RFID Technologie und Implikationen

- **Motivation**
  - Überblick über Anwendungen
    und Funktionsweise der RFID Technologie
  - Einflüsse von RFID auf Privacy
  - Stand der Diskussion zu PET für RFID

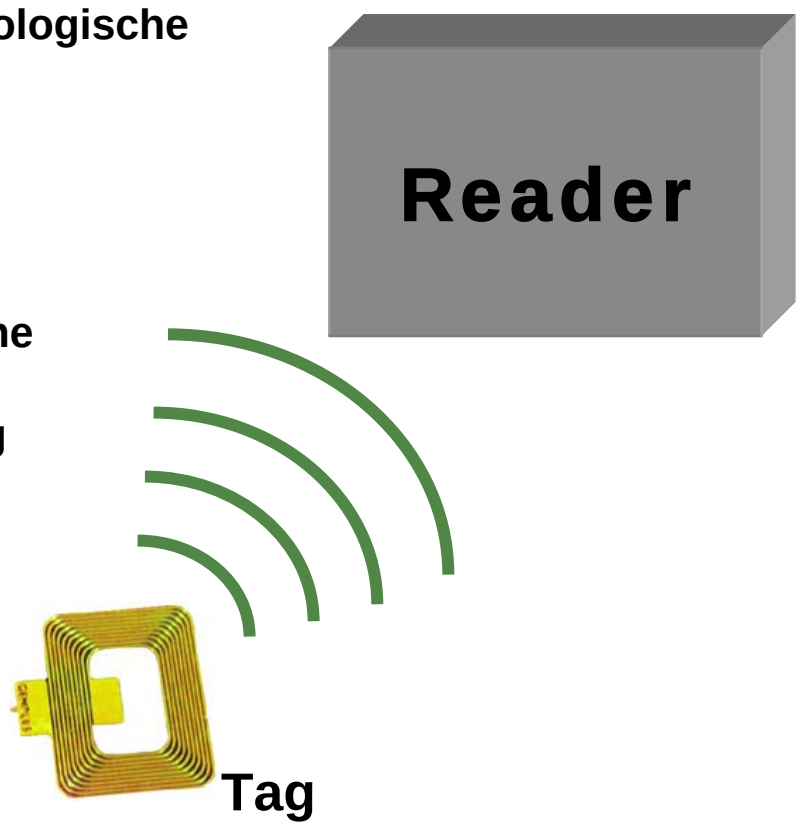
Holger Ziekow
ziekow@wiwi.hu-berlin.de

Inhalt

- **Grundlagen der Technologie**
  - Funktionsweise von RFID
  - Wichtige Tag-Klassen
- **Anwendungen und Infrastruktur der RFID Technologie**
  - RFID im Supply Chain Management
  - Das EPC Netzwerk
  - RFID im Ubiquitous Computing
- **Implikationen der RFID Technologie auf Privacy**
  - Analyse von Bedrohungsszenarien
- **PET für RFID**
  - Schlüsselpunkte zur Prävention
  - Technologien zur Prävention
- **Zusammenfassung**

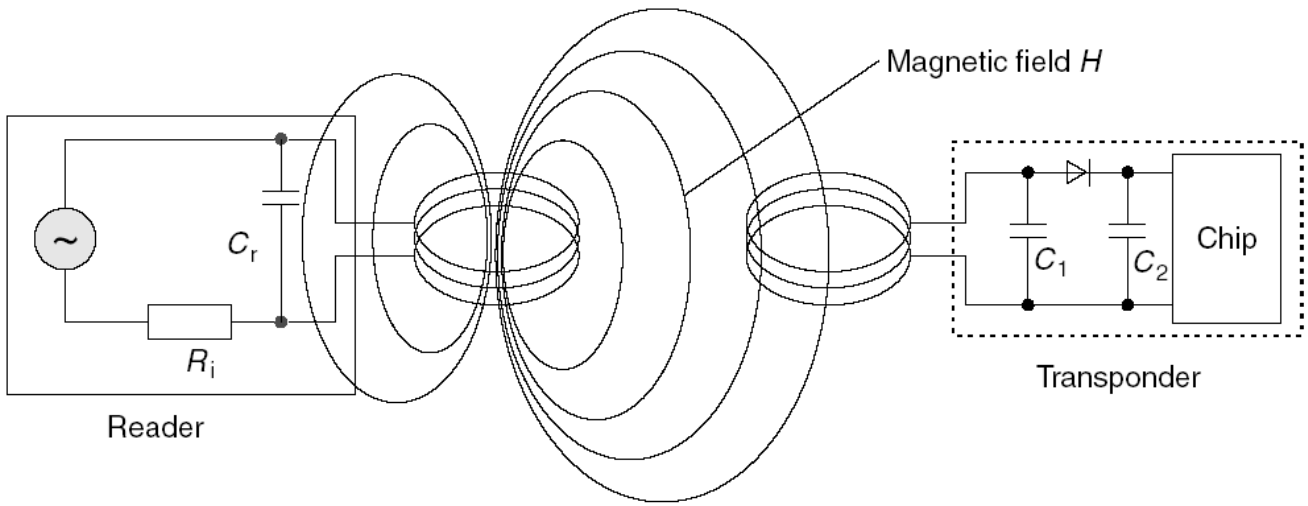
Funktionsweise von RFID

- **RFID steht für Radio Frequency Identification**
- **Mit dient als Oberbegriff für eine technologische Infrastruktur**
  - RFID-Tags
  - Lesegeräte
  - IT-Infrastruktur
- **RFID-Tags sind über Funk auslesbar**
- **Zur Identifikation senden RFID Tags eine Identifikationsnummer**
- **In Abhängigkeit der Energieversorgung wird zwischen aktiven oder passiven Tags unterschieden**



Induktive Kopplung

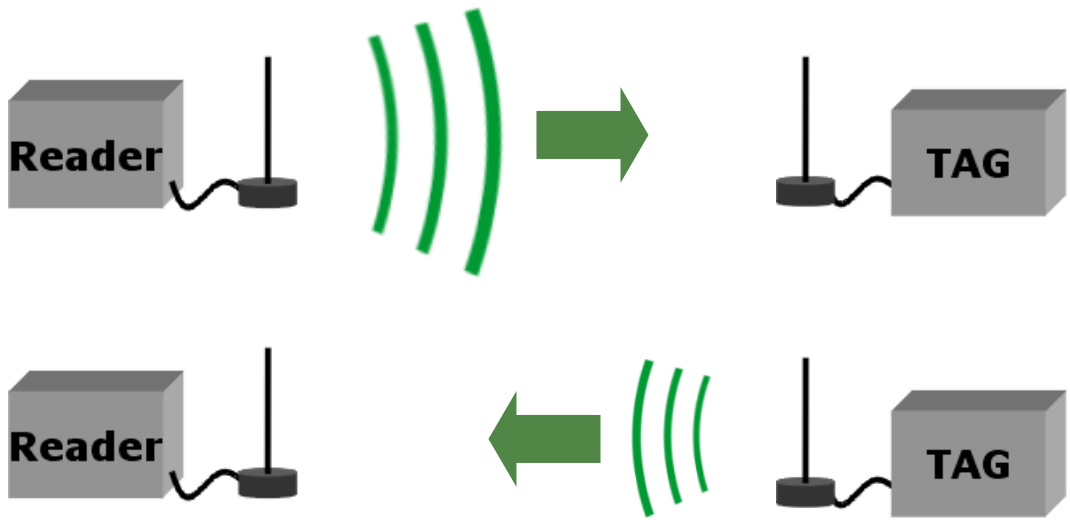
- **Funktioniert im Nahfeld** $\frac{1}{2\pi}\lambda$
- **Arbeitet mit niedrigen Frequenzen**
- **Besitzt eine theoretische Obergrenze für Reichweiten**



Quelle: Klaus Finkenzeller, RFID Handbook

Das Backscatter Verfahren

- **Wird für Kommunikation in Fernfeld eingesetzt**
- **Nutzt mittlere bis hohe Frequenzen**
- **Besitzt keine theoretische Obergrenze für Reichweiten**



Übersicht über Reichweiten

Reichweiten: Passive Tags

Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
6,75 MHz	-	44 Meter	1 Meter	Induktive Koppelung
13,56 MHz	Früher Supply – Chain – Management (Trend geht zu UHF)	3,5 Meter	1 Meter	Induktive Koppelung
UHF (865-928 MHz)	Supply – Chain - Management	unbegrenzt	7 Meter	Backscatter

Reichweiten: Aktive Tags

Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
UHF (868-928 MHz)	Mautsystem (z.B. in Österreich)	unbegrenzt	15 - 30 Meter	Backscatter

Tagklassen

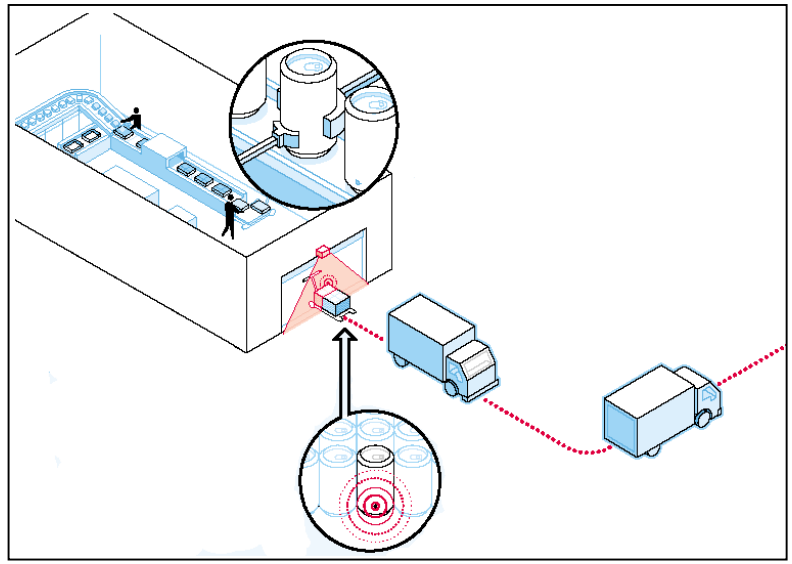
- **In Abhängigkeit der Funktionalität wurden RFID-Tags vom Auto-ID Center in Klassen unterteilt**
- **Passive Tags der Klasse 1 sind gegenwärtig am bedeutendsten**
- **Die Spezifikation für Tags der Klasse 1 befindet sich in Generation 1, wobei die Generation 2 in Arbeit ist**

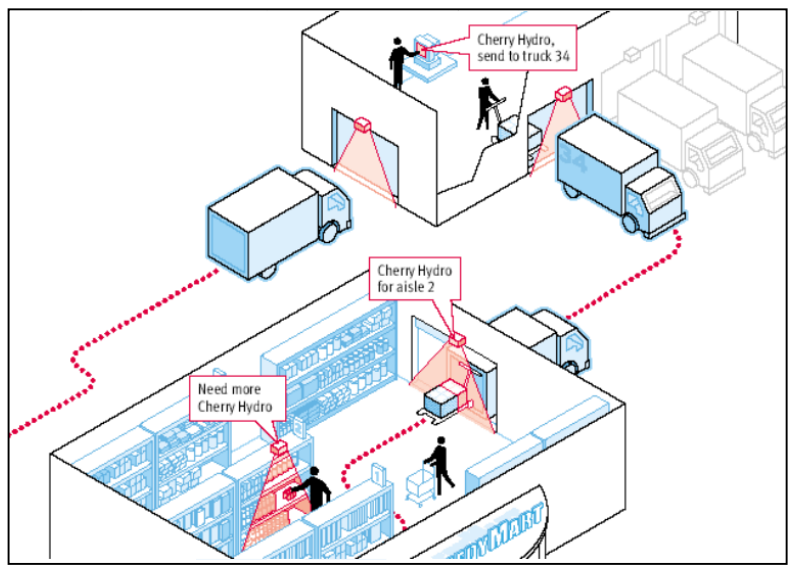
Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

Quelle: Weis, Security and Privacy in Radio-Frequency Identification Devices

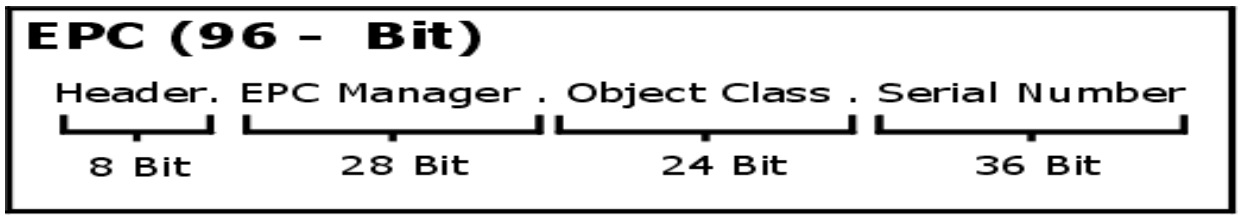
RFID in der Supply Chain

- **RFID erleichtert das automatisierte Auslesen von Produktnummern**
- **Die Produktverfolgung wird vollständiger und leichter**
- **Automatische Informationssammlung ist in neuen Kontexten möglich**
- **RFID ist Wegbereiter für neue Nummerierungsstandards**





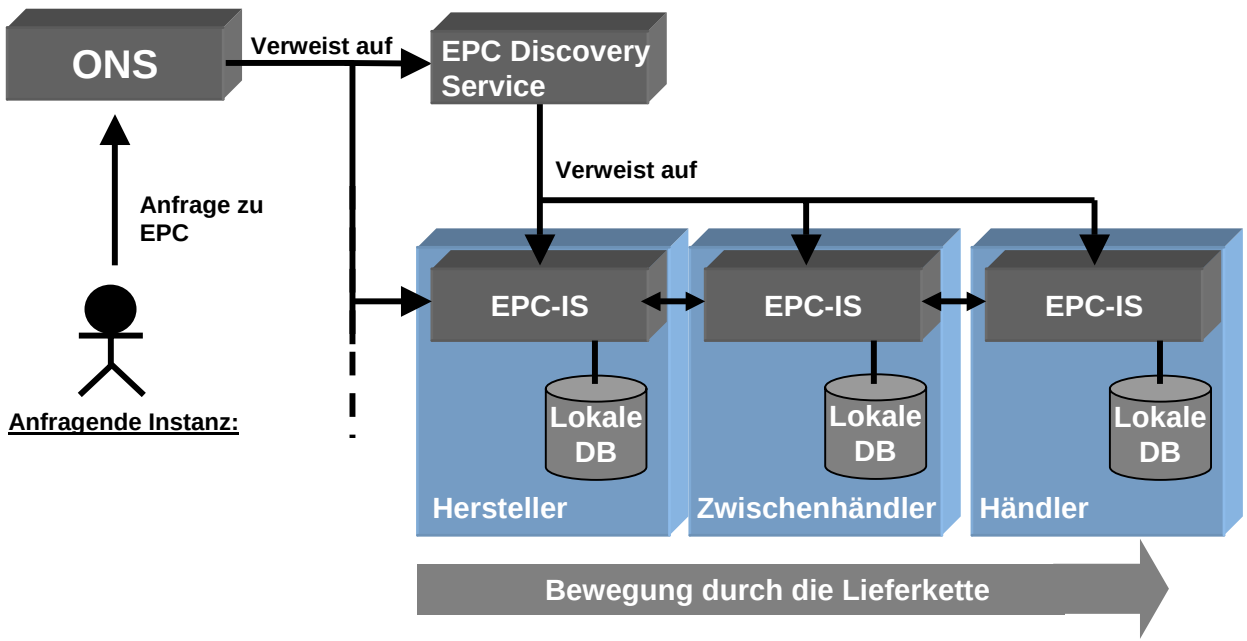
Der Electronic Product Code



- **Weltweit eindeutige Nummer für Objekte**
- **Kann als Primary Key in Datenbanken verwendet werden**
- **Objektspezifische Datenhaltung wird möglich**

Objektdaten im EPC Netzwerk

- **Das EPC Netzwerk soll die Transparenz in der Lieferkette erhöhen**
- **Informationen über ein Objekt werden dezentral gespeichert**
- **Anhand des EPC ist prinzipiell der Zugriff auf alle Stationen des Produktlebenszyklus möglich**
  - Herkunftsgarantien für Lebensmittel
  - Rücknahme/Recycling

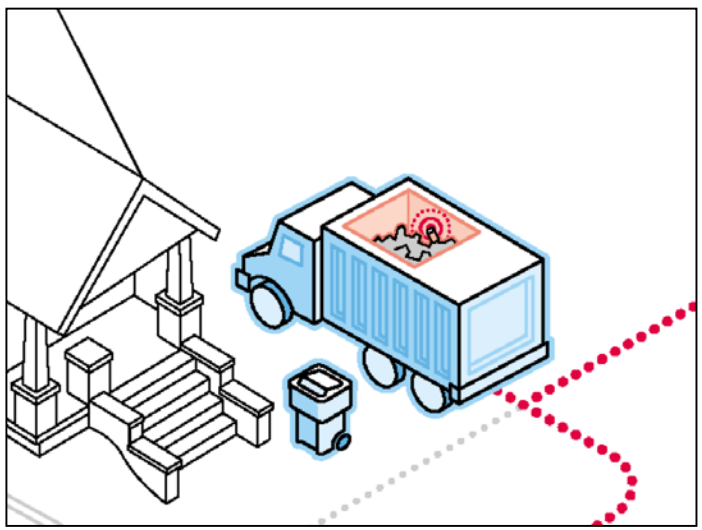


RFID im Ubiquitous Computing

- **PSAs können Einkäufe organisieren**
- **RFID ermöglicht leichten Zugriff auf Produktinformationen**
- **Die Herkunft von Produkten kann individuell nachvollzogen werden**

- **Der Zahlungsvorgang kann durch wesentlich vereinfacht werden**
- **Diebstahlsicherung ist für jedes mit RFID-Tags versehene Produkt leicht realisierbar**

RFID im Ubiquitous Computing



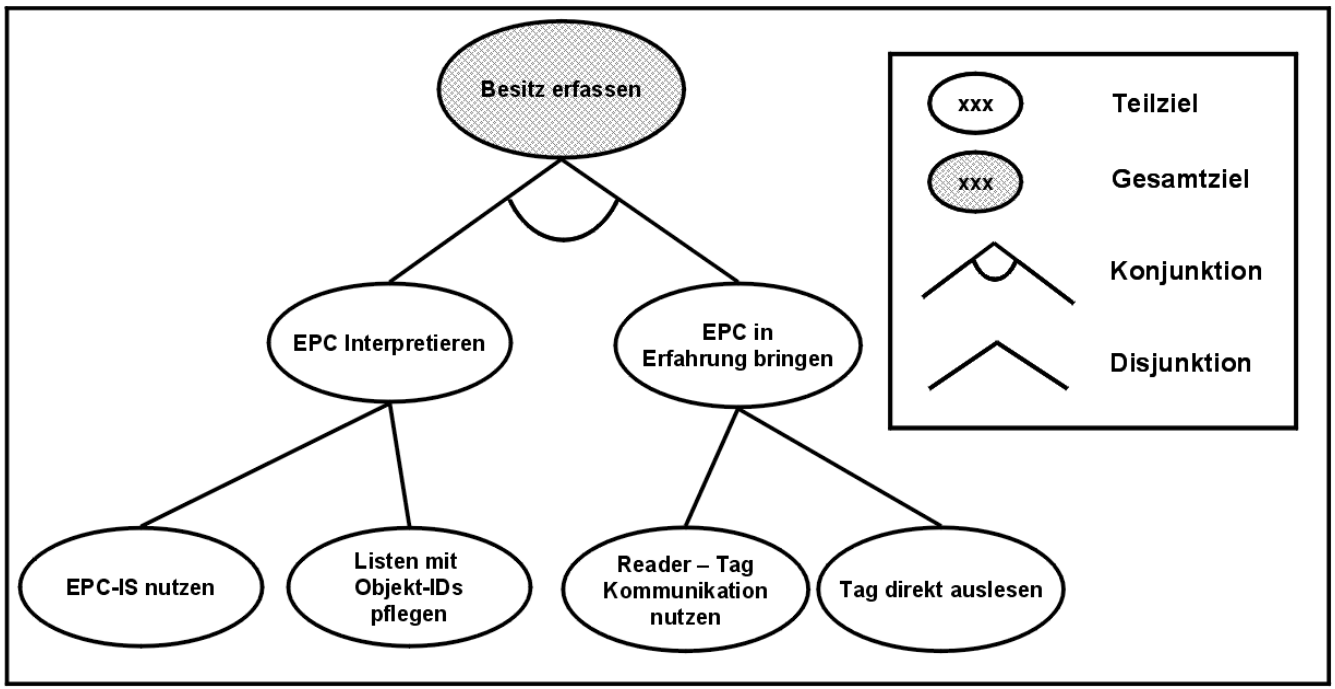
- **Intelligente Kühlschränke, Waschmaschinen, Mikrowellen, Medikamentenschränke etc. könnten gezielt auf Objekte reagieren**
- **Recycling und Müllentsorgung wäre deutlich zu erleichtern**
- **Garantiefälle und könnten ohne Kassenbon behandelt werden**
- **Echtheitsnachweise werden durch RFID erleichtert**

Einflüsse auf Privacy

- **Konfrontiert mit der Technologie entstehen Ängste in der Bevölkerung**
- **Datenschützer weisen auf Probleme in Zusammenhang mit RFID hin**
- **Folgende Szenarien wurden als bedeutend identifiziert:**
  - Unautorisiertes Auslesen von Besitz
  - Tracken von Personen
  - Erweitertes Data-Mining
  - Langfristige Verantwortung für Objekte
  - Ausübung von Verhaltenskontrolle (Technologiepaternalismus)

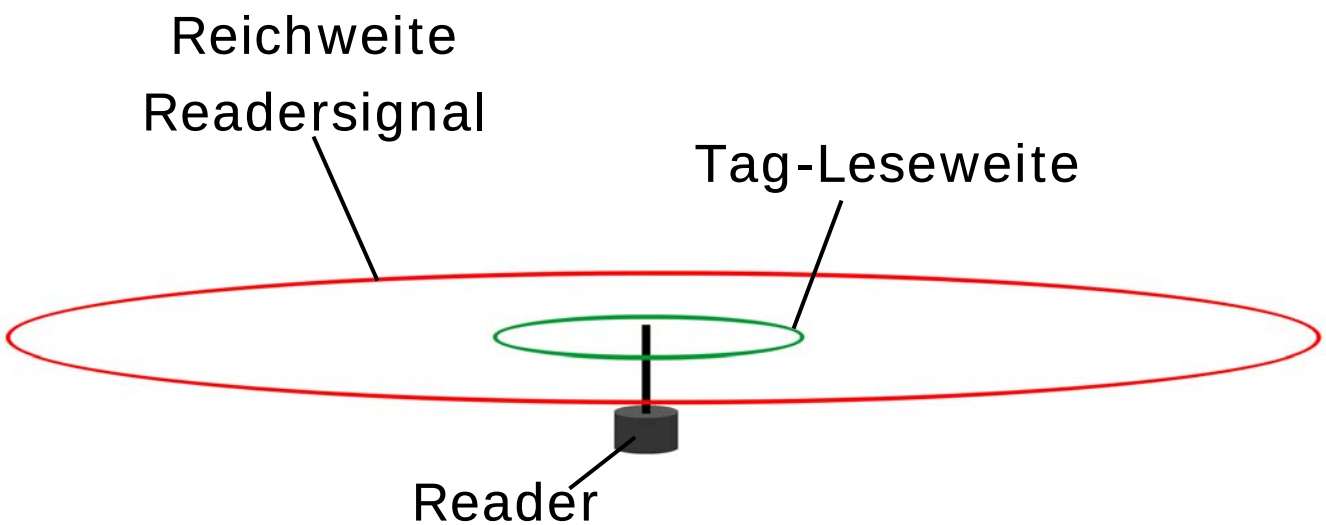
Einflüsse auf Privacy

- **Verwendete Technik: Attack Trees**
  - Beschreibt für einen Angriff notwendige Voraussetzungen (Teilziele)



Abhören des Reader-Signals

- **Informationen aus dem Forward Channel sind aus einer großen Entfernung abhörbar**
- **In Kommunikationsprotokollen der aktuell wichtigsten Tag Klasse (Class 1 Version 1 UHF) werden schützenswerte Informationen über den Forward Channel gesendet**



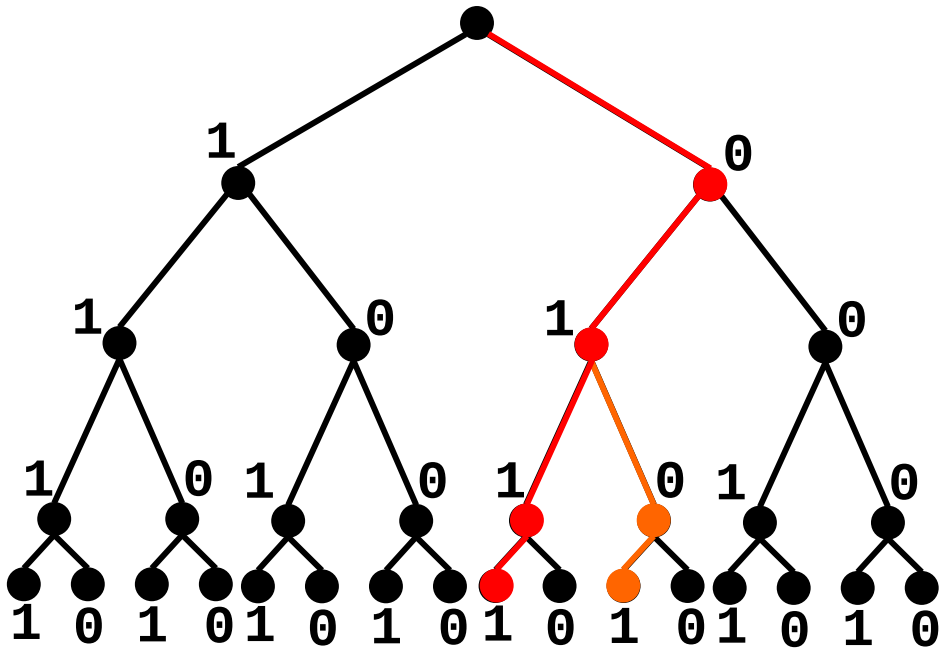
Kollisionsbehandlung

- **Bei Anwesenheit mehrer Tags muss beim Auslesen eine Kollisionsbehandlung erfolgen**
- **Für Class 1 Version 1 (UHF) stehen dazu folgende Befehle zur Verfügung:**
  - **ScrollAllID**
    Argumente: -
    Resultat: Alle Tags antworten mit ihrer ID
  - **ScrollID, PingID**
    Argumente: [VALUE], [PTR], ...
    Resultat: Der passende Tag antwortet mit ID (oder Teilen davon)
  - **Quiet**
    Argumente: [VALUE], [PTR], ...
    Resultat: Der passende Tag geht in einen temporären Ruhemodus
  - **Talk**
    Argumente: [VALUE], [PTR], ...
    Resultat: Der passende Tag kehrt aus dem Ruhemodus zurück

Treewalking

Tag-IDs: A: 0111, B: 0101

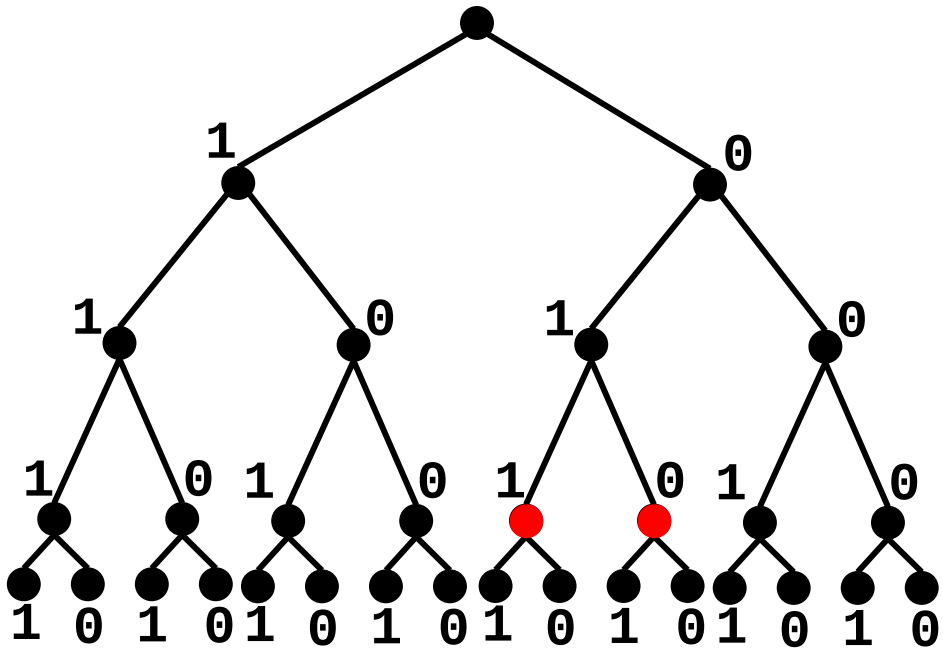
```
Reader: respond if (ID[0] == 0)
Tags responding: A,B

Reader: respond if (ID[1] == 0)
Tags responding: -

Reader: respond if (ID[1] == 1)
Tags responding: A,B

Reader: respond if (ID[2] == 0)
Tags responding: B

Reader: respond if (ID[3] == 0)
Tags responding: -

Reader: respond if (ID[3] == 1)
Tags responding: B
```



Treewalking

Tag-IDs: A: 0111, B: 0101

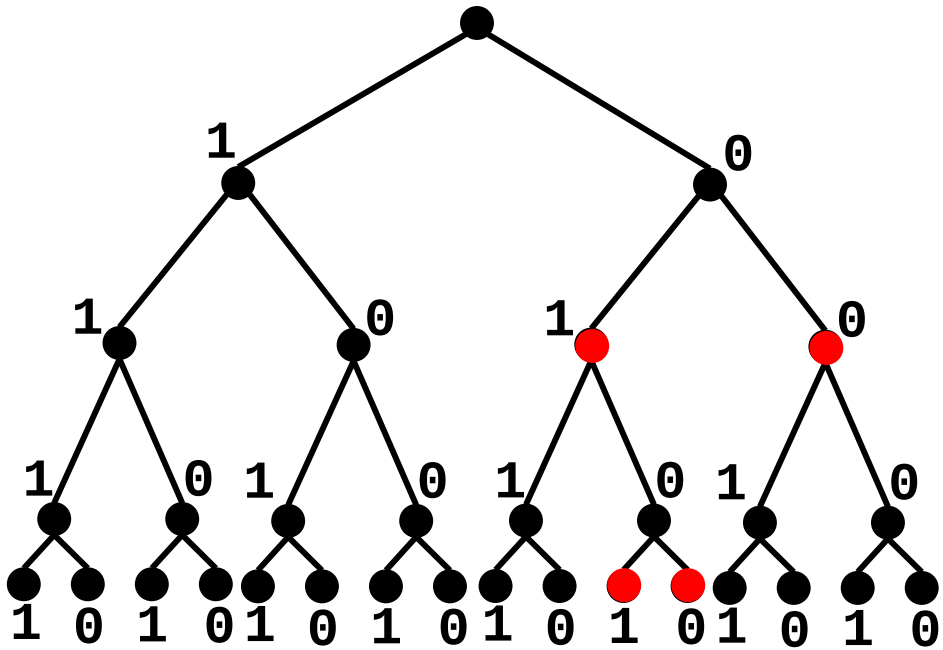
```
Reader: send your IDs
Tags responding: A,B

Reader:be quiet
  if(ID[first_collosions] == 0)

Reader: send your IDs
Tags responding: A
```



Aktiver Angriff zum Erfahren der ID

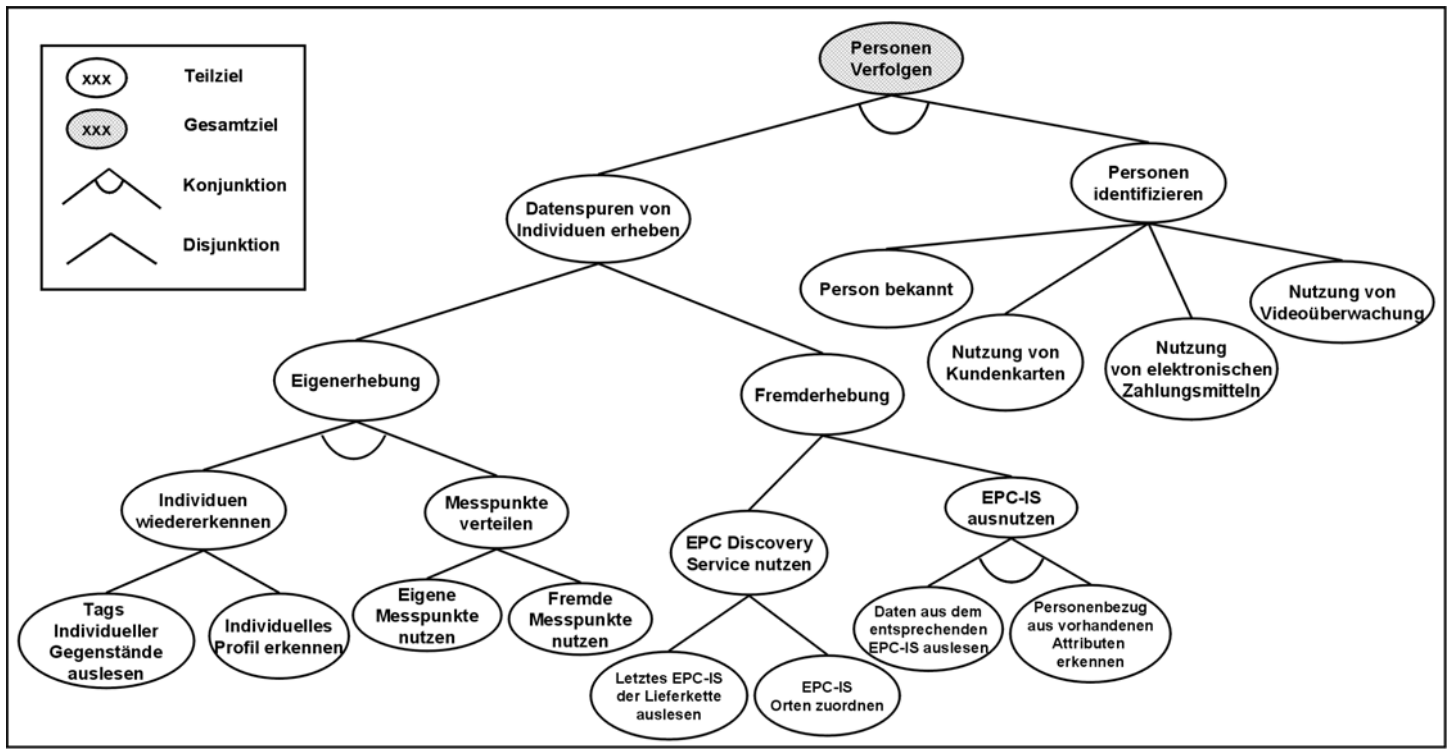
Tag-IDs: A: 0101
Gefälschter Tag: G1: 0000, G2: 0100

```
Reader: send your IDs
Tags responding: A,G1

Reader:be quiet if(ID[1] == 0)
Reader: send your IDs
Tags responding: A, G2

Reader:be quiet if(ID[3] == 0)
```



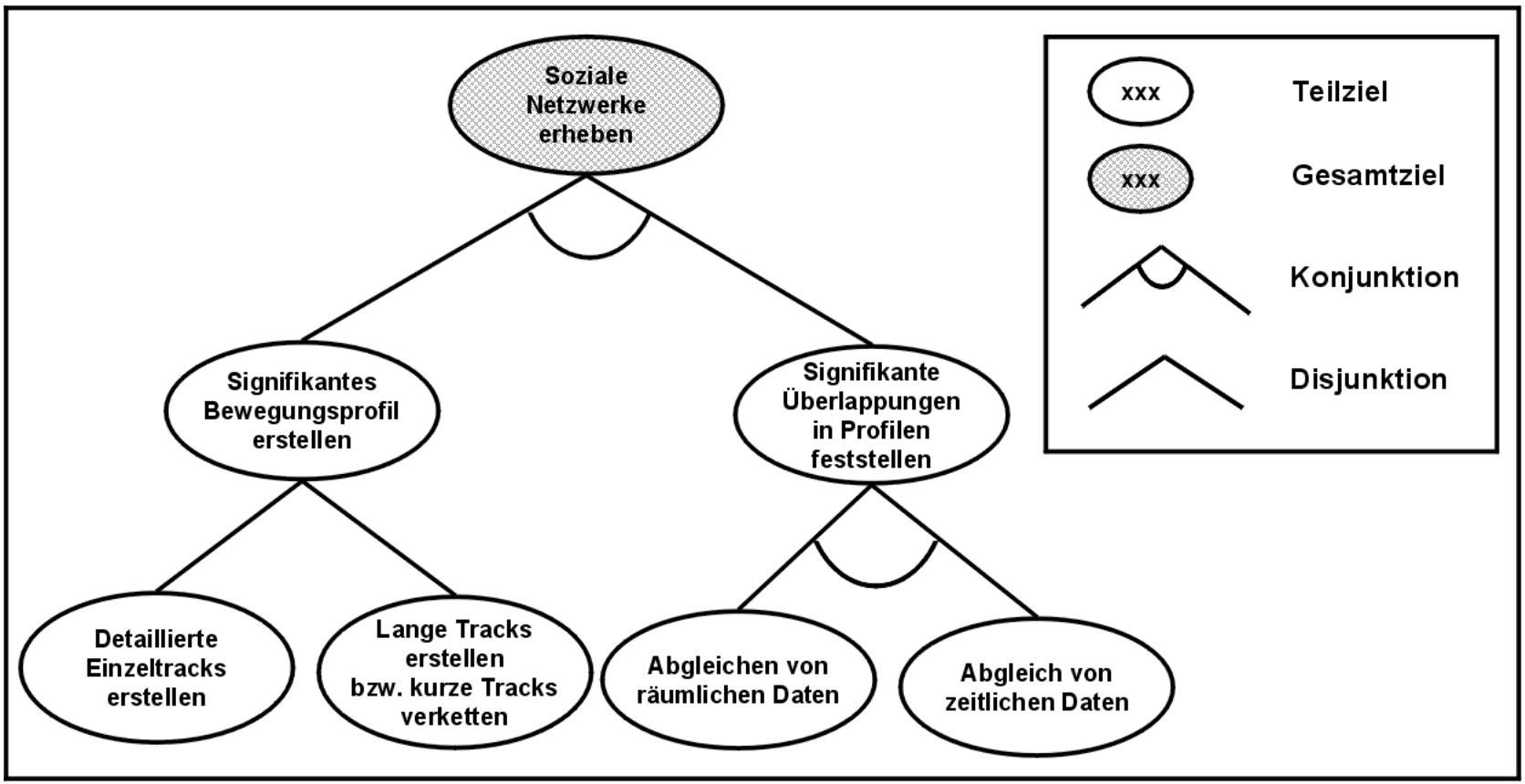
Bewegungsprofile von Personen

- **Nur linke Seite: Pseudonyme Bewegungsprofile durch wiedererkennbare Identifikationsdaten der RFID- Tags**

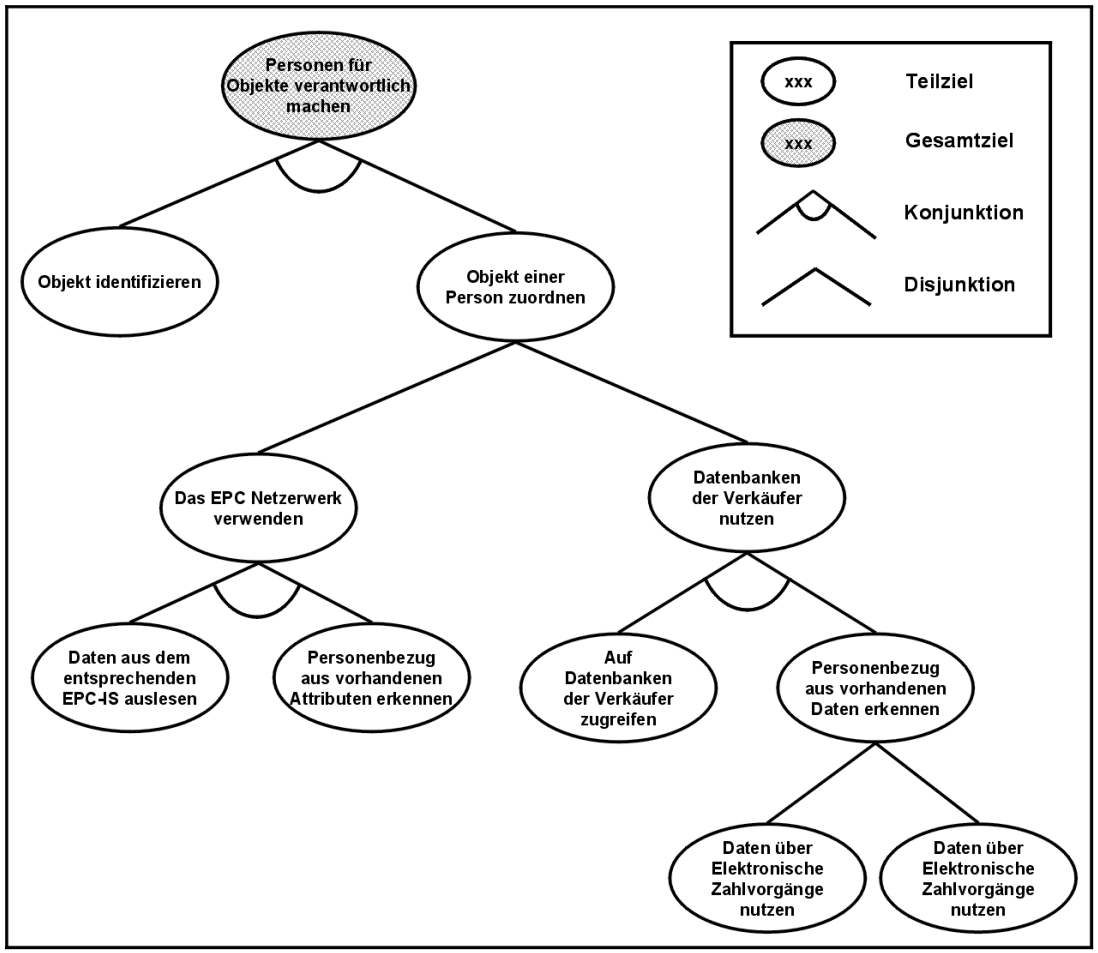


Automatisiertes Erheben sozialer Netzwerke

- **Aus der Analyse gesammelter Daten können weitere Bedrohungen der Privatsphäre entstehen**

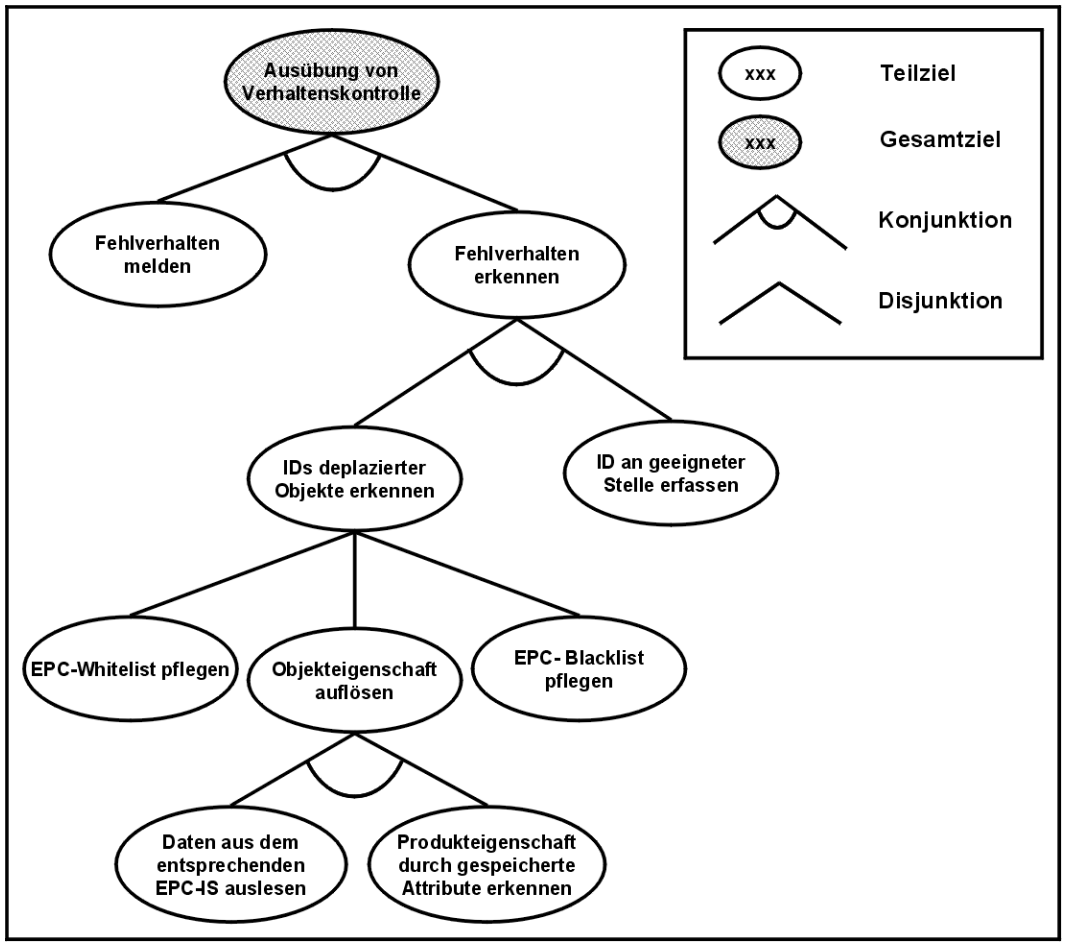


Langfristige Verantwortung für Objekte



- **Die Verwendung von RFID-Tags auf Objektebene birgt die Gefahr einer langfristigen Identifizierbarkeit des Käufers**
- **Vorteile (z.B. bei der Behandlung von Garantiefällen) können in Nachteile umschlagen, wenn der Käufer für das Objekt verantwortlich gemacht wird**

Automatisierte Verhaltenskontrolle



- **Durch RFID wird es möglich, dem Umgang mit Objekten automatisch zu kontrollieren**

7 – Punkte Plan zur Prävention von Angstszenarien

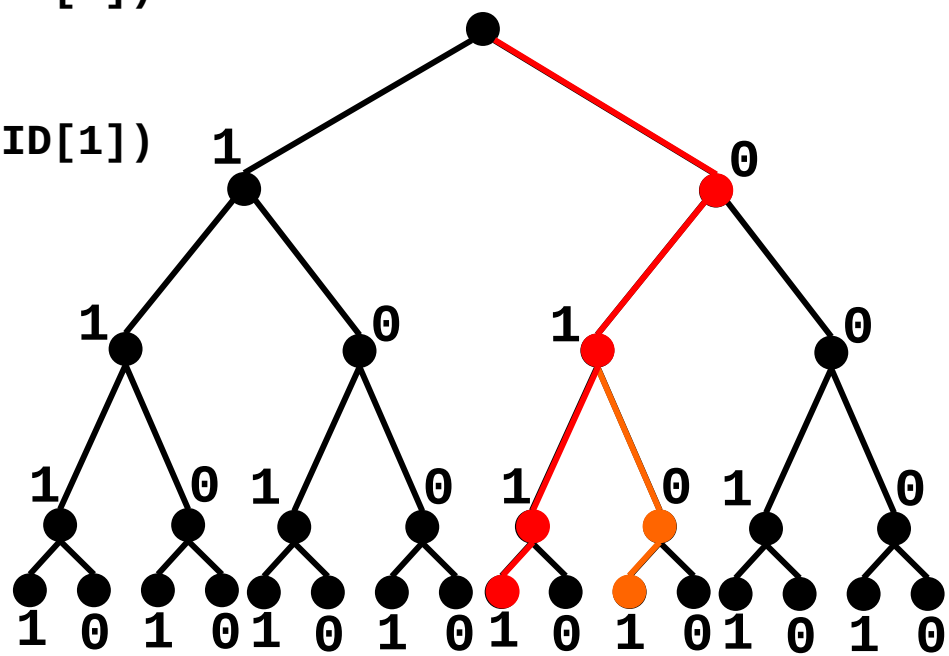
Durch folgende Maßnahmen könnten durch RFID entstehende Bedrohungen für die Privatsphäre eingeschränkt werden.

- **Verwendung sicherer Kollisionsbehandlung**
- **Standardmäßiges Zerstören oder schützen der Tags am Ladenausgang**
- **Minimale Granularität für Tracking-Daten (begrenzte Genauigkeit der Timestamps)**
- **Teilweise oder komplette Löschung der EPC-Nummer**
- **Strenge Kontrolle und transparente Kommunikation der Zugriffsrechte im EPC Netzwerk**
- **Besitzer haben Kontrolle über (persönliche) Informationen, welche zu verkaufen Objekten gespeichert werden**
- **Löschung aller objektbezogenen Daten nach einer Definierten Zeitspanne**

Blinded Treewalking

Bekanntes gemeinsames Prefix Vorraussetzung
Tag-IDs: A: 0111, B: 0101

```
Reader: respond if (ID[1]==0 XOR ID[0])
Tags responding: A,B

Reader: respond if (ID[2]==0 XOR ID[1])
Tags responding: -

Reader: respond if (ID[2]==1 XOR ID[1])
Tags responding: A,B

...
```



Probleme

- **Eingeschränkter Anwendungskontext durch gemeinsames Prefix**
- **Prefix als Geheimnis fraglich**

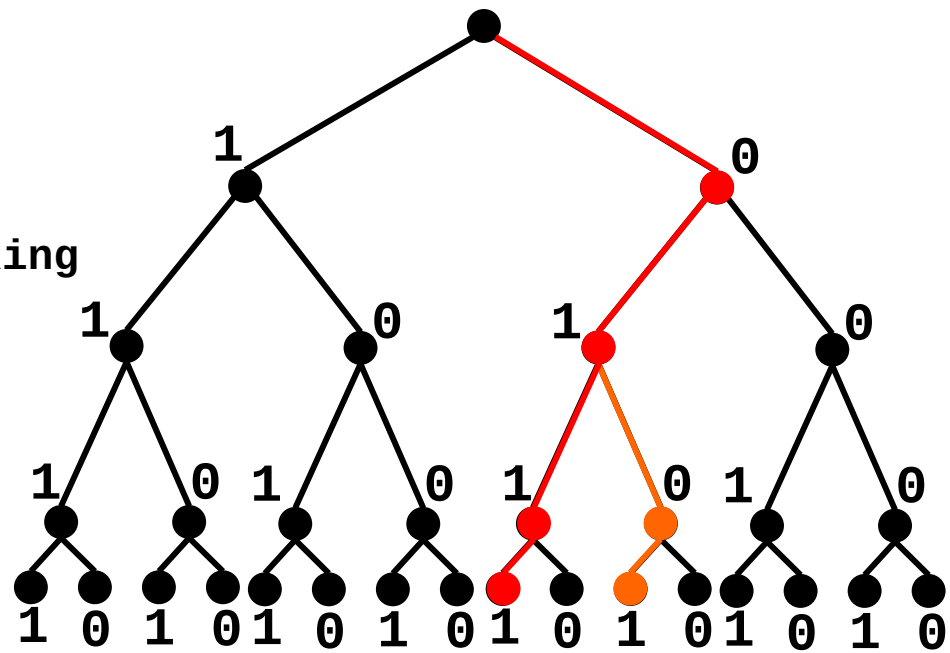
Randomized Treewalking

Bekanntes gemeinsames Prefix Vorraussetzung
Tag-IDs: A: 0111, Arand: 0011, B: 0101, Brand: 1011

```
Reader: respond if (rand[1]==0)
Tags responding: A
...
Reader: respond if (rand[3]==1)
Tags responding: A

Reader: send ID if (rand == 0011)

if (collison) use ID for treewalking
```

Probleme

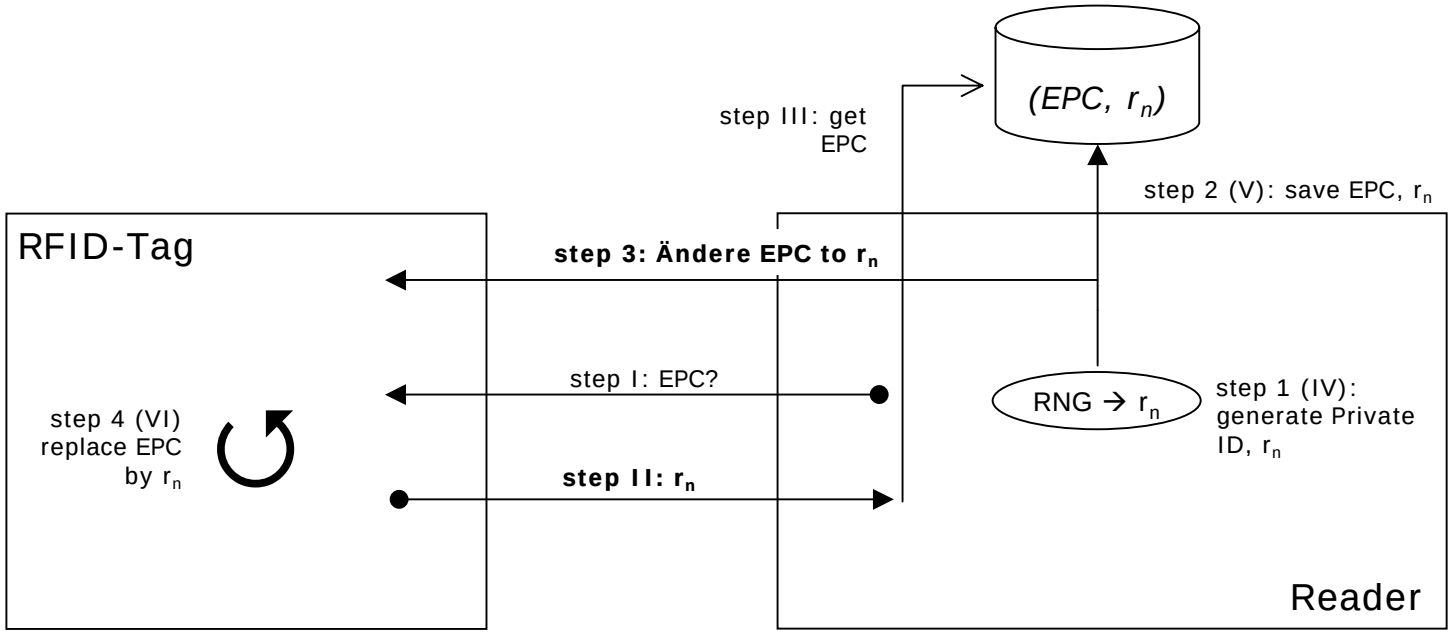
- **Zusatzkosten durch zusätzlichen Speicher und Zufallsgenerator**
- **Spezialfall mit Rückgriff auf ID kann von aktiven Angreifern erzwungen werden**



Der Kill-Befehl

- **In der Spezifikation für Class 1 Tags ist ein Kill-Befehl festgelegt**
  - **`Kill`**
    `Argumente: [VALUE] (ID + Passwort)`
    `Resultat: Permanente Deaktivierung des Tags`
- **Probleme dieser Umsetzung**
  - Nachgelagerte Anwendungen sind nur unter Verzicht auf Schutz möglich
  - Das kurze Passwort ermöglicht die Zerstörung von 20 Tags pro Sekunde
  - Beim Kill-Befehl wird die zu schützende ID über das starke Readersignal gesendet

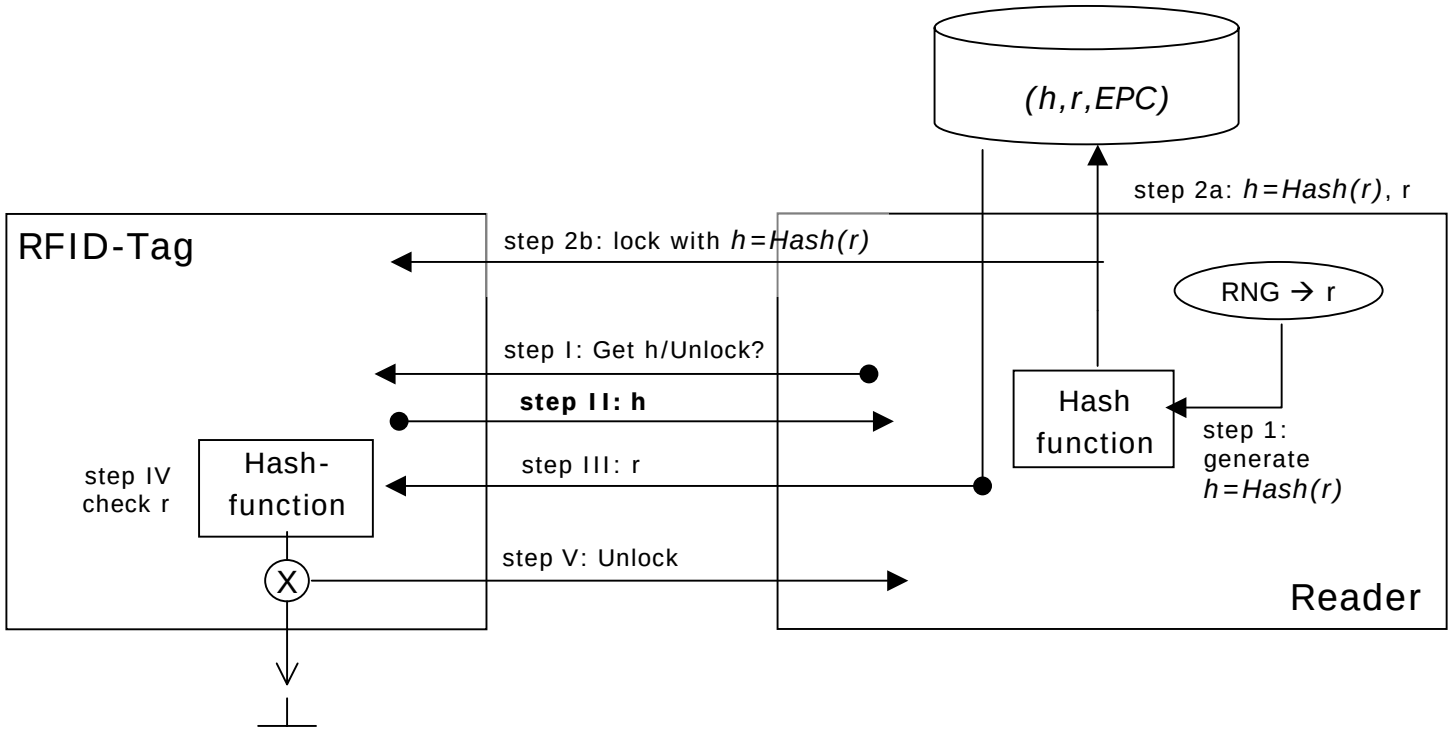
Private ID



+ Preiswert, da keine Kryptofunktionalität auf den Tags

- Kein Schutz vor Manipulation
- Gleichbleibende zufällige ID (r) → Tracking möglich
- Datenbank + vernetzte Reader im Nutzerbereich
- Echtheitsprüfung von Produkten unmöglich
- Starke Einschränkungen für nachgelagerte Anwendungen

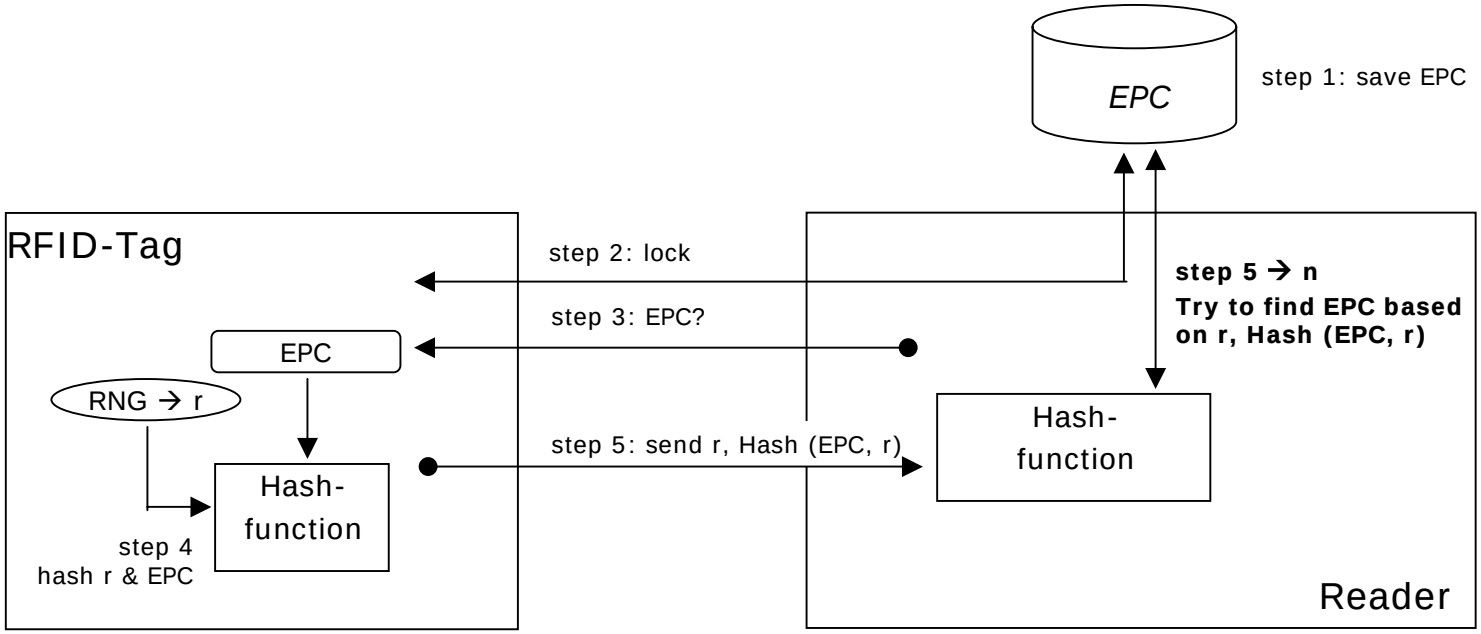
Hash-Look Model (Sarma et al.)



+ Schutz der EPC Daten vor unkontrolliertem Auslesen
+ Echtheitsnachweis möglich

- Gleichbleibende zufällige ID (h) → Tracking möglich
- Hash Funktion auf dem Tag → ca. 20% teuer
- Datenbank + vernetzte Reader im Nutzerbereich

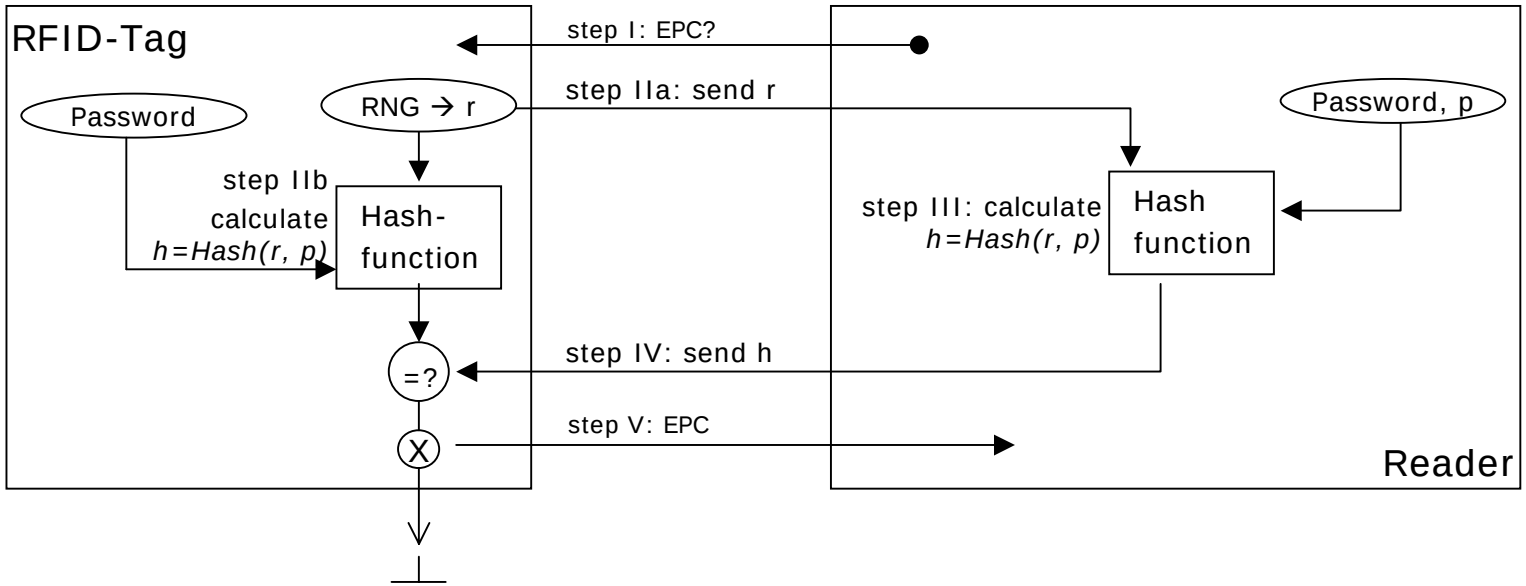
Randomized Hash-Look Model (Weis et al.)



+ Tracking wird verhindert, keine gleichbleibende ID

- Hash Funktion und Zufallsgenerator auf dem Tag → ca. 20% teuer
- Hohe Transaktionskosten, da bei jeder Anfrage alle Einträge der Datenbank durchgerechnet werden müssen
- Einschränkungen für nachgelagerte Anwendungen

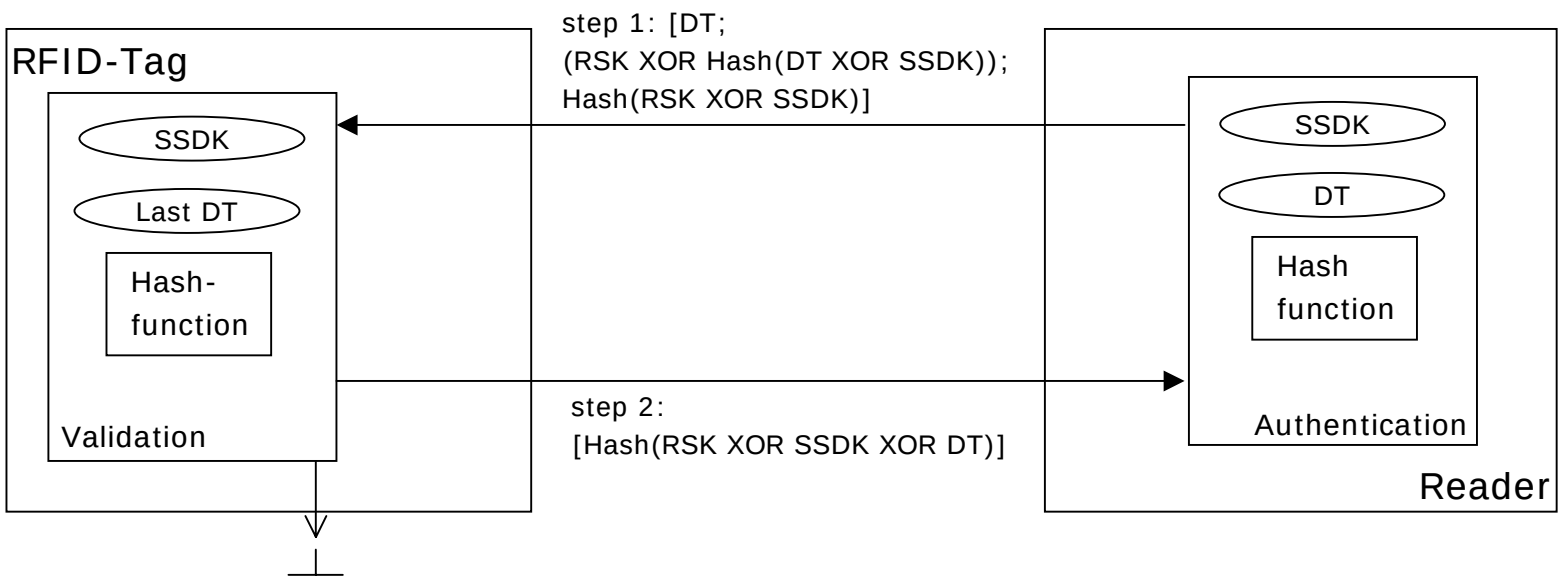
Passwort Model (Spiekermann und Berthold, 2004)



+ Keine gleichbleibenden, verfolgbaren Identifikationsdaten
+ Keine Datenbank, keine Vernetzung der Reader – nur ein Passwort

- Hash Funktion und Zufallsgenerator auf dem RFID-Tag notwendig (nur bei sicherer Passwortverifikation)
- Gemeinsames Passwort: Sobald einmal ermittelt, können alle Objekte eines Nutzers kontrolliert werden

Zero-knowledge Authentication



+ Kann sicher gegenüber Anhören
+ Vermeidet Speicherung des EPC auf dem Tag

- Hash Funktion, Zufallsgenerator und beschreibbarer Speicher auf dem RFID-Tag notwendig
- Nachgelagerte Funktionen stark eingeschränkt
- Aufwand und Sicherheitsrisiken bei der Verwaltung des Geheimnisses (SSDK)

Bewertung von PET für RFID (Henning et al.)

Privacy Checklist bietet Anhaltspunkte zur Bewertung von PET

- **Argumente bedürfen der Gewichtung bzw. sind kontrovers**
- **Granularität der Checklist ist oft zu grob**

- O enforces making sparing use of data?
- O makes privacy the default?
- O transfers control to citizens?
- O sends tags to a secure mode automatically?[5]
- O can prove automatic secure mode activation always works?
- O prevents eavesdropping of communication?
- O protects citizens from producer?
- O protects citizens from retailer?
- O protection includes in-store problem?
- O protects tag against presence spotting?
- O does not rely on active protection means?
- O does not interfere with active protection means?[6]
- O avoids use of central database(s)?
- O avoids use of databases at all?
- O enables functionality after point of sale in a secure way?[7]
- O needs to change RFID technology?
- O makes tags much more expensive?
- O makes tags a little more expensive?
- O additional harm to privacy?
- O additional benefits for privacy?
- O retailer also benefits from concept?

Zusammenfassung

- **RFID hat ein enormes Nutzenpotential**
- **Bedenken in Bezug auf die Privatsphäre sind ernst zu nehmen**
- **Nicht nur die Chips sondern auch die IT-Infrastruktur ist zu beachten**
- **Die Herausforderung ist PET zu entwickeln, welche mit den Anwendungsmöglichkeiten harmonieren**
- **Einige Probleme lassen sich nicht durch Technik lösen und bedürfen gesetzlicher Regelungen oder freiwilliger Selbsteinschränkungen**

Danke für Ihre Aufmerksamkeit

Folien unter http://interval.hu-berlin.de (ab morgen) erhältlich (RFID-Sektion)

Working Paper:
Sarah Spiekermann, Holger Ziekow (2004): "Technische Analyse RFID-bezogener Angstszenarien"

Kontakt:
ziekow@wiwi.hu-berlin.de