



# **RFID: Schnüffelchips für die Überwachungsgesellschaft**

oder geht das auch  
datenschutzfreundlich?

Andreas Krisch <[andreas.krisch@vibe.at](mailto:andreas.krisch@vibe.at)>

[www.edri.org](http://www.edri.org), [www.vibe.at](http://www.vibe.at)

# European Digital Rights – EDRI

---

- Dachorganisation europ. Datenschutz- und Bürgerrechtsorganisationen
- gegründet 2002
- 28 Mitgliedsorganisationen
- 17 europäische Länder
  
- Newsletter EDRI-gram seit 2003
- deutschsprachige Ausgabe seit 2006 auf [www.unwatched.org](http://www.unwatched.org)

# Überblick

---

- Was können RFIDs?
  - Wofür werden sie verwendet?
- Globales Produktinformationssystem
  - Das EPC Global Network
- EDRI Datenschutzpositionen zu RFID
  - Lösungs- und Gestaltungsvorschläge
- EU-Empfehlung zu RFID u. Datenschutz
  - Schritt 2 im gesellschaftlichen Interessensausgleich
- Geht das also auch datenschutzfreundlich?

# Was können passive RFIDs?

---

- Daten speichern
- Daten per Funksignal versenden
- einfache Berechnungen durchführen
- mit Sensoren Umweltzustände erfassen
  
- Einsatz oft nur zum Kennzeichnen mit einer ID
- Datenverarbeitung erfolgt „im Hintergrund“
- Datenübertragung ist für Laien nicht erkennbar

# RFIDs lesen

---

- (günstige) RFIDs
  - senden ihre Daten immer und an jeden
- Lesegeräte
  - lesen alle RFIDs in ihrer Umgebung
  - geben empfangene Daten an Backend-Systeme weiter (Warenwirtschaft, ...)
- Backend-Systeme
  - fragen mit ID Datenbanken ab
  - entscheiden über Datennutzung und -verknüpfung

# Transport & Logistik



- automatische Produkterfassung bei
  - Versand, Transport
  - Lieferung, Lagerung
- Verfolgung von Postsendungen
  - Automatisierung von Verteilzentren
  - RFIDs in Briefkästen
    - ermöglichen End-to-End Verfolgung
    - It. UPU in Saudi Arabien im Einsatz
    - Kommunikationsgeheimnis?

Bildquelle: [www.ndrtv.de](http://www.ndrtv.de)

# Personenverkehr

---



- RFID in Fahrausweisen
  - automatische Fahrt-Erfassung
  - automatisierte Verrechnung
  - zentrale Speicherung von personenbezogenen Bewegungsprofilen
- Praxiseinsatz
  - London: Oystercard
  - Deutschland: Einführungsprojekte

Bildquelle: [www.twl.de](http://www.twl.de)

# Einzelhandel



- Einsatz von RFID für
  - Lagerverwaltung, Regalbetreuung
  - Inventur
  - Diebstahlssicherung
  - Verrechnung
  - Kundenkarten
- Praxiseinsatz
  - Prada, Metro Group, Carrefour, ...
  - Pilotprojekt: Galeria Kaufhof, Essen

Bildquelle: [www.blogrocker.com](http://www.blogrocker.com)

# Ticketing

---



- Einsatz für
  - Personalisierung von Tickets
  - Erhöhung der Fälschungssicherheit
  - Behinderung des Schwarzhandels
  - „Komfortfunktionen“
- Praxiseinsatz
  - Fußball-WM 2006 Deutschland
  - Konferenzen
  - Konzerte, Vergnügungsparks, ...

Bildquelle: [www.tripadvisor.com](http://www.tripadvisor.com)

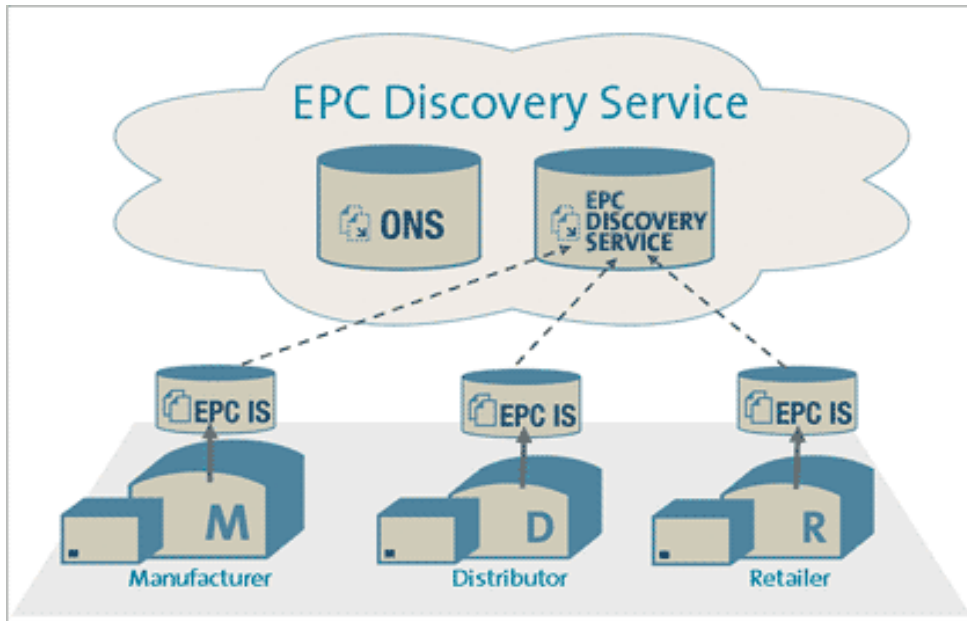
# Gastronomie / Nachtclubs



- Einsatz von RFID für
  - VIP-Kennzeichnung
  - automatische Verrechnung
  - Rabatt-Programme
- Praxiseinsatz
  - z.B. spanischer Nachtclub
  - RFID-Implantate f. Stammgäste
  - Entfernung: nur chirurgisch möglich

Bildquelle: [www.kitekultur.com](http://www.kitekultur.com)

# Das EPC-Netzwerk



Quelle: VeriSign

- Komponenten:
  - Electronic Product Code
    - um Produkte eindeutig zu kennzeichnen
  - Physical Markup Language
    - um Produkte zu beschreiben
  - EPC Discovery Service
    - um Produktinformationen zu finden

# Das EPC-Netzwerk (2)

---

- Electronic Product Code

– z.B.: EPC 01.0037F2.001508.000319F827

Header

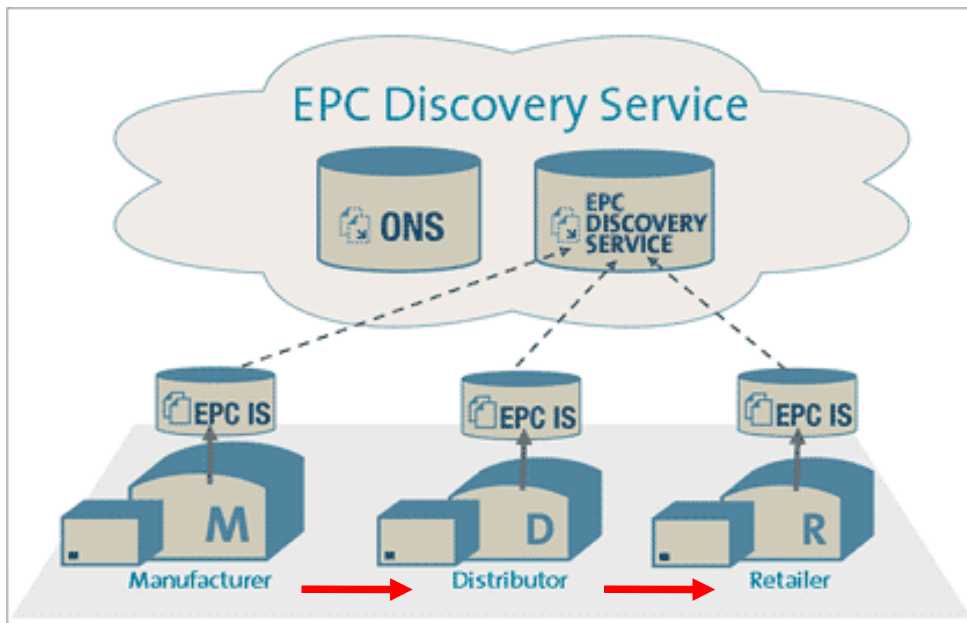
Hersteller-ID

Produktgruppen-ID

Produkt-ID

Potential: je Hersteller mehr Produkt-IDs als jährlich produzierte Reiskörner weltweit.

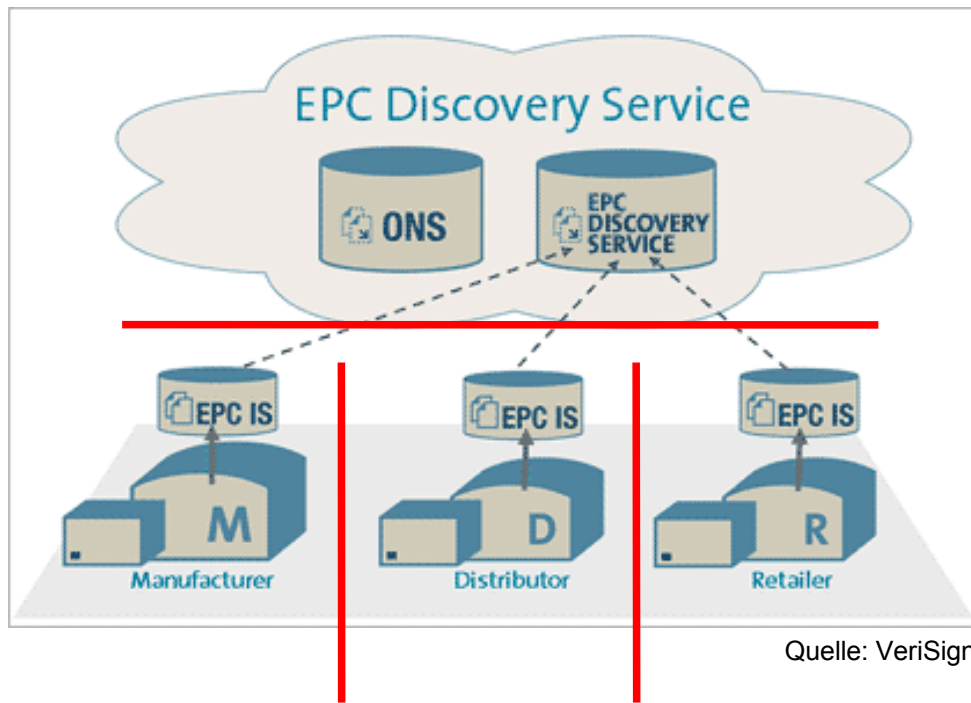
# Das EPC-Netzwerk (3)



Quelle: VeriSign

- Komponenten:
  - Object Name Service
    - Verzeichnis aller EPC-Informationquellen
  - EPC Info Service
    - Informationssysteme, enthalten Daten zu EPCs
  - EPC Discovery Service
    - Verzeichnis aller Informationquellen zu Produkten eines bestimmten Herstellers

# Das EPC-Netzwerk (4)



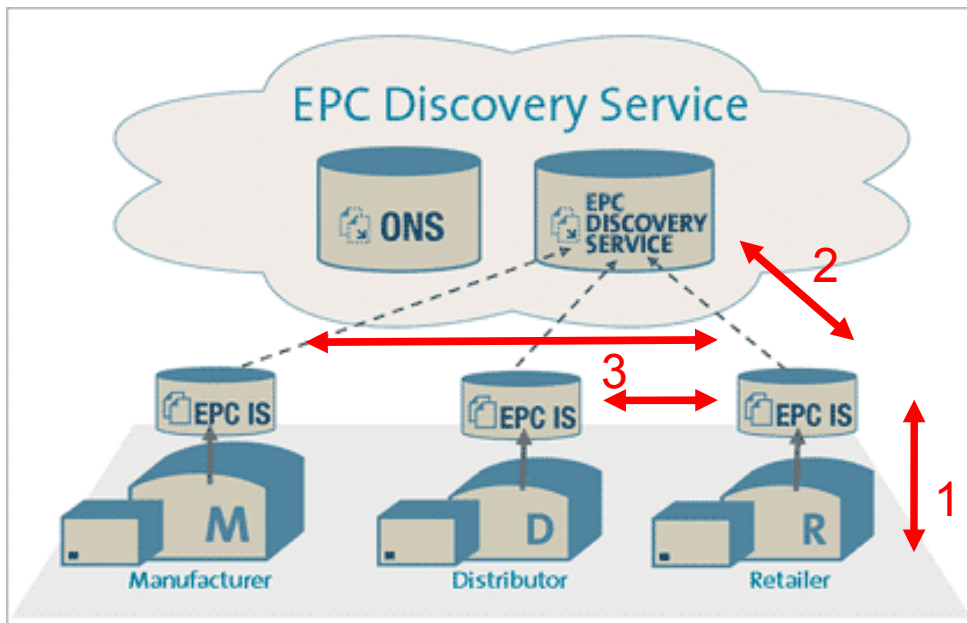
Quelle: VeriSign

**Staats- bzw. Unternehmensgrenzen**

- globales Netzwerk
  - überschreitet Unternehmens- und Staatsgrenzen
  - beschafft Informationen aus allen Teilen des Netzwerks
  - hinterlässt Informationen in allen Teilen des Netzwerks

# Das EPC-Netzwerk (5)

- Ablauf Datenabruf



Quelle: VeriSign

1. Handel liest EPC und fragt eigenes EPC IS
2. Anfrage an EPC Discovery Service
3. Anfrage an EPC IS von Großhändler u. Hersteller

# Das Problem

---

- RFIDs enthalten eindeutige Kennzeichen (IDs)
- eindeutige Kennzeichen können
  - ein Produkt identifizieren
  - eine Person identifizieren
  - als Schlüssel für Datensammlungen dienen
  - die Grundlage für Verhaltensprofile sein
- Schutzwürdig sind
  - personenbezogene Daten
  - und **personenbeziehbare** Daten

# EDRi - Positionen

---

- Identifikation vs. Information
  - RFIDs **identifizieren** Objekte
  - ein globales System zur Objekt-Identifizierung kann zu einem System zur Personen-Identifizierung werden.
  - Hauptzweck von RFID ist oft **Bereitstellen von Informationen** zu Objekten
    - > Identifikation minimieren
    - > Personen sollten Interaktionen mit Anwendungen auslösen, nicht umgekehrt

# EDRi - Positionen

---

- **Datenschutz**
  - Aufsichtsbehörden stärken (finanziell, organisatorisch, technisch)
  - personenbezogene Daten minimieren, datenschutzfreundliche Standardeinstellungen
  - standardisierte Datenschutz-Audits (EuroPriSe)
  - wirksame Sanktionen bei Verstößen
- **offene Standards**
  - Vielfalt ermöglichen, KMU stärken, FOSS ermöglichen

# EDRi - Positionen

---

- Empowerment & Bewusstseinsbildung
  - Vertrauen ist Grundvoraussetzung f. erfolgreichen RFID-Einsatz
  - gesucht: effektive Werkzeuge zum Schutz der Privatsphäre; ausreichende Information
  - Kontrolle über Datensammlungen f. Betroffene
  - Identitätsmanagement zur Verwaltung von Zustimmungen
  - ausgewogene, verständliche, objektive Information

# EDRi - Positionen

---

- Informationen über RFID-Einsatz
  - klar ersichtliche Kennzeichnung von Lesegeräten und RFID-bestückten Objekten
  - generelle Informationen über Zweck des Einsatzes, Art der erfassten Daten, Speicherdauer, ...
  - Informationen über systematische Zusammenhänge (EPC-Netzwerk, Datenweitergaben, ...)

# EDRi - Positionen

---

- Informierte Zustimmung

Bei aktiv belassenen RFIDs sind folgende Informationen erforderlich:

- welche Daten sind am Tag gespeichert
- wer kann (möglicherweise) darauf zugreifen
- welche Anwendungen stecken „hinter“ den Lesegeräten
- generelle Info über Funktionsweise von RFID

**Entscheidungsbasis für Betreten von RFID-Zonen!**

# EDRi - Positionen

---

- Opt-In oder Opt-Out

EDRi setzt sich entschieden für Opt-In ein weil ...

- ... dadurch jedermann per default geschützt ist (auch ohne RFID-Wissen)
- ... keine ausreichende Zugriffskontrolle verfügbar ist
- ... die Entscheidung auf grundsätzlicher Ebene (RFID ja/nein) erfolgen muss
- ... jederzeit Opt-In möglich ist
- ... unzureichende Informationen vorliegen werden (z.B. im Supermarkt zur Hauptgeschäftszeit)

# EDRi - Positionen

---

- Entfernen von RFID-Tags
  - ist einfach, effektiv und leicht nachvollziehbar
  - derzeit der beste Schutzmechanismus
- Verändern der gespeicherten Daten
  - ist keine brauchbare Lösung
- Verändern der Funktionalität
  - „Kill“-Funktion, „Sleep-Modus“
  - ist teuer und langsam; kann künftige Lösung sein
  - Voraussetzung: Zugriffskontrolle durch Betroffene

# EDRi - Positionen

---

- Zuständigkeiten für Schutzmechanismen

Opt-In erfordert Zuständigkeit der Distributoren

- wer Technik verbreitet trägt Verantwortung
- Verantwortung kann weitergegeben werden (z.B. Lieferkette)
- Funktionalität muss entfernt werden, wenn der Nächste in der Kette nicht damit umgehen kann
- Vorteil: tauglich auch für kleine Einzelhändler
- Vorteil: konsistent mit derzeitiger Produktsicherung
- Vorteil: entspricht allgemeiner Erwartungshaltung

# Empfehlung der EU-Kommission

---

- RFID Experten-Gruppe
  - Vertreter von Industrie, Datenschützern, Verbraucherorganisationen, Gewerkschaften
  - Dauer: 07.2007 – 05.2009
  - Themenbereiche:
    - Privatsphäre und Sicherheit
    - RFID und Internet der Dinge
  - beratendes Gremium
  - Entscheidungen trifft die EU-Kommission

# Empfehlung der EU-Kommission

---

- Eckpunkte:
  - Datenschutz-Folgeabschätzung vor Inbetriebnahme
  - Ergreifen von ausreichenden Schutzmaßnahmen
  - Benennen verantwortlicher Person (Kontrolle, Verbesserung)
  - Entwicklung von spezifischen Verhaltensregeln (codes of conduct)
    - Anregung durch Mitgliedstaaten
    - Einbindung von Datenschutzbehörden
    - Europaweite Regeln möglich und erwünscht

# Empfehlung der EU-Kommission

---

- Eckpunkte:
  - Informationsbereitstellung:
    - bei Einsatz in öffentlich zugänglichen Plätzen: schriftliche, verständliche Leitlinien bereitstellen
    - Identität u. Adresse des Betreibers
    - Zweck der RFID-Anwendung
    - Art der verarbeiteten Daten
    - Verbindungen zu personenbezogenen Daten
    - Art und Dauer der Speicherung
    - Zugriffsmöglichkeiten für Dritte
  - Logo zur Kennzeichnung von Lesegeräten

# Empfehlung der EU-Kommission

---

- Eckpunkte:
  - Einrichten von Informationssicherheits-Management
  - Mitgliedstaaten sollen Anleitung zur Einschätzung der Bedrohlichkeit bereitstellen
  - Zertifizierungsschemata, Selbstverpflichtungen sollen entwickelt / ausgebaut werden
  - Einzelhandel:
    - Know-How-Weitergabe entlang der Wertschöpfungskette
    - harmonisiertes Zeichen für RFID-Einsatz in Produkten

# Empfehlung der EU-Kommission

---

- Eckpunkte:
  - Einzelhandel:
    - Deaktivieren von RFID wenn Erzeugung von personenbezogenen Daten wahrscheinlich ist (Opt-In ist möglich)
    - Bereitstellen einer leicht zugänglichen Deaktivierungsmöglichkeit wenn Erzeugung personenbezogener Daten unwahrscheinlich ist
    - Deaktivierung soll sofort und kostenlos erfolgen
  - Keine Verknüpfung von RFID und Garantierechten

# Empfehlung der EU-Kommission

---

- Eckpunkte:
  - Mitgliedstaaten, Industrie, Interessensvertreter
    - sollen Wirtschaft und Bevölkerung über RFID informieren
    - sollen best-practice Beispiele identifizieren
  - Forschungspolitik
    - soll privacy und security by design anregen
  - Folgemaßnahmen
    - Mitgliedstaaten berichten nach 18 Monaten
    - Kommission evaluiert innerhalb von 3 Jahren
    - Bei Bedarf werden verpflichtende Maßnahmen folgen

# EDRi-Position zur Empfehlung

---

- grundsätzlich ein Schritt in die richtige Richtung
- viele wichtige Punkte werden behandelt
- Problembereiche
  - unverbindlicher Charakter
  - Bewertung der Gefährdungssituation durch Handel
  - keine Definition von Datenschutz-Folgeabschätzung
  - Verlassen auf Selbstregulierung
  - unkontrollierte Funktionalität bleibt im Umlauf

# Geht das also auch datenschutzfreundlich?

---

- im Prinzip: Ja
- in der Praxis werden benötigt:
  - (politischer) Wille zur datenschutzfreundlichen Gestaltung
  - technische Verbesserungen
  - Kontroll- und Steuermöglichkeiten für Betroffene
  - ausgewogene Informationen
  - überzeugende RFID-Anwendungen

# Ausblick

---

- RFID Experten-Gruppe:
  - Internet der Dinge
    - Vernetzung
    - spontane Interaktion von Komponenten
    - Einbindung von Sensoren
    - Verknüpfung mit anderen Technologien



## **Danke für die Aufmerksamkeit!**

Andreas Krisch

[andreas.krisch@vibe.at](mailto:andreas.krisch@vibe.at)

<http://www.edri.org/> <http://www.vibe.at/>

## **Danke für die Spenden!**

European Digital Rights AISBL

IBAN: BE32 7330 2150 2102

BIC: KREDBEBB