Privacy barát RFID technológia

Knoll Tímea
meak@meak.hu

Hacktivity 2008
Budai Fonó Zeneház, 2008. szeptember 21.

RFID technológia

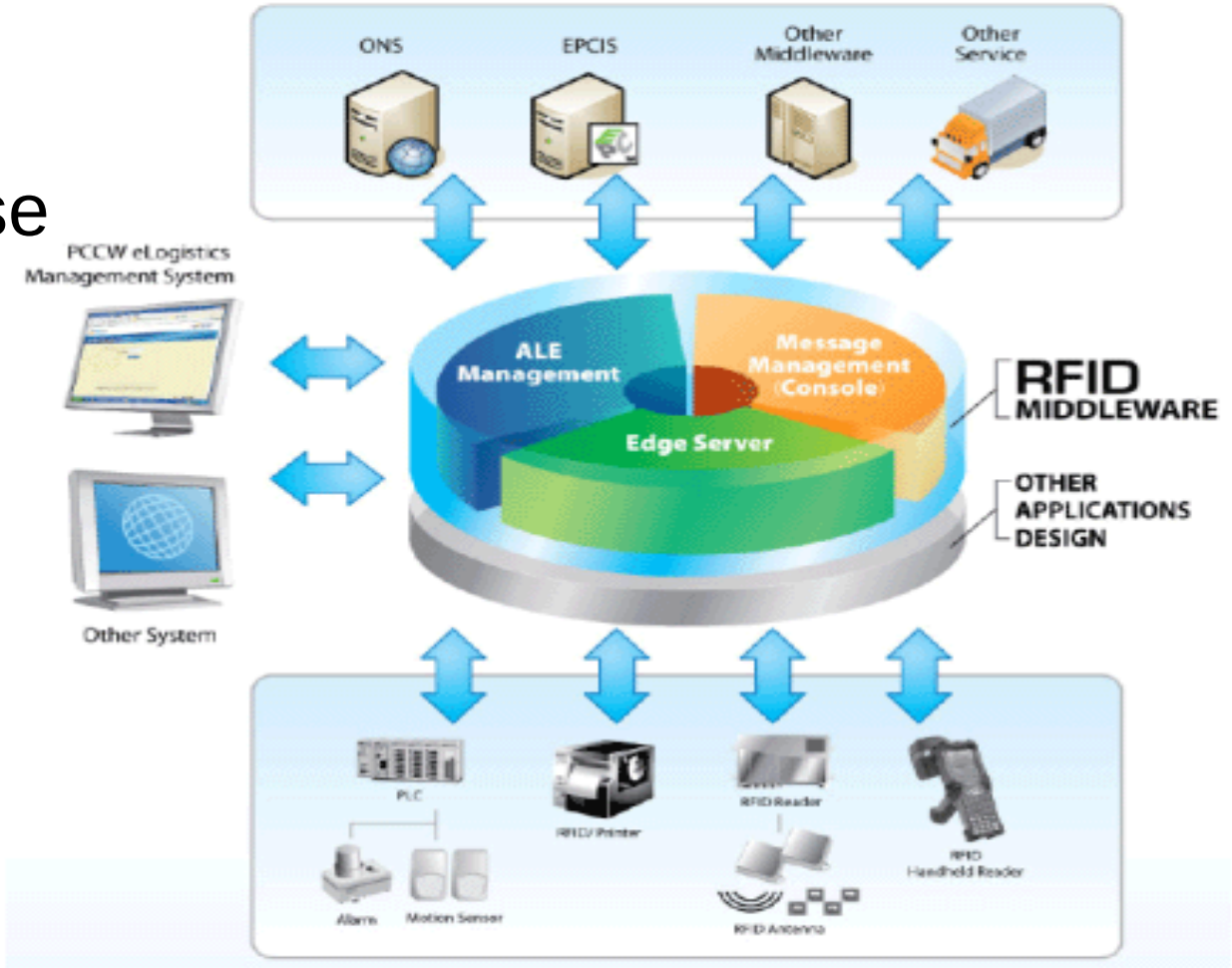
- RF alrendszer, azaz a tag és az olvasó

Mifare Classic kártya és PCR300 RFID író és olvasó

Londoni metró – Oyster kártya olvasók

RFID technológia

- Enterprise alrendszer
- Inter-enterprise alrendszer



Általános RFID alkalmazások

- **asset management**
- tracking
- matching
- process control
- access control
- automated payment
- supply-chain management

Általános RFID alkalmazások

- asset management
- **tracking**
- matching
- process control
- access control
- automated payment
- supply-chain management

Általános RFID alkalmazások

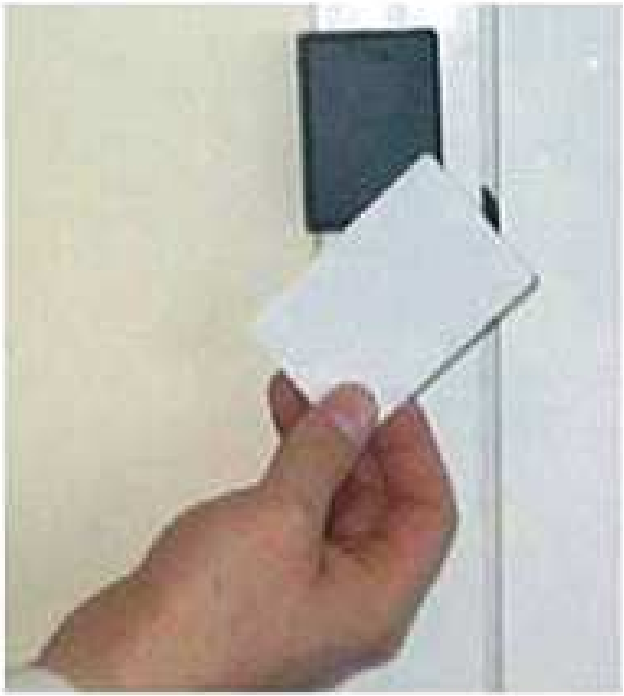
- asset management
- tracking
- **matching**
- process control
- access control
- automated payment
- supply-chain management

Általános RFID alkalmazások

- asset management
- tracking
- matching
- **process control**
- access control
- automated payment
- supply-chain management

Általános RFID alkalmazások

- asset management
- tracking
- matching
- process control
- **access control**
- automated payment
- supply-chain management



Általános RFID alkalmazások

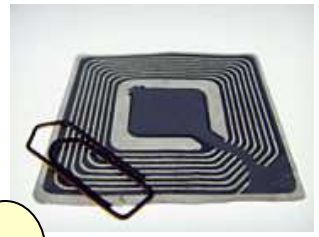
- asset management
- tracking
- matching
- process control
- access control
- **automated payment**
- supply-chain management

Általános RFID alkalmazások

- asset management
- tracking
- matching
- process control
- access control
- automated payment
- **supply-chain management**

RFID és a személyes adataink

- Mit tudhatunk meg a mellettünk ülő emberekről?
- Akarjuk-e, hogy mások tudják csíkos a zoknim?
- Szívesen elmondanád mindenkinek a bankszámlaszámod vagy egészségügyi állapotod?



Privátszférát erősítő technológiák

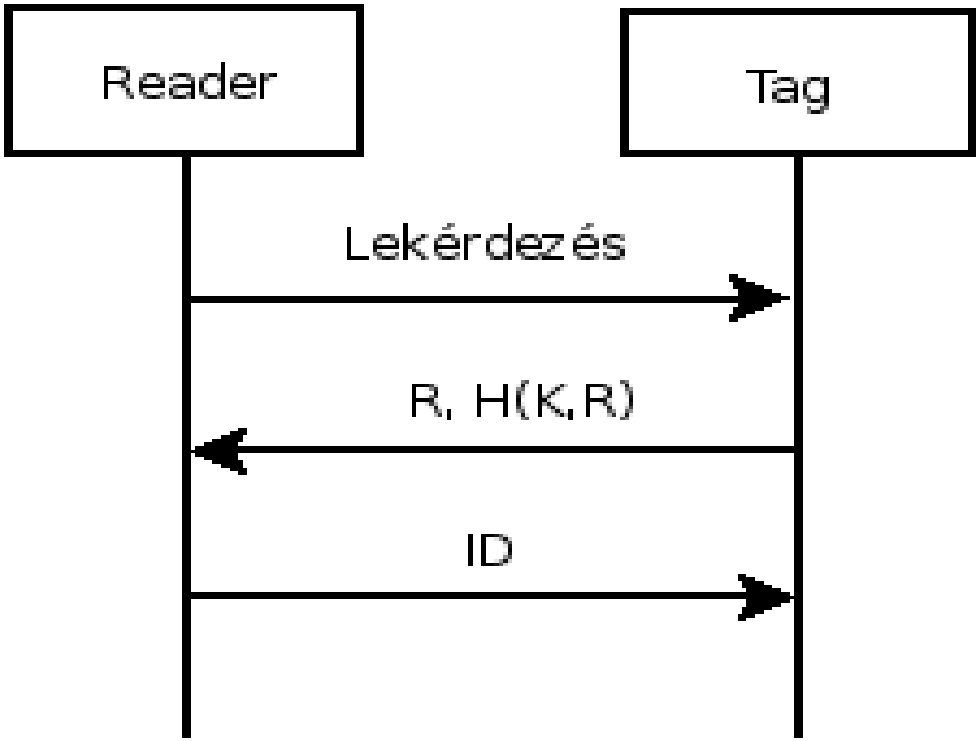
- PET – Privacy Enhancing Technologies
- Célja: nem csak az adatok védelme, hanem az adatok tulajdonosának a védelme is
- Alkalmazások:
  - anonim böngészés
  - anonim üzenet továbbítás
  - bioszkript
  - ...

RFID néhány támadása

- Támadás alapjául a RF alrendszer használható
- Az alap támadásokon kívül a vezeték nélküli kapcsolat és az architektúra újabb támadási felületeket nyitott
- Lehallgatás, üzenetek visszajátszása, módosítása, törlése, Man in the Middle, DoS
- Zavarás: a RF hálózaton a kommunikáció blokkolása
- Klónozás: bitről bitre való másolás más kártyára
- Követhetőség: megfigyelhet-e a „Nagy Testvér”?
- Forward Privacy: az előzetes RFID események visszakövethetősége

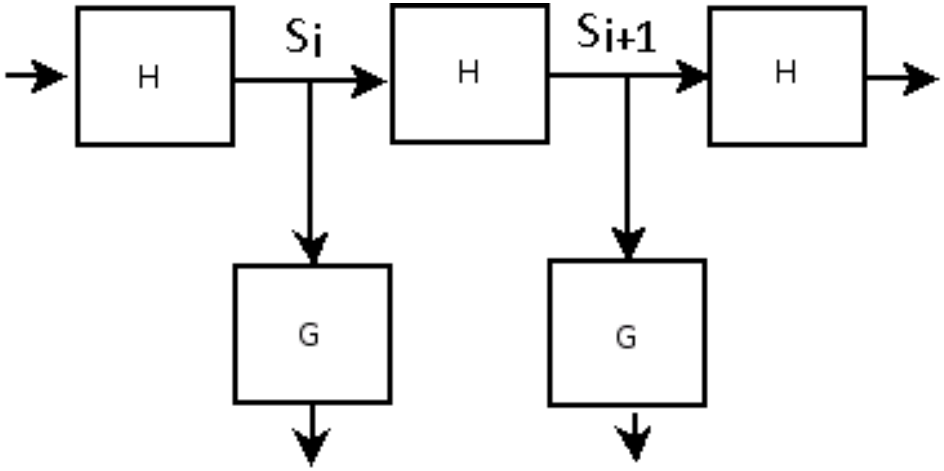
Hash-lock protokoll kiegészítve véletlen számmal

- Az adatbázis a Kulcs- ID párost tárolja
- Visszajátszásos támadás lehetséges
- Nyomkövetés nem lehetséges
- Forward privacy-t nem biztosít



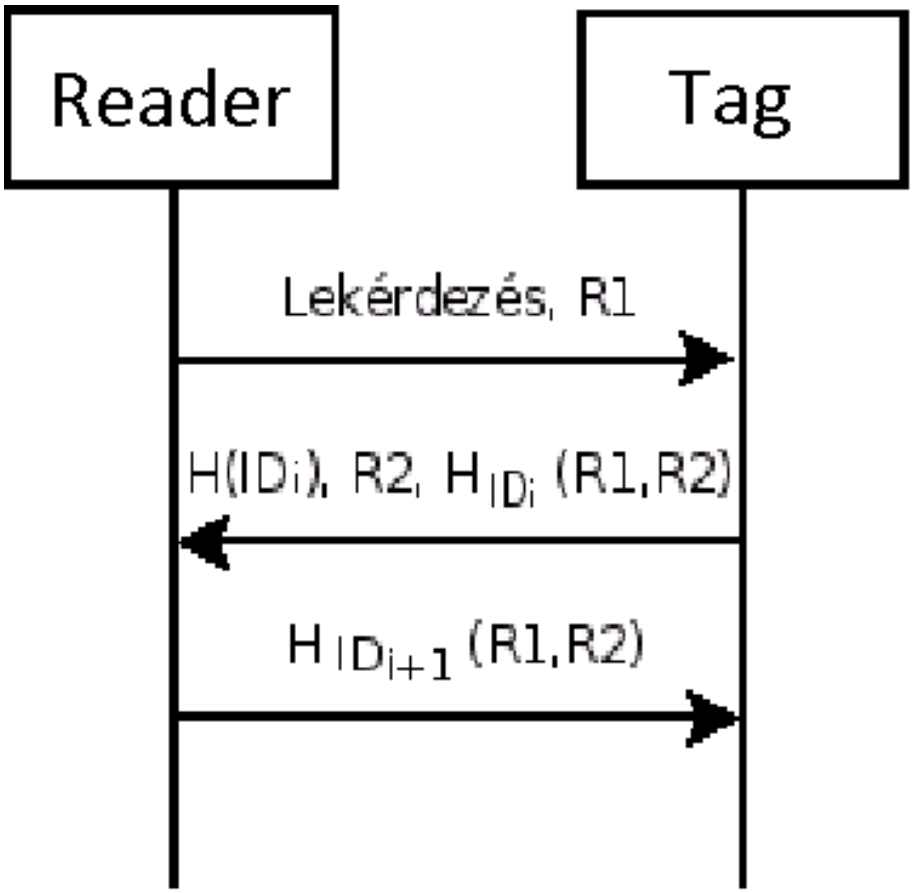
Ohkubo hash-lánc protokoll

- Minden futáskor új kulcs: G(H(Si))
- Az adatbázis az eredeti kulcsot és a H hash-ek számát tárolja
- A back-end i db H hash-t és G hash-t hajt végre
- Visszajátszásos támadás lehetséges
- Forward privacy érvényesül



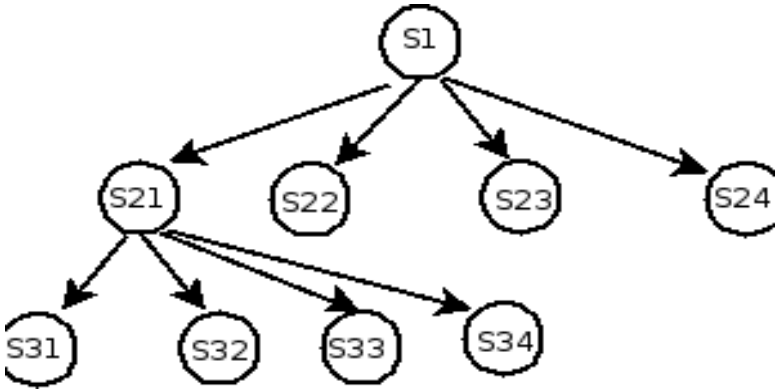
Dimitiou hitelesítési protokollja

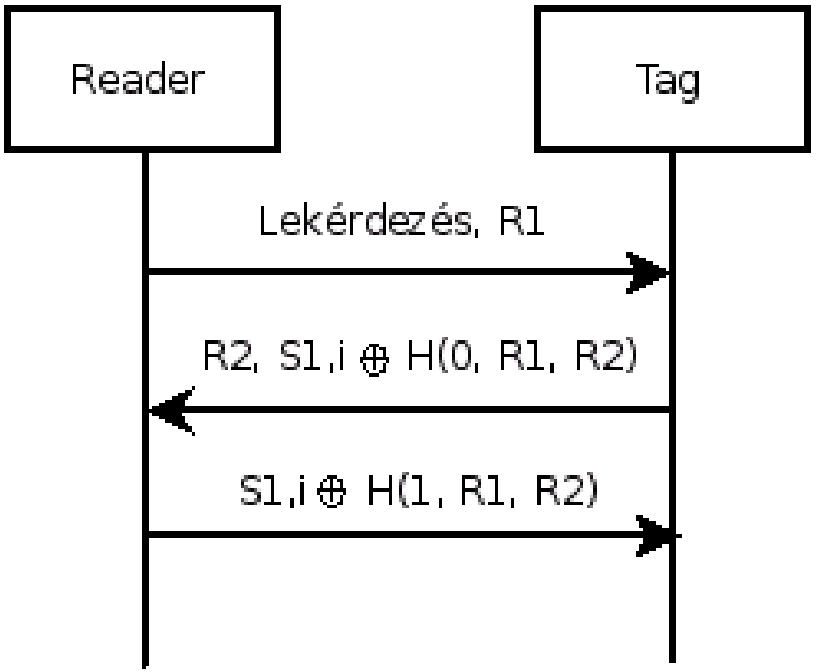
- Anonim
- Visszajátszásos támadás nem lehetséges
- Nyomkövetni nem lehet
- Forward privacy-t biztosít
- Deszinkronizálható



Molnar és Wagner fa alapú protokollja

- Fa levelei a tagok
- Visszajátszásos támadás nem lehetséges
- Nyomkövetés nem lehetséges
- Forward privacy-t biztosít
- Probléma: a kompromitálódott tag csökkenti az anonimitás



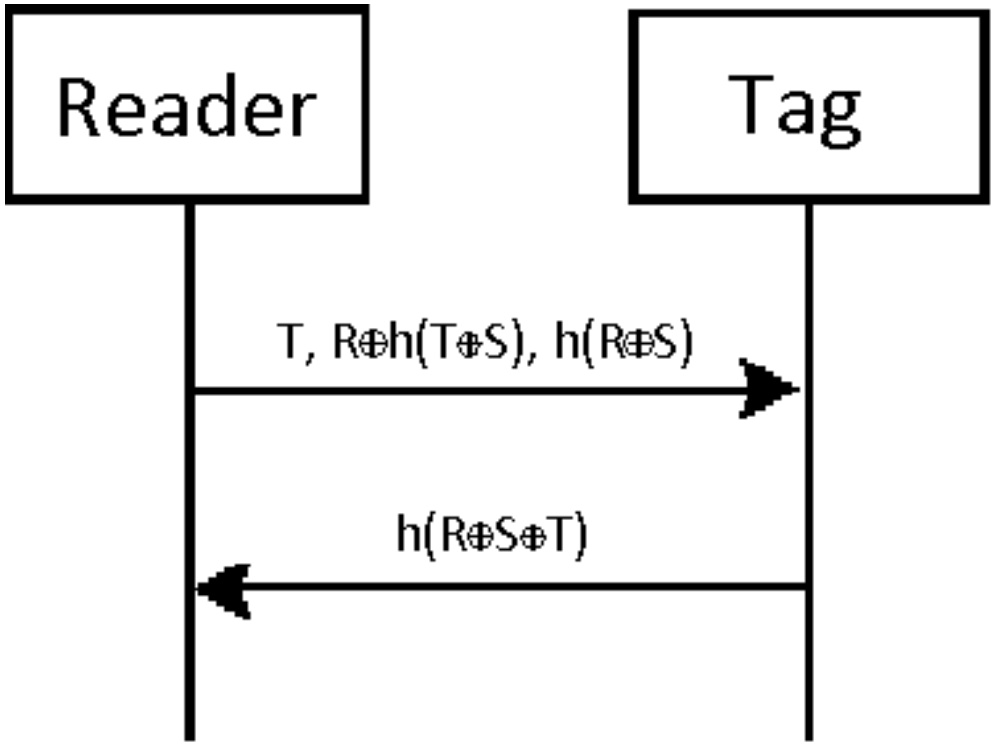


RFID 2.0 – rfidsec.com

- Erős kriptográfiai megoldás
- 128 bit-es titkosító kulcsok és erős hash
- Dinamikus titkosítás, klónozott tagok veszélyének csökkentése
- Egy lépéses authentikáció, előre authentikált olvasóval
- Fejlesztett hozzáférés menedzsment a tag adatokhoz
- A tulajdonos teljesen vezérelheti a tag hozzáférését
- Silent Mode – csak authorizált olvasóknak válaszol

RFID 2.0 – rfidsec.com

- T számláló vagy időbélyeg
- R véletlen szám
- S közös titkos kulcs
- Visszajátszás a T számláló miatt nem lehetséges
- Anonimitást biztosít
- Silent Mode



Mifare

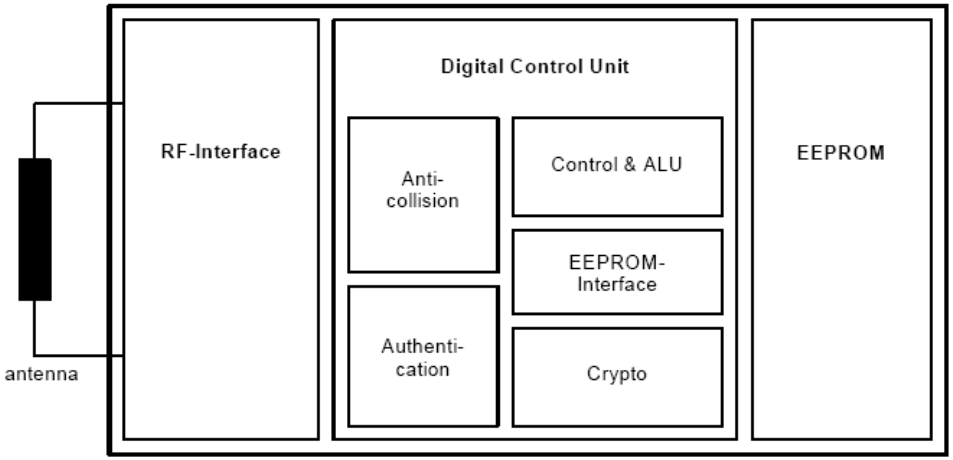
- Gyártó: NXP – Philips Semiconductor
- Szabvány: ISO/IEC 14443 Type A
- Operációs frekvencia: 13.56 MHz ISM sáv
- Ajánlott felhasználási területek:
  - Tömegközlekedés
  - Hozzáférés vezérlés
  - Események jegykezelése
  - Játék & azonosítás

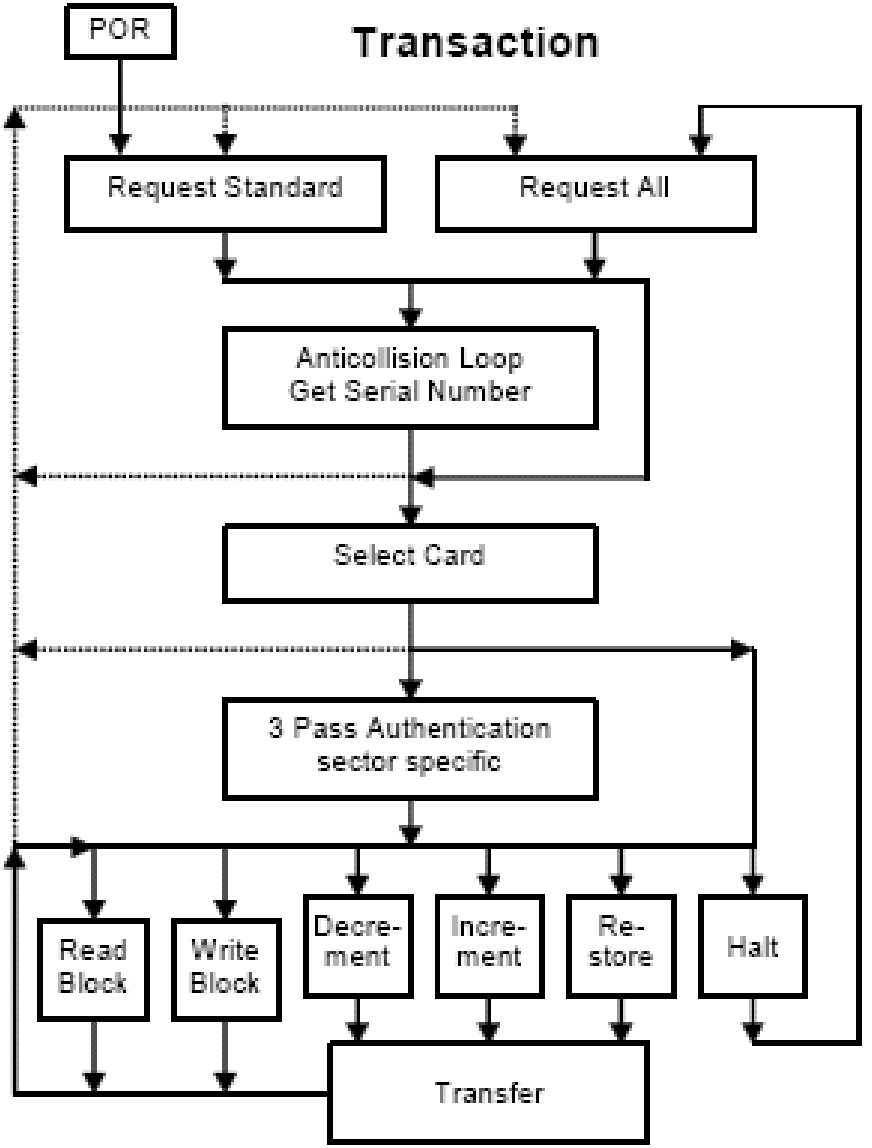
- Több típus: Classic, UltraLight, DESfire, ProX, SmartMX

Mifare Classic és a biztonság

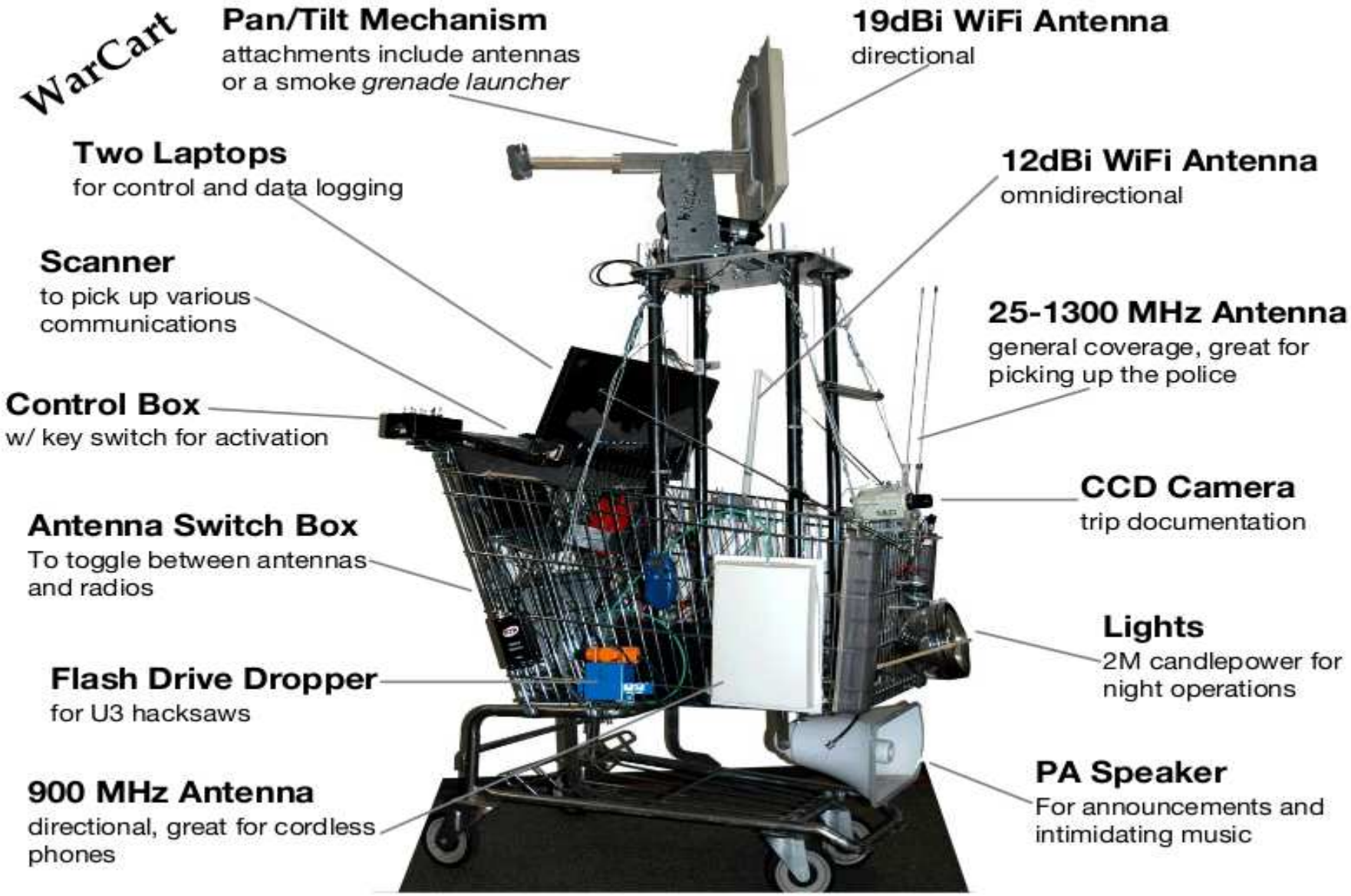
- Kölcsönös 3-utas authentikáció (ISO/IEC DIS 9798-2)
- Eszközönként egyedi ID
- 2 kulcs, mely szektor függő
  - A: A0A1A2A3A4A5 FFFFFFFFFFFF
  - B: B0B1B2B3B4B5 FFFFFFFFFFFF
- 48 bites kulcsok
- Beépített PRNG a belső órajelből generálja a véletlenszámot
- http://www.youtube.com/watch?v=NW3RGbQTLhE

Mifare Classic blokkvázlat és kommunikáció



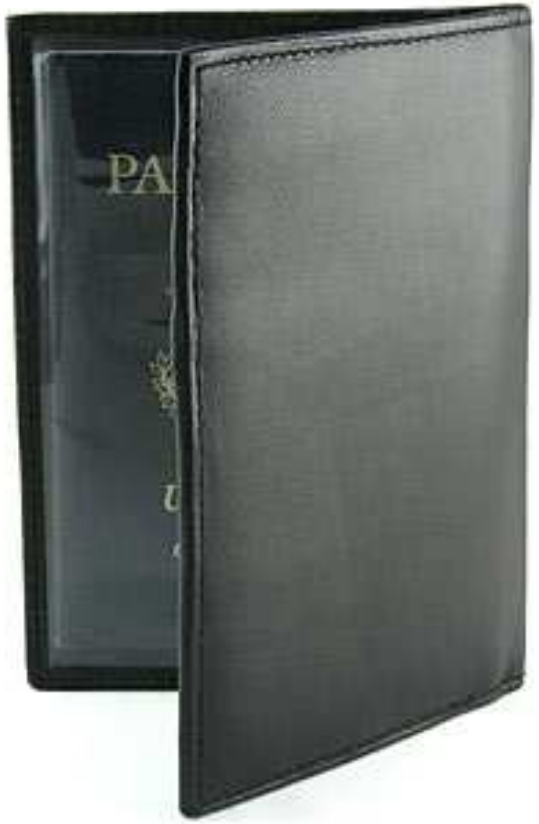


Devcon 2008 - WarCart



E-útlevél

- Sok országban elterjedt
- Szabvány: Nemzetközi Civil Repülési Szervezet (ICAO)
- ISO/IEC 14443 szabványú RFID
- USA-ban BAC és PIN megadása az olvasón kötelező
- Fémtok a távoli olvasás elleni védekezéshez



RFID a bankkártyákban

- Visa, American Express, MasterCard
- Reklám:
  - Biztonságosabb: nem adod ki a kezedből
  - Gyorsabb: 10 másodperc alatt a teljes fizetés
  - Kényelmesebb: nem kell kód $25 alatt
  - Zéró felelősség: csalás bebizonyítása után a bank fizet
- Black Hat - Adam Laurie - élő AmEx törés
- MythBuster show vs Texas Instruments
  http://www.youtube.com/watch?v=X034R3yzDhw
- How to hack RFID-enabled Credit Cards for $8
  http://www.youtube.com/watch?v=vmajlKJlT3U

RFID vs SD card alias SDiD

- SD kártyába épített RFID író és olvasó
- PDA-ba vagy okos telefonba
- Támogatja a NFC-ket
- Mozgatható olvasó
- Hasonló megoldások más kártyákba

RFID által védett külső merevlemezek

- hardware és firmware titkosítás
- nem kell külön driver
- titkosítva formázatlannak tűnik

RFID érdekességek

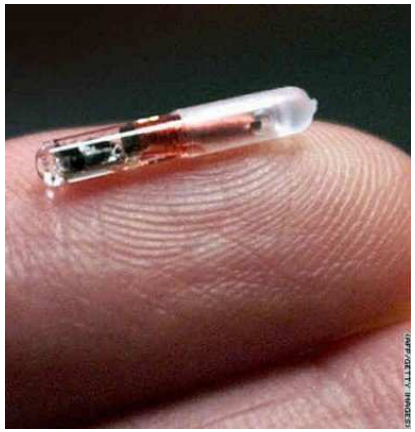
USB és RFID egyben a francia tömegközlekedésben

Tiszteletadás előtt és után használd az RFID kártyád a Japánoknál

Nijmegen-ben rendezett 4 napos gyalogló versenyen RFID kapszulák a versenyzőkben

RFID érdekességek

Kártyapakli RFID taggal ellátva – avagy mire jó ha megfigyelhetjük a lapmozgást



Szerinted hogyan találják meg az elveszett golflabdákat a golfpályákon?

Raknál-e testrészeidbe RFID-t?

Konklúzió

- Jobb, mint a vonalkód
- Drágább még, mint egy vonalkód
- Jól használható
- Érdekes felhasználások lehetségesek
- Biztonságosabbá tehető hitelesítési protokollok megfelelő alkalmazásával és titkosítással

Köszönöm a figyelmet!

Kérdések?