# Sicherheitsrisiken von Transpondern

– Schutzmaßnahmen und Handlungsbedarf –

VDE/ITG Workshop RFIDs
Intelligente Funketiketten – Chancen und Herausforderungen
Darmstadt 15. February 2005

Prof. Dr. Hartmut Pohl
Fachhochschule Bonn-Rhein-Sieg
*ISIS* – InStitut für InformationsSicherheit, Köln

# Radio Frequency Identification

- Identifizierungs- und Markierungstechnik
  für physische Objekte (Waren, Sendungen)
- **Ohne Sichtkontakt**
  Radiowellen: Kommunikation, Energieübertragung
- **Programmgesteuert** (ohne menschliche Interaktion)
- Auslesen und (**Wieder-)Beschreiben**

---

**Barcode**

- nur mit menschlicher Interaktion
- kontaktlos/optisch - notwendige Sichtverbindung
- kontaktgebunden

# RFID Beschreibungsparameter

- Stromversorgung
- Reichweite: Frequenz (Dämpfung), Antenne, Sendeleistung
- Zuverlässigkeit, Störanfälligkeit
- Anti-Kollisionsverfahren
- Speicher: Nur-lesen, wieder-beschreibbar. Speicherkapazität
- Verdrateter Zustandsautomat - freiprogrammierbarer Prozessor
- Antwortzeit

# Speicherkapazität mehrdimensionaler Barcodes

## SSCC Composite


# Nutzen, Anwendungen

Markierungs- und Identifizierungstechnologie
für physische Objekte (Waren, Sendungen): ID

- Mess- und Steuergeräte im menschlichen Körper
- Infineon, ...
- VW, Porsche, ...
- Metro, Wal-Mart
- Logistik: Waren
  DoD, Bierdosen, Joghurt, Rasierklingen, CDs, ...
- (Benetton), Gerry Weber, ...
- Zutrittskontrolle, Marathon-Läufe,
- Scheckkarte, Kreditkarte, Kundenausweis, Eintrittskarte
- Inventarverwaltung, Aktenkontrolle, ...

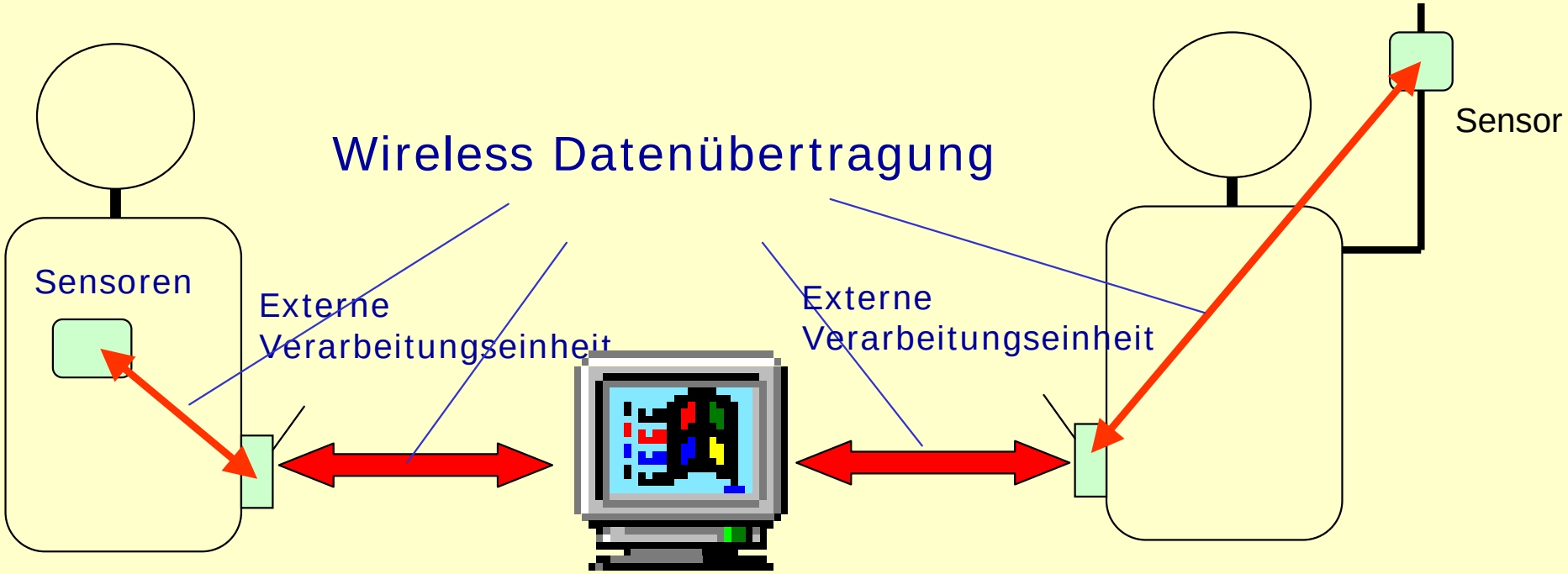
**Fälschungssicherheit?**

# smart shopping

**Anpassung des Preises:** Bierdose

- Jahreszeit, Tageszeit, Wochentag
- Außentemperatur
- Mindesthaltbarkeitsdatum
- Bekannter Biertrinker

# Intra- und extrakorporale Sensoren




Intrakorporale Sensoren:
Augeninnendruck, Glucose ...

Extrakorporale Sensoren:
Temperatur, EKG, EEG, Gewicht ...

# Sicherheitsrisiken von Transpondern

1. Technik und Funktionsweise, Stand der Technik
2. Sicherheitsrisiken: Spionage, Sabotage, Fälschung
3. Schutzmaßnahmen
4. Exkurs: Fälschungssicherheit
5. Technikakzeptanz
6. Handlungsbedarf

# RFID System

tag

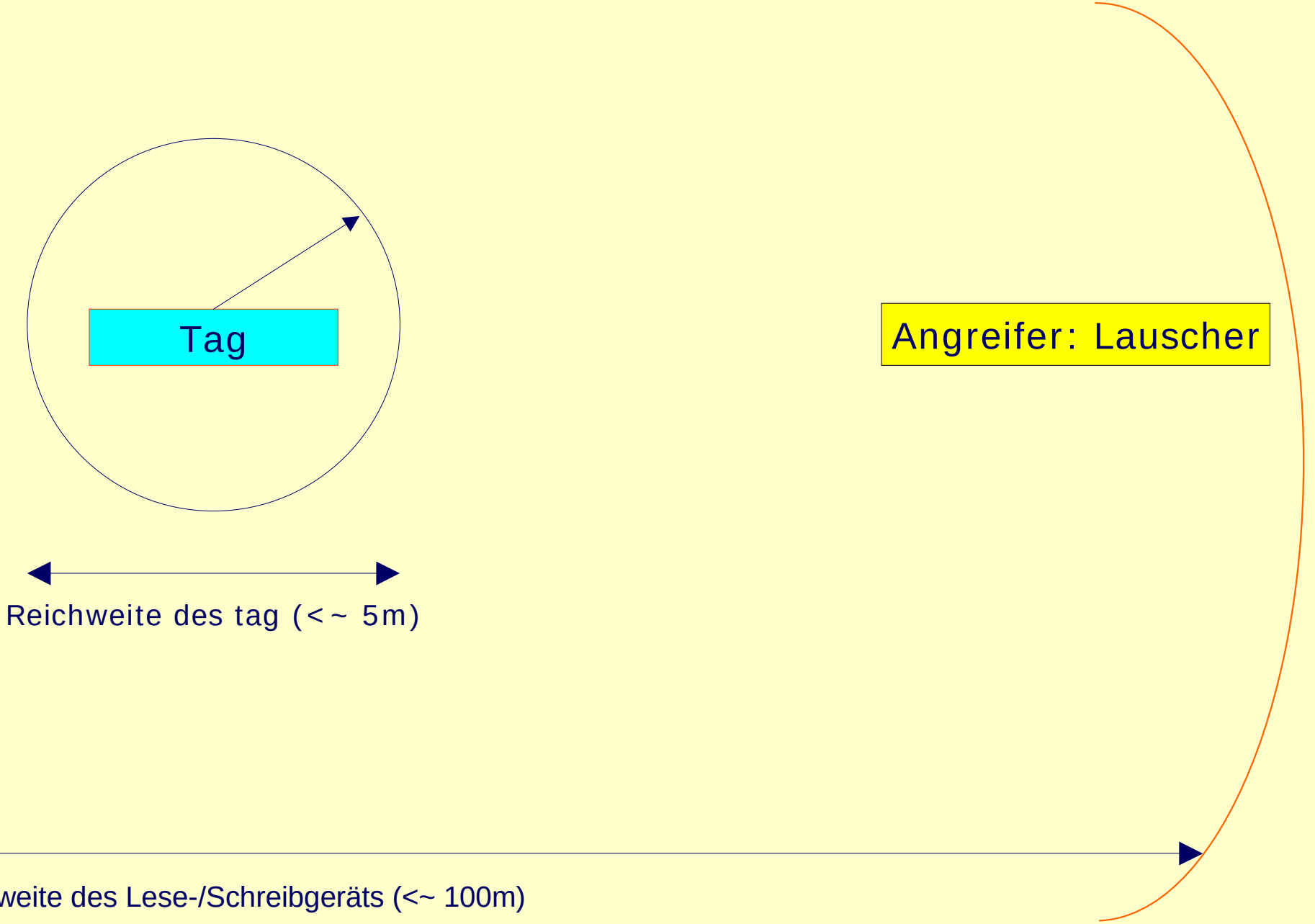
Energy, Clock, Data

Request/
Response

Reader

Application System

# Asymmetric Channels



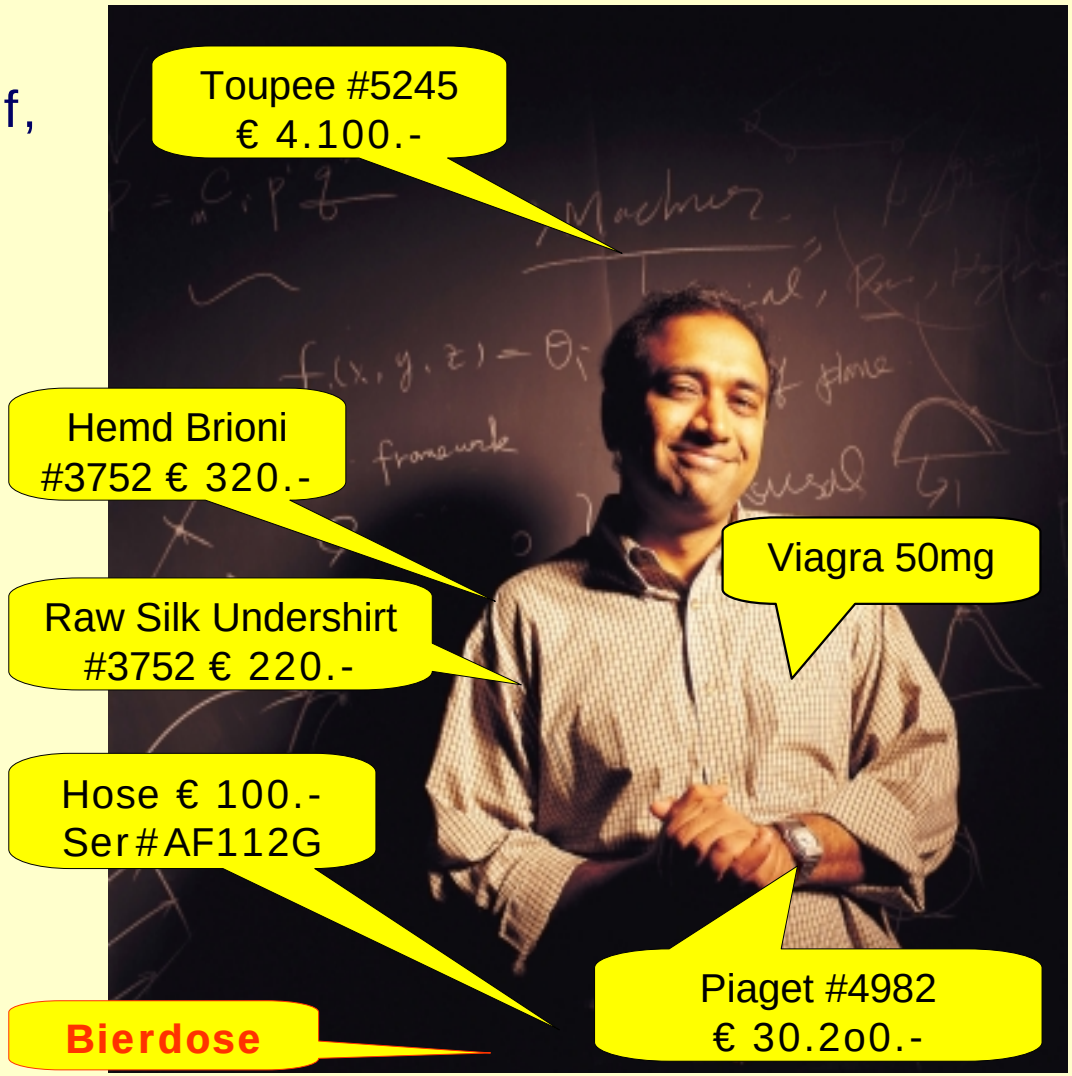
# Szenario: Überwachung, Verfolgung

- Verbraucher, Mitarbeiter - jedermann
- Im Handel, im Geschäft, nach dem Kauf, in getragener Kleidung
- Überall: **Item level tags**
- Verhaltens- und Bewegungsprofile, Einkaufsprofile

**Nicht erkennbar (Verbraucher):**

- Eingebaute/eingewebte Transponder: Personenbezogene Daten
- Schreib-/Lesevorgänge

**Location Privacy**



# Gefühlte Sicherheit

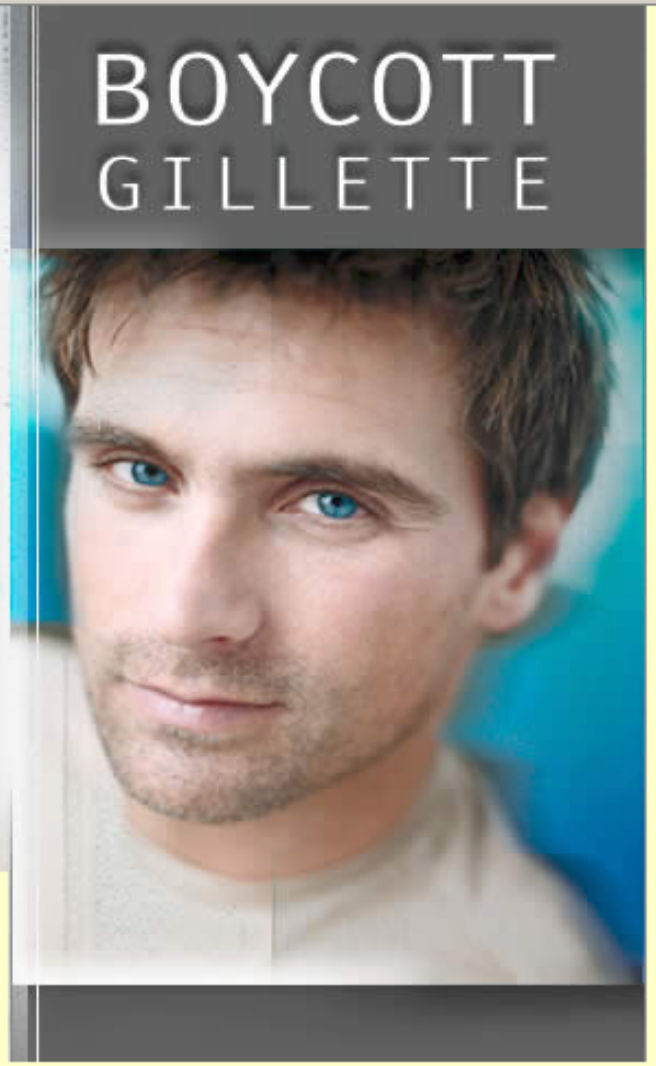
**Befürchtete** Überwachungsmöglichkeiten:
Erhebliche Widerstände breiter Bevölkerungskreise gegen RFID-Verfahren

Verbraucherorganisationen [FoeBud*, C.A.S.P.I.A.N.**]:
Internationaler Boykott

* FoeBud – Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.,

** C.A.S.P.I.A.N. – Consumers against Supermarket Privacy Invasion and Numbering

http://www.boycottgillette.com/


## GILLETTE SNAPS YOUR PHOTO!?!

Hidden cameras in GILLETTE spy shelves take mug shots of people who pick up their products!

Consumers have asked Gillette to stop putting RFID "spy chips" in their products, but Gillette has ignored our concerns.

**Don't let Gillette spy on YOU next!**

**STAY INFORMED**

Enter your email address to receive our newsletter

Subscribe

## WHAT IS RFID?

# Schwachstellen, Risiken

- Auslesen gespeicherter Daten
- Manipulation gespeicherter Daten:
  Verändern, Löschen, falsche Daten speichern
- Mitlesen der Kommunikation:
  - Lesegerät ⇒ tag
  - tag ⇒ Lesegerät
- Stören der Kommunikation; Deaktivierung
- Stehlen, ablösen, zerstören

# Sachziele der Informationssicherheit

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Verbindlichkeit: Gegenseitige Authentizität
- Anonymität, Pseudonymität
- ...

# Sicherheitsmaßnahmen

- Zugriffskontrolle: **Password**

  **Aber:** Brute Force Attack gegen Passwords (Antwortzeit)

- Message Authentication Code (**MAC**)

- **Verschlüsselung**

  - der Kommunikation
  - gespeicherter Daten
  - Anti-Counterfeiting - Fälschungen erschweren
  - **Aber**: Ressourcenbedarf

# Untersuchungen

- Brute Force Attack Passwords ⇔ Antwortzeit 0.07 Sekunden
- Meta–ID (verschlüsselte ID) – Schutz vor Überwachung
- Nenn–Reichweiten

**Aber**: Technische Entwicklung

z.B. Geheimhaltung der Verschlüsselungsschlüssel: Geheime, private. Algorithmen. ⇔ Chipkarte

# Roadmap

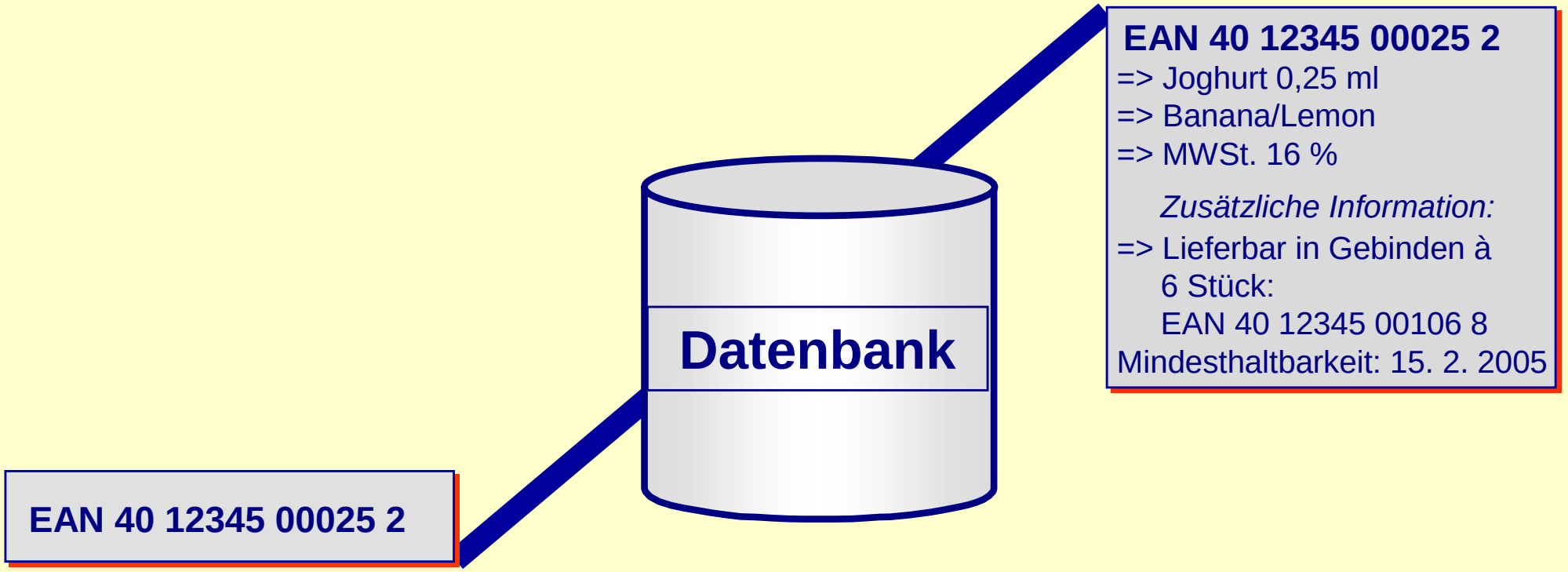
- Ticketing ⇒ Logistik ⇒ Verbraucher
- Ressourcenbegrenzung ⇒ PW, Meta–ID
  ⇒ techn. Entwicklung ⇒ Forschung
- Gefühlte Sicherheit: Null

# Fälschungssicherheit?

# Anforderungen an Techniken zur Fälschungssicherheit

- Wirtschaftlichkeit
- Kompatibilität zum Produkt
- Nachhaltige Sicherheit
- Verbraucherfreundlichlichkeit

# Zuordnung der ID



# Maßnahmen zur Fälschungssicherheit

- Überprüfung der **Authentizität**:

  - **Hersteller**: Labortest - chemische Analyse:
    Wirkstoffe, Zusammensetzung, (geringe, markierende) Beimengungen
    Verpackung: Hologramm, Farbmarkierungen

  - **Verbraucher**: Verpackung:
    Faltschachtel/Blister, Siegel, Druck (Hologramm etc.), lfd. Nummer

  - optische,biologische,chemische und elektronische Verfahren
  - Offene/verdeckte Merkmale

- Überprüfung der Authentizität oder Identität?

- Track & Trace: Identifikationsnummer

- Challenge-Response-Verfahren

- ...

**Clonen der Transponder?**

# Datenschutz-Maßnahmen

Verbraucher können mit erstellbaren personalisierten Einkaufs-, Nutzungs-, Verhaltens- und **Bewegungsprofile** in Geschäften und nach dem Kauf eines Gegenstands überall weiterverfolgt und überwacht werden.

- Für Verbraucher erkennbar markieren
  - In Waren eingebaute oder eingewebte Transponder
  - Schreib-/Lesevorgänge
- Partizipation - keine Rechtebeschränkung
  Recht auf Lesen, Entfernen, Deaktivieren, Zerstören
  Mitspracherecht: Auskunft, Übermittlung, Berichtigung
- Stören: Blocker tag
- Zugriffskontrolle
- Transponder-Lebensweg vollständig regeln:
  Herstellung (Zulieferer) bis zur Entsorgung (ggf. beim Kunden)
- Transparenz:
  Vollständige Information: Verwendung der Daten – Weitergabe

# Auslesen strafbar

§ 202a StGB: Unberechtigtes Auslesen auf Transpondern gespeicherter Information, bei besonderer Sicherung (Zugriffskontrolle, Verschlüsselung).

§ 86 TKG: Telekommunikationsgesetz:
Auslesen der Transponder-ID und der gespeicherten Informationen unzulässig (Abhörverbot)

§ 95 TKG Freiheitsstrafe bis 2 Jahre oder Geldstrafe

# Umfrage zur Akzeptanz

| | % |
|---|---|
| Kennen Sie die RFID-Technik (Transponder)? | 0 |
| Bewerten Sie die Überwachungsmöglichkeiten negativ? | 100 |

# **Vertrauen** (Trust)

## Unverzichtbare Voraussetzung

für die Durchsetzung einer neuen Technik (Anwendung)

## Das Vertrauen der Benutzer

**Verbraucher, Mitarbeiter, Hersteller, Anwender ...**

# Ziel

**Hohes Vertrauensniveau**

**entsprechend dem Barcode und insbesondere der EAN**

# Arbeitsfelder

- **Zugriffskontrollsysteme**
  Berechtigungssystem, Kontrollsystem: Protokollierung von Zugriffen, Erkennung unberechtigter Zugriffe. Meldung bei Kill-Funktion.

- **Low-cost Kryptographie**
  PKI, Hash-Funktionen, Verschlüsselungsverfahren ...

- Trusted Anti-Kollisionsprotokolle

- Fälschungssicherheit mit Transpondern

# 7 Thesen zu RFIDs im Verbraucherumfeld

## 1. Zukunftstechnik

Aktive Unterstützung von Entwicklung, Herstellung und Einsatz: Logistik ...
Nicht schrankenlos: Gesellschaftliche Folgen und Folgen für den Einzelnen?

## 2. Bewertung

- Simulationsstudien
- Datenschutz-rechtliche Erforschung des tag-Einsatzes.

## 3. Beherrschbarkeit durch den Verbraucher

- Differenzierte und granuläre Zugriffskontrolle
- Erkennbarkeit von Transpondern und Lesegeräten
- Erkennbarkeit der Schreib-/Leseprozesse
- Datenschutzregelungen:
  . Benutzerfreundliches Auslesen und Korrigieren gespeicherter Daten
  . Entfernen, Deaktivieren oder Zerstörung
  . Auskunftsrecht

# 7 Thesen zu RFIDs im Verbraucherumfeld

## 4. Gesetzliche Verbote

- Verfolgung von Bürgern
- Zahlungsmittel wie Geldscheinen oder Münzen

## 5. Forschung und Entwicklung

- Einführungs- und Betriebsstrategien (best practice)
- Zugriffskontrolle, Verschlüsselungsverfahren und Verfahren zur Fälschungssicherheit

## 6. Unabhängiges Competence Center

- Verdächtigungen, Befürchtungen, sich entwickelnde/geschürte **Ängste**: Unbeschränkte Überwachungs- und Kontrollmöglichkeiten: Technikakzeptanz ⇔ Technikfeindlichkeit
- Unabhängige Information über Vor- und Nachteile: Verbraucher – Unternehmen.
- Weiterbildungs- und Informationsveranstaltungen.

## 7. Vertrauensniveau

- Europäischen Artikelnummer (EAN)
- Hersteller- und Anwender-Interessen
- Alternative: Ablehnung der gesamten Technik?