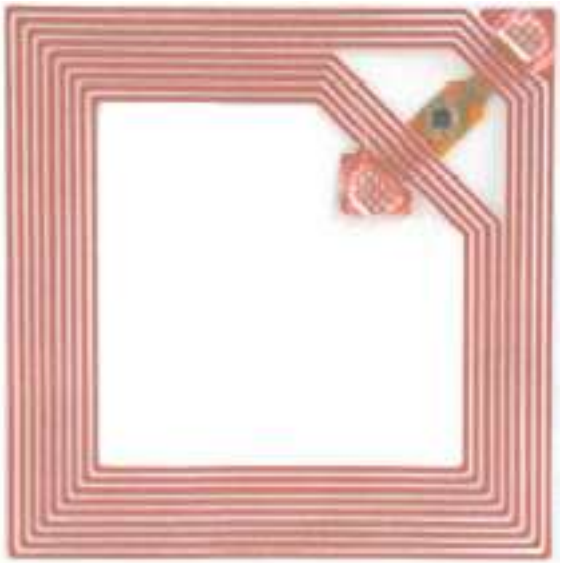
# RFID
# Zwischen Paranoia und Innovation



Frank Rosengart <*frank@rosengart.de*>

# keine neue Technik

- 60er Jahre: Electronic Article Surveillance, EAS
- 70er Jahre: Kennzeichnung von Tieren
- 80er Jahre: Mikrowellentechnik für Mautsysteme
- 90er Jahre: erste Zugangsysteme, Bezahlsysteme
- um 2000: starker Preisverfall, Massenkennzeichnung kommt
- zunehmende Miniaturisierung

*(Quelle: de.wikipedia.org)*

# Anwendungsgebiete

- Zutrittskontrolle / Bezahlsysteme
  - Skipass, Schwimmbad
  - Öffentlicher Nahverkehr
  - Schließanlagen, Wegfahrsperre
  - Reisepass


- Artikelindentifikation
  - Einzelartikel: Electronic Product Code EPC
  - Büchereien, Archive
  - Logistik
  - Dokumenteverwaltung

# Gründe für RFID

- „einfach“
- „bequem“
- kontaktlos → Karte muss nicht in ein Lesegerät gesteckt werden
- keine mechanischen Teile (Kontaktfedern)
- bulk reading – mehrere Tags können in einem Durchgang gelesen werden
- Kontaktchipkarten sind „out“

# Funktionsweise

1. Antennenspule im Lesegerät erzeugt elektrisches Feld, induktive Kopplung
2. Tag wird mit Strom versorgt und 'wacht auf'
3. Das Lesegerät sendet auf eine Trägerfrequenz modulierte Bits
4. Der Chip antwortet, in dem der „Stromverbrauch“ aus dem elektrischen Feld gesteuert wird.
   → Lastmodulation

# Aufbau

| BLOCK DATA | LOCK BITS (0 = unlocked, 1 = irreversibly locked) | | Settings/Comments |
|---|---|---|---|
| | FACTORY LOCKED | USER LOCKED | |
| SID ADDRESS 32 bit | 1 | | Unique factory-programmed number |
| R/O Memory 32bit (Version Info) | | | Mask programmed. Contains info on manufacturer code, chip/tag version and memory architecture. Accessed via Get_Version or SID_Poll Commands. |
| BLOCK 0 32bit | 0 | 0 | Read/Write application data |
| BLOCK 1 32bit | 0 | 0 | Read/Write application data |
| BLOCK 2 32bit | 0 | 0 | Read/Write application data |
| BLOCK 3 32bit | 0 | 0 | Read/Write application data |
| BLOCK 4 32bit | 0 | 0 | Read/Write application data |
| BLOCK 5 32bit | 0 | 0 | Read/Write application data |
| BLOCK 6 32bit | 0 | 0 | Read/Write application data |
| BLOCK 7 32bit | 0 | 0 | Read/Write application data |

Speicherorganisation TagIt

# Praktische Probleme

- Reichweite Chip->Leser stark eingeschränkt
- Metall, Wasser und hohe Materialdichte verkürzen die Reichweite (bis auf null)
- Kollisionsbehandlung schwer umzusetzen
- unterschiedliche Standards und Datenorganisation
- hoher Preis von Lesegeräten (insbesondere Longrange) und Chips

# Standards

- Low Frequency (125/134 kHZ)
  Philips Hitag1/2, EM40xx, Tiris, ISO-“Animal“
- High Frequency (13,56 MHz)
  Mifare, Legic, ISO 15693, ISO 14443a/b
- Ultra High Frequency (900 MHz und größer)
  EPC, aktive Longrange Systeme
- Aktive Tags auf ISM-Bändern mit eigener Batterie

# Chip-Typen

- analoge Transponder – kein Chip! (Elektronische Artikelsicherung)
- Nur-lese-Transponder mit UID
- ISO15693 beschreibbar
- ISO14443 als Standard für CPU-Karten (Publickey, proprietäre Anwendungen)
- Mifare, Hitag - „Multiapplikation“ durch getrennt geschützte Speicherbereiche

# Privacy Probleme

- Auslesen/Beschreiben ohne Einwilligung des Inhabers
- unter Idealbedingungen abhörbar über mehrere Meter (30m laut BSI)
- Tracking durch Unique ID der Chips möglich
- Durch Zusammenfügen von gelesenen Tags umfangreiches Kauf-/Persönlichkeitsprofil

# Abhören

- Studie des BSI spricht von bis zu 30 Meter
- unter realen Bedingungen deutlich weniger
- Daten vom Leser zur Karte sind ein „aktives“ Signal
- Karte zum Leser: „passive“ Daten, nur mit hohem Aufwand über Reichweite lesbar

*Versuchsaufbau BSI-Studie*

# Unsicherheiten

- Sicherheit des Systems oft nur durch UID, also eindeutige Seriennummer des Chip
  → als Verweis auf zentrale Datenbank
- Speicherbereiche (z.B. Mifare) durch 6 Byte symmetrischen Key geschützt, im Lesegerät abgelegt
- meist proprietäre, leistungsschwache Cryptoalgorithmen (z.B. Tiris → Wegfahrsperre)
- kein Platz für Pufferkondensatoren

# Gegenmaßnahmen

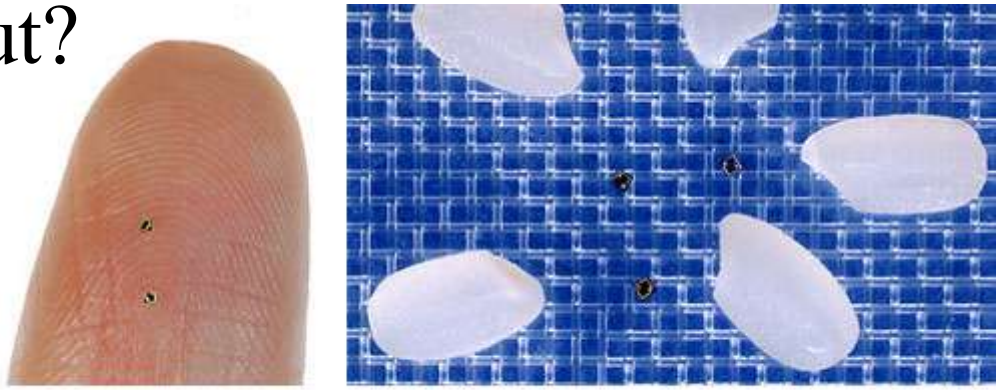
- leistungsfähige Cryptohardware auf dem Chip (teuer)
- öffentlich dokumentiertes Publickey-Verfahren (ICAO → Reisepässe) Lob: BSI, ICAO!
- Verzicht auf Funkübertragung, Rückkehr zur Kontaktchipkarte
- Einwilligung des Nutzers holen (PIN, optisches Einlesen) – Nachteil: Vertrauen erforderlich
- UID zufällig vergeben (→ Pässe)

# Spaß am Gerät

- Einfache „Tagfinder“ von c't und Elektor
- relativ preiswerte Lese-/Schreibgeräte mit serieller/USB, 50-150 Euro
  für ISO 15693/14443/Mifare
  oder Hitag, Tiris, EM40xx
- 'Blue Reader Tool' – Reisepässe auslesen
- Spaßbremsen:
  - meist nicht der richtige Leser parat
  - sicherheitskritische Bereiche oft Legic
  - oft nur die Karten-UID verwendet

# Fragen & Diskussion

- ist RFID eine Gefahr für die Privatsphäre?
- wie sicher sind die WM-Tickets?
- was wird aus den Reisepässen?
- Chips unter die Haut?



A New RFID with Embedded Antenna μ-Chip

Frank Rosengart <*frank@rosengart.de*>