EMES: Eigenschaften mobiler und eingebetteter Systeme

RFID: Radio Frequency Identification

Dr. Siegmar Sommer, Dr. Peter Tröger

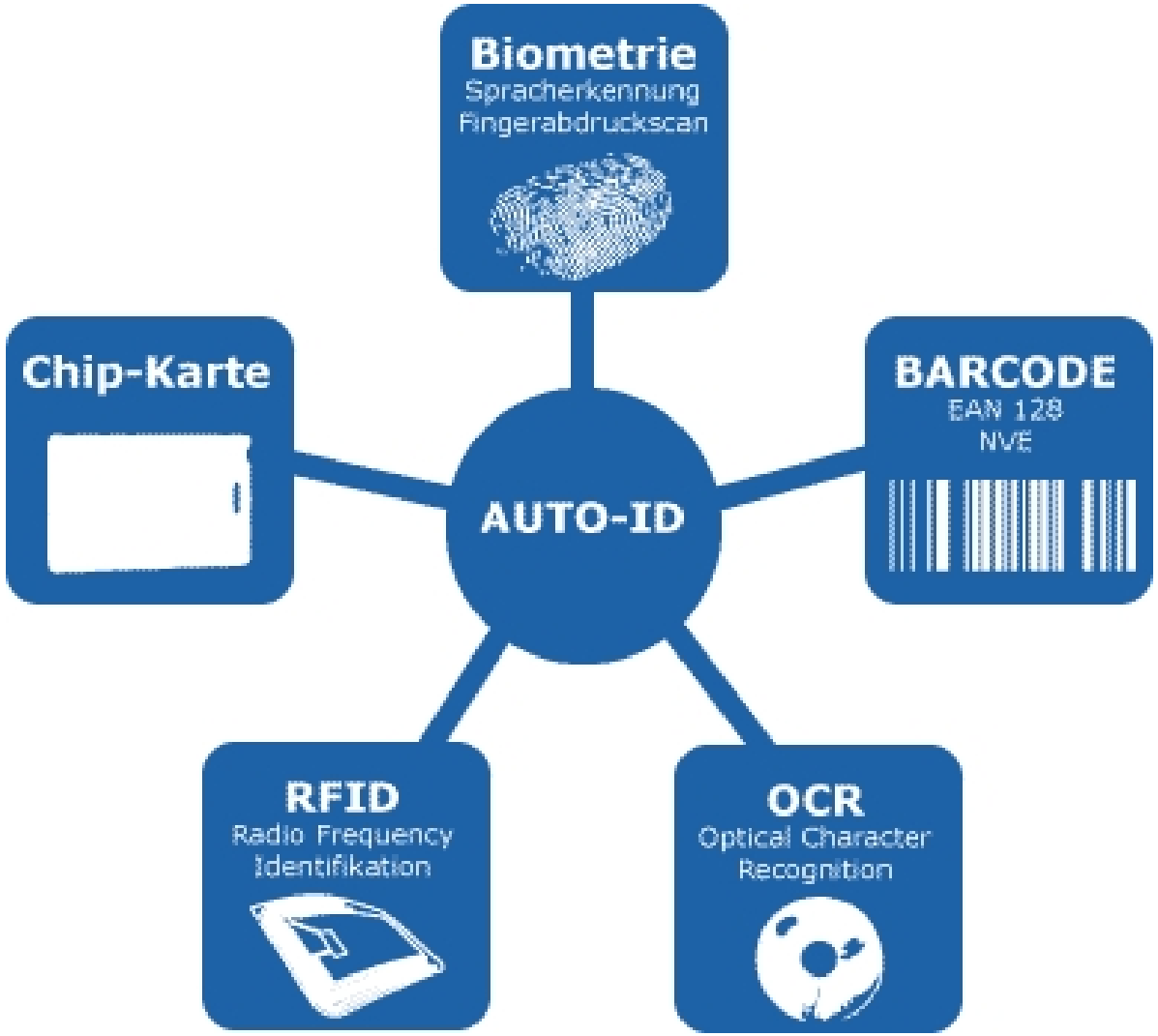
Wintersemester 2009/2010

Einleitung: Was ist RFID?

- Radio Frequency Identification
- Verfahren zur automatischen Identifizierung von Objekten mittels Funk
- Neben automatischer Erfassung auch Speicherung von Daten

Quellen: Veröffentlichungen im Internet, Seminarvortrag von André Stephan und Jens Hackenberg im Sommersemester 2007

Automatische Identifikation: Techniken



Vorteile von RFID

Parameter/System	Barcode	OCR	Chipkarte	RFID
Typische Datenmenge (Byte)	1 ~ 100	1 ~ 100	16 ~ 64k	16 ~ 64k
Einfluss von Schmutz/ Nässe	sehr stark	sehr stark	möglich (Kontakte)	kein Einfluss
Einfluss von (opt.) Abdeckung	totaler Ausfall	totaler Ausfall	möglich	kein Einfluss
Einfluss von Richtung und Lage	gering	gering	sehr hoch (eine Steckrichtung)	kein Einfluss
Anschaffungskosten/ Leseelektronik	sehr gering	mittel	gering	mittel
Lesegeschwindigkeit (inkl. Handhabung des Datenträgers)	gering ~ 4 s	gering ~ 3 s	gering ~ 4 s	sehr schnell ~ 0,5 s

Geschichte

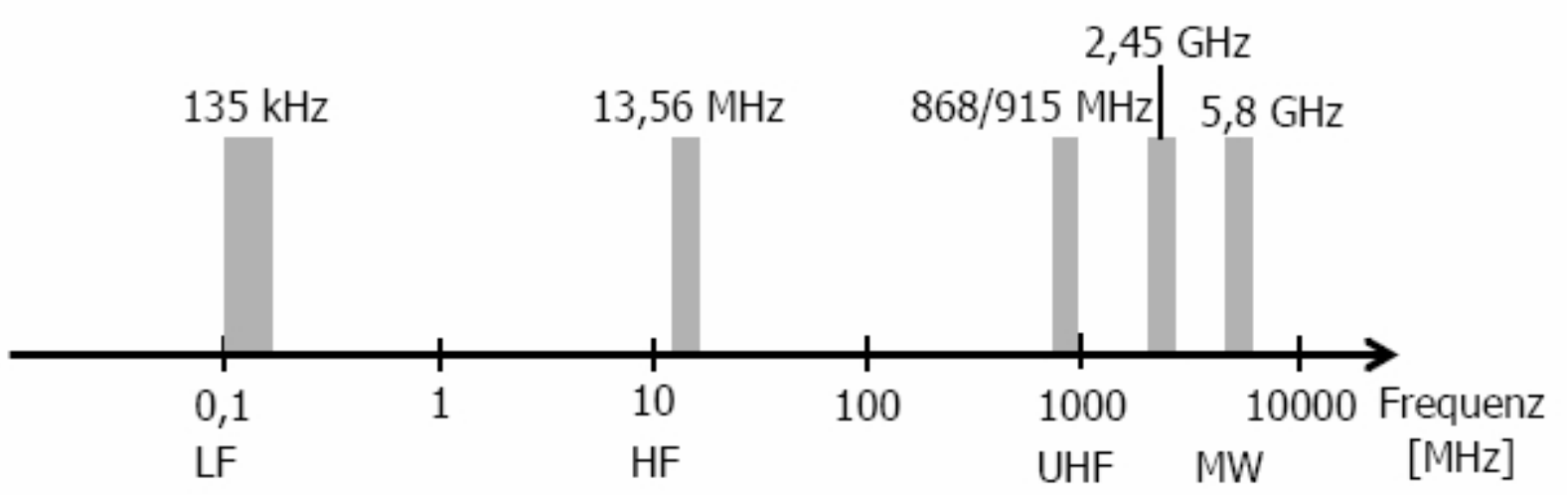
- Erstmals im 2. Weltkrieg als Sekundärradar: Unterscheidung von Freund und Feind auf Radarschirm (Identification Friend or Foe (IFF))
- Ende 60er Jahre SICARID („Siemens Car Identification“) zur eindeutigen Identifizierung von Eisenbahnwagen und später Autoteilen in der Lackiererei
- 70er Jahre erste kommerzielle Vorläufer als elektronisches Warensicherungssystem („Electronic Article Surveillance“, EAS)
- 1979 viele Neuerungen mit Schwerpunkt Tierkennzeichnung
- 80er Jahre im Mautsystem
- 90er Jahre Systeme für Zutrittskontrolle, bargeldloses Zahlen, Wegfahrsperre, ...

Komponenten

- Transponder („Transceiver“ und „Responder“) auch Tag genannt
  - dient als Datenträger (eindeutige ID, ...)
  - wird an Objekt angebracht (z. B. an Ware) oder in dieses integriert (z. B. in Chipkarte)
  - kann nur ausgelesen oder auch beschrieben werden (ROM- und RAM-Speicher im Einsatz)
- Reader
  - Lese- und Schreibzugriffe auf Daten des Transponders

Frequenzen und Beispiele

- Betriebsfrequenz = Arbeitsfrequenz des Readers (Sendefrequenz des Transponders meist die gleiche)

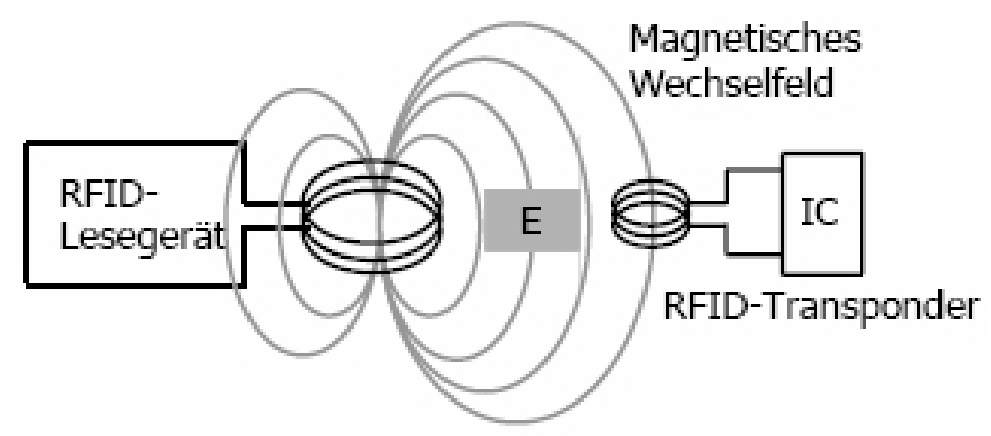


- 125 kHz : Tiermarkierung
- 5,8 GHz : Fahrzeug-Identifizierung (Maut-System)
- Achtung: je höher die Frequenz, umso höher sind Energieverluste an Metalloberflächen und Absorption durch Wasser

Übertragung von Energie und Daten

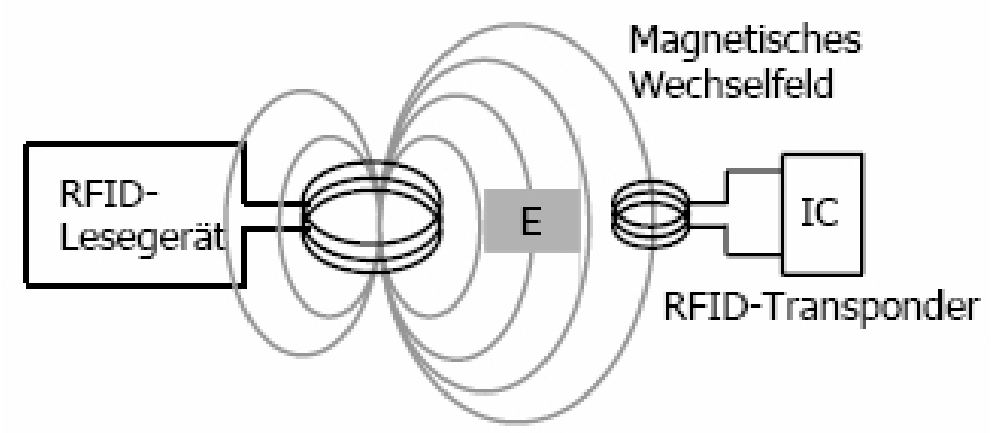
- Induktive Kopplung
- Elektromagnetische Kopplung

Induktive Kopplung I



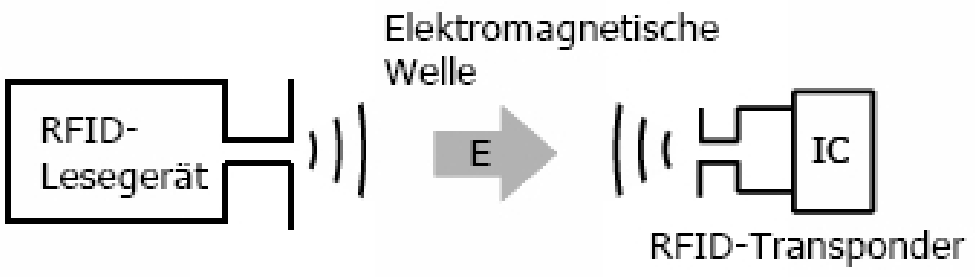
- Bei RFID-Systemen von 135kHz und 13,56 MHz (LF und HF)
- Spule des Readers erzeugt magnetisches Wechselfeld in der Sendefrequenz (induziert Wechselspannung in Transponder, wird gleichgerichtet)
- Bei passiven Transpondern Energieversorgung des Mikrochips
- An- und Ausschalten eines Lastwiderstandes an Transponderantenne bewirkt Spannungsänderung an Antenne des Readers

Induktive Kopplung II



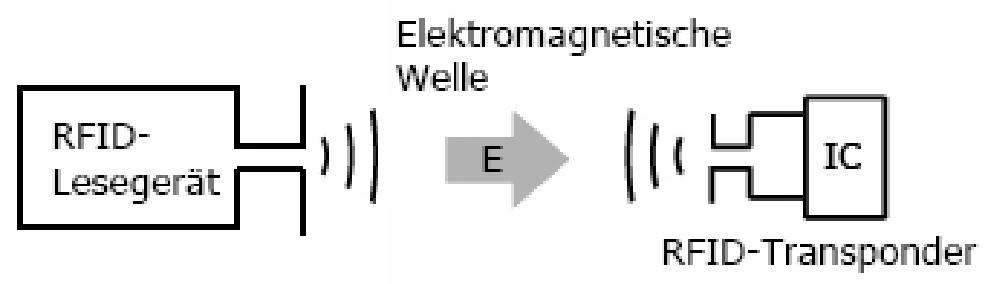
- Datenübertragung: Schalten des Lastwiderstandes gesteuert durch Daten auf Mikrochip = Lastmodulation (Amplitudenmodulation)
- Induzierte Spannung ist abhängig von Sendefrequenz und Anzahl der Windungen der Spule des Transponders bei konstanter Feldstärke
- Bei 135 kHz ca. 1000 Windungen, bei 13,56 MHz ca. 10 Windungen

Elektromagnetische Kopplung I



- Sendefrequenzen: 868, 915 MHz sowie 2,45 GHz und 5,8 GHz
- Antenne des Readers erzeugt elektromagnetische Welle mit Sendefrequenz
- Welle induziert in Antenne des Transponders Wechselspannung (im Transponder gleichgerichtet)
- Antenneneigenschaft: ein Teil der Leistung wird aufgenommen, anderer Teil wird reflektiert
- Aufgenommene Leistung: bei passiven Transpondern Energieversorgung des Mikrochips

Elektromagnetische Kopplung II



- Datenübertragung: auch hier Lastmodulation, bewirkt Modulation der reflektierten Welle („modulierter Rückstrahlquerschnitt“)
- Energie im Fernfeld nimmt umgekehrt proportional zum Quadrat der Entfernung der Antenne ab (Abstand von 10m auf 100m: Feldstärke $1/10^2$)
- Achtung: Sendeleistung ist durch Zulassungsvorschriften beschränkt
- Reichweite: passive Systeme mit 5 - 7m und aktive Systeme bis zu 100m (500m)

Transponder

- Aktive Transponder
- Unterscheidung: normal aktiv und „beacon“ (Blinklicht)
- Interne Energiequelle (Batterie, Solarzellen) für Versorgung des Microchips und evtl. der Datenübertragung

  - Für raue Industrieumgebungen (Lebensdauer (Batterie) ca. 6 Jahre bei 600 Abfragen pro Tag)

Reader I

- Einsatz: Identifikation, Verfolgung, Lokalisierung

Reader II

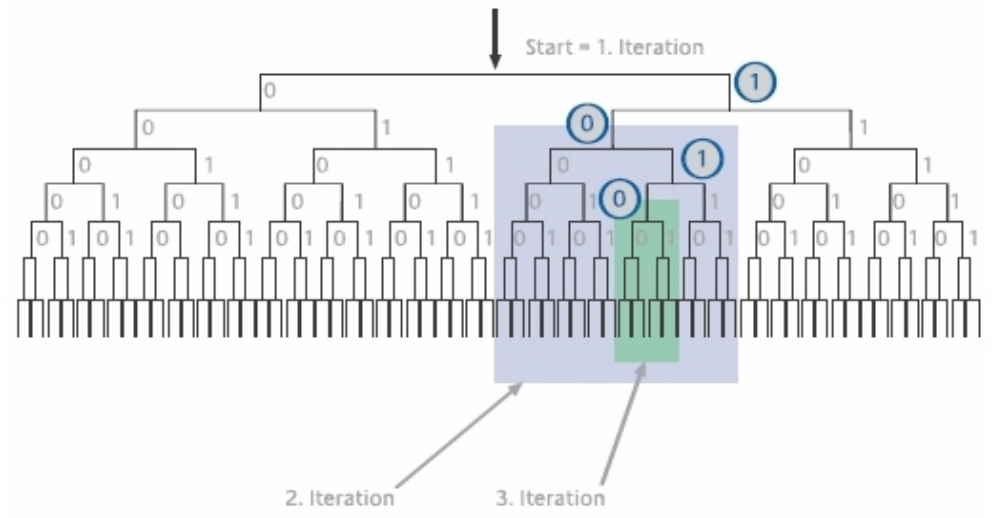
	LF 0-135 kHz	HF 3-30 MHz	UHF 200 MHz-2 GHz	MW > 2 GHz
Art der Kopplung	Induktive Kopplung (arbeitet im Nahfeld)		Elektromagnetische Kopplung (arbeitet im Fernfeld)	
Typische Frequenz	134,2 kHz	13,56 MHz	868 MHz (EU) 915 MHz (USA)	2,45 GHz 5,8 GHz
Typische Lesereichweite	< 1,5 m	< 1,0 m	Passive Transponder: < 3 m (EU bei 0,4 W) ca. 3-5 m (EU bei 2 W, geplant) ca. 5-7 m (US bei 4 W)	

Zugriffsverfahren

- Da Transponder nur über begrenzte Leistungsfähigkeit verfügt und günstig in Herstellung sein sollen, hauptsächlich Zeitmultiplex, selten Frequenzmultiplex (oder Kombination beider)

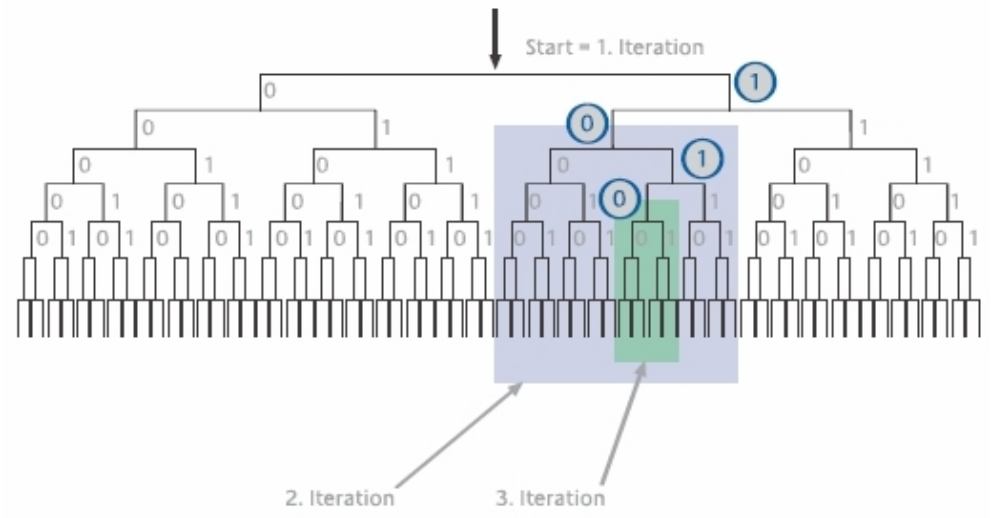
- Zwei grundsätzliche Verfahren für Identifizierung aller Transponder im Lesebereich des Readers:
  - Deterministische Verfahren (Reader fordert IDs der Transponder an und filtert einzeln jede ID im Lesebereich raus)
  - Probabilistische Verfahren (Transponder senden zu zufälligen Zeitpunkten ihre ID)

Treewalking I



- In jedem Schritt werden alle Transponder aufgefordert, (mit bestimmter prä-ID) ihre ID zu senden
- Reader durchschreitet einen Binärbaum, um eine einzige ID extrahieren zu können
- Durch geschickte Modulation können Kollisionen an einer ID-Stelle festgestellt werden

Treewalking II



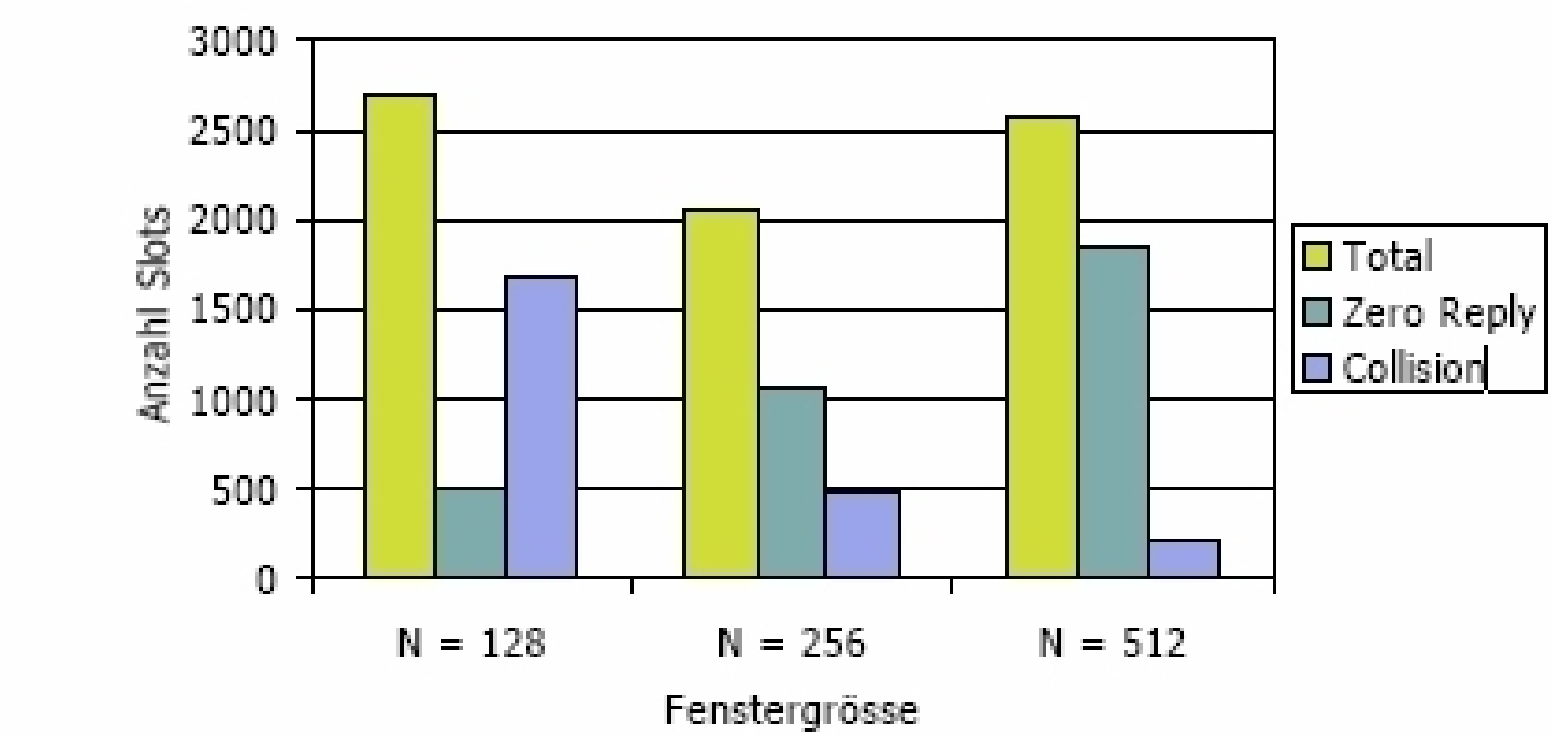
- Nach jeder Kollision fordert der Readers alle Transponder zur Antwort auf, die mit Sub-ID (ab Kollisionsstelle) mit 1 bzw. 0 weitergeht
- Sukzessive Verkleinerung des Suchraumes, bis nur noch ein Transponder antwortet
- Treewalking-Verfahren ist auf hohe Datenübertragungsraten angewiesen für hohe Erkennungsraten

Slotted-ALOHA-Algorithmus I

- Reader stellt den Transpondern Zeitfenster zur Verfügung
- Zeitfenster in Zeitslots unterteilt
- Jeder Transponder wählt zufällig einen Zeitslot zur Übertragung der ID
- Erkannte Transponder werden stumm geschaltet

Slotted-ALOHA-Algorithmus II

- Wahl der Anzahl der Zeitslots beeinflusst Erfassungszeit (Anzahl Slots)



Einsatzgebiete (heute/morgen)

- Objektkennzeichnung
- Echtheitsprüfung von Dokumenten
- Diebstahlsicherung
- Zutritts-/Routenkontrollen
- Umweltmonitoring/Sensorik
- Supply-Chain-Management

Diebstahlsicherung/Wegfahrsperre

- Diebstahlsicherung:
  - 1Bit-Transponder
  - Schon lange im Einsatz (Richtlinie VDI 4470)
  - Sensorschranken lesen Bit aus und geben ggf. Alarm
- Wegfahrsperre:
  - Lesegerät im Zündschloß
  - Transponder im Schlüssel

Tiere/Nutztierhaltung

- Tiermarkierung von Nutztieren mittels Transponder: Ohrmarke, Injektat
- 1998-2002 von EU erprobt, ab 2008 für Schafe und Ziegen Pflicht
- Mehr Kontrolle über Herkunft von Fleisch
- Seit 2004: alle Wiener Hunde “getagt”
- Vereinfachung biologischer Forschung

Bibliotheken

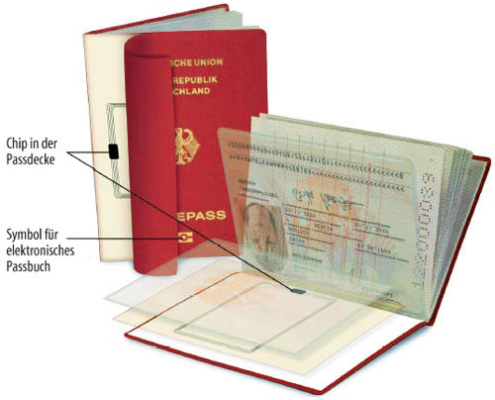
- RFID-Chip an jedem Buch erleichtert Verwaltung
- Schnelle Verbuchung, Sicherung und Ausleihe (stapelweise)
- Automatisierte Medienrückgabe (auch nachts)
- Bibliotheken in München, Stuttgart, Hamburg,...

City-Maut

- e-Plate-Nummernschilder (bis 10m Reichweite), auch bei 250km/h
- Zugangskontrollen, Mautsysteme und Section-Control Geschwindigkeitsmessungen möglich
- Wegeprofile bei ausreichend dichtem Sensornetz
- Electronic Road Pricing System in Singapur
- Edinburgh: Busse veranlassen Ampeln auf Grün zu schalten $\longrightarrow$ 10% schnellere Fahrten

Pässe

- Fälschungssicherheit
- 2004 von EU beschlossen, biometrische Merkmale in Pässen aufzuneh men
- digitales Lichtbild, später Fingerabdrücke, evtl. Iris-Scan
- Speicherung in zentraler Datenbank?
- In Deutschland seit Nov. 2005 RFID-Reisepass
- Visafreie Einreise in USA nur noch mit RFID-Pass möglich
- Transponder mit mind. 64kB Speichervolumen

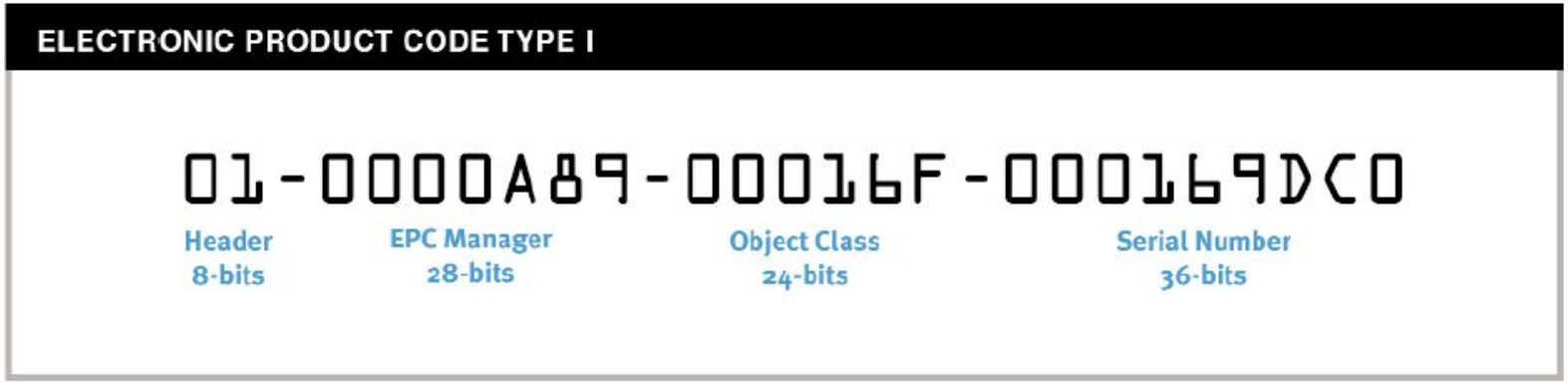


Einkaufen

- Massenhafte Anwendung von RFID-Chips an Produkten (260Mrd./Jahr in EU)
- Bessere Kontrolle des Warenflusses, Optimierung, schnelle Bezahlung
- Intelligente Einkaufswagen: ermitteln Inhalt, addieren Preise, geben Kaufvorschläge
- Intelligente Regale: merken Entnahme, wissen, wann sie aufgefüllt werden müssen
- Metro, Rewe, Tesco, Wal-Mart sind Vorreiter
- 2003 erster Future-Store in Rheinberg

EPC - Electronic Product Code

- EPCglobal führt mit EPC eindeutige Kennzeichnung von Objekten ein
- Header: Versionsnummer, erlaubt verschiedene EPC-Längen
- EPC Manager: Hersteller-ID
- Object Class: Produkt-Typ
- Serial Number: Für jedes Produktexemplar eindeutige ID



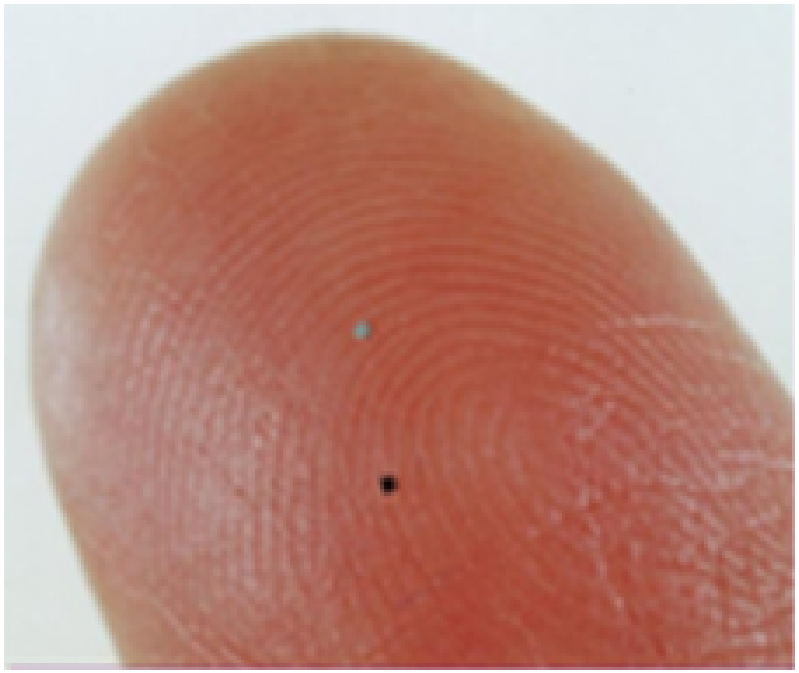
- Object Name Service: EPC $\longrightarrow$ Produktbezeichnung

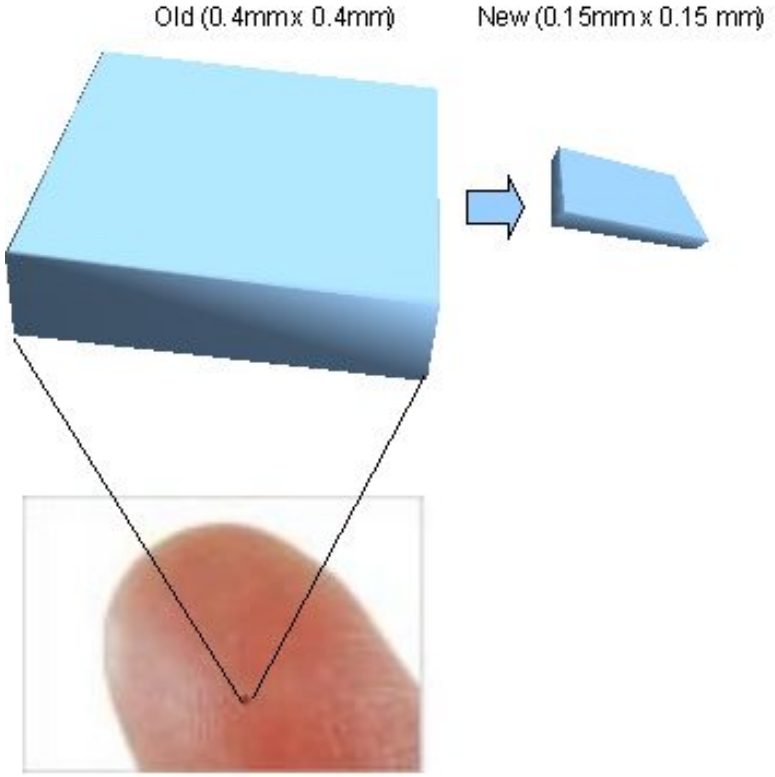
Weitere Anwendungsgebiete

- Mensakarten
- Stadionkarten
- Banknoten
- Medizin (Patienten/Medikamente)
- Marathon
- Bekleidung
- Mülltonnen

Größe

- Transponder können buchgroß bis sehr, sehr klein sein
- Hitachi fertigte Feb. 2007 staubkorngroße RFID-Chips
- 128bit-ROM, 30cm Reichweite (2,45GHz)
- "smart dust"





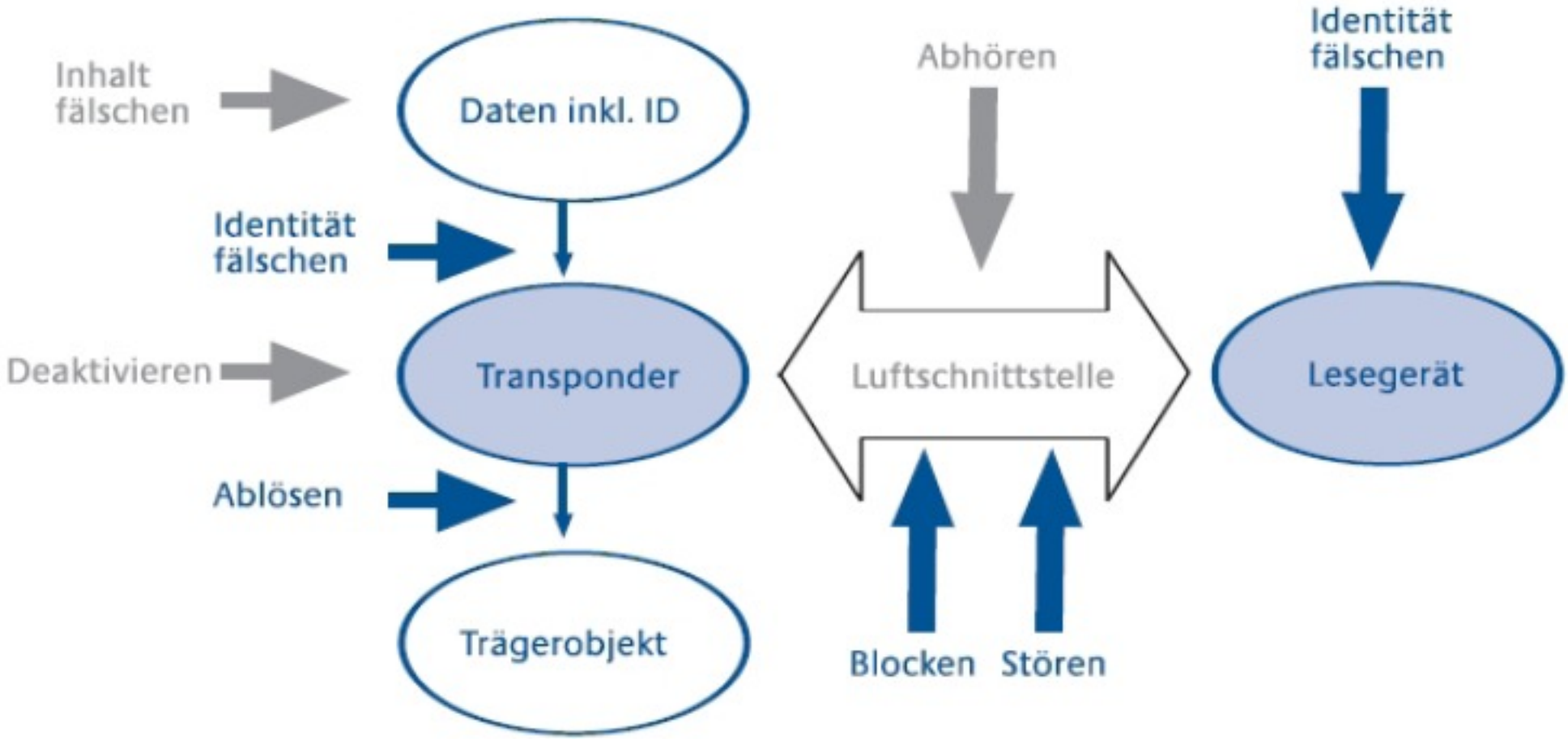
Kosten/Wiederverwendung

- Kosten:
  - Preis reduzierbar auf 5ct pro Transponder
  - Transponder mit höherer Leistung sind teurer
  - Lesegeräte 100-1500 Euro
  - $\longrightarrow$ für Masseneinsatz in Kaufhäusern noch zu kostspielig
- Wiederverwendung:
  - Smart-Tags nur einmal verwendbar, da aufgeklebt
  - Chips für Diebstahlsicherung teilweise wiederverwendbar

Datenschutz und Risiken

- Datenschutzgesetz:
  - Informierung des Kunden über Datenerfassung
  - Datenerfassung auf das Nötigste reduzieren
- Recht auf informationelle Selbstbestimmung
- Gefahr des "gläsernen Kunden":
  - Einkaufswagen weiß, was der Kunde letztes Mal gekauft hat
  - Heimlicher RFID-Transponder in Kundenkarte?
  - Mangel an Transparenz und Kontrolle der Datenerhebung und -verarbeitung

Angriffsszenarien

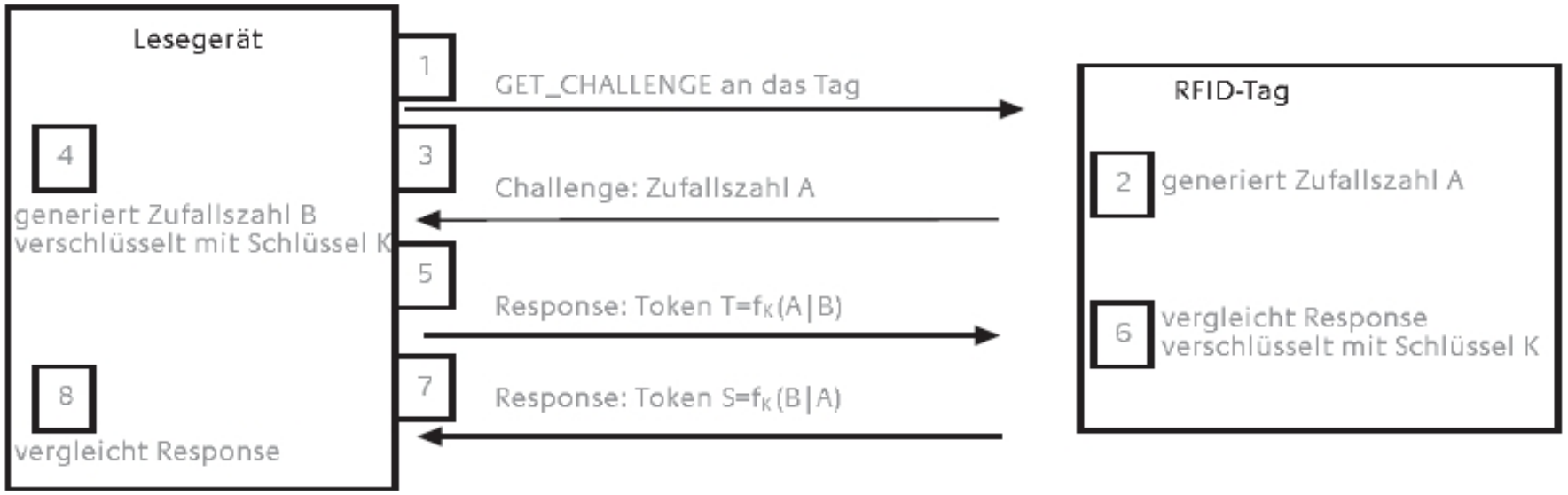


Angriffszwecke

	Ausspähen	Täuschen	Denial of Service	Schutz der Privatsphäre
Inhalt fälschen		■		
Identität fälschen (Tag)		■		
Deaktivieren		■	■	■
Ablösen		■		■
Abhören	■			
Blocken		■	■	■
Stören		■	■	■
Identität fälschen (Leser)	■			

Schutz vor Spionage

- Gegenseitige Authentifizierung: Challenge-Response-Verfahren

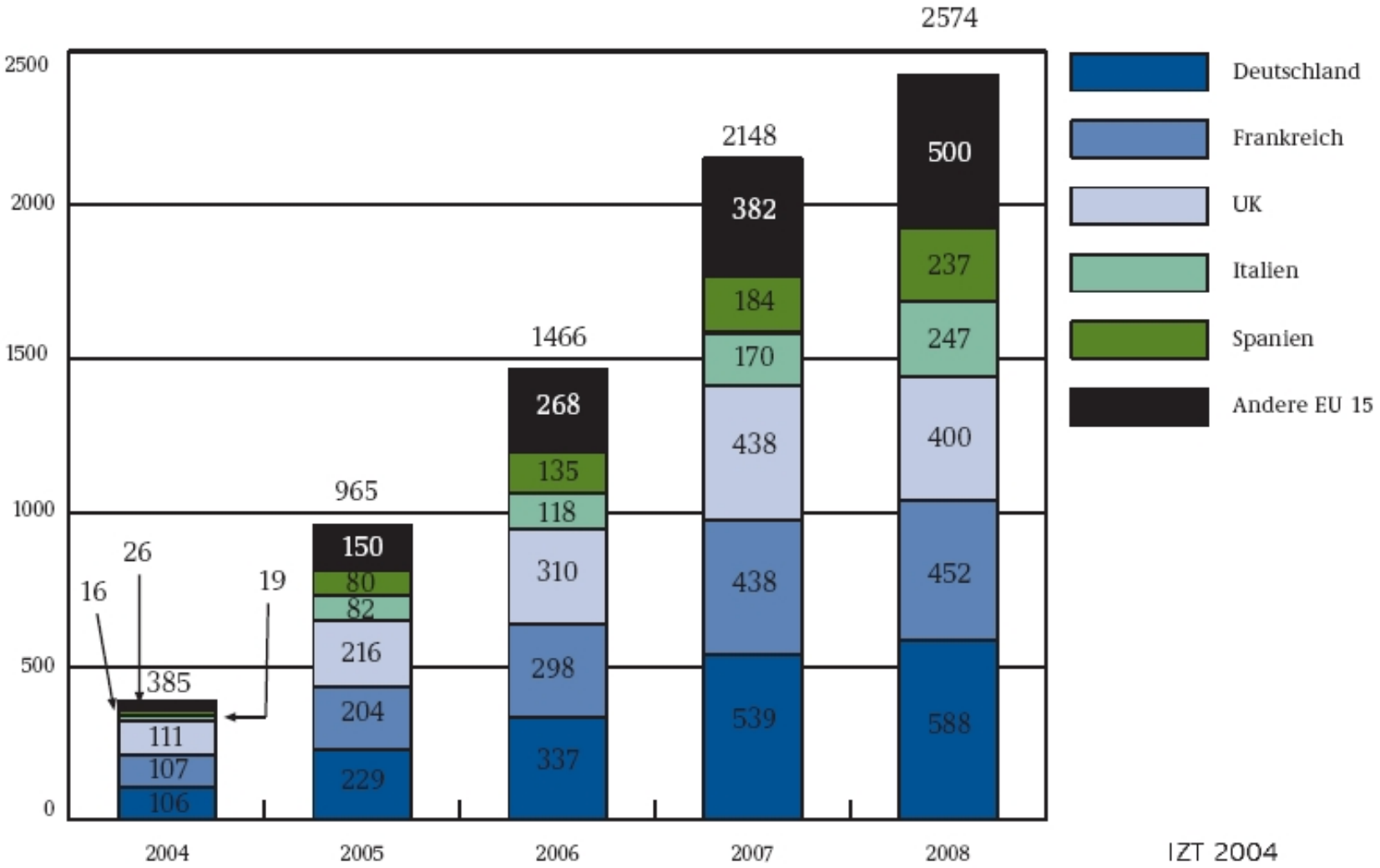


- Verschlüsselung: Session-Key zwischen Lesegerät und Transponder

Schutz vor Spionage

- Ansätze basierend auf geringerer Uplink-Reichweite:
  - Silent-Tree-Walking:
    Reader fordert “next bit” statt konkretem Bit, um die Information in den Uplink zu legen
  - Aloha-Verfahren mit temporären IDs:
    Lesegerät benutzt nur Zufallszahlen, um Tags zu identifizieren
- Blocker-Tags (sind verboten)
- Privat: deaktivieren der Tags (kill-Befehl/Feldeinwirkung)
- Abschirmung

Aktueller Markt



Zukunftsvisionen

- Mülltrennung
- Positionsbestimmung (Tags und Reader)
- intelligente Müllkippen?
- essbare RFIDs?
- ...