Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Verbraucherschutz

Handlungsbedarf im Zusammenhang mit RFID-Technologie

Bericht in Erfüllung des Postulates 05.3053 Allemann vom 9. März 2005

Autorenschaft und Mitwirkung

Bundesamt für Gesundheit (BAG):
Mirjana Moser, Salome Ryf, Martin Meier, Andrea Nagel
Bundesamt für Kommunikation (BAKOM):
Rolf Burgherr, Mark Fitzpatrick, Ka Schuppisser, Damien Scherrer
Eidgenössische Materialprüfungs- und Forschungsanstalt (EMPA): Lorenz Hilty
Stiftung für Datenschutz und Informationssicherheit: Beat Rudin
Büro für Konsumentenfragen (BK): Benno Maurer, Jean-Marc Vögele
Schweizerisches Heilmittelinstitut (Swissmedic) : Daniel Reusser
Stiftung Risiko-Dialog: Jaqueline Lätsch
IT'IS Foundation: Niels Kuster, Sven Kühn
Ocha GmbH: David C. Gürlet
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB): Urs Scherrer
TA-SWISS (Zentrum für Technologiefolgen-Abschätzung): Sergio Bellucci, Fulvio Caccia

Federführung

Bundesamt für Gesundheit (BAG): Mirjana Moser

Weitere Informationen

Diese Publikation ist auch in französischer und italienischer Sprache erhältlich
Der Bericht wird unter **www.bag.admin.ch/rfid-bericht** veröffentlicht.

Zusammenfassung

Der vorliegende Bericht wurde als Antwort auf das Postulat Allemann „Handlungsbedarf im Zusammenhang mit RFID-Technologie“ (05.3053) von einer Gruppe von Expertinnen und Experten aus der Verwaltung, Forschung, Industrie und unabhängigen Organisationen erarbeitet. Die Federführung lag beim Bundesamt für Gesundheit.

Im Postulat wird der Bundesrat beauftragt zu prüfen, „*welcher Handlungsbedarf sich aus dem absehbaren flächendeckenden Einsatz der RFID-Technologie ergibt. Insbesondere soll das Augenmerk auf folgende Punkte gerichtet werden:*

- *datenschutzrechtliche Probleme, die von der geltenden Datenschutzgesetzgebung noch nicht abgedeckt werden*
- *gesundheitliche Risiken (insb. Risikopotenzial der Strahlung)*
- *Umweltrisiko und Abfallentsorgung (insb. Abfallrecycling)*
- *Konsumentenschutz / -information: Deklarationspflicht der eingesetzten RFID-Chips bei Konsumartikeln“*

RFID steht für “Radio Frequency IDentification” und bedeutet die kontaktlose Identifizierung von Objekten mittels Funkübertragung von Daten. Ein RFID-System besteht aus so genannten Tags (bestehend aus einer Antenne und einem Chip), die auf oder in zu identifizierenden Objekten angebracht werden sowie einem Lesegerät, welches mit den Tags kommuniziert. Dadurch ist es möglich, die Objekte berührungslos und ohne Sichtkontakt zu identifizieren, zu registrieren sowie objektspezifische Daten und Informationen auszutauschen und zu verarbeiten.
RFID-Technologie gilt allgemein als eine zukunftsweisende Technologie, deren Vorteile und Chancen für die Innovation, Technologieentwicklung und Wirtschaftsförderung unumstritten sind. Es wird aber auch anerkannt, dass RFID einige potenzielle Risiken in sich birgt, denen mit geeigneten Massnahmen zu begegnen ist. Einige solche Massnahmen werden von der Expertengruppe empfohlen.
Die Expertengruppe hat die RFID-Technologie, ihre voraussehbare Entwicklung sowie heutige und zukünftige Anwendungen in Bezug auf potenzielle Risiken analysiert. Die vorhandenen gesetzlichen und institutionellen Rahmenbedingungen für ein Risikomanagement wurden auf ihre „RFID-Tauglichkeit“ hin überprüft. Allgemein kann festgestellt werden, dass die Rahmenbedingungen weitgehend vorhanden sind, dass es aber Schwachstellen gibt. Diese betreffen meistens nicht nur RFID, sondern auch andere Bereiche.
Im Bereich **Datenschutz** bietet das Datenschutzgesetz gute Rahmenbedingungen. Angesichts der grossen Menge von Personendaten, die in Zukunft verarbeitet und durch Vernetzung zusammengeführt werden können, besteht aber vermehrt das Risiko eines Missbrauches. Gefordert sind deshalb eine vorsorgliche Datensparsamkeit sowie strengere Sanktionen bei einem Verstoss gegen das Datenschutzgesetz.
Über die **Strahlung** von RFID-Systemen und deren gesundheitlichen Risiken ist sehr wenig bekannt – es braucht diesbezüglich mehr gezielte Forschung. Generell gibt es für die Begrenzung der elektromagnetischen Strahlung internationale Grenzwerte. Die geltenden RFID-Produktenormen sind jedoch nicht tauglich, das Einhalten dieser Grenzwerte zu überprüfen. Zusätzlich besteht die Möglichkeit, dass aktive medizinische Implantate durch RFID-Strahlung gestört werden. Das Problem muss gelöst werden – z.B. mit einer zusätzlichen Produktenorm.
Die **Entsorgung** der Tags wird heute als unproblematisch eingestuft. In Zukunft könnten aber wegen der sehr grossen Menge an Tags und der darin enthaltenen Stoffe Probleme bei der Abfallentsorgung und dem Recycling auftreten. Dies soll durch vorsorgliche Massnahmen verhindert werden.
Im **Konsumbereich** ist dafür zu sorgen, dass die Konsumentinnen und Konsumenten ausreichend informiert sind und dass die Voraussetzungen bestehen, damit sie ihr Recht auf Selbstbestimmung und Wahlfreiheit ausüben können.
Die RFID-Technologie ist sehr dynamisch, komplex und vielfältig. Deswegen ist es nötig, dass die Entwicklung der Technologie aufmerksam verfolgt wird und alle Stakeholder an der Erarbeitung der Strategien zum Risikomanagement beteiligt sind.

Um potenzielle Risiken der RFID-Technologie zu minimieren und somit auch ihre Chancen zu maximieren, werden zum oben aufgeführtem Handlungsbedarf folgende Empfehlungen gemacht:

Empfehlung 1
Die Entwicklung der RFID-Technologie muss laufend verfolgt werden. Vorhandene gesetzliche und institutionelle Instrumente müssen periodisch auf ihre RFID-Tauglichkeit überprüft werden. Ziel ist es, optimale Bedingungen für die Forschung, Entwicklung und wirtschaftliche Nutzung der RFID-Technologie in der Schweiz zu schaffen. Gleichzeitig soll der Schweizer Bevölkerung eine maximal mögliche Sicherheit vor Gesundheits- und Umweltrisiken sowie der Datenschutz garantiert werden. Dabei ist eine internationale Harmonisierung anzustreben.

Empfehlung 2
Stakeholder-Plattformen sollen mit dem Ziel errichtet werden, eine gemeinsame Strategie zu erarbeiten, um die Chancen der RFID-Technologie maximal auszunutzen und gleichzeitig die Risiken zu minimieren. In diesen Plattformen sollen die Forschung & Entwicklung, die Behörden, die Industrie sowie die Anwender der Technologie und die Konsumenten vertreten sein.

Empfehlung 3
In der Forschung zu elektromagnetischen Feldern (EMF) und deren Gesundheitsrisiken sollen die in der Realität auftretenden Expositionen durch RFID-Systeme (insbesondere durch die Lesegeräte) stärker berücksichtigt werden. Zudem sollen andere mögliche Gesundheitsrisiken von RFID wie z.B. von implantierten Tags bei Menschen untersucht werden.

Empfehlung 4
In Bezug auf die Gesundheitsrisiken der Strahlung müssen die vorhandenen, harmonisierten Produktenormen zu RFID, welche die Konformität mit den internationalen Grenzwertempfehlungen zu elektromagnetischen Feldern überprüfen sollen, so geändert werden, dass die Grenzwertempfehlungen konsequent umgesetzt werden, was heute nicht der Fall ist. In Bezug auf mögliche Störungen von elektronischen Implantaten durch RFID sollen auf internationaler Ebene im Bereich Produktesicherheit zusätzliche Massnahmen ergriffen werden. Die Schweiz soll sich auf internationaler Ebene dafür einsetzen.

Empfehlung 5
In der RFID-Technologieentwicklung sind wirtschaftlich tragbare Lösungen zu suchen, wie die Tags konstruiert sein sollen, damit sie umweltfreundlich entsorgt oder rezykliert werden können.

Empfehlung 6
Bei einer Verschärfung der Datenschutzproblematik durch grosse Mengen an Daten, welche unbemerkt gesammelt werden können, soll die Einführung des Prinzips der Datenvermeidung und Datensparsamkeit in Bezug auf Personendaten im Bundesgesetz über den Datenschutz neu überprüft werden. Gleichzeitig soll das Sanktionierungssystem im Datenschutzbereich überprüft werden. Verstösse gegen das Datenschutzgesetz sollen so geahndet werden, dass die Strafe klar grösser ist als der allenfalls aus dem Verstoss gezogene Nutzen.

Empfehlung 7
Konsumenten müssen über Eigenschaften, Nutzen und Risiken von RFID-Systemen im Konsumbereich verständlich informiert werden. Ausserdem müssen RFID-Tags im Konsumbereich klar als solche gekennzeichnet sein. Verbraucher müssen die Möglichkeit haben, mit einem Produkt erworbene Tags ohne vermeidbare negative Konsequenzen zu zerstören, zu entfernen oder auszuschalten.

1. Einleitung

RFID steht für “Radio Frequency IDentification” und bedeutet die kontaktlose Identifizierung von Objekten mittels Funkübertragung von Daten. Ein RFID-System besteht aus so genannten „Tags“ – (bestehend aus einer Antenne und einem Chip), die auf oder in den zu identifizierenden Objekten angebracht wird, und Lesegeräten. Dadurch ist es z.B. möglich, in einem Supermarkt einen Einkaufswagen voll „getagter“ Waren an der Kasse auf einen Schlag berührungslos und ohne Sichtkontakt zu registrieren. RFID-Systeme in Logistik, Verkehr oder für die Tieridentifikation (z.B. obligatorische Hundetags) sind alltäglich geworden. Im Medizinbereich bietet die RFID-Technologie durch die Identifizierung von Medikamenten, Blutkonserven oder auch Patienten die Chance, potenzielle Fehler, Fälschungen oder Verwechslungen zu reduzieren. Die Erweiterung der Tags mit Sensoren und Lokalisierungssystemen vergrössert die Einsatzmöglichkeiten. Zur Vision der RFID-Technologie gehört es auch, mit intelligenten Funktionen und Vernetzungsmöglichkeiten in einem zukünftigen „Internet der Dinge“ Wertschöpfungsketten oder andere Objektbewegungen zukünftig "live" über das Internet verfolgen zu können.

Es ist unbestritten, dass RFID eine zukunftsweisende Technologie mit einem hohen Nutzenpotenzial für die Industrie, den Dienstleistungssektor und die Konsumenten ist. Viele Anwendungen dienen der Sicherheit, der Gesundheit und tragen zur Schonung natürlicher Ressourcen und zum Umweltschutz bei. Während die Chancen und Vorteile der Technologie offensichtlich sind, tauchen vermehrt die Fragen nach möglichen Risiken auf: Wie steht mit den Gesundheitsrisiken durch die Strahlung? Ist der Schutz der Personendaten („gläserner Mensch“) gewährleistet? Wie werden die Milliarden von Tags entsorgt? Es sind solche Fragen, welche Nationalrätin Evi Allemann veranlasst haben, die Initiative zu ergreifen. Ihr Postulat „Handlungsbedarf im Zusammenhang mit RFID-Technologie“ (05.3053) hat der Nationalrat dem Antrag des Bundesrates vom 18.5.2005 folgend am 17.6.2005 angenommen. Im Postulat wird der Bundesrat beauftragt zu prüfen, „*welcher Handlungsbedarf sich aus dem absehbaren flächendeckenden Einsatz der RFID-Technologie ergibt. Insbesondere soll das Augenmerk auf folgende Punkte gerichtet werden:*

- *datenschutzrechtliche Probleme, die von der geltenden Datenschutzgesetzgebung noch nicht abgedeckt werden*
- *gesundheitliche Risiken (insb. Risikopotenzial der Strahlung)*
- *Umweltrisiko und Abfallentsorgung (insb. Abfallrecycling)*
- *Konsumentenschutz / -information: Deklarationspflicht der eingesetzten RFID-Chips bei Konsumartikeln“*

Der vorliegende Bericht erteilt Auskunft auf die im Postulat Allemann gestellten Fragen[1]. Der Bericht wurde von einer Arbeitsgruppe bestehend aus Experten aus der Verwaltung, Forschung, Industrie und unabhängigen Organisationen erstellt. Die Federführung lag beim Bundesamt für Gesundheit.

Im Bericht werden die RFID-Technologie und einige, vor allem in der Medizin und dem Konsumbereich bereits vorhandene Anwendungen beschrieben (Kapitel 2). Die im Postulat erwähnten Aspekte Strahlung, Gesundheit, Umweltschutz, Datenschutz, Datensicherheit und Konsumentenschutz werden in den Kapiteln 3-6 ausführlich abgehandelt und im Hinblick auf mögliche Risiken analysiert. Die vorhandenen gesetzlichen und institutionellen Rahmenbedingungen für ein Risikomanagement wurden auf ihre „RFID-Tauglichkeit“ hin überprüft. Der diesbezügliche Handlungsbedarf wird im Kapitel 8 zusammengefasst und mögliche Lösungsansätze in Form von sieben Empfehlungen aufgelistet. Da die Empfehlungen verschiedene „Stakeholders“ betreffen und in verschiedenen Kompetenz- und Zuständigkeitsbereichen liegen, wurden im Bericht keine konkreten Umsetzungsvorschläge angegeben.

[1] Als Ergänzung zum vorliegenden Bericht werden zwei weitere Berichte zur Lektüre empfohlen:
- „Nichtionisierende Strahlung und Gesundheitsschutz in der Schweiz“ , der als Antwort zum Postulat Sommaruga (00.3565) erarbeitet wurde. Er behandelt detailliert Expositionen, gesundheitliche Wirkungen und die rechtliche Situation im Bereich der nichtionisierenden Strahlung. www.bag.admin.ch/nis-bericht
- „Risikopotential von drahtlosen Netzwerken“ wurde als Antwort auf Postulat Allemann (04.3594) erstellt. www.bag.admin.ch/wlan-bericht

In den letzten Jahren wurden einige Berichte zur RFID-Technologie national und international erstellt. Einige Projekte, Aktionen und Veranstaltungen haben in der EU stattgefunden. Diese Berichte und Aktivitäten wurden im vorliegenden Bericht berücksichtigt, die wichtigsten Dokumente der EU zum Thema RFID sind im Kapitel 7 zusammengefasst. Die wichtigsten Quellen sind im Kapitel 9 aufgelistet.

Der Bericht wird auf der Internetseite des BAG unter http://www.bag.admin.ch/rfid-bericht veröffentlicht werden.

2. RFID Grundlagen

2.1 RFID-Technologie

Radio Frequency IDentification (RFID) ist die Identifizierung von Objekten über Funk. Ein RFID-System besteht aus verschiedenen Komponenten. Am zu identifizierenden Objekt ist ein Etikett angebracht, welches Tag genannt wird. Beim Objekt kann es sich um eine Ware, ein Fahrzeug, einen Ort, ein Tier, einen Menschen etc. handeln. Der Tag besteht aus einem Chip, auf dem Daten gespeichert sind, und einer kleinen Antenne, welche die Daten übermitteln kann. Ein Lesegerät empfängt diese Daten, kann sie entweder selber verarbeiten oder an einen zentralen Computer weiterleiten. RFID-Tags werden oft auch als Smart Labels bezeichnet. Es gibt jedoch auch Tags, die nicht die Form eines Etiketts bzw. Labels haben, z.B. wenn sie dazu gedacht sind, in das Trägerobjekt integriert zu werden.

Die RFID-Technologie weist gegenüber anderen Technologien zur Identifikation von Objekten folgende spezifische Vorteile auf:

- Die Identifikation eines RFID-Tags ist berührungslos und ohne Sichtkontakt möglich.
- Die Länge der Identifikationsnummern reicht theoretisch aus, um jedes auf der Welt existierende Objekt eindeutig zu kennzeichnen. Bei RFID-Anwendungen im Einzelhandel wird deshalb (im Unterschied zum heutigen Barcode) das sog. *Item-level Tagging* realisiert werden: Zwei Exemplare des gleichen Artikels haben verschiedene Identifikationsnummern.
- Neben der Identifikationsnummer können weitere Daten auf dem RFID-Tag gespeichert werden, z.B. ein Verfalldatum oder Wartungsinformationen.
- Die RFID-Lesegeräte können mehrere RFID-Tags in einem Arbeitsgang auslesen *(Bulk Reading).* Die Objekte müssen also nicht einzeln am Lesegerät vorbeigeführt werden.
- Aufgrund der technischen Möglichkeiten und der Marktentwicklung kann von weiteren massiven Preissenkungen für RFID-Tags und -Lesegeräte ausgegangen werden. Die Kosten pro elektronisch gekennzeichneten Objekt werden im Rappenbereich liegen.

Da die Anwendungsgebiete der RFID-Technologie sehr vielfältig sind, werden auch sehr unterschiedliche Systeme eingesetzt. Es gibt unterschiedliche Bauformen von Tags und unterschiedliche Lesegeräte. Die Systeme arbeiten auf verschiedenen Frequenzen (Langwellen- bis Mikrowellenbereich) und haben Reichweiten zwischen 1cm und 100m.

Tags

Die Bauform eines RFID-Tags hängt stark von seiner Anwendung ab. Die Tags können sehr klein oder hauchdünn sein und so in Gegenstände integriert werden. Bei Anwendungen in der Logistik oder bei Mautsystemen können die Tags auch gross sein. Hier werden einige Beispiele von Bauformen aufgeführt[2].

Kontaktlose Chipkarte: Eine grosse, flache Antenne wird zwischen zwei PVC-Folien einlaminiert. Diese Karten werden z.B. für Zutrittskontrollen (Badge) verwendet (Abbildung 1A).

Disks und Münzen: Spritzgussgehäuse mit einem Durchmesser von wenigen mm bis 10 cm mit einem Loch für die Befestigungsschraube in der Mitte.

Glaszylinder: Für die Tieridentifizierung (z.B. Katze, Hund) werden kleine Glastags unter die Haut injiziert (Abbildung 1B).

Einbau in Metalloberflächen: Zur Identifizierung von Werkzeugen oder Gasflaschen kann der Tag direkt in die Metalloberfläche eingebaut werden.

Smart-Label: Dies sind papierdünne Etiketten. Die Antenne wird durch Siebdruck oder Ätztechnik auf eine Plastikfolie aufgebracht, welche mit einer Papierschicht laminiert und mit Kleber beschichtet wird. Diese Klebeetiketten können bedruckt werden (z.B. zusätzlich mit einem Strichcode) und dann auf Gepäckstücke, Pakete, Waren etc. aufgeklebt werden (Abbildung 1C).

[2] K. Finkenzeller: RFID Handbuch. 2006


A

B

C

D

Abbildung 1: *A: Kontaktlose Chipkarte, B: Glaszylinder für Tieridentifikation mit Applikator, C Smart-Label[3], D: Verwandte Technologie: Goldchip*

Man unterscheidet die folgenden Typen von RFID-Tags:

- **Passive Tags:** Diese verbreiteten Tags besitzen keine eingebaute Energiequelle, die sie zum Aussenden eines elektromagnetischen Feldes verwenden könnten; sie beziehen die zum Antworten benötigte Energie vollständig aus dem Feld des Lesegerätes. Passive Tags sind daher eher für kurze Auslesedistanzen geeignet.
- **Aktive Tags:** Sie beziehen die zum Senden benötigte Energie aus einer eingebauten Quelle. Dies ist in der Regel eine Batterie, die für mehrere Jahre Betriebsdauer ausgelegt ist. Aktive Tags sind grösser, schwerer und teurer als passive und sind für grössere Auslesedistanzen geeignet. Zum Auslesen wird kein starkes Versorgungsfeld benötigt.

Daneben werden zunehmend die folgenden Kategorien von RFID-Tags wichtig:

- Tags, die zwar über eine eigene Energiequelle verfügen, damit aber nur den Mikrochip oder eingebaute Sensoren betreiben, nicht jedoch die Sende- und Empfangseinheit. Bezüglich des Auslesevorgangs verhalten sie sich wie passive Tags. Diese Tags werden von einigen Autoren als semi-passive[4, 5], von anderen synonym als semi-aktive[4], von einzelnen sogar als aktive Tags bezeichnet. In diesem Bericht betrachten wir sie als Untergruppe der passiven Tags.
- Tags, die zwar mittels einer eingebauten Energiequelle ihr Signal aussenden, dies jedoch nur nach Aufforderung durch ein Lesegerät tun. Ausserhalb der Lesezeiten befinden sie sich in einem "Schlafmodus" und senden kein Signal aus. Sie werden gelegentlich als semi-aktive[5] Tags bezeichnet, was jedoch zu Verwechslungen führen kann (siehe oben). In diesem Bericht betrachten wir sie als Untergruppe der aktiven Tags. Wir werden diese Untergruppe jeweils explizit umschreiben, wo es in diesem Bericht erforderlich ist. Die Unterscheidung von anderen (regelmässig sendenden) aktiven Tags kann im Zusammenhang mit unerwünschten Auswirkungen elektromagnetischer Felder relevant sein.

Einige Autoren rechnen aktive Tags nicht der RFID-Technologie zu. Da wir von einer möglichst breiten Definition von RFID ausgehen, verwenden wir die oben eingeführte, weithin üblichere Terminologie, die auch Tags mit batteriebetriebenem Sender umfasst.

Lesegeräte und Deaktivatoren

Auch bei den Lesegeräten gibt es sehr unterschiedliche Bauformen. Bei Artikelüberwachungssystemen werden fest installierte Tore eingesetzt (Abbildung 2A). In der Lagerbewirtschaftung, in Bibliotheken, zur Tier- oder Patientenidentifizierung (Abbildung 4A) etc. werden auch Handlesegeräte (Abbildung 2B) eingesetzt. Das Lesegerät kann aber auch beispielsweise in ein Schloss integriert sein. Deaktivatoren sind z.B. im Ladentisch oder in der Bibliothek im Ausleihterminal integriert.

[3] Quelle: Philips Semiconductors
[4] RFID Technologies: Emerging Issues, Challenges and Policy Options, Eur 22770 EN -2007
[5] National Institute of Standards and Technology: Guidelines for Securing Radio Frequency Identification Systems, Special Publication 800-98


A

B

C

Abbildung 2: RFID-Lesegeräte *A: Tor zur Artikelüberwachung[6] , B: Handlesegerät[7], C: Lesegerät in einem Türschloss[8]*

Informationsverarbeitungssysteme[2]

Bei den Tags gibt es ganz unterschiedliche Informationsverarbeitungssysteme. Bei den einfachen Systemen wird entweder nur ein Bit („ein Tag ist anwesend", z.B. bei Warensicherungsanlagen) oder eine Identifizierungsnummer (z.B. bei Paletten, Containern, Tieren) übermittelt. Bei etwas komplexeren Systeme haben die Tags beschreibbare Speicher und können einfache Kommandos zum Lesen oder Schreiben abarbeiten. Dies ermöglicht das Anwenden von einfachen Datenverschlüsselungen, einer Authentifizierung und das gleichzeitige Auslesen mehrerer Tags. Die Daten auf dem Tag können durch das Lesegerät bearbeitet werden, es können neue Informationen auf den Tag geschrieben werden.
Bei den komplexesten Systemen haben die Tags einen Mikroprozessor und ein Chipkartenbetriebssystem, welches komplexe Verschlüsselungsalgorithmen erlaubt.
Die Lesegeräte können entweder die ausgelesenen Daten selber verarbeiten oder mit einem Computer („back-end") verbunden sein, auf dem die ausgelesenen Daten überprüft (z.B. bei einer Zugangskontrolle), gespeichert und bearbeitet werden.

Verwandte Technologien

Kontaktbehaftete Chipkarten: Diese Karten werden über einen Kontakt (Goldkontakt, Abbildung 1D) ausgelesen. Sie werden vor allem im Zahlungsverkehr und im Mobiltelefon (SIM-Karte) angewendet, wo eine hohe Sicherheit bei der Verarbeitung und Übertragung der Daten gefordert ist. In Bereichen, in denen Benutzerfreundlichkeit (z.B. Zutrittskontrolle) oder kurze Transaktionszeiten (z.B. Ticketing) gefordert sind, kommen eher kontaktlose Chipkarten zum Einsatz. Es gibt auch hybride Karten (Dual Interface Card), welche sowohl ein kontaktloses als auch ein kontaktbehaftetes Interface haben.
Strichcode oder Barcode: Strichcodes sind aus dem Handel, der Industrie und Lagern bekannt, wo Daten von Waren schnell aufgenommen werden müssen. Mit einem optischen Lesegerät oder einer Kamera können die Codes maschinell eingelesen und weiterverarbeitet werden. Am weitesten verbreitet sind eindimensionale Strichcodes, es gibt jedoch auch zwei- bis vierdimensionale Versionen[9]. Die Strichcodeetiketten werden in einigen Bereichen mit Smartlabels kombiniert, da der Strichcode einige Nachteile hat, welche mit der RFID-Technologie behoben werden. Beim Strichcode muss zum Auslesen Sichtkontakt bestehen, es kann gleichzeitig nur ein Etikett gelesen werden, der Strichcode kann durch Beschädigung oder Verschmutzung des Etiketts unlesbar werden. Ausserdem kann der Code durch das Lesegerät nur gelesen und nicht verändert werden.
Telemetrie: Bei diesen Systemen werden Messdaten von einem Sensor über Funk zu einer Messstation geschickt. Ein Wetterballon z.B. sendet so Informationen zu Position, Druck, Temperatur etc. zur Messstation. Es gibt auch RFID-Tags, welche mit einem Sensor versehen sind. Die gemessenen Daten können zusammen mit der Uhrzeit auf dem Chip gespeichert und bei Bedarf ausgelesen oder (bei aktiven Tags) kontinuierlich gesendet werden. Die Grenzen zwischen Telemetrie und RFID sind mit unserer weiten Definition von RFID fliessend.

[6] Quelle: Bibliotheka
[7] Quelle: www.dataident.com
[8] Quelle: www.baulinks.de
[9] Vgl. http://science.orf.at/science/news/149643

2.2 Telekommunikationsaspekte der RFID

Um gegenseitige Störungen bei Funkanwendungen zu verhindern, wird die Benutzung des Frequenzspektrums reglementiert. Für die Nutzung ist grundsätzlich eine Funkkonzession notwendig. In der Funkkonzession werden die Frequenzen, die Ausgangsleistung sowie weitere Parameter festgelegt. Zuweisungen von Frequenzen an Dienste und Anwendungen werden international koordiniert. Für die globale Koordination ist die ITU (International Telecommunications Union) zuständig. Auf der europäischen Ebene werden von CEPT[10]/ECC[11] Empfehlungen und Entscheidungen zur Frequenzzuweisung erarbeitet, diese bilden die Grundlage für die nationalen Regulierungsentscheide und Anforderungen für Funkdienste bzw. –anlagen. In der Schweiz werden die Frequenzen im nationalen Frequenzzuweisungsplan NaFZ definiert. Die detaillierten Bedingungen (insbesondere Frequenzen, Sendeleistungen, Kanalbandbreiten) für die Benutzung durch bestimmte Anwendungen werden in den so genannten Schnittstellenanforderungen (Radio Interface Regulation RIR) aufgeführt.
Gewisse Frequenzbereiche für Anwendungen mit kurzer Reichweite (z.B. RFID) wurden von der Konzessionspflicht befreit[12]. Da bei der konzessionsfreien Nutzung eines Frequenzbandes meist eine grosse Vielfalt von Anwendungen möglich ist und die Zahl der Benutzer unbeschränkt ist, sind gegenseitige Störungen nicht ausgeschlossen. Diverse lizenzfreie Frequenzbereiche stehen für alle Anwendungen des Kurzstreckenfunks (Short Range Devices, SRD) zur Verfügung, diese Bereiche können teilweise auch für RFID-Anwendungen genutzt werden (RIR-1008, RIR-1005). Gestützt auf Annex 11 der CEPT Empfehlung ERC/REC 70-03 sind in der Schnittstellenanforderung RIR-1011 Frequenzen speziell für RFID-Anwendungen freigegeben worden.

Tabelle 1: *Die am häufigsten verwendeten Frequenzbereiche für RFID.*

A: Frequenzen bis 30 MHz

Frequenzbereich (MHz)	< 0,135	0,4-0,6	3,155-3,400	6,765-6,795	7,4 – 8,8	10,2-11	13,56	26,957-27,283
Sendeleistung des Lesegerätes / Magnetfeld (dBµA/m)[13]	72 -3dB/octave see RIR1005-01	-8	13,5	42	9	9	60	42
Art des Tags	passiv	passiv	passiv	passiv	passiv	Passiv	meist passiv	meist passiv
Lesedistanz	kurz ~ 0.4m	kurz	kurz	kurz	kurz	Kurz	mittel ~ 1m	mittel
Schnittstellenanforderung	RIR-1005-01	RIR-1005-14	RIR-1005-10	RIR-1005-02	RIR-1005-03	RIR-1005-11	RIR-1005-12	RIR-1005-05
ISM Bereich	ja	nein	nein	nein	nein	nein	ja	ja
Anwendungsbeispiele	Zugangskontrolle, Identifikation von Gütern und von Tieren (Hundechip)	Electronic Article Surveillance (EAS)	Zugangskontrolle, EAS, Identifikation von Gütern und von Tieren	Zugangskontrolle, EAS, Identifikation von Gütern und von Tieren	EAS, Identifikation von Gütern und von Tieren	EAS, Identifikation von Gütern und von Tieren	Zugangskontrolle, Smartcards, EAS	EAS, Identifikation von Gütern und von Tieren

[10] Conférence Européenne des Administrations des Postes et des Télécommunications
[11] Electronic Communications Committee (ECC ist ein Teilbereich von CEPT)
[12] Verordnung über Frequenzmanagement und Funkkonzessionen FKV, SR 784.102.1
[13] Gemessen bei 10m. Maximalwerte, siehe detaillierte Sendeleistungsangaben in entsprechenden RIR Dokument

B: Frequenzen ab 30 MHz

Frequenz-bereich (MHz)	433,05-434,79	865-868	2446-2454	5795 – 5805	5805 – 5815
Sendeleistung des Lesegerä-tes	10 mW ERP (<10% Duty Cycle)	100 mW ERP[14] 500 mW ERP [14] [15] 2 W ERP [14] [15]	500 mW EIRP 4 W EIRP[16]	2 W EIRP	2 W EIRP
Art des Tag	Aktiv /Passiv	Aktiv / Passiv	Aktiv	Aktiv	Aktiv
Lesedistanz	mittel, einige Meter	gross 6-8m	gross >10m	gross	Gross
Schnittstellen-anforderung	RIR-1008-05	RIR-1011-02 bis -06	RIR-1011-01	RIR-1012-01	RIR-1012-02
ISM Bereich	ja	nein	ja	ja	ja benötigt eine Funkkonzession!
Anwendungs-beispiele	Verkehrs-überwachung, Logistik	Verkehrs-überwachung, Logistik	Zahlstellen im Strassen-verkehr, Tra-cking von Container	MAUT In der Schweiz für LSVA (MAUT)	Nur für Strassen-verkehrs-anwednungen (MAUT)

Einige der lizenzfreien Frequenzbänder verwenden so genannte ISM- (Industrial, Science, Medical) Frequenzen[17]. In diesen Frequenzbereichen können neben Funkanwendungen auch andere Hochfrequenzanwendungen betrieben werden. Entsprechend können Störungen bzw. Einschränkungen beim Betrieb von Funkanlagen nicht ausgeschlossen werden.

UWB- (Ultra Wide Band)Technologie

Die UWB-Technologie arbeitet mit sehr grossen Frequenzbandbreiten kommt jedoch mit geringen Sendeleistungen aus. Die UWB-Technologie hat das Potenzial für eine grosse Vielfalt von Kurzstreckenfunkanwendungen in den Bereichen Kommunikation, Messtechnik, Ortsbestimmung (Groud-Radar), Überwachung, Medizinaltechnik, Verfolgen von Objekten etc. 90% der UWB-Anwendungen werden für die drahtlose Kommunikation über kurze Distanzen mit hohen Datenraten (500 Mb/s) im Heim- und Bürobereich genutzt. UWB ist aber auch für RFID-Anwendungen geeignet, insbesondere kombiniert mit der Möglichkeit einer sehr genauen und schnellen Ortsbestimmung (precise RTLS – Real Time Location Systems).
Beispiele sind[18] [19]

- Precise Manufacturing Positioning Systems (in der Industrieautomation)
- Arbeitsplatzsicherheitssysteme (z.B. Überwachung der Beseitigung von hochgiftigen Abfällen z.B im Entsorgungslager Kölliken)
- Schnelle und exakte Positionierung bei Spital-Asset-Management in Notfall-Abteilungen
- Simulations-Systeme für para- und militärische Beübungs-Simulatoren

[14] mit LBT Funktion (Listen before talk)
[15] eingeschränktes Frequenzband (siehe RIR Dokument)
[16] nur in Gebäuden, max. 15 % Duty Cycle
[17] ISM Frequenzen (industrial, scientific and medical applications of radio energy); ISM Frequenzen sind in der Regel von der Konzessionspflicht ausgenommen, es existieren aber auch konzessionsfreie Frequenzen ausserhalb von ISM Bereichen (z.B. 865 MHz Bereich). Bei ISM Anwendungen handelt es sich um Nicht-Telekommunikationsanwendungen (z.B. Mikrowellenofen etc.)
[18] http://www.ubisense.de/
[19] http://www.timedomain.com

Abbildung 3: *Patientenortung mit UWB auf 75 cm genau*[20]

In weiten Teilen Europas sind die Frequenzbänder harmonisiert und können lizenzfrei (mit Ausnahmen) verwendet werden. Die Frequenzen liegen zwischen 1,6 GHz und 10,6 GHz. Die Anforderungen sind in der Schnittstellenanforderung RIR-1023 definiert.

2.3 RFID-Anwendungen

Anwendungen im Konsumbereich

Mittels RFID-Tags können Waren entlang der ganzen Wertschöpfungskette vom Hersteller bis zum Kunden identifiziert werden. Das System des elektronischen Produktecodes (EPC: electronic product code) sieht sich als möglicher Nachfolger des Handelsstrichcodes (EAN: european article number). Mit Hilfe eines Object Name Service (ONS) soll es möglich sein, eine Internetadresse für weiterführende Informationen zu einem Produkt zu erhalten, um auf diese bequem zuzugreifen. Da jedes Exemplar einer Ware eine individuelle Nummer trägt, erlaubt der EPC auch eine individuelle Rückverfolgung eines Produktes (item level tagging).
Logistische Prozesse werden durch den Einsatz von RFID transparenter und schneller, da viele Schritte automatisiert werden können (Sortieren, Wareneingang und –Ausgang etc.). Lagerbestände können kleiner gehalten werden, ohne dass dadurch Versorgungslücken an Verkaufsstellen entstehen.
Im Laden selber können z.B. im Regal eingebaute Lesegeräte Empfang und Entnahme von Waren registrieren oder das Verfallsdatum feststellen. Auch der Einkaufswagen, die Umkleidekabine, die Waage etc. können mit Lesegeräten ausgestattet werden, damit die Kunden individuell beraten werden können und der Preis der eingekauften Ware automatisch berechnet wird. RFID-Kassensysteme erkennen die Einkäufe automatisch. Im Idealfall werden alle Tags an den Produkten gleichzeitig gelesen, was heute aber noch auf praktische Schwierigkeiten stösst. Am Ausgang des Warenhauses wird überprüft, ob die Tags deaktiviert bzw. die Produkte bezahlt worden sind. Die Identifizierung der Waren durch Tags erlaubt eine lückenlose Rückverfolgung ihrer Herkunft und des Transportwegs. Jede Station der Wertschöpfungskette hinterlegt auf dem Tag oder auf der zugehörigen Datenbank die relevanten Informationen, so dass die Kundin oder der Kunde beim Auslesen eines Produktes über dessen Herkunft informiert wird. Der Zugriff auf die Datenbank erfolgt via ONS vollautomatisch über das Internet. Entsprechende RFID-Systeme wurden bereits getestet, z.B. beim Future-Store der deutschen Metro-Gruppe, bei Wal Mart oder Tesco. In Entwicklung sind auch Anwendungen, bei den Kunden ihre Erfahrungen mit Produkten, z.B. Weinsorten, im Internet bekannt geben können (ähnlich wie die Kundenrezensionen für Bücher bei Amazon).

Artikelüberwachungssysteme (Electronic Article Surveillance EAS)

Elektronische Artikelüberwachungssysteme (engl. EAS: electronic article surveillance) werden zur Verhinderung von Diebstählen an den Ausgängen von Läden, Museen, Bibliotheken oder anderen öffentlich zugänglichen Orten mit gesicherten Wertgegenständen eingesetzt. Diese Systeme umfassen neben den Tags und dem Lesegerät auch ein Deaktivierungsgerät, mit dem das Personal die Tags an der bezahlten Ware deaktivieren kann, und evtl. einem Aktivierungsgerät bei Anwendungen wie z.B. in einer Biblio-

[20]Quelle:http://www.rfidproductnews.com/issues/2008.03/cover.story.php

thek, wo das Buch wieder zurückgebracht wird und der Tag von neuem aktiviert werden muss. Es gibt auch EAS-Systeme, bei denen die Tags an der Kasse mit einem besonderen Mechanismus entfernt und für andere Artikel wiederverwendet werden.

Lesegerät: Das Lesegerät besteht aus Sende- und Empfangeseinheiten, die auf einer oder beiden Seiten einer überwachten Zone stehen. Die Sendeeinheit strahlt ein elektromagnetisches Feld in die überwachte Zone ab, das anschliessend von der Empfangseinheit empfangen und ausgewertet wird.

Tag: Die Tags bestehen aus Metallstreifen oder einfachen elektrischen Schaltkreisen. Ist der Tag aktiv, so wird beim Passieren der überwachten Zone Alarm ausgelöst, im deaktivierten Zustand löst der Tag keinen Alarm aus. Aktivierte Tags verändern das von der Sendeeinheit abgestrahlten elektromagnetischen Feldes auf eine charakteristische Weise, so dass sie detektiert werden können. Diese Tags sind äusserst billig und sehr weit verbreitet.

Deaktivierungsgerät, Deaktivator: Wieder verwendbare Tags werden vom Bedienungspersonal nach erfolgter Zahlung entfernt, Einweg-Tags werden mittels eines Deaktivators so zerstört oder umprogrammiert, dass sie keine Störung des Feldes mehr verursachen. Deaktivatoren produzieren statische, gepulste oder wechselnde Magnetfelder, sie bestehen aus Permanentmagneten oder aus Wechselstrom durchflossenen Elektromagneten.

Artikelüberwachungssysteme werden, je nach Funktionsart und der verwendeten Frequenz, in verschiedene Gruppen aufgeteilt (Tabelle 2). Je nach verwendetem System ist die Überwachungszone mehr oder weniger breit (1 – 5 m).

Tabelle 2: *Verschiedene Artikelüberwachungssysteme (EAS-Systeme)*

	Magnetisch	**Akusto-magnetisch**	**Frequenzteiler**	**Radiofrequenz**	**Mikrowellen**
Tag	 Quelle [21]	 Quelle [22]	Chip und Schwingkreis-spule Hartetikette	 Quelle [23]	Diode Hartetikette
Breite der Zone (m)	1,5	5	?	2	?
Verwendung	Bibliotheken, Waren aus Metall	sehr verbreitet	?	?	Textilien
Grundfrequenz	10 Hz – 20 kHz	35; 58; 132 kHz	100 -135 kHz	1,8 – 8,6 MHz	916 MHz, 2,45; 5,6 GHz
Zusatzfrequenz	20 Hz – 5 kHz	keine	keine	85; 141 Hz	2- und 3-faches der Grundfrequenz
Pulsung	keine	50 – 90 Hz	12.5, 25 Hz	keine	
Deaktivation	50 – 650 Hz	statisches Mag-netfeld	Tag entfernen	RF Puls	Tag entfernen
Reaktivation	keine	Wechselfeld	Tag wieder an-bringen	keine	Tag wieder anbringen

Anwendungen in der Medizin

In der Medizin und im Spital gibt es sehr verschiedene Einsatzbereiche der RFID-Technologie, z.B. in der Logistik oder zur Identifizierung von Personen, Medikamenten, Instrumenten oder Mobiliar.

[21] http://www.highdubai.com/pics/TH_67425_2.JPG
[22] http://en.wikipedia.org/wiki/Image:RFID_and_magneto-acoustic_tags.JPG
[23] http://static.howstuffworks.com/gif/anti-sec-tag3.jpg

Patientenidentifizierung: Um Verwechslungen z.B. bei Operationen, bei der Zuordnung von Blutproben oder beim Verabreichen von Medikamenten zu vermeiden, ist es wichtig, dass Patienten eindeutig identifiziert werden. Dazu kann den Patienten z.B. ein Armband mit einem Smartlabel angelegt werden. Auf dem Armband ist die Patientennummer gespeichert, welche die behandelnde Person z.B. mit einem RFID-fähigen PDA (personal digital assistent, mobiler Computer) auslesen kann (Abbildung 4A). Via WLAN kann dann auf einen Server zugegriffen werden, auf dem die Behandlungsdaten gespeichert sind. Solche Armbänder wurden im Kantonsspital St. Gallen erfolgreich in einem Pilotprojekt getestet. In Grossbritannien werden in Spitälern auch aktive Tags (Abbildung 4B) zur Babydiebstahlsicherung und Identifikation durch die Mutter eingesetzt.

A

B

***Abbildung 4 Patientenidentifizierung: A** Armband kann durch einen PDA ausgelesen werden (Quelle[24]); **B** aktiver Tag zur Babydiebstahlsicherung (Quelle[25])*

Identifizierung von Medikamenten: Laut einer Studie des Universitätsspitals Genf leiden jährlich in der Schweiz 20'000 Spitalpatienten unter Komplikationen, weil sie ein falsches Medikament erhalten haben. Dies kann passieren, weil rund zwei Drittel aller Medikamente unvollständig beschriftet sind. Dieses Problem könnte durch eine eindeutige Kennzeichnung der Medikamente durch einen Strichcode (wie dies in den USA vorgeschrieben ist) oder evtl. durch einen RFID-Tag behoben werden.
Weltweit sind auch gefälschte Medikamente ein grosses Problem. Eine eindeutige Identifizierung der Medikamentenpackung durch RFID könnte Fälschungen wesentlich erschweren.
Identifizierung von Blutkonserven: Momentan werden Blutkonserven mit Hilfe von Strichcodes eindeutig identifiziert. Viele Konserven müssen vernichtet werden, weil unklar ist, ob sie wegen mangelnder Kühlung verdorben sind. In Zukunft (ab 2008) können die Blutbeutel mit einem Temperatursensor und einem RFID-Tag versehen werden, welcher die Identifikations- und Temperaturdaten speichert. Ein entsprechendes Pilotprojekt läuft am Kantonsspital St. Gallen seit 2007
Operationsmaterial: Bei einer Operation werden viele Tücher, Tupfer und Instrumente verwendet. Um sicher zu gehen, dass kein Operationsmaterial im Patienten gelassen worden ist, muss das Material während und nach der Operation gezählt werden. Durch das Anbringen von RFID-Tags am Operationsmaterial soll das Nachzählen des Materials automatisiert und das Auffinden z.B. eines Tupfers im Patienten erleichtert werden. Ein Pilotprojekt dazu läuft im Klinikum Rechts der Isar in München.

***Abbildung 5:** Operationstuch mit RFID-Tag[26]*

Bettenmanagement: Für eine effiziente Nutzung der Ressourcen ist es im Spital wichtig, den Überblick darüber zu haben, wo sich gerade welches Gerät oder welches Bett befindet. Im Inselspital in Bern wer-

[24] Siemens
[25] http://www.guardian.co.uk/uk_news/story/0,,1507497,00.html
[26] Quelle: Siemens

den seit 2006 für das Bettenmanagement die Bettgestelle mit aktiven RFID-Tags und die Matratzen mit passiven Tags versehen. An den Türen befinden sich Lesegeräte, welche die Tags an den durchfahrenden Betten zum Senden auffordern und registrieren. So ist es immer klar, wo sich welche sauberen Betten befinden und welche Matratzen sterilisiert sind.

Abbildung 6: *Bettenmanagement am Inselspital*[27]

Patientenlokalisierung: In Pflegeeinrichtungen z.B. für desorientiert Patienten können Lokalisierungssysteme mit RFID-Technologie verwendet werden (z.B. Spital Le Locle und Home Le Castel St. Blaise). Der Patient trägt einen aktiven Tag. Einerseits kann so überwacht werden, wo sich welcher Patient befindet, andererseits können Türen selektiv gewisse Personen durchlassen (z.B. Personal, Besucher) und andere nicht (z.B. Patienten). Ein anderes System ist der mobile Schwesternruf, bei dem die Patientin überall mittels Knopfdruck um Hilfe rufen kann. Mit Hilfe des Tags ist ersichtlich, woher der Hilferuf kam (realisiert im Home SIKNA Zürich und Home Le Castel St. Blaise). Da auch das Personal mit Tags ausgerüstet ist, wird der Hilferuf automatisch im Server dokumentiert und bei Annähern der Pflegeperson der Alarm mit der Personal-Nummer quittiert. Bei Nichtbeachtung des Alarms eskaliert der Hilferuf zur Einsatzzentrale. Ähnlich funktionieren auch Personalschutzsysteme, mit denen das Pflegepersonal bei einer Attacke um positionsabhängige Hilfe rufen kann.

eHealth[28]

Am 27. Juni 2007 hat der Bundesrat die «Strategie eHealth Schweiz» für die Jahre 2007 – 2015 genehmigt. Kernelemente der Strategie sind eine Versichertenkarte und ein elektronisches Patientendossier, das Ärzten und anderen Leistungserbringern des Gesundheitswesens mit dem Einverständnis des Patienten Zugriff auf behandlungsrelevante Informationen ermöglicht. Die Versichertenkarte, welche 2009 eingeführt wird und auf der Notfalldaten des/der Versicherten gespeichert werden können, wird eine kontaktbehaftete Chipkarte sein (mit Goldchip) und nicht auf RFID-Technologie basieren. Bei der Umsetzung der eHealth-Strategie steht keine Technologie im Vordergrund. Bei Umsetzungsentscheiden, welche die Bevölkerung betreffen, werden Akzeptanzmassnahmen zu prüfen sein.

Zugangskontrolle

Mit kontaktlosen RFID-Zugangskontrollen wird der Zutritt von berechtigten Personen zu den für sie freigegebenen Bereichen in Gebäuden oder Arealen gesteuert. Tags müssen in der Regel in einem geringen Abstand an den Lesegeräten vorbeigeführt werden, können in Abhängigkeit von der Sendeleistung des Lesegeräts aber bis hin zu einem Meter und mehr erkannt werden. Sehr verbreitet sind Chipkarten im ISO-Kartenformat und Schlüssel, welche einerseits mechanisch ins Schloss passen müssen und andererseits einen RFID-Tag integriert haben, der durch den Leser im Schloss ausgelesen wird. Tags lassen sich auch in Schlüsselanhänger, Armbanduhren, Handys, Kleidungsstücke integrieren. Zutrittskontroll- und elektronische Zahlungssysteme mit implantierten Tags existieren im Ausland für Besucher von Diskotheken, die einen sofortigen Zutritt zum Lokal wünschen. Neuerdings werden RFID-Tags auch bei elektronisch gesteuerten Katzenklappen verwendet, die einen zeitgesteuerten Zugang für mehrere Katzen erlauben.

[27] Quelle: D.Gürlet, Ocha GmbH
[28] http://www.ehealth.admin.ch

Es wird zwischen Online- und Offline-Systemen unterschieden: Online-Systeme bestehen aus einem Lesegerät (Terminal), das die Identifikationsnummer empfängt und diese an die Datenbank eines zentralen Rechners übermittelt. Die Entscheidung über den Zutritt erfolgt durch den zentralen Rechner. Online-Systeme eignen sich für Zutrittskontrollen bei wenigen Eingängen, die von vielen Personen benutzt werden (Verwaltungsgebäude, Skilifte etc). Tags müssen nur wenige Informationen gespeichert haben, da die weiteren notwendigen Informationen in der Datenbank gespeichert sind
Bei Offline-Systemen erfolgt die Entscheidung über die Zutrittsberechtigung im Terminal: Offline-Systeme eignen sich für die Kontrolle von Räumen, die nur von wenigen Personen benutzt werden (z.B. Hotelzimmer) Bei Offline-Systemen sind sämtliche notwendigen Informationen auf dem Tag gespeichert, das Terminal prüft diese Schlüsselkennungen und gibt bei Übereinstimmung mit den eigenen gespeicherten Informationen den Zutritt frei.

Tieridentifizierung

Tieridentifikationen mittels RFID haben den Vorteil, dass die Identifikationsinformationen keiner Alterung unterworfen sind. Tags werden bei Tieren in der Landwirtschaft, Wildtieren, Haustieren und Zootieren angewendet. Grundsätzlich eignen sich alle Tierarten, die von ihrer Grösse her einen RFID-Tag aufnehmen können. Das Tier erhält eine weltweit eindeutige Identifikationsnummer.
In der **Rinderhaltung** werden Halsbandtags sowie Ohrmarkentags und implantierbare Tags, die unter der Haut platziert sind, und auch Boli, welche im Vormagentrakt (Pansen) abgelegt sind, verwendet.
In der **Schweinehaltung** läuft in der Schweiz das Projekt „Elektronische Ohrmarken für eine lückenlose automatische Identifikation von Schweinen von der Geburt bis zur Schlachtung“[29]. Es hat zum Ziel, die Handhabbarkeit verschiedener Ohrmarken von der Kennzeichnung der Tiere bis zur Entnahme am Schlachtkörper in verschiedenen schweizerischen Haltungssystemen zu untersuchen. Der Tag speichert Daten zur Herkunft, Abstammung, Impfungen, Gesundheit des Tiers. Die automatische Futterzuteilung geschieht mit einem Lesegerät am Trog, ein Sensor misst die Körpertemperatur des Tiers und speichert diese auf dem Tag. Zusätzlich ist dient das System auch der Diebstahlsicherung.

Abbildung 7: *Schwein mit Ohrmarke*[30]

In der Schweiz gilt für **Hunde** gemäss Tierseuchenverordnung eine Kennzeichnungspflicht, bei der die Implantation von RFID-Tags obligatorisch ist. Die Implantation ist gemäss Verordnung über Einfuhr von Heimtiere auch bei Hunden, Katzen und Frettchen obligatorisch, die in die Schweiz eingeführt werden. Bis 2011 besteht eine Übergangsfrist für Kennzeichnungen mittels Tätowierungen.
Der auf dem Tag gespeicherte Informationscode wird zusammen mit weiteren Angaben (Datum der Implantation, Tiername, Geschlecht, Rasse, Abstammung, Angaben zu Tierhalter und kennzeichnendem Tierarzt) in der Schweiz in der Anis-Heimtierdatenbank [31] registriert.

Implantierte Tags für Menschen

Es werden auch RFID-Systeme mit implantierbaren Tags für Menschen eingesetzt. Wie bei den Haustieren wird der kleine Glaszylinder mit dem Tag unter die Haut gespritzt. Der implantierbare Tag wurde in den USA durch die Food and Drug Administration (FDA) als Medizinprodukt zugelassen. Der Tag wird

[29] Forschungsanstalt Agroscope Reckenholz-Tänikon
[30] Quelle: www.art.admin.ch
[31] www.anis.ch

von Spitälern zur Patientenidentifikation und in Betrieben für Zutrittskontrollen implantiert. Auf dem Tag ist nur eine Identifikationsnummer gespeichert. Das Spital hat Zugriff auf einen Server, auf dem die entsprechenden Patientendaten bereitliegen. In Grossbritannien wird der Einsatz von implantierten Tags in Kombination mit GPS für den elektronisch überwachten offenen Strafvollzug (electronic monitoring) erwägt.

Industrie und Logistik

In der Industrie werden RFID-Systeme in der Logistik und der Automation eingesetzt. In der Automobilindustrie z.B. werden die einzelnen Produktionsabläufe (z.B. Lackieren in der richtigen Farbe) durch RFID-Systeme gesteuert und überwacht. So können auch Einzelanfertigungen automatisch hergestellt werden. RFID-Systeme werden auch in der Lagerbewirtschaftung, zur Lokalisierung von Geräten, zum Kennzeichnen von Behältern etc. eingesetzt. Dies kann die Effizienz und auch die Sicherheit erhöhen, z.B. indem automatisch erkannt wird, dass in einem Lager Kerosin und explosive Stoffe nicht nebeneinander gelagert werden. Auch die Angestellten können mit RFID-Tags versehen werden, um zum Beispiel bei einem Unfall die einzelnen Personen lokalisieren zu können oder bei Einzelarbeitsplätzen in kritischen Bereichen eine Ohnmacht der Person detektieren zu können.
In logistischen Betrieben werden RFID-Systeme zur effizienten Steuerung und Überwachung des Warenflusses eingesetzt.

Abbildung 8: *Fertigungssystem-Ortung mit UWB (vgl. Kap. 2.2)beim Fahrzeugbau*

Bibliotheken

In Bibliotheken werden RFID-Systeme nicht nur zur Diebstahlsicherung sondern auch zur Selbstausleihe eingesetzt (z.B. in der Berner Kornhausbibliothek ab Sommer 2008). Beim Terminal wird der Benutzerausweis eingelesen und die Informationen auf den RFID-Tags in den Büchern. Die Bücher werden auf dem entsprechenden Konto verbucht und die Diebstahlsicherung wird deaktiviert. Dies wird alles durch die Bibliotheksbenutzer erledigt, es braucht dazu kein Personal.

Verkehr

Im **Zugverkehr** wird in Europa ein einheitliches Eisenbahnverkehrsleitsystem, das European Train Control System (ETCS), eingeführt. Bestandteil davon sind die Eurobalisen in den Schwellen, welche mit einem RFID-Tag versehen sind und dem Zug sicherheitsrelevante Daten wie die Position mitteilen.
Im **Auto** werden RFID im Schlüssel für die Wegfahrsperre eingesetzt. In Malaysia sind die Nummernschilder mit einem aktiven RFID-Tag versehen, der bis zu einer Distanz von 100 m ausgelesen werden kann. In London wird dieses System auch in Betracht gezogen, um Mautprellern mit gefälschten Nummernschildern auf die Schliche zu kommen.
In Dänemark wird mit Hilfe eines RFID-Systems die Sicherheit der **Velo**fahrer erhöht. Am Velo wird ein aktiver RFID-Tag angebracht, welcher an besonders gefährlichen Kreuzungen ein Warnsignal für Lastwagenfahrer aufleuchten lässt.

Zahlungsverkehr

Der elektronische Zahlungsverkehr mittels RFID verbreitet sich momentan in folgenden Gebieten:
Mautsysteme: RFID-basierte Mautsysteme werden in Österreich zur Bezahlung der LkW-Maut verwendet. Die RFID-Tags sind in einer Box an der Windschutzscheibe befestigt und enthalten Daten über das Kennzeichen und die Art des Fahrzeugs. An den Autobahnen sind brückenförmige Mautportale mit RFID-Lesegeräten angebracht, welche die Tags bei voller Fahrt des Tags auslesen und die Maut abbuchen. Bezahlt wird entweder mit einem vorher bezahlten Guthaben oder mit Kreditkarte. Ähnliche Systeme werden in Italien zur Bezahlung der Autobahngebühren verwendet.
Elektronische Fahrkarten bei öffentlichen Transportmitteln: Im öffentlichen Verkehr werden herkömmliche Fahrkarten z.T. durch kontaktlose elektronische Fahrkarten ersetzt weil sich die Verkehrsbetriebe davon kleinere Schwarzfahrerraten und schnellere Abfertigungszeiten versprechen. Die Oyster Card in London ist eine solche elektronische Fahrkarte mit RFID (Abbildung 9).
Kontaktlose Kreditkarten: Momentan kommen kontaktlose Kreditkarten zur Anwendung, mit denen sich Transaktionen kleiner Geldbeträge durchführen lassen, ohne dass die Karte in ein Lesegerät gesteckt werden muss. Für die Transaktionen ist keine Eingabe eine PIN nötig, allerdings verfolgen die Chips auf den Karten die Zahlungsaktivitäten und verlangen aus Sicherheitsgründen in unregelmässigen Abständen die Eingabe einer PIN.

Abbildung 9: *Teilweise zerstörte Oyster Card mit RFID-Tag rechts unten*[32]

Elektronischer Reisepass

Reisepässe werden zunehmend mit elektronisch lesbaren Merkmalen ausgestattet. Die Überprüfung der Identität kann damit automatisiert und beschleunigt werden, Passfälschungen und das Reisen mit einem fremden Pass werden erschwert.
In der Schweiz kann seit dem 4.9.2006 im Rahmen eines Pilotprojekts der elektronische Pass 06 beantragt werden, der mit einem RFID-Tag ausgerüstet ist. Auf dem Chip sind alle Daten gespeichert, die auch im Pass in gedruckter Form enthalten sind. Dazu gehört ein Passfoto in digitaler Form, das mit dem gedruckten Foto im Pass identisch ist. Möglich wird auf diese Weise ein elektronischer Vergleich zwischen dem gespeicherten Gesichtsbild und dem Live-Bild der Person, die den Pass vorlegt.
Datenschutz und Informationssicherheit werden durch elektronische Signaturen und Schlüssel gewährleistet. Die gespeicherten Daten werden so abgelegt, dass sie nach der Herstellung des Passes nicht mehr verändert werden können. Zudem kann anhand einer elektronischen Signatur jederzeit die Authentizität der Daten überprüft werden; die gespeicherten Daten werden dazu durch die ausstellende Behörde elektronisch unterschrieben. Die Daten können von RFID-Lesegeräten nur aus kurzer Distanz und bei Vorhandensein des dazu notwendigen elektronischen Schlüssels gelesen werden. Für die Berechnung des korrekten Schlüssels muss der Pass geöffnet werden, so dass das Lesegerät die maschinenlesbare Zone optisch lesen und aus diesen Informationen den Schlüssel errechnen kann.
In Zukunft sollen in der Schweiz nur noch elektronische Pässe ausgestellt werden, die gemäss den Standards der Europäischen Union zudem zwei Fingerabdrücke enthalten. Mittels eines elektronischen Zertifikats kann in diesen zukünftigen Pässen gesteuert werden, welche Stellen in welchen Ländern den Zugriff auf die im Ausweis gespeicherten Daten erhalten.

[32] http://en.wikipedia.org/wiki/Image:Oyster_card_partially_destroyed.jpg

2.4 Technologische Risiken

Die oben erwähnten Vorteile der RFID-Technologie gegenüber verwandten Technologien wie z.B. Strichcode (Kap. 2.1) sind wie alle neuen technischen Möglichkeiten auch mögliche Ausgangspunkte von Missbrauch und anderen Risiken (Abbildung 10):

- RFID-Tags können grundsätzlich unbemerkt ausgelesen werden, also auch ohne Wissen und Zustimmung des Besitzers des gekennzeichneten Objekts (vgl. Kap. 5.1). Entscheidend ist hierfür die maximale Lesedistanz, die stark von der verwendeten Technologie abhängig ist (von Millimetern bis zu mehreren Metern).
- Wenn weltweit eindeutige Identifikationsnummern für Produkte vergeben werden, ist es prinzipiell möglich, den Weg dieser Produkte (z.B. eines Kleidungsstücks, eines Buches oder Koffers) weltweit zu verfolgen. Damit können Bewegungsprofile von Personen erstellt werden, falls man die Gegenstände Personen mit hinreichender Wahrscheinlichkeit zuordnen kann. Voraussetzung ist allerdings, dass die Tags immer wieder mit entsprechenden Lesegeräten ausgelesen werden und dass die Daten an zentraler Stelle zusammengeführt werden.
- Wenn neben der Identifikationsnummer zusätzliche Daten auf RFID-Tags gespeichert werden, besteht ein zusätzliches Risiko der Verfälschung dieser Daten durch Dritte. Daten auf einem RFID-Tag sind schlechter gegen unautorisierten Zugriff geschützt als Daten in einer Datenbank.
- Insgesamt besteht bei zunehmender Abhängigkeit alltäglicher Vorgänge von RFID ein höheres Risiko, von einem Ausfall der Systeme betroffen zu werden. Ausfälle können technisch bedingt sein oder aber durch Hacker-Angriffe oder gezielte physikalische Störung des Systems verursacht werden. Aufgrund der höheren Komplexität und Vernetzung der RFID-Technologie im Vergleich zu konventionellen Identifikationssystemen (wie Strichcode) sind die Möglichkeiten der Störung vielfältiger.

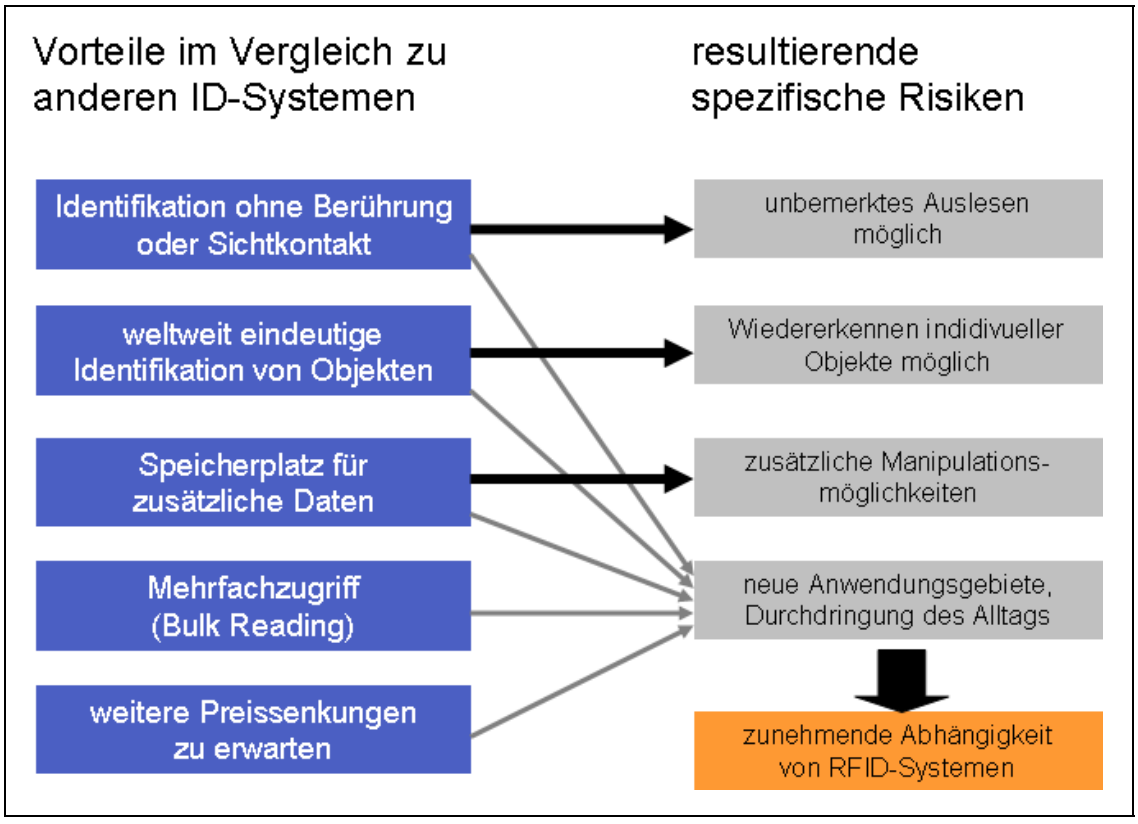

Abbildung 10: *Spezifische Vorteile und Risiken von RFID* [33]

[33] Quelle: Lorenz Hilty (Empa), Vortrag BAG, Bern, 24.10.07

3. Strahlung, gesundheitliche Auswirkungen und elektromagnetische Verträglichkeit

3.1 Strahlung und Exposition

In einem RFID-System wird die Information zwischen dem Tag und dem Lesegerät durch elektromagnetische Felder (EMF) übermittelt. Diese Felder werden durch das Lesegerät und zum Teil auch durch den Tag erzeugt. Bei Artikelüberwachungssystemen (EAS, vgl. Kapitel 2.3) kommt noch das Deaktivierungsgerät als Quelle von Feldern hinzu. Es werden für verschiedene RFID-Systeme ganz unterschiedliche Frequenzen und Sendeleistungen eingesetzt (Tabelle 1, Kapitel 2.2), die Charakteristik der Felder ist deshalb sehr unterschiedlich.

Im Strahlenschutz werden folgende Begriffe verwendet, um die Stärke der Strahlung sowie ihre Wirkungen zu bezeichnen:

- **Emission** ist die Strahlung, die von einer Strahlungsquelle ausgesendet wird.
- **Immission** ist die Strahlung an einem bestimmten Ort. Die Immission ist meistens niedriger als die Emission, da die Strahlung zwischen der Strahlungsquelle und dem Ort der Immission abgeschwächt werden kann. Die Stärke der Strahlung nimmt mit dem Abstand zur Quelle ab.
- **Exposition** ist die Strahlung (Immission), welcher ein Objekt (Mensch, Tier, Pflanze, Boden oder Sachgut) während einer bestimmten Dauer (Expositionszeit) ausgesetzt ist.

Zur Beurteilung der Exposition werden neben der Stärke des auftreffenden Feldes auch die Dauer (Kurzzeit- oder Langzeitexposition), die betroffenen Körperteile (lokale Exposition, Teilkörper- oder Ganzkörperexposition) und die Situation (Exposition am Arbeitsplatz oder Exposition der Bevölkerung) berücksichtigt. Bezüglich der Exposition gegenüber Feldern von RFID-Systemen unterscheiden wir folgende Expositionsszenarien:

Lesegeräte

- Teilkörper- oder Ganzkörperexposition am Arbeitsplatz, Kurzzeit- oder Langzeitexposition
- Teilkörper- oder Ganzkörperexposition der Bevölkerung, Kurzzeit- oder Langzeitexposition

Tags

- Lokale Kurzzeit- oder Langzeitexposition am Arbeitsplatz
- Lokale Kurzzeit- oder Langzeitexposition der Bevölkerung

RFID-Tags

Passive RFID-Tags beziehen die Energie zum Aussenden der Informationen aus dem Feld des Lesegerätes beziehen (vgl. Kap. 2.1). Aktive Tags haben eine Batterie und erzeugen selber ein Feld, entweder, wenn sie durch ein Lesegerät dazu aufgefordert werden, oder unaufgefordert in bestimmten Zeitabständen. Zur Stärke dieser Felder gibt es bisher keine Untersuchungen.

Für mögliche Expositionsszenarien sind RFID-Tags von Interesse, welche am oder sogar im Körper getragen werden. Diese könnten zu lokalen EMF-Expositionen führen, möglicherweise auch über längere Zeit wie z.B. bei Personenlokalisierungssystemen. Es sind jedoch keine Daten dazu vorhanden, ob und wie stark Personen tatsächlich relevanten Feldern von RFID-Tags exponiert sind.

RFID-Lesegeräte und Deaktivierungsgeräte

RFID-Lesegeräte können grosse Sendeleistungen aufweisen (vgl. Kap. 2.4), was zu starken elektromagnetischen Feldern führen kann. Messungen dieser Felder wurden vor allem bei im Schleusenbereich von EAS-Systemen gemacht. In verschiedenen Untersuchungen[34] [35] [36] [37] [38] [39] [40] [41] wurden teilweise

[34] AKNIR. Arbeitskreis nichtionisierende Strahlung. Nichtionisierende Strahlung und Arbeitsmedizin. Strahlenschutzpraxis 1995;2:11-2.
[35] Allgemeine Unfallversicherungsanstalt. Messung und sicherheitstechnische Beurteilung der elektromagnetischen Felder im Bereich von Diebstahlsicherungsanlagen. 1998. http://www.auva.at/mediaDB/118617.PDF
[36] Casamento JP. Characterizing Electromagnetic Fields of Common Electronic Article Surveillance Systems, Compliance Engi-

sehr hohe Werte gemessen. Um einen Eindruck über die Stärke der Felder zu geben, werden diese mit dem ICNIRP-Referenzwert verglichen (vgl. Kapitel 3.3). Die höchsten Werte wurden bei den sogenannten „magnetischen" EAS-Systemen (vgl. Tabelle 2, Kap. 2.3) festgestellt. Bei Abständen unter 0,5 m wurden teilweise Werte gemessen, welche 10- bis 40-mal grösser als der ICNIRP-Referenzwert sind. Auch bei den modernsten Systemen, den „akustomagnetischen" EAS-Systemen, wurden sehr hohe Werte gemessen. Auch bei den EAS-„Radiofrequenzsystemen" wurden in Abständen unter 0.5 m Werte gemessen, die bis 10-mal grösser als der entsprechende Referenzwert sind. Bei EAS-„Mikrowellensystemen" wurden weniger Messungen durchgeführt, die gemessenen Werte lagen alle unter dem Referenzwert.
Zur Deaktivierung von RFID-Tags werden zum Teil sehr starke Permanentmagnete, starke niederfrequente Magnetfelder oder ein starker Hochfrequenzpuls verwendet (Kapitel 2.3). Auch hier wurden Werte gemessen, welche die entsprechenden Referenzwerte überschreiten.
Zur Stärke der Felder von anderen RFID-Lesegeräten sind nur sehr wenige Daten vorhanden.

Es ist nicht bekannt, wer in welchem Masse gegenüber Feldern von RFID-Systemen exponiert ist.
Mögliche Expositionsszenarien sind z.B:

- Kurzzeitexposition der allgemeinen Bevölkerung (auch Kinder, alte Menschen, schwangere Frauen) gegenüber Feldern von EAS, welche sehr stark sein können.
- Kurzzeit- oder evtl. Langzeitexposition von Berufstätigen (auch schwangeren Frauen), welche im Bereich von EAS-Toren oder an Deaktivierungsgeräten arbeiten.
- Langzeitexposition von Berufstätigen bei Einzelarbeitsplatzüberwachung, Personenlokalisierungssystemen, in der Logistik, in der Industrie.
- Teilkörperexpositionen von Berufstätigen durch Handlesegeräte.

Fazit

Über die Strahlung und die realen Expositionen von RFID-Systemen ist sehr wenig bekannt. Aus Messungen von EAS-Systemen ergeben sich Hinweise, dass die Felder unter Umständen sehr stark sein können. Forschungsbedarf besteht zu den Feldern von Lesegeräten, zu den durch sie verursachten Teil- oder Ganzkörperexpositionen sowie zu lokalen Expositionen durch Tags. Zudem wird ein Überblick benötigt, welche Expositionssituationen im Alltag vorkommen können (Exposition der Bevölkerung, am Arbeitsplatz, Dauer der Exposition, exponierte Körperteile).

3.2 Gesundheitliche Auswirkungen

Es gibt keine Studien, welche sich mit den gesundheitlichen Auswirkungen der Strahlung von RFID-Systemen befassen. Zur Beurteilung möglicher Gesundheitsrisiken müssen allgemeine Kenntnisse über Auswirkungen elektromagnetischer Feldern (EMF) herangezogen werden. Viele RFID-Systeme arbeiten im mittleren Frequenzbereich (kHz), für welchen die gesundheitlichen Auswirkungen sehr schlecht untersucht sind.

Die Wirkung eines elektromagnetischen Feldes auf den menschlichen Körper hängt stark von seiner Frequenz ab. Wissenschaftlich nachgewiesen sind folgende akute Auswirkungen, welche ab einem Schwellenwert auftreten:

---

neering 1999. http://www.ce-mag.com/archive/1999/sepoct/Casamento.html
[37] Cooper TG. Occupational Exposure to Electric and Magnetic Fields in the Context of the ICNIRP Guidelines. 2003. NRPB. http://www.hpa.org.uk/radiation/publications/w_series_reports/2002/nrpb_w24.htm
[38] Eskelinen T et al. Occupational exposure to magnetic fields from EAS devices. 2001. EBEA 2001 Helsinki.
[39] Estenberg U et al. Kartläggning av exponering för magnetfält runt larmbågar och RFID-system. 2006. http://www.ssi.se/ssi_rapporter/pdf/ssi_rapp_2006_03.pdf
[40] Harris C et al. Electromagnetic field strength levels surrounding electronic article surveillance (EAS) systems. Health Phys 2000;78:21-7.
[41] Kjellson N et al. Mätningar av magnetfält alstrade av kommersiella stöldskyddssystem. 2002. Arbetslivinstitutet. Arbetslivsrapport nr 2002:6, ISSN 1400-8211. http://mobil.svt.se/content/1/c6/57/82/74/arb2002_06.pdf

Muskel- und Nervenstimulationen: Elektromagnetische Felder in Frequenzbereich von 1 Hz – 10 MHz induzieren im Körper elektrische Felder und Wirbelströme. Ab bestimmten Schwellenwerten können diese Muskeln und Nerven stimulieren. Die relevante Dosisgrösse ist die Stromdichte im Körper (in Ampère pro Quadratmeter, A/m^2)
Thermische Effekte: Hochfrequente elektromagnetische Felder (100 kHz – 10 GHz) werden vom Körper absorbiert und führen zu einer Erwärmung des Gewebes. Eine Temperaturerhöhung von mehr als 1°C kann zu Gewebeschädigungen oder Problemen mit der Thermoregulation führen. Die relevante Dosisgrösse ist die im Gewebe absorbierte Energie, die spezifische Absorptionsrate (SAR in Watt pro Kilogramm, W/kg).

Im Frequenzbereich zwischen 100 kHz und 10 MHz sind beide Effekte vorhanden.

Diese nachgewiesenen Effekte bilden die Grundlage für die Festlegung der Grenzwerte (vgl. Kap. 3.3). Es bestehen aber gewisse Hinweise darauf, dass EMF auch unterhalb der Schwellenwerte weitere Auswirkungen haben könnten. Diese sind jedoch noch ungenügend untersucht. Die Unsicherheiten bestehen insbesondere bei Langzeitauswirkungen und Auswirkungen bei lokalen Körperexpositionen. Zudem bestehen offene Fragen bezüglich der biologischen Relevanz bestimmter Strahlungseigenschaften (Frequenz, Modulation, Pulsform, zeitliches Muster der Strahlung etc.).

Fazit

Gesundheitliche Auswirkungen der EMF von RFID-Systemen sind nicht erforscht, im Allgemeinen gibt es zu gesundheitlichen Auswirkungen von EMF viele Unsicherheiten. Bezüglich der RFID-Systeme besteht Forschungsbedarf zu Auswirkungen von Langzeitexpositionen, die unterhalb der Schwellenwerte für bisher nachgewiesene Wirkungen liegen, zu Auswirkungen von lokalen Expositionen sowie zu Auswirkungen von EMF im Kilohertz-Bereich.

3.3 Grenzwerte und rechtliche Vorschriften zur Strahlung

ICNIRP-Grenzwerte

Die **Grenzwertempfehlungen der ICNIRP** [42] (International Commission for Non-Ionizing Radiation Protection) basieren auf den vorher beschriebenen akuten Auswirkungen (Kap. 3.2). Wegen der Frequenzabhängigkeit der Auswirkungen von EMF gelten für verschiedene Frequenzen unterschiedliche Grenzwerte. Die empfohlenen Grenzwerte erlauben nur Felder, die mindestens um einen Faktor 50 für die Bevölkerung bzw. Um einen Faktor 10 für Arbeitnehmende unterhalb der Schwellenwerte für gesundheitlich relevante Effekte liegen.
Die ICNIRP-Grenzwerte sind für die Dosisgrössen (Körperstromdichte, SAR) definiert, sie werden **Basisgrenzwerte** genannt. Da die Dosisgrössen im Körper sehr schwierig zu messen sind, stehen zusätzlich **Referenzwerte** zur Verfügung, die angeben, wie gross das äussere verursachende magnetische oder elektrische Feld sein darf, damit der Basisgrenzwert nicht überschritten wird. Die Referenzwerte können nur angewendet werden, wenn die Feldquelle genügend weit entfernt ist, damit das Feld homogen ist, oder wenn das Feld über den Köper der exponierten Person gemittelt wird.

Bei lokalen Expositionen muss direkt die Dosisgrösse bestimmt und mit dem Basisgrenzwert verglichen werden. Sowohl Körperstromdichte als auch SAR können durch aufwändige numerische Simulationen bestimmt werden. Die induzierten Ströme und die absorbierte Energie hängen dabei stark von der Grösse einzelner Körperstrukturen und ihrer Lage im Feld ab. Für eine korrekte Überprüfung der Basisgrenzwerte müssen deshalb für unterschiedliche Körpermodelle (Männer, Frauen, Kinder) verschiedene Körperhaltungen im Feld simuliert werden. Die SAR kann auch experimentell mit Hilfe eines Phantoms bestimmt werden, welches dieselben elektrischen Eigenschaften wie der Körper hat.

[42] ICNIRP. Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields up to 300 GHz. Health Phys. 75: 494-521.

Eine aktuelle Untersuchung[43] an numerischen Modellen einer virtuellen Familie zeigt, dass trotz Einhalten des Referenzwertes der Basisgrenzwert bei der Frau und dem Kind überschritten werden kann, was auch durch eine andere Studie[44] bestätigt wird. Dieselbe Untersuchung zeigt auch, dass die von ICNIRP vorgeschlagene räumliche Mittelung des Feldes über den Körper lokale Überschreitungen des Basisgrenzwertes zulässt und deshalb nicht sinnvoll ist.
Eine weitere Studie[45], in welcher die Exposition eines Kindes gegenüber einem EAS-Lesegerät modelliert wird, zeigt ebenfalls ein Überschreiten des Basisgrenzwertes.

Grenzwerte und rechtliche Vorschriften zu EMF in der Schweiz

Umweltschutz: Verordnung über den Schutz vor nichtionisierender Strahlung (NISV)
Der Schutz vor schädlicher oder lästiger nichtionisierender Strahlung ist Gegenstand der Artikel 11 ff. des Umweltschutzgesetzes (USG). Die Verordnung über den Schutz vor nichtionisierender Strahlung (NISV),[46] welche die Vorschriften des USG hinsichtlich des Schutzes des Menschen konkretisiert, regelt die Emissionsbegrenzung der elektromagnetischen Strahlung im Frequenzbereich von 0 Hz bis 300 GHz, die beim Betrieb von ortsfesten Anlagen erzeugt wird.
Sie regelt jedoch nicht die Emissionsbegrenzung von Strahlung, die in Betrieben erzeugt wird, soweit sie auf das Betriebspersonal einwirkt, oder von Strahlung von Geräten wie Mikrowellenöfen, Kochherden, Elektrowerkzeugen oder Mobiltelefonen. Ebenfalls nicht geregelt wird in der NISV die Begrenzung der Einwirkungen von Strahlung auf elektrische oder elektronische medizinische Lebenshilfen wie Herzschrittmacher.
Für die allgemeine Bevölkerung sind in der NISV für den ganzen genannten Frequenzbereich Immissionsgrenzwerte festgelegt worden. Diese entsprechen den Referenzwerten der ICNIRP und sollen den Schutz des Menschen vor wissenschaftlich gesicherten, akuten schädlichen Einwirkungen sicherstellen. Die Immissionsgrenzwerte müssen überall dort eingehalten werden, wo sich Menschen – auch nur kurzfristig – aufhalten können. Sie gelten jedoch nur für Strahlung, die gleichmässig auf den ganzen menschlichen Körper einwirkt (Ganzkörperexpositionen).
Für einige Anlagetypen, z. B. Mobilfunkbasisstationen, Rundfunksendeanlagen, Hochspannungs- und Eisenbahnleitungen ist in der NISV eine vorsorgliche Emissionsbegrenzung definiert (Anhang 1 NISV). RFID-Anlagen werden darin nicht erwähnt. Bei Anlagen, für die Anhang 1 NISV keine Vorschriften enthält, ordnet die Behörde Emissionsbegrenzungen so weit an, als dies technisch und betrieblich möglich und wirtschaftlich tragbar ist.

Arbeitnehmerschutz
Der Arbeitnehmerschutz, d.h. die Gesundheit und Sicherheit am Arbeitsplatz, ist heute im Wesentlichen in zwei Gesetzgebungen geregelt. Während das Bundesgesetz über die Unfallversicherung (UVG)[47] die Arbeitssicherheit (Verhütung von Berufsunfällen und Berufskrankheiten) regelt, enthält das Arbeitsgesetz (ArG)[48] die Vorschriften über den allgemeinen Gesundheitsschutz.
Beim Auftreten von gesundheitsgefährdenden elektromagnetischen Strahlen muss der Arbeitgeber die erforderlichen Schutzmassnahmen treffen. Die Schweizerische Unfallversicherungsanstalt (Suva) hat für berufliche Expositionen Richtlinien über maximale Arbeitsplatz-Konzentrationen gesundheitsgefährdender Stoffe sowie über Grenzwerte für physikalische Einwirkungen erlassen (so genannte „MAK-Werte“). Die darin enthaltenen arbeitshygienischen Grenzwerte für EMF entsprechen den ICNIRP-Empfehlungen.

[43] Kühn S. et al.: Assessment of induced electromagnetic fields in the human body in the presence of heterogeneous field distributions. 29th Annual Meeting of the Bioelectromagnetics Society (BEMS 2007), Kanazawa, Japan, June 10–15, 2007.
[44] Conil E. et al. Variability analysis of SAR from 20 MHz to 2.4GHz for different adult and child models using finite-difference time domain. Phys. Med. Biol 53 (2008), 1511-1525.
[45] Gandhi OP et al. Calculation of induced current densities for humans by magnetic fields from electronic article surveillance devices. Phys Med Biol 2001; 46:2759-71.
[46] SR 814.710 Verordnung über den Schutz vor nichtionisierender Strahlung (NISV). 2000.
[47] UVG; SR 832.20
[48] ArG; SR 822.11

Produktebezogene Regelungen

In Bezug auf EMF und RFID sind folgende zwei Verordnungen von Interesse:

- Die Verordnung über Niederspannungserzeugnisse (NEV)[49] regelt elektrische Geräte wie beispielsweise Haushaltsgeräte, Lampen, gewisse RFIDs usw.
- Die Verordnung über Fernmeldeanlagen (FAV)[50] regelt alle Geräte oder Einrichtungen, die zur fernmeldetechnischen Übertragung von Informationen bestimmt sind oder benutzt werden, wie z.B. Mobiltelefone, Endgeräte von drahtlosen Netzwerken wie WLAN, ‚gewisse RFIDs, Mobilfunkantennen usw. Die FAV verweist für den Gesundheitsschutz und die elektrische Sicherheit auf die NEV.

In den beiden Verordnungen sind die Anforderungen an das Produkt in Bezug auf den Gesundheitsschutz vor EMF auf zwei Arten geregelt: Nach dem „new and global approach" und nach dem Prinzip der anerkannten Regeln der Technik. Nach dem „new and global approach" der EU[51] werden für das Inverkehrbringen grundlegende Sicherheits- und Gesundheitsanforderungen an das Produkt gestellt. Zur Konkretisierung dieser Anforderungen verweisen die Behörden auf international harmonisierte Produktenormen (siehe unten „Produktenormen für RFID" und Webseite des BAKOM [52]).

Gesetz über technische Handelshemmnisse und Verfahren der gegenseitigen Anerkennung

Bei der Vorbereitung, dem Erlass oder der Änderung von technischen Vorschriften im Reglungsbereich des Bundes müssen aufgrund verschiedener bi- und multilateraler Abkommen, welchen die Schweiz beigetreten ist, Handelshemmnisse vermieden werden. Gemäss dem Bundesgesetz über die technischen Handelshemmnisse[53] müssen die technischen Vorschriften der Schweiz so ausgestaltet sein, dass sie so wenige Handelshemmnisse wie möglich schaffen und im Rahmen des Möglichen mit den Vorschriften unserer Handelspartner vereinbar sind. Die Schweiz hat mit der Europäischen Gemeinschaft ein Abkommen zur gegenseitigen Anerkennung im Bereich der Konformitätsbewertung abgeschlossen (Mutual Recognition Agreement, MRA). Dieses Abkommen dient der Eliminierung technischer Handelshemmnisse beim Verkehr mit Industrieprodukten, da es die gegenseitige Anerkennung von Konformitäten zwischen der Schweiz und der EU vorsieht. Von diesem Abkommen sind beispielsweise Medizinprodukte, Telekommunikationsendgeräte und elektrische Betriebsmittel erfasst. Für fast alle unter das MRA fallenden Produktekategorien kann der schweizerische Gesetzgeber also in Bezug auf die Gesundheit keine strengeren Vorschriften erlassen als jene, die in der EU gelten. Abweichungen von diesem Grundsatz sind ausnahmsweise möglich, wenn sie durch ein überwiegendes öffentliches Interesse wie etwa dem Schutz der öffentlichen Ordnung, der Gesundheit oder der Umwelt gerechtfertigt sind.

EU Regelungen

Die Grenzwertempfehlungen der ICNIRP wurden in folgende EU Dokumente übernommen:

- Empfehlung (1999/519/EG)[54] bezüglich der Begrenzung der Exposition von Personen gegenüber EMF
- Richtlinie (2004/40/EG) über Mindestvorschriften zum Schutz von Sicherheit und Gesundheit der Arbeitnehmer vor der Gefährdung durch physikalische Einwirkungen.

[49] NEV; SR 734.26
[50] FAV; SR 784.101.2
[51] Vgl. Nichtionisierende Strahlung und Gesundheitsschutz in der Schweiz: Grundlagen (Kap. 4.3.2), www.bag.admin.ch/nis-bericht
[52] www.bakom.admin.ch/org/grundlagen/00563/00575/01142
[53] Bundesgesetz vom 6. Oktober 1995 über die technischen Handelshemmnisse, SR 946.51
[54] Empfehlung des europäischen Rates 1999/519/EG bezüglich der Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern

Internationale Produktenormen für RFID

Auf Basis der Empfehlung 1999/519/EG wurden den europäischen Standardisierungsgremien Mandate erteilt, Produktenormen bzw. Anforderungen an Mess- und Beurteilungsprozesse zu definieren.
Die zulässige Strahlenbelastung durch RFID-Systeme ist in der europäischen und schweizerischen harmonisierten Norm EN SN 50364[55] geregelt. Die dazugehörige Grundnorm 50357[56] beschreibt die Anforderung an die zu verwendende Messmethodik. Die Anforderung ist erfüllt, wenn durch eine der folgenden Methoden das Einhalten des Grenzwertes gezeigt werden kann.

1. Messung der elektromagnetischen Felder in vorbestimmten Abständen zum Gerät und Vergleich des Maximalwertes mit dem Referenzwert
2. Messungen der elektromagnetischen Felder in vorbestimmten Abständen zum Gerät, räumliche Mittelung und Vergleich mit dem Referenzwert.
3. Numerische oder experimentelle Bestimmung der Körperstromdichte bzw. der thermischen Effekte und Vergleich mit den Basisgrenzwerten.

Der vorgeschriebene Messabstand ist je nach Aufbau des Systems 10, 20 oder 30 cm. Kleinere Distanzen durch direkten Kontakt der Personen mit den Lesegeräten (z.B. Skilift-Zugangskontrolle, handgeführte RFID-Lesegeräte bei implantierten Tags) sind jedoch in alltäglichen Situationen durchaus zu erwarten.
Die numerischen Simulationen werden entweder an homogenen Sphäroiden durchgeführt, welche dieselben elektrischen Eigenschaften und Ausdehnungen haben wie ein Mensch, oder an Modelldaten eines erwachsenen Mannes.

Die Grundnorm 50357 von 2001 wird demnächst durch die neue Norm IEC 62369-1[57] abgelöst, welche einen grösseren Frequenzbereich abdeckt (bis 300 GHz statt bis 10 GHz). Die Methoden bleiben jedoch dieselben. Wegen der in Kapitel 3.3 erwähnten Probleme wurde von der Schweiz für die neue Norm unter anderem gefordert:

- Einhalten der Basisgrenzwerte auch in numerischen Modellen von Kindern
- Keine räumliche Mittelung der Messwerte
- Messung in geringerem Abstand zum Gerät

Da diese Forderungen nicht erfüllt wurden, hat die Schweiz im Abstimmungsverfahren gegen die Norm gestimmt. Da die Norm jedoch von der Mehrheit akzeptiert worden ist, wird sie trotz ihrer Mängel auch in der Schweiz gelten,

Fazit

Das Einhalten der Basisgrenzwerte wird meist mit Hilfe der Referenzwerte überprüft. Die ICNIRP-Referenzwerte sind nicht genügend konservativ, um dies zu garantieren, und müssen überarbeitet werden. Eine räumliche Mittelung eines inhomogenen Feldes ist nicht sinnvoll, da so lokale Grenzwertüberschreitungen übersehen werden. Zur Überprüfung der Basisgrenzwerte braucht es exakte anatomische Modelle von Menschen mit unterschiedlichem Körperbau.
Die geltende und die zukünftige Norm taugen nicht dazu, in allen realen Alltagssituationen ein Einhalten der ICNIRP-Basisgrenzwerte zu garantieren. Die Norm muss so überarbeitet werden, dass sie das Einhalten der Basisgrenzwerte bis zum minimal zugänglichen Abstand (also unter Umständen 0 cm) garantiert. Bei kleinen Abständen kann dies nur durch eine experimentelle Messung der Dosisgrössen in einem Phantom geschehen. Dazu müssen standardisierte Messverfahren zur Überprüfung der Basis-

[55] CENELEC: Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die im Frequenzbereich von 0 Hz bis 10 GHz betrieben und in der elektronischen Artikelüberwachung (en: EAS), Hochfrequenz-Identifizierung (en: RFID) und ähnlichen Anwendungen verwendet werden; EN SN 50364:2001
[56] CENELEC: Ermittlung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die in der elektronischen Artikelüberwachung (en: EAS), Hochfrequenz-Identifizierung (en: RFID) und ähnlichen Anwendungen verwendet werden; EN SN 50357:2001
[57] IEC: Evaluation of human exposure to electromagnetic fields from Short Range Devices (SRDs) in various applications over the frequency range 0-300 GHz. Part 1: Fields produced by devices used for Electronic Article Surveillance, Radio Frequency Identification and similar systems. IEC 62369-1

grenzwerte entwickelt werden. Bei numerischen Modellen müssen auch Modelle von Frauen und Kindern berücksichtigt werden. Eine räumliche Mittelung bei einem inhomogenen Feld ist nicht zulässig.

3.4 Elektromagnetische Verträglichkeit: Störungen von Implantaten

Elektromagnetische Verträglichkeit (EMV) bezeichnet den Zustand, dass technische Geräte einander nicht durch elektromagnetische Felder störend beeinflussen. EMV setzt voraus, dass auf der einen Seite ein Gerät, welches EMF erzeugt, gewisse Grenzwerte einhält, und dass auf der anderen Seite ein Gerät, welches in den Bereich dieser Felder kommt, eine gewisse Störfestigkeit besitzt. Von besonderem Interesse sind dabei aktive elektronische Implantate wie Herzschrittmacher oder implantierte Defibrillatoren. Diese Implantate sind weit verbreitet, die Patienten können in verschiedenen Situationen elektromagnetischen Feldern ausgesetzt sein, welche möglicherweise ihr Implantat stören. Daraus entstehende gesundheitliche Auswirkungen sind nur indirekt Auswirkungen der EMF.

Beeinflussung von Implantaten durch EAS-Systeme

Zu möglichen Störungen von elektronischen Implantaten durch Artikelüberwachungssysteme wurden mehrere Studien durchgeführt. Ein Review der zwischen 1973 und 1999[58] durchgeführten Studien kommt zum Schluss, dass gewisse Artikelüberwachungssysteme Fehlfunktionen bei Implantaten auszulösen können. Die Autoren folgern, dass durch diese Fehlfunktionen keine lebensgefährlichen Risiken entstehen sollten unter der Voraussetzung, dass Personen mit Implantaten die Artikelüberwachungssysteme schnell durchschreiten.
Gemäss der amerikanischen Food and Drug Administration[59] kann das normale Funktionieren von elektronischen Medizinprodukten wie Herzschrittmachern und Defibrillatoren durch Artikelüberwachungsgeräte gestört werden. Die Behörde empfiehlt im Jahr 1998 Personen mit elektronischen Medizinprodukten, sich nicht länger als nötig in der Nähe von Artikelüberwachungssystemen aufzuhalten, sich nicht gegen die Systeme zu lehnen und sich bewusst zu sein, dass die Systeme unter Umständen nicht gut erkennbar sind. Im Jahre 2000 empfiehlt die FDA, Artikelüberwachungssysteme so zu kennzeichnen, das Personen vor dem Eintreten in den überwachten Bereich auf das Vorhandensein eines Systems aufmerksam werden.
Die Folgerungen der FDA werden in einem umfassenden Review der ICNIRP von 2002[60] bestätigt. Die ICNIRP stellt eine Reihe von Empfehlungen für Sicherheitssysteme (Artikelüberwachungssysteme, andere RFID-Systeme und Metalldetektoren) auf:

- Wissensbeschaffung zu möglichen Interaktionsmechanismen zwischen Implantaten und den Feldern von Sicherheitssystemen, zu optimierten Designs und Testprozeduren sowohl für Implantate als auch Sicherheitssysteme. Einsetzen einer europäischen Arbeitsgruppe, in der sowohl die Hersteller von Implantaten als auch Sicherheitssystemen beteiligt sind. Angestrebt soll die Förderung des Informationsaustausches über bestehende und neue Produkte werden, um so Störungen von aktiven Implantaten durch Sicherheitssysteme zu minimieren
- Information durch die Implantatshersteller über mögliche Gefahren zuhanden der Ärzteschaft und der Personen mit Implantaten: Desgleichen Information über mögliche Risiken in der Produktinformation von Sicherheitssystemen bzw. Einführung eines entsprechenden Labelling bei den Geräten
- Verbesserte Risiko-Information der Personen mit Implantaten durch Ärzteschaft, Gesundheitsbehörden und Fachgremien

[58] Kainz W et al. Electromagnetic compatibility of electronic implants--review of the literature. Wien.Klin.Wochenschr. 2001;113:903-14.
[59] FDA. Important Information on Anti-Theft and Metal Detector Systems and Pacemakers, ICDs, and Spinal Cord Stimulators. 1998. http://www.fda.gov/cdrh/safety/easnote.html
[60] ICNIRP. Possible health risk to the general public from the use of security and similar devices 2002. ISBN 3-934994-01-6. http://www.icnirp.de/documents/ExSummary.pdf

- Datenbeschaffung zu den Charakteristiken der Felder von Sicherheitssystemen sowie den auftretenden Interferenzen mit aktiven medizinischen Implantaten. Die Daten müssen öffentlich für Hersteller, Ärzteschaft und Patienten zugänglich sein
- Durchführung von Studien über die funktionellen und technologischen Limitationen von aktiven Implantaten, Einfluss der Feldeigenschaften, Erarbeitung von verfeinerten Interaktionsmodellen, Kompatibilitätsprüfung von neuen Technologien wie Neurostimulatoren
- Ziel für Standardisierungsgremien und Hersteller von Implantaten und Sicherheitssystemen ist es, gemeinsame Grenzwerte für die abgestrahlten Felder von Sicherheitssystemen einerseits und die Störfestigkeit von aktiven Implantaten andererseits einzuführen. Behörden, Betreiber von Sicherheitssystemen, Ärzteschaft und Patienten sind angesprochen, die bestehenden Inkompatibilitäten durch die nach wie vor im Umlauf befindlichen älteren inkompatiblen Geräte zu begrenzen.

Ein Review von 2004[61] stellt fest, dass trotz grundsätzlicher Störmöglichkeiten Reaktionen aktiver Implantate auf die Felder von Artikelüberwachungssystemen relativ selten sind. Das höchste Störpotenzial wird den akustomagnetischen Systemen zugewiesen, welches die modernsten Systeme sind.

Beeinflussung von Implantaten durch andere RFID-Systeme

Gemäss der amerikanischen Food an Drug Administration FDA sind mit Ausnahme der EAS in Bezug auf RFID keine gesundheitsgefährdenden Vorfälle mit implantierten Medizinprodukten bekannt. Im Gegensatz zu Warensicherungsanlagen sind Interferenzen von sonstigen RFID-Systemen mit Medizinprodukten noch weitgehend unerforscht. Erste Labortests zeigen aber ähnliche unerwünschte Auswirkungen der RFID-Systeme auf Medizinprodukte während der Abfrage der Tags.

Fazit

Aktive medizinische Implantate wie z.B. Herzschrittmacher können durch Artikelüberwachungssysteme (EAS) und evtl. durch andere RFID-Systeme gestört werden. Wegen der weiten Verbreitung von EAS und der wachsenden Verbreitung von RFID-Systemen und Herzschrittmachern müssen gemeinsame Grenzwerte für die abgestrahlten Felder von RFID-Systemen einerseits und die Störfestigkeit von aktiven Implantaten andererseits eingeführt werden. Solange noch Herzschrittmacher und RFID-Systeme in Verkehr sind, welche diese Anforderung nicht erfüllen, müssen die Bereiche mit Schildern gekennzeichnet werden, in denen für Implantate potenziell gefährliche Felder auftreten.

3.5 Problematik implantierter RFID-Tags

Erhöhtes Krebsrisiko bei implantierten RFID-Tags

In einer Reihe von wissenschaftlichen Publikationen[62] [63] [64] [65] [66] [67] [68] wurden kanzerogene Effekte von implantierten RFID-Tags insbesondere bei Nagetieren beschrieben. Es handelt sich dabei teilweise um bösartige Tumorerkrankungen des Bindegewebes, die im Bereich des eingepflanzten Tags aufgetreten

[61] Fröhlig G. Active implantable medical devices and interference from electronic security systems. Herzschr Elektrophys 2004; 15:55-64.
[62] Siegal-Willott J et al. Microchip-associated leiomyosarcoma in an Egyptian fruit bat (Rousettus aegyptiacus). J Zoo.Wildl.Med 2007;38:352-6.
[63] Vascellari M, Melchiotti E, Mutinelli F. Fibrosarcoma with typical features of postinjection sarcoma at site of microchip implant in a dog: histologic and immunohistochemical study. Vet.Pathol. 2006;43:545-8.
[64] Le Calvez S, Perron-Lepage MF, Burnett R. Subcutaneous microchip-associated tumours in B6C3F1 mice: a retrospective study to attempt to determine their histogenesis. Exp.Toxicol.Pathol. 2006;57:255-65.
[65] Vascellari M et al. Liposarcoma at the site of an implanted microchip in a dog. Vet.J 2004;168:188-90.
[66] Elcock LE et al. Tumors in long-term rat studies associated with microchip animal identification devices. Exp.Toxicol.Pathol. 2001;52:483-91.
[67] Blanchard KT et al. Transponder-induced sarcoma in the heterozygous p53+/- mouse. Toxicol.Pathol. 1999;27:519-27.
[68] Tillmann T et al. Subcutaneous soft tissue tumours at the site of implanted microchips in mice. Exp.Toxicol.Pathol. 1997;49:197-200.

sind. Ob die Effekte durch die Strahlung, den Tag oder den Eingriff selbst verursacht wurden, ist unklar. Inwieweit diese Resultate auch für Menschen relevant sind, kann nicht beurteilt werden.

Implantierte RFID bei Magnetresonanztomografie Untersuchungen (MRT)

Im Gegensatz zu anderen bildgebenden Verfahren arbeitet die Magnetresonanztomografie (MRT) nicht mit ionisierender Strahlung, sondern mit elektromagnetischen Feldern. Eine Untersuchung[69] hat gezeigt, dass implantierte RFID-Tags, wie sie in den USA z.T. zur Patientenidentifikation oder für Zugangskontrollen verwendet werden (vgl. Kap. 2.3), stark magnetisch sind und sich nach der Richtung des statischen Magnetfeldes ausrichten. Eine Gesundheitsgefährdung durch eine verstärkte Wanderung der Tags im Gewebe während einer MRT-Untersuchung ist nicht zu erwarten, da die Tags nicht in der Nähe empfindlicher Organe eingepflanzt werden. Es wurde auch keine übermässige Temperaturerhöhung im Bereich des Tags festgestellt. Die Qualität des MR-Bildes ist im Umkreis der RFID-Tags jedoch stark beeinträchtigt, so dass MRI-Untersuchungen unter Umständen bei Patienten mit implantierten RFID-Tags nur noch eingeschränkt angewendet werden können.
Armbänder zur Patientenidentifizierung (vgl. Kap. 2.3) werden momentan für das MRT getestet. Erste Untersuchungen deuten darauf hin, dass die Armbänder keine Probleme im MRT verursachen und die Qualität der Bilder dadurch nicht beeinträchtigt wird[70].

Fazit

Implantierte RFID-Tags können Probleme bei Magnetresonanzuntersuchungen verursachen. Es gibt zudem Hinweise auf Tumore bei Tieren mit implantierten Tags. Dies sind lediglich zwei Beispiele. Da sich bei jeder Anwendung spezifische Probleme auftreten können, sollte auch für jede Anwendung eine entsprechende Risikoanalyse durchgeführt werden.

[69] Ryf et al. MR safety evaluation of implantable RF transponders for animals. Proceedings der Gemeinsamen Jahrestagung der Deutschen, Österreichischen und Schweizerischen Gesellschaft für Biomedizinische Technik, 6.-9. September 2006, Zürich.
[70] Lüchinger R., Institut für Biomedizinische Technik, Universität und ETH Zürich, persönliche Mitteilung

4. Umweltrisiko: Abfallentsorgung und Recyclingsysteme

Chancen und Risiken des RFID-Einsatzes bei der Abfallentsorgung und beim Recycling
In Bezug auf die Abfallentsorgung bietet die RFID-Technologie die Möglichkeit, Produkte mit detaillierten Informationen zur Materialzusammensetzung und zum Recycling zu versehen. Gleichzeitig bestehen Befürchtungen in Bezug auf die Abfallentsorgung vor allem wegen der Kupfer und anderen Schwermetallen, aber auch Silizium etc., aus denen die Tags bestehen. Schwierigkeiten können sich dann ergeben, wenn der Tag in die Verpackung eingearbeitet ist. Konsumentenverbände fordern deshalb, dass ökologisch neutrale oder zerlegbare („decomposable") Materialien genutzt werden.

Interpellation (05.3067) Hollenstein
In seiner Antwort vom 18.05.2005 zur Interpellation Hollenstein[71] schreibt der Bundesratbezüglich Recycling und Entsorgung von RFID-Tags: „Um die Umweltbelastung von ausgedienten RFID-Tags abschätzen zu können, müssen verschiedene Parameter wie deren Zusammensetzung, Grösse und Energieverbrauch berücksichtigt werden. Die Auswirkungen auf die Umwelt bei der Entsorgung der Tags zusammen mit Siedlungsabfällen in Kehrichtsäcken sind insgesamt als unproblematisch einzustufen. Beim Recycling von mit RFID-Tags versehenen Gegenständen können dagegen gewisse Probleme auftreten (z. B. Glasrecycling: Verfärbungen, Materialdefekte), sofern keine vorsorglichen Massnahmen getroffen werden. Der Bundesrat kann, gestützt auf Artikel 30a des Umweltschutzgesetzes, die Verwendung von Stoffen verbieten, welche die Entsorgung erheblich erschweren. Entsprechender Handlungsbedarf besteht derzeit jedoch nicht. Eine separate Sammlung der Tags würde einen enormen logistischen und technischen Aufwand erfordern. Ein Recycling der Tags lohnt sich wegen Miniaturisierung kaum und wird zusätzlich durch die Stoffvielfalt wesentlich erschwert."

Schweizer Studie: „Are RFID Tags a Threat to Waste Management?"
In dieser Studie[72] von 2005 untersuchte die Abteilung „Technologie und Gesellschaft" der EMPA, wie sich der breite Einsatz von Smart-Labels anstelle des Handelsstrichcodes im Detailhandel auf den Abfall und das Recycling auswirken würde. Sie kommt zum Schluss, dass es z.B. beim Glasrecycling zu Verunreinigungen durch Aluminium kommen könnte und dass beim Entsorgen der Smart-Label im Haushaltmüll wertvolle Rohstoffe wie z.B. Kupfer verloren gehen können. Heute bestehen diese Probleme noch nicht, und sie können in Zukunft durch vorsorgliche Massnahmen verhindert werden. Die Smart-Label Produzenten müssen deshalb beim Design der Tags auch deren Auswirkungen auf etablierte Recyclingverfahren und deren eigene Recyclingfähigkeit mitberücksichtigen[73].

Deutsche Studie: „RFID-Masseneinsatz: Auswirkungen auf Entsorgung und Recyclingssysteme"
In einer 2007 veröffentlichte Studie[74] analysiert eine Forschungsgruppe der Universität Dortmund die Auswirkungen eines RFID-Masseneinsatzes auf Entsorgungs- und Recyclingsysteme. Gemäss der Studie liegt die Problematik der RFID-Entsorgung in der Mengenentwicklung der RFID-Komponenten. In Zukunft ist damit zu rechnen, dass grössere Mengen von Tags entsorgt werden müssen (falls in Deutschland alle Verkaufsverpackungen mit einem Tag ausgestattet werden, beläuft sich die Zahl der benötigten Tags auf 200 Milliarden pro Jahr).
Die an Glas, Aluminium oder Kunststoff angebrachten Tags könnten in solchen Mengen die Qualität der Recyclate aus diesen Materialien durch eine grosse Anzahl Störstoffe negativ beeinflussen. Bei der Restmüllverwertung könnte es zu Überschreitungen der Grenzwerte für Kupfer, Silber und Chloride kommen.

[71] Interpellation (05.3067) Hollenstein: Bedroht die Anwendung von RFID den Datenschutz
[72] Ph. Kräuchi et al., EMPA: „Impacts of Pervasive Computing: Are RFID tags a Threat to Waste Management" IEEE Technology & Society Magazine, Special Issue "Sustainable Pervasive Computing", 2005, 24(1), S. 45-53, sowie P. Wäger et al., EMPA: Smart labels in municipal solid waste — a case for the Precautionary Principle? Environmental Impact Assessment Review 25/2005, S. 567-586. Eine aktualisierte und erweiterte Studie zum gleichen Thema erstellt die EMPA derzeit im Auftrag des deutschen Umweltbundesamtes (Kontakt: L. Hilty, EMPA). Erste Ergebnisse sind im Sommer 2008 zu erwarten.
[73] siehe auch: SR 814.620 Verordnung über die Rückgabe, die Rücknahme und die Entsorgung elektrischer und elektronischer Geräte (VREG) vom 14. Januar 1998
[74] Studie „RFID Masseneinsatzes auf Entsorgungs- und Recyclingsysteme"; Universität Dortmund, gefordert von Bundesministerium für Bildung und Forschung, Förderkennzeichen 16SV2280 (2007)

Bei einem Mehreinsatz von RFID wird der Bedarf an wertvollen Rohstoffen erheblich steigen. Die steigenden Kosten werden das Recycling fördern, vorausgesetzt dass die Aufbereitung für das Recycling nicht zu aufwändig ist. Zur Lösung des Problems ist deswegen wichtig, technische Lösungen zu finden, welche eine Wiederverwendung der wertvollen Komponenten des Tags (besonders die materialintensiven Antennen, die Aluminium, Kupfer oder Silber enthalten) mit vertretbarem Aufwande zu ermöglichen.

Fazit

Zurzeit wird die Abfallentsorgung der Tags als unproblematisch eingestuft. In Zukunft ist allerdings damit zu rechnen, dass durch die Menge der Tags Probleme bei der Abfallentsorgung und bei Recyclingsystemen auftauchen. Die Lösung könnte in der Anwendung leicht trennbarer Materialien mit anschliessender der Verwertung der wertvollen Komponenten liegen. Innovative Lösungen werden gesucht, damit solche Lösungen wirtschaftlich tragbar werden.

5. Datensicherheit und Datenschutz

5.1 Datensicherheit (Informationssicherheit)

In einem RFID-System werden Daten zwischen einem Tag und einem Lesegerät ausgetauscht und weiterverarbeitet. In diesem System gibt es verschiedene Missbrauchs- und Angriffsmöglichkeiten auf diese Daten, wie Abbildung 11 zeigt. Ein Angriff kann beim Tag, bei der Luftschnittstelle, beim Lesegerät oder auch bei der zugehörigen Datenbank (Backend) geschehen.

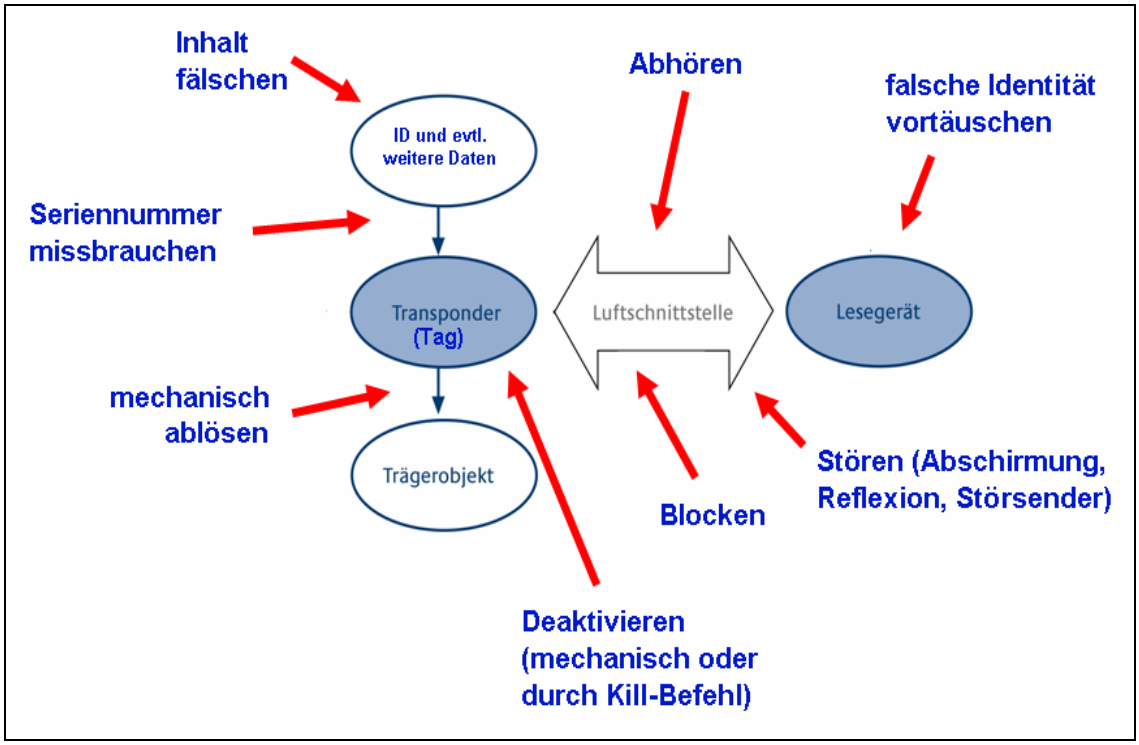

Abbildung 11: *Angriffspunkte auf ein RFID-System* [33]

Eine umfassende Datensicherheitsanalyse sollte deswegen alle diese Angriffsarten und Angriffspunkte berücksichtigen.

Obwohl RFID schon weit verbreitet ist, ist die Technologie bzw. deren Anwendung noch in der Aufbauphase. Da sich die Anwendungen noch in der Entwicklung befinden, sind auch die Bedrohungen in einer frühen Phase. Die nachfolgende Diskussion der Gefahren basiert deshalb zum Teil auf theoretischen Überlegungen und Laborversuchen. Die Gefahren sind deswegen nicht weniger bedeutend. Da die RFID-Technologie in immer mehr Anwendungen eine immer grössere Verbreitung im Alltag findet, werden immer mehr potenzielle Angreifer neue Angriffsarten entwickeln, wie dies in den vergangenen Jahren schon beim Internet zu beobachten war.

Datensicherheit umfasst die Bereiche Vertraulichkeit, Integrität und Verfügbarkeit von Daten.

Vertraulichkeit

Vertraulichkeit von Daten bedeutet, dass die Daten nicht von Unbefugten bearbeitet[75] wie bspw. abgefangen oder überwacht werden können. Sie ist besonders wichtig bei der Übertragung von schützenswerten Daten, wie z.B. biometrischen Daten auf einem Reisepass. Ein besonderes Problem in diesem Bereich ist, dass das Mitschneiden (Aufzeichnen, Aufnehmen) oft ein rein passiver Angriff ist und nicht direkt entdeckt werden kann. Dazu kommt, dass die meisten RFID-Tags sehr einfach sind, jedem Lesegerät antworten und keinen Rekord der Lesevorgänge speichern[76]. Beispiele einer Verletzung der Vertraulichkeit bei RFID sind:

- Bei einer schwachen Implementierung der Verschlüsselung auf RFID-Reisepässen ist es möglich, diese zu lesen und den RFID-Tag zu klonen. Die Fälschung eines Reisepasses wird dadurch erleichtert.[77]
- Eine Organisation hört die RFID-Lesevorgänge eines Konkurrenten ab, um Informationen über seinen Betrieb zu sammeln.[78]
- Ein Laden erhält über RFID Informationen über die von einem Kunden mitgeführten Gegenstände, z.B. Kleidungsstücke oder Einkäufe bei Konkurrenten. Dies erfolgt ohne Wissen oder Zustimmung des Kunden[76].

Authentifizierung

Die Authentifizierung ist ein Instrument zur Sicherstellung der Vertraulichkeit. Da sie bei Identifikationssystemen wie RFID von grosser Bedeutung ist, wird sie hier separat behandelt. Die Authentifizierung soll die Identitäten von berechtigten kommunizierenden Instanzen bestätigen bzw. die Kommunikation für nicht berechtigte Instanzen verunmöglichen. Eine Authentifizierung kann für verschiedene Zwecke eingesetzt werden, z. B. für die Benutzung einer Einrichtung oder den Zugriff auf Daten. Wenn der Authentifizierungsmechanismus Sicherheitslücken aufweist, kann ein Angreifer auf Ressourcen zugreifen, obwohl er nicht dazu berechtigt ist. Beispiele eines Versagens der Authentifizierung sind:

- Bei RFID wird der Tag und nicht der Benutzer authentifiziert. Wenn z.B. ein RFID-Zutrittsbadge in die Hände eines Angreifers fällt, geniesst er die gleichen Berechtigungen wie der echte Besitzer des Badges.
- Durch Abhören eines RFID-Systems und die Verarbeitung der dabei gesammelten Daten kann ein Angreifer entweder mit einem Emulator (Gerät, das das Verhalten eines Tags simuliert) oder einem geklonten Tag die Identität eines berechtigten Benutzers übernehmen und mit seinen Berechtigungen handeln (z.B. Betrug bei der Bezahlung der Maut auf Autobahnen [76]).
- Um Vertraulichkeit bei gewissen RFID-Anwendungen sicherzustellen, wird eine Authentifizierung des Lesegeräts eingeführt, d.h. das Lesegerät muss sich gegenüber dem Tag als leseberechtigt (oder auch schreibberechtigt) „ausweisen“. Wenn es einem Angreifer gelingt, sich in den Besitz der entsprechenden Passwörter oder Schlüssel zu bringen, kann er jedoch mit einem eigenen Lesegerät unbemerkt auf die scheinbar sicheren Tags zugreifen.

Integrität

Integrität bedeutet, dass die Daten während der Bearbeitung vollständig, unverfälscht und widerspruchsfrei bleiben. Beispiele einer Verletzung der Integrität sind:

- Ein Angreifer schreibt auf einen RFID-Tag. Dies ist nur möglich bei Tags, die veränderbaren Inhalt speichern. Ein berechtigtes Lesegerät liest später die verfälschten Daten.[79]

---

[75] Bearbeiten ist gemäss DSG Art. 3 Bst. e wie folgt definiert:
Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

[76] 'RFID Privacy: an Overview of Problems and Proposed Solutions', Garfinkel, Juels, Pappu, IEEE Security & Privacy, May/June 2005

[77] 'Arphid Watch: Find Own Foot, Aim Hastily, Pull Trigger', Bruce Sterling, 17. November 2007, http://blog.wired.com/sterling/2006/11/arphid_watch_fi.html

[78] 'Guidelines for Securing Radio Frequency Identifikation (RFID) Systems', National Institute of Standards and Technology, April 2007

[79] 'Risiken und Chancen des Einsatzes von RFID-Systemen', Bundesamt für Sicherheit in der Informationstechnik, 2005 (Studie des IZT Berlin und der EMPA im Auftrag des deutschen Bundesamtes für Sicherheit in der Informationstechnik)

- Ein Angreifer entfernt oder ersetzt den RFID-Tag von einem Gegenstand. Ein Lesegerät liest gar keine bzw. verfälschte Informationen [79].
- Ein Angreifer greift über das Internet das Backend eines RFID-Systems an und verändert Daten in einer Datenbank des Systems. Die Datenintegrität des Gesamtsystems wird beeinträchtigt.

Verfügbarkeit

Verfügbarkeit heisst, dass Systeme und Dienste in Betrieb sind, Daten bereit stehen usw. Gefahren für die Verfügbarkeit sind vor allem technische Pannen, aber auch Angriffe (sog. ‚Denial of Service'-Attacken). Beispiele für Nichtverfügbarkeit sind:

- Ein Konferenzbesucher wickelt sein RFID-Badge in Alufolie, um die Überwachung durch den Sicherheitsdienst zu verhindern[80].
- Eine Datenverbindung zwischen einem Lagerhaus und dem Rechenzentrum wird unterbrochen. Das RFID-Inventarsystem fällt deswegen aus[78].
- Ein Angreifer benutzt ein Blocker-Tag, das verhindert, dass normale Tags in der Umgebung gelesen werden können, indem es die Lesegeräte überfordert[79].

Standards und Richtlinien zur Datensicherheit

Ein RFID-System sollte immer im Kontext zur gesamten Informatik-Landschaft einer Organisation betrachtet werden. Dieser Grundsatz gilt auch für Regelungen, Standards und Richtlinien zur Datensicherheit bei RFID.
Beispielsweise könnte eine Supermarktkette RFID in ihrem Inventar-Management einsetzen. Der Supermarkt wird schon zu diesem Zeitpunkt einer Gesetzgebung und Vorschriften unterliegen (z.B. dem Lebensmittelgesetz). Aus diesen Anforderungen auf höchster Ebene kann der Supermarkt Anforderungen auf sein Inventar-Management und folglich für seine Informatik-Infrastruktur einschliesslich RFID-Systeme ableiten. Die Anforderungen des Finanzwesens oder des Datenschutzes könnten weitere Anforderungen an die Informatiksysteme einschliesslich RFID stellen. Dieses Ableiten der Anforderungen für das RFID-System aus den höchsten Zielen der Organisation ist logisch und richtig. Es wäre unnötig und sehr problematisch, gesetzliche Anforderungen zur Datensicherheit direkt an die Technologie oder deren Anwendung zu stellen.
Verschiedene Publikationen geben praktische Hinweise zur Sicherung von RFID-Systemen, wie z.B. die oben referenzierten Publikationen[78, 79].
Eine Organisation könnte, falls nötig, ein Informationssicherheits-Managementsystem (ISMS) führen und sich – falls gewünscht oder nach ISO 27001 gefordert – zertifizieren lassen. Ein solches System bildet einen Teil der integralen Sicherheit der Organisation und ist nicht RFID-spezifisch. Im ISMS enthalten ist jedoch die Informatik-Sicherheit, die ein mögliches RFID-System abdecken würde.

Der Handlungsbedarf zur Erreichung eines guten Sicherheitsstandards ist unterschiedlich und von den Eigenschaften des RFID-Systems abhängig (Abbildung 12). Aus Sicht der IT-Sicherheit ist der Handlungsbedarf umso höher, je mehr die folgenden Voraussetzungen zutreffen:

- Es handelt sich um ein offenes RFID-System (die RFID-Tags zirkulieren nicht in einem geschlossenen System, z.B. zur Kennzeichnung von umlaufenden Containern, sondern werden weitergegeben, z.B. an Kunden)
- Es sind grössere Lesedistanzen vorgesehen (über ca. 50 cm)
- Die ausgelesenen Daten werden via Internet übertragen (Hacker-Angriffe möglich)
- Die RFID-Tags werden nicht mit der Verpackung entsorgt, sondern bleiben in einem Produkt langfristig aktivierbar.
- Die RFID-Tags sind für Laien nicht erkennbar.

[80] 'Stallman Foils United Nations Security at Tech Conference', K. C. Jones, 22. November 2005, http://www.informationweek.com/software/opensource/174401536

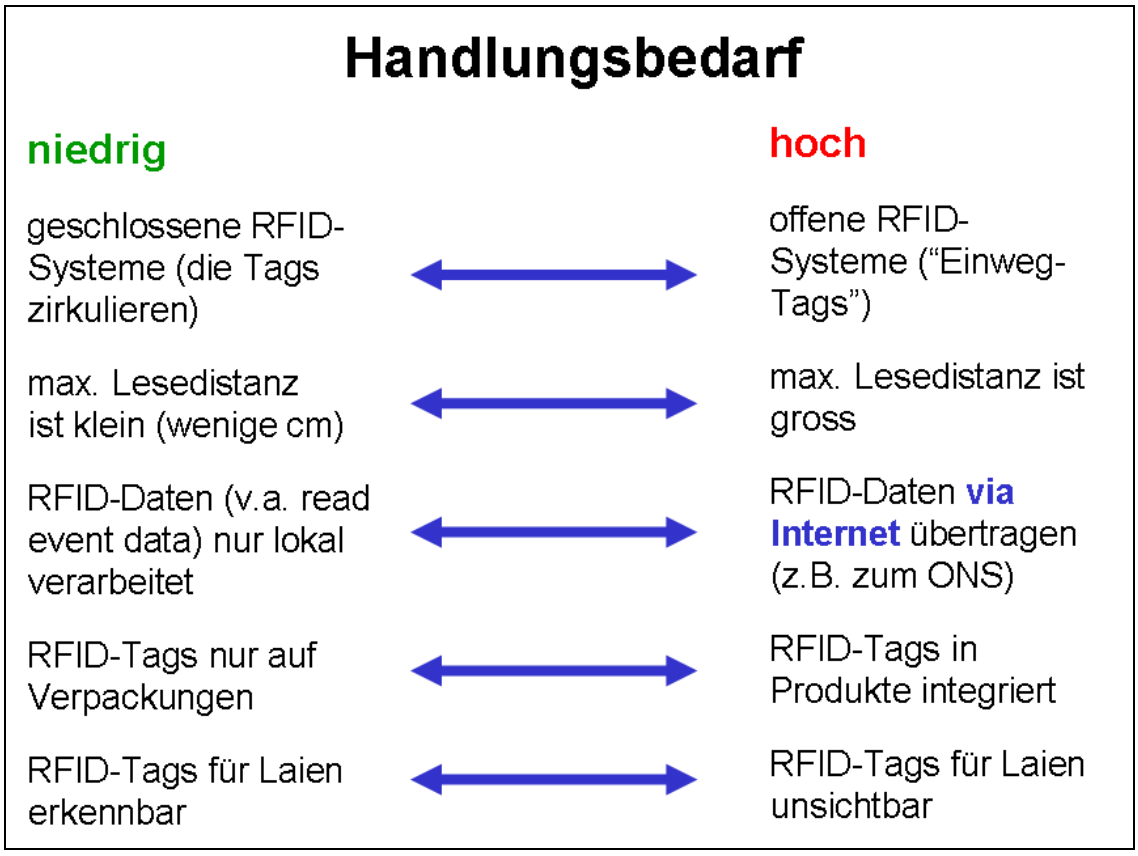

Abbildung 12: *Handlungsbedarf zum Erreichen eines Sicherheitsstandards* [33]

Fazit

In Bezug auf die Datensicherheit sollte jede Organisation die Anforderungen an ihre möglichen RFID-Systeme aus den übergeordneten Zielen der Organisation ableiten. Es kann notwendig oder nützlich sein, dass die Organisation ein Informationssicherheits-Managementsystem führt und sich eventuell nach einem geeigneten Standard zertifizieren lässt. Ressourcen zur Sicherung von RFID-Systemen sind verfügbar.

5.2 Datenschutz

RFID-Anwendungen werden zum Datenschutzthema, sobald dadurch *Personendaten* bearbeitet werden. Personendaten, also Angaben über bestimmte oder bestimmbare Personen (Artikel 3 litera a DSG), fallen an, wenn *unmittelbar* mit RFID-Tags Menschen gekennzeichnet werden (durch ein Implantat vgl. Kap. 2.3), aber auch bereits durch das Tragen eines RFID-Armbands, z.B. das Patientenarmband im Spital Thun) oder wenn *mittelbar* aus dem Kontext Schlüsse auf eine bestimmte oder bestimmbare Person – Konsument(in), Patient(in) usw. – möglich werden, beispielweise durch Bezahlung einer mit einem RFID-Tag markierten Sache (Ticket, Kleidungsstück, Skipass usw.) mit Rechnung oder mit einer Kreditkarte, durch die Identifikation oder Autorisierung einer Person mit einer Kundenkarte, einem Personalausweis oder durch den Aufenthalt an einem «identifizierenden» Ort, etwa am individuellen Arbeitsplatz.

Jede Bearbeitung von Personendaten berührt das Grundrecht auf informationelle Selbstbestimmung (Artikel 13 Absatz 2 BV[81]). Zum Ausgleich der involvierten Interessen der Datenbearbeiter und der betroffenen Personen hat jede Bearbeitung von Personendaten die folgenden *Grundsätze* zu beachten:

[81] Präziser formuliert dieses Grundrecht die am 12. Dezember 2007 in Strassburg proklamierte Charta der Grundrechte der

- Sie muss rechtmässig und verhältnismässig sein und hat nach Treu und Glauben zu erfolgen (Artikel 4 Absätze 1 und 2 DSG)
  private Personen dürfen Personendaten bearbeiten, wenn
  - der Betroffene eingewilligt hat, oder
  - wenn ein überwiegendes privates oder öffentliches Interesse vorhanden ist, oder
  - gesetzliche Regelungen bestehen (Art. 13 DSG)
  Bundesorgane dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Legalitätsprinzip) (Art. 17 DSG)
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Artikel 4 Absatz 3 DSG).
- Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein (Artikel 4 Absatz 4 DSG); falls besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden, muss die betroffene Person informiert werden (Artikel 7a DSG).
- Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt; bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen (Artikel 4 Absatz 5 DSG).
- Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern; er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind Personendaten müssen richtig sein. Die betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden (Artikel 5 DSG).

Eine Beurteilung aus datenschutzrechtlicher Sicht ist nicht allgemein möglich, sondern nur im konkreten Anwendungsfall. Immerhin kann aber festgehalten werden, welche Aspekte die datenschutzrechtliche Problematik besonders beeinflussen:

- Die Kleinheit von RFID-Tags ermöglicht es, dass RFID-Tags verdeckt angebracht werden können, so dass die Datenbearbeitung für die betroffenen Personen nicht erkennbar ist und diese deshalb weder Schutzmassnahmen ergreifen noch ihre Rechte geltend machen können.
- Die Verwendung drahtloser Funktechnologie ermöglicht es, dass das Auslesen der auf den Chips gespeicherten Daten ohne Wissen der betroffenen Personen erfolgen kann.
- Solange RFID-Tags nicht zerstört oder deaktiviert oder die Daten darauf gelöscht worden sind, können sie weiter ausgelesen bzw. die Daten weiter bearbeitet werden, so dass mit der Zeit Verhaltens- oder Bewegungsprofile erstellt werden können.
- Auch wenn eine RFID-Anwendung primär nicht für ein personenbezogenes Erfassen von Daten eingesetzt wird (beispielsweise im Supply Chain Management), kann – wie oben erwähnt – ein Personenbezug entstehen, so dass aus Daten, die technisch notwendigerweise anfallen («Randdaten», die für das Funktionieren von technischen Systemen notwendig sind, wie Verbindungsdaten oder Protokollierungen), Personendaten werden, die dann durchaus personenbezogen verwendet werden können (Verhaltens- oder Bewegungsprofile etwa für Marketingzwecke).

Daraus folgt die datenschutzrechtliche Forderung nach folgenden Massnahmen[82]:

- Die betroffenen Personen müssen umfassend über den Einsatz von RFID-Systemen informiert werden.

Europäischen Union (ABl. C 303 vom 14.12.2007, 1 ff.) in Artikel 8 (Schutz personenbezogener Daten): *«(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.»*

[82] Vgl. dazu auch die Veröffentlichung des EDÖB «Datenschutzrechtliche Probleme bei dem Einsatz der RFID-Technologie»: http://www.edoeb.admin.ch/dokumentation/00445/00509/00510/00816/index.html?lang=de.

- Kommunikationsvorgänge mit RFID-Tags, die eine Bearbeitung personenbezogener Daten auslösen, müssen für die betroffenen Personen transparent und eindeutig erkennbar sein.
- Daten auf RFID-Tags dürfen nur so lange gespeichert sein, wie es zur Erreichung des Zwecks erforderlich ist.
- Es müssen Möglichkeiten zur Deaktivierung bzw. Löschung der Daten von RFID-Tags geschaffen werden.
- Die Datensicherheit (Informationssicherheit) muss sichergestellt werden. Massnahmen für die Umsetzung dieser sind u. a. die Authentifizierung der beteiligten Peripheriegeräte (v.a. Lesegeräte) sowie der Einsatz von Verschlüsselungsverfahren.

Die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre hat bereits 2003 in Sydney in einer Resolution[83] auf die Risiken der RFID-Technologie hingewiesen. Folgende Grundsätze wurden im Einzelnen formuliert:

- Jeder Datenbearbeiter sollte vor der Einführung von RFID-Tags, die mit personenbezogenen Daten verknüpft sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen.
- Falls der Datenbearbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden.
- Personenbezogene Daten dürfen nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden, und sie dürfen nur so lange aufbewahrt werden, wie es zur Erreichung dieses Zwecks erforderlich ist.
- Soweit RFID-Tags im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung bzw. Zerstörung der RFID-Tags haben.

Die datenschutzgesetzlichen Rahmenbedingungen sind in Form der oben erwähnten Grundsätze des Datenbearbeitens weitgehend gegeben. Die Herausforderung liegt in der *Umsetzung* im konkreten Anwendungsfall. Die Betreiber von RFID-Systemen haben dafür zu sorgen, dass die gesetzlichen Vorschriften eingehalten werden, und die Datenschutzkontrollorgane – der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte für Datenbearbeitungen durch Bundesorgane und Private, die kantonalen Datenschutzbeauftragten für Datenbearbeitungen durch öffentliche Organe der Kantone und Gemeinden – haben in ihrer Aufsichtstätigkeit eine wirksamen Kontrolle sicherzustellen. Ein (allerdings nicht RFID-spezifisches) Problem sind die kaum vorhandenen, auf jeden Fall wenig wirksamen Sanktionierungsmöglichkeiten bei Datenschutzverletzungen; hier besteht der Bedarf, das Sanktionierungssystem im Datenschutzbereich generell einer Prüfung zu unterziehen.

Eine gesetzgeberische Lücke besteht ausserdem dort, wo es um die Verhinderung der personenbezogenen Verwendung von ursprünglich nicht zu personenbezogenen Zwecken erhobenen Daten («Randdaten») geht, ein Problem, das allerdings über RFID-Anwendungen hinaus generell IT-Systeme betrifft. Moderne Datenschutzgesetze im In- und Ausland[84] statuieren deshalb das *Prinzip der Datenvermeidung*

---

83 http://www.privacyconference2003.org/resolutions/RFIDResolutionGe.doc.

84 Vgl. nur etwa § 4 Absatz 1 des Schleswig-Holsteinischen Gesetzes vom 9. Februar 2000 zum Schutz personenbezogener Informationen *(«Die datenverarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten»)*; § 3a des (deutschen) Bundesdatenschutzgesetzes (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I 66) *(«[1]Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. [2]Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht»)*; § 5a des (Berliner) Gesetzes zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz, BlnDSG) *(«[1]Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. [2]Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht »)*; § 11 des (kantonalzürcherischen) Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4), teilweise in Kraft seit 1. Juli 2007, gesamthaft in Kraft ab 1. Juli 2008 *(«Das öffentliche Organ gestaltet Datenbearbeitungssysteme und -programme so, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind. [2]Es löscht, anonymisiert oder pseudonymisiert solche Personendaten, sobald und soweit dies möglich ist»)*; § 9 des (aargauischen) Gesetzes vom 24. Oktober 2006 über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG-AG), in Kraft voraussichtlich ab 1. Juli 2008 *(«Grundsätzlich ist das Prinzip der Datenvermeidung und Datensparsamkeit zu beachten, insbesondere beim Einsatz von Informatiksyste-*

und Datensparsamkeit. Dieses Prinzip ist mehr, als was das Verhältnismässigkeitsprinzip (Artikel 4 Absatz 2 DSG) bereits vorschreibt. Datenvermeidung und Datensparsamkeit «sind als gezielte Restriktion der Verwendung personenbezogener Daten entstanden, sollten also auch und gerade klarstellen, dass die Verarbeitung personenbezogener Angaben stets als begründungsbedürftige Ausnahme gesehen und behandelt werden muss. Mit anderen Worten: Auf personenbezogene Daten lässt sich erst zugreifen, wenn es keine andere Möglichkeit mehr gibt, die jeweils notwendigen Informationen zu bekommen. Der Datenschutz materialisiert sich mithin nicht erst in jenem immer wieder angeführten Verbot mit Erlaubnisvorbehalt oder gar in der Verpflichtung, nur die ‹erforderlichen› Daten zu verwenden, vielmehr zunächst und vor allem im prinzipiellen Verzicht auf personenbezogene Angaben und damit in der Suche nach Alternativen sowie der Pflicht, ihnen unbedingt den Vorzug zu geben.»[85] Das Prinzip der Datenvermeidung und Datensparsamkeit soll zu einem Umdenken führen, indem die Technologie den Anforderungen des Rechts zu folgen hat und nicht umgekehrt. Die IT-Systeme sind so zu gestalten, dass keine oder so wenig personenbezogene und personenbeziehbare Daten wie möglich anfallen. Ist es systembedingt unvermeidbar, dass personenbezogene oder personenbeziehbare Daten erhoben werden, sollen «Privacy Enhancing Technologies» (PET, datenschutzfreundliche Technologien) zum Einsatz kommen, das heisst, die Personendaten sollen anonymisiert oder pseudonymisiert werden, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Handlungsbedarf besteht also – über den RFID-Bereich hinaus generell für IT-Systeme, bei denen personenbezogene und personenbeziehbare Daten anfallen – in der Einführung des Prinzips der Datenvermeidung und Datensparsamkeit im Bundesgesetz über den Datenschutz.

Fazit

Die Datenschutzproblematik ist bei RFID-Systemen nicht grundsätzlich anders als anderswo. Die bestehenden Probleme können durch die Verbreitung der RFID-Technologie jedoch insofern verschärft, als mit geringem Aufwand eine viel grössere Menge an Daten gesammelt werden kann und dies auch unbemerkt geschehen kann. In diesem Fall sollte die Einführung des Prinzips der Datenvermeidung und Datensparsamkeit in Bundesgesetz über den Datenschutz überprüft werden. Gleichzeitig soll das Sanktionierungssystem im Datenschutzbereich überprüft werden. Wenn die Sanktionen bei einem Verstoss gegen das Datenschutzgesetz zu wenig streng sind, kann für gewisse Firmen der Einsatz eines Systems zur Sicherung der Kundendaten finanziell uninteressant sein. Es ist deshalb notwendig, dass wirksamere Sanktionen bei Verstössen gegen das Datenschutzgesetz drohen.

---

men»); § 13 des Vernehmlassungsentwurfes zu einem Gesetz (der Kantone Basel-Stadt und Basel-Landschaft) über die Information und den Datenschutz (wird demnächst veröffentlicht) (*«[1]Das öffentliche Organ gestaltet informationstechnologische Systeme so, dass keine oder möglichst wenig personenbezogene und personenbeziehbare Daten anfallen. [2]Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht»*). Vgl. dazu HELMUT BÄUMLER, Datenvermeidung und Datensparsamkeit, in: BRUNO BAERISWYL/BEAT RUDIN (Hrsg.); Perspektive Datenschutz, Zürich und Baden-Baden und Wien 2002, 351 ff.

[85] SPIROS SIMITIS, Auf dem Weg zu einem neuen Datenschutzkonzept: Die zweite Novellierungsstufe des BDSG, Datenschutz und Datensicherheit 12/2000, 727 ff.

6. Verbraucherrelevante Aspekte der RFID-Technologie und die Informationsgesellschaft

In diesem Kapitel werden die verbraucherrelevanten Aspekte der RFID-Technologie beschrieben. Es handelt sich dabei zum einen um die in den vorhergehenden Kapiteln beschriebenen Aspekte der Datensicherheit, des Datenschutzes, des Umweltschutzes oder des Gesundheitsschutzes in den für Konsumenten relevanten Anwendungsgebieten von RFID. Zum anderen kommen wirtschaftspolitische Überlegungen, Konsumenteninformation oder die Beteiligung am Festlegen technischer Rahmenbedingungen hinzu.

6.1 Verbraucherrelevante Aspekte der RFID-Technolgoie

Verantwortungsvoll eingesetzt, versprechen RFID-Systeme grosse Vorteile für Verbraucher. Beispiele dafür sind beschleunigte Bezahlvorgänge, bessere Rückverfolgbarkeit von Produkten sowie höhere Produktsicherheit und –qualität. In einigen Bereichen ist der Einsatz der RFID-Technologie auf Verbraucherseite auch schon weit verbreitet (Eintrittskarten, Skipässe, Wegfahrsperren, Zugangskontrollen).

Die rasante Entwicklung, ein vielfältiger Anwendungsbereich sowie ein allgemeines Misstrauen gegenüber neuen Technologien führen jedoch auch zu Einwänden von Seiten der Verbraucher. Vertreter von Konsumentenorganisationen sprechen schon vom „totalen Überwachungsstaat“ oder vom „gläsernen Konsumenten“[86]. Die Bedenken der Konsumenten gegenüber der RFID-Technologie lassen sich grob in drei Kategorien einteilen:

Schutz der Privatsphäre und Zunahme der Informationsasymmetrie zwischen Anbieter und Konsumenten: als Beispiele angeführt werden können. die Angst vor dem Verlust über den eigenen Besitz („wenn man etwas gekauft hat, geht es niemanden mehr etwas an, was man damit macht“), aber auch die Möglichkeit, Gegenstände und damit Kunden zu verfolgen oder in Verbindung zu bringen und schliesslich Informationen zu sammeln und zu personalisieren. Zugleich befürchten die Konsumenten auch einen gewissen Produkt-Paternalismus, d.h. die Technologie könnte menschliches Verhalten interpretieren und darauf reagieren. Dies könnte soweit gehen, dass Konsumgüter bestimmte von Hersteller nicht intendierte Anwendungen (z.B. Einbau des Ersatzteils eines Konkurrenten) erkennen und „bestrafen“.

Sicherheit: Hier geht es um die Angst vor Missbrauch und Diebstahl. Dies kann sich einerseits auf die Datensicherheit beziehen. Andererseits spielen aber auch ganz praktische Überlegungen eine Rolle, z.B. wie man sich davor schützen kann, dass andere erkennen, dass man wertvolle Sachen auf sich trägt.

Gesundheit und Umweltschutz: Vermehrt werden kritische Töne und Fragen in Bezug auf die Gesundheit und Umwelt sowie die Nachhaltigkeit laut[87].

Damit die RFID-Technologie von den Verbrauchern breit akzeptiert wird, sollten vor allem vier Dimensionen Beachtung finden: Wirtschaftspolitisch gilt es erstens zu verhindern, dass Märkte abgeschottet werden. Zudem müssen Aspekte des geistigen Eigentums in Betracht gezogen werden. Zweitens spielen der Wissensstand und die Information der Verbraucher eine grosse Rolle, damit diese die Technologie zu ihrem eigenen Vorteil nutzen können. Drittens sollten die Vorbehalte der Verbraucher schon in der technischen Entwicklung berücksichtigt werden. Viertens spielen auch Aspekte des Datenschutzes für die Verbraucher eine wichtige Rolle[88].

Wirtschaftspolitische Dimension

Wettbewerb: RFID kann dazu eingesetzt werden, den Wettbewerb zu behindern und Märkte zu trennen. Damit würde die Wahlfreiheit der Verbraucher eingeschränkt[89]. Beispielsweise kann ein Printer

[86] Mittelland Zeitung Gesamtausgabe, 20.07.2006: 33
[87] Consumers’ scenarios for a RFID policy. Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, COM(2007) 96: 10.
[88] Aspekte des Datenschutzes wurden im vorangehenden Kapitel behandelt.
[89] RFID technology has the potential to be used in anti-competitive ways, restricting consumer choice. For instance, a car manufac-

mittels RFID erkennen, ob die Nachfüllpatronen seines Herstellers eingesetzt werden um bei ansonsten nicht unterscheidbaren Konkurrenzprodukten die Funktion verweigern. RFID-Anwendungen könnten den Gebrauch von Produkten überwachen und die Konsumenten dazu zwingen, in Ergänzung dazu bestimmte Produkte zu kaufen, welche vielleicht auch teurer sind, und nicht zu einem Konkurrenten zu wechseln („Lock-in-Effekt).

Geistiges Eigentum: Die Technologie könnte auch eingesetzt werden, um vor Fälschung und Produktpiraterie zu schützen. Voraussetzung dazu ist allerdings, dass die RFID-Technologie selbst sicher gegen Fälschung geschützt ist, was heute nicht generell zutrifft. Zudem könnte RFID auch als restriktiver Mechanismus, ähnlich der digitalen Rechteverwaltung (Digital Rights Management, DRM), eingesetzt werden, um die Möglichkeiten der Nutzung eines Produkts künstlich einzuschränken. Solche Massnahmen sind von Konsumentenseite aber umstritten.

Konsumenteninformation und Verbraucherbildung

Das Vertrauen und der Wissensstand der Konsumenten sind wichtige Bedingungen für den Erfolg der Technologie. Die Verbraucher müssen erstens über die Vor- und Nachteile der RFID-Technologie informiert sein und im Einzelfall erkennen können, dass überhaupt RFID-Technologie eingesetzt wird. Sie müssen den Umgang mit der RFID-Technologie erlernen können. Die Verbraucherbildung ist eine wichtige Voraussetzung dafür, dass die Konsumenten ihre Funktion als rationale Marktteilnehmer und als Motor der Wirtschaft ausüben können. Konsumentenorganisationen stellen entsprechende Informationen zur Verfügung und vertreten die Interessen der Konsumenten gegenüber anderen Stakeholdern, z.B. durch Teilnahme an Dialogplattformen.[90]

Diskussion der Chancen und Risiken von RFID: Die Verbraucher müssen über die Vor- und Nachteile der RFID-Technologie informiert sein. Diese Technologie kann in Bereichen wie öffentliche Gesundheit, Lebensmittelsicherheit oder Tiergesundheit zu grossen Fortschritten beitragen. Dies ist aber nur möglich, wenn auch die Risiken offen und sachlich diskutiert werden. Bedenken von Laien dürfen nicht voreilig als ungerechtfertigt zurückgewiesen werden, wenn doch die Wissenschaft selbst noch vor ungeklärten Fragen steht. Das bedeutet, dass auch das Verständnis für die öffentliche Risikowahrnehmung, welche oft von der wissenschaftlichen Perspektive abweicht, verbessert werden muss. Über mögliche Risiken soll klar informiert werden.

Information über den Einsatz von RFID und die Rechte des Verbrauchers: Durch das Identifizieren von Gegenständen wird es theoretisch möglich, auch den Konsumenten zu identifizieren und Profile von ihm zu erstellen. Informationen, welche sich nur auf Konsumgüter beziehen, könnten missbräuchlich mit persönlichen Daten auf der Kreditkarte, Kundenkarte oder auf Banknoten in Verbindung gebracht werden. Ohne dass er es bemerkt, kann der Konsument automatisch identifiziert werden. Viele Verbraucher haben noch nie oder nur vage von RFID gehört und sind sich über mögliche Folgen bezüglich ihrer Grundrechte, ihrer Privatsphäre und Menschenwürde nicht bewusst oder bekunden Unbehagen. Tags sind oft so klein, dass sie im oder am Produkt nicht erkennbar sind. Umso wichtiger ist deshalb die Informationen darüber, dass RFID-Technologie eingesetzt wird. Deshalb sollten RFID-Chips klar gekennzeichnet werden. Dabei ist insbesondere auch auf die Zugänglichkeit („Accessablilty“)[91] zu achten.

Bei den Konsumgütern sollten Verbraucher insbesondere drüber informiert werden:

- ob ein RFID-Tags in einem Produkt vorhanden ist;

---

turer X would design software that exclusively works with the spare-parts of this samemanufacturer X - parts that will have RFID chips embedded (tie-in products). The usage of RFID in applications that control the use of products or force consumers to buy products that are more costly would restrict consumer choice, and consequently impact competition. Similarly, RFID technology must not prevent the use of compatible, alternative printer refill cartridge, i.e. those not produced by the original manufacturer, by means of authenticity certificates. (Consumers' scenarios for a RFID policy. Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework. COM(2007) 96:12)

[90] Zur Bedeutung von Dialogplattformen siehe Kapitel 6.2 Informationsgesellschaft.

[91] Zugänglichkeit oder Barrierefreiheit (Accessablilty) bedeutet, dass Gegenstände und Einrichtungen so gestaltet werden, dass sie von jedem Menschen unabhängig von einer eventuell vorhandenen Behinderung uneingeschränkt benutzt werden können.

- ob der Tag nach dem Verkauf noch einen spezifischen Zweck erfüllt;
- ob vorhersehbare Risiken im Zusammenhang mit dem Vorhandensein des Tags bestehen und mit welchen Massnahmen der Konsument sie einschränken kann.

Informationen über die Möglichkeit des Umgangs mit der Technologie: Verbraucher sollten spätestens nach dem Kauf die Möglichkeit haben, RFID-Tags zu zerstören, zu entfernen oder zu deaktivieren[92]. Eine zusätzliche Möglichkeit sind RFID-Tags, die vom Konsumenten einfach „enthauptet" werden können. Dieser Vorgang könnte automatisch an der Kasse geschehen. Konsumenten, welche sich entschliessen, den Tag zu deaktivieren, sollen nicht diskriminiert werden. Die Deaktivierung des Tags darf keine Relativierung oder gar Beendigung der gesetzlichen Verpflichtungen der Händler oder Hersteller zur Folge haben (z.B. Wegbedingung der Produkthaftpflicht oder keine Benachrichtigung bei Rückrufen etc.). Verbraucher sollten ferner nachprüfen können, dass die Aktion tatsächlich erfolgt ist.
Eine solche Lösung bietet zum Beispiel der „Clipped Tag" (Abbildung 13) [93], dessen grösster Teil der Antenne der Endverbraucher selbst entfernen kann. Somit wird die im RFID-Tag gespeicherte Information nur noch aus einer Entfernung von weniger als 5 cm auslesbar. Im Unterschied zum „Kill Command", bei dem alle gespeicherten Informationen gelöscht würden, bleiben die Daten jedoch prinzipiell erhalten und können mit Zustimmung des Nutzers wieder ausgelesen werden. Dies könnte etwa bei einem Garantiefall im Interesse des Kunden sein. Gleichzeitig müsste der Handel nicht in Geräte zur Chip-Deaktivierung investieren.

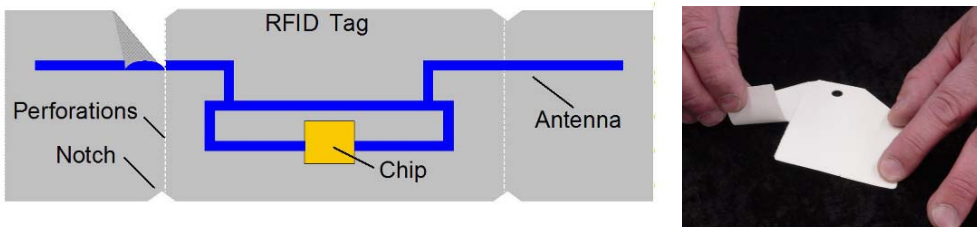

***Abbildung 13** „Clipped Tag" Schematische Darstellung und Prototyp des datenschutz-freundlichen RFID-Tag-Konzeptes*

Anonymes Einkaufen soll weiterhin möglich sein, d.h. ohne den Einsatz von Debit-, Kredit- oder Kundenkarten oder anderen Zahlungssystemen, welche persönliche Daten enthalten. Wenn Kunden Tags aus früheren Einkäufen mitführen (z.B. in Kleidern), sollten sie damit nicht unbemerkt identifiziert werden.

Mitarbeit in der Normengremien (Technische Dimension)

Die Bedenken der Konsumenten sollen vor dem Einsatz von RFID-Technologie berücksichtigt werden und wenn möglich schon früh auch in das Design und die Entwicklung von RFID einfliessen. Diese Aufgabe kommt traditionellerweise der Normung zu. In den Normengremien (SNV[94], CEN[95], ISO[96]) sind aber die Interessen und Sichtweisen der Verbraucher untervertreten. Dies kann dazu führen, dass bei der Normung entscheidende Akzeptanzrisiken übersehen werden. Mangels Alternativen sollten entsprechende Normen einer breiten Konsultation unterzogen werden. Es wäre zudem wichtig, dass entsprechende Standards allen interessierten Kreisen breit zugänglich sind (d.h. sie dürfen nicht kostenpflichtig sein, es darf darauf keine Urheberrechte geben, etc).

[92] In Frankreich hat die CNIL (Commission nationale de l'informatique et des libertés) festgehalten, dass RFID-Chips einen Deaktivationsmechanismus enthalten sollen, welcher es den Konsumenten erlaubt, den Chip auszuschalten.
[93] http://www.zurich.ibm.com/news/06/clippedtag_d.html
[94] Schweizerische Normen-Vereinigung
[95] Comité Européen de Normalisation
[96] International Organization for Standardization

Verbraucherrelevante Aspekte des Datenschutzes

Aspekte des Datenschutzes wurden im Kapitel 5 behandelt. Für die Verbraucher spielt der Datenschutz eine zentrale Rolle. Der Datenschutz umfasst hier unter anderem (nicht ausschliesslich):

- Anforderungen an das Sammeln von Personendaten: Mitteilungen zur Privatsphäre[97] („Privacy notices“) sollten neben den Informationen über die gesammelten Daten, den Zweck der Datensammlung und das Recht auf Zugang zu den gesammelten Daten auch über das Vorhandensein von entsprechenden Tags und deren Inhalt, Verwendung und Kontrolle informieren. Zudem sollten diese auf die Anwesenheit von Lesegeräten, die Möglichkeit zur Deaktivierung von Tags und auf Auskunfts- und Hilfestellen hinweisen.
- Opt-in: die Verbraucher sollen explizit zustimmen müssen, wenn Daten aus von ihnen erworbenen Tags verarbeitet oder ihre persönlichen Daten auf einem Tag gespeichert werden (opt-in System). Dabei sollten die Daten des Konsumenten nur gelesen werden dürfen, wenn dieser explizit seine schriftliche Zustimmung gegeben hat, und dies bevor seine persönlichen Daten auf einem Tag gespeichert werden.

Forderungen aus der Sicht der Verbraucher

- Deklarationspflicht: RFID-Tags sollten klar als solche gekennzeichnet sein. Dabei ist insbesondere auf die Zugänglichkeit („Accessablilty“) zu achten (Nichtdiskriminierung).
- Datensammlung: Ohne ausdrückliche Zustimmung des Konsumenten sollten weder Daten durch Auslesen der ihm erworbenen Tags gesammelt, noch aus den gesammelten Daten Profile erstellt werden dürfen. Privacy Enhancing Technologies (PETs)[98] könnten als Lösungsansatz beigezogen werden.
- Deaktivierung: Verbraucher sollten in der Lage sein, von ihnen erworbene Tags auszuschalten, entweder durch Zerstörung oder durch reversible Deaktivierung Diese erlaubt es, den Tag bei Bedarf zu reaktivieren, z.B. im Falle von Reklamationen. Die Deaktivierung des Tags darf nicht die gesetzlichen Verpflichtungen (z.B. Produkthaftpflicht) des Verkäufers oder Herstellers reduzieren oder gar beenden (Nichtdiskriminierung).
- Frühzeitige Information: Erstellung einer Informations- und Diskussionsplattform, welche Verbraucher auf breiter Basis einbezieht.
- Internationale Kooperation: Fortsetzung der Zusammenarbeit von Schweizer Stellen mit der EU und mit internationalen Normungsgremien auf allen Ebenen, um einen handelshemmenden Schweizer Alleingang zu vermeiden. Verbraucherorganisationen sollen bei Normenarbeiten miteinbezogen werden.
- Gesundheit und Umwelt: Aus Sicht der Verbraucher ist es entscheidend, dass im Bereich der Gesundheit eine vertiefte Auseinandersetzung mit der Technologie stattfindet, da noch wenig über die gesundheitlichen Auswirkungen von elektromagnetischen Feldern bekannt ist. Verbraucherorganisationen fordern nachhaltige und umweltfreundliche Tags. Der zu erwartende Anstieg des Bedarfs an informationstechnischer Infrastruktur (Lesegeräte, Backend-Datenbanksysteme) soll nicht zu einem Anstieg des Energieverbrauchs führen[99].
- Haftung: Es sollte geklärt werden, inwiefern ein Anbieter für Schäden haftet, welche den Konsumenten durch Sicherheitslücken in der RFID-Technologie entstehen.

Der rasch zunehmende Einsatz von RFID-Systemen drängt zum Handeln. Datenschutz und Sicherheit sollten bereits vor der Einführung der RFID-Technologie beachtet werden, damit eventuell auftretende

[97] Dies kann z.B. durch Icons auf den getagten Produkten, Hinweistafeln oder Leseterminals zum Abrufen der gespeicherten Daten geschehen. Ebenso sollten Standort und Reichweite von Lesegeräten deutlich gekennzeichnet werden.
[98] Privacy Enhancing Technologies (PET) sind technologische Massnahmen, welche in Ergänzung zu rechtlichen Massnahmen den Schutz der Privatsphäre bezwecken. Die Europäische Kommission fördert und fordert in einer Mitteilung die Entwicklung und Anwendung solcher technologischer Massnahmen um Identitätsdiebstahl und andere Angriffe auf die Privatsphäre zu verhindern. Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre (Quelle: http://eur-lex.europa.eu/LexUriServ/site/de/com/2007/com2007_0228de01.pdf)
[99] Consumers’ scenarios for a RFID policy. Joint ANEC/BEUC Comments on the Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, COM(2007) 96: 10

Probleme nicht im Nachhinein gelöst werden müssen, wenn das Vertrauen in die Technologie durch negative Erfahrungen beschädigt ist. Sowohl die Anforderungen der aktiv am Aufbau der RFID-Systeme beteiligten Akteure (z.B. Unternehmen, öffentliche Verwaltungen, Krankenhäuser) als auch die betroffenen Endnutzer (Bürger, Verbraucher, Patienten, Angestellte) müssen beim Systementwurf einbezogen werden. Konsumentenorganisationen sollen an der Ausarbeitung anwendungsbezogener Leitlinien (Verhaltensregeln, gute Praktiken) beteiligt sein.

Fazit

Konsumentinnen und Konsumenten müssen Zugang zu Informationen über RFID erhalten. Eine offene Diskussion der Chancen und Risiken ist notwendig, insbesondere hinsichtlich denkbarer Gesundheits- und Datenschutzrisiken. RFID-Tags und ihre Lesegeräte müssen klar gekennzeichnet sein. Tags müssen von ihrem Besitzer aus- und eingeschaltet werden können. Die Interessen der Konsumentinnen und Konsumenten sollen in den Normengremien besser vertreten sein.

6.2 RFID und die Informationsgesellschaft

Durch die rasante Zunahme der Internetnutzung, die zunehmende Vernetzung aller Lebensbereiche sowie die neuen elektronischen Dienstleistungsangebote hat die Informationsgesellschaft in der Schweiz in den vergangenen Jahren gewaltige Fortschritte gemacht. Bei der zukünftigen Entwicklung der Informationsgesellschaft stellt die RFID-Technologie eine der wichtigen Grundlagen dar. Einerseits eröffnet der Einsatz von RFID der Informationsgesellschaft Schweiz die Chancen auf mehr Sicherheit und Effizienz und anwenderfreundlichere Dienstleistungen. Andererseits können RFID-Anwendungen speziell in personenidentifizierenden Anwendungsbereichen die Angst vor einer Kontroll- und Überwachungsgesellschaft hervorrufen. Die technologischen Entwicklungen stellen für Anbieter, Anwender und Regulierer somit eine grosse Herausforderung dar.
Zukünftig sind deshalb nicht nur die Robustheit und Integrität der kritischen Informations-Infrastruktur, z.B. der Telekommunikationsnetze, zu garantieren, sondern auch die Transparenz für den Endnutzer zu schaffen. Die Bevölkerung der Schweiz soll dazu in geeigneter Form auf den Umgang mit RFID im täglichen Leben vorbereitet werden. Dafür sind beispielsweise Partnerschaften zwischen Anbietern von Anwendungen mit Medien und Bildungsinstitutionen denkbar. Aber auch frühzeitig eingeleitete partizipative Verfahren tragen dazu bei, das Bewusstsein sämtlicher Stakeholder aus Wirtschaft, Verwaltung, NGOs etc. für die Sichtweisen anderer zu erhöhen.
Zu den partizipativen Verfahren gehört die sogenannte Dialog-Plattform. Sie bietet den Stakeholdern die Möglichkeit, eine gemeinsam getragene Strategie zu erarbeiten, die datenschutzrelevante, ökonomische und ethische Aspekte berücksichtigt. Erstrebenswert wäre in einem solchen Rahmen die Erarbeitung einer RFID-Strategie durch die Stakeholder. Diese soll den Rahmen für die Entwicklung, den Einsatz und die Nutzung von RFID bilden und einen adäquaten Umgang mit potenziellen Chancen und Risiken ermöglichen. Gelingt den Stakeholdern gar die Formulierung eines „Code of Conduct“[100], können sie so den gesetzlichen Regulierungsdruck verkleinern.[101]

Fazit

Die RFID-Technologie ist ein wichtiger Baustein der Informationsgesellschaft, welche durch die starke Vernetzung aller Lebensbereiche geprägt ist. Um Vertrauen und Transparenz zu schaffen sowie das Bewusstsein sämtlicher Stakeholder aus Wirtschaft, Verwaltung, NGO etc. für die Sichtweisen der anderen zu erhöhen, sollten frühzeitig partizipative Verfahren wie z.B. Dialog-Plattformen eingerichtet werden.

[100] Code of Conduct: Verhaltenskodex; Selbstverpflichtung, bestimmten Verhaltensmustern zu folgen bzw. diese zu unterlassen.
[101] Eine Stakeholder-Dialog-Plattform zu RFID kann auf den "Kompass zu einem verantwortungsvollen Einsatz von Pervasive Computing (PvC)“ zurückgreifen, welcher von Stakeholdern aus Wirtschaft, Wissenschaft, Datenschutz-, Konsumenten-, Patienten- und Umweltorganisationen und Verwaltung mit der Stiftung Risiko-Dialog 2004 bis 2006 durchgeführt worden ist. Der Kompass dient Organisationen und Personen, die PvC-Technologien entwickeln, herstellen, vertreiben, anwenden oder nutzen, als Empfehlung: http://www.risiko-dialog.ch/Themen/Kommunikationstechnologien/263

7. RFID Thematik in der EU

RFID stellt in der EU ein sehr wichtiges Thema dar. Es wurde früh erkannt, dass die Technologie ein grosses Potenzial für die Förderung der Innovation und des Wirtschaftswachstums besitzt. Europa ist schon heute führend in der RFID-Forschung und –Entwicklung, der Produktion von RFID-Komponenten sowie der Entwicklung von Anwendungen und deren Markteinführung. Diese Stellung soll gehalten bzw. noch verstärkt werden. Voraussetzungen dazu sind ein Gesetzesrahmen, der den Bürgern wirksame Schutzvorkehrungen bietet sowie Institutionen, welche die Technologieentwicklung fördern, Chancen und Risiken analysieren und notwendige Massnahmen koordinieren. In den letzten zwei Jahren (2006 / 2007) sind in der EU einige Initiativen entstanden, welche die heutige Situation, mögliche Entwicklungsszenarien sowie den Handlungsbedarf analysieren und Lösungsmöglichkeiten aufzeigen. Einige Projekte sind in den folgenden Kapiteln erläutert.

Mitteilung der EU-Kommission „RFID in Europa: Schritte zu einem ordnungspolitischen Rahmen“

Die Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen mit dem Titel „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“[102] basiert auf den Ergebnissen einer öffentlichen Konsultation, welche die Kommission im Jahr 2006 durchgeführt hat. Zu folgenden Themen wurde Stellung bezogen:

Datenschutz, Wahrung der Privatsphäre und Datensicherheit: RFID als eine grundlegende und überall einsetzbare Technik hat das Potenzial, in die Privatsphäre einzudringen und diese zu verletzen. Der Schutz personenbezogener Daten ist ein wichtiger Grundsatz in der EU; er wurde als eine der Freiheiten in Artikel 8 der Charta der Grundrechte der EU aufgeführt und in der allgemeiner Datenschutzrichtlinie 95/46/EG[103] geregelt. Die Richtlinie ist unabhängig von den für die Datenverarbeitung verwendeten Mittel und gilt für alle Technologien einschliesslich der RFID. Die Mitgliedstaten sorgen für die Umsetzung.
Die allgemeine Datenschutzrichtlinie wird ergänzt durch die Datenschutzrichtlinie für die elektronische Kommunikation[104], die für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen gilt. Wegen dieser Einschränkung fallen viele RFID-Anwendungen nur unter die allgemeine Datenschutzrichtlinie und nicht direkt in den Anwendungsbereich der Datenschutzrichtlinie für die elektronische Kommunikation.
Für die praktische Einführung neuer Technologien wie z.B. RFID sehen beide Richtlinien die Ausarbeitung besonderer **Verhaltensregeln** vor. Es handelt sich dabei um Gestaltungskriterien für Datenschutz und Datensicherheit, die sowohl auf technologischer und organisatorischer Ebene als auch in Geschäftsabläufen anzuwenden sind. Da die konkreten Sicherheits- und Datenschutzrisiken von der Art der jeweiligen RFID-Anwendung abhängig sind und sich schnell verändern, braucht es differenzierte Lösungen, die dem aktuellen Stand der RFID-Technologie entsprechen Die EU wird die Ausarbeitung der Verhaltensregeln durch eine Arbeitsgruppe aus Fachleuten aller beteiligten Seiten unterstützen. Die Überprüfung der Umsetzung erfolgt auf einzelstaatlicher Ebene durch die zuständige Datenschutzbehörde bzw. auf europäischer Ebene durch die „Artikel-29-Datenschutzgruppe“[105].

„Internet der Dinge“: Eine wichtige Komponente der RFID-Systeme sind die Datenbanken für die Registrierung von identifizierten Objekten im künftigen „Internet der Dinge“, in dem mehrere Milliarden Ob-

[102] KOM(2007) 96
[103] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener daten und zum freien datenverkehr, ABI L 28 vom 23.11.1995
[104]Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.
[105]Die Artikel-29-Datenschutzgruppe hat hierzu ein Arbeitspapier 105 „Datenschutzfragen im Zusammenhang mit der RFID-Technik“ (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf) vorgelegt.

jekte zu einer global vernetzten Kommunikationsinfrastruktur verbunden werden können. Es ist wichtig, dass die Datenbanken interoperabel, offen und diskriminierungsfrei sind. Es darf nicht zugelassen werden, dass sie von Einzelnen für Sonderinteressen benutzt werden. Überdies müssen in Bezug auf Sicherheit, Ethik und Datenschutz die Bedürfnisse aller Beteiligten beachtet werden. Einige Vorgaben für Management und Kontrolle wurden im Rahmen des Weltgipfels über die Informationsgesellschaft (WSIS)[106] ausgearbeitet.

Funkfrequenzen: Wie für alle drahtlosen Geräte müssen auch für RFID-Anwendungen ausreichende Funkfrequenzen zur Verfügung stehen. Besonders wichtig ist hierbei die Harmonisierung der Bedingungen für eine Frequenznutzung. Neben mehreren lizenzfreien Frequenzbändern für RFID-Systeme hat die Kommission vor kurzem eine Entscheidung[107] über RFID-Frequenzen im UHF-Band erlassen, um der wachsenden Nachfrage Rechnung zu tragen. Dadurch entsteht eine harmonisierte europäische Grundlage für RFID-Anwendungen im europäischen Binnenmarkt. Angesichts der zunehmenden RFID-Nutzung muss die Nachfrage allerdings weiter beobachtet werden.

Normen: Die zügige Verabschiedung internationaler Normen[108] und die Harmonisierung regionaler Normen ist für eine reibungslose Einführung der Dienste genauso wichtig wie die Interoperabilität RFID-gestützter Informationssysteme. Die EU-Kommission soll eine aktive Rolle bei der Ausarbeitung eines europäischen Ansatzes für die RFID-Normung übernehmen.

Umwelt: Aus umweltpolitischer Sicht fallen RFID-Komponenten unter die Definition elektrischer und elektronischer Geräte, welche in den Richtlinien 2002/96/EG über Elektro- und Elektronik-Altgeräte (WEEE) und 2002/95/EG zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten (RoHS) enthalten ist. Hiernach fallen RFID-Komponenten in die Kategorie 3 „IT- und Telekommunikationsgeräte“. Damit unterliegen RFID-Komponenten dem Geltungsbereich der RoHS Richtlinie, die die Verwendung der gefährlichen Stoffe Cd, Hg, Pb, CrVI, polybromierte Biphenyle (PBB) oder polybromierte Diphenylester (PBDE) einschränkt.

Gesundheit: Hinsichtlich der Gesundheitsaspekte beobachtet die Kommission seit langem mit Unterstützung des Wissenschaftlichen Ausschusses[109] mögliche Auswirkungen elektromagnetischer Felder (EMF) auf die menschliche Gesundheit. Ferner wurden rechtliche Rahmenbedingungen für den Schutz der Arbeitnehmer und der Bürger geschaffen. So gibt es Grenzwerte für die Exposition der Bevölkerung gegenüber elektromagnetischen Feldern (Empfehlung 1999/519/EG des Rates[110] vom 12. Juli 1999, die gegenwärtig überprüft wird) und Vorschriften für die Exposition der Arbeitnehmer (Richtlinie 2004/40/EG[111]). Ausserdem wurden Beschränkungen für die EMF-Emissionen, die von Produkten auf dem EU-Markt ausgehen dürfen, festgelegt, um die Sicherheit der Nutzer und der Nichtnutzer zu gewährleisten (Richtlinie 1999/5/EG[112]).
Die Kommission wird fortfahren, die Einhaltung der rechtlichen Rahmenbedingungen sowohl auf EU-Ebene als auch in den Mitgliedstaaten sicherzustellen, und in aktiver Weise die Forschung und Auswertung wissenschaftlicher Nachweise, insbesondere mit Bezug auf Akkumulationseffekte bei der Exposition gegenüber elektromagnetischen Feldern unterschiedlicher Emissionsquellen, unterstützen[113].

Forschung und Innovation: Die Kommission wird künftig Forschungsarbeiten auf dem Gebiet der Sicherheit von RFID-Systemen fördern. Ausgehend von den Ergebnissen der europaweiten Konsultation

[106] Auf dem Wege zu einer globalen Partnerschaft in der Informationsgesellschaft: Folgemaßnahmen nach der Tunis-Phase des Weltgipfels über die Informationsgesellschaft (WSIS), KOM(2006) 181 endgültig.
[107] Entscheidung 2006/804/EG der Kommission vom 23. November 2006 zur Harmonisierung der Frequenzbänder für Geräte zur Funkfrequenzkennzeichnung (RFID-Geräte) im Ultrahochfrequenzband (UHF).
[108] Insbesondere die ISO-RFID- Norm für die Artikelkennzeichnung (ISO 18000) und die in Vorbereitung befindlichen ISO-Vorschriften für aktive Transponder.
[109] http://ec.europa.eu/health/ph_risk/committees/committees_de.htm
[110] http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999H0519:DE:HTML
[111] http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004L0040R(01):DE:HTML
[112] http://europa.eu.int/eur-lex/pri/de/oj/dat/1999/l_091/l_09119990407de00100028.pdf
[113] Solche Untersuchungen werden mit Unterstützung der Wissenschaftlichen Ausschüsse der Kommission, insbesondere des SCENIHR, durchgeführt. (http://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_006.pdf).

wird die Kommission überdies die Weiterentwicklung der Technologien für einen besseren Schutz der personenbezogenen Daten als Mittel zur Minderung der Datenschutzrisiken unterstützen. In gross angelegten Pilotprojekten in bestimmten Anwendungsbereichen sollen Erfahrungen über Vorteile und möglichen Risiken gesammelt und analysiert werden.

Mitteilung der EU-Kommission „Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung[114]

Diese Mitteilung überprüft die gegenwärtigen Bedrohungen der Sicherheit der Informationsgesellschaft und legt dar, welche zusätzlichen Schritte unternommen werden sollten, um die Netz- und Informationssicherheit zu verbessern. Im Vordergrund steht dabei die Weiterentwicklung einer dynamischen Strategie, die folgende drei Punkte umfasst: Massnahmen zu Verbesserung der Netz- und Informationssicherheit, Erarbeitung von Rechtsrahmen für die elektronische Kommunikation (einschliesslich Datenschutzfragen) sowie die Bekämpfung der Internet-Kriminalität.
Grundlage der Strategie zur Netz- und Informationssicherheit ist die Förderung von **Verschiedenartigkeit, Offenheit und Interoperabilität**. Mitgliedstaaten und Wirtschaft werden aufgefordert, entsprechende Massnahmen zu ergreifen und sich an den europäischen Plattformen zu beteiligen. Als solche Plattform wurde im Jahre 2004 die Europäischen Agentur für Netz- und Informationssicherheit (ENISA) eingerichtet. Die Strategie basiert auf drei Grundlagen: Dialog, Partnerschaft und Delegation der Verantwortung. So soll der Dialog zwischen den Mitgliedstaaten sowie zwischen der Wirtschaft und den Endnutzern gefördert werden. Die ENISA soll versuchen, eine Partnerschaft mit den Mitgliedstaaten und den Interessenvertretern aufzubauen. Weiterhin soll den einzelnen Interessengruppen mehr Verantwortung übertragen werden. Nur so lässt sich deren Bewusstsein über Risiken und die Notwendigkeit der Massnahmen stärken.

Bericht "RFID Technologies: Emerging Issues, Challenges and Policy Options"[115]

Der 274 Seiten lange Bericht wurde im Auftrag der EU-Kommission vom „DG Joint Research Centre, Institute for Prospective Technological Studies" ausgearbeitet. Ziel war es, die sozioökonomischen Auswirkungen der RFID-Technologie zu untersuchen sowie politische Kriterien festzulegen, die den Bedürfnissen der EU-Bürger entsprechen. Aufgrund von Fallstudien zur ökonomischen Entwicklung der vorhandenen und kommenden RFID-Technologien, ihrer Marktparameter und sozialen Aspekte wurden folgende fünf Themenbereiche untersucht: Tieridentifikation, health care, öffentlicher Transport, Personenidentifikation, ICT-Bereich[116]. Eine Auswahl an möglichen Interventionsinstrumenten wurde aufgezeigt, deren Realisierung im Rahmen der Gesetzgebung, Selbstregulierung oder durch technische Lösungen erfolgen kann:

- Harmonisierung von Frequenzen und Sicherheitsstandards zur Förderung der Interoperabilität
- Organisation der Infrastruktur als Vorbereitung für das Internet der Dinge
- Informationskampagnen, um die Akzeptanz der Technologie bei der Bevölkerung zu fördern
- Adäquate Gesetzgebung sowie Richtlinien und Verhaltensregeln für den Umgang mit Risiken
- Förderung der Forschung sowohl im Bereich der Technologieentwicklung wie auch zu möglichen Risiken. Aufzeigen von Lösungen zur Risikominimierung

Die Ausführungen dieses Berichts decken sich weitgehend mit denjenigen in anderen europäischen Dokumenten.

Expertenkonferenz "RFID: Towards the Internet of Things" / Bericht "European Policy Outlook RFID"

Mehr als 400 internationale Experten haben anlässlich der Konferenz „Radio Frequency Identification (RFID) – Auf dem Weg zum Internet der Dinge" im Juni 2007 in Berlin Strategien für die erfolgreiche

[114] KOM(2006) 251
[115] EUR 22770 EN 2007
[116] Information- and Communication Technologies

Einführung von RFID in Europa diskutiert. Die Konferenz wurde im Rahmen der deutschen EU-Ratspräsidentschaft durchgeführt. Als Basis für die Konferenz wurde ein Grundsatzpapier „European Policy Outlook RFID“ unter Mitwirkung massgeblicher Vertreter aus Wirtschaft, Verbänden, Regierungsstellen und der europäischen Kommission entworfen. Als Ausgangsbasis für das weitere Vorgehen auf europäische Ebene wurden im Grundsatzpapier die Positionen der verschiedenen Interessengruppen aus Wirtschaft, Wissenschaft und Gesellschaft erstmals konsensual zusammengeführt und nationale und europäische Aktionsfelder aufgezeigt. Die Schweiz war sowohl an der Konferenz wie auch bei der Ausarbeitung des Grundsatzpapiers beteiligt. Im Grundsatzpapier wird festgehalten, dass die Einführung von RFID zu einer der wichtigsten technologischen Herausforderungen der kommenden Jahre in Europa gehört. RFID bietet enorme Potenziale zur Produktivitätssteigerung und für die Entstehung neuer Geschäftsmodelle mit Perspektiven für Wachstum und Beschäftigung. Um diese Chancen auszunutzen, wurden folgende politische Schwerpunkte besonders empfohlen:

- Förderung des Zugangs kleiner und mittlerer Unternehmen zu RFID
- Verbreitung der Funktechnik innerhalb der Bevölkerung
- Vermeidung von Marktbehinderungen
- Harmonisierung von Frequenzen
- Vertretung europäischer Interessen in einem globalen „Netzwerk der Dinge“
- Unterstützung der Technologie-Forschung in Europa, insbesondere für übergreifende „Prestige-Projekte“
- Koordination der RFID-Aktivitäten in Europa

In Bezug auf mögliche Risiken wurden folgende Punkte erwähnt:

- Um den Datenschutz zu gewährleisten, braucht es gegenwärtig kein spezielles RFID-Gesetz, da die Datenschutz-Gesetzgebung weiterhin technologieneutral ausgerichtet sein sollte. Allerdings werden die Mitgliedsstaaten und die EU-Kommission aufgefordert, diese Gesetze in Bezug auf die RFID-Anwendungen periodisch zu überprüfen. Im Moment sei die Selbstregulierung der Wirtschaft gefragt.
- Auch zu Gesundheits- und Umweltschutz braucht es gegenwärtig keine neue Regulierung. Längerfristig soll die Abfallentsorgung näher untersucht werden.

Generell werden im Grundsatzpapier die Chancen der RFID-Technologie höher bewertet als potenzielle Risiken. Dementsprechend liegt der Handlungsbedarf in Förderung der Technologie. Diese soll aber auch im Hinblick auf mögliche aufkommende Risiken sorgsam verfolgt werden.

8. Handlungsbedarf und Empfehlungen

8.1 Allgemein: Technologieentwicklung und Stakeholder-Beteiligung

Die RFID-Technologie ist eine zukunftsträchtige Technologie, deren Nutzen und Vorteile offensichtlich sind. Es ist deshalb nicht erstaunlich, dass beispielsweise in der EU der Handlungsbedarf vor allem darin gesehen wird, die Rahmenbedingungen für die RFID-Technologie so zu gestalten, dass ihre Vorteile und Chancen maximal genutzt werden können. Dadurch sollen sowohl die Innovation wie auch das Wirtschaftswachstums gefördert werden. Obwohl anerkannt wird, dass die RFID-Technologie auch einige Risiken in sich birgt, werden diese im Moment meistens als unproblematisch eingestuft.

Der vorliegende Bericht geht sowohl auf Vorteile und Chancen wie auch potenzielle Risiken der RFID-Technologie ein. Der Handlungsbedarf wird vor allem darin gesehen, mögliche Risiken frühzeitig zu erkennen und zu minimieren, also bevor sie in einer sehr breiten Anwendung von RFID zu Schäden und Vertrauensverlust führen können. Offene Fragen zu möglichen Risiken in den vier Bereichen Gesundheit-, Daten-, Umwelt- und Konsumentenschutz sind nicht neu; gleiche oder ähnliche Fragen wie z.B. gesundheitliche Risiken elektromagnetischer Strahlung oder der Schutz von Personendaten wurden bei anderen Technologien bereits früher behandelt. Der vorliegende Bericht zeigt aber, dass diese Risiko-Problematik bei RFID-Anwendungen verschärft ist und dass in Zukunft durch die Allgegenwart von RFID-Anwendungen im Alltag weitere Risikopotenziale zum Vorschein kommen könnten.

Mit Ausnahme einiger Produktenormen gibt es weder in der Schweiz noch international spezifische RFID-Regelungen. Die untersuchten Risiko- und Sicherheitsaspekte der RFID-Technologie fallen in die Geltungsbereiche folgender sektorieller Regelungen: Datenschutz, Gesundheitsschutz, Umweltschutz, Konsumentenschutz, Produktesicherheit, usw. Im Bericht wurden die vorhandenen, sektoriellen Instrumente und Rahmenbedingungen (Gesetze, Regulierung, Institutionen) auf ihre RFID-Tauglichkeit überprüft sowie der Handlungsbedarf abgeleitet, der in den nachfolgenden 10 Empfehlungen zum Ausdruck kommt. In den meisten Fällen sind die notwendigen Rahmenbedingungen vorhanden. Es wurden jedoch auch Schwachstellen gefunden, die bei RFID-Anwendungen besonders problematisch sind und auch in anderen Gebieten relevant sein könnten. Sie sind also nicht spezifisch für RFID, aber könnten bei einer sehr breiten Anwendung dieser Technologie neue Bedeutung erhalten. Die heute bestehenden Schwachstellen sowie entsprechende Lösungsansätze sind in diesem Kapitel aufgeführt. Um auf Technologieentwicklungen schnell reagieren zu können, müssen Nutzen-Risiko-Analysen periodisch wiederholt und die Rahmenbedingungen regelmässig überprüft werden – sowohl bezüglich der Maximierung der Chancen wie auch auf Minimierung der Risiken.

Die RFID-Technologie wird in sehr unterschiedlichen Sektoren (Medizin, Verkehr, Produktion, Konsum) angewendet. In jedem Sektor haben sowohl Chancen wie auch Risiken eine andere Bedeutung. Der Schutz der Personendaten hat z.B. in Medizin und im Konsumbereich eine grössere Bedeutung als in Produktionsabläufen. Diese sektorspezifischen Eigenschaften sollen in den Nutzen-Risiko Analysen berücksichtigt werden.

Bei Suche nach optimalen Lösungen in Nutzen-Risiko Analysen ist es zudem wichtig, dass wirtschaftliche, gesellschaftliche und politische Interessen gleichwertig vertreten sind. Zu diesem Zweck sollen Stakeholder- bzw. Dialog-Plattformen errichtet werden, in welchen Forschung, Entwicklung, Behörden, Industrie wie auch die Anwender der Technologie und die Konsumenten vertreten sind. Damit können gemeinsame Strategien erarbeitet werden, die nach Möglichkeit alle Interessen berücksichtigen. Solche Stakeholder-Plattformen werden heute bereits in der EU angewendet. Durch diesen Dialog könnte auch die heutige Situation verbessert werden, wo Technologierisiken oft nicht von denjenigen getragen werden, die den Nutzen aus der Technologie ziehen. Bei den Lösungen ist zudem eine internationale Harmonisierung anzustreben.

Empfehlung 1
Die Entwicklung der RFID-Technologie muss laufend verfolgt werden. Vorhandene gesetzliche und institutionelle Instrumente müssen periodisch auf ihre RFID-Tauglichkeit überprüft werden. Das Ziel ist es, optimale Bedingungen für die Forschung, Entwicklung und wirtschaftliche Nutzung der RFID-Technologie in der Schweiz zu schaffen. Gleichzeitig soll der Schweizer Bevölkerung eine maximal mögliche Sicherheit vor Gesundheits- und Umweltrisiken sowie der Datenschutz garantiert werden. Dabei ist eine internationale Harmonisierung anzustreben.

Empfehlung 2
Stakeholder-Plattformen sollen mit dem Ziel errichtet werden, eine gemeinsame Strategie zu erarbeiten, um die Chancen der RFID-Technologie maximal auszunutzen und gleichzeitig die Risiken zu minimieren. In diesen Plattformen sollen die Forschung & Entwicklung, die Behörden, die Industrie sowie die Anwender der Technologie und die Konsumenten vertreten sein.

8.2 Strahlung, gesundheitliche Auswirkungen und elektromagnetische Verträglichkeit

Über die von RFID-Anwendungen verursachten elektromagnetischen Felder (EMF) ist sehr wenig bekannt. EMF-Expositionen durch Lesegeräte und Tags sind mit Ausnahme der Artikelüberwachungssysteme nicht untersucht. Die Messungen an Artikelüberwachungssystemen zeigen jedoch, dass die Felder stark sein können. Es ist deshalb nötig, sowohl die im Alltag der Bevölkerung vorkommenden Expositionssituationen als auch die Expositionen an Arbeitsplätzen zu untersuchen.

Spezifische Studien zu möglichen gesundheitlichen Auswirkungen zu den von RFID erzeugten elektromagnetischen Feldern sind nicht bekannt. Die heutige Forschung ist vorwiegend auf die mobile Telekommunikation ausgerichtet. Angesichts der zunehmenden Verbreitung von RFID-Anwendungen im Alltag besteht ein Bedarf nach einer verstärkten Erforschung möglicher gesundheitlicher Auswirkungen der RFID-Technologie. Die bestehenden offenen Fragen und Unsicherheiten bezüglich Gesundheitsrisiken von elektromagnetischen Feldern sind bei RFID-Anwendungen besonders stark ausgeprägt. Sie betreffen gesundheitliche Auswirkungen von Langzeitexpositionen insbesondere durch Lesegeräte am Arbeitsplatz, von nahe am Körper getragenen oder sogar implantierten Strahlungsquellen sowie von schlecht erforschten Frequenzbereichen. Forschungsbedarf besteht im Weiteren zu anderen RFID-spezifischen Gesundheitsrisiken wie z.B. möglichen kanzerogenen Effekten bei implantierten Tags.

Die international empfohlenen Grenzwerte für elektromagnetische Felder gelten auch für RFID-Systeme und sind in den harmonisierten Produktenormen für RFID übernommen. Das Problem liegt darin, dass die Grenzwertempfehlungen durch die in den Normen beschriebenen Messmethoden teilweise stark abgeschwächt werden. In den RFID-Normen sind beispielsweise neben „worst case“-Situationen auch im Alltag durchaus vorkommende Expositionssituationen der Bevölkerung (z.B. exponierte Kinder) nicht berücksichtigt.

Mangelnde elektromagnetische Verträglichkeit (EMV) zwischen RFID-Systemen auf der einen Seite und elektronischen medizinischen Implantaten wie Herzschrittmacher oder implantierte Defibrillatoren auf der anderen Seite kann zu einer Störung der Implantate und so zu indirekten Auswirkungen der EMF auf die Gesundheit führen. Untersuchungen haben gezeigt, dass aktive medizinische Implantate wie z.B. Herzschrittmacher durch Artikelüberwachungssysteme (EAS) und evtl. durch andere RFID-Systeme gestört werden können. Wegen der weiten Verbreitung von EAS und der wachsenden Verbreitung von RFID-Systemen und Herzschrittmachern müssen gemeinsame Grenzwerte für die abgestrahlten Felder von RFID-Systemen einerseits und die Störfestigkeit von aktiven Implantaten andererseits eingeführt werden. Solange noch Herzschrittmacher und RFID-Systeme in Verkehr sind, welche diese Anforderung

nicht erfüllen, müssen die Bereiche mit Schildern gekennzeichnet werden, in denen für Implantate potenziell gefährliche Felder auftreten.

Empfehlung 3
In der Forschung zu elektromagnetischen Feldern (EMF) und deren Gesundheitsrisiken sollen die in der Realität auftretenden Expositionen durch RFID-Systeme (insbesondere durch die Lesegeräte) stärker berücksichtigt werden. Zudem sollen andere mögliche Gesundheitsrisiken von RFID wie z.B. von implantierten Tags bei Menschen untersucht werden.

Empfehlung 4
In Bezug auf die Gesundheitsrisiken der Strahlung müssen die vorhandenen, harmonisierten Produktenormen zu RFID, welche die Konformität mit den internationalen Grenzwertempfehlungen zu elektromagnetischen Feldern überprüfen sollen, so geändert werden, dass die Grenzwertempfehlungen konsequent umgesetzt werden, was heute nicht der Fall ist. In Bezug auf mögliche Störungen von elektronischen Implantaten durch RFID sollen auf internationaler Ebene im Bereich Produktesicherheit zusätzliche Massnahmen ergriffen werden. Die Schweiz soll sich auf internationaler Ebene dafür einsetzen.

8.3 Umweltrisiko: Abfallentsorgung und Recyclingsysteme

Zurzeit wird die Entsorgung der Tags als unproblematisch eingestuft. In Zukunft ist allerdings damit zu rechnen, dass durch die grosse Menge der Tags verschiedene Probleme auftauchen könnten. Eine mögliche Lösung liegt in Anwendung von leicht trennbaren Materialien und der Verwertung der wertvollen Einzelkomponenten. Damit solche Lösungen auch wirtschaftlich tragbar sind, müssen innovative Lösungen gesucht werden.

Empfehlung 5
In der RFID-Technologieentwicklung sind wirtschaftlich tragbare Lösungen zu suchen, wie die Tags konstruiert sein sollen, damit sie umweltfreundlich entsorgt oder rezykliert werden können.

8.4 Datenschutz und Datensicherheit

Im Bereich der Datensicherheit muss jede RFID-Anwendung vor der Einführung auf maximale Sicherheit bezüglich Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Daten überprüft werden. Bei personenbezogenen Daten muss die Vertraulichkeit der gespeicherten und der übertragenen Daten durch wirksame Authentifizierung der beteiligten Peripheriegeräte und durch Verschlüsselung sichergestellt werden.

Im Bereich des Datenschutzes muss bei der Bearbeitung von Personendaten zudem dem Grundrecht auf informationelle Selbstbestimmung[117] Rechnung getragen werden. Dafür müssen bei den RFID-Anwendungen folgende Grundsätze beachtet werden:

- Die betroffenen Personen müssen umfassend über den Einsatz von RFID-Systemen informiert werden.
- Kommunikationsvorgänge mit RFID-Tags, die eine Bearbeitung personenbezogener Daten auslösen, müssen für die betroffenen Personen transparent und eindeutig erkennbar sein.
- Daten auf RFID-Tags und in RFID-Lesevorgängen gewonnene auf Personen beziehbare Daten dürfen nur so lange gespeichert sein, wie es zur Erreichung des Zwecks erforderlich ist.
- Es müssen Möglichkeiten zur Deaktivierung bzw. Löschung der Daten von RFID-Tags geschaffen werden.

[117] Artikel 13 Absatz 2 BV

Die datenschutzgesetzlichen Rahmenbedingungen für Umsetzung dieser Anforderungen sind im Datenschutzgesetz[118] weitgehend gegeben:

- Die Betreiber von RFID-Systemen haben dafür zu sorgen, dass die gesetzlichen Vorschriften und Datensicherheits-Leitlinien eingehalten werden,
- Datenschutzkontrollorgane – der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte für Datenbearbeitungen durch Bundesorgane und Private, die kantonalen Datenschutzbeauftragten für Datenbearbeitungen durch öffentliche Organe der Kantone und Gemeinden – haben in ihrer Aufsichtstätigkeit eine wirksamen Kontrolle sicherzustellen.

Ein generelles, nicht nur RFID-spezifisches Problem sind die kaum vorhandenen und wenig wirksamen Sanktionierungsmöglichkeiten bei Datenschutzverletzungen. Hier besteht der Bedarf, das Sanktionierungssystem im Datenschutzbereich einer generellen Prüfung zu unterziehen.

Eine gesetzgeberische Lücke besteht dort, wo es um die Verhinderung der personenbezogenen Verwendung von ursprünglich nicht zu personenbezogenen Zwecken erhobenen Daten («Randdaten») geht. Dieses Problem betrifft neben den RFID-Anwendungen generell die IT-Systeme. Moderne Datenschutzgesetze im In- und Ausland statuieren deshalb das *Prinzip der Datenvermeidung und Datensparsamkeit*.

Empfehlung 6
Bei einer Verschärfung der Datenschutzproblematik durch grosse Mengen an Daten, welche unbemerkt gesammelt werden können, soll die Einführung des Prinzips der Datenvermeidung und Datensparsamkeit in Bezug auf Personendaten im Bundesgesetz über den Datenschutz neu überprüft werden. Gleichzeitig soll das Sanktionierungssystem im Datenschutzbereich überprüft werden. Verstösse gegen das Datenschutzgesetz sollen so geahndet werden, dass die Strafe klar grösser ist als der allenfalls aus dem Verstoss gezogene Nutzen.

8.5 Konsumentenschutz

Viele RFID-Anwendungen fallen in den Konsumbereich. Der Erfolg der Technologie hängt somit auch vom Vertrauen und dem Informationsstand der Konsumenten bezüglich der Technologie ab. Das angestrebte Verständnis für die Technologie mit ihren Möglichkeiten und Grenzen soll dazu führen, dass Konsumenten im Rahmen ihrer Selbstverantwortung Massnahmen ergreifen können, um Risiken der RFID-Technologie zu minimieren. Transparenz im Umgang mit RFID kann zudem dazu beitragen, dass die Technologie breiter akzeptiert wird.

Damit die Konsumenten ihre Rechte wahrnehmen können, müssen bei RFID-Anwendungen im Konsumbereich zusätzlich folgende Anforderungen erfüllt werden:

- Deklarationspflicht: RFID-Tags müssen klar als solche gekennzeichnet sein.
- Deaktivierung: Konsumenten müssen in der Lage sein, mit einem Produkt erworbene Tags zu zerstören, zu entfernen oder auszuschalten. Diese Deaktivierung des Tags darf nicht eine Einschränkung oder gar Beendigung der gesetzlichen Verpflichtungen der Händler oder der Hersteller des Produkts zur Folge haben

Anforderungen des Datenschutzes an RFID im Konsumbereich sind in den Datenschutzregelungen bereits enthalten. Z.B. dürfen ohne ausdrückliche Zustimmung der Konsumenten aus den gesammelten Daten keine Profile von Konsumenten erstellt werden.

[118] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG) SR 235.1

Empfehlung 7

Konsumenten müssen über Eigenschaften, Nutzen und Risiken von RFID-Systemen im Konsumbereich verständlich informiert werden. Ausserdem müssen RFID-Tags im Konsumbereich klar als solche gekennzeichnet sein. Verbraucher müssen die Möglichkeit haben, mit einem Produkt erworbene Tags ohne vermeidbare negative Konsequenzen zu zerstören, zu entfernen oder auszuschalten.

9. Quellen

9.1 Literatur

BAG: Bericht „Nichtionisierende Strahlung und Gesundheitsschutz in der Schweiz“ , wurde als Antwort zum Postulat Sommaruga (00.3565) erarbeitet www.bag.admin.ch/nis-bericht

BAG: Bericht „Risikopotential von drahtlosen Netzwerken“ wurde als Antwort auf Postulat Allemann (04.3594) erstellt. www.bag.admin.ch/wlan-bericht

ICNIRP. Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields up to 300 GHz. Health Phys. 75: 494-521.

ICNIRP. Possible health risk to the general public from the use of security and similar devices 2002. ISBN 3-934994-01-6. http://www.icnirp.de/documents/ExSummary.pdf

Guidelines for Securing Radio Frequency Identification (RFID) Systems', National Institute of Standards and Technology, April 2007

National Institute of Standards and Technology: Guidelines for Securing Radio Frequency Identification Systems, Special Publication 800-98

Bericht: RFID Technologies: Emerging Issues, Challenges and Policy Options, Eur 22770 EN -2007

Bericht “European Policy Outlook RFID” www.bmwi.de

RFID Privacy: an Overview of Problems and Proposed Solutions', Garfinkel, Juels, Pappu, IEEE Security & Privacy, May/June 2005

Risiken und Chancen des Einsatzes von RFID-Systemen', Bundesamt für Sicherheit in der Informationstechnik, 2005

EDÖB «Datenschutzrechtliche Probleme bei dem Einsatz der RFID-Technologie»: http://www.edoeb.admin.ch/dokumentation/00445/00509/00510/00816/index.html?lang=de.

Studie „RFID Masseneinsatzes auf Entsorgungs- und Recyclingsysteme“; Universität Dortmund, gefordert von Bundesministerium für Bildung und Forschung, Förderkennzeichen 16SV2280 (2007)

Ph. Kräuchi et. Al. EMPA: „Impacts of pervasive Computing: Are RFID tags a Threat to Waste Management?” IEEE Technology & Society Magazine, Special Issue “Sustainable Pervasive Computing”, 2005, 24(1), S. 45-53,

P. Wäger et al., EMPA: Smart labels in municipal solid waste — a case for the Precautionary Principle? Environmental Impact Assessment Review 25/2005, S. 567-586.

K. Finkenzeller: RFID Handbuch. 2006.

Risikodialog: Broschüre "Kompass zu einem verantwortungsvollen Einsatz von Pervasive Computing http://www.risiko-dialog.ch/Themen/Kommunikationstechnologien/263

Interpellation (05.3067) Hollenstein: Bedroht die Anwendung von RFID den Datenschutz?

9.2 Relevante rechtliche Vorschriften zu RFID in der Schweiz

Datenschutzgesetz (DSG SR 235.1)

Verordnung über Frequenzmanagement und Funkkonzessionen FKV, SR 784.102.1

Verordnung über den Schutz vor nichtionisierender Strahlung (NISV). 2000. SR 814.710

Bundesgesetz über die Unfallversicherung (UVG SR 832.20)

Arbeitsgesetz (ArG SR 822.11)

Verordnung über Niederspannungserzeugnisse (NEV SR 734.26)

Verordnung über Fernmeldeanlagen (FAV SR 784.101.2)

Verordnung über die Rückgabe, die Rücknahme und die Entsorgung elektrischer und elektronischer Geräte (VREG SR 814.620) vom 14. Januar 1998

9.3 EU Dokumente

Charta der Grundrechte der Europäischen Union (ABl. C 303 vom 14.12.2007, 1 ff.)

Richtlinie (2004/40/EG) über Mindestvorschriften zum Schutz von Sicherheit und Gesundheit der Arbeitnehmer vor der Gefährdung durch physikalische Einwirkungen.

Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABI L 28 vom 23.11.1995

Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

Richtlinie 2002/96/EG über Elektro- und Elektronik-Altgeräte (WEEE)

Richtlinie 2002/95/EG zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten (RoHS)

Empfehlung des europäischen Rates 1999/519/EG bezüglich der Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern

Entscheidung 2006/804/EG der Kommission vom 23. November 2006 zur Harmonisierung der Frequenzbänder für Geräte zur Funkfrequenzkennzeichnung (RFID-Geräte) im Ultrahochfrequenzband (UHF)

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ KOM(2007) 96

Mitteilung der EU-Kommission „Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung KOM(2006) 251

9.4 Internationale Produktenormen

CENELEC: Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die im Frequenzbereich von 0 Hz bis 10 GHz betrieben und in der elektronischen Artikelüberwachung (en: EAS), Hochfrequenz-Identifizierung (en: RFID) und ähnlichen Anwendungen verwendet werden; EN SN 50364:2001

CENELEC: Ermittlung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die in der elektronischen Artikelüberwachung (en: EAS), Hochfrequenz-Identifizierung (en: RFID) und ähnlichen Anwendungen verwendet werden; EN SN 50357:2001

IEC: Evaluation of human exposure to electromagnetic fields from Short Range Devices (SRDs) in various applications over the frequency range 0-300 GHz. Part 1: Fields produced by devices used for Electronic Article Surveillance, Radio Frequency Identification and similar systems. IEC 62369-1.

10. Anhang

10.1 Abkürzungen und Begriffe

BAG	Bundesamt für Gesundheit
BAFU	Bundesamt für Umwelt
BAKOM	Bundesamt für Kommunikation
Bandbreite	Zwei Bedeutungen: Kapazität eines Übertragungskanals Frequenzbereich eines Übertragungskanals
Blocker Tag	Blocker Tags senden Störsignale aus, um die Kommunikation zwischen einem RFID-Tag und dem Lesegerät zu blockieren.
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique, Normierungsgremium
CEPT	conférence européenne des administrations des postes et des télécommunications
Chip	Integrierter Schaltkreis. Auf dem Chip sind die Daten des RFID-Tags gespeichert.
Code of conduct	Verhaltenskodex; Selbstverpflichtung, bestimmten Verhaltensmuster zu folgen bzw. diese zu unterlassen
Datenrate	Datenmenge, die pro Zeiteinheit transportiert wird
DG	directorate general: Generaldirektion in der europäischen Kommission
DNS	domain name system: Dienst im Internet, welcher Internetadressen in die zugehörige IP-Adresse umsetzt
DoS-Angriff	Denial of Service, Angriff mit dem Ziel, einen Computer oder ein ganzes Netzwerk unbenutzbar zu machen
Dosis	ist die physikalische Grösse, welche diejenigen Eigenschaften der Strahlung, welche für bestimmte biologische Veränderungen relevant sind, am besten beschreibt. Dementsprechend sind für unterschiedliche biologische und gesundheitliche Auswirkungen unterschiedliche Dosisgrössen relevant.
DSG	Datenschutzgesetz
duty cycle	Tastgrad: Verhältnis der Impulsdauer zur Periodendauer
EAN	european article number: europäischer Handelsstrichcode
EAS	electronic article surveillance: Artikelüberwachungssystem, Diebstahlsicherung
ECC	electronic communications committee, Teilbereich von CEPT
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
E-Feld	Elektrisches Feld
EIRP	equivalent isotropically radiated power: Sendeleistung, mit welcher ein Isotropstrahler versorgt werden müsste, um in der Ferne dieselbe Feldstärke zu erzeugen wie eine Richtantenne in ihrer Hauptsenderichtung.
EMF	Elektromagnetisches Feld
Emission	ist die Strahlung, die von einer Strahlungsquelle ausgesendet wird.
EMPA	Eidgenössische Materialprüfungs- und Forschungsanstalt, Forschungsinstitution im ETH-Bereich
EMV	elektromagnetische Verträglichkeit
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EPC	electronic product code: möglicher Nachfolger des Handelsstrichcodes basiernd auf RFID-Technologie
ERP	Effective Radiated Power : Sendeleistung, mit welcher eine Dipolantenne versorgt werden müsste, um in der Ferne dieselbe Feldstärke zu erzeugen wie eine Richtantenne in ihrer Hauptsenderichtung.
Exposition	ist die Strahlung (Immission), der ein Objekt (Mensch, Tier, Pflanze, Boden oder Sachgut) während einer bestimmten Dauer (Expositionszeit) ausgesetzt ist. Man unterscheidet zwischen Ganzkörperexposition und Teilkörperexposition.
FAV	Verordnung über Fernmeldeanlagen
FDA	food and drug administration: Behörde in den USA, welche für die Heilmittelzulassung

	und den Verbraucherschutz zuständig ist
FDV	Verordnung über Fernmeldedienste
Fernfeld	Vgl. Nahfeld
FKV	Verordnung über Frequenzmanagement und Funkkonzessionen
Frequenz	Anzahl von Schwingungen pro Sekunde
Herzschrittmacher	implantierter Pulsgenerator zur Behandlung bradykarder Herzrhythmusstörungen
Hz	Hertz: Einheit für die Frequenz, 1/s
ICD	implantet cardioverter defibrillator: implantierter Defibrillator zur Behandlung tachykarder Herzrhythmusstörungen
ICNIRP	International Commission of Non-Ionizing Radiation Protection
IEC	International Electrotechnical Commission: Normierungsgremium
IEEE	Institute of Electrical and Electronics Engineers
Immission	ist die Strahlung an einem bestimmten Ort. Die Immission ist meistens niedriger als die Emission, da die Strahlung zwischen der Strahlungsquelle und dem Ort der Immission abgeschwächt werden kann.
Immunität	Fähigkeit eines Gerätes, unter Einwirkung elektromagnetischer Störsignale einwandfrei zu funktionieren
IP-Adresse	Internetprotokolladresse: eindeutige Nummer für jeden am Internet teilnehmenden Computer
ISM-Band	Industrial Scientific Medical-Band, frei zugänglicher Frequenzbereich
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization, Internationale Organisation für Normung
IT	Informationstechnologie
IT'IS	Foundation for Research on Information Technologies in Society, ETH Zürich
kHz	Kilohertz: Tausend Hertz
LBT	listen before talk: das Gerät hört zuerst das Übertragungsmedium ab und sendet erst, wenn dieses frei ist.
Maut	Wegzoll
MHz	Megahertz: Million Hertz
Nahfeld, Fernfeld	Im hochfrequenten Bereich unterscheidet man zwischen Nah- und Fernfeld, je nachdem, ob der Abstand zur Quelle kleiner oder grösser als die Wellenlänge der Strahlung ist. Im Fernfeld nimmt die elektrische Feldstärke umgekehrt proportional mit der Entfernung ab (1/r), die Leistungsdichte umgekehrt quadratisch ($1/r^2$)
NISV	Verordnung über den Schutz vor nichtionisierender Strahlung
ONS	object naming service: mit dem EPC verbundener Service, der mit Hilfe von Einträgen im DNS Informationen zu Produkten im Internet zur Verfügung stellt
opt-in / opt-out	aus dem Email-Marketing bekanntes Verfahren, bei dem man sich explizit in eine Abonnementsliste eintragen muss (opt-in) oder sich austragen muss (opt-out). Dies lässt sich auch auf Anwendungen im RFID-Bereich übertragen.
PDA	personal digital assistent: kleiner mobiler Computer, elektronische Agenda
PvC	pervasive computing: Durchdringung des Alltags durch intelligente Gegenstände (mit Sensoren und Computer) (PVC: Polyvinylchlorid)
PVC	Polyvinylchlorid: harter, weisser Kunststoff
RFID	Radio Frequency IDentification
RIR	radio interface regulation: Schnittstellenanforderung für Funkanwendungen
SAR	Spezifische Absorptionsrate, die Einheit ist W/kg. Der SAR-Wert ist die physikalische Grösse und das Mass für die Absorption von hochfrequenter Strahlung in biologischem Gewebe. Sie ist sowohl von der Frequenz als auch von der Grösse des absorbierenden Körpers abhängig.
Server	zentraler Rechner in einem Netzwerk, der den Arbeitsstationen Ressourcen (z.B. Internetzugang) und Daten zur Verfügung stellt
Smart Label	papierdünner RFID-Tag: Die Antenne wird durch Siebdruck oder Ätztechnik auf eine Plastikfolie aufgebracht, welche mit einer Papierschicht laminiert und mit Kleber beschichtet wird. Diese Klebeetiketten können bedruckt werden (z.B. zusätzlich mit ei-

	nem Strichcode) und dann auf Gepäckstücke, Pakete, Waren etc. aufgeklebt werden
SNV	Schweizerische Normen-Vereinigung
SRD	short range device: Kurzstreckenfunkgerät
supply chain management	Versorgungskettenmanagement
Tag	Teil im RFID-System, das an dem zu identifizierenden Objekt angebracht wird. Der Tag besteht aus einem Chip mit den gespeicherten Daten und einer Antenne.
Telemetriesystem	Automatische Übertragung von Messwerten oder –daten, über grössere Entfernungen, Fernüberwachung
UWB	ultra wide band: Funktechnologie, welche mit grosser Funkbandbreite und geringer Sendeleistung arbeitet.
WLAN	wireless local area network: drahtloses Netzwerk zur Verbindung von Computern untereinander oder mit dem Internet

10.2 Postulat Allemann (05 3053) Handlungsbedarf im Zusammenhang mit RFID-Technologie

Wortlaut des Postulates vom 9. März 2005

Der Bundesrat wird beauftragt, zu prüfen, welcher Handlungsbedarf sich aus dem absehbaren flächendeckenden Einsatz der RFID-Technologie (Radio-Frequency-Identification) ergibt. Insbesondere sollen das Augenmerk auf folgende Punkte gerichtet werden:
datenschutzrechtliche Probleme, die von der geltenden Datenschutzgesetzgebung noch nicht abgedeckt werden

- gesundheitliche Risiken (insb. Risikopotenzial der Strahlung)
- Umweltrisiko und Abfallentsorgung (insb. Abfallrecycling)
- Konsumentenschutz / -information: Deklarationspflicht der eingesetzten RFID-Tags bei Konsumartikeln

Begründung

Die RFID-Technologie, mittels der Daten von sehr kleinen Tags drahtlos per Funk übertragen werden können, ist eine neuartige Technologie, welche viele Anwendungsbereiche beeinflussen wird. Mit ihrer Hilfe können Gegenstände, aber auch Menschen exakt und eindeutig identifiziert und verfolgt werden. Damit eröffnet sich etwa in der Produktion und Logistik, aber auch im Konsumbereich ein weites Anwendungsfeld.
Die dabei verwendeten RFID-Tags, auch Funketiketten genannt, sind kleine elektronische Bauteile, die mindestens eine weltweit eindeutige Identifikationsnummer enthalten, je nach Bauform aber auch weitere Informationen speichern können. Diese Daten werden drahtlos, je nach Bauform über mehrere dutzend Meter, per Funk ausgelesen. Damit wird es möglich, die Tag-Träger berührungslos und unbemerkt ohne Sichtkontakt eindeutig zu identifizieren Die Tags sind ca. einen halben Quadtratmillimeter klein und können so auf Gegenstände aufgeklebt, in Kleider eingewoben oder bei Tieren und Menschen implantiert werden.
Mögliche Anwendungen, die alle mindestens zu Testzwecken bereits heute funktionieren, gibt es viele: Statt einem Barcode wird im Warenhaus an der Kasse der RFID-Tag eingelesen, im Reisepass sind die biometrischen Daten von einem RFID-Tag abrufbar oder medizinische Daten eines Menschen werden im unter der Haut implantierten Tag gespeichert.
Die Einführung der RFID-Technologie ist nicht aufzuhalten. Ein weltweiter und praktisch flächendeckender Einsatz zeichnet sich bereits heute ab. Deshalb müssen in folgenden Bereichen Abklärungen vorgenommen und allenfalls rechtzeitig geeignete Massnahmen ergriffen werden:
Datenschutz
Da die RFID-Tags fast unsichtbar sind und darauf gespeicherte Informationen unbemerkt abgefragt werden können, besteht keine Kontrolle darüber, wo und wann welche Daten abgerufen werden. Ein in

einem Kleidungsstück eingenähter Tag etwa, der primär zur Verrechnung an der Kasse dient, kann auch später noch verwendet werden und beispielsweise darüber Auskunft geben, wann der Kunde im entsprechenden Kleidungsstück den Laden erneut betritt, was er dann kauft etc. Zusammen mit den bereits heute verbreiteten Kundenkarten, die ebenfalls mit RFID-Tags ausgerüstet werden können, wären die gewonnenen Daten problemlos personalisierbar.

Gesundheitsrisiken

RFID-Tags strahlen verhältnismässig schwach. Da die Strahlenbelastung aber überproportional zunimmt, je näher die Strahlenquelle ist, und die RFID-Tags unmittelbar auf oder sogar unter der Haut platziert sein können, ist ein erhebliches Gesundheitsrisiko denkbar. Im Hinblick auf eine flächendeckende Verbreitung der RFID-Technologie müssen deshalb zum heutigen Zeitpunkt die Gesundheitsrisiken seriös abgeklärt und allenfalls Regelungen zum Schutze der Gesundheit getroffen werden.

Umweltrisiko / Abfallentsorgung

RFID-Tags sind meist unlösbar mit einem Gegenstand verbunden und ausserdem fast unsichtbar. Bei der Entsorgung ist eine Separation kaum möglich. Viele RFID-Tags und das in ihnen enthaltene Kupfer (je nach Bauform auch die Batterien) dürften damit im Hausmüll landen oder beim Recycling durch Verunreinigung Probleme verursachen.

Deklarationspflicht

Aus oben genannten Gründen ist es gerade für den Konsumenten und die Konsumentin wichtig zu wissen, wann die RFID-Technologie eingesetzt wird. Da aber die RFID-Tags fast oder gänzlich unsichtbar sind, kann dies nur durch eine Deklarationspflicht im Konsumbereich gewährleistet werden. Es ist deshalb abzuklären, welche Vorschriften zum Schutze der Konsumentinnen und Konsumenten getroffen werden müssen.