

A példa cardletek specifikációja

Az ID cardlet:

Az ID cardlet feladata a kártya biztonsági funkcióinak megvalósítása. A biztonság jelen esetben az intelligens kártyáknál széles körben alkalmazott User PIN/Master PIN megoldáson alapul, melynek lényege, hogy a kártya tulajdonosa csak a User PIN-t (tulajdonosi titkos kódot) ismeri, és ezzel csak használni tudja a kártyát, de lényeges adatot nem tud módosítani benne, ez csak a Master PIN segítségével lehetséges, amelyet azonban csak a gyártó/kártyakibocsátó ismer. Azt, hogy ez ténylegesen mennyire biztonságos megoldás, majd a cardletek bemutatása után fogjuk elemezni. A biztonsági funkciók (User PIN és Master PIN ellenőrzése, illetve megfelelő Master PIN birtokában új User PIN megadása) megvalósításán túl ez a cardlet tartalmazza a kártya egyedi 8 byte-os azonosítóját is, mely a külvilág felől bárki számára olvasható, de senki által nem módosítható. Ezen kívül ez a cardlet kezeli a tulajdonos személyére jellemző adatokat is, melyek jelenleg 32 bájtól tárolhatók (ezen pl. a tulajdonos neve és igazolvány száma el is férhet), de ez az adatmező különösebb nehézség nélkül kiterjeszthető.

A cardlet CLA kódja: AA

A cardlet által kezelt ISO kompatibilis adatállományok:

idFile EF

FID=0x9102; SFI=2; hossza: 8 bájt

Az állomány mindenki számára olvasható, de senki számára sem írható.

Ez az ISO állomány tartalmazza a kártya egyedi 8 byte-os azonosítóját.

dataFile EF

FID=0x9104; SFI=4; hossza: 32 bájt

Az állomány csak a User PIN prezentálása után olvasható, és csak a Master PIN prezentálása után írható.

Ez az ISO fájl tartalmazza a kártyatulajdonos személyi adatait.

A cardlet által értelmezett parancsok:

ChangeUserPin:

C-APDU:

Mező	Érték	Hossz
CLA	AA	1
INS	10	1
P1	00	1
P2	00	1
Lc	a tulajdonosi PIN hossza	1
Adat	az új tulajdonosi PIN	1-4
Le	0	1

Státusz:

SW_NO_ERROR ha sikerült

SW_CONDITIONS_NOT_SATISFIED ha nem sikerült

A cardlet által értelmezett ISO kompatibilis parancsok:

Select DF/EF:

C-APDU:

Mező	Érték	Hossz
CLA	0	1
INS	A4	1
P1	02	1
P2	Mindegy	1
Lc	2	1
Adat	FID	2
Le	0	1

Hatása:

Kiválasztja az adott FID-jű adatállományt.

ReadBinary:

C-APDU:

Mező	Érték	Hossz
CLA	0	1
INS	B0	1
P1	0	1
P2	0	1
Lc	0	1
Adat	-	0
Le	kívánt byte-ok száma	1

Hatása:

Kiolvassa az aktuális file Le számú byte-ját.

R-APDU:

Mező	Érték	Hossz
Adat	A file adatai	a byte-ok száma

UpdateBinary:

C-APDU:

Mező	Érték	Hossz
CLA	0	1
INS	D6	1
P1	0	1
P2	0	1
Lc	byte-ok száma	1
Adat	a beírni kívánt adat	1-32
Le	0	1

Hatása:

Az aktuális fájl első Lc számú byte-ját átírja a megadottra.

VerifyPin:

C-APDU:

Mező	Érték	Hossz
CLA	0	1
INS	20	1
P1	0	1
P2	PIN típusa: 0x81 = Master PIN 0x82 = User PIN	1
Lc	A PIN hossza	1
Adat	PIN	1-8
Le	0	1

Hatása:

A kártya ellenőrzi a prezentált PIN-kódot.

Státusz:

SW_NO_ERROR, ha jó a PIN

SW_PIN_FAILED, ha hibás a PIN, ekkor az ISO 7816 szabványnak megfelelően a visszaadott státusz utolsó négy bitjének értéke megadja a még rendelkezésre álló próbálkozások számát.

Azaz pl. ha az SW_PIN_FAILED értéke 0x69C0, és még négy próbálkozásunk van hátra, akkor a ténylegesen visszaadott státusz 0x69C4 lesz.

A Phone cardlet:

Ez a cardlet látja el a telefonkártya funkcióit. A telefonkártyán levő egységek számát bárki kiolvashatja, de a számukat csak a User PIN prezentálása után lehet csökkenteni, így az esetleges tolvaj nem tud vele telefonálni, hiszen nem tudja a megfelelő PIN kódot. A kártyát újra feltölteni csak a központban lehet, ahol ismerik a Master PIN-t.

A cardlet CLA kódja: AB

A cardlet által kezelt ISO kompatibilis adatállományok:

creditFile EF

FID=0x9103; SFI=3; hossza: 2 bájt

Az állomány mindenki számára olvasható, de senki számára sem írható.

A cardlet által értelmezett parancsok:

SetCredit:

C-APDU:

Mező	Tartalom	Hossz
CLA	AB	1
INS	10	1
P1	0	1
P2	0	1
Lc	2	1
Adat	egységek száma	2
Le	0	1

Hatás:

Ha az ID cardletnek helyesen megadtuk a Master PIN-t, akkor beállítja az új egységszámot.

R-APDU:

Mező	Érték	Hossz
Adat	a kreditek száma	2

Státusz:

SW_NO_ERROR ha sikerült

SW_CONDITIONS_NOT_SATISFIED ha a Master PIN-t még nem adtuk meg

DecCredit:

C-APDU:

Mező	Tartalom	Hossz
CLA	AB	1
INS	20	1
P1	0	1
P2	0	1
Lc	0	1
Adat	nincs	0
Le	0	1

Hatás:

Az egységek számát csökkenti eggyel, ha az ID cardletnek már sikeresen megadtuk a tulajdonosi PIN-t.

R-APDU:

Mező	Érték	Hossz
Adat	a megmaradt kreditek száma	2

Státusz:

SW_NO_ERROR ha sikerült

NO_MORE_CREDITS (0x9101) ha már nincs több egység a telefonkártyán

SW_CONDITIONS_NOT_SATISFIED ha a PIN-t még nem adtuk meg

A cardlet által értelmezett ISO kompatibilis parancsok:

Select DF/EF, és ReadBinary, leírásukat lásd az ID cardletnél.

A BTC_Pass cardlet:

Ez a cardlet valósítja meg a BKV bérlet funkciókat. Az érvényességét az aktuális dátum után megadása után bárki lekérdezheti, ha belegondol az ember, ez az egyetlen módja annak, hogy az ellenőrök egy egyszerű olvasóval, bármiféle titkos kód ismerete nélkül ellenőrizni tudják a bérleteket. A bérlet érvényességi idejének beállítása természetesen csak a Master PIN megadása után lehetséges. Azáltal hogy az érvényességi időt az időszak kezdő és befejező dátumával adjuk meg, lehetővé válik, hogy a cardlet a napijegytől az éves bérletig mindenféle bérletfajtát megvalósítson.

Az cardlet CLA kódja: AC

A cardlet által értelmezett parancsok:

SetValid:

C-APDU:

Mező	Tartalom	Hossz
CLA	AC	1
INS	10	1
P1	0	1
P2	0	1
Lc	8	1
Adat	kezdő dátum + lejárat dátum	8
Le	0	1

Hatás:

Ha az ID cardletnek helyesen megadtuk a Master PIN-t, akkor beállítja a kezdő és a lejárat dátumot.

R-APDU:

Mező	Érték	Hossz
Adat	az új kezdő és lejárat dátum	8

Státusz:

SW_NO_ERROR ha sikerült

SW_DATA_INVALID ha érvénytelen dátumokat adtunk meg

A dátumokat 4 bájtól ábrázoljuk: YYMD

Egy dátum érvényes, ha:

1980 < YY < 2050

0 < M < 13

0 < D < 32

Ezenkívül a lejárat dátum nem lehet korábbi, mint a kezdő dátum.

SW_CONDITIONS_NOT_SATISFIED ha nem adtuk meg a Master PIN-t.

IsValid:

C-APDU:

Mező	Tartalom	Hossz
CLA	AC	1
INS	20	1
P1	0	1
P2	0	1
Lc	4	1
Adat	a mai dátum	4
Le	0	1

Hatás:

Ellenőrzi, hogy a prezentált mai dátum korábbi, vagy egyenlő-e, mint a lejárat dátum, és későbbi vagy egyenlő-e, mint a kezdő dátum, azaz a bérlet érvényes-e.

Státusz:

SW_NO_ERROR ha érvényes

NOT_VALID (0x9101) ha nem érvényes

A Student cardlet:

Ez a cardlet valósítja meg a diákigazolvány funkciókat. Az érvényességét bárki ellenőrizheti (hiszen erre bárhol szükség lehet, a vasúttól kezdve a múzeumokig számtalan területen), az érvényesség lejártának időpontját beállítani azonban csak a Master PIN segítségével, a központban lehet.

Az cardlet CLA kódja: AD

A cardlet által értelmezett parancsok:

SetExpDate:

C-APDU:

Mező	Tartalom	Hossz
CLA	AD	1
INS	10	1
P1	0	1
P2	0	1
Lc	4	1
Adat	lejárat dátum	4
Le	0	1

Hatás:

Ha az ID cardletnek helyesen megadtuk a MasterPIN-t, akkor beállítja a diákigazolvány lejárat dátumát a megadottra.

R-APDU:

Mező	Érték	Hossz
Adat	az új lejárat dátum	4

Státusz:

SW_NO_ERROR ha sikerült

SW_DATA_INVALID ha érvénytelen dátumot adtunk meg

A dátumokat 4 bájton ábrázoljuk: YYMD

Egy dátum érvényes, ha:

1980 < YY < 2050

0 < M < 13

0 < D < 32

SW_CONDITIONS_NOT_SATISFIED ha nem adtuk meg a Master PIN-t.

IsValid:

C-APDU:

Mező	Tartalom	Hossz
CLA	AD	1
INS	20	1
P1	0	1
P2	0	1
Lc	4	1
Adat	mai dátum	4
Le	0	1

Hatás:

Ellenőrzi, hogy a prezentált mai dátum korábbi, vagy egyenlő-e, mint a lejárat dátum, azaz érvényes-e a diákigazolvány.

Státusz:

SW_NO_ERROR ha érvényes

SW_CONDITIONS_NOT_SATISFIED ha nem érvényes