

Fiktives Gutachten

DATENSCHUTZ UND RFID-TECHNIK

Veranstaltung: Information Rules 1

Betreut durch: Prof. Dr. Lutterbeck

Technische Universität Berlin

Februar 2004

GUTACHTEN

DATENSCHUTZ UND RFID-TECHNIK

INHALT

Empfehlungen	2
Inhaltsverzeichnis	3
RFID-Technik	4
Anwendungsmöglichkeiten	14
Datenschutz-Probleme	19
Literaturverzeichnis	26

Erstellt Im Auftrag des Ministeriums für Verbraucherschutz

Jan Suhr
Malwina Prokopczyk
Frank Reimann

Abstract

Zur **RFID-Technik** gehören kleinste Chips, die in Waren eingebaut werden, Lesegeräte die über Funk auf diese zugreifen und eine weltweit eindeutige Nummer auslesen, sowie Datenbanken in denen zu den jeweiligen Produkten weitere Informationen gespeichert sind.

In absehbarer Zeit werden nahezu **alle Konsumgüter mit RFID-Chips ausgestattet werden**, einschließlich der Produkte, die der Verbraucher in der Öffentlichkeit bei sich trägt, wie Kleidungsstücke, Mobiltelefon etc.

Die RFID-Technik **ermöglicht etwaigen Missbrauch**, da der Zugriff auf die Chips der Konsumgüter nicht wirksam beschränkt ist, und so von jedem Interessierten mit einem Lesegerät unbemerkt ausgelesen werden kann.

Wir **empfehlen** daher, in Produkten integrierte RFID's beim Verkauf an den Verbraucher, **funktionsunfähig** zu machen, alle übrigen Chips mit **sicheren Authentifizierungsmechanismen** auszustatten und **Transparenz** bei der Verwendung der RFID-Technik herzustellen.

0. EMPFEHLUNGEN

Die zukünftige Verwendung der RFID-Technik wird dazu führen, dass die Verbraucher sowohl in der Öffentlichkeit als auch im Privaten, Gegenstände am Körper tragen, die mit funktionsfähigen RFID-Tags ausgestattet sind. Auf diese Tags kann ohne Einschränkung von jedem RFID-Lesegerät zugegriffen werden, das sich in der Reichweite des RFID-Chips befindet. Die ausgelesenen Informationen lassen erkennen welche Gegenstände die Person am Körper trägt und können zur automatischen Erstellung von Verhaltensprofilen verwendet werden. (Gfaller 2003) Die für RFID nötigen Datenbanken eröffnen die Möglichkeit, diese Profile über viele Jahre zu führen und übers Internet miteinander zu verknüpfen. (Heise 2004 A) Der Verbraucher wird dadurch sein Recht auf informationelle Selbstbestimmung (BVG 1983) verlieren, welches ihm auf Basis unseres Grundgesetzes zu steht. Die Folge davon könnte unter anderem Preisdiskriminierung zum Nachteil der Verbraucher sein. (Computer Zeitung 2004 A) Ebenfalls ist eine Diskriminierung von kranken Menschen durch Versicherungen, Banken oder bei der Jobsuche möglich, da Informationen über den Gesundheitszustand des jeweiligen Verbrauchers leicht zugänglich sein werden. (BigBrotherAwards 2003) Um diese Benachteiligungen zu vermeiden muss die Möglichkeit der informationellen Selbstbestimmung gewährleistet sein. Wir empfehlen zu dessen Sicherstellung folgende drei Maßnahmen:

Deaktivierung: Alle Tags, die für Logistikzwecke *in* oder *an* Produkten bzw. deren Verpackungen befestigt wurden, müssen beim Verkauf an den Endverbraucher unumkehrbar funktionsunfähig gemacht oder entfernt werden.

Dadurch wird vermieden, dass die Verbraucher mit nutzlosen RFID-Tags am Körper, persönliche Informationen über sich unbemerkt preisgeben. Es bleibt weiterhin das Problem der RFID-Chips bestehen, die z.B. auf Kredit- oder Büchereikarten integriert sind.

Sicherheit: Der Zugriff auf von Verbrauchern verwendete RFID-Tags darf nur von den für den Verwendungszweck erforderlichen Institutionen erfolgen *können*.

Dritte können nicht auf die verbleibenden RFID's zugreifen, da dafür eine Authentifizierung erforderlich ist. Es ist aber weiterhin für zugriffsberechtigte Institutionen möglich, Verhaltensprofile zu erstellen oder anderen Missbrauch zu betreiben.

Transparenz: RFID-Chips und installierte Lesegeräte müssen gekennzeichnet werden. Werden Daten erhoben muss der Betroffene über deren genaue Art und Umfang sowie den Zweck der Datenerhebung informiert werden.

Der letzte Aspekt kann die Verwendung versteckter RFID-Technik und geheimer Datenbanken verhindern.

INHALTSVERZEICHNIS

0. EMPFEHLUNGEN	2
INHALTSVERZEICHNIS	3
1. RFID-TECHNIK.....	4
1.1 Aufbau, Eigenschaften und Funktionsweise.....	4
1.2 Verwendete Frequenzen.....	7
1.3 Standardisierung und Vernetzung.....	8
1.4 Verschlüsselung der Informationen.....	11
1.5 Geschichte der technischen Entwicklung.....	13
2. ANWENDUNGSMÖGLICHKEITEN.....	14
3. DATENSCHUTZ-PROBLEME.....	19
3.1 Betreffen RFID's persönliche Informationen?.....	19
3.2 Kann der Verbraucher RFID's meiden?.....	20
3.3 Kann der Verbraucher den Zugriff auf seine RFID's beschränken?.....	21
3.4 Welche nachteiligen Folgen kann RFID für Verbraucher haben?.....	22
3.5 Wird der Verbraucher durch geltendes Recht geschützt?.....	24
3.6 Ist mit einer kundenfreundlichen Regelung der Wirtschaft zu rechnen?.....	24
3.7 Wie beurteilen Verbraucher die Datenschutzprobleme?.....	25
3.8 Welche zukünftigen Entwicklungen wird es geben?.....	25
4. LITERATURVERZEICHNIS.....	26

1. RFID-TECHNIK

Die Bezeichnung **RFID (Radio Frequency Identification)** steht für Radiofrequenztechnik zu Identifikationszwecken oder kurz Identifizierung per Funk.

Da meist RFID-Systeme in Form und Größe eines Etikett oder einer Plakette (engl. Tag) gemeint sind, spricht man von einem RFID-Tag oder auch Smart Tag.

1.1 AUFBAU, EIGENSCHAFTEN UND FUNKTIONSWEISE

„Der **Aufbau** eines RFID-Tags sieht prinzipiell eine Antenne, einen analogen Schaltkreis zum Empfangen und Senden (Transponder), sowie einen digitalen Schaltkreis vor.“

Der digitale Schaltkreis ist bei komplexeren Modellen ein Rechner mit dazugehörigem Speicher, welcher Programme und Daten speichern kann. (*Wikipedia 2004 C*)

Genau wie beim Strichcode (Barcode) ermöglicht auch RFID eine berührungslose Datenübertragung. Dadurch können Informationen über unterschiedliche Entfernungen hinweg ausgetauscht werden. Der Unterschied besteht darin, dass keine Hell-Dunkel-Felder abgetastet werden, sondern elektromagnetische Wechselfelder als Übertragungsmedium genutzt werden. (Füßler 2002)

Begriff **Transponder**

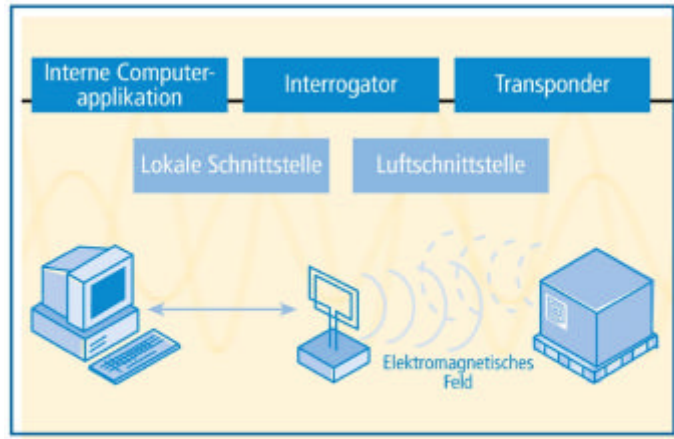
„Ein Transponder ist ein drahtloses Kommunikations-, Anzeige- oder Kontrollgerät, das eingehende Signale aufnimmt und automatisch darauf antwortet. Der Begriff Transponder ist zusammengesetzt aus den Begriffen **TRANSmitter** und **resPONDER**. Transponder können passiv oder aktiv sein.

Ein **passiver Transponder** erlaubt einem Computer oder Roboter, ein Objekt zu identifizieren. Magnetstreifen sind Beispiele hierfür. Ein aktiver Sensor (in Verbindung mit dem Computer) liest und dekodiert die Daten, die der passive Transponder enthält.

Einfache **aktive Transponder** werden zum Beispiel bei der Lokalisierung, Identifizierung und Navigation von Flugzeugen verwendet: Der im Flugzeug eingebaute Transponder empfängt ein kodiertes Signal einer Überwachungs- und Kontrollstelle und beantwortet dieses Signal auf einer vorgegebenen Frequenz mit den erforderlichen Daten, ebenfalls in kodierter Form (z.B. Flughöhe, Geschwindigkeit). Dieses Antwortsignal wird von der Überwachungsstelle empfangen und z.B. auf einem Radarschirm sichtbar gemacht.“ (*Wikipedia 2004 D*)

„Ein RFID-Tag kann in Form und Größe variieren, je nach Modell und Ausführung von wenigen Millimetern bis einigen Zentimetern. Das Aussehen kann von rund und massiv, bis flach und ...

flexibel beliebig angepasst werden.“ (*Wikipedia 2004 D*) RFID-Tags (Antenne, Chip und ggf. Batterie) können, je nach Anwendungszweck, in verschiedenen Bauformen realisiert oder auf verschiedene Trägermaterialien aufgebracht, bzw. mit verschiedenen Materialien umhüllt werden. Damit lassen sich die Tags **an verschiedenste Umgebungen und Anforderungen anpassen** und sind **extrem robust und langlebig**. RFID-Tags sind damit anderen automatisierten Identifikationssystemen **in extremen Umgebungen** durch Resistenz gegen Schmutz, aggressive chemische Substanzen, mechanische Einwirkung

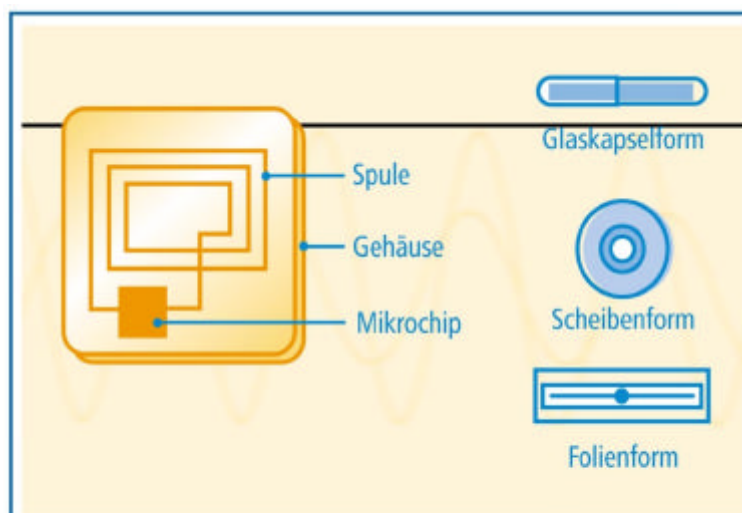


Komponenten eines RFID-Systems

Coorganisation 3/2002 · EAN-UCC – The Global Language of Business

und starke Temperaturschwankungen **überlegen**. Zusätzlich bietet die Informationsübertragung per Funk die Möglichkeit die Daten vieler Transponder automatisch auf einmal zu erfassen. (sog. **Pulkerfassung**) Das Übertragungsprotokoll vermeidet dabei Kollisionen beim Auslesen zwischen den einzelnen Tags. „Jedes automatisierte Identifikationssystem [AutoID-System (Anm. d. Autors)] basiert auf dem Einsatz eines Codiersystems. Dieses besteht aus einer Schreibstation (dem Codierer), dem Datenträger sowie einer Lesestation (Decodierer). Bei einem Radiofrequenz-System zu Identifikationszwecken (RFID-System) erfolgen Codierung und Decodierung über die **Schreib-/Lesestation (Interrogator)**, während

Transponder als programmierbare Datenträger eingesetzt werden.“ (*Füßler 2002*)



Transponderaufbau (induktive Kopplung)

Coorganisation 3/2002 · EAN-UCC – The Global Language of Business

(u.a. Arbeitstakt), sowie ggf. Energie. Diese Versorgung erfolgt berührungslos über elektromagnetische Wechselfelder.

Der **Interrogator** stellt also die **Abfrageeinrichtung** dar. Ein geeignet konstruiertes RFID-Tag in Verbindung mit einer passenden Abfrageeinrichtung kann auch dazu genutzt werden die Daten auf dem RFID-Chip zu verändern. Weiterhin dient diese Abfrageeinrichtung zur Übertragung von Daten, Kommandos

Es existieren auch RFID-Tags, die Eigenschaften von passiven und aktiven Transpondern besitzen. Eine in das Tag eingebaute Energiequelle sorgt nur für den Stromverbrauch des Transponders. Die Batterie (Akkumulator) kann jedoch durch ein Lesegerät immer wieder aufgetankt werden, so dass das Tag seine Informationen abgeben kann. (*Ostler 2003*)

Ähnlich wie bei den Transponder-Arten unterscheidet man auch bei den RFID-Tags zwischen aktiven und passiven Ausführungen/Bauformen.

„Aktive RFID-Tags

Aktive RFID-Tags sind **batteriebetrieben** und können typischerweise sowohl **gelesen, als auch beschrieben** werden. Aktive Tags befinden sich normalerweise im Ruhezustand, d.h. sie senden keine Informationen aus. Nur wenn ein spezielles Aktivierungssignal empfangen wird, aktiviert sich der Sender. Der interne Speicher kann, je nach Modell, bis zu 1 Million Bytes [Zeichen (Anm. d. Autors)] aufnehmen. Aktive RFID-Tags sind im Vergleich zu passiven Tags meist größer, besitzen eine **höhere Sendereichweite**, haben eine geringere Lebensdauer und sind **signifikant teurer**.

Passive RFID-Tags

Passive Tags beziehen ihre **Energie** zur Übertragung der Informationen **aus den empfangenen Funkwellen**. Die gespeicherten **Daten können nur gelesen werden**, außerdem ist die Menge der speicherbaren Daten wesentlich geringer als bei aktiven Tags. Dieser Speicher wird üblicherweise benutzt, um eine eindeutige Identifikationsnummer zu hinterlegen. Passive RFID-Tags sind im Vergleich zu aktiven Tags kleiner und leichter, haben eine **geringe Reichweite**, haben eine **nahezu unbegrenzte Lebensdauer**, brauchen eine stärkere Leseinheit, sind dafür aber **günstiger** in der Produktion.“

(*Wikipedia 2004 C*)

Diese Mischformen werden als semi-aktive oder semi-passive RFID-Systeme bezeichnet.

Die Entwicklung der RFID-Tags ist einer **ständigen Weiterentwicklung** unterworfen. Seit der Verwendung dieser Technik im zivilen Bereich übertrafen sich die Hersteller gegenseitig bei den Neuentwicklungen. So wurden die RFID-Chips, auch unter Verwendung neuer Herstellungstechniken und kleinerer Strukturgrößen, immer **kleiner, verbrauchten weniger Strom und erhöhten somit Batterie-Lebensdauer** (aktive RFID-Tags), **Reichweite** sowie **Speicherkapazität**.

Momentan kann ein aktives RFID-Tag mit einer Batterie ca. 6-10 Jahre in Funktion bleiben. Die Reichweite der aktiven Tags beträgt aktuell bis zu 30m (Schätzungen halten bis zu 100m für realisierbar (*Glasmacher 2003*)) und die der passiven Tags bis maximal 2,5m. Mit aufwendig konstruierten Lesegeräten können auch noch größere Reichweiten erzielt werden. Es ist zu erwarten, dass die maximale Reichweite in Zukunft noch weiter vergrößert werden kann. **Die Reichweite ist stark abhängig von der Komplexität des verwendeten RFID-Chips.** Einfach aufgebaute RFID-Chips haben die höchste Reichweite.

Durch die Verkleinerung der Chips und neue Herstellungstechniken ist es auch möglich geworden die Herstellungskosten zu senken. Die zurzeit kleinsten RFID-Chips sind **so groß wie ein halbes Sandkorn**. Dadurch ergeben sich völlig neue Anwendungsfelder. (siehe Kapitel Anwendungen)

1.2 VERWENDETE FREQUENZEN

Passive RFID-Tags verwenden eher die niedrigeren Frequenzbereiche (z.B. 134,2kHz, 13,56 Mhz) mit hoher Durchdringungsfähigkeit (bis auf Metall), wogegen jedoch aktive Tags meist die hohen Frequenzbereiche (z.B. 868MHz, 915MHz, sowie 2,45GHz) mit einer Durchdringungsfähigkeit, die stark vom Material abhängt, benutzen. Die Frequenzen 868MHz (**Europäische Union**) und 915MHz (**USA**) kommen auch in (semi-)passiven RFID-Bauformen vor. (*Glasmacher 2003*) (*Trautner 2002*)

Metall, Wasser sowie andere Geräte, die im gleichen Frequenzband funken (Störsender) sind geeignet um die **RFID-Übertragung zu beeinträchtigen oder zu verhindern**. „Für den Einsatz werden drei Frequenzbänder vorgeschlagen

Niedrige Frequenzen (30-500 KHz), diese Systeme besitzen eine geringe Reichweite, lange Übertragungszeiten, sind aber günstig in der Anschaffung“.

„Mittlere Frequenzen (10-15 MHz), kurze bis mittlere Reichweite, mittlere Übertragungsgeschwindigkeit, mittlere bis günstige Preisklasse.

Hohe Frequenzen (850-950 MHz, 2,4 – 2,5 GHz), hohe Reichweite (max. 30 Meter), schnelle Lesegeschwindigkeit, Preise steigen aber rapide bei höherer Leistung der Systeme.“ (*Wikipedia 2004 C*)

„RFID-Systeme, die ab einer Entfernung von zwei Metern Objekte identifizieren, werden als **RFID-Reichweitensysteme** bezeichnet.“ (z.B. Identifikation von Fahrzeugen an einer **Mautbrücke**) „Große Reichweiten werden mit hochfrequenten Systemen erzielt (433MHz, 868MHz, 2,45 oder 5,8GHz; 5,8GHz ist für Mautsysteme reserviert). Auf

grund der großen Reichweite könnte die Identifikation fremder Objekte jedoch zu Fehlle-
sungen führen. Daher verfügen viele RFID-Reichweitensysteme über einen gerichteten
Lesekegel. [...] Ein weiterer Vorteil von RFID-Reichweitensystemen ist, dass sie hervor-
ragend auf Metall montiert werden können. **Aufgrund der hohen Frequenz kommt es bei
diesen Systemen nicht zu Fehlle-**sungen oder Frequenzverschiebungen. Ganz im Gegen-
teil: Ein metallischer Untergrund fördert die Reflexionseigenschaften des Transponders
dieser Systeme.

Die **Lebensdauer der Reichweitensysteme** ist abhängig davon, ob es sich um ein aktives
oder ein semi-passives System handelt. Bei **aktiven Systemen** ist der Transponder als
Sender konzipiert der Energie in Abhängigkeit zur Nutzungshäufigkeit verbraucht: Je häu-
figer ein Objekt erkannt werden muss, desto schneller wird die im Transponder eingebaute
Batterie entladen.

Bei den **semi-passiven Systemen** dagegen werden die Objekte aufgrund der Reflexionsei-
genschaften der Transponder erkannt. Denn diese Systeme senden das vom Lese-
/Schreibgerät empfangene Signal nicht aktiv zurück, sondern reflektieren es lediglich. Da-
her entspricht der Energieverbrauch dieser Transponder in etwa dem Wert der Eigentla-
dung der verwendeten Batterie, wodurch die Lebensdauer von typisch 6 oder 10 Jahren
realisiert werden.“ (*I.D. Systems AG 2003*)

1.3 STANDARDISIERUNG UND VERNETZUNG

Der **Standardisierungsprozess** der RFID-Technik befindet sich „in vollem Gange“ und
ist noch lange **nicht abgeschlossen**. Einige Teilbereiche sind schon nach **ISO-Normen**
(International Organization for Standardization) (*Finkenzeller 2003*) und **EAN-UCC-**
Normen standardisiert.

Wie der Titel des Unterkapitels schon erahnen lässt, sind Standards überall da erforder-
lich, wo Systeme begrenzter Reichweite verschiedener Hersteller und Anwender zusam-
mengeschaltet/vernetzt werden sollen, um somit **Informationen zwischen den einzelnen
Anwendern austauschen** zu können.

Da die Verarbeitung der mit RFID gewonnenen Informationen letztlich im Computer statt-
findet können **alle gängigen/bekanntem Vernetzungsarten zum globalen Internet**
(damit meist auch (relativ) kostengünstig) **zum Einsatz kommen**. Sehr interessante Mög-
lichkeiten bieten hier drahtlose lokale Netze (**Wireless Local Area Networks – kurz
WLAN**) und direkte **Satellitenfunk**-Übertragung.

Mit WLAN können sehr preiswert lokale Netze intern an den jeweiligen Standorten einer
Firma oder großen Transportern, wie z.B. Contain-Frachtern (Container-Schiffen), aufge-
baut werden ohne teure Kabelverlegearbeiten durchführen zu müssen.

Zwischen den Standorten können vorhandene Infrastrukturen der Langstreckenver-

netzung zum Einsatz kommen.

So kann ein Container-Schiff die Daten über die geladenen Container per RFID-Tags an die RFID-Lese-/Schreibstationen auf dem Schiff weitergeben. Diese sind wiederum per drahtlosem lokalem Netzwerk (WLAN) mit der Logistik-Zentrale des Schiffs verbunden, welche die Daten in das globale Internet per direkter Satelliten-Verbindung einspeist und **alle benötigten Informationen mit einer globalen Datenbank abgleicht.**

Standardisierte RFID-Systeme können also ohne besonders großen Aufwand und ohne besonders hohe Kosten global vernetzt werden, da bereits vorhandene globale Infrastrukturen, insbesondere in Form des Internet, benutzt werden können.

Besonderen Nutzen haben davon Institutionen (z.B. Armee) und Firmen, die **Waren und Materialströme analysieren und steuern** müssen. Abgesehen davon, dass Standards durch **Vereinheitlichung der Systeme sinkende Kosten** nach sich ziehen, ist es essenziell von Bedeutung **Standards zum Austausch von Daten** zwischen den einzelnen am Warenverkehr beteiligten Institutionen und Unternehmen zur Verfügung zu haben. Erst dann erschliesst sich das komplette **Rationalisierungspotential** der Technik, was den **Einsatz in der Logistik** sinnvoll macht.

„RFID-Systeme sind Funkanlagen, für die die Vorschriften des Post- und Telekommunikationswesens gelten. [sog. **Funkzulassungsvorschriften** (Anm. des Autors)] Es können nur bestimmte Frequenzbereiche, insbesondere die für **Industrielle**, wissenschaftliche (**Scientifical**) oder **Medizinische** Anwendungen freigegebenen **ISM-Frequenzen**, genutzt werden. Es handelt sich um eine handvoll Frequenzbänder, die quer über das gesamte Spektrum vom Kurz- bis hin zum Mikrowellenbereich verteilt sind.

Die Frequenz eines RFID-Systems ist ein herausragendes Merkmal, da ihre Wahl wesentlich die technischen Möglichkeiten mitbestimmt. Dies sei hier verdeutlicht:

Je höher die Frequenz, desto schneller vollzieht sich eine Schwingung und damit steigt wiederum die übertragene Menge an Daten und Energie pro Zeiteinheit. Wie wünschenswert dies ist, erschließt sich nicht allein durch das Bild des Auslesens großer Datenmengen auf einem Transponder. **Oftmals ist hohe Übertragungsleistung gerade da gefordert, wo ein Pulk an Transpondern**, womöglich noch unbekannter Anzahl, in einem Feld **ausgelesen wird**, da sich die einzelnen Datenvolumina zu einer beachtlichen Größe summieren können.“ Ausserdem spielen **Reichweite und Durchdringungsfähigkeit** von verschiedenen Materialien (z.B. wasserhaltige Substanzen) eine große Rolle bei der Auswahl der Frequenz für ein RFID-System. (siehe Unterkapitel „Verwendete Frequenzen“) „Da physikalische Gesetzmäßigkeiten nicht umgangen werden können, bleibt festzuhalten: **Es gibt keinen Frequenzbereich, der bezüglich der unterschiedlichen Parameter ausschließlich positiv zu bewerten ist.**“ [...] „Es kommt entscheidend darauf an, die jeweiligen Mindestanforderungen abzudecken, sodass **keine Anwendung aufgrund von**

K.o.-Kriterien ausgeschlossen ist. Wird die Einzelanwendung isoliert betrachtet, kommt unter Umständen nur die zweitbeste Variante zum Einsatz. Allerdings entsteht bei Einsatz einer **Kompromisslösung** für alle Beteiligten immer noch eine Win-Win-Situation, wenn der Gesamtnutzen die Summe der Einzelnutzen übersteigt.

Die internationale EAN-Organisation kommt in ihrem Abwägungsprozess zu dem Schluss, dass das Frequenzband um 900MHz in der Gesamtbewertung am ehesten geeignet ist, die Anforderungen der EAN-Anwender an RFID-Systeme abzudecken. [...] In der Vergangenheit war die RFID-Technik aufgrund fehlender Absprachen und Standards für unternehmensübergreifende Anwendungen nur schwer einsatzfähig. „EAN und UCC haben dieses Problem mit der Vorlage eines Standards nunmehr gelöst. [...] **Als Richtgröße sieht der EAN-RFID-Standard das Erfassen von 250 Tags bei einem jeweiligen Nutzdatenspeicher von 128 Bits innerhalb von fünf Sekunden vor.**“ (Füßler 2002)

„Die **EAN (Europäische Artikelnummer)** ist eine ursprünglich europaweit, heute weltweit **eindeutige Produktkennzeichnung für Handelsartikel.**

Die EAN wird in der Regel als maschinenlesbarer Strichcode (Barcode) aufgedruckt, der durch Laserscanner gelesen werden kann. [Beispiel Supermarkt-Kasse (Anm. d. Autors)] Neben schneller Abfertigung der Kunden an Scannerkassen wird dadurch vor allem der Warenverkehr und die Lagerhaltung erleichtert. [...]

Bereits 1973 wurde in den USA der **Uniform Product Code (UPC)** [...] eingeführt. Ein Jahr später machte sich Europa die ersten Gedanken über ein ähnliches System, das zum UPC kompatibel sein sollte. 1977 wurde die **European Article Association** gegründet, die **später in EAN International umbenannt** wurde. Sie hat Mitgliedsorganisationen in 98 Ländern.

Durch die Integrierung des amerikanischen Produktcodes, der vom **Uniform Code Council (UCC)** betreut wird, wird das **System heute als EAN·UCC bezeichnet.**“

Zum 1. Januar 2005 wird die EAN-13 Standard-Kodierung auch in Nordamerika eingeführt. (Wikipedia 2004 A)

Die EAN·UCC hat vor die **RFID-Technik** (mit ihren Transpondern) zusätzlich in das bestehende System aufzunehmen und **parallel zu anderen möglichen AutoID-Techniken**, wie z.B. Magnetstreifen, Barcode, Datenfunk, OCR, Biometrik, Spracherkennung, zu verwenden. In der technischen Realisierung wird der AutoID-Teil dann über eine Zwischenschicht verarbeitet (abstrahiert), **so dass es für die bestehende Software egal ist, ob nun z.B. ein Strichcode oder die Daten eines RFID-Tags ausgelesen werden.** Das spart erheblich Investitionen und ermöglicht die Integration in alle bestehenden Systeme.

Auf den RFID-Tags wird der **Elektronische Produkt Code** zum Einsatz kommen. „Der Elektronische Produkt Code (**EPC**) ist eine Kennzeichnung von Waren und soll der Nachfolger des EAN-Barcodes werden. Mit einer Länge von 96 Bit [ein Bit = 2 Zustände, also die kleinste mögliche Informationseinheit (eine Binärzahl – engl. binary digit, kurz Bit (Anm. d. Autors))] können **Waren weltweit mit einer eindeutigen Nummer** versehen werden. Im Zusammenhang mit der RFID-Technik können somit Waren von der Herstellung über den Handel bis zum Verbraucher verfolgt werden. Die Standardisierungsorganisationen UCC und EAN International haben für die **Vermarktung des EPC die Firma EPCglobal Inc. gegründet.**“ (*Wikipedia 2004 B*) Des Weiteren enthält der EPC Informationen über den Hersteller des Produktes, die Produktserie und eine Versionsnummer für zukünftige Anwendungen.

„VERISIGN MIT WELTWEITER RFID-ADRESSIERUNG BEAUFTRAGT

EPCglobal, das mit der Einführung des Electronic Product Code (EPC) befasste Industriekonsortium, gab [...] seine Zusammenarbeit mit dem kalifornischen Unternehmen VeriSign bekannt. **VeriSign werde den globalen Verzeichnisdienst für das RFID-basierte EPC-Netzwerk stellen.**“ (*nhe 2004*)

Die **EPC-Spezifikation Version 1.0** wurde bereits ausgearbeitet und beschreibt die Verwendung von RFID-Technik mit 900MHz, 13,56MHz, 860 und 930MHz sowie die Übertragungsprotokolle. (*EPCglobal, Inc., 2003*) *Noch im aktuellen Quartal soll die Verabschiedung der Spezifikation geschehen.* (*Windeck 2004*)

1.4 VERSCHLÜSSELUNG DER INFORMATIONEN

Bei der Kommunikation zwischen Schreib-/Lesestation und RFID-Tag können Codier- und Daten-Komprimierungsverfahren angewendet werden. (*Füßler 2002*)

Besondere Anforderungen werden an RFID-Tags gestellt, wenn diese zum Bezahlen eingesetzt werden. „Der **Geldwert der Karten macht diese auch für mögliche Angreifer interessant.** Der Schreib- und Lesezugriff auf die Karten ist deshalb nur nach einer gegenseitigen Authentifizierung zwischen der kontaktlosen Chipkarte und dem Lesegerät möglich. Dieser Vorgang überprüft, ob ein geheimer, kryptographischer Schlüssel in der Chipkarte und dem Lesegerät gespeichert ist.

Geeignete Algorithmen [Algorithmus: definierter schrittweiser Ablaufplan um ein Problem zu lösen (Anm. d. Autors)], wie sie etwa in der ISO-Norm 9798 beschrieben sind, **können verhindern, daß ein Angreifer den geheimen Schlüssel ausspäht.** Dieser könnte ohne diese Maßnahme die Funkverbindung zwischen der Chipkarte und dem Lesegerät einfach abhören und so den geheimen Schlüssel ausspionieren. Die einer erfolgreichen Authentifizierung **folgende Kommunikation zwischen der Karte und dem Lesegerät**

wird ebenso verschlüsselt, um auch das Abhören und das erneute Einspielen der zu übertragenden Daten zu verhindern.“ (*Finkenzeller 1998*)

„DIE MEISTEN RFID-TAGS SENDEN IHRE INFORMATIONEN IN KLARTEXT, EINIGE MODELLE VERFÜGEN ABER AUCH ÜBER DIE MÖGLICHKEIT, IHRE DATEN VERSCHLÜSSELT ZU ÜBERTRAGEN.“ (WIKIPEDIA 2004 C)

Anders als heutige Tags, die gegen Diebstahl angewendet werden (siehe EAS im folgenden Unterkapitel) hat **jeder RFID-Chip eine weltweit einzigartige Seriennummer.** (*Garfinkel 2004*) *Man kann ihn also quer durch die ganze Welt verfolgen und dadurch auch den Inhaber, sofern bekannt, damit verknüpfen. Geschäfte könnten z.B. erkennen, welcher Kunde den Laden betreten hat, wenn das unverschlüsselte RFID-Tag noch aktiv ist.*

Die Verschlüsselung der Informationen **erfolgte bisher nur, wenn die auf dem RFID-Chip gespeicherten Informationen direkt geeignet waren finanzielle Transaktionen auszulösen.**

Das Verschlüsseln der Informationen sollte auch im Interesse der Firmen liegen, die diese Technik verwenden. Wenn die Informationen der Tags ohne Authentifizierung ausgelesen und verfolgt werden können, dann ist Industriespionage nicht ausgeschlossen und die Anwenderfirmen können erheblichen wirtschaftlichen Schaden davontragen. Diese Problematik beschränkt sich leider nicht nur auf Firmen, sondern wird auch relevant, wenn einzelne Bürger mit ungeschützten RFID-Tags ausgestattet werden und persönliche Daten darauf gespeichert sind. Die Verknüpfung von solchen Daten in einer großen Datenbank kann erhebliche Begehrlichkeiten wecken.

Eine weitere Lösung zum Schutz der Privatsphäre, die jedoch nichts mit Kryptographie zu tun hat, wird momentan von Mitarbeitern der Firma RSA-Security diskutiert. **Dabei handelt es sich um ein sogenanntes RFID „Blocker Tag“, das in der Lage ist ein Lesegerät allgemein oder selektiv daran zu hindern RFID-Chips in der Nähe des Blocker Tags auszulesen, also das Lesegerät zu blockieren.** Der Trick dabei ist, dass dieses Tag alle möglichen Tags mit ihren ID-Kennungen oder auch nur eine bestimmte Untermenge an ID-Kennungen simulieren kann. Das Lesegerät kann jedoch immer nur die Daten eines RFID-Tags einlesen. Wenn zwei Tags gleichzeitig senden, dann entsteht eine Kollision der Informationen und das Lesegerät ist nicht in der Lage Daten auszulesen. (*Juels, Rivest, Szydlo 2003*) *Unter normalen Umständen existieren keine zwei RFID-Tags mit der gleichen Kennung. Die Kennung dient dem Lesegerät dazu die RFID-Tags zu unterscheiden, jeweils nur einem der Tags das Senden der Daten zu erlauben und in der*

gleichen Zeit allen anderen das Senden zu verbieten. Diese werden in eine Warteschlange eingereiht, welche dann nach und nach abgearbeitet wird. Das „Blocker Tag“ ist also sozusagen ein „anarchisches“ RFID-Tag, welches sich nicht an die Spielregeln hält und deswegen zu einer Verklemmung/Blockade beim Einlesen der Tags führt, auf deren Kennung es sich in die Kommunikation einmischen soll. Es „redet“ also immer dazwischen, wenn das Lesegerät mit dem entsprechenden RFID-Tag „sprechen“ will.

1.5 GESCHICHTE DER TECHNISCHEN ENTWICKLUNG

„Transponder wurden Mitte der dreißiger Jahre erfunden. Im zweiten Weltkrieg waren Transponder große unhandliche Kästen, die in die Nase eines Flugzeugs eingebaut wurden. Im Krieg wurde die Technik dazu benutzt, dass sich Flugzeuge der eigenen Einheiten untereinander identifizieren konnten. Erst 1977 wurde die Transpondertechnik für den zivilen Einsatz freigegeben; es dauerte dann noch bis 1988, bis die ersten kommerziellen Transponder zum Einsatz kamen.“ (*Borchers 2001*)

„In den 1960ern wurden die ersten kommerziellen Vorläufer der RFID-Technologie auf den Markt gebracht. Es handelte sich dabei um elektronische Warensicherungssysteme (engl. **E**lectronic **A**rticle **S**urveillance, **EAS**), um Diebstähle zu unterbinden.“ Es war nur möglich 2 Zustände, also die kleinste mögliche Informationseinheit (eine Binärzahl – engl. binary digit, kurz Bit), zu speichern. Diese beiden Zustände können z.B. als ja/nein, an/aus oder 0/1 interpretiert werden. Dadurch „konnte also nur das Vorhandensein oder das Fehlen der Markierung geprüft werden. Die Systeme basierten auf Mikrowellentechnik oder Induktion.“ (*Wikipedia 2004 C*)

2. ANWENDUNGSMÖGLICHKEITEN

Zurzeit gibt es viele sinnvolle Einsatzmöglichkeiten für RFID. Eine davon ist die Wirtschaft, besonders der Bereich Logistik. Sehr viele Unternehmer statten ihre Waren mit Smart Tags aus, um Lagerbestände und Lieferungen automatisch zu verwalten. Hersteller von Produkten verschiedener Arten können ihre Güter, denen ein Smart Tag eingebaut wurde, rund um den Globus verfolgen und so die gesamte Logistik optimieren. (Kleinwaechter 2003) Die Kontrolle der Logistik ist besonders bei solchen Produkten wie Medikamente wichtig. Das soll bewirken, dass diese Produkte nicht gefälscht werden und dass sie in korrekter Weise aufgehoben werden. Dank RFID-Systemen kann man den Lieferweg kontrollieren und erkennen, ob Produkte verloren gehen oder gestohlen werden.

Benetton war eine der ersten Firmen, die Tags in ihre Produkte integriert hat, um den Transport der teuren Ware in die Boutiquen zu verbessern. Inzwischen versprach der italienische Bekleidungshersteller zumindest bei den Kleidungsstücken auf RFID-Etiketten zu verzichten, da deren Verwendung nach öffentlicher Aufmerksamkeit für ein negatives Bild in der Presse gesorgt hat. Der Hersteller steht für Weltoffenheit, Toleranz und Vertrauen und das sollte auch diese Marke symbolisieren. (Hillenbrand 2003) Das stimmt natürlich nicht mit der Anwendung der RFID-Technik überein, da das Vertrauen der Kunden dadurch missbraucht wird.

Firma Marks & Spencer hat 3,5 Mio. Tabletten zur Auslieferung mit RFID-Tags im Mai 2002 ausgerüstet. Das Personal und die Zulieferer sollten sechsmal schneller detaillierte Informationen über Tabletten geliefert bekommen. Nach dem der Transportwagen die Schranke passiert hat, hat es de facto fünf Sekunden gedauert, bis die Daten über die Ware mit hoher Verlässlichkeit gescannt wurden. Das Scannen mit einem traditionellen Barcode beträgt immerhin 29 Sekunden. (Gatzke 2003) Die gesamte Transportleistung wurde dank RFID verbessert.

In einem Distributionszentrum für Milchfrischprodukte von Nestlé werden die Produkte in Kanallagern mit Rollpalettenuntersätzen gelagert. Diese Organisationsart ermöglicht kurze Durchlaufzeiten für verderbliche Ware. Alle Lagerplätze werden von halbautomatischen Regalbediengeräten kontrolliert und bedient. Wegen Einschränkung von einer optischen Verbindung und einer technisch ausgeschlossenen Pulkerfassung wäre es unglaublich schwierig, einen Barcode von einer Palette abzulesen. Deswegen hat Nestlé sich für die RFID-Technik entschieden. (Füßler 2002) Das zeigt ein Potenzial von RFID-Technologie.

Der Reifenhersteller Michelin hat sich vorgenommen, in nächster Zeit bei allen seinen Produkten RFID Chips einzubauen. Der Hersteller will erreichen, dass die Fahrzeuge nicht falsch bereift werden. Michelin will seine Kunden vor gefälschten Produkten schützen,

was gleichzeitig den Verlust der Privatsphäre der Verbraucher bedeutet. (Gatzke 2003) Eine weitere Rolle spielt ein neues Gesetz in den USA, wonach Reifenhersteller in der Lage sein müssen, sämtliche betroffenen Reifen zurückzurufen, wenn in einer Produktionsreihe ein Fehler bekannt wird.

Auto-ID Center ist ein Unternehmen, das dem weltweiten Durchbruch von RFID-Technologie verhelfen will. Die Lobbygruppe war beteiligt bei der Entwicklung von einem besonderen Verkaufsregal, das RFID Etiketten benutzt, um den Status von Produkten zu beobachten und auf dem Display anzuzeigen. Falls ein Artikel gestohlen wird, werden auch die Verkäufer gleich benachrichtigt. Falls sich zu wenig Waren auf den Regalen befinden, bekommt das Personal eine Nachricht über möglichen Nachschub. Genau diese Technik ist auch bei Gillette-Produkten angewendet worden. Jeder Kunde, der ein Klingepäckchen in die Hand nimmt bzw. berührt wird gleich fotografiert, denn er könnte ein möglicher Dieb sein. (Gatzke 2003)

Einen etwas netteren Einsatz kann man in Prada-Geschäften in New York finden. Der Modehersteller wollte mit RFID noch mehr Kunden von seiner Marke überzeugen. Jeder, der eine Umkleidekabine betritt, bekommt gleich – dank Smart Tags – eine Modeschau auf einem flachen Bildschirm zu sehen, wo genau die Kleiderstücke, die er gewählt hat, vorgeführt werden. (Hillenbrand 2003) Das zeigt das Potential der RFID-Technik.

Eine Anwendung der RFID-Technologie bietet auch für Arbeitgeber neue Möglichkeiten. In Sydney hat ein Casino alle Uniformen der Angestellten mit Smart Chips ausgestattet. So sollte es verhindert werden, dass die Mitarbeiter ihre Uniformen suchen müssen, bzw. besonders teure und schöne Stücke irgendwo verschwinden. Diese Technologie gibt dem Arbeitgeber eine Möglichkeit seine Mitarbeiter ständig unter Kontrolle zu haben. Man kann theoretisch herausfinden, wer sich in welchen Räumen aufgehalten hat und wie viel Zeit er dort



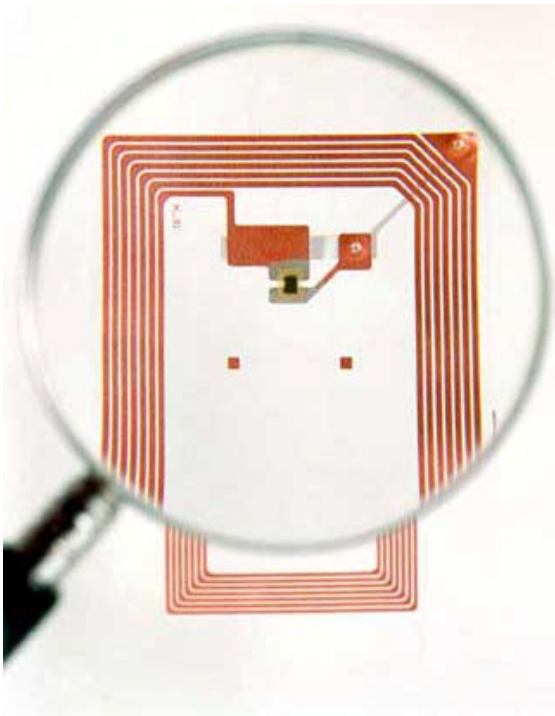
verbracht hat, egal ob das die Toilette war oder das Büro mit Aktenschränken. RFID-Tags sind überall installiert. (Hillenbrand 2003)

Auch der Öffentliche Personennahverkehr (ÖPNV) ist von den positiven Seiten des Einsatzes von RFID-Systemen überzeugt. Die Einführung von kontaktlosen Chipkarten, statt Papierscheinen bringt nicht nur Vorteile für die Benutzer des öffentlichen Verkehrs, sondern auch für den Betreiber selbst. Das Prinzip ist simpel. Ein Fahrgast erwirbt erstmal eine Plastikkarte mit eingebautem Chip, lädt sie mit Geld auf und schon ist er für Nutzung des Verkehrs vorbereitet. Er braucht kein zusätzliches Bargeld mit sich zu tragen. Die kontaktlosen Chipkarten, die vorher bezahlt wurden, sind auch bei der Umstellung des Tarifs gültig. Der Fahrgast muss nicht genaue Preise für die Fahrstrecke kennen. Der Fahrweg wird automatisch einem bestimmten Tarif zugeordnet und die nötige Summe wird

abgebucht. Die Lesegeräte, die mit Chipkarten kommunizieren, werden an Bahnhöfen, am Eingang zu den Fahrzeugen, eingesetzt. Die Passagiere brauchen nicht mal ihre Tickets aus der Tasche zu nehmen, denn das Lesegerät kann bis zu einer bestimmten Entfernung die notwendigen Daten von der Karte ablesen. Die Vorteile für die Verkehrsunternehmen sind deutlich: keine Wartungs- und Reparaturarbeiten an den Verkaufsautomaten, keine zusätzlichen Kosten bei der Umstellung auf neue Tarife – neue Fahrscheine müssen nicht gedruckt werden. Die Firmen des ÖPNV vermuten, dass die Verluste, die durch Schwarzfahrer entstanden sind, erheblich reduziert werden. (Finkenzeller 2002)

RFID – Technik hilft bei der Auffindung von toxischen Gegenständen, insbesondere wenn sie bei der Mülldeponie landen. Gasflaschen und Chemikalienbehälter müssen genau beschriftet und eindeutig gekennzeichnet werden. Auf einem Chip kann man viel mehr relevante Informationen wie: Flaschen- bzw. Behälternummer, Eigentümer, TÜV – Termin, Inhalt, Volumen, maximaler Fülldruck, als auf einem Barcode speichern. Die Daten können jederzeit verändert werden. Mit dem Sicherheitsmechanismus – Authentifizierung, kann man vermeiden, dass jedes Lesegerät auf dem Tag gespeicherte Informationen abliest. Die RFID – Transponder besitzen eine besondere Eigenschaft, die sie gegenüber dem traditionellen Barcode hervorhebt. Die „intelligenten“ Chips ertragen sehr hohe und niedrige Temperaturen, Schmutz, Feuchtigkeit, Strahlen, Vibrationen und Säuren. Unter dem Einfluss von Staub und Schmutz wird die Funktionalität der Barcodelesegeräte sehr negativ beeinträchtigt, den RFID – Lesegeräten stören solche Umweltbedingungen überhaupt nicht. (Finkenzeller 2002)

Die Smart Tags – Technologie hat ihren Einsatz in „elektronischen Wegfahrsperrern am Zündschloss“ gefunden. Hier wird eine Kombination aus einem mechanischen Zündschlüssel und einem Transponder realisiert. In dem Zündschloss wird ein Lesegerät eingebaut. Wenn man den Zündschlüssel in einem Zündschloss umdreht, folgt der Datenaustausch zwischen den beiden. In dieser Zeit werden drei Verfahren durchgeführt, um die Authentizität des Zündschlüssels zu überprüfen. Zuerst wird die individuelle Seriennummer (Unique Number) kontrolliert. Die Nummer von dem Transponder am Zündschlüssel wird mit der Referenznummer des Zündschlosses verglichen. Wenn diese gleich sind, wird die Motorelektronik von dem Sicherheitsmechanismus befreit. Da die Angreifer die individuelle Seriennummer ablesen können, hat man ein Wechselcodeverfahren (Rolling Code) eingesetzt. Beim Umdrehen des Zündschlüssels im Zündschloss wählt ein Zufallsgenerator eine neue Zahl, die dann auch im Speicher des Zündschlüssels abgelegt wird. Es ist nicht möglich, die gleiche Zahl rauszubekommen, denn bei jedem Schlüssel zum Fahrzeug wird eine neue Zufallsnummer erzeugt. Das sicherste Verfahren ist jedoch eine Authentifizierung (challenge response). Während diesem kryptologischen Vorgehen wird ein geheimer, binärer Schlüssel überprüft. Er muss jedoch zum Zündschloss nicht übertragen werden. Dann folgt die Kommunikation des Lesegeräts mit der Motorelektronik. Mit Hilfe von Authentifizierung werden die Kraftstoffversorgung und Zündanlage kontrolliert. Bei diesem Verfahren werden alle Vortäuschungsversuche gegenüber dem Lesegerät zunichte.



(Finkenzeller 2002)

Das Anwendungspotenzial von RFID – Technologie findet in fast allen Bereichen unseres Lebens statt. Im Moment arbeitet die UN-Luftfahrtorganisation ICAO an der Implementierung des RFID – Tag in einem Flugticket. (Pichet 2003) Das Lufthansa – Unternehmen hat schon 1995 erste Versuche der Einführung von kontaktlosen Chipkarten gestartet. Es wurde eine Chipkarte produziert, in der sich unter anderem ein Transponder befindet. Der Chipkartenbesitzer kann telefonisch seinen Flug buchen. Dabei braucht er nur seine Kartenummer anzugeben. Im zentralen Rechner der Lufthansa befindet sich ein elektronisches Ticket, in dem die persönlichen Daten der Kunden gespeichert sind. Dazu kommen noch die Daten, die den gebuchten Flug betreffen. Nach der Ankunft am Flughafen muss sich der Chipkarten-

besitzer nur noch beim Chip-In – Terminal anmelden und der Beleg mit Einsteige-Gate und Sitzplatznummer wird gedruckt. Dabei kann die Lufthansa – Chipkarte in der Tasche bleiben. Die Vorteile sind vor allem für die Passagiere sichtbar. Einchecken dauert nur noch ca. 10 Sekunden. Was den Passagieren am meisten gefällt, ist die bequeme und einfache Buchung. Auf diese Weise wurden das Einchecken und die Buchung der Lufthansa und Airplus optimiert.

Die Verfolgungsmöglichkeit kann auch nützlich sein. Mit Hilfe von RFID Chips, ist man in der Lage entlaufene Katzen und Hunde und ausgeflogene Hausvögel nach vorheriger Standortbestimmung schneller zu finden. (Hillenbrand 2003) Es besteht auch eine Chance, dass man Smart Tags auch bei Menschen implantieren kann. Die Firma VeriChip hat im Jahr 2003 bei 2.700 Bewohnern von Lateinamerika die kleinen Chips eingesetzt. Alle Patienten wollten sich auf diese Weise vor Entführungen schützen. In Zukunft wird es möglich sein, die implantierbaren Tags mit Hilfe von Satelliten zu lokalisieren. (Kleinwaechter 2003) Somit könnte man den Aufenthaltsort von entführten Personen schneller bestimmen. Eine Familie aus Florida hatte auch den Wunsch, so einen „intelligenten“ Chip bei ihren Kindern zu implantieren. Das hat eine große Diskussion im US-Kongress hervorgerufen, denn es gibt keine Gesetzgebung über mögliche Implantation von RFID Tags in menschliche Körper. (Kleinwaechter 2003)

In den USA, an der Privatschule Enterprise Charter School in Buffalo, wird die neuste RFID – Technik praktiziert. Ziel ist es, das Objekt ständig zu überwachen. Jeder Schüler trägt um den Hals eine Plastikkarte, die mit einem Smart Tag ausgestattet ist. Bei dem Eingang zur Schule werden sie jeden Tag neu identifiziert. Die Angestellten sind genauso dazu verpflichtet, bevor sie die Schule betreten, sich identifizieren zu lassen. Die kleinen

Chips sind in fast allen Gebrauchsgegenständen der Schule wie: Bücher, Laptops, usw. eingebaut. Der Direktor ist über den RFID – Einsatz so begeistert, dass er schon neue Anwendungsmöglichkeiten in der Schule gefunden hat. (Pichet 2003)

Es werden immer mehr Anwendungsmöglichkeiten für die RFID Technologie entdeckt. Die nächste Idee kam von der Europäischen Zentralbank; jeder Schein von 5 bis zu 500 Euro sollte mit dem RFID gekennzeichnet werden. Somit könnte man den Weg des Geldes genau identifizieren. Die Gegner des RFID-„Wunders“ erklären, dass die Anonymität des Geldes verloren geht. Es wird aber möglich, gestohlene Scheine zu identifizieren und damit vielleicht auch den Dieb zu fangen. (Kleinwaechter 2003)

Die hier erwähnten Beispiele für Anwendungen zeigen eine sehr große Vielfalt der innovativen RFID – Technologie. Die Radiofrequenztechnologie zu Identifikationszwecken (RFID) nimmt immer mehr an Bedeutung zu. Die Einschränkungen, die durch Strichcodierung aufgestellt wurden, können jetzt – dank RFID – überschritten werden. Zurzeit ist es möglich den geografischen Ort eines Gegenstandes mit implantiertem RFID-Chip bis zu einer begrenzten Entfernung zu bestimmen. In der Zukunft wird es zusammen mit GPS global funktionieren. Man muss nur den festgelegten RFID-Code bzw. die IPv6-Adresse kennen. So könnten die Hersteller die gesamte Logistik beobachten und, falls nötig, optimieren. Die eTags werden vermutlich in der Lage sein, untereinander zu kommunizieren, sog. kosmische Kommunikation, so dass ich in meiner Wohnung Sachen wie Schuhe und Uhr mit Hilfe meines mobilen Telefons ganz schnell wieder finden kann. (Kleinwaechter 2003) Wann mein Haushaltskühlschrank vor dem Ablauf eines Mindesthaltbarkeitsdatums automatisch neue Milchpackung selbständig bestellt und die Lieferungsprozedur auslöst, wird in der nahen Zukunft bekannt. (Füßler 2002) Dank der Zusammenarbeit von RFID-Technologie und GPS wird es möglich, die Datenbanken der ganzen Welt zu vernetzen, was den globalen Datenaustausch ermöglicht. Die Daten werden ständig, durch Ergänzung und Vervollständigung, aktualisiert.

3. DATENSCHUTZ-PROBLEME

Den teilweise dargestellten sinnvollen Anwendungsmöglichkeiten stehen gefährliche Folgen gegenüber, wenn wie zu erwarten, in Zukunft massenhaft Produkte mit eingebauten RFID's bis zu den Verbrauchern gelangen. (Gfaller 2003) In diesem Abschnitt sollen derartige Probleme aus informatischer Sicht betrachtet werden.

3.1 BETREFFEN RFID'S PERSÖNLICHE INFORMATIONEN?

Da die EPCs der RFIDs einmalig sind, können darüber die zugehörigen Produkte eindeutig identifiziert werden. Werden die Produkte von Menschen bei sich geführt, so können diese Personen ebenfalls identifiziert bzw. pseudonymisiert werden. Unter Pseudonymisieren verstehen wir die Möglichkeit, Personen über Pseudonyme wiedererkennen zu können, ohne jedoch die realen Personendaten, wie Name, Geburtsdatum und Anschrift zu kennen. Im Zusammenhang mit der RFID-Technik bieten sich selbstverständlich die EPCs der Tags als Pseudonyme an.

Um Verbraucher wiedererkennen bzw. pseudonymisieren zu können, kommen insbesondere Gegenstände in Betracht, die mit RFID's ausgestattet sind und häufig von der gleichen Person am Körper getragen werden. Diese Anforderungen erfüllen beispielsweise Schuhe und Kleidungsstücke (Heise 2003 C)(Heise 2003 D) oder mobile Gebrauchsgegenstände wie Schlüsselanhänger und Mobiltelefone (Time 2003).

Die Kombination mehrerer EPCs verringert die Wahrscheinlichkeit, Personen zu verwechseln, sollten einige Gegenstände ausgetauscht werden. (Weis 2003) Beispielsweise kann ein Handy verkauft werden, aber es ist unwahrscheinlich, dass das Handy zusammen mit den Schuhen des Verkäufers verkauft wird. So lässt sich der Verkäufer immer noch über die Schuhe wiedererkennen.

Aufgrund der erwähnten Anforderungen eignen sich ebenfalls Fortbewegungsmittel, wie Autos oder Fahrräder, um auf eine einzelne Person schließen zu können.

Beispiel: Frau Meier betritt einen Supermarkt, und geht dabei, für sie unbemerkt, an einem RFID-Lesegerät vorbei. Dieses erkennt in dem Moment zwei bestimmte RFID's im Schuh bzw. im Mobiltelefon von Frau Meier. An der Kasse bezahlt sie mit Bargeld ihren Einkauf. Das an der Kasse angebrachte Lesegerät liest die EPCs des Schuhs und des Mobiltelefons aus und verknüpft diese Informationen mit den gekauften Produkten.

Besucht Frau Meier den Supermarkt zu einem späteren Zeitpunkt erneut, so kann sie automatisch als ein „Altkunde“ mit einem bestimmten Einkaufsverhalten erkannt werden. Dieses Einkaufsverhalten umfasst Daten darüber wie häufig sie einkauft, wann sie dies getan hat, wie lange sie sich im Supermarkt aufgehalten hat und was sie gekauft hat. Sollten im Supermarkt noch weitere Lesegeräte

angebracht sein, könnte erkannt werden, an welcher Stelle sie sich im Supermarkt wie lange aufgehalten hat und welche Waren sie betrachtet hat.

Die Identifizierung erfordert im Gegensatz zur Pseudonymisierung das Zusammenführen von Personendaten und EPCs. Dies kann z.B. dadurch geschehen, dass der Verbraucher an der Kasse mit Kreditkarte bezahlt oder eine persönliche Kundenkarte verwendet. Das Problem wird weiter verschärft, wenn persönliche Kunden-, Kredit- oder Fahrkarten mit der RFID-Technik ausgestattet werden. Dadurch ließen sich möglicherweise unbemerkt Personendaten, wie Name, Anschrift oder Geburtsdatum, von jeder beliebigen Person im Sendebereich der RFIDs auslesen.

Den EPCs ist außerdem zu entnehmen, in welchem Produkt es eingebaut ist und von welchem Hersteller dieses stammt.

Beispiel: Frau Meier kauft wie immer in ihrem nahegelegenen Supermarkt ein. Heute bezahlt sie nicht mit Bargeld, sondern mit ihrer neuen Kreditkarte. Das Lesegerät der Kasse erkennt wie immer an den Tags im Schuh und im Handy, dass es sich um einen bestimmten Kunden handelt, dessen Name aber bisher unbekannt ist. Durch die Kreditkarte können nun allerdings die Daten, die bei Frau Meiers Einkäufen der letzten Jahre angefallen und gespeichert worden sind, (siehe vorhergehendes Beispiel) mit dem Namen und der Anschrift von Frau Meier in Verbindung gebracht werden.

Der Unterschied zu gewöhnlichen Identifikationsmöglichkeiten besteht darin, dass die RFIDs leicht maschinell ausgelesen werden können und keine komplizierte Erkennung von analogen Personenmerkmalen, wie Gesicht, Fingerabdruck etc., vorgenommen werden muss.

Ergebnis: RFIDs werden in einfacher Weise dazu genutzt werden können, sensible persönliche Informationen über jeden einzelnen Verbraucher zu erhalten.

3.2 KANN DER VERBRAUCHER RFID'S MEIDEN?

RFIDs werden in der Regel **nicht gekennzeichnet** und sind auf Grund ihrer Größe kaum zu erkennen. Eine weite Verbreitung und Verwendung von Lesegeräten, die RFIDs erkennen können, ist nicht zu erwarten.

Selbst wenn der Verbraucher über die Existenz von RFIDs informiert ist, hat er beschränkte Möglichkeiten, diese zu **zerstören**. Befinden sich die RFIDs in Produkt-Verpackungen, dann können diese mit einigem Aufwand lokalisiert und entfernt oder mit physischer Gewalt zerstört werden. Der Verbraucher hat aber nicht die Möglichkeit zu überprüfen, ob die vermeintlich zerstörten RFIDs wirklich unbrauchbar sind. Handelt es sich um in Produkten integrierte RFIDs, so lassen sich diese in den meisten Fällen nicht

zerstören, ohne das jeweilige Produkt in Mitleidenschaft zu ziehen.

Einige Geschäfte die RFID-Technik bereits verwenden stellen **Automaten** auf, an denen sich die RFIDs **deaktivieren** lassen. Dazu muss sich der Kunde nach dem Kauf der Waren an den Automaten begeben, möglicherweise erneut anstellen, und dort in einer aufwändigen Prozedur jeden Gegenstand einzeln „deaktivieren“. (RFID Journal 2004) Der Verbraucher erfährt dabei nicht, dass die Tags nicht wirklich unbrauchbar gemacht werden, sondern nur der EPC teilweise überschrieben wird. (FoeBuD 2004)

Sollte das Deaktivieren irgendwann wirklich an solchen Automaten funktionieren, ist trotzdem nicht mit einer umfassenden Nutzung durch den Verbraucher zu rechnen, sofern es sich um einen zusätzlichen Vorgang handelt, der aufwändig ist und Zeit erfordert. Das Deaktivieren wäre nämlich sehr zeitaufwändig, da in absehbarer Zeit in nahezu jedem Massenprodukt bzw. dessen Verpackung ein Tag enthalten sein wird.

Bei einer zunehmenden Integration von RFIDs in Konsum- und Gebrauchsgütern wird es aus Mangel an Alternativen vermutlich praktisch unmöglich sein, Gegenstände ohne RFIDs erwerben zu können, so dass sich der Verbraucher unumgänglich mit RFID-Tags am Körper wird bewegen müssen.

Ergebnis: Der Verbraucher wird in Zukunft nicht mehr die Möglichkeit haben, über die Existenz von RFIDs in seinem Eigentum oder deren Funktionsfähigkeit zu entscheiden.

3.3 KANN DER VERBRAUCHER DEN ZUGRIFF AUF SEINE RFIDS BESCHRÄNKEN?

Der Besitzer eines Produktes mit eingebautem RFID kann den informellen **Zugriff** darauf ohne weiteres **nicht** technisch **beschränken**. Kommt das Produkt in die Reichweite eines Lesegerätes, kann der RFID-Chip ausgelesen werden. Außerdem lassen sich Lesegeräte versteckt anbringen, so dass alle vorbeigehenden Personen unbemerkt gescannt werden können. (Garfinkel 2004)

Der Verbraucher kann darüber hinaus nicht **erkennen**, und somit auch nicht darauf reagieren, *wann* bzw. *ob* auf seine RFIDs **zugegriffen** wird, *von wem* dies getan wird und *was* mit den Daten geschieht.

Als technische Schutzmöglichkeit wurde vorgeschlagen, das Auslesen der RFIDs zu stören. Der sogenannte **RFID-Blocker** hat ähnliche Auswirkungen wie ein Störsender, obwohl diesem eine andere technische Arbeitsweise zu Grunde liegt, die im ersten Kapitel erläutert wurden. (Juels, Rivest, Szydlo 2003) Leider weist dieser Ansatz folgende Nachteile auf:

- Es wird technisch immer möglich sein, spezielle Lesegeräte zu entwickeln, die einen solchen RFID-Blocker umgehen können. Selbst bei der gewöhnlichen technischen Entwicklung ist damit zu rechnen, dass die normalen Lesegeräte in Zukunft solche RFID-Blocker umgehen könnten. Bei der Verwendung solcher RFID-Blocker würde dies einen technischen Wettlauf bedeuten, der es für den Verbraucher erfordern

würde, sich die aktuelle Technik anzuschaffen und zu verwenden.

- Der Verbraucher muss ein entsprechendes technisches Verständnis und Problembewusstsein besitzen, um einen RFID-Blocker zu erwerben und entsprechend zu benutzen. Die Erfahrung mit anderen datenschutzrechtlichen Problemen lässt ein solches Verhalten nur bei einer Minderheit der Verbraucher erwarten.
- Der Verbraucher kann nicht mit Sicherheit erkennen, ob nicht doch auf seine RFIDs zugegriffen wird. Dies könnte möglich sein, wenn der RFID-Blocker defekt ist, er zu weit von einigen RFIDs entfernt getragen wird oder aus den oben genannten technischen Gründen.
- RFID-Blocker könnten in bestimmten Bereichen, z.B. einzelnen Kaufhäusern oder terroristisch gefährdeten Objekten, verboten werden.

Zusammenfassend kann festgestellt werden, dass RFID-Blocker kein geeignetes Mittel sein werden, um massenhaften Datenschutzverletzungen vorzubeugen.

Eine weitere technische Maßnahme um genügenden Datenschutz zu gewährleisten könnte **Verschlüsselung** darstellen. Dabei sind folgende Aspekte zu berücksichtigen:

- Verschlüsselung würde die Kosten für die RFID-Technik erhöhen, so dass mit einer weiten Verbreitung nicht zu rechnen ist.
- Durch Verschlüsselung könnte lediglich der Zugriff von Dritten verhindert werden. Ein interner Missbrauch würde diese Maßnahme nicht beeinflussen. Die Verknüpfung der persönlichen Daten über das Internet stellt ein wesentliches Problem dar, dem mit diesem Ansatz nicht begegnet werden kann.
- Die Geheimhaltung der Schlüssel müsste durch die Verkaufsstellen bzw. Hersteller sichergestellt werden. Dies würde eine technisch aufwändige Infrastruktur für die gesamte Logistik erfordern. Da die Verkaufsstellen offensichtlich kein eigenes Interesse daran haben, ist mit einer entsprechend sorgfältigen Infrastruktur nicht zu rechnen, die die Geheimhaltung des Schlüssels sicherstellen könnte.

Da dadurch der interne Missbrauch nicht verhindert und die Sicherheit der Schlüssel nicht sichergestellt werden kann, scheint Verschlüsselung keine brauchbare Maßnahme, um den Datenschutz zu gewährleisten.

Ergebnis: Der Verbraucher verliert die Möglichkeit der informationellen Selbstbestimmung, (BVG 1983) da er den Zugriff auf seine RFIDs nicht beschränken kann.

3.4 WELCHE NACHTEILIGEN FOLGEN KANN RFID FÜR VERBRAUCHER HABEN?

Durch die neuen technischen Möglichkeiten, die mit der RFID-Technik einhergehen, wird der Verbraucher die Möglichkeit der **informationellen Selbstbestimmung** verlieren, die ihm nach Beschluss des Bundesverfassungsgerichts nach dem Grundgesetz zusteht.

(Kleinwächter 2003) Dieses Recht besagt, dass jeder selbst darüber entscheiden kann, ob und in welchem Rahmen persönliche Lebenssachverhalte offenbart werden. (BVG 1983) Sollte also für jeden Interessierten ersichtlich sein welche Gegenstände ein bestimmter Verbraucher bei sich trägt, oder sollten umfangreiche Verhaltensprofile automatisch über ihn erstellt werden können, (c't 2004) so besteht nicht mehr die Möglichkeit über die Weitergabe der betroffenen persönlichen Informationen zu entscheiden.

Der Verlust der informationellen Selbstbestimmung kann für den Verbraucher viele negative Auswirkungen haben. Dieses Kurzgutachten beschränkt sich aus zeitlichen Gründen lediglich auf die Darstellung der Preisdiskriminierung.

Beispiel: Frau Meier geht im Supermarkt einkaufen, der über neue Einkaufswagen mit Bildschirmen und Computern verfügt. Auf dem Bildschirm wird Frau Meier entsprechend ihrer Einkaufsliste durch das Geschäft geleitet. Die Preise der jeweiligen Produkte werden nicht mehr im Regal ausgewiesen, sondern auf dem Bildschirm angezeigt. Außerdem ist der Computer mit einem RFID-Lesegerät ausgestattet und kann so Frau Meiers Kundenkarte auslesen. Auf Grund der angefallenen Daten kann der Einkaufswagen die Preise an das Kundenprofil anpassen. Er setzt die Preise für Süßigkeiten und Toilettenpapier um einige Prozent höher, oder bietet Frau Meier einen Rabatt an, damit sie das teurere Make-up ausprobiert. Der Einkaufswagen kann auf ältere Datenbestände zurückgreifen und so erkennen, dass nach einer „Preiserhöhung“ für Frau Meier vor zwei Wochen ein bestimmtes Produkt nicht mehr gekauft wurde. Daher kann er dieses nun im Preis wieder senken. (Computer Zeitung 2004 A) (BigBrotherAwards 2003)

Beispiel: Den Verbrauchern droht auch Diskriminierung auf Grund von Krankheiten. Beispielsweise kann, wie erwähnt, problemlos erkannt werden, dass ein Mensch eine Schnapsflasche oder bestimmte Medikamente gegen eine schwere Krankheit, wie Migräne oder Asthma, bei sich trägt. Bei einem Bewerbungsgespräch, in der Bank oder bei Versicherungen könnten kranken Verbrauchern dadurch Nachteile entstehen, da ihnen die Lebensversicherung, der Existenzgründungskredit oder der Job vorenthalten wird. (BigBrotherAwards 2003)

Ob für ein solches Szenario eine gesetzliche Grundlage besteht, soll an dieser Stelle nicht weiter betrachtet werden. Die Erfahrung zeigt, dass technische Möglichkeiten häufig umgesetzt werden, sofern sich davon ein Nutzen erhofft wird.

Auch wenn das Datenschutzgesetz die Möglichkeit der Korrektur von falschen Daten vorsieht, wird dessen Umsetzung in Zeiten von RFID kaum möglich sein. Elementares Problem ist dabei, dass der einzelne Verbraucher nicht weiß, wo welche Daten über ihn angefallen sind, wo diese gespeichert werden und an wen diese weitergegeben wurden. Insbe-

sondere tritt diese Problematik zu Tage, wenn Daten aus unterschiedlichen Quellen verknüpft werden. Praktisch hat der Verbraucher dadurch kaum noch die Möglichkeit falsche Daten korrigieren zu können, oder anders reglementierend auf diese einzuwirken.

Ergebnis: Aus technischer und ökonomischer Sicht wird die RFID-Technik individuelle Preise auf Kosten des Verbrauchers nach sich ziehen. Es ist zu erwarten, dass sich die Industrie für eine entsprechende rechtliche Regelung einsetzen wird.

3.5 WIRD DER VERBRAUCHER DURCH GELTENDES RECHT GESCHÜTZT?

Die gesetzlichen Datenschutzgesetze und -Mechanismen in Deutschland stammen aus der Zeit, als es große Zentralrechneranlagen gab und PCs, Vernetzung, Internet und RFIDs unvorstellbar waren. Der sich rasant entwickelnden RFID-Technik sind diese Datenschutzmechanismen daher nicht mehr gewachsen. Sie verbieten beispielsweise *nicht* das Auslesen der RFIDs von fremden Personen oder das Erstellen von Bewegungsprofilen. Fatale Folgen könnte eine **EU-Richtlinie** nach sich ziehen, die das Deaktivieren, Entfernen oder Zerstören von RFIDs durch Verbraucher und Verkaufsstellen generell verbieten würde. (Heise 2004 A)

Ergebnis: Von rechtlicher Seite ist der Verbraucher nicht ausreichend geschützt; im Gegenteil ist mit einer erschreckenden Verschärfung der Rechtslage zu Lasten der Verbraucher zu rechnen.

Es ist fraglich, inwieweit für den Verbraucher Nachteile entstehen werden, wenn er Ware mit deaktiviertem RFID umtauschen oder Garantieansprüche wahrnehmen möchte. (Weis 2003)

3.6 IST MIT EINER KUNDENFREUNDLICHEN REGELUNG DER WIRTSCHAFT ZU RECHEN?

Die RFID-verwendende Wirtschaft behauptet häufig, dass es mit RFID keine Einschnitte in die Privatsphäre der Verbraucher gäbe und sie dem Datenschutz eine hohe Bedeutung zumisst. Andererseits werden aber Sachverhalte publik, die diese Aussage wenig glaubwürdig erscheinen lassen. Beispielsweise wurden in einigen Supermärkten zur Bekämpfung des Ladendiebstahls heimlich alle Verbraucher fotografiert, die mit RFID ausgestattete Rasierklingen aus dem Regal nahmen, ohne sie darüber zu informieren. (Heise 2003 F) Darüber hinaus wird die RFID-Technik in der Praxis kaum gekennzeichnet und die Kunden über deren Einsatz kaum informiert. (FoeBuD 2004) Interne Dokumente des weltweiten RFID-Interessenverbandes AutoID-Center belegen eine Desinformationskampagne gegen Verbraucherschutz- und Bürgerrechtsorganisationen (Auto-ID Center 2002) und stehen damit nicht allein (Albrecht 2004). Diese Vorfälle lassen an den verbraucherfreundlichen Interessen der Industrie zweifeln.

Es gibt viele Fälle, in denen Unternehmen auf Grund von öffentlicher Kritik an der RFID-Anwendung die Verwendung der Technik einstellten oder zu einer verbraucherfreundlichen Praxis übergangen. Dies zeigt, dass eine verbraucherfreundliche Politik der Wirtschaft durchaus in ihrem eigenen Interesse liegen sollte.

Ergebnis: Zu ihrem eigenen Nachteil verfolgt die Industrie beim Einsatz von RFID keine verbraucherfreundliche Politik.

3.7 WIE BEURTEILEN VERBRAUCHER DIE DATENSCHUTZPROBLEME?

Es gibt eine Untersuchung, die unter Verbrauchern bezüglich dieses Themas vorgenommen wurde. Die befragten Personen lasen einen informativen Text über die RFID-Technik und wurden anschließend über ihre möglichen Befürchtungen befragt. Die Studie ergab, dass 55% der Befragten in der RFID-Technik eine Gefahr für ihre eigene Privatsphäre sahen. (Subcommittee 2003)

Es sei an dieser Stelle nur kurz erwähnt, dass die Befürchtungen der Kunden um ihre Privatsphäre oder Datenschutz entscheidend für den wirtschaftlichen Erfolg einer Technik sein kann. (Cantwell 2003)

Ergebnis: Datenschutz wird von Verbrauchern als wichtig betrachtet und kann für den wirtschaftlichen Erfolg oder Misserfolg neuer Technologien entscheidend sein.

3.8 WELCHE ZUKÜNFTIGEN ENTWICKLUNGEN WIRD ES GEBEN?

Die Verwendung von RFIDs wird in Zukunft zunehmen, neue Einsatzmöglichkeiten entwickelt und neue Anwendungsfelder erschlossen werden. Bereits heute werden RFIDs in Personaldokumenten eingesetzt (Heise 2003 E). Die Europäische Zentralbank denkt über die Integration in Geldscheinen nach. (Albrecht 2004) (Heise 2001) Selbst das Implantieren von RFIDs für Kreditkartenanwendungen ist möglich, wird bereits heute vorgenommen (Heise 2003 B) und könnte in Zukunft größere Verbreitung finden. Zukünftige Verwendung von Lesegeräten innerhalb von Privatwohnungen wird neue Überwachungsmöglichkeiten eröffnen. (Albrecht 2003)

Ergebnis: Die RFID-Technik und -Anwendung ist ständiger Weiterentwicklung unterworfen. Es ist daher nicht abzusehen, wozu RFIDs in fernerer Zukunft eingesetzt werden (können).

4. LITERATURVERZEICHNIS

Albrecht 2003: Katherine Albrecht, Tracking everything, everywhere, 2003, http://spychips.com/rfid_overview.htm

Albrecht 2004: Katherine Albrecht, CASPIAN Newsletter 12.01.2004

Auto-ID Center 2002: Auto-ID Center, Managing External Communications, 2002, http://quintessenz.org/rfid-docs/www.autoidcenter.org/media/external_comm.pdf

BigBrotherAwards 2003: BigBrotherAwards Deutschland. Kategorie Verbraucherschutz, 2003,

Borchers 2001: Detlef Borchers, Plaudertaschen in der Gepäckabfertigung Transponder erhöhen die Sicherheit auf Flughäfen, Artikel. In: NZZ Online - Medien · Informatik, 28. September 2001, <http://www.nzz.ch/2001/09/28/em/page-article7OIYN.html> [15. Feb 2004]

BVG 1983: Urteil des BVG vom 15.12.1983; Az.: 1 BvR 209/83; NJW 84, 419

Cantwell 2003: Brian Cantwell, Why Technical Breakthroughs Fail, 2003

Computer Zeitung 2004 A: rr, Objekte werden schlau, 2004

c't 2004: Angela Meyer, Lückenlos dokumentiert, 2004

Finkenzeller 1998: Klaus Finkenzeller, "Kontaktlose Chipkarten", Artikel aus der Funkschau - Heft 19/1998 S.40-43, 1998, <http://www.rfid-handbook.de/downloads/fs9819040.pdf> [15. Feb 2004]

Finkenzeller 2002: Finkenzeller, Klaus, Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 2002

Finkenzeller 2003: Klaus Finkenzeller, Standardization of RFID, 2. Oktober 2003, <http://www.rfid-handbook.de/rfid/standardization.html> [15. Feb. 2004]

FoeBuD 2004: FoeBuD e.V., FoeBuD deckt auf: Versteckte RFID in Metro-Payback-Kundenkarte, 2004,

Füßler 2002: Dr. Andreas Füßler, EAN-RFID - Ein neuer Standard steht zur Wahl Automatisch Daten erfassen - aber richtig!. In: EAN·UCC · Centrale für Coorganisation (CCG), März 2002, http://www.ccg.de/Magazin/coorganisation/32002/c302_38.pdf [15. Feb 2004]

Garfinkel 2004: Simon L. Garfinkel, The Trouble with RFID, Artikel. In: The Nation (2004), 3. Februar 2004, <http://www.thenation.com/doc.mhtml?i=20040216&s=garfinkel> [15. Feb 2004]

Gatzke 2003: Gatzke, Monika, RFID-Tags: Alles wird anders, 2003

Gfaller 2003: Hermann Gfaller, Big Brother is watching you!, 2003

Glasmacher 2003: Alexander Glasmacher, RFID in der Praxis Produkte und Anwendungen, Präsentation, 6. Juni 2003, https://dienst.cognid.de/pub/bscw.cgi/d1627494/G3_IDSsystems_Glasmacher.pdf [15. Feb 2004]

Heise 2001: Dr. Wolfgang Stieler, Identifikations-Chips für Euro-Banknoten geplant, 2001, <http://www.heise.de/newsticker/meldung/23559>

Heise 2003 B: Andreas Wilkens, RFID-Chip als implantierte Kreditkarte, 2003, <http://www.heise.de/newsticker/data/anw-26.11.03-004/>

Heise 2003 C: Wolfgang Stieler, Waschbare elektronische Etiketten von Texas Instruments, 2003, <http://www.heise.de/newsticker/data/wst-12.08.03-003/>

Heise 2003 D: Clemens Gleich, Transponder in Benetton-Wäsche, 2003, <http://www.heise.de/newsticker/data/cgl-13.03.03-000/>

Heise 2003 E: Detlef Borchers, CAST-Forum: Passvergrößerung gefragt, 2003, <http://www.heise.de/newsticker/data/jk-23.10.03-007/>

Heise 2003 F: pmz, Gillette will von Bespitzelung durch RFID-Tags nichts wissen, 2003, <http://www.heise.de/newsticker/data/pmz-15.08.03-000/>

Heise 2004 A: Jürgen Kuri, Datenschützer übt massive Kritik an Copyright-Richtlinie der EU, 2004

Hillenbrand 2003: Hillenbrand, Thomas, Smart-Chip-Risiken: Der Feind in meinem Schuh,

I.D. Systems AG 2003: I.D. Systems AG, Reichweitensysteme, 2003, <http://www.idsystems-ag.de/de/reichweite-rfid.php> [15. Feb. 2004]

Juels, Rivest, Szydlo 2003: Ari Juels, Ronald L. Rivest, und Michael Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: RSA Security (2003) - RSA Laboratories, 2003, <http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/index.html> [15. Feb 2004]

Kleinwaechter 2003: Kleinwaechter, Wolfgang, Wunderwaffe gegen Diebstahl: Das Ende vom Anfang oder der Anfang vom Ende?, 2003

nhe 2004: nhe, VeriSign mit weltweiter RFID-Adressierung beauftragt. In: heise online (2004). - heise newsticker, 13. Januar 2004, <http://www.heise.de/newsticker/meldung/43570> [15. Feb 2004]

Ostler 2003: Ulrike Ostler, Der Chip im Ohr lässt Rinder mit Datenbanken sprechen. In: ZDNet (2003). - ZDNet IT Manager, 7. Juli 2003, <http://www.zdnet.de/itmanager/tech/0,39023442,2137121,00.htm> [15. Feb 2004]

Pichet 2003: Pichet, Anne, Alle wollen die kleinen "Alleskönner", 2003

RFID Journal 2004: , NCR Prototype Kiosk Kills RFID Tags, 2004

Subcommittee 2003: , Hearing on RFID and Privacy. Testimony of Kevin Ashton, 2003

Time 2003: Cathy Booth-Thomas, The See-It-All Chip, 2003

Trautner 2002: Stefan Trautner, Radiofrequenz-Identifikation in der Supply Chain, Präsentation, Juni 2002, [http://www.competence-site.de/pps.nsf/4B222B598931FB88C1256C4C00451BFD/\\$File/rfid.pdf](http://www.competence-site.de/pps.nsf/4B222B598931FB88C1256C4C00451BFD/$File/rfid.pdf) [15. Feb 2004]

Weis 2003: Stephen August Weis, Security and Privacy in Radio-Frequency Identification Devices, 2003

Wikipedia 2004 A: Wikipedia, die freie Enzyklopädie, EAN, 28. Januar 2004, <http://de.wikipedia.org/wiki/EAN> [15. Feb 2004]

Wikipedia 2004 B: Wikipedia, die freie Enzyklopädie, Elektronischer Produkt Code, 28. Januar 2004, http://de.wikipedia.org/wiki/Elektronischer_Produkt_Code [15. Feb 2004]

Wikipedia 2004 C: Wikipedia, die freie Enzyklopädie, RFID, 30. Januar 2004, <http://de.wikipedia.org/wiki/RFID> [15. Feb 2004]

Wikipedia 2004 D: Wikipedia, die freie Enzyklopädie, Transponder, 19. Januar 2004, <http://de.wikipedia.org/wiki/Transponder> [15. Feb 2004]

Windeck 2004: Christof Windeck, Der Electronic Product Code soll den Strichcode ablösen. In: heise online (2004). - heise newsticker, 12. Januar 2004, <http://www.heise.de/newsticker/meldung/43557> [15. Feb 2004]

Wenn nicht anders vermerkt, sind alle Links am 16.02.2004 überprüft worden.

Die verwendeten Grafiken auf Seite 5 stammen aus Füller 2002, die auf Seite 15 und 17 von Spiegel Online.