

# Ubiquitous Computing

(Ubiquitäre Informationstechnologien)

Vorlesung im WS 09/10

---



**Christian Decker**

Universität Karlsruhe

Institut für Telematik

Telecooperation Office

[www.teco.uni-karlsruhe.de](http://www.teco.uni-karlsruhe.de)

# RFID Technologie

## RFID: Radio Frequency Identification

- Erfunden 1948, Integrierte Schaltung mit RF-Transponder
- Benötigt immer Lesegerät zum Auslesen des Transponder, Transponder initiiert/steuert Kommunikation
- kleiner mobiler Speicher für ID und evtl. weitere Daten
  - Zugriff: Read, Read/Append, Read/Write
  - 1 bit bis 64 kbyte
  - selten Authentifizierung, OS
- berührungsloses Auslesen
  - Reichweite typisch ~0.5mm, bis 10m
  - ggf. Anti-Kollisionsprotokolle
- (oft) keine Batterie an Bord!
  - Energieversorgung beim Auslesen
  - induktiv, kapazitiv
- klein, unauffällig, Preis <1 US\$ (ab 1000), verschiedenste Form-Faktoren
- Hauptproblem: Preis >5 Cent incl. Antenne (<1 Cent ohne Antenne)



Quelle: ti.com

# RFID - Geschichtlicher Überblick

---

## Erfunden 1948 (!)

- Militärische Anwendung (Freund / Feind Kennung)
- Harry Stockman. „Communication by Means of Reflected Power“ (Proceedings of the IRE, pp 1196–1204, October 1948)

## 1960er

- EAS: Diebstahlsicherung (1-bit Transponder)

## 1970er

- 1973: Mario Cardullo „Transponder apparatus and system“ U.S. Patent 3,713,148
- Tierkennzeichnung (Passive Transponder)

## 1980er

- RFID basierte Mautsysteme, Bezahlungssysteme (USA, Skandinavien)

## 1990er

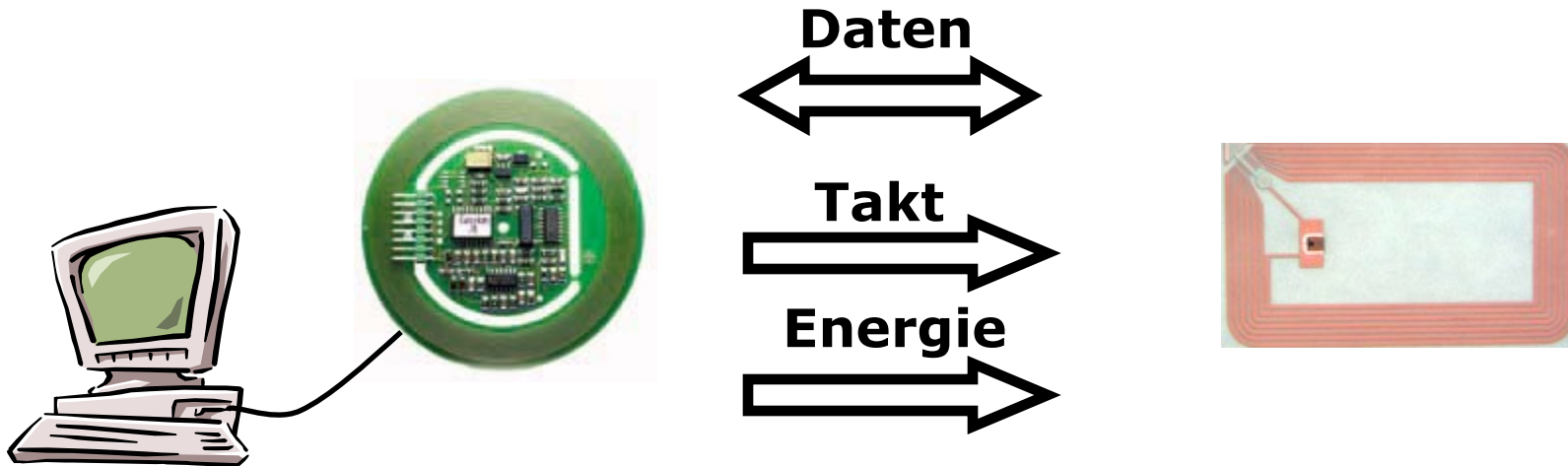
- Zugangssysteme, Wegfahrsperrern, Skipässe, Tankkarten
- Einsatz in Logistiksystemen, Standards z.B. EPC

## Heute

- Smart-Label, Sensor-RFID, Polymertransponder
- Integration in ERP Systeme durch RFID-Middleware, z.B. Auto-ID Infrastructure, „Internet of Things“

# Passives RFID System

---



## RFID-Reader

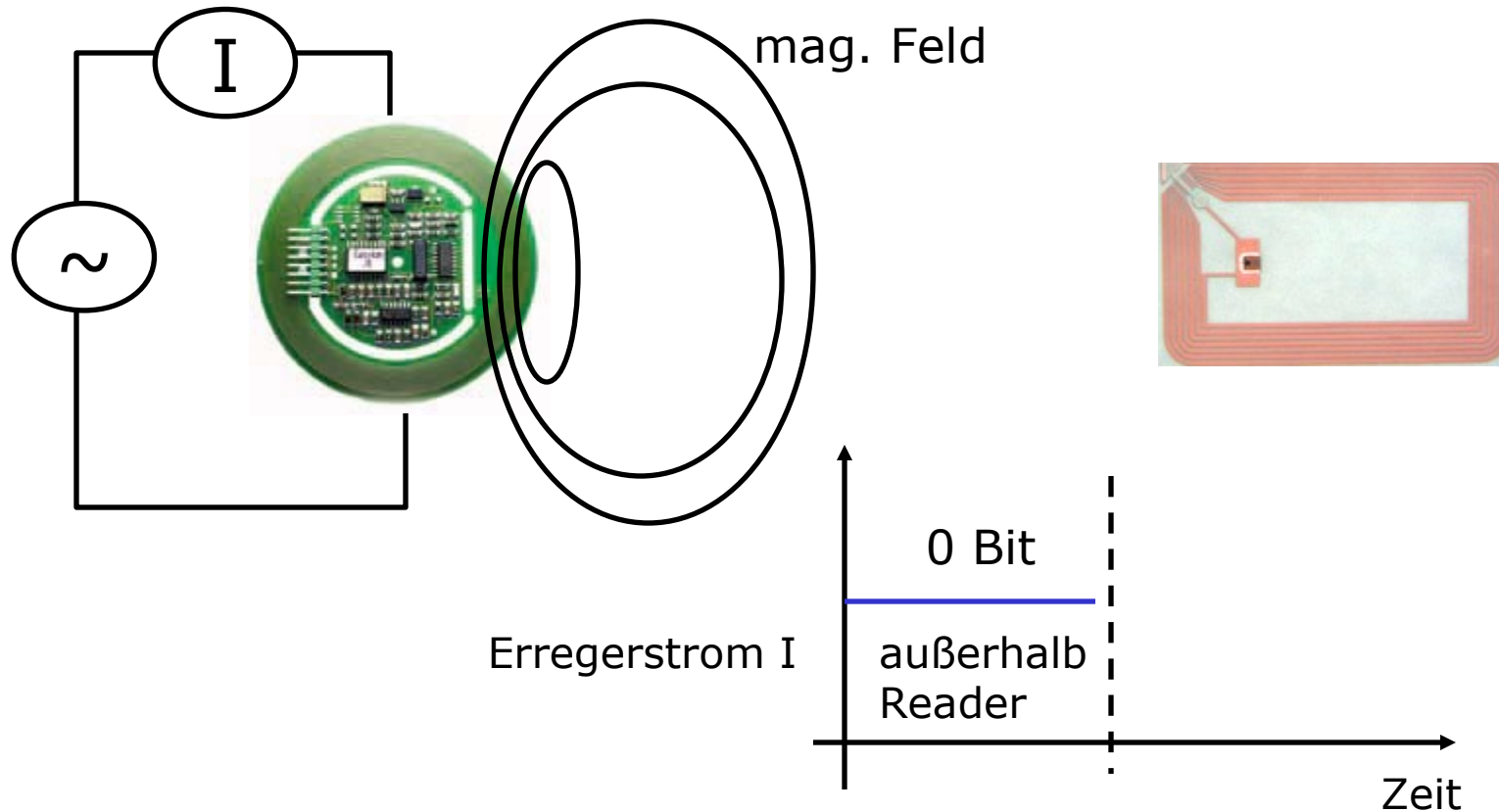
- Direkt oder über Middleware mit Applikation (PC) verbunden
- Multiple RFID-Standards + Frequenzen, Antikollision
- Standardschnittstelle zu Computersystemen (z.B. RS232)

## Transponder

- Keine eigene Energieversorgung (passiv)
- Chip, Datenspeicher (ID, weitere Daten)
- Optional: Sensorik, Verschlüsselung

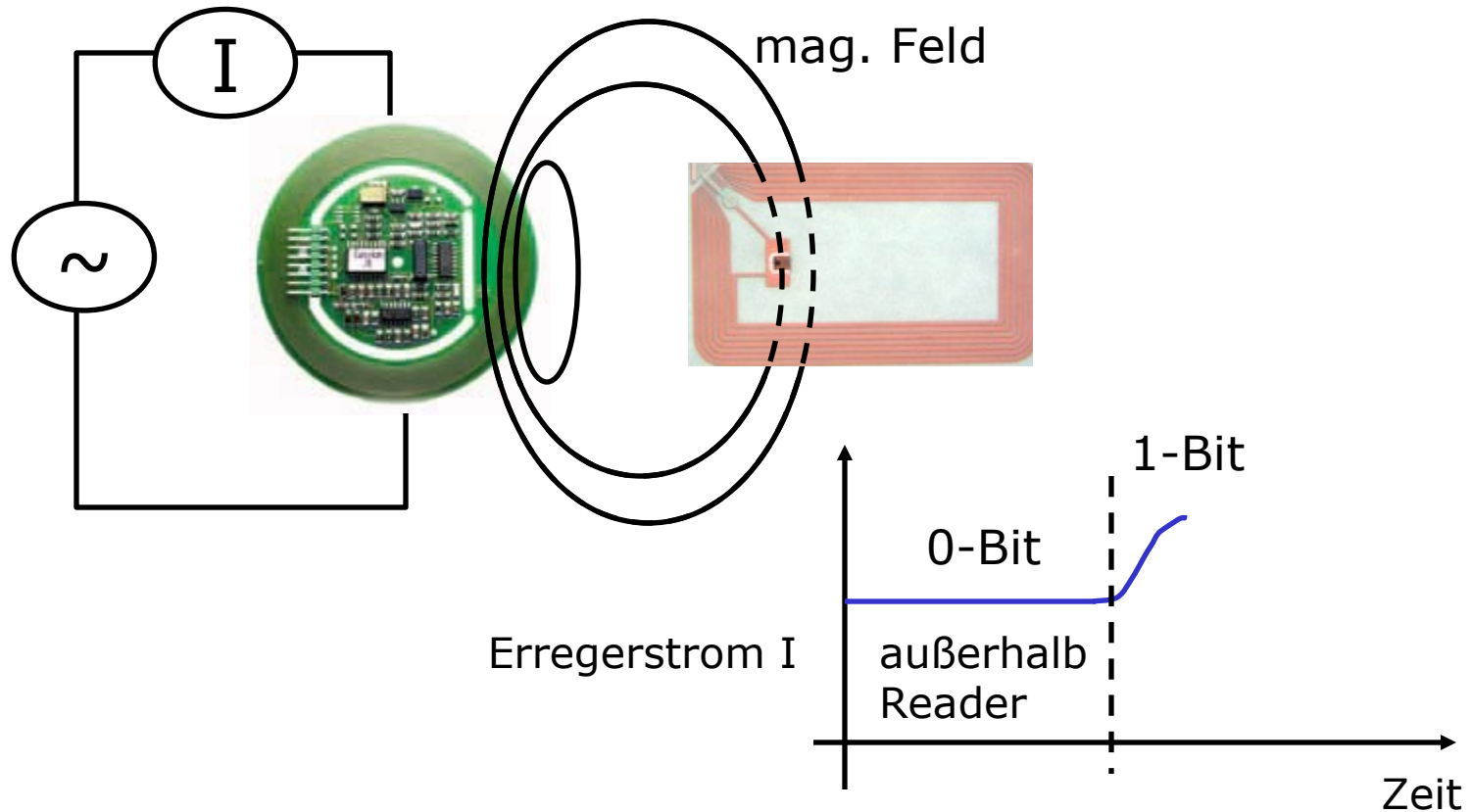
# Generelle Funktionsweise

- Induktive Kopplung von Schwingkreisen
- Daten = Modulation des Erregerstromes (Lastmodulation)



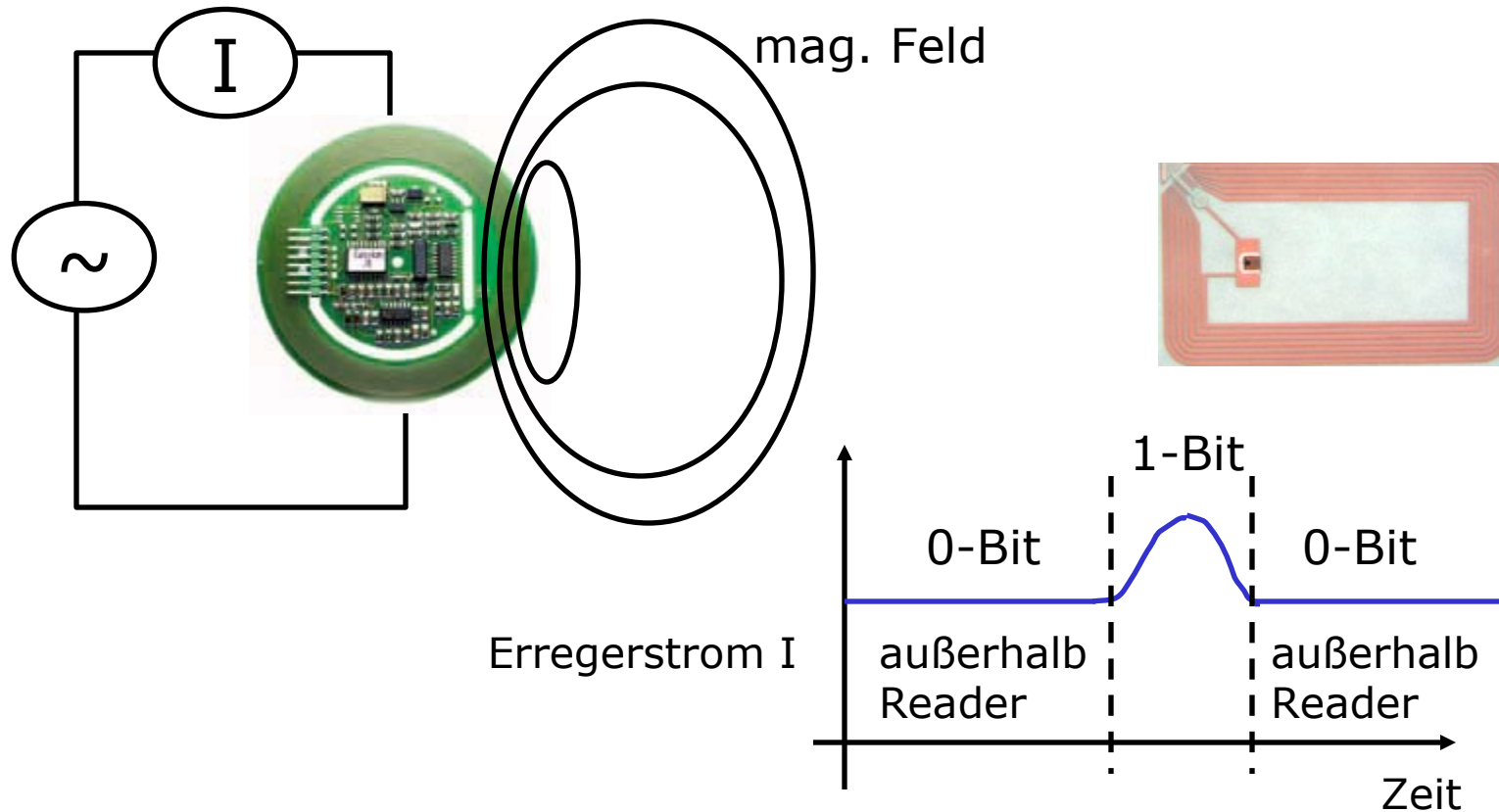
# Generelle Funktionsweise

- Induktive Kopplung von Schwingkreisen
- Daten = Modulation des Erregerstromes (Lastmodulation)



# Generelle Funktionsweise

- Induktive Kopplung von Schwingkreisen
- Daten = Modulation des Erregerstromes (Lastmodulation)



# Beispiele

- Reichweite:  $\sim 2\text{m}$
- Zuverlässigkeit:  $\sim 70\%$



- Reichweite: wenige cm
  - Transponder: ISO-Karte, Schlüsselanhänger, Uhren, Armbänder, etc.
- 
- Andere Verfahren: Mikrowellen, elektro-magnetische Kopplung, kapazitive Kopplung, Backscatter Kopplung

# Aktive und Passive Transponder

---

## Passive Transponder

- Energie zum Betreiben der internen Logik (ID, Speicher) wird aus dem Lesefeld gewonnen

## Aktive Transponder

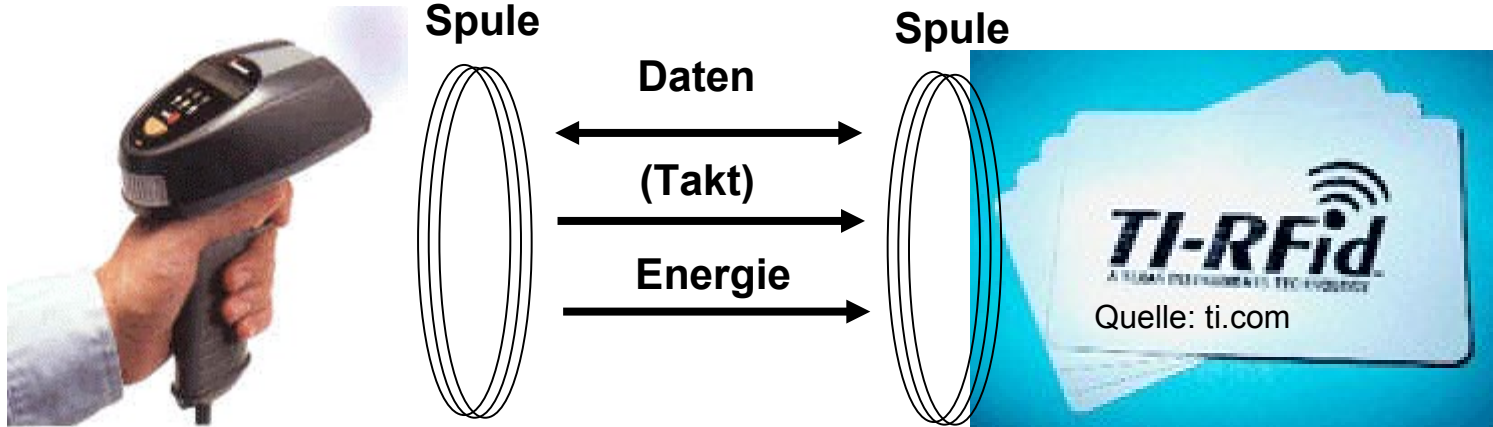
- Eigene Energieversorgung durch Batterie
- Energie des Lesefeldes aktiviert interne Logik (Wechsel zwischen Power-States), Kommunikation über Lesefeld
- Sonderfall Beacon:
  - Kein Lesefeld notwendig
  - Transponder wechselt eigenständig zwischen Power-States und sendet (Beacon) in bestimmten Zeitintervallen

# RFID Kommunikation (passiv)

## Kommunikation

- Prinzip: Lastmodulation (Kurzschluß), Harmonisch ( $n \cdot \text{Freq.}$ ), Subharmonisch (z.B.  $1/2 \text{ Freq.}$  Der Energie= Antwortfrequenz), Backscatter Kopplung
- Modulation: ASK, FSK, PSK
- Codierung: NRZ, Manchester, Differentiell, Pulse-Pause (DutyCycle)

RFID Reader (Leser)



Quelle: rfid.com

# Passive Transponder

## Eigenschaften

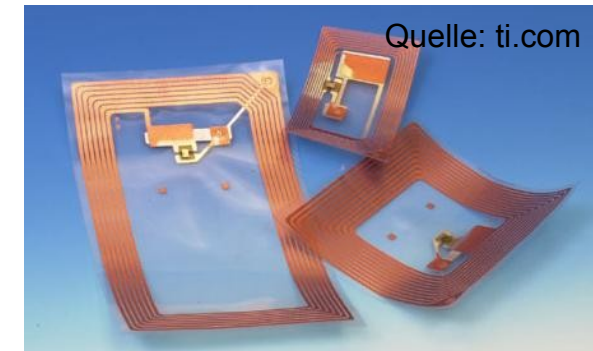
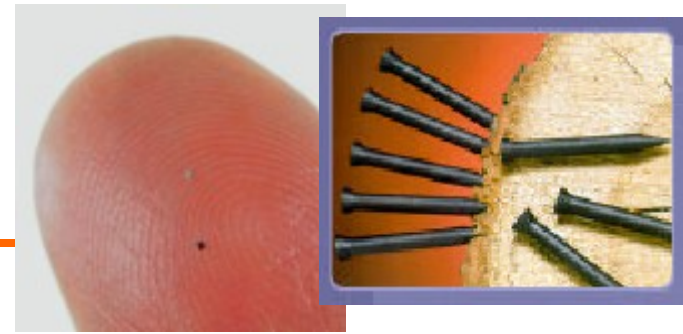
- Energie wird vom Leser durch induktive Kopplung übertragen
- Takt wird oft mitübertragen
- Dadurch sehr preiswert
- Mit und ohne Microprozessor, oft nur lesbare ID
- Sehr klein, aber Problem: Antenne

## Bauformen

- ISO Karte, Armbänder, Uhren, Discs, Glastransponder, Smart Labels (laminiert)

## Speicher

- Read-only (RO), nur ID, <128bit
  - Bei Produktion festgelegt, weltweit eindeutig
- Read-Write (RW), ID ist RO, 32 kbyte für Daten
  - Daten: z.B. Verfallsdatum



# Smart Labels

## RFID Tags als „Smart Label“

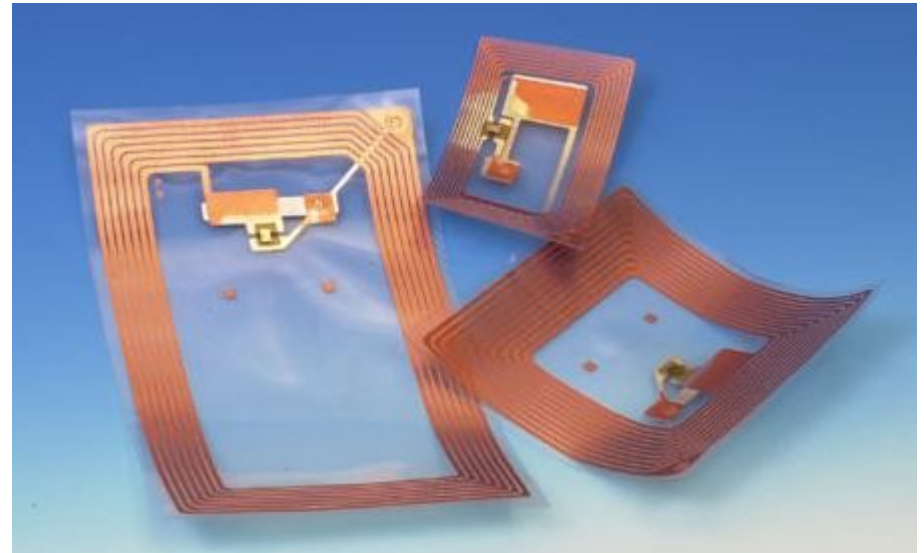
- in Papier einlaminiert
- nachträgliches Markieren von Objekten

## Chip (ohne Antenne)

- ~ 2 mm x 2 mm x 10 µm
- vgl. Papier 80 µm dick

## Antenne

- Kritisch für die Reichweite
- Teuer in der Anbringung, da separater Prozess
- aus Kupfer, oder
- aufgedruckt mit leitfähiger Tinte, (Reichweitenproblem) oder
- auf CMOS-Basis (Reichweitenproblem)



Quelle: ti.com



# Standards + Frequenzen

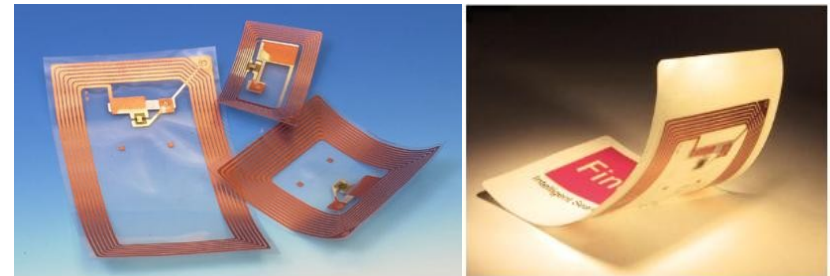
## 125KHz (LF)

- Zutrittskontrolle, meistens Read-only Transponder
- Reichweite: ~ 10cm
- Standards: EM 40xx, HITAG 1,2



## 13,56MHz (HF)

- Flexible Etiketten
- Reichweite: ~1m
- Standards: i-Code, Tag-it, MIFARE

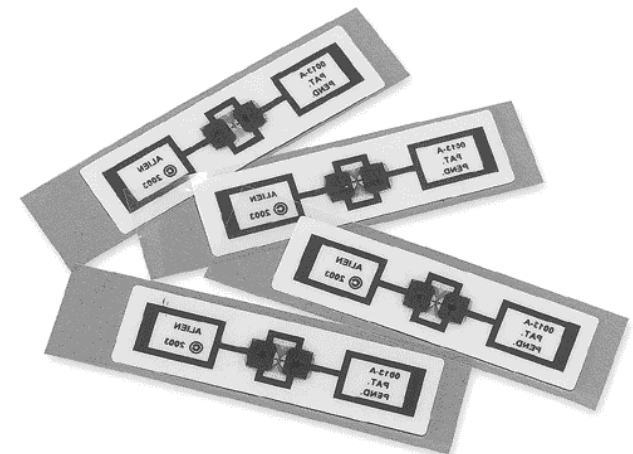


## 860-956MHz (UHF)

- Flexible Etiketten
- Reichweite: bis zu 3m
- Standards: ISO 18000-6-A/B, EPC UHF class 1, EPC UHF Gen 2

## 2,45GHz (vgl. WLAN)

- Dokumente mit Transpondern
- Long Range Systeme: mehrere Meter
- Standards: ISO 18000-4



# Aktive Transponder

## Eigenschaften

- Batterie betrieben (Laufzeit!)
- Teurerer, integrierter Microcontroller
- Hohe Reichweite (mehrere 10 Meter) im Vgl. zu passiven RFID
- Reader oder Beacon/Barke Betrieb
- Technisch Systemen in ad-hoc Netzwerken ähnlich, aber
  - (meist) ohne Sensorik
  - Nie P2P Kommunikation, sondern immer zum Reader

## Anwendungsbereiche (Weitbereich-ID)

- Palettenidentifikation, Containeridentifikation
- Mautsysteme
- Tracking -> z.B. WhereNet



# Aktive Transponder – Tracking

## Lokationstechnologie

- Active RFID, 2.4 GHz, bis 100 m TDOA Verfahren
- Genauigkeit: 3-5m
- WhereLAN (WLAN + Reader)

## Infrastruktur

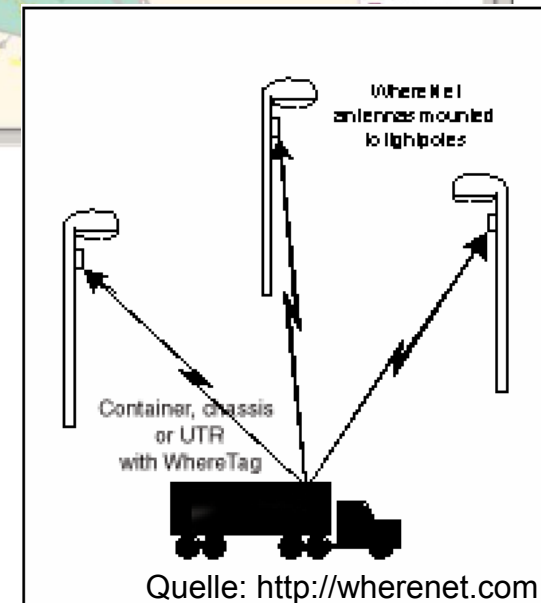
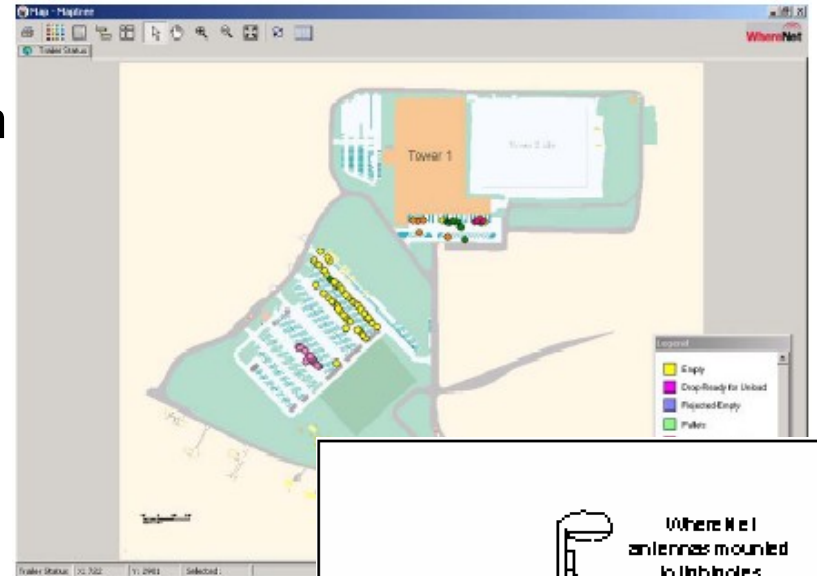
- Wireless LAN (WhereLAN)
- Transponder Reconfiguration für mehr Messdaten (WherePort)

## Laufzeit

- 7 Jahre (Transponder)

## Back-end Software

- WhereSoft (Real-time location system)



# Sensor-RFID

## Eigenschaften

- Active-RFID + Sensoren
- Sensoren
  - Temperatur, Druck, Bewegung (MEMS)
- Speicherfähigkeiten
  - bei Abwesenheit des Readers
  - 2 kBit SRAM, Speicherbare Temperaturwerte: max. 64 (KSW TempSens)
- Konfigurierbar:
  - Beispiel TempSens: Alle Zeit-/Temperaturwerte, Zeit-/Temperaturwerte außerhalb des Limits, Temperaturmaximal-/minimalwerte

## Anwendungsbereiche

- Qualitätssicherung für temperaturempfindliche Produkte
- Pharmazeutische Logistik, z.B. Temperaturüberwachung medizinischer Produkte und Blutkonserven, Feinchemikalien
- Elektronische Siegel (eSeals)



Quelle: <http://ksw-microtec.de/>

# Elektronische Siegel (eSeals)

## eSeals

- Active RFID zur Überwachung von Gütern (Container) gegen Eindringen, Aufbrechen, Beschädigungen

## Lokationstechnologie

- Active RFIDs transponder, 50m Reichweite
- GPS in DataReader, z.B. HiTeK

## eSeal Sensoren

- Bewegung, Unterbrechung, optional weitere
- Eindring-Sensorik gegen eSeal-Attacken (tamper resistan)

## Laufzeit / Energieversorgung

- Transponder: 3 Jahre @ 50 Abfragen pro Tag
- Reader: 5W, 12V/24V

## eSeal Eigenschaften

- Angebracht an Ventilen, Türen, Schlössern
- Benachrichtigung und Aufzeichnung von Angriffen auf zu schützende Güter
- GPS + GPRS (Reader) zum Tracking des eSeal



Tags, eSeals



Readers

Quelle: <http://www.higtek.com>

# RFID Programmierung und Lesegeräte

---

## Programmierung Transponder

- ID wird normalerweise bei der Fertigung eingebrannt und kann nicht verändert werden. Dies sichert universelle Einmaligkeit der ID innerhalb eines Systems zu
- Write-once-read-many Transponder erlauben z.T. das kundenspezifische Einbringen von ID oder Teilen der ID
- Manche Systeme erlauben das Verändern von Teilen der Daten mit Hilfe spezieller Soft-/Hardware und kryptographischer Sicherung

## Lesegeräte

- Verschiedene Ausführungen, je nach Reichweite
- Als stationäre Geräte, als Handgeräte oder als Steckkarte (CF-Karte, Zusatz für Mobiltelefon etc.)
- Benötigt z.T. erheblich Energie
- Stationäre Geräte besitzen oft mehrere Antennen oder Leseinheiten für parallele Verarbeitung und zur Fehlerkorrektur

# RFID Daten

---

- Nur lesbar oder lesbar und beschreibbar

## Gespeicherte Informationen

- Identifikatoren: Eine ID, welche auf weitere Daten verweisen kann, die ausführlichere Informationen enthalten, meist im ROM
- Zusätzliche Daten: Informationen, die direkt für sich selbst stehen und auch verändert werden können. Ein Rückgriff auf eine Datenbank ist dann nicht notwendig. Daten meist im RAM

## Kapazität

- Ein Bit: Diebstahlüberwachung, Zähl Anwendungen
- < 128 bits
  - ID bzw. Seriennummer
- 128- 512 bits
  - Meist Beschreibbar,
  - Enthält meist ID und weitere Informationen (z.B. Verfallsdatum, Handhabungsanweisungen)
- Mehrere Kilobit
  - Kann eigene Programme beinhalten, die dann auf Leser ausgeführt werden

# RFID Reichweiten (passiv)

---

## Reichweite bestimmt durch

- Abgegebene Leistung des Lesers an der Antenne (beschränkt)
- Stromverbrauch des Tags
- Antennen-Design, insbesondere des Tags; dies bestimmt auch die Ausbreitungscharakteristik der Welle und damit den Abdeckungsbereich
- Umgebungsbedingungen, insbesondere Belegung des Frequenzbands, Störungen auf dem Kanal, Material (insb. Metall und/oder Wasser, je nach Frequenz), Luftfeuchtigkeit

## Frequenzbänder

- Niedrig (100-500kHz): geringe Reichweite, preiswert, langsam
- Medium (10-15MHz): mittlere Reichweite, mittlere Geschwindigkeit, preiswert
- Hoch (850-950MHz, 2.4-5.8GHz): hohe Reichweite, schnell, teuer

# RFID Technik Charakteristik

	RFID technology (by carrier frequency)			
	Low frequency	High frequency	Ultra high frequency	Microwave
<b>Data Capacity (tag type)</b>	Typically, 64 bits to 2kbits. (Passive or active)	Typically 512bits to 8kbits. (Passive or active)	Typically 32bits to 4kbits. (Passive or active)	Typically 128bits to 32kbits. (Passive or active)
<b>RW /RO</b>	Both available	Both available	Both available	Both available
<b>Transfer rate</b>	Typically 200bits/s to 1kbit/s	Typically 25kbits/s to 100kbit/s	Typically 28kbits/s	Typically 100kbits/s to 1Mbit/s
<b>Read (and write) time</b>	Typically 0.5s <sup>2</sup>	Typically 2ms <sup>3</sup>	Typically 2ms <sup>4</sup>	Typically 0.05s <sup>2</sup>
<b>Range</b>	Near contact, or up to 0.5m, for an active tag	1.2m for RW , 1.5m for RO passive tags	1.2m for RW , 1.5m for RO passive tags	1 to 2m for passive tags, active tags > 10m
<b>Accuracy and repeatability</b>	Single tag and multi tag anti-collision systems	Single tag and multi tag anti-collision systems. Better noise immunity than low frequency systems	Single tag and multi tag anti-collision systems.	Single tag and multi tag anti-collision systems.
<b>Tag shape and robustness</b>	Wide variety available, but susceptible to low frequency interference	Wide variety available, including smart cards and smart labels. Rigid and flexible substrates available	Wide variety available	Wide variety available, including smart cards and smart labels. Rigid and flexible substrates available

# RFID Übertragungsverfahren

**Verfahren:** (down: von Leser zu Tag, up: von Tag zu Leser)

## Full Duplex (FDX)



## Half Duplex (HDX)



## Sequentiell (SEQ)



# Störeinflüsse

## Transponder/Tags

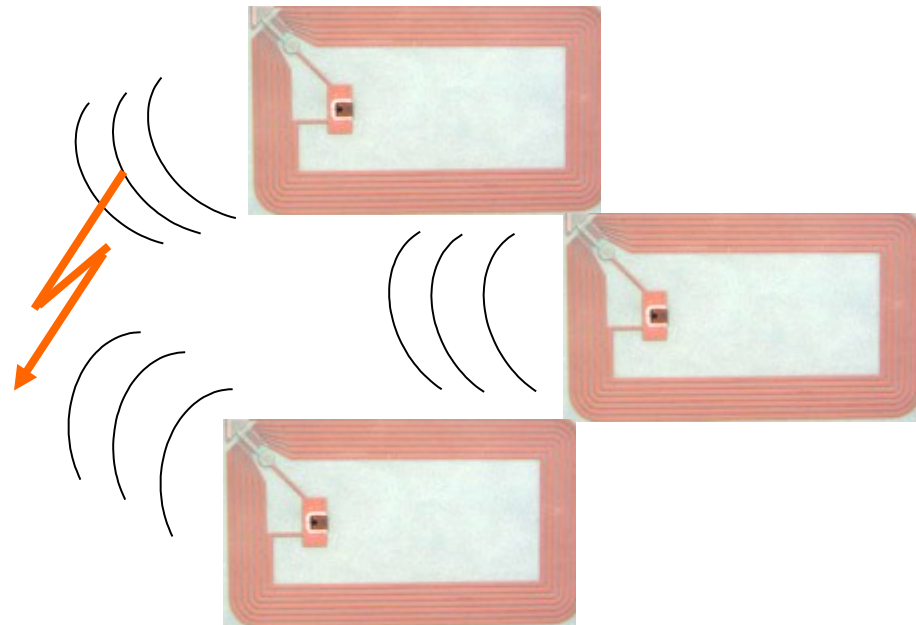
- Mehrere Transponder im Lesefeld
- Kollision beim Rücksenden der ID zum Lesegerät

## Maßnahmen

- Antikollisionsverfahren



Quelle: rfid.com



# Störeinflüsse

---

## Lage / Orientierung im Raum

- Lage der Antennen von Transponder + Lesegerät beeinflusst die Energieeinkopplung

## Maßnahmen

- Mehrere Transponder (benötigt Antikollision)

# Störeinflüsse

## Abschirmung

- Umgebung und Materialien dämpfen das Lesefeld
- Energieeinkopplung gering, Transponder antwortet nicht

## Maßnahmen

- Ortswechsel bei Umgebungseinfluss
- Anbringung an anderen Materialien
- Mehr Leistung (Regulierung)
- Mehrere Lesegeräte
- Mehrere Transponder

Verpackung	Leserate
Pappkarton	58%
Beschichtetes Papier	67%
Textilien (ohne Verpackung)	44%
Kunststoffolie	50%
TetraPak	0%
Dose	0%
Glasflasche	0%

Messung von Produkten im Regal  
(Projekt Locostix, R.Kestel)

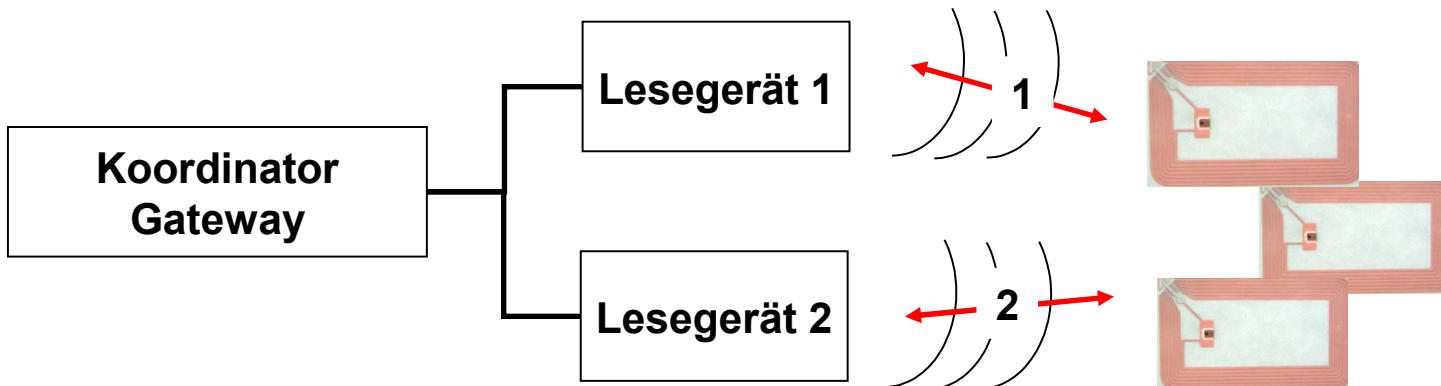
# Störeinflüsse

## Multiple Lesegeräte

- Mehrere Lesegeräte erzeugen gleichzeitig ein Lesefeld
- Überlagerung, Lesebefehle an Transponder werden zerstört

## Maßnahmen

- Konfiguration und Koordination der Lesegeräte
- Koordinator Gateway, spezifische HW Lösung zum Betrieb von Lesegeräten



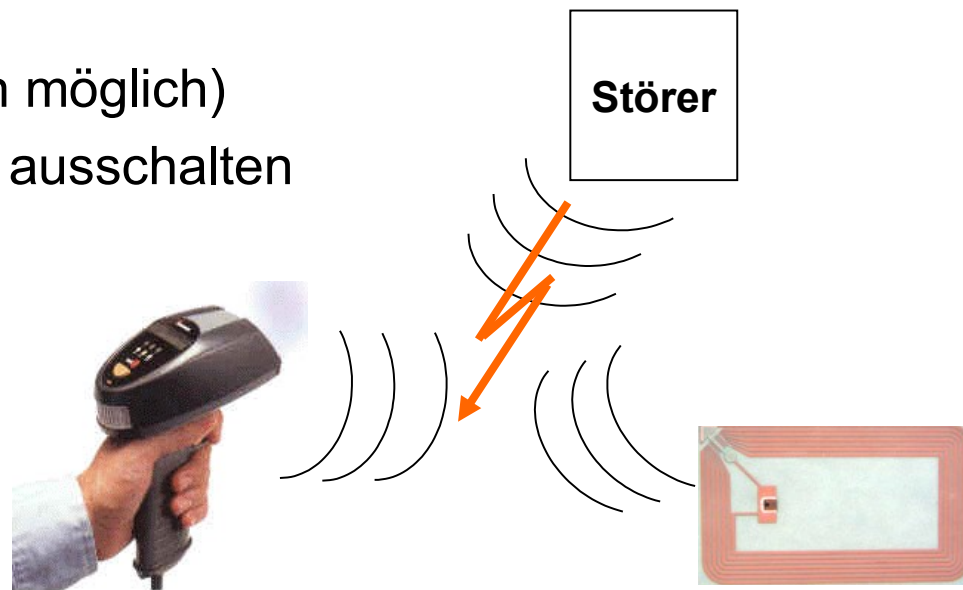
# Störeinflüsse

## Schmalbandfunkstörer

- Frequenz des Lesefeldes wird gestört

## Maßnahmen

- Ortswechsel
- Frequenzwechsel (wenn möglich)
- Störer identifizieren und ausschalten



Quelle: rfid.com

# RFID

## Antikollision

---

### Kollisionsauflösung

- Tag zu Leser, kein Tag zu Tag
- Mehrere Tags im Feld eines Readers möglich -> Antikollision notwendig
- Für Systeme im  $>13$  MHz Band, ansonsten keine Antikollision!
- Meist TDMA
  - Zeitkritisch, schlecht bei vielen Tags
  - (Slotted) ALOHA: Schlechter Durchsatz bei mehreren Transpondern, bei vielen Tags Lesezeit für 99% Leseerfolg aller Transponder im Sekundenbereich
  - Besser für viele Tags: Binary Search Tree Algorithmus
- Besser: FTDMA:
  - Mehrere Frequenzen, dort TDMA
  - Dadurch Vervielfachung des Kanals und schnelleres Lesen
  - Erfordert teure Mehrfrequenz-Leser

# RFID

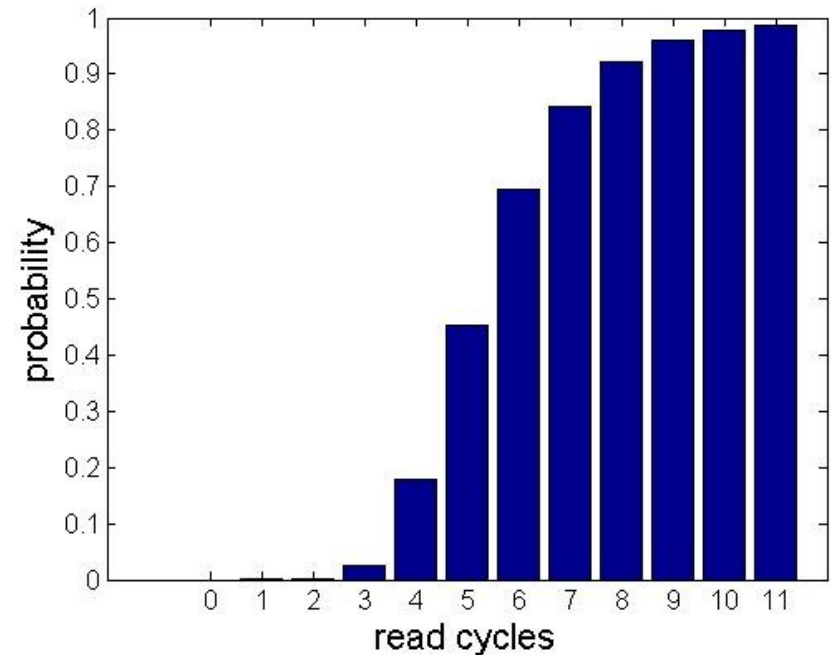
## Antikollision

### Slotted Aloha

- Reader sendet REQ
- Tags wählen einen zufälligen Antwort-Slot
- Reader sammelt Antworten ein
- Beginn des nächsten Zyklus (nächstes REQ)

### Problem

- Nicht deterministisches Verfahren
- Wurden alle Tags gelesen?



Wahrscheinlichkeit alle Tags gelesen zu haben  
in Abhg. von Lese-Zyklus (insg. 40 Tags)

# RFID

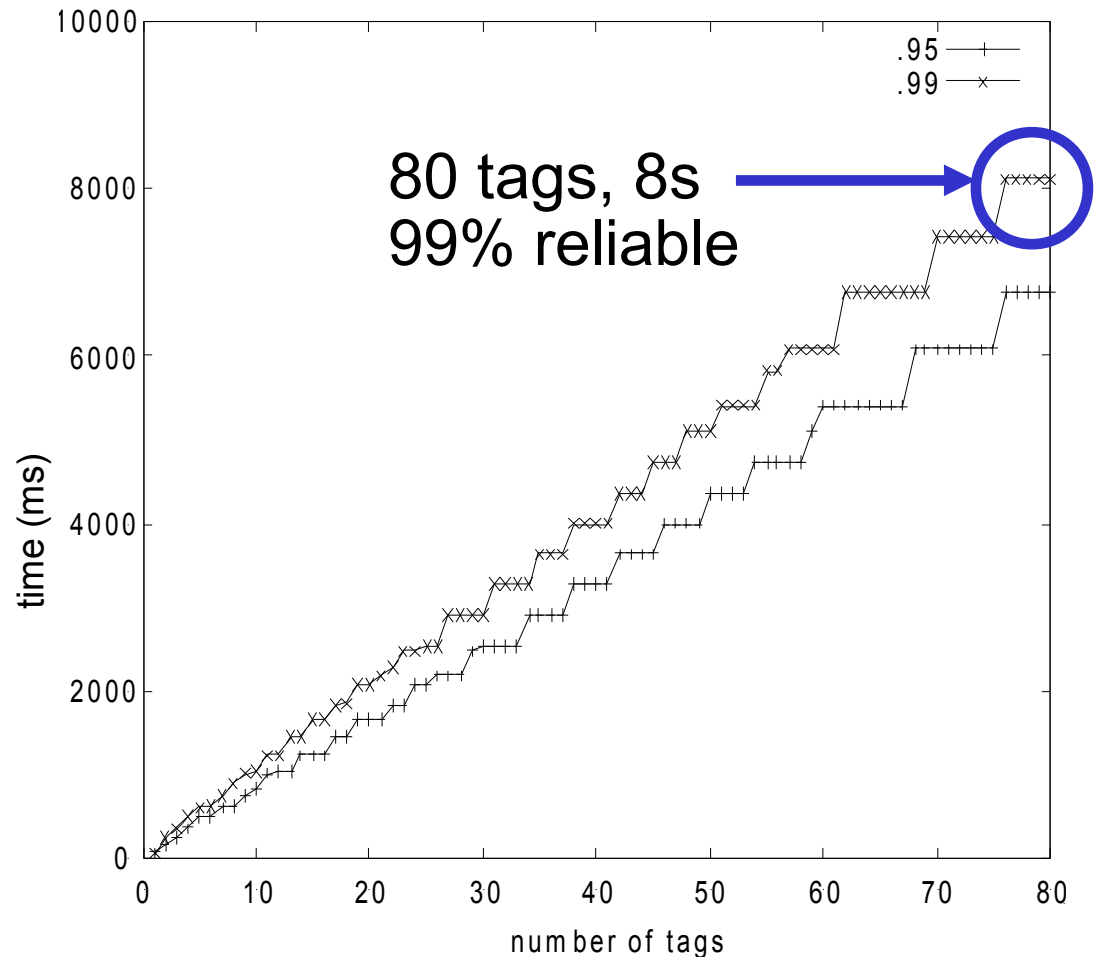
## Antikollision

### Performance

- Lange Lesedauer für viele Tags

### RFID Protokoll

- EPC Gen2



Source: Vogt, H. (2002). Efficient Object Identification with Passive RFID Tags.

# RFID

## Antikollision

### Binary Search Tree Algorithmus

- Voraussetzung: Erkennung von Kollisionen auf Bitebene. Nicht alle Codes können eingesetzt werden
- Verwendete Codes: Manchester-Codierung, NRZ
- Verfahren: Aufforderung/Auswahl/Lesen
- Iteration für das Auslesen der anderen Tags

Downlink Leser zu Transponder	REQUEST 11111111	REQUEST 10111111	REQUEST 10111011	SELECT 10111011	READ
Uplink	1xx1xx11	10111x11	10111011	10111011	
Transponder 1	11011111				
Transponder 2	10111011		10111011	10111011	10111011
Transponder 3	10111111		10111111		
Transponder 4	11110011				

# RFID

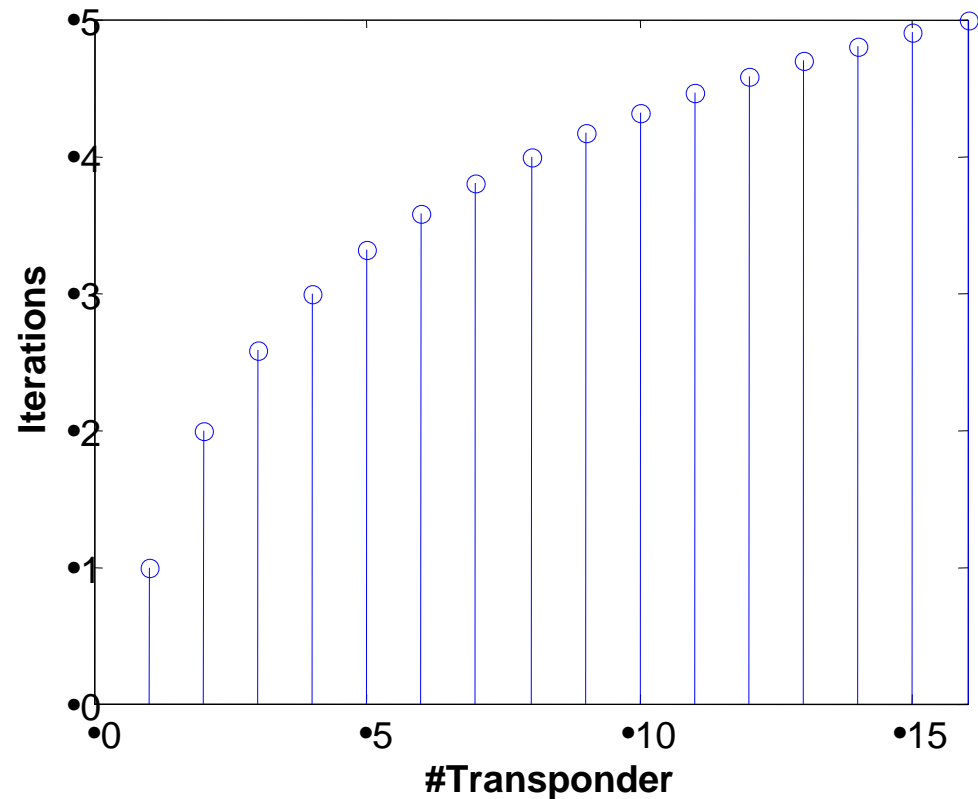
## Antikollision

### Performance

- $L(N) = \text{ld}(N) + 1$ 
  - $L(N)$ : Anzahl Iterationen
  - $N$ : Anzahl Tags

### Beispiele

- 32 Tags: 6 Iterationen
- 64 Tags: 7 Iterationen
- 128 Tags: 8 Iterationen

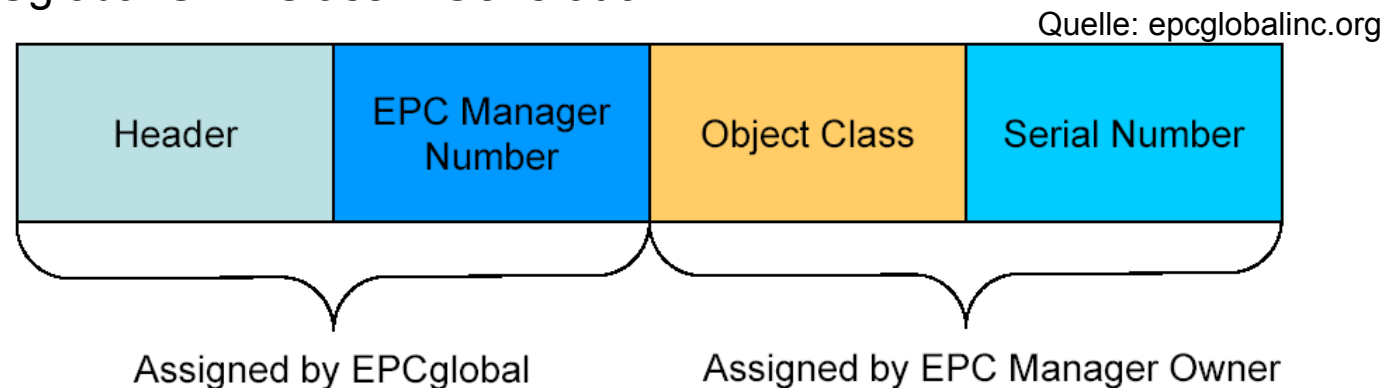


# EPC Standard

- EPC = electronic product code
- Standardisierung: MIT / autoid-center.org → EPCGlobal Inc.
- EPC Gen2: EPCglobal UHF Class 1 Generation 2

## Format:

- 64 oder 96 bit



- Header: Länge, Typ, Struktur, Version, Generation
- EPC Manager Number: Hersteller, verantw. für Vergabe der Obj. und serial numbers
- Object Class: Typ des Objekt, z.B, Deutsche Mineralwasserflasche, 750 ml
- Serial Number: identifiziert Artikel

# EPC

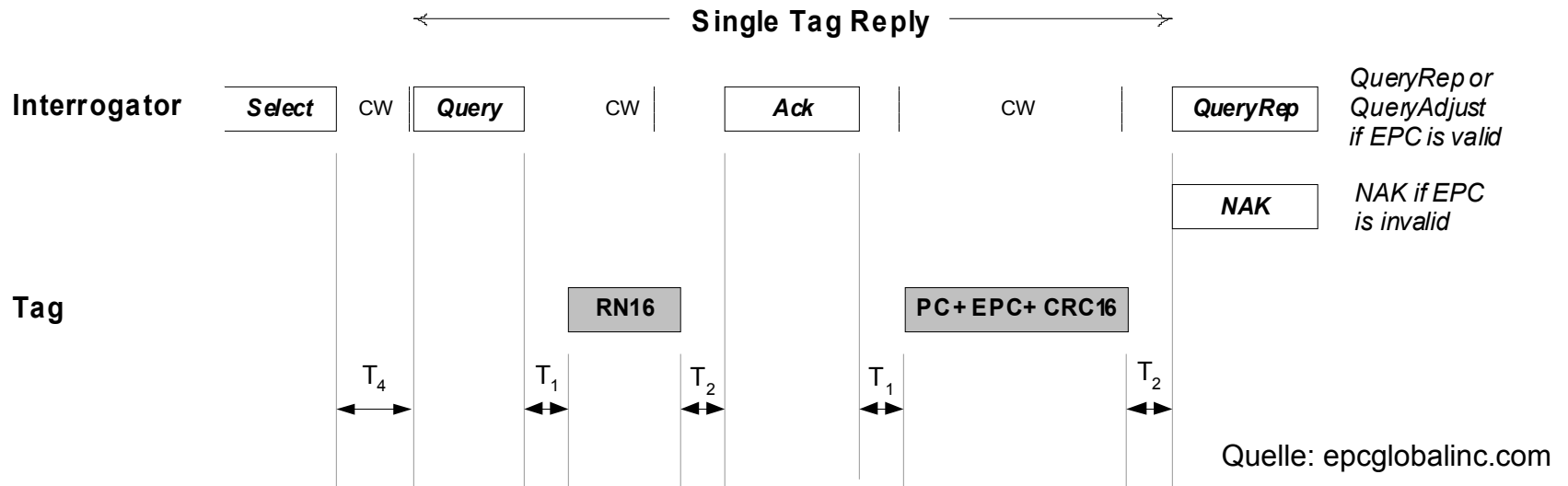
## Beispiel

Quelle: epcglobalinc.org

Partition	Value	Binary Number
Header	48	0011 0000
Filter Value	3	011
Partition	5	101
Company Prefix	0614141	000010010101111011111101
Item Reference	000734	00000000001011011110
Serial Number	203886	00000000000000000000110001110001101110

- Filter: erlaubt ausmaskieren beim Lesen, kein Teil der ID!
- Partition: erlaubt versch. Company.Pref. → Länge: 20-40 bit
- Item Ref.: Object class, 4 – 24 bit, durch Partition bestimmt
- Serial Number: Artikel ID, 38 bit

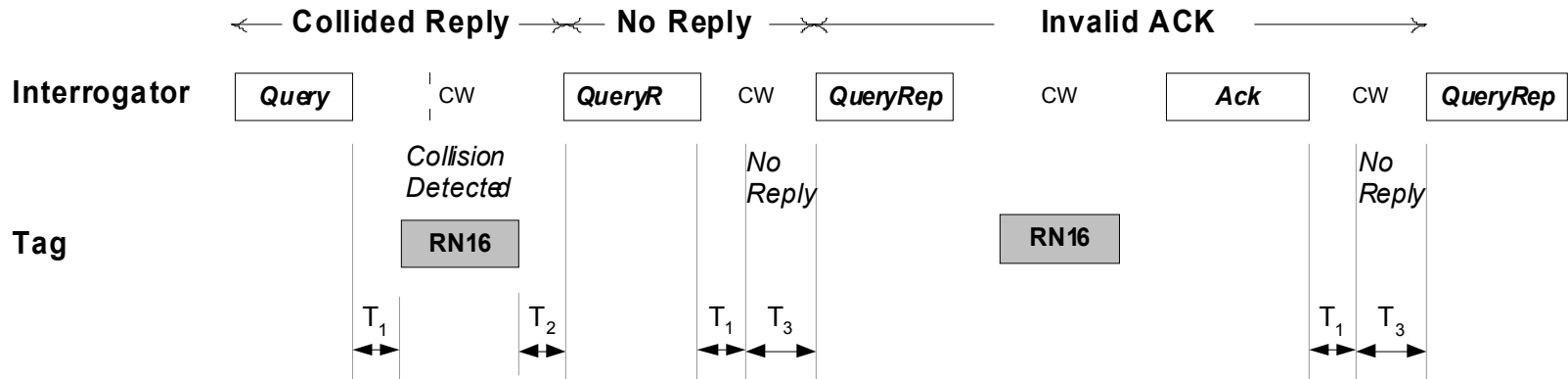
# EPC Protokoll



- **Select:** EPC masking, Tag Bestand gemäß Benutzerkriterium einschränken (analog zu SQL select)
- **Query:** Read Session, Tag sendet 16bit Zufallszahl (slotted Aloha)
- **Ack:** Zufallszahl valid (keine Kollision), jetzt Tag EPC schicken
- **QueryRep.:** EPC valid, Wiederholung Query
- **NAK,** wenn EPC invalid

# EPC

## Protokoll bei Kollision



Quelle: epcglobalinc.com

- **Query:** Reader beginnt Verfahren, Kollisionen bei Antwort (Zufallszahl) des Tags festgestellt
- **QueryRep:** wiederholt Query mehrmals, Zufallszahl wird gesendet (slotted Aloha)
- **Ack:** Zufallszahl ohne Kollision empfangen

### Aber:

- Tag hat Ack nicht empfangen → QueryRep

# RFID Anwendung

## Anwendungen

- Electronic Article Surveillance (EAS - Diebstahlüberwachung) = 1 bit transponder
- Inventur
  - z.B. Minibar im Hotelzimmer
- Bibliotheken, Videotheken
- Gepäck-Label
- ...



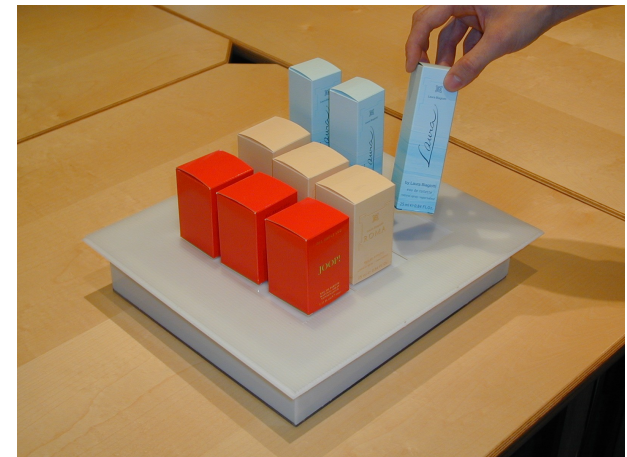
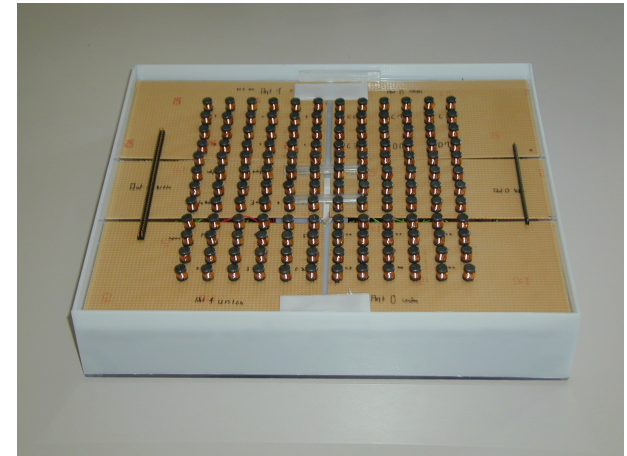
# RFID Anwendung - SmartShelf

## Prinzip & Nutzen

- Echtzeit Erkennung von Produkten & Position auf Verkaufsregal
- Nutzen: Ausverkaufte Ware erkennen, Nachfüllen von Waren, Sortieren von Waren
- hochwertige Ware (Parfüm etc.)

## Technologie

- Antennenarray & mehrere Reader
- Dadurch Position, Vermeidung von Fehllesungen
- Preiswerte Tags, teure Lesertechn.
- SmartShelf, da über eigenen Zustand informiert
- TecO 2002



# Anwendungen

## Online-Handbücher

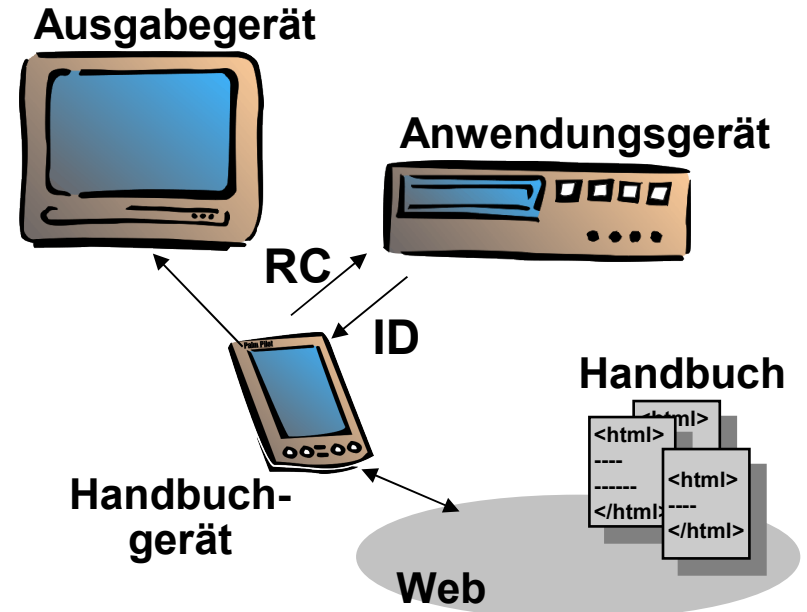
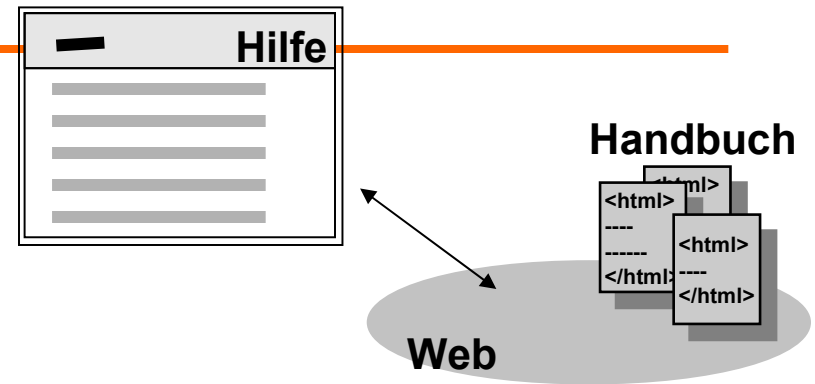
- Stand der Technik für Software-Applik.
- Abruf bei Bedarf statt Verteilung
- multimedial, aktuell, interaktiv

## Electronic Manual

- Objektidentität als Informationsfilter
- Verknüpfung von realen Geräten mit virtuellen Handbüchern

## Elektronisches Handbuch

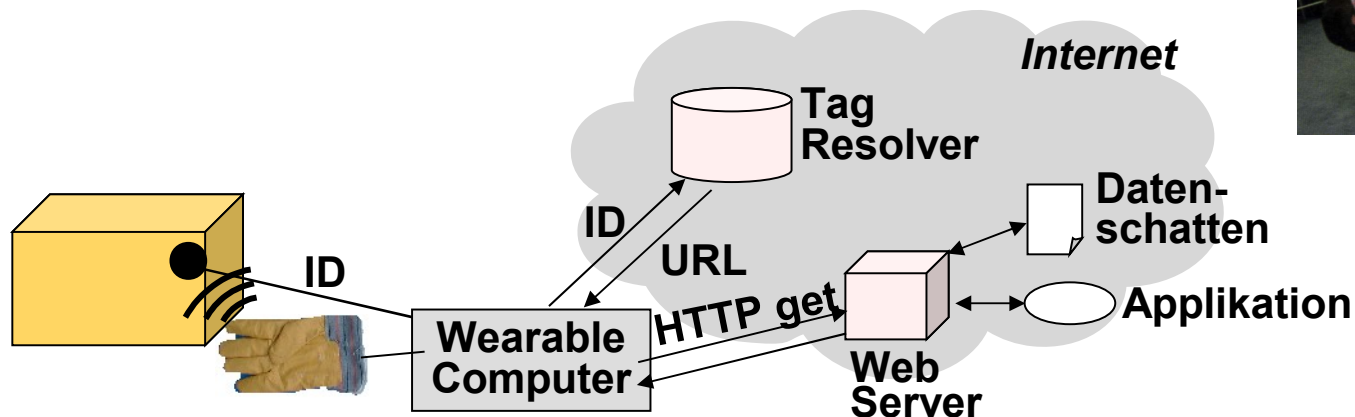
- Übertragung in den Alltag: Appliances mit Online-Handbuch verbinden
- Handbuch-Lesegerät ersetzt Papier-Handbücher



# Anwendungen

## „Wearable Tag Reader“

- A. Schmidt, TecO, 2000
- Antenne in Arbeitshandschuh, Lese-Elektronik am Gürtel, serielle Schnittstelle zum Wearable Computer
- **Tangible UI**: implizite Computer-Interaktion bei Handhabung von Gegenständen
- **Augmented Reality**: z.B. in Paket „reinschauen“



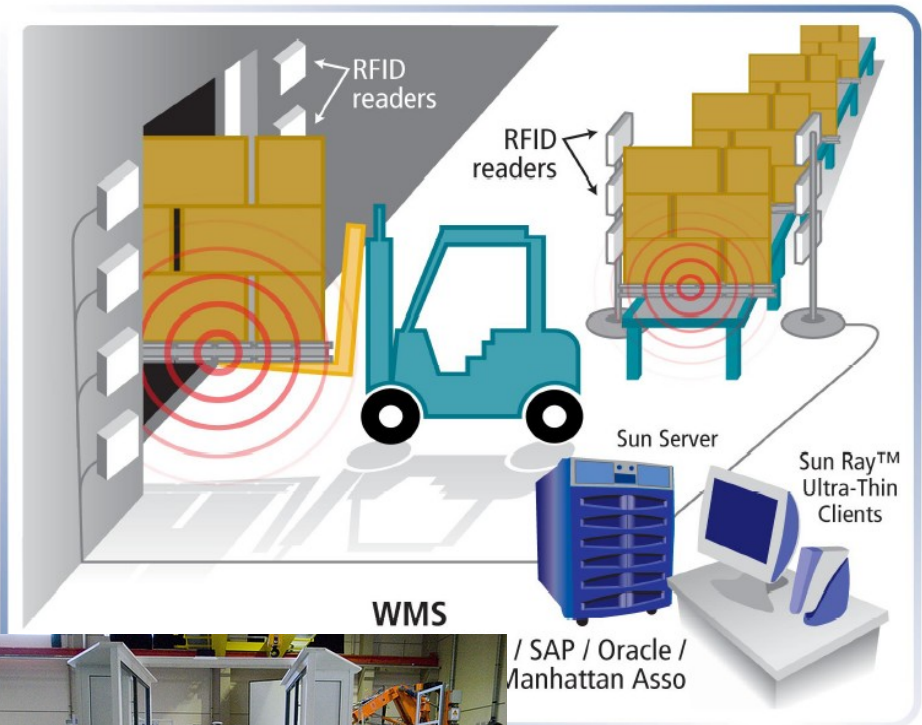
# Anwendungen

## Prozessautomatisierung

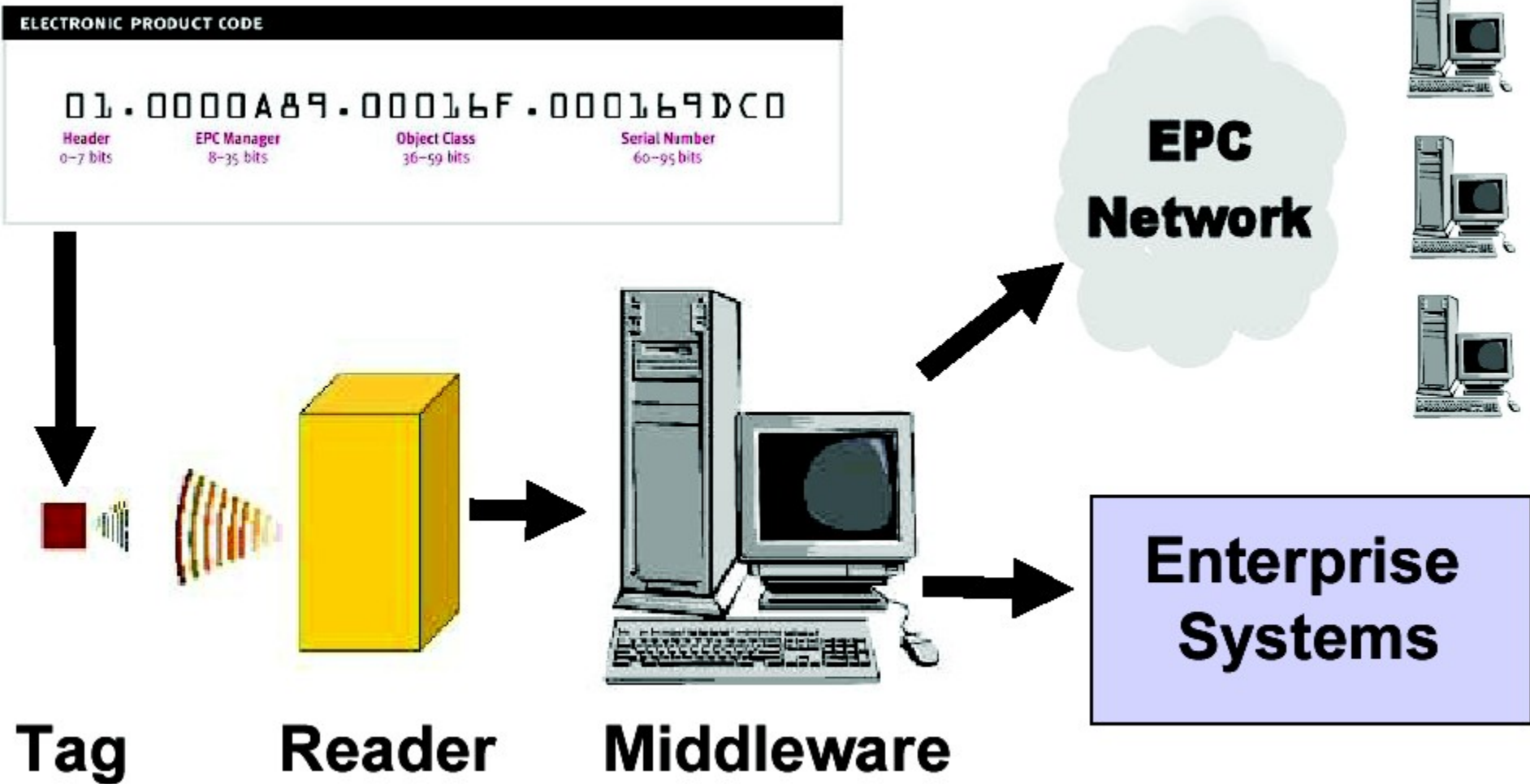
- Lieferketten zw. Unternehmen, sogenanntes Supply Chain Management
- Innerhalb Produktionsanlage

## Vorteile

- Schließt die Brücke zw. virtuellen Daten in der Datenbank und dem tatsächlichen Status eines Produkts/einer Gruppe von Produkten
- Reduktion von Fehlleitungen, Wiederauffinden von Gütern (insb. auch innerhalb von Produktionsanlagen)
- Automatisierung von Abläufen, z.B. Inventur, „smarte“ Rückrufaktionen
- Bessere Kenntnis über Abläufe
- Kostenreduktion durch Automatisierung



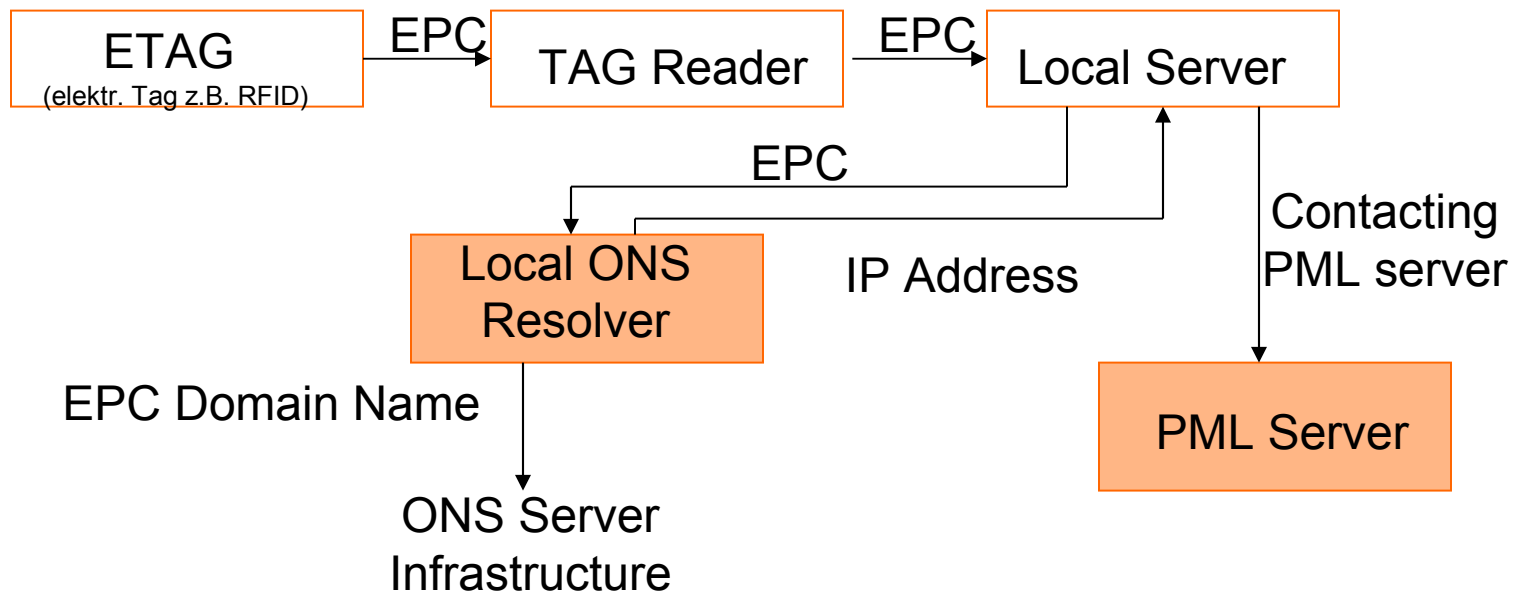
# AutoID: RFID Tags in Geschäftsanw.



# Verarbeitung von IDs

## Idee

- Weltweit auflösbare Identifikation
- Benutzung von Internet-Technologie (IP Adressen, TCP/IP, DNS, XML)
- Auflösung ähnlich DNS: Object Naming Service (ONS)
- PML: Physical Markup Language, XML Standard für Beschreibung Objekt, Raum und Beziehung der Objekte darin



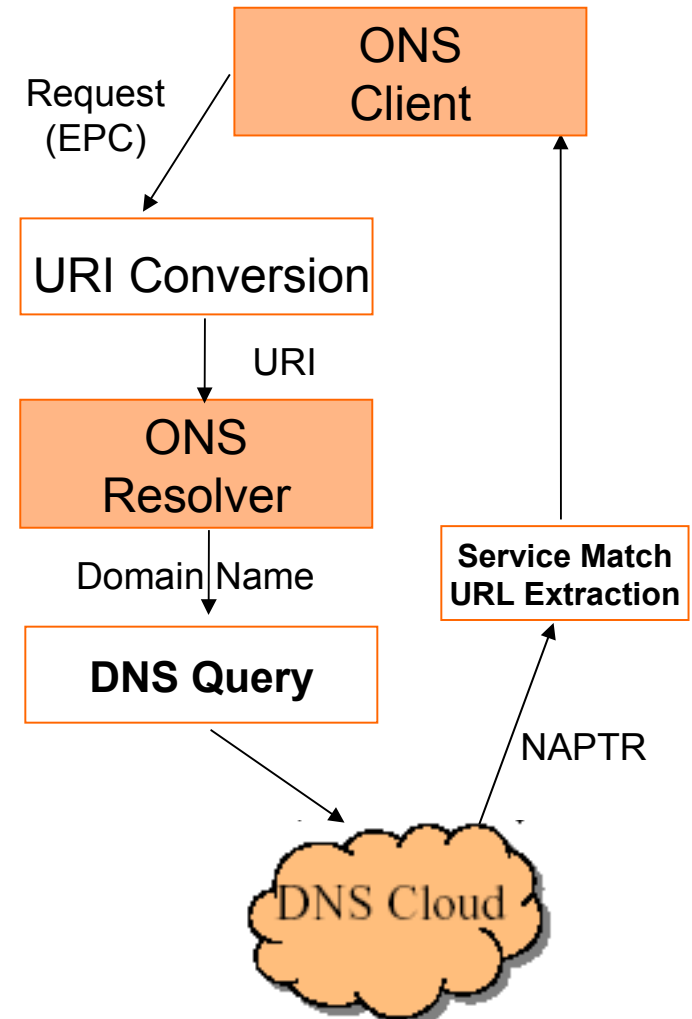
# ONS over DNS

## Motivation

- Nutzung von DNS (nur eine Infrastruktur)
- Service orientiertes Konzept (IP Adresse nicht ausreichend)

## Beispiel: Client stellt Anfrage nach EPC

- EPC (RFID Reader):  
(10 000 0000000000000000  
0000000000000000000011000  
00000000000000000000110010000)
- EPC→URI (Local server):  
*urn:epc:id:sgtin:0614141.000024.400*
- URI→Domain Name (ONS Resolver):  
*000024.0614141.sgtin.id.onsepc.com*
- DNS query for Naming Authority PoinTeR (NAPTR) records
- Extraktion der URLs nach Servicewunsch des ONS Clients :  
*http://epc-is.example.com/epc-wsdl.xml*



# Services

Order	Pref	Flags	Service	Regexp	Replacement
0	0	u	EPC+ws	!^.*\$!http://example.com/autoid/widget100.wsdl!	.
0	0	u	EPC+epcis	!^.*\$!http://example.com/autoid/cgi-bin/epcis.php!	.
0	0	u	EPC+html	!^.*\$!http://www.example.com/products/thingies.asp!	.
0	0	u	EPC+xmlrpc	!^.*\$!http://gateway1.xmlrpc.com/servlet/example.com!	.
0	1	u	EPC+xmlrpc	!^.*\$!http://gateway2.xmlrpc.com/servlet/example.com!	.

## NAPTR:

NAPTR records auf DNS, Quelle: epccglobalinc.com

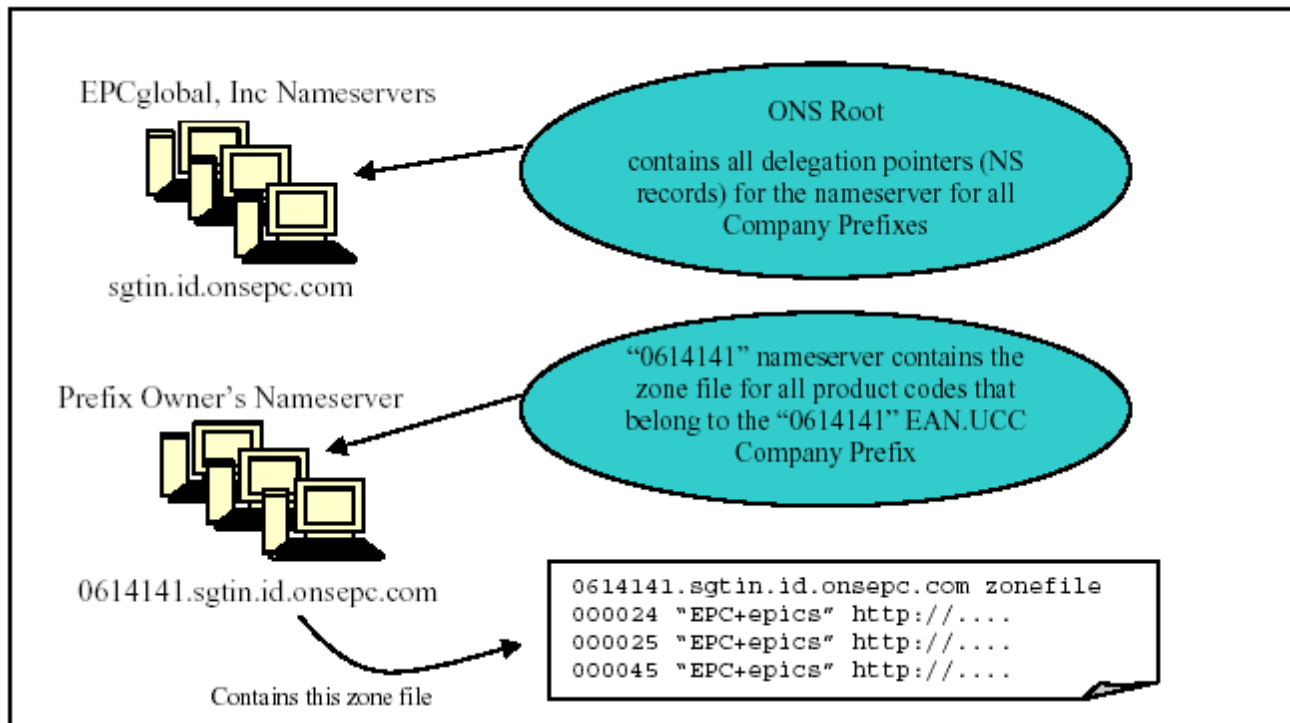
- Pref: Priorität, kleinste wird genommen
- Flag: u for URI
- Service: EPC+<service id>
- Regexp: Service URL, regexp für URL Rewriting (future app.)

## Ablauf:

- DNS liefert NAPTR records an Client
- ONS Client filtert anhand der Service-Beschreibungen
- ONS Client stellt separate Anfrage an Server (Service provider)

# ONS over DNS Delegation

Quelle: epcglobalinc.com



- Hersteller Nameserver über IP Adresse und Company Prefix bei onsepc.com angemeldet
- DNS Queries werden zu Hersteller Nameserver geroutet
- Hersteller publiziert Item Reference codes und Services

# RFID Sicherheit

---

## Attacken (2006)

### RFID Pass (Riscure Security Lab)

- Angriff: Passinformationen auslesen durch Brute-Force Angriff (Schlüsselraten) auf Basic Access Control (BAC)
- Ausgenutzte Schwachstelle: IDs waren teilweise vorhersagbar, Schlüsselraum kleiner

### RFID-Verschlüsselung (Shamir und Oren)

- Angriff: Extrahieren des Kill-Commands bei EPC Gen1 Transpondern durch Mithören (side-channel attack)
- Ausgenutzte Schwachstelle: unzureichende Implementierung des Sicherheitsstandards

### RFID-Virus (Rieback, Crispo, Tanenbaum)

- Angriff: Schadcode einschleusen
- Ausgenutzte Schwachstelle: SQL-Injection in RFID Middleware