RFID-Technologie

Dieses Buch steht im Regal Elektrotechnik sowie im Regal EDV.

„RFID-Technologie“ ist nach Einschätzung seiner Autoren zu 50% fertig

Diese Seite hat mittlerweile eine Größe erreicht, die es als geeignet erscheinen lässt, sie in mehrere einzelne Seiten zu zerlegen. In welche Teile diese Seite zerlegt werden könnte, kann auf der Diskussionsseite besprochen werden. Wie man es macht, steht im Wikibooks-Lehrbuch im Abschnitt **Buch in Kapitel untergliedern**.

1 Einleitung

Radio **F**requency **ID**entification (engl. für Funkfrequenz-Identifizierung) ist eine Methode, um Daten berührungslos und ohne Sichtkontakt lesen und speichern zu können. RFID-Systeme eignen sich grundsätzlich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss[1].
Durch die rasante Ausbreitung der Technologie im privaten und wirtschaftlichen Bereich ist der Begriff aktueller denn je. Trotzdem werden nur wenige Themen so kontrovers diskutiert wie der Einsatz der RFID-Technologie. Einerseits sind die Unternehmen bestrebt, die Möglichkeiten und Chancen der RFID-Technologie zu bewerben (Beispiel Werbespot von IBM) und eine breite Akzeptanz zu schaffen, andererseits versuchen Datenschützer und Bürgerrechtler, der immer größer werdenden Überwachung durch Sensibilisierung der Bürger entgegenzuwirken.

Kern der Diskussion bildet die Frage, wieviel Daten wirklich erfasst werden müssen und welche Daten die Persönlichkeitsrechte der Bürger verletzen.
Die folgende Arbeit wird die verschiedenen Standpunkte der Befürworter und Kritiker der Technologie beleuchten. Ausgehend von der historischen Entwicklung, der Vorstellung der Technologie (Aufbau und Formen) und dem Aufzeigen der vielfältigen (Einsatz-)Möglichkeiten sollen die Chancen und Risiken genauer betrachtet werden. Ziel ist es nicht, vorgefertige Meinungen zu präsentieren, sondern vielmehr die Argumente der verschiedenen Parteien gegenüberzustellen und es dem Leser zu überlassen, wie er sich positioniert.

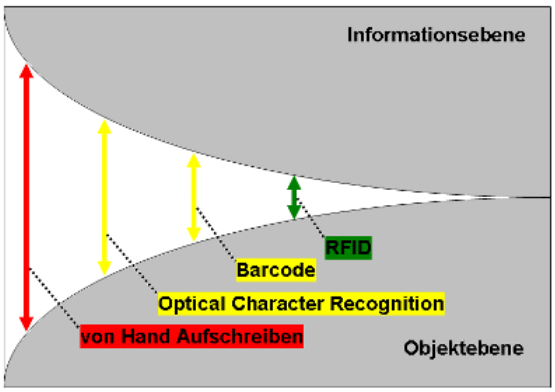
2 Geschichte von RFID

Die ersten Einsätze der RFID verwandten Technologien datieren aus dem zweiten Weltkrieg. Als Erste entwickelten die Briten ein aktives auf Radar- und Rundfunktechnologie basierendes System zur Flugzeugerkennung (Freund- und Feinderkennung). Als Grundlage dieses Systems gilt die Radarentwicklung aus dem Jahr **1935** vom schottischen Physiker Robert Alexander Watson-Watt. Jedes britische Flugzeug sendete aktiv ein Signal aus, welches vom Bodenradar empfangen wurde und so das Flugzeug als Freund oder Feind eindeutig identifiziert werden konnte.

Als die eigentliche Geburtsstunde der modernen RFID-Technologie gilt die Publikation „Communications by Means of Reflected Power“ von Stockman aus dem Jahr **1948**. Der Autor beschreibt die Möglichkeit, RFID-Transponder mit Hilfe der von dem Radiosignal ausgestrahlten Energie zu betreiben und führt somit das Konzept der passiven RFID-Systeme ein (vgl. Garfinkel/Rosenberg 2006, S. 16). In den 50er und 60er Jahren entwickelten Forscher auf der ganzen Welt die Idee der RFID-Technologie weiter. Gegenstand der Untersuchungen war, wie die vorhandene Technologie genutzt werden kann, um Objekte schnell und fehlerfrei zu identifizieren. Während in den 50er Jahren die Technologie vor allem militärisch genutzt wurde, setzte sich die kommerzielle Nutzung als Artikelsicherung im Laufe der 60er Jahre durch. 1-Bit-Transponder wurden an den Artikeln befestigt und lösten ein Signal aus, sobald sie in die Nähe eines Lesegerätes kamen.

Mario Cardullo patentierte **1973** als erster die aktive RFID-Technologie mit einem wiederbeschreibaren Chip. Im selben Jahr patentierte Charles Walton eine passive RFID-Technologie, um Türen ohne einen Schlüssel zu öffnen. Eine Karte kommunizierte mit einem Lesegerät in der Nähe der Tür, um den/die Besitzer zu identifizieren. Im Laufe der Zeit verbesserten verschiedene Hersteller die Technologien, um mehr Daten speichern zu können und um die Reichweite der Transponder sukzessive zu erhöhen. Beispielsweise entwickelte IBM **1990** ein “ultra-high frequency"-(UHF-)RFID-System. UHF erlaubt eine Sendereichweite von bis zu 6,5 Metern (20 Fuß). Das System wurde zusammen mit dem Pilotkunden Wal-Mart getestet, musste aber aus finanziellen Gründen Mitte der 90er Jahre eingestellt werden.

Zur Jahrtausendwende erlebte die RFID-Technologie einen nochmaligen Schub, als zwei Professoren, David Brock und Sanjay Sarma, preisgünstige RFID-Chips entwickelten, um jedes Produkt damit auszustatten. Außerdem nutzten sie die Chips als mobile Datenbanken, um alle Informationen über das Produkt und alle Produktbewegungen zu dokumentieren. Damit war es beispielsweise möglich, Warenbewegungen nicht nur für den Lieferanten, sondern auch für den Kunden so transparent zu gestalten, dass jederzeit der Status der Lieferung überwacht werden konnte.



3 Auto-ID-Systeme

RFID-Systeme gehören zur Gruppe automatischer Identifikationssysteme (Auto-ID-Systeme). Dieser Gruppe werden bspw. auch die folgenden Systeme, Technologien bzw. Verfahren zugeordnet:[2][3][4]

- Barcode
- Schrifterkennung (Optical Character Recognition - OCR)
- Spracherkennung
- Biometrische Verfahren
- Warensicherungssysteme auf RF- oder EM-Grundlage
- Magnetstreifen
- Kontakt-Chipkarten

Eine Hauptaufgabe solcher Systeme besteht, wie es die Bezeichnung Auto-ID-Systeme bereits vermuten lässt, darin, automatisiert Objekte (bspw. Personen, Tiere, Güter, Waren, Gegenstände, …) zu identifizieren und sie für Maschinen lesbar zu machen. Dies reduziert nicht nur den Aufwand bei der Datenerfassung, sondern führt bspw. auch zu einer Verringerung von Ungenauigkeiten und somit zu entsprechend weniger Prüfungsaufwand.[2] Zur besseren Abgrenzung der unterschiedlichen Einsatzgebiete (z.B. in Bezug auf genutzte Standards, Frequenzen etc.) wurde im Rahmen einer EU-Studie ein RFID Referenzmodell entwickelt (“RFID Referencemodell”).

Die zwischen Objekt- und Informationsebene bestehende Lücke kann durch Auto-ID-Systeme so überwunden bzw. verkleinert werden.[2] Weil der Abstand zwischen beiden Welten gerade bei RFID gestützten Systemen nur noch sehr klein ist, ist bereits von einem “Internet der Dinge” die Rede.

Neben der Identifikation können Auto-ID-Systeme weitere Aufgaben wie bspw. Tracking und Tracing oder auch Sicherheit übernehmen.[4] Die Anwendungsbereiche die sich daraus ableiten, decken ein Spektrum ab, welches von der Erfassung von Warenflüssen über Zugangskontrollen für Gebäude bis hin zu Abrechnungssystemen reicht. Dementsprechend unterschiedlich können dann auch die Anforderungen an ein solches Auto-ID-System sein. Sind bei Massenanwendungen im Bereich der Warenkennzeichnung kostengünstige Systeme wie der Barcode gefragt, müssen bei Zutrittskontrollen fälschungssicherere und zuverlässigere, entsprechend teurere Systeme, wie bspw. biometrische Systeme zur Personenidentifikation, eingesetzt werden.[2]

Aufgrund dieser vielfältigen Möglichkeiten sind Auto-ID-Systeme seit Jahren etabliert.

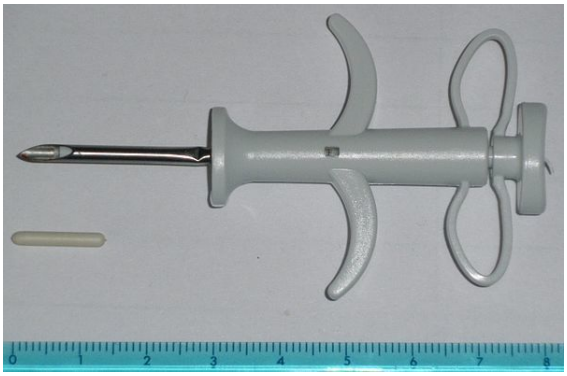
4 Grundlagen der RFID-Technologie

4.1 Systembestandteile

Ein RFID-System besteht grundsätzlich aus mindestens zwei Hauptkomponenten, einem RFID-Lesegerät und einem RFID-Datenträger (RFID-Transponder). Vorwiegend gehören jedoch mehrere Lesegeräte und ein vielfaches mehr an Transpondern zu einem RFID-System. Ein RFID-Transponder braucht nicht mit dem Lesegerät in Kontakt zu kommen, deshalb wird meist von kontakt- oder berührungslosen Systemen gesprochen. Der Transponder kann in Sekunden ausgelesen werden, wobei die Umgebungstemperatur und -beschaffenheit keine Rolle spielt. Durch Kommunikation über Radiowellen können verschiedene Materialien durchdrungen werden.Der Grundaufbau eines RFID-System soll in der Grafik verdeutlicht werden.[3]

4.1.1 RFID-Datenträger

Der RFID-Datenträger wird meist unter dem Begriff Transponder (olaf und porter) verwendet. Ein RFID-Transponder besteht aus einem Mikrochip. Dieser Chip



ist mit einer Antenne (Spule oder Dipol) versehen, die mit dem entsprechenden Lesegerät kommuniziert. Über ein elektronisches Kopplungsverfahren werden alle Daten per Modulation ausgetauscht. Die Energieversorgung der Transponderchips wird bei vielen RFID-Systemen ebenfalls über die Kopplung realisiert. Bei den RFID-Transpondern wird auch häufig von RFID-Chips, -tags, -labeln oder -etiketten gesprochen.
In biometrischen Authentifikationssystemen werden die RFID-Transponder als Datenspeicher für technische Abbilder von persönlichen Körpermerkmalen genutzt. Sie werden als Schlüssel bei den autorisierten Personen getragen. Diese Arten von Transpondern können in Plastikkarten, z. B. kontaktlosen Chipkarten einlaminiert werden.
Bei der Art der Informationsverarbeitung im Transponder gibt es ein breites Spektrum zwischen Low-End- und High-End-Systemen: [3]

- 1-Bit-Transponder
  Diese so genannten EAS-Systeme (elektronische Artikelsicherung) dienen nur zum Erkennen, ob sich ein Transponder im Empfangsbereich des Erfassungsgerätes befindet. Haupteinsatzgebiet ist die Diebstahlsicherung von Waren. Am Ausgang des Geschäftes befindet sich ein Empfangsgerät, welches registriert, wenn sich ein nicht deaktivierter Transponder in dessen Empfangsbereich befindet.

- Read-only-Transponder
  Diese Transponder sind mit einem Mikrochip ausgestattet, auf dem eine eindeutige Seriennummer gespeichert ist. Diese wird in der Regel bereits bei der Produktion des Transponders generiert. Sobald sich ein solcher Transponder im Empfangsbereich eines Erfassungsgerätes befindet, beginnt dieser ständig seine Seriennummer zu senden (unidirektionaler Datenfluss). Diese Verfahrensweise ist überall dort gut geeignet, wo es auf die eindeutige Identifizierung von Objekten ankommt (z. B. Tieridentifikation, Sendungsverfolgung).

- Transponder mit beschreibbarem Speicher
  Als Speicher wird hier ein EEPROM (passive Transponder) bzw. ein SRAM (aktive, also batteriegestützte Transponder) genutzt. In einer fest codierten State-Machine können diese Transponder einfache Kommandos des Erfassungsgerätes ausführen. Dadurch wird ein selektives Lesen bzw. Beschreiben des Speichers ermöglicht.

- kontaktlose Chipkarten mit Betriebssystem
  Aufgrund des Einsatzes eines eigenen Betriebssystems (Smart-Card-OS) und eines Mikroprozessors sind komplexe Algorithmen zu Chiffrierung und Authentifizierung möglich.

4.1.2 RFID-Lesegerät

Das Lesegerät besteht je nach eingesetzter Technologie aus einer Lese- bzw. einer Schreib-/ Leseeinheit. Die Einheit liest somit Daten vom Transponder und weist diesen gegebenenfalls an, weitere Daten zu speichern. Darüber hinaus kontrolliert das Lesegerät die Qualität der Datenübermittlung. Die Lesegeräte sind typischerweise mit einer zusätzlichen Schnittstelle ausgestattet, um die empfangenen Daten an ein anderes System (z. B. PC, Automatensteuerung oder Authentifikationssystem) weiterzuleiten und dort zu verarbeiten.
Das RFID-Lesegerät, welches die RFID-Transponder in seiner Reichweite erkennt startet die Kommunikation die einem bestimmten Protokoll unterliegt. Diese Informationen werden auf Energiewellen ausgetauscht, wobei das zu übertragende Nutzsignal in ein so genanntes Trägersignal umgewandelt wird. Das zur Kommunikation erzeugte Feld wird auch als RF-Feld (Radio-Frequenz-Feld) bezeichnet.

Alle Schreib- und Leseoperationen, die im RFID-System erfolgen, werden nach dem hierarchischen Master-Slave-Prinzip durchgeführt. An oberster Stelle steht hierbei die Applikationssoftware, von der alle Operationen ausgehen. Das Erfassungsgerät wirkt dabei als Interface zwischen Applikation und Transponder. Mit Hilfe des Erfassungsgerätes, welches aus einem Hochfrequenzinterface, einem Controller und einer Antenne besteht, kann man die Daten des Transponders auslesen und gegebenenfalls auch auf diesen schreiben. Das HF-Interface wird zur Erzeugung der hochfrequenten Sendeleistung, zur Modulation des Sendesignals und zum Empfang und Demodulation von HF-Signalen eingesetzt. Die Steuerung (control unit) hat folgende Aufgaben:[3]

- Kommunikation mit der Applikationssoftware

- Ausführung von Kommandos der Applikationssoftware

- Steuerung der Kommunikation mit dem Transponder (Master-Slave)
- Signalcodierung und -decodierung
- ggf. Ausführung des Antikollisionsverfahrens
- ggf. Chiffrierung und Dechiffrierung des Datenstroms zw. Transponder und Erfassungsgerät
- ggf. Abwicklung der Authentifizierung zw. Transponder und Erfassungsgerät

4.2 Ausführungen und Bauformen 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:[3]

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:[3]

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.

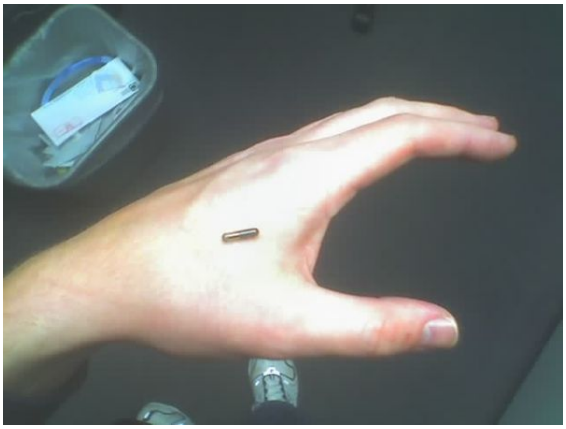
RFID-Systeme können darüber hinaus weitere Leistungsmerkmale aufweisen, z. B. die Speicherung von zusätzlichen Daten sowie Sicherheitsfunktionen oder die Kopplung mit Sensoren.

Ein RFID-Tag kann in Form und Größe variieren, je nach Modell und Ausführung von wenigen Millimetern bis einigen Zentimetern. Das Aussehen kann von rund und massiv, bis flach und flexibel beliebig angepasst werden. Je nach Anwendungsgebiet unterscheiden sich auch die sonstigen Kennzahlen wie z. B. Funkfrequenz, Übertragungsgeschwindigkeit, Lebensdauer, Kosten pro Einheit, Speicherplatz und Funktionsumfang. Maßgeblich für die Baugröße sind die Antenne und das Gehäuse. Die Form und Größe der Antenne ist abhängig von der Frequenz bzw. Wellenlänge. Je nach geforderter Anwendung werden Transponder in unterschiedlichen Bauformen, Größen und Schutzklassen angeboten. Im folgenden Abschnitt soll auf die geläufigsten Bauformen von RFID-Transpondern eingegangen werden:[3]

Disks und Münzen

Die am häufigsten verwendeten RFID-Tags sind die Disks (Münzen). Die Größe dieser Transponder ist sehr variabel. Der Durchmesser reicht von von wenigen Millimetern bis zu 10 cm. Die Disks sind in ein rundes Spritzgussgehäuse eingearbeitet. Eine in der Mitte befindliche Bohrung dient zur Aufnahme einer Befestigungsschraube. Wird statt dem Spritzgussgehäuse ein Gehäuse aus Polystyrol oder Epoxidharz verwendet, so erweitert sich der Temperaturbereich in dem der Transponder eingesetzt werden kann.

Glasgehäuse



Die Glastransponder wurden vor allem für die Identifizierung von Tieren entwickelt, denn dieses RFID-Gehäuse kann unter die Haut des Tieres implantiert werden. Das Glasgehäuse ist lediglich 10 bis 32 mm lang. Innerhalb des Glasgehäuses befinden sich ein Microchip und ein Chipkondensator zur Glättung der gewonnenen Versorgungsspannung. Die Transponderspule besteht aus nur

0,03 mm dickem Draht, welcher auf einen Ferritkern gewickelt ist. Alle Transponderkomponenten sind in einem Weichkleber eingebettet. Nur so kann die mechanische Stabilität und die Haltbarkeit des Transponders gewährleistet werden.

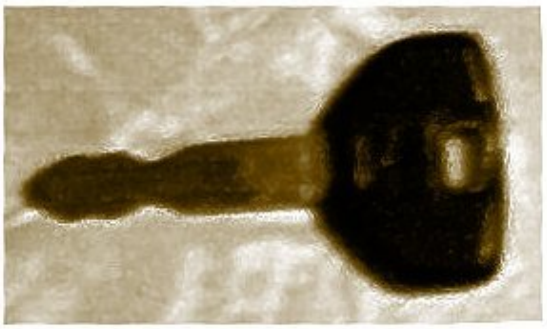
Plastikgehäuse

Unterliegt der Transponder besonders hohen mechanischen Belastungen, so kommt zum Schutz der Transponderkomponenten meist ein Plastikgehäuse (plastic package, PP) zum Einsatz. Solch eine Transponderform kann auch in andere Bauteile eingebaut werden (z. B. Autoschlüssel für elektronische Wegfahrsperren). Im PP befinden sich die gleichen Komponenten wie im Glastransponder, jedoch ist die Spule etwas länger. Somit hat der PP-Transponder eine größere Funktionsreichweite. Auch kann der PP-Transponder größere Microchips aufnehmen und weist eine hohe Belastungsfähigkeit gegenüber mechanische Vibrationen auf. Auch hinsichtlich anderer Qualitätsparameter, wie Temperatur-Zyklen oder Falltest, kann der PP-Transponder überzeugen.

Werkzeug- und Gasflaschenidentifikation

Diese spezielle Bauform wurde für den Einbau induktiv gekoppelter Transponder in Metalloberflächen entwickelt. Die Transponderspule wird in einen Ferritschalenkern gewickelt. Auf der Rückseite des Ferritschalenkerns wird der Chip angebracht und der Kontakt zur Transponderspule hergestellt. Transponder dieser Bauform müssen eine ausreichend hohe mechanische Stabilität, sowie eine hohe Vibrations- und Hitzebeständigkeit aufweisen. Dazu werden Transponderchip und Ferritschalenkern in einer Halbschale aus PPS (hochtemperaturbeständiger thermoplastischer Kunststoff) vergossen. Für die Außenabmessungen des Transponders bei der Nutzung zur Werkzeugidentifikation gibt es entsprechende Din-Normen.

Schlüssel und Schlüsselanhänger

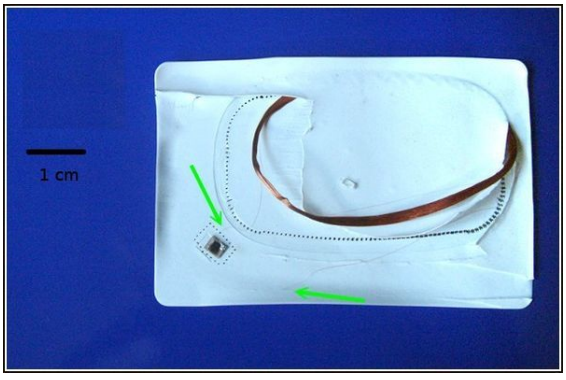


Diese Bauart baut auf der PP-Transponder-Technologie auf, denn hierbei wird ein PP-Transponder in den Schlüsselknauf eines mechanischen Schlüssels oder in einen Schlüsselanhänger eingegossen bzw. eingespritzt. Verwendung findet diese Bauform bei Wegfahrsperren oder Türschließsystemen mit besonders hohen Sicherheitsanforderungen.

Uhren

Diese Bauform wird vor allem bei Zutrittskontrollsystemen genutzt. Entwickelt wurde diese Art des Transponders Anfang der 90er Jahre von der österreichischen Firma Ski-Data.

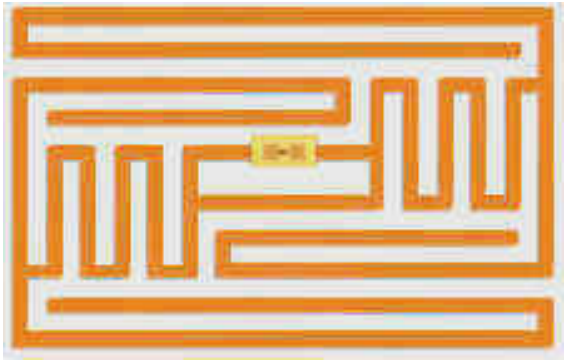
Kontaktlose Chipkarten



Diese Bauform erlangt immer größere Bedeutung, denn sie hat den Vorteil der hohen Reichweite, welche aus einer großen Spulenfläche resultiert. Für die Herstellung einer kontaktlosen Chipkarte wird ein Transponder z. B. zwi-

schen vier PVC-Folien einlaminiert. Temperaturen von über 100 °C und ein hoher Druck lässt die Einzelfolien zu einer unlösbaren Einheit werden. Die kontaktlose Chipkarte basiert häufig auf der Bauform ID-1 (85,72 mm x 54,03 mm x 0,76 mm ± Toleranzen), welche von Kredit- und Telefonkarten bekannt ist.

Smart Label



Bei der Bauform “Smart Label” handelt es sich um eine papierdünne Transponderbauform. Grundlage für diese Bauform ist eine 0,1 mm dicke Plastikfolie, auf welche die Transponderspule durch Siebdruck oder Ätztechnik aufgebracht wird. Die Folie kann anschließend laminiert und mit einem Kleber beschichtet werden und so als Selbstklebeetiketten in verschiedenen Bereichen zum Einsatz kommen (z. B. Gepäckstücke, Pakete und Waren aller Art). Vorteil dieser Transponder ist, dass nachträglich weitere Daten mit bereits gespeicherten Daten verknüpft werden können, da die Klebeetiketten auf der Vorderseite bedruckbar sind (z. B. Barcode).

Coil-on-Chip

Die Coil-on-Chip-Bauform (kontaktloser Speicherbaustein) ist eine nichthybride Technologie, da die Spulen auf dem Chip des Transponders integriert sind. Hierbei handelt es sich um eine Spule in Form einer einlagigen Spiralanordnung. Diese wird auf den Isolator des Chips aufgebracht und anschließend mit der darunter befindlichen Schaltung verbunden. Durch diese Technologie kann die Größe des Transponders reduziert werden, sie beträgt lediglich 3 x 3 mm^2. Es ist möglich diesen Transponder in einen Kunststoffkörper einzubetten um somit eine bessere Handhabung zu gewährleisten.

Weitere Bauformen
Es existieren weitere anwendungsspezifische Sonderbauformen, wie zum Beispiel “Brieftaubentransponder” oder “Champion-Chip”.

4.3 Funktionsweise

Zunächst soll die allgemeine Funktionsweise der wichtigsten RFID-Komponenten erläutert werden: Das Lesegerät erzeugt ein magnetisches bzw. elektromagnetisches Feld, welches von der Transponderantenne empfangen wird. Von dort wird es an den Mikrochip weitergeleitet. Mit dem Feld werden Signale an den Transponder übermittelt. Der Transponder antwortet auf diese Signale und sendet in das elektromagnetische Feld. Jedoch wird durch den Transponder kein eigenes magnetisches bzw. elektromagnetisches Feld erzeugt. Der Transponder verändert das elektromagnetische Feld des Lesegerätes. Das Lesegerät nimmt die Veränderungen wahr und interpretiert die Veränderungen als Antwort auf die Abfrage. Dieser Prozess benötigt nur wenig Zeit. In der Praxis genügen Bruchteile von Sekunden. Diese berührungslose Methode des Datenaustausches funktioniert über eine Distanz von einigen Zentimeter und auch über größere Entfernungen. Störfaktoren beeinträchtigen jedoch die Datenübermittlung. Solche Störfaktoren treten zumeist im Zusammenhang mit den elektromagnetischen Feldern auf. Denn die Strahlung dieser Felder kann durch verschiedene andere Medien, wie Wasser oder Metall, beeinflusst werden.

Ein weiterer wichtiger Aspekt, welcher beim Einsatz der RFID-Technologie zu berücksichtigen ist, ist die Energieversorgung von Transponder und Mikrochip. Die Energieversorgung erfolgt zumeist über das magnetische Feld des Lesegerätes. Die Stärke dieser ausgesendeten Feldenergie nimmt allerdings bei größeren Entfernungen kontinuierlich ab, so dass entweder ein sehr starkes elektromagnetisches Feld benötigt wird oder aber die Entfernung zwischen Transponder und Lesegerät muss verringert werden. Ist eine große Distanz zwischen Lesegerät und Transponder von besonderer Bedeutung so kann dies nur durch zusätzliche technische Lösungen erreicht werden. [5]

4.4 Unterscheidungsmerkmale von RFID-Systemen

Im nachfolgenden Kapitel werden die wichtigsten Kriterien beschrieben. Mit diesen Kriterien zeigt sich anhand wie vieler Varianten RFID-Systeme unterschieden werden können.

4.4.1 Frequenzbereiche

Ein zentraler Einflussfaktor bei der Entwicklung von RFID-Lösungen sind gesetzliche Vorschriften. Da RFID-Systeme in verschiedenen Frequenzbereichen und Reichweiten arbeiten, müssen die Funkvorschriften der jeweiligen Regionen und Länder berücksichtigt werden. Für RFID-Anwendungen werden folgenden Frequenzen genutzt:

- Industrial-Scientifical-Medical-Frequenzen (Frequenzen, die für industrielle, wissenschaftliche und

medizinische Anwendungen bereitgestellt werden)

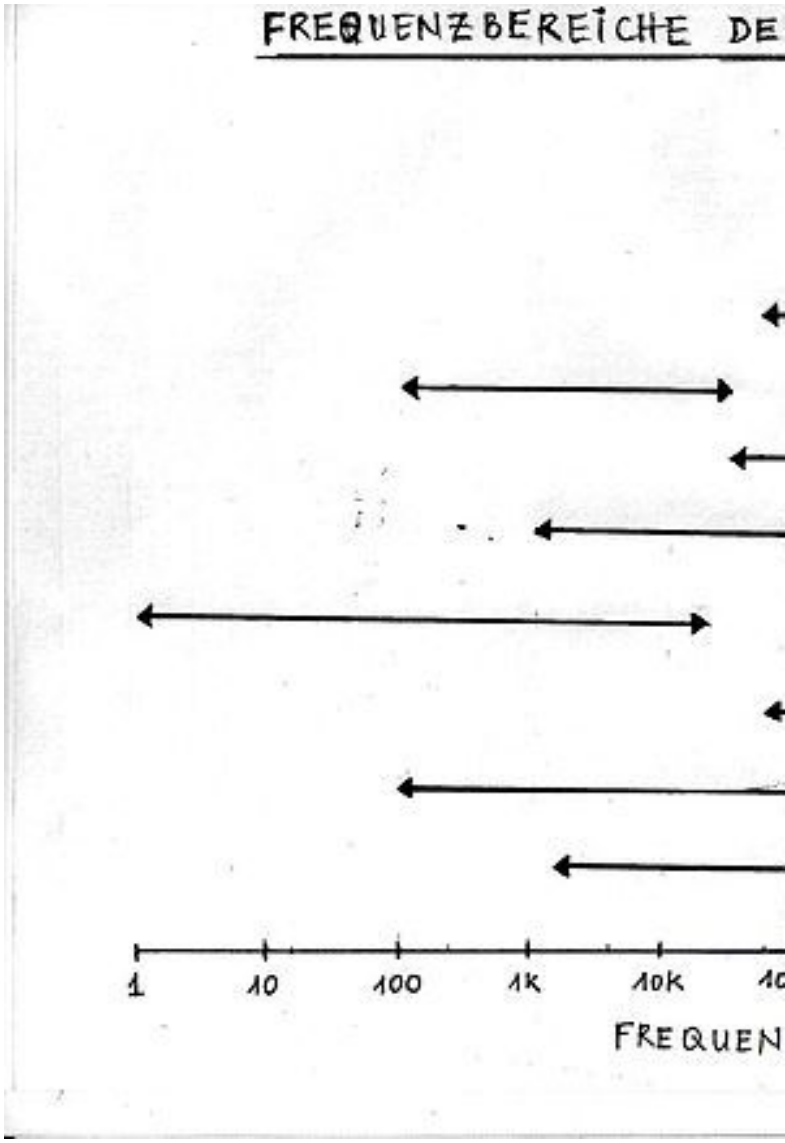
- zusätzlich in Europa: Frequenzbereich unter 135 kHz

- zusätzlich in Amerika und Japan: Frequenzbereich unter 400 kHz

Ein international einheitlicher Standard für RFID-Systeme ist nicht gegeben. Somit existieren nationale und internationale Lösungen, welche jeweils unterschiedliche Frequenzbänder nutzen. Die Regelungen zur Nutzung von Frequenzbändern unterscheiden sich von Land zu Land und damit ergeben sich in Abhängigkeit vom genutzten Frequenzband verschiedene Vorteile in Bezug auf Lesegeschwindigkeit, Reichweite, Preis und Einsatzfähigkeit der einzelnen Lösungen.

Für den kommerziellen Einsatz werden hauptsächlich Frequenzbereiche unter 135 kHz (Low Frequenz, LF), 13,56 MHz (High Frequenz, HF), 869 bzw. 915 MHz (Ultra High Frequenz, UHF) belegt. Dabei haben sich die Frequenzbänder unter 135 kHz sowie bei 13,56 MHz im weltweiten Einsatz besonders bewährt. Insgesamt ist die Frequenzregulierung bei der Entwicklung von international einsetzbaren RFID-Systemen jedoch ein besonderes Problem, denn weltweit sind die Verordnungen zur Frequenznutzung sehr uneinheitlich. Neben der unterschiedlichen Zuteilung der Frequenzbänder sind auch die Vorschriften hinsichtlich der Sendestärken von Lesegeräten international verschieden geregelt. Dies hemmt die Entwicklung von leistungsstarken internationalen RFID-Lösungen.

Ein Beispiel: 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.[6]



Da es keinen einheitlichen RFID-Standard gibt, der ein bestimmtes Frequenzband vorschreibt, haben sich verschiedene nationale und internationale Lösungen entwickelt. Die für die Nutzung freigegebenen Frequenzbänder unterscheiden sich also von Land zu Land. Weiterhin bieten die einzelnen Frequenzbänder verschiedene Vorteile in Bezug auf Lesegeschwindigkeit, Reichweite, Preis und Einsatzfähigkeit.[1]

Es kommen den vielfältigen Einsatzbereichen entsprechend unterschiedliche Transponder und somit unterschiedliche Frequenzen zum Einsatz:[1]

- 30 bis 500 kHz (LF): kostengünstige Systeme zum Beispiel für Zugangskontrollen und Wegfahrsperren in Kraftfahrzeugen; relativ geringe Lesegeschwindigkeit und Reichweite aber sehr gute Einsatzfähigkeit in rauen Umgebungen

- 10 bis 15 MHz (HF): Smart Label-Technologie zum Beispiel für Warenkennzeichnung im Einzelhandel; mittlere Reichweite und mittlere Übertragungsge-

schwindigkeit

- 865 bis 950 MHz (UHF): RFID-Chips vor allem in der Logistik, zum Beispiel in den Bereichen des Behältermanagements und der Palettenidentifikation; relativ hohe Reichweite und Lesegeschwindigkeit (zugelassen ist in Europa der Bereich von 868 MHz bis 870 MHz)

- 2,4 bis 2,5 GHz und 5,8 GHz (Super Ultra High Frequenz, SUHF): in Europa bisher kaum praxistaugliche Lösungen; in den USA schon zahlreichere Lösungen zum Beispiel der Einsatz beim Mautsystem; hohe Reichweite und Lesegeschwindigkeit

Eine Übersicht über die Frequenzbänder im MHz-Bereich gibt die folgende Abbildung.

4.4.2 Reichweite

Grundsätzlich kann gesagt werden, dass eine größere Reichweite auch mit größeren Aufwand verbunden ist, denn je größer die Reichweite, desto mehr potentielle Störquellen können auf das RFID-System einwirken. Um eine größere Reichweite zu generieren, muss eine Vielzahl von RFID-Systemfaktoren verbessert werden:[5]

- Verstärkung des Magnetfeldes zur Sicherstellung der Kommunikation zwischen Sender und Empfänger

- Einsatz von technisch höherwertigen und teureren Komponenten zur Eliminierung von auftretenden Störquellen

- Einsatz von größeren Transpondern mit ausreichender Energieversorgung und hoher Sendestärke

RFID-Systeme werden hinsichtlich ihrer Reichweite in drei Bereiche unterteilt - Close-Coupling-, Remote-Coupling- und Long-Range-Systeme:[6]

- Bei **Close-Coupling-Systemen** liegt die Reichweite im Bereich bis zu einem Zentimeter. Close-Coupling-Systeme können in Abhängigkeit von der Kopplung auf nahezu beliebigen Frequenzbändern (von Niederfrequenz bis 30 MHz) betrieben werden. 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. Diese RFID-Systeme werden in Bereichen mit hohen Sicherheitsanforderungen eingesetzt, beispielsweise bei Chipkarten mit Zahlungsfunktion oder im Bereich der Zutrittskontrolle.

- **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.

- 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).

In den meisten Fällen werden in der Praxis jedoch Abstriche bei der Reichweite gemacht, da große Reichweiten zu viele Probleme mit sich bringen. Theoretisch kann ein RFID-Transponder über Strecken bis zu über einem Kilometer ausgelesen werden und wahrscheinlich werden diese Weiten mit fortschreitender Entwicklung der RFID-Systeme noch erhöht. Allerdings müssen dann auch Möglichkeiten gefunden werden, die Probleme bei höheren Reichweiten einzuschränken.

4.4.3 Speichertechnologie

RFID-Systeme können nach der zum Einsatz kommenden Speichertechnologie unterschieden werden. Dabei sind grundsätzlich zwei Speichertechnologien bekannt:

- **Read-only-Transponder:** Diese Transponder können nach dem Programmiervorgang beim Hersteller vom Lesegerät nur gelesen werden. Sie sind kostengünstiger in der Herstellung. Die 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:** Diese Transponder beinhalten einen Speicher und sind daher teurer in der Herstellung. Es können leistungsfähige Sicherheitsmechanismen implementiert und auch variable Informationen auf dem Transponder durch das Anwendungssystem neu gespeichert werden.

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

Eine **ROM**-Lösung (Read Only Memory) besteht aus einem digitalen Festwertspeicher, in dem Daten persistent gespeichert werden. Die Daten werden somit fest in der Halbleiterstruktur abgelegt und können weder elektrisch noch optisch gelöscht oder verändert werden. ROM-Lösungen lassen weiter unterscheiden in EPROM, EEPROM und Flash-EPROM. Bei dieser Art der Speicherbausteine können Daten gelöscht und anschließend neu in den Speicher geschrieben werden.

- 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 über 100-mal wiederholt werden. Der Speichervorgang wird über eine serielle Leitung durchgeführt. Für RFID-Systeme haben vor allem EEPROM-Systeme eine hohe zahlenmäßige Bedeutung erlangt.
- 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.

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. Die FRAM-Technologie übersteige auch mit bis zu über 1000 Schreib- und Lesezyklen die Leistungsfähigkeit von EEPROMs.[6]

4.4.4 Energieversorgung der Transponder

Grundsätzlich gibt es zwei Transpondertypen sowie Mischformen beider Typen:

- **Aktive Transponder** haben eine eigene Energiequelle zur Erzeugung elektromagnetischer Wellen. Sie sind batteriebetrieben, befinden sie sich jedoch solange im Ruhezustand bis sie von einem Lesegerät ein Aktivierungssignal empfangen. Dadurch kann die Lebensdauer der Energiequelle erhöht werden. Aktuell sind Transpondertypen mit internem Speicher bis zu 1 Million Bytes erhältlich.
- **Passive Transponder** werden dagegen bei Lesevorgängen über Funkwellen durch die Lesegeräte mit Energie versorgt. Sie haben eine geringere Reichweite als die aktiven Transponder. Für die Energieversorgung des passiven RFID-Transponders sind besonders leistungsstarke Lesegeräte als aktive RFID-Systeme notwendig. Es können deutlich weniger Informationen als bei aktiven Tags gespeichert werden.

Die Leistungsmerkmale der einzelnen Transponder-Typen sind in RFID-Klassen eingeteilt. In den Klassen 0 bis 4 spiegeln sich die aktiven und passiven Transpondertypen wieder.[1]

Der EPCglobal-Standard EPC Generation 2 (Gen 2) avanciert, als Nachfolger des klassischen 96-bit Transponders, zum internationalen Standard. Die Vorteile des neuen Standards Gen 2 sind:[1]

- das Lesen von bis zu 600 Transpondern je Sekunde
- höhere Pulkfähigkeit
- Kill-Kommando für die sofortige Zerstörung des Transponders
- Schutz der Daten auf dem Chip mittels Passwörtern

4.4.5 Übertragungsverfahren der Transponder

Zur Verständigung von Transpondern werden im Normalfall verschiedene Verfahren eingesetzt: Dies ist zum

einen die induktive Kopplung, das auf dem Radarprinzip beruhende Backscatter-Verfahren und das so genannte “Close-Coupling-System”. Dieses kann aufgrund des geringen Abstands zwischen Transponder und Erfassungsgerät über eine kapazitive Kopplung mit Energie versorgt werden.

Kapazitive Kopplung Die kapazitive Kopplung nutzt das Prinzip des Plattenkondensators. Die Signalübertragung erfolgt zwischen zwei voneinander isolierten elektrischen Leitern, die sowohl im Transponder, sowie auch im Lesegerät parallel angeordnet sind. Wird durch ein elektrisches Signal eine Ladungsveränderung auf einem Leiter erzeugt, wirkt sich diese Veränderung über ein elektrisches Feld auf die Ladungsträger des zweiten Leiters aus. Die so erreichte Koppelkapazität ist verhältnismäßig gering und ist deshalb für die Energieversorgung von Mikroprozessoren ungeeignet. Diese Energieversorgung muss deshalb ergänzend induktiv erfolgen.[6]

Induktive Kopplung Bei den induktiv gekoppelten Transpondern wird fast die gesamte, für den Betrieb erforderliche Energie durch das Lesegerät zur Verfügung gestellt. Diese Transponderart besteht aus einem elektronischen Datenträger und einer groß-flächigen Spule, die als Antenne dient. Zur Energieversorgung des Transponders wird von der Antennenspule des Lesegeräts ein elektromagnetisches Feld erzeugt. Dabei durchdringt ein Teil des ausgesendeten Feldes die Antennenspule des Transponders. Durch eine 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 parallel zur Antennenspule des Lesegeräts ein Kondensator geschaltet. Dieser bildet gemeinsam mit der Spuleninduktivität der Antennenspule den Parallelschwingkreis. Dabei entspricht die Resonanzfrequenz des Schwingkreises der Sendefrequenz des Lesegeräts. Die Antennenspule des Transponders bildet zusammen mit einem Kondensator ebenfalls einen Schwingkreis, welcher auf die Sendefrequenz des Lesegeräts eingestellt ist. Wird nun ein Transponder in das magnetische Wechselfeld der Lesegerätantenne 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 Transponderantenne 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 Lesegerätantenne abgegriffenen Spannung.[6]

Backscatter-Verfahren Das Backscatter-Verfahren basiert, wie schon angesprochen auf dem Radartechnikprinzip und kommt hauptsächlich bei Long-Range-Systemen zum Einsatz. 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. Gerät dabei das Objekt auf welches die Wellenfront trifft in Resonanz, so werden die elektromagnetischen Wellen besonders gut reflektiert. Da dieser Effekt für die RFID-Technologie ausgenutzt wird, wurde für das Lesegerät und den Transponder eine Dipolantenne konstruiert, die für die jeweils verwendete Frequenz ein Resonanzverhalten zeigt. Zur Energieversorgung wird von der Lesegerätantenne 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. 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” bezeichnet.[6]

5 Einsatzbereiche / Einsatzmöglichkeiten von RFID-Systemen

Entsprechend der unter Punkt Auto-ID-Systeme genannten Aufgaben und Einsatzbereiche automatischer Identifikationssysteme, leitet sich natürlich auch ein Teil der im Folgenden aufgezeigten Einsatzgebiete für RFID-Systeme aus bereits bestehenden Anwendungsbereichen dieser Systeme ab. Weil RFID-Systeme in vielen Bereichen effektiver und effizienter als herkömmliche Auto-ID-Systeme sind, lösen sie diese zunehmend ab. In der Tat ist dies vielfach bereits geschehen und so sind RFID-Tags schon seit einiger Zeit Bestandteil unseres täglichen Lebens.[7] Darüber hinaus werden gleichzeitig aber auch immer neue Einsatzgebiete von der RFID-Technologie erschlossen.

Der entscheidende Vorteil von RFID gegenüber anderen Auto-ID-Systemen liegt in der kontaktlosen Datenübermittlung zwischen Objekt und Lesegerät. In der Regel werden zu identifizierende Objekte mit einem Transponder versehen, dessen Daten (Informationen) von einem Lesegerät abgerufen werden können. Die Position des Objektes sowie physikalische Grenzen (bspw. in Form von Verpackungen) zwischen Objekt (Transponder) und Lesegerät spielen für Radiowellen keine bzw. eine unter-

geordnete Rolle. Ein weiterer Vorteil dieser Technologie ist auch die Möglichkeit, Daten auf Transpondern zu ändern und zu speichern (sofern der im Transponder implementierte Funktionsumfang bezüglich der Informations- und Datenverarbeitung sowie die Größe des im Transponder verfügbaren Datenspeichers dies unterstützen).[2]

RFID-Systeme können darüber hinaus weitere Aufgaben übernehmen, bspw. die Lokalisierung von Objekten in bestimmten Räumen oder Monitoring. So sind leistungsfähige Transponder mit integriertem Temperatursensor u.a. in der Lage die Überwachung der Kühlkette während eines Transportvorgangs zu übernehmen.[4]

Hinzu kommen sinkende Preise bei der Herstellung der Transponder.[4] Dies macht den Einsatz von RFID verstärkend attraktiv. Natürlich sollte der Umstellung von einem etablierten Auto-ID-System auf RFID oder der Einführung eines RFID-Systems immer eine genaue Kosten / Nutzen Analyse vorausgehen (vgl. auch Wirtschaftliche Aspekte von RFID). Gerade Barcodesysteme bieten, günstiger als RFID-Systeme, ähnlich viele Anwendungsmöglichkeiten wie diese.[2]

Innerhalb der einzelnen Einsatzbereiche können von einem RFID-System zusammengefasst folgende Aufgaben übernommen werden:[2]

- Identifikation der Objekte anhand einer im Transponder gespeicherten “Unique Identification Number” (je nach Anwendungsbereich erfolgt die Übermittlung der UID und weiterer Daten verschlüsselt oder unverschlüsselt). Die Identifikation erfolgt abhängig von den verwendeten Komponenten nur in einer bestimmten Distanz zwischen Lesegerät und Transponder und ist abhängig von der Bewegungsgeschwindigkeit der Objekte.
- Übermittlung weiterer Daten vom Transponder zum Lesegerät. Da ein RFID-System in der Regel direkt oder indirekt über ein Netzwerk an ein weiteres EDV-System angeschlossen ist erfolgt in einem nächsten Schritt die Übertragung der Daten in das angebundene System.
- gezielte Kommunikation mit einzelnen Transpondern, wenn sich mehrere Objekte gleichzeitig im Lesebereich eines Lesegerätes befinden
- Speicherung von Daten im Transponder, welche durch ein Lesegerät übermittelt wurden.
- Überprüfung auf Fehler in übermittelten Daten, Kopplung mit Sensoren und Steuerung.

Denkbar ist also eine ganze Reihe an Szenarien für RFID-Systeme, wobei sich die tatsächlichen technischen Realisierungen der Systeme natürlich stark voneinander unterscheiden können, abhängig vom speziellen Anwendungsbereich. Nachfolgend werden einige dieser Einsatzbereiche, gegliedert nach ihrem primären Identifizierungs- bzw. Bezugsobjekt (Personen, Tiere, Produktionsgüter, Waren, Gegenstände, ...), stellvertretend vorgestellt. Folgende Aspekte sollen dabei u.a. betrachtet werden:

- Worin liegt die hauptsächliche Motivation für den Einsatz des Systems (Hauptaufgabe, bspw. Zutrittskontrolle, Qualitätssicherung, Prozessbeschleunigung,…)
- Ggf. Vor- und Nachteile der Systeme gegenüber Alternativen
- Art der eingesetzten Transponder (aktiv, passiv), Geschlossenheit des RFID-Systems (geschlossenes oder offenes System), damit verbunden die Nutzungsdauer der Transponder (können diese ggf. wieder verwendet werden, Einweg- / Mehrwegtransponder), welche Transponder-Bauform(en) kommen im Anwendungsbereich zum Einsatz (Glaskapseln, Aufklebe- oder Anhängeetiketten, Karten,…), welche Lesegeräte werden verwendet (mobile / stationäre Lesegeräte)
- Funktionsweise des Systems (Zeitpunkt der Identifikation, Verarbeitung / Verwendung der Daten)

Zur besseren Abgrenzung der unterschiedlichen Einsatzgebiete (z.B. in Bezug auf genutzte Standards, Frequenzen etc.) wurde im Rahmen einer EU-Studie ein RFID Referenzmodell entwickelt “RFID Referencemodell”.

5.1 Personenidentifikation (Personenbezug)

Elektronischer Reisepass

Auf ein völlig neues Niveau möchte man die Sicherheit von Reisepässen in der EU mit der neuen ePass-Generation heben (ePass steht für “elektronischer Pass”).[8] Im Gegensatz zu herkömmlichen europäischen Reisepässen besitzen ePässe einen kontaktlosen Mikroprozessorchip welcher alle Passdaten, inklusive personenbezogene- sowie biometrische Daten des Inhabers, in digitaler Form bereithält. Da der Chip nicht sichtbar in den Deckel des Passes eingearbeitet ist, werden diese Pässe deshalb äußerlich durch einen stilisierten Chip auf der Titelseite gekennzeichnet[3] (das Symbol steht für Biometrie). Neben der erhöhten Fälschungssicherung dürfte auch die schnellere Abwicklung der Personenkontrolle beim Grenzübergang Hauptargument für den ePass sein.

“Mit Biometrie wird das Reisen sicherer und einfacher. Die Ausstellung biometrieunterstützter Reisepässe in Europa ist ein Baustein im Kampf gegen organisierte Kriminalität und den internationalen Terrorismus” Otto Schily (Bundesinnenminister a.D.).[9]

In Deutschland werden seit November 2005 ausschließlich elektronische Reisepässe herausgegeben. Damit ge-

hört Deutschland zu einem der Vorreiter bei der Umsetzung einer EU-Verordnung (2252 / 2004), die vorsieht, dass bis August 2006 alle europäischen Mitgliedsländer ihre Reisedokumente entsprechend “aufrüsten”. Außerhalb der EU werden auch Japan, die USA, Australien, Rußland, Kanada, die Schweiz und andere Staaten ePässe einführen.[3][9]

Die technische Spezifikation biometrischer Reisepässe orientiert sich an Empfehlungen der New Technologies Working Group (NTWG), der Internationalen Zivilluftfahrtbehörde (ICAO), in der auch Deutschland mit dem Innenministerium (BMI) vertreten ist. Bewusst wurden die Anforderungen an einen ePass zunächst minimal formuliert, da nur so eine größtmögliche weltweite Interoperabilität verschiedener Lesegeräte und Reisepässe erreicht werden kann. International ist so bspw. nur das Lichtbild als biometrisches Merkmal verpflichtend.

Die EU geht an dieser Stelle allerdings noch einen Schritt weiter: Neben personenbezogenen Daten wie Name, Geburtstag, Geschlecht, usw. sowie der digitalisierten Version des Lichtbilds, werden in einer zweiten Stufe zusätzlich zwei Fingerabdrücke als weiteres biometrisches Merkmal des Inhabers elektronisch im Pass gespeichert. Der minimale Speicherplatz für alle zu speichernden Daten wurde mit 32kByte festgelegt, in deutschen Reisepässen werden Mikroprozessoren von Infineon (64kByte) und Philips (72kByte) verwendet.[3]

Um die anfangs genannte angestrebte Fälschungssicherheit zu erreichen und um die gespeicherten Daten vor unbefugtem Auslesen zu schützen, sollen folgende Maßnahmen helfen:[3][8]

- die auf dem RFID-Chip gespeicherten Daten werden durch die ausstellende Behörde elektronisch unterschrieben. Diese digitale Signatur soll die Integrität und die Authentizität der Daten sicherstellen. Manipulationen sollen dadurch erkennbar werden
- um Manipulationen von vornherein zu verhindern, werden die Chips nach der Herstellung gegen Löschen oder Ändern der Daten versiegelt (Einwegtransponder / offenes System)
- nur über das vorherige optische Auslesen der maschinenlesbaren Zone (MRZ) anhand derer das RFID-Lesegerät den Zugriffsschlüssel für die Daten im kontaktlosen Chip berechnet, ist der Zugang zu zum Chip und damit zu den biometrischen Daten möglich, d.h. solange der Pass geschlossen aufbewahrt wird, ist er wie vorher auch vor unberechtigtem Lesezugriff geschützt (Basic Access Control)
- mit der zweiten Phase des ePasses, d.h. nach Integration der Fingerabdrücke, wird ein zusätzliches kryptographisches Protokoll für den Zugriff auf die biometrischen Daten verwendet, nur von explizit von Deutschland autorisierten Lesesysteme können dann zugreifen
- das unberechtigte Abhören der Daten während der Kommunikation zwischen Chip und Lesesystem wird durch Verschlüsselung verhindert, dazu wird im Rahmen des Verbindungsaufbaus zwischen Lesesystem und Chip ein sicherer Kanal aufgebaut
- die Lesereichweite des RFID-Chips beträgt 10 cm

Damit Bürgerinnen und Bürger ihre auf dem Chip gespeicherten persönlichen Daten einsehen können, sollen neben Grenzkontrollpunkten auch die Passbehörden mit entsprechenden ePass-Lesern ausgestattet werden.

Mitarbeiterkarte

…

Öffentlicher Personennahverkehr

…

Wegfahrsperre beim Auto

…

Sportveranstaltungen

…

Skipässe

…

Krankenhäuser

Um in Krankenhäusern trotz unterschiedlicher und komplexer Prozesse die Qualität der medizinischen Betreuung zu sichern, ist es notwendig Abläufe zu optimieren bzw. zu standardisieren (vgl. Total Quality Management). Erst durch das reibungslose Zusammenwirken, speziell in den Schnittstellenbereichen einzelner Behandlungsschritte sowie dem medizinischen Prozess selbst, können Risiken minimiert und die Patientensicherheit erhöht werden. Doch stehen gerade im Klinikbetrieb Mitarbeiter und Ärzte oft unter hohem Zeitdruck, sind überlastet, teilweise mangelhaft ausgebildet. Dies kann dann u.a. zu Fehlern bspw. bei der Patientenidentifikation oder bei der Erfassung oder Übermittlung von Patientendaten führen, was im schlimmsten Fall in einer medizinischen Falschbehandlung resultieren kann, bis hin zur Transplantation falscher Organe.

Mit einem RFID-basierten System zur Patientenidentifikation können Fehler wie diese vermieden, zumindest verringert werden, weil es neben der exakten Identifikation auch eine effizientere Erfassung und Verwaltung der Daten unterstützt sowie eine genaue Zuordnung von Patient und Patientendaten ermöglicht. Dies ist bspw. wichtig bei:

- der Diagnose,
- der Zuteilung von Medikamenten,
- der Zuteilung von Diäten,
- Infusionen,

- Bluttransfusionen,
- der Identifikation im OP vor der Operation,
- oder der Identifikation im Röntgenraum.

Passive, wieder verwendbare Transponder (geschlossenes System), vor allem in Form RFID-Chip versehener Armbänder oder Armbanduhren, RFID-Etiketten oder kontaktlose ISO Karten werden verwendet, um Patienten zu „kennzeichnen“ und zu identifizieren und Patientendaten bspw. über den Personal Digital Assistant (PDA) des Arztes mit dem Patienteninformationssystem im Krankenhaus zu koppeln. Im einfachsten Fall erfolgt diese Kopplung über eine auf dem Chip gespeicherte eindeutige ID. Darüber hinaus können allerdings auch weitere Daten wie Blutgruppe, Allergien u.ä. hinterlegt werden. Vor allem in Notaufnahmen kann es lebensrettend sein, wenn Patientendaten bereits während des Transports auf den Transponder gespeichert wurden und bei Ankunft direkt verfügbar sind.[2] In den USA geht man bei in Frage kommenden Transpondern noch einen Schritt weiter. Dort genehmigte im November 2004 die US-amerikanische Gesundheitsbehörde (FDA) den Einsatz des „VeriChip” am Menschen. Der Transponder der US-amerikanischen Firma Applied Digital Solutions wird unter der Haut eingepflanzt. Geworben wird mit einfacher Verfügbarkeit lebenswichtiger Informationen im Notfall.[10]

Doch allein mit der exakten Identifikation eines Patienten kann man nicht den anfangs erwähnten Qualitäts- und Sicherheitsansprüchen gerecht zu werden. So wird bei allen Behandlungsschritten auch festgehalten (teilweise unter Vergabe von Vorgangsnummern) was von wem zu welchem Zeitpunkt durchgeführt wurden. Zuvor wird ggf. noch geprüft ob eine behandelnde Person überhaupt berechtigt ist eine bestimmte Tätigkeit durchzuführen. Auch hier wird zur Identifikation des Klinikpersonals RFID benutzt, da dies häufig sowieso bereits für die Zugangs- und Arbeitszeitkontrolle eingesetzt wird (vgl. Mitarbeiterkarten).

Obwohl der Einsatz von RFID-Systemen im Krankenhausbereich also viele Vorteile mit sich bringt, stehen die Entwicklung und der Einsatz solcher Systeme hier aber noch am Anfang ihrer vielfältigen Möglichkeiten.[2]

Kinder in Schulen oder Freizeitparks

…

5.2 Tieridentifikation

Nutztiere

Die Viehverkehrsverordnung (ViehVerkV) regelt in Deutschland u.a. auch die Kennzeichnung von Nutztieren (Rinder, Schweine, Schafe undZiegen) mit visuell lesbaren Ohrmarken. Entsprechend ist dies die am weitesten verbreitete Art und Weise der Kennzeichnung bei diesen Tieren. Wachsende Anforderungen auch in der Nutztierhaltung, qualitativ und quantitativ, sind der Grund, dass bereits seit fast 20 Jahren mehr und mehr auch elektronische Kennzeichnungssysteme in diesem Bereich zum Einsatz kommen. Die Tieridentifikation war und ist eine der wichtigsten Triebfedern für die Entwicklung moderner RFID-Systeme. Dies liegt vor allem mit den vielfältigen Anwendungsmöglichkeiten in diesem Bereich, sowohl inner- als auch überbetrieblich. Folgende Tabelle gibt einen Überblick der Nutzungsmöglichkeiten von RFID[2].

Steht bei der innerbetrieblichen Nutzung vor allem die Funktionssicherheit im Vordergrund, so ist als Motivation für eine betriebsübergreifende Kennzeichnung die Fälschungssicherheit zu nennen. Insgesamt kann mit Hilfe von RFID auch die artgerechte(re) Haltung der Tiere unterstützt werden (Tiere dürfen sich freier bewegen und bspw. nur bei Bedarf die Futterautomaten aufsuchen, von denen sie dann RFID-unterstützt ihre Ration(en) erhalten) und das trotz größer werdenden Produktionsmengen mit der Vorgabe geringerer Kosten. Die gesetzlich vorgeschriebenen Ohrmarken dürften bei den genannten Nutzungsbeispielen schnell ihre Grenzen erreicht haben bzw. überhaupt nicht anwendbar sein. Sie sind weder fälschungssicher, noch praktikabel. Sie reißen aus, ihre Nummern verblassen und haben zu wenige Stellen. Alternative Ohrmarken die den Barcode zur Identifikation verwenden sind hier in jedem Fall eine Verbesserung, insbesondere was das maschinelle automatische Auslesen und Identifizieren betrifft, haben allerdings ebenfalls Grenzen (eingeschränkte Lesereichweite sowie Leseposition, Verschmutzungen / Verwitterung).

Die einzigen Auto-ID-Systeme für die direkte Kennzeichnung, die auch den härteren Umweltbedingungen in der Nutztierhaltung standhalten sind RFID-Systeme. Mit ihrer Möglichkeit zur berührungslosen, fälschungssicheren und breit einsetzbaren Identifikation werden so mittlerweile nicht nur Rinder, Schweine, Schafe und Ziegen mit Transpondern ausgestattet sondern auch Hühner, Pferde und Strauße, sogar landwirtschaftlich gezüchtetes Dam- oder Rotwild.[2]

Mit RFID kann so „der Weg der Steaks“ über den gesamten Produktionsprozess nachverfolgt werden [11]. Nicht zuletzt wegen des breiten Einsatzes gibt es seit 1996 die ISO-Normen 11784, 11785 sowie seit 2003 die ISO 14223. Sie regeln Datenübertragungs- und Codierungsverfahren für RFID-Systeme im Bereich der Tierhaltung, bspw. die zu verwendenden Frequenzen. Welche Transponderarten letztlich zum Einsatz kommen und wie diese an den Tieren „befestigt“ werden, kann sehr unterschiedlich gehandhabt werden und ist zum einen von der Tierart, zum anderen vom konkreten Einsatzzweck (inner-, überbetrieblich) und den damit verbundenen konkreten Anforderungen (z. B. Fälschungssicherheit) abhängig. Kein Identifikationssystem ist auch für alle Tiere gleich gut geeignet. Sowohl offene als auch geschlossene Systeme sind üblich.

Nachfolgend die häufigsten Verfahren Nutztiere mit RFID-Chips zu kennzeichnen:[2][3]

- Halsbandtransponder: eigenen sich besonders für den innerbetrieblichen Einsatz, da sie sehr leicht von einem Tier auf ein anderes gewechselt werden können. Für den überbetrieblichen Einsatz sind sie deshalb eher ungeeignet. Die Größe der Transponder beträgt ca. 100 mm x 80 mm x 20 mm.

- Ohrmarken: werden inner- und überbetrieblich eingesetzt, wobei Fälschungssicherheit erst mit zusätzlichen im Chip gespeicherten biometrischen Kennwerten (DNA, Iriserkennung, Nasenabdruck) gegeben ist. Ohrmarken können direkt ab Geburt bei den Tieren angebracht werden, die Abmessungen betragen ca. 30 mm im Durchmesser und 6 mm in der Stärke. Die Lesereichweite kann von ca. 40 cm bis zu 1 m reichen. Ohrmarken mit RFID-Chip konkurrieren besonders mit Barcode-Ohrmarken, deren o.g. Nachteile vor allem wegen der noch immer günstigeren Preise in Kauf genommen werden.

- Injizierbare Transponder: werden mit einem Spezialwerkzeug unter die Haut des Tieres platziert. Sie sind seit etwa 10 Jahren im Einsatz und sind insbesondere auch für eine überbetriebliche Nutzung geeignet, da Transponder und Tier fest miteinander verbunden sind und der RFID-Chip nur durch einen operativen Eingriff wieder entfernt werden kann. Zum Einsatz kommen Glastransponder mit Längen zwischen 10 und 32 mm, wobei nur Transponder zwischen 24-32 mm auch entsprechende Lesereichweiten von 30-40 cm erreichen. Eine typische Bauform ist deshalb die Abmessung 23,1 mm x 3,85 mm. Injiziert werden die Transponder entweder mit sog. „Single-shot"-Geräten bzw. „Multi-shot"-Geräten mit Magazin für mehrere Transponder. Diese unterscheiden sich neben der Menge an Transpondern die sie ohne „Nachladen" injizieren können darüber hinaus noch durch ihre Nadelformen, geschlossene Hohlnadeln („O"-Form) bei „Single-shot"-Geräten, leichter zu reinigende offene Hohlnadeln („U"-Form) bei „Multi-shot"-Geräten. Eine weitere Möglichkeit zur Injektion stellen transpondergefüllte, steril verpackte Einwegnadeln dar. Ein Problem injizierbarer Transponder ist, dass sie Fremdkörper im Gewebe des Tieres sind und unter Umständen im Körper der Tiere „wandern". Dies muss gar nicht für die Gesundheit der Tiere nachteilig sein, kann aber das Auslesen der Chips negativ beeinflussen. So haben Untersuchungen gezeigt, dass bspw. bei Rindern der beste Platz für die Transponder über dem Ansatz des rechten Ohres ist (Dreieckknorpel, *Scutulum*).

- Bolus: besteht aus einem Glastransponder, der in einem säurebeständigen, zylindrischen, 65 x 25 mm großen Gehäuse, bspw. aus Keramik, untergebracht wird. Über eine Sonde wird er im Vormagentrakt (dem sog. Pansen) von Wiederkäuern (Rindern, Schafen, Ziegen) untergebracht, wo er unter normalen Umständen aufgrund seines hohen Gewichts während der gesamten Lebensdauer der Tiere verbleibt. Allerdings kann der Bolus erst bei voller Entwicklung des Pansens verwendet werden, da ansonsten Ausscheidungsgefahr besteht. Aufgrund der sonstigen Vorteile wie die einfache, verletzungsfreie Einführung des Transponders in den Körper der Tiere sowie die einfachere Entsorgung der Boli im Schlachthof was die Auffindung und Entnahme betrifft ist diese Form der Kennzeichnung besonders für den Einsatz in der extensiven Rinderhaltung (Australien, Südamerika) geeignet.

Zusammenfassend bleibt festzuhalten, dass Injektat und Bolus die einzig fälschungssicheren Kennzeichnungsmöglichkeiten in der Tierhaltung sind. Was sich betriebsübergreifend letztlich durchsetzt bleibt noch abzuwarten.

Haustiere

...

5.3 Objektidentifikation (Produktionsgüter, Waren, Gegenstände, ...)

Barrierefreiheit im Alltag blinder Menschen

RFID-Tags auf Alltagsgegenständen helfen bei der Identifikation von Objekten, insbesondere solchen, die sich in Form und Haptik ähneln.[12] Intelligente Blindenstöcke könnten mit Hilfe von RFID die Orientierung erleichtern. [13] [14]

Warenhäuser / Supply Chain Management

Just in Time… Erst mit der lückenlosen Überwachung der sehr komplexen logistischen Abläufe innerhalb der Lieferkette (supply chain) kann dieses „Prinzip der Lagerhaltung" effizient funktionieren. Mit der Feststellung, wo sich eine Ware zu einem bestimmten Zeitpunkt befindet, können Lagerbestände von Waren- und Versandhäusern, Supermärkten, Produktionsbetrieben, usw. exakter angepasst, im Besten Fall sogar gegen null heruntergefahren werden. Dies senkt die Lagerhaltungskosten und minimiert gerade bei Supermärkten auch den Anteil nicht mehr verkaufbarer Waren, die vor allem im Lebensmittelbereich aufgrund abgelaufener Haltbarkeitsdaten problematisch sind. Trotzdem sind immer alle Waren verfügbar.[2][11][15]

Einer der wichtigsten und vielseitigsten Anwendungsgebiete von RFID-Systemen ist deshalb genau dieser Bereich, angefangen beim RFID-Einsatz zur Kontrolle des Warenflusses (Ein- und Ausgangskontrollen an jedem Glied der Lieferkette) bis zur RFID-System gestützten Fälschungs- und Diebstahlsicherung. Motivation für letzteres dürften vor allem Zahlen wie diese sein:

- jährlich werden Waren im Wert von 5-7% des Welthandelsvolumens gefälscht
- Waren im Wert von 1,8% des Gesamtumsatzes werden von Kunden und Personal gestohlen.[2]

Durch die Kennzeichnung jeder einzelnen Ware („item level tagging“) ergeben sich im Verkauf ein großes Potential für Rationalisierungen sowie vollkommen neue Möglichkeiten, z. B. durch:

- Bezahlung an Selbstbedienungsterminals bzw. bezahlen durch einfaches Vorbeiführen des gefüllten Einkaufswagens an einer entsprechenden RFID-Kassenstation, welche alle Waren direkt im Einkaufswagen erfasst und automatisch die Rechnung erstellt oder den Betrag gleich vom Konto des Kunden einbezieht[16][15]
- elektronische Preisauszeichnung, d.h. der Artikel sendet seinen Preis an ein Display am Regal, welches diesen darstellt (Preisänderungen würden dann nicht mehr manuell durch den Austausch der Preisschilder erfolgen, sondern bspw. durch Neuprogrammierung der Transponder)angepasste
- Spezialangebote, bspw. können einem Kunden, der in einer Umkleidekabine ein bestimmtes Kleidungsstück anprobiert auf einem Bildschirm dazu passende weitere Kleidungsstücke oder Accessoires präsentiert werden.[2]

Bei allem bisher genannten, spielt allerdings die Kundenakzeptanz eine entscheidende Rolle. Nicht alles was möglich und auf den ersten Blick Erfolg versprechend ist, gefällt auch dem Kunden. Entsprechend überlegt sollten die Potentiale der Technologie genutzt werden.[15]

Beim sog. „item level tagging“ kommen für die Markierung einzelner Gegenstände besonders HF-Transponderetiketten in Frage, da sie unempfindlicher als andere Transponder-Bauformen bezüglich umgebender Materialien sind. Sie sind zudem einfach anzubringen sind und ermöglichen ein zuverlässiges Auslesen. Es handelt sich in diesem Bereich des Anwendungsgebietes i.d.R. also um offene RFID-Systeme, die Transponder werden nicht wieder verwendet (Einwegtransponder).[2]

Anders kann es sich dagegen bei der Kennzeichnung von Containern, Paletten und Verpackungen innerhalb der Lieferkette verhalten. Hier sind sowohl offene als auch geschlossene Systeme vorzufinden. Die eingesetzten HF- und UHF-Transponder, die sich bspw. in Hohlräumen der Palettenfüsse befinden können, müssen entsprechend hohe Lesereichweiten und Lesegeschwindigkeiten aufweisen um beim Durchgang an der Laderampe sämtliche Informationen zu erfassen. Vorteile die sich durch den Einsatz von RFID im Bereich der Lieferketten zusätzlich ergeben, sind bspw. dass Verpackungen nicht mehr geöffnet werden müssen, um den Inhalt zu prüfen und diese Inhalte auch während des Transportes nicht mehr verändert werden können. Zeitverluste für die Erfassung beim Be- und Entladen gehören mit RFID der Vergangenheit an.[2][11]

Trotz enormer zu erwartender Investitionsaufwände bei der Umstellung von Barcode auf RFID-Systeme, vor allem natürlich bei den Lieferanten, steht für Kenner der Branche außer Frage, dass sich RFID in diesem Anwendungsbereich in Zukunft durchsetzen wird.

Industrielle Fertigung

...

Werkzeugidentifikation

...

Bücher in Bibliotheken

...

Akten in Behörden, Ämtern, Kanzleien

...

6 Datenschutz

6.1 Grundlagen

Datenschutz spielt in Deutschland eine große Rolle. Jede Person soll die Möglichkeit haben, sich darüber zu informieren, wer welche Daten zu welchem Zweck über die eigene Person speichert (Informationelle Selbstbestimmung). Immer mehr Organisationen sammeln, erfassen und werten verschiedene Informationen über Personen aus. Davor sollen jeder Einzelne geschützt werden, insbesondere dann, wenn er nichts von der Speicherung seiner Daten weiß. Dabei kann es sich sowohl um private Organisationen (wie z. B. Auskunfteien, Adresshandel, Arbeitgeber etc.) als auch um staatliche Stellen (z. B. Polizei und Geheimdienste, gesetzliche Sozialversicherungen, sonstige Ämter und Behörden) handeln. Im deutschen wie im europäischen Recht sollen Gesetze der Sicherung dieses Rechts dienen.[17]

Die immer größere Verbreitung moderner IT Systeme ermöglicht die immer schnellere Erfassung von Daten in immer kürzeren Zeiträumen. “Umso wichtiger ist es, gesetzlich zu Regeln, welche Rechte und Pflichten einem Jedem zur Verfügung stehen, um über seine Daten selbst bestimmen zu dürfen . Grundsätzlich soll jeder selbst darüber entscheiden dürfen, welche personenbezogenen Daten preisgegeben werden. „Als personenbezogene bezeichnet man Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Definition in §3 I Bundesdatenschutzgesetz - BDSG)" [18]

Im folgenden Abschnitt sollen die Risiken bei dem Einsatz der RFID Technologie aufgezeigt werden. Sie sollen den Stärken der neu entwickelten Systeme gegenüber-

stellt werden und mögliche Mißbrauchsszenarien aufzeigen. Bei allem “Hype” um die neuen Möglichkeiten der Technologien sollten mögliche Risiken nicht leichtfertig abgetan werden.

Bundesdatenschutzbeauftragter fordert RFID-Gesetz

6.2 RFID als Datenschutzrisiko

Die Diskussion um die RFID Technologie umfasst oft nur wirtschaftliche Bereiche, die die Informationserfassung, Informationsverwaltung und Informationsverdichtung thematisieren. Welche Daten sind zur Erfassung relevant und wie kann man sie am effizientesten weiterverwenden? Ziel ist es, nicht nur Warenursprünge und Warenbewegungen zu erfassen, sondern auch die für Unternehmen relevanten Daten, wie Kundenprofile und Kundenverhalten zu dokumentieren und auszuwerten. Zusätzlich erobert die RFID Technologie aber auch den privaten Bereiche, wie zum Beispiel die Reisepässe. Biometrische Daten sind in den kleinen RFID Chips gespeichert und können bei Bedarf ausgelesen werden. Immer mehr Daten werden auf diesem Weg gespeichert und können später drathlos ausgelesen werden. Doch wie kann der Verbraucher entscheiden, wer jetzt seine Daten auslesen darf und wer nicht. Zum Auslesen der Informationen wird die betroffene Person nicht benötigt, sprich, der Auslesende muss nicht durch eine Handlung autorisiert werden. Mit einem entsprechenden Lesegerät kann jeder entsprechende Informationen abrufen. Natürlich können die Daten verschlüsselt auf den Chips abgelegt werden, jedoch

Folgende Liste faßt nochmal die wichtigsten Datenschutzrisiken in Verbindung mit RFID Technologie zusammen (Vgl: www.datenschutz.de)

Risiken

- RFID-Systeme arbeiten drahtlos, so dass das Auslesen der Daten ohne Wissen des Besitzers erfolgen kann.
- RFID-Tags werden in Bauformen angeboten, die ein verstecktes Anbringen auf Waren ermöglichen. Der Käufer kann keine Schutzmaßnahmen ergreifen, wenn er über die Existenz des RFID-Tags nichts weiß.
- RFID-Tags ermöglichen eine weltweite eindeutige Kennzeichnung von einzelnen Gegenständen. Erworbene Produkte könnten somit weltweit eindeutig einzelnen Personen zugeordnet werden.
- Durch die Zusammenführung der Informationen aus RFID-Tags mit personenbezogenen Daten (z. B. Kundenkarten) lässt sich das Kaufverhalten einzelner Kunden detailliert analysieren.

Mit der rasanten Verbreitung der RFID Technologie und den damit verbundenen Risiken, ist es notwendig, dass der Gesetzgeber ein Rahmen definiert, in welchen klar geregelt ist, wer welche Rechte und Pflichten im Umgang mit den persönlichen Daten eines Jeden hat. Momentan fällt es den Privatpersonen immer schwerer, ihre privaten Daten vor zugriffen Dritter zu schützen. Dieser Effekt wird noch verstärkt durch die Verbreitung neuer Technologien. Die Datenschutzbeauftragten haben folgenden Maßnahmenkatalog vorgeschlagen, um einen umfangreichen Schutz der Privatpersonen aufzubauen (Vgl: www.datenschutz.de).

Maßnahmen

- Die betroffenen Personen müssen umfassend über Einsatz, Verarbeitung und Inhalt von RFID-Tags informiert werden.
- Kommunikationsvorgänge mit RFID-Tags, die eine Verarbeitung personenbezogener Daten auslösen, müssen für die betroffenen Personen transparent und eindeutig erkennbar sein.
- Daten auf RFID-Tags dürfen nur so lange gespeichert sein, wie es zur Erreichung des Zwecks erforderlich ist.
- Möglichkeiten zur Deaktivierung bzw. Löschung der Daten von RFID-Tags müssen geschaffen werden.
- Die Vertraulichkeit der gespeicherten und der übertragenen Daten muss durch wirksame Authentisierung der beteiligten Peripheriegeräte und durch Verschlüsselung sichergestellt werden.
- Bei RFID-Technologie mit Verarbeitungsfunktion müssen Systeme angeboten werden, die keine Seriennummern tragen.

7 Sicherheit von RFID-Systemen

Inhalt dieses Abschnitts ist es, die aus der Anwendung von RFID-Systemen hervorgehende Bedrohungslage sowie mögliche Sicherheitsmaßnahmen darzustellen. Dazu gehört eine Übersicht über mögliche Angriffe und Gegenmaßnahmen, sowie die Einschätzung der Bedrohungslage – insbesondere hinsichtlich Praktikabilität und Kosten der Angriffe und Gegenmaßnahmen.

7.1 Problemaufriss

Die Datensicherheit spielt beim Einsatz von RFID eine große Rolle. Dabei ist entscheidend, ob die Daten auf dem Chip gespeichert sind oder der Chip nur eine Nummer trägt, zu der Daten im System hinterlegt sind. Daten auf einem Transponder kann prinzipiell jeder abrufen, der mit einem Lesegerät Kontakt zum Transponder aufbauen kann. Um die Daten vor fremdem Auslesen zu

schützen, können der Zugriff oder die Daten beispielsweise durch Passwörter oder Chiffrierung gesichert werden. Allerdings benötigen kryptologische Verfahren Speicherplatz und Rechenleistung und machen so den Transponder teurer. Im System hinterlegte Daten können auf herkömmliche Weise gesichert werden, beispielsweise mit einer Firewall.

In den Medien wurde über erfolgreiches Hacking von RFID-Chips berichtet. Häufig besitzen kostengünstige Transponder keinen oder nur geringen Schutz gegen unerlaubtes Auslesen. Allerdings kann auf diesen auch meist nicht mehr als eine Produktnummer gelesen werden. Es gibt aber auch schon relativ günstige Transponder, die gegen Überschreiben geschützt sind und bei denen Abfragen nur nach einer Authentifizierung möglich sind. Transponder mit aufwendiger Codierung bieten zusätzliche Sicherheit. Da jeder Angriff Zeit und eine konstante Verbindung zum Transponder benötigt, ist das Hacken “im Vorbeigehen” kaum möglich. Sensible Daten werden durch weitere Sicherheitsvorkehrungen geschützt. Um beispielsweise die Daten auf dem deutschen Reisepass lesen zu können, muss zuerst die maschinenlesbare Zone auf der Datenseite des Passes optisch gelesen werden. Dadurch wird der Aufbau eines kryptographisch abgesicherten Kommunikationskanals zum Transponder ermöglicht. Erst nach der Berechnung des Zugriffsschlüssels können die Daten aus dem RFID-Tag gelesen werden.

Außer dem direkten Auslesen der Daten auf dem Chip kann auch versucht werden, die Datenübermittelung zwischen Transponder und Lesegerät zu “belauschen”. Dafür müsste aber das Lesegerät sehr nah an die Übertragung gebracht werden, da sensible Daten meist nur über kurze Distanzen übertragen werden. Zudem sind die abgehörten Daten meist verschlüsselt, zum Beispiel mit 224 Bits beim deutschen Reisepass. Durch Regelungen im Bundesdatenschutzgesetz (BDSG), dem Telekommunikationsgesetz (TKG) und dem StGB ist zudem das unbefugte Auslesen von Transpondern und das Abhören von Datenübertragung untersagt.

Im Vergleich zu anderen ID-Systemen gibt es spezifische RFID-Probleme:

- Identifikation ohne Berührung oder Sichtkontakt
- weltweit eindeutige Identifikation von Objekten
- Speicherplatz für zusätzliche Daten
- Mehrfachzugriff
- massive Preissenkungen zu erwarten

Aus diesen Problemen ergeben sich folgende sicherheitsrelevante Konsequenzen:

- unbemerktes Auslesen möglich
- Wiedererkennen individueller Objekte möglich
- zusätzliche Manipulationsmöglichkeiten
- neue Anwendungsgebiete, tiefere Durchdringung
- zunehmende Abhängigkeit von RFID-Systemen

7.2 Grundlegende Angriffsarten

RFID-Systeme bestehen aus drei wichtigen Beziehungen.[6] Es ist deshalb entscheidend für die Integrität von RFID-Systemen, dass diese drei Beziehungen gesichert sind:

1. Die Transponder-Daten-Verbindung.
   Die Beziehung zwischen dem Transponder (Tag) und den auf dem Transponder gespeicherten Daten. Da der Transponder ausschließlich durch die Daten identifiziert wird, muss es sich hierbei um eine eindeutige Beziehung handeln. Um ausschliessen zu können, dass zwei Tags gleicher Identität existieren, gehört zu diesen Daten eine eindeutige ID-Nummer (Seriennummer). Zusätzlich können auch Schlüssel oder andere Sicherheitsinformationen auf dem Transponder abgelegt sein.

2. Die mechanische Verbindung.
   Die Beziehung zwischen dem Transponder und dem Trägerobjekt, zu dessen Identifikation er dient. Diese Beziehung muss ebenfalls eindeutig sein, d.h. ein Transponder darf während seiner Nutzungsphase nicht wechselnden Objekten zugeordnet werden.

3. Die Luftschnittstelle.
   Die Beziehung zwischen Transponder und Lesegerät. Diese Schnittstelle muss autorisierten Lesegeräten die Anwesenheit des Transponders sichtbar machen und den korrekten Datenzugriff ermöglichen. Nicht autorisierte Lesegeräte sollen dagegen vom Zugriff ausgeschlossen bleiben.

Die Abbildung zeigt die grundlegenden Angriffsarten[6], die im Folgenden erläutert werden.

7.2.1 Angriffe auf den Transponder

Inhalt fälschen
Die Daten des Tags werden durch unautorisierte Schreibzugriffe gefälscht. Dabei bleiben die ID (Seriennummer) und eventuelle Sicherheitsinformationen (z. B. Schlüssel) unverändert, so dass das Lesegerät die Identität des Transponders weiterhin korrekt erkennt. Demzufolge ist dieser Angriff nur bei solchen RFID-Systemen möglich, die neben ID und Sicherheitsinformationen weitere Inhalte auf dem Tag speichern.

Identität fälschen (Transponder)
Bei diesem Angriff wird ein neues Tag als Duplikat des

alten hergestellt (Cloning) oder durch ein Gerät das Tag emuliert. Dazu muss der Angreifer über die ID und eventuelle Sicherheitsinformationen des zu fälschenden Tags verfügen. Diese benutzt der Angreifer, um gegenüber einem Lesegerät die Identität des Tags vorzutäuschen. Dieser Angriff hat zur Folge, dass mehrere Transponder mit gleicher Identität existieren.

Deaktivieren
Durch unautorisierten Gebrauch von Lösch- oder Kill-Befehlen oder durch physische Zerstörung wird der Transponder unbrauchbar gemacht. Als Folge dieses Angriffs kann das Lesegerät die Identität des Tags nicht mehr feststellen oder die Anwesenheit des Tags im Lesebereich nicht mehr erkennen.

7.2.2 Angriffe auf die mechanische Verbindung

Ablösen
Ähnlich wie zum Beispiel beim „Umkleben“ von Preisschildern wird der Transponder vom Trägerobjekt getrennt und möglicherweise einem anderen Objekt zugeordnet. Da RFID-Systeme davon abhängig sind, dass die Transponder ihre Trägerobjekte eindeutig identifizieren, geht es hierbei um ein grundlegendes Sicherheitsproblem.

7.2.3 Angriffe auf die Luftschnittstelle

Abhören
Die Kommunikation zwischen Lesegerät und Transponder über die Luftschnittstelle wird aufgefangen und die Funksignale werden dekodiert. Diese Art des Angriffs ist eine der wesentlichsten Bedrohungen von RFID-Systemen.

Blocken
Dem Lesegerät wird die Anwesenheit einer beliebigen Anzahl von Transpondern simuliert. Diese so genannten Blocker-Tags führen dazu, dass das Lesegerät blockiert wird. Dabei muss ein Blocker-Tag für das jeweils verwendete Antikollisionsprotokoll ausgelegt sein.

Stören
Durch passive Maßnahmen (Abschirmen) oder durch aktive Maßnahmen (Störsender) wird der Datenaustausch über die Luftschnittstelle gestört. Dabei sind aufgrund der hohen Empfindlichkeit der Luftschnittstelle bereits einfache passive Maßnahmen wirksam.

Identität fälschen (Lesegerät)
In einem sicheren RFID-System muss das Lesegerät seine Berechtigung gegenüber dem Tag nachweisen. Damit ein Angreifer die Daten mit einem eigenen Lesegerät auslesen kann, muss dieses die Identität eines autorisierten Lesegeräts vortäuschen. Diese Art von Angriff reicht auf der Skala der Durchführbarkeit von „sehr einfach“ bis „praktisch unmöglich“, in Abhängigkeit von den verwendeten Sicherheitsmaßnahmen. Zum Beispiel könnte das Lesegerät Zugang zum Backend benötigen, um dort hinterlegte Schlüssel abzurufen.

7.3 Motive von Angriffsarten

Ein Angriff auf ein RFID-System kann mit unterschiedlichen Motiven erfolgen.[6] Diese Motive lassen sich in drei Arten unterscheiden:

1. Ausspähen: Der Angreifer verschafft sich Informationen über einen unberechtigten Zugriff.
2. Täuschen: Der Angreifer täuscht durch falsche Informationen den Betreiber oder Benutzer eines RFID-Systems.
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 möchte diese durch einen Angriff auf das System schützen.

Diese Unterteilung nach dem Motiv des Angriffs ist nicht scharf abgrenzbar. So kann es zum Beispiel vorkommen, dass ein Angreifer zunächst in der Absicht des Ausspähens Tag-IDs ermittelt, um sie später in Täuschungsabsicht zu verwenden.

Die oben aufgeführten Angriffsarten lassen sich nun ihrem (primären) Motiv zuordnen:[6]

7.4 Bedrohungslage der beteiligten Parteien

Typischerweise sind die Interessen der Betreiber eines RFID-Systems mit den Interessen ihrer Kunden oder Angestellten nicht deckungsgleich. Folglich gibt es bei RFID-Systemen zwei Parteien mit unterschiedlichen Interessen zu beachten:[19]

Aktive Partei Der Betreiber des RFID-Systems.

Die aktive Partei gibt die Tags aus und verwaltet die mit ihnen assoziierten Daten. Ferner hat sie die Daten des RFID-Systems und ihre Verwendung unter Kontrolle.

Passive Partei Träger von Tags oder mit Tags versehenen Objekten.

Die passive Partei ist in der Regel ein Kunde oder Angestellter des Betreibers des RFID-Systems. Obgleich die passive Partei im Besitz von Tags ist, hat sie in der Regel keinen Einfluss auf deren Verwendung.

Der Betreiber ist an der fehlerfreien Funktionsweise des RFID-Systems interessiert. Die passive Partei ist daran nur insoweit interessiert, als das ihr durch das System nicht mehr Nachteile als Vorteile entstehen. Vor allem Verbraucherorganisationen befürchten eine zusätzliche Bedrohung der Privatsphäre durch den Einsatz von RFID-Systemen. Zum Beispiel trägt das Abhören der Luftschnittstelle zu diesem Bedrohungspotenzial bei. Andererseits kann die Verwendung von Blocker-Tags zum Schutz der Privatsphäre beitragen und somit die Einflussmöglichkeiten der passiven Partei stärken.

Grundsätzlich wird die Bedrohungslage aus der Sicht verschiedener Akteure betrachtet.

7.4.1 Bedrohungslage für die aktive Partei

Dieser Abschnitt stellt die Bedrohungslage aus der Perspektive der aktiven Partei dar, also dem Betreiber des RFID-Systems.

Die Bedrohungslage der aktiven Partei setzt sich zusammen aus:[19]

- Angriffen der passiven Partei (Angestellte oder Kunden)
- Angriffen einer Drittpartei (Konkurrenten, Wirtschaftsspione, Cyberterroristen).

Die möglichen Angriffe auf die aktive Partei werden im Folgenden erläutert.

Ausspähen von Daten
Das Ausspähen von Daten durch den Angreifer kann wie folgt geschehen:

- Die Kommunikation zwischen Tags und Lesegeräten wird vom Angreifer mit einem eigenen Empfänger abgehört. Dabei kann die Entfernung größer sein als die standardmäßig vorgesehene Lesedistanz.
- Die Daten aus den Tags werden vom Angreifer mit einem eigenen Lesegerät auslesen. Dabei kann das Lesegerät versteckt installiert sein oder auch mobil eingesetzt werden. Darüber hinaus muss der Angreifer die Identität des Lesegeräts fälschen können, für den Fall dass eine Authentifizierung des Lesegeräts vorgesehen ist.

Einspeisen falscher Daten (Täuschen)
Folgende Angriffe können vom Angreifer in Täuschungsabsicht durchgeführt werden:

- Der Inhalt eines Tags wird vom Angreifer verändert. Diese Art des Angriffs ist jedoch nur möglich, wenn die der ID zugeordneten Daten auf den Tags selbst (und nicht im Backend) gespeichert werden. In den meisten Anwendungen ist dies aber nicht der Fall.
- Tags werden vom Angreifer emuliert oder dupliziert (Cloning). Um die Identität gegenüber dem Lesegerät vortäuschen zu können, muss der Angreifer hierzu mindestens von der ID (Seriennummer) und, je nach Sicherheitsverfahren, auch von Passwörtern oder Schlüsseln Kenntnis haben.
- Das Tag wird vom Trägerobjekt losgelöst, um dessen Bewegungen vor dem Lesegerät zu verbergen oder ein anderes Objekt als das ursprüngliche Trägerobjekt auszugeben. Da der Angreifer dazu das Trägerobjekt beschädigen muss, wird der Nutzen des Angriffs stark verringert.

Denial of Service
Der Angreifer hat viele Möglichkeiten, um die korrekte Funktionsweise eines RFID-Systems zu beeinträchtigen:

- Mechanische oder chemische Zerstörung der Tags (durch Knicken, Druck- oder Zugbelastung, Säureeinwirkung etc.).
- Zerstörung der Tags durch elektromagnetische Feldeinwirkung (durch eigens dafür ausgelegte Sender oder durch Mikrowellenherde), ähnlich dem regulären Verfahren zur Deaktivierung von 1-Bit-Transpondern (Diebstahlsicherung).
- Deaktivieren der Tags durch Missbrauch von Lösch- oder Kill-Befehlen. Dafür muss der Angreifer die Identität eines autorisierten Lese- bzw. Schreibgerätes vortäuschen.
- Entladen der Batterie aktiver Tags durch eine Serie von Anfragen. Dies ist bei passiven Tags nicht möglich, da sie ihre Energie ausschließlich über das Lesegerät beziehen.
- Simulation der Anwesenheit beliebig vieler Tags gegenüber dem Lesegerät durch ein Blocker-Tag, um die Erfassung der vorgesehenen Tags zu verhindern.
- Die Kommunikation zwischen Erfassungsgerät und Tag wird durch Störsender verhindert. Dieser Angriff wäre leicht zu entdecken, da für größere Distanzen sehr starke Sender erforderlich wären.
- Löschung des elektromagnetischen Feldes durch reflektierende Objekte.
- Die Feldfrequenz wird durch die Nähe von Wasser, Metall oder Ferrit verstimmt.
- Abschirmung der Tags gegen elektromagnetische Felder durch metallische Folien oder mit Metallstreifen versehenen Taschen.

Bislang ist allerdings noch wenig Erfahrung vorhanden bezüglich der praktischen Durchführbarkeit dieser Angriffe und der Wirksamkeit von Gegenmaßnahmen.[6]

7.4.2 Bedrohungslage für die passive Partei

Dieser Abschnitt stellt die Bedrohungslage aus der Perspektive der passiven Partei dar, also z. B. aus Sicht des Kunden oder eines Arbeitnehmers des Betreibers. Die passive Partei benutzt Tags oder mit Tags gekennzeichnete Objekte, hat aber keine Kontrolle über die auf den Tags gespeicherten Daten.

Die Bedrohungslage der passiven Partei besteht aus:[19]

- Nutzung oder Weitergabe der Daten durch die aktive Partei zum Nachteil der passiven Partei
- Angriffen durch eine Drittpartei

Die Themen Datenschutz bzw. Bedrohungen der Privatsphäre prägen die Diskussion über RFID-bedingte Risiken für die passive Partei. Bedrohungen der Privatsphäre können von der aktiven Partei oder von Drittparteien ausgehen.

Da die aktive Partei als Betreiber des RFID-Systems die volle Kontrolle darüber hat, ist in diesem Fall kein Angriff auf das System erforderlich. Beispielsweise könnte die aktive Partei sensible Daten weitergeben, ohne dass die betroffenen Personen davon wissen. Allerdings verstößt die aktive Partei dabei gegen geltendes Datenschutzrecht.

Im zweiten Fall führt eine Drittpartei einen Angriff auf das RFID-System aus. Da das Ziel des Angriffs unautorisierter Zugang zu Daten ist, sind die Folgen für die passive Partei sehr ähnlich. Auch in diesem Fall können sensible Daten ohne Wissen und Zustimmung des Betroffenen in fremde Hände gelangen.

Bei den Bedrohungen der Privatsphäre werden Data Privacy und Location Privacy unterschieden.[6]

Data Privacy Schutz von Daten gegen unbefugten Zugriff, aus denen Aussagen über Personen abgeleitet werden können.

Location Privacy Schutz von Daten gegen unbefugten Zugriff, aus denen momentane oder frühere Aufenthaltsorte von Personen abgeleitet werden können.

Insgesamt wird aber die Privatsphäre der passiven Partei weniger durch Angriffe auf RFID-Systeme als durch ihren Normalbetrieb bedroht, weil die aufgebauten Datenbestände nachträglich zweckfremde Auswertungen ermöglichen. Allerdings besteht diese Gefahr auch bei akzeptierten Systemen wie Kreditkarten, Kundenkarten, Mobiltelefonie.

Bedrohung der Data Privacy
Durch die Speicherung personenbezogener Daten in einem RFID-System kann die Privatsphäre der passiven Partei bedroht sein:

- Ein potenzieller Angreifer kann sich durch Abhören der Luftschnittstelle oder unautorisiertes Auslesen von Tags unberechtigt Zugang zu Daten verschaffen.
- Aufgrund der zunehmenden Dichte der von Personen hinterlassenen Datenspuren könnten neben personenbezogenen Daten auch potenziell personenbezogene Daten zu einem Angriffsziel werden. Potenziell personenbezogene Daten sind anonymisierte Daten, die durch Kombination von Daten mit hoher Wahrscheinlichkeit treffend einzelnen Personen zugeordnet werden können.
- Mit der steigenden Verfügbarkeit der Daten steigt auch das Risiko, dass die Datenbestände ohne Wissen der Betroffenen zu nicht bestimmungsgemäßen Zwecken ausgewertet werden. Insbesondere kann ein neuer Bedarf an Auswertungen der Daten entstehen (bei der aktiven Partei oder bei einer Drittpartei, z. B. auch bei staatlichen Kontrollinstanzen), die möglicherweise nicht im Interesse der passiven Partei liegen.

Bedrohung der Location Privacy
Eine weitere Bedrohung der Privatsphäre ist die Möglichkeit des Tracking. Beim Tracking werden durch wiederholtes Auslesen der IDs (Seriennummern) Bewegungsprofile erstellt. Voraussetzungen für erfolgreiches Tracking sind:

- Tags befinden sich über einen längeren Zeitraum im Besitz der gleichen Person
- großer Umlauf an Tags (allgegenwärtig im Alltagsleben)

Eine Bedrohung der Privatsphäre kann auch dann vorliegen, wenn beim Auslesen von RFID-Tags ausschließlich IDs übertragen werden und alle anderen Daten ins Backend verlagert sind. Denn bei der Verfolgung mehrerer Personen lassen sich so auch Kontaktprofile erstellen.

Das Abhören der Luftschnittstelle ist hier wiederum eine RFID-spezifische Bedrohung, bei der neben dem geographischen Aufenthaltsort auch die genaue Interaktion mit vorhandenen Betrieben und Infrastrukturen festgestellt werden kann. Im Vergleich zur Benutzung von Mobiltelefonen erzeugt die Benutzung von RFID-Tags also wesentlich präzisere Datenspuren.[6]

7.5 Sicherheitsmaßnahmen

Die BSI-Studie[6] nennt eine Reihe von Sicherheitsmaßnahmen, um die Bedrohung durch Angriffe auf RFID-Systeme zu verringern.

8 Wirtschaftliche Aspekte von RFID

Fallende Preise für RFID-Tags werden die Ausbreitung von RFID stark vorantreiben. Für einfache RFID-Tags kann der Preis schon bald bei weniger als 10 Cent liegen. Sollte der Preis für RFID-Tags auf unter 1 Cent pro Chip sinken, können vor allem grosse Handelsketten wie Metro und Wal Mart damit beginnen, alle Produkte mit RFID auszeichnen.

Bis zum flächendeckendem Einsatz von RFID stehen allerdings auch noch technische Hindernisse im Weg: Derzeit ist beispielsweise noch ungeklärt, wie sich metallische Produkte und Getränke mit RFID auszeichnen lassen – beide Materialien stören die Funkübertragung bisher empfindlich. Auch Geräte, mit denen sich RFID-Chips nach dem Einkauf "unschädlich" machen lassen, sind noch unausgereift, denn die weltweit eindeutige ID des RFID-Chips bleibt dabei erhalten. Außerdem muss der Kunde jeden Chip einzeln deaktivieren, was bei einer großen Anzahl eingekaufter Produkte sehr lästig ist.

8.1 Der Kostenfaktor

Kosten für den elektronischen Reisepass

Ein zehn Jahre gültiger ePass wird in Deutschland 59 EURO kosten (zum Vergleich USA: voraussichtlich ca. 75 EURO, Großbritannien 103 EURO). Für einen fünf Jahre gültigen ePass, der Personen ausgestellt wird, die das 26. Lebensjahr noch nicht vollendet haben, beträgt die Gebühr 37,50 EURO.

8.2 Nutzen von RFID

Studien belegen das große Potenzial der RFID-Technologie. Danach werden durch Einsatz von RFID und Electronic Data Interchange (EDI) Einsparungen in Millionenhöhe erwartet. Mit Hilfe von RFID kann die Warenverfügbarkeit deutlich gesteigert werden. Das wiederum wird sich signifikant auf den Umsatz und die Kundenzufriedenheit auswirken. Auch die Effizienz der Wiederbeschaffung wird durch RFID merkbar unterstützt. Fehlbestände können mithilfe von RFID deutlich schneller wieder aufgefüllt werden. So lassen sich interne Unternehmensprozesse effizienter gestalten. Auch wenn es um die Sicherheit und Integrität von Produkten und Prozessen geht, wird RFID schon erfolgreich eingesetzt. Prominentestes Beispiel ist hier der Pharma-Hersteller Pfizer, der sein Medikament „Viagra" in den USA mithilfe der Transponder auf den Verpackungen vor Fälschungen schützt.

8.3 Einsatzbeispiele und Nutzenpotentiale

9 Ausblick

10 Quellen

[1] http://www.pco-barcode.de/staticsite/staticsite.php?menuid=235&topmenu=296&keepmenu=inactive Stand: 22.01.2007

[2] Christian Kern: „Anwendung von RFID-Systemen - 2., verbesserte Auflage", Springer-Verlag, 2006, ISBN 3-540-44477-7

[3] Klaus Finkenzeller: „RFID Handbuch – 4. Auflage", Hanser Verlag, 2006, ISBN 3-446-40398-1

[4] Wolfgang Seifert, Josef Decker: „RFID in der Logistik, Erfolgsfaktoren für die Praxis", Deutscher Verkehrs-Verlag, 2005, ISBN 3-87154-322-5

[5] http://www.rfid-journal.de/rfid-technik.html Stand: 22.01.2007

[6] Bundesamt für Sicherheit in der Informationstechnik: Risiken und Chancen des Einsatzes von RFID-Systemen, http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf Stand: 29.10.2006

[7] http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf Stand: 12.01.2007

[8] http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/ePass__Biometrie/Biometrie__FAQ.html Stand: 12.01.2007

[9] http://www.golem.de/0506/38374.html Stand: 12.01.2007

[10] http://de.wikipedia.org/wiki/Radio_Frequency_Identification Stand:12.01.2007

[11] Robert und Gabriele Schoblick: „RFID – Radio Frequency Identification", Franzis Verlag, 2005, ISBN 3-7723-5920-5

[12] http://www.abendblatt.de/ratgeber/wissen/forschung/article364540/Ein-Chip-hilft-Blinden-beim-Suchen.html

[13] http://www.gesundheitsforschung-bmbf.de/de/2227.php

[14] http://www.rfid-im-blick.de/200908181564/rfid-erleichtert-alltag-von-blinden-studierenden.html

[15] http://www.eicar.org/rfid/infomaterial/Spiegel_Nr.46_08.11.2004_RFID.pdf

[16] http://www.tec-channel.de/technologie/trends/431196

[17] Virtuelles Datenschutzbüro - Was ist Datenschutz (www.datenschutz.de)

[18] Virtuelles Datenschutzbüro - Was ist Datenschutz (www.datenschutz.de)

[19] Hilty, L.: Risiken und Chancen des Einsatzes von RFID-Systemen, EMPA, 17.11.2004

11 Links

http://rfid-informationen.de/

http://www.rfid-in-action.eu/public/rfid-reference-model/rfid-reference-model/

http://www.epass.de/

http://www.rfidjournal.com/ Internationale RFID-Zeitschrift

http://www.rfid-grundlagen.de/

http://www.rfid-ready.de/

http://rfid-im-blick.de/

http://www.epcglobal.de/

http://www.rfid-basis.de/

http://www.meyerrfid.com/

http://en.wikipedia.org/wiki/RFID

http://www.rfidnews.info/

http://www.mac-dos.de/index.php?id=391

http://www.rfidgazette.org/ http://rfidiot.org/ Englischsprachige Seite mit vielen Informationen über RFID-Programmiergeräte und die TAGs. Software in Python zum Ändern der Informationen auf den TAGs.

12 Text- und Bildquellen, Autoren und Lizenzen

12.1 Text

- **RFID-Technologie** *Quelle:* https://de.wikibooks.org/wiki/RFID-Technologie?oldid=813055 *Autoren:* ThePacker, Klaus Eifert, Dr. Gert Blazejewski, MichaelFrey, SvonHalenbach, CommonsDelinker, Gottschalk47, Thorgal~dewikibooks, Heuler06, TCUhimself, Fippteh-ler~dewikibooks, Chatter, Juetho, Qwertz84 und Anonyme: 26

12.2 Bilder

- **Datei:EPC-RFID-TAG.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/c/c6/EPC-RFID-TAG.jpg *Lizenz:* CC-BY-SA-3.0 *Autoren:* ? *Ursprünglicher Schöpfer:* ?
- **Datei:Frequenzbereiche.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/a/ab/Frequenzbereiche.jpg *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Siwita
- **Datei:Gnome-applications-office.svg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/e/e0/Gnome-applications-office.svg *Lizenz:* CC BY-SA 3.0 *Autoren:* HTTP / FTP *Ursprünglicher Schöpfer:* GNOME icon artists
- **Datei:Key.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/e/ef/Key.jpg *Lizenz:* Public domain *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Tnicol01
- **Datei:Lücke.png** *Quelle:* https://upload.wikimedia.org/wikibooks/de/e/ef/L%C3%BCcke.png *Lizenz:* ? *Autoren:* ? *Ursprünglicher Schöpfer:* ?
- **Datei:MAutoRace.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/4/4a/MAutoRace.jpg *Lizenz:* Public domain *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* JMinter
- **Datei:QSicon_Formatierung_Blue.svg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/7/74/QSicon_Formatierung_Blue.svg *Lizenz:* CC-BY-SA-3.0 *Autoren:* Image:QSicon_Formatierung.svg *Ursprünglicher Schöpfer:* kaneiderdaniel
- **Datei:RFID_hand_1.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/9/99/RFID_hand_1.jpg *Lizenz:* CC BY-SA 2.0 *Autoren:* ? *Ursprünglicher Schöpfer:* ?
- **Datei:Rfidrp.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/5/57/Rfidrp.jpg *Lizenz:* CC-BY-SA-3.0 *Autoren:* ? *Ursprünglicher Schöpfer:* ?
- **Datei:Transponder.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/e/ee/Transponder.jpg *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Uwe Gille

12.3 Inhaltslizenz

- Creative Commons Attribution-Share Alike 3.0