RFID

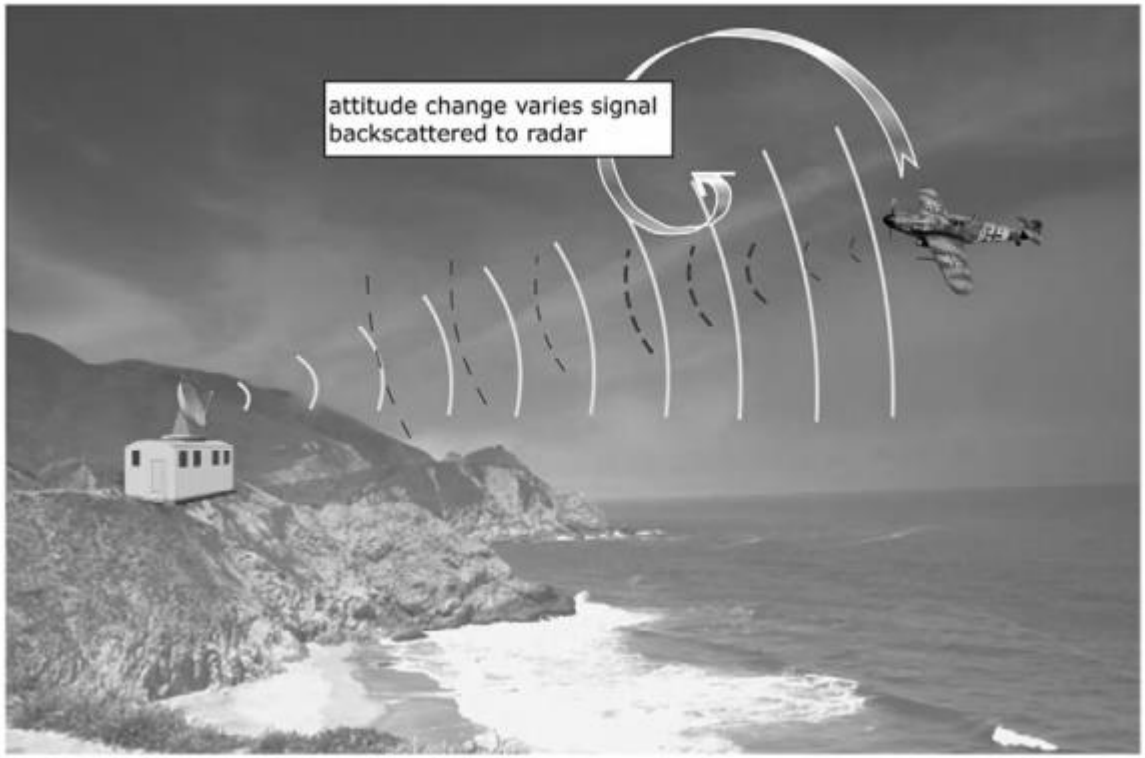
Balogh András
BME-HIT

Az RFID technológia kialakulása

- RFID = Radio Frequency Identification
- Alapvetően az IFF problémakörre vezethető vissza
  - IFF = Identification Friend or Foe
    - Barát vagy ellenség?
  - Az 1930-as években már alkalmazták a mikrohullámú radarokat
    - Az objektumokat azonban csak detektálni tudták
    - Ennek (is) voltak köszönhetők a Pearl Harborban történtek
      - Összetévesztették őket egy US bombázórajjal
    - A Luftwaffe-nek megvolt erre a módszere
      - A célpontot megközelítve csináltak egy orsót
      - Ez egy „villanást” eredményezett a képernyőn
      - Ezzel kvázi azonosíthatóvá váltak
      - Ez volt az első passzív backscattering technika
        - » Passzív = rádiós interfész alkalmazása nélkül

Az RFID technológia kialakulása

- RFID = Radio Frequency Identification
- Alapvetően az IFF problémakörre vezethető vissza
  - IFF = Identification Friend or Foe
    - Barát vagy ellenség?

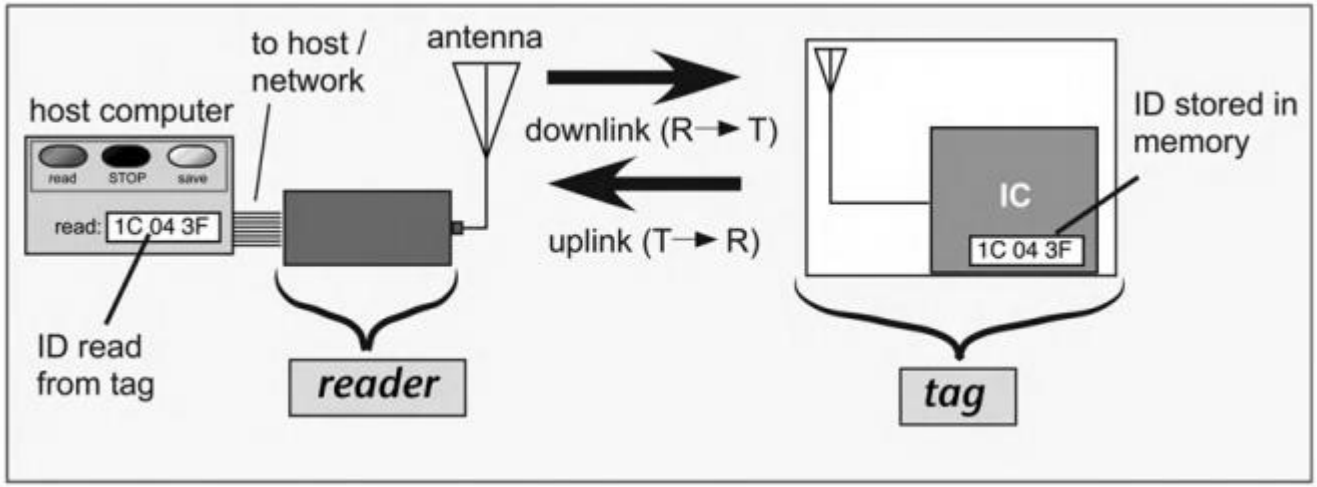


Az RFID technológia kialakulása

- RFID = Radio Frequency Identification
- Alapvetően az IFF problémakörre vezethető vissza
  - IFF = Identification Friend or Foe
    - Barát vagy ellenség?
  - Az 1930-as években már alkalmazták a mikrohullámú radarokat
    - Az objektumokat azonban csak detektálni tudták
  - Az 1950-es évekre ezt a problémakört már megoldották
    - A repülőgépek és a radarállomások kétirányú egyeztetésével
    - UHF sávban (1 GHz környékén)
- Az 1960-70-es években több különböző szabadalom is megjelent
  - 1 GHz környéki megoldások
  - Induktív csatoláson alapuló módszerek
- Célok:
  - Legyen minél olcsóbb (Moore-törvény)
  - Lehetőség szerint ne legyen szükség lokális tápellátásra
  - Minél több eszközt (dolgot) azonosíthassanak vele

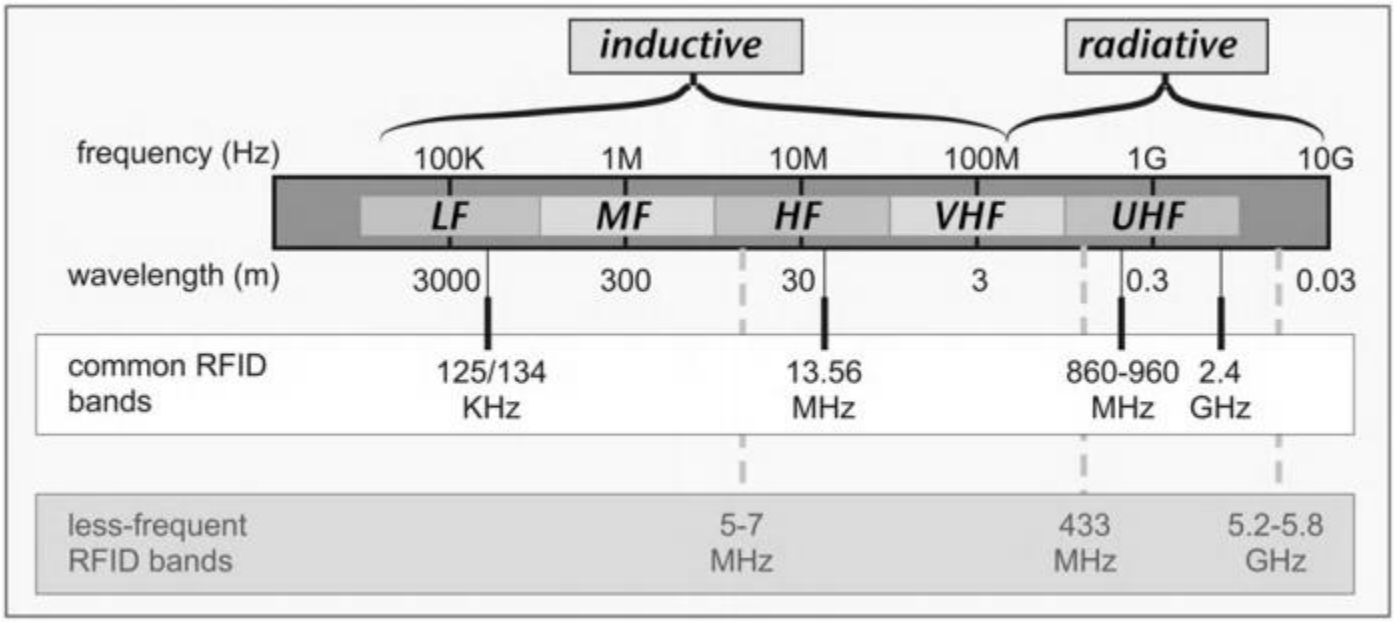
Az RFID technológia működése

- Már az első szabadalmak is két szerepkört definiáltak
  - Olvasó (Reader) és címke (Tag)
- Az olvasó valamilyen vezeték nélküli módszer segítségével kiolvassa címkében található információt:
  - Jellemzően rákérdez
  - A címke válaszol
- A kiolvasott információ alapján a Tag hordozója azonosítható



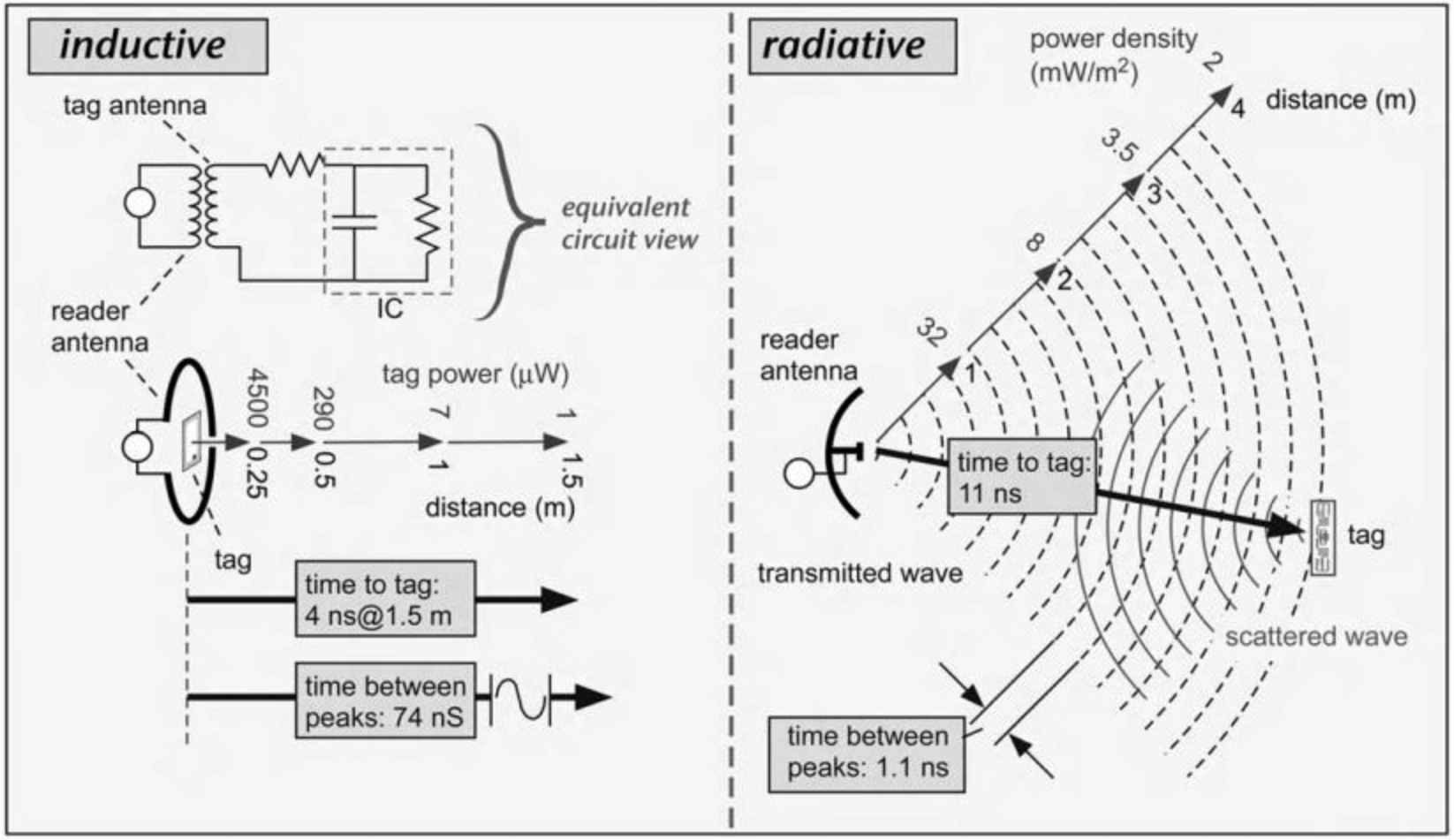
Az RFID technológia működése

- A kommunikációhoz különböző frekvenciasávok alkalmazhatók
  - A frekvenciasávtól függően induktív vagy radiatív csatolás
    - A közeltér/távoltér mintájára
      - Közeltér = induktív és/vagy kapacitív csatolás
      - Távoltér = sugárzási (radiatív) tér (antennák)



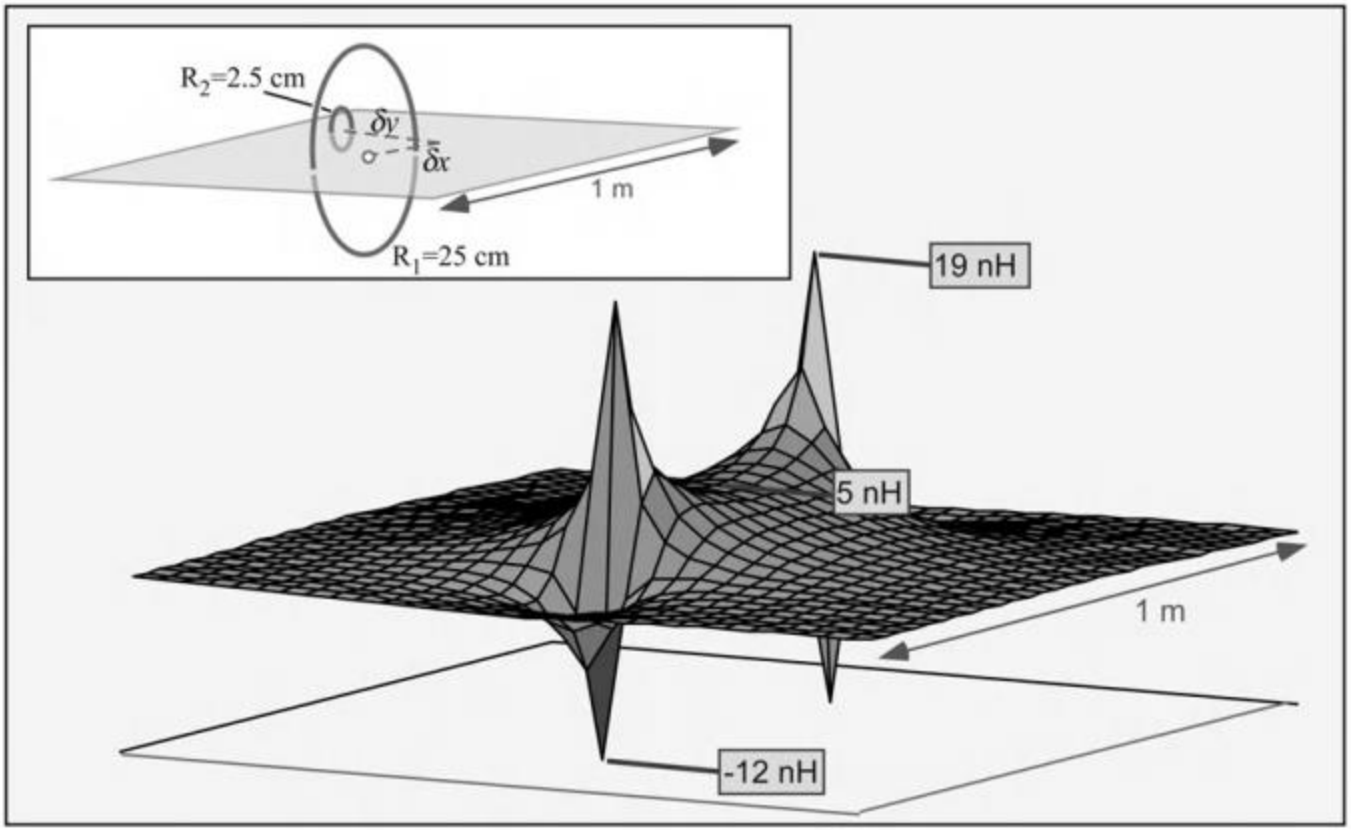
Az RFID technológia működése

- Induktív és radiatív módszerek szemléltetése:



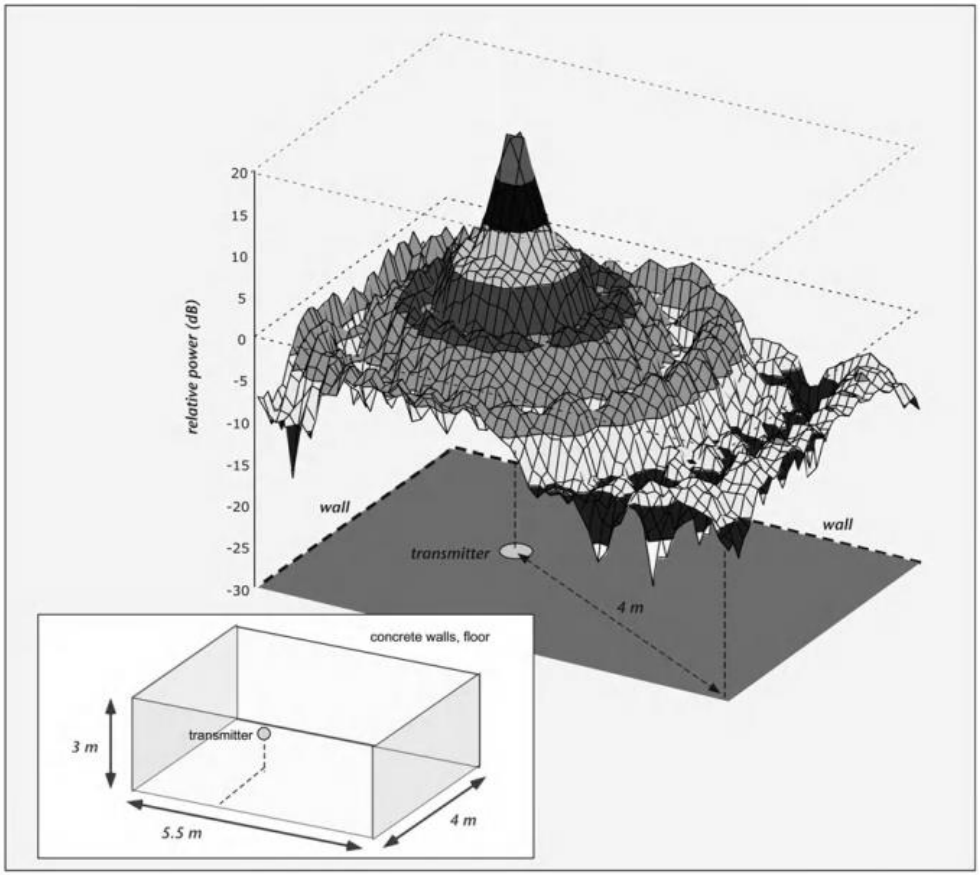
Az RFID technológia működése

- Az induktív csatolás mértéke az olvasó és a tag antenna között
  - Az egymáshoz képesti távolság viszonylatában
  - ~kölcsönös induktivitás
  - Csak kis távolságokban alkalmazható (max. kb. 10 cm)



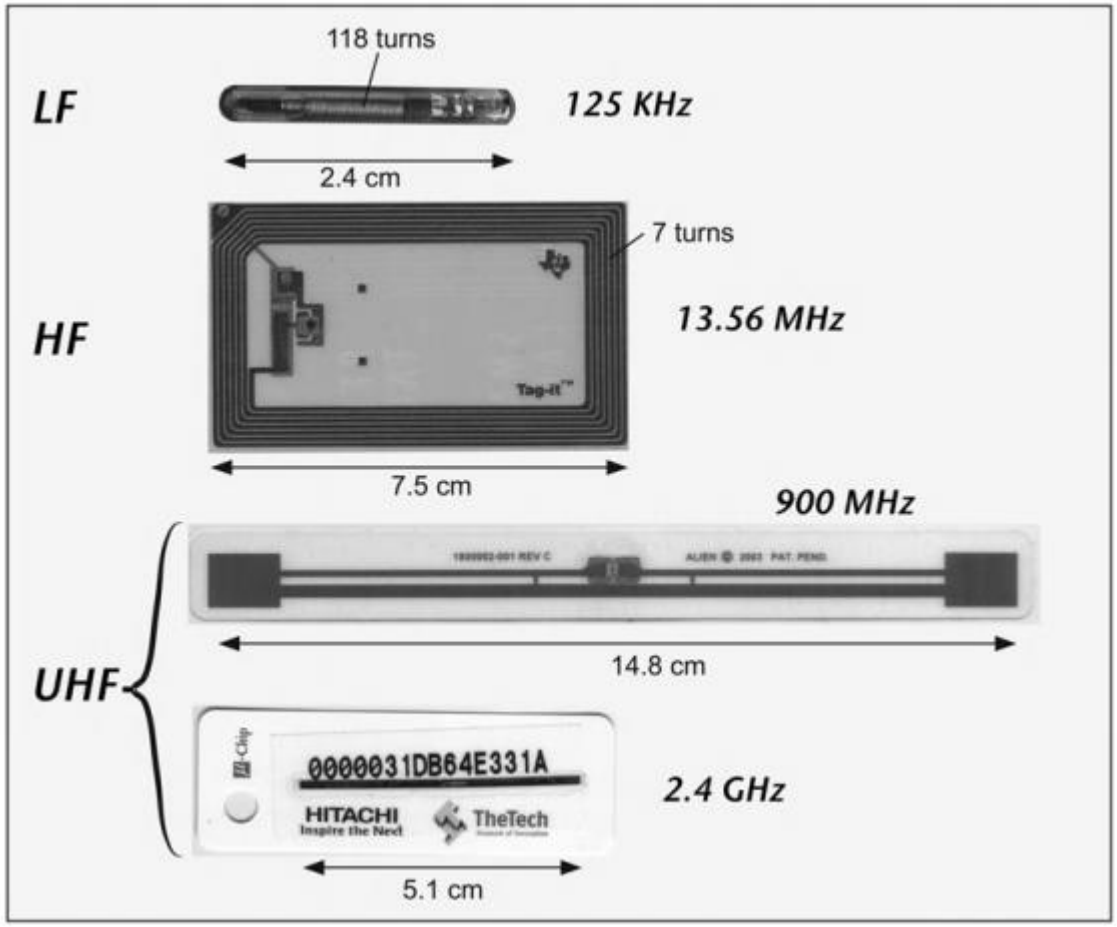
Az RFID technológia működése

- A radiatív csatolás mértéke az olvasó és a tag antenna között
  - Reflexiós jelenségek (többutas terjedés)
  - Nagyobb távolságokban is alkalmazható (max. kb. 10m)



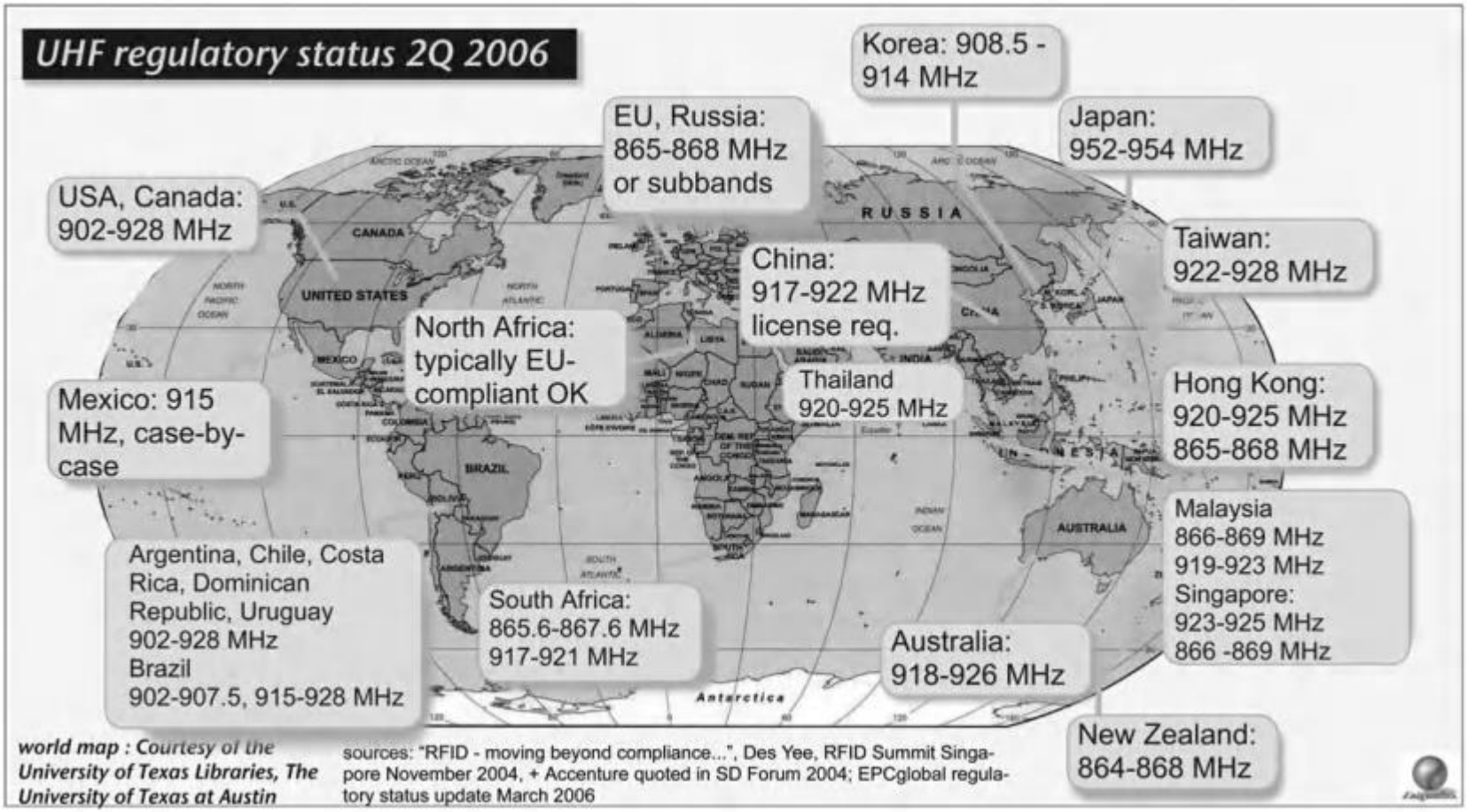
Az RFID technológia működése

- Tipikus (Passzív) RFID Tagek kialakítása



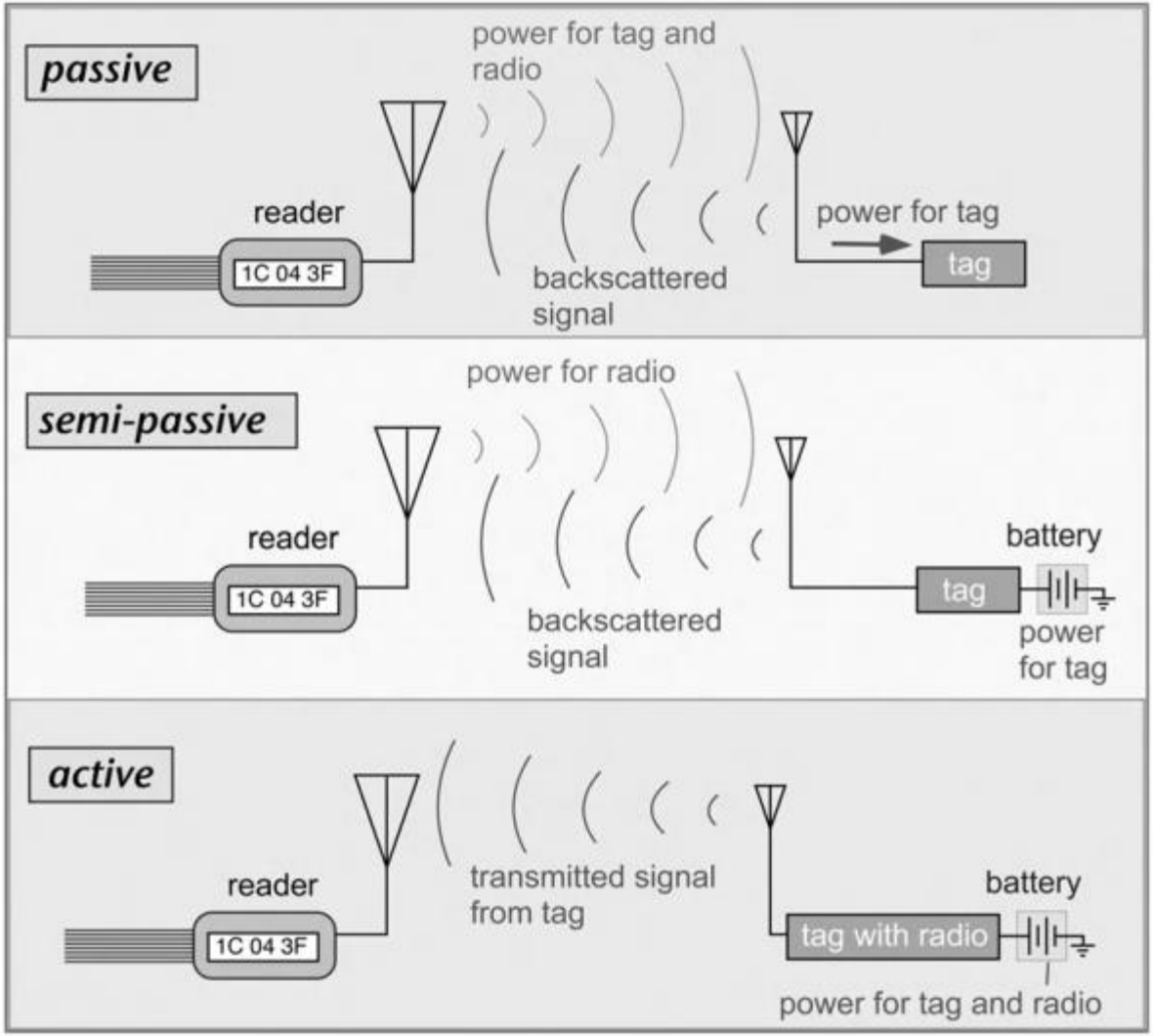
Az RFID technológia működése

- Alkalmazható UHF frekvenciasávok a világ különböző pontjain
  - Előírások 1 GHz környékén



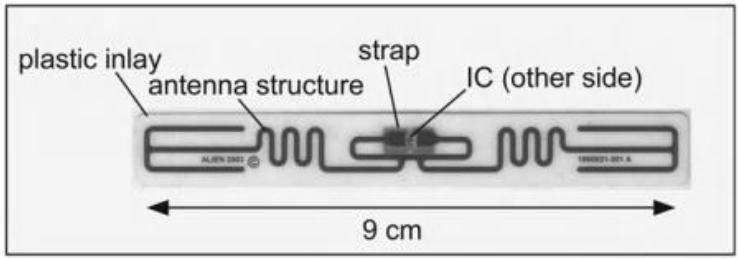
RFID Tagek

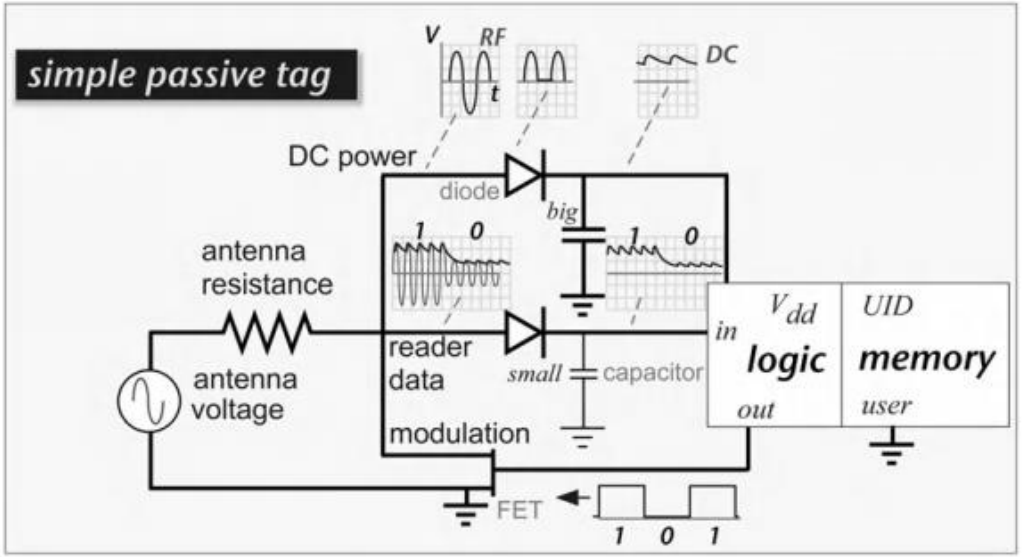
- RFID Tagek osztályozása



RFID Tagek

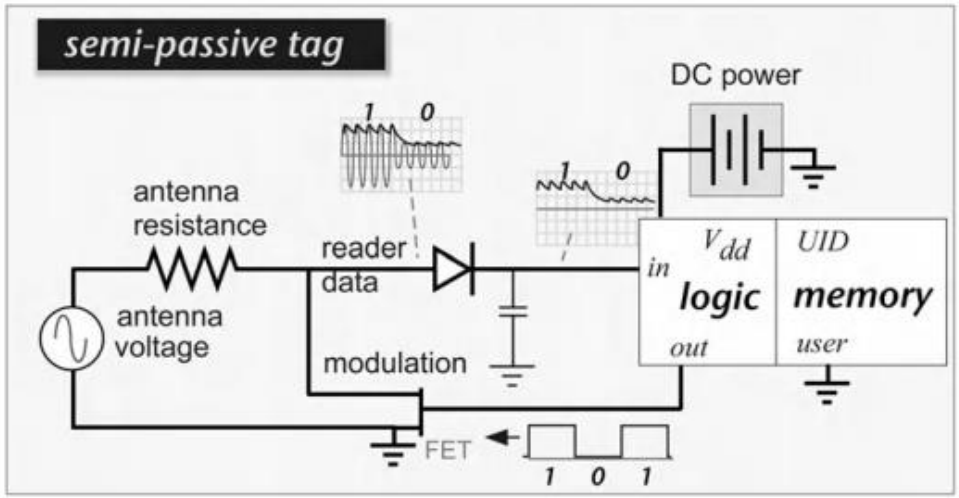
- Passzív RFID Tagek
  - Az olvasó által biztosított nagyobb RF burst-öket egy nagyobb kapacitás töltésére használjuk fel
    - Ez biztosítja a logika és a rádió számára a tápfeszültséget
  - A kisebb RF burst-ök hordozzák az adatot
    - A kisebb kapacitás detektálja a burkolót (envelope)
      - Ez alapján különbözteti meg a 0 és 1 szimbólumokat
  - Nagyon egyszerű logikák futtatására képesek
  - Olcsók (jellemzően < 1 USD)
    - Cserébe: drága olvasók





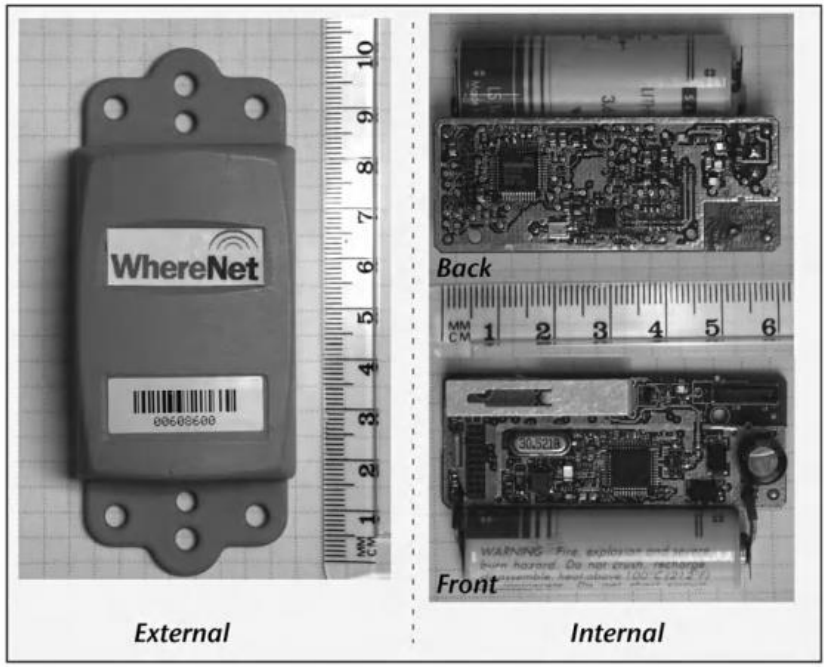
RFID Tagek

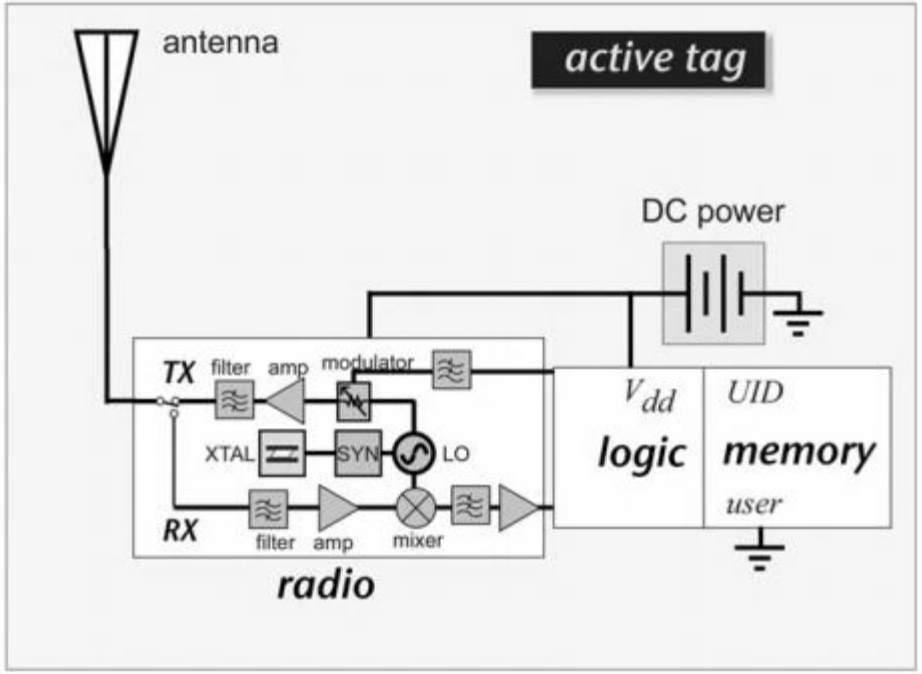
- Szemi-Passzív RFID Tagek
  - Passzív Tag akkumulátorral kiegészítve
    - Az RF frontend lényegében ugyanaz
  - Nagyobb teljesítményen képes uplink irányban kommunikálni
    - Akár több 10 m-es távolságban
    - Nagyobb megbízhatósággal képes válaszolni
  - Egy fokkal drágábbak
  - Bonyolultabb logikák futtatására is képesek
    - Pl. Temperature Logger Tagek



RFID Tagek

- Aktív RFID Tagek
  - Szemi-passzív Tagek komolyabb rádiós képességekkel
    - Különböző modulációk és UHF frekvenciasávok támogatása
      - Pl. 2,4 GHz
    - Különböző csatornahozzáférési képességek
  - Még egy fokkal drágábbak
  - Lényegesen többet fogyaszt





RFID protokollok

- Az RFID igazából egy módszer és nem egy szabvány
  - Temérdek szabványt definiáltak ezen módszer alkalmazására
  - A leggyakoribbak az ISO és az EPC által rögzítettek

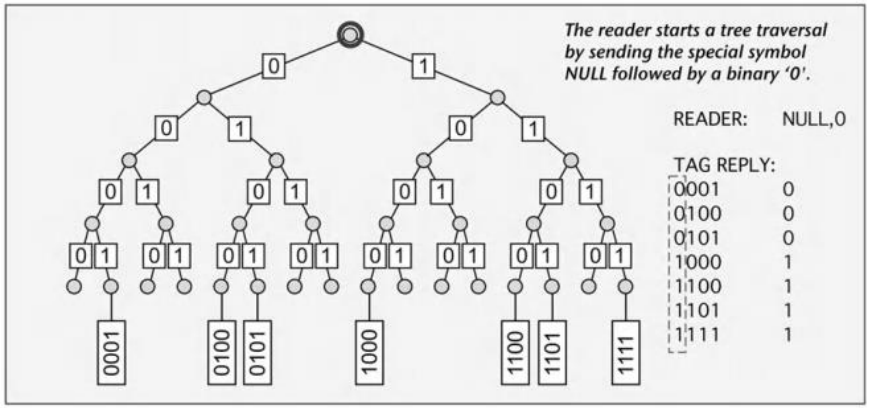
Tag Type	Frequency					
	125/134 KHz	5–7 MHz	13.56 MHz	303/ 433 MHz	860–960 MHz	2.45 GHz
Passive	ISO 11784/5, 14223 ISO18000-2 HiTag	ISO10536 iPico DF/ iPX	MIFARE ISO14443 Tag-IT ISO15693 ISO18000-3 TIRIS Icode		ISO18000-6A,B,C EPC class 0 EPC class 1 Intellitag Title 21 AAR S918 Ucode AAR S918	ISO18000-4 Intellitag µ-chip
Semi-passive					Title 21 EZPass Intelleflex Maxim	ISO18000-4 Alien BAP
Active				ANSI 371.2 ISO18000-7 RFCode		ISO18000-4 ANSI 371.1

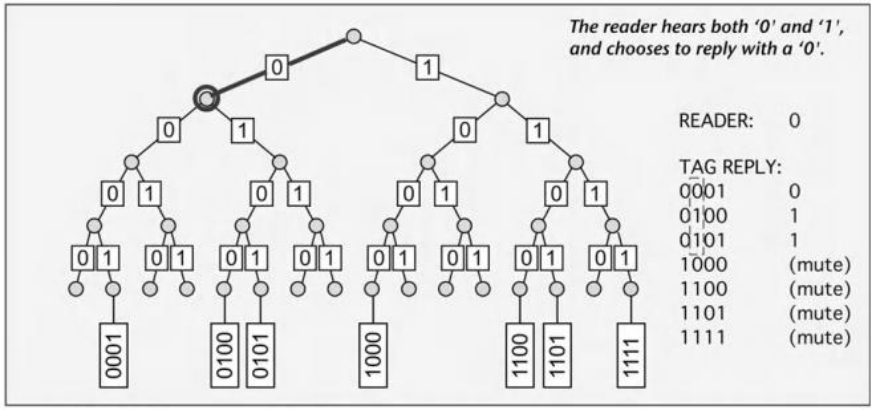
RFID közeghozzáférés

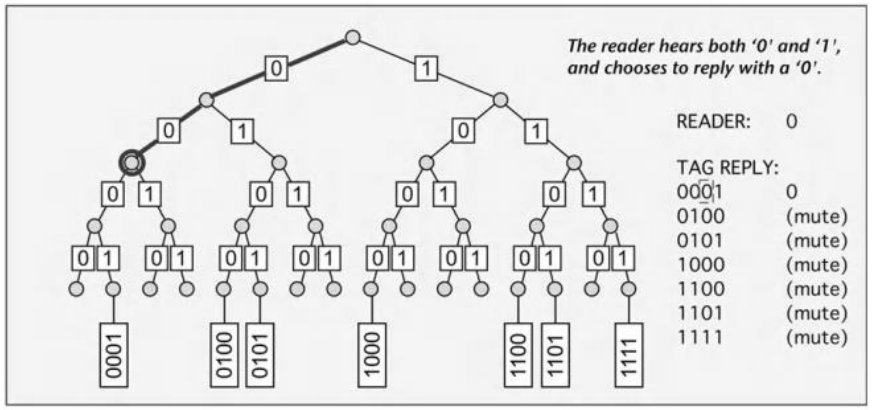
- Alapprobléma
  - 1 olvasó környezetében több Tag is lehet
  - Minden olvasás során felébred az összes
    - Ha többen vannak, kvázi garantált az ütközés
- EPCglobal Class 0
  - A Class 0 esetében alapfeltevés, hogy a Tag ID-ja csak olvasható
    - A gyár fix kódot ír bele (64-96 bit)
  - Az ütközések feloldására, az olvasó bináris keresőfát alkalmaz
    - Folyamatosan növeli a prefix méretét egy NULL üzenetben
      - Tetszés szerint választ 0-t vagy 1-et
      - Elsőre 0 hosszú prefix
    - A Tag mindig az ID-jának az első olyan bitjével válaszol, amit a prefix nem fed le
    - Ha az olvasó egyértelmű választ kap, akkor azt állítja be a prefix következő bitjének
    - A folyamat végeredményeképpen előáll a Tag ID az olvasón

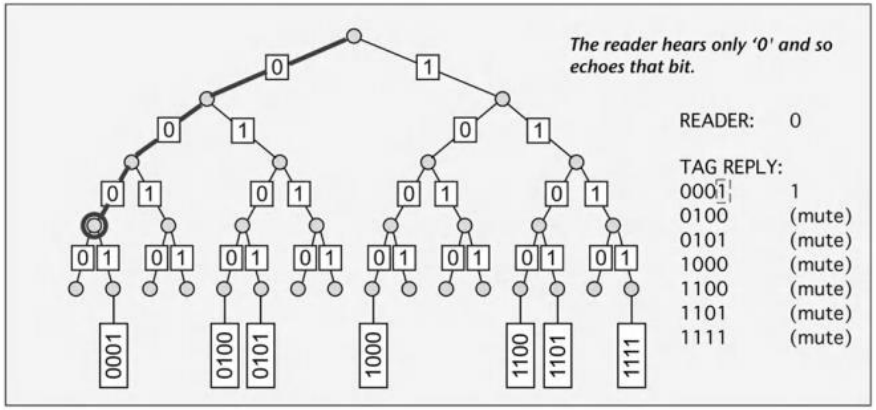
RFID közeghozzáférés

- EPCglobal Class 0
  - Példa 4 bites Tag azonosítóval



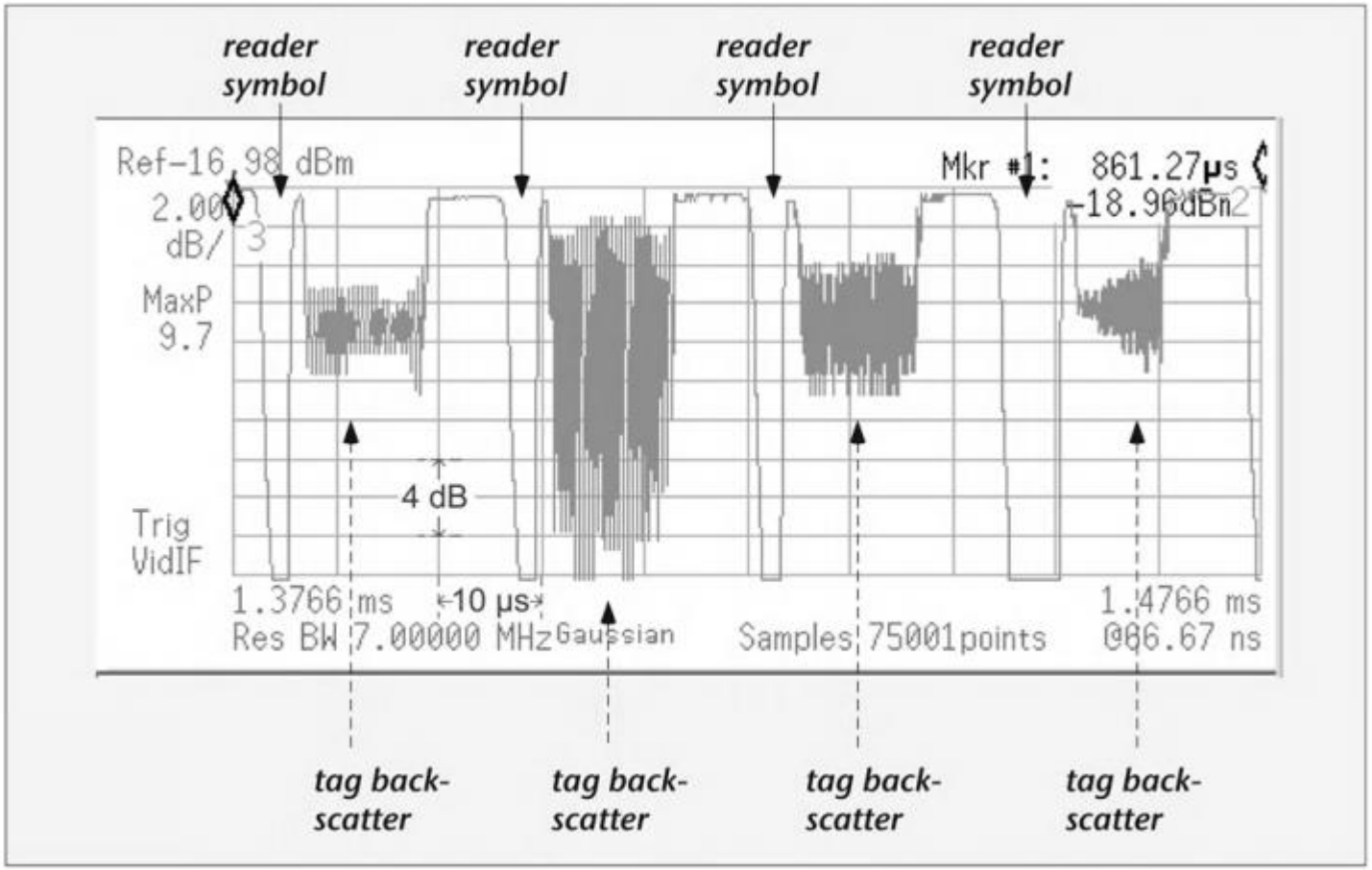






RFID közeghozzáférés

- EPCglobal Class 0
  - Példa 4 bites Tag azonosítóval

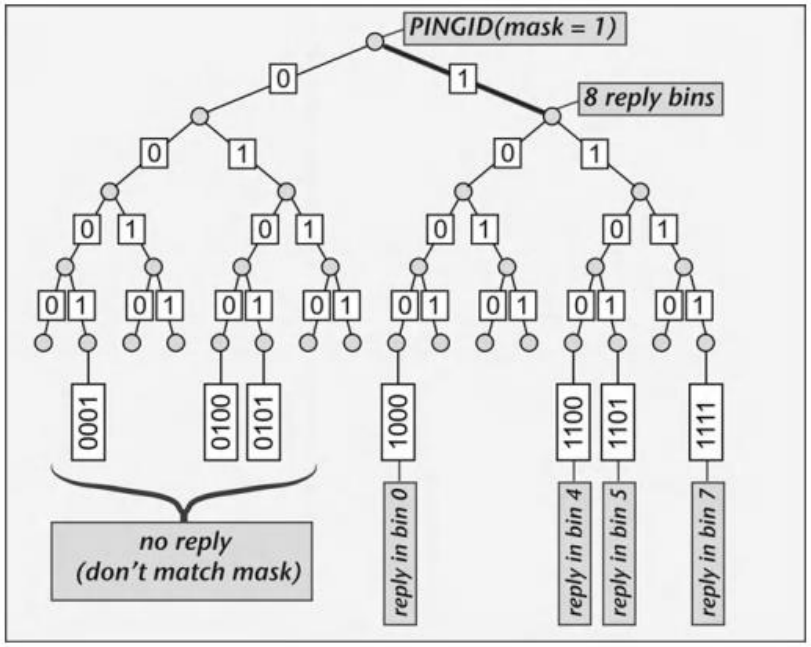


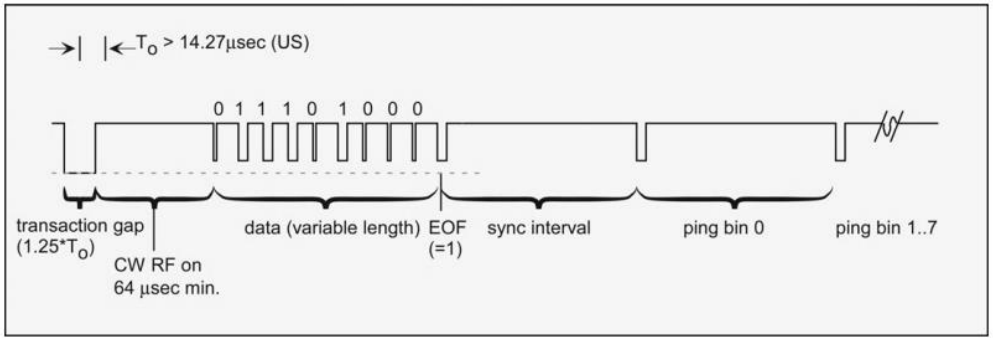
RFID közeghozzáférés

- EPCglobal Class 1 Generation 1
  - A Class 1 esetében már megengedett az átírás
    - Erre definiáltak különböző üzeneteket
      - EraseID, ProgramID
  - Nem kompatibilis a Class 0 Tagekkel
    - A NULL üzenetet nem használják
  - Továbbfejlesztett bináris keresőfa
    - Az olvasó PingID üzenetben küldi a prefixet
      - Itt kijelöl bineket (megmondja azok számát)
      - A bineket a Tagek elosztják maguk között
        - » A nem lefedett ID biteknek megfelelően
      - A Tagek a nekik megfelelő slotokban válaszolnak
    - Lényegesen gyorsabb
  - Egyéb üzenetek:
    - ScrollID – A Tag egyből az egész ID-val válaszol
      - PingScroll esetén a binekben teszi ezt a marad ID-val
    - VerifyID – Security

RFID közeghozzáférés

- EPCglobal Class 1 Generation 1
  - Példa a továbbfejlesztett keresőfára 4 bites ID-kkal
    - Ez esetben egyetlen iteráció elég akár 8 Tag kiszolgálására





RFID közeghozzáférés

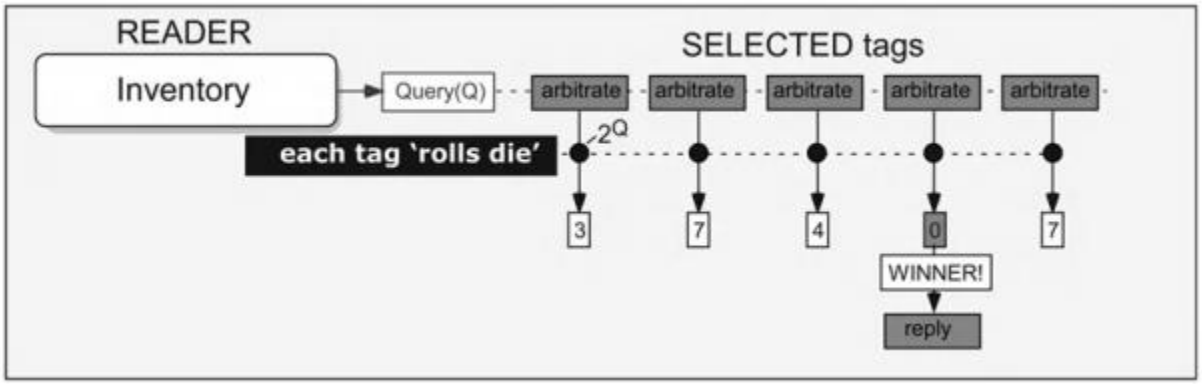
- ISO 18000-6B (Intellitag)
  - Az EPCglobal Gen 1 szabvánnyal párhuzamosan jelent meg
  - Manchester kódolás, ASK moduláció
  - A közeghozzáférés Aloha jellegű
    - 8 bites backoff számláló (0-ról indul), 1 bites random generátor
    - Az olvasó kérdez, a Tag válaszol, amit az olvasó nyugtáz
      - Ha sikeres a Tag ID-jának átvitele (Success nyugta)
        - » Ezt minden más Tag is hallja, csökkentik a számlálót
      - Ha sikertelen (Fail) és a backoff számláló 0 a Tagen
        - » Random 1 bittel növeli, ha újra 0, akkor elküldi az ID-t
      - Ha sikertelen (Fail) és a backoff számláló > 0
        - » Növelik 1-egyel
    - Ha kevés Tag van, akkor 0 közeli backoff értékek jönnek ki
    - Ha sok, akkor felfut egészen, amíg el nem kezdenek Success nyugták érkezni az olvasótól
      - Ekkor elkezdenek csökkenni

RFID közeghozzáférés

- ISO 18000-6C (EPCglobal Class 1 Generation 2)
  - Ez sem kompatibilis az előzőekkel
  - Az előző EPC verziók hátrányai
    - Hátrányos helyzetbe hozták a később érkező Tageket
    - Nem volt titkosítva az Tag ID-k írásának folyamata
    - Nem lehetett rendesen kezelni, ha még nem volt írva a Tag
    - Rossz spektrális hatékonyság
    - Fantom Tag olvasások (zaj)
  - Az új verzió
    - Flexibilis adatráta (spektrum)
    - Aloha jellegű, fair közeghozzáférés (Q protocol)
    - Random számokkal azonosítható logikai session-ök
      - Pl. ha ugyanaz volna Tag azonosítója
    - Secure Tag programming
    - Compliance és interoperabilitási tesztek előírva

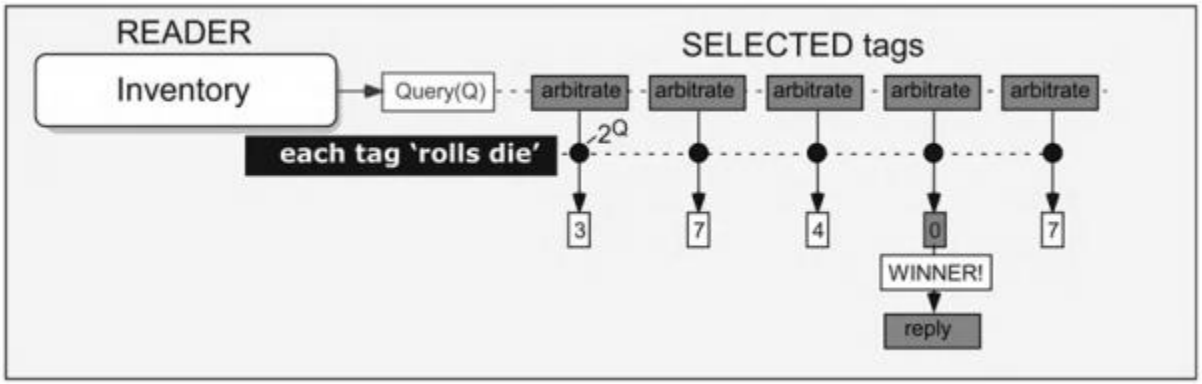
RFID közeghozzáférés

- ISO 18000-6C (EPCglobal Class 1 Generation 2)
  - Q protocol
    - Az olvasü definiálja slotok számát egy inventory round-ban
      - Minden Tag véletlenszerűen választ ezek közül
    - Az olvasó minden slot elején megszolít egy oda került Taget
      - A Tag egy véletlen számmal válaszol
      - Ha az olvasó ezt vissza tudja fejteni (decipher) és jó számot ad vissza (ack)
        - » A Tag elküldi az ID-ját
      - Ugyanez a véletlen szám szolgál a session azonosítására



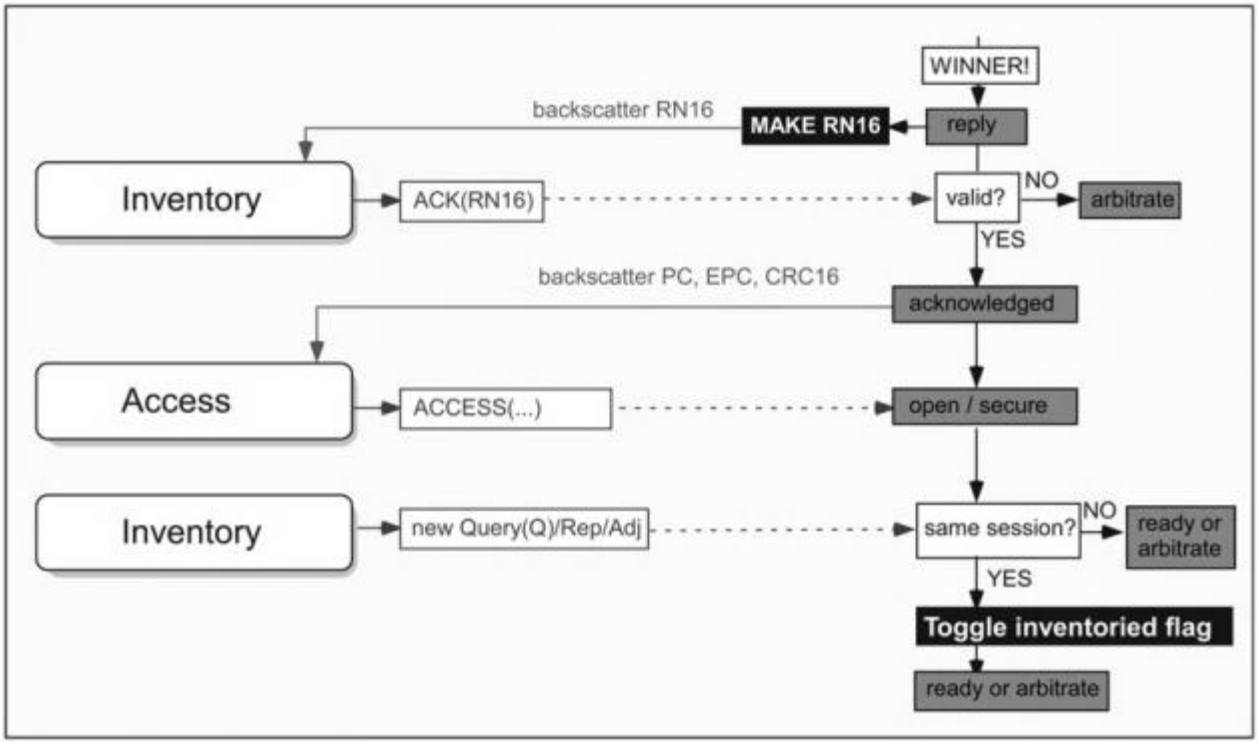
RFID közeghozzáférés

- ISO 18000-6C (EPCglobal Class 1 Generation 2)
  - Q protocol
    - Az olvasó definiálja slotok számát (Q) egy inventory round-ban
      - Minden Tag véletlenszerűen választ ezek közül
    - Az olvasó minden slot elején megszolít egy oda került Taget
      - A Tag egy véletlen számmal válaszol
      - Ha az olvasó ezt vissza tudja fejteni (decipher) és jó számot ad vissza (ack) -> Security
        - » A Tag elküldi az ID-ját
      - Ugyanez a véletlen szám szolgál a session azonosítására



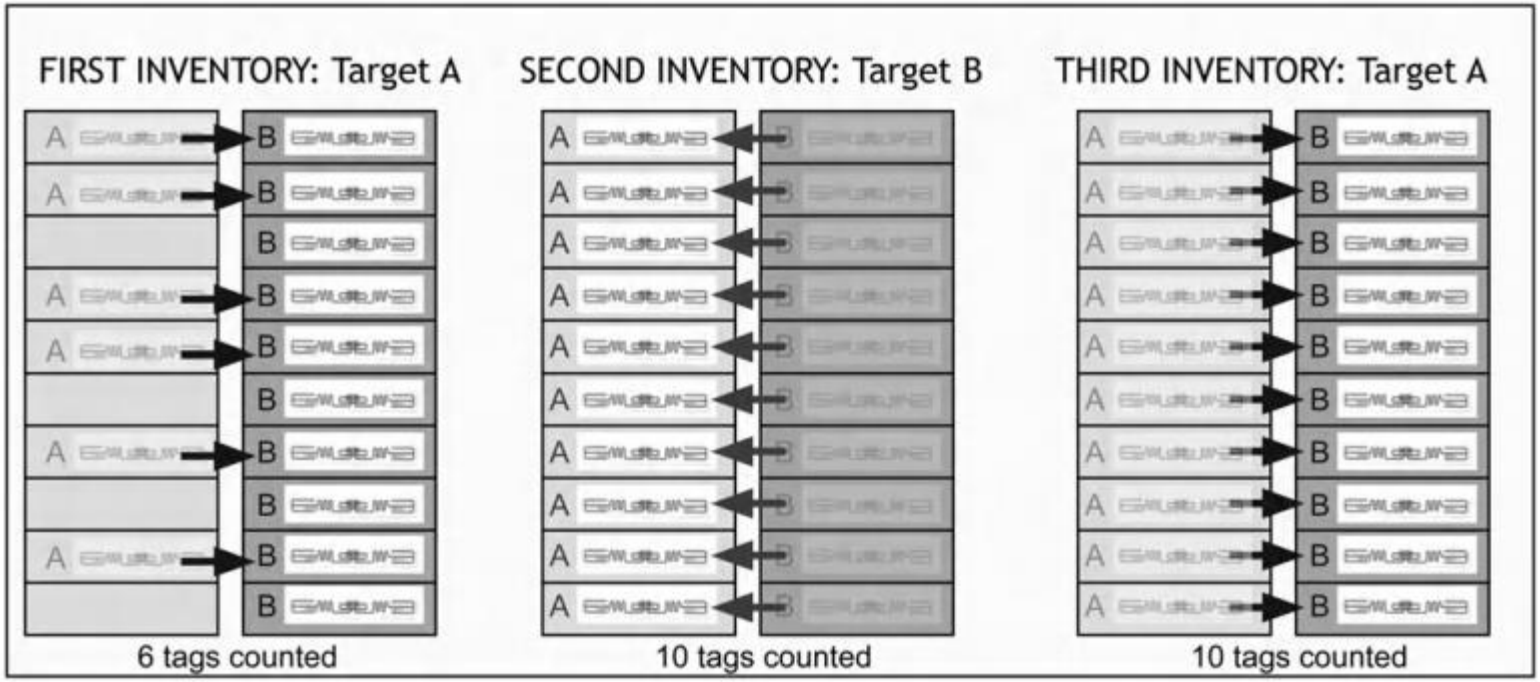
RFID közeghozzáférés

- ISO 18000-6C (EPCglobal Class 1 Generation 2)
  - Q protocol
    - Az ütközéseket nem feltétlenül képes detektálni
    - Növelheti, vagy csökkentheti a Q méretét a zajos/üres slotok számának megfelelően



RFID közeghozzáférés

- ISO 18000-6C (EPCglobal Class 1 Generation 2)
  - Q protocol
    - Az ütközéseket nem feltétlenül képes detektálni
    - Növelheti, vagy csökkentheti a Q méretét a zajos/üres slotok számának megfelelően
      - Amíg már nincs változás



NFC

- NFC = Near Field Communication
  - NFC Forum kezeli a specifikációkat
- RFID alapú kis hatótávolságú (néhány cm) technológia
  - Induktív csatolást alkalmaz 13,56 MHz-en (HF)
  - Manchester kódolás, ASK moduláció
  - Kb. 100-400 kbps adatátviteli sebességek
- Passzív és aktív üzemmódok
  - Passzív = az olvasó „generálja a teret”, a Tag válaszol
  - Aktív = felváltva működnek olvasóként, majd Tagként
    - Ez Peer-to-Peer jellegű kommunikációt tesz lehetővé
- Kommunikácó NDEF üzenetek formájában
  - NDEF = NFC Data Exchange Format
- A legtöbb okostelefon már támogatja
  - Jellemzően nyílt API-ból elérhető