Mitől intelligens, és hogyan lehet megtámadni?

- Intelligens kártyák biztonsági kérdései -

Dr. Berta István Zsolt, PhD, MBA, CISA

Microsec Kft, K+F és folyamatszervezési igazgató

<istvan@berta.hu>
www.berta.hu

Magamról

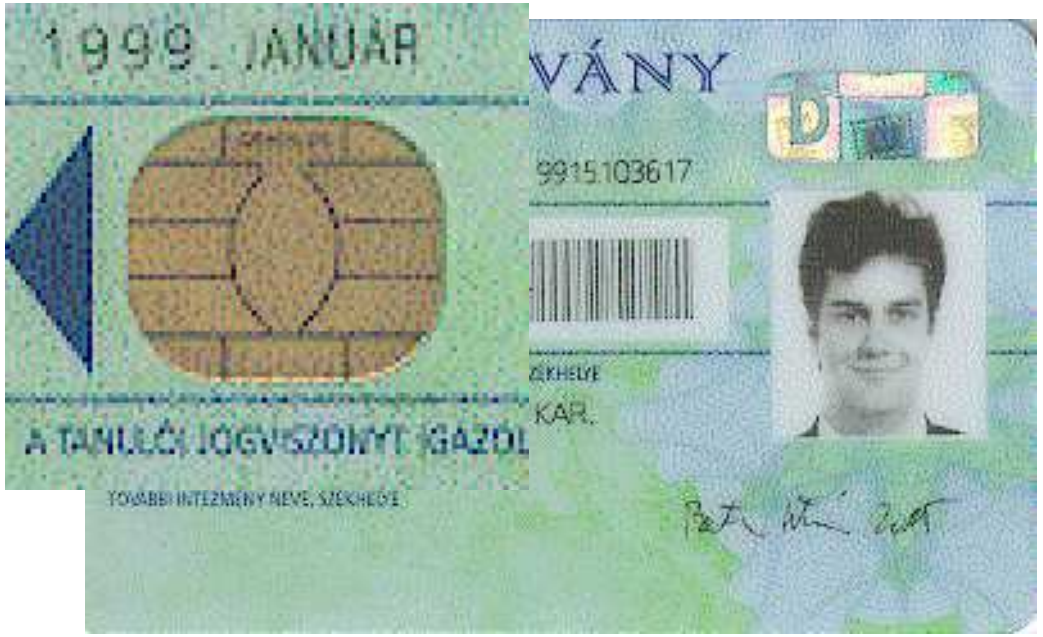
- BME, info szak, 2001.
- BME, CrySys labor (www.crysys.hu)
- Microsec Kft. - e-Szignó Hitelesítés Szolgáltató (www.e-szigno.hu)

Miről fogok beszélni?

1. Mik azok az intelligens kártyák, és miért nevezzük őket intelligensnek?
2. Hogyan lehet megtámadni egy intelligens kártyát (vagy kártyát használó rendszert)?
3. Támadás elektronikus aláírásra szolgáló kártya ellen.

Mik azok az intelligens kártyák, és miért nevezzük őket intelligensnek?

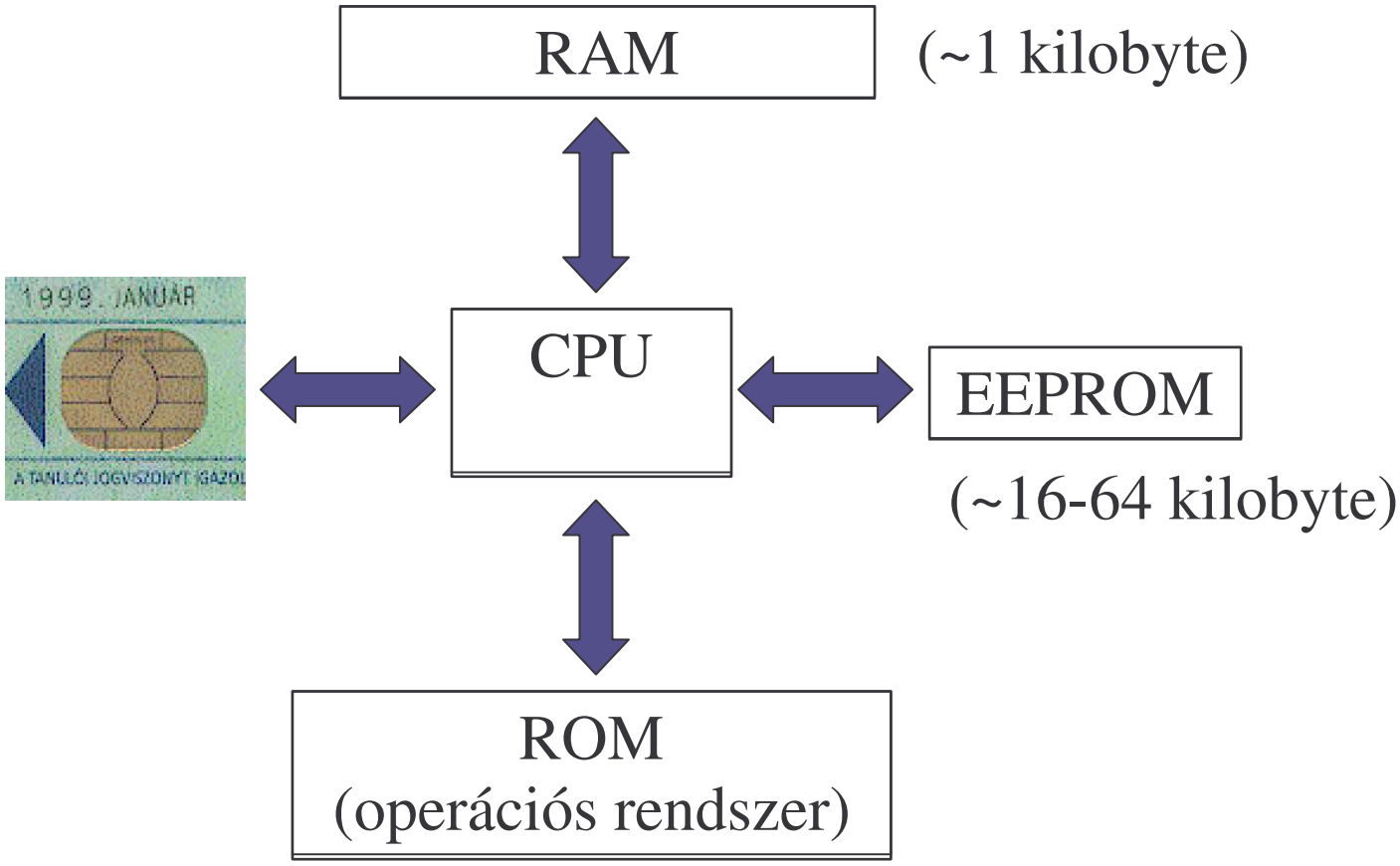
Mik azok az intelligens kártyák?



ISO 7816-2 szabvány írja le

kontaktus nélküli kártyák: ISO 14443

Mi van a kártya belsejében?



Mágneskártya	-	Chipkártya
Az adatokat csak tárolni képes		Adatokat tárol és velük műveleteket végez
Adatai közvetlenül írhatóak/olvashatóak		Tartalma csak védelmi mechanizmusokon keresztül érhető el
Adattároló egység (~floppy disk)		Biztonságos mikroszámítógép

A chipkártyák generációi

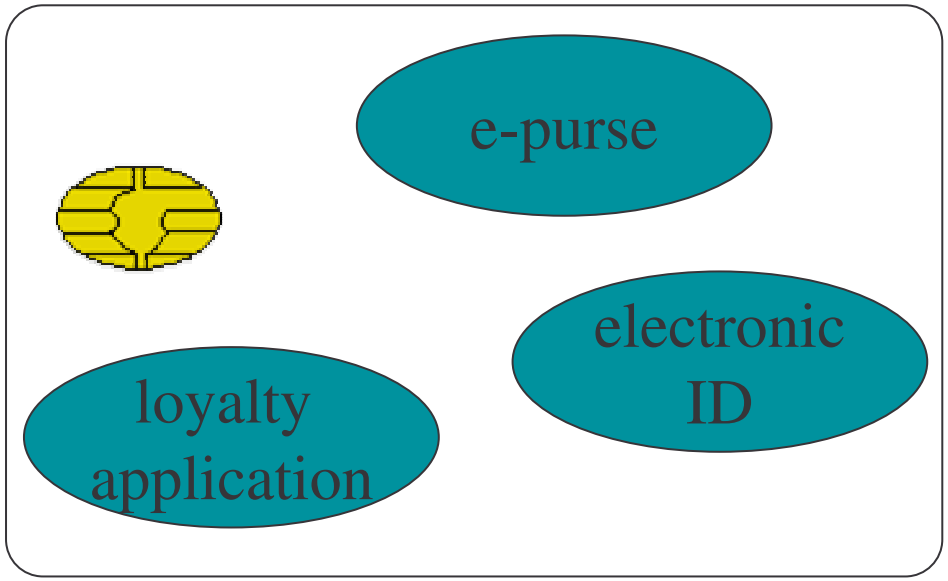
1. Memóriakártyák
   (a kártyán csak memóriachip van)
2. Fájlrendszerkártyák v „generikus” kártyák
   (mikroprocesszor, fájlrendszer, több felhasználó, hozzáférési jogosultságok, kriptográfiai műveletek, …)
3. Programozható kártyák
   A kártyán tetszőleges program futtatható
   - Nyílt és zárt platformok

Különféle elnevezések

- Chipkártya
- Smart card
- Mikroprocesszoros kártya
- Intelligens kártya

Mire használnak chipkártyákat?

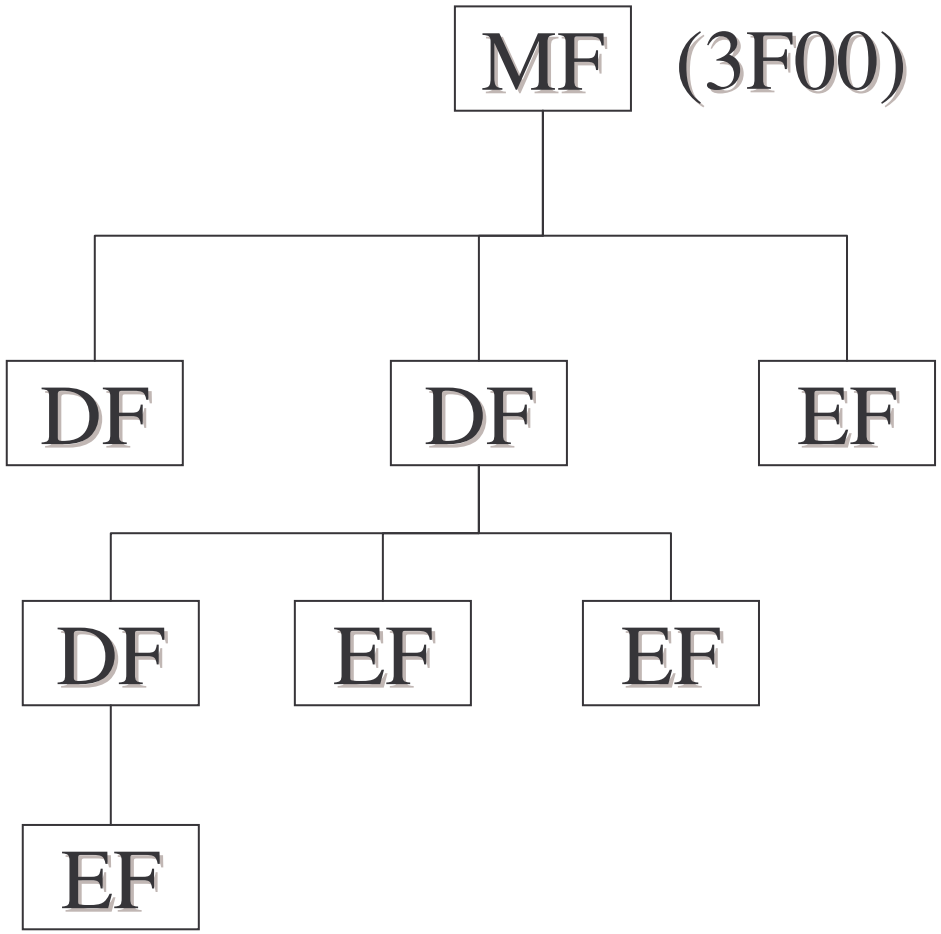
- elektronikus igazolvány
- digitális aláírás
- hozzáférés-védelem
- hitelkártyák
- elektronikus pénztárca
- telefonkártyák
- SIM kártyák
- parkoló v közlekedési kártya
- hűségkártya
- pay TV alkalmazás



Többalkalmazásos kártyák:

- több alkalmazás
- együtt is működhetnek

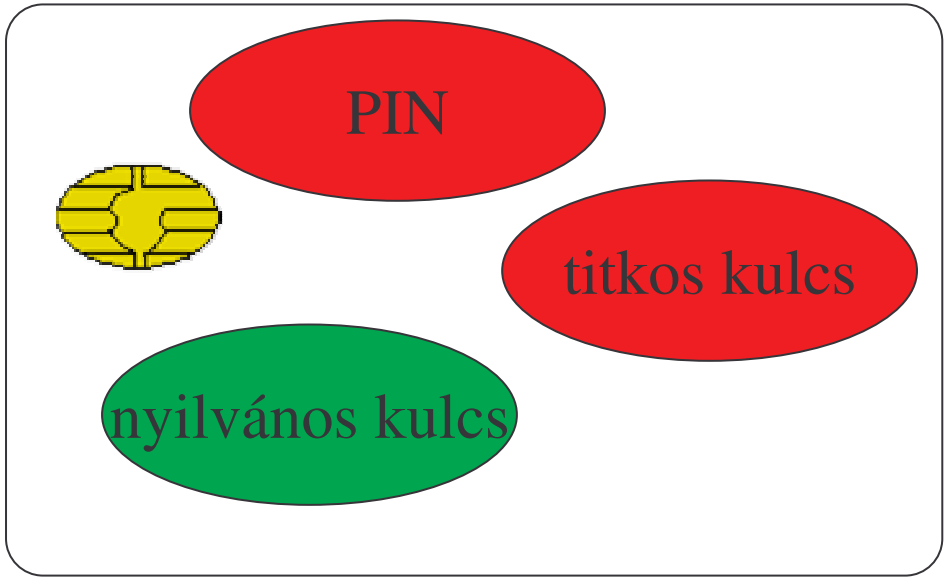
Fájlrendszer



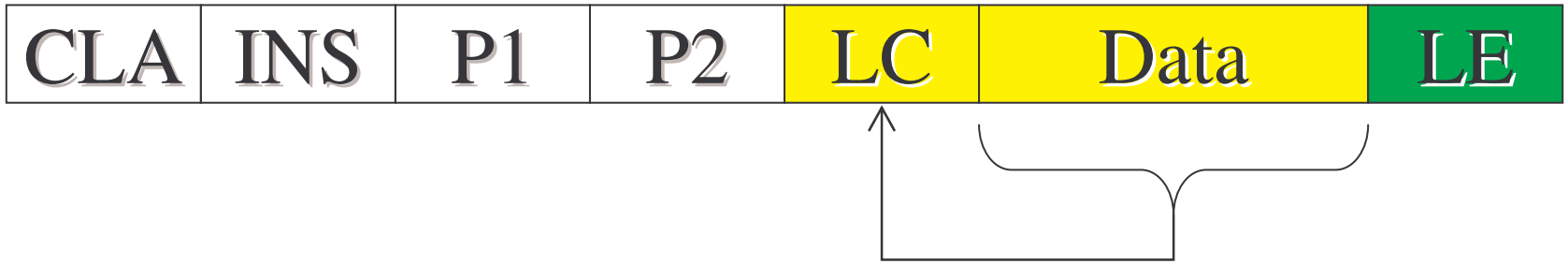
- Fastruktúra
  - →Master file ~ ‘/’
  - →Dedicated file
  - →Elementary file
- Minden fájlnak van azonosítója (FID)
- A DF-eknek neve is lehet
- DF ~ alkalmazás
- Fájlokhoz hozzáférési jogok, PIN kódok rendelhetőek
- Kulcsok…

Gyakori alkalmazás

- A kártya egy v. több kulcspárt véd;
- A kulcsokat a kártya generálja;
- A titkos kulcs nem olvasható ki;
- Helyes PIN megadása esetén a kártya kódol a titkos kulccsal.



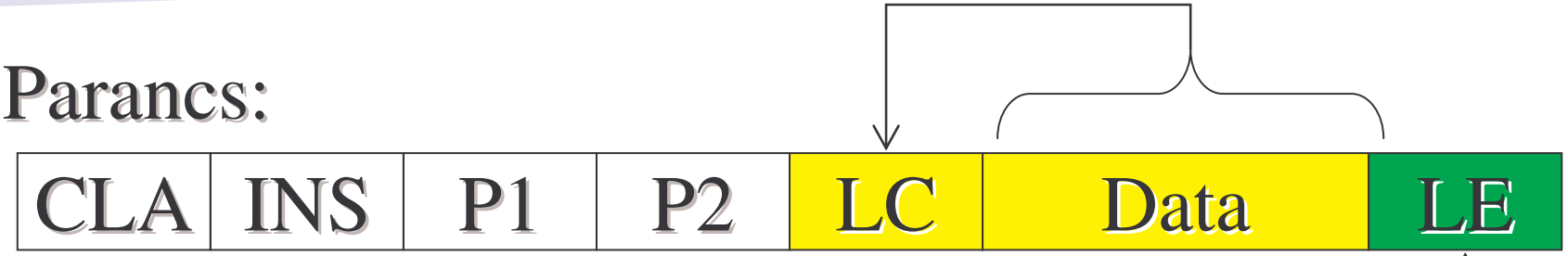
A kártyának küldhető parancs (APDU) formátuma



- CLA (class): függ a kártyától, alkalmazástól, stb.
- INS (instruction): az utasítást választja ki
- P1, P2: paraméterek, az utasítástól függenek
- LC (length command): az adatmező hossza
- LE: a várt adatok hossza

A kártya válaszának formátuma

- Parancs:

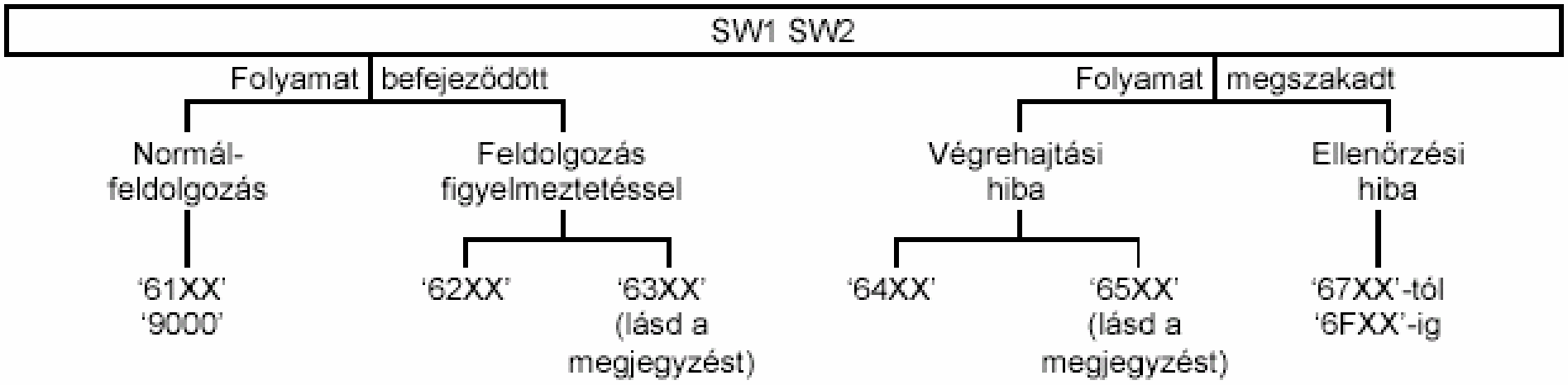


- Válasz:

Négy eset (type):

- LC, se LE
- csak LE
- Csak LC és Data
- LC, Data, LE

A két állapotbájt értéke

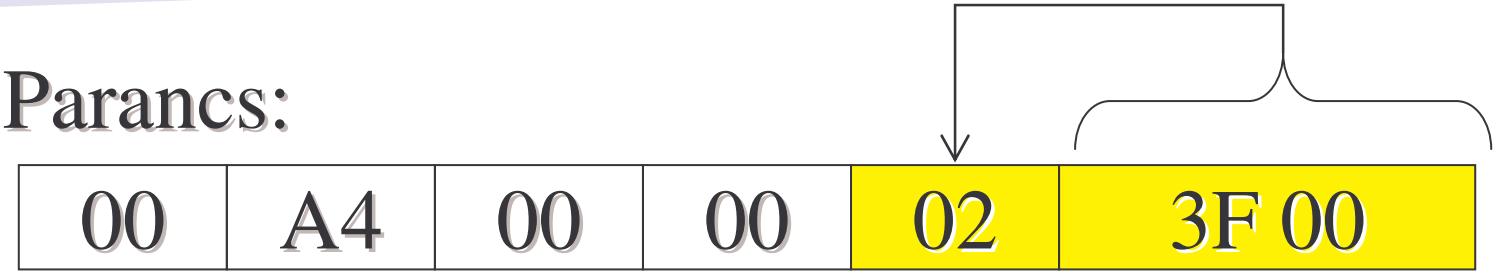


Fontosabb ISO 7816 parancsok

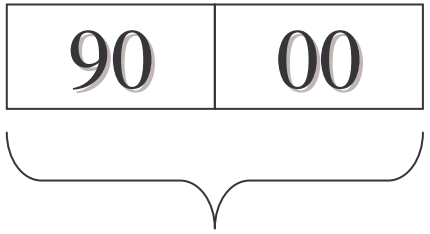
- Select File
- Read/Write/Update/Erase Binary
- Read/Update/… Record
- Get Response
- Verify (PIN),
- Change Reference Data,
- Reset Retry Counter
- Manage Security Environment
- Perform Security Operation (pl.: Hash, Digital Signature, stb.)
- …

MF kiválasztása

- Parancs:



- Válasz:



Type 3

8 byte olvasása az 1234 fájból

- A ‘20 00’ FID-jű DF kiválasztása:

00	A4	00	00	02	20 00

- Az ’12 34’ FID-jű EF kiválasztása:

00	A4	02	00	02	12 34

- 8 byte olvasása:

00	B0	00	00	LE

90	00	11 22 33 44 55 66 77 88

Digitális aláírás HUNEID kártyán

- A szükséges PIN kód ellenőrzése (Verify)

00	20	00	84	04	‘1’:’2’:’3’:’4’

- Az aláírás művelet és az aláíró kulcs kiválasztása (MSE)

00	22	41	B6	03	84 01 84

- Aláírás (PSO: Compute Digital Signature)

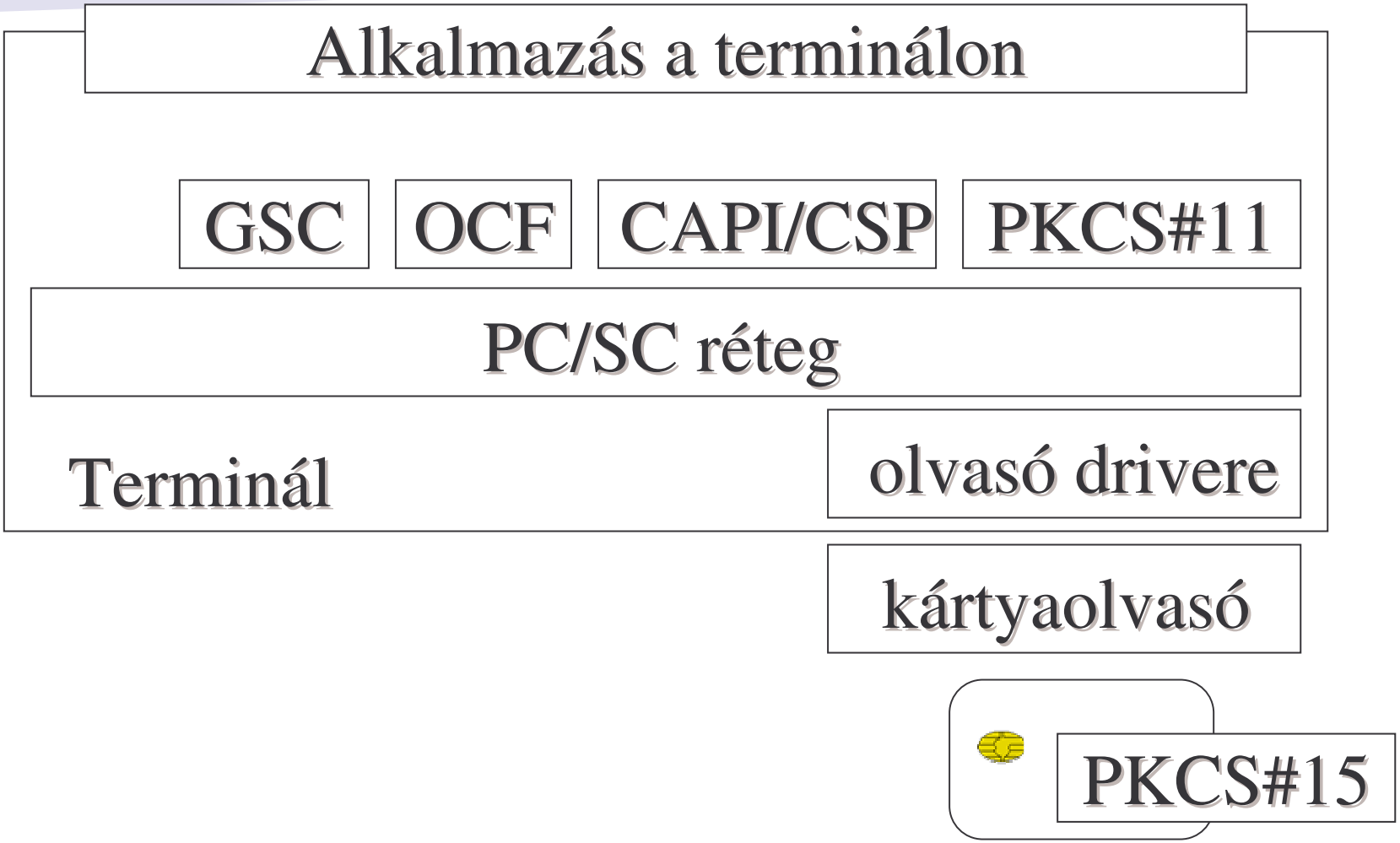
00	2A	9E	9A	14	20=0x14 hash	80

90	00	128 = 0x80 byte aláírás

Diákigazolvány

- Gemplus MPCOS-EMV típusú kártya
- 8k memória
- 3DES kódolás
  (csak szimmetrikus kulcsú kriptográfia!)
- SAM modulok segítségével használható
- SAM modul nélkül csak a CSN olvasható ki
- Digitális pénztárca
- Különböző oktatási intézmények „pecsétjei”
  ~matricák
- Mire lehet használni?

Kommunikáció a kártyával



PKCS#11 (Cryptoki)

- Egységes interfészt az alkalmazás számára
- „Token-drivert” igényel
- ANSI C-ben készült
- Elterjedt (Netscape, Mozilla)
- Login/Logout, Security Officer / User
- Több token párhuzamos használata, egy tokent egyszerre több alkalmazás is használhatja

CryptoAPI, CSP

- Egységes felület (CryptoAPI) Windows alatt a kulcsok, tanúsítványok kezelésére, az egyes kripto-tokeneknek driverei (CSP) vannak.
- Közös funkciók, pl:
  - →aláírás
  - →kulcsgenerálás
  - →titkosítás
- A PKCS#11-hez hasonló felület
- CSP11

Programozható kártyák

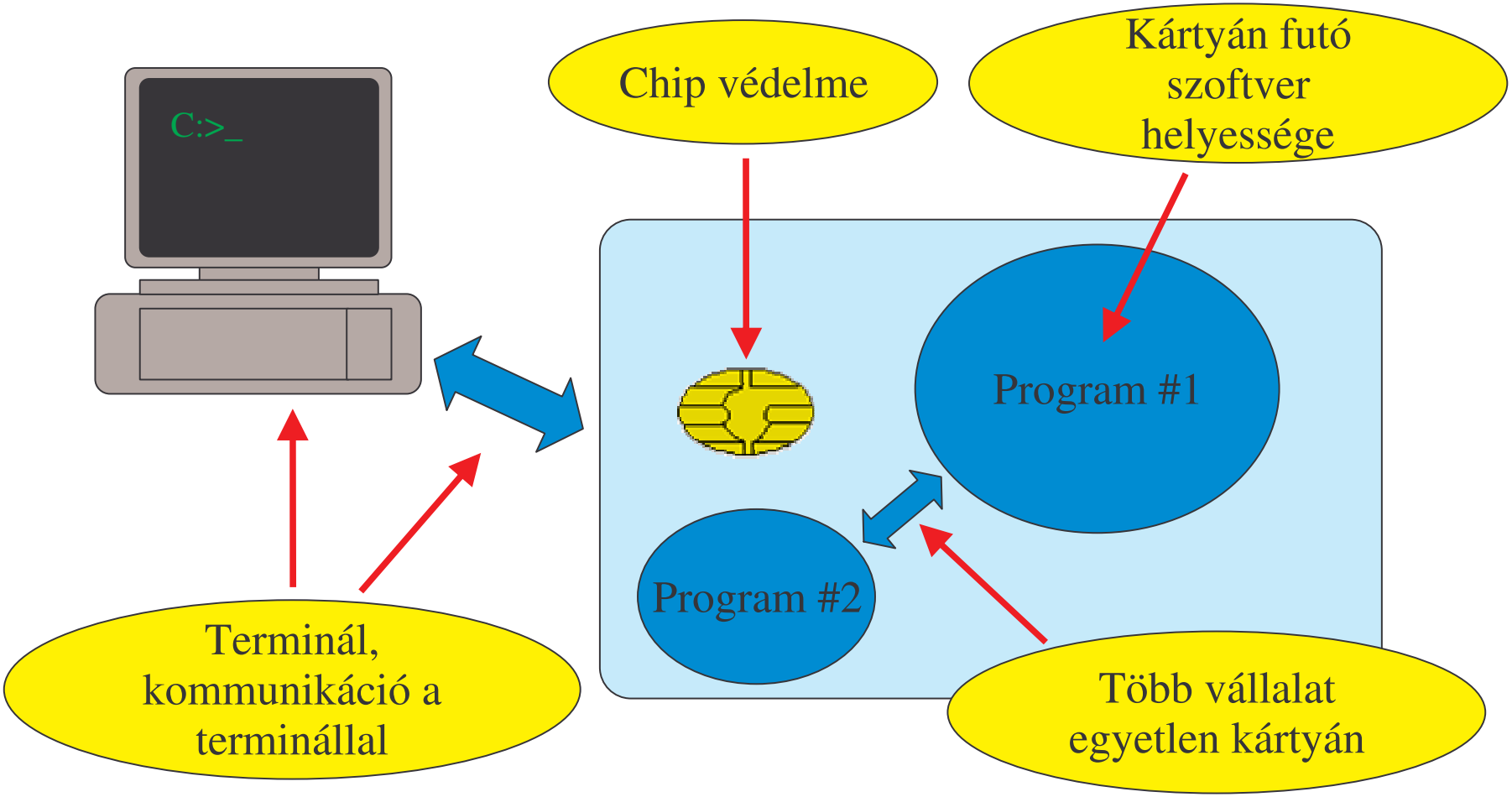
- A kártyára programot lehet feltölteni, így a kártya működése jelentősen testreszabható
- Nyílt platformok, magas-szintű nyelvek esetén ha áttérünk más kártyatípusra, a programot nem kell újra kifejleszteni, verifikálni

Nyílt kártyaplatformok

- Java Card
- MULTOS
- Smart Card for Windows

Hogyan lehet megtámadni egy intelligens kártyát?

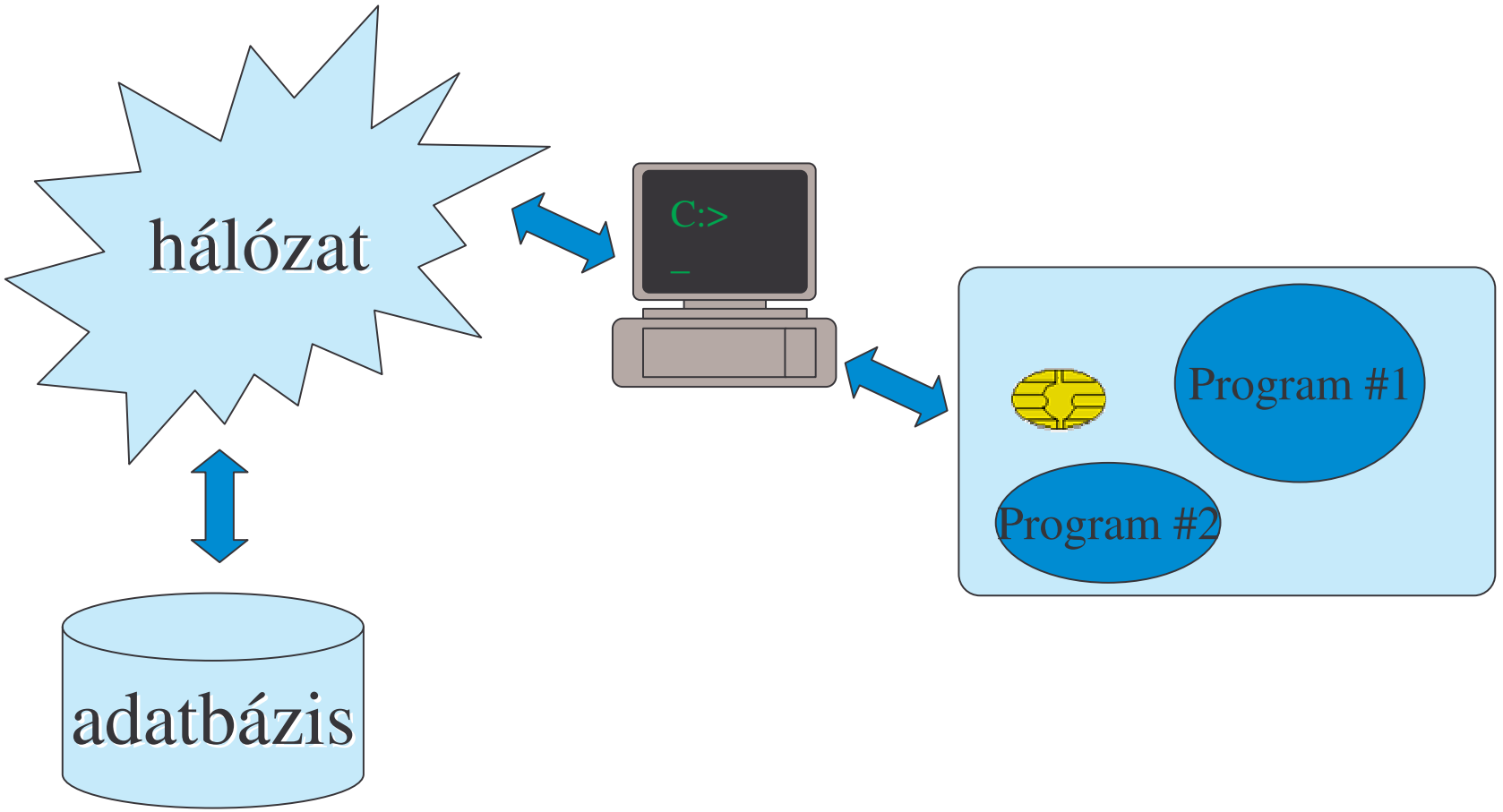
Hogyan lehet megtámadni?



A kártya - egy rendszer része (1)

- A támadó általában nem közvetlenül a kártyát akarja megtámadni.
- A kártya egy rendszerben tölt be valamilyen - biztonsági - funkciót
- A támadó a rendszert akarja „megtámadni”, ezért támadhatja a kártyát.

A kártya - egy rendszer része (2)



A kártya szerepe

- Magánkulcsot tárol
  - →a kulccsal hitelesítheti magát a kártyabirtokos, és hozzáfér egy rendszer szolgáltatásaihoz
  - →elektronikus aláírás, PKI
- Adatokat tárol
  - →egyenleget
  - →a kártyabirtokos adatait

Támadások a chip ellen

- Rácsatlakozás a kártya bus-aira.
- Védekezés: Egy chipbe integrált kártya.
- Memóriaterületek feltérképezése.
- Védekezés: Szándékosan összezagyvált architektúra.
- Kártya szétszedése.
- Védekezés: „Bontásbiztos” kártya.

Támadás a kártyán futó alkalmazás ellen

- A kártyán futó alkalmazás vagy a kártya operációs rendszerében lévő hibák kihasználása
- Védekezés: Bevizsgált, minősített, esetleg formálisan verifikált szoftverek.

Kártyán futó alkalmazás

- A kártyán bonyolult programok futnak
- Érzékeny adatokat bízunk rájuk
- A kártyán futó szoftver működésébe nem mindig van lehetőség később beavatkozni
- A kártyák nagyon nagy példányszámban kerülhetnek forgalomba
- A tesztelés nem bizonyítja egy komplex szoftver helyességét

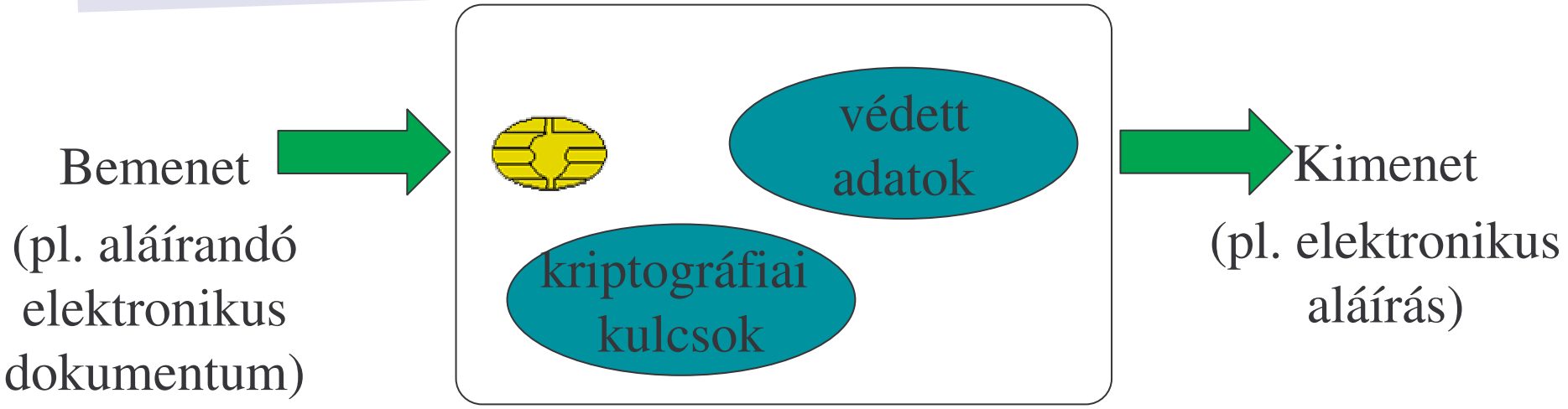
Kártya - Terminál kommunikáció

- Lehallgatás - (pl.: PIN kód elkapása)
- Manipulálás (man-in-the-middle)
  - →byte-ok cserélése
  - →megfigyelt kommunikáció visszajátszása
- Védekezés: PIN lehallgatása ellen PIN pad-es kártyaolvasó
- Védekezés: titkosított és hitelesített kapcsolat kiépítése a kártya és az olvasó között.
  - →secure messaging, ~ SSL
  - →a rendszerhez tartozó terminálok felismerése

Tápfeszültség befolyásolása

- Írás és olvasás eltérő tápfeszültség-igénye
- Védekezés: A kártya ne működjön, ha nem elegendő, vagy ha ingadozik a tápfeszültség.
- Kártya működésének megfelelő pillanatban történő megszakítása; inkonzisztens állapotba hozhatja a kártyát.
- Védekezés: Tranzakció-kezelés.

„Side channel” támadások (1)



Ezen információkból próbálunk a védett adatokra, kulcsokra következtetni

- Időzítések vizsgálata
- Kártya teljesítményfelvétele
- Elektromágneses sugárzások
- Szándékosan elrontott kártya hibás kimenetének vizsgálata
- …

„Side channel” támadások (2)

- Példa: Időzítések vizsgálata PIN kód ellenőrzésekor.
- Példa: RSA magánkulcs meghatározása.
- Védekezés: A kártya ne bocsásson ki magából „zajt”.
- Védekezés: A kártya ne legyen hajlandó működni, ha elrontják.

Többalkalmazásos kártyák - egymást támadó alkalmzások?

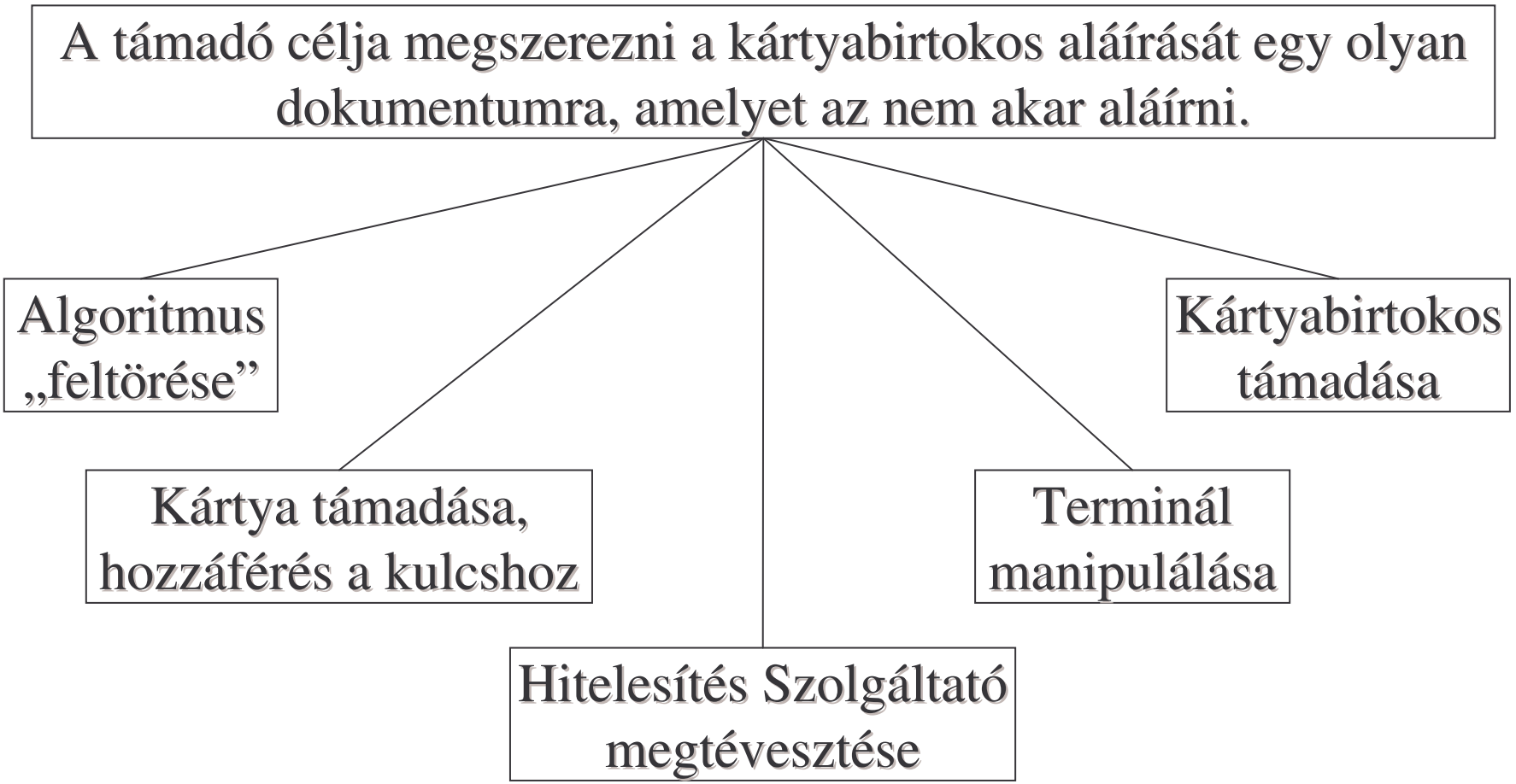
- Az alkalmazásokat védeni kell a kártya felől érkező támadásokkal szemben is
- A támadó is letölthet csaló appleteket
- Appletek közti kommunikáció veszélyei
- A szoftver és hardver minősége központi kérdéssé válik
- Információ szivárgás problémája !

Támadás elektronikus aláírásra szolgáló kártya ellen

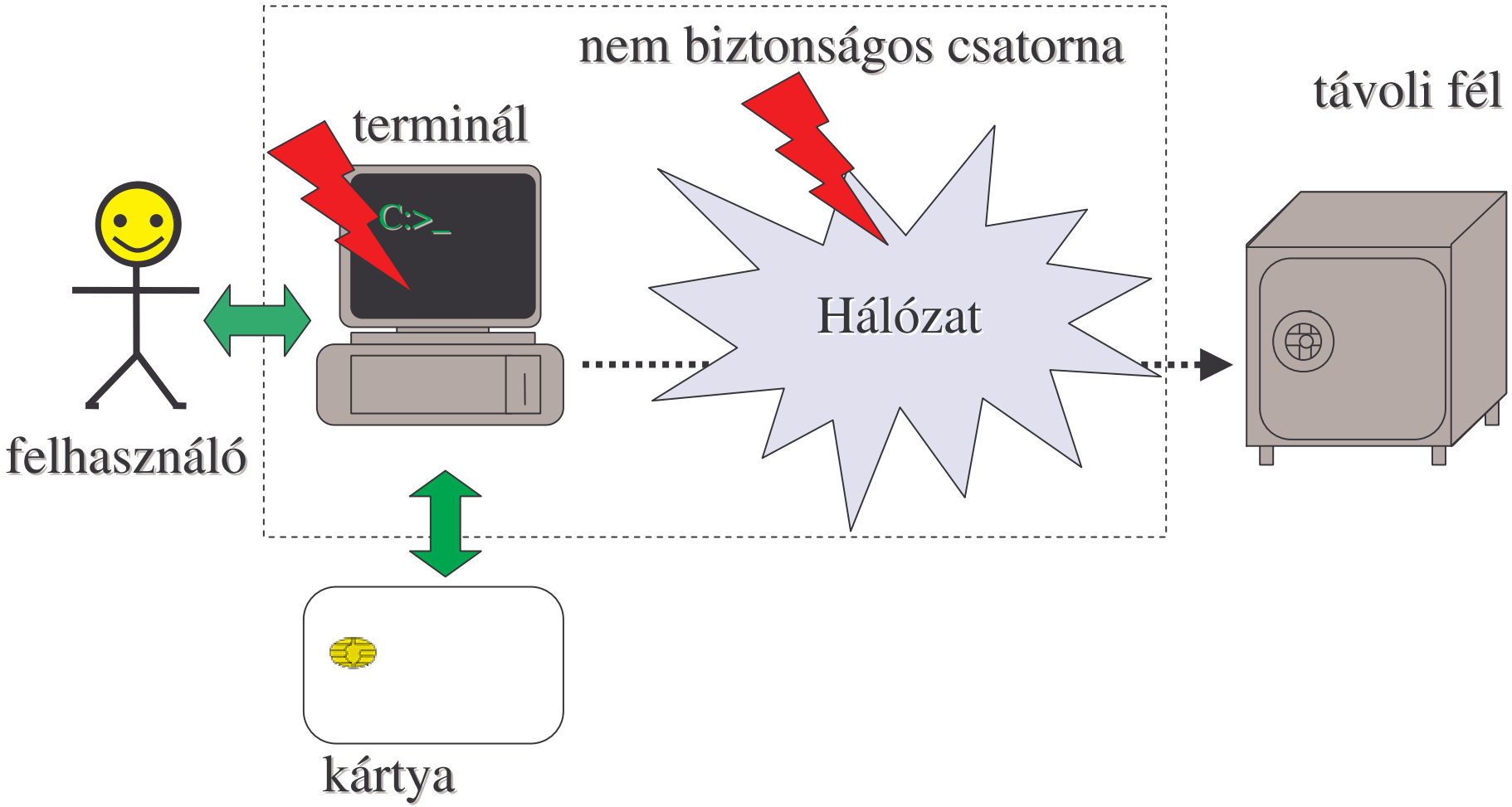
Elektronikus aláírás

- Jogszabály is elismeri (2001. évi XXXV. tv.)
- Minősített aláírás - egyenértékű a kézzel írott aláírással, sőt, teljes bizonyító erejű magánokirat létrehozására alkalmas.
  A létrehozásához kell:
  - → minősített tanúsítvány,
  - → „biztonságos aláírás-létrehozó eszköz (BALE - SSCD) minősítésű eszköz (kártya)

Támadási fa - elektronikus aláírás

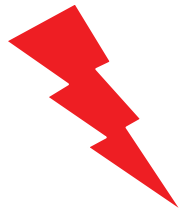


Nem biztonságos terminálok



Nem biztonságos terminálok

- Ha az “ellenség” teljes mértékben irányítása alá vonhatja a terminált,
- a terminál képes a kártya minden inputját és outputját megfigyelni és megváltoztatni,
- természetesen képes a PIN kódot elfogni.
- Hogyan vehetjük észre, ha a terminál man-in-the-middle támadásba kezd?
- Honnan tudjuk, hogy valójában mit írtunk alá a titkos kulcsunkkal?



Hogy lehet kivédeni?

- ~ Sehogy. Ha nem bízunk meg az aláírásra használt számítógépben, hiába biztonságos a kártyánk, nem tudjuk befolyásolni, hogy mit írunk alá.
- Ne használjunk csaló terminált…
- Megoldás: Megbízható terminált kell használni.
  - → biztonságos számítógép
  - → kártya biztosítson lehetőséget az aláírandó dokumentum biztonságos megjelenítésére

Ez esetben mire jó a kártya?

- Biztosítja, hogy az aláíró kulcsunk a zsebünkben van.
- A kulcsról nem lehet másolatot készíteni.
- Ha a kártya egy olvasóhoz csatlakozik, nem tudja befolyásolni, hogy ki, mikor és mit ír vele alá.

Összefoglalás

- Az intelligens kártyák biztonságos mikroszámítógépek;
- Elsősorban magánkulcsok védelmére (a felhasználó kilétének igazolására), vagy egyenleg tárolására használják őket;
- Erős védelmet jelentenek, nagyon nehéz a bennük tárolt információhoz illetéktelenül hozzáférni;
- Nem tudnak közvetlenül a felhasználóval kommunikálni, ez támadási felületet jelent.

A bemutató során használt programok elérhetősége

- Diákigazolvány - GPKPilot (www.gemplus.com ???)
- USB monitor - USBlyzer www.usblyzer.com
- Elektronikus aláírás - e-Szignó www.e-szigno.hu
- Smart Card Toolset www.scardsoft.com
- Hasznos cuccok: www.wrankl.de

Köszönöm a figyelmet!

Mitől intelligens, és hogyan lehet megtámadni?

- Intelligens kártyák biztonsági kérdései -

Dr. Berta István Zsolt, PhD, MBA, CISA

Microsec Kft, K+F és folyamatszervezési igazgató

<istvan@berta.hu>
www.berta.hu