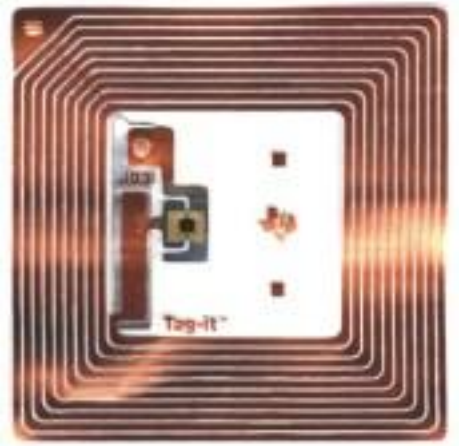
2.5. RFID – общи данни

- Radio-Frequency IDentification
  - Технология за разпознаване на обекти, без осъществяване на физически контакт
- Използва се за:
  - Безконтактни идентификационни карти
  - Електронни паспорти
  - Маркиране на стоки (вместо баркод)
  - Разпознаване на банкноти
  - Имплантирне в живи същества
  - ...

2.5. RFID – технология

- Пасивни RFID устройства
  - Представляват малки електронни чипове с антена
  - За захранване използват силен електромагнитен сигнал от четящото устройство (индукция)
  - След инициализация започва да излъчва константна стойност, която се проверява срещу предварително регистрирани в базата на системата за сигурност номера

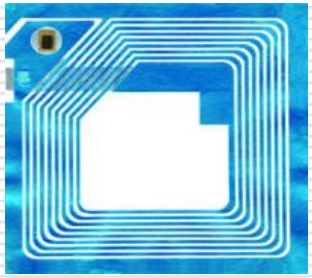


2.5. RFID – технология

- Пасивни RFID устройства
  - Работят на разстояние до 3 метра (3-5 см)
  - Малък обем на излъчваната информация – до 1 KB (64 bits), рядко има възможност да се промени заложената константа
  - Силно ограничени изчислителни възможности на процесора
  - Трудно едновременно разчитане на повече от един чип
  - Предимство – цена, най-често използвани

Захранващ сигнал

Информация, записана в RFID чипа



2.5. RFID – технология

- Активни RFID устройства
  - Използват външно захранване
  - Работят на разстояние 100+ метра
  - Голям обем на излъчваната информация – 128+ KB
  - Възможност за записване на потребителска информация
  - Разширени изчислителни възможности на процесора
  - Възможност за използване на криптографски методи за защита на комуникацията
  - Бързо изчитане на информацията, подходящо за идентификация на подвижни обекти, разчитане на повече от един чип

2.5. RFID – атаки

- Стандартна Man In The Middle (MITM) атака
  - Избягва се чрез екраниране
  - Извличане на лични данни
- Атака срещу идентифициращия модул
  - Отказ от услуга (DoS)
  - Изпращане на валидна идентификационна константа (клониране)
- Атака срещу RFID чипа
  - Отказ от услуга (DoS)
  - Модифициране на изпращаната константа

2.5. RFID – одитиране

- Анализ на риска – трябва ли ни такъв тип идентификация?
- Идентифициране на използваните технологии и устройства
- Преглед на “горещите точки”, където се използва RFID (идентификация)
- Проверка на реакциите на системата при прилагане на различните видове атаки
- Компетентност на служителите
- Комбиниране с други методи за защита – физически (екраниране, видео-наблюдение и др.) и информационни (защитеност на централната оторизационна база, водене на системни журнали/logs и др.)

Към използването на безконтактни схеми за оторизация трябва да се подхожда с голямо внимание, като се идентифицират и анализират всички технологични рискове!

За повече информация:

http://lasecwww.epfl.ch/~gavoine/rfid/