

# RFID

## Verbraucherängste und Verbraucherschutz

### Die Autoren

Oliver Berthold  
Oliver Günther  
Sarah Spiekermann

Oliver Berthold  
Institut für Informatik  
Datenbanken und Informationssysteme  
Humboldt-Universität zu Berlin  
Rudower Chaussee 25  
12489 Berlin

Prof. Oliver Günther,  
Ph.D. Dr. Sarah Spiekermann  
Institut für Wirtschaftsinformatik  
Humboldt-Universität zu Berlin  
Spandauer Straße 1  
10178 Berlin

ten, die Grundlagen für die „intelligente“ Infrastruktur für den Handel von morgen definieren. Das schon länger diskutierte *allgegenwärtige Rechnen* (engl. *Ubiquitous* oder *Pervasive Computing*) hält somit breiten Einzug in die betriebliche Datenverarbeitung.

Neben anderen drahtlosen Technologien wie Sensornetzwerke, Wireless LAN, GSM und GPS ist die RFID-Technik einer der wichtigsten Bausteine des allgegenwärtigen Rechnens. Objekte werden mit einem kleinen Funkchip ausgestattet (engl. *Transponder* oder *Tag*), der trägerunabhängig mit Lesegeräten (*Readers*) kommuniziert. In dem Vorschlag von EPCglobal ist auf dem Tag nur eine Nummer abgespeichert, der so genannte *Electronic Product Code* (EPC), welcher als neuer Nummernstandard den Barcode ablöst und jedem einzelnen Objekt eine eindeutige ID zuweist [A-IDa03; A-IDc03]. Diese Eindeutigkeit kann helfen, diverse Probleme moderner Wertschöpfungsketten zu lösen, wie etwa den Schwund von Produkten, das Ein-

schleusen von Fälschungen in den Lieferprozess oder das Recycling. Des Weiteren führt das automatische Auslesen der Tags zur Reduktion von Personalkosten überall dort, wo Warenlieferungen manuell erfasst und überprüft werden müssen. So berichtet z. B. die Metro AG, dass in den ersten RFID-gesteuerten Distributionszentren eine Senkung der Lohnkosten um 11% erzielt wird; die Verringerung des Schwunds bei Transport und Lagerung liegt bei 11–18% [Wolfr04].

Einmal eingelesen leiten Lesegeräte die EPC-Information weiter an ein EPC-Netzwerk [GCI03], wo ähnlich dem *Domain Name Service* (DNS) ein *Object Name Service* (ONS) erlaubt, Server mit weitergehenden Produktinformationen auf Basis des EPCs zu lokalisieren. Auf den so angesteuerten Serverrechnern und den dort laufenden *EPC-Informationdiensten* sollen dann weitergehende Informationen zu dem jeweiligen Objekt in standardisierter Form zu finden sein, zum Beispiel zu Ort und Zeitpunkt seiner Produktion, Auslie-

### ■ 1 Einleitung

RFID-Technik – kurz für Radiofrequenz-identifikationstechnik – ist derzeit in aller Munde. National wie international sind Unternehmen der unterschiedlichsten Branchen dabei, die technische Infrastruktur für die drahtlose Identifikation von Objekten auszubauen, um Effizienzsteigerungen in Produktions-, Logistik- und Warenverkaufsprozessen zu erzielen. Besonders aktiv sind industrielle Standardisierungsgremien bei EPCglobal ([www.epcglobal.org](http://www.epcglobal.org)) und angeschlossene Forschergruppen im Auto-ID Lab Network ([www.Auto-IDlabs.org](http://www.Auto-IDlabs.org)), die daran arbei-

### Kernpunkte

Der Beitrag gibt einen Überblick über im Zusammenhang mit der RFID-Technologie auftretende Verbraucherängste und technische Möglichkeiten, diese zu adressieren. Er diskutiert die wesentlichen bis dato präsentierten technischen Schutzansätze und propagiert ein passwortbasiertes Schutzverfahren:

- RFID-Technik und Argumente, warum Verbraucherängste gerechtfertigt sind,
- Schutztechnologien zur effektiven Adressierung von RFID-induzierten Ängsten und Schaffung von Kontrolle,
- Plädoyer für einen einfachen Schutz durch einen passwortbasierten Ansatz, mit dem man das Auslesen der RFID-Tags sicher kontrollieren kann.

**Stichworte:** Radio Frequenz Identifikation (RFID), Datenschutz, Privacy Enhancing Technologies (PETs), Kontrolle, Technologiepaternalismus, Kryptographie, Passwortschutz

## 2 | Oliver Berthold, Oliver Günther, Sarah Spiekermann

ferungsstatus und Verkaufsdatum [AutID02]. Auf Basis dieser Technologien hofft die Industrie, den in vielen Anwendungen problematischen Medienbruch zwischen physischen Warenströmen und virtueller Informationswelt zu schließen. Insbesondere erhofft man sich die Echtzeittransparenz von Lieferprozessen und die Reduktion des Prozentsatzes vergriffener Artikel (Out-of-shelf-Situation).

Während einerseits nun diese positiven wirtschaftlichen Potenziale bestehen, wird andererseits derzeit eine heftige Debatte um die gesellschaftlichen Implikationen der Technologie geführt. Wenn RFID-Tags auf den Produkten im Einzelhandel angebracht sind und von dort weiter in die Haushalte gelangen, dann, so schreiben Wissenschaftler [Beckw03; BCLMR04; Leder02; SpBe04] und Verbraucherschützer [FoeB03], könnte es zu einer allgegenwärtigen Überwachung von Menschen auf Basis der ihnen gehörenden Güter kommen. Verbraucherschützer boykottieren deshalb weltweit die RFID-Einführung bei großen Markenartiklern und Handelshäusern wie Benetton, Gillette, Metro oder Walmart.

Der vorliegende Artikel beginnt mit einem Überblick über die Kritikpunkte und Ängste, die von Verbrauchern im Zusammenhang mit der RFID-Technologie geäußert werden. Anschließend wird die technische Realisierbarkeit dieser Ängste diskutiert. In Abschnitt 3 wird eine Auswahl der wichtigsten RFID-relevanten Schutztechnologien vorgestellt. Dabei zeigt sich, dass nur solche Verfahren wirklichen Schutz geben, die eine durch den Nutzer aktiv kontrollierte Auslesung vorsehen. Wir konzentrieren uns auf die wichtigsten gegenwärtig diskutierten technischen Modelle, welche mithilfe von Authentifizierungsverfahren dem Nutzer genau diese Kontrolle geben. Abschnitt 4 schließt mit einer Zusammenfassung und einem Ausblick auf geplante Arbeiten.

## 2 RFID-induzierte Ängste

Die Vorstellung einer Integration von Funkchips in alle uns umgebenden Objekte sowie die damit mögliche „leise“ Kommunikation von Objekten untereinander ruft bei vielen Zeitgenossen Unbehagen hervor. So hat die Gesellschaft für Informatik eine Warnung vor der Technologie formuliert und einen Maßnahmenkatalog aufgestellt, „um die potenziellen Gefahren von Transpondern für die Bürger und die

Gesellschaft auf ein Minimum zu reduzieren“ [Pohl04].

Sowohl im Auto-ID Center als auch an der Humboldt-Universität zu Berlin wurden vor diesem Hintergrund empirische Verbraucheranalysen durchgeführt, die Aufschluss darüber geben sollen, welche Ängste Verbraucher konkret mit der RFID-Technologie verbinden [Duce03; SpGue04]. Dabei kam die im Bereich der Grundlagenforschung der Sozialwissenschaften häufig verwendete Methode der Fokusgruppenanalyse zum Einsatz [ChIa01]. In den Analysen des Auto-ID Center zeigt sich, dass die Angst vor einer Einbuße an Privatsphäre andere Negativpotenziale der Technologie, wie etwa Gesundheitsschäden und Arbeitsplatzverluste, klar überlagert. Die Studien an der Humboldt-Universität widmeten sich der Frage, an welchen Konstrukten eine Verletzung der Privatsphäre festzumachen ist. Zu diesem Zweck wurden 30 Berliner Bürger in 4 Fokusgruppen für 8 Stunden beobachtet. Informationsgrundlage war ein positiv gestalteter Film der *Metro Future Store Initiative* über den Nutzen von RFID im Supermarkt der Zukunft (zu Beginn der Diskussion) sowie ein eher kritischer ARD-Bericht über die RFID-Technik und ihre Anwendungen (gegen Ende der Diskussion). Für Fragen stand ein neutraler Moderator zur Verfügung. Die Zusammensetzung der Gruppenteilnehmer entsprach ungefähr dem Bevölkerungsdurchschnitt in Alter, Bildung und Geschlecht. Ausgehend von den auf Tonband aufgenommenen und transkribierten Gesprächen konnten sechs als wesentlich wahrgenommene Eingriffe in die Privatsphäre isoliert werden:

**a. Kontrollverlust über die eigenen Besitzgegenstände durch Unsichtbarkeit und Unbemerckbarkeit:** Urangst, durch die Unsichtbarkeit und Unbemerckbarkeit der Technologie keine Kontrolle mehr darüber zu haben, was mit den eigenen Objekten passiert bzw. wann und ob man ausgelesen wird oder werden kann.

„... aber wenn **man nicht weiß**, wo dieses Ding ist? Und ich **weiß nicht**, ob es irgendwo draufklebt oder woanders drin ist!“ (Hervorhebungen von den Autoren)

„Das Produkt, das ich gekauft habe, ist in **mein Eigentum** übergegangen, und mit dem möchte ich machen können, was ich will. Das hat dann keinen mehr zu interessieren.“

**b. Verfolgbarkeit (engl. Tracking):** Möglichkeit, dass Informationen über Objekte ausgelesen und für die Erstellung von Bewegungsprofilen genutzt werden. Auf-

enthaltensorte von Individuen könnten über die Überwachung der ihnen zugehörigen Objekte auch über einen längeren Zeitraum hinweg zurückverfolgt werden.

„Wenn sich diese Chip-Anwendung halt eben nur auf diesen Laden und den Anwender der Karte bezieht, ist das ja in Ordnung. Wenn aber eine **Weiterverfolgung außerhalb des Ladens geschieht**, hätte ich damit ein Problem.“

„Die können das in ihrem Umfeld, ihrer Produktionsstätte, ihrem Verkaufsfeld nutzen, aber dann ist Schluss. Dann haben die mich in Ruhe zu lassen. Ich gehe aus dem Laden raus und **will nicht verfolgt werden**.“

„Ich würde anfangen, unter **Verfolgungsangst** zu leiden...“

**c. Objektverantwortlichkeit:** Angst vor der Zuordnung von Personen zu den ihnen jetzt oder früher zugehörigen Objekten. Die Angst ist dadurch motiviert, dass man für den Missbrauch oder Verbleib von Objekten verantwortlich gemacht werden könnte. Dies mag vergleichsweise harmlose Beispiele betreffen, wie die weggeworfene Coladose im Wald, aber auch ernstere Fälle, wie lange verkaufte oder verschenkte Objekte, die in eine kriminelle Handlung involviert sind und den Verdacht auf den früheren Besitzer lenken.

„... sondern es geht mir darum, dass **meine Persönlichkeit, meine Person selber nicht in Verbindung gebracht werden muss mit dem Produkt**, nachdem ich es gekauft habe“

„Dann bin ich als Käufer für die Joghurtflasche **verantwortlich oder was?** Das ist doch bekloppt.“

**d. Technologiepaternalismus:** Möglichkeit, durch die der Technologie inhärente Objekt-Objekt-Erkennung kleinste Fehltritte systematisch und automatisch zu sanktionieren. So könnte die Papiertonne erkennen, dass fälschlicherweise eine Batterie in ihr landet, ein Medikamentenschrank, dass das Medikament vergessen wurde etc. Die resultierenden Warnsignale und Hinweise würden dem Menschen sein Fehlverhalten vorhalten, dieses womöglich öffentlich machen, sanktionieren oder automatisch unterbinden.

Die Frage ist doch, fängt es an zu piepsen, wenn ich einen Joghurt dann doch vor der Kasse abstelle, und dann gibt es ein **Signal und dann wissen die aha** ...

„Dann stelle ich mir vor, ich nehme so irgendwie schönen Kaviar oder so **und mein Computer sagt mir, das kriegst du nicht** ...“

**e. Informationssammlung und Personalisierung:** Nutzung des EPCs als ID oder Merkmalsträger, um Personen auf Ba-

**Tabelle 1 Technische Voraussetzungen für gängige Verbraucherängste**

Ängste	Wesentliche technische Voraussetzung	Standards und ökonomisch-/betriebswirtschaftliche Anreize zur Schaffung der technischen Voraussetzungen
Unbemerkt Auslesen	1 Genügend große Lesedistanz	✓ Das von der Industrie (insbesondere in USA) favorisierte UHF-Frequenzband bei 865–928 MHz erlaubt derzeit Lesereichweiten von 6–8 Metern. Diese Reichweiten sind insbesondere für Logistikanwendungen praktisch erforderlich und sind schon heute für Paletten und Kartons Standard. Die Nutzung eines weiteren Standards (z. B. 13, 56 MHz) mit geringeren Lesereichweiten (1,5 Meter) ist aufgrund doppelter Investitionen ökonomisch offen.
	2 Auslesbarkeit des EPC ohne Authentifizierung	✓ Der gegenwärtige Standard (Class 1, Generation 2) sieht keine Authentifizierung des Lesegerätes vor. Ökonomische Anreize zum Schutz der EPC Information bestehen nicht (siehe offener Aufdruck des Barcodes auf Produkten heute). Soziale Anreize bestehen aufgrund der Privacy-Debatte nur dann, wenn der EPC interpretierbar ist (s.u.). Die Implementierung von Authentifizierungsmechanismen auf dem Chip ist kostenintensiv und treibt den für den breiten Einsatz von RFID notwendigen Stückpreis nach oben.
	3 Interpretierbarkeit des EPC	✓ EPC Information kann, ebenso wie der Barcode heute, aufgelöst und interessierten Parteien zur Verfügung gestellt werden. Dazu gibt es bereits heute etablierte Dienstleister (siehe dazu Sinfos GmbH, <a href="http://www.sinfos.de/sinfosde">http://www.sinfos.de/sinfosde</a> ). ✓ In Produktkategorien, in denen ein hohes Informationsinteresse besteht, könnten freie Produktionsinformationsdienste im Internet entstehen, die auf Basis des EPCs abrufbar sind (ggf. gegen Gebühr). Ein möglicher Vorläufer ist das Greenpeace Einkaufsnetz ( <a href="http://de.einkaufsnetz.org">http://de.einkaufsnetz.org</a> ).
Verfolgbarkeit	1 und 2 sowie 4 Hohe Dichte an Lesegeräten	✓ Der Einsatz von Lesegeräten im Einzelhandel an Regalen, Ein- und Ausgängen macht eine hohe Lesedichte, insbesondere im Innenstadtbereich wahrscheinlich. Ebenso wird über den Einsatz von RFID für die ticketlose Nutzung des öffentlichen Nahverkehrs nachgedacht, über die Nutzung der Technologie an Grenzen und Flughäfen zur Passkontrolle sowie in Stadien.
	5 Verknüpfbarkeit von Bewegungsdaten zu einem Pfad	? Die Verknüpfung stellt praktisch eine Herausforderung dar, wenn für die Erstellung eines Bewegungsprofils mehrere Parteien (Besitzer von Messpunkten) kooperieren müssen. Eine Implementierung des EPC-Netzwerks mit einem zentralen EPC Discovery Service, so wie derzeit von VeriSign propagiert, könnte das Auffinden verteilter Messpunkte erleichtern. Außer für Strafverfolgungszwecke ist ein Zugriff auf die solchen jedoch nicht unbedingt absehbar.
Objektverantwortung	2 sowie 6 Speicherung des eindeutigen EPC zusammen mit dem Objektbesitzer	✓ In Verbindung mit Kundenkarten kann in den Datenbanken des Handels nachvollzogen werden, welcher Person, welches Produkt genau gehört. Diese Information wird für Kundenbindungszwecke (personalisiertes Marketing) genutzt und existiert heute auf Basis des EAN (sog. Bon-Daten). Die Speicherung entspricht i. d. R. der gesetzlich erlaubten Speicherdauer.
Technologiepaternalismus	2 und 3 sowie 7 Whitelists oder Blacklist, die Signal auslösen	✓ Existieren Whitelists oder Blacklists, die das Nichtzusammengehören von eingelesenen Objekten automatisch erkennen, so könnte dieses durch ein Signal sanktioniert oder unterbunden werden. Die Investition in solche Listen und die entsprechende Leseinfrastruktur wird vom jeweiligen Einsatzgebiet abhängig sein.
Informationssammlung & Personalisierung	2 und 3 sowie 8 Datamining 9 Schnittstellen für die Kundenansprache	✓ Für das Datamining von Kundendaten kann auf die seit Jahren im E-Commerce-Umfeld entwickelten Clusteralgorithmen zurückgegriffen werden. ✓ Neue Schnittstellen für die Kundenansprache sind für Supermärkte und Kaufhäuser in der Planung, z. B. in Form des PSA (Personal Shopping Assistant) oder von intelligenten Spiegeln. ✓ Ökonomisch sinnvoll, neue Kanäle zum Kunden auszuschöpfen und Personalisierung einzusetzen, da diese umsatzsteigernd wirkt.

sis der ihnen zugehörigen Objekte wieder zu erkennen und einzuordnen. Eine Informationssammlung über die eigenen Einkäufe, Wiedererkennung und Einordnung, so wird befürchtet, könnten zu einer systematisch personalisierten Ansprache führen. Es wird ein potenziell diskriminierendes „Vorhalten eines Spiegels“ befürchtet.

„... dann bringen sie mich in die niedrigere Preiskategorie und Frau Nachbarin steht daneben und sagt dann, **guck mal, die kriegt nur so billige Sachen angeboten** ...

„Wenn jemand Informationen sammelt, und das bedeutet ja auch immer einen Zugriff auf eine Person, und man kennt diesen Zugriff nicht, **man weiß nicht, dass da je-**

**mand zugreift, das ist ein unangenehmes Gefühl.**

„Die wissen alles über mich, und ich weiß gar nichts über die.“

f. **Krimineller Missbrauch:** Befürchtung, dass Dritte (Nachbarn, Diebe, Hacker) die Technologie missbrauchen könnten, um den eigenen Besitz auszuspähen.

„Ich finde es auch schrecklich und ich glaube auch, dass es ganz schnell **für negative Situationen ausgenutzt** werden kann.

„Ich glaube, dass es ganz schnell **für negative Situationen ausgenutzt** werden kann, für Spionage und alles mögliche.“

Gemeinsamer Nenner all dieser Ängste ist die oft unspezifische Angst vor einem Kontrollverlust:

„... da wird mit mir was gemacht, was ich **gar nicht so richtig kontrollieren kann und überblicken kann und das macht mir Angst.**

„**Wer will das alles kontrollieren, dass die Daten nicht doch irgendwie noch anders verwendet werden. Wo ist da die Sicherheit gegeben?**“

In der Tat sind die geäußerten Verbraucherängste aus technischer Sicht nicht unrealistisch. Tabelle 1 fasst die wesentlichen technischen Grundvoraussetzungen zusammen, welche erfüllt sein müssten, damit die Angstszenarien realisiert werden können und kommentiert diese mit den gegenwärtigen Standards und potenziell wirkenden ökonomischen Anreizen. Dabei wird

### Privatsphärenschutz-Checkliste 1.1

#### Ist das Privacy-Enhancing-Technology-Konzept (PET-Konzept) so geartet, ...

- |    |                                                                                                               |    |                                                                                                  |
|----|---------------------------------------------------------------------------------------------------------------|----|--------------------------------------------------------------------------------------------------|
| a. | dass es Datensparsamkeit erzwingt?                                                                            | l. | dass es aktive Schutzmaßnahmen nicht behindert? <sup>2)</sup>                                    |
| b. | dass es auf der Durchsetzung des Daten- und Privatsphärenschutzes als Grundsatz basiert?                      | m. | dass es die Entstehung und Nutzung zentraler Datenbanken vermeidet?                              |
| c. | dass es dem Bürger die Kontrolle über die Technik überträgt?                                                  | n. | dass es generell die Entstehung und Nutzung von Datenbanken vermeidet? <sup>3)</sup>             |
| d. | dass es das Tag automatisch in einen gesicherten Modus versetzt? <sup>1)</sup>                                | o. | dass es die Nutzung von Funktionalität nach dem Kauf in sicherer Weise ermöglicht? <sup>4)</sup> |
| e. | dass es nachweisbar sicherstellt, dass das automatische Versetzen in den gesicherten Modus immer stattfindet? | p. | dass es mit bestehender RFID-Technologie umgesetzt werden kann?                                  |
| f. | dass die Kommunikation abhörsicher ist?                                                                       | q. | dass die Tag-Kosten dadurch nicht <i>erheblich</i> steigen?                                      |
| g. | dass es den Bürger vor dem Hersteller schützt?                                                                | r. | dass die Tag-Kosten dadurch gar nicht steigen?                                                   |
| h. | dass es den Bürger vor dem Handel schützt?                                                                    | s. | dass dadurch kein weiterer Nachteil für die Privatsphäre entsteht? <sup>5)</sup>                 |
| i. | dass es den Schutz des Bürgers im Laden einschließt?                                                          | t. | dass dadurch eine weiterreichende Verbesserung der Privatsphäre erfolgt? <sup>6)</sup>           |
| j. | dass die Anwesenheit eines Tags im gesicherten Modus nicht erkannt werden kann?                               | u. | dass davon der Handel profitiert?                                                                |
| k. | dass es keine aktiven Schutzmaßnahmen vom Bürger erfordert?                                                   |    |                                                                                                  |

1) Tags ohne sicheren Modus werden automatisch endgültig deaktiviert ("zerstört")

2) z.B. Benutzung von Blocker-Tags. Aktive Schutzmaßnahmen sind umstritten, dennoch sollte sich aus ihrer Benutzung keine Beeinträchtigung der Schutzwirkung anderer Schutzmaßnahmen ergeben

3) Datenbanken, die eine Zuordnung zwischen Objekten und Personen, auch indirekt, ermöglichen

4) z.B. die Nutzung eines intelligenten Kühlschranks oder einer intelligenten Waschmaschine

5) weitere Nachteile sollten zusätzlich zur Checkliste notiert werden

6) weitere Verbesserungen sollten zusätzlich zur Checkliste notiert werden

**Bild 1 Übersetzung der Privacy-Checkliste des FoeBuD und der Universität Bielefeld**

deutlich, dass ein direktes Auslesen von Tag-Information ohne eine vorherige Authentifizierung eine wesentliche Wurzel vieler gefürchteter Ausnutzungs- und Missbrauchsszenarien darstellt. Eine kriminelle Motivation hinter unbemerktem Auslesen oder Verfolgen wird nicht separat aufgeführt, da die technischen Voraussetzungen dieselben sind wie in ökonomisch sinnvollen Szenarien.

Auch Mark Weiser, einer der geistigen Väter des Ubiquitous Computing, beschrieb in seinem ersten visionären Artikel zum Computer des 21. Jahrhunderts [Weis91]: „The problem [with Ubiquitous Computing] while often couched in terms of privacy, is really one of control. If the computational system is invisible as well as extensive, it becomes hard to know what is controlling what, what is connected to

what, where information is flowing, how it is being used, what is broken, and what are the consequences of any given action.“

Gäbe es hingegen für jeden Menschen eine einfache Möglichkeit, das Auslesen oder Verfolgen zu unterbinden, Warntöne abzustellen oder eine Personalisierung abzulehnen, so bestünde aus Verbrauchersicht sicherlich weniger Grund zur Beunruhigung über RFID. Eine Kernfrage der verbraucherfreundlichen Technologiegestaltung ist also, wie für den Einzelnen die Kontrolle über die Systemumwelt erhalten bleiben kann. Obliegt es jedem Einzelnen, das Kommunikationsverhalten der ihm zugehörigen Objekte zu bestimmen, so lassen sich – das ist das Kernargument dieses Artikels – Eingriffe in die Privatsphäre und Freiheitsrechte des Einzelnen bis auf wenige Missbrauchsfälle ausschließen bzw. kontrollieren.

Ängste um einen Verlust der Privatsphäre und Einbuße von Kontrolle sind in der Datenverarbeitung nicht neu. Im Folgenden wollen wir die Frage nach einer kontrollierten RFID-Technik auf das Problemfeld des Auslesevorgangs eingrenzen. Dies geschieht zum einen vor dem herausgearbeiteten Hintergrund, dass die unkontrollierte Auslesung als solche die wichtigste Wurzel der beschriebenen Missbrauchsszenarien darstellt. Zum anderen wollen wir die Ergebnisse einer Kooperation der Universität Bielefeld mit dem Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (www.foebud.org) diskutieren, in deren Rahmen eine RFID-bezogene „Privacy Checklist“ entwickelt worden ist [HeLS04]. Die Checkliste wird im Rahmen der vom FoeBuD ins Leben gerufenen Initiative „Stop

RFID“ propagiert [Foe04]. Konsistent mit unserer Argumentation plädiert sie dafür, dass Auslesevorgänge unter die Kontrolle des Nutzers gestellt werden sollten. Diese Forderung ist für Industriekreise von Interesse, da der FoeBuD mit seiner Initiative „Stop-RFID“ als die aktivste deutsche Interessensgruppe zum Thema RFID-bezogener Verbraucherschutz gilt. Die Checkliste enthält eine Reihe von Anforderungen, die in die Kategorien *Konzept*, *Schutzumfang* und *Praktikabilität* gruppiert werden können (siehe Bild 1). Ungeachtet der gelegentlich als tendenziös interpretierbaren Formulierungen stellt die Liste einen interessanten Leitfadens dar, die wir in die folgende Evaluation von RFID-relevanten Datenschutztechnologien einfließen lassen werden.

Die erste Gruppe der Forderungen bezieht sich auf das Realisierungskonzept der jeweiligen Technik (*a* bis *f*, *j* bis *o*). Es wird unterschieden, ob die Technik den Schutz als Voreinstellung bietet oder dieser Schutz erst nach zusätzlichen Maßnahmen des Konsumenten zum Tragen kommt. Insbesondere wird in Punkt *k* gefordert, dass der Schutz nicht defensiver Natur sein soll, wie etwa die unten beschriebenen Blocker Tags. Auch wird in Punkt *e* die Frage nach der Beweisbarkeit der Sicherheitseigenschaften gestellt. Diese Frage zielt auf das notwendige Vertrauen der Kunden bzw. die Angst vor versteckter Überwachungsfunktionalität ab. Hier ist insbesondere das so genannte „Presence Spotting“ betroffen, wobei die Anwesenheit entsprechend ausgestatteter RFID-Tags festgestellt werden kann, auch wenn diese sich in einem geschützten Modus befinden. Ein Auslesen des EPC ist auch hier ausgeschlossen, aber vor dem Feststellen der Anwesenheit hilft nur die physische Zerstörung des Tags. Vor- und Nachteile dieses „Presence Spotting“ müssen noch intensiver diskutiert werden: Einerseits wird von Datenschützern häufig eine Kennzeichnungspflicht gefordert, wobei die Kennzeichnung, konsequent weitergedacht, auch technisch auslesbar sein sollte, insbesondere um den Einsatz „versteckter“ Tags wirksam zu verhindern. Andererseits wird u. a. im Punkt *j* der Checkliste von RFID-Tags im geschützten Modus gefordert, für Lesegeräte *nicht* wahrnehmbar zu sein, da allein das Vorhandensein von RFID-Tags Rückschlüsse auf den Benutzer ermöglichen könnte, vor allem solange nur wenige Produkte auf diese Weise gekennzeichnet sind. Eine wichtige Anforderung ist auch der Verzicht auf zentrale Datenbanken, welche die Zuordnung zwischen Nutzer und Ob-

jekt speichern (Punkt *m*). Die Nutzung solcher Datenbanken würde zwar das direkte Auslesen von vertraulichen Daten durch Nichtautorisierte verhindern (da der Tag keine derartigen Informationen enthält), andererseits begibt man sich in die informationelle Abhängigkeit des Datenbankbetreibers.

Die zweite Gruppe von Forderungen (*g* bis *i*) bezieht sich auf das Einsatzgebiet, bzw. auf die durch die Schutztechnik überdeckten Bereiche im Lebenszyklus eines Produktes. Hier halten die Autoren der Checkliste es für notwendig, dass Kunden Informationstransparenz gegenüber dem Handel einschränken können, indem sie der Nutzung von RFID-Diensten auf der Verkaufsfläche bewusst nicht zustimmen. Auch vor der Weitergabe von Produktnutzungsdaten an den Handel oder Produzenten (z. B. via des viel zitierten „intelligenten“ Kühlschranks) soll sich der Kunde schützen dürfen.

Die letzte Gruppe der Anforderungen (*p* bis *u*) bezieht sich auf Kriterien zur Evaluation der Praktikabilität von RFID-Schutzlösungen. Hier stehen erwartungsgemäß Kosten, technische Umsetzbarkeit und Nutzeneffekte im Vordergrund.

Grundtenor der Checkliste ist der Schutz der Privatsphäre der Konsumenten gegen jeden beliebigen Dritten. Dies kann jedoch nur gewährleistet werden, wenn kein Dritter (genannt sind in *g* Hersteller, in *h* Händler, in *m* Datenbankbetreiber und in *f* Außenstehende) in der Lage ist, Informationen über den Konsumenten ohne dessen Zustimmung zu erhalten. Die Checkliste fordert folglich die direkte Kontrolle des Nutzers über seine RFID-Tags.

### 3 Technische Schutzmaßnahmen

Im Folgenden wird vor dem Hintergrund dieser Kriterien und unserer eigenen Analysen eine Auswahl von verfügbaren Schutztechniken vorgestellt. Wir beschreiben diese Techniken im Detail und diskutieren insbesondere die Frage der Nutzerkontrolle.

#### 3.1 Abschirmung, Blocker-Tags und Datenschutzagenten

Datenschutzprobleme entstehen, wenn RFID-Tags unbemerkt und ohne Zustimmung des Nutzers ausgelesen werden können. Eine Möglichkeit zur Kontrolle der Auslesevorgänge wäre die *Abschirmung* al-

ler RFID-Tags (beispielsweise durch in Taschen eingenähte Metallfolien).

*Blocker-Tags* [JuRiS03] sind besonders effektive Störsender, die in Kenntnis des Kommunikationsprotokolls zwischen Tag und Lesegerät immer genau dann „dazwischen senden“, wenn andere Tags antworten wollen. So versteht das Lesegerät, welches den Störer auch noch mit der notwendigen Energie versorgt, im Endeffekt keinen der RFID-Tags. Fraglich ist jedoch, ob eine derartige „Denial-of-Service“-Strategie skalierbar ist und flächendeckend eingesetzt werden kann. Darüber hinaus ist zu bemerken, dass Blocker-Tags je nach Lage der Lesenantenne unzuverlässig sind und nicht nur die eigene Tag-Reader-Kommunikation stören, sondern auch die anderer Personen [Langh04]. Der Einsatz von solchen Störsendern scheint daher keine valide technische Antwort auf das Problem eines kontrollierten Auslesens im Sinne der oben beschriebenen Ängste (Kontrollverlust, Verfolgbarkeit) zu sein.

Eine weitere wichtige Schutztechnologie sind *Datenschutz-„Agenten“*. Bekannt geworden sind derartige Ansätze durch das vom W3C-Konsortium betriebene Projekt *Platform for Privacy Preferences (P3P)* in dem Datenaustauschkonditionen zwischen Internetseiten und deren Nutzern definiert werden [Cran03]. Analog dazu ist die Grundidee bei [Floer04; Langh03], wonach sich das Lesegerät gegenüber einem Transponder authentifiziert und dabei Zweck und Umfang seines Einlesegesuchs mitteilt. Auf Nutzerseite gibt es eine Art *Schutz-Tag* (im Internet analog *Privacy Bird* [CrFaR02]), in dem die Datenschutzpräferenzen einer Person gespeichert sind. Mithilfe eines Agentensystems soll abgeglichen werden, ob die Datenschutzpräferenzen einer Person mit den Zielen des Auslesevorgangs vereinbar sind. Wenn ja, kann der Auslesevorgang vonstatten gehen. Wenn nein, wird die Person entweder gewarnt oder der Auslesevorgang wird abgelehnt. Grundsätzlich enthält dieser Vorschlag wichtige Gestaltungsaspekte für die kontrollierte Authentifizierung von Lesegeräten und impliziert auch, dass Nutzer die Wiedererkennung ihrer Objekte beeinflussen können. Delegieren Verbraucher jedoch bei ungeschützten Tags die Entscheidung über eine Auslesung an den Schutz-Tag, was hier grundsätzlich vorgesehen ist, so ergibt sich das Problem einer reduzierten Kontext- und Zweckdarstellung, welche bereits bei P3P stark kritisiert worden ist [SpGrB01] und welche insbesondere bei einer längerfristig gültigen Pauschalzusage (*Opt-in*) zu einem Kontrollverlust führt.

Entscheidend aber ist, dass die Lösung vorsieht, dass RFID-Tags standardmäßig für Lesegeräte zugänglich sind. Kontrollierte Auslesung wird somit auf das Recht reduziert, Informationen des Lesegeräts zu vertrauen, über dessen Konfiguration der Verbraucher aber keine Kontrolle hat.

Die Techniken dieses Absatzes erfordern in jedem Fall eine aktive, vom Nutzer zu betreibende Schutztechnik. Standardmäßig ist der Nutzer jedoch ungeschützt, was den Anforderungen  $b$ ,  $c$  und  $k$  der Checkliste widerspricht.

### 3.2 Kill-Funktion

Eine extreme Form der Deaktivierung ist das vollständige und unwiderrufliche Abschalten der Tags. Laut Spezifikation ist für alle Tags nach den EPC-Standards ein Kill-Befehl vorgesehen [EPC03], wobei jeder Tag ein individuelles Passwort besitzt, mit welchem sich ein zum „Kill“ berechtigtes Lesegerät vor Ausführung autorisieren muss. Der Kill-Befehl wird des Öfteren als Allheilmittel für die Lösung der mit RFID assoziierten Datenschutz- und Kontrollprobleme angesehen. Weder ein Tracking von Personen, noch eine Objektverantwortlichkeit, noch ein Missbrauch, noch eine Personalisierung, noch Technologiepaternalismus wären möglich – wenn jeder RFID-Tag standardmäßig und zuverlässig an der Kasse deaktiviert wird (Anforderung  $a$ ,  $b$  und  $d$  der Checkliste). Die Herangehensweise liegt nahe: Schaltet man die Technik aus, so hat man auch kein Problem mehr.

Nun verzichtet man damit aber natürlich auch auf die Nutzenpotenziale außerhalb von Logistikkette und Supermarkt, die heute vielerorts für den Einsatz von RFID-Technologie gesehen werden (Anforderung  $o$ ). Zu nennen sind hier beispielsweise vereinfachte Prozesse für die Garantie-, Rückgabe- und Recyclingabwicklung, neue Dienste im Sicherheitsbereich und innovative Heimapplikationen wie eine „intelligente“ Mikrowelle oder der notorische „intelligente“ Kühlschrank. Es ist daher durchaus fraglich, in wie weit sich Verbraucher konsequent zu einem kompletten Verzicht auf RFID-basierte Dienste nach dem Kauf entschließen würden.

Möchte man die Nutzenpotenziale von RFID nach dem Kauf wahrnehmen und gleichzeitig Kontrolle über das Kommunikationsverhalten der den eigenen Objekten zugeordneten Tags ausüben, so ist es nötig, auf diese direkt einzuwirken und je nach Kontext die Preisgabe von Information entweder zuzulassen oder abzulehnen. Hierbei ist wichtig, dass nicht nur ein Au-

thentifizierungsverfahren vorgesehen ist, sondern auch ein standardmäßiger Ausleseschutz [SpBe04]. Im Gegensatz zu der oben diskutierten P3P-Lösung entsteht dadurch genau die Umkehrung von Kontrolle – was aus Sicht im Sinne des Verbraucherschutzes wünschenswert ist – nämlich grundsätzliche standardmäßige Anonymität gepaart mit bewusster Offenlegung bei Vorhandensein eines entsprechend interessanten Dienstes.

### 3.3 Hash Lock

Das *Hash-Lock-Verfahren* [ERSW03] sieht eine Zugriffsbeschränkung auf RFID-Tags mittels einer im Tag integrierten kryptographischen Hashfunktion vor. Eine Hashfunktion stellt einen hohen Zugangsschutz nach gegenwärtigem Stand der Technik dar. Geht ein Produkt in den Besitz eines Kunden über, so wird der Tag mit einem Hashwert  $h = \text{Hash}(k)$  über einem zufällig gewählten Schlüsselwert  $k$  gesperrt und der Datensatz  $(h, k)$  an eine private Datenbank des Kunden übergeben. Ein auf diese Weise gesperrter Tag sendet einem Lesegerät auf Anfrage nur noch  $h$  und verschweigt den EPC oder andere Tag-Daten.

Ein mit dem Hash-Lock-Verfahren gesperrter RFID-Tag erlaubt demnach nur solchen Lesegeräten Zugriff auf den EPC, welche einen Zugang zu der privaten Datenbank des Besitzers haben und den zu  $h$  korrespondierenden  $k$ -Wert als Authentifizierungsmerkmal senden können. Der RFID-Tag überprüft diesen mittels seiner integrierten Hashfunktion. Datenschutzprobleme wie unvorhergesehene Objektverantwortlichkeit, krimineller Missbrauch und mögliche Personalisierung werden durch diese Technik effektiv unterbunden. Aus Datenschutzsicht negativ (Punkt  $s$  der Checkliste) ist, dass der Tag wieder erkannt werden kann: Der an jedes Lesegerät ausgesendete Hashwert  $h$  stellt eine langfristig verwendete (wenngleich von Außenstehenden nicht mit dem EPC verknüpfbare) Tagkennung dar. Das Verfahren ist daher nur eingeschränkt geeignet, die Privatsphäre des Nutzers zu schützen. Etwas eingeschränkt wird die Praktikabilität der Lösung ferner durch die Notwendigkeit einer Datenbank im Nutzerbereich, die regelmäßig gepflegt und mit allen Lesegeräten einer Person permanent vernetzt sein muss.

### 3.4 Randomized Hash Lock

Bei dem *Randomized-Hash-Lock-Verfahren* [ERSW03] handelt es sich um eine Weiterentwicklung des ursprünglichen Hash-

Lock-Verfahrens mit dem Ziel, das Wiedererkennungsproblem zu lösen. Ein gesperrter Tag sendet hier nun keinen festen Hashwert  $h$  mehr aus. Stattdessen wird für jede Leseanfrage  $n$  vom RFID-Tag ein neuer Hashwert  $h_n$  erzeugt, und zwar auf Basis des EPCs eines Objekts und einer Zufallszahl  $r_n$ . Die Zufallszahl  $r_n$  und  $h_n = \text{Hash}(\text{EPC} \mid r_n)$  werden auf Anfrage eines Lesegerätes ausgesendet. Nur der Besitzer des Tags, der vorher den EPC eines in seinem Besitz befindlichen Produkts in einer privaten Datenbank abgespeichert hat, ist in der Lage, mithilfe von  $r_n$  und  $h_n = \text{Hash}(\text{EPC} \mid r_n)$  auf den richtigen EPC zu schließen.

Dieses Verfahren benötigt ebenso wie das ursprüngliche Hash-Lock-Verfahren eine vernetzte Datenbank im Nutzerbereich. Wichtigster Nachteil ist jedoch der hohe rechnerische Aufwand für die Ermittlung des EPC auf Basis von  $r_n$  und  $h_n = \text{Hash}(\text{EPC} \mid r_n)$ . Da die Hashfunktion nicht invertiert werden kann, muss auf Basis von  $r_n$  für jeden Datenbankeintrag ein Hashwert berechnet und mit  $h_n$  verglichen werden, um den richtigen EPC zu isolieren. Der Aufwand ist somit linear in der Anzahl der Datenbankeinträge, was zu Skalierungsproblemen führen kann.

### 3.5 Private ID

Eine wesentliche Vereinfachung des Hash-Lock-Verfahrens stellt der *Private-ID-Ansatz* [Inoue04] dar. Hier wird bei Übergabe des Objekts an den Kunden der EPC auf dem Tag einfach durch eine frei wählbare Kennung, eben die *Private ID*, ersetzt. In einer privaten Datenbank des Kunden wird dann die Zuordnung von Private ID zu EPC gespeichert. Fragt ein Lesegerät einen Tag an, erhält es nur die ID des Tags. Zum richtigen EPC zugeordnet werden kann diese jedoch nur, ähnlich den obigen Lösungen, durch den Besitzer der Datenbank. Problematisch ist bei diesem Verfahren neben dem schon beschriebenen Wiedererkennungsproblem, dass keine praktikable Methode vorgeschlagen wurde, wie das unautorisierte Setzen oder Löschen der Private ID verhindert werden kann.

### 3.6 Das Passwort-Modell: Standardmäßige Anonymität und einfache Authentifizierung

Wie die bereits vorgestellten Verfahren basiert das von den Autoren in [SpBe04] vorgeschlagene Passwort-Modell auf einem standardmäßigen Schutz der RFID-Tags, welcher ein Auslesen ohne Zustimmung

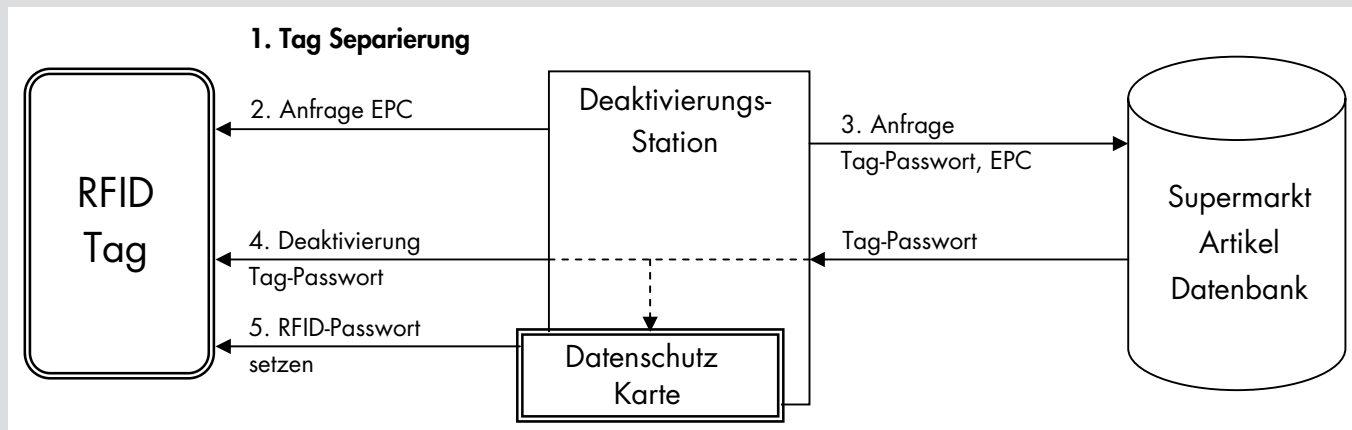


Bild 2 Prozessablauf an der Deaktivierungsstation

des Nutzers verhindert. Die Grundidee ist einfach: Der RFID-Tag wird mit einer Aktivierungsfunktion (*Enable/Disable Function*) ausgestattet. Diese Funktion aktiviert bzw. deaktiviert bestimmte Funktionen des RFID-Tags, insbesondere solche, welche den (Lese-)Zugriff auf den EPC ermöglichen. Ein aktivierter RFID-Tag verhält sich so wie im EPC-Standard vorgesehen: Jedes Lesegerät kann nach erfolgter Separierung eines einzelnen RFID-Tags im Lesebereich den EPC erfragen. Die Infrastruktur in Supermarkt und Logistik muss daher kaum angepasst werden: Jeder RFID-Tag ist aktiv und besitzt ein individuelles „Kill“- bzw. Deaktivierungspasswort, welches analog zum Kill-Ansatz über die Artikel-datenbank der Supermarktkasse verfügbar gemacht wird.

An der Kasse oder einer separaten Deaktivierungsstation wird ein RFID-Tag jedoch nicht durch den Kill-Befehl zerstört, sondern nur temporär deaktiviert. Zusätzlich wird das Tag-Passwort durch ein von Verbraucher gewähltes „RFID-Passwort“ ersetzt, welches beispielsweise auf dessen „Datenschutz-Karte“ gespeichert ist (Bild 2). Deaktivierte RFID-Tags erwarten nach der Separierung das korrekte Passwort zum Auslesen des EPC bzw. zur (Re-)Aktivierung, ansonsten wird der Zugriff verwehrt. Im EPC-Standard für Tags der Generation 2 [AutID05] ist ein Passwortschutz nur zur Absicherung der Kill-Funktion und zur Beschränkung der Schreibrechte vorgesehen. Ein aktivierbarer Passwort-Schutz des Lesezugriffs wie hier vorgeschlagen ist nicht vorgesehen. Allerdings wurde der Anti-Kollisions-Algorithmus so weiterentwickelt, dass eine Separierung der im Lesebereich befindli-

chen Tags ohne Aufdeckung des EPC erfolgt.

Die entscheidende Vereinfachung in unserem Verfahren besteht darin, dass die Kontrolle deaktivierter RFID-Tags nicht mit Tag-spezifischen Schlüsseln ausgeübt wird. Stattdessen hat jeder Verbraucher ein einziges (bzw. einige wenige) Passwort(e) für sämtliche ihm zugehörigen Objekte. Dieses „RFID-Passwort“ ist analog zur heutigen Zugriffsrechtgestaltung im Onlinereich für nur einen Dienst gültig, nämlich den der Deaktivierung und Aktivierung der eigenen Produkte.

Hätte jeder RFID-Tag ein anderes Passwort, wäre wie bei *Private ID* oder *Hash Lock* eine Tag-Kennung erforderlich, die auch im deaktivierten Zustand ausgesendet wird, um dem Lesegerät die effiziente Ermittlung des richtigen Passwortes zu ermöglichen. Dies führt zu dem oben beschriebenen Wiedererkennungsproblem. Das verbraucherspezifische „RFID-Passwort“ ermöglicht hingegen den Verzicht auf die Tag-Kennung, da das zu verwendende Passwort dem berechtigten Lesegerät ja bekannt ist, bzw. nur einige wenige Passwörter durchprobiert werden müssen. Ohne Kenntnis des Passwortes wird nur der Separierungs-Algorithmus ausgeführt – wodurch *Presence Spotting* ohne Identifizierung ermöglicht wird, und damit die Anforderung *j* der Checkliste nicht mehr erfüllt ist.

Das Passwort-Modell legt zwei Realisierungsvarianten nahe: In einer Basisvariante wird das Passwort unverschlüsselt übertragen, so dass der Funktionsumfang der heute preiswert verfügbaren RFID-Tags (z. B. I-Code SL2 ICS11 von Philips [Phili03]) bereits ausreicht. Das Kommunikations-

protokoll ändert sich im deaktivierten Zustand nur in so weit, dass für bestimmte Befehle das Passwort übertragen und überprüft wird. In einer erweiterten Variante wird das Passwort ausschließlich verschlüsselt übertragen, wofür dann allerdings eine Hash-Funktion auf dem RFID-Tag realisiert sein und bei jeder Passwortüberprüfung ausgeführt werden muss. Bereits die Basisvariante schützt gegen Massenüberwachung: Selbst wenn die RFID-Passwörter vieler Menschen abgehört würden, wäre keine massenhafte Identifizierung von Passanten möglich, da gegenüber jeder Person jedes einmal abgehörte Passwort durchprobiert werden müsste. Die erweiterte Version schützt hingegen auch gegen individuelle Überwachung Einzelner. Durch die hohe Sicherheit kann das Passwort zudem zum Beweis des Besitzes verwendet werden: Nur der berechnete Nutzer ist in der Lage, den Tag zu kontrollieren. Gestohlene Ware wäre unverkäuflich, wenn zusätzlich noch die Echtheit des Tags durch ähnliche kryptographische Verfahren unter Einbeziehung des Herstellers überprüfbar wäre.

### 3.7 Zero Knowledge Ansatz

Einen ganz ähnlichen Ansatz verfolgt Engberg et. al. [EnHJ04]. Ebenso wie bei dem Passwort-Modell wird ein Gruppenschlüssel (gemeinsames Passwort) für verschiedene Tags eines Bereiches vorgeschlagen. Allerdings verwendet Engberg ein komplexeres Authentifikationsprotokoll: Ein Lesegerät sendet folgende Nachricht:

```
<t, r XOR hash(t XOR key),
  hash(r XOR key)>
```

wobei  $t$  ein Zeitstempel,  $r$  eine Zufallszahl und  $key$  der Gruppenschlüssel ist. Der RFID-Tag kann diese Berechnung nachvollziehen und somit verifizieren, dass das Lesegerät den Gruppenschlüssel kennt. Der letzte akzeptierte Zeitstempel muss jedoch im RFID-Tag gespeichert werden, um Wiederholungsangriffe zu verhindern. Zudem müssen alle Lesegeräte synchronisiert werden. Der Vorteil dieser Methode ist einerseits der Verzicht auf die Notwendigkeit eines Zufallsgenerators im RFID-Tag, andererseits steht der Wert  $r$  für die Verschlüsselung eines Kommandos oder einer Antwort des Tags zur Verfügung, da ein Abhörer  $r$  nicht ermitteln kann. Eine unverschlüsselte Übertragung des EPC kann so vermieden werden. Zusätzlich propagiert Engberg die Löschung des EPC und die Ersetzung durch einen zufälligen Wert, ähnlich wie bei *Private ID*. Der Vorteil ist ein besserer Schutz vor physischen Angriffen auf die RFID-Tags, wegen des Verzichts auf jegliche identifizierende Daten. Neben der dadurch notwendigen Datenbank im Nutzerbereich ist der wesentliche Nachteil jedoch die fehlende mehrseitige Sicherheit: Ein einmal gesperrter Tag kann niemals gegenüber Dritten beweisen, einen bestimmten EPC zu besitzen – dieser wurde ja gelöscht. Es müsste diesbezüglich dem bisherigen Besitzer völlig vertraut werden. Bearbeitung von Garantiefällen wäre dann auf Basis der RFID-Tags nicht möglich. Zudem ist fraglich, ob ein Schutz des EPC gegen diese relativ theoretischen Angriffe sinnvoll ist, da der Angreifer noch immer den Gruppenschlüssel extrahieren und somit alle Tags dieser Gruppe kontrollieren könnte.

### 3.8 Fazit

Alle vorgeschlagenen Authentifizierungsverfahren haben gemeinsam, dass sie eine standardmäßige Anonymität gewährleisten und die Auslesung der Tag-Inhalte vollständig in die Kontrolle des Endnutzers bzw. -verbrauchers transferieren. Andererseits führen all diejenigen Ansätze, die Hash-Funktionen auf den Tags einsetzen, derzeit noch zu erheblich erhöhten Tagkosten. Eine Einschränkung der Praktikabilität stellt die außer beim Passwort-Modell notwendige vernetzte Datenbank da. Eine aus Datenschutzgründen problematische zentrale Datenbank, wie in der Checkliste unter Punkt  $m$  angesprochen, benötigt hingegen keine der Techniken. Einen Schutz im Supermarkt (Anforderung  $i$ ) kann keine der Techniken bieten, da der Supermarkt vor und an der Kasse zwangs-

läufig Zugang zum RFID-Tag haben muss.

Individuelle Tag-spezifische Passwörter haben entweder einen hohen Berechnungsaufwand beim Auslesen durch berechtigte Lesegeräte (*Randomized Hash Lock*) oder aber die Aussendung einer verfolgbaren Kennung auch an unberechtigte Lesegeräte (*Private ID, Hash Lock*) zur Folge – was aus Datenschutzsicht nachteilig ist (Punkt  $s$  der Checkliste). Die im Passwort-Modell und dem Ansatz von Engberg verwendeten Gruppenpasswörter umgehen diesen Nachteil, ermöglichen aber den Zugriff auf alle Tags der „Gruppe“, wenn dieses Passwort einmal abgehört werden konnte. Die kurze und relativ stabile Liste von Gruppenpasswörtern in einem Haushalt vereinfacht das Handling: Statt alle Geräte zu vernetzen genügt eine einmalige Kopie der Liste. Im Haushalt würden die RFID-Tags dauerhaft deaktiviert bleiben und Auslesevorgänge nur nach Passwortverifikation erfolgen. Eine Reaktivierung der RFID-Tags ist nur dann notwendig, wenn Produkte (vorübergehend) an einen Dritten übergeben werden, wie z. B. bei Abgabe eines Kleidungsstücks bei einer Textilreinigung. Das Reinigungsunternehmen kann nun den EPC des Tags auslesen und zur Abwicklung des Auftrages verwenden, jedoch auf Grund der Unkenntnis des Passwortes den RFID-Tag nicht kontrollieren.

Passwort-Modell, *Randomized Hash Lock* und das Modell von Engberg erfüllen die wesentlichen Punkte der Privacy-Checkliste. In Punkt  $f$  (Abhörsicherheit) bietet das Verfahren von Engberg Vorteile. „Presence Spotting“, Punkt  $j$ , wird von den

Autoren wegen der möglichen Erkennung „versteckter“ Tags eher positiv gesehen; dies ist aber auch kontextabhängig und letztlich Ansichtssache. Engberg propagiert hingegen die von seinem Verfahren ermöglichte Nichtnachweisbarkeit deaktivierter Tags. Mit der beim Passwort-Modell vorgeschlagenen Tag-Deaktivierung an der Supermarktkasse könnten die Forderungen  $b$  bzw.  $d$  der Checkliste erfüllt werden: Der Normalfall ist die Deaktivierung der RFID-Tags, ohne dass der Verbraucher dies explizit fordern muss. Verfügt ein Verbraucher über keine „Datenschutz-Karte“ – oder möchte er sich nicht mit der Technologie befassen – könnte das jeweils notwendige Aktivierungspasswort beispielsweise für Garantiefälle einfach auf die Rechnung gedruckt werden. Die Basisvariante des Passwort-Modells führt zudem zu einer nur minimalen Erhöhung der Kosten für Tagherstellung, Infrastruktur und Organisation/Einsatz im Vergleich zu einem Szenario mit Einsatz der Kill-Funktion, wo der wesentliche Aufwand beim Bereitstellen der individuellen Kill-Passwörter an der Deaktivierstation anfällt.

## 4 Resümee

Industrie und Handel sehen sich an der Schnittstelle zum Kunden mit der Herausforderung konfrontiert, dass viele Menschen die Vorstellung von „lebenden“ Chips in ihren Objekten als unangenehm empfinden. Die empirischen Arbeiten am Auto-ID Center und an der Humboldt-Universität zu Berlin haben diese Ängste

### Abstract

#### RFID: Consumer Fears and Consumer Protection

RFID introduction is a hotly debated public policy issue. The technology enables physical environments to become more interactive and supportive by tagging each item with a chip that wirelessly communicates with a service-enriched backend infrastructure. Based on a number of user studies at Humboldt-Universität and at the Auto-ID Center, this article presents the major fears associated with RFID introduction. We show to what extent these fears are justified and derive a number of system requirements for giving users more control over an RFID-enabled IT infrastructure. After presenting several recent technical proposals for privacy protection, we focus on the question of controlled access to RFID tags. We conclude with a proposal for an easy-to-use private password model.

**Keywords:** Radio Frequency Identification (RFID), Privacy, Privacy Enhancing Technologies (PETs), Control, Technology Paternalism, Cryptography, Password-Protection

konkretisiert. Dabei stehen die Möglichkeiten einer systematischen Überwachung durch unbemerktes Auslesen und Wiedererkennen von Personen durch ihre Objekte, Objektverantwortlichkeit, die unkontrollierbare und teilweise als unangenehm empfundene Zuordnung zu Konsumentenzielgruppen sowie ein potenzieller Technologiepaternalismus und ein genereller Kontrollverlust im Vordergrund der Befürchtungen.

Um diesen Ängsten zu begegnen, wurden diverse Schutztechnologien vorgeschlagen. Die Unterschiede zwischen den vorliegenden Vorschlägen betreffen die Frage, wie viel und wo sie Kontrolle durch den Verbraucher vorsehen. Geht man davon aus, dass es die „intelligente“ Umgebung sein soll, die aktiv (i.A. zu Werbezwecken) auf den Menschen zugeht, so wäre es erforderlich, sich z. B. durch Blocker-Tags vor dieser zu schützen – man geht in die Defensive. RFID-Tags müssten in diesem Szenario für Lesegeräte grundsätzlich auslesbar sein. Geht man jedoch umgekehrt davon aus, dass der Mensch aktiv auf die Systemumgebung zugeht, wenn er Informationen oder Dienste sucht (z. B. durch Abfrage eines RFID-Tags, welches zu Informationszwecken unter einem EPCGlobal-Logo an einem Konzertplakat angebracht ist), so müssten die RFID-Tags grundsätzlich nicht zugänglich sein. Der Verbraucher selbst entscheidet, wann er mehr von seiner „intelligenten“ Umgebung erfahren möchte, und es wird letztendlich die Dienstgüte oder der Kontext sein, die darüber entscheiden, wann er ein Angebot wahrnimmt. Damit geht jedoch auch eine unterschiedliche Qualität an RFID-Tags einher. Will man Hashfunktionen oder auch nur wiederbeschreibbaren Speicher in massenmarktfähige Tags integrieren, so werden diese deutlich teurer. Dieser Trend wird von der Industrie nicht begrüßt, solange man noch bei den einfachsten Tags unter einem zu hohen Preisniveau leidet. Allerdings glauben wir, dass die RFID-Einführung im Handel ohne derartige Investitionen in eine breitere Technikakzeptanz nicht gelingen kann.

Es verbleibt letztlich die Frage nach der einfachen Handhabung der vorgeschlagenen Sicherheitsfunktionen. Für den Massenmarkt glauben wir, dass in vielen Anwendungsbereichen guter Schutz mit einfacher Handhabung besser ist als sehr guter Schutz mit schwieriger Handhabung. Diese Prämisse hat sich in dem von uns vorgeschlagenen Passwortverfahren niedergeschlagen, welches wir mit diesem Artikel zur Diskussion stellen.

## Danksagung

Die Autoren danken der Metro AG und dem Metro Future Store Team für die vertrauensvolle Zusammenarbeit, insbesondere bei der Durchführung der in diesem Artikel diskutierten empirischen Studien.

## Literatur

- [A-IDA03] *Auto-ID Center*: EPC-256: The 256-bit Electronic Product Code Representation. [http://archive.epcglobalinc.org/aboutthetech\\_research.asp](http://archive.epcglobalinc.org/aboutthetech_research.asp), Massachusetts Institute of Technology (MIT), Cambridge, USA 2003.
- [A-IDC03] *Auto-ID Center*: The Use of the Electronic Product Code. [http://archive.epcglobalinc.org/aboutthetech\\_research.asp](http://archive.epcglobalinc.org/aboutthetech_research.asp), Massachusetts Institute of Technology (MIT), Cambridge, USA 2003.
- [Beckw03] *Beckwith, R*: Designing for Ubiquity: The Perception of Privacy. In: IEEE Pervasive 2 (2003) 2, S. 40–46.
- [BCLMR04] *Bobn, Jürgen; Coroama, Vlad; Langheinrich, Marc; Mattern, Friedemann; Robs, Michael*: Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications. In: Journal of Human and Ecological Risk Assessment 10 (2004) 5.
- [ChIa01] *Churchill, Gilbert; Iacobucci, Dawn*: Marketing Research: Methodological Foundations. South-Western College Pub., 2001.
- [Cran03] *Cranor, Lorrie Faith*: P3P: Making Privacy Policies More Useful. 2003. S. 50–55.
- [CrFaR02] *Cranor, Lorrie Faith; Reidenberg, Joel*: Can user agents accurately represent privacy notices? The 30th Research Conference on Information, Communication, and Internet Policy. Alexandria, Virginia, USA, 2002.
- [Duce03] *Duce, Helen*: Public Policy: Understanding Public Opinion. University of Cambridge, Cambridge, UK, 2003.
- [ERSW03] *Engels, Daniel; Rivest, Ronald; Sarma, Sanjay; Weis, Stephen*: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, SPC 2003. Springer Verlag, Boppard, USA, 2003.
- [EPC03] *EPC-Global*: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. [http://www.epcglobalinc.org/standards\\_technology/Secure/v1.0/UHF-class0.pdf](http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf), 2003.
- [Floer04] *Floerkemeier, Christian; Schneider, Roland; Langheinrich, Marc*: Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. 2nd International Symposium on Ubiquitous Computing Systems. Tokyo, Japan, 2004.
- [FoeB03] *FoeBuD e.V.*: Positionspapier über den Gebrauch von RFID auf und in Konsumgütern. FoeBuD e.V., Bielefeld 2003, S. 14.
- [FoeB04] *FoeBuD e.V.*: Studie über Schutz der Privatsphäre vor RFID online. <http://stoprfid.de/aktuell/aktuell18.html>, 2004-11-06.
- [GCI03] *GCI, Global Commerce Initiative*: Global Commerce Initiative EPC Roadmap. 2003.

- [Inoue04] *Inoue, Yasuura*: RFID Privacy Using User-controllable Uniqueness. RFID Privacy Workshop 2004. <http://www.rfidprivacy.org>, Massachusetts Institute of Technology (MIT), Cambridge, USA, 2004.
- [HeLS04] *Hennig, Jan; Ladkin, Peter; Sieker, Bernd*: Privacy-Enhancing Concepts for RFID Technology Scrutinised. RVS Group, Universität Bielefeld, Bielefeld 2004.
- [JuRS03] *Juels, Ari; Rivest, Ronald; Szyldo, Michael*: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. 10th Annual ACM CCS 2003. <http://theory.lcs.mit.edu/~rivest/>, 2003.
- [Langh03] *Langheinrich, Marc*: A Privacy Awareness System for Ubiquitous Computing Environments. 4th International Conference on Ubiquitous Computing, UbiComp2002. Springer-Verlag, Göteborg, Sweden, 2003.
- [Langh04] *Langheinrich, Marc*: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. <http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf>, ETH Zürich, Zürich 2004.
- [Leder02] *Lederer, Scott; Dey, A.*: A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments. UC Berkeley, Berkeley, USA, 2002.
- [Phili03] *Philips*: Data Sheet to Philips I-Code SL2 ICS11. <http://www.semiconductors.philips.com/acrobat/other/identification/SL092030.pdf>, 2003.
- [Pohl04] *Pohl, Hartmut*: Hintergrundinformationen der Gesellschaft für Informatik e.V. (GI) zu RFID – Radio Frequency Identification. 2004.
- [SpBe04] *Spiekermann, Sarah; Berthold, Oliver*: Maintaining privacy in RFID enabled environments – Proposal for a disable-model. In: *Robinson, Philip; Vogt, Harald; Wagealla, Waleed (Eds.)*: Privacy, Security and Trust within the Context of Pervasive Computing. Springer Verlag, Vienna, Austria, 2004.
- [SpGrB01] *Spiekermann, Sarah; Grossklags, Jens; Berendt, Bettina*: E-privacy in 2nd generation E-Commerce. Proceedings of the 3rd ACM Conference on Electronic Commerce EC'01. ACM Press., Tampa, Florida, USA, 2001.
- [SpGue04] *Spiekermann, Sarah; Guenther, Oliver*: RFID & Privacy: Consumer Perspective & Technology Insights. <http://www.m-lab.ch/rfid/ws.html>, St.Gallen, CH, 2004.
- [SpZi04] *Spiekermann, Sarah; Ziekow, Holger*: Technische Analyse RFID-bezogener Angstsznarien. <http://www.wiwi.hu-berlin.de/~sspiek/phdresearch.htm>, Institut für Wirtschaftsinformatik – Humboldt Universität zu Berlin, Berlin 2004, S. 44.
- [Weis91] *Weiser, Mark*: The Computer for the 21st Century. 1991, S. 94–104.
- [Wolfr04] *Wolfram, Gerd*: RFID-Fahrplan der Metro Group im Detail. Präsentation gehalten auf dem RFID-Kongress für die Partner der METRO Group Köln, 2004-05-14.