Hauptseminar
RFID – ein Überblick

Martin Weißbach

martin.weissbach@inf.tu-dresden.de

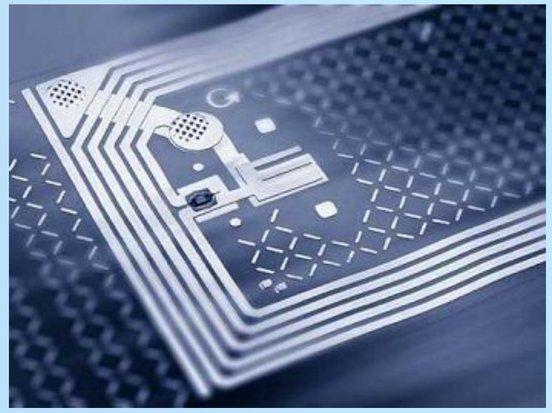
Institut für Technische Informatik
http://www.inf.tu-dresden.de/TeI/

02.05.2007

Gliederung

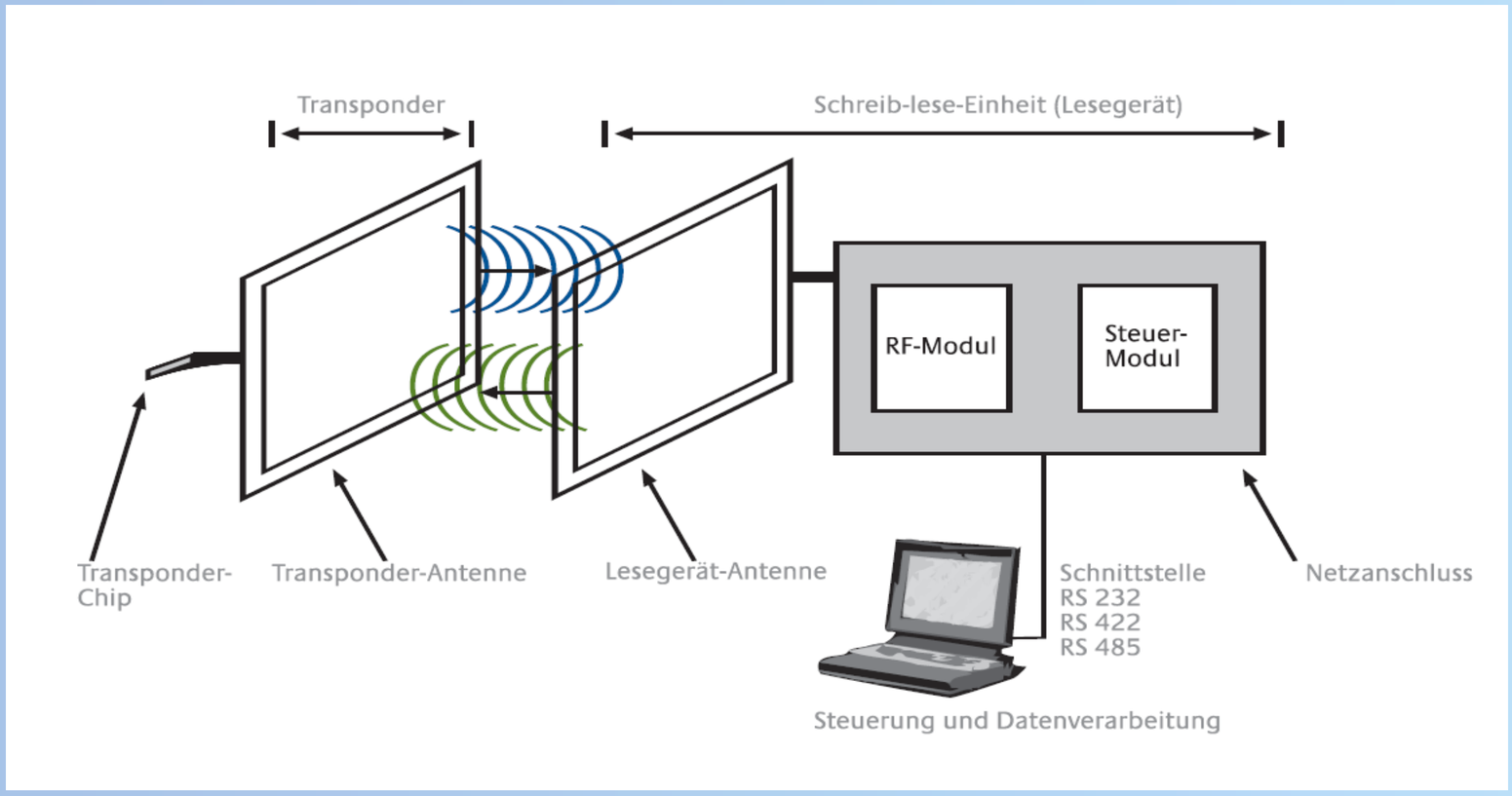
- 1. Einführung
  - Was ist RFID?
- 2. Architektur
  - Grundlegender Aufbau
  - Unterscheidungsmerkmale
- 3. Sicherheit
  - Angriffe
  - Schutzmaßnahmen
- 4. Anwendungsbeispiel: Reisepass
  - Fakten
  - Sicherheit?
- 5. Ausblick

- Was ist RFID?
  - RFID = Radio Frequency IDentification
  - Technologie um Objekte berührungslos per Funk zu identifizieren
  - Vorläufer: Identifikation von britischen Kampfflugzeugen in den 40er Jahren
  - Seit den 60er Jahren im zivilen Bereich (Warensicherungsysteme)
  - Durchbruch in den 80er Jahren
  - Heute: Standardisierung



Quelle: Infineon

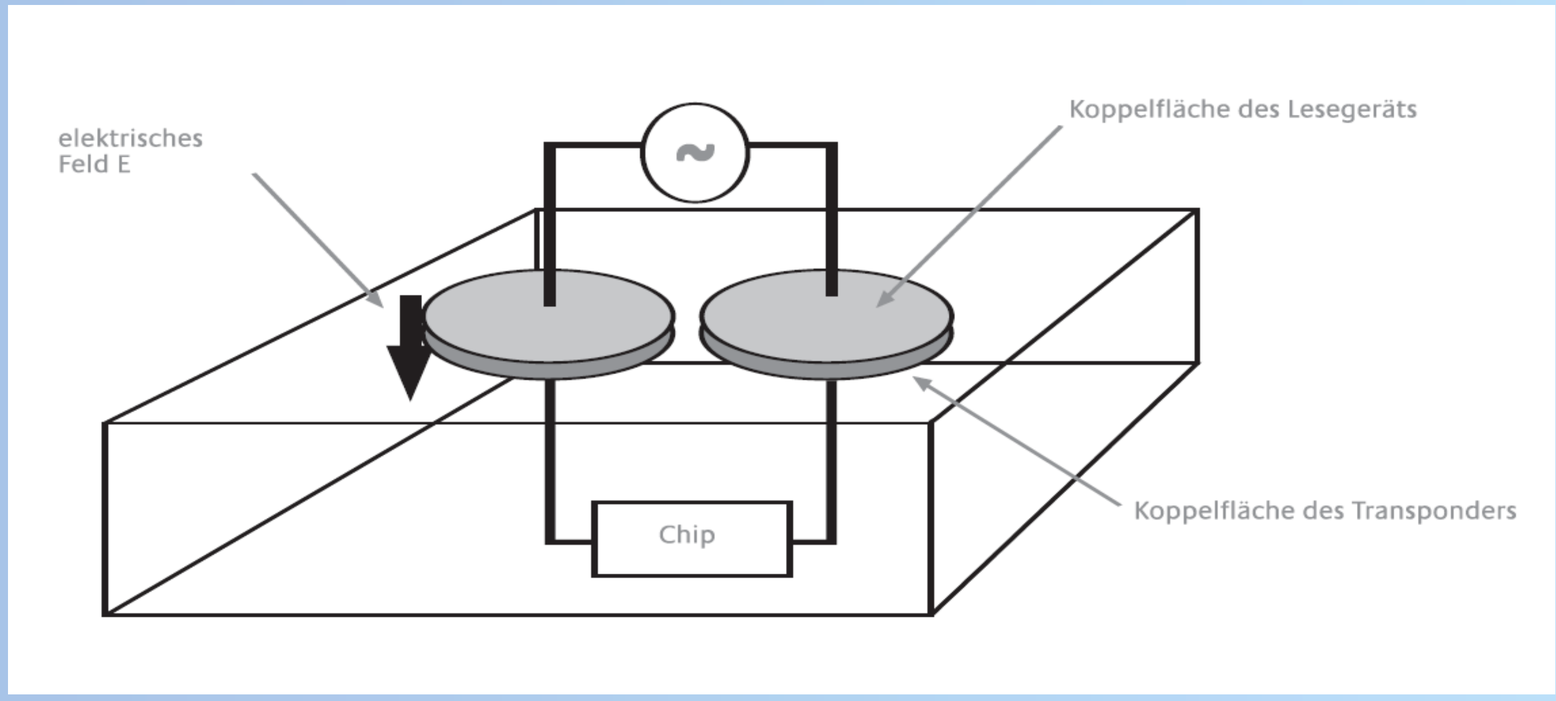
- Grundlegender Aufbau
  - Transponder (auch „Tag“) als Datenträger
  - Reader/Writer als Lese- und Schreibgerät



Quelle: http://www.bsi.de/fachthem/rfid/RIKCHA.pdf

- Unterscheidungsmerkmale
  - Energieversorgung
    - Aktive Transponder
      + Eigene Energiequelle (batteriebetrieben)
      + Befinden sich im Ruhezustand, bis sie von einem Lesegerät aktiviert werden
    - Passive Transponder
      + Keine eigene Energiequelle
      + Energieversorgung über das Lese-/Schreibgerät
      + Geringere Reichweite
      + Leistungsstärkere Lese-/Schreibgeräte notwendig

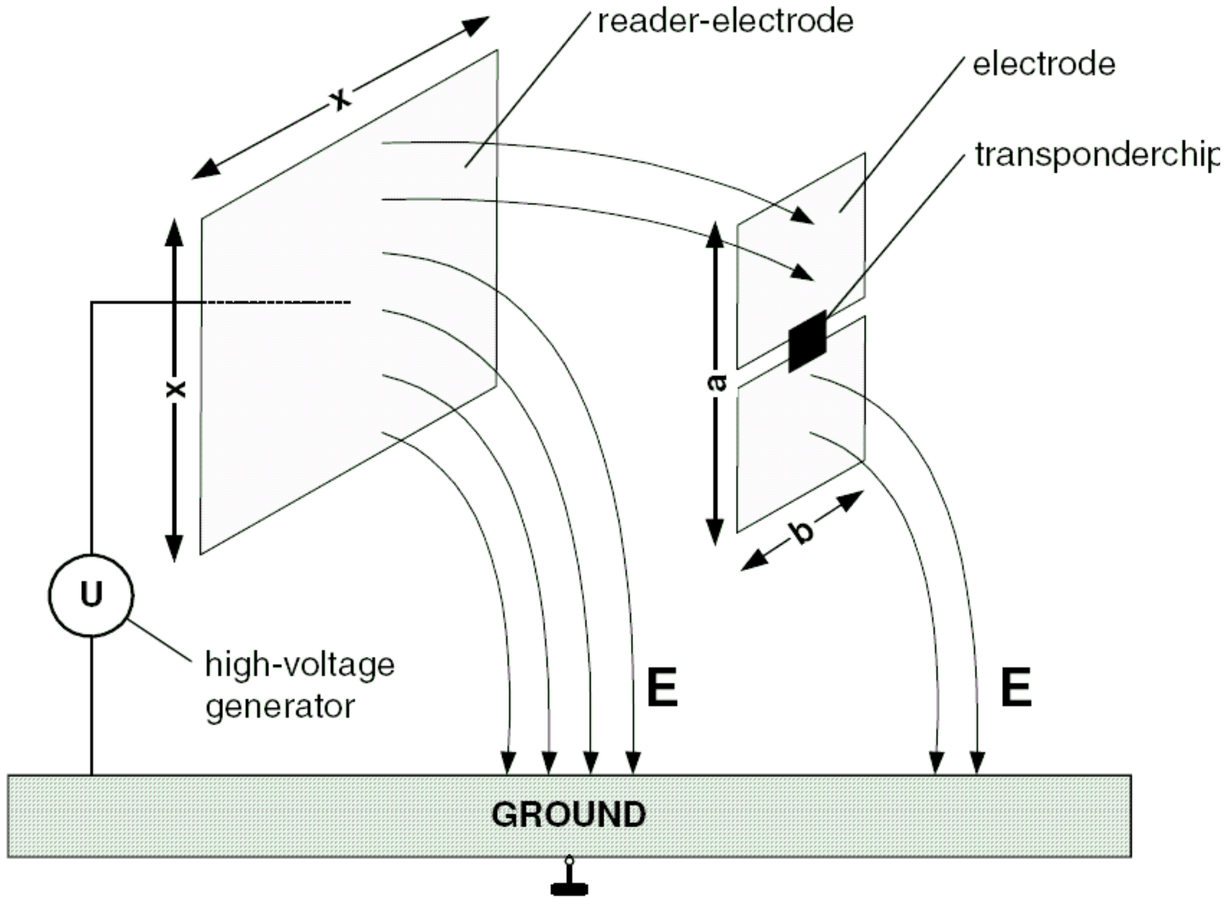
- Unterscheidungsmerkmale
  - Kopplungsverfahren
    - Kapazitive Kopplung (1)
      + Passive Transponder
      + 0.1-1 cm Reichweite („Close Coupling Systeme“)
      + „Plattenkondensatorprinzip“

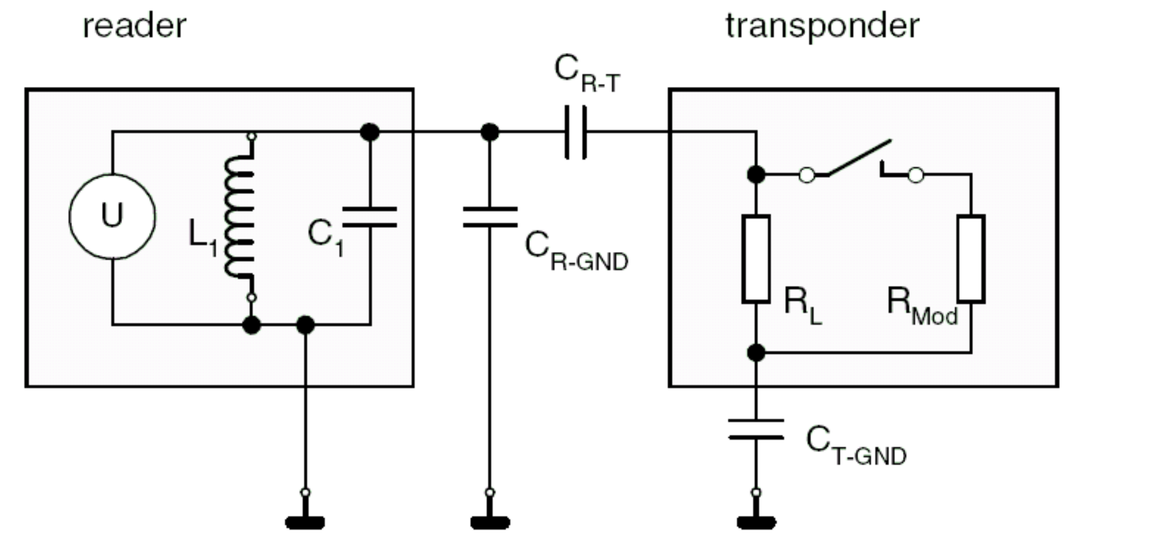


Quelle: http://www.bsi.de/fachthem/rfid/RIKCHA.pdf

Unterscheidungsmerkmale

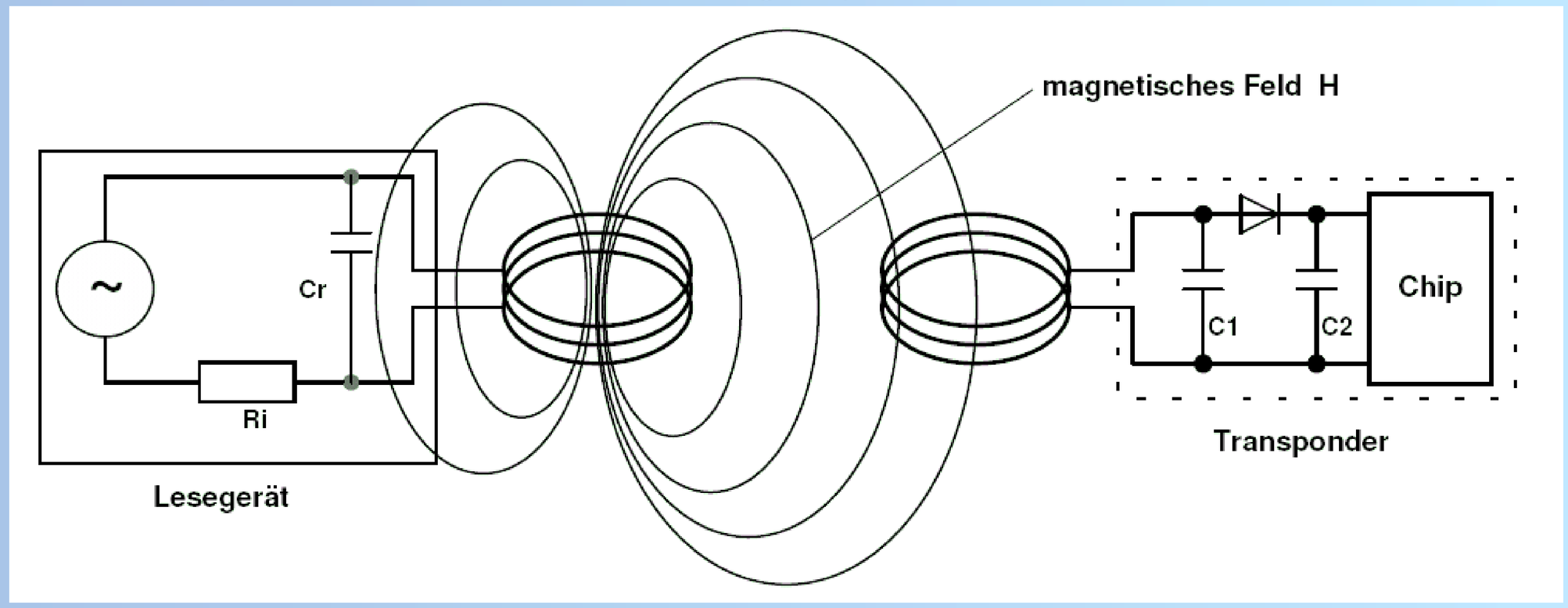
- Kopplungsverfahren
  - Kapazitive Kopplung (2)





Quelle: http://www.rfid-handbook.de/downloads/G3E_3-446-22071-2_leseprobe.pdf

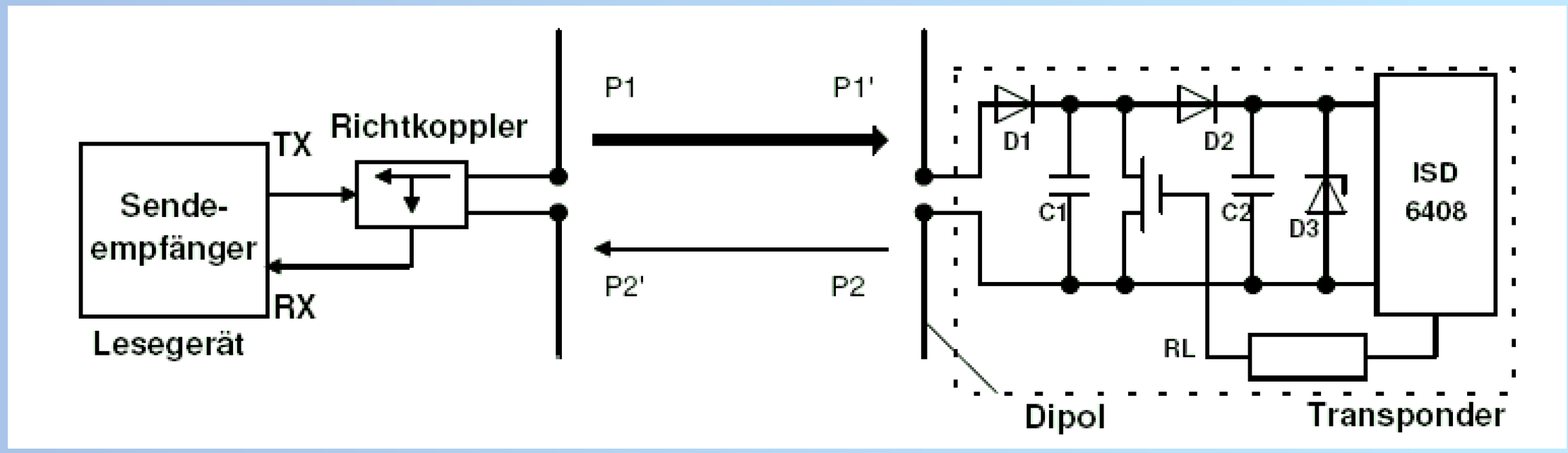
- Unterscheidungsmerkmale
  - Kopplungsverfahren
    - Induktive Kopplung
      - + meist passive Transponder
      - + Reichweite <1m („Remote Coupling Systeme“)
      - + Frequenzbereich (weltweit verfügbar): <135kHz, 13,56 Mhz



http://www.rfid-handbook.de/downloads/G3E_3-446-22071-2_leseprobe.pdf

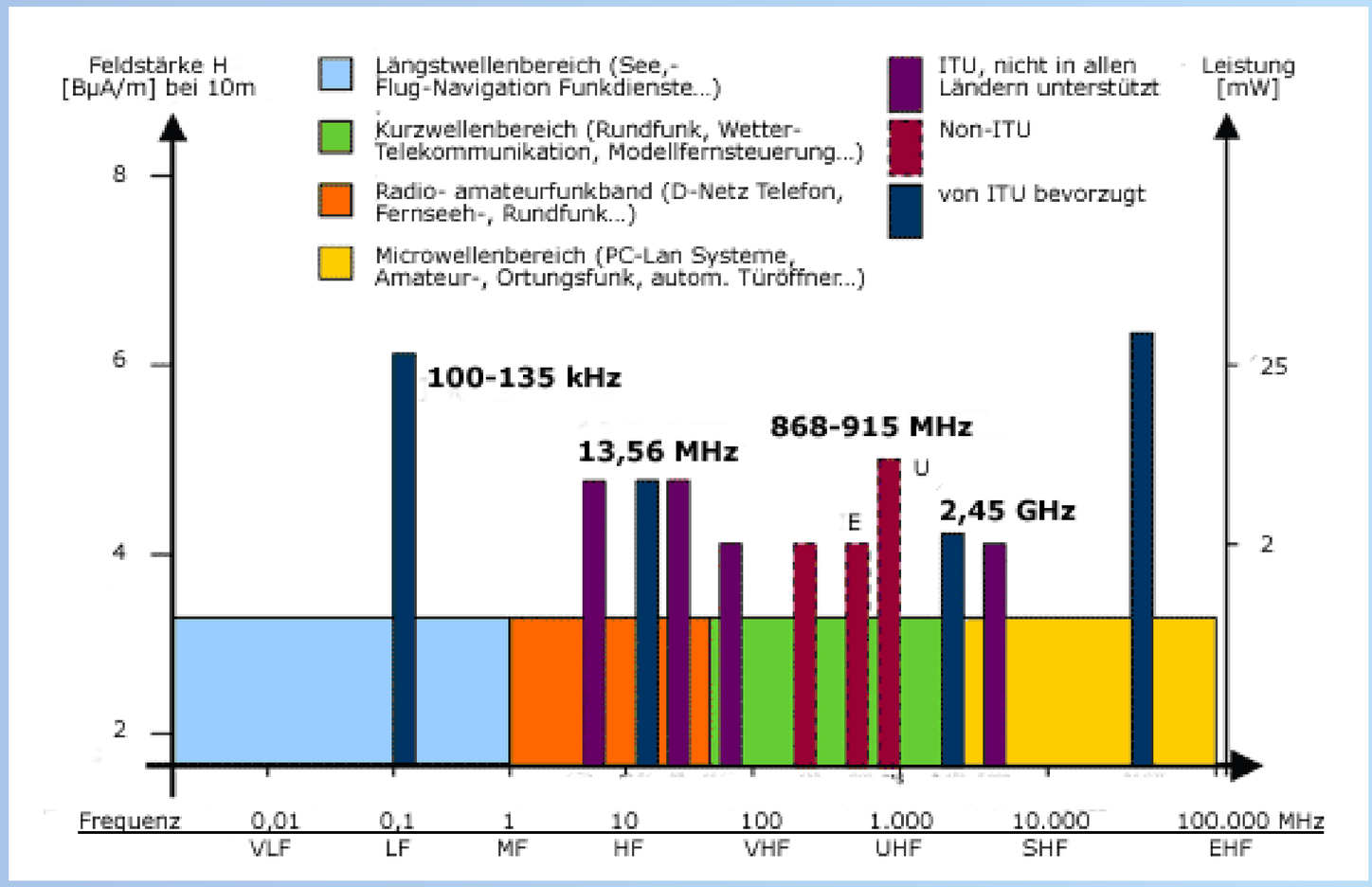
- Unterscheidungsmerkmale
  - Kopplungsverfahren
    - Backscatter Verfahren (1)
      + Aus der RADAR-Technik: „elektromagnetische Wellen werden von Materie, deren Ausdehnung größer als etwa die halbe Wellenlänge der Welle ist, reflektiert“
      + Rückstrahlquerschnitt: Wirksamkeit mit der ein Objekt elektromagnetische Wellen reflektiert
      + Großer Rückstrahlquerschnitt bei Objekten, die zu der eintreffenden Welle in Resonanz sind (z.B. Antennen in der jeweiligen Frequenz)
      + Aktive Transponder (Stützbatterie)
      + Reichweiten > 1 Meter („Long Range Systeme“)
      + Frequenzbereich: 868 Mhz (Europa),915 Mhz(USA), 2.5 Ghz(Weltweit) 5.8 Ghz
      + „Stand-By Mode“

- Unterscheidungsmerkmale
  - Kopplungsverfahren
    - Backscatter Verfahren (2)



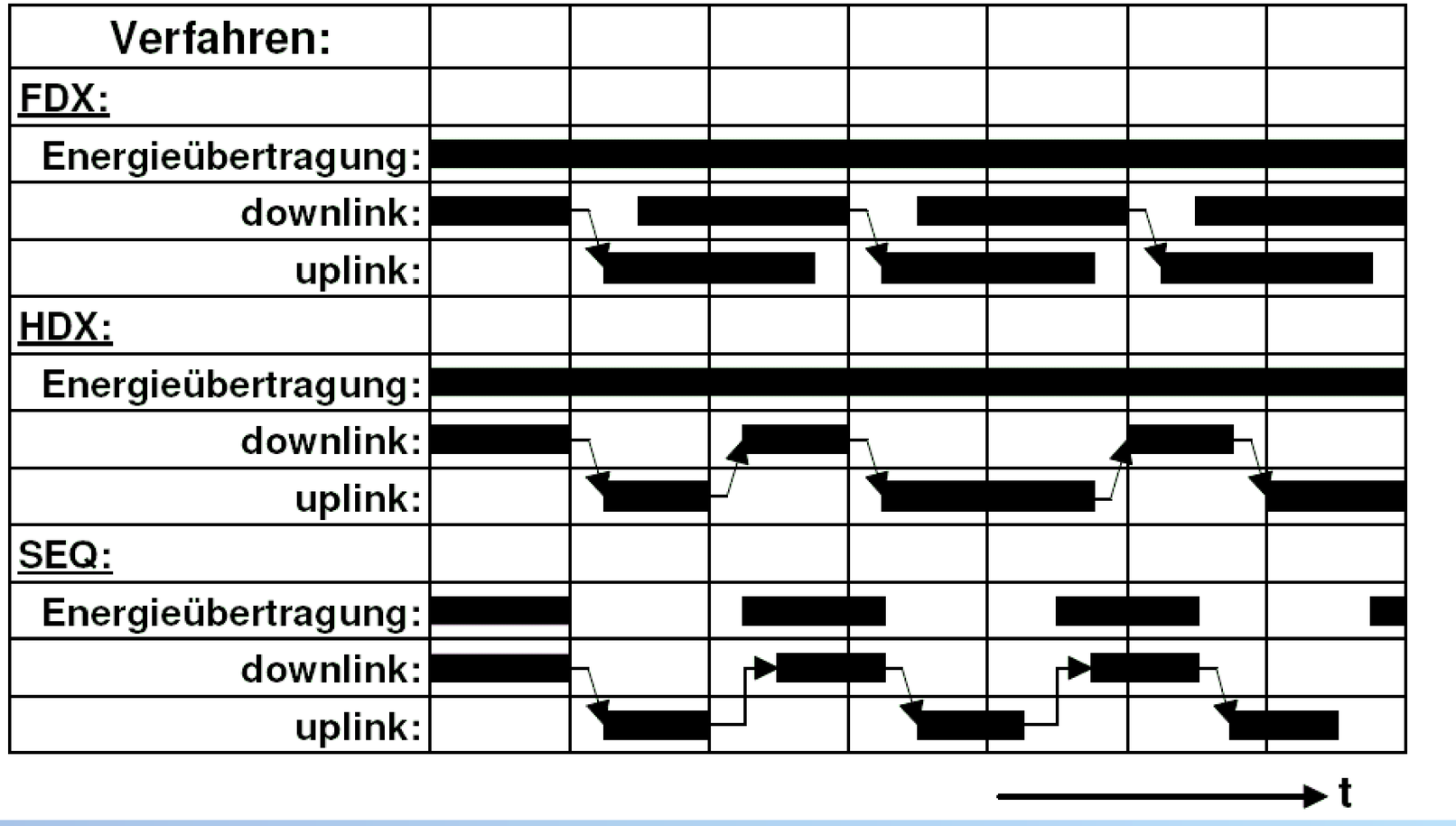
Quelle: http://www.rfid-handbook.de/downloads/G3E_3-446-22071-2_leseprobe.pdf

- Unterscheidungsmerkmale
  - Frequenzbereiche



http://www.gs1austria.at/epc/media/frequenzbereich.gif

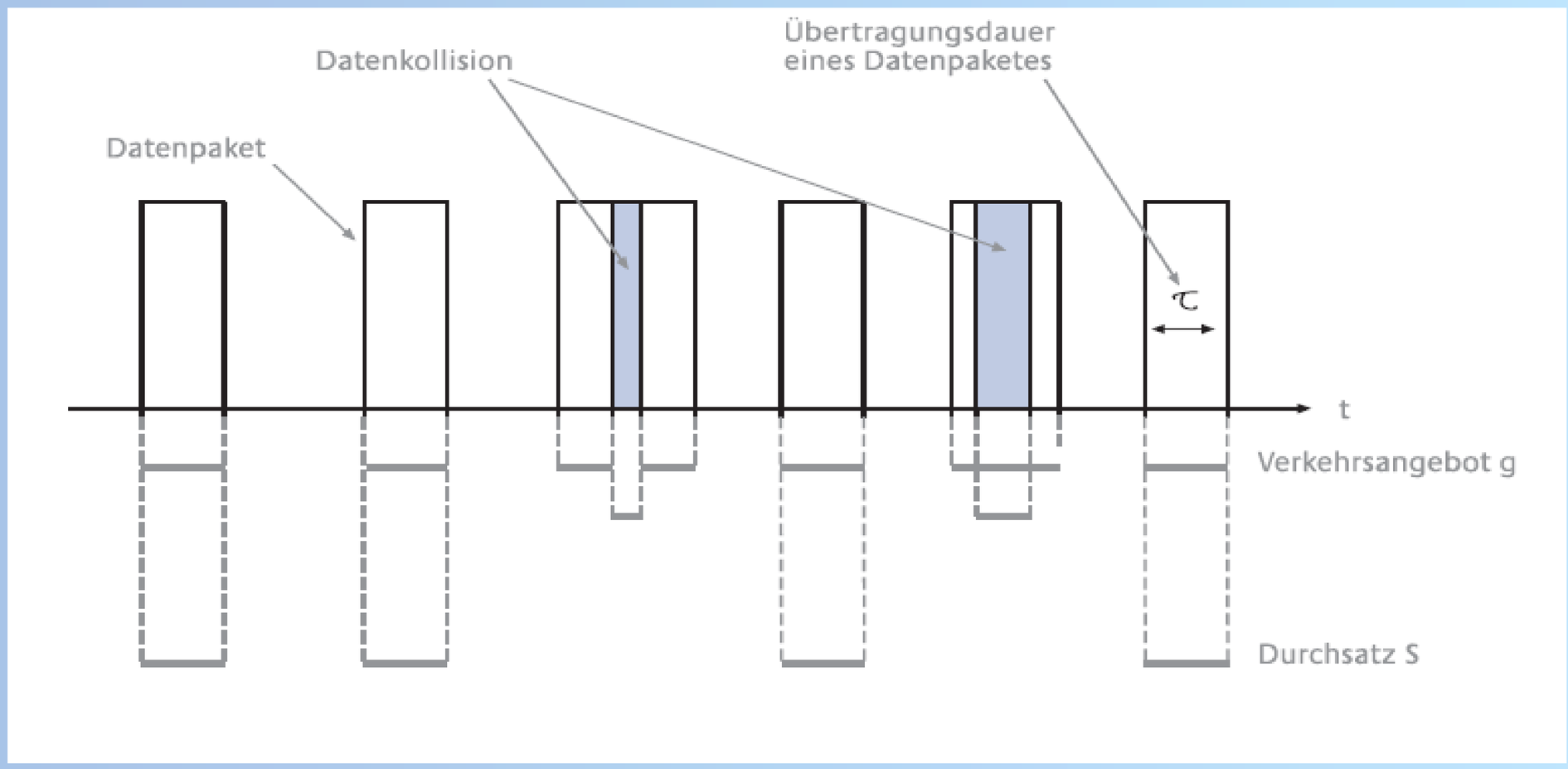
- Unterscheidungsmerkmale
  - Zeitliche Kommunikationsabläufe (Voll- und Halbduplex,Sequentielle Verfahren)



Quelle: http://www.rfid-handbook.de/downloads/G3E_3-446-22071-2_leseprobe.pdf

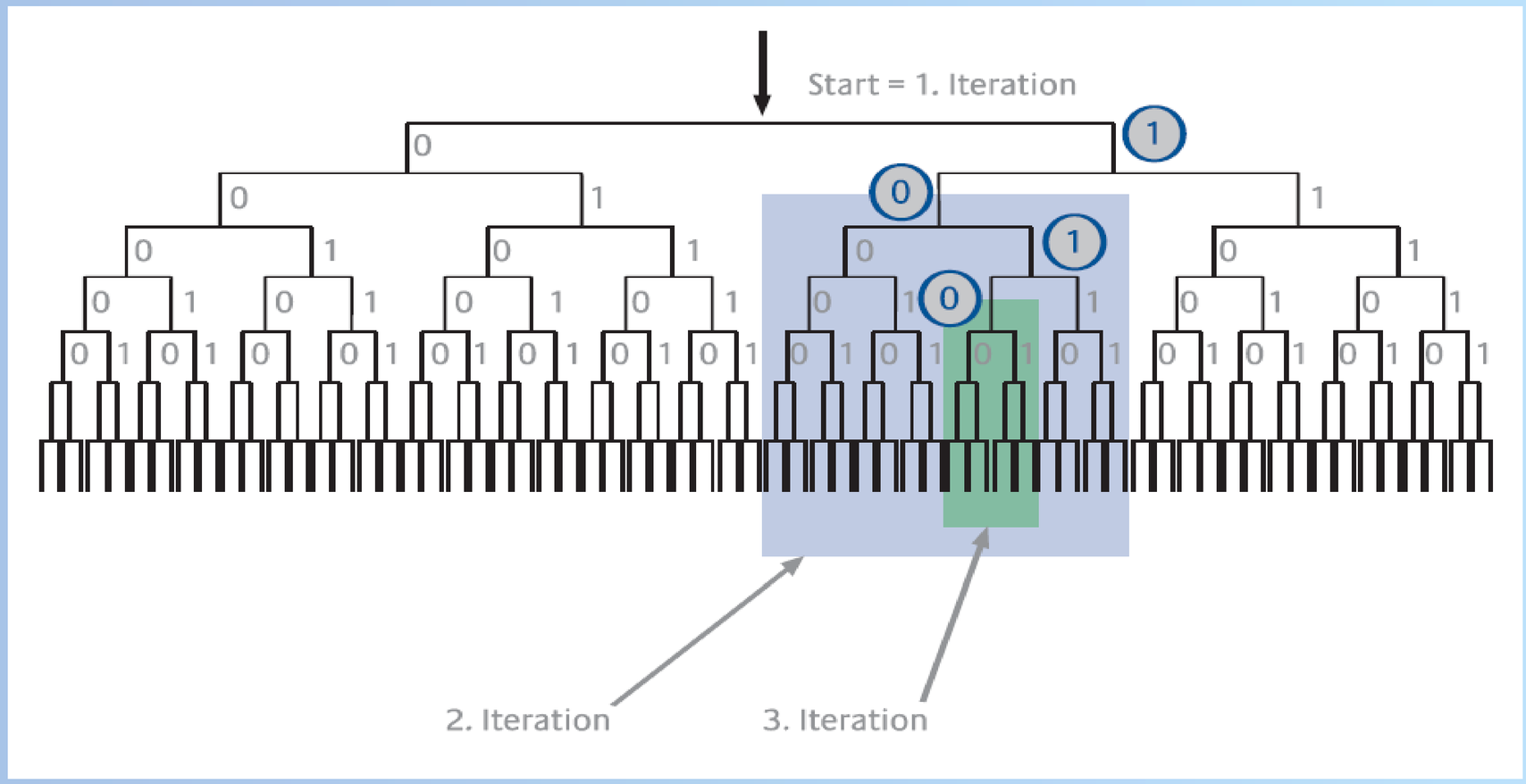
- Unterscheidungsmerkmale
  - Antikollisionsverfahren
    - Problem:
      + mehrere RFID Tags (aber eindeutige ID – meist vom Hersteller vergeben)
      + gleicher Frequenzbereich
      + gleicher Lesebereich
    - Folge:
      + Überlagerung der Signale
      + Kollision
      + Lesegerät kann keines der Tags identifizieren
    - Lösung: Selektionsverfahren/Antikollisionsverfahren (probabilistisch/deterministisch)

- Unterscheidungsmerkmale
  - Antikollisionsverfahren
    - Aloha Verfahren (probabilistisches Verfahren)



Quele: http://www.bsi.de/fachthem/rfid/RIKCHA.pdf

- Unterscheidungsmerkmale
  - Antikollisionsverfahren
    - Tree-Walking-Verfahren (deterministisches Verfahren)

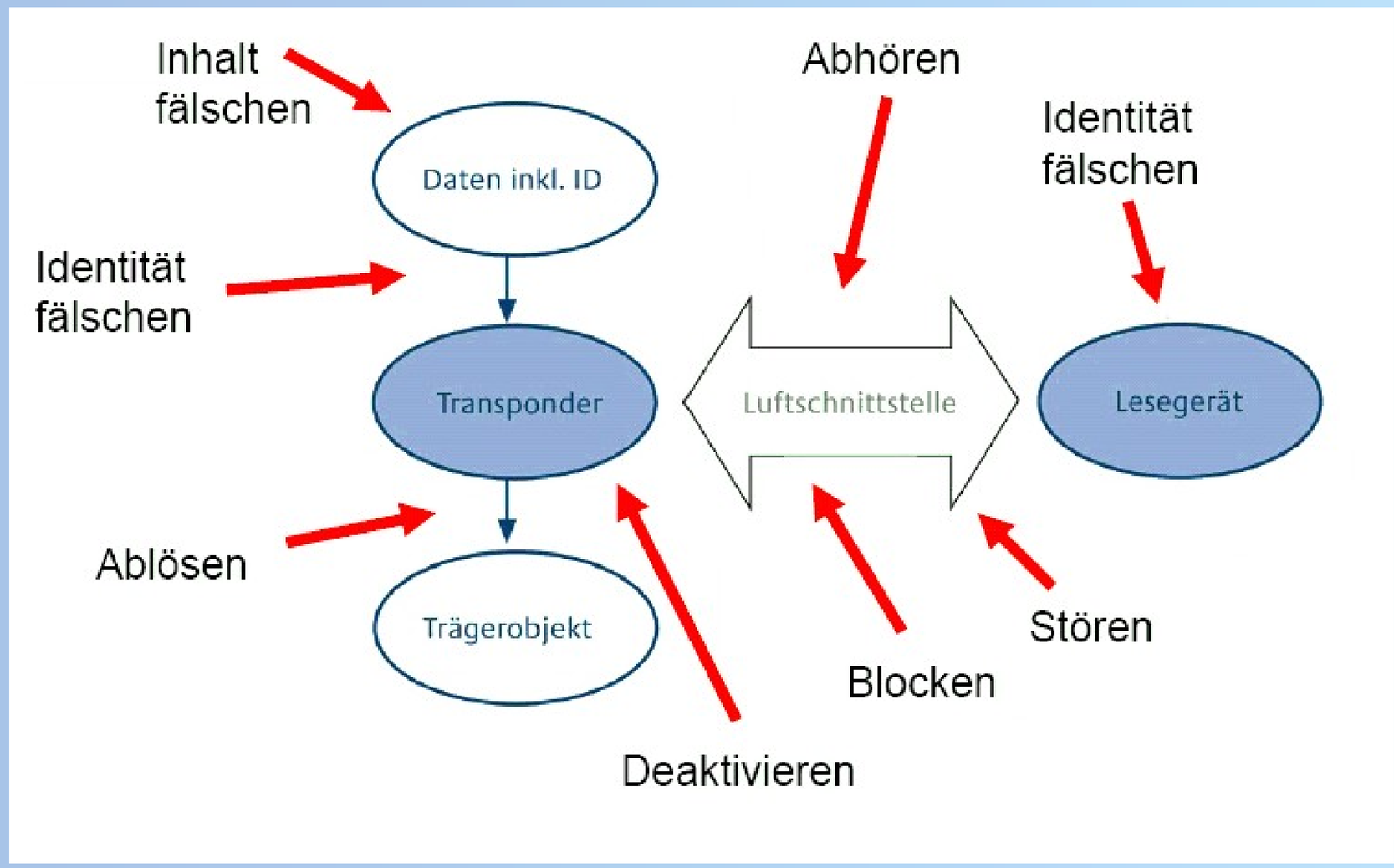


Quele: http://www.bsi.de/fachthem/rfid/RIKCHA.pdf

- Unterscheidungsmerkmale
  - Speichertechnologie
    - Read-only
      + Nur lesbar
      + Variable Informationen über Datenbanksystem möglich (Identifizierung über eindeutige ID)
    - Read-Write
      + Lesbar, schreibbar
      + ROM: EEPROM, Flash EEPROMs (mehrere Byte-KByte)
      + RAM: SRAM, FRAM (Ferroelectric Random Access Memory)

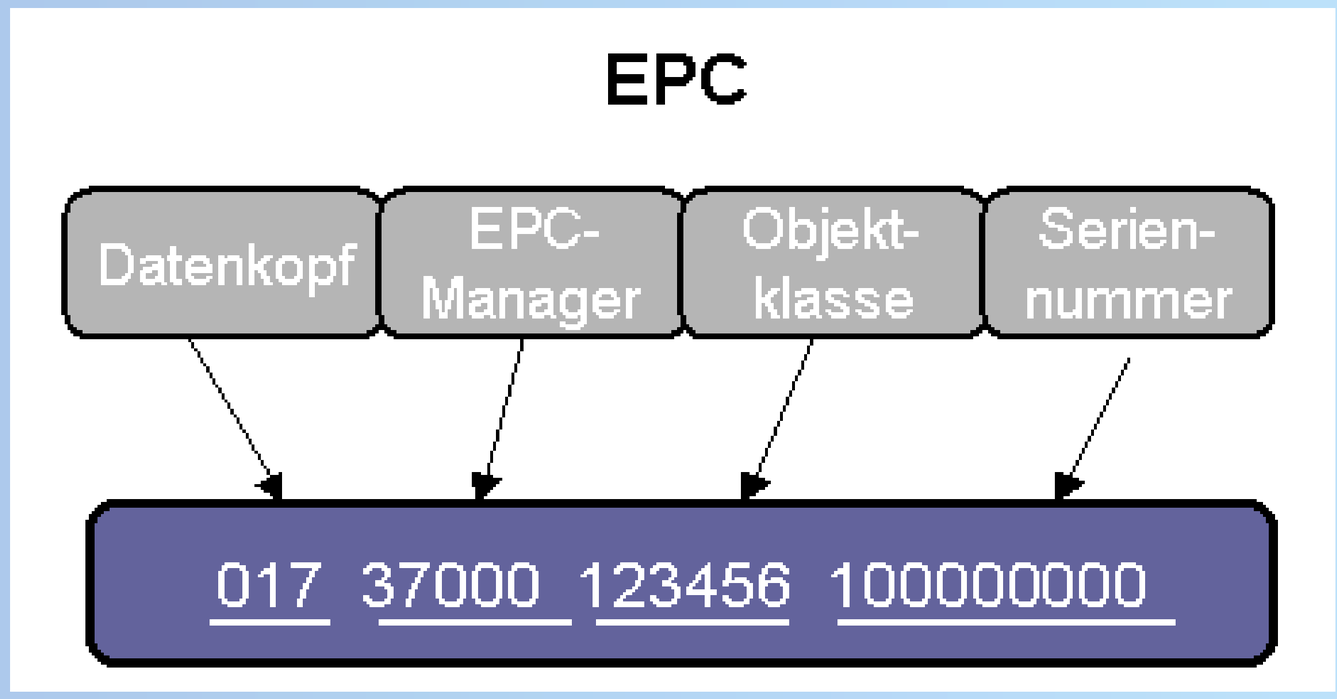
- Angriffe (1)
  - Integrität des RFID Systems beruht auf drei Beziehungen
  - Beziehung zwischen...
    - ...Transponder und gespeicherten Daten (Eindeutigkeit)
    - ...Transponder und Trägerobjekt (Eindeutigkeit)
    - ...Transponder und Lesegerät (Autorisierung)
    -

- Angriffe (2)



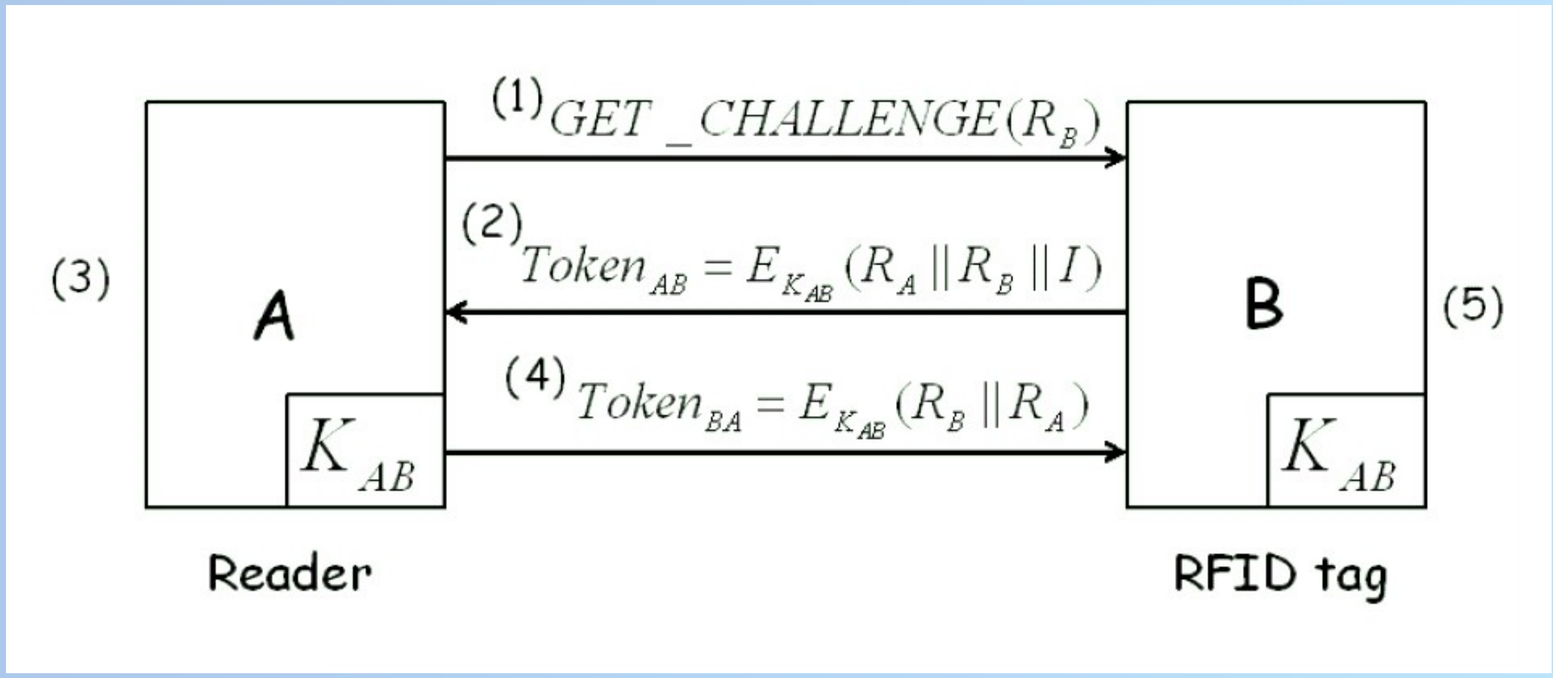
Quelle: http://www.bsi.de/fachthem/rfid/Hilty_BSI_Studie_RFID.pdf

- Schutzmaßnahmen
  - Prüfung der Identität des Tags (1)
    - Weltweit eindeutige Vergabe von IDs für Tags (EPC)



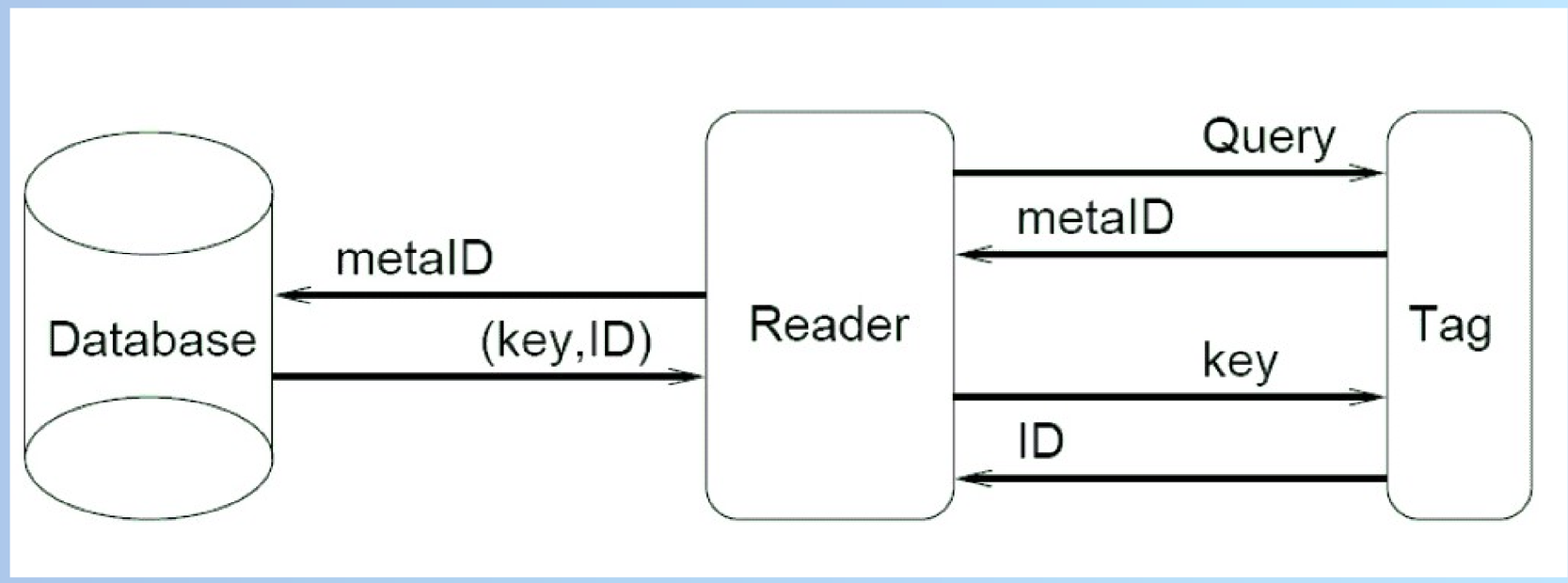
Quelle: http://www.gs1-germany.de/common/grafiken/epcglobal/rfid_epc/aufbau_des_epc.gif

- Schutzmaßnahmen
  - Prüfung der Identität des Tags (2)
    - Authentifizierung durch Challenge-Response-Verfahren (z.B. Mutual Three Pass Authentication)



Quelle: http://ieeexplore.ieee.org/iel5/9999/32116/01493683.pdf

- Schutzmaßnahmen
  - Prüfung der Identität des Lesegeräts
    - Passwortschutz
    - Hash Lock



Quelle: http://rayserv.upb.de/fiff/veroeffentlichungen/rfid.pdf

- Schutzmaßnahmen
  - Verschlüsselung
    - zwischen Transponder und Reader
    - Verschlüsselte Daten im Speicher
  - Abhörsichere Antikollisionsprotokolle
  - Verhindern des Auslesens
    - Blocker Tags, physische Zerstörung, Kill Befehl
  - Umsetzen der „Fairen“ Informationspraktiken in RFID Protokollen

4.Anwendungsbeispiel: Reisepass

- Fakten (1)
  - Seit 1.November 2005
  - Speichert Name, Geburtstag, Geschlecht, Passbild (15 kByte, JPEG)
  - Ab November 2007: Fingerabdruck beider Zeigefinger
  - Zertifizierung durch das BSI in Deutschland
  - Grundlegende technische Spezifikation vom der ICAO (Internationale Zivil-Luftfahrtorganisation) zur Gewährleistung von Interoperabilität von maschinenlesbaren elektronischen Reisedokumenten

4.Anwendungsbeispiel: Reisepass

- Fakten (2)
  - Smart Card Chip P5CD072
    - 24 bit DPTR (16 Mbyte Adressraum)
    - 8051 vollständig befehlskompatibel
    - erweiterter Befehlssatz
    - 160 kByte ROM (Chip OS)
    - 4.6 kByte RAM
    - 72 kByte EEPROM
    - Programmierung über speziellen Assembler/Compiler der Firma Keil
    - 320 μm flach

4.Anwendungsbeispiel: Reisepass

- Fakten (3)
  - Induktive Kopplung: 13,56 Mhz
  - Datenübertragung bis zu 106 kBit/s,212 kBit/s, 424 kBit/s
  - Triple DES Co-Prozessor
  - „FrameXE PKI“ Co-Prozessor (mathematischer Co-Prozessor)
  - Gesamter Speicherzugriff über MMU
  - ...

4.Anwendungsbeispiel: Reisepass

- Sicherheit?
  - statt UID, Random ID
  - Auslesen im Vorbeigehen nicht möglich (!)
  - „Simple Power Analysis“ und „Differential Power Analysis“ nicht möglich
  - Glue Logic
  - Scrambling des gesamten Speichers
  - Dynamische Erzeugung des RAM
  - Keine Veränderung der Daten möglich
  - **Aber:** Klonen von Reisepässen bereits 2006 erfolgreich, Pass auch dann gültig, wenn Chip defekt

5.Ausblick

- „Smart Clothes“
- RFID in der Gesundheitskarte
- „intelligenter“ Einkaufswagen
- „intelligenter“ Kühlschrank
- „intelligente“ Waschmaschine
- …
- …
- …
- Der gläserne Mensch?

Quellen

- http://www.rfid-jounal.de
- http://www.epcglobal.de
- http://www.vs.inf.ethz.ch/res/papers/mlampe-rfid-2005.pdf
- http://page.mi.fu-berlin.de/~ymichel/RFID_article.pdf
- http://www.tecchannel.de
- http://www.bsi.de
- http://www.heise.de
- http://www.rfid-handbook.de
- http://ieeexplore.ieee.org
- http://rayserv.upb.de/fiff/veroeffentlichungen/rfid.pdf
- http://www.taucis.hu-berlin.de/_download/rfid.pdf
- Elektor Magazin - 09/2006, 10/2005, 06/2006
- Schoblick,Robert und Gabriele: RFID, Franzis Verlag