



RFID als Technik des Ubiquitous Computing - Eine Gefahr für die Privatsphäre?

Jürgen Müller
Universität Kassel, provet

Matthias Handy
Universität Rostock, Institut MD

U N I K A S S E L
V E R S I T Ä T

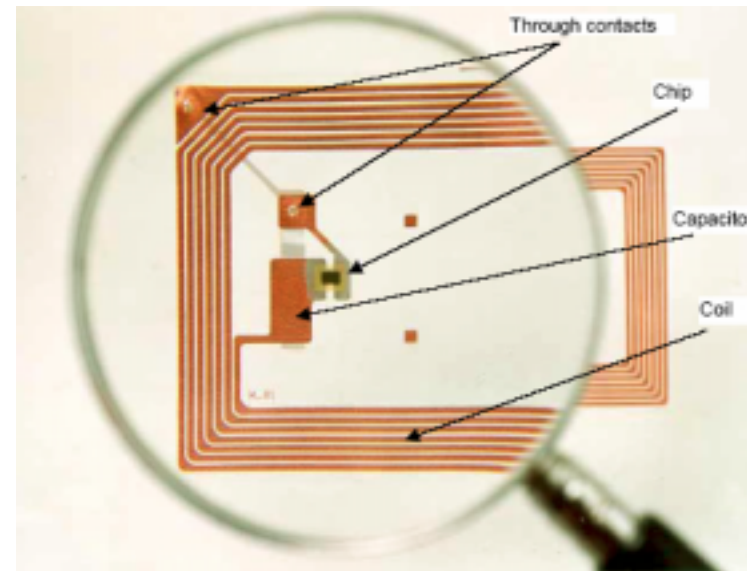
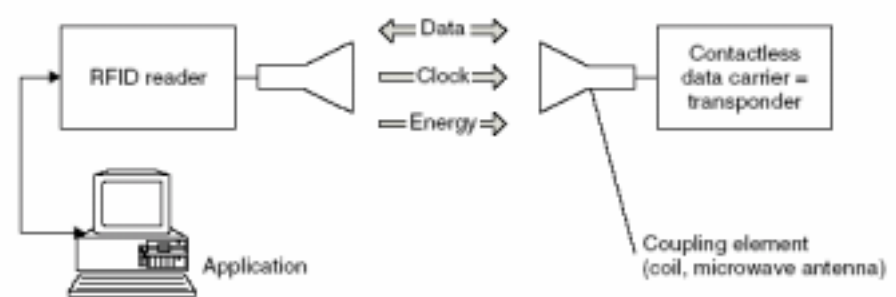


Kurzübersicht

- Anwendungskonstellationen
- Rechtliche Einordnung
- Technikbedingte Möglichkeiten
- Risiken von RFID-Systemen
- Verletzungspotenziale für Rechtsgüter
- Schutzbedarf und Schutzprogramm
- Gestaltungsideen
- Fazit und Ausblick

RFID-Technik und Anwendungsbeispiele

- **RFID-System** bestehend aus
 - Lesegerät
 - RFID-Marke (RFID-Tag)
- **RFID-Marke** bestehend aus
 - RFID-Chip
 - Koppelelement
- Auf der RFID-Marke **gespeichert**
 - Kennung (ID)
 - Sonstige Daten
- **Anwendungsbeispiele**
 - Milchtüte, Kleidungsstück für Wäscherei, Rabattkarte



Quellen:
Finkenzeller, RFID-Handbuch (oben)
TI HFI-Inlays Guide (unten)

Anwendungskonstellationen

#	RFID-Marken ...	Anwendung	
1	... an Gegenständen für die Verwendung durch Dritte	Produkte mit RFID-Marke im Einzelhandel als Kunden-informationssystem	
2	... für Verwendung durch ausgebende Stelle oder Dritte (im eigenen Interesse) bei Ausgabe an den Betroffenen	an Kunden ausgegebene RFID-Marke als Kundenkarte	
3	für interne oder lediglich zweiseitige Verwendung	Stückgut oder Wareneinheiten mit RFID-Marke für interne Logistikaufgaben	

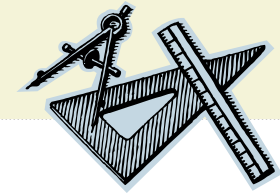
Rechtliche Einordnung

#	TK-Recht	Multimedia-Recht	Datenschutz-Recht	
1	kein TKG, es sei denn bei Kommunikationschnittstelle an fremdem Lesegerät (außer § 89 TKG)	kein TDG für Kennung; TDG für sonstige Daten (sofern Anbieter-Nutzer-Verhältnis und multimedialer Charakter der Daten)	BDSG für Kennung; TDDSG und BDSG für sonstige Daten (aber § 1 Abs. 1 Nr. 1 u. Nr. 2 TDDSG)	
2	kein TKG, außer § 89 TKG	kein TDG für Kennung und kein TDG für sonstige Daten	BDSG für Kennung und BDSG für sonstige Daten (aber derzeit kein §6c BDSG)	
3	kein TKG, außer § 89 TKG	kein TDG für Kennung und kein TDG für sonstige Daten	BDSG für Kennung und BDSG für sonstige Daten	

TKG = Telekommunikationsgesetz
BDSG = Bundesdatenschutzgesetz

TDG = Teledienstegesetz
TDDSG = Teledienste-Datenschutzgesetz

Technikbedingte Möglichkeiten



Technik	Möglichkeiten
Funkschnittstelle	Sichtkontaktlose Kommunikation
Extrem kleine Baugrößen	Unbemerkt Plazieren an und in Gegenständen
Flexible Trägermaterialien	Unlösbar integriert in Gegenstand
Weltweit eindeutige Kennung	Identifizierbarkeit der RFID-Marke
Speicher für sonstige Daten (optional)	Inhaltliche Identität
Einbindung in ein Hintergrund-informationssystem (z.B. ONS)	Unbegrenzte Zusatz- und Kontextdaten über Gegenstand
Kein Ein- und Ausgabemedium außer Lesegerät	Unregistrierbarkeit der Vorgänge
Keine Zugriffsprotokollierung	
Kein Zugangsschutz; Kein Schutz der Daten; Kein Schutz der Kommunikation	Offenliegende Daten und Kommunikation
Geringe Funkreichweite	Überschaubarkeit im Kreis der Reichweite

Risiken von RFID-Systemen



- **Unmerklichkeit**
 - des Vorhandenseins
 - der stattfindenden und erfolgten Datenverarbeitungsvorgänge
- **Keine Kontrolle** bei Verwendung des Gegenstands
- Allgegenwärtigkeit des Einsatzes
- Integration der Datenverarbeitungsvorgänge in das Verhalten und die Handlungen der Betroffenen
- **Kein Entzug** vor den datenverarbeitenden Vorgängen
- Gegenstandsbezogene ...
 - Datenspuren
 - Kontextdaten
- **Wiedererkennbarkeit** des Gegenstands
- Erkennbarkeit und Erschließbarkeit von Mustern
- **Manipulationsgefahr** der offenliegenden Daten und Kommunikation

Verletzungspotenziale für Rechtsgüter



RFID-Systeme sind sowohl Teil eines virtuellen Sozialraums als auch präsent in dem real-körperlichen Sozialraum.

- **Eigentumsrecht**

(Art. 14 GG, Art. II-77 Verfassungsentwurf der EU)

- **Handlungsfreiheit**

(Art. 2 I GG, Art. II-66 Verfassungsentwurf der EU)

- **Brief-, Post-, und Fernmeldegeheimnis**

(Art. 10 GG, Art. II-67 Verfassungsentwurf der EU, Art. 8 EHRC)

- **Informationelle Selbstbestimmung**

(Art. 1 I, 2 I GG, Art. II-68 Verfassungsentwurf der EU)

Schutzbedarf (1)



- **Eigentumsrecht** (§ 903 BGB) und **Besitzrecht** (§ 872 BGB)
 - Entfernen und Deaktivieren aufgrund von Eigentums- und Besitzrecht
 - Aber kein Entfernen und Deaktivieren bei Fremdbesitz (e contrario §872 BGB), weil keine Besitzstörung (§ 858 BGB)
- **technisch-organisatorischer Schutz** (§ 9 BDSG, DSRL 95/46/EG Art. 17)
 - Sicherung der Transponderkommunikation gegen Kenntnisnahme durch Dritte
 - Sicherung vor unbefugtem Zugang und Manipulation

Schutzbedarf (2)



- **Transparenzprinzip** (DSRL 95/46/EG Art. 10, Art. 11 und Art. 12)
 - Wissen um Art und Weise des Einsatzes von RFID-Systemen
 - Wissen um Art und Inhalt der verarbeiteten Daten
 - Wissen um Struktur der datenverarbeitenden Vorgänge (auch Einbindung in ein Hintergrundsystem z.B. ONS)
 - Wissen um Verwendung der Daten
 - Erkennbarkeit der erfolgenden datenverarbeitenden Vorgänge auf RFID-Marke
 - Erkennbarkeit der Kommunikationsvorgänge zwischen RFID-Marke und Lesegerät
 - Erkennbarkeit der Zweckbestimmung der Daten
 - Erkennbarkeit der Adressatenbestimmung der Daten

Schutzbedarf (3)



- **Zweckbindung** (DSRL 95/46/EG Art. 6, Abs. 1 b)
 - Ausschluss der Speicherung und Nutzung von bei der RFID-Marke erhobenen Daten, insbesondere für gewerbliche Verwendung
- **Informationelle Gewaltenteilung** (DSRL 95/46/EG Art. 6, Abs. 1 b)
 - Abschottung von Daten nach ihrer Zweckbestimmung, daher Trennung von Daten in der RFID-Marken-Kennung mit Seriennummerfunktion von Daten mit inhaltlicher Bestimmung
- **Datensparsamkeit** (§ 3a BDSG, DSRL 95/46/EG Art. 6 Abs. 1 c)
 - präventives Gestaltungsgebot gegenüber RFID-Systemen
 - enthält auch Forderung, RFID-Marken als potentieller Gegenstand von Datenverarbeitung deaktivieren oder entfernen zu können

Vorüberlegungen Gestaltung

- **Genereller Schutz vor Auslesen** mit kryptografischen Verfahren bei RFID-Systemen (derzeit):
 - technisch nicht trivial
 - für viele Anwendungen nicht erforderlich / erwünscht
 - Preis / RFID-Marke
- **Schutz vor *unbemerkt*em Auslesen** und/oder Schreiben
 - spezielles Gerät, das Lese/Schreibvorgänge anzeigt ("DataPrivatizer")
 - Log-Funktionalität auf externem Gerät oder auf dem RFID-Marke
 - Zugriffszähler für RFID-Marke-Speicher
 - Selbstauskunft des Lesegerätes
- Problem: **kein einheitlicher Standard**

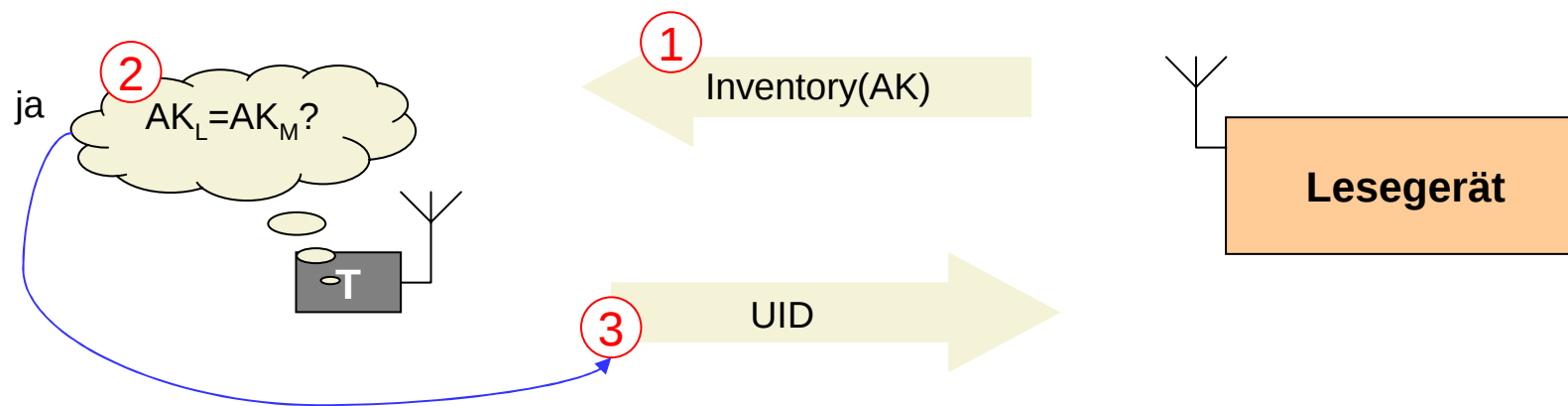
Löschung / Austausch der Seriennummer

- **Eigentumsübergang** von Artikeln mit RFID-Marken
 - bisher vorgestellte Lösungen:
 - Kill-Befehl, Jamming,
 - Blocker-Tag (kein §317 StGB [Störung von TK-Anlagen], aber ggf. Ordnungswidrigkeit nach FTEG*)
- Alternative: **Löschung der Seriennummer, Objektklasse bleibt erhalten**
 - Ersatz der Produktseriennummer durch private (ggf. variable) Inventarnummer
 - Probleme: Verkettung, zielgruppenspezifische Werbung



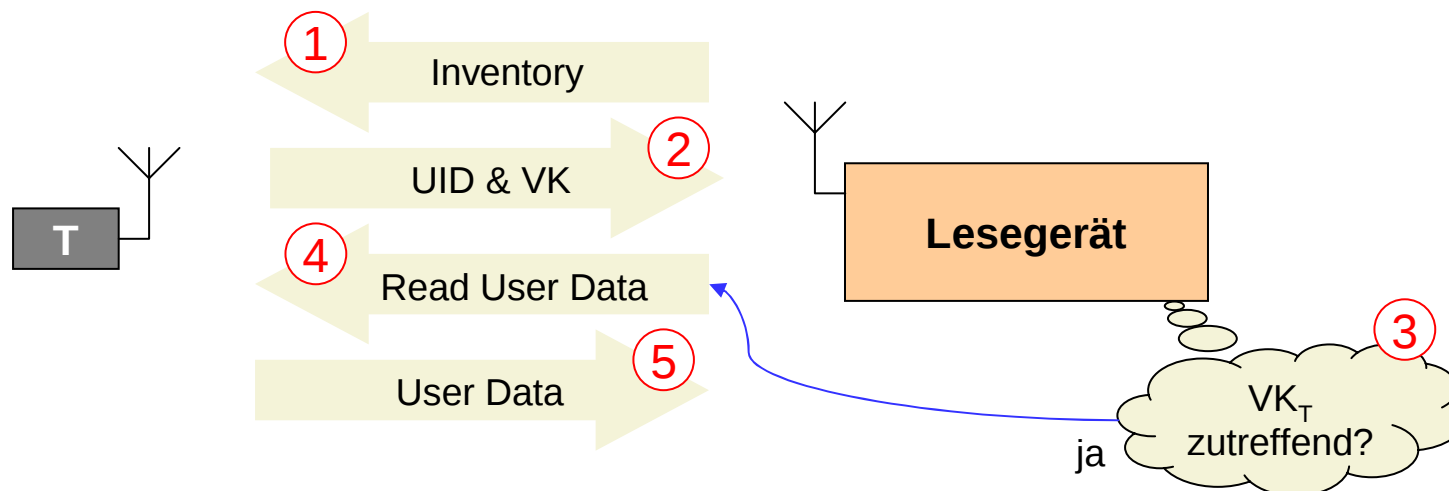
Anwendungskennung (AK)

- **Spez. Speicherbereich** auf RFID-Chip als AK
 - Anfrage des Lesegerätes **zusammen** mit AK
 - RFID-Marke antwortet nur, wenn
$$AK_{\text{Lesegerät}} = AK_{\text{Marke}}$$
 - AK spezifiziert Einsatzfeld des RFID-Marke (z.B. Logistik, Transport)
 - AK sollte **vom Nutzer** gegen Änderungen **gesperrt** werden können
 - Anfrage des Lesegerätes **muss** AK enthalten



Verwendungskennung (VK)

- **Spez. Speicherbereich** auf RFID-Chip als VK
 - VK zeigt Verwendungszweck der Daten an
 - Annahme: Marken-ID allein ist nicht aussagekräftig
 - Lesegerät fragt an → Marke antwortet mit UID und VK
 - Nach Auswertung der VK weiß Lesegerät/Nutzer, ob es zulässig ist, auf der Marke gespeicherte Informationen abzurufen



Fazit

‣ de lege ferenda

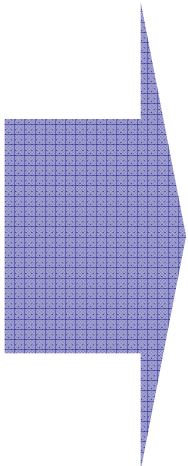
- Erweiterte Transparenzregeln für RFID-Systeme im Multimediarecht
- Erweiterte Transparenzregeln für RFID-Systeme im Datenschutzrecht (Spielraum für Mitgliedsstaaten DSRL 95/46/EG Erwägungsgrund 53)
- Pflicht auf Deaktivierungsmöglichkeit von RFID-Marken
- Pflicht zum Löschen oder Sperren der in Hintergrundsystemen gespeicherten Zusatzdaten

‣ Gestaltung der Technik

- Unterstützung der Transparenz durch VK und AK
- Unterstützung der Zugangskontrolle
- Schutz der auf einer RFID-Marke gespeicherten Daten



- **Kombination von Technik und Recht**
 - gegenüber den Risiken einer Welt des „Ubiquitous Computing“
 - Gewährleistung der zivilisatorischen Errungenschaften
 - wie die in der Verfassung geschützten Rechte
 - mittels Stärkung des Vorsorgeprinzips im Bereich des Multimedia- und Datenschutzrechts (Risikoverwaltung)



**Datenschutz sollte mehr den Gedanken
der **Vorsorge** berücksichtigen, ...**

**... da beim Einsatz von RFID-Systemen
der **Personenbezug** erst später eintritt, ...**

**... dann aber viele **bereits verarbeitete
Daten verknüpft** werden können.**

