító függvénykönyvtár

Az ekiCrypt library minden, a banki kommunikációhoz szükséges titkosító algoritmust tartalmaz. A library-ben a következő függvények találhatók:

Titkosítás (ekiEncodeUrl)

```
INT ekiEncodeUrl (LPSTR inBuffer, INT inBufferSize,
                  LPSTR outBuffer, LPINT outBufferSize,
                  INT cryptoType, LPSTR keyFilePath)
```

Az URL formában megadott üzenetet alapvető ellenőrzéseknek veti alá, URL enkódolja, DES-eli, uuencodolja, és a protokollnak megfelel URL formába illeszti. A DES kulcsot Win32 alatt a registry-ben vagy file-ban, egyéb rendszereken file-ban tároljuk.

Paraméterek:

`inBuffer`: A titkosítandó url-t tartalmazó buffer.

`InBufferSize`: A titkosítandó url hossza.

`OutBuffer`: A titkosított url ebbe a bufferbe fog kerülni.

`OutBufferSize`: Az eredmény mérete
- Input: A titkosított url részére lefoglalt buffer mérete, minimálisan 4/3 * (inBufferSize + 12).
- Output: A titkosított url mérete.

`CryptoType`: A szükséges titkosítás típusa.
- 0 - SSL
- 1 - DES
- 2 - RSA
- 3 - BROWSER

`KeyFilePath`: A titkosító (DES) kulcs file elérési útja, amennyiben a kulcs file-ban tárolódik. NULL, ha a kulcs a registry-ben található (csak Win32).

CIB BANK

Visszafejtés (ekiDecodeUrl)

```
INT ekiDecodeUrl (LPSTR inBuffer, INT inBufferSize,
                  LPSTR outBuffer, LPINT outBufferSize,
                  LPINT cryptoType, LPSTR keyFilePath);
```

A kódolt, url-formátumú inputból kiveszi a titkosított adatokat, uudekódolja, ki- DES-eli és ellenőrzéseket végez rajta. Az üzenetet url-enkódolva adja vissza.

Paraméterek:

`inBuffer`:	A titkosított url-t tartalmazó buffer.
`InBufferSize`:	A titkosított url hossza.
`OutBuffer`:	A titkosítatlan url ebbe a bufferbe fog kerülni.
`OutBufferSize`	Az eredmény mérete Input: A titkosítatlan url részére lefoglalt buffer mérete, minimálisan 4/3 * (inBufferSize + 12). Output: A titkosítatlan url mérete.
`CryptoType`	Ha értéke nem NULL, akkor ebbe a bufferbe kerül a kapott adat titkosításának típusa, és a kititkosított adat nem fogja tartalmazni a Crypto mezőt. Ha NULL, akkor a kititkosított adatban benne hagyja a Crypto mezőt.
`KeyFilePath`:	A titkosító (DES) kulcs file elérési útja, amennyiben a kulcs file-ban tárolódik. NULL, ha a kulcs a registry-ben található (csak Win32).

Kulcs struktúra

A lentebb részletezett struktúra nem azonos a kulcsfile bináris tartalmával, annak csupán egy részét tartalmazza, az `ekiGetKeyInfo` függvény számára.

```
typedef struct
{
   char           fname[13];       /* filenév */
   INT            keySize;         /* kulcsméret */
   char           id[4];           /* belső azonosító - elvileg ua.  mint marketId*/
   unsigned short version;         /* verzió */
   char           marketId[4];     /* áruház azonosítója */
   time_t         creation_time;   /* kulcs elállítási ideje */
} TKeyInfo;
```

CIB BANK

Kulcsinformációk lekérdezése (ekiGetKeyInfo)

```
INT EKIAPI ekiGetKeyInfo(TKeyInfo *ekiKeyInfo, char *keyFilePath,
                         char *boltId);
```

A titkosító kulcs adatait adja vissza a TKeyInfo struktúrában.

Paraméterek:

`ekiKeyInfo`:	Kulcs adatai
`keyFilePath`:	Kulcs file helye
`boltId`:	Áruházazonosító

Lehetséges visszatérési értékek:

UER_OK:	Ok.
UER_NOMEM:	Nincs elég memória.
UER_BADSIZE:	Output buffer mérete (outBufferSize) kicsi.
UER_NOKEY:	Kulcs nem található.
UER_BADKEY:	Rossz kulcs struktúra.
UER_NOFILE:	Kulcs file nem található.

Verziószám lekérdezése (ekiGetLibVersion)

INT EKIAPI ekiGetLibVersion(char *outBuffer, LPINT outBufferSize);

A titkosító modul verziószámának lekérdezése.

Paraméterek:

`outBuffer`:	Ide írja a verziószámot x.y.z formában, \0-val lezárva.
`outBufferSize`:	outBuffer mérete byte-okban, a lezáró nullának is helyet hagyva.

Lehetséges visszatérési értékek:

UER_OK:	Ok.
UER_NOMEM:	Nincs elég memória.
UER_BADSIZE:	Output buffer mérete (outBufferSize) kicsi.

CIB BANK

Titkosító alkalmazás (sakide)

A sakide parancssori példaprogram, mely az ekiCrypt library függvényeit alkalmazza. Használata:

```
sakide [-e|-d] [-c <cryptotype>] [-i <-m <keyfile>>]
       [-p <path>] [-v] [-s <string>] [-S] [-u] [-V]
```

ahol

`-e` titkosító üzemmód
`-d` kititkosító üzemmód
`-c <cryptotype>` a titkosítás típusa (jellemzően 1)
`-m <keyfile>` a kulcsfile neve
`-i` információt szolgáltat a kulcsfile tartalmáról
`-p <path>` a kulcs elérési útja
`-v` extra információt ír STDERR-ra
`-s <string>` a feldolgozandó üzenet
`-S` rendszerinformációkat ad (GNU libc használata esetén)
`-u` kititkosítás előtt URL dekódolást végez az adatokon
`-V` kiírja az alkalmazás verzió számát

Paraméterek nélkül indítva az alkalmazás az STDIN-ről kapott adatokat titkosítja az üzenetben megjelöl PID paraméterben található áruházazonosító titkosítókulcsával (ha az üzenetben PID=CIB0001, akkor az aktuális könyvtárban található CIB.des filet használja).

Példák a sakide alkalmazás használatára:

```
./sakide –e –s „PID=CIB0001&TRID=1234123412341234&MSGT=20”

echo „PID=CIB0001&TRID=1234123412341234&MSGT=20”|./sakide

cat cleartext.dat|./sakide –v 2>&1
```

Utóbbi extra információt szolgáltat az STDOUT csatornára (gyakorlatilag az STDERR átirányítása az STDOUT-ra, hibakeresésnél hasznos).

A legtöbb támogatott operációs rendszer számára két futtatható állomány is található, egy dinamikusan és egy statikusan linkelt (utóbbi neve sakide.static, vagy sakide_static). Utóbbi nem igényel rendszerszintű függvénykönyvtárakat, tehát operációs rendszer verziótól függetlenül alkalmazható.

CIB BANK

Hibalehetőségek, javaslatok

- A bankból jövő adatokat kititkosítás előtt tilos URL dekódolásnak alávetni. A beérkezett adatot először az ekiDecodeUrl-nek átadva ki kell titkosítani, majd az így kapott adatot kell URL dekódolni. Néhány webszervernél elfordulhat, hogy a [9] lépésben kapott 21-es típusú üzenet már URL dekódolva adódik át a szerver oldali programnak. Ennél a lépésnél erősen ajánlott, hogy a kapott paraméterek feldolgozás előtt mindenképpen URL enkódoláson "essenek át".
- Ha a kapcsolat a protokoll bármely pontján megszakad (pl. a vásárló bontja a vonalat, URL-t vált, vonalszakadás a bank és áruház között), a bankban a tranzakció time-outtal végződik. A time-out ideje a bankban 10-15 perc, de ezt az időtartamot, mást mutató tapasztalatok alapján változtathatóra kell programozni. A vezérlés a bankból nem kerül vissza az áruházhoz. Ha a bank számára nem egyértelmű, hogy a tranzakció sikertelen lett, a time-out után a bank ún. reverzált indít, majd lezárja a tranzakciót, és annak adatai többé nem elérhetőek a partnerek számára. Ilyenkor az áruházban a tranzakciónak szintén time-outtal kell végződnie. Tehát egy tranzakció csak akkor tekinthető sikeresen befejezettnek, ha az authorizáció minden lépése lezajlott (utolsó az MSGT=32-re kapott MSGT=31).
- A tranzakció állapotát mindkét félnek (BANK és ÁRUHÁZ) követnie kell ahhoz, hogy mindkettő biztonsággal meg tudja állapítani, hogy egy tranzakció éppen milyen fázisban van, és hogy a megadott időtartam nem telt-e le. Ha a tranzakció bármely fázisában time-outra fut, akkor a bank kötelessége, hogy az esetleges sikeres authorizációt reverzálja, a tranzakciót sikertelenként lezárja, az áruház feladata pedig a megrendelés törlése, valamint a tranzakció áruház oldali nyilvántartásának lezárása. Az állapot nyomonkövetése a 33-as üzenet segítségével lehetséges.

Fontos, hogy az áruház a tranzakciók minden lépését naplózza, hogy mind a banki, mind az áruházi oldalon bármikor visszakereshető legyen, hogy egy tranzakció milyen lépéseken át jutott végállapotba.

Elérhetőségek

Név	Telefon	e-mail	Elérhetőség	Terület
Telefonos ügyfélszolgálat	+36-1-399-8899		Minden nap, 0-24 óráig	Információkérés, technikai kérdés továbbítása
Banki üzletkötő	lásd: www.cib.hu, fióklista	lásd: www.cib.hu, fióklista	Banki nyitvatartási időben	Szerződések, számlaügyek
Fejlesztői segítség		ecommerce@cib.hu	Banki nyitvatartási időben	Technikai segítség fejlesztés/tesztelés idejére