

Universität Karlsruhe (TH)

Fakultät für Informatik  
IPD - Lehrstuhl Prof. Böhm

Seminararbeit

# RFID und Privatheit

**Im Rahmen des Seminars:** Sicherheit und technischer Datenschutz  
in Informationssystemen

**eingereicht von:** Christoph Balling <Christoph.balling@web.de>

**eingereicht am:** 16. November 2006

**Betreuer:** Mirco Stern

## 1 Einleitung

Die RFID-Technik kann den Alltag erleichtern. Benutzer der Universitätsbibliothek in Karlsruhe [13] profitieren von dieser Technik schon heute dadurch, dass sie jederzeit Bücher entleihen und zurückgeben können. Die Ersetzung des Strichcodes in den Büchern durch RFID-Transponder erlaubt dabei die Identifikation aller für die Nutzer zugänglichen Bücher. Im Verbund mit dem Transponder im Bibliotheksausweis wird dadurch der Verleih der Bücher realisiert. Wenn ein Nutzer die Bibliothek mit einem nicht ausgeliehenen Buch verlassen will, erkennen dies RFID-Lesegeräte vor den Türen und ein Alarm wird ausgelöst.

Diese neue Technik birgt jedoch auch Risiken. Unberechtigte Dritte könnten durch Aufstellen von Lesegeräten herausfinden, welche Bücher ein Bibliotheksbenutzer mit sich führt. Beispielsweise könnte ein Chemie-Student, welcher eine Seminararbeit über Sprengstoffe und deren Funktionsweise schreibt, am Flughafen aufgehalten werden, da in seinem Rucksack "verdächtige Bücher" entdeckt wurden.

Um Privatheit herzustellen, stellt sich die Frage, wie man die eindeutige Nummer auf dem RFID-Tag vor unerlaubtem Zugriff schützen kann.

RFID steht für Radio Frequency Identification. RFID-Systeme bestehen aus Lesegeräten und Transpondern. Transponder haben eine eindeutige Nummer, welche von Lesegeräten ohne Sichtkontakt ausgelesen werden kann. Die Transponder lassen sich bereits heutzutage in der Größe eines Sandkorns bauen, was es ermöglicht, diese auf Tieren, Menschen oder sogar auf sehr kleinen Gegenständen anzubringen.

Positiv wird RFID derzeit insbesondere im Handel gesehen, da man mit Hilfe dieser Technologie Warenströme kostengünstiger und besser steuern kann. Beispielsweise kann beim Wareneingang die neue Ware schnell erkannt werden und somit ohne Zeitverlust an die vorgesehenen Stellen geleitet werden.

Doch man sollte beachten, dass diese Technologie auch Gefahren mit sich bringt. So könnte durch die RFID-Technologie die Privatheit von Personen verloren gehen. Für Privatheit werden oft mehrere Begriffe wie Privatsphäre oder Informationelle Selbstbestimmung verwendet. In meiner Seminararbeit werde ich diese Begriffe als Synonyme verwenden. Samuel Warren und Lois Brandeis definierten im Jahre 1890 Privatheit folgendermaßen:

"Privatheit ist das Recht alleine gelassen zu werden"[11]

Privatheit ist im Hinblick auf die RFID-Technologie das Recht, dass der Einzelne selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen kann.

Der Benutzer des RFID-Transponders befindet sich hierbei in einem Dilemma: Auf der einen Seite sollen für den Benutzer Prozesse handhabbar ablaufen, das heißt ohne dass der Anwender explizit jeweils die Herausgabe seiner Informationen einzeln bestätigen muss. Auf der anderen Seite will er die Kontrolle haben, an wen die Informationen seines RFID-Transponders preisgegeben werden. Der Benutzer kann in einem komplexen Datennetz nicht mehr kontrollieren, welche

Informationen zu anderen übermittelt werden und wie die Informationen benutzt werden.

Durch die RFID-Technologie entstehen neue Anforderungen an den Gesetzgeber, da der derzeitige Rechtsrahmen den Schutz der Privatheit ohne Anpassungen an diese neue Technologie nicht gewährleistet. Diese Seminararbeit zeigt auf, dass das Recht dem rasanten Wandel der Technologie nur mit zeitlicher Verzögerung folgen kann. Eine Anpassung an diese veränderten Gegebenheiten kann durch Maßnahmen wie das Datenschutzaudit erreicht werden.

In Deutschland wird mit dem Grundrecht der Informationellen Selbstbestimmung dem Bürger ein Instrument an die Hand gegeben, welches ihn gegen unangebrachte Eingriffe in seine Privatheit schützen soll. Die Anwendung dieses Instruments ist jedoch kompliziert, da nicht immer offensichtlich ist, ob es sich um einen angebrachten oder einen unangebrachten Eingriff handelt. Dieses Problem wird in dieser Arbeit anhand des Rasterfahndungsurteils veranschaulicht. Neben dem rechtlichen Rahmen müssen auch auf technischer Seite alle Möglichkeiten ausgeschöpft werden, Eingriffe in die Privatheit zu verhindern. Bedrohungen dabei sind vor allem unbemerktes Auslesen, Verfolgbarkeit, Erkennbarkeit sozialer Netzwerke, Objektverantwortlichkeit, Technologiepaternalismus und Personalisierung. Im Laufe dieser Arbeit werden wir im Detail auf diese Probleme eingehen. Technische Verfahren, den Privatheitsschutz herzustellen, sind beispielsweise das Clipped-Tag-Verfahren oder das Killer-Tag-Verfahren. Bei Letzterem wird der RFID-Transponder durch eine software- oder hardwaretechnische Lösung nicht mehr auslesbar gemacht. Eine genauere Darstellung dieser sowie weitere Verfahren und deren Beurteilung bilden den letzten Schwerpunkt dieser Seminararbeit.

In Kapitel 2 werde ich auf den momentan existierenden rechtlichen Rahmen eingehen. Zunächst werde ich hierbei einen Abriss über das europäische Datenschutzrecht geben, bevor ich auf die nationalen rechtlichen Gegebenheiten eingehe. Am Ende zeige ich noch eine Möglichkeit auf, wie die Privatheit mit Hilfe einer Selbstregulierung geschaffen werden kann.

Die Vorteile der RFID-Technologie werden anhand von ausgewählten Anwendungsbeispielen in Kapitel 3 behandelt. In Kapitel 4 werden verschiedene Risiken beim Einsatz der RFID-Technologie beleuchtet.

Technische Möglichkeiten zur Sicherstellung der Privatheit werde ich in Kapitel 5 aufgreifen.

## **2 Rechtlicher Rahmen der RFID-Technologie**

### **2.1 Die Entwicklung des europäischen Datenschutzrechts**

Die Technologie und das Recht sind voneinander abhängig. Durch das Recht wird die Anwendung einiger Technologien erst ermöglicht, wie beispielsweise die elektronische Signatur.

Bei einem Rückblick auf die letzten Jahrzehnte, erkennt man, dass sich die

Technik der Datenverarbeitung in einem rasanten Wandel befindet. In den 70er Jahren wurde Datenverarbeitung überwiegend in Rechenzentren betrieben. In den 80er Jahren gab es eine Datenverarbeitung auch an verteilten PCs. Im nächsten Jahrzehnt fand die Datenverarbeitung mit Hilfe des World Wide Web weltweit statt. Momentan beobachtet man eine zunehmende Informatisierung und Vernetzung physischer Dinge. Diesem schnellen Wandel kann der rechtliche Rahmen meist nicht folgen, da momentane Gesetzgebungsverfahren durch Mitwirkung vieler Verfassungsorgane eine längere Zeit benötigen. Die RFID-Technologie ermöglicht die Anwendung neuer Prozesse, die auf der Identifikation von Objekten basieren. In momentanen Gesetzen werden die Rahmenbedingungen, welche durch neue Prozesse geschaffen wurden, oft noch nicht berücksichtigt. Der Gesetzgeber versucht durch Datenschutzgesetze die Datenverarbeitungen für betroffene Personen transparenter zu gestalten. Transparenz ist insbesondere bei der RFID-Technik nicht einfach herzustellen, da diese Technik meist für den Benutzer im Hintergrund abläuft.

Im Gegensatz zu den USA ist der Schutz der Privatheit keine Verhandlungssache, sondern eine Grundfreiheit. Durch unterschiedliche Verwaltungs- und Rechtsvorschriften in den einzelnen Mitgliedsstaaten der Europäischen Union gibt es jedoch noch einmal Unterschiede im Niveau des Schutzes dieser Grundfreiheit. Damit diese unterschiedlichen Schutzniveaus der einzelnen Mitgliedsstaaten kein Hemmnis für die Ausübung einer Reihe von Wirtschaftstätigkeiten in Europa darstellt, ist eine stete europäische Harmonisierung notwendig.

Die Grundfreiheit des Schutzes personenbezogener Daten ist in Artikel 8 der Charta der Grundrechte der Europäischen Union festgehalten:

1. Jede Person hat das Recht auf Schutz der sie betreffenden 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.

Es ist geplant, dass die Charta in die künftige europäische Verfassung eingeht. Wenn in 3 Jahren beispielsweise die Europäische Verfassung in Kraft tritt, ist die Europäische Charta für alle Europäer unmittelbar geltendes Recht.

Diese Absichten des Artikels 8 der Charta der Grundrechte der Europäischen Union wurden bereits in einigen Richtlinien aufgegriffen. Richtlinien sind inhaltliche Vorgaben, welche von den einzelnen Mitgliedstaaten in ihr nationales Recht umzusetzen sind. Die EG-Datenschutzrichtlinie 95/46/EG<sup>1</sup> regelt in Artikel 1 Nummer 1 den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Artikel 20 der EG-Datenschutzrichtlinie verlangt von den Mitgliedsstaaten eine Festlegung darüber, welche Datenverarbeitung zuerst von einer Kontrollstelle oder dem internen Datenschutzbeauftragten geprüft werden müssen und sieht somit eine Vorabkontrolle für bestimmte Bereiche der Datenverarbeitung vor.

<sup>1</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT>

Es erweist sich insbesondere bei der RFID-Technologie als besonders schwierig, die Datenverarbeitung durch geeignete Gesetzesvorgaben transparenter zu gestalten, da diese Technologie eine unsichtbare Einbettung von Computertechnik in den Alltag ermöglicht. Des Weiteren hat der rechtliche Rahmen die Schwierigkeit, dem rasanten Fortschritt in der Datenverarbeitung zu folgen. Allein durch einen rechtlichen Rahmen einen Schutz der Privatsphäre zu gewährleisten scheint aus den genannten Gründen somit nicht realisierbar zu sein. Ergänzend könnte man den Schutz der Privatsphäre durch technische Schutzmechanismen herstellen, welche ich in Kapitel 5 vorstelle.

## 2.2 Informationelle Selbstbestimmung in Deutschland

Informationelle Selbstbestimmung ist in Deutschland im Grundgesetz im Artikel 2 in Verbindung mit Artikel 1 Absatz 1 geregelt. Informationelle Selbstbestimmung gibt die Befugnis, selbst über die Preisgabe und Verwendung von personenbezogenen Daten zu bestimmen. Grundrechtsträger ist jede natürliche Person, das heißt auch Ausländer haben dieses Recht. Neben der Kommunikationsfreiheit ist die Informationelle Selbstbestimmung ein zentrales Grundrecht in der Informationsgesellschaft. Es ist ein eigenständiges Grundrecht und nicht subsidiär gegenüber anderen Grundrechten.

Das Grundrecht auf Informationelle Selbstbestimmung dient als Abwehrrecht gegenüber hoheitlichem Handeln. Hoheitlich bedeutet, dass zwischen Behörde und Bürger ein gewisses "Über-Unterordnungsprinzip" besteht. Ein Beispiel für ein hoheitliches Handeln sind verabschiedete Gesetze oder ein beschlossener Verwaltungsakt.

Informationelle Selbstbestimmung besitzt auch Schranken. Wenn der Staat beispielsweise zum Erreichen eines zulässigen Zwecks auf eine Datenverwendung nicht verzichten kann, ist eine staatliche Datenverwendung erlaubt. Diese hoheitliche Datenverwendung darf jedoch nur in dem Maß stattfinden, in welchem es erforderlich ist. Der Bürger muss somit Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Ob das allgemeine Interesse dem Grundrechtseingriff überwiegt, ist dann der entscheidende Punkt. Welche Seite hierbei stärker ins Gewicht fällt, ist keine einfache Frage, was beispielsweise die Uneinigkeit der Bundesverfassungsrichter beim Urteil über die Rasterfahndung<sup>2</sup> zeigt. Bei dem Urteil im Mai 2006 ging es um die Frage, ob durch die Terrorgefahr, die insbesondere seit dem 11. September 2001 gegeben war, Datenbanken der Universitäten, Einwohnermeldeämtern und Ausländerzentralregister miteinander verknüpft werden dürfen, um so genannte „Schläfer“ ausfindig zu machen. Hier entschieden zwei der acht Bundesverfassungsrichter, dass das Allgemeininteresse überwiegen würde und somit ein Eingriff in die Privatheit des Bürgers gerechtfertigt sei. Bundesverfassungsrichterin Haas, welche zuletzt Genanntes befürwortet, war der Auffassung, dass der Staat mit der Sicherheit zugleich auch die Freiheit des Einzelnen gewährleisten solle,

<sup>2</sup> <http://www.bundesverfassungsgericht.de>

denn Sicherheit sei Grundlage der Freiheit und deshalb Teil derselben. Demgegenüber seien die zur Stärkung der Freiheit durch die Rasterfahndung notwendigen Eingriffe in Grundrechte der Betroffenen von nur geringem Gewicht. Die Maßnahme der Rasterfahndung sei ein Eingriff von minderer Intensität schon deshalb, weil nur solche Daten erfasst und abgeglichen würden, die bereits vom Betroffenen offenbart und in Dateien mit seiner Kenntnis gespeichert worden seien. Die Bedrohungslage für eine terroristische Gefahr sei hinreichend. Eine Gewährleistung von Sicherheit und Freiheit habe ein höheres Gewicht als die hinzunehmenden Beeinträchtigungen einer Rasterfahndung. Der Rechtsstaat erfahre durch diese Entscheidung, welche das Abwehrrecht bejaht, keine Stärkung, sondern die Rasterfahndung mache den Staat gegenüber drohenden Terrorangriffen wehrlos [12].

Die Senatsmehrheit folgte diesen Argumenten nicht und sah die informationelle Selbstbestimmung der betreffenden Bürger verletzt. Die allgemeine Bedrohungslage reiche nicht aus, um dem Bürger das Recht auf Privatsphäre zu entziehen.

Im Bundesdatenschutzgesetz<sup>3</sup> (BDSG) ist der Schutz der Privatsphäre genauer als im Grundgesetz geregelt. So kommt dieses Gesetz beispielsweise zur Anwendung, wenn es um die Erhebung oder Verarbeitung von personenbezogenen Daten geht, welche durch die Identifikation mit Hilfe von Funkwellen gewonnen wurden. Nach Paragraph 1 Absatz 1 BDSG ist Zweck dieses Gesetzes, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Personenbezogene Daten sind gemäß § 3 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person. Der Schutzbereich der informationellen Selbstbestimmung bezieht sich hierbei nicht nur auf Daten die eine Person eindeutig identifizieren, sondern auch auf personenbeziehbare Daten. Personenbeziehbare Daten sind Einzelangaben, die eine bestimmte Person zwar nicht eindeutig identifizieren, deren Identität aber mit Hilfe anderer Informationen feststellbar ist. Insbesondere ist dies oft durch das Verknüpfen mehrerer Daten möglich.

Gemäß § 4 Absatz 1 BDSG dürfen personenbezogene Daten nur erhoben, verarbeitet und genutzt werden, wenn eine Einwilligung der betroffenen Person vorliegt oder eine Rechtsvorschrift dies erlaubt. Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er nach § 19a BDSG von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten in Kenntnis zu setzen, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

Nach § 19 und § 20 BDSG hat jede Person das Recht Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

---

<sup>3</sup> <http://www.gesetze-im-internet.de>

Für den Verbraucher ist es schwierig zu der Kenntnis zu gelangen, welches Unternehmen überhaupt personenbezogene Informationen von ihm gespeichert hat, um diese dann um Auskunft zu bitten oder die Daten löschen zu lassen. Einige enge Ausnahmen regelt § 28 des Bundesdatenschutzgesetzes. So ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel beispielsweise für die Erfüllung eigener Geschäftszwecke zulässig, falls es der Zweckbestimmung eines Vertragsverhältnisses dient. Die Nutzung von RFID wird vom Bundesdatenschutzgesetz erfasst, sobald personenbezogene Daten verarbeitet werden. Das Gesetz schützt personenbezogene Daten gemäß § 3 Absatz 1 BDSG und das Speichern und das Nutzen personenbezogener Daten bedarf einer Einwilligung des Betroffenen nach § 4 Absatz 1 BDSG.

### 2.3 Datenschutzaudit

Damit die neue Technologie auch beim Verbraucher Anwendung findet, muss der Nutzen für ihn größer sein als die Risiken, welche er mit dieser Technologie eingeht. Für den Verbraucher ist es wichtig eine einfache Übersicht zu haben, welche Unternehmen mit der RFID-Technologie behutsam umgehen. Durch Wahl solcher Unternehmen könnte er die Wahrscheinlichkeit reduzieren seinen Privatheitsschutz zu verlieren. Das Datenschutzaudit bietet hierbei eine Möglichkeit, die Unternehmen in 2 Klassen einzuteilen. Die rechtliche Grundlage für dieses Verfahren findet sich in § 9a BDSG. Beim Datenschutzaudit wird das Unternehmen extern überprüft. Unternehmen, welche vorgegebene Regeln, wie Datenvermeidung, Datensparsamkeit und Datensicherheit, einhalten, erhalten das Datenschutzauditzeichen, siehe Abbildung 1. Artikel, welche mit solch einem Zeichen versehen sind, könnten bevorzugt von den Verbrauchern gewählt werden, da sie bei diesen einen Verlust des Schutzes auf Privatheit mit hoher Wahrscheinlichkeit nicht befürchten müssen. Die Bevorzugung solcher ausgezeichneten Produkte schafft für Unternehmen den Anreiz ihr Unternehmen zertifizieren zu lassen. Um zertifiziert zu werden, müssen sie dazu meist eine Reihe von Veränderungen in ihrer Datenverarbeitung vornehmen. Der Vorteil bei diesem Verfahren ist, dass hier der Staat nicht selbst die Einhaltung überprüfen muss. Die Selbstregulierung mit Hilfe des Datenschutzaudits ist ein Instrument, welches auf verändernde Situationen schnell reagieren kann und nicht erst durch langjährige Gesetzgebungsverfahren den passenden Rechtsrahmen hierfür schaffen muss. Zielsetzung des Datenschutzaudits ist die Verbesserung des Datenschutzes, aber auch der Datensicherheit durch die freiwillige Überprüfung der datenschutzrechtlichen Eignung von Produkten und Datenschutzkonzepten. Das unabhängige Landeszentrum für Datenschutz Schleswig Holstein<sup>4</sup> ist momentan das einzige Institut welches dieses Verfahren anwendet.

---

<sup>4</sup> <http://www.datenschutzzentrum.de/index.htm>



Abbildung 1. Das Datenschutzauditzeichen von Schleswig Holstein

### 3 Die RFID-Technologie

#### 3.1 Unterschiedliche Transponder

Radio Frequency Identification bedeutet eine drahtlose Übertragung<sup>5</sup> von Informationen zwischen einem Transponder und einer Basisstation. Bei dieser Arbeit betrachte ich nur den Aspekt, dass der RFID-Transponder eine eindeutige Identifikationsnummer an das RFID-Lesegerät überträgt.

Je nach Anwendung sollte man unterschiedliche Transponder und Frequenzen verwenden. Bei den Transpondern unterscheidet man passive, semiaktive und aktive Transponder. In dieser Reihenfolge erhöht sich auch ihre Reichweite; bei aktiven Transpondern beträgt diese bis etwa 100 Meter. Der passive Transponder besitzt keine eigene Batterie. Der semiaktive versorgt seinen Transponder mit einer Batterie. Und der aktive Transponder kann zusätzlich mit seiner Batterie auch selbst mit dem Lesegerät kommunizieren.

Des Weiteren kann man diese auf unterschiedlichen Frequenzen betreiben. Je nach Frequenz haben diese noch einmal unterschiedliche Eigenschaften. Niedrigere Frequenzen haben den Vorteil, dass die Wellen Wasser einfacher durchdringen können. Im Gegensatz dazu haben hohe Frequenzen größere Lesedistanzen und können mehr Daten pro Zeiteinheit übertragen. Für viele Anwendungsfelder sind passive Transponder mit niedriger Frequenz sinnvoll, da sie zum einen preiswert herzustellen sind und durch die niedrige Frequenz eine niedrigere Fehleranfälligkeit gegenüber wechselnden Umgebungen haben. Die Tatsache, dass passive Transponder nur kurze Lesereichweiten besitzen, ist oft sogar ein Vorteil. An den Eingangsbereichen bei Skiliften ist es zum Beispiel wichtig, den Transponder von der richtigen Person, welche direkt vor dem Drehkreuz steht, auszulesen und nicht den Transponder der Person dahinter. Zur eindeutigen Identifikation wäre es daher sinnvoll einen passiven Transponder mit einer niedrigen Frequenz zu wählen, damit die Lesereichweite sehr kurz ist und die Fehleranfälligkeit, welche durch Schnee zwischen Transponder und Lesegerät verstärkt werden kann, in Grenzen gehalten wird. Wie dieses Beispiel zeigt, ist

<sup>5</sup> mittels Nutzung von Radiowellen

ein teurer aktiver Transponder mit der einhergehenden größeren Reichweite nicht immer sinnvoll.

### 3.2 Erfolgsfaktoren des RFID-Einsatzes

Wie schnell sich die RFID-Technologie künftig ausbreiten wird, hängt von mehreren Faktoren ab. Zum einen erhöht sich der Nutzen wenn ein RFID-Transponder in der kompletten Wertschöpfungskette eines Produktes Anwendung findet. Durch einen lückenlosen RFID-Einsatz in der Wertschöpfungskette vom Hersteller bis zum Einzelhändler erwartet man sich eine insgesamt transparentere Wertschöpfungskette. Beispielsweise kann man hierdurch Engpässe der Zulieferindustrie früher erkennen und durch eingeleitete Gegenmaßnahmen anders als unter Verwendung eines Barcodes häufiger einen Stillstand des Bandes verhindern. Hierzu müssen jedoch erst einmal Vereinbarungen über die genauere Ausgestaltung, wie beispielsweise die verwendete Frequenz und wie die Kosten der RFID-Technologie, verteilt werden, die zwischen den unterschiedlichen Unternehmen gemacht werden. Teilweise machen größere Unternehmen<sup>6</sup> Vorgaben, wie Produkte vom Zulieferer mit RFID-Transpondern zu versehen sind. Unternehmen mit entsprechender Marktmacht werden künftig die Verbreitung des RFID-Einsatzes wesentlich bestimmen.

Bei den RFID-Komponenten beobachtet man einen Preisverfall. Gerade wenn RFID-Transponder in Massen hergestellt werden, sind die Kosten meist kein entscheidendes Hindernis mehr, RFID-Transponder einzusetzen. Im Jahre 2006 werden rund eine halbe Milliarde Transponder hergestellt. Bis 2015 soll sich die Zahl laut Forschungsinstituten auf eine Billionen Transponder pro Jahr erhöhen<sup>7</sup>, was im Durchschnitt 150 RFID-Transponder pro Bürger bedeuten würde.

Die RFID-Verbreitung wird auch entscheidend vom Verbrauchervertrauen abhängig sein. Oft zögern Menschen Artikel zu verwenden, welche mit einem RFID-Transponder versehen sind. Verbraucherverbände bündeln diese Bedenken der Verbraucher und tragen diese an die Öffentlichkeit. In der Vergangenheit zeigte sich, dass Verbraucherverbände eine nicht zu unterschätzende Rolle für die Verbreitung der RFID-Technologie besitzen. Verbraucherverbände könnten beispielsweise durch Boykottaufrufe RFID-Einsätze rückgängig machen<sup>8</sup>.

Es ist deswegen unabdingbar, dass die Firmen, welche einen RFID-Einsatz planen, in einen offenen Dialog mit den Verbrauchern treten und schon im Vorfeld über die Funktionsweise und die Gefahren die Verbraucher informieren. Unternehmen versuchen sich gesetzeskonform zu verhalten, um Sanktionen und einem Imageverlust zu verhindern.

Bei der RFID-Technologie wird ein hoher Prozentanteil an Straftaten, wie beispielsweise das unbemerkte Auslesen ohne Einwilligung, nicht erkannt. Die Dunkelziffer bei der RFID-Technologie dürfte hoch sein, da die Technik ein verstecktes Anbringen erlaubt und die Rekonstruierbarkeit, wie die Daten gewonnen

<sup>6</sup> wie zum Beispiel das Unternehmen Walmart

<sup>7</sup> <http://www.heise.de/newsticker/meldung/77431>

<sup>8</sup> <http://www.boycottbenetton.com/>

wurden, verschwindet. Unternehmen könnten verleitet werden das Risiko einzugehen, da die Chancen, unbemerkt das Gesetz zu brechen, hoch sind. Diesen Gesetzesbruch kann der Gesetzgeber mit entsprechend hohen Strafen entgegenwirken. Ein Verkehrsunternehmen beispielsweise, welches nur sehr selten seine Fahrgäste kontrolliert und einem Schwarzfahrer nur mit niedrigen Sanktionen droht, wird viele Fahrgäste haben, welche kein gültiges Ticket besitzen<sup>9</sup>. Damit Unternehmen in diese Technologie investieren, ist es wichtig das Gesetze klar und verständlich ohne große Lücken formuliert werden. Ansonsten besteht eine zu hohe Planungsunsicherheit für die Unternehmen.

### 3.3 RFID und Barcode im Vergleich

Der Barcode ist eine maschinenlesbare Schrift. Sie besteht aus verschiedenen breiten schwarzen Strichen. Diese können über einem Barcodelesegerät maschinell ausgelesen werden.

Im Vergleich zum Barcode bietet die RFID-Technologie einige Vorteile. Zum Beispiel benötigt sie zum einen im Gegensatz zum Barcode keine Sichtverbindung um ein Objekt auszulesen. Dies ermöglicht es in kürzester Zeit mehrere Objekte auszulesen. Des Weiteren hat man beim Barcode keine Fälschungssicherheit, da sich ein Barcode leicht kopieren lässt. Mit Hilfe des RFID-Transponders werden Objekte eindeutig identifiziert und nicht, wie beim Strichcode üblich, in Objektklassen eingeteilt.

Der Barcode besitzt jedoch auch einige Vorteile gegenüber der RFID-Technologie. Mit Hilfe der RFID-Technologie können Eingriffe in die Privatheit entstehen, da sich Objekte eindeutig identifizieren lassen. Letzteres ist beim Barcode nicht der Fall. Über den Barcode besitzt man schon über viele Jahre hinweg gesammelte Erfahrungen und der Barcode ist somit sehr sicher in seiner Funktion. Bei Betrachtung der Kosten<sup>10</sup> ist ein Blatt Papier noch um einiges kostengünstiger als ein RFID-Transponder. Da man den Strichcode sehr günstig einsetzen kann und sich die Technologie bewährt hat, lohnt sich ein Umrüsten auf die RFID-Technologie nicht immer.

### 3.4 Anwendungsbeispiele der RFID-Technologie

**Identifikation** Die RFID-Technologie kann für die eindeutige Identifikation von Personen genutzt werden. Zum Beispiel benutzt man die RFID-Technologie zur Zeit schon bei Zugangskontrollen<sup>11</sup> für Gefängnisse in Südamerika. Berechtigte Personen bekommen einen RFID-Transponder implantiert. Dieser Transponder zeigt den Lesegeräten an Eingangstüren, dass eine autorisierte Person den Bereich passiert. Ein weiterer Vorteil ist auch, dass das Lesegerät im Vergleich zu herkömmlichen Magnetkartenlesegeräten keinen mechanischen Belastungen

<sup>9</sup> <http://www.tagesspiegel.de/berlin/nachrichten/bvg-schwarzfahrer/71188.asp>

<sup>10</sup> Ein RFID-Transponder kostet momentan um die 15 Cent. In den nächsten Jahren soll der Preis unter 5 Cent liegen

<sup>11</sup> <http://www.aska.com/produkte/RFID-Zugangskontrolle.html>

ausgesetzt ist, was sich in deutlich längeren Lebensdauern und längeren Wartungsintervallen der Lesegeräte bemerkbar macht.

Durch eine eindeutige Identifikation kann auch individueller auf einzelne Personen eingegangen werden. Zum Beispiel könnten Rettungskräfte bei verletzten Risikopatienten sofort erkennen, welche Maßnahmen sie einzuleiten haben. Der Risikopatient bekommt hierzu im Vorfeld einen RFID-Transponder implantiert. Der Transponder besitzt eine eindeutige Nummer, welche er einem Lesegerät übermittelt. In einer Datenbank könnten zu dieser Nummer wichtige Informationen, wie beispielsweise die entsprechende Blutgruppe, hinterlegt sein. Am Unfallort können die Rettungskräfte mit einem Lesegerät die Transpondernummer auslesen. Hätte der Verletzte beispielsweise einen hohen Blutverlust würden die Blutkonserven der richtigen Blutgruppe benötigt. Mit Zugriff auf die Datenbank können die Helfer mit der ausgelesenen Nummer erkennen, welche Blutgruppe der Verletzte besitzt und somit könnte man ihn sofort am Unfallort mit den richtigen Blutkonserven versorgen.

**Reduzierung von menschlich verursachten Fehlern** Mit Hilfe von RFID kann man das Verhalten von Menschen und Tieren teilweise digital erfassen. Weicht eine Person von vorher festgelegten Verhaltensabläufen ab, kann man sie darauf aufmerksam machen. Zum Beispiel erkennt eine smarte Werkzeugkiste, welche Werkzeuge sich in ihr befinden, protokolliert, welche Werkzeuge verwendet wurden und warnt den Mechaniker bei Unvollständigkeit oder falls Werkzeuge falsch verwendet wurden. Bei einer Routinekontrolle eines Flugzeugtriebwerks, werden üblicherweise Werkzeuge in der gleichen Reihenfolge verwendet. Falls nun ein Werkzeug nicht zur Anwendung kommt, könnte dies ein Indiz sein, dass der Mechaniker einen Arbeitsschritt vergessen hat. Mit Hilfe einer Warnmeldung über das ausgelassene Werkzeug, kann der Mechaniker gegebenenfalls den ausgelassenen Kontrollschritt noch durchführen. Es wird dem Mechaniker am Ende der Routinekontrolle erspart, den Werkzeugkasten auf Vollständigkeit zu überprüfen, da dies für ihn die smarte Werkzeugkiste automatisch durchführt. Wartungen und Reparaturen werden neben der erhöhten Sicherheit, da zum Beispiel kein Werkzeug mehr unbemerkt im Triebwerk eines Flugzeugs liegen bleibt, auch mit kürzeren Durchschnitszeiten durchgeführt.

**Erhöhung der Prozessgeschwindigkeit** Gerade da im Gegensatz zu anderen automatischen Identifikationen ein multiples Auslesen möglich ist und keine Sichtlinie bestehen muss, ist eine Prozessgeschwindigkeitserhöhung oft durchführbar. Durch die Verwendung der RFID-Technologie kann zum Beispiel die Inventur erleichtert werden. Man muss lediglich noch mit einem Lesegerät durch die Regale laufen. Außerdem gibt es Überlegungen an jedes Regal ein Lesegerät anzubringen, so genannte smart shelves. Dies würde eine Echtzeitausgabe des tatsächlichen Lagerbestands mit den genauen Standorten der Artikel ermöglichen.

## 4 Risiken beim Einsatz der RFID-Technologie

Die RFID-Technologie würde der Wirtschaft Einsparungen in Milliardenhöhe bringen. Jedoch sollten die Risiken, die mit dieser neuen Technologie einhergehen, auch beachtet werden. Einige Bürger befürchten, durch die neue Transpondertechnologie Eingriffe in ihre Privatsphäre hinnehmen zu müssen. Angelehnt an Sarah Spiekermann kann man die Konsumentenbedenken der RFID-Technologie in 6 Kategorien klassifizieren [1].

### 4.1 Unbemerktles Auslesen

Die RFID-Technologie erlaubt das unsichtbare Auslesen von Transpondern. Hierbei sieht der Benutzer die Gefahr, dass er überhaupt nicht mitbekommt, wenn einer seiner RFID-Transponder ausgelesen wird. Personen können somit nicht mehr überwachen, wann und wo Informationen von ihnen preisgegeben werden. Vielen Verbrauchern sind sich der Tatsache nicht bewusst, dass durch einzelne wenige Daten weit reichende Rückschlüsse gezogen werden können. Unternehmen sammeln häufig scheinbar wertlose Informationen. Durch das Verknüpfen mit anderen Informationen kann man oft zu wichtigen Erkenntnissen gelangen. Beispielweise könnten Unternehmen durch Verknüpfung einer Telefonnummer mit einem Telefonverzeichnis die Anschrift des Kunden ermitteln. Diese Anschrift kann daraufhin mit einer Datei abgeglichen werden, welche Auskunft über die erwartete Bonität dort lebender Anwohner gibt.

Die RFID-Technologie könnte auch kriminell missbraucht werden, wenn RFID-Transponder unbemerkt ausgelesen werden können. Dritte könnten unbemerkt den privaten Besitz auslesen und somit erkennen, ob ein Überfall lohnenswert sei.

### 4.2 Verfolgbarkeit

Einige Bürger sehen bei der RFID-Technologie die Gefahr, dass von ihnen Bewegungsprofile erstellt werden könnten. RFID-Lesegeräte könnten registrieren, wann sich welche RFID-Transponder in ihrem Lesebereich aufhalten. Zum einen könnten Angreifer RFID-Lesegeräte unbemerkt an verschiedenen Orten aufstellen. Zum anderen könnten unbefugte Dritte auch an die benötigten Informationen von aufgestellten RFID-Lesegeräten durch Sicherheitsschwachstellen gelangen. Zum Beispiel könnten Menschen bestochen werden, damit sie die von den RFID-Lesegeräten gewonnenen Informationen an Angreifer weitergeben. Gerade wenn die Angreifer Zugriff zu vielen RFID-Lesegeräten haben, können sie sich ein genaues Bewegungsprofil von den gewünschten Personen erstellen. Dem Angreifer würde teilweise auch die Information von einem Lesegerät genügen. Dabei könnte es sich beispielsweise um ein Lesegerät eines Arztes handeln, der sich auf krebskranke Menschen spezialisiert hat. Eine Krankenversicherung könnte mit diesem Wissen die Aufnahme solcher Personen, welche von dem Lesegerät erkannt worden sind, verweigern und somit Kosten sparen.

### 4.3 Erkennbarkeit sozialer Netzwerke

Eine andere Gefahr könnte darin bestehen, dass Angreifer mit Hilfe von Bewegungsprofilen soziale Netzwerke aufdecken könnten. Beispielsweise könnte man Personen, welche sich regelmäßig sonntags in einer katholischen Kirche aufhalten, als Katholiken auffassen. Das Aufdecken sozialer Netzwerke kann eventuell noch vereinfacht werden, wenn man die Bewegungsprofile mit verschiedenen Informationen verknüpft. Dadurch, dass Bevölkerungsschichten durch die RFID-Technologie leichter abgrenzbar wären, bestünde die Möglichkeit, Personen dieser Bevölkerungsschicht zu diskriminieren.

### 4.4 Objektverantwortlichkeit

Die nächste Kategorie, die Objektverantwortlichkeit, betrifft das Problem der Bürger, dass Gegenstände, die vorher nicht zugeordnet werden konnten, nun auf sie zurückgeführt werden können. Dies reicht vom Wegwerfen einer Coladose in einem Park bis zum Aufklären eines Mordes, bei dem verschiedene Gegenstände eine Rolle spielten. Das Problem hierbei ist, dass Personen unverschuldet in Verdacht kommen könnten. Beispielsweise könnten Tiere die Coladose aus dem Mülleimer entnommen haben.

Oft werden auch RFID-Transponder an Gegenständen von Bürgern angebracht, ohne dass diese Kenntnis davon erlangt haben. In England zum Beispiel wurden an 500 000 Mülltonnen RFID-Transponder angebracht, ohne die betroffenen Mülltonnenbesitzer darüber zu informieren. Durch die elektronische Kennzeichnung wäre es nun möglich, dass jeder Haushalt nach seiner produzierten Müllmenge, die durch eine Waage am Müllwagen gemessen wird, abgerechnet wird. Auch eine falsche Sortierung kann hierdurch geahndet werden, da die falsch sortierte Mülltonne eindeutig auf den Mülltonnenbesitzer schließen lässt.<sup>12</sup>

### 4.5 Technologiepaternalismus

Technologiepaternalismus bedeutet nach Sarah Spiekermann den Verlust von Kontrollrechten im Namen eines angeblich höheren Besseren. Viele Menschen sind besorgt, dass die RFID-Technologie die Handlungsmöglichkeiten einschränkt und gewissermaßen das Verhalten des Menschen steuert. Dadurch, dass mit Hilfe der RFID-Technologie erkannt werden kann, wie sich der Mensch verhält, kann man ihn durch verschiedene Maßnahmen in seinem Verhalten steuern. Zum Beispiel würde beim Nichtanlegen eines Gurtes ein Warnsignal ertönen oder der Motor des Fahrzeugs ließe sich nicht starten.

### 4.6 Personalisierung

Von einigen Personen wird die Gefahr erkannt, dass die RFID-Technologie dazu benutzt werden könnte, Personen eindeutig zu identifizieren und dass man hierdurch Nachteile haben könnte. Wie schon beim "Customer Relationship Management" üblich, könnte eine ABC-Analyse über dem Kundenbestand durchgeführt

<sup>12</sup> <http://www.heise.de/newsticker/meldung/77348>

werden. Hierbei werden die Kunden in die Klassen A, B und C eingeteilt. In der genannten Klassenreihenfolge sinkt auch der Profit pro Person und steigt die Anzahl der Kunden. Pro Kunde der Gruppe A erzielt das Unternehmen einen hohen Profit. Das Unternehmen würde sich daher auf die Wünsche der Kunden der Gruppe A konzentrieren, da deren Bestand essentiell für das Unternehmen ist. Dahingegen werden Kunden der Gruppe C eher automatisch abgefertigt. Kunden in Gruppe C haben durch diese Personalisierung meist negative Konsequenzen. Das Abwandern von Personen dieser Gruppe zur Konkurrenz kann das Unternehmen eher verkraften als jenes von Kunden der Gruppe A. In einem Bekleidungsgeschäft beispielsweise könnte die RFID-Technologie im Eingangsbereich erkennen, welche Kleider der Kunde trägt und damit erkennen, welcher der drei Gruppen er angehört. Wenn ein Mitarbeiter gerade einen Kunden der Gruppe C bedient, könnte er die momentane Beratung abbrechen, da gerade ein Kunde der Gruppe A oder B den Laden betreten hat.

## 5 Privacy Enhancing Technologies

Man kann versuchen, Privatheit auf mehreren Wegen herzustellen. Zum einen könnte man soziale Mittel benutzen. Ein Unternehmen könnte zum Beispiel Leitlinien für seine Mitarbeiter erstellen, wie sie mit Daten umzugehen haben. Zum anderen, gibt es wie in Kapitel 2 aufgezeigt wurde, auch rechtliche Mittel, welche Datenschutzverletzungen sanktionieren. Im Folgenden wird auf Privacy Enhancing Technologies (PET) eingegangen. Diese versuchen, Privatheit durch technische Mittel herzustellen und bieten für Anwender der RFID-Technologie einen Selbstschutz. Der Anwender des RFID-Tags kommt durch ein effektives technisches Verfahren nicht mehr in die Situation, unbewusst personenbezogene Daten preiszugeben.

### 5.1 Killer-Tag-Verfahren

Beim Killer-Tag-Verfahren werden die RFID-Transponder einzeln unbrauchbar gemacht. Der RFID-Transponder kann somit keine Informationen mehr freigeben. Unbrauchbarkeit kann durch software- oder hardwaretechnische Lösungen hergestellt werden. Bei einer hardwaretechnischen Lösung wird der RFID-Transponder mit Hilfe eines starken elektromagnetischen Feldes unbrauchbar gemacht. Für den Kunden ist eine elektromagnetische Zerstörung zuverlässiger als eine softwaretechnische Lösung, welche durch eine entsprechende Software realisiert wird. Beim Metro Future Store<sup>13</sup> beispielsweise wurde bei der softwaretechnischen Lösung nicht der komplette RFID-Transponder unbrauchbar gemacht<sup>14</sup> und man konnte somit noch wichtige Informationen vom Transponder auslesen. Momentan wird meist eine softwaretechnische Lösung verwendet, da sie im Vergleich zur hardwaretechnischen Lösung kostengünstiger zu realisieren ist.

<sup>13</sup> <http://www.future-store.org>

<sup>14</sup> <http://www.foebud.org/rfid/metro>

Der Verbraucher hat das Problem, dass er nicht einfach erkennen kann, ob sein RFID-Transponder wirklich unlesbar gemacht wurde.

Ein weiterer Nachteil beim Killer-Tag-Verfahren ist, dass man den Transponder nach dem Deaktivieren nicht mehr für sinnvolle Zwecke einsetzen kann. Ein Beispiel für einen solchen sinnvollen Zweck wäre, dass man bei einer Reklamation die beanstandete Ware genau identifizieren könnte. Mit Hilfe von genaueren Informationen, in welchem Werk und zu welchem Zeitpunkt die Ware hergestellt wurde, könnte sich beispielsweise eine Rückrufaktion einer mangelhaft hergestellten Brems Scheibe eines Fahrzeugs erheblich eingrenzen lassen.

## 5.2 Clipped-Tag-Verfahren

Beim Clipped-Tag-Verfahren zerstört der Verbraucher die Antenne des RFID-Transponders. Dies geschieht entweder durch das Rubbeln auf dem Etikett, das Entfernen einer vorperforierten Stelle oder das Abziehen einer Folie. Jede dieser drei Maßnahmen verringert die Reichweite des RFID-Transponders und damit dessen Auslesbarkeit auf eine sehr kurze Distanz.

Ein Nachteil ist, dass der RFID-Tag noch auf kürzeren Distanzen auslesbar ist. Dieser Nachteil könnte von einem Angreifer genutzt werden, um die eindeutige Identifikationsnummer des RFID-Transponders herauszufinden. Voraussetzung dafür ist, dass der Angreifer mit einem Lesegerät in die direkte Umgebung des RFID-Transponders gelangt.

Ein großer Vorteil beim Clipped-Tag-Verfahren ist, dass der Verbraucher selbst bestimmen kann, zu welchem Zeitpunkt die Auslesedistanz von diesem Transponder reduziert wird. Das gibt dem Verbraucher das Gefühl der Kontrolle und dürfte somit bei Endkunden beliebt sein. Des Weiteren ist das Verfahren einfach durchführbar und die Transponder sind nur geringfügig teurer als herkömmliche Transponder. Ein weiterer Vorteil ist, dass der Transponder durch Anbringung einer Zusatzantenne wieder eine größere Reichweite erzielen kann. Beispielsweise könnte dies bei der Reklamation einer Ware Anwendung finden.

## 5.3 Blocker-Tag-Verfahren

Beim Blocker-Tag-Verfahren täuscht der Blocker-Tag dem Lesegerät vor, es wären Billionen Transponder in seinem Umfeld. Dies bewirkt, dass normale Transponder somit nicht auslesbar wären.

Dieses Verfahren funktioniert nur, wenn das so genannte Tree-Walking Singulation Protokoll verwendet wird. Bei diesem Protokoll kann das Lesegerät zu einem Zeitpunkt nur mit einem Transponder kommunizieren. Das Protokoll sorgt dafür, dass die Transponder einzeln mit dem Lesegerät kommunizieren. Wie das Tree-Walking Singulation Protokoll funktioniert, wird nun anhand eines kleinen Beispiels [5] erklärt. Im Lesefeld eines Lesegerätes befinden sich drei Transponder mit den Kennungen 001, 011 und 110. Die von den Transpondern ausgesandten Transpondernummern können vom Lesegerät nicht gleichzeitig empfangen werden. Es kommt stattdessen zu einer Kollision, da das Lesegerät zu einem

Zeitpunkt nur die Daten von einem Transponder auslesen kann. Die Transpondernummern kann man sich als Blätter in einem Binärbaum vorstellen (siehe Abbildung 2). Das Lesegerät beginnt nun eine Tiefensuche, bis keine Kollision mehr auftritt. Das Lesegerät sendet hierzu zuerst eine Null. Darauf antworten nur noch Transponder, wenn ihre Transpondernummer ein Präfix dieser Nummer ist. In unserem Beispiel würden die Transponder mit den Nummern 001 und 011 antworten. Dies würde wiederum zu einer Kollision führen. Aus diesem Grund sendet das Lesegerät im darauf folgenden Schritt zwei Nullen aus. Nun antwortet nur noch der Transponder mit der Nummer 001. Dieser kann nun vom Lesegerät ausgelesen werden. Als nächstes würde das Lesegerät eine 01 aussenden, was ihm das Auslesen des nächsten Transponders ermöglichen würde.

Ein Blocker-Tag gibt dem Lesegerät immer vor, dass es eine Kollision gibt. Da Lesegeräte nur rund 100 000 Transponder pro Sekunde auslesen können, ist das Lesegerät bei  $2^{64}$  Blättern nicht mehr in der Lage, in akzeptabler Zeit die Transponder auszulesen.

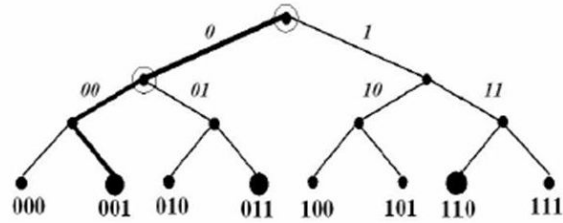
Die Blocker-Tags sind nicht teurer als herkömmliche RFID-Transponder. Ein großer Nachteil dieses Verfahrens ist, dass durch Blocker-Tags andere Leser gestört werden könnten. Den störenden Blocker ausfindig zu machen kann sich als schwierig erweisen, gerade wenn es sich um Transponder handelt, welche eine größere Auslesedistanz besitzen. Durch bessere Lesegeräte können Blocker-Tags umgangen werden, indem man diese durch Triangulation oder Signalstärke ausfindig macht. Somit könnte der komplette Schutzmechanismus umgangen werden. Des Weiteren könnten andere Lesegeräte ungewollt durch Blocker-Tags beeinträchtigt werden. Dies könnte geschehen, wenn beispielsweise eine Person einen Blocker-Tag beim Betreten einer Bibliothek, welche mit einem RFID-System ausgestattet ist, mit sich führt. Der Blocker-Tag, welcher nur mit der Intention an der Kleidung angebracht wurde, um ein ungewolltes Auslesen von mitgeführten RFID-Transpondern der Kleidung zu verhindern, kann den RFID-Scanner am Bibliothekseingang überlasten.

Das Blocker-Tag-Verfahren sollte möglichst keine Anwendung finden, da kein Schutz der Privatsphäre gegeben ist und hierdurch andere Lesegeräte gestört werden könnten.

#### 5.4 Hash-Lock-Verfahren

Eine Hashfunktion auf dem Transponder wird beim Hash-Lock-Verfahren verwendet. Soll der Transponder für Dritte nicht mehr seine gespeicherten Informationen preisgeben, wird ein Hashwert  $h^{15}$  mit einem zufällig ausgewählten Schlüssel  $k$  ausgewählt. Das Tupel  $(h,k)$  wird in einer Datenbank abgelegt und der Hashwert  $h$  wird auf dem Transponder gespeichert. Der Transponder sendet dann nur noch den Hashwert  $h$ . Zum Auslesen der Transpondernummer muss das Lesegerät den in der Datenbank abgelegten Schlüssel  $k$  an den Transponder senden. Dieser überprüft anhand seiner Hashfunktion, ob der Schlüssel  $k$  den Hashwert  $h$  liefert.

<sup>15</sup> Hashwert  $h = \text{Hash}(k)$



**Folgende Tags sind im Lesebereich:**

1: 001  
 2: 011  
 3: 110

**Abbildung 2.** Beispiel zum Tree-Walking-Singulation Protokoll

Falls dies zutrifft, können alle Lesegeräte, welche diesen Transponder in ihrem Leseumfeld haben, seine Nummer auslesen. Zu diesem Zeitpunkt könnten somit auch Angreifer die RFID-Transponder auslesen.

Der Hashwert  $h$  könnte über die Verwendung von mehreren Lesegeräten die Verfolgbarkeit eines Objekts ermöglichen. Ein weiterer Nachteil ist, dass die RFID-Lesegeräte mit der Datenbank vernetzt sein müssen, was auch für Angreifer eine Angriffsmöglichkeit böte. Beispielsweise könnte ein Angreifer versuchen die Kommunikation zwischen den Lesegeräten abzuhören, um an den entsprechenden Schlüssel  $k$  zu gelangen.

### 5.5 Randomized-Hash-Lock-Verfahren

Das Randomized-Hash-Lock-Verfahren ist eine Weiterentwicklung des Hash-Lock-Verfahrens. Die beim Hash-Lock-Verfahren noch mögliche Verfolgbarkeit wird beim Randomized-Hash-Lock-Verfahren erschwert, indem bei jeder Leseanfrage ein anderer Hashwert ausgesendet wird. Dies funktioniert folgendermaßen: Die Transpondernummer und eine Zufallszahl  $r$ , welche bei jeder Leseanfrage neu gewählt wird, werden konkateniert und dann zusammen gehasht. Dem Lesegerät wird dann die Zufallszahl  $r$  und der Hashwert  $h = \text{Hash}(\text{Transpondernummer}||r)$  zugesendet. Voraussetzung dafür, dass das Lesegerät die Transpondernummer herausfindet, ist, dass es Zugriff auf eine Datenbank hat, auf der die im Umlauf befindlichen Transpondernummern abgelegt sind. Die in der Datenbank abgelegten Transpondernummern mit der konkatenierten Zufallszahl  $r$  werden einzeln nacheinander gehasht bis das Ergebnis gleich dem Hashwert  $h$  ist.

Bei diesem Verfahren hat man einen hohen rechnerischen Aufwand, da der Benutzer so lange hashen muss, bis die richtige Transpondernummer beim Hashen verwendet wurde. Somit steigt der Rechenaufwand linear mit der Anzahl der im

Umlauf befindlichen Transponder. Neben der fehlenden Skalierbarkeit ist Verfolgbarkeit im Nachhinein noch möglich, wenn einmal eine Transpondernummer offengelegt wurde.

Der Vorteil dieses Verfahrens ist, dass es im Vergleich zu kryptographischen Verfahren nicht so aufwendig ist, jedoch auch nicht kryptographisch robust ist.

## 5.6 Wirksamkeit der Privacy Enhancing Technologies

In diesem Kapitel wurden einige Verfahren vorgestellt, welche den Schutz der Privatsphäre herzustellen versuchen. Die einzelnen Verfahren sind sehr unterschiedlich in ihrer Wirksamkeit. In Abbildung 3 werden die einzelnen Verfahren den Risiken, welche in Kapitel 3 vorgestellt wurden, gegenübergestellt. Die Wirksamkeit untergliedert sich in drei Stufen: 1. Gefahr wird verhindert, 2. Gefahr wird eingeschränkt oder 3. Gefahr wird nicht verhindert.

	Unbemerkt Auslesen	Verfolgbarkeit	Objektverant- wortlichkeit	Technologie- paternalismus	Personalisierung	Krimineller Missbrauch
Killer Tag	++	++	++	++	++	++
Clipped Tag	+	++	-	++	++	++
Blocker Tag	-	-	-	-	-	-
Hash Locks	++	-	+	+	+	++
Randomized Hash Locks	++	+	+	++	++	++

wird verhindert (++)	wird eingeschränkt (+)	wird nicht verhindert (-)
----------------------	------------------------	---------------------------

Abbildung 3. Wirksamkeit der verschiedenen PET

Der Killer-Tag verhindert alle Bedenken, wenn der Transponder richtig unbrauchbar gemacht wird. Bei diesem Verfahren ist jedoch zu berücksichtigen, dass der RFID-Transponder nach der Deaktivierung nicht mehr zum Einsatz kommen kann.

Das Clipped-Tag-Verfahren räumt die meisten Bedenken aus. Objektverantwortlichkeit wird hier jedoch nicht verhindert, da Objekte bei kurzen Auslesedistanzen noch ausgelesen werden können. Dieses Verfahren hat den Vorteil, dass es Personen das Gefühl der Kontrolle gibt.

Beim Blocker-Tag wird kein Schutz der Privatsphäre gewährleistet, da dieser

durch gute Lesegeräte umgangen werden kann.

Das Hash-Lock-Verfahren bietet nur einen begrenzten Schutz, da man durch den Hashwert verfolgbar bleibt, was eindeutig einen Nachteil dieses Verfahrens bedeutet.

Das Randomized-Hash-Lock-Verfahren verbessert noch einmal das Hash-Lock-Verfahren und schränkt die Verfolgbarkeit ein. Es ist jedoch nicht skalierbar.

Privacy Enhancing Technologies bieten unterschiedliche Möglichkeiten, Eingriffe in den Schutz der Privatsphäre zu reduzieren. Momentan steht man jedoch mit der Entwicklung noch am Anfang. Alle vorgestellten Verfahren besitzen zur Zeit noch gravierende Nachteile. Einfachere Handhabbarkeit bedeutet meist gleichzeitig auch einen Verlust an Schutz der Privatheit. Beispielsweise ist das Hash-Lock-Verfahren im Vergleich zum Randomized-Hash-Lock-Verfahren nicht so rechenaufwändig, bietet jedoch keinen guten Schutz gegen Verfolgbarkeit. Festzuhalten ist, dass das Killer-Tag-Verfahren und das Clipped-Tag-Verfahren unter vertretbarem Aufwand einen angemessenen Privatheitsschutz gewährleisten können.

## 6 Zusammenfassung

Der Konflikt zwischen der Kontrolle der persönlichen Informationen und einer allgegenwärtigen, intelligenten Informationsverarbeitung wird in den nächsten Jahren immer mehr in den Vordergrund treten, gerade da die RFID-Technologie künftig noch verstärkt eingesetzt werden wird. Wie in der Arbeit gesehen gibt es bisher jedoch noch kein Verfahren, welches diesen Konflikt löst. Um eine breite Markteinführung der RFID-Technologie zu ermöglichen, ist deshalb ein gutes Zusammenspiel von rechtlichen und technischen Schutzmechanismen unabdingbar. In Kapitel 2 wurde aufgezeigt, dass der momentane rechtliche Rahmen der schnellen technologischen Entwicklung nicht standhalten kann. Ein Ausweg aus diesem Dilemma wäre eine Selbstregulierung, etwa in Form eines Datenschutzaudits. Die in Kapitel 5 vorgestellten Privacy Enhancing Technologies, welche die potenziellen Gefahren der RFID-Technologie auf ein Minimum reduzieren können, erfordern die Abwägung zwischen Handhabbarkeit und dem Schutz der Privatheit.

Schon bei der Konzeption von RFID-Systemen sollten Unternehmen berücksichtigen, dass die benötigte Auslesedistanz nicht zu stark überschritten wird. Ein unberechtigter Zugriff ließe sich gerade über eine geringe Lesedistanz stark einschränken.

Damit Unternehmen die Vorteile der RFID-Technologie nutzen können und ohne große Verbraucherängste ihre Produkte mit RFID-Transpondern absetzen können, werden sie wohl zuerst überwiegend das Killer-Tag-Verfahren und das Clipped-Tag-Verfahren anwenden.

Um das Verbrauchervertrauen aufzubauen wird es wichtig sein, dass die Unternehmen mit den Verbrauchern statt einer emotionalisierten Diskussion einen offenen Dialog führen und sie über die entsprechenden Verfahren rechtzeitig informieren. Datenschutz sollte von den Unternehmen eher als Wettbewerbsvorteil gesehen werden als ein Hindernis, die Technologie einzusetzen.

## Literatur

- [1] O.Berthold, O.Günther, S.Spiekermann, RFID: Verbraucherängste und Verbraucherschutz - eine Frage der Kontrolle, *Wirtschaftsinformatik* 6 (Vol. 47) pp. 422-430 Vieweg, 2005.
- [2] U.Eisenberg, J.Puschke, T.Singelstein, Überwachung mittels RFID, *Zeitschrift für Rechtspolitik* (Vol. 38) pp. 9-11, 2005.
- [3] S.Garfinkel, A.Juels, R.Pappu, RFID Privacy - An Overview of Problems and Proposed Solutions, *IEEE Security and Privacy* (Vol. 3, No. 3) pp. 34-43, 2005.
- [4] B.Holznagel, M.Bonnekoh, Radio Frequency Identification - Innovation vs. Datenschutz?, *Multimedia und Recht* Heft 1 pp. 7-12, 2006.
- [5] A.Juels, R.Rivest, S.Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, 10th Annual ACM CCS, 2003.
- [6] M.Langheinrich, RFID and Privacy, Milan Petkovic, Willem Jonker (Eds.): *Security, Privacy, and Trust in Modern Data Management*, Springer-Verlag, 2006.
- [7] M.Langheinrich, Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie, *Institute for Pervasive Computing ETH Zürich*, 2004.
- [8] A.Roßnagel, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung. *Multimedia und Recht* Heft 2 pp. 71 - 75, 2005.
- [9] S.Spiekermann, H.Ziekow, RFID: A Systematik Analysis of Privacy Threats and a 7-Point Plan to Adress Them, *Journal of Information System Security* (Vol. 1, No. 3), 2006.
- [10] M.Tinnefeld, Vom archimedischen Punkt in einer Zivilgesellschaft, *Multimedia und Recht* Heft 12 pp. 797-801, 2004
- [11] S. Warren, L. Brandeis, The Right to Privacy, *Harvard Law Review*, 1890
- [12] Das Bundesverfassungsgericht. <http://www.bverfg.de>
- [13] Die Universitätsbibliothek Karlsruhe. <http://www.ubka.uni-karlsruhe.de>