Bundesamt
für Sicherheit in der
Informationstechnik

Risiken und Chancen des Einsatzes von RFID-Systemen

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Die vorliegende Studie wurde im Auftrag und in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer interdisziplinären Kooperation vom IZT – Institut für Zukunftsstudien und Technologiebewertung und der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA) erstellt.

Die dieser Studie zugrunde liegende Expertenbefragung wurde im Sommer 2004 durchgeführt. Der vorliegende Bericht spiegelt ausschließlich die Meinungen der mitwirkenden und befragten Expertinnen und Experten sowie der ausgewerteten Literatur wider.

Bundesamt für Sicherheit in der Informationstechnik

Risiken und Chancen des Einsatzes von RFID-Systemen

Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit

SecuMedia

Bibliografische Informationen
der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISBN 3-922746-56-X

und

SecuMedia Verlags-GmbH,

Postfach 1234, 55205 Ingelheim,
Tel. 06725/93040, Fax. 06725/5994,
E-Mail info@secumedia.de

Grafik und Layout: Milman
Umschlaggestaltung: Conrad Schmitt, BSI
Herstellung: Schmidt & more Drucktechnik,
Haagweg 44, 65462 Ginsheim-Gustavsburg

Printed in Germany

Autoren

An der Erstellung dieser Studie waren beteiligt:

IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH

- Britta Oertel
- Michaela Wölk

Unter Mitarbeit von:
Barbara Debus
Volker Handke
Mandy Scheermesser

Empa – Eidgenössische Materialprüfungs- und Forschungsanstalt

- Prof. Dr. Lorenz Hilty
- Andreas Köhler

Unter Mitarbeit von:
Claudia Som
Thomas Ruddy

BSI – Bundesamt für Sicherheit in der Informationstechnik

- Harald Kelter
- Markus Ullmann
- Stefan Wittmann

Experten

- Klaus Finkenzeller
  Fa. Giesecke & Devrient
  Forschung & Entwicklung Chipkarten
  Abteilung Neue Technologien
- Christian Flörkemeier
  Institut für Pervasive Computing, ETH Zürich
- Dirk Henrici
  Fachbereich Informatik,
  Universität Kaiserslautern
- Peter Jacob
  Eidgenössische Materialprüfungs- und Forschungsanstalt, Dübendorf
- Marc Langheinrich
  Institut für Pervasive Computing,
  ETH Zürich
- Gregor Ponert
  Leiter der Abteilung Research & Development, Skidata AG
- Thomas Schoch
  Intellion AG, St.Gallen
- Moritz Strasser
  Institut für Informatik und Gesellschaft,
  Universität Freiburg
- Jens Strücken
  Institut für Informatik und Gesellschaft,
  Universität Freiburg
- Dr. Frédéric Thiesse
  Institut für Technologiemanagement,
  Universität St. Gallen
- Dr. Martin Wölker
  COGNID Consulting GmbH

Unser Dank gilt neben den vorangestellten Experten auch denjenigen Expertinnen und Experten, die an der empirischen Online-Erhebung teilgenommen haben.

Ein besonderer Dank gilt Herrn Klaus Finkenzeller, der die Mehrzahl der Abbildungen zur RFID-Technologie für die vorliegende Studie bereitgestellt hat.

Wir weisen an dieser Stelle gern auf das von ihm verfasste RFID-Handbuch (http://www.rfid-handbook.de) hin, das für alle Interessierten umfassendes technisches Detailwissen aufbereitet.

Abbildungs– und Tabellenverzeichnis

Bei Betrachtung der technischen Möglichkeiten moderner RFID-Technologie sowie der damit einhergehenden Gefährdungen wird klar, dass Auswirkungen des Einsatzes dieser Technologie auf den verschiedensten Ebenen der IT-Sicherheit und der Gesellschaft nicht ausbleiben können.

Bereits heute sind RFID-Tags bei Zutrittskontrollanlagen kombiniert mit einem Firmenausweis im Einsatz, die Europäische Zentralbank plant die Verwendung von kleinsten RFID-Tags für Banknoten zur Erhöhung der Fälschungssicherheit und Verkehrsgesellschaften möchten die Fahrausweise ihrer Kunden mit Transponder versehen, die einem zentralen Abrechnungssystem mitteilen, wann wer welche Verkehrsverbindung genutzt hat.

Das Verhindern von Geldfälschung oder eine bequeme Abrechnung der ÖPNV-Nutzung sind sinnvolle Anwendungsgebiete von RFID-Chips. Im Interesse des Bürgers steigt hier durch die RFID-Technik die Sicherheit und die Kundenfreundlichkeit. Bedenken gegen die unscheinbaren Sender bestehen trotz oder gerade wegen ihrer Unsichtbarkeit: Die aktuelle Diskussion um den Metro Future Store, in dessen Umfeld RFID-Tags eingesetzt werden, zeigt, dass ein Unternehmen, das seine Kunden über den RFID-Einsatz nicht rechtzeitig aufklärt, schnell in den Fokus von Datenschutz- und Bürgerrechtsorganisationen geraten kann.

Der Grund für das Unbehagen liegt in der Möglichkeit des unberechtigten und vor allem unbemerkten Auslesens der Chips: Der Inhalt der Einkaufstüte könnte plötzlich genauso transparent werden wie die persönliche Geldbörse.

Welche Schlussfolgerungen lassen sich aus diesen Tatsachen ableiten?

Die neue Technologie bietet enorme Chancen, da RFID-Systeme in vielen Bereichen, darunter dem gesamten Logistikbereich und der Lagerbewirtschaftung, bereits heute nutzbringend eingesetzt werden. Was noch getan werden muss ist, den Technikeinsatz hinsichtlich seiner Auswirkungen in unterschiedlichsten Anwendungsfeldern zu untersuchen, die Auswirkungen des Technikeinsatzes zu beschreiben und zu bewerten sowie die sich ergebenden Chancen und Risiken zu benennen, um zu Handlungsempfehlungen für Politik, Industrie und Wissenschaft zu gelangen.

Die in der vorliegenden Studie gefundenen Antworten sollen dabei einen Beitrag zur Versachlichung der Diskussion über den Einsatz der RFID-Technologie leisten und helfen, zu einem nutzbringenden und datenschutzkonformen Technikeinsatz zu gelangen.

Bonn, im Oktober 2004

Dr. Udo Helmbrecht
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

2. Geleitwort

Mit dem Begriff “Revolution“ sollte man vorsichtig und sparsam umgehen. Bei der Entwicklung des Technik-Zukunftsbildes „Pervasive Computing“ bzw. „Ubiquitous Computing“ halten wir es allerdings für angebracht, von einer revolutionären Technik-Perspektive zu sprechen. Diese Annahme bezieht sich vor allem auf zwei Gründe: Die Technik-Entfaltung des Pervasive Computing (alles durchdringendes Computing) oder Ubiquitous Computing (allgegenwärtiges Computing) vereinigt ganz grundlegende Techniken wie den Einsatz von Mikroprozessoren, drahtlose Funktechniken und die Datenübertragung durch universale Netze wie das Internet. Schon heute zeichnen sich solche Entwicklungen vor allem in den Bereichen „Produktion und Warendistribution“, „Produktauthentifizierung“ und „Tieridentifikation“ ab. Aber auch in den Bereichen „Echtheitsprüfung von Dokumenten“, „Instandhaltung und Reparatur“, „Zutritts- und Routenkontrolle“, „Diebstahlsicherung“ sowie „Umweltmonitoring“ sind neue Einsatzpotenziale deutlich erkennbar.

Die Plausibilität des Eindringens in alle Lebensbereiche ergibt sich vor allem aus der wichtigsten Eigenschaft der zugrunde liegenden Technologien, einer Steigerung der Effizienz hinsichtlich Arbeitseinsatz, Zeit und Raum sowie einer schnelleren Reaktionsfähigkeit auf Veränderungen von Objektparametern. Die damit verbundenen Innovations- und Automatisierungspotenziale sind in in einer zunehmend internationalisierten Wettbewerbswirtschaft starke Anreize für eine zügige Umsetzung.

Vor diesem Hintergrund kann es kaum einen Zweifel geben, dass insbesondere die heute schon fortgeschrittenen automatischen Identifikationssysteme (Auto-ID-Systeme) vor allem in denjenigen Branchen verstärkt eingesetzt werden, in denen Produktivitätsfortschritte durch eine verstärkte Automatisierung erzielt werden können. Dies gilt in besonderem Maße für RFID-Systeme (Radio-Frequency-Identification), die die Funktionen und Einsatzmöglichkeiten von bisherigen Lösungen zur Autoidentifikation wie Barcode oder Optical Character Recognition (OCR) erweitern und als zentraler Schritt zur weiteren integrierenden Technikentwicklung in Richtung „Pervasive Computing“ bzw. „Ubiquitous Computing“ verstanden werden können.

Wie immer bei revolutionären Technikschüben liegen die Chancen und Risiken eng beieinander. In sozialer Hinsicht zählen zu den Risiken vor allem die Folgen der zu erwartenden Rationalisierungseffekte und neuer Modelle der Arbeitsorganisation bei ohnehin bereits hochmobilen und flüchtigen Lebens- und Arbeitswelten. In ökologischer Hinsicht ist es die allgegenwärtige Nutzung technischer Mikrosysteme, die enorme Reboundeffekte und eine zunehmende Feinverteilung wertvoller Materialien und ökologisch bedenklicher Inhaltsstoffe von Elektronikprodukten erwarten lässt. Vor diesem Hintergrund ist es somit eine der wichtigsten Aufgaben von Wissenschaft, die Chancen, aber eben auch die Probleme und Risiken frühzeitig und möglichst umfassend aufzuzeigen. Die sozialverträgliche Gestaltung von Technik beinhaltet den Ausgleich und zuvor die Auseinandersetzung zwischen unterschiedlichen gesellschaftlichen Interessensgruppen sowie wirtschaftlichen und politischen Akteuren.

Wenn die Bewegung und Benutzung von Alltagsgegenständen Datenspuren hinterlässt, die sich zunehmend der Kontrolle des Benutzers entziehen, so kann dies tiefgreifende Auswirkungen für unser Verständnis von Sicherheit und Privatsphäre haben. Aufbauend auf einer Abschätzung der Technikfolgen und in permanenter Rückkopplung von Wissenschaft und Gesellschaft muss ein öffentlicher Dialog mit der Politik, der Wirtschaft, den zivilgesellschaftlichen Gruppen und Organisationen sowie den Bürgern über diese Probleme geführt werden. Nur in einem solchen fachlich-wissenschaftlich gestützten öffentlichen Diskussionsprozess lässt sich herausfinden, welche wünschbaren Ziele angesteuert werden sollten und welche

Technikentwicklungen dafür geeignet sind, um die Chancen zu maximieren und die Risiken zu vermeiden oder zumindest zu minimieren.

In diesem Sinne bietet die vorliegende Studie einen Überblick über die zentralen technologischen Entwicklungen und ökonomischen Anwendungsgebiete von RFID-Systemen. Zudem werden die grundsätzlich möglichen Bedrohungslagen analysiert sowie gängige Sicherheitsmaßnahmen aufgezeigt.

Wir danken allen Autoren und Experten, die an dieser Stelle mitgewirkt haben für die gewissenhafte und zukunftsweisende Arbeit und ihre wichtigen Ergebnisse. Wir sind zuversichtlich, dass der erforderliche gesellschaftliche Dialog über diese wichtigen Zukunftsfragen durch diese Studie wesentliche Impulse erhält.

Berlin und St. Gallen, im Oktober 2004

Prof. Dr. Rolf Kreibich

Dr. Xaver Edelmann

3. Zusammenfassung

Ausgangssituation

Das Technikleitbild „Pervasive Computing“ bzw. „Ubiquitous Computing“ bezeichnet eine neue Entwicklung in der Informations- und Kommunikationstechnologie. „Pervasive“ steht für „(alles) durchdringend“, „ubiquitous“ für „allgegenwärtig“. Im Zuge dieser Entwicklung werden zukünftig immer mehr Alltagsgegenstände mit Mikroelektronik ausgestattet sein. Die so entstehenden „intelligenten“ Objekte, auch „Smart Objects“ genannt, werden nahezu alle Bereiche des täglichen Lebens beeinflussen. Computer werden ihren Dienst zunehmend unsichtbar im Hintergrund ausführen.

Einen wesentlichen Entwicklungsstrang im Rahmen des Pervasive Computing bilden digitale automatische Identifikationssysteme (Auto-ID-Systeme), die traditionelle Lösungen wie Barcode oder Optical Character Recognition (OCR) zukünftig ersetzen sollen. Aufgabe und Ziel der Auto-ID-Technologie ist grundsätzlich die Bereitstellung von Informationen zu Objekten (Personen, Tieren, Gütern oder Waren). RFID-Systeme (Radio-Frequency-Identification) erweitern die Funktionalitäten und Einsatzmöglichkeiten traditioneller Auto-ID-Systeme und bieten hohe Effizienzsteigerungspotenziale beispielsweise in der Produktion und Warendistribution sowie im Bereich der Produktauthentifizierung oder des Customer Relationship Managements.

Die Vision der „totalen Vernetzung“ des Alltags bietet nicht nur neue Möglichkeiten und Chancen, sondern birgt auch Risiken. Dabei entwickelt sich die Frage nach der Sicherheit von RFID-Systemen immer mehr zu einer Schlüsselfrage für die Entwicklung und Gestaltung des gesellschaftlichen Daten-, Informations- und Wissensaustauschs. Vor allem der wirtschaftliche Erfolg von Unternehmen hängt davon ab, inwieweit es gelingt, die internen Datenbestände und die externe Kommunikation gegen Datenverlust und Datenmissbrauch erfolgreich zu schützen. Aber auch die Frage, ob und in welcher Form zusätzliche verbraucher- bzw. datenschutzrechtliche Regelungen durch den breiteren Einsatz von RFID-Systemen erforderlich sind, rückt zunehmend in den Mittelpunkt der gesellschaftlichen Debatte (Stichwort „gläserner Kunde“ bzw. „gläserner Bürger“).

In den vergangenen Jahren ist die Erkenntnis gewachsen, dass die Bewertung technischer Entwicklungen vorausschauend und problemorientiert erfolgen sollte, um Hinweise für eine zukunftsfähige Technikgestaltung zu gewinnen. Hierzu zählt auch die interdisziplinäre Abschätzung der Chancen und Risiken des Einsatzes von RFID mit fokussiertem Blick auf die Bereiche IT-Sicherheit und Datenschutz. Nur so können echte oder vermeintliche Sicherheitsprobleme als zentrale Barriere der wirtschaftlichen Nutzung der RFID-Technologie frühzeitig erkannt und so weit als möglich auch vemieden werden.

Ziele der Studie

Ziel der vorliegenden Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ ist es, der interessierten (Fach-)Öffentlichkeit einen Überblick über die technischen Grundlagen, Anwendungspotenziale und Risiken von RFID-Systemen zu geben. Der Schwerpunkt der Arbeit liegt in der prospektiven Analyse möglicher Bedrohungslagen, die aus der Anwendung von RFID-Systemen hervorgehen, einschließlich der Einschätzung der Wirksamkeit von bestehenden Sicherheitsmaßnahmen. Darüber hinaus wird anschaulich und mit praktischen Beispielen erläutert, welche RFID-Systeme bereits heute angewendet werden und welche sich in der Erprobungsphase befinden.

Um die Chancen und Risiken von RFID-Systemen zu bewerten, wird eine Einschätzung der wesentlichen technologischen, ökonomischen, rechtlichen und gesellschaftlichen Entwicklungen im Kontext von RFID-Systemen vorgenommen, die einen Zeithorizont bis 2010 aufspannen. Fiktive Fallbeispiele dienen der Veranschaulichung von grundsätzlich möglichen Risiken, sind aber

explizit nicht als prognostische Abschätzung zu verstehen.
Die vorgeschlagene Untersuchung will dazu beitragen, für das Thema der IT-Sicherheit in dem Innovationsfeld RFID zu sensibilisieren, anhand konkreter Potenziale und Gefährdungen bei den Entscheidungsträgern Bewusstsein zu wecken und zu motivieren, die informationstechnischen Systeme in den Unternehmen und Organisationen angemessen zu analysieren und nachhaltig zu schützen.

Definition RFID-Systeme
RFID bezeichnet Verfahren zur automatischen Identifizierung von Objekten über Funk. Der Einsatz von RFID-Systemen eignet sich grundsätzlich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss. RFID-Systeme werden in vielfältigen Varianten angeboten. Trotz der großen Bandbreite der RFID-Lösungen ist jedes RFID-System durch die folgenden drei Eigenschaften definiert:

1. **Elektronische Identifikation:**
   Das System ermöglicht eine eindeutige Kennzeichnung von Objekten durch elektronisch gespeicherte Daten.
2. **Kontaktlose Datenübertragung:**
   Die Daten können zur Identifikation des Objekts drahtlos über einen Funkfrequenzkanal ausgelesen werden.
3. **Senden auf Abruf (on call):**
   Ein gekennzeichnetes Objekt sendet seine Daten nur dann, wenn ein dafür vorgesehenes Lesegerät diesen Vorgang abruft.

Ein RFID-System besteht technologisch betrachtet aus zwei Komponenten, einem Transponder und einem Lesegerät:

- Der Transponder – auch als „Tag“ bezeichnet – fungiert als eigentlicher Datenträger. Er wird an einem Objekt angebracht (beispielsweise an einer Ware oder einer Verpackung) bzw. in ein Objekt integriert (z. B. in eine Chipkarte) und kann kontaktlos über Funktechnologie ausgelesen und je nach Technologie auch wieder beschrieben werden. Grundsätzlich setzt sich der Transponder aus einer integrierten Schaltung und einem Radiofrequenzmodul zusammen. Auf dem Transponder sind eine Identifikationsnummer und weitere Daten über den Transponder selbst bzw. das Objekt, mit dem dieser verbunden ist, gespeichert.
- Das Erfassungsgerät – typischerweise und auch im Folgenden kurz nur als Lesegerät bezeichnet – besteht je nach eingesetzter Technologie aus einer Lese- bzw. einer Schreib-/Leseeinheit sowie aus einer Antenne. Das Lesegerät liest Daten vom Transponder und weist ggf. den Transponder an, weitere Daten zu speichern. Weiterhin kontrolliert das Lesegerät die Qualität der Datenübermittlung. Die Lesegeräte sind typischerweise mit einer zusätzlichen Schnittstelle ausgestattet, um die empfangenen Daten an ein anderes System (PC, Automatensteuerung, ...) weiterzuleiten und dort weiter zu verarbeiten.

RFID-Systeme nutzen unterschiedliche Frequenzbereiche vom Langwellen- bis zum Mikrowellenbereich. Ein weiteres Unterscheidungsmerkmal von RFID-Systemen besteht in der jeweils zum Einsatz kommenden Speichertechnologie. Hierbei wird grundsätzlich zwischen Read-only- und Read-write-Systemen unterschieden. Auch die Art der Energieversorgung des Transponders und die daraus resultierende Unterscheidung in aktive Transponder mit eigener Energiequelle bzw. passive Transponder, die durch das Lesegerät mit Energie versorgt werden, ist von grundlegender Bedeutung.

Aufgrund dieser Merkmale können Gruppen von RFID-Systemen gebildet und bezüglich der Leistungsfähigkeit ihrer jeweiligen Komponenten in Low-End-Systeme, Systeme mittlerer Leistungsfähigkeit und High-End-Systeme unterschieden werden. Eine weitere Gruppierung von RFID-Systemen kann entsprechend ihrer jeweiligen Reichweite – also des maximal möglichen Abstandes zwischen

Transponder und Lesegerät – erfolgen. Hier werden in der Regel Close-Coupling-, Remote-Coupling- sowie Long-Range-Systeme unterschieden.

Die Bauformen von Transpondern reichen vom Glas-Injektat über die elektrische Ohrenmarke bis hin zu Scheckkartenformaten, verschiedenen Scheibenbauformen sowie schlagfesten und bis zu 200°Celsius hitzebeständigen Datenträgern für die Lackierstraßen der Automobilindustrie. Die flexible Auslegbarkeit der Identifikationspunkte, Baugröße, Form und Feldcharakteristik der Antenne machen RFID-Systeme insgesamt zu einer sehr vielseitigen automatischen Identifikationstechnologie.

Diese Gruppierungen ermöglichen sowohl eine Einordnung von RFID-Systemen hinsichtlich der auf ihnen basierenden möglichen Anwendungen sowie eine Einschätzung der damit verbundenen Fragen zur Informationssicherheit und zum Datenschutz.

Bedrohungslage und Bestandsaufnahme gängiger Sicherheitsmaßnahmen
Die Integrität von RFID-Systemen beruht entscheidend darauf, dass die folgenden drei Beziehungen gesichert sind:

1. Die Beziehung zwischen den auf einem Transponder (RFID-Tag) gespeicherten Daten und dem Transponder selbst.

   Hierbei muss es sich um eine eindeutige Beziehung handeln, weil der Transponder ausschließlich durch die Daten identifiziert wird. Wichtigster Bestandteil der Daten ist eine eindeutige ID-Nummer (Seriennummer). In jedem Fall muss ausgeschlossen werden, dass zwei Tags mit gleicher Identität existieren.

2. Die Beziehung zwischen dem Transponder und dem Trägerobjekt, zu dessen Identifikation er dient (mechanische Verbindung).

   Diese Beziehung muss ebenfalls eindeutig sein, das heißt, es darf nicht vorkommen, dass ein Transponder während seiner Nutzungsphase wechselnden Objekten zugeordnet wird.

3. Die Beziehung zwischen Transponder und Lesegerät (Luftschnittstelle).

   Sie muss so realisiert sein, dass autorisierte Lesegeräte auf die Daten korrekt zugreifen können, nicht autorisierte Lesegeräte dagegen vom Zugriff ausgeschlossen bleiben.

Aus diesen Voraussetzungen ergeben sich unter anderem die folgenden grundlegenden Angriffsarten auf RFID-Systeme, die sich jeweils gegen eine oder mehrere der Voraussetzungen richten:

- **Abhören der Kommunikation zwischen RFID-Tag und Erfassungsgerät:**
  Das Abhören der Luftschnittstelle ist prinzipiell möglich. Das Risiko wächst mit der maximalen Lesedistanz des regulären Lesevorgangs. Bei Transpondern mit sehr kurzer Reichweite ist das Risiko eher gering.

- **Unautorisiertes Auslesen der Daten:**
  Für die übliche Lesedistanz ist dies ohne allzu hohe Kosten für den Angreifer möglich. Dieser muss das Lesegerät erwerben und eventuell den Aufwand für einen unauffälligen Einbau treiben. Es werden bereits Softwareprodukte angeboten, die auf mobilen Lesegeräten zum Einsatz kommen und z. B. in Supermärkten einfache Tags sowohl auslesen als auch beschreiben können. Die Möglichkeiten solcher Angriffe sind aufgrund der kurzen Reichweite eng begrenzt; in einem kontrollierten Umfeld können sie deshalb unterbunden werden.

- **Unautorisiertes Verändern der Daten:**
  Bei wieder beschreibbaren Tags sind die Möglichkeiten zum unautorisierten Verändern der Daten die gleichen wie im Fall des unautorisierten Auslesens.

Werden Read-only-Tags verwendet, ist das unautorisierte Verändern der Daten intrinsisch ausgeschlossen. Diesem Vorteil der Read-only-Tags steht der Nachteil gegenüber, dass Verschlüsselung und sichere Authentifizierung mit ihnen nicht realisierbar sind.

- **Cloning und Emulation:**
  Beim Cloning wird der Dateninhalt eines Tags ausgelesen oder auf andere Weise in Erfahrung gebracht, um damit ein neues Tag zu beschreiben. Dieses wird dann benutzt, um die Identität des Original-Tags vorzutäuschen. Daneben ist der Einsatz von Geräten mit hoher Funktionalität denkbar, die benutzt werden, um bei gegebenem Dateninhalt beliebige Tags zu emulieren.

- **Ablösen des Tags vom Trägerobjekt:**
  Dieser Angriff erscheint trivial, ist aber gerade deshalb mit zu berücksichtigen. Jedes RFID-System ist davon abhängig, dass die Tags sich auf den dafür vorgesehenen Objekten befinden. Das „Umkleben“ von Tags (wie heute auch von Preisschildern) in Betrugsabsicht oder einfach nur in der Absicht, Verwirrung zu stiften, ist eine nahe liegende Manipulation.

- **Mechanische oder chemische Zerstörung:**
  RFID-Tags können mechanisch oder chemisch beschädigt werden. Insbesondere die Antennen sind angreifbar.

- **Zerstörung durch Feldeinwirkung:**
  Die Zerstörung durch Feldeinwirkung ist bei den herkömmlichen Tags zur Elektronischen Artikelsicherung (EAS, 1-Bit-Transponder) standardmäßig vorgesehen (Deaktivierung an der Kasse). Alle Transponder können durch ein ausreichend starkes elektromagnetisches Feld zerstört werden. Generell ist dies wegen der hohen erforderlichen Feldstärke nur aus unmittelbarer Nähe möglich. Es gibt Hinweise darauf, dass Funkeninduktoren oder in unmittelbarer Nähe stattfindende Hochspannungs-Schaltvorgänge ausreichende Spannungsspitzen in Transpondern induzieren, um die Chips zu beschädigen.

- **Zerstörung durch Missbrauch eines Kill-Kommandos:**
  Wenn Tags aus Gründen des Datenschutzes mit einer Kill-Funktion ausgestattet werden, die den Dateninhalt teilweise oder vollständig löscht, so besteht grundsätzlich die Möglichkeit, dass ein Angreifer diese missbraucht.

- **Entladen der Batterie (nur bei aktiven Tags):**
  Bei aktiven Tags, die über eine Stützbatterie verfügen, kann diese entladen werden, indem das Tag durch eine rasche Abfolge von Anfragen zum häufigen Senden angeregt wird.

- **Blocken:**
  Die Benutzung von Blocker-Tags ist im Gegensatz zu Störsendern nicht gesetzlich verboten, weil es sich aufgrund der passiven Ausführung nicht um Sendeanlagen handelt. Grundsätzlich gibt es innerhalb eines gegebenen Protokolls keinen absoluten Schutz gegen das Blocken. Da verschiedene Protokolle im Einsatz sind, muss der Benutzer des Blocker-Tags entweder mehrere solche mit sich führen, um alle in Frage kommenden Protokolle abzudecken, oder ein einziges Blocker-Gerät, das alle verwendeten Protokolle beherrscht.

- **Störsender:**
  Eine wirkungsvolle Störung des Betriebs auf Entfernung erfordert starke Sender. Der Betrieb solcher Störsender ist illegal, und sie sind für technisch nicht versierte Personen schwer zu beschaffen; Amateurfunker haben jedoch Zugang zu dieser Technologie.

- **Frequenzverstimmung:**
  Dieser Angriff beruht darauf, relevante Mengen von z. B. Wasser, Metall oder Ferrit in die Nähe der Tag-Antenne zu

bringen. Frequenzverstimmung ist aus Sicht eines Angreifers aber weniger zuverlässig in der Wirkung als die Abschirmung.

- **Abschirmung:**
  Tags werden elektromagnetisch abgeschirmt, indem man sie in metallische Folie einwickelt (z. B. Alufolie), oder sie in alubeschichtete Gefrierbeutel oder mit Metallstreifen ausgestattete Handtaschen legt.

Gegen die meisten dieser Bedrohungen gibt es Gegenmaßnahmen, die zum Teil mit höherem, zum Teil mit niedrigerem Aufwand verbunden sind als der jeweilige Angriff.

Diese Bedrohungen sind zunächst für die aktive Partei relevant, also für den Betreiber des RFID-Systems, der die Tags und die mit ihnen assoziierten Daten verwaltet. Für die passive Partei, die die Tags zwar verwenden will oder muss, aber keine Kontrolle über die Daten hat, ist die Bedrohungslage nicht identisch. Hier steht eine mögliche Verletzung der Privatsphäre im Vordergrund, insbesondere wenn durch RFID-Anwendungen Datenspuren von Objektbewegungen in zentralen Datenbanken abgelegt werden. Der Zugriff auf die Datenbanken im Backend des RFID-Systems stellt für die passive Partei möglicherweise ein größeres Risiko dar, als der Angriff auf das Frontend (z. B. das Abhören der Luftschnittstelle). Spezifisch für RFID-Systeme ist die hohe räumliche und zeitliche Dichte der Datenspuren, die häufig die nachträgliche Erstellung von personalisierten Bewegungs- und Kontaktprofilen erlaubt, selbst wenn die Daten ursprünglich in einer pseudonymisierten oder anonymisierten Form vorliegen. Entsprechende Verletzungen der Data Privacy oder der Location Privacy können insbesondere dann eintreten, wenn die aktive Partei selbst gegen das Datenschutzrecht oder faire Informationspraktiken verstößt oder wenn sie von einem Dritten gezwungen wird, ihre Datenbestände offen zu legen. Inwieweit RFID-Anwendungen hier den bereits durch andere Systeme (wie Kreditkarten, Kundenkarten, Mobiltelefonie) erzeugten Datenspuren ein relevantes Bedrohungspotenzial hinzufügen, ist unter Fachleuten umstritten. Neben der Verletzung der Privatsphäre ist die Abwälzung der technisch bedingten Risken von der aktiven auf die passive Partei als mögliche Bedrohung zu betrachten.

Anwendungen

In ausgewählten Marktsegmenten zeigen RFID-Systeme bereits seit Jahrzehnten eine kontinuierliche Marktentwicklung (z. B. im Bereich der Tieridentifikation oder in Form der Kfz-Wegfahrsperre). In Abhängigkeit von unterschiedlichen, zum Teil branchenspezifischen Einsatzbedingungen werden RFID-Systeme in der ganzen Bandbreite möglicher technologischer Komplexität eingesetzt. In anderen Segmenten befindet sich die automatische und berührungslose Identifikation in zahlreichen Pilotvorhaben in der Erprobung.

Die RFID-Technologie ist eine typische Querschnittstechnologie, deren Anwendungspotenziale in nahezu allen Lebens- und Wirtschaftsbereichen liegen. Theoretisch sind die Einsatzgebiete von RFID-Systemen unbegrenzt. Grundsätzlich geht es bei ihrem Einsatz funktional immer um die Identifikation von Objekten. Branchen übergreifend können die folgenden Anwendungsgebiete unterschieden werden:

- Kennzeichnung von Objekten
- Echtheitsprüfung von Dokumenten
- Instandhaltung und Reparatur, Rückrufaktionen
- Diebstahlsicherung und Reduktion von Verlustmengen
- Zutritts- und Routenkontrollen
- Umweltmonitoring und Sensorik
- Supply-Chain-Management: Automatisierung, Steuerung und Prozessoptimierung

Die vorliegenden Marktdaten zum Einsatz von RFID-Systemen sind in der Regel punktuell, beziehen sich auf einzelne volkswirt-

schaftliche Sektoren und geben keinen umfassenden Marktüberblick. Die von den verschiedenen Beratungsunternehmen verwendeten Datengrundlagen, Erhebungsmethoden und Marktabgrenzungen sind sehr unterschiedlich, nicht immer transparent und können nicht miteinander verglichen werden. In der Folge bleiben der Stand der Diffusion, Umsätze und Marktanteile von RFID-Systemen national wie international unscharf. Ob RFID-Systeme zukünftig auch als Massentechnologie eingesetzt werden, hängt nicht zuletzt von den Erfolgen der laufenden Pilotprojekte ab.

In den einzelnen Anwendungszusammenhängen kann gezeigt werden, welche Vorteile der Einsatz von RFID-Systemen beispielsweise für den Handel, das produzierende Gewerbe oder für Logistik-Dienstleister bietet. Chancen lassen sich vor allem in Anwendungsgebieten und Branchen ausmachen, in denen Produktivitätsfortschritte durch eine verstärkte Automatisierung erzielt werden sollen. Eine Studie von Booz Allen Hamilton und der Universität St. Gallen in der Logistik- und Automobilbranche zeigt allerdings, dass für viele Unternehmen Investitionen in RFID immer noch riskant sind und ein positiver Return on Investment heute hauptsächlich für Nischenanwendungen existiert. Vor diesem Hintergrund ist es nicht verwunderlich, dass in der Praxis noch unternehmensinterne Einzellösungen von RFID-Systemen überwiegen. Das Potenzial von RFID-Systemen besteht jedoch insbesondere im unternehmensübergreifenden Einsatz, beispielsweise bei der Warenrückverfolgung über die gesamte Wertschöpfungskette hinweg.

Transponder ermöglichen mittlerweile neben der reinen Identifikation von Objekten auch die Steuerung von Waren und Gütern in komplexen Systemen. Hierin begründet sich auch der zunehmende Einsatz von Transpondern in der Logistik. Für eine effiziente Steuerung der Logistikprozesse werden immer mehr Daten benötigt, die entlang der kompletten Supply-Chain automatisch erfasst und verarbeitet werden müssen. In diesem Anwendungssegment eröffnet die RFID-Technologie umfassende Lösungspotenziale. Aber auch im Bereich des Umweltmonitoring können RFID-Systeme zukünftig mit hochgradig miniaturisierten Sensoren dazu beitragen, die vielfältigen Phänomene der natürlichen Umwelt in bislang nicht möglicher Genauigkeit zu beobachten und Umweltbelastungen zu überwachen.

Zu den Hauptwachstumsfaktoren für die weitere Verbreitung von RFID-Systemen zählen sinkende Preise und zunehmende gesetzliche Vorgaben. So rücken RFID-Lösungen im Zuge von Vorschriften der Europäischen Union immer stärker in den Blickpunkt der ökonomischen Akteure aus Logistik und Landwirtschaft einschließlich aller vor- und nachgelagerten Stufen der Wertschöpfung (z. B. Rückverfolgbarkeit von Lebensmitteln, Seuchenschutz). Aber auch die Kompatibilität und Interoperabilität sowie die Durchsetzung von einheitlichen Standards sind wesentliche Elemente, die die zukünftigen Entwicklungsmöglichkeiten von RFID-Systemen maßgeblich beeinflussen. Positive Impulse gehen zudem von der zunehmenden Bekanntheit der RFID-Lösungen und vom Angebot kundenorientierter Lösungen aus.

Erwartete Entwicklungen und Herausforderungen

Die Entwicklungsperspektiven der RFID-Technologie werden nicht allein von den technischen Möglichkeiten geprägt. Neben Technologie und Standardisierung sind auch die Markt- und Preisentwicklung, die Anforderungen an die Informationssicherheit und den Datenschutz sowie der gesellschaftliche Diskurs im Kontext von RFID zu berücksichtigen.

Für die kommenden zehn Jahre ist mit einer weiteren exponentiellen Steigerung der Leistungsentwicklung der Informations- und Kommunikationstechnologie zu rechnen. Neben der Verbesserung des Preis-Leistungsverhältnisses werden sich die eingesetzten technologischen Komponenten weiterhin

drastisch verkleinern. Wenngleich die Verkleinerung der Transponderantennen an physikalisch bedingte Grenzen stößt, könnten andere Möglichkeiten wie das Einweben der Antennen in Textilien dazu beitragen, dass RFID-Tags praktisch unsichtbar werden. Die Miniaturisierung der Mikrochips wird voraussichtlich noch etwa zehn Jahre ohne Technologiebruch voranschreiten. Sie ist eine wesentliche Triebkraft für die Realisierung der Vision des „Pervasive Computing".

Nach Einschätzung von Expertinnen und Experten aus Unternehmen und Forschungseinrichtungen, die im RFID-Sektor tätig sind, werden technische Probleme, die derzeit noch die Verbreitung von RFID-Systemen hemmen, bis zum Jahr 2007 bzw. bis zum Jahr 2010 weitgehend überwunden sein. Hierzu zählen beispielsweise Probleme bei der Pulk-Erfassung und in der Erkennung auf unterschiedlichen Frequenzbändern. Die Überwindung der Inkompatibilitäten zwischen den RFID-Lösungen der einzelnen Hersteller wird zunächst nicht erwartet. Die Untersuchungsergebnisse verweisen für die kommenden Jahre bis 2010 auf eine insgesamt positive oder stabile Marktentwicklung von RFID-Systemen in Deutschland. Auch werden insgesamt fallende Preise erwartet. Die Einschätzungen, in welchen Anwendungsgebieten sich RFID-Systeme weiter durchsetzen werden, sind durchaus heterogen. Langfristig wird vor allem in den Anwendungsgebieten „Überwachung von Zutritt, Räumen und Routen", „Supply Chain: Automatisierung, Steuerung und Prozessoptimierung", „Kennzeichnung von Waren, Objekten, Tieren oder Personen", „Verleih- und Mehrwegsysteme, Entsorgung und Recycling" sowie „Instandhaltung und Reparatur, Rückrufaktionen" eine positive Marktentwicklung von RFID-Systemen erwartet.

Eine stark informatisierte Alltags- und Berufswelt mit Gegenständen, die Teilaspekte ihrer Umgebung erfassen und miteinander kommunizieren, hat neben den ökonomischen Potenzialen auch grundsätzliche Auswirkungen auf die Informationssicherheit und die Privatsphäre (Datenschutz). Auf der Grundlage von RFID-Systemen können Daten sehr viel leichter als bisher gesammelt werden. Im Zuge der weiteren Verbreitung der RFID-Technologie stellt sich die Frage, wer darüber bestimmen kann oder darf, ob und mit welchen Informationen elektronisch aufgewertete Dinge verknüpft werden. Schließlich ist auch zu berücksichtigen, dass in einer wesentlich stärker informatisierten Welt das korrekte Funktionieren der informationstechnischen Infrastruktur überlebenswichtig für die Gesellschaft oder Einzelne werden kann. Gerade wegen der zunehmenden Allgegenwart und Unauffälligkeit informationstechnischer Systeme ist zu befürchten, dass bestehende rechtliche Regelungen immer weniger durchsetzbar sind. Es gilt, der zunehmenden Undurchschaubarkeit der technischen Systeme entgegen zu wirken und durch die Sicherstellung von hoher Transparenz das Vertrauen der Nutzerinnen und Nutzer in die RFID-Technologie zu sichern.

Um die Chancen von RFID zu nutzen und gleichzeitig die Bedrohung für die Persönlichkeitssphäre so gering wie möglich zu halten, müssen die Grundsätze eines zeitgemäßen Datenschutzrechts in RFID-Systemen bereits frühzeitig im Design-Prozess und in der Markteinführung umgesetzt werden. Hierzu zählen vor allem der Grundsatz der Datensparsamkeit und die schnellstmögliche Anonymisierung oder Pseudonymisierung personenbezogener Daten. Dies gilt umso mehr, als politische und rechtliche Rahmenbedingungen im Zuge der fortschreitenden Globalisierung zunehmend schwieriger zu gestalten sind.

Die Frage, ob und wie schnell sich die gesellschaftlichen Gruppen der RFID-Technologie gegenüber öffnen werden, ist schwer zu beantworten. In der Debatte um die Möglichkeiten und Grenzen der RFID-Technologie kristallisieren sich zwei gegenüberstehende Positionen heraus: Während auf der einen Seite die Chancen in den

Vordergrund gestellt werden, die sich aus der Nutzung von RFID ergeben, werden auf der anderen Seite vor allem die Risiken, Bedrohungen und Beschränkungen thematisiert. Der Fokus der vorliegenden Studie liegt auftragsgemäß mehr auf den Risiken als auf den Chancen. Im Sinne der Vorsorge sollten Risiken möglichst frühzeitig erkannt werden, damit die Entwicklung reflektiert und in eine positive Richtung gelenkt werden kann.

Da in einer modernen, differenziert strukturierten Gesellschaft eine Vielzahl von Interessengruppen existiert, ist es für die weitere Entwicklung wichtig, diesen Meinungspluralismus auch im Umfeld von RFID in einem angemessenen Verhältnis widerzuspiegeln. Es gilt, in den einzelnen Akteursgruppen mehr Transparenz in der Diskussion um RFID herzustellen. Sie ist ein zentraler Schritt zur Versachlichung der Diskussion und für die gesellschaftliche Meinungsbildung.

4. Einführung

4.1. RFID als Schlüsseltechnologie des Pervasive Computing

Vielfältige Faktoren bestimmen seit Jahren die Entwicklung informationstechnischer Systeme: Hierzu zählen die fortschreitende Miniaturisierung der Komponenten, die steigende Leistungsfähigkeit von Prozessoren, die Verfügbarkeit von Speicherkapazität auch auf kleinstem Raum, höhere Kommunikationsbandbreiten im Telekommunikationsbereich sowie Fortschritte in den Materialwissenschaften. Der schnelle Austausch digital gespeicherter Informationen in großen Netzwerken über eine steigende Anzahl von Akteuren und Übertragungswegen gilt als zentrales Merkmal von Informations- und Wissensgesellschaften. Mehr und mehr wird die Mensch-Maschine-Kommunikation durch die Kommunikation und Vernetzung von Maschinen – ohne direkte Einbindung des Menschen ergänzt.

Vor diesem Hintergrund sind die Begriffe „Ubiquitäres Computing“ oder „Pervasive Computing“ verstärkt in den Mittelpunkt der öffentlichen Diskussion gerückt: Der Begriff des allgegenwärtigen „ubiquitären“ Computing beschreibt eine „unaufdringliche“ Technikvision, in der das heute vertraute Erscheinungsbild des Computers in den Hintergrund tritt und „smarte“ Objekte direkt miteinander kommunizieren.

Im Bereich der Wirtschaft wird für dieses Paradigma der Begriff „Pervasive Computing“ verwendet. Er beschreibt ebenfalls die allgegenwärtige, alles durchdringende Informationsverarbeitung und Vernetzung, rückt jedoch im Gegensatz zum ubiquitären Computing in naher Zukunft machbare Lösungen in den Mittelpunkt. [LaMa 03] Pervasive Computing wird als neue Anwendungsform von Informations- und Kommunikationstechnologien (ICT) betrachtet und ist durch folgende Merkmale gekennzeichnet:

- „Miniaturisierung: ICT-Komponenten werden kleiner und damit portabler als die heute üblichen Geräte.
- Einbettung: ICT-Komponenten werden häufiger in andere Geräte und Gegenstände des täglichen Gebrauchs eingebettet („Smart Objects“).
- Vernetzung: ICT-Komponenten sind in der Regel drahtlos miteinander vernetzt.
- Allgegenwart: ICT wird allgegenwärtig und versieht ihren Dienst immer unauffälliger oder gar unsichtbar.
- Kontextsensitivität: ICT-Komponenten können sich durch drahtlosen Datenaustausch und mittels Sensoren Informationen über ihre Umgebung beschaffen.“ [HBBB 03]

Einen wesentlichen Entwicklungsstrang im Rahmen des Ubiquitous oder Pervasive Computing bilden RFID-Systeme (RFID = Radio Frequency IDentification), die zu den automatischen Identifikationsverfahren zählen und die in den vergangenen Monaten verstärkt in den Mittelpunkt auch der öffentlichen Diskussion gerückt sind. Sinngemäß übersetzt steht RFID für „kontaktlose Identifikation“.

Aufgabe der automatischen Identifikation ist es, Informationen zu Personen, Tieren, Gütern oder Waren klar definiert und strukturiert so bereitzustellen, dass diese Daten maschinell erfasst und weiter verarbeitet werden können. Zukünftig wird RFID die heute weit verbreiteten automatischen Identifikationsverfahren wie Barcode, Optical Character Recognition (OCR) – optische Zeichenerkennung – oder kontaktbehaftete Chipkarten ersetzen oder ergänzen. RFID-Systeme können als leistungsstarke Identifikationssysteme eingesetzt werden, mit denen eine hohe Datenmenge erfasst und ggf. laufend aktualisiert werden kann. Ihr volles Leistungsspektrum entfaltet die RFID-Technologie aber erst dann, wenn sie zur Steuerung und Kontrolle von Prozessen in einer Vielzahl von Anwendungsbereichen genutzt wird. Von der Zutrittskontrolle über

das Verfolgen von Warenflüssen vom Hersteller bis zum Verbraucher – die Palette der bereits etablierten oder in Pilotvorhaben erprobten Anwendungsgebiete wächst ständig.

RFID ist keine neue Technologie. Beim US-Militär werden RFID oder deren Vorgängertechnologien bereits seit 1940 genutzt, um den Verbleib von Nachschub wie Treibstoff oder Munition zu verfolgen oder die Freund-Feind-Erkennung alliierter Flugzeuge zu ermöglichen. Seit 1977 sind RFID-Systeme für zivile Anwendungen freigegeben. Zu den ersten Anwendungen zählten Ende der 80er Jahre Transponder für die Tieridentifikation. [Krem 04]

RFID bezeichnet Verfahren, um Objekte über gewisse Entfernungen berührungslos zu identifizieren. Die überbrückbare Distanz (Reichweite) liegt dabei typischerweise im Zentimeter- oder Meterbereich.

Ein RFID-System besteht technologisch betrachtet aus zwei Komponenten, einem Transponder und einem Lesegerät:

- Der Transponder – auch als „Tag“ bezeichnet – fungiert als eigentlicher Datenträger. Er wird an einem Objekt angebracht (beispielsweise an einer Ware oder einer Verpackung) bzw. in ein Objekt integriert und kann kontaktlos über Funktechnologie ausgelesen und je nach Technologie auch wieder beschrieben werden. Grundsätzlich setzt sich der Transponder aus einer integrierten Schaltung sowie einem RF-Modul zusammen. Auf dem Transponder sind eine Identifikationsnummer und weitere Daten über den Transponder selbst bzw. das Objekt, mit dem dieser verbunden ist, gespeichert.
- Das Erfassungsgerät – typischerweise und auch im Folgenden kurz nur als Lesegerät bezeichnet – besteht je nach eingesetzter Technologie aus einer Lese- bzw. einer Schreib-/Leseeinheit sowie aus einer Antenne. Das Lesegerät liest Daten vom Transponder und weist ggf. den Transponder an, weitere Daten zu speichern. Weiterhin kontrolliert das Lesegerät die Qualität der Datenüber-

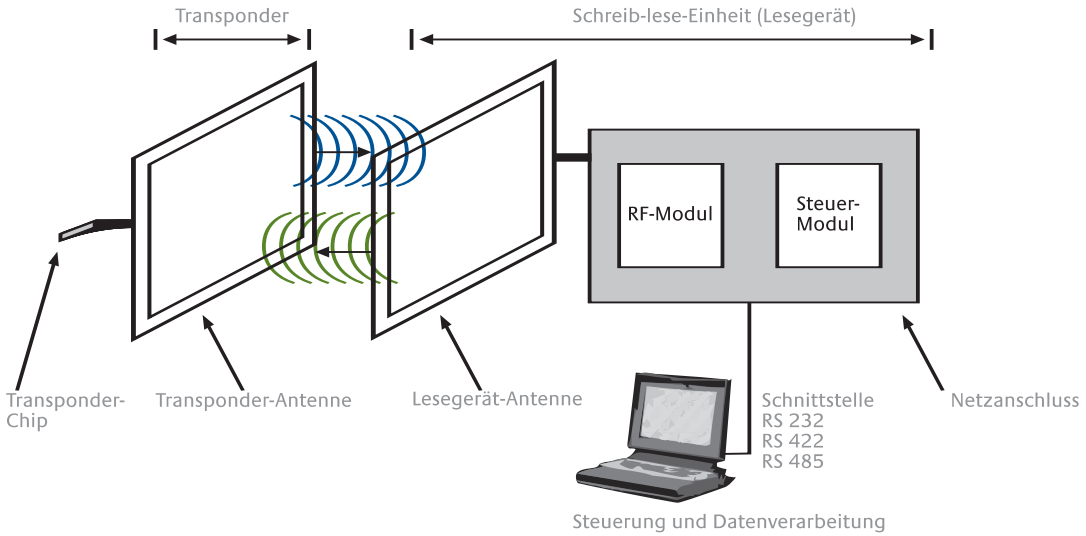


Abbildung 4-1: Aufbau und grundsätzliche Funktion von RFID-Systemen [Vinc 03]

mittlung. Die Lesegeräte sind typischerweise mit einer zusätzlichen Schnittstelle (RS 232, RS 485 etc.) ausgestattet, um die empfangenen Daten an ein anderes System (PC, Automatensteuerung, ...) weiterzuleiten und dort weiterzuverarbeiten.

Das große Interesse der gewerblichen Wirtschaft an RFID-Systemen beruht auf der Annahme, dass die Kosten für RFID-Systeme zukünftig sinken werden. Vor diesem Hintergrund können die im Vergleich zu anderen Auto-ID-Verfahren erweiterten Potenziale von RFID-Systemen ausgeschöpft werden, Prozessveränderungen in der Distributionslogistik, im Product-Lifecyle-Management und im Customer Relationship Management umzusetzen. Aber auch im öffentlichen Sektor werden RFID-Anwendungen beispielsweise als Echtheitszertifikat für Reisepässe und als Träger biometrischer Merkmale zunehmend diskutiert.

Die Einsatzbereiche sind heute häufig dadurch gekennzeichnet, dass durch eine wiederholte und langjährige Nutzung oder aufgrund des hohen Wertes der gekennzeichneten Produkte die Kosten pro RFID-Tag eine vergleichsweise geringe Bedeutung haben. Für die kommenden Jahre prognostizieren sowohl die Anbieter von RFID-Systemen als auch Marktforscher ein stark steigendes Wachstum des RFID-Einsatzes.

Der mit der Informations- und Kommunikationstechnik einhergehende technische, ökonomische und gesellschaftliche Wandel wirft aber nicht nur Fragen nach den Chancen, sondern auch nach den Gefahren dieser Technologien auf. Die Frage nach der Sicherheit von Informations- und Kommunikationsbeziehungen entwickelt sich dabei immer mehr zu einer Schlüsselfrage – für die Entwicklung und Gestaltung neuer Ebenen des Daten- und Wissensaustauschs. Der wirtschaftliche Erfolg von Unternehmen hängt davon ab, inwieweit es gelingt, die internen Datenbestände und die externe Kommunikation gegen Datenverlust und Datenmissbrauch zu schützen. Aus der Sicht des Verbraucher- und Datenschutzes gilt es, in „der Welt künftiger vernetzter und allgegenwärtiger Datenverarbeitung“ die „Grund-sätze der Vermeidung des Personenbezugs, der Erforderlichkeit und der Zweckbindung“ bei der Datenerfassung und -verarbeitung umzusetzen, wann immer Daten – auch nachträglich – Personen zugeordnet werden können. [RPG 01]

So wächst die Erkenntnis, dass die Bewertung technischer Entwicklungen vorausschauend und problemorientiert erfolgen sollte, um frühzeitig Hinweise für eine zukunftsfähige Technikgestaltung zu gewinnen. Hierzu zählt auch die interdisziplinäre Abschätzung der Chancen und Risiken des Einsatzes von RFID-Systemen mit fokussiertem Blick auf die Bereiche Informationssicherheit und Datenschutz. Nur so können echte oder vermeintliche Sicherheitsprobleme als zentrale Barriere der wirtschaftlichen Nutzung der RFID-Technologie frühzeitig erkannt und so weit als möglich auch vermieden werden.

4.2. Ziele, methodische Herangehensweise und Aufbau der Studie

Vor diesem Hintergrund ist es das Ziel der Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“, die derzeitige technologische Entwicklung in einem Teilbereich des Pervasive Computing, nämlich des Einsatzes von RFID-Systemen,

- zu dokumentieren und ausgewählte Anwendungsfelder zu beleuchten,
- Auswirkungen im Bereich der IT-Sicherheit abzuschätzen sowie
- Chancen und Risiken des Einsatzes von RFID-Systemen darzustellen.

Die Untersuchung soll dazu beitragen, für das Thema der Informationssicherheit im Innovationsfeld RFID zu sensibilisieren, anhand konkreter Potenziale und Gefährdungen bei den Entscheidungsträgern Bewusstsein zu wecken und zu motivieren, die informationstechnischen Systeme in den Unter-

nehmen und Organisationen angemessen und proaktiv zu analysieren und nachhaltig zu schützen.

Die methodische Herangehensweise der vorliegenden Untersuchung basiert auf einem gezielten Mix von quantitativen und qualitativen Ansätzen. Im Rahmen einer umfassenden Literatur- und Dokumentenanalyse wurde zunächst der Sachstand aufgearbeitet. Unternehmen, die RFID-Lösungen in Deutschland anbieten, wurden recherchiert und die Leistungspalette ihrer auf dem Markt verfügbaren RFID-Systeme erfasst. Auf der Grundlage dieser Untersuchungsergebnisse werden die Grundlagen der RFID-Technologie dargestellt, das Leistungsportfolio heutiger Lösungen ermittelt und die verfügbaren RFID-Systeme klassifiziert (Kapitel 5 und 6).

Hierauf aufbauend wurde eine Strukturierung der Angriffe und Gegenmaßnahmen im Bereich der Informationssicherheit von RFID erarbeitet. Als qualitativer Input wurden Experteninterviews genutzt, die entlang eines Leitfadens telefonisch oder persönlich durchgeführt wurden. Die bewertenden Einschätzungen von ausgewiesenen Fachleuten aus Unternehmen und Forschungseinrichtungen ergänzen und vertiefen die Erkenntnisse der Literatur- und Dokumentenanalyse sowie der Analyse der Herstellerangaben auf dem Markt verfügbarer RFID-Systeme (Kapitel 7).

Einen weiteren Schwerpunkt der Studie bildet die Ermittlung von bestehenden und zukunftsfähigen Anwendungsbereichen der RFID-Technologie. Heute bereits eingesetzte, aber auch in Pilotvorhaben getestete Verfahren und Herangehensweisen werden umfassend dargestellt (Kapitel 8).

Die fördernden und hemmenden Faktoren für einen weiteren Einsatz von RFID-Systemen, die Stärken und Schwächen von ausgewählten Auto-ID-Verfahren im Vergleich, die erwartete Marktentwicklung sowie die Anwendung von Authentifizierungsverfahren und weiteren Sicherheitsmechanismen aus Unternehmenssicht wurde mit einem quantitativen Ansatz erfasst. Mit einer Online-Befragung, die im August 2004 durchgeführt wurde, konnten Einschätzungen von 70 Unternehmen, die im Handlungsfeld RFID bereits praxisrelevante Erfahrungen gesammelt haben, erhoben werden. Per E-Mail angeschrieben wurden insgesamt 160 Vertreterinnen und Vertreter von Unternehmen und Forschungseinrichtungen. Unter den angeschriebenen Organisationen sind alle im „Verband für Automatische Datenerfassung, Identifikation und Mobilität“ (AIM-D e. V.) organisierten Einrichtungen. Innerhalb von drei Wochen nahmen 43,75 Prozent der angeschriebenen Unternehmen und Forschungseinrichtungen an der Online-Befragung teil.

Die Abbildung 4-2 zeigt die Verteilung der antwortenden Unternehmen auf die verschiedenen Wirtschaftssegmente, Mehrfachnennungen waren möglich. Sieben der 160 Unternehmen teilten mit, dass sie nicht im RFID-Sektor tätig sind, zwei Fragebögen wurden von Unternehmen ausgefüllt, die nicht direkt angeschrieben wurden.

Die Ergebnisse der Online-Befragung bilden neben den Ergebnissen der Literatur- und Dokumenten-analyse sowie der durchgeführten Experten-interviews zum einen die Basis der Identifikation von fördernden und hemmenden Faktoren für den Einsatz von RFID-Systemen. Zum anderen dienen sie der Analyse zentraler Stärken und Schwächen von ausgewählten automatischen Identifikationsverfahren im Vergleich (Kapitel 9).

Des Weiteren dienten die Ergebnisse dazu, die Entwicklungsperspektiven von RFID-Systemen für den Zeitraum bis zum Jahr 2010 abzuschätzen. Hierfür wurden in den Anwendungszusammenhängen „Kennzeichnung von Produkten“ sowie „Zutritt und Routenkontrolle“ zunächst fiktive Fallbeispiele entwickelt, die grundsätzlich mögliche Risiken des Einsatzes von RFID-Systemen veranschaulichen. Die Fokussierung auf etwaige Risiken beruht auf der Annahme, dass ein entscheidender Erfolgsfaktor für die

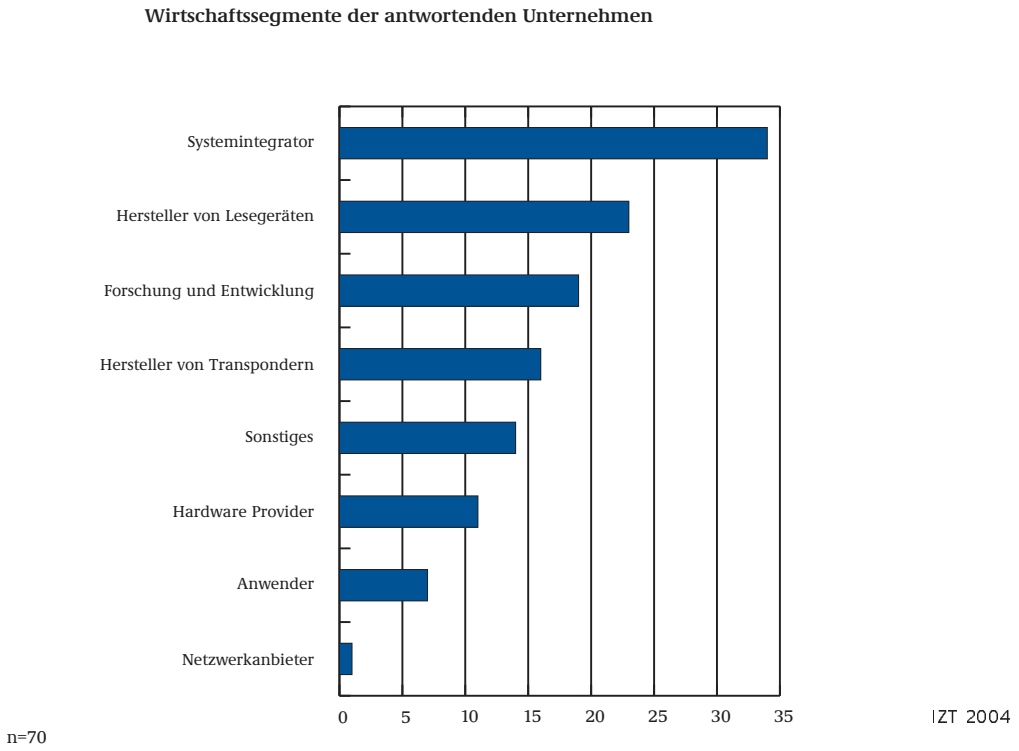


Abbildung 4-2: Wirtschaftssegmente der antwortenden Unternehmen

zukunftsfähige Entwicklung der RFID-Technologie und darauf basierenden Diensten und Anwendungen darin liegt, die Erfordernisse der Informationssicherheit und des Datenschutzes in allen Phasen der Gestaltung und Umsetzung frühzeitig zu berücksichtigen. Die Fallbeispiele sind somit als Diskussionsbeitrag zur Sensibilisierung in einer derzeit häufig kontrovers geführten Diskussion zu verstehen.

Den Abschluss der Studie bildet die Darstellung absehbarer Entwicklungen im Kontext von RFID-Systemen. Hierzu zählen neben den technologischen Entwicklungssträngen auch die qualitativ veränderten Anforderungen in den Bereichen Informationssicherheit und Datenschutz sowie der gesellschaftlichen Akzeptanz von RFID-Systemen (Kapitel 10).

5. Grundlagen der RFID-Technologie

5.1. Eigenschaften und Ausführungen von RFID-Systemen

RFID-Systeme werden in vielfältigen Varianten angeboten. Trotz der großen Bandbreite der RFID-Lösungen ist jedes RFID-System durch die folgenden drei Eigenschaften definiert:

1. **Elektronische Identifikation:**
   Das System ermöglicht eine eindeutige Kennzeichnung von Objekten durch elektronisch gespeicherte Daten.

2. **Kontaktlose Datenübertragung:**
   Die Daten können zur Identifikation des Objekts drahtlos über einen Funkfrequenzkanal ausgelesen werden.

3. **Senden auf Abruf (on call):**
   Ein gekennzeichnetes Objekt sendet seine Daten nur dann, wenn ein dafür vorgesehenes Lesegerät diesen Vorgang abruft.

RFID-Systeme zählen zu den Funkanlagen. Durch die elektronische Identifikation sowie die Eigenschaft, dass Transponder nur auf Abruf Daten übermitteln, grenzen sich RFID-Systeme von anderen digitalen Funktechnologien wie Mobilfunk, W-LAN oder Bluetooth ab.

RFID-Systeme müssen mindestens die folgenden Leistungen erbringen:

1. die Identifizierung des Transponders innerhalb einer jeweils spezifizierten Reichweite,
2. das Auslesen der Daten des Transponders,
3. die Selektion der für das jeweilige System relevanten Transponder,
4. die Gewährleistung, dass mehrere Transponder innerhalb der Reichweite des Lesegeräts gleichzeitig verwaltet werden,
5. das Durchführen der Fehlererkennung zur Gewährleistung der Betriebssicherheit.

RFID-Systeme können darüber hinaus weitere Leistungsmerkmale aufweisen, z. B. die Speicherung von zusätzlichen Daten sowie Sicherheitsfunktionen oder die Kopplung mit Sensoren. Es handelt sich dann um spezielle Unterklassen von RFID-Systemen. Leistungsmerkmale zur Gewährleistung der Informationssicherheit (z. B. kryptografische Verfahren zur Verschlüsselung der übertragenen Daten) werden in Kapitel 7 dargestellt.

Als wichtiges Kriterium insbesondere für überbetriebliche Anwendungen wird die so genannte ISO/IEC-Kompatibilität weiter an Bedeutung gewinnen. Im Bereich der RFID-Systeme übernimmt die International Organization for Standardization (ISO) die Aufgabe der internationalen Normung. Die ISO/IEC-Standards legen beispielsweise Frequenzen, Übertragungsgeschwindigkeiten, Protokolle und Kodierungen fest. Derzeit liegen erst für wenige RFID-Systeme Regelungswerke vor. Hierzu zählen Close-Coupling-Systeme sowie Vicinity und Proximity Cards, die in ihren Abmessungen typischen Smart Cards – beispielsweise Kreditkarten – entsprechen. Funktionen von Vicinity Cards werden durch ISO/IEC 15693 geregelt. ISO/IEC 14443 definiert den Funktionsumfang von Proximity Cards. Zu den wichtigsten Normen zählt des Weiteren der zukünftige ISO/IEC-18000-Standard, der die Luftschnittstelle für RFID-Systeme unterschiedlicher Frequenzbereiche definieren wird. Dieser Standardisierungsprozess wird in Kürze publiziert und damit abgeschlossen sein.

Sowohl Transponder als auch Lesegeräte werden derzeit in verschiedenen Ausführungen angeboten, die jeweils auf spezifische Anwendungsfelder und Einsatzbereiche ausgerichtet sind. Das Angebot an Lesegeräten kann grob in stationäre und mobile Ausführungen gegliedert werden, die teilweise auch für die Nutzung in rauen Umgebungen geeignet sind. Auch das Angebot der Transponder-Ausführungen ist vielfältig. Hierzu zählen beispielsweise:

- Smart Labels: Transponder, die zur Waren- oder Preisauszeichnung, aber auch auf Paketen, Boxen und Paletten im Logistikbereich oder als Fluggepäckaufkleber verwendet werden. Es handelt sich dabei um Identifikationsetiketten, die meist auf Papier, Pappe oder Kunststofffolie aufgebracht werden;
- Glaszylinder-Transponder für Anwendungen, die kleine Abmessungen erfordern (z. B. als Wegfahrsperren oder zur Tieridentifikation);
- Transponder in einer Kunststoffhülle für robuste Anwendungen, beispielsweise in der Fertigung oder Anwendungen mit Feuchtigkeitseinwirkung, z. B. laminierte Disc-Tags;
- Industrietransponder in metallischer Bauform für Anwendungen im Bereich der industriellen Fertigung mit besonderen Anforderungen an Hitze- und Chemikalienbeständigkeit;
- Großformatige Transponder im Long-Range-Bereich für Anwendungen in der Container- und Waggonlogistik;
- Card-Transponder: in Kunststoff eingebettete Transponder im Scheckkartenformat (z. B. für Zugangskontrollen und Ticketing oder als Kunden-, Bonus- oder Servicekarten).

5.2. Unterscheidungsmerkmale von RFID-Systemen

5.2.1. Frequenzbereiche

RFID-Systeme nutzen einerseits Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Anwendungen bereitgestellt werden (so genannte ISM-Frequenzen). Andererseits kann in Europa der Frequenzbereich unter 135 kHz – in Amerika und Japan unter 400 kHz – für RFID-Anwendungen genutzt werden. Weltweit haben sich die Frequenzbereiche unter 135 kHz, 13,56 MHz, 869 bzw. 915 MHz (EU bzw. USA) für den kommerziellen Einsatz von RFID-Systemen etabliert. Der Frequenzbereich 2,45 GHz hat noch keinen hohen Produktreifegrad erreicht. In der Diskussion befindet sich des Weiteren der Frequenzbereich 5,8 GHz, für

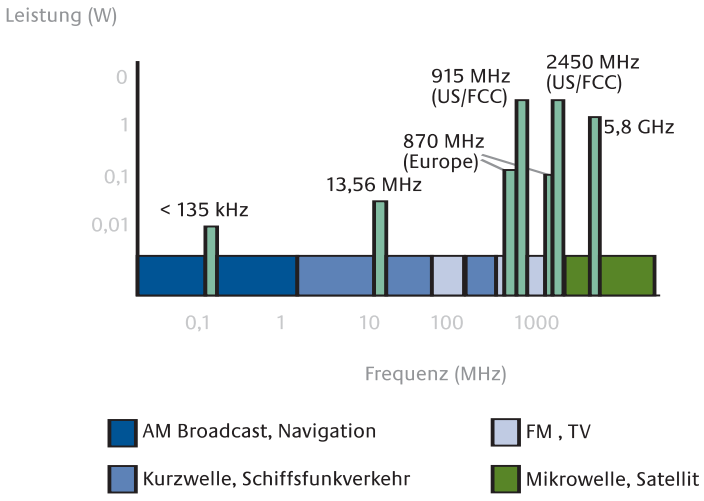


Abbildung 5-1: Weltweite Zuteilung von Funkfrequenzen für RFID [Schu 00]

Parameter	Niedrig-frequenz	Hochfrequenz	Ultrahoch-frequenz	Mikrowelle
Frequenz	125 – 134 kHz	13,56 MHz	868 bzw. 915 MHz	2,45 bzw. 5,8 GHz
Leseabstand	bis 1,2 m	bis 1,2 m	bis 4 m	bis zu 15 m (in Einzelfällen bis zu 1 km)
Lesegeschwin-digkeit	langsam	je nach ISO-Standard*	schnell	sehr schnell (aktive Transponder)
Feuchtigkeit**	kein Einfluss	kein Einfluss	negativer Einfluss	negativer Einfluss
Metall**	negativer Einfluss	negativer Einfluss	kein Einfluss	kein Einfluss
Ausrichtung des Transpon-ders beim Auslesen	nicht nötig	nicht nötig	teilweise nötig	immer nötig
Weltweit akzeptierte Frequenz	ja	ja	teilweise (EU/USA)	teilweise (nicht EU)
Heutige ISO-Standards	11784/85 und 14223	14443, 15693 und 18000	14443, 15693 und 18000	18000
Typische Transponder-Bautypen	Glasröhrchen-Transponder, Transponder im Plastikgehäuse, Chipkarten Smart Label, Chipkarten	Smart Label, Industrie-Ttransponder	Smart Label, Industrie-Ttransponder	Großformatige Transponder
Beispielhafte Anwendungen	Zutritts- und Routen-kontrolle, Wegfahr-sperren, Wäsche-reinigung, Gasablesung	Wäschereinigung, Asset Management, Ticketing, Tracking & Tracing, Pulk-Erfassung	Paletten-erfassung, Container-Tracking	Straßenmaut, Container-Tracking

* unter 1 s bis 5 s bei ISO 14443 (5 s für 32 kByte), mittel (0,5 m/s Vorbeibewegung bei ISO 15693)

** Der Einfluss von Metall und Flüssigkeiten variiert je nach Produkt. Auch werden mittlerweile RFID-Tags angeboten, die den Einsatz nach Herstellerangaben auch im Niedrigfrequenzbereich erlauben (beispielsweise „((rfid))-onMetal-Label“ von Schreiner Logidata).

Tabelle 5-1: Kenngrößen von RFID-Technologien [erweiterte Darstellung in Anlehnung an Isch 04]

den jedoch derzeit kaum Nachfrage zu verzeichnen ist. Als weltweit harmonisiert und bewährt gelten die Frequenzbänder unter 135 kHz sowie bei 13,56 MHz.

Die Frequenzregulierung ist aufgrund der weltweit uneinheitlichen Vorschriften ein Hauptproblem für die Entwicklung von international einsetzbaren RFID-Systemen. Neben Abweichungen bei der Zuteilung der Frequenzbänder sind auch unterschiedliche Vorschriften hinsichtlich der Sendestärke von Lesegeräten ein bedeutender hemmender Faktor. Im Bereich 869/915 MHz ist etwa in den USA eine maximale Sendeleistung von vier Watt zugelassen, in Europa sind dagegen nur 0,5 Watt erlaubt. Daraus resultiert ein erheblicher Unterschied der Reichweite: Trotz gleicher Bauweise von RFID-Systemen können in Europa nur aus einem Abstand von ca. einem Meter bis 2,5 Metern Daten gelesen werden. Für die USA errechnet sich dagegen eine Reichweite von ungefähr sechs bis acht Metern. [IDTE 04, RF-ID 04]

Aus den Charakteristika der unterschiedlichen Frequenzbereiche resultieren spezifische Eigenschaften, die bei RFID-Lösungen berücksichtigt werden müssen. So haben sich typische Einsatzfelder entwickelt, die sich auch bei den Transpondertypen widerspiegeln (siehe Tabelle 5-1).

5.2.2. Speichertechnologie

Allgemeines
Ein zentrales Unterscheidungsmerkmal von RFID-Systemen besteht in der jeweils zum Einsatz kommenden Speichertechnologie, wobei grundsätzlich zwischen Read-only- und Read-write-Systemen unterschieden werden kann:

- Read-only-Transponder, die nach dem Programmiervorgang beim Hersteller vom Lesegerät nur gelesen werden können, sind kostengünstiger in der Herstellung. Variable Information, die mit dem Tag assoziiert werden soll, muss in einer Datenbank im Backend des RFID-Systems abgelegt werden. Beim Auslesen des Tags wird diese Information anhand der ID-Nummer (Seriennummer) des Tags aus der Datenbank abgerufen.
- Read-write-Transponder sind durch den bereitgestellten Speicher teurer in der Herstellung. Dadurch können leistungsfähige Sicherheitsmechanismen implementiert und auch variable Informationen auf dem Transponder selbst neu gespeichert werden.

In RFID-Systemen kommen die im Folgenden erläuterten ROM- und RAM-Technologien zum Einsatz.

ROM-Lösungen (EPROM, EEPROM und Flash-EPROM)
Ein ROM (Read Only Memory) ist ein digitaler Festwertspeicher, in dem Daten dauerhaft und unveränderlich gespeichert werden. Die Daten werden während der Produktion fest in der Halbleiterstruktur abgelegt und können weder elektrisch noch optisch gelöscht oder verändert werden.

Dagegen lassen sich bei EPROM, EEPROM und Flash-EPROM Daten löschen und neu schreiben. Das EPROM (Erasable Programmable ROM) benötigt hierfür bestimmte Spannungsimpulse, für die ein Zusatzgerät, der EPROM-Programmierer, genutzt wird. Ein Löschvorgang dauert mehrere Minuten.

Auch für das Wiederbeschreiben der EEPROM (Electrically Erasable Programmable ROM) werden Spannungsimpulse genutzt, um die Speicherzellen zu programmieren bzw. zu löschen. Die Schreib-Lese-Zyklen können bis zu 10^6- bzw. 10^8-mal wiederholt werden. Der Speichervorgang wird über eine serielle Leitung durchgeführt.

Beim Flash-EPROM ist die Speicherung von Daten funktionell identisch zum EEPROM. Die Daten werden allerdings wie bei einer Festplatte blockweise geschrieben und gelöscht. Das Programmieren ist ebenfalls zeitaufwendig und kompliziert. Der Vorteil

von Flash-EPROM ist, dass die erreichbare Speichergröße durch die einfache und Platz sparende Anordnung der Speicherzellen nach oben offen ist. Die Daten bleiben ohne Stromzufuhr bis zu zehn Jahren erhalten. Zu den typischen Anwendungen von Flash Memory zählen kleine Speicherkarten im PCMCIA- oder Compact-Flash-Format.

Für RFID-Systeme haben vor allem EEPROM-Systeme eine hohe zahlenmäßige Bedeutung erlangt. Flash-EPROMs sind überwiegend auf Smart Cards beschränkt.

RAM-Lösungen (DRAM, SRAM, FRAM)
Ein RAM (Random Access Memory) wird umgangssprachlich als Arbeitsspeicher bezeichnet. Die Haupteigenschaft eines RAM ist es, den Speicherbaustein mit Daten zu beschreiben. Für den Datenerhalt ist jedoch eine kontinuierliche Stromversorgung erforderlich, bei einer Stromunterbrechung werden die Daten gelöscht. RAM stehen einem Chip als schneller Zwischenspeicher für Daten und Programme zur Verfügung mit dem Ziel, die Gesamtleistung des Systems durch schnelle Zugriffe zu steigern.

Im Bereich der RFID-Systeme finden so genannte SRAM (Static Random Access Memory) Verwendung, bei denen im Gegensatz zu dynamischen RAM (DRAMs) der Speicherinhalt nicht regelmäßig aufgefrischt werden muss. Nachteilig wirkt sich die relativ hohe Stromaufnahme aus. Aufgrund ihres vergleichsweise hohen Preises finden SRAMs zunehmend weniger Verwendung.

FRAM (Ferroelectric Random Access Memory) ist eine neue Entwicklung und weist gegenüber herkömmlichen Festwertspeichern viele Vorteile auf: FRAM benötigt für den Datenerhalt keine Stromversorgung. FRAM-Speicher sind kompatibel zu gängigen EEPROMs, ermöglichen jedoch in Vergleich zu diesen (wie auch zur Flash-Technologie) bis zu 10.000-fach schnellere Schreib- und Lesevorgänge. Die Datenhaltbarkeit liegt bei über zehn Jahren, auch dann, wenn der Chip starken Temperaturschwankungen ausgesetzt ist. Mit garantierten 10^{10} Schreib- und Lesezyklen übersteigt FRAM auch bei diesem Merkmal die Leistungsfähigkeit von EEPROMs.

5.2.3. Energieversorgung der Transponder und Datenübertragung

Aktive und passive Transponder
Grundsätzlich gibt es zwei Transpondertypen sowie Mischformen beider Typen: aktive und passive Transponder.

- Aktive Transponder verfügen über eine eigene Energiequelle zur Erzeugung elektromagnetischer Wellen. Obwohl sie batteriebetrieben sind, befinden sie sich im Ruhezustand, sofern nicht von einem Lesegerät ein Aktivierungssignal empfangen wird.
- Passive Transponder werden dagegen bei Lesevorgängen über Funkwellen durch die Lesegeräte mit Energie versorgt. Im Vergleich zu aktiven Transpondern verfügen sie typischerweise über eine geringe Reichweite, benötigen jedoch für die Energieversorgung des Transponders leistungsstärkere Lesegeräte als aktive RFID-Systeme.

Zur Energieversorgung und Kommunikation von bzw. mit Transpondern werden in der Regel zwei Verfahren eingesetzt: die induktive Kopplung und das auf dem Radarprinzip beruhende Backscatter-Verfahren. Close-Coupling-Systeme können darüber hinaus aufgrund des geringen Abstands zwischen Transponder und Erfassungsgerät auch über eine kapazitive Kopplung mit Energie versorgt werden.

Kapazitive Kopplung
Die kapazitive Kopplung beruht auf dem Plattenkondensator-Prinzip. Die Signalübertragung erfolgt zwischen zwei voneinander isolierten elektrischen Leitern, die sowohl im Transponder als auch im Lesegerät parallel angeordnet sind. Wird durch ein elektrisches Signal eine Ladungsveränderung auf einem

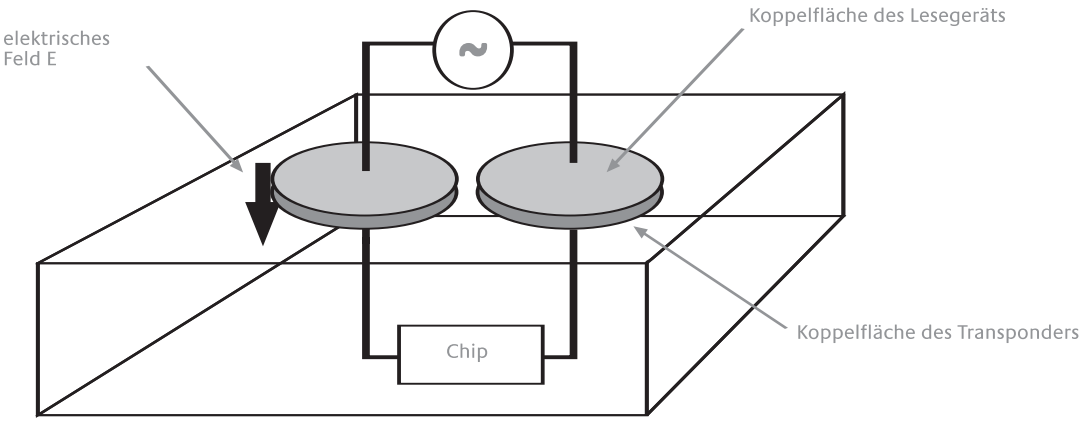


Abbildung 5-2: Kapazitive Kopplung [Fink 02]

Leiter erzeugt, wirkt sich diese Veränderung über ein elektrisches Feld auf die Ladungs–träger des zweiten Leiters aus. Die so erreichte Koppelkapazität ist verhältnismäßig gering und ist somit nicht für die Energieversorgung von Mikroprozessoren geeignet. Diese Energieversorgung muss deshalb ergänzend induktiv erfolgen.

Induktive Kopplung

Induktiv gekoppelte Transponder zählen fast immer zu den passiven Transpondern, so dass die gesamte, für den Betrieb erforderliche Energie durch das Lesegerät zur Verfügung gestellt werden muss. Ein induktiv gekoppelter Transponder besteht aus einem elektronischen Datenträger und einer großflächigen Spule, die als Antenne dient.
Zur Energieversorgung des Transponders wird von der Antennenspule des Lesegeräts ein elektromagnetisches Feld erzeugt. Ein

Teil des ausgesendeten Feldes durchdringt die Antennenspule des Transponders. Durch Induktion wird an der Antennenspule des Transponders eine Spannung generiert. Diese Spannung wird gleichgerichtet und dient der Energieversorgung des Transponders. Zur Vorbereitung der Datenübertragung wird der Antennenspule des Lesegeräts ein Kondensator parallel geschaltet, dessen Kapazität so gewählt wird, dass zusammen mit der Spuleninduktivität der Antennenspule der Parallelschwingkreis gebildet wird, dessen Resonanzfrequenz der Sendefrequenz des Lesegeräts entspricht. Die Antennenspule des Transponders bildet zusammen mit einem Kondensator ebenfalls einen Schwingkreis, welcher auf die Sendefrequenz des Lesegeräts abgestimmt ist.

Wird ein resonanter Transponder in das magnetische Wechselfeld der Antenne des Lesegeräts gebracht, entzieht dieser dem magnetischen Feld Energie. Die dadurch hervorgerufene Rückwirkung des Transponders auf die Antenne des Lesegeräts kann als transformierte Impedanz in der Antennenspule des Lesegeräts dargestellt werden. Das Ein- und Ausschalten eines Lastwiderstandes

an der Antenne des Transponders bewirkt eine Veränderung der transformierten Impedanz und damit Spannungsänderungen an der Antenne des Lesegeräts. Dies entspricht in der Wirkung einer Amplitudenmodulation durch den entfernten Transponder. Wird das An- und Ausschalten des Lastwiderstandes durch Daten gesteuert, können diese Daten vom Transponder zum Lesegerät übertragen werden.

Die Rückgewinnung der Daten im Lesegerät geschieht durch eine Gleichrichtung der an der Antenne des Lesegeräts abgegriffenen Spannung.

Backscatter-Verfahren

Das Backscatter-Verfahren kommt hauptsächlich bei Long-Range-Systemen zum Einsatz und basiert auf den Prinzipien der Radartechnik. Die zugrunde liegende Radargleichung besagt, dass elektromagnetische Wellen von Materie, die eine Ausdehnung von mehr als der halben Wellenlänge der ausgesandten elektromagnetischen Welle besitzt, reflektiert werden. Besonders gut werden elektromagnetische Wellen dann reflektiert, wenn das Objekt, auf das die Wellenfront trifft, in Resonanz gerät.

Um diesen Effekt für die RFID-Technologie auszunutzen, wird sowohl für das Lesegerät als auch für den Transponder eine Dipolantenne konstruiert, die für die jeweils verwendete Frequenz ein Resonanzverhalten zeigt. Zur Energieversorgung wird von der Antenne des Lesegeräts eine bestimmte Sendeleistung abgestrahlt. Die am Transponder ankommende Leistung steht als Hochfrequenzspannung an den Anschlüssen der Antenne zur Verfügung und kann nach Gleichrichtung zur Energieversorgung des Transponders verwendet werden.

Ohne Stützbatterie wird mit dieser Technik bei einer Sendefrequenz von 868 MHz eine Reichweite von ca. drei Metern erreicht, bei 2,45 GHz kann immerhin noch eine Entfernung zwischen Transponder und Lesegerät von etwas über einem Meter erzielt werden.

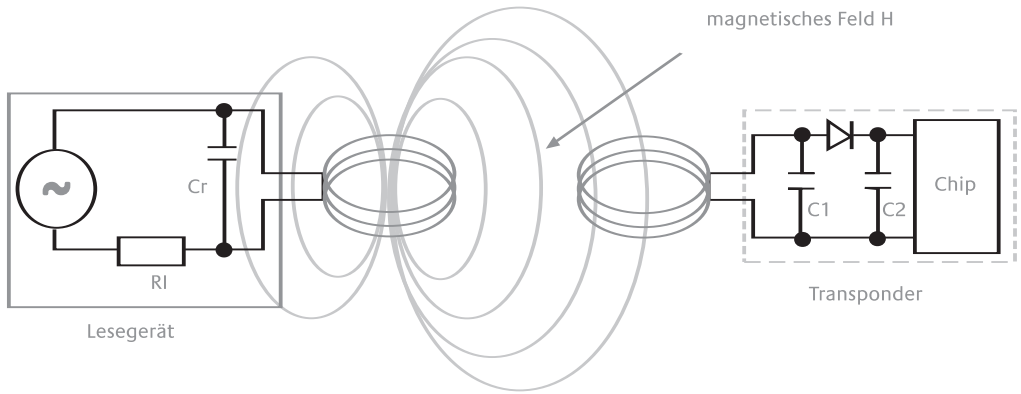


Abbildung 5-3: Spannungsversorgung eines induktiv gekoppelten Transponders aus der Energie des magnetischen Wechselfeldes, das vom Lesegerät erzeugt wird [Fink 02]

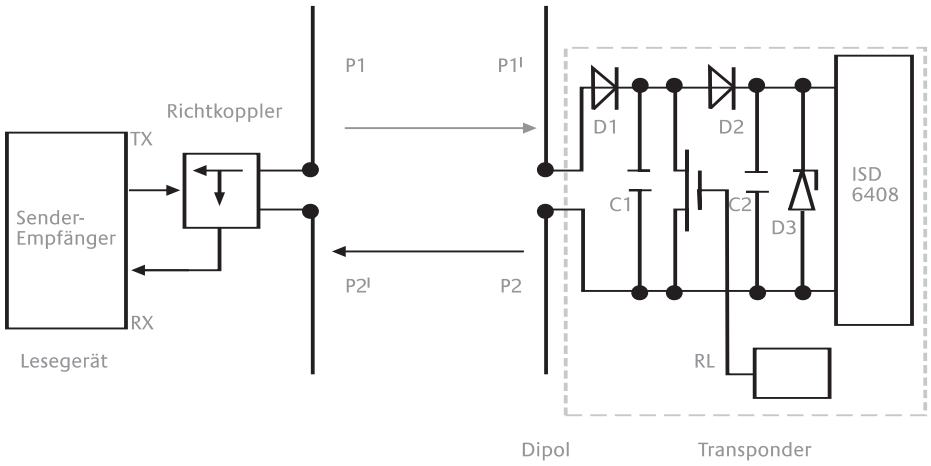


Abbildung 5-4: Funktionsweise eines Backscatter-Transponders [Fink 02]

Ein Teil der an der Transponderantenne ankommenden Leistung kann nicht zur Stromversorgung genutzt werden und wird reflektiert. Welcher Leistungsanteil reflektiert wird, kann über die Antenneneigenschaften bestimmt werden. Mit dem Ziel der Datenübertragung wird im Transponder ein Lastwiderstand parallel zur Dipolantenne geschaltet. Wird der Lastwiderstand im Takt des zu übertragenden Datenstroms ein- und ausgeschaltet, entsteht ein amplitudenmoduliertes Signal, das von der Antenne des Lesegeräts aufgenommen werden kann. Das Verfahren wird als „modulierter Rückstrahlquerschnitt“ bzw. „modulated backscatter“ bezeichnet.

Betriebsart

Zur Übertragung von Daten zwischen dem Transponder und einem Lesegerät kommen zwei grundsätzlich unterschiedliche Verfahren zum Einsatz: Duplexverfahren – wobei zwischen Vollduplexverfahren (FDX) und Halbduplexverfahren (HDX) unterschieden wird – sowie sequentielle Systeme (SEQ). Voll- und Halbduplex-Verfahren ist gemeinsam, dass die Energieübertragung zwischen Lesegerät und Transponder sowohl im Uplink als auch im Downlink kontinuierlich und unabhängig von der Datenübertragung erfolgt. Bei sequentiellen Systemen dagegen wird der Transponder nur in den Pausen der Datenübertragung vom Tag zum Lesegerät mit Energie versorgt.

5.2.4. Mehrfachzugriffsverfahren bzw. Antikollisionsverfahren

Allgemeines

Eine besondere Herausforderung besteht, wenn sich mehrere RFID-Tags gleichzeitig im Lesebereich befinden und ihre Identifikationsnummer an das Lesegerät senden. Da alle Tags eines bestimmten Typs im selben Frequenzbereich senden, überlagern sich deren Signale und das Lesegerät kann keines der Tags identifizieren (Kollision). Ein Lesegerät muss deshalb mit einen Selektionsver-

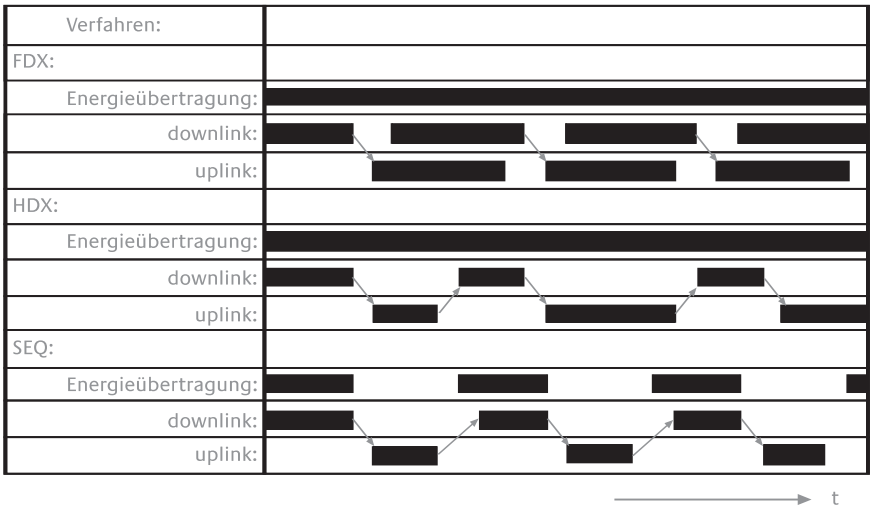


Abbildung 5-5: Darstellung der zeitlichen Abläufe bei Vollduplex-, Halbduplex- und sequentiellen Systemen. Der Übertragungskanal vom Lesegerät zum Transponder wird als Downlink, der umgekehrte Übertragungskanal als Uplink bezeichnet. [Fink 02]

fahren dafür sorgen, dass die Chips ihre Information einzeln senden. Für Anwendungsfälle, bei denen sich die Anwesenheit mehrerer RFID-Tags nicht ausschließen lässt oder bei denen dies sogar erwünscht ist (Pulkerkennung) kommen Antikollisions-Verfahren zur Anwendung.

Die in RFID-Systemen am häufigsten verwendeten Antikollisions-Verfahren basieren auf dem TDMA-Prinzip (Time Division Multiple Access). Hierbei wird die gesamte im Frequenzkanal zur Verfügung stehende Übertragungskapazität nacheinander auf die einzelnen Tags aufgeteilt (Zeitmultiplex). Transpondergesteuerte Verfahren sind verhältnismäßig langsam, da das Lesegerät seine Anfrage (Request) wiederholen muss, bis alle Tags mit hinreichender Wahrscheinlichkeit erkannt worden sind. Bei lesegerätgesteuerten Verfahren selektiert das Lesegerät die einzelnen Tags hingegen nacheinander in rascher zeitlicher Abfolge. In der Praxis haben hauptsächlich das transpondergesteuerte Aloha-Verfahren und das lesegerätgesteuerte Tree-Walking-Verfahren Bedeutung erlangt.

Aloha-Verfahren

Das transpondergesteuerte Aloha-Verfahren beruht auf einer probabilistischen Abfrage der Identifikationsnummern (ID-Nummern) aller im Lesebereich befindlichen Tags. Das Lesegerät sendet ein stets gleichlautendes Request-Kommando an alle Tags, sich mit ihrer vollen ID-Nummer zu identifizieren. Jedes Tag reagiert darauf mit einer individuellen, zufälligen Zeitverzögerung und sendet die ID-Nummer in voller Länge. Da die Datenübertragung eines Tags verglichen mit der Dauer des Request-Intervalls kurz ist, kommt es bei einer begrenzten Anzahl von Tags im Lesebereich nur sehr selten zu einer Kollision. Durch mehrfaches Durchlaufen des Request-Zyklus haben alle Tags eine hohe Chance, ihre ID-Nummer mindestens einmal kollisionsfrei zu übertragen. Nach einiger Zeit (im Sekundenbereich) hat das Lesegerät

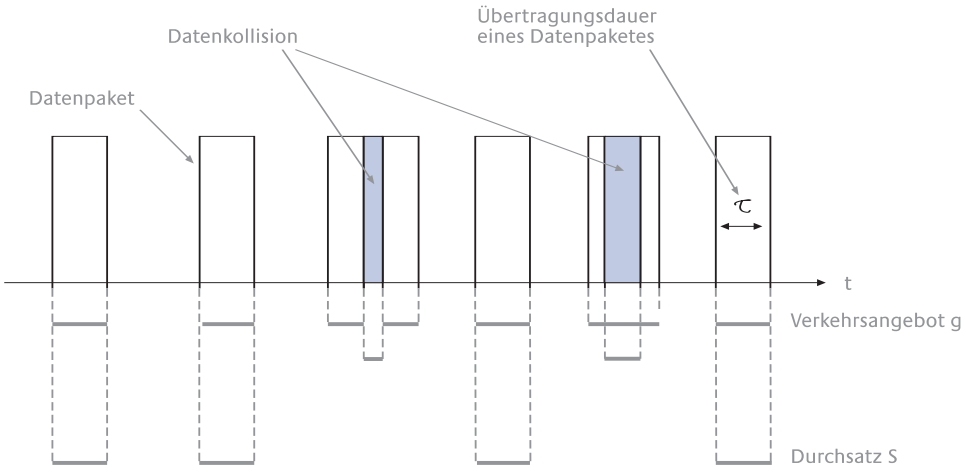


Abbildung 5-6: Definition von Verkehrsangebot G und Durchsatz S eines Aloha-Systems. Mehrere Transponder senden ihre Datenpakete zu zufälligen Zeitpunkten. Dabei kommt es ab und zu auch zu Datenkollisionen, durch welche der (Daten-)Durchsatz S für die kollidierten Datenpakete zu null wird. [Fink 02]

mit großer Wahrscheinlichkeit alle Tags erkannt. Bei einigen Variationen dieses Protokolls lassen sich die erkannten Tags auf Kommando des Lesegeräts stumm schalten, um die Wahrscheinlichkeit von Kollisionen in nachfolgenden Request-Zyklen zu verringern. In diesem Fall müssen die ID-Nummern auch über den Downlink übertragen werden und könnten deshalb von einem Angreifer aus größerer Distanz abgehört werden. [Vogt 02]

Tree-Walking-Verfahren

Im Gegensatz zum Aloha-Verfahren wird die Selektion der Tags hier durch das Lesegerät aktiv gesteuert. Es führt eine deterministische Suche durch den Adressraum der möglichen Identifikationsnummern aus. Das Lesegerät fordert, beginnend von der höchsten Stelle der ID-Nummer, alle in seiner Reichweite befindlichen Tags auf, ihre ID zu übertragen (REQUEST). Wenn man davon ausgeht, dass die vom Lesegerät empfangenen Bitfolgen im oberen Teil der ID-Nummer (höherwertige Bits) häufig übereinstimmen, ist dieses Verfahren relativ effizient. Beispielsweise sieht der vom Auto-ID-Center vorgeschlagene Electronic Product Code (EPC) vor, dass die ID mit dem sog. „Company Prefix Index“ beginnt, der in vielen Anwendungen für alle Tags gleich ist, weil sie Produkte vom gleichen Hersteller markieren. An einer niederen Stelle i der Bitfolge differenzieren sich die ID-Nummern der einzelnen Tags und es tritt eine Kollision auf (zwei Tags senden an der Stelle i gleichzeitig verschiedene Bits). Das Lesegerät erweitert nun die Abfrage, indem es an der Stelle i eine Verzweigung des binären Adressbaumes auswählt und diese zunächst weiterverfolgt. Es spricht nur noch jene Tags an, deren ID mit dem bisher bekannten Präfix und dem gewählten Wert an der Stelle i übereinstimmen. Diese Tags antworten nun mit dem Rest ihrer ID. Kommt es an niedrigeren Stellen zu weiteren Kollisionen, wird der Vorgang schrittweise so lange wiederholt, bis nur noch ein einziges Tag antwortet und keine Kollision mehr auftritt. Dieses Tag kann nun vom Lesegerät

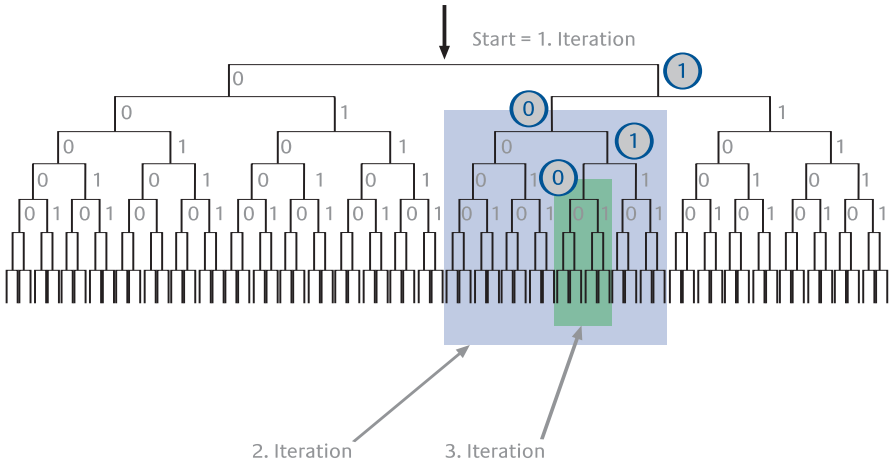


Abbildung 5-7: Binärer Suchbaum. Mit der sukzessiven Verkleinerung des Suchbereichs kann schließlich ein einzelner Transponder identifiziert werden. [Fink 02]

anhand seiner ID-Nummer eindeutig selektiert (SELECT) und ausgelesen werden (READ_DATA). Mit dem Kommando UNSELECT wird das aktive Tag anschließend stumm geschaltet.

Nachfolgend werden die restlichen Tags ab der Stelle i der ersten Verzweigung im Binärbaum nach dem gleichen Muster selektiert, bis schließlich alle im Lesebereich vorhandenen Tags mit ihrer ID-Nummer eindeutig angesprochen worden sind. Mit diesem Verfahren lässt sich eine sehr große Anzahl an Tags im Lesefeld einzeln ansprechen.

6. Klassifizierung von RFID-Systemen

6.1. Allgemeines

RFID-Systeme lassen sich entsprechend ihrer jeweiligen Leistungsmerkmale klassifizieren. Die so entstandenen Gruppen werden bezüglich der Leistungsfähigkeit ihrer jeweiligen Komponenten in Low-End-Systeme, Systeme mittlerer Leistungsfähigkeit und High-End-Systeme unterschieden. Eine weitere Gruppierung von RFID-Lösungen kann entsprechend ihrer jeweiligen Reichweite — also des maximalen Abstandes zwischen Transponder und Lesegerät – erfolgen. Hier wird in der Regel in Close-Coupling-, Remote-Coupling- sowie Long-Range-Systeme unterschieden. Die Reichweite wird als ein von der Leistungsfähigkeit unabhängiges Kriterium betrachtet.

Diese Gruppierungen ermöglichen nicht nur eine Bewertung von RFID-Systemen hinsichtlich der auf ihnen basierenden möglichen Anwendungen. Sie erlauben auch eine erste, überblickartige Einschätzung der damit verbundenen Fragen zu Informationssicherheit und Datenschutz.

6.2. Klassifizierung von RFID-Systemen nach Leistungsfähigkeit

6.2.1. Low-End-Systeme

Typische Low-End-RFID-Systeme sind einerseits so genannte 1-Bit-Systeme, die bereits langjährig für einfache Überwachungs- oder Signalisierungsfunktionen genutzt werden. Diese Systeme signalisieren einem Lesegerät nur das Vorhandensein bzw. das Nichtvorhandensein eines Transponders im Feld. Sie benötigen keine integrierte Schaltung und können somit preisgünstig „für Bruchteile eines Cents“ hergestellt werden. Beispiels-weise werden 1-Bit-Systeme zur elektronischen Diebstahlsicherung (electronic article surveillance = EAS) seit ca. 40 Jahren im Einzelhandel genutzt.

Zu den Low-End-Systemen zählen weiterhin diejenigen RFID-Lösungen, die nicht wieder beschreibbar sind und von denen somit nur Daten ausgelesen werden können. Hierfür bedarf es keines Mikroprozessors; diese Aufgaben können auch von einem Zustandsautomaten geleistet werden. Verschlüsselungsfunktionen werden typischerweise nicht unterstützt, so dass die Daten dieser Transponder durch jedes zu ihnen kompatible Lesegerät ausgelesen werden können. Überwiegend werden Low-End-Systeme im Bereich der Warenflüsse, der Identifikation von Paletten, Containern und Gasflaschen sowie der Tieridentifikation genutzt.

Ein für Low-End-Systeme typisches RFID-Produkt wird von Siemens angeboten. Der so genannte MOBY R arbeitet im 2,45-GHz-Bereich und überbrückt einen Abstand zwischen Transponder und Lesegerät von bis zu 300 Metern. Mit einem 32-bit-read-only-Code ist er beispielsweise für Einsatzgebiete im Bereich Lokalisierung vorgesehen.

6.2.2. Systeme mittlerer Leistungsfähigkeit

Das Mittelfeld des Leistungsspektrums wird durch RFID-Systeme mit wieder beschreibbaren Datenspeichern (beispielsweise EEPROM bei passiven, SRAM bei aktiven Transpondern) von wenigen Byte bis über 100 Kbyte gebildet. In diesem Segment ist die Typenvielfalt mit Abstand am größten. Systeme mittlerer Leistungsfähigkeit können sowohl mit einem Zustandsautomaten als auch mit einem Mikroprozessor ausgestattet sein. In der Regel werden in dieser Klasse Antikollisionsverfahren benutzt, um mehrere Transponder im Sichtfeld der Erfassungseinrichtung selektiv ansprechen zu können. Vor unberechtigtem Auslesen werden Systeme mittlerer Leistungsfähigkeit durch Authentifizierungs- oder auch Kryptofunktionen geschützt.

Beispielsweise ist der Infineon my-d vicinity-SRF 55V10P im Bereich von 13,56 MHz mit einem 10-Kbit-EEPROM und somit einem wieder beschreibbaren Speicher ausgerüstet.

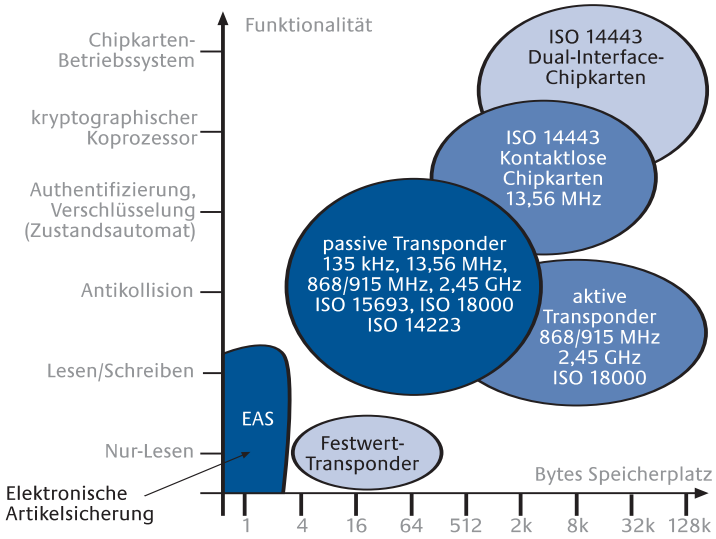


Abbildung 6-1: Klassifizierung von RFID-Systemen nach Low-End bis High-End [Fink 02]

Je nach Antenne kann das System bis zu 1,2 Metern Reichweite erzielen. Es unterstützt Antikollision und entspricht dem ISO/IEC-Standard 15693 [vgl. Infi 02].

6.2.3. High-End-Systeme

Im High-End-Bereich finden sich überwiegend kontaktlose Chipkarten mit Mikroprozessor und einem Chipkarten-Betriebssystem (Smart Card OS). Die Karten verfügen über komplexere Algorithmen zur Authentifizierung und Verschlüsselung, die nicht mit einem „festverdrahteten" Zustandsautomaten (State Machine) realisiert werden können. Das obere Ende des High-End-Bereichs bilden schließlich Dual-Interface-Karten, welche mit einem kryptografischen Co-Prozessor ausgestattet sind. Die Arbeitsfrequenz liegt typischerweise bei 13,56 MHz, die Reichweite unterhalb von15 Zentimetern (im Close-Coupling- oder Proximity-Bereich).

Anwendung finden derartige Chipkarten in Bereichen mit hohen Sicherheitsanforderungen wie elektronische Börsensysteme, Ticketing und für Bezahlfunktionen.

Philips bietet beispielsweise mit dem SmartMX ein High-End-System an. Der SmartMX erfüllt den ISO-14443-Standard und bietet 72 kByte Speicher und die Möglichkeit, weitere Funktionalitäten auf dem Tag zu integrieren. Er unterstützt Antikollision. Die Datenübertragungsrate kann bis zu 848 kBit/s betragen. Mit einem kryptografischen Co-Prozessor werden asymmetrische Verschlüsselungsverfahren unterstützt.

6.3. Klassifizierung von RFID-Systemen nach Reichweiten

RFID-Systeme werden hinsichtlich ihrer Reichweite in drei Bereiche unterteilt – Close-Coupling-, Remote-Coupling- und Long-Range-Systeme:

- Bei **Close-Coupling-Systemen** liegt die Reichweite im Bereich bis zu einem Zenti-

meter. Close-Coupling-Systeme können mit nahezu beliebigen Frequenzen arbeiten (von Niederfrequenz bis 30 MHz), abhängig von der Art der Kopplung. Bei induktiver Kopplung liegt die Frequenz meistens zwischen einem MHz und zehn MHz. Die Datenübertragung erfolgt bei Close-Coupling-Systemen entweder über eine induktive oder – möglich bei einer sehr geringen Entfernung zwischen Transponder und Lesegerät – über eine kapazitive Kopplung. Close-Coupling-Systeme werden in Bereichen mit hohen Sicherheitsanforderungen – beispielsweise bei Chipkarten mit Zahlungsfunktion oder im Bereich der Zutrittskontrolle – eingesetzt.

- **Remote-Coupling-Systeme** verfügen über eine Reichweite von bis zu ca. einem Meter. Sie arbeiten typischerweise im Frequenzbereich unter 135 kHz sowie bei 13,56 MHz. Die Kopplung zwischen Lesegerät und Transponder erfolgt induktiv. Remote-Coupling-Systeme werden in der Regel in Proximity Cards (maximal 20 Zentimeter Abstand zwischen Transponder und Lesegerät) und Vicinity Cards (bis zu ca. einem Meter Abstand zwischen Transponder und Lesegerät) unterschieden.
- Als **Long-Range-Systeme** werden RFID-Systeme mit Reichweiten von über 1,5 bis typischerweise zehn Metern bezeichnet. In Ausnahmefällen sind auch höhere Reichweiten möglich: etwa 100 Meter oder sogar 1 Kilometer, wie sie im Frequenzspektrum um 5,8 GHz, das sich derzeit in einem sehr frühen Entwicklungsstadium befindet, erreicht werden können. Die Reichweiten von Long-Range-Systemen werden im Mikrowellenbereich, im 868/915-MHz-Bereich sowie im 2,45-GHz-Bereich erreicht. Long-Range-Systeme unterscheiden sich von den beiden zuvor Genannten durch die Energieversorgung der Transponder (aktiv) und der Datenübertragungsverfahren (Backscatter).

6.4. Die Klassifizierung des Auto-ID-Centers

Das Auto-ID-Center hat die folgenden Klassen von RFID-Tags spezifiziert:

- UHF Class 0 [Auto 03]
- UHF Class 1 [Auto 02]
- HF Class 1 [Auto 03b]

Transponder der UHF-Klassen arbeiten bei einer Frequenz zwischen 860 MHz bis 930 MHz nach dem Backscatter-Prinzip. Bei einer Sendeleistung des Lesegeräts von vier Watt wird eine Lesedistanz von bis zu sieben Metern erreicht. In Europa sind gegenwärtig lediglich 0,5 Watt Sendeleistung zulässig, wodurch die Lesedistanz deutlich kürzer ist. Beide Spezifikationen sehen das Tree-Walking-Verfahren als Antikollisionsmechanismus vor und unterstützen ausschließlich Read-only-Transponder. Weiterhin fordern die Spezifikationen eine Möglichkeit zur permanenten Deaktivierung eines Tags durch ein passwortgeschütztes „Kill-Kommando“ (siehe Kapitel 7.7.6.1.). Konforme Tags dürfen nach Ausführung der Kill-Funktion in keiner Weise auf Signale eines Lesegeräts reagieren.

UHF-Class-0-Tags werden während des Produktionsprozesses mit dem Electronic Product Code (EPC) beschrieben und können nachträglich nicht mehr umprogrammiert werden. UHF-Class-1-Tags können vom Anwender einmalig mit dem EPC beschrieben werden, sie verhalten sich wie ein WORM-Medium (write once read many). Eine Zusammenfassung der UHF-Klassen zu einer UHF-Class 1 Generation 2 ist beabsichtigt [RFID 03].

HF-Class-1-Tags unterscheiden sich von den oben genannten Klassen in der Frequenz (13,56 MHz) sowie im Antikollisionsmechanismus (Aloha-Verfahren). Ansonsten werden an Transponder dieser Klasse die gleichen Anforderungen wie an UHF-Class-1-Tags gestellt. Insbesondere ist auch hier eine Deaktivierungsfunktion (DESTROY Command) vorgesehen.

7. Bedrohungslage und Bestandsaufnahme gängiger Sicherheitsmaßnahmen

7.1. Übersicht

Zu den Zielen der vorliegenden Studie gehört es, die aus der Anwendung von RFID-Systemen hervorgehende Bedrohungslage prospektiv zu untersuchen (Zeithorizont drei bis fünf Jahre) sowie die Wirksamkeit von Sicherheitsmaßnahmen einzuschätzen. Dieses Kapitel stellt die Ergebnisse dieses Arbeitsschrittes dar.

Die Abschnitte 7.2 bis 7.7 geben eine Übersicht über mögliche Angriffe und Gegenmaßnahmen. Abschnitt 7.8 enthält eine bewertende Einschätzung der Bedrohungslage – insbesondere hinsichtlich Praktikabilität und Kosten der Angriffe und Gegenmaßnahmen. Die Liste der hierzu befragten Experten ist am Anfang der Studie im Abschnitt „Autoren und Experten“ zu finden. In Abschnitt 7.9 wird die derzeitige Verfügbarkeit von Sicherheitsmaßnahmen kurz dargestellt.

7.2. Grundlegende Angriffsarten

RFID-Systeme dienen dazu, die virtuelle Welt der Daten besser mit der Welt der realen Objekte zur Deckung zu bringen [Flei 01]. Die Integrität von RFID-Systemen beruht deshalb entscheidend darauf, dass drei Beziehungen gesichert sind:

1. Die Beziehung zwischen den auf einem Transponder (Tag) gespeicherten Daten und dem Transponder selbst. Hierbei muss es sich um eine eindeutige Beziehung handeln, weil der Transponder ausschließlich durch die Daten identifiziert wird. Wichtigster Bestandteil der Daten ist eine eindeutige ID-Nummer (Seriennummer). Um die Identität zusätzlich zu sichern, können auch Schlüssel oder andere Sicherheitsinformationen auf dem Transponder abgelegt sein. In jedem Fall muss ausgeschlossen werden, dass zwei Tags mit gleicher Identität existieren.
2. Die Beziehung zwischen dem Transponder und dem Trägerobjekt, zu dessen Identifikation er dient (mechanische Verbindung).

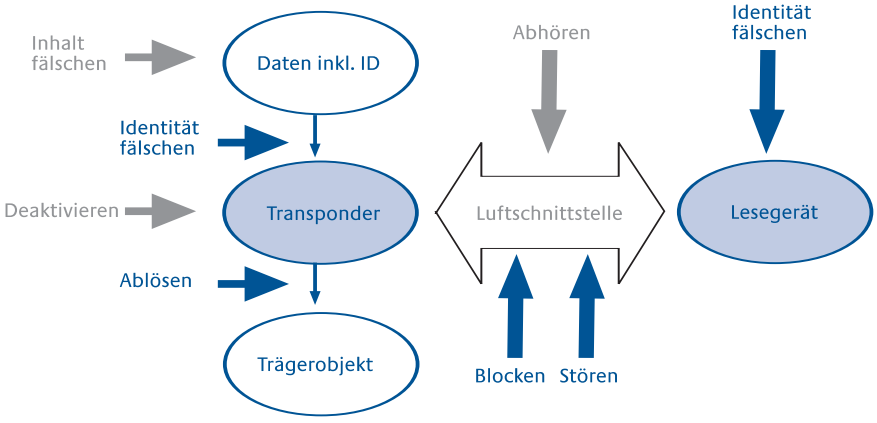


Abbildung 7-1: Grundlegende Angriffsarten bei RFID-Systemen

Diese Beziehung muss ebenfalls eindeutig sein, d. h., es darf nicht vorkommen, dass ein Transponder während seiner Nutzungsphase wechselnden Objekten zugeordnet wird.

3. Die Beziehung zwischen Transponder und Lesegerät (Luftschnittstelle). Sie muss so realisiert sein, dass autorisierte Lesegeräte die Anwesenheit des Transponders feststellen und auf die Daten korrekt zugreifen können, nicht autorisierte Lesegeräte dagegen vom Zugriff ausgeschlossen bleiben.

Daraus ergeben sich die in Abbildung 7-1 gezeigten grundlegenden Angriffsarten, die im Folgenden erläutert werden.

Inhalt fälschen
Durch unautorisierte Schreibzugriffe auf das Tag können die Daten verfälscht werden. Dieser Angriff eignet sich nur dann für eine gezielte Täuschung, wenn dabei die ID (Seriennummer) und eventuelle Sicherheitsinformationen (z. B. Schlüssel) unverändert bleiben, so dass das Lesegerät die Identität des Transponders weiterhin korrekt erkennt. Der Angriff ist nur bei RFID-Systemen möglich, die neben ID und Sicherheitsinformationen weitere Inhalte auf dem Tag speichern.

Identität fälschen (Transponder)
Der Angreifer bringt sich in den Besitz von ID und eventuellen Sicherheitsinformationen eines Tags und benutzt diese, um gegenüber einem Lesegerät dessen Identität vorzutäuschen. Dies kann durch ein Gerät geschehen, das beliebige Tags emulieren kann, oder indem ein neues Tag als Duplikat des alten hergestellt wird (Cloning). Dieser Angriff bewirkt, dass mehrere Transponder mit gleicher Identität in Umlauf sind.

Deaktivieren
Der Transponder wird durch unautorisierten Gebrauch von Lösch- oder Kill-Befehlen oder durch physische Zerstörung unbrauchbar gemacht. Je nach Art der Deaktivierung kann das Lesegerät die Identität des Tags nicht mehr feststellen oder auch die Anwesenheit des Tags im Lesebereich nicht mehr erkennen.

Ablösen
Ein Transponder wird physisch vom Trägerobjekt getrennt und eventuell mit einem anderen Objekt assoziiert, analog zum „Umkleben“ von Preisschildern. Da RFID-Systeme vollständig davon abhängig sind, dass die Transponder ihre Trägerobjekte eindeutig identifizieren, ist hier ein fundamentales, wenn auch auf den ersten Blick trivial erscheinendes Sicherheitsproblem gegeben.

Abhören
Die Kommunikation zwischen Lesegerät und Transponder über die Luftschnittstelle wird durch Auffangen und Dekodieren der Funksignale abgehört. Hierbei handelt es sich um eine der spezifischsten Bedrohungen von RFID-Systemen [FiKe 04].

Blocken
Durch so genannte Blocker-Tags wird gegenüber dem Lesegerät die Anwesenheit einer beliebigen Anzahl von Transpondern simuliert, so dass dieses blockiert wird. Ein Blocker-Tag muss für das jeweils verwendete Antikollisionsprotokoll ausgelegt sein.

Stören
Der Datenaustausch über die Luftschnittstelle kann durch passive Maßnahmen wie Abschirmen oder durch aktive Maßnahmen (Störsender) gestört werden. Aufgrund der geringen Robustheit der Luftschnittstelle können bereits einfache passive Maßnahmen wirksam sein.

Identität fälschen (Lesegerät)
In einem sicheren RFID-System muss das Lesegerät seine Berechtigung gegenüber dem Tag nachweisen. Will ein Angreifer die Daten mit einem eigenen Lesegerät auslesen, so muss dieses die Identität eines autorisierten Lesegeräts vortäuschen. Abhängig von den verwendeten Sicherheitsmaßnahmen ist dieser Angriff von „sehr einfach“ bis „praktisch unmöglich“ durchzuführen. Das Lesegerät benötigt unter Umständen Zugang zum Backend, z. B. um dort hinterlegte Schlüssel abzurufen.

7.3. Angriffsarten nach Zweck

Eine Person, die ein RFID-System angreift, kann unterschiedliche Zwecke verfolgen. Diese Zwecke können wie folgt klassifiziert werden:

1. Ausspähen: Der Angreifer verschafft sich unberechtigten Zugang zu Informationen.
2. Täuschen: Der Angreifer täuscht den Betreiber oder Benutzer eines RFID-Systems, indem er unzutreffende Informationen einspeist.
3. Denial of Service (DoS): Die Verfügbarkeit von Funktionen des RFID-Systems wird beeinträchtigt.
4. Schutz der Privatsphäre: Der Angreifer sieht seine Privatsphäre durch das RFID-System bedroht und schützt diese durch einen Angriff auf das System.

Die Zwecke sind nicht scharf gegeneinander abgrenzbar. Beispielsweise kann ein Angreifer durch Ausspähen Tag-IDs ermitteln, um sie später in Täuschungsabsicht zu verwenden. Die oben eingeführten Angriffsarten lassen sich nun ihrem (primären) Zweck zuordnen (siehe Tabelle 7-1).

Es ist zu beachten, dass es in einem typischen Verwendungskontext von RFID-Systemen zwei Parteien mit unterschiedlichen Interessen gibt [HMM 04]. Auf der einen Seite steht der Betreiber des RFID-Systems, im Folgenden aktive Partei genannt. Die aktive Partei hat die Daten des RFID-Systems und ihre Verwendung unter Kontrolle. Sie ist es auch, die die Tags ausgibt und die mit ihnen assoziierten Daten verwaltet. Auf der anderen Seite steht als passive Partei der aktuelle Träger eines Tags bzw. eines gekennzeichneten Objekts. Dies ist in der Regel ein Kunde oder Angestellter des Betreibers. Die passive Partei ist zwar im Besitz von Tags, hat aber in der Regel keinen Einfluss auf deren Verwendung [HMM 04].

Der Betreiber hat ein Interesse an der korrekten Funktion des RFID-Systems. Die Interessen der passiven Partei decken sich damit nur insoweit, als die Vorteile, die das System für sie bietet, die erwarteten Nachteile überwiegen. Insbesondere Verbraucherorganisationen befürchten heute, dass RFID-Systeme eine zusätzliche Bedrohung der Privatsphäre mit sich bringen. Einige der erwähnten Angriffsarten wie das Abhören der Luftschnittstelle tragen zu diesem Bedrohungspotenzial bei, andere können dagegen zum Schutz der Privatsphäre beitragen und die Einflussmöglichkeiten der passiven Partei stärken. Letzteres gilt z. B. für die Verwendung von Blocker-Tags. Eine Analyse der Interessenlagen der an RFID-System beteiligten Parteien sowie möglichen Drittparteien bildet einen notwendigen Kontext für Sicherheitsstrategien, kann aber in dieser Studie nicht geleistet werden.

Aktive und passive Partei: Die Interessen der Betreiber eines RFID-Systems sind mit den Interessen ihrer Kunden oder Angestellten nicht deckungsgleich.

Henrici, Müller und Müller [HMM 04] haben ein RFID-Framework vorgeschlagen, das ohne „destruktive“ Elemente wie Blocker-Tags auskommt und nach Ansicht der Autoren ausreichenden Schutz für die Privatsphäre bietet.

	Ausspähen	Täuschen	Denial of Service	Schutz der Privatsphäre
Inhalt fälschen		■		
Identität fälschen (Tag)		■		
Deaktivieren		■	■	■
Ablösen		■		■
Abhören	■			
Blocken		■	■	■
Stören		■	■	■
Identität fälschen (Leser)	■			

Tabelle 7-1: Angriffsarten und ihre möglichen Zwecke

7.4. Exkurs: Angriff auf das Backend

Datenhaltung im Backend: Für die meisten Anwendungen genügt es, nur ID-Nummern auf den Tags zu speichern. Die damit assoziierten Daten werden in Datenbanken im so genannten Backend des RFID-Systems verwaltet.

Ein RFID-System ist darauf angewiesen, dass die vom Lesegerät erfassten Daten über weitere Kommunikationskanäle mit anderen Datenbeständen verknüpft werden. Die Sicherheitsaspekte in diesem so genannten Backend des RFID-Systems sind nicht spezifisch für RFID und gehören deshalb nicht zum Kernthema dieser Studie. Dennoch soll an dieser Stelle zumindest ein Überblick über denkbare Angriffe auf das Backend gegeben werden, zumal nicht auszuschließen ist, dass hier in der Summe größere Sicherheitsrisiken bestehen als im Frontend-Bereich.

Abbildung 7-2 zeigt eine mögliche Architektur für die Backend-Verarbeitung in einem RFID-System (angelehnt an das Konzept von EPCglobal, vgl. [EPC 04]). Das Lesegerät ist in ein Netzwerk auf Grundlage der Savant-Software eingebunden und nutzt einen zentralen Object Name Service (ONS). Der Savant-Computer sendet jede gelesene Seriennummer an den ONS-Server und bekommt jeweils die Adresse eines Servers zurück, der die damit assoziierten Daten verwaltet (PML Server). Als Format für diese Daten wird die Physical Markup Language (PML) verwendet.

Alle Intranet- und Internet-Verbindungen sind grundsätzlich dem Risiko des Abhörens ausgesetzt. Alle mit dem Internet verbundenen Computer sind grundsätzlich durch Intrusion (Hacking und Cracking) und das Einbringen von Software-Anomalien (vor allem Viren und Würmer) bedroht. Dies kann auch dazu führen, dass die Identität eines Lesegeräts mit autorisiertem Zugang zum Backend gefälscht wird. Wie bereits erwähnt, sind dies jedoch keine für RFID spezifischen Sicherheitsprobleme und werden deshalb hier nicht näher behandelt. Angriffe auf das Backend können mit den üblichen IT-Sicherheitsverfahren abgewehrt werden. Diese lassen sich leichter neuen Erfordernissen anpassen als auf den Tags implementierte Sicherheitsverfahren.

Es ist allerdings zu bedenken, dass durch RFID-Systeme erstmals größere Teilbereiche der physischen Welt zeitnah in der virtuellen

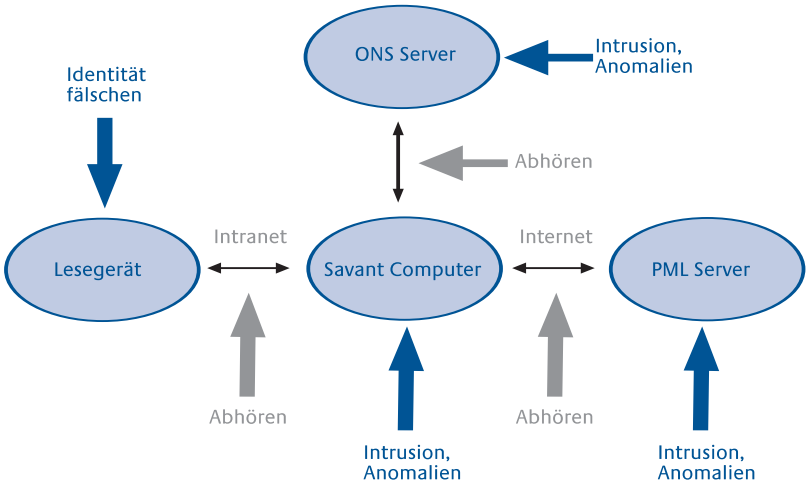


Abbildung 7-2: Exemplarische Architektur des Backends von RFID-Systemen und relevante Angriffsarten

Welt abgebildet werden. Es werden Datenbestände aufgebaut, aus denen insbesondere Bewegungsprofile von Objekten und daraus ableitbare Informationen extrahiert werden können, die früher nicht in dieser Dichte zur Verfügung standen. Dadurch könnte sowohl die Motivation von Angreifern als auch die potenzielle Schadenshöhe nach erfolgreichen Angriffen eine neue Größenordnung erreichen.

7.5. Bedrohungslage für die aktive Partei

Dieser Abschnitt stellt die Bedrohungslage aus der Perspektive der aktiven Partei dar, also derjenigen Partei, die das RFID-System betreibt.

Als Angreifer kommt grundsätzlich die passive Partei in Frage (Angestellte oder Kunden) oder eine Drittpartei (Konkurrenten, Wirtschaftsspione, Cyberterroristen).

7.5.1. Ausspähen von Daten

Ein Angreifer kann auf folgende Weise Daten ausspähen:

(a) Er kann mit einem eigenen Empfänger die Kommunikation zwischen Tags und Lesegeräten abhören. Die Entfernung kann dabei größer sein als die standardmäßig vorgesehene Lesedistanz (siehe Abschnitt 7.8.2.).

(b) Er kann mit einem eigenen Lesegerät Daten aus den Tags auslesen. Dieses kann er versteckt installieren oder auch mobil zum Einsatz bringen. Soweit eine Authentifizierung des Lesegeräts vorgesehen ist, muss der Angreifer in der Lage sein, die Identität des Lesegeräts zu fälschen.

7.5.2. Einspeisen falscher Daten (Täuschen)

Ein Angreifer kann in Täuschungsabsicht folgende Angriffe durchführen:

(c) Er kann den Inhalt, nicht aber die ID (Seriennummer) eines vorhandenen Tags verändern. Dies ist nur möglich, wenn mit der ID assoziierte Daten auf den Tags selbst (und nicht im Backend) gespeichert werden, was in den meisten Anwendungen nicht notwendig ist.

(d) Der Angreifer kann Tags emulieren oder duplizieren (Cloning), um gegenüber dem Leser deren Identität vorzutäuschen. Hierzu muss er zuvor mindestens die IDs (Seriennummern), je nach Sicherheitsverfahren auch Passwörter oder Schlüssel in Erfahrung gebracht haben.

(e) Er kann das Tag vom Trägerobjekt ablösen, um dessen Bewegungen vor dem Lesegerät zu verbergen oder ein anderes Objekt als das ursprüngliche Trägerobjekt auszugeben. Abhängig von den vorgesehenen mechanischen Sicherheitsmaßnahmen muss er dazu das Trägerobjekt beschädigen, was den Nutzen des Angriffs in vielen Fällen stark verringert.

7.5.3. Denial of Service

Ein Angreifer hat vielfältige Möglichkeiten, das korrekte Funktionieren eines RFID-Systems zu beeinträchtigen und so die mit diesen Systemen angestrebte Kongruenz zwischen realer und virtueller Welt zu unterminieren:

(f) Tags werden mechanisch oder chemisch zerstört (durch Knicken, Druck- oder Zugbelastung, Säureeinwirkung etc.).

(g) Tags werden durch elektromagnetische Feldeinwirkung zerstört, ähnlich dem regulären Verfahren zur Deaktivierung von 1-Bit-Transpondern (Diebstahlsicherung). Dies kann prinzipiell durch eigens dafür ausgelegte Sender, aber auch durch Mikrowellenherde oder durch starke Induktionsfunken erreicht werden.

(h) Tags werden durch Missbrauch von Lösch- oder Kill-Befehlen außer Betrieb gesetzt. Dies setzt voraus, dass der

Angreifer die Identität eines autorisierten Lese- bzw. Schreibgerätes vortäuschen kann.

(i) Die Batterie aktiver Tags wird durch eine Serie von Anfragen entladen. Bei passiven Tags ist dies nicht möglich, weil sie ihre Energie ausschließlich aus dem Versorgungsfeld des Lesers beziehen.

(j) Ein Blocker-Tag simuliert die Anwesenheit beliebig vieler Tags gegenüber dem Lesegerät, um die Erfassung der vorgesehenen Tags zu verhindern.

(k) Störsender verhindern die Kommunikation zwischen Erfassungsgerät und Tag. Um Wirkung auf größere Distanz zu erzielen, wären sehr starke Sender erforderlich. Dieser Angriff wäre leicht zu entdecken.

(l) Durch reflektierende Objekte wird eine Auslöschung des elektromagnetischen Feldes erreicht.

(m) Durch die Nähe von z. B. Wasser, Metall oder Ferrit wird eine Verstimmung der Feldfrequenz bewirkt.

(n) Die Tags werden durch metallische Folien oder mit Metallstreifen versehenen Taschen gegen elektromagnetische Felder abgeschirmt.

Bezüglich der praktischen Durchführbarkeit dieser Angriffe und der Wirksamkeit von Gegenmaßnahmen sind noch wenig Erfahrungen vorhanden. Einschätzungen von Experten sind in Abschnitt 7.8.2. zusammengestellt.

DATA PRIVACY: Daten, aus denen Aussagen über Personen abgeleitet werden können, müssen gegen unbefugten Zugriff geschützt sein.

Potenziell personenbezogene Daten: Durch Kombination von Daten können auch anonymisierte Daten mit guter Treffsicherheit einzelnen Personen zugeordnet werden.

7.6. Bedrohungslage für die passive Partei

Dieser Abschnitt stellt die Bedrohungslage aus der Perspektive der passiven Partei dar. Dies kann z. B. ein Kunde oder ein Arbeitnehmer des Betreibers sein. Die passive Partei benutzt Tags oder mit Tags gekennzeichnete Objekte, hat aber keine Kontrolle über die Daten, die auf den Tags gespeichert sind.

Die Diskussion über RFID-bedingte Risiken für die passive Partei ist bisher stark vom Thema Datenschutz bzw. Bedrohungen der Privatsphäre geprägt. Andere denkbare Nachteile – etwa eine Abwälzung technischer Risiken von der aktiven auf die passive Partei oder die zunehmende Bevormundung der Benutzer [vgl. Hilt 04] – werden dagegen kaum diskutiert. An dieser Stelle sei lediglich auf die Relevanz dieser Fragen hingewiesen. In Kapitel 10 werden diese Aspekte im Rahmen von fiktiven Fallbeispielen wieder aufgenommen.

Bedrohungen der Privatsphäre können von der aktiven Partei oder von Drittparteien ausgehen. Im ersten Fall ist offensichtlich kein Angriff auf das RFID-System erforderlich, denn die aktive Partei hat die volle Kontrolle über das System. Sie könnte beispielsweise gegen geltendes Datenschutzrecht verstoßen, indem sie sensible Daten ohne Wissen der betroffenen Personen weitergibt.

Im zweiten Fall führt eine Drittpartei einen Angriff auf das RFID-System aus, um sich unautorisierten Zugang zu Daten zu beschaffen. Die Konsequenzen für die passive Partei sind sehr ähnlich, da sensible Daten ohne Wissen und Zustimmung des Betroffenen in fremde Hände gelangen.

7.6.1. Bedrohung der Data Privacy

Wenn in einem RFID-System personenbezogene Daten gespeichert werden, so kann dadurch die Privatsphäre der passiven Partei bedroht sein. Für unsere Betrachtung seien nur die RFID-spezifischen Aspekte der Bedrohungslage erwähnt:

(a) Durch Abhören der Luftschnittstelle oder unautorisiertes Auslesen von Tags stehen einem potenziellen Angreifer neue Wege zur Verfügung, sich unberechtigt Zugang zu Daten zu verschaffen.

(b) Neben personenbezogenen Daten könnten zunehmend auch potenziell personenbezogene Daten zu einem Angriffsziel werden. Dies sind Daten, die zwar anonymisiert oder pseudo-

nymisiert sind, aber mit hoher Wahrscheinlichkeit deanonymisiert werden können, also rückwirkend plausible Rückschlüsse auf Einzelpersonen erlauben. Mit RFID nimmt die zeitliche und räumliche Dichte der von Personen hinterlassenen Datenspuren zu, was die Möglichkeiten zur Deanonymisierung aus rein statistischen Gründen verbessert.

(c) Die entstehende hohe Kongruenz zwischen virtueller und realer Welt — ein erklärtes Ziel des RFID-Einsatzes — kann bei der aktiven Partei oder bei einer Drittpartei (z. B. auch bei staatlichen Kontrollinstanzen) neue Bedürfnisse nach Auswertungen wecken, die möglicherweise nicht im Interesse der passiven Partei liegen. Mit der Verfügbarkeit der Daten erhöht sich das Risiko, dass die Datenbestände früher oder später ohne Wissen der Betroffenen zu nicht bestimmungsgemäßen Zwecken ausgewertet werden.

7.6.2. Bedrohung der Location Privacy

Unter der Annahme, dass Tags sich über längere Zeiträume im Besitz der gleichen Person befinden, können durch wiederholtes Auslesen der IDs (Seriennummern) Bewegungsprofile erstellt werden (Tracking). Diese Möglichkeit wird dann zu einer Bedrohung der Privatsphäre, wenn RFID-Systeme zu einem ubiquitären Bestandteil des Alltagslebens werden. Auch wenn beim Auslesen von RFID-Tags also ausschließlich IDs übertragen werden und alle anderen Daten ins Backend verlagert sind, kann davon eine Bedrohung der Privatsphäre ausgehen. Je mehr Tags im Verkehr sind, desto besser sind die Möglichkeiten des Trackings. Bei Verfolgung mehrerer Personen lassen sich auch Kontaktprofile erstellen.

Besonders spezifisch für RFID ist hier wiederum die Möglichkeit, die Luftschnittstelle abzuhören. Es ist jedoch nicht auszuschließen, dass von Angriffen im Backend-Bereich größere Bedrohungen für die Privatsphäre ausgehen als von der Luftschnittstelle. Im Vergleich zur Benutzung von Mobiltelefonen erzeugt die Benutzung von RFID-Tags wesentlich präzisere Datenspuren, da nicht nur der geographische Aufenthaltsort, sondern die konkrete Interaktion mit vorhandenen Betrieben und Infrastrukturen festgestellt werden kann.

Location Privacy: Daten, aus denen momentane oder frühere Aufenthaltsorte von Personen abgeleitet werden können, müssen gegen unbefugten Zugriff geschützt sein.

7.7. Sicherheitsmaßnahmen

7.7.1. Authentifizierung

Bei einer Authentifizierung wird die Identität einer Person oder eines Programms überprüft. Auf dieser Basis erfolgt dann die Autorisierung, also die Gewährung von Rechten, z. B. Zugriffsrechten auf Daten. Bei RFID-Systemen ist insbesondere die Authentifizierung von Tags durch das Lesegerät und umgekehrt von Bedeutung. Darüber hinaus müssen sich Lesegeräte auch gegenüber dem Backend authentifizieren, jedoch bestehen hier keine RFID-spezifischen Sicherheitsprobleme.

7.7.1.1. Prüfung der Identität des Tags

Das RFID-System muss beim Erfassen eines Tags dessen Identität überprüfen, um festzustellen, ob das Tag überhaupt zur Teilnahme an dem System berechtigt ist. Eine weltweit eindeutige Regelung zur Vergabe der ID-Nummern (Seriennummern) von Tags, wie es z. B. in Form des Electronic Product Code (EPC) vorgeschlagen wird, bietet einen gewissen Schutz vor gefälschten Tags. Zumindest kann das Auftauchen nicht vergebener Nummern oder von Duplikaten (Cloning) in manchen Anwendungsfällen erkannt werden.

Authentifizierung des Tags: Diese Maßnahme dient dazu, die Fälschung von Transpondern möglichst auszuschließen.

Darüber hinaus kann eine Authentifizierung durch Challenge-Response-Verfahren erfolgen, bei denen das Lesegerät an das Tag eine Zufallszahl oder einen Zeitstempel sendet (Challenge), die dieser verschlüsselt an den Leser zurücksendet (Response). Der dabei verwendete Schlüssel ist ein gemeinsam bekanntes Geheimnis, mit dem das Tag seine Identität beweist. Entscheidend an diesem Verfahren ist, dass der Schlüssel selbst nie übertragen wird und für jede Challenge eine

andere Zufallszahl verwendet wird, so dass durch Aufzeichnen und Wiedervorspielen der Kommunikation (Replay-Attacke) das Lesegerät nicht getäuscht werden kann. Dieses einseitige Authentifizierungsverfahren ist als „Symmetric-key two-pass unilateral authentication protocol“ in der ISO-Norm 9798 definiert.

Ein Angreifer müsste sich in Besitz des Schlüssels bringen, der sowohl auf dem Tag als auch im Backend des RFID-Systems gespeichert ist. Dazu wäre es nötig, die verschlüsselt übertragenen Response-Daten zu entschlüsseln, was je nach Schlüssellänge sehr aufwendig bis praktisch unmöglich ist. Der Schlüssel könnte grundsätzlich auch mit physikalischen Methoden aus den Speicherzellen des Chips ausgelesen werden, jedoch würde dies sehr aufwendige Labortechniken wie „Focused Ion Beam“ (FIB) erfordern. Dabei werden mit einem Ionenstrahl schrittweise sehr dünne Schichten (wenige Atomlagen) abgetragen, um den Inhalt mikroskopisch zu analysieren.

Ein Challenge-Response-Verfahren kann auch zur *gegenseitigen* Authentifizierung von Leser und Tag verwendet werden, wobei das Tag dann zusätzlich in der Lage sein muss, Zufallszahlen zu generieren (siehe Abschnitt 7.7.1.3.).

7.7.1.2. Prüfung der Identität des Lesegeräts

Authentifizierung des Lesegeräts: Diese Maßnahme dient dazu, das Auslesen der Transponder durch nicht zum RFID-System gehörende Lesegeräte möglichst auszuschließen.

Die einfachste Möglichkeit der Authentifizierung des Lesegeräts gegenüber dem Tag ist der Passwortschutz. Das Lesegerät identifiziert sich beim Tag durch Übertragung des Passworts. Der Transponder vergleicht es mit dem im Speicher abgelegten Passwort. Stimmen beide überein, gewährt das Tag vollen Zugriff auf die gespeicherten Daten. Einige Produkte gewähren Passwortschutz für ausgewählte Speicherbereiche.

Bei einfachen Systemen enthalten alle Tags das gleiche Passwort in einem geschützten Bereich ihres Speichers. Für aufwendigere Read-only-Systeme wird jedem Transponder vom Hersteller ein individuelles Passwort zugeordnet und mittels Laser in dessen Speicher abgelegt. Variable Passwörter können höheren Schutz gewähren, setzen aber Read-write-Transponder voraus. Typische Passwortlängen sind 8, 24 oder 32 Bit.

Passwortsysteme ohne Verschlüsselung gelten als schwache Identifikationsmethode, da ein Abhören der Passwortübertragung über die unsichere Luftschnittstelle möglich ist. Zudem lassen sich kurze Passwörter schon durch systematisches Ausprobieren ermitteln.

Passwortsysteme ohne Verschlüsselung können in jenen Fällen adäquat sein, in denen das Tag nur ein einziges Mal angesprochen werden soll oder die Gefahr des Ausspähens von Passwörtern ohnehin gering ist. Falls nur eine begrenzte Zahl von Zugriffen erforderlich ist, kann statt eines Passworts auch eine Liste von Einmalpasswörtern verwendet werden, die im Transponder und im Backend gespeichert ist.

Im Gegensatz zu kryptografischen Verfahren stellen solche Passwortsysteme nur geringe Anforderungen an die Tags und sind bereits mit einfachen Read-only-Tags zu realisieren.

Höhere Sicherheit gegen unautorisiertes Auslesen wird durch das Hash-Lock-Verfahren erreicht. Dazu wird vor dem erstmaligen Beschreiben eines Tags mithilfe einer Hash-Funktion, deren Berechnung praktisch nicht umkehrbar ist, aus einem Schlüssel eine so genannte Meta-ID als Pseudonym für das Tag erzeugt und im Tag gespeichert. Das Tag ist von diesem Zeitpunkt an gesperrt (locked), d. h., es reagiert auf die Signale eines Lesegeräts ausschließlich mit dem Senden der Meta-ID. Um das Tag zu entsperren, muss das Lesegerät in einer Backend-Datenbank den zur Meta-ID gehörenden Schlüssel abrufen und zum Tag übertragen. Das Tag wendet die Hash-Funktion auf den empfangenen Schlüssel an und überprüft, ob das Ergebnis mit seiner Meta-ID identisch ist. Ist dies der Fall, ist das Lesegerät authentifiziert und das Tag gibt den Zugriff auf seine Daten frei.

Das Zurückrechnen auf den ursprünglichen Schlüssel wäre für einen Angreifer mit erheblichem Aufwand verbunden. Eine Meta-ID reicht daher als Schutz vor unautorisiertem Auslesen bei vielen praktischen Einsatzgebieten aus. Allerdings kann der zu einer Meta-ID gehörige geheime Schlüssel bei der Übertragung durch die Luftschnittstelle von einem Angreifer ausgespäht werden, der dem Tag damit später ein autorisiertes Lesegerät vortäuschen kann (Replay-Attacke). Das Hash-Verfahren kann auf Transpondern auch ohne Einsatz aufwendiger Kryptoprozessoren implementiert werden [Weis 03], so dass dieses Verfahren auch für niedrigpreisige Transponder in Frage kommt.

Höchsten Schutz vor unautorisiertem Zugriff auf die Tags bieten Authentifizierungsverfahren mit Verschlüsselung nach dem bereits erwähnten Challenge-Response-Prinzip (starke kryptografische Verfahren). Diese setzen jedoch voraus, dass das Tag nicht nur kryptografische Algorithmen ausführen, sondern auch Zufallszahlen generieren kann. Bei Tags, die diese Voraussetzungen erfüllen und somit die Berechtigung des Lesegeräts auf hohem Sicherheitsniveau prüfen können, lohnt es sich nicht, beim umgekehrten Problem (Authentifizierung des Tags gegenüber dem Lesegerät) Kompromisse zu schließen, denn die Verarbeitungskapazität im Lesegerät bzw. im Backend stellt keinen Engpass dar. Somit sind bei leistungsfähigeren Transpondern starke gegenseitige Authentifizierungsverfahren angemessen (siehe Abschnitt 7.7.1.3.).

7.7.1.3. Starke gegenseitige Authentifizierung

Die ISO-Norm 9798 definiert verschiedene Challenge-Response-Verfahren für die starke Authentifizierung bei kontaktbehafteten Chipkarten und RFID-Systemen, darunter auch die gegenseitige Authentifizierung nach dem „Three-pass mutual authentication protocol“.

Auf ein „get challenge“ Kommando des Lesegeräts hin generiert das angesprochene Tag eine Zufallszahl A und sendet diese an

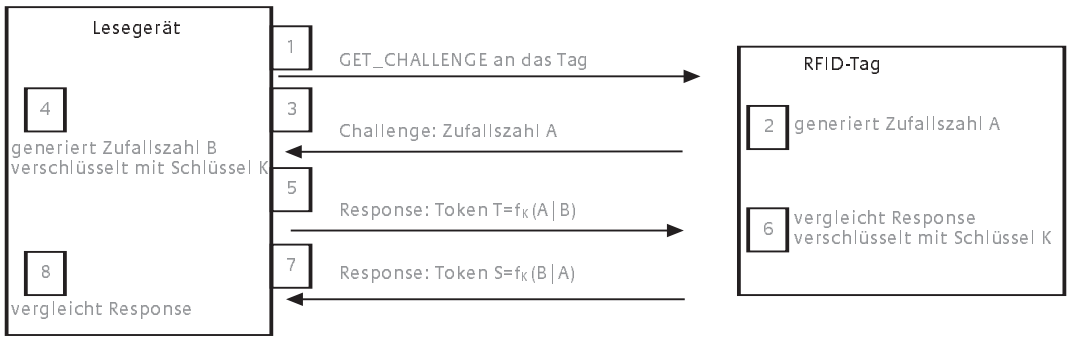


Abbildung 7-3: Challenge-Response-Verfahren zur gegenseitigen Authentifizierung nach [FrSt 2004]

das Lesegerät. Das Lesegerät generiert ebenfalls eine Zufallszahl B und erzeugt mit dieser und der Zufallszahl A auf Basis eines Verschlüsselungsalgorithmus und eines geheimen Schlüssels K einen verschlüsselten Datenblock (Token T). Dieser wird an das Tag zurückgesendet. Da beide Seiten den gleichen Verschlüsselungsalgorithmus verwenden und der Schlüssel K auf dem Tag gespeichert ist, kann das Tag den Token T entschlüsseln. Stimmen die ursprüngliche und die nun entschlüsselte Zufallszahl A und A' überein, ist die Authentizität des Lesegeräts bewiesen. Die Prozedur wird nun zur Authentifizierung des Tags gegenüber dem Lesegerät wiederholt, indem im Tag ein zweites Token S erzeugt und an das Lesegerät übertragen wird. Bei Übereinstimmung der entschlüsselten Zufallszahlen B und B' ist auch die Authentizität des Tags gegenüber dem Lesegerät bewiesen.

Da bei diesem Verfahren niemals geheime Schlüssel, sondern nur verschlüsselte Zufallszahlen über die unsichere Luftschnittstelle übertragen werden, ist ein hoher Grad an Sicherheit gegenüber unautorisiertem Zugriff gegeben. Auch durch Aufzeichnen und späteres Wiedervorspielen der Initialisierungssequenz (Replay-Attacke) kann kein Zugriff auf das Tag oder das Lesegerät erlangt werden.

Replay-Attacke: Durch das Aufzeichnen und Wiedereinspielen der Kommunikation zwischen Lesegerät und Tag könnten Sicherheitsschranken umgangen werden. Challenge-Response-Verfahren können dies verhindern.

Neben den hier vorgestellten Authentifizierungsverfahren auf Basis symmetrischer Kryptografie sind auch Verfahren basierend auf asymmetrischer Kryptografie für den Einsatz innerhalb von RFID-Systemen denkbar.

7.7.2. Verschlüsselung

Ein Mittel gegen das Abhören der Kommunikation über die Luftschnittstelle ist die Verschlüsselung der übertragenen Daten. Die Verschlüsselung ist eng mit der Authentifizierung verknüpft. Wenn ein Transponder für starke kryptografische Verfahren ausgelegt ist, so können sowohl eine starke gegenseitige Authentifizierung als auch eine sichere Verschlüsselung der nachfolgend übertragenen Daten realisiert werden. Insbesondere kann die oben beschriebene Three-Pass-Authentifizierung genutzt werden, um aus den Zufallszahlen der Initialisierungssequenz einen gemeinsamen temporären Schlüssel (Session Key) für die Verschlüsselung der danach zu übertragenden Daten zu erzeugen.

Wenn dagegen der Transponder keine starken kryptografischen Verfahren unterstützt, ist nur eine schwache Authentifizierung möglich. Eine sichere Verschlüsselung der nachfolgend übertragenen Daten ist dann aus den gleichen Gründen ebenfalls nicht möglich.

Die wirkungsvollste Maßnahme gegen einen Lauschangriff auf die Luftschnittstelle besteht jedoch darin, keine Inhalte auf dem Tag selbst zu speichern und lediglich die ID des Tags auszulesen. Die damit assoziierten Daten werden aus einer Backend-Datenbank abgerufen. Diese in der Fachliteratur meistens empfohlene und von EPCglobal vorgesehene Maßnahme [EPC 04] hat die zusätzlichen Vorteile, dass kostengünstigere Tags benutzt werden können, der Speicherplatz für die assoziierten Daten im Backend praktisch unbegrenzt ist und die üblichen Verfahren zum Datenmanagement und zur IT-Sicherheit eingesetzt werden können.

Das Problem, die Luftschnittstelle gegen unbefugtes Abhören zu sichern, beschränkt sich dann auf den Authentifizierungsvorgang und das Übertragen der ID-Nummer. Ersteres ist durch die Authentifizierungsverfahren zu lösen (siehe Abschnitt 7.7.1.), und das Abhören der ID ist in vielen Anwendungen keine Bedrohung, z. B. in einem Produktionsprozess. Bei flächendeckenden Anwendungen kann dies aber die Location Privacy der Träger getaggter Objekte gefährden und damit Datenschutzprobleme aufwerfen. In diesem Fall bieten sich Gegenmaßnahmen wie abhörsichere Antikollisionsprotokolle und die Pseudonymisierung der Tags an (siehe nachfolgende Abschnitte).

Für Anwendungen, bei denen relevante Inhalte auf den Tags selbst gespeichert werden müssen, bieten nur starke Verschlüsselungsverfahren einen sicheren Schutz gegen das Abhören.

7.7.3. Abhörsichere Antikollisionsprotokolle

Bei Antikollisionsprotokollen, die auf dem Absuchen eines Binärbaumes (Tree Walking) basieren (siehe Abschnitt 5.2.4.), kann auch aus größerer Distanz aus den Signalen des Lesegeräts auf die ID-Nummern der Tags zurückgeschlossen werden [LLS 00]. Aus diesem Grund wurden Alternativen zum Tree-Walking-Verfahren vorgeschlagen, die das Extrahieren von ID-Nummern durch Abhören des Downlinks (Datenübertragung vom Lesegerät zum Tag) ausschließen.

Beide genannten Maßnahmen haben keinen Einfluss auf die Möglichkeiten, ID-Nummern durch Abhören des Uplinks (Datenübertragung vom Tag zum Lesegerät) zu ermitteln. Sie gewinnen ihren Nutzen dadurch, dass der Uplink aufgrund der geringen Sendeleistung des passiven Transponders und der Überlagerung mit den starken Signalen des Lesegeräts in der Regel nur auf kürzere Distanz abgehört werden kann als der Downlink. Diese Einschätzung wird allerdings durch neuere Untersuchungen des BSI zumindest für induktiv gekoppelte Transponder im 13,56-MHz-Bereich in Frage gestellt [FiKe 04].

7.7.3.1. Silent Tree-Walking

Diese Modifikation des Tree-Walking-Verfahrens wurde von Weis et al. vorgeschlagen [WSRE 03]. Anstatt die nächste Verzweigung im Binärbaum aktiv im Klartext „auszurufen“, sendet das Lesegerät lediglich die Aufforderung zum Senden des jeweils nächsten Bits ihrer ID-Nummer an die Tags im Lesefeld. Das Lesegerät fragt die Bereiche übereinstimmender Bitfolgen aller Tags in absteigender Reihenfolge ab, bis an einer Stelle i eine Kollision auftritt. Bei i verzweigt das Lesegerät die Abfrage der Teilbäume mittels SELECT-Befehl. Im Gegensatz zum normalen Tree-Walking wird nun nicht der gesamte schon bekannte Abschnitt des Adressraums gesendet, sondern ein XOR-Wert aus dem aktuellen Bit an der Stelle i mit dem vorhergehenden Bit. Die Tags bilden ihrerseits mit diesem Wert und ihrem Bit einen XOR-Wert und vergleichen das Ergebnis mit der nächsten Stelle ihrer ID-Nummer. Bei Übereinstimmung sind sie selektiert und senden das nächste Bit. Ein Angreifer aus der Ferne, der lediglich den Downlink vom Lesegerät zum Tag belauschen kann, erfährt die ID-Nummer nicht vollständig. Jene Bereiche der ID-Nummern, an denen keine Kollision auftritt, bleiben ihm verborgen, so dass er weder den selektierten Teilbaum ermitteln noch die vom Lesegerät gesendeten Bitwerte durch Umkehr der XOR-Funktion ermitteln kann.

Dieses Verfahren ist im Gegensatz zum normalen Tree-Walking mit Read-only-Tags nicht realisierbar, da ein dynamischer Speicher benötigt wird. Dies verteuert das Silent Tree-Walking im Vergleich zum einfachen Tree-Walking-Verfahren.

7.7.3.2. Aloha-Verfahren mit temporären IDs

In der Spezifikation des Auto-ID Centers für Class-0-Tags ist als Alternative zum Tree-Walking ein Verfahren angelegt, bei dem die ID-Nummern der Tags nicht auf dem abhörbaren Vorwärtskanal (Downlink) gesendet werden [Auto 03]: Statt mit ihrer ID-Nummer identifizieren sich die Tags zunächst durch eine in jedem Lesezyklus neu generierte Zufallszahl, die als temporäre ID-Nummer dient. Das Lesegerät verwendet diese, um ein erkanntes Tag individuell stumm zu schalten. Nach Erkennung aller Tags im Lesefeld werden deren wahre ID-Nummern durch Senden der temporären ID abgefragt. Bei diesem Verfahren kann ein Angreifer durch Abhören des Downlinks lediglich die zur temporären Identifikation benutzten Zufallszahlen in Erfahrung bringen. Voraussetzung für dieses Verfahren sind Tags, die über einen Zufalls-

zahlengenerator sowie eine Funktion zur Stummschaltung verfügen.

7.7.4. Pseudonymisierung

Durch Pseudonymisierung kann die Identität des Tags verschleiert werden, so dass nur autorisierte Leser die „wahre“ Identität des Tags ermitteln können. Das oben beschriebene Hash-Lock-Verfahren (siehe 7.7.1.2.) beruht auf der Vergabe von Pseudonymen (Meta-IDs). Da jedoch das Tag während seiner gesamten Lebensdauer die gleiche Meta-ID behält, bietet dieses Verfahren noch keinen Schutz gegen das Tracking von Tags. Das Hash-Lock-Verfahren kann also zur Data Privacy, nicht aber zur Location Privacy beitragen. Aus diesem Grund wurden verschiedene Erweiterungen des Hash-Lock-Verfahrens vorgeschlagen.

7.7.4.1. Randomized Hash-Lock

Dieses von Weis et al. [WSRE 03] vorgeschlagene Verfahren basiert auf der dynamischen Generierung einer neuen Meta-ID bei jedem Auslesevorgang. Zu diesem Zweck generiert das Tag bei jeder Aktivierung eine Zufallszahl r, die mit der wahren ID-Nummer des Tags gehasht wird. Die Zufallszahl und der Hash-Wert h werden vom Tag an das Lesegerät gesendet. Zur Berechnung der wahren ID-Nummer des Tags müssen dem Betreiber des Lesegeräts alle zur jeweiligen Applikation zugehörigen ID-Nummern bekannt sein. Das Lesegerät bzw. dessen Server generiert nun mit der vom Tag generierten Zufallszahl die Hash-Werte aller bekannten ID-Nummern, bis ein übereinstimmender Hash-Wert gefunden ist. Damit ist die ID-Nummer des Tags gefunden.

Dieses Verfahren ist bei einer sehr großen Zahl von Tags kaum praktikabel. Trotz dieser Einschränkungen ist es für den RFID-Einsatz interessant, da es mit geringen Kosten implementierbar ist. Allerdings setzt es voraus, dass die Tags über einen Zufallszahlengenerator verfügen.

7.7.4.2. Chained Hashes

Ohkubo et al. [OSK 03] schlagen das Chained-Hash-Verfahren als kryptografisch robuste Alternative vor. Das Tag berechnet bei jeder Aktivierung mit zwei verschiedenen Hash-Funktionen eine neue Meta-ID. Die aktuelle Meta-ID wird zunächst einmal gehasht, um eine neue Meta-ID zu erzeugen, welche anschließend mit der zweiten Funktion erneut gehasht wird. Diese zweite Meta-ID wird an das Lesegerät übertragen. Zur Dechiffrierung muss dieses hashen, bis eine Übereinstimmung zur vom Tag übertragenen Meta-ID gefunden ist. Der Vorteil dieser Vorgehensweise ist die Unempfindlichkeit gegenüber einem wiederholten Ausspähen der Meta-ID während der Übertragung durch die Luftschnittstelle. Ein Angreifer könnte die ausgespähten Meta-IDs nicht zurückrechnen, wodurch die Anonymität aller vorausgehenden Datenbankeinträge (Logeinträge) des betreffenden Tags gewahrt bleibt.

7.7.4.3. Verfahren von Henrici und Müller

Henrici und Müller [HeMü 04] schlagen ein Verfahren vor, das eine gegenseitige Authentifizierung von Tag und Lesegerät, die Verschlüsselung der Kommunikation sowie die Sicherstellung der „Location Privacy“ ermöglicht. Daneben werden auf einem Tag keine Schlüssel oder andere verwertbare Daten längerfristig gespeichert, wodurch physikalische Angriffe auf die Chiphardware uninteressant werden. Das Verfahren kommt mit einem Minimum an Nachrichtenaustausch aus und ist zudem gegen Störungen auf dem Übertragungskanal (Luftschnittstelle) resistent.

Zur Sicherstellung der Location Privacy wird die Tag-Kennung (ID) regelmäßig geändert. Nach außen hin gibt das Tag nie die aktuelle ID, sondern lediglich deren Hash-Wert preis. Dieser wird vom Tag auf Basis von jeweils neuen, mit dem Backend des Lesegeräts synchronisierten Transaktionsnummern berechnet. Dadurch werden Angriffe wie Replay-Attacken verhindert und Nachrichtenverluste

erkannt. In der Backend-Datenbank werden pro Tag je zwei Eintragungen gespeichert, da der Fall berücksichtigt werden muss, dass die letzte Nachricht vom Backend an das Tag verloren geht. Die aufwendigere Datenhaltung und -synchronisation im Backend-Bereich stellt aber keine wesentliche Einschränkung dar, weil hier ausreichende Ressourcen vorhanden sind. Hingegen werden an die Hardware des Tags relativ geringe Anforderungen gestellt. Der Chip muss Hash-Werte berechnen können, ein Zufallszahlengenerator wird nicht benötigt.

Die Skalierbarkeit des Verfahrens macht es für den Masseneinsatz interessant. Die Implementierungskosten bei Massenproduktion liegen nach Einschätzung der Autoren des Verfahrens bei 0,5 Eurocent pro Tag. Damit ist es auch für Tags im Low-End-Bereich ökonomisch realisierbar.

7.7.5. Verhindern des Auslesens

RFID-Tags besitzen im Gegensatz zu den meisten anderen elektronischen Alltagsprodukten keinen Ein/Aus-Schalter. Sie sind also jederzeit von außen aktivierbar, ohne dass der Besitzer eine Aktivierung überhaupt feststellen kann.

Als Methode, das autorisierte oder unautorisierte Auslesen eines Tags vorübergehend zu verhindern, wurden die so genannten Blocker-Tags entwickelt [JRS 03].

7.7.5.1. Verwendung von Blocker-Tags

Ein Blocker-Tag ist ein Transponder oder ein Gerät höherer Funktionalität, das sich als Transponder ausgibt und gegenüber einem Lesegerät jede mögliche ID-Nummer vortäuscht. Durch sein ständiges Antworten auf jede Sendeaufforderung des Lesegeräts macht ein Blocker-Tag ein Scannen der gleichzeitig in seiner Umgebung befindlichen Tags unmöglich. Die tatsächlich vorhandenen Tags werden effektiv in einer großen Menge von virtuellen Tags (praktisch mehrere Billiarden Tags) versteckt. Juels et al. haben vorgeschlagen, Blocker-Tags mit zwei Antennen auszustatten, um jede Präfix-Singularisation gleichzeitig mit 0 und 1 zu beantworten. Ein derartiges Blocker-Tag kann Lesegeräte, die nach dem Binärbaum-Verfahren arbeiten, effektiv blockieren.

Damit Blocker-Tags in der Praxis nicht eine völlige Blockade aller RFID-Anwendungen verursachen, werden Verfahren vorgeschlagen, durch die Blocker-Tags nur bestimmte Teilräume des ID-Adressraums blockieren [JRS 03]. Damit lassen sich geschützte Adressbereiche festlegen, in denen ein Auslesen blockiert wird, ohne dass andere Anwendungen beeinträchtigt werden.

Die Verlässlichkeit von passiven Blocker-Tags ist als gering einzuschätzen. Da die Aktivierung des passiven Blocker-Tags über die Energie des elektromagnetischen Felds des zu blockenden Lesegeräts erfolgt, schränken die zufällige räumliche Orientierung, Abschirmungseffekte und die Distanz des Blocker-Tags zum Lesegerät die Zuverlässigkeit des Schutzes ein. Zudem kann sich der Nutzer nicht über die korrekte Funktion des Blocker-Tags vergewissern.

Ungewollte Störungen von erwünschten RFID-Anwendungen in der Nähe lassen sich nicht ausschließen und auch nicht direkt erkennen.

7.7.6. Dauerhafte Deaktivierung

Die dauerhafte Deaktivierung eines Transponders am Ende seiner Nutzungsphase ist die zuverlässigste Maßnahme, ihn vor späterem Missbrauch jeglicher Art zu schützen. Sie verhindert andererseits auch eine spätere Realisierung von Vorteilen durch RFID, im Falle von Smart Labels z. B. die Nutzung von Daten bei Umtausch, Reparatur, Weiterverkauf oder Recycling.

7.7.6.1. Kill-Befehl

Ein Kill-Befehl ermöglicht die Anonymisierung von Transpondern, indem ein Auslesen

Blocker-Tags: Sie überfordern das Lesegerät und verhindern so, dass andere Tags in der Nähe ausgelesen werden können.

des Tags dauerhaft unmöglich gemacht wird. Das schützt Träger von getaggten Gegenständen vor unbemerkter Identifikation und damit vor Tracking.

Kill-Befehl: Auch nach Ausführung der Kill-Funktion kann die ID-Nummer im Tag gespeichert bleiben.

Ein Kill-Befehl ist bereits in der 2002 publizierten Auto-ID-Spezifikation enthalten [Auto 02]. Die aktuelle EPCglobal-Spezifikation des Auto-ID-Centers definiert einen 8-Bit passwortgeschützten Kill-Befehl. Laut Spezifikation dürfen konforme Tags nach ihrer Deaktivierung mit dem passwortgeschützten Kill-Befehl nicht mehr auf Signale eines Lesegeräts reagieren [Auto 03].

Die bisher diskutierten Verfahren basieren auf einer softwaretechnischen Deaktivierung. Damit ist theoretisch ein späteres Reaktivieren des Tags möglich.

Der Kill-Befehl wird als Möglichkeit diskutiert, Smart Labels auf Konsumgütern am Point of Sale zu deaktivieren. Die Konsumenten können allerdings kaum überprüfen, ob die Labels tatsächlich dauerhaft deaktiviert sind. Da bisherige Kill-Verfahren lediglich die variablen Speicherzellen im Transponder, nicht aber die eindeutige ID-Nummer (EPC) löschen, bleibt die Wirksamkeit des Kill-Befehls aus Sicht des Datenschutzes fragwürdig. Zudem ist die Deaktivierung mittels Passwort wenig praktikabel, wenn Konsumenten die Tags nach dem Einkauf einzeln und manuell deaktivieren müssen.

7.7.6.2. Deaktivierung durch Feldeinwirkung

Eine elektromagnetische Deaktivierung der Hardware durch eine Sollbruchstelle, wie sie bei den bekannten Artikelsicherungen (1-Bit-Transpondern) eingesetzt wird, wäre ebenfalls denkbar, wird aber bisher nicht angeboten.

7.7.7. Umsetzung der Fairen Informationspraktiken in RFID-Protokollen

Faire Informationspraxis: Es soll erkennbar sein, wer wann für welchen Zweck Daten erhebt.

Ausgehend von den Prinzipien der „Fair Information Practices (FIP)“, auf denen u. a. die europäische Datenschutz-Direktive 95/46/EC aufbaut [EC 95], schlagen Flörkemeier et al. Maßnahmen vor, die Transparenz hinsichtlich der Betreiber des Lesegeräts und Verwendung der Daten schaffen sollen [FSL 04]. Unter der Annahme, dass heutige RFID-Protokolle vor allem hinsichtlich technischer Leistungskriterien und Kosten, nicht aber hinsichtlich des Schutzes der Privatsphäre optimiert wurden, zielen die Vorschläge auf einfach zu implementierende Modifikationen heutiger RFID-Protokolle ab. Grundprinzipien der FIP auf Zweckbestimmung, limitierte Nutzung, Transparenz und Verantwortbarkeit können durch relativ geringe Änderungen existierender RFID-Protokolle realisiert werden.

Dazu gehört, dass Anfragen des Lesegeräts nicht anonym bleiben, sondern mit der eindeutigen Kennung des Lesegeräts versehen werden. Bei Verletzung der Datenschutzprinzipien könnte der Betreiber des Lesegeräts dann identifiziert und zur Verantwortung gezogen werden. Außerdem sollte jeweils der Zweck der Datenerhebung, z. B. das Auslesen von Seriennummern zu Marketing-Zwecken, vom Lesegerät signalisiert werden. RFID-Transponder könnten so programmiert werden, dass sie nur auf Anfragen mit erwünschter Zweck-Deklaration, z. B. zur Bezahlung, mit ihren Seriennummern antworten.

Die zusätzlichen Informationen über den Betreiber des Lesegeräts und den Zweck der Datenerhebung könnten mit Hilfe eines speziellen Anzeigegeräts entschlüsselt und für den Besitzer der Tags sichtbar gemacht werden. Damit wird dem Benutzer der Tags zu einem gewissen Grad die Möglichkeit gegeben, die Funktion der Tags zu kontrollieren und die Verwendung der ausgelesenen Daten zu verstehen. Der Vorteil des Verfahrens ist der relativ geringe Zusatzaufwand zur Implementierung in bestehende RFID-Systeme. Die damit geschaffene Transparenz könnte dazu beitragen, das Vertrauen der passiven Partei zu erhalten oder wiederzugewinnen.

7.8. Einschätzung der Bedrohungslage und Diskussion der Sicherheitsmaßnahmen

7.8.1. Gesamteinschätzung

Die Experten wurden zunächst nach ihrer generellen Einschätzung zur Relevanz von Sicherheitsfragen bei RFID-Anwendungen befragt. Dabei kristallisierten sich die folgenden Punkte heraus:

- Zurzeit ist die Bedrohung durch Angriffe auf RFID-Systeme im Vergleich zu den technischen Schwierigkeiten ihres Betriebs in der Praxis sehr gering.
- Das Bedrohungspotenzial könnte durch Massenanwendung von RFID zunehmen, der flächendeckende Einsatz könnte Versuchungen zum Angriff auf die Systeme oder zu datenschutzrechtlich fragwürdigen Auswertungen wecken.
- Wo RFID-Systeme Auswirkungen auf die physische Sicherheit haben (Krankenhaus, wichtige Ersatzteile, Personenidentifikation) ist die IT- Sicherheit besonders wichtig.
- Die Privatsphäre ist insgesamt weniger durch Angriffe auf RFID-Systeme als durch den Normalbetrieb bedroht.
- Unterschiedliche Meinungen bestehen hinsichtlich der zusätzlichen Risiken von RFID für die Privatsphäre, von Null (alles schon mit bisherigen Systemen möglich) bis sehr hoch (Tracking durch RFID als neue Qualität der Überwachung).
- Sicherheitsmaßnahmen verteuern nicht nur die Fixkosten, sondern auch die variablen Kosten für RFID. Auch bei den Sicherheitsverfahren können nur hohe Stückzahlen die Kosten senken.

7.8.2. Einschätzung einzelner Angriffsarten und Diskussion der Gegenmaßnahmen

Die Ergebnisse der Experteneinschätzung sind in Tabelle 7-2 zusammengefasst und werden nachfolgend erläutert. Die aufgeführten Angriffe entsprechen den Angriffen (a) bis (n) aus Abschnitt 7.5. Wesentlich für eine Beurteilung der Gefahren, die mittel- bis langfristig von den Angriffen ausgehen, sind sowohl die Kosten, die der Angreifer aufwenden muss, als auch die Kosten für die Gegenmaßnahmen. Diese Kosten lassen sich nur qualitativ schätzen. Die Schätzungen in Tabelle 7-2 sind aus den technischen Voraussetzungen des jeweiligen Angriffs bzw. der Gegenmaßnahme abgeleitet. Gegenmaßnahmen, die auf dem Tag realisiert werden, sind bei der Produktion von Großserien häufig preiswert realisierbar. Als mittlere Kosten werden hier Zusatzkosten für Sicherheitsmaßnahmen bezeichnet, die in der gleichen Größenordnung wie die Kosten für das System ohne zusätzliche Sicherheit liegen. Als Gegenmaßnahmen mit hohen Kosten werden jene bezeichnet, die sich ohne einen Generationswechsel der Technologie praktisch nicht realisieren lassen.

Abhören der Kommunikation zwischen Tag und Erfassungsgerät

Das Abhören der Luftschnittstelle ist prinzipiell möglich. Das Risiko wächst mit der maximalen Lesedistanz des regulären Lesevorgangs. Bei Transpondern mit sehr kurzer Reichweite ist das Risiko gering.

Bei induktiv gekoppelten Systemen (unter 135 kHz, 13,56 MHz) kann der Downlink bis zu einigen zehn Metern abgehört werden, der Uplink aber nur wesentlich kürzer, etwa bis zum Fünffachen des maximal vorgesehenen Leseabstandes. Es handelt sich hier um theoretische Abschätzungen, die auf dem Verhältnis der Sendeleistungen von Lesegerät und Tag beruhen. Finke und Kelter haben experimentell gezeigt, dass das Abhören der Kommunikation von RFID-Karten nach ISO 14443 (13,56 MHz, Arbeitsbereich zehn bis 15 Zentimeter) bis mindestens zwei Meter Entfernung möglich ist [FiKe 04]. In dieser Untersuchung des BSI erwies sich der Unterschied in der Sendeleistung von Lesegerät und Tag für das Abhören als nicht wirklich gravierend. Weitere Untersuchungen zu den Möglichkeiten und Bedingungen des Abhö-

rens von induktiv gekoppelten Tags sind angezeigt.

Bei Backscatter-Systemen (868 MHz und 2,45 GHz) ist bei zwei Watt Leistung der Downlink bis max. 100 bis 200 Meter abhörbar, mit Richtantenne bis max. 500 bis 1.000 Meter. Die Entfernungen, aus denen der Uplink abgehört werden kann, sind um zwei bis drei Größenordnungen kürzer, liegen also im Bereich weniger Meter. Die geringe Genauigkeit der Angaben spiegelt den Mangel an gesichertem Wissen wider. Auch hier handelt es sich um theoretische Abschätzungen, die noch durch systematische Experimente zu validieren sind.

Generell stellt sich beim Abhören aus Distanz das Problem der räumlichen Zuordnung der Signale, da Signale aus verschiedenen Quellen sich überlagern. Das Mithören aus größerer Distanz wird dadurch zusätzlich erschwert.

Die Kosten für den Angreifer sind hoch, da in jedem Fall eine professionelle Ausrüstung und Know-how zur Dekodierung der Daten benötigt werden. Es ist zu bedenken, dass auch der Aufbau einer normal funktionierenden RFID-Systemkonfiguration in der Praxis nicht trivial ist, da die Zuverlässigkeit von einer Vielzahl von Einflussfaktoren abhängt (Reflexionen, Abschirmungen, Rauschabstand, häufige Störquellen). Ein Abhörangriff aus größerer Entfernung hätte noch wesentlich schlechtere Voraussetzungen, besonders bei hohen Bandbreiten wie 106 – 848 Kbit/s bei Systemen gemäß ISO 14443.

Gegenmaßnahmen:

- Verlagerung aller Daten bis auf die ID ins Backend, was auch aus Gründen des Datenmanagements empfehlenswert ist
- Abschirmen von Zonen, in denen Lesegeräte eingesetzt werden, gegen elektromagnetische Strahlung (Metallfolien-Tapete)
- Verschlüsselung der Datenübertragung

Die Kosten für Gegenmaßnahmen müssen unter normalen Bedingungen nicht hoch sein, um einen guten Schutz gegen das Abhören der Luftschnittstelle zu erreichen.

Unautorisiertes Auslesen der Daten
Dieser Angriff erfordert ein Erfassungsgerät, das unbemerkt (verdeckt) eingesetzt wird. Für die übliche Lesedistanz ist dies ohne allzu hohe Kosten möglich: Der Angreifer muss das Lesegerät erwerben und eventuell den Aufwand für einen unauffälligen Einbau treiben. Es werden bereits Softwareprodukte angepriesen, die auf mobilen Lesegeräten zum Einsatz kommen und z. B. in Supermärkten einfache Tags sowohl auslesen als auch beschreiben können [Klaß 04].

Die Möglichkeiten solcher Angriffe sind aufgrund der kurzen Reichweite eng begrenzt; in einem kontrollierten Umfeld können sie deshalb unterbunden werden. Die Spezialanfertigung von Lesegeräten mit höheren Reichweiten ist nur in engen physikalischen Grenzen möglich und mit hohen Kosten verbunden. Bei induktiv gekoppelten Systemen lässt sich die Reichweite unter hohem Aufwand etwa verdoppeln. Ein Meter gilt als sichere Obergrenze bei induktiver Kopplung.

Im UHF-Bereich ist die Sendeleistung gesetzlich auf zwei Watt begrenzt, was eine maximale Lesedistanz von drei bis fünf Metern ermöglicht. Für eine Reichweite von zehn Metern wären ca. 30 Watt Sendeleistung, für 20 Meter bereits 500 Watt Sendeleistung erforderlich. Dies sind Sendeleistungen im Bereich von Rundfunksendern, die für eine verdeckte Operation nicht praktikabel sind. Die Ausweitung der Lesedistanz wird auch dadurch erschwert, dass das schwache Signal des Tags durch das stärkere Signal des Lesegeräts mehr und mehr „überstrahlt“ wird. Viele RFID-Anwendungen werden schon aus funktionalen Gründen Tags mit sehr kurzer Lesedistanz vorsehen, etwa Chipkarten oder Banknoten.

Die Möglichkeiten zum verdeckten Auslesen passiver Transponder sind somit räumlich

eng begrenzt. Bei aktiven Transpondern ist die Situation völlig anders. Jedoch besteht meist keine Notwendigkeit, aktive Tags zur Identifikation einzusetzen (die typische Anwendung ist die Ortung von Objekten), so dass diese Anwendungen in der Regel nicht in die Kategorie RFID fallen.

Gegenmaßnahmen:

- Verlagerung der Daten in das Backend
- Detektoren, die das Versorgungsfeld eines Lesegeräts erkennen
- Authentifizierung: Zur Authentifizierung des Erfassungsgeräts gegenüber dem Tag sind verschiedene Verfahren denkbar (z. B. nach ISO 9798, siehe Abschnitt 7.7.1.).

Die Kosten der Gegenmaßnahmen können gering sein, wenn mit wenigen Detektoren der gewünschte Zweck erreicht wird. Als schwächere Variante ist auch eine stichprobenartige Suche nach Lesegeräten denkbar. Authentifizierung würde den Stückpreis der Tags dort spürbar erhöhen, wo sonst einfache Read-only-Tags genügen würden. Nach Expertenschätzungen ist zu erwarten, dass Tags mit Challenge-Response-Verfahren in der Massenproduktion um einen Faktor drei bis fünf teurer bleiben als die einfachsten Tags.
Laut Infineon soll dies dagegen zu einem Aufpreis von 20 Prozent möglich sein.

Unautorisiertes Verändern der Daten
Bei wieder beschreibbaren Tags sind die Möglichkeiten zum unautorisierten Verändern der Daten wie auch die Gegenmaßnah-

Angriff	Kosten	Gegenmaßnahmen	Kosten
Abhören der Kommunikation zwischen Tag und Lesegerät	hoch	Verlagerung ins Backend Abschirmung Verschlüsselung	mittel
Unautorisiertes Auslesen der Daten	mittel bis hoch	Detektoren Authentifizierung	mittel
Unautorisiertes Verändern der Daten	mittel bis hoch	Read-only-Tags Detektoren Authentifizierung	gering bis mittel
Cloning und Emulation	mittel	Erkennung von Duplikaten Authentifizierung	mittel
Ablösen des Tags vom Trägerobjekt	gering	Mechanische Verbindung Alarmfunktion (aktive Tags) Zusatzmerkmale	gering bis mittel
Mechanische oder chemische Zerstörung	gering	Mechanische Verbindung	gering bis mittel
Zerstörung durch Feldeinwirkung	mittel	selbst heilende Sicherung (nur begrenzt wirksam)	in Serie gering
Zerstörung durch Missbrauch eines Kill-Befehls	mittel	Authentifizierung	mittel
Entladen der Batterie (nur aktive Tags)	mittel	Schlafmodus	in Serie gering
Blocker-Tag	gering	Verbot in AGB (nur begrenzt wirksam)	gering
Störsender	mittel bis hoch	Messungen Frequenzsprungverfahren	mittel bis hoch
Feldauslöschung	gering (jedoch schwierig)	keine	-
Feldverstimmung	sehr gering	aktive Frequenznachführung	mittel bis hoch
Abschirmung	sehr gering	verbesserte Lesestationen (nur begrenzt wirksam)	mittel

Tabelle 7-2: Angriffe auf RFID-Systeme und Gegenmaßnahmen

men die gleichen wie im Fall des unautorisierten Auslesens (siehe oben).

Werden dagegen Read-only-Tags verwendet, ist das unautorisierte Verändern der Daten intrinsisch ausgeschlossen. Hier muss abgewogen werden gegen andere Sicherheitsnachteile der Read-only-Tags, die keine Verschlüsselung und bestenfalls eine schwache Authentifizierung (Passwort ohne Schutz gegen Replay-Attacken) ermöglichen.

Cloning und Emulation
Beim Cloning wird der Dateninhalt eines Tags ausgelesen oder auf andere Weise in Erfahrung gebracht, um damit ein neues Tag zu beschreiben. Dieses wird dann benutzt, um die Identität des Original-Tags vorzutäuschen.

Daneben ist der Einsatz von Geräten mit hoher Funktionalität denkbar, die benutzt werden, um bei gegebenem Dateninhalt beliebige Tags zu emulieren. Ein solcher Emulator könnte relativ klein sein (wenn auch größer als die Tags). Wenn die Möglichkeit besteht, den Emulator jeweils manuell in die Nähe des Erfassungsgeräts zu bringen, ist damit eine recht flexible Fälschungsmöglichkeit gegeben: Man entfernt ein Objekt aus einem Güterstrom, liest mit einem tragbaren Erfassungsgerät (das auch im Emulator integriert sein kann) dessen Tag ab und geht anschließend zum vorgesehenen Erfassungsgerät, wo man mithilfe des Emulators unauffällig vortäuscht, dass das Objekt diese Stelle passiert habe.

Ein dupliziertes Tag könnte man ähnlich benutzen, indem man beispielsweise aus einem „smart shelf“ einen Artikel entnimmt und das Duplikat an seinen Platz legt, so dass die intendierte Diebstahlsicherung nicht greift.

Weil das Cloning und Emulieren das Auslesen oder Abhören voraussetzt, sind die Gegenmaßnahmen die gleichen wie gegen diese Angriffe (siehe oben). Beide müssen verhindert werden, um Cloning und Emulation auszuschließen.

Eine zusätzliche Gegenmaßnahme können Plausibilitätschecks im Backend sein, die Duplikate erkennen (z. B. weil diese an verschiedenen Orten auftauchen).

Ablösen des Tags vom Trägerobjekt
Dieser Angriff erscheint trivial, ist aber gerade deshalb mit zu berücksichtigen. Jedes RFID-System ist davon abhängig, dass die Tags sich auf den dafür vorgesehenen Objekten befinden. Das „Umkleben“ von Tags (wie heute auch von Preisschildern) in Betrugsabsicht oder einfach nur in der Absicht, Verwirrung zu stiften, ist eine naheliegende Manipulation.

Die mechanische Manipulation ist an keine besonderen Voraussetzungen gebunden und verursacht daher eher geringe Kosten.

Gegenmaßnahmen:

- Eine enge mechanische Verbindung zwischen Tag und Trägerobjekt sorgt dafür, dass die Entfernung des Tags zur Beschädigung des Produkts führt (z. B. Einweben in Textilien, Eingießen in Kunststoffteile).
- Bei einigen Anwendungen können Tags so angebracht werden, dass sie schwer aufzufinden oder unzugänglich sind.
- Bei aktiven Tags ist auch eine Alarmfunktion denkbar: Ein Sensor stellt fest, dass der Transponder manipuliert wurde, speichert diese Information und sendet eine Alarmmeldung an ein Lesegerät, sobald dieses in Reichweite ist.
- Bei hochwertigen oder sicherheitsrelevanten Trägerobjekten kann durch Zusatzmerkmale auf dem Objekt (z. B. einen Barcode oder ein unauffälliges Zeichen) erreicht werden, damit bei Bedarf manuell überprüft werden kann, ob sich das Tag auf dem richtigen Objekt befindet. Die Zuordnung zwischen Zusatzmerkmalen und Tag-ID ist im Backend gespeichert.

Mechanische oder chemische Zerstörung
RFID-Tags können mechanisch oder chemisch beschädigt werden. Insbesondere die Antennen sind angreifbar.

Gegenmaßnahmen:

- Eine enge mechanische Verbindung zwischen Tag und Trägerobjekt kann auch dazu beitragen, dass eine Zerstörung des Tags ohne Beschädigung des Trägers schwierig ist.
- Bei einigen Anwendungen können Tags so angebracht werden, dass sie schwer aufzufinden oder unzugänglich sind.

Zerstörung durch Feldeinwirkung
Die Zerstörung durch Feldeinwirkung ist bei EAS-Tags zum Diebstahlschutz (1-Bit-Transponder) standardmäßig vorgesehen (Deaktivierung an der Kasse). Obwohl dies mit relativ einfachen Mitteln auch vom Kunden im Laden durchgeführt werden könnte, scheint es in der Praxis nicht vorzukommen.

Diese Art der Deaktivierung ist grundsätzlich bei allen induktiv gekoppelten Tags möglich, auch wenn keine Sollbruchstelle vorgesehen ist wie bei EAS. Normalerweise begrenzen Zenerdioden oder interne Stabilisatorschaltungen die Spannung, die in der Antenne induziert wird, auf die vorgesehene Betriebsspannung. Übersteigt die in der Spule induzierte Spannung jedoch die Belastungsgrenze der Spannungsstabilisierung, so kann es zur irreversiblen Zerstörung des Chips kommen. Gegen Überspannung gibt es nur begrenzten Schutz, da die Fähigkeit der Stabilisierungsschaltung zur Aufnahme überschüssiger Energie durch deren Fläche (Wärmeabfuhr) im Chip begrenzt ist. Im Allgemeinen ist eine Feldstärke von mindestens 12 A/m erforderlich.

Dieser Angriff ist wegen der hohen erforderlichen Feldstärke nur aus unmittelbarer Nähe möglich. Dies gilt auch für UHF-Tags.

Weil die Feldstärke mit der dritten Potenz der Entfernung abnimmt, wären für eine „Massenzerstörung“ von Tags auf Meterdistanz Sender mit sehr großer Antenne und Leistung (Rundfunksender) erforderlich. Dies ist für den Angreifer kaum praktikabel.

Mit einem Mikrowellenherd lassen sich Tags grundsätzlich zerstören, jedoch nicht zuverlässig. Wenn das Tag eng mit dem Trägerobjekt verbunden ist (und das ist ein nahe liegendes Motiv für die Zerstörung in der Mikrowelle), dann kann die starke Erhitzung des Tags evtl. das Produkt beschädigen.

Ferner besteht ein begründeter Verdacht, dass auch Funkeninduktoren und örtlich nahe gelegene Hochspannungs-Schaltvorgänge ausreichende Spannungsspitzen im Tag induzieren, um das Chip zu beschädigen. Diesbezügliche Untersuchungen werden derzeit an der EMPA durchgeführt.

Als Gegenmaßnahme gegen die Zerstörung durch Feldeinwirkung kommen selbst heilende Sicherungen in Frage. Diese sind bisher in den Normen nicht vorgesehen. Allerdings würde diese Maßnahme nichts an der Tatsache ändern, dass die Energieaufnahmekapazität für überschüssig induzierte Energie durch die Fläche begrenzt ist, über die die Wärme abgegeben werden kann. Einen absoluten Schutz gegen die Zerstörung durch Feldeinwirkung gibt es daher prinzipiell nicht.

Zerstörung durch Missbrauch eines Kill-Kommandos
Wenn Tags aus Gründen des Datenschutzes mit einer Kill-Funktion ausgestattet werden, die den Dateninhalt teilweise oder vollständig löscht, so kann diese missbraucht werden.

Eine Gegenmaßnahme ist die Authentifizierung für das Kill-Kommando (z. B. Passwortschutz). Es erfordert relativ aufwendige organisatorische Vorkehrungen, das Passwort an befugte Personen (z. B. den Käufer des Produkts, auf dem sich das Tag befindet) weiterzugeben, aber vor anderen geheim zu halten. Dieser Vorgang ist mit der Ausgabe einer Chipkarte mit PIN vergleichbar.

Entladen der Batterie (nur bei aktiven Tags)
Bei aktiven Tags, die über eine Stützbatterie verfügen, kann diese entladen werden, indem

das Tag durch eine rasche Abfolge von Anfragen zum häufigen Senden angeregt wird.

Als Gegenmaßnahme kommt ein „Schlafmodus“ in Frage, der nach einer erfolgten Interaktion eine Pause erzwingt. Die Zahl der pro Zeiteinheit möglichen Interaktionen wird dadurch begrenzt. Ähnliche Funktionen existieren bereits, um die Doppelauslesung zu verhindern.

Blocken
Die Benutzung von Blocker-Tags ist im Gegensatz zu Störsendern nicht gesetzlich verboten, weil es sich aufgrund der passiven Ausführung nicht um Sendeanlagen handelt. Ihr Gebrauch könnte jedoch in den Allgemeinen Geschäftsbedingungen (AGB), z. B. von Supermärkten, untersagt werden. Das Blocken in Betrugsabsicht würde dadurch allerdings nicht verhindert.

Ein Vorteil von Blocker-Tags ist grundsätzlich die Skalierbarkeit der Störreichweite und die Konfigurierbarkeit für bestimmte Adressräume; ein Schutz der Privatsphäre kann dadurch selektiv eingestellt werden. Jedoch ermöglichen gerade die individuellen Einstellungen das Verfolgen von Personen (Tracking), so dass das eigentliche Ziel, Location Privacy zu sichern, ad absurdum geführt wird.

Der am Markt erhältliche Blocker-Chip von RSA ist nur beim Tree-Walking-Antikollisionsverfahren wirksam. Gegen das Aloha-Protokoll lassen sich aber auch Blocker-Tags entwickeln. Grundsätzlich gibt es innerhalb eines gegebenen Protokolls keinen absoluten Schutz gegen Blocken. Da verschiedene Protokolle im Einsatz sind, muss der Benutzer des Blocker-Tags entweder mehrere solche mit sich führen, um alle in Frage kommenden Protokolle abzudecken, oder ein einziges (etwas größeres) Blocker-Gerät, das alle Protokolle beherrscht.

Einzige Gegenmaßnahme gegen Blocker-Tags ist das Verbot Ihrer Benutzung in den AGB, technische Gegenmaßnahmen gibt es nicht.

Störsender
Eine wirkungsvolle Störung des Betriebs auf Entfernung erfordert starke Sender. Der Betrieb solcher Störsender ist illegal, und sie sind für technisch nicht versierte Personen schwer zu beschaffen; Amateurfunker haben jedoch Zugang zu dieser Technologie.

Störungen aus der Nähe sind durch schwächere Sender oder auch durch Wechselwirkungen mit anderen elektronischen Geräten zwar möglich (Interferenzen, Protokollkollisionen), jedoch ist es schwierig, solche Effekte gezielt und zuverlässig einzusetzen.

Gegenmaßnahmen:

- Aufspüren von Störsendern durch stichprobenartige Messungen oder fest installierte Felddetektoren.
- Einführung eines Frequenzsprungverfahrens (wie bei Bluetooth) in zukünftigen RFID-Generationen. Mit dieser allerdings sehr weit reichenden Maßnahme wäre auch das zunehmende Problem der normalen Störquellen in den Griff zu bekommen.

Feldauslöschung
Im UHF-Bereich sind Auslöschungszonen eine normale Erscheinung, jedoch schwierig zu modellieren. Deshalb erscheint es unwahrscheinlich, dass es einem Angreifer gelingt, diesen Effekt z. B. durch Aufstellung von Reflektoren gezielt einzusetzen.

Generelle und präventiv wirkende Gegenmaßnahmen gibt es nicht. Sollte die gezielte Feldauslöschung doch zum Bestandteil von Angriffen werden, müssen auf den Einzelfall abgestimmte Gegenmaßnahmen gefunden werden.

Frequenzverstimmung
Dieser Angriff beruht darauf, relevante Mengen von z. B. Wasser, Metall oder Ferrit in die Nähe des Feldes bzw. der Tagantenne zu bringen. Eventuell genügt schon das Abdecken des Tags mit der Hand. Frequenzverstimmung ist aber weniger zuverlässig in

der Wirkung als die Abschirmung und nicht weniger auffällig.

Als Gegenmaßnahme ist grundsätzlich die aktive Frequenznachführung denkbar. Der technische Aufwand hierfür erscheint jedoch nicht angemessen, weil andere, einfacher durchzuführende Angriffe wie Abschirmung damit nicht verhindert werden. Darüber hinaus würden unter Umständen die hochfrequenztechnischen Zulassungsvoraussetzungen für solche Systeme verletzt werden.

Abschirmung
Abschirmung von Tags ist möglich, indem man sie in metallische Folie einwickelt (z. B. Alufolie) oder sie in alubeschichtete Gefrierbeutel oder mit Metallstreifen ausgestattete Handtaschen legt.

Als Gegenmaßnahme können bei induktiv gekoppelten Systemen verbesserte Lesestationen eingesetzt werden, die weniger empfindlich gegen Abschirmung sind. Insbesondere können mehrere Antennen in verschiedenen Winkeln die Abschirmung erschweren. Einen sicheren Schutz gegen Abschirmung gibt es nicht.

7.8.3. Einschätzung der Bedrohung für die Privatsphäre und Diskussion der Gegenmaßnahmen

Die Ergebnisse der Experteneinschätzung sind in Tabelle 7-3 zusammengefasst und werden nachfolgend erläutert. Bei divergierenden Expertenmeinungen werden im Text die verschiedenen Standpunkte dargestellt.

Bereits die generelle Relevanz von RFID für die Bedrohung der Privatsphäre bzw. den Datenschutz wird kontrovers eingeschätzt. Einige der von uns befragten Experten sehen keine solche Relevanz mit der Begründung, dass bereits ohne RFID durch Kreditkartenzahlungen, Mobiltelefonieren und Kundenkarten sehr viele Datenspuren erzeugt werden. RFID würde diesen bereits heute kaum genutzten Datenbeständen nichts Wesentliches hinzufügen.

Andere Experten sehen speziell in zukünftigen Möglichkeiten des Trackings von Personen eine RFID-spezifische Bedrohung der Privatsphäre, die als relevantes Risiko dieser Technologie einzustufen ist, besonders wenn die Tags in den Besitz des Konsumenten gelangen. Dieser wird in vielen Fällen zwischen Chancen und Risiken abwägen müssen, denn gerade die anspruchsvolleren und datenintensiven zukünftigen Anwendungen wie „Supply Chain Recording“ oder „Product Life Time Recording“ könnten ihm einen relevanten Nutzen bringen, etwa hinsichtlich der Transparenz der Lieferkette (Herkunft, soziale und ökologische Aspekte) sowie bei Leasing, Wartung, Reparatur, Wiederverkauf oder Recycling.

Abhören der Kommunikation zwischen Tag und Erfassungsgerät
Hier handelt es sich um einen Angriff, der die aktive und die passive Partei in gleicher Weise bedroht.

Die Gegenmaßnahmen sind deshalb im Kern identisch (vgl. Abschnitt 7.4.2):

- Verlagerung der Daten ins Backend
- Abschirmung
- Verschlüsselung der Datenübertragung

Diese Maßnahmen sollten jedoch so umgesetzt werden, dass die passive Partei zu den sie betreffenden Daten autorisierten Zugang hat. Anderenfalls würde durch Verlagerung der Daten ins Backend oder Verschlüsselung die Transparenz des Systems für die passive Partei geringer werden, was ihrem Bedürfnis nach Kontrolle über die eigenen Daten widerspricht.

Durch die Notwendigkeit, Zugriffsrechte zu verwalten, steigt der Aufwand für diese Sicherheitsmaßnahmen erheblich.

Als weitere Gegenmaßnahme kann der Selbstschutz der passiven Partei durch (legitime oder illegitime) Angriffe auf das RFID-System, wie sie in Abschnitt 7.3.2. beschrieben wurden, aufgefasst werden.

Kontroversen:
Die Kenntnisse von RFID für den Datenschutz werden von Fachleuten heute unterschiedlich beurteilt.

Bedrohung	Gegenmaßnahmen
Abhören der Kommunikation zwischen Tag und Lesegerät	Verlagerung ins Backend mit autorisiertem Zugriff durch passive Partei Abschirmung Verschlüsselung mit autorisiertem Zugriff durch passive Partei *Angriffe zum Selbstschutz (siehe Tabelle 7-2):* Ablösen des Tags Zerstörung des Tags Blocker-Tag Störsender Feldauslöschung Feldverstimmung Abschirmung
Unautorisiertes Auslesen der Daten	Detektoren im Besitz der passiven Partei Authentifizierung mit autorisiertem Zugriff durch passive Partei *Angriffe zum Selbstschutz (siehe Tabelle 7-2):* Ablösen des Tags Zerstörung des Tags Blocker-Tag Störsender Feldauslöschung Feldverstimmung Abschirmung des Tags
Tracking von Personen	Variable ID-Nummern *Angriffe zum Selbstschutz (siehe Tabelle 7-2):* Ablösen des Tags Zerstörung des Tags Blocker-Tag Störsender Feldauslöschung Feldverstimmung Abschirmung des Tags
Manipulation der Daten zum Nachteil der passiven Partei	Authentifizierung mit autorisiertem Zugriff durch passive Partei Erkennung von Duplikaten
Nicht bestimmungsgemäße Auswertung der Daten	Keine technischen Gegenmaßnahmen

Tabelle 7-3: Bedrohung der Privatsphäre durch RFID-Systeme und Gegenmaßnahmen

Unautorisiertes Auslesen der Daten
Auch hier handelt es sich um einen Angriff, der die aktive und die passive Partei in gleicher Weise bedroht.

Gegenmaßnahmen:

- Detektoren, die das Versorgungsfeld eines Lesegeräts anzeigen, können auch von der passiven Partei eingesetzt werden.
- Werden Authentifizierungsverfahren eingesetzt, sollte die passive Partei die Zugriffsrechte zu den sie betreffenden Daten erhalten. Anderenfalls würde durch Authentifizierungsverfahren die Transparenz des Systems für die passive Partei geringer werden, was ihrem Bedürfnis nach Kontrolle über die eigenen Daten widerspricht. Durch die Notwendigkeit, Zugriffsrechte zu verwalten, steigt der Aufwand für diese Sicherheitsmaßnahme erheblich.

Als weitere Gegenmaßnahme kann auch hier der Selbstschutz der passiven Partei durch (legitime oder illegitime) Angriffe auf das RFID-System, wie sie in Abschnitt 7.3.2. beschrieben wurden, aufgefasst werden.

Tracking von Personen
Die Gefahr des Trackings von Personen durch RFID wird kontrovers beurteilt.

Einigkeit besteht darin, dass Tracking durch verdeckte Lesevorgänge (Abhören, unautorisiertes Auslesen) eher unwahrscheinlich ist und eher reguläre Datenerfassungen die Grundlage für die Erstellung von Bewegungsprofilen bilden müssten. Dies wird unter anderem mit den technischen Schwierigkeiten des verdeckten Auslesens begründet (siehe Abschnitt 7.3.2.).

Kontrovers wird dagegen der Beitrag von RFID zum Risiko des Trackings von Personen beurteilt.

Auf der einen Seite wird argumentiert: Daten, die ein Tracking ermöglichen würden, werden heute schon erfasst (z. B. über Kundenkarten), aber nicht in diesem Sinne ausgewertet. Anwendungen von RFID, die dem Entscheidendes hinzufügen würden, sind weder geplant noch praktikabel. Insbesondere denkt kein Unternehmen heute daran, RFID-Daten außerhalb der Logistikkette zu erfassen. Hypothetische Anwendungen wie der Auto-Checkout im Supermarkt werden in den nächsten zehn Jahren nicht zum Masseneinsatz kommen. Die Kosten für die Tags (> 5 Eurocent) und technische Schwierigkeiten auf der physikalischen Ebene verhindern eine rentable Anwendung. Unternehmen werden auch nicht ihr Renommee und das Vertrauen der Kunden aufs Spiel setzen. Derzeitige Rationalisierungsbemühungen zielen ausschließlich auf die Optimierung der Lieferkette bis zum Verkaufsregal (smart shelf). Dabei ist nur bei hochwertigen Produkten der Einsatz von RFID-Labels auf dem Einzelprodukt zu erwarten, in den meisten Fällen stattdessen auf dem Liefergebinde (z. B. Palette). Daraus ergibt sich kein zusätzliches Risiko der Verfolgung von Personen anhand von Gütern. Selbst wenn man RFID-Daten zum Tracking verwenden wollte, wäre es sehr schwierig, daraus Bewegungsprofile abzuleiten, weil es sich um extrem fragmentierte Daten handelt. Der Aufwand zur Erstellung eines Gesamtbildes wäre enorm. Es besteht daran kein wirtschaftliches Interesse. Selbst die heute über Kundenkarten erfassten Daten werden meist zu Datenfriedhöfen, weil sich die Erstellung von Kundenprofilen nicht lohnt.

Auf der anderen Seite wird vorgebracht: Bei einem flächendeckenden Einsatz von RFID werden wesentlich mehr Vorgänge (wenn auch nicht jeder Kauf eines billigen Massenprodukts) digital erfasst, es entstehen mehr Datenspuren, die auch mehr Auswertungsmöglichkeiten zulassen. Dadurch werden neue „Begehrlichkeiten“ der Auswertung geweckt, z. B. bei staatlichen Stellen. Außerdem hat der Einzelhandel ein Interesse an Bewegungsprofilen der Kunden innerhalb der Verkaufsräume. Das verdeckte Auslesen von Daten wird zwar die Ausnahme sein, aber es kann auch nicht völlig ausgeschlossen

werden. Sind RFID-Tags bei der Entsorgung von Produkten nicht definitiv deaktiviert, ist es eventuell möglich, durch Auslesen der Tags aus dem Abfall auf den Verkaufsort, Verkaufszeitpunkt und auf den Käufer des Produkts zurückzuschließen. Eine besondere Eigenschaft von RFID im Vergleich zu anderen Identifikationssystemen ist, dass die sonst gegebene Anonymität der Abfallentsorgung potenziell eingeschränkt wird. Besonders heikel ist es ferner, biometrische Merkmale auf Transpondern zu speichern.

Eine mögliche Gegenmaßnahme ist die Verwendung variabler ID-Nummern, z. B. auf der Grundlage der erweiterten Hash-Lock-Verfahren (siehe Abschnitt 7.7.4.).

Manipulation der Daten zum Nachteil der passiven Partei

Nicht nur das unautorisierte Lesen, sondern jegliche Art der Manipulation der Daten durch Dritte kann für die passive Partei eine Bedrohung darstellen, zumal sie zunächst keine Überprüfungsmöglichkeiten hat.

Um den Zugriff durch Dritte generell zu verhindern, sind ausreichend sichere Authentifizierungsverfahren erforderlich. Zur Verhinderung von Manipulationen ist es besonders wichtig, dass die passive Partei selbst autorisierten Zugriff auf die sie betreffenden Daten hat, um deren Korrektheit überprüfen zu können.

Auch in diesem Fall kann als zusätzliche Gegenmaßnahme der Selbstschutz der passiven Partei durch (legitime oder illegitime) Angriffe auf das RFID-System, wie sie in Abschnitt 7.3.2 beschrieben wurden, aufgefasst werden.

7.9. Verfügbarkeit der Sicherheitsmaßnahmen

Tabelle 7-4 stellt die von den größeren Herstellern angebotenen Transponderprodukte zusammen. Für diese Tabelle wurden die Transponder auf der Basis von Datenblättern der Hersteller wie folgt klassifiziert:

Typ 1: Low-End
(ID-Label mit Zustandsautomat)
Typ 2: Systeme mittlerer Leistungsfähigkeit
Typ 3: High-End
(Smart Card mit Mikroprozessor)

Die Tabelle erhebt keinen Anspruch auf Vollständigkeit. Auch für Aktualität kann nicht garantiert werden, da sich der Markt rasch ändert.

Zum Zeitpunkt der Drucklegung dieser Studie scheinen keine Transponder mit Kill-Funktion und keine Transponder mittleren Typs mit der Fähigkeit, Hash-Funktionen ohne Kryptoprozessor zu berechnen, auf dem Markt zu sein.

Bezeichung	Standard	Typ	Benutzerspeicher	Frequenz	Passwort	Authentifizierung	Verschlüsselung
Atmel							
AT88SC0104CRF	ISO 14443 Type B	3	1 Kbit	13,56 MHz		•	•
AT88SC0204CRF	ISO 14443 Type B	3	2 Kbit	13,56 MHz		•	•
AT88SC0404CRF	ISO 14443 Type B	3	4 Kbit	13,56 MHz		•	•
AT88SC0808CRF	ISO 14443 Type B	3	8 Kbit	13,56 MHz		•	•
AT88SC1616CRF	ISO 14443 Type B	3	16 Kbit	13,56 MHz		•	•
AT88SC3216CRF	ISO 14443 Type B	3	32 Kbit	13,56 MHz		•	•
AT88SC6416CRF	ISO 14443 Type B	3	64 Kbit	13,56 MHz		•	•
AT88RF001	ISO 14443-2 Type B	2	256 bit	13,56 MHz	•		
AT88RF020	ISO 14443-2 Type B	2	2 Kbit	13,56 MHz	•		
T5552		2	992 bit	125 kHz			
T5557	ISO 11748 / 785	1	330 bit	125 kHz	•		
T5554		1	224 Kbit	125 kHz	•		
TK5561A-PP		2	128 Kbit	125 kHz		•	•
EM Microelectronic							
EM4469/4569	ISO 11785,11785	2	512 OTP Option	125 kHz	•		
EM4450/4550		1	1024 bit	125 kHz	•		
EM4055		1	1024 bit	125 kHz	•		
EM4056		1	2048 bit	125 kHz	•		
EM4170		2	256 bit	125 kHz		•	
EM4034	ISO 15693, 18000-3	1	448 bit	13,56 MHz	•		
EM4035	ISO 15693, 18000-3	2	3200 bit	13,56 MHz		•	•
EM4135	ISO 15693, 18000-3	1	2304 bit	13,56 MHz			
Infineon							
SLE 66CL160S	ISO7816+14443 A+B	3	16 Kbyte + 1,3k RAM	13,56 MHz			•
SLE 66CL80P	ISO7816+14443 A+B	3	8 Kbyte + 2,3k RAM	13,56 MHz			•
SLE 66CLX320	ISO7816+14443 A+B	3	32 Kbyte + 5k RAM	13,56 MHz			•
SRF 55V02P	ISO15693	3	256 byte + 32 byte Admin	13,56 MHz	•		
SRF 55V10P	ISO15693	3	1024 byte + 256 byte Admin	13,56 MHz	•		
SRF 55V02S	ISO15693	3	256 Byte + 64 Byte Admin	13,56 MHz		•	•
SRF 55V10S	ISO15693	3	1024 Byte + 256Byte Admin	13,56 MHz		•	•
SLE 55R01	ISO 14443 A	3	128 byte + 32Byte Admin.	13,56 MHz		•	•
SLE 55R04	ISO 14443 A	3	616 Byte + 154 Byte Admin	13,56 MHz		•	•
SLE 55R08	ISO 14443 A	3	1024 Byte + 256 Byte Admin.	13,56 MHz		•	•
SLE 55R16	ISO 14443 A	3	2048 Byte + 256 Byte Admin	13,56 MHz		•	•
SLE44R35T	ISO 14443 A	3	1024 Byte + 256 Byte Admin	13,56 MHz		•	
SLE44R35S	ISO 14443 A	3	1024 Byte + 256 Byte Admin	13,56 MHz		•	
Philips							
HT1DC20S30		2	2048 bits	125 kHz		•	•
HT2DC20S20	ISO 11785	2	256 bits	125 kHz	•	•	•
HT2MOA3S20	ISO 10536.1	2	256 bits	125 kHz	•	•	•
PCF793XAS		2	128 – 768 bits	125 kHz		•	
Mifare MFO IC U1X	ISO 14443 A	3	64 Byte	13,56 MHz		•	•
Mifare MF1 IC S50	ISO 14443 A	3	1024 Byte	13,56 MHz		•	•
Mifare MF1 IC S 70	ISO 14443 A	3	4096 Byte	13,56 MHz		•	•
Mifare MF3 IC D40	ISO 14443 A	3	4096 Byte	13,56 MHz		•	•
Mifare ProX P8RF6X	ISO7816 / 14443 A	3	4 – 16 KByte	13,56 MHz		•	•
SmartMX P5Sxxxx	ISO7816 / 14443	3	10 – 72 KByte	13,56 MHz		•	•
SmartMX P5Cxxx	ISO7816 / 14443	3	10 – 72 KByte	13,56 MHz		•	•
Texas Instruments							
RI-TH1-CB2A	ISO15693	3	2 Kbit	13,56 MHz			•
RI-TRP-B9WK-xx		2	88 bits	134.2 kHz	•		•
RI-TRP-V9WK		2	50 Byte	134.2 kHz		•	•
RI-TRP-BRHP-xx		2	88 bits	134.2 kHz	•	•	•
TMS37122	-	3	-	125 kHz			•

Tabelle 7-4: Verfügbarkeit der Sicherheitsfunktionen Passwortschutz, weitergehende Authentifizierung und Verschlüsselung bei RFID-Transpondern

8. Anwendungsgebiete von RFID-Systemen

8.1. Die Anwendungsgebiete im Überblick

Einsatzmöglichkeiten:
In ausgewählten Segmenten zeigen RFID-Systeme seit Jahrzehnten eine kontinuierliche Marktentwicklung.
Neue Anwendungen werden im Rahmen von zahlreichen Pilotprojekten erprobt.

Forciert durch technischen Fortschritt und die damit verbundenen Leistungssteigerungen sowie durch neue kostengünstigere Prozessorproduktionsverfahren beeinflusst RFID mittlerweile zahlreiche Anwendungsgebiete und schafft darüber hinaus die Grundlage für neue Anwendungen in der Zukunft. Einsatzmöglichkeiten von RFID-Systemen lassen sich nahezu in allen Wirtschaftssegmenten identifizieren und die Palette der diskutierten Anwendungsgebiete steigt beständig. Bislang scheiterte eine weit verbreitete Nutzung der Technologie an den relativ hohen Kosten der Implementierung. Hierzu zählen Kosten für die Hardwarebeschaffung, die zusätzlichen Softwarekomponenten und – oft vernachlässigt – die Aufwendungen einer organisatorischen Anpassung an neue bzw. veränderte Geschäftsprozesse. [Prog 04]

Aktuell werden RFID-Systeme im Einzelhandel intensiv diskutiert. Die Handelskonzerne Metro Group, Wal-Mart und Tesco zählen zu den Frühadoptoren und Protagonisten der fortgeschrittenen RFID-Technologie. Im Rahmen von Pilotprojekten werden insbesondere die Kostensenkungs- und Prozessoptimierungspotenziale von RFID-Systemen geprüft. Eine Studie von A.T. Kearney schätzt, dass Einzelhändler ihre Lagerkosten um bis zu fünf Prozent und ihre Personalkosten um bis zu zehn Prozent durch den Einsatz der RFID-Technologie senken können. Für den deutschen Einzelhandel entspricht dies einer Summe von etwa sechs Mrd. Euro pro Jahr. [ATKe 04] Neben dem Einzelhandel erhoffen sich aber zunehmend auch die Logistiker zur weiteren Automatisierung und Optimierung ihrer Geschäftsprozesse ökonomische Vorteile durch den Einsatz von RFID.

Vorliegende Marktdaten und Berichte zum Einsatz von RFID-Systemen sind häufig punktuell, beziehen sich auf einzelne volkswirtschaftliche Sektoren und Anwendungsgebiete und geben keinen umfassenden Marktüberblick. Es gibt keine aussagekräftigen amtlichen Statistiken, sondern ausschließlich Marktanalysen von verschiedenen Beratungsunternehmen. Die verwendeten Datengrundlagen, Erhebungsmethoden und Marktabgrenzungen sind sehr unterschiedlich, nicht immer transparent und daher nicht miteinander vergleichbar. Der Stand der Diffusion, der Umsätze und der Marktanteile von RFID-Systemen bleibt in der Folge national wie international unscharf. Im Laufe der letzten Jahre hat die RFID-Technologie erfolgreich Nischenmärkte besetzt. Ob sie zukünftig als Massentechnologie eingesetzt wird, hängt nicht zuletzt von den Erfolgen der laufenden Pilotprojekte von Pionieranwendern ab.

Die RFID-Technologie ist eine typische Querschnittstechnologie, deren Anwendungspotenziale in nahezu allen Lebens- und Wirtschaftsbereichen liegen. Grundsätzlich geht es bei ihrem Einsatz funktional immer um die Identifikation von Objekten. Branchen übergreifend können die folgenden Anwendungsgebiete unterschieden werden:

- Kennzeichnung von Objekten
- Echtheitsprüfung von Dokumenten
- Instandhaltung und Reparatur, Rückrufaktionen
- Diebstahlsicherung und Reduktion von Verlustmengen
- Zutritts- und Routenkontrollen
- Umweltmonitoring und Sensorik
- Supply-Chain-Management: Automatisierung, Steuerung und Prozessoptimierung

Im Folgenden wird auf Basis der vorangestellten Branchen übergreifenden Anwendungscluster der Status quo im Hinblick auf den Einsatz der RFID-Technologie aufgezeigt. Eine anwendungsbezogene Risiko- und Bedrohungsbetrachtung von RFID-Systemen wird hierbei nicht vorgenommen, da dies den Rahmen der vorliegenden Studie überschreiten würde. Die Durchführung einer solchen Betrachtung wäre Aufgabe der Betreiber der

jeweiligen Anwendungen. Als Basis für eine solche Betrachtung können die in Abschnitt 7 dargestellten Bedrohungspotenziale sowie die ebenfalls aufgeführten technischen Maßnahmen zur Bewältigung der möglichen Bedrohungen dienen.

8.2. Kennzeichnung von Objekten

Praxisrelevante Anwendungen der kontaktlosen RFID-Identifikationssysteme im Anwendungsgebiet „Kennzeichnung von Objekten" finden sich beispielsweise in den Bereichen Tieridentifikation, Behälteridentifikation und Abfallentsorgung. Aber auch die eindeutige Kennzeichnung von Waren und die Personenidentifikation zählen zu den relevanten Anwendungsgebieten der RFID-Technologie.

Elektronische Kennzeichnungssysteme in der Nutztierhaltung (z. B. Rind, Schaf, Schwein) werden bereits seit über 20 Jahren eingesetzt. Der mit den Identifikationsdaten ausgestattete Transponder wird am Tier angebracht oder in das Tier injiziert. Die erforderlichen internationalen Normen für die Tierkennzeichnung wurden im Oktober 1996 verabschiedet. Von der International Organization for Standardization (ISO) ist eine Vereinbarung hinsichtlich des Formates des Codes (ISO-Norm 11784) und der technischen Übertragung (ISO-Norm 11785) getroffen worden. Die weltweit einmalige Identifikationsnummer besteht aus einer 15-stelligen Zahl und gliedert sich in eine dreistellige Ländernummer und eine zwölfstellige nationale Tiernummer. [Texa 04] Für die Positionierung der Transponder am oder im Tier stehen heute drei Möglichkeiten zur Verfügung: das Transponderinjektat, der Bolus und die elektronische Ohrmarke. Bei dem Bolus handelt es sich um Keramik- oder Plastikzylinder, die einen Transponder enthalten und im Vormagentrakt von Wiederkäuern, dem Pansen, abgelegt werden. Um die so genannten Lebensmitteltiere elektronisch zu kennzeichnen, sind international gültige Injektionsorte für die schnelle Tieridentifikation und die sichere Transponder-Entfernung im Schlachthof Voraussetzung. Die Tiere werden in der Regel „auf der linken Seite" gekennzeichnet. Bei Wiederkäuern und Schweinen zählen die Knorpelverdickungen an den Ohrbasen zu den geeigneten, schmerzfreien Stellen. Bei Pferden ist die linke Halsseite in der Höhe des vierten Halswirbels üblich. [Idel 98] In der Nutztierhaltung werden passive RFID-Systeme eingesetzt. Nur beim Ablesevorgang der Identifikationsinformationen durch mobile oder stationäre Systeme wird der Chip durch die Radiowellen des Lesegeräts aktiviert (134,2 kHz). Batterien für die Transponder sind nicht erforderlich.

Die Nutzenpotenziale von RFID-basierten Tierkennzeichnungssystemen liegen in der schnellen, automatisierten und elektronischen Identifizierung von Tieren, in der betrugssicheren und eindeutigen Kennzeichnung von Tieren sowie in der betriebsübergreifenden lückenlosen Verfolgbarkeit der Tiere von der Geburt bis zur Schlachtung bzw. zum Verkauf des Fleisches. Dies ist insofern bedeutend, als das ein verlässlicher Nachweis über die Herkunft von Lebensmittelfleisch nach den Erfahrungen mit BSE (Bovine Spongiforme Enzephalopathie) und anderen Tierseuchen für die Verbraucherinnen und Verbraucher in Deutschland zu den zentralen Entscheidungskriterien für den Fleischkauf zählt. [Hand 04] Auch ist eine Verbindung der elektronisch erfassten Identifikationsmerkmale mit weiteren Bewegungs- und Gesundheitsdaten möglich (z. B. kann jedem Tier eine für die Aufzucht optimierte Futterration bereitgestellt werden). Hinzu kommt, dass die elektronische Kennzeichnung im Vergleich zu traditionellen Verfahren wie Tätowierung oder Brand weitaus tierfreundlicher ist sowie jederzeit die sofortige Verfügbarkeit der Daten sichergestellt werden kann. [Vere 04]

Die Europäische Kommission hat die elektronische Kennzeichnung von Tieren im Rahmen des Projektes „IDEA" (Electronic Identification of Animals) erprobt, das von März 1998 bis Dezember 2002 lief.

Nutztierhaltung: Elektronische Kennzeichnungssysteme in der Nutztierhaltung werden zu einem zunehmend wichtigen und weltweiten Markt für RFID-basierte Identifikationslösungen. Gesetzliche Vorschriften – z. B. zur Sicherstellung der Qualität und Herkunft von Fleischwaren – forcieren diese Entwicklung

Knapp eine Million Nutztiere wurden in den sechs EU-Staaten Deutschland, Frankreich, Italien, Niederlande, Portugal und Spanien mit einer elektronischen Ohrmarke, unter die Haut injizierten Chips oder einem Pansenbolus elektronisch gekennzeichnet, um die Durchführbarkeit der verschiedenen Markierungssysteme für Wiederkäuer (Rinder, Büffel, Schafe und Ziegen) zu untersuchen. Für einen Leistungsvergleich der einzelnen Transponderarten wurden rund 390.000 Rinder, 500.000 Schafe und 29.000 Ziegen mit einer Auswahl geprüfter und zertifizierter elektronischer Ohrmarken, Pansenkugeln oder injizierbarer Transponder versehen. Die ordnungsgemäße Funktion der auf- oder eingebrachten Transponder wurde zum einen durch Ablesungen verifiziert, die nach einem Tag, einem Monat und dann jährlich stattfanden, zum anderen bei Bewegungen der Tiere (z. B. bei der Schlachtung und nach der Entnahme des Transponders). Die Ergebnisse des IDEA-Projektes zeigen, dass sich die Überwachung durch die elektronische Kennzeichnung von Nutztieren deutlich verbessern lässt und dass der Einführung von RFID-Systemen bei Rindern, Büffeln, Schafen und Ziegen keine grundsätzlichen technischen Hindernisse im Wege stehen. Im Rahmen des Projektes wurde die RFID-Technologie dabei unter sehr unterschiedlichen Bedingungen getestet: Intensiv- und Extensivhaltung, Transporte innerhalb und außerhalb Europas, unterschiedliche Schlachttechniken sowie extreme Umweltverhältnisse im Norden und Süden der EU. [Euro 03] Bei den Versuchen haben sich jedoch auch einige Nachteile der elektronischen Tieridentifikation gezeigt. So gehen die elektronischen Ohrmarken genauso schnell verloren wie die traditionellen Ohrmarken. Auch können die Pansenboli bei Kälbern zu medizinischen Komplikationen führen. Die RFID-Technik ist zudem empfindlich gegen elektromagnetisches Rauschen auf den Bauernhöfen. [Hand 04]

Die breitere Einführung von RFID-Systemen wird zunehmend auch durch gesetzliche Verordnungen zur elektronischen Kennzeichnung von Tieren forciert. Unterstützt durch die Ergebnisse des IDEA-Projektes hat der EU-Ministerrat kürzlich europaweit eine Verordnung zur Kennzeichnung und Registrierung von Schafen und Ziegen als neuen Sicherheits- und Qualitätsstandard zur Bekämpfung von Tierseuchen verabschiedet. Die hohe Bedeutung der lückenlosen Nachvollziehbarkeit der Herkunft und Aufenthaltsorte von Schafen und Ziegen haben Tierseuchen wie die Maul- und Klauenseuche im Jahr 2001 eindrücklich unterstrichen: Da die Infektionsherde nicht rechtzeitig herausgefunden werden konnten, mussten letztlich Tausende gesunder Tiere zur Verhinderung der Seuchenverschleppung getötet werden. Viele Tierhalter hat dies in ihrer Existenz bedroht. Aber auch Hobbytierhalter waren maßgeblich betroffen: Nicht selten wurde der Zuchterfolg vieler Jahre vernichtet. [aid 04]

Das Ziel der neuen Verordnung ist es, die Gesundheit der Tiere zu verbessern, ihre Bewegungen zu überwachen und Subventionen zu überprüfen – und damit allen Verbraucherinnen und Verbrauchern in der EU einen besseren Schutz zu bieten. Nach der neuen Verordnung ist die Kennzeichnung von Schafen und Ziegen mittels Transponder gemäß ISO-Norm 11784/85 zunächst optional und wird nach einer Übergangsphase ab dem 1. Januar 2008 für die EU-Mitgliedsstaaten mit einer Schaf- und Ziegenpopulation von über 600.000 Tieren verpflichtend. Die gesammelten Informationen werden nach der Verordnung in jedem Mitgliedsland in einer zentralen Datenbank zusammengeführt. Register der landwirtschaftlichen Betriebe enthalten zukünftig auch Informationen darüber, von welchen Betrieben einzelne Tiere kommen bzw. wohin sie versandt wurden. Bislang beziehen sich die Aufzeichnungen nur auf die Bewegungen ganzer Herden. Mit der Einführung einer elektronischen Kennzeichnung werden in den Registern zudem detailliertere Informationen als bislang üblich festgehalten: Geschlecht, Stamm und Genotyp (soweit bekannt), Geburten und Todesfälle von Tieren sowie Bewegungen in den oder aus dem Betrieb. Ein spezielles Versanddokument

wird zum einen Informationen über die Ausgangs- und Zielstationen von Tiertransporten enthalten, zum anderen Informationen über die Gesamtzahl der beförderten Tiere. Das Versanddokument wird auch Angaben zur individuellen Identifizierung der Tiere enthalten. Bis Mitte 2005 soll eine Datenbank mit allen Informationen zu den landwirtschaftlichen Betrieben (Betreiber, Tierarten, Zahl der Tiere) aufgebaut sein. Gleichzeitig werden Informationen über Bewegungen von Gruppen von Tieren aufgezeichnet. Unter Berücksichtigung der Schlussfolgerungen des IDEA-Projekts wird der „Ständige Ausschuss für die Lebensmittelkette und Tiergesundheit" weitere Leitlinien und Verfahren für die Durchführung der elektronischen Kennzeichnung verabschieden: Leitlinien und Verfahren für die genaue technische Durchführung, Prüfverfahren und Akzeptanzkriterien für Geräte sowie Unterstützung für die Angleichung der Datenbanken und Kommunikationsprotokolle. [pres 03]

Vergleichbare Bestrebungen sind gegenwärtig auch in Nordamerika zu beobachten: In Kanada ist die elektronische Kennzeichnung ab dem 1. Januar 2005 vorgeschrieben und in den USA wird angesichts der jüngsten BSE-Fälle ebenfalls über die verpflichtende elektronische Kennzeichnung von Nutztieren diskutiert. [Phil 04]

Ein neues vernetztes RFID-System zur Tieridentifikation mittels elektronischer Ohrmarken haben im Rahmen des Projektes „Innovative Technologien zur elektronischen Kennzeichnung von Rindern – ITeK-Rind" die Vereinigte Informationssysteme Tierhaltung (VIT), Verden, und die Landwirtschaftskammer Weser-Ems entwickelt. Das Ziel besteht darin, die gesetzlich vorgeschriebene Qualitäts- und Herkunftssicherung rindviehhaltender Betriebe einfacher, sicherer und schneller zu gestalten. Rinder sollen automatisch über einen Chip im Ohr zu erkennen sein und die Daten an den Zentralrechner des Herkunftsinformationssystems Tiere (HIT) in München übermittelt werden. In einer ersten Erprobungsphase wird das System seit August 2003 auf dem Versuchsbetrieb Infeld der Landwirtschaftskammer Weser-Ems sowie drei Rindermastbetrieben und einem Schlachthof eingesetzt. Die Rinder tragen RFID-Etiketten mit einer nach ISO-Standard gespeicherten 15-stelligen Identifikationsnummer. Sämtliche Tierbewegungen werden somit automatisiert erfasst. Die Daten werden nicht nur an die zentrale HIT-Datenbank übertragen, sondern durch Lese- und Kommunikationstechnik auch auf dem Schlachthof genutzt. Projektförderer sind die CMA Centrale Marketing-Gesellschaft der deutschen Agrarwirtschaft mbH sowie die Kuratorien des Milchförderfonds Weser-Ems und Hannover-Braunschweig. [Flei 04] In der zweiten Projektphase soll seit dem Sommer 2004 die mobile Datenkommunikation ausgebaut werden, so dass die Tiermeldungen kabellos von jedem Standort der teilnehmenden Betriebe abgesetzt werden können. Es sollen zusätzlich aus Fremddatenbanken (sowohl VIT-intern als auch extern) Daten zur Verfügung gestellt werden, beispielsweise Leistungsdaten oder Zuchtinformationen. Durch die Einbindung weiterer Akteure (Schlachtbetriebe, Berater, Tierärzte) in das System soll zudem die Entwicklung eines umfassenden mobilen Informationssystems sichergestellt werden. Zeitgleich soll das Projekt auf etwa 15 weitere landwirtschaftliche Betriebe ausgedehnt werden, die das Informationssystem unter realen Bedingungen einsetzen und testen. [Vit 04]

Die Identifikation von Hunden mit injiziertem Mikrotransponder ist vor dem Hintergrund der zunehmenden Chip-Pflicht für bestimmte Hunde ein weiteres Einsatzgebiet der RFID-Technologie. Bereits seit dem 1. Januar 2003 ist in Nordrhein-Westfalen laut Landeshundegesetz der Einsatz von Mikrochips zur Identifizierung von Hunden ab 20 Kilogramm Gewicht beziehungsweise über 40 Zentimetern Schulterhöhe vorgeschrieben. In anderen Bundesländern ist das Gesetz in Vorbereitung. In der Europäischen Union gilt ab Juli 2004 bei der Einreise die Chip-Pflicht für Hunde und in der Schweiz ab dem Jahresende 2004.

Der miniaturisierte Chip wird mit einer Injektionsspritze unter die Halshaut platziert. Der kontrollierende Ordnungsbeamte kann die Nummer mit einem Einfachlesegerät ablesen, um anschließend per Telekommunikation über die zentrale Datenbank abzuklären, ob der betreffende Hund beispielsweise an der Leine zu führen ist, einen Maulkorb tragen muss oder ob die Hundesteuer gezahlt wurde. [Buch 04]

Behälteridentifikation:
RFID-Systeme zur elektronischen Kennzeichnung von Behältern werden in der chemischen Industrie und in der Abfallentsorgung verstärkt eingesetzt. Hierdurch können Transporte von Gefahrgütern besser gesichert und Abfallmengen leistungsbezogen angerechnet werden.

Im Bereich der elektronischen Behälteridentifikation ist die RFID-Technologie bereits langjährig im Einsatz. Gasflaschen und Chemikalienbehälter müssen, wenn sie toxische Substanzen beinhalten, genau beschriftet und eindeutig gekennzeichnet sein. Die hochwertigen Leihbehälter und -flaschen werden zunehmend mit RFID-Transpondern ausgestattet und sind so zu jedem Zeitpunkt der Anlieferung direkt zuzuordnen. Im Vergleich zu Barcodes bieten Transponder den Vorteil der deutlich höheren Speicherkapazität: Neben der Behälternummer können beispielsweise auch Eigentümer, TÜV-Termin, Inhalt, Volumen oder der maximale Fülldruck gespeichert werden. Durch den Einsatz von beschreibbaren Transpondern lassen sich die Daten – unter Beachtung von Schreib- und Lese-Zugriffsrechten – aktualisieren. Zudem halten die Transponder im Vergleich zu traditionellen Barcode-Labels schwierigere Umweltbedingungen wie sehr hohe und sehr niedrige Temperaturen, Schmutz, Feuchtigkeit, Strahlen, Vibrationen und Säuren aus. Die verwendeten Transponder in der Behälteridentifikation sind induktiv gekoppelt und arbeiten im Frequenzbereich unter 135 kHz. Ein Übertragungsverfahren für die Transponder zur Behälteridentifikation ist bislang nicht standardisiert worden, so dass unterschiedliche Systeme auf dem Markt angeboten werden. [Fink 02]

Vor dem Hintergrund gestiegener direkter und indirekter Entsorgungskosten ergeben sich für die RFID-Technologie auch im Bereich der Abfallentsorgung neue Möglichkeiten. Entsorgungskosten sind zum einen Kosten, die vertraglich mit den Entsorgungspartnern vereinbart werden und zum anderen die ablauforganisatorischen Kosten bei jedem Prozessbeteiligten (Bearbeitung von Wiegescheinen, Lieferscheinen, Rechnungen, Erstellung von Abfallstatistiken, Abfallbilanzen). Diese Kosten werden mit der fortschreitenden Komplexität der Nachweisverfahren voraussichtlich auch weiterhin ansteigen.

In verschiedenen Gemeinden Deutschlands – beispielsweise in den bayerischen Landkreisen Hof, Erlangen-Höchstadt, Mühldorf am Inn, Kehlheim oder Heiligenstadt – wurden vor diesem Hintergrund im Frequenzbereich unter 135 kHz RFID-Anwendungen eingeführt, um eine Prozessoptimierung zu erzielen oder eine verursachergerechte Kostenabrechnung einzuführen. Dabei werden die Mülltonnen mit einem Transponder und damit mit einer einmaligen Kennziffer ausgestattet. Dieser ID-Nummer werden die Grundstücksdaten und die Behältergröße zugeordnet. Hierdurch lässt sich feststellen, wem eine bestimmte Tonne gehört, anonyme Müllbehälter sind zukünftig ausgeschlossen. Die Transponder verfügen über einen passiven RFID-Transponder zur Identifikation durch das Müllfahrzeug. Durch ein Lesegerät am Müllfahrzeug wird der Transponder erkannt und die Leerungsdaten (Häufigkeit, Zeitpunkt der Leerung) werden auf einer Chipkarte im Bordrechner des Müllfahrzeuges gespeichert. Nach dem Ende der Schicht werden die Daten an eine Auslesestation des Entsorgungsbetriebs übergeben. Von dort aus erfolgt die Übermittlung der Daten an die Gebührenstelle im Landratsamt, wo sie ausgewertet werden. Einige Gemeinden bieten ihren Bürgern bereits den Service der Müllabgabenverrechnung nach Gewicht. Durch robuste Transponder auf den Mülltonnen sowie Waagen auf den Entsorgungsfahrzeugen bekommt jeder Haushalt exakt die produzierte Müllmenge verrechnet. Für die Gemeinden bietet sich zudem der Vorteil, die Routen der Müllwagen genau verfolgen zu können. Auch können sie die verrechneten Kosten der externen Müllentsorgungsbetriebe besser überwachen und Fahrtstrecken der Müllwagen optimieren. [Land 04]

Zu den grundsätzlichen Vorteilen der elektronischen Mülltonnenidentifikation zählen eine verbesserte Behälterlogistik und Verwaltung, geringere Möglichkeiten des Leistungsmissbrauchs durch die Registrierung der Tonnen (so können künftig keine Tonnen mehr zur Leerung bereit gestellt werden, die nicht bei der Abfallwirtschaft eines Landkreises angemeldet sind), einfachere Gebührenbescheide, neue Möglichkeiten der Mengenerfassung, eine Individualisierung und Flexibilisierung des Systems (der Kunde kann teilweise selbst bestimmen, wie oft er von der Dienstleistung „Müllabfuhr" Gebrauch macht) sowie Möglichkeiten der Gebühreneinsparung durch Abfalltrennung und -vermeidung.

Auch im Gesundheitswesen und in der pharmazeutischen Industrie sind strukturelle Veränderungen zu beobachten, die den Einsatz der elektronischen Identifikation befördern. Hierzu zählt beispielsweise die Kennzeichnung medizinischer Produkte wie Blutplasma oder Proben. Die RFID-Technologie soll in diesem Anwendungssegment dazu beitragen, die Kosten zu senken und Personal einzusparen sowie gleichzeitig die Qualitätsstandards zu wahren und Serviceleistungen zu verbessern. Zu den betriebswirtschaftlichen Vorteilen der elektronischen Identifikation im Gesund-heitswesen zählt zum einen die Zeitersparnis: Transponder in den Kitteltaschen von Ärzten und Pflegepersonal können die Benutzer automatisch und somit Zeit sparend authentifizieren. Zum anderen kommen Kostensen-kungspotenziale hinzu: Die Inventarisierung von Geräten und Materialien kann über die Ausstattung mit Transpondern zuverlässig und Zeit sparend erfolgen. Die direkte Folge ist eine Reduktion der im Bestellwesen und bei der Geräteüberwachung anfallenden Kosten. Darüber hinaus werden Kennzeichnungssysteme zur Gewährleistung der Qualität von medizinischen Produkten erprobt. So zeichnen beispielsweise an Blutbeuteln angebrachte aktive Transponder eventuelle Temperaturabweichungen auf und beugen einer Schädigung des Patienten durch die Verabreichung verfallener Blutprodukte vor. [ACG 04]

Auf der Kinderintensivstation des Universitätsklinikums Mainz befindet sich ein RFID-System im Rahmen eines Pilotprojektes in der Erprobung. Im Ausland wurden im Gesundheitswesen bereits Erfahrungen in der Praxis gewonnen. So vereinfachen in der Klinik Rotterdam Transponder die logistischen Prozesse bzw. den Umgang mit täglichem Bedarfsmaterial. Jede Mitarbeiterin bzw. jeder Mitarbeiter hat drei oder vier Arbeitskittel, die umlaufend in einer Wäscherei gewaschen werden. Wenn ein Kittel verschmutzt ist, wird er in das System eingespeist. Innerhalb von zehn Sekunden wird ein gereinigter Kittel ausgegeben. So sollen eine große Zeitersparnis bei der Kittelausgabe und die Versorgung der Wäscherei mit aussagekräftigen statistischen Werten erreicht werden. [Euro 04]

In Schweden wurde kürzlich ein neues RFID-System für die Anbringung an pharmazeutischen Verpackungen entwickelt, das bereits in einem Feldversuch im Einsatz ist. Der Chip, der über einen Speicher von 32 Kilobyte verfügt, kann laut dem Herstellerunternehmen Cypak umfassende Bestände verschlüsselter Daten sammeln, bearbeiten und austauschen. [ORF 04a]

Auch einige Großlabors nutzen die RFID-Technologie bereits heute, um ihre umfassenden Bestände an Gewebe- oder Blutproben zu verwalten. Wenn Arzneimittel lückenlos mit RFID-Transpondern ausgestattet wären, ließen sich Missbrauch und Fehlanwendungen deutlich reduzieren. Patienten könnten gewarnt werden, wenn sie ein Medikament zu häufig oder zu selten einnehmen. Sehbehinderten, so ein Szenario von Sun Microsystems, könnte ein Ausgabegerät Hinweise geben: „Dies ist Aspirin. Nehmen Sie zwei pro Tag". [Hill 03a]

Die elektronische Kennzeichnung von Objekten eröffnet grundsätzlich neue Möglichkeiten der Organisation der materiellen Umgebung für Blinde und Sehbehinderte und eventuell auch für ältere Menschen. So besteht das Ziel des RFID-basierten Systems

Gesundheitswesen: RFID-Systeme bieten aufgrund ihrer spezifischen Leistungsmerkmale im Transformationsprozess der pharmazeutischen Industrie und des Gesundheitswesens neue Möglichkeiten, die Versorgungsqualität zu verbessern, die Effizienz zu steigern und Kosten zu senken.

„TagIt“ darin, das Identifizieren und Auffinden von Büchern, Schachteln, Kleidungsstücken, elektronischen Geräten, CDs, Medikamenten etc. für die genannte Zielgruppe deutlich zu erleichtern. Die eingesetzten Etiketten sind passive und damit nicht allzu kostenintensive Transponder. Wird beispielsweise ein Buch gesucht, so müssen die Nutzerinnen und Nutzer zunächst den Suchbegriff in das System eingeben und mit dem RFID-Lesegerät vor dem Regal entlang fahren. Sobald das System fündig wird, gibt es ein entsprechendes Signal aus. [DrLi 04]

Die eindeutige Identifikation von Waren zu jedem Zeitpunkt eröffnet nicht zuletzt für den Einzelhandel Potenziale bei der unternehmensinternen Disposition sowie übergreifend bei den Partnern der gesamten Wertschöpfungskette. Die Logistikkette wird in der modernen Warenwirtschaft zunehmend global und komplex. Da es im Einzelhandel in aller Regel um die Optimierung von logistischen Prozessen geht, wird dieses Anwendungsgebiet in Abschnitt 8.8 „Supply-Chain-Management“ dargestellt.

Personenidentifikation: RFID-Systeme zum Zwecke der Personenidentifikation befinden sich in der Erprobungsphase. Die Anwendungszusammenhänge erfordern in der Regel eine Verknüpfung mit hochsensiblen Informationen, so dass Fragen des Datenschutzes eine besondere Rolle spielen.

Die RFID-Technologie wird nicht nur zur Identifikation von Tieren, Behältern und Waren, sondern auch zur Personenidentifikation eingesetzt. So hat Siemens Business Services in einem Pilotprojekt im New Yorker Krankenhaus Jacobi Medical Center mehr als 200 Menschen mit einem RFID-Armband ausgestattet. Im Armband ist ein Transponder integriert. Das RFID-System soll die schnelle und zielgerichtete Behandlung von Patienten unterstützen. Auf den einen halben Quadratmillimeter großen Transpondern sind Daten der Patienten hinterlegt, die der Arzt mit einem RFID-fähigen mobilen Kleincomputer, beispielsweise einem PDA oder einem Tablet-PC, auslesen kann. Bei einer Klinikaufnahme werden die Daten der Patienten in einer elektronischen Akte gespeichert. Anschließend erhält der Patient seinen Transponder. Über W-LAN erhält der Arzt automatisierten Zugriff auf die Datenbank und kann alle patientenbezogenen Informationen auf den Kleincomputer herunterladen. [ORF 04b]

In Taiwan wird die RFID-Technologie in ähnlicher Weise zur Bekämpfung der gefährlichen Form der atypischen Lungenentzündung SARS (Schweres Akutes Respiratorisches Syndrom) eingesetzt. Die Patienten und das Personal in der Klinik tragen RFID-Transponder am Körper. An Türen und anderen wichtigen Stellen des Gebäudes sind RFID-Lesegeräte zur Routenkontrolle installiert. Auf diese Weise lassen sich im Bedarfsfalle mögliche Infektionswege in der Klinik genau nachvollziehen. [Zeid 03]

Im japanischen Osaka soll ab Oktober 2004 ein RFID-System zur eindeutigen Personenidentifikation von Schülerinnen und Schülern an einer Schule eingeführt werden. Dazu werden Tags wahlweise in den Schulranzen, das Namensschild oder die Schuluniform, die in Japan fast überall Pflicht ist, fest eingebaut. Nach den Plänen der Schulträger sollen entsprechende RFID-Lesegeräte zur Identifizierung der Etiketten auf den Schulranzen an den Schultoren automatisch festhalten, wann jedes Kind zum Unterricht erscheint und wo es sich aufhält. Weitere Lesegeräte sollen an Orten aufgestellt werden, die Lehrer und Eltern als nicht wünschenswerte Aufenthaltsorte für die Schulkinder betrachten. Sobald ein Kind an so einem Ort eintrifft, könnten entsprechende Informationen per E-Mail oder Handy den Eltern übermittelt werden. [Heis 04a]

8.3. Echtheitsprüfung von Dokumenten

Derzeit werden weltweit verschiedene Ansätze getestet, um RFID-Transponder in Personalausweise und Reisepässe zu integrieren. Diese Transponder werden verwendet, um elektronische Fälschungsschutzmechanismen umzusetzen und damit erweiterte Echtheitsprüfungen zu ermöglichen sowie biometrische Merkmale – beispielsweise das Gesicht oder einen Fingerabdruck – im Ausweissystem (z. B. Reisepass) zu speichern. Die Tendenz geht hin zu einer Vernetzung der verschiedenen Identifikationsmerkmale in so genannte Multibiometrie-Plattformen, um die

Schwächen von einzelnen technischen Verfahrensweisen auszugleichen.

Die Europäische Union (EU) hat beschlossen, ab 2005 biometrische Merkmale in die Ausweise aufzunehmen. Bis Ende 2004 will der EU-Rat seinen Vorschlag präzisieren. Erste europäische Staaten bereiten die Einführung in der Praxis vor. So ist auch die Bundesdru-ckerei, die bislang 62 Mio. EU-Pässe auslieferte, mit Vorbereitungen beschäftigt. Auf der CeBIT 2004 stellte sie einen Reisepass mit eingearbeitetem Transponder sowie entsprechende Lesegeräte und Prüfanlagen erstmals vor. Das so genannte „Verifier Terminal" wurde bereits in einige europäische Länder für Feldtests verkauft, ebenso nach Asien. [Borc 04a]

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) schätzt die Kosten für die Einführung von biometrischen Reisepässen mit RFID-Transpondern in Deutschland auf rund 670 Mio. Euro. Bei den laufenden Kosten erhöht sich der Finanzbedarf um jährlich 610 Mio. Euro. Der Rechnungshof der USA kalkuliert für die Einführung biometrischer Pässe in den USA mit Anfangskosten von 8,8 Mrd. US Dollar und mit rund 2,4 Mrd. US Dollar jährlichen Folgeausgaben. Hinzu kommen die Kosten für die erforderlichen biometrischen Visa. Diese werden mit 2,9 Mrd. US Dollar Anfangsinvestitionen und jährlichen Folgekosten von bis zu 1,4 Mrd. US Dollar veranschlagt. [TAB 03]

Die Internationale Zivilluftfahrtorganisation (ICAO) hat sich eingehend mit der IT-Sicherheitsproblematik von Pässen beschäftigt und zugehörige Sicherheitsspezifikationen erarbeitet [ICAO 04a]. Diese betreffen insbesondere den Fälschungsschutz und die damit verbundene Möglichkeit von Echtheitsprüfungen sowie Zugriffsmechanismen auf die biometrischen Daten. Die ICAO arbeitet an internationalen Standards für Reisepässe. Die UN-Behörde hat einen Vorschlag erarbeitet, nach dem ab 2006 alle Länder Reisepässe ausstellen können, deren biometrische Daten sich über einen Transponder aus bis zu zehn Zentimetern Entfernung auslesen lassen.

Als biometrisches Verfahren bestimmt die ICAO die Gesichtserkennung. Gemäß den ICAO-Vorgaben sollen in der EU Passbilder als biometrische Daten auf RFID-Transpondern gespeichert werden. Optional darf ein Staat zusätzliche biometrische Merkmale entweder im Pass oder in einer nationalen Datenbank speichern. [GinO 04] .

Die bisherigen Systemerfahrungen zeigen noch erhebliche Fehlerraten. So hat ein Test der „International Biometric Group (IBG)", in dem Produkte von insgesamt elf Herstellern geprüft wurden, Fehlerraten bis zu 23 Prozent festgestellt. Unklar ist den Expertinnen und Experten noch, wie ein Reisepass mit eingebettetem Chip und Antenne aussehen müsste, der dem Abstempeln und Knicken zehn Jahre lang Stand hält. Aber auch die Frage nach der erforderlichen Interoperabilität der eingesetzten technischen Systeme ist bislang noch nicht beantwortet. [Schu 04a]

Laut ICAO soll der Transponder auf dem Pass mindestens 32 Kilobyte speichern können [ICAO 04b]. Dabei sind 20 Kilobyte für den Rohdatensatz eines Gesichts nötig, mit JPEG Komprimierung nur 16 Kilobyte. Damit die Länder mit unterschiedlichen Extraktionsmerkmalen arbeiten können, muss der Pass laut ICAO die Originaldaten enthalten und kein Template, d. h. keine auf die Parameter eines gegebenen Merkmalsraums reduzierten Daten. Bei den zusätzlichen biometrischen Merkmalen dürfen dagegen ersatzweise auch Templates gespeichert werden. Pro Finger sind zehn Kilobyte Speicherplatz erforderlich. Das Template, in diesem Fall das Abbild der charakteristischen Punkte eines Fingerabdrucks (Minutien), hat eine Größe zwischen 250 und 750 Byte. Für die Speicherung der Iris werden 30 Kilobyte im Original bzw. 512 Byte als Template benötigt. Neben diesen biometrischen Daten müssen auf dem Transponder ferner die persönlichen Daten – beispielsweise Name, Geburtsdatum, Wohnort etc. – sowie etwaige Zusatzvermerke wie „Botschaftsangehörige" gespeichert sein. Das US-Innenministerium präferiert aufgrund des hohen Bedarfs an Speicherplatz im Gegen-

Echtheitsprüfung: RFID-Systeme werden für die Echtheitsprüfung von Dokumenten weltweit getestet. Um die Chancen zu nutzen und die Risiken zu beherrschen, müssen Gestaltung und Anwendung der Systeme vor allem die Kriterien hohe Sicherheit und umfassende Vertrauenswürdigkeit erfüllen.

satz zur ICAO einen 64-Kilobyte-Chip. Bislang gibt es jedoch noch keinen Hersteller, der solche Chips in Massenproduktion herstellt. Infineon verfügt mit dem SLE 66CLX320 über einen für die Massenproduktion reifen 32-Kilobyte-Chip und hat für September 2004 einen 64-Kilobyte-Chip angekündigt. Philips hat bereits eine kleine Charge von 72-Kilobyte-Chips für Reisepass-Prototypen produziert und kann nach eigenen Aussagen sofort mit der Massenfertigung beginnen. [Schu 04a]

Das niederländische Ministerium für innere Angelegenheiten – zuständig für die Ausgabe von Reisepässen und Ausweisen – hat das Projekt „2B or not 2B“ gestartet, in dessen Rahmen die Integration von biometrischen Daten in Reisepässen untersucht wird. Bis zu 15.000 freiwillige Tester in sechs Gemeinden erhalten einen Pass, in dem auf einem RFID-Chip biometrische Daten gespeichert werden. Beim Abholen des Reisedokuments werden die im Testdokument erfassten biometrischen Daten verifiziert. In Einklang mit den Vorgaben der internationalen Behörde für zivile Luftfahrt ICAO werden als Erkennungssysteme die Fingerabdruck- und die Gesichtserkennung verwendet: Die Test-Reisepässe werden vom Grenzkontrollkiosk der kanadischen Firma BioDentity geprüft, den auch die deutsche Bundesdruckerei bei ihrem automatischen Grenzkontrollsystem nutzt. [Borc 04b, MBZK 04]

8.4. Instandhaltung und Reparatur, Rückrufaktionen

RFID-Transponder werden von Unternehmen unterschiedlichster volkswirtschaftlicher Branchen zunehmend auch für individualisierte und automatisierte Instandhaltungs- und Reparaturdienste sowie für Rückrufaktionen genutzt.

RFID-Transponder kommen beispielsweise im Rahmen der Werkzeugidentifikation und des dazu gehörigen Wartungsmanagements zum Einsatz. Im Kern geht es dabei darum, dass Werkzeuge am richtigen Arbeitsplatz eingesetzt und den Arbeitsplatzvorschriften entsprechend gepflegt werden. Betriebsmittel wie Werkzeuge gelten in den Betrieben und Unternehmen zunehmend als Schlüssel für Qualität, Termintreue und Wirtschaftlichkeit. Während in der Vergangenheit vor allem Entwicklungsarbeit in die Optimierung der Werkzeuge investiert wurde, ist im Zuge der fortschreitenden 1:1-Losgrößen-Produktion vor allem die Prozessoptimierung von Bedeutung. Die vielen einzelnen Projektentwicklungsstufen müssen schließlich mit der Vielzahl anfallender Termine, Daten und Änderungsinformationen in einem Umfeld immer kürzer werdender Produktentwicklungs- und Lebenszeiten sinnvoll organisiert werden. Neben den Potenzialen zur Kostensenkung und Sicherheitserhöhung werden sich unter anderem aus der Verlängerung der Gewährleistung auf 24 Monate durch das neue EU-Schuldrecht neue Anforderungen an den Werkzeugbau ergeben. Zukünftig werden Werkzeugbaubetriebe nicht umhinkommen, Verschleißteile und ihre Lebensdauer eindeutig zu definieren. Der Werkzeugbauer wird nur dann Haftung übernehmen wollen, wenn eine fachgerechte Instandhaltung durchgeführt und nachgewiesen wird. [ISK 03] Vor diesem Hintergrund wird hier der breitere Einsatz von RFID erwartet.

Die Flugzeug AG hat beispielsweise einen Werkzeugkasten getestet, dessen Werkzeuge mit RFID-Transpondern ausgestattet sind. Der Werkzeugkasten selbst ist mit einem RFID-Lesegerät ausgerüstet. Die Transponder enthalten eine Seriennummer der Werkzeuge sowie eine Nummer des dazugehörigen Werkzeugkastens. Die Hauptfunktion des Werkzeugkastens ist die automatische Überwachung seines Inhalts mittels der RFID-Technologie. Auf diese Weise kann die Applikation sofort feststellen, wenn fremde Werkzeuge versehentlich abgelegt wurden. Zusätzlich protokolliert die Applikation die Nutzungshäufigkeit der Werkzeuge anhand der Häufigkeit, mit der Werkzeuge aus dem Werkzeugkasten genommen und wieder zurückgelegt werden. Diese Daten werden im Werkzeugmanagementsystem ausgewertet.

Auf Grundlage dieser Information benachrichtigt das System die Mechaniker, wenn Werkzeuge ausgetauscht oder gewartet werden sollten. Die Applikation läuft im Hintergrund und entlastet die Mechaniker von den traditionell aufwendigen Kontrollen, da sie von dem RFID-gestützten System nur beim Auftreten von Fehlern benachrichtigt werden. [StFl 04]

Auch Airbus, einer der weltweit führenden Flugzeughersteller, nutzt RFID-Etiketten für die Kennzeichnung von Werkzeugen zur Verbesserung des Wartungsprozesses. Präzisionswerkzeuge zur Reparatur hochsensibler Flugzeugteile werden von Airbus nicht nur selber verwendet, sondern im Leasing-Verfahren auch an Wartungsgesellschaften verliehen. Die mit RFID-Etiketten ausgestatteten Werkzeuge liefern nun unmittelbar alle wichtigen Informationen zur Identifizierung und Lokalisierung, aber auch zu ihrem gesamten Lebenszyklus – beispielsweise um die regelmäßige Kalibrierung und Wartung der Werkzeuge richtig zu terminieren. Zwischen Airbus, den Wartungswerkstätten der Werkzeuge und den Kunden besteht ein Prozesskreislauf, dessen Status mithilfe von RFID überwacht wird. Ist es notwendig, dass die Werkzeuge gewartet werden müssen, erfolgt ein Aufruf, sie an die Werkstatt zu senden. [SAP 04]

Rückrufaktionen sind für die Unternehmen teuer, betreffen heute noch und verärgern darüber hinaus die Kunden. Allein im Jahr 2001 gab es in Deutschland beispielsweise von der Automobilindustrie 113 Rückrufe. In der Öffentlichkeit bekannt geworden ist das Beispiel des Reifenherstellers Firestone, der nach zahlreichen tödlichen Unfällen auf Firestone-bereiften Ford Explorern eine der größten Reifenrückruf-Aktionen der Geschichte einleiten musste.
Im Jahr 2000 rief der Hersteller aufgrund eines Produktionsfehlers bzw. möglicher Abrieb- und Platzgefahren 14,4 Mio. ausgelieferte Reifen zurück. Gleichwohl sind noch heute von dieser Charge 6,5 Mio. Produkte in Gebrauch. Auch aufgrund dieses Vorfalls reagieren vor allem die US-Behörden mit strengeren Auflagen im Bereich der Qualitätssicherung. [ZDNe 04]
So brachte die „National Highway Traffic Safety Administration (NHTSA)“ eine Regelung auf den Weg, die die Fahrzeughersteller dazu verpflichtet, ihre Autos mit einem Reifendruck-Kontrollsystem auszustatten. Bis zum 31. Oktober 2006 dürfen sich die Automobilhersteller frei für eines der auf dem Markt erhältlichen Systeme entscheiden. Bisher sind zwei Kontrollsysteme verfügbar, die auch von deutschen Automobilzulieferern angeboten werden. Bei den präzise messenden so genannten „direkten“ Kontrollsystemen findet eine direkte Überwachung des Reifendrucks statt. Das Gerät warnt die Fahrerin bzw. den Fahrer, wenn ein oder mehrere Reifen einen potenziell gefährlichen Unterdruck erreichen. Bei der zweiten Variante des so genannten „indirekten“ Reifendruck-Kontrollsystems wird per Sensor die Rotationsfrequenz der Reifen überwacht. Reifen mit Unterdruck sind im Durchmesser kleiner und rotieren daher schneller. Der Nachteil dieser weitaus preisgünstigeren Variante ist, dass das Verhalten der Reifen nur im Vergleich mit den anderen Reifen des selben Wagens kontrolliert wird. Daher würde das System eine synchrone Verschlechterung mehrerer Reifen nicht melden. Am 1. März 2005 will die NHTSA bekannt geben, welches System nach dem 31. Oktober 2006 Pflicht werden soll. [Mark o. J.]

Der Reifenhersteller Michelin plant nach eigenen Angaben als erstes Unternehmen, RFID-Transponder serienmäßig in Reifen einzubauen. Ab 2005 soll diese Technologie als Zubehör bei von Michelin ausgestatteten Neuwagen zu erwerben sein. Der Speicher des miniaturisierten Elektronikteiles kann über Funk mit neuen Informationen versehen werden, so dass neben der Reifennummer auch die Fahrgestellnummer oder andere Daten gespeichert werden können. Der Abruf der Informationen ist mit entsprechenden Geräten bis zu einer Entfernung von etwa 60 Zentimetern möglich. Alter, Reifendruck, Straßenzustand und ähnliche Informationen können so auch automatisch an

Instandhaltung und Reparatur: RFID-Systeme werden in den Bereichen Instandhaltung und Reparatur zunehmend zur Prozessoptimierung und Qualitätssteigerung eingesetzt. Die laufenden Kosten können durch verbesserte Datentransparenz deutlich gesenkt werden.

Rückrufaktionen: Elektronisch gespeicherte Produktinformation und Produktgeschichte bilden die Grundlage für die effiziente und effektive Durchführung von RFID-basierten Rückrufaktionen.

den Bordcomputer des Fahrzeuges übermittelt werden. Die Elektronik wird von den Unternehmen Fairchild Semiconductor und Philips unter Lizenz von Intermec Technologies geliefert. [Inno 04a]

Bei der Deutschen Bahn wird RFID gegenwärtig für einen qualitativ verbesserten Wartungsservice erprobt. Das Pilotprojekt ist in einem Duisburger Ausbesserungswerk angesiedelt. Gemeinsam mit der Symbol Technologies testet die Euro I.D. den Einsatz eines RFID-Systems im Bereich der Überholung und Wartung von Waggons. Ziel dieses Projektes ist die sichere Datenerfassung der Wartungsdaten. Die Daten wurden bislang auf Manschetten eingestanzt. Da diese häufig von den Achsen wegbrechen, fehlen bei der späteren Wartung jegliche Bezugsdaten. In diesem Umfeld sollen Transponder helfen. So wurden beschreibbare Transponder direkt an der Achswelle der Waggons angebracht und mit allen Daten, die im Rahmen der Ausbesserung anfallen, beschrieben. Die Basisdaten werden nur ein Mal elektronisch aufgenommen. Sämtliche Daten können dann von verschiedenen Wartungsorten aus gelesen und ergänzt werden. Die Fehlerquelle der manuellen Erfassung soll durch den Einsatz der RFID-Technologie beseitigt werden. [Euro 04]

Darüber hinaus ist die Identifikation von Lebensmitteln ein bedeutendes Einsatzgebiet der RFID-Technologie für die effiziente Steuerung von Warenrückrufaktionen. Zum Schutz der Verbraucher hat die Europäische Union mit der Verordnung (EG) Nr. 178/2002 die allgemeinen Grundsätze des Lebensmittelrechts festgelegt. Die Verordnung fordert alle Beteiligten der Prozesskette „Lebensmittel“ dazu auf, bis zum 31. Dezember 2004 die Rückverfolgbarkeit ihrer Produkte sicherzustellen und den Behörden diese Informationen auf Anfrage mitzuteilen. Des Weiteren verpflichtet die Verordnung alle Unternehmen zum Rückruf von Lebensmitteln, die den gesetzlichen Anforderungen an Lebensmittel nicht genügen. Hierbei genügt schon der Verdacht. [ECR 04]

Da die Chips mit einer 96-Bit-langen Identifikationsnummer neben dem Hersteller- und Produktnamen die individuelle Serien- und Produktnummer transportieren können – der bislang übliche Barcode wird in aller Regel verwendet, um die Produktbezeichnung und den Hersteller zu codieren – lässt sich die Herstellung der Produkte auf Grundlage der RFID-Technologie zurückverfolgen, wie es zunehmend durch gesetzliche Auflagen vorgeschrieben ist. Gleichzeitig kann im Bereich von verderblichen Waren ein Verfallsdatum und ein aktueller Lagerplatz zugeordnet werden, so dass der Supermarkt über die Information verfügt, ob und wie viele Waren mit demnächst überschrittenem Verfallsdatum in den Regalen liegt. Daraufhin können beispielsweise Sonderpreisaktionen initiiert oder mit einer Umsortierung auf die so genannte „Pole-Position“ im Regal der Abverkauf beschleunigt werden. [Sinn 04]

8.5. Zutritts- und Routenkontrolle

Magnetkarten- oder Chipkarten-Anwendungen – ob als Ausweis für den Zutritt zu Räumen oder Gebäuden, als Guthabenkarten beispielsweise für den Zugang zu öffentlichen Kartentelefonen oder als Kreditkarte – gehören mittlerweile zum Alltag. Typischerweise müssen diese Karten in ein Terminal eingeführt werden, das dann die Verbindung zu weiteren IT-Anwendungen, so zur Zeiterfassung oder Bargeldauszahlung von Guthabenkonten, herstellt. RFID-Systeme ermöglichen es heute, kontaktlos Daten zu erfassen und so die Leistungsmerkmale der bekannten Kartenanwendungen zu erweitern. Als Bauform der Transponder wird häufig die vielen Nutzern vertraute Plastikkarte gewählt, aber auch Schlüsselanhänger und Armbänder werden eingesetzt. Elektronische Ausweise arbeiten typischerweise im Bereich von 13,56 MHz. Die Erfassungsgeräte müssen in einem Leseabstand von maximal einem Meter errichtet werden. Die Systeme verfügen typischerweise über eine mittlere Leistungsfähigkeit: Neben der Identifikation im eigentlichen Sinne sind auch Schreibvorgänge mög-

lich, um die Daten bei Bedarf zu aktualisieren oder um eine Multifunktionalität des RFID-Systems zu unterstützen.
Kontaktlose Zutrittssysteme haben sich bereits heute auf dem Markt durchgesetzt, wenn der Anbieter eine schnelle Identifikation von Einzelpersonen oder Gruppen unterstützen oder langwierige Kontrollverfahren verkürzen möchte. Dabei sind RFID-Systeme immer dann unter ökonomischen Kriterien attraktiv, wenn Personen Kontrollpunkte wiederholt passieren müssen. Als typisches und langjähriges Einsatzfeld haben sich elektronische Zugangskontrollsysteme in Urlaubsressorts etabliert, die in der Regel mit einer digitalen „Geldbörse“ kombiniert werden.

So wurde in der österreichischen Region Nassfeld/Sonnenalpe – wie in vielen anderen Urlaubsressorts – in der Saison 1999/2000 eine RFID-Lösung umgesetzt, die eine Vielzahl unterschiedlicher touristischer Leistungsträger, wie Hotel-, Skihütten-, Skilift- oder Bergbahnbetreiber, mit einbezieht. Der Gast soll sich während des gesamten Aufenthalts „berührungs- und bargeldlos“ in der Region bewegen können. Mit einer Investitionsgesamtsumme von 715.000 Euro wurden 80 Erfassungsgeräte, zehn Standardkassensysteme sowie 50 so genannte Offsite Points Of Sale – Ausgabestellen in Hotels- und Beherbergungsbetrieben, Skiverleihstellen und Skischulen – aufgebaut. Leistungen können auch über das Internet oder Mobilfunknetze gebucht und dann bei jeder Ausgabestelle auf dem Transponder gespeichert werden. Hierfür wurde ein regionales Funknetz aufgebaut, das über 40 Sende- und Empfangsstationen PCs mit einem Server verbindet, der Gästedaten zentral speichert.

Zum Einsatz kommen zwei unterschiedliche Typen von Transpondern im Kartenformat: Karten im Frequenzbereich 122,8 kHz werden für Multiapplikationskarten genutzt (die auch als „Hotelschlüssel“ Verwendung finden), Karten im Frequenzbereich 13,56 MHz finden nur als Skipass Verwendung. Die Speichergröße beträgt bei den eingesetzten 13,56-MHz-Karten 2048 Bit. Die 13,56-MHz-Datenträger haben eine Up- und Downlink-Geschwindigkeit von bis zu 26 kbit/s, die 122,8-kHz-Karten nur drei kbit/s. Zwar erfüllt das Kartenformat die ISO-Norm 7810 und dann hat damit die typischen Chipkartengröße von 85,6 x 54 Millimeter. Das eigentliche RFID-System jedoch ist kein ISO-Datenträger. Der maximale Lese- und Schreibabstand beträgt jeweils 40 Zentimeter.

Antikollisionsverfahren sind zwar grundsätzlich möglich, wurden aufgrund einer „extremen Verschlechterung der Performance“ auf der Hardware-Seite im Erfassungsgerät aber nicht umgesetzt. Da Personen im Ski-Bereich einen durchschnittlichen Abstand von 80 Zentimetern halten, ist auch die Zahl der Transponder im Erkennungsbereich begrenzt. Um Fehler bei der Übertragung der Daten erkennen zu können, wird der Cyclic Redundancy Check (CRC) eingesetzt. Auf den meisten der verwendeten Datenträger ist es möglich, mehrere Ebenen mit Berechtigungen zu belegen (z. B. Skipass auf der ersten Ebene, Hotelschlüssel auf der zweiten Ebene). Die Berechtigungen werden passwortgeschützt gespeichert. Eine Verschlüsselung der gespeicherten Daten erfolgt für jede einzelne Ebene.

Dem Gast wird bei Ankunft eine Karte für Zimmer, Skidepot, Skiverleih, Skipass und Geldbörse ausgestellt. Je nach den gebuchten Leistungen ermöglicht die Karte den Zutritt zu Skilifts, die Nutzung des Ski- und Boardverleihs sowie weiterer Angebote in der gesamten Region. Typischerweise erfolgt die Zutrittskontrolle über Schleusensysteme oder durch in Türrahmen installierte Zugangskontrollen. In Bars und Restaurants werden zu zahlende Beträge mit mobilen Erfassungsgeräten abgebucht.

Die hohe Akzeptanz auf der Kundenseite begründen die Betreiber vor allem mit der Bequemlichkeit für den Kunden. Am Skilift entfällt beispielsweise das umständliche Suchen nach dem Skipass. Sofern die Karte verloren geht, kann sie schnell gesperrt und neu ausgestellt werden. Sofern an einer

Zutrittssysteme: Das Bedürfnis zur Identifizierung und Verifizierung von Personen im privatwirtschaftlichen Bereich nimmt weiterhin zu. RFID-Systeme werden in verschiedenen Anwendungsbereichen für eine elektronische Zutrittskontrolle, aber auch für das elektronische Ticketing genutzt.

Verkaufsstelle mit Wartezeiten zu rechnen ist, können Leistungen auch an einer anderen Verkaufsstelle erworben werden. Für den Betreiber ergeben sich Einsparungspotenziale durch den schnelleren Zugang und somit die Vermeidung von Wartezeiten beispielsweise an Skilifts, durch den geringeren Personalaufwand bei der Zutrittskontrolle oder durch die schnellere Abwicklung von Zahlungsprozessen bei allen beteiligten Leistungsanbietern. Darauf aufbauend ermöglichen es die Daten des zentralen Marketingservers aber auch, das Leistungsangebot einzelner Leistungsträger oder des Zielgebietes insgesamt zu optimieren. Die Anwendung ermöglicht eine detaillierte Auswertung der Daten einzelner Kunden bzw. der Nachfrage nach Leistungen und des Umsatzvolumens insgesamt. Es entsteht eine hohe Datenmenge personenbezogener Daten, die durchaus ein genaues Bild der Präferenzen und der Aufenthaltsorte bzw. der Pfade des Kunden während des Aufenthaltes in der Region abgeben können. An jeder Kasse kann eine genaue Routenverfolgung des Datenträgers erfolgen (benutzte Anlagen, zurückgelegte Höhenmeter, etc.). Diese Daten können für die Optimierung der Liftauslastung, der Infrastrukturplanung etc. herangezogen werden. Gegenwärtig wird an Programmen gearbeitet, die es ermöglichen sollen, eben diese Kundenströme grafisch darzustellen und damit auch dem Skigast eine Information z. B. über die Gebietsauslastung zu geben.

Dass die Leistungsmerkmale der Transponder an die Anforderungen des Einsatzgebietes angepasst werden können, verdeutlicht ein anderes Beispiel der Zutrittskontrolle aus dem Freizeitbereich. In einem Fitness-Klub erhalten Kunden Armbänder, die über einen hitzebeständigen Transponder verfügen und auch im Saunabereich getragen werden können. Auch die Schlagunempfindlichkeit des Bautyps erweitert das Leistungsspektrum. [Euro 04]

Ein anderes prominentes Beispiel von RFID-basierten Zutrittskontrollen ist im Zuge der Fußball-Weltmeisterschaft 2006 (WM 2006) geplant. So sollen alle Eintrittskarten der WM 2006 in Deutschland mit einem Transponder und die Eingänge der zwölf Fußballstadien jeweils mit RFID-Lesegeräten ausgestattet werden. Hierdurch soll das Fälschen von Karten erschwert sowie sichergestellt werden, dass Karten nur an berechtigte Personen und nicht an bekannte Gewalttäter verkauft werden. [Pößn 04] Die Eintrittskarten für die Veranstaltung werden hauptsächlich über das Internet verkauft. Der Besteller erhält zunächst ein Zertifikat, das seinen Anspruch auf ein Ticket bestätigt. Vier bis sechs Wochen vor der Fußball-Weltmeisterschaft werden dann die personalisierten Eintrittskarten per Briefpost – nicht mehr per Wertbrief – verschickt. Die Daten werden in das elektronische Einlasssystem überspielt. Verlorengegangene Tickets können gesperrt und neu ausgestellt werden. Der Karteninhaber hält bei Eintritt in das Fußballstadion seine Eintrittskarte an das Lesegerät und seine Daten werden mit dem elektronischen Einlasssystem abgeglichen. Nach der WM 2006 soll das Konzept von den Stadienbetreibern für die Bundesliga und andere Großveranstaltungen genutzt werden. [ECIN 04, Heis 04b]

Die hier skizzierten Leistungsmerkmale von RFID-basierten Zugangssystemen sind charakteristisch für weitere Einsatzbereiche wie das Ticketing von Veranstaltungen im Freizeitbereich (Theater, Konzerte, Sportveranstaltungen). RFID-Systeme erleichtern das Ausstellen von Tickets für Einzelveranstaltungen bzw. Events wie Weltmeisterschaften, bei denen der Zutritt für mehrere Veranstaltungen oder einen bestimmten Zeitabschnitt auf einem elektronischen Ticket gespeichert werden kann. Das Ticket kann durch Schreibgeräte direkt an der Verkaufsstelle ausgestellt werden. Im Falle des Verlusts kann eine Sperrung und Neuausstellung erfolgen. Beim Einlass kann auf die Einzelkontrolle verzichtet werden. Fälschungen werden erschwert.

Einen weiteren Schwerpunkt des RFID-Einsatzes bilden Berechtigungsprüfungen zu Räumen mit beschränktem Zutritt. Sie sind

derzeit vor allem in Unternehmen etabliert, werden aber auch für öffentliche Räume, z. B. für Flughäfen, zunehmend diskutiert. Berechtigte Personen erhalten einen personalisierten Transponder, der in unterschiedliche Bauformen eingebettet werden kann. Die Berechtigung kann differenziert erfolgen und so den Zugang nicht nur zum Gelände insgesamt, sondern auch zu spezifischen Räumen erlauben oder verwehren. Über entsprechende Lesegeräte an den Türen und eventuell über Schleusensysteme kann der Zutritt gewährt oder verweigert werden. Auch in diesem Anwendungsgebiet werden in der Regel weitere Funktionen im RFID-System implementiert. Für den Unternehmensbereich ist die Erfassung von Zutritts- bzw. Arbeitszeiten typisch.

In (Hoch-)Sicherheitsbereichen können die auf dem Transponder gespeicherten Daten auch biometrische Merkmale der Autoidentifikation wie die Gesichtsgeometrie, den Fingerabdruck und die Irisstruktur des Auges umfassen. Allgemein umfasst die Nutzung von biometrischen Merkmalen in der Autoidentifikation das Auslesen der biometrischen Daten aus dem RFID-Speicherchip der Identifikationsdokumente, das Einlesen der biometrischen Merkmale mit entsprechender Sensorik und den Vergleich der Daten mit bereits gespeicherten Datenbeständen auf Übereinstimmung. Grundsätzlicher Zweck ist es also, die gemessenen biometrischen Daten einer Person mit den im elektronischen Dokument gespeicherten biometrischen Referenzdaten zu vergleichen.

Die Identifikation von Objekten, Personen oder unterschiedlichen Standorten erlaubt auch eine Verlaufs- und Routenkontrolle. Ein relativ neues Einsatzgebiet bildet das Aufzeichnen der Wege bzw. Anwesenheitszeiten an diversen Standorten von Personen. Vor dem Hintergrund, dass zunehmend Aufgaben an Fremdfirmen übergeben werden, ermöglicht RFID es hier, einerseits eine indirekte Kontrolle der erbrachten Leistungen durchzuführen, andererseits diese Leistungen zeitgenau abzurechnen. So stattete die Stadt Dresden beispielsweise ausgewählte Service-Objekte wie Haltestellenhäuschen oder Spielplätze mit Transpondern aus. Die Auftragnehmer verfügen über mobile Lesegeräte, mit denen die erbrachten Leistungen am Objekt gespeichert werden können. Die Daten sollen der Stadt Dresden auch dazu dienen, ausgelagerte Dienstleistungsprozesse besser zu planen und weiter zu optimieren. Für dieses System werden Chipkartensysteme eingesetzt, deren Leistungsmerkmale den oben dargestellten elektronischen Ausweisen zur Zutrittskontrolle entsprechen. [Euro 04]

Zunehmend kommt die Routenkontrolle im Gepäck- und Paketbereich zum Einsatz. So führen die Fluggesellschaften Systeme ein, um Gepäckstücke per RFID zu identifizieren. Neben dem Gepäck-Routing bildet das Paket-Routing ein weiteres, bereits heute weit verbreitetes Einsatzfeld. Grund hierfür ist, dass das RFID-System unternehmensintern betrieben wird. Schnittstellen zu weiteren Wirtschaftsakteuren müssen in der Regel nicht bedacht werden. Für die Anwendung reichen einfache Tags, die einmal zu Beginn des Verfahrens mit einer Identifikationsnummer versehen werden. Ein Wiederbeschreiben ist nicht erforderlich. Die Identifikation kann auch bei einer Vorwärtsbewegung von bis zu vier Metern pro Sekunde erfolgen. Als Frequenzbereich wird 13,56 MHz verwendet. Die Verlaufskontrolle erfolgt über eine zentrale Datenbank, die immer dann aktualisiert wird, wenn das Objekt einen neuen Kontrollpunkt passiert hat. So kann nicht nur der Paketdienstbetreiber, sondern auch der Kunde über das Internet die Zustellung seiner Sendung verfolgen.

Der RFID-Einsatz für Briefe und Päckchen steht im Mittelpunkt eines siebenjährigen Pilotprojektes, das die „International Post Corporation“ (IPC) im Mai 2004 startete. In der IPC sind 23 europäische, amerikanische und asiatische Postunternehmen zusammengeschlossen, unter ihnen auch die Deutsche Post. IBM entwickelt für das Vorhaben ein Softwareprodukt, das die Koordination der Postsendungen verwalten soll. Im Rahmen

Verlaufs- oder Routenkontrolle: RFID-Systeme werden für die Verlaufs- und Routenkontrolle von Gepäckstücken oder Paketen eingesetzt. Die Tags werden im Flugverkehr z. B. an Stelle der bislang üblichen Papierstreifen an den Gepäckstücken befestigt und lassen sich entlang des Transportweges erfassen.

des Pilotvorhabens sollen 3.000 Testnutzer pro Jahr etwa eine halbe Million Briefe und Päckchen, die jeweils mit einem aktiven RFID-Tag ausgestattet werden, zwischen 26 Staaten versenden. Die genutzten aktiven Transponder werden meist im Ultrahochfrequenz- oder Mikrowellenbereich betrieben. Diese RFID-Systeme zeichnen sich durch Reichweiten von bis zu einhundert Metern aus, sind jedoch vergleichsweise teuer und wegen der Transponder-Batterie nur in einem eingeschränkten Temperaturbereich einsetzbar. [Sili 04]

Tracking und Tracing: RFID-Systeme ermöglichen die automatische und lückenlose Weiterverfolgung von betrieblichen Objekten innerhalb der Wertschöpfungskette.

Eine weitere sehr leistungsfähige Lösung im Ultrahochfrequenzbereich mit einem aktiven Transponder und Lese-/Schreibfunktion wird seit 2002 von der Deutschen Post zur Kennzeichnung von Lastwagen und Containern genutzt. Diese Anwendung ist auch für den Einsatz in rauen Umgebungen geeignet. Installiert wurden 66 Schreib-/Lese-Einheiten und 11.000 Transponder in 33 Fachzentren. Jedes Gefährt und jeder Container ist mit einem Transponder ausgestattet. Die Identifikationsnummer dieses Tags kann nicht verändert werden. Darüber hinaus können 56 Kilobytes an Informationen bis zu 100.000-mal verändert werden. Die Erfassungsgeräte werden an Knotenpunkten, beispielsweise dem Eingang des Frachtzentrums, installiert. Die gleichzeitige Identifikation mehrerer tausend Objekte wird nach Angaben des Herstellers Identec Solutions (Produkt: i-Q series) durch Antikollisionsverfahren gewährleistet. Der Transponder ist aufgrund seiner Robustheit auch für industrielle Anwendungen geeignet. Im Anschluss an die automatische Erkennung erhält die Fahrerin bzw. der Fahrer einen Ausdruck mit Informationen, an welcher Rampe die Ladung angeliefert oder neue Ladung aufgenommen werden soll. Das System steuert darüber hinaus auch die Zugangskontrolle. Die RFID-Lösung ermöglicht so den Überblick über die Zahl der sich vor Ort befindenden Lastwagen und Container in „Echtzeit“. Sofern Änderungen der Lieferkette nötig sind, können diese Maßnahmen über das zentrale Datenbanksystem zeitnah umgesetzt werden. [Kric oJ]

Die vorangestellte RFID-Lösung wird auch beim Automobilhersteller Volkswagen zur Identifikation von Fahrzeugen sowie zum Tracking und Tracing bis zu einer Reichweite von 100 Metern genutzt. In Wolfsburg werden Fahrzeuge für die Abholung vorbereitet. Nach Abschluss der Fertigung werden die Fahrzeuge mit einem Transponder ausgestattet, der mit der Identifikationsnummer des Fahrzeuges und einer Liste der noch durchzuführenden Aufgaben versehen wird. Der Transponder ermöglicht es – durch Blinken mittels eines eingebauten LEDs – einem mobilen Erfassungsgerät, das Fahrzeug aufzufinden. Durchgeführte Leistungen werden automatisch, beispielsweise bei der Anfahrt in eine Waschanlage, auf dem Transponder vermerkt. Der Transponder unterstützt aber auch die Steuerung von Prozessabläufen in der Autostadt. So werden die Abmessungen von automatischen Transportsystemen an den Radabstand der Fahrzeuge angepasst. Das RFID-Tag kann wieder verwendet werden. [Iden 04]

In anderen Ländern wird die Ausstattung von Fahrzeugen mit RFID-Technologie beispielsweise für eine automatische Maut-Erhebung getestet. So wurden im Rahmen eines Pilotprojektes in Südafrika die Nummernschilder von Fahrzeugen mit passiven RFID-Tags ausgestattet, die noch auf eine Entfernung von sechs Metern ausgelesen werden konnten. Im Rahmen des Tests wurden vier Fahrzeuge mit jeweils zwei RFID-Etiketten hinter der Windschutzscheibe versehen und an einem RFID-Lesegerät vorbeigefahren. Die Lesegeräte konnten bis zu 7.200 RFID-Tags pro Minute auslesen. Zur Simulation eines hohen Verkehrsaufkommens wurden die Fahrzeuge bei Geschwindigkeiten zwischen 80 und 100 Kilometern pro Stunde und zum Teil auch deutlich schneller nach-, hinter-, neben- oder auch gegeneinander an den Lesegeräten vorbei gefahren. Selbst bei Geschwindigkeiten um die 250 Stundenkilometer ließen sich die RFID-Tags noch ohne Probleme auslesen. Die RFID-Tags erwiesen sich in den Tests als sehr temperaturresistent, da sie bei Temperaturen

zwischen -40° und +85°Celsius funktionierten. [SEC 04a]

Im öffentlichen Verkehr wird die RFID-Technologie ebenfalls getestet. So wurden beispielsweise im schottischen Edinburgh Busse mit RFID-Transpondern ausgestattet. Sobald sich die Fahrzeuge einer Ampel nähern, schaltet diese automatisch auf Grün. Dadurch können diese öffentlichen Verkehrsmittel ihre Strecken zehn Prozent schneller zurücklegen als bisher. [Hill 03b]

8.6. Diebstahlsicherung und Reduktion von Verlustmengen

Als weiterer Nutzen von RFID-System wird die Reduktion von Schwund und Diebstahl diskutiert. So dient beispielsweise der RFID-Einsatz bei Fluggesellschaften nicht nur der Routenkontrolle, sondern auch der Reduktion bzw. dem schnelleren Auffinden von verlorenen gegangenen Gepäckstücken. Beispielsweise transportiert die Fluggesellschaft Delta zwischen 35 und 85 Mio. Gepäckstücke pro Jahr. Obwohl von diesen weniger als ein Prozent fehlgeleitet werden, entstehen Kosten in Höhe von 100 Mio. US Dollar pro Jahr. Die Investitionssumme für die Implementierung eines RFID-Systems wird dagegen mit 25 Mio. US Dollar veranschlagt. [tecc 04]

Auch im Bereich des Container- und Behältermanagements soll bei Fluggesellschaften der Schwund durch RFID reduziert werden. Hier bestehen derzeit Probleme bei der Inventurhaltung, aber auch bei der Rückgabe von Behältern, die an Dritte verliehen wurden. Mit RFID soll das Asset Management durch Lokalisierungsfunktionen verbessert werden. Auch in anderen Industriezweigen, zum Beispiel dem Automobilbereich, werden derartige Systeme genutzt.

Weit und langjährig verbreitet sind RFID-Lösungen im Bereich der Wegfahrsperren von Kraftfahrzeugen, die entweder die Zündung, den Anlasser oder die Treibstoffzufuhr unterbrechen und über einen RFID-Transponder im Autoschlüssel deaktiviert werden. In diesem Bereich werden von Siemens Lösungen entwickelt, die über einen ins Mobiltelefon integrierten „Smart Key“ in Kombination mit einem Erfassungsgerät den Zutritt zu Gebäuden oder den Gebrauch von Kraftfahrzeugen ermöglichen. Der heute bekannte Autoschlüssel könnte so entfallen. Das Mobiltelefon könnte auch weitere Funktionen übernehmen – als elektronische Geldbörse, als Fahrausweis im Öffentlichen Nahverkehr oder als Scanner zum Auslesen von Tags im Erfassungsbereich. Siemens testet hierfür eine Kombination von RFID- und NFC-Technologie (Nearfield Communication – siehe hierzu auch Abschnitt 10). [Gole 04]

Ein anderes Einsatzfeld des Asset Managements sind Büroumgebungen. Hier dienen RFID-Systeme einerseits der Diebstahlsicherung vor allem bei hochwertigen tragbaren Geräten wie Laptops, andererseits aber auch dem Auffinden von Akten oder der Steuerung von Rohrpostsystemen. Beispielsweise nutzen amerikanische Anwaltsfirmen elektronische Etiketten zur Kennzeichnung ihrer Dokumente. Die Etiketten werden mit einer Schreibeinrichtung gekennzeichnet und aufgeklebt. Im Sekretariat oder in der Registratur dienen so genannte „Tracking Pads“ vor der Weitergabe der Dokumente zur Kontrolle. Diese Informationen werden in einer zentralen Datenbank gespeichert, über die auch der Standort der Dokumente abgefragt werden kann. Mobile Erfassungsgeräte unterstützen die Inventarisierung oder das Auffinden verloren gegangener Schriftstücke. Das Unternehmen 3M gibt als Anbieter von Tracking-Lösungen für dieses Einsatzgebiet an, dass mit dem RFID-System 95 Prozent der Dokumente sofort auffindbar sind (File Accuracy). Dagegen sei in einem Praxisbeispiel mit einer gut etablierten Barcode-Lösung nur ein Wert von 65 Prozent erzielt worden. [Malo 04] Die Nutzung von RFID-Systemen bei Rohrpostsystemen dient dazu, die Zahl der Irrläufer zu vermeiden. Darüber hinaus können die Büchsen automatisch wieder an die Absenderstation zurückgeleitet werden.

Diebstahlsicherung:
Mit der heute verfügbaren Technik lassen sich RFID-Etiketten zur Diebstahlsicherung gut handhaben.
Die Deaktivierung und Aktivierung der Diebstahlsicherung kann auch als integrierter Bestandteil traditioneller Ausleih- und Rückgabevorgänge vorgenommen werden.

Über Datenbankanwendungen ist es möglich, Durchlaufzeiten zu kontrollieren und zu optimieren.

Ein Telekommunikationsunternehmen in Hongkong lokalisiert Einrichtungsgegenstände nahezu „in Echtzeit“. Das Inventar ist mit Transpondern versehen, die von Beschäftigen über PC oder Mobiltelefon geortet werden können. Somit ist auch eine Inventur per Computer ohne manuelle Kontrolle grundsätzlich möglich. Das System dient ferner der Optimierung von Unternehmensressourcen. [Comp 04c]

Vergleichbare RFID-Lösungen dienen auch zur Diebstahlsicherung bzw. zur Reduktion von Verlustmengen im Einzelhandel. Hier werden so genannte 1-Bit-Systeme bereits seit etwa 40 Jahren zur elektronischen Diebstahlsicherung (Electronic Article Surveillance = EAS) genutzt. Diese Systeme signalisieren einem Erfassungsgerät nur das Vorhandensein bzw. das Nichtvorhandensein eines Transponders im Feld. Diese heute weit verbreiteten Sicherungsetiketten – beispielsweise an Kleidung – müssen an der Kasse auf „Null“ gesetzt werden, um die Auslösung eines Alarms beim Verlassen des Ladens zu vermeiden (siehe hierzu auch Abschnitt 8.8 „Supply-Chain-Management“).

Diese Lösungen können mit heutigen RFID-Systemen „intelligenter“ realisiert werden, d. h., der Transponder kann ggf. bereits beim Hersteller versteckt integriert und mit detaillierten Informationen zum Produkt versehen werden, um beispielsweise das Austauschen von Preisetiketten zu verhindern. Typischerweise werden solche Lösungen jedoch nicht allein zur Diebstahlsicherung eingesetzt, sondern dienen auch der Bereitstellung von Produktinformationen, um beispielsweise Inventuraufgaben im Einzelhandel zu optimieren. Sie können jedoch auch genutzt werden, um – beispielsweise bei dem Modeunternehmen Prada getestet – Kunden weitere Informationen zum Produkt zu geben, die dann über Bildschirme im Geschäft angezeigt werden.

Durch den Einsatz von äußerlich nicht sichtbaren Transpondern ergeben sich auch für den Umgang mit Kleintieren, Zuchttieren oder geschützten Tierarten neue Möglichkeiten zum Schutz vor Diebstahl, Missbrauch oder Verlust. Durch injizierte Mikrotransponder ist es möglich, ein Tier weltweit unverwechselbar, unverlierbar und unverfälschbar zu kennzeichnen. Behörden, Tierärzte, Tierheime, nationale und internationale Zuchtverbände, Universitäten oder Zoos können über ein Lesegerät eingehende Tiere identifizieren und mit den in einer zentralen Datenbank gespeicherten Informationen abgleichen. In diesem Zusammenhang werden Transponder beispielsweise im Rahmen des Washingtoner Artenschutzübereinkommens „Convention on International Trade in Endangered Species of wild Fauna and Flora (CITES)“ zur Kontrolle des internationalen Handels mit bedrohten Tier- und Pflanzenarten eingesetzt. Als Instrument verbindlichen internationalen Rechts gilt CITES in über 150 Nationen (Vertragsstaaten). [Euro 04]

Aber auch entlaufene oder gestohlene Haustiere können auf Grundlage der RFID-Technologie identifiziert und der eigentliche Besitzer ermittelt werden. Grundsätzlich können aus medizinischer Sicht fast alle Haustiere mittels Transpondern gekennzeichnet werden. Bei Hunden, Katzen und Nagern wird der Chip an der linken Halsseite von einem Tierarzt mithilfe eines sterilen Einmal-Applikators unter die Haut appliziert.

Nach der Injektion des Transponders müssen die Haustiere in verschiedenen Datenbanken registriert werden. Zu den relevanten Datenbanken zählen beispielsweise das Deutsche Haustierzentralregister, TASSO und IFTA (internationale Registrierung). Lesegeräte sind in Tierheimen, vielen Tierarztpraxen, an Grenzstellen sowie in der Regel auf Ausstellungen, Turnieren und Auktionen verfügbar. [Katz 04]

8.7. Umweltmonitoring und Sensorik

Um den Zustand der Umwelt mithilfe von RFID zu überwachen, sind zwei Anwendungsformen denkbar:

- Tags werden an Tieren befestigt, durch in der Natur installierte Lesestationen abgelesen und unterstützen dadurch das Monitoring der Fauna. Hieraus können auch vielfältige Rückschlüsse auf andere Parameter des Umweltzustandes gezogen werden.
- Tags werden mit Sensoren versehen, die Umweltparameter wie Temperatur, Feuchtigkeit oder die Anwesenheit von Schadstoffen messen. Diese Sensor-Tags werden in feste oder mobile Objekte eingebracht und periodisch oder am Ende eines vorgesehenen Lebenszyklus ausgelesen.

Beide Ansätze sind noch nicht direkt für die Überwachung des Umweltzustandes in Gebrauch, jedoch gibt es verwandte Anwendungsgebiete, die die Praktikabilität dieser Verfahren demonstrieren.

So wird in Schweden seit 1997 im Fluss Vindelalven ein so genanntes „Lachsracet" (Lachsrennen) veranstaltet, an dem sich die Öffentlichkeit beteiligen kann. Hier wurden insgesamt 50 Lachsen mit einem Körpergewicht zwischen 4,4 und 11,5 Kilogramm Mikrotransponder mittels einer Kanüle unter die Haut injiziert. Die Transponder sind in biokompatibles Glas eingekapselt und haben einen Durchmesser von 2,2 und eine Länge von 11,5 Millimetern. Bei der Aufwanderung im Fluss werden die Lachse durch künstliche Engpässe, z. B. in Fischaufstiegsanlagen, geführt, wo dann ein Lesegerät mit einer Reichweite von 38 Zentimetern den Code des Fisches erfasst und aufzeichnet. Eine Batterie im Transponder ist nicht erforderlich. Durch das Vorbeischwimmen am Lesegerät werden die Kennzeichnungsdaten der Lachse, die nur einmal weltweit vergeben sind, registriert. So kann jedes einzelne Tier bei der Aufwanderung im Fluss Vindelalven unverwechselbar beim Passieren der Antennen registriert werden. Im Vindelalven wurden von der Quelle bis zur Mündung eine Serie von 25 Lesegeräten installiert. Für das „Lachsrennen", bei dem auf einzelne Tiere Wetten abgeschlossen werden können, wurden prominente Paten akquiriert. Unter den insgesamt 50 Lachspaten befinden sich neben Kronprinzessin Victoria beispielsweise die Transponder-Firma Trovan-Transponder/ DaimlerChrysler Industries, verschiedene Wasserkraftbetreiber, Kommunen, Banken, Sportartikel- und Maschinenbaufirmen, Fischereiverbände sowie Ericsson und Microsoft, die das Projekt mit finanziellen Mitteln unterstützen. [AOLm 04]

Chips mit Sensoren werden zunehmend zur Überwachung von spezifischen Umwelteinflüssen auf Transportgut eingesetzt. So bezieht beispielsweise ein Chiphersteller in Dresden temperaturempfindliche Fotochemikalien von einem Zulieferer aus Amsterdam. Um zu vermeiden, dass die Chemikalien während des Transports zu hohen Temperaturen ausgesetzt werden und verderben, setzt der Hersteller digitale Temperaturlogger ein. Diese werden in einen Transportbehälter gegeben und zeichnen die Temperaturentwicklung permanent auf. Nach dem Auslesen der Messdaten werden diese in ein XML-Format umgewandelt. Bei der Ankunft am Werk können die Werte unmittelbar in das MySAP PLM-System eingespeist werden. Verdorbene Ware kann dadurch sofort erkannt und zurückgewiesen werden. In etwaigen Schadensfällen kann darüber hinaus festgestellt werden, wo und durch wen die Schädigung verursacht wurde. [Fleis 02]

Bei der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA) ist ein Projekt in Vorbereitung, das den Einbau von RFID-Transpondern mit Sensoren in Brücken und Straßenbelägen zum Ziel hat, die mechanische Parameter und Umweltparameter erheben und die im Vorbeifahren abgelesen werden können.

Umweltmonitoring: RFID-Systeme können in Verbindung mit hochgradig miniaturisierten Sensoren dazu beitragen, die vielfältigen Phänomene der Umwelt in bislang nicht möglicher Genauigkeit zu beobachten.

8.8. Supply-Chain-Management: Automatisierung, Steuerung und Prozessoptimierung

Als Anwendungsgebiet von RFID-Systemen wird besonders häufig das Supply-Chain-Management genannt. In der Praxis ist „Supply Chain“ ein Netzwerk verschiedener Unternehmen, die zusammen arbeiten, um ein Produkt herzustellen und es zum Endkunden zu bringen. Dabei wird die Steuerung und Überwachung der Lieferkette in Zeiten von Lagerreduktionen und der Durchsetzung des „Just-in-Time“-Prinzips zum entscheidenden Erfolgsfaktor. Schwierigkeiten in der Produktion, beim Lieferanten oder während des Transports der Ware können gravierende Auswirkungen auf nachgelagerte Prozesse haben.

Steuerung von logistischen Prozessabläufen: RFID gilt als bedeutende Technologie in den Logistiknetzwerken der Zukunft. Voraussetzung ist die Definition gemeinsamer Standards sowie Lösungen, die Kosten und Nutzen adäquat auf die beteiligten Akteure der Wertschöpfungskette verteilen.

Vor diesem Hintergrund werden der RFID-Technologie hohe Chancen zugesprochen, durch die Schaffung von Transparenz eine effizientere Steuerung von logistischen Prozessabläufen zu ermöglichen. Im Kern geht es um die Erschließung von Rationalisierungspotenzialen innerhalb unternehmensübergreifender Wertschöpfungsketten bzw. um die Realisierung einer größtmöglichen Effizienz bei den übergreifenden Material-, Informations- und Geldmittelflüssen. Die RFID-Technologie ermöglicht es dabei, Produkte und Materialien in Echtzeit bis auf „Losgröße Eins“ über das gesamte Logistiknetzwerk hinweg zu verfolgen. An den Waren angebrachte Funketiketten liefern Daten zu Produkten und deren zeitlichen und räumlichen Bewegungen.

Nachdem die IT-Beratungsgruppe LogicaCMG im April 2004 den baldigen Durchbruch der RFID-Technologie angekündigt hat, beurteilt Booz Allen Hamilton in einer gemeinsamen Studie mit der Universität St. Gallen wenige Monate später die Marktchancen deutlich vorsichtiger. [Booz 04] Die empirische Studie „RFID – Technologie: Neuer Innovationsmotor für Logistik und Industrie?“ wurde weltweit mit über 30 führenden Großunternehmen aus Deutschland, Frankreich, Österreich, Schweiz, Großbritannien und den USA durchgeführt. Dabei standen Transport- und Logistikanbieter sowie Anwender der Automobilindustrie im Vordergrund. Den Untersuchungsergebnissen zufolge rechnet sich der Einsatz von RFID in denjenigen Branchen, in denen aufgrund hoher Nachweispflichten höchste Prozesssicherheit erforderlich wird und zudem ein geschlossener Logistikkreislauf die Wiederverwendbarkeit der bislang noch teuren Tags sicherstellt. Hierzu zählt in erster Linie die Automobilindustrie. Offene Systeme, die heute Grundlage der Anwendung im Handel und der Konsumgüterindustrie sind, kommen laut Studie dagegen aufgrund der hohen Investitionen in Tags, Reader-Infrastruktur und Systemintegration noch nicht auf ein ertragreiches Kosten-Nutzen-Verhältnis.

Vor dem Hintergrund des intensivierten Wettbewerbsdrucks ist der Einzelhandel derzeit dennoch bestrebt, flächendeckende Kostensenkungspotenziale mithilfe der RFID-Technologie in der Logistik zu realisieren. Insgesamt ergeben sich nach einer Studie von A.T.Kearney zwei Vorteile für die Warenwirtschaft: die Reduzierung von Beständen und damit die Reduzierung von Lager- und Kapitalbindungskosten sowie die Reduzierung von Personalkosten in den Geschäften und Lagern. [ATKe 04]

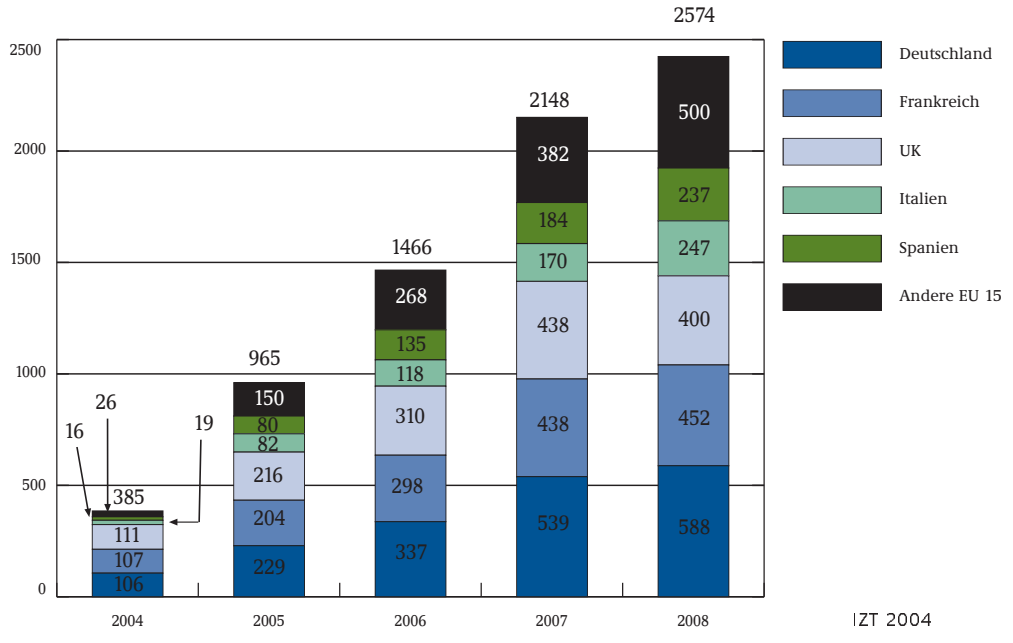
Nach einer aktuellen Prognose von Soreon Research zur Entwicklung des RFID-Marktes im Handelssektor soll der RFID-Markt innerhalb der kommenden vier Jahre von knapp 400 Mio. (2004) auf 2,5 Mrd. Euro (2008) in Europa insgesamt wachsen. Führender RFID-Markt in Europa soll Deutschland mit einem Volumen von knapp 600 Mio. Euro im Jahr 2008 sein. Die Analysten erwarten in den kommenden Jahren einen schnellen Preisverfall bei Transpondern durch die Verwendung preisgünstiger Materialien in der Produktion und die Realisierung von Einsparungen auf Basis von Massenfertigungsprozessen. Das geschätzte Marktwachstum wird unter anderem damit begründet, dass im Einzelhandel nicht nur Paletten und Kartons mit Tags aus-

gestattet werden sollen, sondern ab 2006 zunehmend auch einzelne Produkte am Point of Sale. Soreon Research geht davon aus, dass bis 2008 rund fünf Prozent aller in Europa über den Einzelhandel vertriebenen Produkte zusätzlich zum oder anstatt des Barcodes ein RFID-Tag erhalten werden. Der Einzelhandel in Europa (EU 15) vertreibt pro Jahr über 260 Mrd. Einzelprodukte. [Sore 04]

Die Entwicklungen im Handel können stellvertretend durch die globalen Treiber der RFID-Technologie Metro, Wal-Mart und Tesco beschrieben werden.

Der „Future Store“ der METRO Group Future Store Initiative – eine Kooperation der METRO Group mit SAP, Intel und IBM sowie weiteren Partnerunternehmen aus den Bereichen Informationstechnologie und Konsumgüterindustrie – bildet im nordrhein-westfälischen Rheinberg das Pilotprojekt für Supermärkte mit einem Bündel von technologischen Neuerungen. Es wird dort ein vollständig integriertes System in den Bereichen Lagermanagement, Information und Kasse umgesetzt. Langfristig besteht das Ziel darin, den Strukturwandel im Einzelhandel zu forcieren, weltweit einheitlich umsetzbare Standards für den Handel zu entwerfen und den gesamten Supermarkt drahtlos zu vernetzen. Auch die manuelle Barcode-Erfassung an der Kasse soll durch elektronische Erfassung im Einkaufswagen ersetzt werden. Antennen und Displays erfassen hierfür laufend den Warenbestand im Einkaufswagen und übermitteln ihn zuletzt an ein Zahlungssystem. Die Daten der RFID-Tags werden in einem Zentralrechner, dem so genannten RFID-Warenfluss-System, gesammelt. Alle Partner der Logistikkette – also Handel, Zentraleinkauf, Warenlager, Zwischenhändler und Hersteller – haben Zugriff auf diese Datenbank. In dem Pilotprojekt werden darüber hinaus auch vollautomatisierte „Selbstzahlerkassen“ erprobt: Der Kunde zieht seine Artikel über einen 360-Grad-Scanner und erfasst die Preise. Im Anschluss legt er die Produkte in eine Warentüte, die automatisch gewogen wird. Weicht das Ergebnis von dem der gescannten Erzeugnisse ab, erhält eine Mitarbeiterin bzw. ein Mitarbeiter am

Gesamtmarkt RFID im Handel nach Ländern EU 15 in Mio. Stück



n=70

Abbildung 8-1: Gesamtmarkt RFID im Handel nach Ländern EU 15 [Sore 04]

Informationsschalter eine automatische Meldung. Stimmt es überein, werden die Tags entwertet und die Produkte aus dem Warenwirtschaftssystem ausgebucht.

Das weltweit viertgrößte Handelsunternehmen Metro Group hat mittlerweile ein „RFID Innovation Center“ in Neuss eröffnet. Dort können sich Vertriebslinien, Technologiepartner und Lieferanten auf den Einsatz der RFID-Technologie vorbereiten, bevor sie bei Metro in die Prozesskette integriert wird. Die METRO Group wird vermutlich als weltweit erstes Handelsunternehmen die bislang üblichen Barcodes in der gesamten Lieferkette durch RFID-Transponder ersetzen. Die erste Phase des Roll-outs soll im November 2004 mit zunächst 20 Lieferanten beginnen und in Deutschland sukzessive auf rund 100 Lieferanten, acht Lager und 269 Standorte der Vertriebslinien Metro Cash & Carry, Real und Kaufhof erweitert werden. Den Planungen zufolge sollen bis Anfang 2006 insgesamt 300 Lieferanten mit Funkchips bestückte Paletten an die Verteilerzentren der Metro Group schicken. [Com 04b]

Die Einführung von RFID-Systemen im Metro Future Store hat bereits zu einer starken Verunsicherung von Verbraucherinnen und Verbrauchern geführt. Da die Metro-Gruppe ohne Information an die Verbraucherinnen und Verbraucher eine Payback-Kundenkarte mit Transponder ausgegeben hatte, übten Datenschschützer deutliche Kritik. Darüber hinaus kritisierte der „Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.“ (FoeBuD), dass die in den Preisetiketten enthaltenen RFID-Tags auch nach dem Verlassen des Ladens ihre Funktionsfähigkeit behielten. In der Folge wurde der BigBrotherAward in der Kategorie „Verbraucherschutz“ Ende des Jahres 2003 an die METRO-Gruppe für ihre „Future Store Initiative“ vergeben.

Die britische Supermarktkette Tesco hatte im vergangenen Jahr in ihrer Niederlassung in Cambridge sämtliche Packungen mit Rasierklingen der Marke Gillette Mach3 mit RFID-Tags ausgestattet. Das Gillette-Produkt „Mach3“ ist nach Angaben des Herstellers aufgrund des hohen Preises und der hohen Weiterverkaufsmöglichkeit „das begehrteste Objekt von britischen Ladendieben“. Das Unternehmen verliert durch Diebstahl ca. 30 Mio. US Dollar pro Jahr. [Hand 03, McKa 03] In dem mittlerweile abgeschlossenen Pilotprojekt ging es nach Aussagen von Tesco darum, Erkenntnisse im Bereich der Warenlogistik zu sammeln. Die Vereinigung „Consumers Against Supermarket Privacy Invasion and Numbering“ (CASPIAN) proklamierte allerdings, dass der Supermarktbetreiber zusätzlich auch eine Diebstahlsicherung eingebaut hatte und jeden Kunden heimlich fotografierte, der nach den mit Funk-Etiketten ausgestatteten Rasierklingenpackungen griff. Auch an den Kassen sollen Kameras postiert gewesen sein, die alle Kunden filmten, die mit einer RFID-gesicherten Ware den Laden verlassen wollten. CASPIAN rief daraufhin zu einem weltweiten Boykott gegen Gillette auf. [Heis 03]

Der US-amerikanische Big Player im Handel Wal-Mart hat sein Pilotprogramm zur Einführung von RFID-Etiketten in seinen Märkten und seinem Distributionsnetz mittlerweile nach eigenen Angaben ohne Probleme abgeschlossen und will die Technik auf breiterer Basis einsetzen. Zunächst hatte Wal-Mart die RFID-Technologie nur im Raum Dallas erprobt. Dabei wurden Kisten und Paletten für 21 Produkte von acht Lieferanten mit RFID-Tags versehen ins Auslieferungslager in Sanger, Texas, geliefert und anschließend von dort aus in sieben örtliche „Super Center“ weiterverteilt. Bis Januar 2005 will das Unternehmen die wichtigsten 100 Lieferanten auf die RFID-Technologie umstellen. Wal-Mart plant derzeit ein Gespräch mit 200 großen Zulieferern, um den weiteren Ausbau des RFID-Programms zu diskutieren. [Com 04a]

Auch in der industriellen Fertigung kommt die RFID-Technologie zur Optimierung der Geschäftsprozesse immer öfter zum Einsatz. Die Transponder werden auf den Fertigungsteilen angebracht und ermöglichen nicht nur

ein Auslesen von Daten, sondern auch das Beschreiben der Datenträger. In den Transpondern kann neben der Identität Objekts auch der momentaner Zustand (z. B. Bearbeitungsgrad, Qualitätsdaten), die Vergangenheit und die Zukunft (gewünschter Endzustand) des Objekts dokumentiert werden. Da in der Automobilindustrie ausschließlich auftragsgebunden produziert wird und zwei bestellte Fahrzeuge selten identisch sind, gehört die automatische Materialflussverfolgung in dieser Branche mittlerweile zu den wichtigsten Voraussetzungen für einen reibungslosen Betrieb. Auch der immer größer werdende Kostendruck in der Automobilindustrie bei der Produktion von neuen Baureihen fördert die ständige Reduzierung der Prozesskosten. Um dieses Ziel zu erreichen, wird einerseits der Automatisierungsgrad in Produktion und Logistik erhöht. Andererseits wird versucht, die Produktionsversorgung mit immer weniger Lagerhaltung vor Ort zu gewährleisten. RFID-Technologien werden vor allem im Bereich der chaotischen Fertigung eingesetzt.

So wird bei DaimlerChrysler in den USA und bei Volkswagen in Südafrika bereits in einem sehr frühen Fertigungsstadium jede Rohkarosserie mit einem Transponder ausgestattet, das für den gesamten Lebenszyklus am Fahrzeug verbleibt. Über die unverwechselbare Codierung wird der Fertigungsprozess gesteuert (Zuführung der Baugruppen, Farbwahl, Motorvariante etc.). Später kann die Transponder-Identifikationsnummer für die Identifikation des Fahrzeuges in den Servicestützpunkten, z. B. zur zweifelsfreien Information über die eingesetzten Baugruppenversionen für die Ersatzteilbeschaffung, genutzt werden. Neben der direkten Kennzeichnung der Fahrzeuge werden auch die Transportrahmen (Skids) mit Transpondern versehen. Hierfür ist der Einsatz von robusten Transpondern erforderlich, da die Transponder beim Einbrennen des Lackes immer wieder einer Temperatur von ca. 220°Celsius ausgesetzt werden. Bei der chaotischen Fertigung verschiedener Fahrzeugtypen auf einem Band ist die zweifelsfreie Identifikation der zugeführten Baugruppen von größter Wichtigkeit. Zu diesem Zweck werden bei Opel (Belgien) sowohl die Werkstückträger als auch die Aufnahmevorrichtungen mit Transpondern markiert. Als Vorteile ergeben sich: Keine Zuführung falscher Teile, Optimierung des Montage-Ablaufs, keine Umrüst- und Wartezeiten, effizientere Produktion sowie ein optimaler Informationsfluss an den Servicestationen. [Euro 04]

Zur Optimierung des logistischen Gesamtprozesses hat ein großer Automobilhersteller aus Baden-Württemberg in Zusammenarbeit mit einigen Zulieferern eine RFID-basierte Lösung für das Behältermanagement realisiert. Der Lieferant schreibt hierbei die behälterspezifischen Daten wie Stückzahl, Sachnummer, Behälteridentifikation etc. mit einem Schreiblesegerät auf den Transponder, der mit dem Ladungsträger fest verknüpft ist. Alle für den Hersteller relevanten Daten sind somit mit dem Behälter verbunden. Nach der Verladung der einzelnen Behälter auf einen Trailer werden die durch das Lesegerät gesammelten Daten zu einem Lieferschein integriert, der ebenfalls auf einen am Trailer befestigten Transponder geschrieben wird. Verlässt der Lkw das Werk des Lieferanten, werden die Lieferscheindaten automatisch von einer am Werksausgang installierten Antenne empfangen und als Vorabinformation an den Automobilbauer übermittelt. Gleichzeitig nutzt der Lieferant die elektronischen Lieferscheindaten, um den Bestand aus dem eigenen Lagerverwaltungssystem auszubuchen. Trifft der Lkw auf dem Werksgelände des Automobilherstellers ein, so werden die Lieferscheindaten bereits am Eingangstor von einer dort installierten Antenne ausgelesen und an das Wareneingangssystem übermittelt. Bei der Entladung des Lkw im Wareneingang werden die einzelnen Behälter durch eine an der Eingangsschleuse installierten Antenne ausgelesen. Diese Daten werden mit dem Lieferschein abgeglichen und an das Lagerverwaltungssystem übermittelt. Die vereinnahmten Behälter werden im Anschluss durch fahrerlose Transportsysteme an die einzelnen Verbauorte

weitertransportiert. Zur Gewährleistung der Anlagenverfügbarkeit wird vor jedem Transport eine Sicherheitsabfrage durchgeführt. Bei Ankunft an einer automatisierten Zelle wird vor dem Einsetzen der Behälter geprüft, ob tatsächlich der richtige Behälter mit dem entsprechenden Material eingesetzt werden kann. Fällt die Prüfung positiv aus, wird der Behälter eingesetzt, das fahrerlose Transportsystem bestätigt den ausgeführten Fahrauftrag und die vom Transponder ausgelesene Stückzahl wird aus dem Lagerverwaltungssystem ausgebucht. Durch den Einsatz von RFID konnten die Logistikkosten pro Jahr um 15 Prozent reduziert werden. Durch weitere Optimierungen in der Prozesskette sollen weitere zehn Prozent eingespart werden. Auswertungen aus den Behälterumläufen zeigten zudem, dass durch die genaue Bestimmung der erforderlichen Behälteranzahl eine Reduzierung der Investitionskosten bis zu zehn Prozent möglich ist. [Mose 04]

In der Automobilindustrie wird besonders das RFID-System OIS-P eingesetzt. OIS-P arbeitet im Frequenzbereich von 2,45 GHz. Es kann über Entfernungen von bis zu zehn Metern Daten schreiben und lesen und zeichnet sich durch seine Unempfindlichkeit gegenüber elektromagnetischen Störungen, seine robuste Ausführung und durch die hohe Hitzebeständigkeit (235°Celsius) der Datenträger aus. Die Datenträger haben bis zu 32 kByte Speicherplatz und sind für den durchgängigen Einsatz im Automobilbereich, d. h. für den Rohbau, Lack und in der Endmontage hervorragend geeignet. [Baum 04]

Auch im Motorsport werden von einigen Herstellern für die Gewährleistung einer kompletten Verfolgung der Fertigungsschritte und der Qualitätsüberwachung sowie zur Kontrolle bei Gewährleistungsansprüchen alle verwendeten Baugruppen mit Transpondern versehen (NITEC, Porsche). Dabei ist bei jedem Schritt der Produktion und Montage jegliche Information abrufbar, alle Schritte und Verarbeitungsdetails können gespeichert werden und stehen bei Bedarf zur Verfügung. [Euro 04]

RFID-Systeme werden zunehmend zur logistischen Optimierung von verkehrlichen Umschlagsplätzen wie Häfen oder Flughäfen genutzt. Auf dem Container Terminal Altenwerder (CTA) des Hamburger Hafens werden bereits heute Verladung, Zwischenlagerung und Weitertransport der standardisierten Stahlboxen nahezu lückenlos von einem Computerprogramm organisiert. Sieben halbautomatische Brücken am Kai platzieren die Container präzise auf 35 fahrerlose Lastwagen, die – über Transponder geleitet – jeweils einen der 11 Lagerblöcke ansteuern. Auf dem CTA-Gelände werden die Routen der automatischen Fahrzeuge über einen Computer geplant und gesteuert. Ein feinmaschiges Netz von im Asphalt integrierten Transpondern kontrolliert dabei ständig die Position der Fahrzeuge in dem 100 mal 1.400 Meter großen Areal zwischen Kai und Lager. Nahezu 12.000 Transponder sollen bis Ende 2005 im Asphalt versenkt sein und insgesamt 65 computergesteuerte, automatische Fahrzeuge mit stets aktualisierten Positionsdaten versorgen. [Enge 03]

Ein weiteres Anwendungsbeispiel im Bereich der industriellen Fabrikation praktiziert der Computerhersteller Dell. In den Produktionsstätten in China werden die Endfertigung, die Installation und Verpackung sowie die Auslieferung der Computer mithilfe von RFID-Tags gesteuert. Dell hat damit die Produktionseffizienz verbessert und – nach eigenen Angaben – sein Image als Innovationsunternehmen positiv gestärkt. [LePh 04]

Aber nicht nur die Optimierung, auch die Überwachung der Lieferketten ist ein Anwendungsgebiet, auf dem RFID neue Möglichkeiten bietet. Die TK-LOG Tiefkühllogistik ist seit Ende 2003 an einem Projekt zur Implementierung einer automatisierten Überwachung des Temperaturverlaufs von Waren in der Kühlkette unter Einsatz der RFID-Technologie beteiligt. Dabei soll der Transport- und Temperaturverlauf von Tiefkühlprodukten vom Hersteller bis in die Tiefkühlregale überwacht, kontrolliert und damit die Qualität der Produkte gewähr-

leistet werden. Projektpartner sind neben TK-LOG das massex systemhaus als IT-Anbieter sowie Langnese Iglo und Lupo. An jedem Transporthilfsmittel, jeder Palette oder jedem Rollbehälter werden aktive RFID-Transponder mit integrierten Temperatursensoren angebracht, die die Umgebungstemperaturen entlang der logistischen Kette bis zur Warenübergabe an den Kunden aufzeichnen. Die Planungen sehen vor, die Transponder am Warenausgang der TK-LOG mit einem elektronischen Paletteninhaltsschein zu beschreiben und mit der Temperaturaufzeichnung bei der Verladung zu beginnen. Mit einem RFID-tauglichen mobilen Datenerfassungsgerät sollen die Produkttemperaturen für jede Auftauklasse auf Basis der aufgezeichneten Umgebungstemperaturen simuliert und die Einhaltung der Kühlkette mittels Unterschrift auf dem elektronischen Display bestätigt werden. Für den Wareneingang wurden tragbare RFID-Lesegeräte zur Erfassung der Transponderdaten gewählt. Die Daten werden hierzu visualisiert. [MASS 04]

Gefördert durch das Bundesministerium für Wirtschaft und Arbeit untersucht das Institut für Handelsforschung an der Universität zu Köln (IfH) und das Forschungsinstitut für Management und Getränkelogistik (FIM) der Versuchs- und Lehranstalt für Brauerei in Berlin gegenwärtig die Chancen von RFID für die Mehrweglogistikoptimierung im Mittelstand. Dabei werden bis Juni 2005 die technischen Einsatzmöglichkeiten der RFID-Technologie bei der Distribution von Mehrwegkästen einer Brauerei zu Einzelhändlern sowie der Redistribution des Leergutes analysiert. In diesem Handlungsfeld ist vor allem die Pulk-Erfassung von Paletten relevant. Die mögliche Übertragbarkeit auf weitere Warengruppen und Handelsbranchen mit geschlossenen Kreisläufen bildet einen weiteren Untersuchungsschwerpunkt. Im Rahmen des Feldversuchs wurde der Frequenzbereich von 13,56 MHz gewählt. Die wieder beschreibbaren Transponder entsprechen dem ISO-15693-Standard und wurden mit individueller Kennzeichnung an den Getränkekästen angebracht. Die maximale Entfernung der Erfassungsgeräte liegt bei 1,5 Metern. Umflaufdaten wurden in mehreren zentralen Datenbanken erfasst. Die Anwendung arbeitet unabhängig von bestehenden IT-Systemen zur Warenwirtschaft oder Lagerverwaltung. Nur in der Brauerei erfolgte eine Anbindung an das Steuerungssystem der Abfülllinie. Die Daten der einzelnen Prozesspunkte können dann so ausgewertet werden, dass sich ein geschlossener Kreislauf für die Getränkekästen ergibt.

Das Fraunhofer-Institut für Fabrikbetrieb und -automatisierung (Fraunhofer IFF) hat an seinem Standort in Magdeburg ein Test- und Entwicklungslabor für RFID-Technologien aufgebaut. Das im Juni 2004 eröffnete „LogMotionLab“ offeriert der Industrie, dem Handel und Dienstleistern eine Vielzahl an RFID-Technologien und -Systemen zum praxisnahen Testen. Auch werden Möglichkeiten vorgestellt, wie mithilfe der RFID-Technik logistische Prozesse überwacht und gesteuert werden können. Auf Wunsch können Interessenten mobile Komponenten des Labors ausleihen. Das Ziel des Labors besteht darin, insbesondere für Logistikprozesse RFID-Technologien auf ihre Praxistauglichkeit zu testen, anzupassen und schließlich zu bewerten. Daher sind in dem Labor auch zwei Materialflusssysteme verfügbar, die Waren auf einem Förderband und auf Metallrollen bewegen. Auf dieser 15 Meter langen Strecke bewegen sich Objekte mit Transponder in hoher Geschwindigkeit, wenn nötig auch im tagelangen Dauertest. Untersucht wird beispielsweise, wie viele Daten sich bei welchen Geschwindigkeiten noch korrekt erfassen lassen und wie die Transponder auf Temperatur, Vibration, Stöße, chemische Substanzen und elektromagnetische Einflüsse reagieren. [Mylo 04]

9. Fördernde und hemmende Faktoren für den Einsatz von RFID

Die RFID-Technologie wird seit einigen Jahrzehnten für verschiedenste Zwecke experimentell eingesetzt und konnte sich in ausgewählten Teilbereichen am Markt durch setzen. Vielfältige neue Anwendungen werden im Rahmen von Pilotprojekten erprobt. In Abhängigkeit zu den unterschiedlichen Einsatzumgebungen und Rahmendaten wird die gesamte Bandbreite von RFID-Systemen unterschiedlicher technologischer Komplexität eingesetzt. Dabei werden generalisierbare fördernde und hemmende Faktoren deutlich, die die weitere Verbreitung von RFID-basierten Anwendungen beeinflussen. RFID-Systeme stehen mit anderen automatischen Identifikationssystemen wie Barcode, OCR und Chipkarte im Wettbewerb. Die einzelnen Verfahren unterscheiden sich in zentralen Leistungsparametern der Auto-ID-Systeme (siehe Tabelle 9.1.).

Auch die Ergebnisse der im August 2004 im Rahmen dieser Studie durchgeführten Online-Befragung verweisen auf deutliche Unterschiede in der Bewertung der Stärken und Schwächen der Auto-ID-Techniken Barcode, Chipkarte (kontaktbehaftet), OCR und RFID im Vergleich. Die befragten Expertinnen und Experten haben dabei die

Parameter/System	Barcode	OCR	Chipkarte	RFID
Typische Datenmenge (Byte)	1 ~ 100	1 ~ 100	16 ~ 64k	16 ~ 64k
Datendichte	gering	gering	sehr hoch	sehr hoch
Maschinenlesbarkeit	gut	gut	gut	gut
Lesbarkeit durch Personen	bedingt	leicht	unmöglich	unmöglich
Einfluss von Schmutz/ Nässe	sehr stark	sehr stark	möglich (Kontakte)	kein Einfluss
Einfluss von (opt.) Abdeckung	totaler Ausfall	totaler Ausfall	möglich	kein Einfluss
Einfluss von Richtung und Lage	gering	gering	sehr hoch (eine Steckrichtung)	kein Einfluss
Abnutzung/ Verschleiß	bedingt	bedingt	bedingt	kein Einfluss
Anschaffungskosten/ Leseelektronik	sehr gering	mittel	gering	mittel
Unbefugtes Kopieren/ Ändern	leicht	leicht	schwierig	schwierig
Lesegeschwindigkeit (inkl. Handhabung des Datenträgers)	gering ~ 4 s	gering ~ 3 s	gering ~ 4 s	sehr schnell ~ 0,5 s
Maximale Entfernung zwischen Datenträger und Lesegerät	0 ... 50 cm	< 1 cm (Scanner)	direkter Kontakt	0 ... 5 m, Mikrowelle

Tabelle 9-1: Eigenschaften ausgewählter Auto-ID-Systeme im Vergleich [in Anlehnung an Fink 02, in Teilen modifiziert]

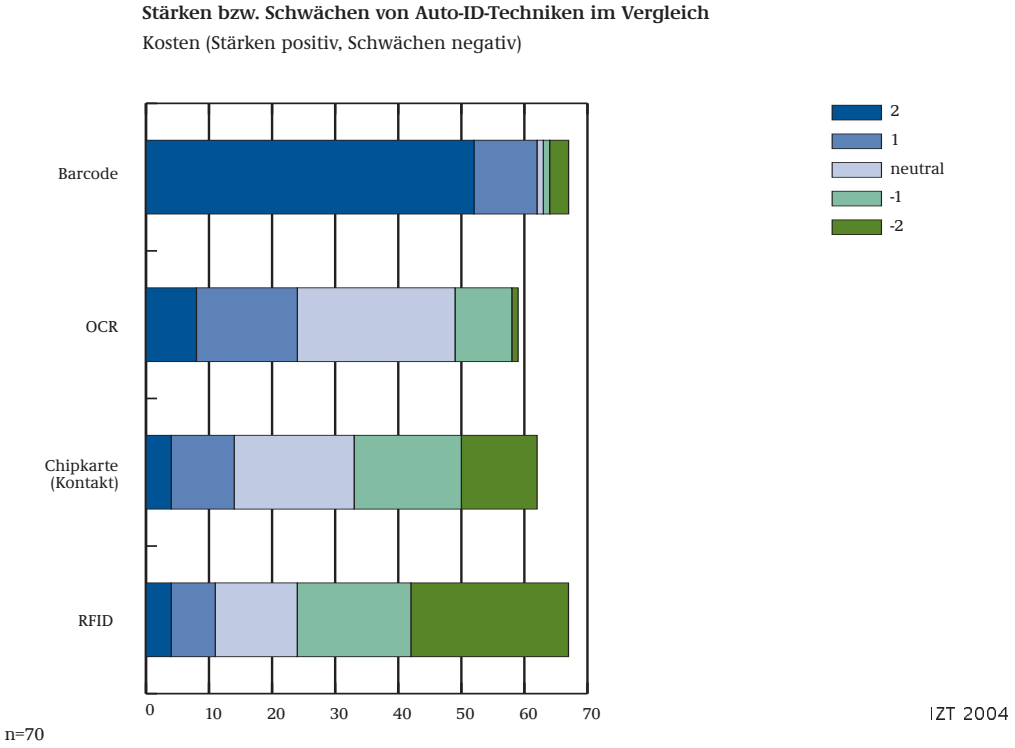


Abbildung 9-1: Wesentliche Schwächen bzw. Stärken von Auto-ID-Techniken im Vergleich – Kosten für die Auto-ID-Technik

abgefragten Techniken im Hinblick auf die Parameter „Kosten“, „Leistungsfähigkeit“, „Kosten-Nutzen-Verhältnis“, „Funktionssicherheit“ und „Informationssicherheit“ in einem Spektrum von „+2“ (deutliche Stärke) bzw. „+1“ (Stärke) über „0“ (neutral, d. h. weder Stärke noch Schwäche) bis hin zu „-1“ (Schwäche) bzw. „-2“ (deutliche Schwäche) bewertet (siehe Abbildungen 9-1 bis 9-5).

Im Vergleich zu anderen Auto-ID-Systemen zeichnen sich RFID-Systeme vor allem durch eine hohe Leistungsfähigkeit aus. Hierzu zählen beispielsweise die typische zu verarbeitende Datenmenge und Datendichte, die Lesbarkeit und Lesegeschwindigkeit des Datenträgers durch Maschinen oder auch die Resistenz des Datenträgers gegen äußere Einflüsse wie Nässe und Schmutz. Von den befragten Expertinnen und Experten bewerten 93 Prozent die Leistungsfähigkeit von RFID-Systemen als Stärke und immerhin zwei Drittel der Befragten (67 Prozent) als deutliche Stärke (siehe Abbildung 9-2).

RFID-Systeme verfügen über den Vorteil, dass kein Sichtkontakt zwischen Transponder und Lesegerät erforderlich ist und dass Erfassungen im Pulk sowie die Lesbarkeit durch verschiedene Materialien hindurch möglich sind. Darüber hinaus sind einige Transpondertypen mehrfach neu beschreibbar. Hierdurch ergibt sich ein größerer Einsatzbereich im Vergleich zur Barcode-Technik (z. B. Eignung für die Mehrweglogistik).

Von den befragten Expertinnen und Experten werden, wie in den Abbildungen 9-4 und 9-5 verdeutlicht, zudem die Parameter Funktionssicherheit und Informationssicherheit von RFID-Systemen im Vergleich zu den anderen abgefragten Auto-ID-Techniken Barcode, kontaktbehaftete Chipkarte und OCR als wesentliche Stärke hervorgehoben (Stärke insgesamt: 79 bzw. 80 Prozent, deutliche Stärke: 41 bzw. 30 Prozent). Vor allem dieses Leistungsspektrum fördert die Nutzung von RFID-Systemen.

9. Fördernde und hemmende Faktoren für den Einsatz von RFID

Zu den Nachteilen der RFID-Technologie zählen neben den hohen Kosten für die Anschaffung und Implementierung der RFID-Systeme der bislang geringe Standardisierungsgrad und die Unsicherheit, ob RFID von den unternehmerischen Nutzern zukünftig akzeptiert wird und ob die RFID-Systeme mit den bestehenden EDV-Systemen und –Strukturen wirtschaftlich und technisch erfolgreich verknüpft werden können. So bewerten z. B. von den befragten Expertinnen und Experten insgesamt 66 Prozent die anfallenden Kosten als Schwäche der RFID-Technik, immerhin 33 Prozent sogar als deutliche Schwäche (siehe Abbildung 9-1). Aufgrund der hohen Leistungsfähigkeit von RFID werden die hohen Kosten in der Einschätzung des Kosten- Nutzen-Verhältnisses relativiert. Das Kosten-Nutzen-Verhältnis wird von 29 Prozent als Schwäche und von 11 Prozent der Befragten als deutliche Schwäche bewertet (siehe Abbildung 9-3).

Die Stärken des Barcodes liegen hingegen vor allem in den relativ niedrigen Kosten und dem günstigen Kosten-Nutzen-Verhältnis. So bewerten 89 Prozent der befragten Expertinnen und Experten die erforderlichen Kosten für den Einsatz des Barcodes als Stärke und 74 Prozent der Befragten als deutliche Stärke im Vergleich zu Chipkarte, OCR und RFID (siehe Abbildung 9-1). Das Kosten-Nutzen-Verhältnis der Barcode-Technik wird von knapp drei Vierteln der Befragten als Stärke bewertet (79 Prozent), dabei von knapp der Hälfte der Befragten (49 Prozent) als deutliche Stärke (siehe Abbildung 9-3).

Weitere Vorteile des Barcodes sind der vergleichsweise hohe Grad der Standardisierung und die hohe Akzeptanz bei den Nutzern. Zu den Nachteilen zählen, dass der Barcode eine direkte Sichtverbindung erfordert, vergleichsweise anfällig gegen Verschmutzungen und unflexibel im Hinblick auf nachträgliche Änderungen ist. Die Leistungsfähigkeit der Barcode-Technik wird dennoch nur von 27 Prozent der Befragten als Schwäche und von 11 Prozent als deutliche Schwäche bewertet (siehe Abbildung 9-2).

Als wichtigster Vorteil der OCR-Systeme wird die Möglichkeit genannt, die Daten zur Kontrolle oder im Notfall auch visuell erfassen zu können. Die Untersuchungsergebnisse der Online-Befragung zeigen, dass der OCR-Technik im Vergleich zu den anderen angesprochenen Auto-ID-Techniken insgesamt die geringsten Stärken zugesprochen werden. Allerdings werden die erforderlichen Kosten für den Einsatz der OCR-Technik von 59 Prozent der Befragten als Stärke und von 23 Prozent als deutliche Stärke bewertet (siehe Abbildung 9-1). Als Nachteil wird vor allem die vergleichsweise geringe Leistungsfähigkeit von OCR-Systemen erachtet. So bewerten 36 Prozent der Befragten die Leistungsfähigkeit der OCR-Technik als Schwäche und 17 Prozent als deutliche Schwäche (siehe Abbildung 9-2).

Einer der Vorteile von kontaktbehafteten Chipkarten liegt darin, dass die in ihr gespeicherten Daten gegen unerwünschte (Lese-) Zugriffe und Manipulation geschützt werden können. Die Luftschnittstelle entfällt. Die Untersuchungsergebnisse der Online-Befragung veranschaulichen, dass der kontaktbehafteten Chipkarte ein vergleichsweise hoher Grad an Informationssicherheit zugesprochen wird. So bewerten 64 Prozent der Befragten den Parameter „Informationssicherheit“ der Chipkarte als Stärke, 30 Prozent sogar als deutliche Stärke (siehe Abbildung 9-5). Auch die Funktionssicherheit der kontaktbehafteten Chipkarte wird im Vergleich der abgefragten Auto-ID-Techniken deutlich positiv bewertet. Über die Hälfte der Befragten bewerten die Funktionssicherheit der Chipkarte als Stärke (56 Prozent), ein Fünftel (20 Prozent) der Befragten als deutliche Stärke (siehe Abbildung 9-4).

Nachteilig ist dagegen die Anfälligkeit der Kontakte für Abnutzung, Korrosion und Verschmutzung. Vor allem häufig benutzte Lesegeräte und Chipkarten verursachen hohe Kosten durch Ausfall. Zudem können frei zugängliche Lesegeräte (z. B. Telefonzellen) nicht gegen Sabotage geschützt werden. 41 Prozent der befragten Expertinnen und

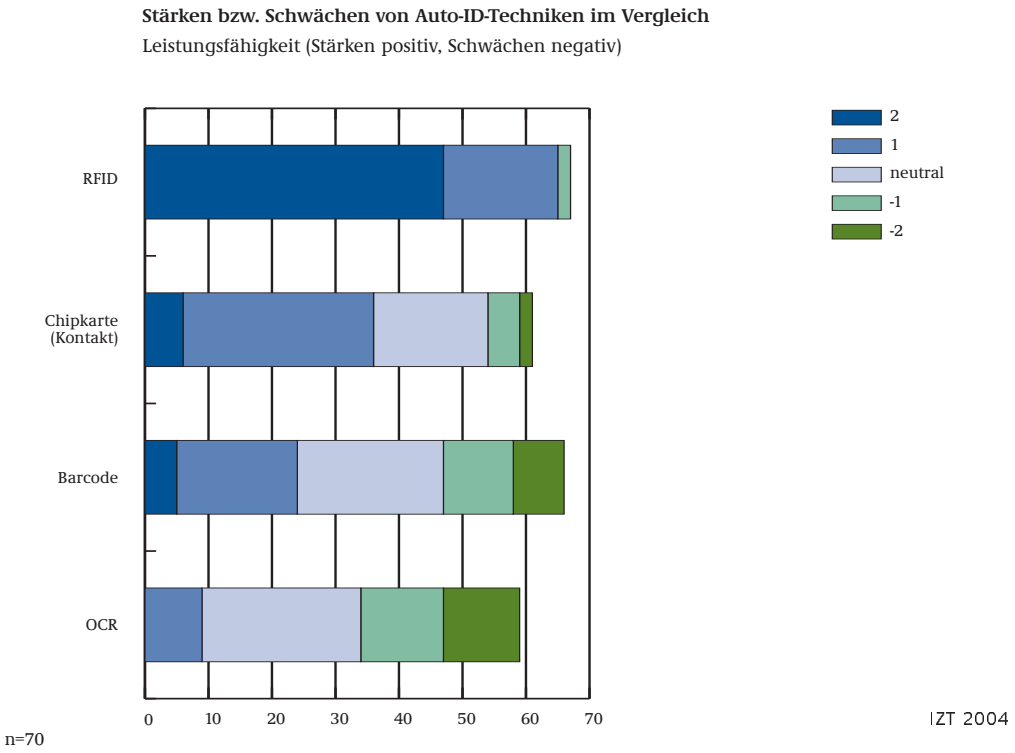


Abbildung 9-2: Wesentliche Schwächen bzw. Stärken von Auto-ID-Techniken im Vergleich – Leistungsfähigkeit

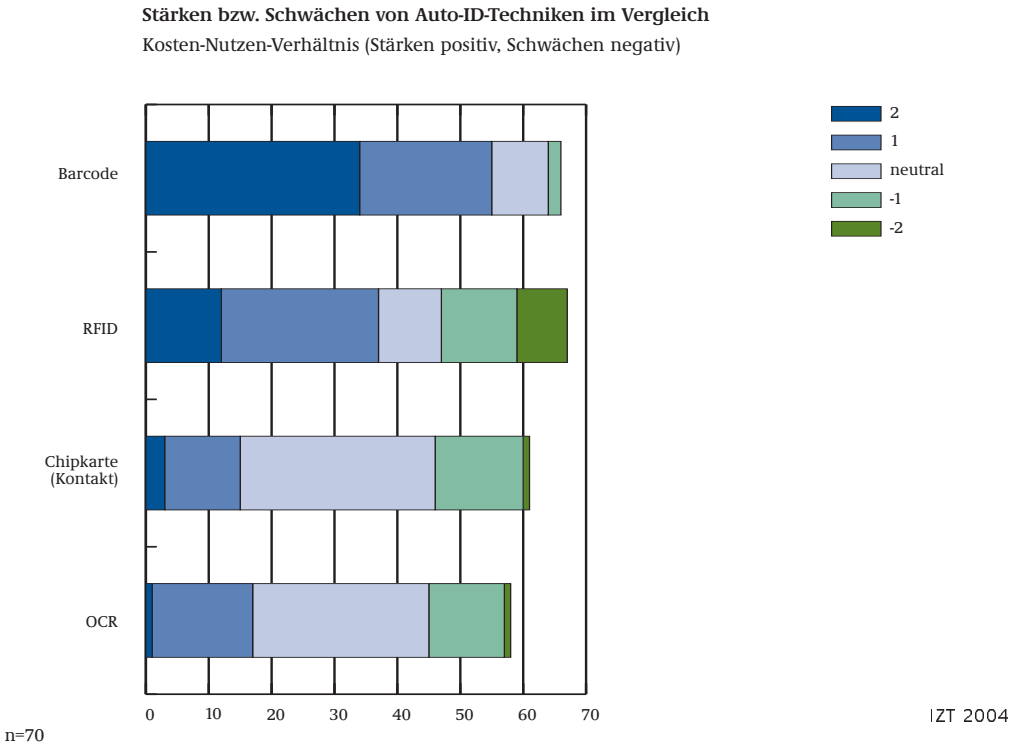


Abbildung 9-3: Wesentliche Schwächen bzw. Stärken von Auto-ID-Techniken im Vergleich – Kosten-Nutzen-Verhältnis

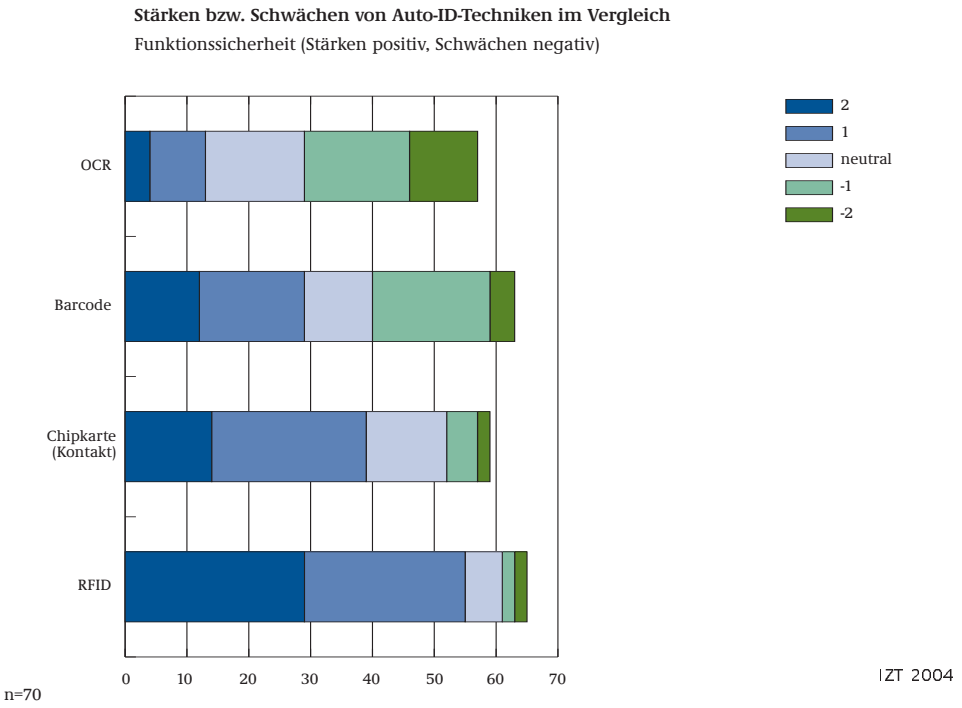


Abbildung 9-4: Wesentliche Schwächen bzw. Stärken von Auto-ID-Techniken im Vergleich - Funktionssicherheit

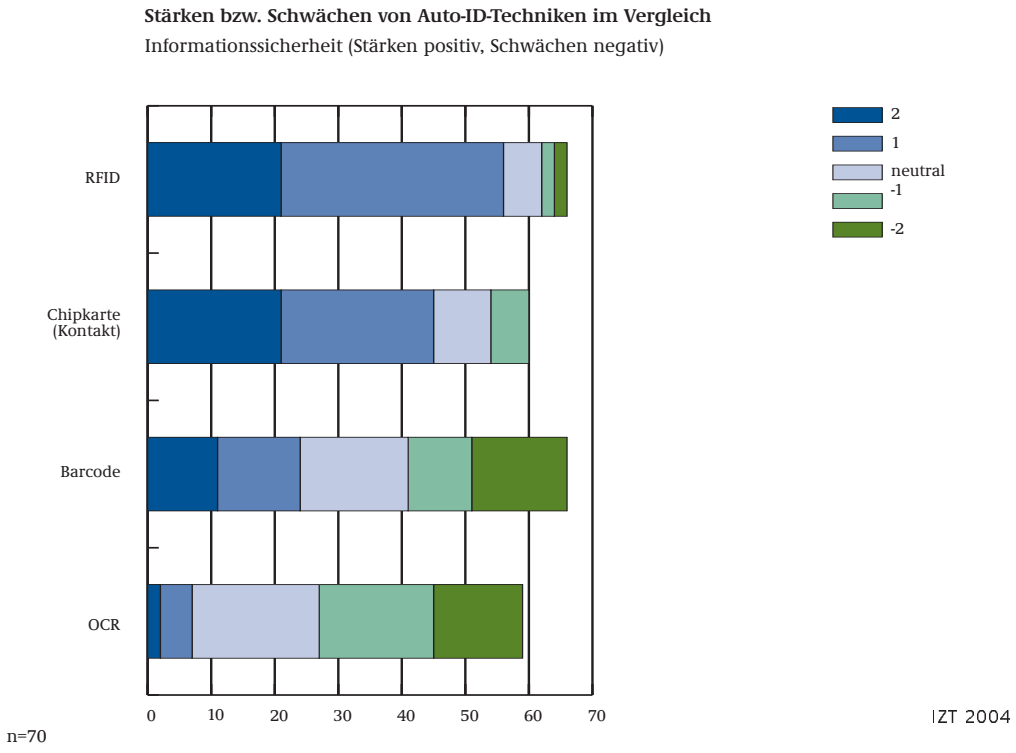


Abbildung 9-5: Wesentliche Schwächen bzw. Stärken von Auto-ID-Techniken im Vergleich – Informationssicherheit

Experten bewerten zudem die erforderlichen Kosten für den Einsatz der kontaktbehafteten Chipkarte im Vergleich der abgefragten Auto-ID-Systeme als Schwäche, davon 17 Prozent als deutliche Schwäche (siehe Abbildung 9-1).

Die besonderen Funktionalitäten der Transpondertechnologie tragen wesentlich zur Erschließung der ökonomischen Potenziale bei. Vor allem die High-End-Transponder führen zu wesentlich besseren Automatisierungsmöglichkeiten in der Massenproduktion sowie zu höheren Datenübertragungsraten, die wiederum komplexere Anwendungen ermöglichen. Die Transponder-Technologie ist nahezu beliebig integrierbar (z. B. in Produkte, Verpackungen, Ladeeinheiten, Ladungen). Die größere Speicherkapazität, die Möglichkeit der Mehrfach-Applikation sowie nicht zuletzt der Nutzerkomfort zählen zu den Vorteilen kontaktloser RFID-Systeme. Aber auch ökonomische Rahmenbedingungen und gesetzliche Vorschriften fördern den Einsatz von RFID-Systemen:

Ökonomische Rahmenbedingungen
Aus ökonomischer Perspektive unterstützt der verschärfte Kosten und Wettbewerbsdruck auf internationalen Märkten den breiteren Einsatz von RFID-Systemen. Chancen lassen sich vor allem in Anwendungsgebieten und Branchen ausmachen, in denen Produktivitätsfortschritte durch eine verstärkte Automatisierung erzielt werden sollen. Insgesamt wird durch den Einsatz von RFID die Transparenz der Supply Chain erhöht und die Transaktionskosten für die Unternehmen verringern sich. Aber auch die zunehmende Verflechtung der Märkte fördert den Einsatz von RFID-Systemen. Dabei geht es im Kern um die Erschließung von Wettbewerbsvorteilen durch die systematische Erfassung und Steuerung der komplexen logistischen Zusammenhänge im Wertschöpfungsnetz. Nicht zuletzt soll die RFID-Technologie die Massenproduktion von Produkten unterstützen, die an spezielle Kundenwünsche angepasst werden, indem sich die Maschinen automatisch an die jeweiligen Produktionsanforderungen anpassen (Mass Customization). Damit ist nicht nur die Spezifikation des fertigen Produktes verbunden, sondern auch Detailinformationen dazu, wie einzelne Produktionsmaschinen konfiguriert werden müssen, um dieses spezifische Produkt zu erzeugen.

Gesetzliche Vorschriften
RFID-Anwendungen werden für Unternehmen aufgrund der steigenden Anzahl gesetzlicher Vorschriften in den verschiedensten Einsatzgebieten interessant. So rücken RFID-Lösungen im Zuge von EU-Vorschriften immer stärker in den Blickpunkt der ökonomischen Akteure aus Logistik und Landwirtschaft einschließlich aller vor- und nachgelagerten Stufen der Wertschöpfung (z. B. Rückverfolgbarkeit von Lebensmitteln, Seuchenschutz). Zunehmend strenge Anforderungen an die Qualität, Sicherheit und Dokumentation forcieren darüber hinaus Branchen übergreifend den Einsatz von RFID-Systemen für die Wartung technischer Einrichtungen (z. B. sicherheitsrelevante Bauteile in Klima- und Lüftungsanlagen). Auch die Kennzeichnung chemischer Rohstoffe unterliegt einer Vielzahl von Auflagen und wird daher in fortschreitendem Maße durch RFID-Systeme unterstützt: Neben auch in anderen Segmenten üblichen Produktbezeichnungen und Mindesthaltbarkeitsangaben sind beispielsweise Gefahrstoff-, Lager- und Transporthinweise sowie eine detaillierte Inhaltsangabe zwingend vorgeschrieben.

Dagegen wird der breite Einsatz von RFID-Systemen derzeit durch folgende Faktoren gehemmt:

Technische Probleme
Beim Einsatz von RFID-Systemen treten verstärkt Schwierigkeiten bei der Datenerfassung in der Nähe von Metall oder Flüssigkeiten in einzelnen Frequenzbereichen sowie Probleme bei der Erkennung von Gebinden auf. Mehr als zwei Drittel bzw. knapp die Hälfte der im Rahmen dieser Studie befragten Expertinnen und Experten von RFID-Systemen benannten diese Probleme als „sehr hohes“ bzw. „hohes Hemmnis“ (siehe Abbildung 9-6).

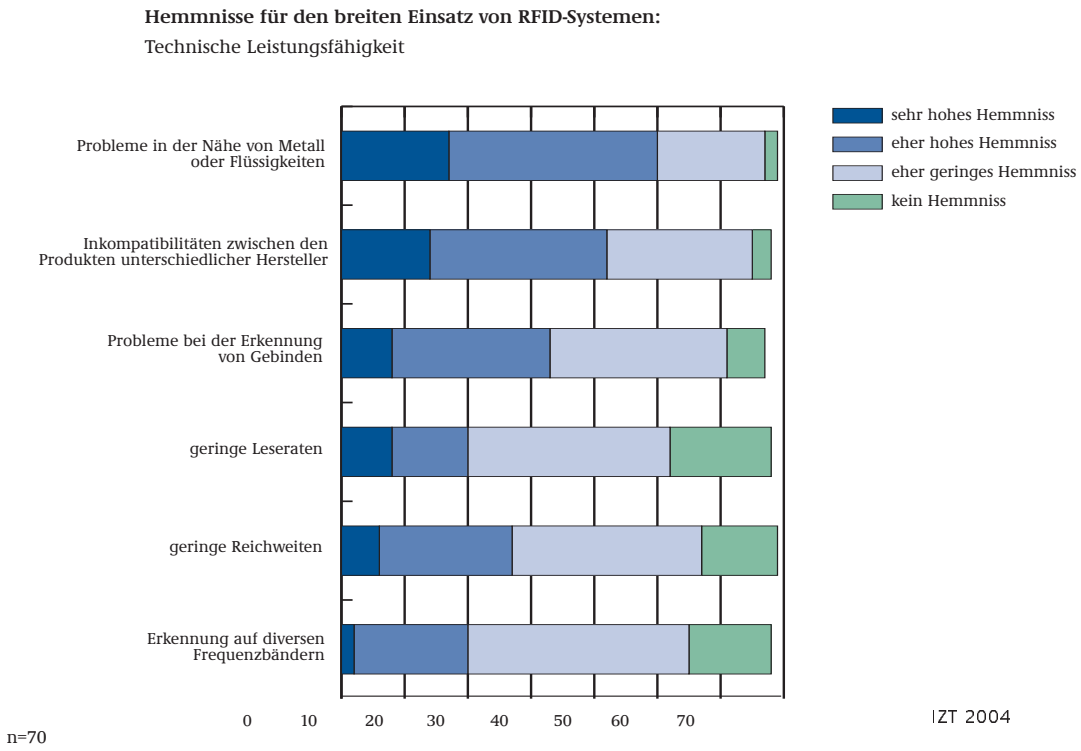


Abbildung 9-6: Hemmnisse für den breiten Einsatz von RFID-Systemen: Technische Leistungsfähigkeit

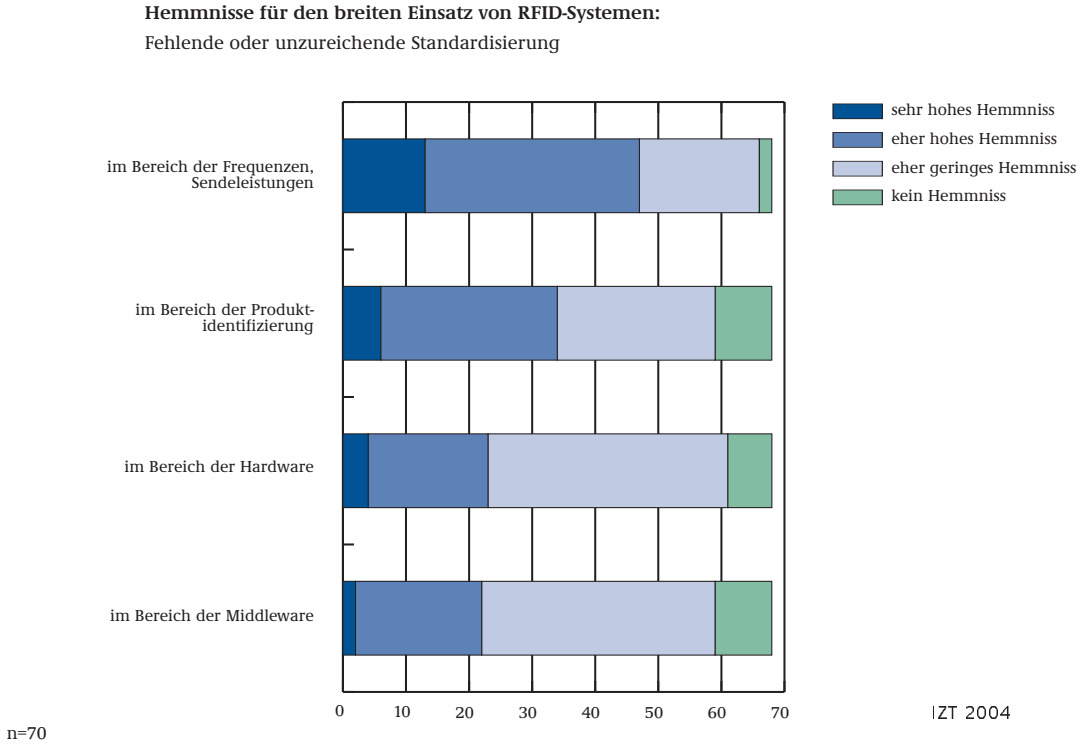


Abbildung 9-7: Hemmnisse für den breiten Einsatz von RFID-Systemen: Fehlende oder unzureichende Standardisierung

Lange Auslesezeiten von mehreren Sekunden, Abschattungseffekte zwischen fast gleichartigen Signalfolgen, Funkinterferenzeffekte sowie Frequenzverschiebungen durch zufällig aufliegendes Metall werden ebenfalls als Hemmnisse benannt. Diese Effekte müssen weiterhin bei der Auswahl der RFID-Lösung gezielt berücksichtigt werden.

Unzureichende Standardisierung
Obwohl die internationale Standardisierung von RFID fortschreitet, fehlen in Teilbereichen weiterhin weltweite Standards, was die Implementierung überbetrieblicher Anwendungen deutlich erschwert. Eine weltweite Standardisierung ist eine zwingende Voraussetzung dafür, dass Hard- und Softwarehersteller sich auf verlässliche technische Rahmenbedingungen verlassen können und die derzeitigen Probleme von Anwendern bei der Nutzung von Komponenten unterschiedlicher Hersteller behoben werden. Vor diesem Hintergrund ist das Fehlen von Standards aus ökonomischer Perspektive das vorrangige Hindernis.

Immerhin 60 Prozent der im Rahmen dieser Studie Befragten sind der Auffassung, dass Inkompatibilitäten zwischen Transpondern und Lesegeräten unterschiedlicher Hersteller auftreten (siehe Abbildung 9-6).

Heute existieren auf dem Markt jeweils herstellerabhängige Einzellösungen, die erforderliche Software und Hardware ist in vielen Fällen nicht zu anderen Lösungen kompatibel. Vergleichbares gilt im Bereich der Datenmodelle: Obwohl – vor allem in Nordamerika – herstellerübergreifend der so genannte Electronic Product Code (EPC) favorisiert wird, ist auch in diesem Teilbereich der RFID-Technologie die Standardisierung noch nicht abgeschlossen.

Ein weiteres Handlungsfeld bildet die Frequenzregulierung. Derzeit müssen beispielsweise die Waren multinationaler Konzerne mit Transpondern unterschiedlicher Frequenzbereiche ausgestattet werden. Obwohl Transponder im UHF- und Mikrowellenbereich an Bedeutung gewinnen, stehen die hierfür benötigten Frequenzen in Japan und in Teilen von Europa nicht für den kommerziellen Einsatz zur Verfügung.

Zwei Drittel der befragten RFID-Expertinnen und -Experten bezeichnen die fehlende oder unzureichende Harmonisierung im Bereich der Frequenzen bzw. Sendeleistungen als hohes oder sehr hohes Hemmnis (siehe Abbildung 9-7).

Hohe Transponder- und Integrationspreise
Im Jahr 2003 lag der durchschnittliche Preis eines Transponders auch aufgrund der vergleichsweise niedrigen Produktionsstückzahlen bei 91 Eurocent für einen passiven HF-Transponder und bei 57 Eurocent für einen passiven UHF-RFID-Transponder [Ward 04]. Für viele Unternehmen werden passive Transponder erst ab einem Stückpreis von zehn Eurocent interessant [Höni 03]. Auch wenn Marktforscher davon ausgehen, dass sich der Preis pro passivem Transponder in der näheren Zukunft auf deutlich unter zehn Eurocents reduziert, hemmen derzeit die hohen Kosten pro Tag den RFID-Einsatz für Massenprodukte [Booz 04].

Die Anschaffungskosten pro Transponder und pro Lesegerät sind nach Ansicht von knapp einem Drittel der im Rahmen dieser Studie Befragten (jeweils 29 Prozent) der größte hemmende Faktor auf der Kostenseite (siehe Abbildung 9-8). Neben diesen Anschaffungskosten sind erhebliche Investitionen in die Infrastruktur des RFID-Systems zu tätigen. Dazu zählen Kosten für die Sammlung, Verarbeitung und Auswertung der gesammelten Daten sowie die Bereitstellung eines entsprechenden Rechner Netzwerks. Hinzu kommen Kosten für die Reorganisation der Geschäftsprozesse. Typischerweise wird es gerade in der Einführungsphase auch zu einer Parallelität von RFID- und traditionellen Systemen kommen. Diese Rahmenbedingungen hemmen insbesondere bei denjenigen kleinen und mittelständischen Unternehmen die Einführung von RFID-Systemen, die bereits über ein Auto-ID-System verfügen.

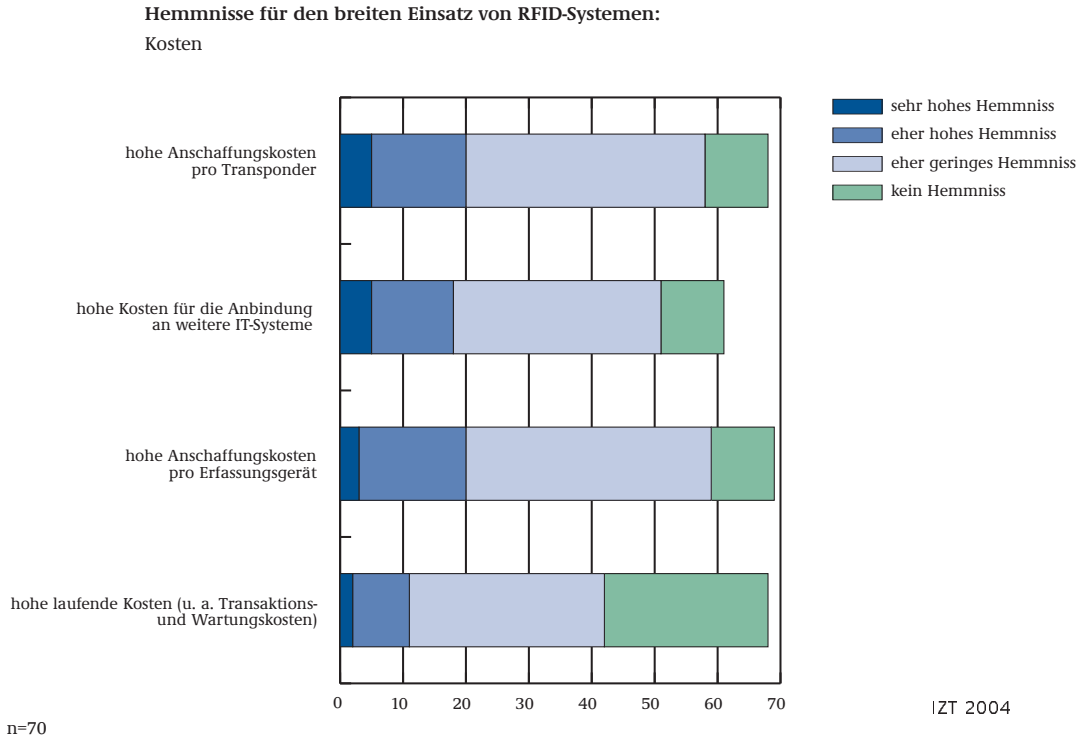


Abbildung 9-8: Hemmnisse für den breiten Einsatz von RFID-Systemen: Kosten

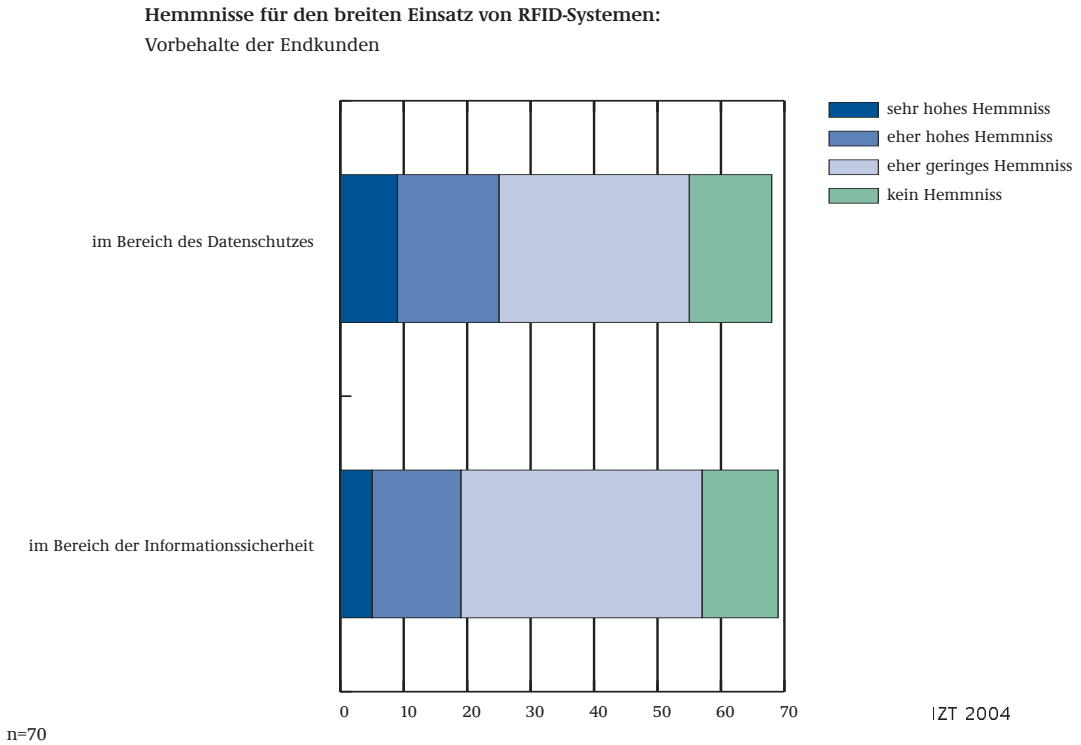


Abbildung 9-9: Hemmnisse für den breiten Einsatz von RFID-Systemen: Vorbehalte der Endkunden

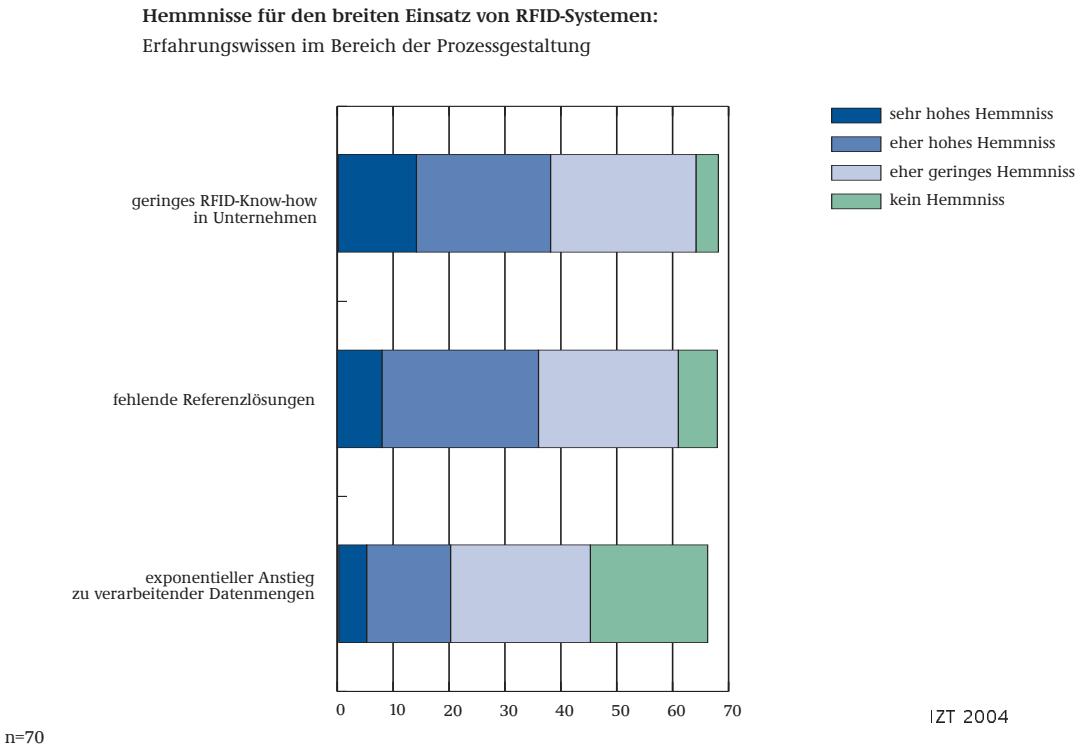


Abbildung 9-10: Hemmnisse für den breiten Einsatz von RFID-Systemen: Erfahrungswissen im Bereich der Prozessgestaltung

Informationssicherheit/Datensicherheit
RFID-Systeme schaffen eine neue Dimension der Verfügbarkeit zuverlässiger Daten über Objektbewegungen. Sie verbessern damit die Kongruenz zwischen der virtuellen Welt der Daten und der Welt der realen Objekte, auf die sich die Daten beziehen. Ökonomische Prozesse werden diese Kongruenz nicht nur nutzen, sondern zunehmend auch als gegeben voraussetzen. Eine logische Konsequenz dieser Entwicklung ist die wachsende Abhängigkeit der Prozesse von der Integrität der RFID-Daten. Damit sind offensichtliche Risiken verbunden, die nur durch ausreichende Informations- bzw. Datensicherheit begrenzt werden können. Ob diese gewährleistet werden kann, ist heute nur schwer einzuschätzen, da die weitere Entwicklung von RFID noch relativ offen ist.

Bisherige Erfahrungen im Bereich der IT-Sicherheit zeigen allerdings, dass auch als sicher geltende Verfahren im Laufe der wissenschaftlich-technischen Entwicklung unsicher werden können, weil zuvor unbekannte Lücken entdeckt werden. Aufgrund der hohen Investitionen in die RFID-Technologie, die eher als Infrastruktur denn als Einzelanwendung zu betrachten ist, und der Tatsache, dass die wesentlichen Datenträger (die Tags) in großer Zahl verteilt sind, dürften nachträgliche Veränderungen der Sicherheitsverfahren in RFID-Systemen einen sehr hohen Investitionsaufwand erfordern. Praktisch werden sie nur bei einem Generationswechsel der Technologie realisierbar sein. Die latente Gefahr der Entwertung beträchtlicher Infrastrukturinvestitionen aufgrund von Sicherheitsproblemen ist daher ein hemmender Faktor für RFID-Systeme.

Offene Fragen im Bereich von Datenschutz und Privatsphäre
Der fortschreitende Einsatz von RFID-Systemen wird in der Öffentlichkeit sowie in den Medien mit großer Aufmerksamkeit verfolgt und kontrovers diskutiert. Aus gesellschaft-

licher Perspektive spielen die Gewährleistung der Privatsphäre und Aspekte des Datenschutzes in der Auseinandersetzung eine zunehmend wichtige Rolle (Stichworte „gläserner Kunde“ und „gläserner Bürger“). Bürgerrechtsorganisationen haben ein gemeinsames Positionspapier zum Einsatz von RFID und den damit verbundenen Gefährdungen für den Datenschutz herausgebracht [FoeB 04].

Die unterzeichnenden Organisationen erkennen an, dass es auf Seiten der Wirtschaft berechtigte Interessen für den Einsatz von RFID geben kann, fordern aufgrund der erheblichen Gefährdungen jedoch Händler und Hersteller auf, zunächst im Zuge eines freiwilligen Moratoriums auf den Einsatz von RFID bei Konsumgütern zu verzichten, bis in einer umfassenden Technikfolgenabschätzung alle Risiken und mögliche Gegenstrategien erarbeitet worden sind.

Von den befragten RFID-Expertinnen und Experten werden Vorbehalte der Endkunden im Bereich des Datenschutzes von etwas mehr als einem Drittel (36 Prozent) als sehr hoher oder hoher hemmender Faktor bezeichnet (siehe Abbildung 9-9).

Fehlendes Erfahrungswissen:
Aus ökonomischer Perspektive zählt defizitäres Erfahrungswissen zu den zentralen hemmenden Faktoren für den breiteren Einsatz von RFID-Systemen. So werden geringes RFID-Know-how von Unternehmen sowie fehlende Referenzlösungen jeweils von über der Hälfte der im Rahmen dieser Studie Befragten als sehr hoher oder hoher hemmender Faktor benannt (siehe Abbildung 9-10.)

10. Entwicklungsperspektiven der RFID-Technologie

10.1. Veranschaulichung der Risiken in Form von fiktiven Fallbeispielen

10.1.1. Einleitung

Zum einen eröffnet die RFID-Technologie für die Gesellschaft und ihre Wirtschaft zahlreiche Chancen. Zum anderen sind mit dem breiten Einsatz der Technologie auch wachsende Risiken verbunden. Der wirtschaftliche Erfolg der RFID-Technologie – bzw. der in diese Technologie investierenden Unternehmen – hängt auch davon ab, inwieweit es gelingt, die internen Datenbestände und die externe Kommunikation gegen Datenverlust und Datenmissbrauch zu schützen.

Die folgenden fiktiven Fallbeispiele veranschaulichen für den Zeithorizont 2010 grundsätzlich mögliche Risiken der RFID-Technologie in den ausgewählten Anwendungszusammenhängen „Kennzeichnung von Produkten“ sowie „Zutritts- und Routenkontrolle“. Dabei werden auf der einen Seite bereits vorliegende Erfahrungen im Praxiseinsatz der RFID-Technologie berücksichtigt und auf der anderen Seite ein möglichst breites Spektrum der eingesetzten RFID-Technologie („Low-End“ bis „High-End“).

Die fiktiven Fallbeispiele sind explizit nicht als prognostische Abschätzung zu verstehen. Sie sollen vielmehr dazu beitragen, Entscheidungsträger für das Thema der IT-Sicherheit in dem Innovationsfeld RFID zu sensibilisieren, Bewusstsein für Gefährdungen zu wecken und sie zu motivieren, die informationstechnischen Systeme in den Unternehmen und Organisationen angemessen zu analysieren und nachhaltig zu schützen.

10.1.2. Anwendungsgebiet „Kennzeichnung von Produkten“

Die RFID-Technologie bietet zur eindeutigen Kennzeichnung von Produkten in ausgewählten wirtschaftlichen Systemen hohe ökonomische Potenziale. RFID-Tags werden sukzessive weiteren Einzug in die alltäglichen Gegenstände des Lebens halten. Vor allem hochwertige und fälschungsgefährdete Produkte werden zunehmend mit einem passiven RFID-Transponder ausgestattet sein. Hierzu können beispielsweise Produkte der pharmazeutischen Industrie, der Automobilindustrie oder der Textil- und Modebranche zählen. Eine flächendeckende und globale Ausbreitung wird bis 2010 nicht stattfinden. Die Kosten für den Einsatz der RFID-Technologie werden voraussichtlich moderat sinken, die Standardisierung wird in Teilbereichen weiter voranschreiten. Ein umfassender Branchen und Länder übergreifender Einsatz der RFID-Technologie wird sich infolge der immer noch unzureichenden Standardisierung bis zum Jahr 2010 nicht durchsetzen.

Neben RFID-Systemen werden sich voraussichtlich auch ergänzende Anwendungen weiter verbreiten, die maßgeblich zu einer Ausweitung kundenbezogener Datenbestände beitragen. Hierzu zählt beispielsweise die Kundenkarte, durch deren Nutzung Einzelhandelsunternehmen und große Supermarktketten einen zunehmend umfassenden Einblick in das individuelle Kaufverhalten ihrer Kunden erhalten und die bei Privatkunden aufgrund der damit verbundenen Preisvorteile Akzeptanz finden.

Die zunehmende Verbreitung der RFID-Technologie im Bereich der Identifikation von Produkten führt zu erweiterten Möglichkeiten der Datensammlung und -verarbeitung. Hieraus entstehen verschiedene Missbrauchspotenziale, deren Kontrolle auch aufgrund der fehlenden Transparenz erschwert wird. Es besteht die Gefahr, dass mit der breiteren Einführung von gekennzeichneten Produkten Verbindungen zwischen den RFID-Kennungen und den Kunden bzw. Nutzerinnen und Nutzern der Produkte hergestellt und gespeichert werden. Dies wird auch in der derzeitigen Diskussion zum Daten- und Verbraucherschutz thematisiert.

Fiktives Fallbeispiel 1:
Künstliche Einschränkung der Kompatibilität und Lebensdauer
RFID-Etiketten sind im Jahr 2010 bei vielen Gütern zum integralen Bestandteil des Produkts geworden und lassen sich nicht entfernen.

Viele Geräte akzeptieren Austauschteile nur noch bei Vorhandensein eines auf dem RFID gespeicherten Autorisierungsschlüssels. Dadurch konnten billige Plagiate von Ersatzteilen vom Markt verdrängt und die Sicherheit erheblich gesteigert werden. Z. B. wurde so das Risiko explosionsgefährdeter asiatischer Ersatzakkus für Handys gebannt. Der Erfolg dieses Konzepts hat auch Hersteller anderer Produkte angeregt, Autorisierungs-Chips zu verwenden, um Märkte besser ausdifferenzieren zu können. So statten große Hersteller von „Convenient Food" die Verpackungen mit regional verschieden codierten RFID-Tags aus, die nur Mikrowellengeräte der gleichen Region mit Zusatzinformation über Zubereitungszeit und Rezeptvorschlägen versorgen. Verpackungen aus „falschen" Herkunftsgebieten (z. B. Osteuropa) bieten diese Zusatzfunktion nicht, selbst wenn sie technisch vorhanden ist.

Eine noch weitergehende Bevormundung der Konsumenten hat in Teilen der Bevölkerung Unmut ausgelöst: Rasierapparate, Tintenstrahldrucker und Fotoapparate akzeptieren nur noch Austauschteile vom gleichen Hersteller. Beispielsweise können Waschmaschinen nur noch mit Pellets bestückt werden, die eingepresst einen „richtigen" Einweg-RFID enthalten. „Fremde" Waschmittel werden also nicht akzeptiert.

Die meisten neu hergestellten Autos enthalten ein RFID-System, das die Originalität und das Alter von Ersatz- und Austauschteilen (z. B. Reifen) automatisch überwacht. Diese sind mit RFID-Tags und teilweise auch mit Sensoren ausgestattet. In Vertragswerkstätten werden Teile, die eine vom Hersteller vorgegebene Maximallebensdauer erreicht haben oder deren Nutzungslizenz erloschen ist, erkannt und gewechselt. Es können nur Austauschteile von lizenzierten Herstellern eingebaut werden. Der Bordcomputer prüft und akzeptiert diese anhand ihrer verschlüsselten ID. Ohne das Vorhandensein einer noch gültigen ID verweigert das Fahrzeug die Funktion. Die Hersteller legitimieren ihre Vorgehensweise mit Sicherheitsargumenten, die Kunden können diese jedoch nicht im Detail nachprüfen und sind gezwungen, dem Hersteller „blind" zu vertrauen. Als Konsequenz werden RFID-Tags aus Unfallfahrzeugen, deren Zeitlimit noch nicht abgelaufen ist, auf dem Schwarzmarkt gehandelt.

Fiktives Fallbeispiel 2:
Auswertung der Datenspuren von Objekten in Ermittlungsverfahren
Die Umsetzung des „Internet der Dinge" ist im Jahr 2010 weiter vorangeschritten. Diese Entwicklung ermöglicht auch eine Ausweitung staatlicher Überwachungsmaßnahmen im Rahmen der Strafverfolgung auf dingliche Objekte des Alltags, wie sie 2004 nur im Bereich der Telekommunikation möglich gewesen ist.

Obwohl der Nutzen solcher Datensammlungen für die Strafverfolgung von Beobachtern immer wieder in Zweifel gezogen wurde, hat die Auswertung von Logfiles ein nie gekanntes Ausmaß angenommen. Neben Verbindungsdaten aus dem Bereich der Telekommunikation müssen nun auch Daten aus RFID-Systemen mit personenbezogenen Daten gespeichert werden. Standardmäßig werden Datensätze von Tankstellen, Mautbrücken etc. im Rahmen der Terrorismusabwehr in die Rasterfahndung einbezogen. Zudem findet eine Zusammenführung solcher Daten mit den Telekommunikationsdaten statt, wodurch sich Datenspuren von dinglichen (z. B. Waren) und logischen (z. B. Internetanschlüssen, Kreditkartennummern) Objekten verbinden lassen.

Nach verschiedenen Gesetzesänderungen sind praktisch alle Betreiber von offenen RFID-Systemen verpflichtet, die Logfiles aller RFID-Transaktionen über einen längeren

Zeitraum aufzubewahren und den Strafverfolgungsbehörden auf Verlangen zur Verfügung zu stellen.

Diese Situation hat vor allem Betreiber kleinerer Applikationen vor ökonomische Probleme gestellt, denn obwohl die direkten Kosten für die Datenspeicherung in den letzten Jahren gesunken sind, haben sich die Aufwendungen für das Datenmanagement rapide erhöht.

Die Entwicklung, der Aufbau und der Unterhalt der polizeilichen Informationssysteme können trotz hoher Investitionen mit der technischen RFID-Entwicklung nicht Schritt halten, weisen innere Inkompatibilitäten auf und sind einer wirkungsvollen Kontrolle durch das Parlament kaum mehr zugänglich.

10.1.3. Anwendungsgebiet „Zutritts- und Routenkontrolle“

Die Zutritts- und Routenkontrolle mittels RFID-Systemen und die Speicherung der Daten in zentralen Datenbanken werden im Jahr 2010 sowohl im öffentlichen bzw. halböffentlichen Raum als auch in unternehmensinternen Bereichen weit verbreitet sein. Wesentlich wird die Verbreitung dadurch gefördert, dass Inkompatibilitäten bei geschlossenen Systemen nicht ins Gewicht fallen.

Vor allem große Unternehmen, die neue Standorte eröffnen oder die ihre bestehenden IT-Lösungen im Bereich „Zutritt“ erneuern müssen, werden sich für ein RFID-System entscheiden. Unternehmensintern werden RFID-basierte Zutritts- und Routenkontrollen nicht nur im Eingangsbereich von Unternehmensgeländen eingesetzt, sondern auch mit weiteren Funktionen (Zeiterfassung auch zur Ermittlung von Pausenzeiten, Zutritt zu sicherheitsrelevanten Bereichen innerhalb des Geländes, Optimierung von Prozessen und somit Ermittlung auch von personenbezogenen Daten zur Leistungskontrolle).

Unternehmen nutzen bereits heute die Möglichkeiten von Informations- und Kommunikationstechnologien zur Verhaltens- und Leistungskontrolle von Erwerbstätigen – auch in Subunternehmen. Nicht immer werden Erwerbstätige darüber informiert, dass Informations- und Kommunikationstechnologien zu Kontrollzwecken eingesetzt werden.

Auch im Freizeitbereich etablieren sich RFID-Systeme zur Zutrittskontrolle. Obwohl sie auch zur Routenkontrolle genutzt werden können, steht die Funktion bei der Einführung von RFID-Systemen nicht im Mittelpunkt. Vielmehr wirken die steigende Akzeptanz des Online-Shopping über Internet und Mobilfunk im Bereich des Ticketing sowie der Vorteil, dass Tickets im Verlustfall ersetzt werden können, als Enabler.

Sowohl für den unternehmensinternen Bereich als auch für den (halb) öffentlichen Bereich eröffnet die RFID-basierte Zutritts- und Routenkontrolle erweiterte Potenziale zur Kontrolle. Es entsteht ein Spannungsfeld zwischen Effizienz und Bequemlichkeit auf der einen und Sicherheit und Datenschutz auf der anderen Seite.

Fiktives Fallbeispiel 1:
Überwachung von Fußballfans
Eintrittskarten zu Sportgroßveranstaltungen enthalten im Jahr 2010 generell einen RFID-Chip, der einen automatischen Einlass ins Stadion ermöglicht. Einerseits sollen den Fußballfans lange Wartezeiten beim Einlass erspart, andererseits soll der Schwarzhandel mit Tickets unterbunden werden. Durch eine zentrale Datenbankanbindung wird gewährleistet, dass im Verlustfall ein neues Ticket ausgestellt und das alte gesperrt werden kann.

Die Zuordnung von Ticketnummer zur Person erfolgt bereits beim Vorverkauf und ist nicht veränderbar. Einzig die Besitzer von Geschenktickets müssen sich beim ersten Eintritt ins Stadion in einem separaten Schritt durch Vorlage eines Personaldokuments identifizieren.

Das Stadion wird nicht nur im Eingangsbereich, sondern an allen Durchgangspunkten mit Lesegeräten ausgestattet. Diese Vorgehensweise wurde zuvor durch die Allgemeinen Geschäftsbedingungen legitimiert. Die personenbezogenen Daten werden an den Veranstalter, einen privaten Sicherheitsdienst und an die Polizei übermittelt. Letztere hat bereits beim Verkauf der Tickets personalisierte Datenbestände angelegt und ist so jederzeit über den Aufenthaltsbereich im Stadion von Personen informiert, die aus Polizeikontrollen von früheren Anlässen bekannt sind. Auffällig werdende Fanblocks werden als Pulk erfasst, ohne dass die Polizei konfrontative und aufwendige Personenkontrollen durchführen muss.

Unbeteiligte Personen, die sich zufällig im Lesebereich der entsprechenden Blocks aufhalten, werden in diesen Fällen ebenfalls registriert.

Fiktives Fallbeispiel 2:
Leistungs- und Verhaltenskontrolle in Betrieben

Der Betriebsrat hat im Jahr 2010 der Einführung eines RFID-Systems nach § 87 Abs. 1 Nr. 6 des BetriebsVG zugestimmt, um den Zutritt zu sicherheitsrelevanten Bereichen zu kontrollieren. Gleichzeitig werden Synergieeffekte genutzt und die Zugangskontrolle mit der Zeiterfassung im Unternehmen verbunden. Weitere Funktionalitäten wie eine Zahlungsfunktion für die Kantine werden ebenfalls integriert. Die so gewonnenen Daten der Erwerbstätigen werden zusammengeführt. Durch die Auswertung dieser Daten kann einer Arbeitnehmerin oder einem Arbeitnehmer ein schuldhaft begangener, arbeitsvertraglicher Pflichtverstoß nachgewiesen werden.

Die Erfassung und Auswertung arbeitnehmerbezogener Daten werden mitbestimmungswidrig vom Unternehmen zur Leistungs- und Verhaltenskontrolle durchgeführt. Auf Grundlage dieser Daten kommt es zur Kündigung eines Mitarbeiters. Der Betriebsrat stimmt dieser Kündigung zu, obwohl die durch das RFID-System gewonnenen Daten mitbestimmungswidrig zur Kontrolle von Verhalten oder Leistung genutzt wurden. Die Daten können vor Gericht verwandt werden, da der Betriebsrat den Verstoß gegen § 87 Abs. 1 Nr. 6 BetrVG kennt und der Verwertung der so gewonnenen Beweismittel sowie der darauf gestützten Kündigung zustimmt.

Diese Rechtslage bezieht sich nicht auf „arbeitnehmerähnliche Personen“ – „Kleinstunternehmen“, „Einpersonenfirmen", Scheinselbstständige bzw. „neue Selbstständige“, die sich nicht selten in hoher Abhängigkeit von einem Auftraggeber befinden. Hier gelten nicht einmal die Regelungen des Mitbestimmungsrechts bzw. des Kündigungsschutzes. Aufhebungen oder die Nichtverlängerung von Vertragsbeziehungen als Resultat von Leistungs- und Verhaltenskontrollen durch RFID können die Folge sein.

10.2. Erwartete Entwicklungen bis 2010

10.2.1. Vorbemerkung

Die Entwicklungsperspektiven der RFID-Technologie werden nicht allein von den technischen Möglichkeiten geprägt. Neben Technologie und Standardisierung sind auch die Markt- und Preisentwicklung, Informationssicherheit und Datenschutz sowie der gesellschaftliche Diskurs zu diesen Anforderungen zu berücksichtigen.

Im Folgenden werden die zukünftigen Entwicklungen in den Bereichen „Technologie und Standardisierung“ sowie „Markt- und Preisentwicklung“ aus Sicht von Expertinnen und Experten im RFID-Sektor bewertet. Anschließend wird der derzeitige Stand der öffentlichen Diskussion im Kontext von RFID umrissen.

10.2.2. Technologie und Standardisierung

Für die kommenden zehn Jahre ist mit einer weiteren exponentiellen Steigerung der Leistungsentwicklung der Informations- und Kommunikationstechnologie zu rechnen. Neben der Verbesserung des Preis-Leistungsverhältnisses werden sich die eingesetzten technologischen Komponenten weiterhin drastisch verkleinern. Die Miniaturisierung der Mikroelektronik wird voraussichtlich noch etwa zehn Jahre ohne Technologiebruch voranschreiten. Sie ist eine wesentliche Triebkraft für die Realisierung der Vision „Pervasive Computing". [HBBB 03] Die Entwicklung im RFID-Sektor wird auch durch neue Technologien gefördert: Für den Einsatz in RFID-Systemen wird seit Ende 2002 auch die Nahfunktechnik Near Field Communication (NFC) diskutiert, mit der Sony und Philips einen drahtlosen Vernetzungsstandard etablieren wollen. Die NFC-Technologie basiert auf einer Kombination aus kontaktloser Identifikation mittels RFID und drahtloser Verbindungstechnologie. NFC nutzt 13,56 MHz und soll mit einer Reichweite von wenigen Zentimetern vor allem die Vernetzung per Bluetooth oder W-LAN erleichtern, indem sich Endgeräte per NFC automatisch identifizieren und eine Datenverbindung aufbauen. Eine von Philips entwickelte Pilotanwendung ermöglicht beispielsweise den Ticketkauf per Internet, indem ein mit einem NFC-Tag ausgestattetes Werbeplakat kontaktlos und „automatisch eine Webadresse an einen davor gehaltenen PDA oder ein Handy schickt". Als weitere Anwendungen werden sichere Bezahl- und Transaktionsverfahren sowie die Zutrittskontrolle und -überwachung in Gebäuden diskutiert [HAMM 04]. Gemeinsam mit Nokia gründeten Sony und Philips das NFC-Forum [NFC 04a], um die Verbreitung der NFC-Technologie zu fördern. Das neue Forum will die Implementierung und Standardisierung der NFC-Technologie vorantreiben, um die Kompatibilität zwischen Geräten und Diensten sicherzustellen. [NFC 04b]

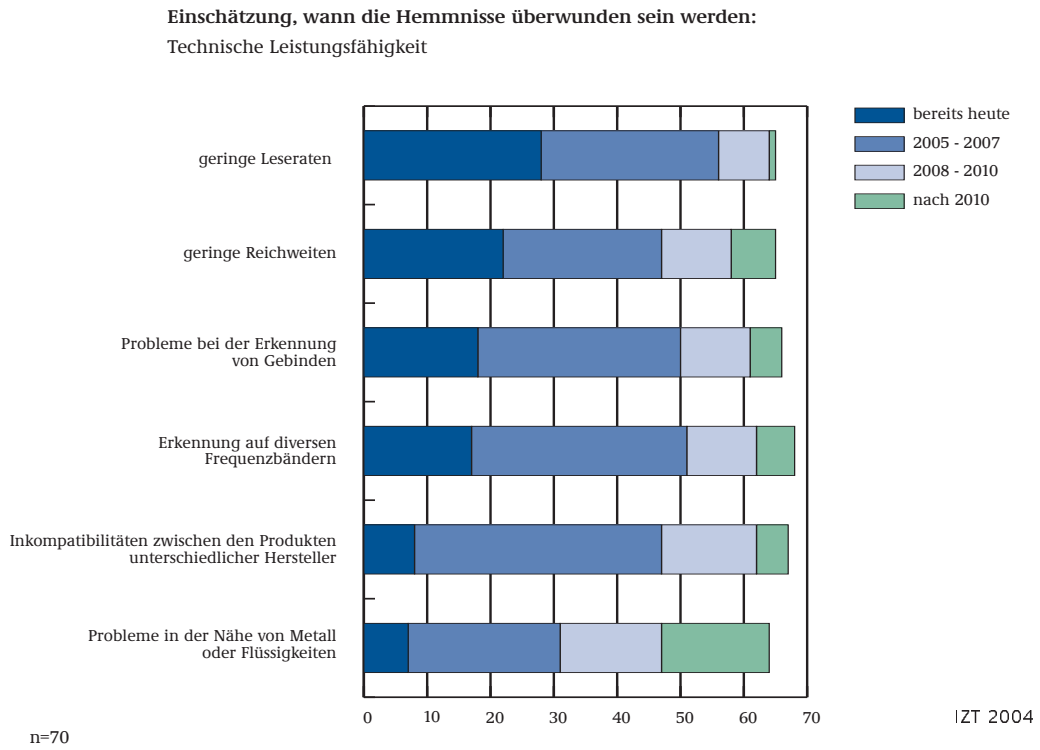


Abbildung 10-1: Einschätzung, wann die Hemmnisse überwunden sein werden: Technische Leistungsfähigkeit

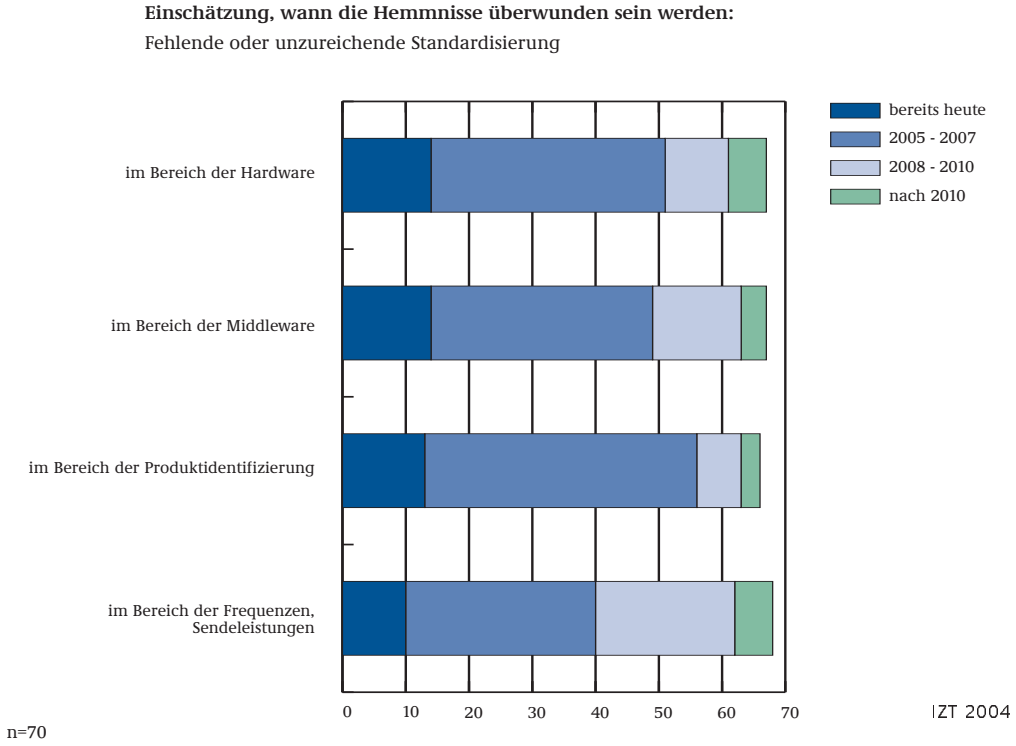


Abbildung 10-2: Einschätzung, wann die Hemmnisse überwunden sein werden: Fehlende oder unzureichende Standardisierung

Nach Einschätzung von Expertinnen und Experten aus Unternehmen und Forschungseinrichtungen, die im RFID-Sektor tätig sind, werden wesentliche technische Faktoren, die derzeit noch die Verbreitung und Nutzung von RFID-Systemen hemmen, bis zum Jahr 2007 bzw. bis zum Jahr 2010 überwunden sein. Hierzu zählen die geringen Leseraten und Reichweiten, Probleme bei der Pulk-Erfassung und die Erkennung auf unterschiedlichen Frequenzbändern. Die größte Skepsis der befragten Expertinnen und Experten zeigt sich in der Annahme, dass die bestehenden Probleme bei der Erkennung von Transpondern in der Nähe von Metall bzw. Flüssigkeiten in einzelnen Frequenzbereichen bis zum Jahr 2010 nicht gelöst sein werden. (Siehe Abbildung 10-1)

10.2.3. Markt- und Preisentwicklung

Die Untersuchungsergebnisse der Online-Befragung, die im Rahmen des vorliegenden Projektes durchgeführt wurde, verweisen für die kommenden Jahre 2005 bis 2010 auf eine insgesamt positive oder stabile Marktentwicklung von RFID-Systemen in Deutschland. So wird von 43 Prozent der Befragten eine positive, von 33 Prozent eine stabile Marktentwicklung erwartet (siehe Abbildung 10-4). Ein geringer Anteil der Befragten geht von einer stagnierenden Marktentwicklung aus (3 Prozent). Auch im Bereich der Preisentwicklung für RFID-Systeme bis zum Jahr 2010 sind sich die Befragten vergleichsweise einig: 90 Prozent erwarten insgesamt fallende Preise (siehe Abbildung 10-4). Dabei erwarten 36 Prozent der Befragten eine stark fallende Preisentwicklung, während 54 Prozent lediglich von einer leicht fallenden Preisentwicklung ausgehen. Aufgrund der hohen Bedeutung der Kosten bei etwaigen Investitionsentscheidungen kann ein lediglich moderater Preisverfall die weitere Verbreitung der RFID-Technologie deutlich dämpfen.

Die Einschätzungen, in welchen Anwendungsgebieten sich RFID-Systeme weiter durchsetzen werden, fallen unterschiedlich aus. Langfristig – für die Jahre zwischen 2008

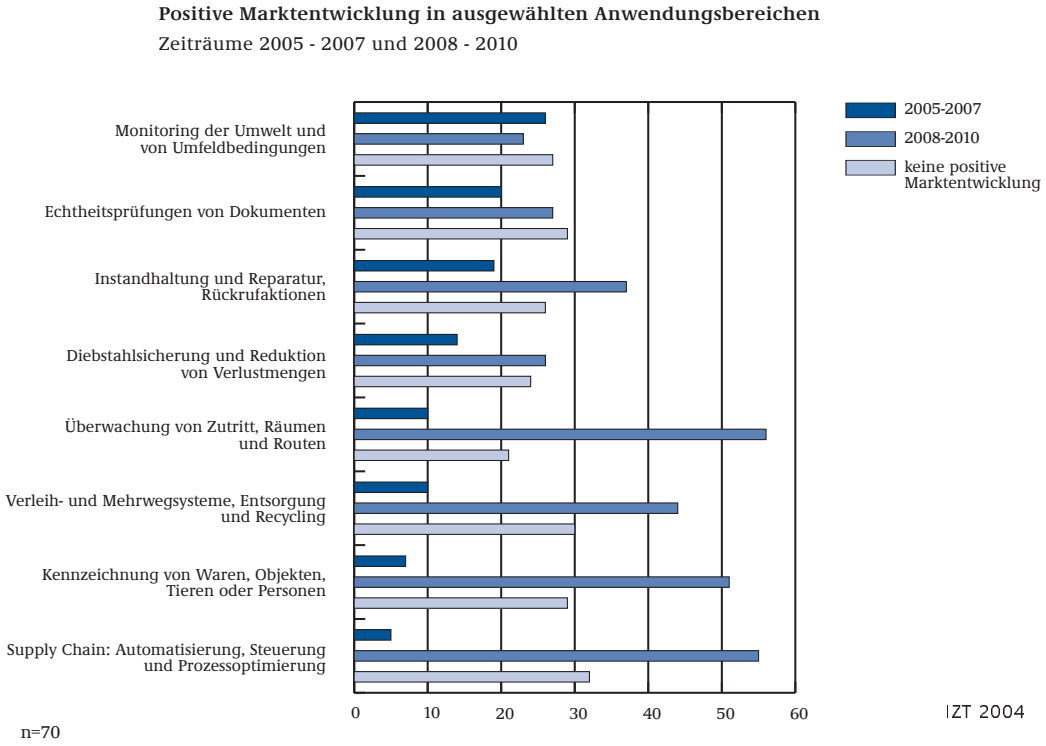


Abbildung 10-3: Marktentwicklung von RFID-Systemen in Anwendungsbereichen

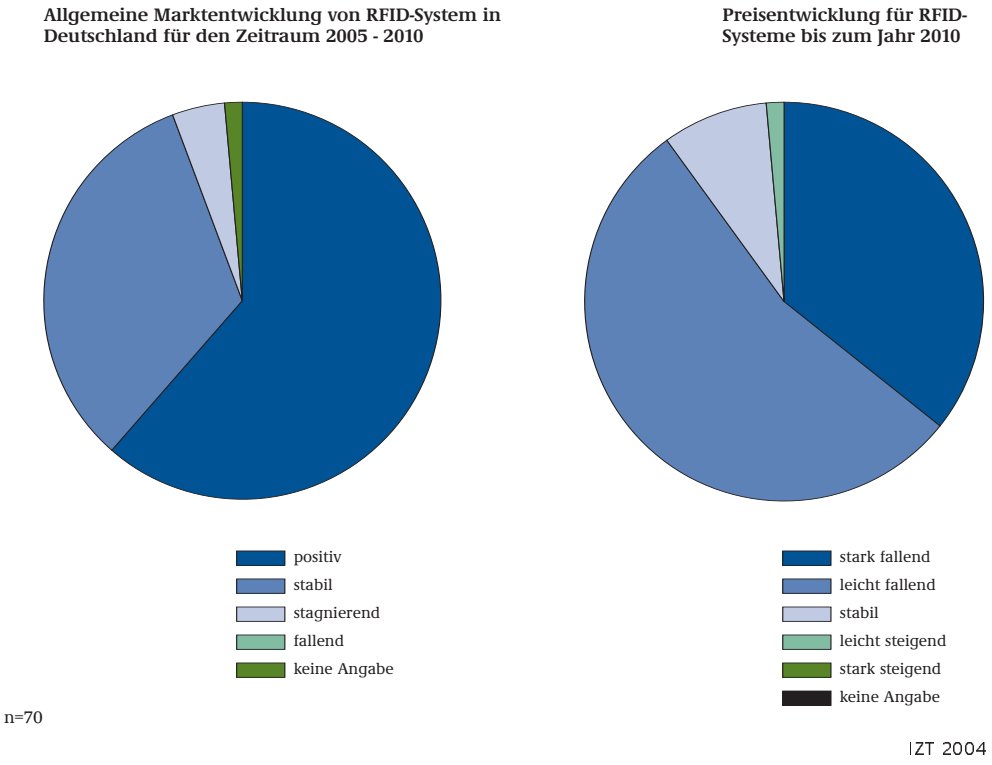


Abbildung 10-4: Allgemeine Marktentwicklung von RFID-Systemen in Deutschland für den Zeitraum 2005-2010 sowie Preisentwicklung von RFID-Sytemen bis zum Jahr 2010

und 2010 – gehen jeweils über die Hälfte der Befragten davon aus, dass sich in den Anwendungsbereichen „Überwachung von Zutritt, Räumen und Routen“ (80 Prozent), „Supply Chain: Automatisierung, Steuerung und Prozessoptimierung“ (79 Prozent), „Kennzeichnung von Waren, Objekten, Tieren oder Personen“ (73 Prozent), „Verleih- und Mehrwegsysteme, Entsorgung und Recycling“ (63 Prozent) sowie „Instandhaltung und Reparatur, Rückrufaktionen“ (53 Prozent) eine positive Marktentwicklung zeigen wird (siehe Abbildung 10-3).

10.2.4. Anforderungen an Informationssicherheit, Datenschutz und Privatsphäre

Im Vergleich zu den heutigen Anwendungen der Informations- und Kommunikationstechnologie werden zukünftige Anwendungen des Pervasive Computing durch eine große Verteiltheit, spontane Vernetzung und eine eng damit verbundene erhöhte Systemkomplexität gekennzeichnet sein. Gleichzeitig werden die Zusammenhänge zwischen Handlungen und deren Folgen durch die vernetzt erbrachten Funktionen und Dienstleistungen zunehmend intransparent. Die Ursachen von etwaigen Fehlfunktionen, aber auch etwaige Missbräuche sind in der Folge schwerer zu ermitteln. Zukünftige technische Systeme werden mithin auch schwerer beherrschbar. Die für das Pervasive Computing typische große Bandbreite an technischen Geräten erfordert zunehmend individuelle Sicherheitslösungen (z. B. in Abhängigkeit von den genutzten Geräteressourcen, von der Art der zu übertragenden Daten oder der jeweiligen Nutzungssituation). [Lang 04]

Mit der stärkeren Informatisierung und Vernetzung des Alltags steigt insgesamt die Abhängigkeit von technologischen Hintergrundprozessen an. Es gilt, der zunehmenden Undurchschaubarkeit der technischen Systeme entgegen zu wirken und durch die Sicherstellung von hoher Transparenz das Vertrauen der Nutzerinnen und Nutzer in die RFID-Technologie zu steigern.

Eine stark informatisierte Alltags- und Berufswelt mit Gegenständen, die Teilaspekte ihrer Umgebung erfassen und miteinander kommunizieren, hat somit neben den ökonomischen Potenzialen auch grundsätzliche Auswirkungen auf die Informationssicherheit und Privatsphäre (Datenschutz).

In der öffentlichen Diskussion über RFID steht im Augenblick der Datenschutz im Mittelpunkt, während die Betrachtung der Informationssicherheit eher eine untergeordnete Rolle spielt. Einen guten Eindruck im Hinblick auf die Gefährdungen durch RFID-Systeme vermitteln die Kapitel 7.4 und 7.5 zur Bedrohungslage der aktiven und passiven Partei. Bereits hier wird deutlich, dass die Bedrohungen der Informationssicherheit (Einspeisen falscher Daten, Denial of Service) primär den Betreiber eines RFID-Systems – und damit die aktive Partei – betreffen. Diese potenziellen Bedrohungen werden im Zuge der zunehmenden Einführung automatisierter industrieller Verarbeitungsabläufen zu realen Gefahren. Dabei können das Einspeisen falscher Daten in RFID-Systeme und Manipulationen der korrekten Funktionsweise von RFID-Systemen großen Einfluss auf die ordnungsgemäßen Produktionsabläufe haben und damit zu großen wirtschaftlichen Schäden führen.

Hingegen ist bei der passiven Partei – den Kunden oder Arbeitnehmern eines RFID-System-Betreibers – durch den Einsatz von RFID-Systemen die Data Privacy bzw. Location Privacy bedroht. Dass diese Bedrohung als reale Gefahr durchaus gegeben ist, legt die vom Auto-ID Center des Massachusetts Institute of Technology (MIT) ins Leben gerufene Web Services WAN Special Interest Group nahe, die an einem Prototypen für eine Standardarchitektur arbeitet. [Robe 04] Mit dieser Architektur können in Echtzeit grundsätzlich beliebig viele Interessenten auf Daten zugreifen, die beim Auslesen von RFID-Labels generiert werden. Hier greifen RFID-Systeme in einen speziellen Aspekt des Allgemeinen Persönlichkeitsrechts – das Recht auf informationelle Selbstbestimmung – ein,

welches die Befugnis des Einzelnen, prinzipiell selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, regelt. Mit diesen technischen Voraussetzungen können Daten nicht nur durch den Staat, sondern auch durch nicht öffentliche Stellen wie privatwirtschaftliche Unternehmen erfasst, verarbeitet und jenseits ihres ursprünglichen Zwecks genutzt werden.

Die Regelungen des heutigen Datenschutzrechts beziehen sich auf personenbezogene Daten. Der Begriff der „personenbezogenen Daten" umfasst auch „auf Personen beziehbare Daten". In einem Gutachten für das Bundesinnenministerium kommen Roßnagel, Pfitzmann und Garstka zu dem Schluss: „In der Welt künftiger vernetzter und allgegenwärtiger Datenverarbeitung wird es immer öfter vorkommen, dass Daten – etwa zu Netzadressen oder zu anderen „Identifiers" – verarbeitet werden, für die zu diesem Zeitpunkt unbekannt ist, ob sie sich auf bestimmte Personen beziehen (Beispiel: IP-Adressen), auf welche Personen sie sich beziehen (Beispiel: Globally Unique Identifier – GUID) oder welchen Personen sie künftig zugeordnet werden (Beispiel: RFID-Tags). Auch wenn die Daten (noch) nicht den Begriff der personenbezogenen Daten erfüllen, sollten im Sinn der Vorsorge dennoch die Grundsätze der Vermeidung des Personenbezugs, der Erforderlichkeit und der Zweckbindung auf sie Anwendung finden, wenn zu erwarten ist, dass der Personenbezug hergestellt wird oder werden kann." [RPG 01]

Auf der Grundlage von RFID-Systemen können Daten „auf Vorrat" gesammelt werden. Aus einer Vielzahl von Messgrößen kann anschließend ein Kontextverständnis generiert werden, das sich aufgrund der Heterogenität und der großen Zahl der beteiligten Komponenten der Kontrolle durch den Datenschutz entzieht. Mattern und Römer sprechen von einem Paradigmenwechsel: „Verarbeitete man früher mit der ‚EDV' Daten [...], so erfasst man jetzt – automatisch, online und in Realzeit – die physischen Phänomene selbst, was in einem viel größeren Umfang möglich ist und eine ganz neue Qualität von Resultaten ermöglicht." [MaRö 03 sowie ECPS 02]

Vor diesem Hintergrund ist die Datensparsamkeit und Zweckbindung der gesammelten Daten als wesentliches Kriterium für die zukünftige Gewährleistung des Rechts auf Privatsphäre zu betrachten. Im Zuge der weiteren Verbreitung der RFID-Technologie stellt sich mithin die Frage, wer darüber bestimmen kann oder darf, ob und mit welchen Informationen elektronisch aufgewertete Dinge verknüpft werden. Schließlich ist auch zu berücksichtigen, dass in einer wesentlich stärker informatisierten Welt das korrekte Funktionieren der informationstechnischen Infrastruktur „überlebenswichtig" für die Gesellschaft oder für Einzelne werden kann. Gerade aufgrund der fortschreitenden Miniaturisierung technologischer Systeme ist zu befürchten, dass bestehende rechtliche Verbote im Zuge der weiteren Verbreitung von RFID-Systemen nicht kontrollierbar bzw. durchsetzbar sind. Für diese Fälle müssen also gleichermaßen Lösungsstrategien entwickelt werden.

Gegen den Einsatz von RFID-Systemen, soweit er auf gesetzlicher Grundlage und unter Beachtung der datenschutzrechtlichen Bestimmungen erfolgt, ist laut Bundesdatenschutzbericht grundsätzlich nichts einzuwenden: „Es ist legitim, die neuen technischen Entwicklungen zu nutzen [...]. Zugleich werden aber technische Kontrollsysteme und eine Überwachungsstruktur aufgebaut, die, einmal vorhanden, auch noch zu ganz anderen Zwecken genutzt werden könnten und deren gesetzes- und datenschutzkonforme Anwendung letztlich nicht mehr kontrollierbar ist. [...] Auch hier zeigt sich wieder, dass die Summe von nützlichen und für sich gesehen datenschutzkonformen Anwendungen insgesamt ein Bedrohungspotenzial für das Grundrecht auf informationelle Selbstbestimmung darstellt, das von den Betroffenen und auch in der gesellschaftspolitischen Diskussion so zunächst nicht wahrgenommen wird." [BuDa 01/02]

Um die Chancen von RFID zu nutzen und gleichzeitig die Bedrohung für die Persönlichkeitssphäre so gering wie möglich zu halten, wird es entscheidend darauf ankommen, dass die Grundsätze des modernen Datenschutzrechts wie die Datensparsamkeit sowie schnellstmögliche Anonymisierung oder Pseudonymisierung personenbezogener Daten in RFID-Systemen bereits frühzeitig im Design-Prozess und bei der Markteinführung umgesetzt werden. Dies gilt umso mehr, als politische und rechtliche Rahmenbedingungen im Zuge der fortschreitenden Globalisierung zunehmend schwieriger zu gestalten sind.

10.2.5. Gesellschaftliche Akzeptanz

Die zukünftigen Entwicklungen im Bereich des Pervasive Computing sowie der RFID-Technologie haben Auswirkungen auf weite Teile des privaten, beruflichen und öffentlichen Lebens. Damit stellt sich die Frage nach der gesellschaftlichen Akzeptanz der neuen Technologien. Dabei setzt eine möglichst objektive und vom Einzelnen nachvollziehbare Beurteilung der Chancen und Risiken des Pervasive Computing sowie der RFID-Technologie eine offene, sachliche und umfassende Information voraus.

Für die öffentliche sowie individuelle Wahrnehmung und Kommunikation technologiebedingter Chancen und Risiken haben die Medien eine hohe Bedeutung. Ihnen kommt nicht nur die Rolle eines Informationslieferanten zu, sondern auch eine zentrale Funktion als Informations-Bündeler und -Verstärker. Erst die Resonanz in den Massenmedien verleiht einer potenziellen Chance gesellschaftliche Anerkennung, einem potenziellen Risiko gesellschaftliche und politische Brisanz. [Büll 03]

Im Hinblick auf RFID-Systeme hat die Aufmerksamkeit der Medien in den vergangenen Jahren deutlich zugenommen. In den Fachmedien findet – auch in Abhängigkeit zu der Bedeutung von RFID in der jeweiligen Branche – eine mehr oder weniger intensive Berichterstattung statt. In der an die breitere Öffentlichkeit gerichteten Presse wurden im vergangenen Jahr eine Reihe von Berichten mit durchaus kritischen oder negativen „Headlines“ publiziert (z. B. „RFID – Der Schnüffel-Chip im Joghurtbecher“, „Spione im Einkaufswagen“, „Satans Werk oder der nächste Schritt in eine digitalisierte Welt?“). Da die möglichen Wirkungen von RFID-Systemen im Einzelhandel auf das Alltagsleben der Bevölkerung besonders umfassend sind, spielen hier Privacy-Gedanken und Datenschutzaspekte in der medialen Auseinandersetzung eine zunehmend wichtige Rolle. Eine empirische Medienanalyse, die verlässlich darüber Auskunft geben könnte, wie die bisherige Information und Kommunikation zu den Chancen und Risiken von RFID-Systemen bislang in den Massenmedien und relevanten Fachmedien verlaufen ist, wurde nicht durchgeführt. Ob in der medialen Berichterstattung bzw. in der öffentlichen Kommunikation bestimmte Unterthemen und Probleme im Kontext von RFID-Systemen betont oder als unwichtig klassifiziert werden, kann daher nicht abschließend geklärt werden.

Die Frage, ob bzw. wie stark und schnell sich die gesellschaftlichen Gruppen der RFID-Technologie gegenüber öffnen oder wie zögerlich oder indifferent sie sich gegenüber den weiteren Entwicklungen verhalten werden, ist schwer einzuschätzen. In der Debatte um die Möglichkeiten und Grenzen der RFID-Technologie kristallisieren sich zwei gegenüberstehende Positionen heraus: Während auf der einen Seite die Chancen gesehen werden, die sich aus der Nutzung von RFID ergeben, werden auf der anderen Seite vor allem die Risiken, Bedrohungen und Beschränkungen thematisiert.

Aus verbraucherpolitischer Sicht besteht der potenzielle Nutzen von RFID-Systemen für die Verbraucherinnen und Verbraucher darin, zu größerer Sicherheit und einer bequemeren Handhabung alltäglicher Lebenssituationen zu gelangen. Damit ist einerseits eine hohe gesellschaftliche Akzeptanz in Bezug auf

RFID-Systeme zu erwarten. Dies auch, da es bereits Produkte gibt, die auf gesellschaftliche Zustimmung und Nachfrage treffen (z. B. Kundenkarten, RFID-basierte Skipässe). Offensichtlich ist der erlebte Nutzwert in diesen Fällen von höherer Bedeutung als die Befürchtungen um etwaige Einschnitte der Privatsphäre. Hierauf verweisen auch die vorliegenden Untersuchungsergebnisse aus der Akzeptanzforschung, nach der auf Informations- und Kommunikationstechnologien basierende Anwendungen von den Verbraucherinnen und Verbrauchern nur dann angenommen werden, wenn sie einen deutlichen Mehrwert bieten können. Deshalb steht für jede einzelne RFID-Anwendung die Frage des Abwägens von Chancen und Risiken im Zentrum der gesellschaftlichen Diskussion und Akzeptanz.

Auch mit RFID verwandte Technologien bzw. Anwendungen werden heute schon umfassend von der Bevölkerung genutzt und akzeptiert. So werden in den Bereichen der Werbung und Markt- und Meinungsforschung zur Erstellung von umfassenden Kundenprofilen auf Grundlage immer neuer Verfahren immer mehr Kundendaten gesammelt und ausgewertet. Dabei kommen Methoden des Data Mining zum Einsatz. Durch Anreizsysteme der Anbieter fallen unter aktiver Mitwirkung der Konsumentinnen und Konsumenten vermehrt und regelmäßig Daten an. Laut einer Untersuchung von Emnid ist beispielsweise die Kundenkarte nach der Krankenversicherungs- und ec-Karte die wichtigste Karte in der Brieftasche eines großen Anteils der deutschen Bevölkerung geworden. Im März 2002 hatten bereits mehr als die Hälfte aller Deutschen mindestens eine Kundenkarte, in Großbritannien waren es 2003 sogar mehr als 86 Prozent. [Scha 04] „Für Rabatte von oftmals weniger als einem Prozent des Warenwertes ist ein Großteil der Verbraucher scheinbar bereit, das Kaufverhalten offen zu legen und zum Zwecke der Marktforschung und zur individuellen Angebotsunterbreitung analysieren zu lassen.“ [Lang 04]

Anderseits müssen RFID-Systeme im Kontext des Pervasive Computing als ein Bündel von Innovationen betrachtet werden, das fundamentale Neuerungen hervorbringen wird und überraschende Anwendungsmöglichkeiten verspricht. Damit ist zunächst grundsätzlich offen, welche gesellschaftlichen Bedarfe und Vorbehalte zukünftig bestehen werden. Dabei ist zu berücksichtigen, dass in Teilen der Bevölkerung bereits heute die zweifelnden Stimmen zunehmen, die bei einer weiteren Penetration der RFID-Technologie den Datenschutz und die Privatsphäre gefährdet sehen. Konsumentenvereinigungen haben bereits zum Boykott von Unternehmen aufgerufen, die die RFID-Technologie vorantreiben bzw. einsetzen. Marc Langheinrich schreibt: „RFID-Tags oder Smart Labels haben wohl wie keine andere Technologie des Ubiquitous Computing Ängste in der Bevölkerung mobilisiert, in naher Zukunft in einem Überwachungsstaat zu leben.“ [Lang 04]

Da in einer modernen, differenziert strukturierten Gesellschaft eine Vielzahl von mehr oder weniger großen, zum Teil in Konkurrenz zueinander stehenden Interessengruppen existiert, ist es für die weitere Entwicklung wichtig, diesen Meinungspluralismus auch im Umfeld von RFID in einem angemessenen Verhältnis widerzuspiegeln. Es gilt, mehr Transparenz in der Diskussion um RFID in den einzelnen Akteursgruppen herzustellen. Sie ist ein zentraler Schritt zur Versachlichung der Diskussion und für die gesellschaftliche Meinungsbildung.

11. Abkürzungsverzeichnis

AIM:	Verband für Automatische Datenerfassung, Identifikation und Mobilität
BSI:	Bundesamt für Sicherheit in der Informationstechnik
CRC:	Cyclic Redundancy Check
DRAM:	Dynamic Random Access Memory
EAS:	Electronic Articel Surveillance
EEPROM:	Electrically Erasable Programmable Read Only Memory
EMPA:	Eidgenössische Materialprüfungs- und Forschungsanstalt
EPC:	Electronic Product Code
EPROM:	Erasable Programmable Read Only Memory
EU:	Europäische Kommission
FoeB:	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs
FRAM:	Ferroelectric Random Access Memory
GHz:	Gigahertz
GUID:	Globally Unique Identifier
HF:	High Frequency
ICT:	Information and Communication Technology
IP:	Internet Protocol
ISO:	International Organization for Standardization
IZT:	Institut für Zukunftsstudien und Technologiebewertung
KHz:	Kilohertz
LF:	Low Frequency
MHz:	Megahertz
NFC:	Near Field Communication
OCR:	Optical Character Recognition
ONS:	Object Name Service
PLM:	Product Lifecycle Management
PML:	Procedural Markup Language
RAM:	Random Access Memory
RFID:	Radio Frequency Identification
ROM:	Read Only Memory
SRAM:	Static Random Access Memory
TA-SWISS:	Zentrum für Technologiefolgen-Abschätzung beim Schweizerischen Wissenschafts- und Technologierat
UHF:	Ultra High Frequency
USA:	United States of America
VIBE!AT:	Verein für Internet-Benutzer Österreichs
W-LAN:	Wireless LAN
XML	Extensible Markup Language

12. Index

[ACG 04]
ACG IDENTIFICATION TECHNOLOGIES GMBH, http://www.acg.de, Abruf vom 02.07.2004
≠
[AdHö 04]
AUF DEM HÖVEL, J.: Smarte Chips für die Warenwelt. In: Morgenwelt – Magazin für Wissenschaft und Kultur vom 4.06.2004, http://www.morgenwelt.de/418.html, Abruf vom 12.07.2004

[aid 04]
AID INFODIENST, VERBRAUCHER-SCHUTZ, ERNÄHRUNG, LANDWIRT-SCHAFT E. V.: Neue Kennzeichnung-svorschriften für Schafe und Ziegen, http://www.aid.de/downloads/ER_Kennzeichnungsvorschriften.pdf, Abruf vom 15.07.2004

[AOLm 04]
AOL MEMBER BEREICH: Lachs-Rennen in Schweden. http://members.aol.com/vhsf/lachrenn.htm, Abruf vom 04.08.2004

[ArKo 04]
ARBEITSKREIS KONTAKTLOSE CHIPKARTEN-SYSTEME FÜR ELECTRONIC TICKETING E. V. (KONTIKI): Feldversuche E-Ticketing im ÖPV, http://www.kontiki.net/deutsch/index_dt.html, Abruf vom 09.08.2004

[ATKe 04]
A.T. KEARNEY: RFID spart dem deutschen Einzelhandel sechs Milliarden Euro pro Jahr. Nutzen für Händler – Kosten für Hersteller, Pressemitteilung vom 08. März 2004, http://www.atkearney.de/content/veroeffentlichungen/pressemitteilungen_detail.php/id/49046, Abruf vom 14.7.2004

[Auto 02]
AUTO-ID CENTER: 860 MHz – 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification. Auto-ID Center /EPCglobal, Cambridge, MA, USA. verfügbar unter: www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf. (16.07.2004)

[Auto 03]
AUTO-ID CENTER: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. Auto-ID Center/EPCglobal, Cambridge, MA, USA. verfügbar unter: www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf. (16.07.2004)

[Auto 03b]
AUTO-ID CENTER (2003) Technical Report: 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Recommended Standards, Version 1.0.0, http://archive.epcglobalinc.org/publishedresearch/mit-autoid-tr011.pdf, Abruf vom 09.09.2004

[Baum 04]
BAUMER IDENT: Branchenlösungen Automobilindustrie. http://www.baumerident.com/deutsch/4_branchen/automobil.htm, Abruf vom 15.07.2004

[BCLM 03]
BOHN, J., COROAMA, V., LANGHEINRICH, M., MATTERN, F. und ROHS, M.: Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge. In: GRÖTKER, RALF (Herausgeber): Privat! Kontrollierte Freiheit in einer vernetzten

13. Quellenverzeichnis

Welt. Heise-Verlag, 2003. http://www.inf.ethz.ch/vs/publ/papers/allvercom.pdf, Abruf vom 19.08.2004

[Biob 04]
BIOBOARD.DE. DAS FORUM FÜR BIOLOGIE: Kostenlose Hilfen für Biologie http://.www.bioboard.de, Abruf vom 03.07.2004

[Booz 04]
BOOZ ALLEN HAMILTON in Kooperation mit der UNIVERSITÄT ST. GALLEN: RFID-Technologie: Neuer Innovationsmotor für Logistik und Industrie?, http://www.boozallen.de/content/downloads/5h_rfid.pdf, Abruf vom 19.07.2004

[Borc 04a]
BORCHERS, D.: Reisepass mit Transponder. In: Heise Online vom 19.03.2004, http://www.heise.de/newsticker/meldung/45780, Abruf vom 18.07.2004

[BORC 04b]
BORCHERS, D: Holland testet Biometrie im Pass. In: Heise Online vom 02.07.2004. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48809, Abruf vom 18.07.2004

[BSI 03]
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI in Kooperation mit der TECHNISCHEN UNIVERSITÄT MÜNCHEN UND DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN: Kommunikations- und Informationstechnik 2010+3 – Neue Trends und Entwicklungen in Technologie, Anwendungen und Sicherheit. Secu Media Verlag: Ingelheim.

[Buch 04]
BUCHHOLZ, T.: RFID-Technologie zur Identifizierung von Hunden. In: Logistik Inside vom 19.2.2004, http://www.logistikinside.de/sixcms4/sixcms/detail.php/69876/de_news, Abruf vom 06.07.2004

[BuDa 01/02]
BUNDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ: Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz. 19. Tätigkeitsbericht. Über: Bundesdatenschutzbericht: http://www.bfd.bund.de/information/19tb0102.pdf, Abruf vom 11.06.2004

[Büll 03]
BÜLLINGEN, F.: Elektrosmog durch Mobilfunk? Akzeptanz und Risiko im Licht der öffentlichen Debatte. In: Aus Politik und Zeitgeschichte (B 42/2003), http://www.bpb.de/publikationen/9EP0Y6,1,0,Elektrosmog_durch_Mobilfunk.html, Abruf vom 22.08.2004

[CCG 03]
CENTRALE FÜR COORGANISATION GMBH (CCG) (HRSG.): „RFID – Optimierung der Value Chain – Einsatzbereiche, Nutzenpotenziale und Herausforderungen“, Managementinformation Mai 2003

[CMBC 03]
CLEMENTS, B., MAGHIROS, I., BESLAY L., CENTENO, C., PUNIE, Y., RODRÍGUEZ, C., MASERA, M.: Security and privacy for the citizen in the Post-September 11 digital age: A prospective overview. Über: http://www.jrc.es/home/publications/publication.cfm?pub=1118, Abruf vom 12.05.2004

[Com 04a]
Wal-Mart treibt RFID-Nutzung voran. In: Computerwoche vom 19.05.2004: http://www.computerwoche.de/index.cfm?pageid=254&artid=61149, Abruf vom 2.07.2004

[Com 04b]
Metro eröffnet RFID-Zentrum. In: Computerwoche vom 08.07.2004:, http://www.computerwoche.de/index.cfm?pageid=254&artid=62890, Abruf vom 13.7.2004

[Comp 04c]
Schinken an Zentrale: „Bin reif". In: Computerwoche Online: CW-EXTRA Nr. 01 vom 15.02.2002 Seite 12-13, http://www1.computerwoche.de/heftarchiv/2002/20020215/a80106467.html, Abruf vom 04.07.2004

[ComW 04]
Preismanipulation bei RFID-Transpondern. In: Computerwelt, http://www.computerwelt.at/detailArticle.asp?a=84374&n=4, Abruf vom 12.08.2004

[DrLi 04]
DRÄGER & LIENERT: TagIt Informationsmanagement. http://dlinfo.de/tagit.htm, Abruf vom 12.07.2004

[EC 95]
EUROPEAN COMMISSION: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 1995.

[ECIN 04]
ECIN: Fußball-WM 2006 baut auf RFID. In: Ecin.de, http://www.ecin.de/news/2004/01/16/06623/, Abruf vom 05.08.2004-08-09

[ECPS 02]
ESTRIN, D., CEILLER, D., PISTER, K. UND SUKHATME, G.: Connecting the Physical World with Pervasive Networks. IEEE Pervasive Computing, 1 (1): 59-69.

[ECR 04]
EFFICIENT CONSUMER RESPONSE INITIATIVE DEUTSCHLAND ÖSTERREICH UND SCHWEIZ (ECR D-A-CH): Rückverfolgbarkeit von Lebensmittel und Warenrückruf. http://www.ecr.de/ecr/award/e21/e24/e307, Abruf vom 20.07.2004

[Enge 03]
Engelhardt, Torsten: Der Hamburger Hafen. In: GEO 11/2003.

[EPC 04]
EPCGLOBAL INC.: http://www.epcglobalinc.org, Abruf vom 19.07.2004

[EPCG 04]
CCG-Expertenrunde „RFID/EPC" nimmt Arbeit auf, In: EPCGlobal vom Juni 2004, http://www.epcglobal.de/ccg/Inhalt/e56/e131, Abruf vom 19.07.2004

[Euro 03]
EUROPÄISCHE KOMMISSION: Überwachung aller Nutztiere in Europa durch elektronische Markierung, In: Innovationsreport 2003, Forum für Wissenschaft, Industrie und Wirtschaft, http://www.innovationsreport.de/html/berichte/agrar_forstwissenschaften/

bericht-18194.html, Abruf vom 14.07.2004

[Euro 04]
EURO I.D. IDENTIFIKATIONSSYSTEME, RF-IDENTIFIKATION: Für eine runde Lösung mit System, Anwendungen in der Transpondertechnologie, http://www.euroid.com, Abruf vom 02.07.2004

[FiKe 04]
FINKE, T., KELTER, H.: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. BSI, http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf, Abruf vom 12.10.2004

[Fink 02]
FINKENZELLER, K.: RFID-Handbuch. Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 3. aktualisierte und erweiterte Auflage, Hanser Fachbuchverlag, Oktober 2002, Wien. http://www.rfid-handbook.de

[FiRo]
FISHKIN, K.P. UND ROY, S.: Enhancing RFID Privacy via Antenna Energy Analysis. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA.

[Flei 01]
FLEISCH, E.: Was bringt die nächste Technologiewelle? Wenn Dinge denken lernen... http://www.m-lab.ch/pubs/Akzente_01efl.pdf, Abruf vom 11.07.2004

[Flei 04]
Die Ohrmarke bekommt elektronische Konkurrenz. In: fleischwirtschaft.de vom 03.02.2004, http://www.fleischwirtschaft.de/dokumentation/onlinearchiv/pages/show.prl?params=keyword%3DITeK%26all%3D%26type%3D1%26laufzeit%3D0&id=4454&currPage=1, Abruf vom 10.07.2004

[Fleis 04]
FLEISCH, .E.; HALLER, S.; STRASSNER, M.: Regal ruft Palette. In: SAP Info vom 16.12.2002. http://www.sap.info/public/de/article.php4/Article-49043df892f123d88/de, Abruf vom 04.08.2004

[FoeB 04]
VEREIN ZUR FÖRDERUNG DES ÖFFENTLICHEN BEWEGTEN UND UNBEWEGTEN DATENVERKEHRS E. V. (FOEBUD): Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, http://www.foebud.org/rfid/positionspapier#1, Abruf vom 12.08.2004

[FrSt 04]
FREY, H. und STURM, P. (Universität Trier): UBICOMP Episode 14. http://www.syssoft.uni-trier.de/systemsoftware/Download/Sommersemester_2004/Vorlesungen/Ubiquitous_Computing/14%20RFID.pdf

[FSL 04]
FLOERKEMEIER, C., SCHNEIDER, R., LANGHEINRICH, M.: Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), Tokyo, Japan, November 2004 http://www.vs.inf.ethz.ch/publ/papers/floerkem2004-rfidprivacy.pdf Abruf vom 09.09.2004

[FSL 04]
FLOERKEMEIER, C.; SCHNEIDER, R. und

LANGHEINRICH, M. (2004): Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols, Institute for Pervasive Computing ETH Zurich, Switzerland, http://www.inf.ethz.ch/~langhein/articles/

[GCIB 03]
GLOBAL COMMERCE INITIATIVE/IBM: Global Commerce Initiative EPC Roadmap Executive Brief, Published in association with IBM November 2003

[GInO 04]
GERMANY.INDYMEDIA.ORG vom 24.05.2004: Wer wann mit wem... , http://germany.indymedia.org/2004/05/84254.shtml, Abruf vom 12.08.2004

[Gole 04]
GOLEM.DE vom 29.03.2004: Transponder macht Handy zum Türschlüssel oder zur Geldbörse. Siemens zeigt Einsatz von Transponder in Mobiltelefonen, http://www.golem.de/0403/30559.html, Abruf vom 04.07.2004

[HaHa 04]
Der Hamburger Hafen bleibt auch 2004 auf Rekordkurs. In: DIE WELT Online vom 10. Juni 2004, http://www.welt.de/data/2004/06/10/289082.html, Abruf vom 26.08.2004

[HAMM 04]
HAMMERSCHMIT, C.: CeBIT: Nokia, Philips und Sony forcieren neuen Kommunikations-standard. In: EETIMES.de vom 18. März 2004, http://www.eetimes.de/story/OEG20040318S0010, Abruf vom 26.08.2004.

[Hand 03]
Funkchips sichern Ware gegen Diebstahl. In: HANDELSBLATT vom 19. August 2003, http://www.handelsblatt.com/pshb/fn/relhbi/sfn/buildhbi/cn/GoArt!200104,203116,654244/SH/0/depot/0/, Abruf vom 08.07.2004

[Hand 04]
Biometrie fürs Schlachtvieh – Gesetzlich geforderte Überwachung. In: Handelsblatt, Freitag, 11. Juni 2004, 13:32 Uhr, http://www.handelsblatt.com/pshb/fn/relhbi/sfn/buildhbi/cn/GoArt!200104,204819,746496/SH/0/depot/0/, 17.06.2004, Abruf vom 28.07.2004

[HBBB 03]
HILTY, L., BEHRENDT, S., BINSWANGER, M., BRUININK, A., ERDMANN, L.Z, FRÖHLICH, J., KÖHLER, A., KUSTER, N., SOM, C. und WÜRTENBERGER, F.: Das Vorsorgeprinzip in der Informationsgesellschaft Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Eine Studie der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA) und des IZT – Institut für Zukunftsstudien und Technologiebewertung im Auftrag des Zentrums für Technologiefolgen-Abschätzung beim Schweizerischen Wissenschafts- und Technologierat (TA-SWISS) von August 2003 (TA 46/2003), http://www.ta-swiss.ch/www.remain/projects_archive/information_society/pervasive_d.htm, Abruf vom 16.08.2004.

[Heis 03]
Gillette will von Bespitzelung durch RFID-Tags nichts wissen. In: Heise Online vom 15.08.2003, http://www.heise.de/newsticker/meldung/39458

13. Quellenverzeichnis

[Heis 04a]
Funketiketten für japanische Schulkinder. In: Heise Online vom 11.07.2004, http://www.heise.de/newsticker/meldung/49004, Abruf vom 23.07.2004

[Heis 04b]
RFID-Umfrage – Fußball-WM 2006 soll den Durchbruch bringen. In: Heise Online vom 21.04.2004, http://www.heise.de/newsticker/meldung/print/46724, Abruf vom 05.08.2004

[Heis 04c]
Fußball-WM 2006: Nur mit RFID ins Stadion. In: Heise Online vom 15.01.2004, http://www.heise.de/newsticker/meldung/43645, Abruf vom 26.06.2004

[Heis 04d]
Münchner Grüne wollen City-Maut mit RFID-Technologie. In: Heise Online vom 23.05.2004 http://www.heise.de/newsticker/meldung/47583, Abruf vom 26.08.2004

[HeMü 04]
HENRICI, D. und MÜLLER, P. (2004): Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha A., Mattern F.: Pervasive Computing (Proceedings of PERVASIVE 2004, Second International Conference on Pervasive Computing). Springer-Verlag, LNCS 3001: 219-224

[Hill 03a]
HILLENBRAND, T.: Wissen ist Verbrauchermacht. In: Spiegel Online vom 3. September 2003, http://www.spiegel.de/wirtschaft/0,1518,262761,00.html, Abruf vom 12.07.2004

[Hill 03b]
HILLENBRAND, T.: Zeigefreudige Models, hilfsbereite Mülltonnen. In: Spiegel Online vom 3. September 2003, http://www.spiegel.de/wirtschaft/0,1518,262758,00. html, Abruf vom 12.07.2004

[Hilt 04]
HILTY, LORENZ: Verselbständigt sich der Computer? Pervasive Computing könnte den Menschen schrittweise entmündigen. Electrosuisse Bulletin SEV/AES, 9/2004

[HMM 04]
HENRICI, D., MÜLLER J. und MÜLLER P. (in press): Sicherheit und Privatsphäre in RFID-Systemen. AG Integrierte Kommunikationssysteme, Technische Universität Kaiserslautern, 18. DFN-Arbeitstagung über Kommunikationsnetze, Springer, Lecture Notes in Informatics. 1.-4. Juni 2004, Düsseldorf

[Höni 03]
HÖNICKE, INA: Probleme und Problemchen mit RFID. In: ZDNet. http://www.zdnet.de/itmanager/tech/0,39023442,2137403,00.htm, Abruf vom 27.08.2004

[ICAO 04a]
INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO): PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Technical Report, published by authority of the Secretary General, http://www.icao.int/mrtd/Home/Index.cfm, Abruf vom 10.09.2004

[ICAO 04b]
INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO): Development of a logical data stucture – LDS. For optional Capacity Expansion Technologies, Revision -1.7, published by authority of the Secretary General http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf, Abruf vom 10.09.2004

[Idel 98]
IDEL, A.: Krankheitsresistenzen bei landwirtschaftlich genutzten Tieren. In: Nutztierhaltung 4/1998. http://www.ign-nutztierhaltung.ch/NTH/PDF1998/nutz_498.pdf, Abruf vom 10.07.2004

[Iden 04]
IDENTEC SOLUTIONS: Volkswagen Processes Pre-delivery Automobiles with RFID. http://www.identecsolutions.com/pdf/IDENTEC%20SOLUTIONS_Volkswagen%20Case%20Study_2003.pdf, Abruf vom 24.07.2004

[IDTE 04]
IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. May 20, 2004. URL: http://www.idtechex.com/products/en/article.asp?articleid=7&topicid=79.

[IEEE 04]
IEEE: P1363.2: Standard Specifications for Password-Based Public-Key Cryptographic Techniques, version D16, July; verfügbar unter: http://grouper.ieee.org/groups/1363/passwdPK/draft.html (16.07.2004)

[Infi 02]
INFINEON: Short Product Information: Security & Chip Card Ics my-d products for contactless systems my-s vicinity SRF 55V10P July 2002 http://www.infineon.com/cmc_upload/documents/029/172/SPI_SRF55V10P_0702.pdf

[Inno 04a]
Innovationsreport – Forum für Wissenschaft, Industrie und Wirtschaft: Michelin bringt funkende Reifen, http://www.innovations-report.de/html/berichte/innovative_produkte/bericht-15756.html, Abruf vom 10.07.2004

[Inst o.J.]
INSTITUTE FOR THE PROTECTION AND SECURITY OF THE CITIZEN: IDEA Project – Identification Electronique des Animaux, Final Report, http://idea.jrc.it/pages%20idea/index%20of%20final%20report.htm, Abruf vom 04.08.2004

[Isch 04]
ISCHEBECK, B.: Objekte an der Funkleine. In: Funkschau 13/2004, S. 31 – 33

[ISK 03]
ISK – ISERLOHNER KUNSTSTOFF-TECHNOLOGIE GMBH: Verbundprojekt: Werkzeugidentifikation und -Management, http://www.isk-design.de/pdf/prospekte/transponder_flyer.pdf, Abruf vom 05.08.2004

[JRS 03]
JUELS, A., RIVEST, R.L. und SZYDLO, M.: The Blocker Tag: Selective Blocking of RFID-Tags for Consumer Privacy. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/

[Katz 04]
KATZENFREUNDE NORDEUTSCHLAND E. V.: Mikrochip: Sichere Identifizierung Ihres

13. Quellenverzeichnis

Tieres – ein Leben lang. http://www.kfndev.de/informatives_mikrochip. html, Abruf vom 04.08.2004

[Klaß 04]
KLAß, C.: Einkaufsbetrug mit RFID-Umprogrammierung. In: Networld, 29.07.2004 http://www.golem.de/0407/32666.html

[Krem 04]
KREMPL, S.: Das Internet der Dinge. In: Computerworld 5/2004, http://viadrina.euv-frankfurt-o.de/~sk/Pub/rfid-cw04.html, Abruf vom 02.07.2004

[Kric oJ]
KRICK, O.: Identsystem OIS-U: RFID Solution for Deutsche Post, http://www.identecsolutions.com/pdf/IDENTEC%20SOLUTIONS_Deutsche%20Post%20Case%20Study_2003.pdf, Abruf vom 25.08.2004

[Land 01]
LANDT, JEREMY: Shrouds of Time – The history of RFID. An AIM (The Association for Automatic Identification and Data Capture Technologies) Publication, http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf, Abruf vom 09.08.2004

[Land 04]
LANDKREIS BAMBERG: Restmülltonne mit Identsystem – Abfalltrennung wird künftig belohnt, http://www.landkreis-bamberg.de/index.phtml?start=1sowie http://www.markt-heiligenstadt.de/verwaltung/umwelt/abfallkonzept/restmuelltonne.shtml, Abruf vom 10.07.2004

[Lang 04]
LANGHEINRICH, M.: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. Über http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf [13.08.2004]

[LePh 04]
LE PHAN MICHÈLE LA: RFID – Große Wirkung kleiner Chips. In: comtec 03/2004 http://www.swisscom-comtec.ch/pdf/comtec032004130.pdf, Abruf vom 05.08.2004

[LLS 00]
LAW, C., LEE, K. und SIU, K.Y.: Efficient Memoryless Protocol for Tag Identification. Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Boston, MA, USA. 75-84, verfügbar unter: http://portal.acm.org/citation.cfm?id=345865&dl=ACM&coll=portal (16.07.2004)

[Malo 04]
MALONE, M.: Case in Point. High Volume File Management Made Efficient with RFID Technology. http://multimedia.mmm.com/mws/mediawebserver.dyn?qqqqqq&8iBEqKUrq1UrqqqORGaQQQQQ5-, Abruf vom 21.07.2004

[Mark o.J.]
o.V. Druckkontrolle gegen Autorolle. In: Informations- und Beratungsplattform www.MarkteinstiegUSA.de, http://www.markteinstiegusa.de/Reifendruck-Kontrollsysteme.521.0.html, Abruf vom 08.09.2004

[MaRö 03]
MATTERN, F. UND RÖMER, K.: Drahtlose Sensornetze. In: Informatik-Spektrum, Vol. 26 No. 3, S. 191-194.

[MASS 04]
MASSEX SYSTEMHAUS: x-trade und RFID in der Kühlkette, http://www.maxess.de/index.php?id=113&backPID=25&L=0&tt_news=7, Abruf vom 05.08.2004

[Matt 02]
MATTERN, F.: Der Trend zur Vernetzung aller Dinge – Pervasive Computing und die Zukunft des Internets. In: Neue Kommunikationsanwendungen in modernen Netzen, Seiten 9-13. ITG-Fachtagung, Februar 2002. http://www.inf.ethz.ch/vs/publ/papers/VernetzungAllerDinge.pdf, Abruf vom 19.08.2004

[MBZK 04]
Ministerie van Binnenlands Zaken en Koninkrijksrelaties: Praktijkproef biometrie in reisdocumenten start 1 september in zes gemeenten. Pressemitteilung vom 27.05.2004, http://www.minbzk.nl/persoonsgegevens_en/in_het_kort/persberichten/praktijkproef, Abruf vom 18.10.2004

[McKa 03]
MCCUE, A. und KAUFMANN, J.: Sun eröffnet RFID-Testcenter in Europa. In: ZDNet vom 08.12.2003, http://www.zdnet.de/news/business/0,39023142,39118100,00.htm), Abruf vom 12.07.2004

[Mose 04]
MOSER, P.: Praxisbeispiel aus der Automobilindustrie zeigt Einsparpotentiale der RFID-Technologie. In: Logistik für Unternehmen vom 08.04.2004, http://www.mylogistics.net/de/news/themen/key/news104382/jsp, Abruf vom 07.07.2004

[Mylo 04]
Mylogistics.net – Logistik für Unternehmen: Fraunhofer-Gesellschaft gründet RFID-Test-Labor in Magdeburg, http://www.mylogistics.net/de/news/themen/key/news146902/jsp, Abruf vom 14.7.2004

[NFC 04a]
NFC Forum, http://www.nfc-forum.org/ , Abruf vom 25.07.2004

[NFC 04b]
Nokia, Philips and Sony establish the Near Field Communication (NFC) Forum. Forum will drive industry uptake of intuitive NFC technology that enables touch-based interaction with electronic devices. Presseerklärung von Nokia, Philips und Sony, 18.03.04, http://www.nfcforum.org/pdfs/NFC_Forum_Announcement.PDF, Abruf vom 23.08.2004

[Noga 00]
NOGALA, D. F: Der Frosch im heißen Wasser – Die Trivialisierung von Überwachung in der informatisierten Gesellschaft des 21. Jahrhunderts. In: TELEPOLIS, http://www.heise.de/tp/deutsch/inhalt/co/8988/1.html, Abruf vom 18.08.2004

[OECD 80]
OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal

13. Quellenverzeichnis

Data, O.E.C.D. Document C(80)58(Final), October 1, 1980

[ORF 04a]
Ein RFID-Rechner aus Pappkarton. In: ORF FutureZone vom 05.03.2004, http://futurezone.orf.at/futurezone.orf?read=detail&id=219132&tmp=7798, Abruf vom 20.07.2004

[ORF 04b]
RFID-Armbänder für Patientendaten. In: ORF FutureZone vom 27.07.2004, http://futurezone.orf.at/futurezone.orf?read=detail&id=240826&channel=1, Abruf vom 30.07.2004

[OSK 03]
OHKUBO, M., SUZUKI, K. und KINOSHITA, S.: Cryptographic Approach to „Privacy-Friendly" Tags. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA.

[Phil 01]
Product News From Philips Semiconductors: Philips Semiconductors launches SmartMX, a versatile, highly secure 8051-based family of smart card microcontrollers, tailored to current and future market requirements. Pressemitteilung vom 23. Oktober 2001, http://www.semiconductors.philips.com/news/content/file_758.html, siehe auch ergänzend http://www.semiconductors.philips.com/news/publications/ content/file_927.html, Abruf vom 14.09.2004

[Phil 04]
PHILLIPS AUSTRIA: it Philips RFID Know-how gegen Tierseuchen in Europa, http://www.philips.at/InformationCenter/NO/FArticleSummary.asp?lNodeId=1253&channel=1253&channelId=N1253A3254, Abruf vom 09.08.2004

[Pößn 04]
PÖßNECK, L.: Fußball-WM: Golden Goal für RFID? Die Fans wollen ein Fußballfest, die Industrie eine IT-Mustermesse. In: Silicon.de, http://www.silicon.de/cpo/hgrmobile/detail.php?nr=14566&directory=hgr-mobile, Abruf vom 05.08.2004

[Pres 03]
PRESS RELEASES: Tierseuchenbekämpfung: Byrne begrüßt die Verabschiedung von Kennzeichnungsvorschriften für Schafe und Ziegen durch den Rat, Reference: IP/03/1761, Brüssel, den 17.12.2003, http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/03/1761&format=HTML&aged=0&language=DE&guiLanguage=en#file.tmp_Ref_1, Abruf vom 03.08.2004

[Prog 04]
PROGRESS SOFTWARE O. V.: RFID-Integration – Brückenschlag vom Transponder zur Unternehmensanwendung, http://www.progress.com/worldwide/de/docs/rfid_whitepaper_de_gif.pdf, Abruf vom 24.07.2004

[Quac 04]
QUACK, K.: Transponder meldet: „Wartung ausgeführt". In: Computerwoche Online, http://www.computerwoche.de/index.cfm?pageid=256&artid=52033, Abruf vom 12.07.2004

[RaEf 02]
RANKL, W.; EFFING, W.: Handbuch der Chipkarten. Aufbau – Funktionsweise – Einsatz von Smart Cards. 2., überarbeitete und aktualisierte Auflage. München und Wien.

[RFID 03]
RFID Journal (2003) Class 1, G2, EPC Tags Ready by Q4, http://www.rfidjournal.com/article/articleview/714/1/1, Abruf vom 09.09.2004

[RF-ID 04]
RFID-ID.com: 869MHz RF-ID Tags Read Only and Programable, http://www.rf-id.com/rfidit.html, Abruf vom 26.08.2004

[Richt 02]
RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

[Robe 04]
ROBERTI, MARK: Standardizing EPC Data-Sharing. In: RFID Journal, http://www.rfid-journal.com/article/articleview/ 878/1/1/, Abruf vom 20.04.2004

[Roth 03]
ROTHE, M.: Big Brother im Panopticon? Überwachung aus liberaler und autonomiekritischer Sicht. In: TELEPOLIS, http://www.heise.de/tp/deutsch/inhalt/co/12842/1.html, Abruf vom 09.08.2004

[RPG 01]
ROßNAGEL, A.; PFITZMANN, A.; GARSTKA, H.: Modernisierung des Datenschutzrechts. Berlin: Bundesministerium des Innern, 2001

[SAP 04]
SAP: SAP-Lösungen mit RFID finden steigende Verbreitung. http://www.sap.com/austria/company/presse/texte_2004/press39_04_07.asp, Abruf vom 31.07.2004

[Scha 04]
SCHAAR, P.: „Smart Chips: Kleine Brüder oder große Chance? Datenschutz und Verbraucherschutz vor neuen Herausforderungen". Referat des Bundesbeauftragten für den Datenschutz auf der Veranstaltung der Heinrich-Böll-Stiftung in Kooperation mit dem Netzwerk Neue Medien e. V. am 05. April 2004 in Berlin, http://www.bfd.bund.de/aktuelles/akt20040513.pdf, Abruf vom 19.08.2004

[Schl 03]
SCHLÜTER, A.: Integrationshandbuch Microsoft-Netzwerk. Windows Server 2000/2003, Active Directory, Exchange Server, Windows XP und Office XP/2003 im Einsatz. Bonn, S. 841 ff. Hier zitiert nach http://www.wintotal.de/Artikel/Internetarbeit/internetarbeit.php [13.08.04]

[Schu 00]
SCHUERMANN, J.: Information technology – Radio frequency identification (RFID) and the world of radio regulations. In: ISO Bulletin May 2000, S. 4. http://www.iso.org/iso/en/commcentre/pdf/Radio0005.pdf

[Schu 04a]
SCHULZKI-HADDOUTI, C.: Elektronischer Pass – „Biometrische Reisepässe" mit RFID-Transpondern in der Einführungsphase. In: c't 9/2004, S. 52: Biometrie, http://www.heise.de/ct/04/09/052/default.shtml, Abruf vom 18.07.2004

[Schu 04b]
SCHULZKI-HADDOUTI, C.: Neue Reisepässe: Mit Sicherheit teuer, In: Online Magazin Sicherheit heute, http://www.sicherheitheute.de/index.php?cccpage=readtechnik&set_z_artikel=8, Abruf vom 12.07.2004

[SEC 04a]
SEC-WORLS.NET: Erste Auto-Nummernschilder mit RFID-Technologie, http://www.sec-world.net/news/66876-erste-autonummernschilder-mit-rfidtechnologie.html, Abruf vom 16.08.2004

[SEC 04b]
SEC-WORLS.NET: Infineon – Gesprächige Chipkarten, http://www.sec-world.net/news/66688-infineon-gespraechige-chipkarten.html, Abruf vom 16.08.2004

[Sili 04]
Silicon.de vom 06.04.2004: RFID – Die Technik macht Missbrauch leicht möglich, http://www.silicon.de/cpo/hgrmobile/detail.php?nr=14036, Abruf vom 05.08.2004

[Sili 04]
Silicon.de vom 25.05.2004: Postunternehmen starten RFID-Mega-Test. http://www.silicon.de/cpo/news-mobile/detail.php?nr=14739&directory=news-mobile, Abruf vom 12.07.2004

[Sinn 04]
SINN, D.: Auf RFID ist die IT schlecht vorbereitet, In: Computerwoche Online, http://www.computerwoche.de/index.cfm?pageid=256&artid=58094&main_id=58094&category=25&currpage=1&type=detail&kw=, Abruf vom 8.07.2004

[Sore 04]
SOREON RESEARCH: Überholspur: RFID-Markt Handel in Europa 2004-2008.Pressemitteilung: 11.05.2004 – Soreon Research http://www.pressrelations.de/index.cfm?start_url=http%3A//www.pressrelations.de/search/release.cfm%3Fr%3D155879%26style%3D, Abruf vom 14.7.2004

[SSSR oJ]
STEPHEN A. WEIS, SANJAY E. SARMA, RONALD L. RIVESTAND DANIEL W. ENGELS: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems

[Stan 04]
PHILIPS SEMICONDUCTORS: Mehr Mitarbeiter, neue Kontaktlos-Technologie. In: Der Standard vom 10. Juni 2004, http://derstandard.at/?url=/?id=1684583, Abruf vom 10.08.2004

[StFl 04]
STRASSNER, M. und FLEISCH, E.: Ubiquitous Computing in der Flugzeugwartung. http://www.m-lab.ch/pubs/Strassner_Lampe_Fleisch_MultiK2004.pdf, Abruf vom 31.07.2004

[TAB 03]
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG: „Biometrie und Ausweisdokumente“ Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zusammenfassung des TAB-Arbeitsberichtes Nr. 93, http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.htm, Abruf vom 12.05.2004

[tecc 04]
techchannel.de vom 02.07.2004: Delta Air Lines verfolgt Gepäck mit RFID, http://www.tecchannel.de/news/hardware/16170/, Abruf vom 04.07.2004

[Texa 04]
Elektronische Tiererkennung. In: Texas Trading Rinderhaltung 2003 / 2004, http://www.texas-trading.de/pdf/elektronische_tiererkennung_03-04.pdf, Abruf vom 27.07.04

[Verdi 04]
Presseinformation des Bundesvorstands ver.di Vereinte Dienstleistungsgesellschaft vom 07. Juli 2004: Bespitzelung von Beschäftigten nimmt zu. Über http://www.onlinerechte-fuerbeschaeftigte.de/service/press_releases/040624155116 [13.08.04]

[Vere 04]
Nutztieridentifikation durch Retina-Scanning – Optibrand stellt neue Lösung für Identifikation und Nachverfolgung von Nutztieren vor. In: Veredelungsproduktion – das Infoportal für Landwirte. http://www.veredelungsproduktion.de/pages/de/grundlagen/cpd/836.html, Abruf vom 28.07.2004.

[Vibe 04]
VEREIN FÜR INTERNET-BENUTZER ÖSTERREICHS (VIBE!AT) ÖSTERREICHS: Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, http://www.vibe.at/verein/, Abruf vom 12.08.2004

[Vinc 03]
VINCENZ, M.: Möglichkeiten und Grenzen heutiger Transpondertechnologien in der Logistik. Idealisierter Wunschtraum versus bezahlbare Realität. VDI Bericht Nr. 1744 zum 12ten Deutschen Materialflusskongress, März 2003, verfügbar unter: http://www.iqpaper.com/pdf/M%F6glichkeiten %20und%20Grenzen%20heutiger%20Transpondertechnologien.pdf, o. S.

[Vit 04]
VEREINIGTE INFORMATIONSSYSTEME TIERHALTUNG W. V. (VIT): ITeK-Rind, http://www.vit.de/ITeK-Rind.html#Section946, Abruf vom 04.08.2004

[Vogt 02]
VOGT, H.: Efficient Object Identification With Passive RFID Tags. In: Mattern F., Nagshineh M.: Proceedings of the First International Conference on Pervasive Computing (Pervasive 2002). Springer-Verlag, LNCS 2414, 98-113

[Ward 04]
WARD, DIANE MARIE: 5-Cent Tag Unlikely in 4 Years. In: RFID Journal, http://www.rfidjournal.com/article/articleview/1098/1/1/, Abruf vom 15.09.2004

[Weis 03]
WEIS, S.A.: Security and Privacy in Radio-Frequency Identification Devices. Masters Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, verfügbar unter: http://theory.lcs.mit.edu/~sweis (16.07.2004)

[WSRE 03]
WEIS, S.A., SARMA, S.E., RIVEST, R.L. und ENGELS, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, Boppard, März 2003. Springer-Verlag, LNCS 2802: 201-212

[ZDNe 04]
o.V.: RFID-Zentrum von Infineon präsentiert industrielle Lösungen. Flächendeckender Einsatz von RFID-Chips. In: ZDNet.de, http://www.zdnet.de/itmanager/tech/0,39023442,391216812,00.htm, Abruf vom 09.08.2004

[ZEBR 03]
ZEBRA TECHNOLOGIES CORP.: RFID – The Next Generation of AIDC Application white paper (2003) Im Internet u. a. unter http://www.rsiidtech.com/brochures/Zebra%20RFID%20White%20paper.pdf.

[Zeid 03]
ZEIDLER, M.: RFID – Der Schnüffelchip im Joghurtbecher. In: Monitor vom 08.01.2004, http://www.wdr.de/tv/monitor/pdf/040108f_rfid.pdf, Abruf vom 12.08.2004