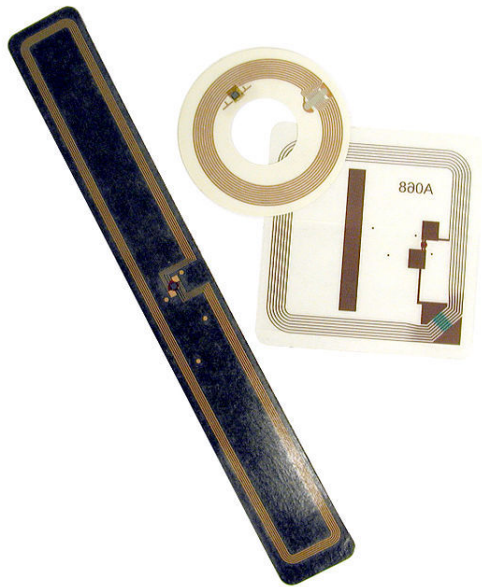


RFID



Verschiedene RFID-Transponder



Universelles RFID-Handlesegerät für 125 kHz, 134 kHz und 13,56 MHz; optional Barcode

RFID (englisch radio-frequency identification ['reɪdrəs 'f.i:kwənsi aɪ'dentɪfɪ'keɪʃn] „Identifizierung mit Hilfe elektromagnetischer Wellen“) bezeichnet eine Technologie für Sender-Empfänger-Systeme zum automatischen



Medea, ein mobiles Gerät mit Kreuzdipol und 2D-Barcode Imager, 630 mW Leistung



RFID-Bluetooth-Handlesegerät für 13,56 MHz, mit Ferritantenne zum Auslesen sehr kleiner Transponder aus Metall

und berührungslosen Identifizieren und Lokalisieren von Objekten und Lebewesen mit Radiowellen.

Ein RFID-System besteht aus einem **Transponder** (umgangssprachlich auch *Funketikett* genannt), der sich am oder im Gegenstand bzw. Lebewesen befindet und einen kennzeichnenden Code enthält, sowie einem *Lesegerät* zum Auslesen dieser Kennung.

RFID-Transponder können so klein wie ein Reiskorn sein und implantiert werden, etwa bei Haustieren oder Menschen. Darüber hinaus besteht die Möglichkeit, RFID-



LogiScan, ein mobiles Android-5.1-Gerät mit LF- und HF-RFID in einem Gerät

Transponder über ein spezielles Druckverfahren stabiler Schaltungen aus Polymeren herzustellen.^[1] Die Vorteile dieser Technik ergeben sich aus der Kombination der geringen Größe, der unauffälligen Auslesemöglichkeit (z. B. bei dem am 1. November 2010 neu eingeführten Personalausweis in Deutschland) und dem geringen Preis der Transponder (teilweise im Cent-Bereich).

Die Kopplung geschieht durch vom Lesegerät erzeugte magnetische Wechselfelder in geringer Reichweite oder durch hochfrequente Radiowellen. Damit werden nicht nur Daten übertragen, sondern auch der Transponder mit Energie versorgt. Zur Erreichung größerer Reichweiten werden aktive Transponder mit eigener Stromversorgung eingesetzt, die jedoch mit höheren Kosten verbunden sind.

Das Lesegerät enthält eine Software (ein Mikroprogramm), die den eigentlichen Leseprozess steuert, und eine RFID-Middleware mit Schnittstellen zu weiteren EDV-Systemen und Datenbanken.

1 Entwicklungsgeschichte

Die ersten RFID-Anwendungen wurden Ende des Zweiten Weltkrieges im Luftkrieg zwischen Großbritannien und Deutschland eingesetzt. Dort diente ein Sekundärradar zur Freund-Feind-Erkennung.^[2] In den

Flugzeugen und Panzern waren Transponder und Lesereinheiten angebracht, um zu erkennen, ob die zu beschießende Stellung oder die anfliegenden Flugzeuge anzugreifen waren oder nicht. Bis heute werden Nachfolgesysteme in den Armeen eingesetzt. Harry Stockman gilt als derjenige, der die Grundlagen von RFID mit seiner Veröffentlichung „Communication by Means of Reflected Power“ im Oktober 1948 gelegt hat.^[3]

Ende der 1960er-Jahre wurde als eine von vielen proprietären Lösungen die „Siemens Car Identification“, kurz SICARID, entwickelt. Damit war es möglich, zunächst Eisenbahnwagen und später Autoteile in der Lackiererei eindeutig zu identifizieren. Eingesetzt wurde es bis in die 1980er-Jahre. Die Identifikationsträger waren Hohlraumresonatoren, die durch das Eindrehen von Schrauben einen Datenraum von 12 bit abdecken konnten. Abgefragt wurden sie durch eine lineare Frequenzrampe. Diese Hohlraumresonatoren können als erste rein passive und elektromagnetisch abfragbare Transponder betrachtet werden. Der erste passive Backscatter-Transponder der heute noch verwendeten Bauart mit eigener digitaler Logikschaltung wurde erst 1975 in einem IEEE-Aufsatz vorgestellt.

In den 1970er-Jahren wurden die ersten primitiven kommerziellen Vorläufer der RFID-Technik auf den Markt gebracht. Es handelte sich dabei um elektronische Warensicherungssysteme (engl. *Electronic Article Surveillance*, EAS). Durch Prüfung auf Vorhandensein der Markierung kann bei Diebstahl ein Alarm ausgelöst werden. Die Systeme basierten auf Hochfrequenztechnik bzw. niedrig- oder mittelfrequenter Induktionsübertragung.

Das Jahr 1979 brachte zahlreiche neue Entwicklungen und Einsatzmöglichkeiten für die RFID-Technik. Ein Schwerpunkt lag dabei auf Anwendungen für die Landwirtschaft, wie beispielsweise Tierkennzeichnung, z. B. für Brieftauben, Nutzvieh und andere Haustiere.

Gefördert wurde die Anwendung der RFID-Technik seit den 1980er-Jahren besonders durch die Entscheidung mehrerer amerikanischer Bundesstaaten sowie Norwegens, RFID-Transponder im Straßenverkehr für Mautsysteme einzusetzen. In den 1990ern kam RFID-Technik in den USA verbreitet für Mautsysteme zum Einsatz.

Es folgten neue Systeme für elektronische Schlösser, Zutrittskontrollen, bargeldloses Zahlen, Skipässe, Tankkarten, elektronische Wegfahrsperren und so weiter.^{[4][5]}

1999 wurde mit Gründung des Auto-ID-Centers am MIT die Entwicklung eines globalen Standards zur Warenidentifikation eingeläutet. Mit Abschluss der Arbeiten zum Electronic Product Code (EPC) wurde das Auto-ID Center^[6] 2003 geschlossen. Gleichzeitig wurden die Ergebnisse an die von Uniform Code Council (UCC) und EAN International (heute GS1 US und GS1) neu gegründete EPCglobal Inc. übergeben.

2006 ist es Forschern des Fraunhofer-Institut für

Fertigungstechnik und Angewandte Materialforschung (IFAM) in Bremen erstmals gelungen, temperaturunempfindliche RFID-Transponder in metallische Bauteile aus Leichtmetall einzugießen. Durch diese Verfahrensentwicklung ist es möglich, die herkömmlichen Methoden zur Produktkennzeichnung von Gussbauteilen durch die RFID-Technologie zu ersetzen und die RFID-Transponder direkt während der Bauteilherstellung im Druckgussverfahren in dem Bauteil zu integrieren. 2011 gab das IFAM bekannt, dass es auch gelungen sei, einen RFID-Chip mit dem **generativen Fertigungsverfahren des Laserschmelzens** in chirurgische Instrumente mit komplexem Innenleben zu integrieren.^[7]

2 Technik

Die RFID-Transponder unterscheiden sich zunächst je nach Übertragungsfrequenz, Hersteller und Verwendungszweck voneinander. Der Aufbau eines RFID-Transponders sieht prinzipiell eine **Antenne**, einen **analogen Schaltkreis** zum Empfangen und Senden (**Transceiver**) sowie einen **digitalen Schaltkreis** und einen permanenten Speicher vor. Der digitale Schaltkreis ist bei komplexeren Modellen ein kleiner **Mikrocontroller**.

RFID-Transponder verfügen über einen mindestens einmal beschreibbaren Speicher, der ihre unveränderliche Identität enthält. Werden mehrfach beschreibbare Speicher eingesetzt, können während der Lebensdauer weitere Informationen abgelegt werden.

Nach Anwendungsgebiet unterscheiden sich auch die sonstigen Kennzahlen, wie z. B. Taktfrequenz, Übertragungsrate, Lebensdauer, Kosten pro Einheit, Speicherplatz, Lesereichweite und Funktionsumfang.

2.1 Funktionsweise

Die Übertragung der Identinformation erfolgt bei Systemen, die nach ISO 18000-1 ff. genormt sind, folgendermaßen: Das Lesegerät (Reader), das je nach Typ ggf. auch Daten schreiben kann, erzeugt ein hochfrequentes elektromagnetisches Wechselfeld, dem der RFID-Transponder (RFID-Tag; von engl. *tag*: Etikett, Anhängerzettel) ausgesetzt wird. Die von ihm über die Antenne aufgenommene Hochfrequenzenergie dient während des Kommunikationsvorganges als Stromversorgung für seinen Chip. Bei aktiven Tags kann die Energieversorgung auch durch eine eingebaute Batterie erfolgen. Bei halbaktiven Tags übernimmt die Batterie lediglich die Versorgung des Mikrochips.

Der so aktivierte Mikrochip im RFID-Tag decodiert die vom Lesegerät gesendeten Befehle. Die Antwort codiert und moduliert das RFID-Tag in das eingestrahlte elektromagnetische Feld durch Feldschwächung im kontaktfreien Kurzschluss oder gegenphasige Reflexion des vom Lesegerät ausgesendeten Feldes. Damit überträgt das Tag

seine eigene unveränderliche Seriennummer, weitere Daten des gekennzeichneten Objekts oder andere vom Lesegerät abgefragte Information. Das Tag erzeugt selbst also kein Feld, sondern beeinflusst das elektromagnetische Sendefeld des Readers.

Die RFID-Tags arbeiten je nach Typ im Bereich der **Langwelle** bei 125 kHz, 134 kHz, 250 kHz, 375 kHz, 500 kHz, 625 kHz, 750 kHz, 875 kHz, der **Kurzwelle** (HF) bei 13,56 MHz, der **UHF** bei 865–869 MHz (europäische Frequenzen) bzw. 950 MHz (US-amerikanische und asiatische Frequenzbänder) oder der **SHF** bei 2,45 GHz und 5,8 GHz. Die freigegebenen Frequenzen für LF- und UHF-Tags unterscheiden sich regional für Asien, Europa und Amerika und sind von der **ITU** koordiniert.

HF-Tags verwenden **Lastmodulation**, das heißt, sie verbrauchen durch Kurzschließen einen Teil der Energie des magnetischen Wechselfeldes. Dies kann das Lesegerät, theoretisch aber auch ein weiter entfernter Empfänger, detektieren. Die Antennen eines HF-Tags bilden eine **Induktionsspule** mit mehreren Windungen.

UHF-Tags hingegen arbeiten im **elektromagnetischen Fernfeld** zum Übermitteln der Antwort; das Verfahren nennt man **modulierte Rückstreuung**. Die Antennen sind meist lineare, gefaltete oder spiralförmige Dipole, der Chip sitzt in der Mitte zwischen den linearen oder mehrfach gewinkelten Dipolarmen des RFID-Tags. Es gibt auch UHF-Tags ohne solche Antennen, deren Reichweite ist extrem kurz.

Damit ein Tag sowohl horizontal als auch vertikal gelesen werden kann, verwendet man häufig **zirkuläre Polarisation**. Diese reduziert zwar das **Signal-Rausch-Verhältnis**, dafür ist irrelevant, in welcher Orientierung das Tag auf die Ware geklebt wird. Da Wasser die UHF-Energie sehr stark absorbiert und Metall diese elektromagnetischen Wellen sehr stark reflektiert, beeinflussen diese Materialien die Ausbreitung der Antennenfelder. Weiterhin ‚verstimmen‘ dielektrische Untergrundmaterialien die **Resonanzfrequenz** der Antennen, daher ist es notwendig, UHF-Tags möglichst genau auf die Materialien der gekennzeichneten Objekte abzustimmen oder die Tags mit einer vom Untergrund abschirmenden Metallfolie auszustatten.

Die UHF- oder SHF-Technik sind wesentlich komplexer ausgelegt als die LF- oder HF-Technik. Aufgrund ihrer Schnelligkeit können UHF- und SHF-Tags bei einer Passage erheblich längere Datensätze übertragen.

Ein handelsüblicher passiver UHF-Tag mit NXP-Chip nach **ISO/IEC 18000-6C** benötigt für den Chip etwa 0,35 Mikroampere an Strom. Die Energie dafür liefert das **Strahlungsfeld** des Readers. Da die Intensität quadratisch mit der Entfernung abnimmt, muss der Reader entsprechend stark senden; üblicherweise verwendet man hier zwischen 0,5 und 2 Watt **EIRP**-Sendeleistung. Semiaktive Tags kommen für gleiche Reichweite mit einem Hundertstel dieser Sendeleistung aus.

Für komplexere Anwendungen können auch **Kryptographiemodule** oder externe **Sensoren** wie z. B. **GPS** in den RFID-Transponder integriert sein. Die RFID-Sende-Empfangseinheiten unterscheiden sich in Reichweite, Funktionsumfang der Kontrollfunktionen und im Aussehen. So ist es möglich, sie direkt in Regale oder Personenschleusen (z. B. bei der Zugangssicherung und in Toreinfahrten) zu integrieren.

Die Vielzahl von unterschiedlichen Geräten und Etiketten ist im Rahmen der verschiedenen Normen (ISO/IEC-Standards ISO/IEC 18000-x) vollständig kompatibel. Es werden jedoch laufend neue proprietäre Lösungen vorgestellt, die von diesen Standards abweichen und zum Teil auch nicht gleichzeitig in einer Nachbarschaft verwendet werden können.

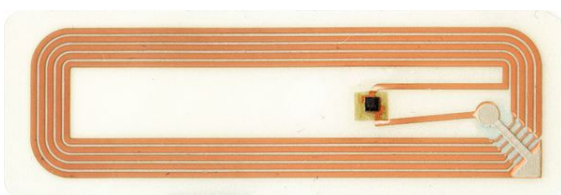
Auf verschiedenste Art kann es zu Problemen kommen, weil der RFID-Transponder direkt am **Erzeugnis** sitzt und dieses elektromagnetisch schlecht mit dem ausgewählten Tag verträglich ist. Um elektromagnetische Anpassungsprobleme zu umgehen, werden in der Logistik u. a. sogenannte Flap- oder Flag-Tags eingesetzt, die im **rechten Winkel** vom Produkt abstehen und so einen großen Abstand zum Produkt haben.

Der Leseerfolg (Lesequote) einer RFID-Lösung kann von einer Vielzahl von Fehlerfällen gemindert werden (Tag defekt, Leser defekt, Tag fehlt, Leser offline, Bewegung in der falschen Richtung, zu schnell oder zu dicht nacheinander usw.).

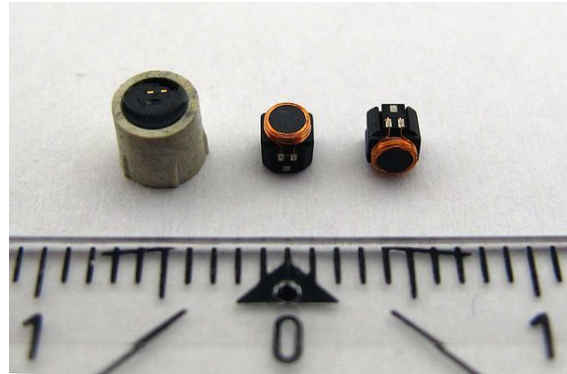
2.2 Baugröße, Bauformen



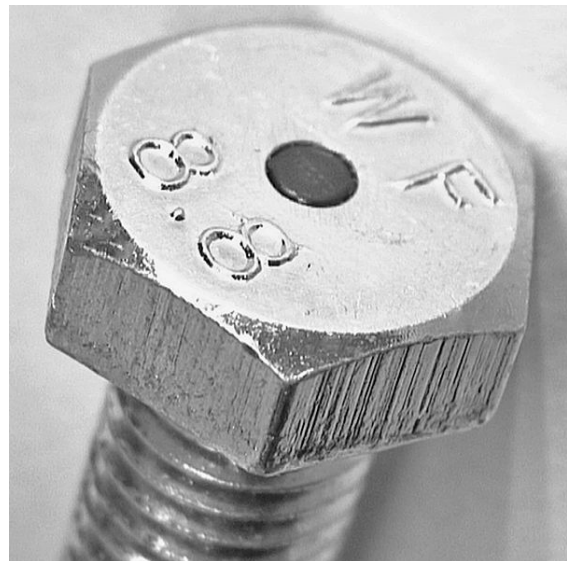
125-kHz-Transponder mit Spule auf Ferritkern



13,56-MHz-Transponder mit gedruckter Spule



13,56-MHz-Transponder nach ISO15693, Miniaturausführung



Nahaufnahme eines Schraubenkopfes mit zentrisch eingepresstem 13,56-MHz-Transponder (NeoTAG)

Transponder bestehen aus:

- Mikrochip, von der Größe um einem Millimeter im Durchmesser.
- Antenne, meist in Form einer Spule. Bei Miniaturtranspondern beträgt der Durchmesser der Antennen in der Regel einige wenige Millimeter, bei Anwendungen mit größeren Reichweiten kann es zu Antennendurchmessern von bis zu einem halben Meter kommen.
- einem Träger oder Gehäuse. Das Gehäuse schützt die Transponderelektronik vor der Umgebung.
- Nur bei aktiven Transpondern: Eine Energiequelle, beispielsweise eine Batterie. Bei passiven Transpondern erfolgt die Energieversorgung über die Antenne von außen.

Maßgeblich für die Baugröße sind die **Antenne** und das Gehäuse; der **Mikrochip** kann hinreichend klein gefer-

tigt werden. Dabei werden, bis auf die Antenne, alle benötigten elektronischen Bauelemente auf den Mikrochip integriert. Die Form und Größe der Antenne ist abhängig von der Frequenz bzw. Wellenlänge und Anwendung. Je nach geforderter Anwendung werden Transponder in unterschiedlichen Bauformen, Größen und **Schutzklassen** angeboten. Die Reichweite von passiven Transpondern ist neben der Frequenz auch maßgeblich von der Antennen- oder Spulengröße (Inlaygröße) abhängig. Die Reichweite sinkt sowohl bei UHF als auch bei HF mit kleineren Antennen rapide ab.

Aktive RFID-Transponder können, je nach Einsatzgebiet, durchaus die Größe von Büchern besitzen (z. B. in der Containerlogistik). Jedoch ist es mit heutiger Technik auch möglich, sehr kleine passive RFID-Transponder herzustellen, die sich in Geldscheinen oder Papier einsetzen lassen.

Transponder wurden ab Beginn des Einsatzes seit 1980 zunächst vorwiegend als "LF 125 kHz passive" produziert und eingesetzt. ISOCARD- und CLAMSHELL-Card-Bauformen aus dem LF-125-kHz-Bereich sind die weltweit am häufigsten verwendeten Bauformen im Bereich Zutrittskontrolle und Zeiterfassung. Genauso existieren auch Bauformen, die im **Autoschlüssel** eingebaut sind (Wegfahrsperrung) bzw. als **Implantate**, **Pansenboli** oder **Ohrmarken** zur Identifikation von Tieren dienen. Zudem gibt es die Möglichkeit zur Integration in Nägel oder PU-Disk-TAGs zur Palettenidentifikation, in Chipcoins (Abrechnungssysteme z. B. in öffentlichen Bädern) oder in **Chipkarten** (Zutrittskontrolle).

Im Bereich elektronischer Fahrscheine, elektronischer Geldbörse oder elektronischer Ausweise findet die 13,56-MHz-Mifare- bzw. -I-Code-Technologie nach Standards wie **ISO 15693** Anwendung. Die Transponderchips werden unter anderem von **NXP Semiconductors** hergestellt. In diesem Bereich gibt es auch spezielle Transponder, die direkt in metallischen Objekten wie z. B. metallische Werkzeugen eingesetzt werden können. Der Aufbau basiert auf einen Wickelkörper für die Antennenspule und Träger für den Transponderchip. Um den Transponder vor äußeren mechanischen Einflüssen und chemischen Medien zu schützen und für eine Einpressung in eine 4 mm-Lochbohrung ausreichend haltbar zu machen, sind entsprechende Gehäuseformen verfügbar. Diese Transponder, die ebenfalls im 13,56-MHz-Band, können allerdings aufgrund der abschirmenden Wirkung der metallischen Umgebung nur im Nahbereich ausgelesen werden. Es ist dabei allgemein notwendig, das Auslesegerät und die Antennenspule in Form eines ca. 4 mm dicken Stiftes direkt auf den Transponder zu halten.^[8]

2.3 Energieversorgung

Das deutlichste Unterscheidungsmerkmal stellt die Art der Energieversorgung der RFID-Transponder dar.

- **Passive RFID-Transponder** versorgen sich aus den Funksignalen des Abfragegerätes. Mit einer Spule als **Empfangsantenne** wird durch Induktion ähnlich wie in einem **Transformator** ein Kondensator aufgeladen, der es ermöglicht, die Antwort in Unterbrechungen des Abfragesignals zu senden. Das erlaubt einen empfindlicheren Empfang des Antwortsignals ungestört von Reflexionen des Abfragesignals von anderen Objekten. Bis allerdings genug Energie für ein Antwortsignal bereitsteht, vergeht eine Latenzzeit. Die geringe Leistung des Antwortsignals beschränkt die mögliche Reichweite. Aufgrund der geringen Kosten pro Transponder sind typische Anwendungen jene, bei denen viele Transponder gebraucht werden, beispielsweise zur Auszeichnung von Produkten oder zum Identifizieren von Dokumenten. Oft geschieht das mit Reichweiten von lediglich wenigen Zentimetern, um die Zahl der antwortenden Transponder klein zu halten.

RFID-Transponder mit eigener Energieversorgung ermöglichen höhere Reichweiten, geringere Latenzen, einen größeren Funktionsumfang, etwa eine Temperaturüberwachung von Kühltransporten, verursachen aber auch erheblich höhere Kosten pro Einheit. Deswegen werden sie dort eingesetzt, wo die zu identifizierenden oder zu verfolgenden Objekte selbst teuer sind, z. B. bei wiederverwendbaren Behältern in der **Containerlogistik** (für See-Container bisher nur vereinzelte Einführung, noch keine weltweit wirksame Übereinkunft) oder bei **Lastkraftwagen** im Zusammenhang mit der Mauterfassung.

Batteriebetriebene Transponder befinden sich meist im Ruhezustand (*sleep modus*) und senden keine Informationen aus, bevor sie durch ein spezielles Aktivierungssignal aktiviert (*getriggert*) werden. Das erhöht die Lebensdauer der Energiequelle auf Monate bis Jahre. Es werden zwei Arten von gesondert mit energieverborgten RFID-Transpondern unterschieden:

- **Aktive RFID-Transponder** nutzen ihre Energiequelle sowohl für die Versorgung des Mikrochips als auch für das Erzeugen des modulierten Rücksignals. Die Reichweite kann – je nach zulässiger Sendeleistung – Kilometer betragen.
- **Semi-aktive RFID-Transponder** oder auch **Semi-passive RFID-Transponder** sind sparsamer, denn sie besitzen keinen eigenen Sender, sondern modulieren lediglich ihren Rückstreuungskoeffizienten, siehe **Modulierte Rückstreuung**. Dafür ist die Reichweite abhängig von Leistung und Antennengewinn des Senders auf maximal 100 m reduziert. Die anderen Vorteile gegenüber passiven Transpondern bleiben erhalten.

2.4 Frequenzbereiche

Für den Einsatz wurden bisher verschiedene **ISM-Frequenzbänder** vorgeschlagen und zum Teil europaweit oder international freigegeben:

- Langwellen (LF, 30–500 kHz). Sie weisen eine geringe bis mittlere Reichweite (≤ 1 Meter) bei geringer Datenrate auf. Erkennungsraten von 35 Transpondern pro Sekunde für bis zu 800 Transpondern im Antennenfeld sind möglich. LF-Transponder sind etwas teurer in der Anschaffung, jedoch sind die Schreib-Lese-Geräte vergleichsweise günstig. Dies verschafft den LF-Systemen Kostenvorteile, sofern relativ wenige Transponder, jedoch viele Schreib-Lese-Geräte benötigt werden. Die LF-Systeme kommen mit hoher (Luft-)Feuchtigkeit und Metall zurecht und werden in vielfältigen Bauformen angeboten. Diese Eigenschaften begünstigen den Einsatz in rauen Industrieumgebungen, sie werden jedoch auch z. B. für Zugangskontrollen, **Wegfahrsperren** und Lagerverwaltung (häufig 125 kHz) verwendet. Einige LF-Versionen eignen sich auch für den Einsatzfall in explosionsgefährdeten Bereichen und sind **ATEX**-zertifiziert.
- Kurzwellen (HF, 3–30 MHz). Kurze bis mittlere Reichweite, mittlere bis hohe Übertragungsgeschwindigkeit. Mittlere bis hohe Preisklasse für Lesegeräte mit Reichweiten größer 10 cm, günstige Lesegeräte für kurze Reichweite. In diesem Frequenzbereich arbeiten die sog. **Smart Tags** (meist 13,56 MHz).
- Sehr hohe Frequenzen (UHF, 433 MHz (**USA, DoD**), 850–950 MHz (**EPC** und andere)). Hohe Reichweite (2–6 Meter für passive Transponder **ISO/IEC 18000-6C**; um 6 Meter und bis 100 m für semiaktive Transponder) und hohe Lesegeschwindigkeit. Einsatz z. B. im Bereich der manuellen, halbautomatischen, automatisierten Warenverteilung mit **Paletten** und **Container**-Identifikation (Türsiegel, License-Plates) und zur Kontrolle von einzelnen Versand- und Handelseinheiten (EPC-Tags) sowie für Kfz-Kennzeichen (bisher nur in Großbritannien). Typische Frequenzen sind 433 MHz, 868 MHz (Europa), 915 MHz (USA), 950 MHz (Japan). Durch ihren geringen Preis werden sie inzwischen auch dauerhaft auf Produkten für den Endverbraucher wie zum Beispiel Kleidung eingesetzt, ihre Reichweite von mehreren Metern verursacht jedoch manchmal falsche Lesungen durch die Leser, zum Beispiel durch Reflexionen.^[9]
- Mikrowellen-Frequenzen (SHF, 2,4–2,5 GHz, 5,8 GHz und darüber). Kurze Reichweite für ausschließlich semi-aktive Transponder von 0,5 m bis 6 m bei höherer Lesegeschwindigkeit wegen hoher Passagegeschwindigkeit für Fahrzeuganwendungen

(PKW in Parkhäusern, Waggonen in Bahnhöfen, LKW in Einfahrten, alle Fahrzeugtypen an Mautstationen).

2.5 Verschlüsselung

Die älteren Typen der RFID-Transponder senden ihre Informationen, wie in der Norm ISO/IEC 18000 vorgesehen, in **Klartext**. Neuere Modelle verfügen zusätzlich über die Möglichkeit, ihre Daten **verschlüsselt** zu übertragen oder Teile des Datenspeichers nicht jedem Zugriff zu öffnen. Bei speziellen RFID-Transpondern, die beispielsweise zur Zugriffskontrolle von externen mobilen Sicherheitsmedien dienen, werden die RFID-Informationen bereits nach **AES**-Standard mit 128-Bit verschlüsselt übertragen.

2.6 Modulations- und Kodierungsverfahren

Keying/Modulation bezeichnet ein Verfahren, um digitale Signale über analoge Übertragungskanäle leiten zu können. Der Begriff Keying kommt aus den Anfangszeiten des Telegraphen. Modulationsverfahren sind unter anderem:

- **Amplitude Shift Keying (ASK)**: verwendet beim *proximity and vicinity coupling*
- **Frequency Shift Keying (FSK, 2 FSK)**: verwendet beim *vicinity coupling*
- **Phase Shift Keying (PSK, 2 PSK)**: verwendet beim *close coupling*
- **Phasenjittermodulation, (PJM)**: statistisches Modulationsverfahren und in ISO/IEC 18000-3 für die Anwendung bei RFIDs genormt.

Höhere Modulationsverfahren wie die Phasenjittermodulation werden bei RFID-Systemen dann eingesetzt, wenn sehr viele RFIDs in räumlicher Nähe nahezu zeitgleich ausgelesen werden sollen.

Die **Leitungscodierung** („encoding“) legt zwischen Sender und Empfänger fest, wie die digitalen Daten so umcodiert werden, um bei der Übertragung möglichst optimal an die Eigenschaften des Übertragungskanals, in diesem Fall der Funkstrecke, angepasst zu sein. Die meistverwendeten Kanalcodierungsverfahren im RFID-Bereich sind:

- **Biphase-Mark-Code** und der dazu invertierte Biphase-Space-Code
- **Pulsphasenmodulationen** in Kombination mit dem **RZ-Code**
- **Manchester-Code**

- **Miller-Code**

Einen Sonderfall stellen **SAW-Tags** dar, die **SAW-Effekte** nutzen. Dabei wird die Kennung in der Laufzeit der reflektierten Signale kodiert.

2.7 Bulk-Erkennung

Unter dem Begriff Bulk-Erkennung versteht man eine Nutzung bekannter Protokolle, in dem einzelne RFID-Tags unmittelbar nacheinander gelesen werden, wobei sich dieser Prozess selbst organisiert. Das heißt, dass

- sich nicht alle Tags gleichzeitig bei dem gleichen Reader melden, und
- jedes Tag möglichst lediglich einmal gelesen wird, und
- ein einmal gelesenes Tag nach dem ersten erfolgreichen Lesen schweigt, bis es das Lesefeld verlässt oder das Lesefeld abgeschaltet wird,
- oder das einzelne dort bereits bekannte Tag vom Leser direkt erneut aktiviert wird.

Viele Anwendungen dieser auch „Singulation“ genannten funktechnischen Vereinzelung soll es dem Empfänger ermöglichen, die verschiedenen Identitäten der vorhandenen Tags streng nacheinander zu erkennen. Das Konzept ist in der Norm in verschiedener Ausprägung vorgesehen, aber bisher erkennbar nicht verbreitet. Weitere proprietäre Ausprägungen finden sich bei den verschiedenen Herstellern. An technischen Problemen mit passiven Tags ändert nichts, dass aktive Tags sich willkürlich bei einem Empfänger melden können.

Folgendes Problem wird allein durch RFID-Tags nicht gelöst: Zu erkennen,

- wie viele Objekte,
- wie viele Tags und
- wie viele gelesene Kennzeichen

einen guten Leseerfolg ausmachen.

Seit ersten Berichten bis heute sind keine Einrichtungen der Bulk-Erkennung bekannt, die eine vollständige Erfassung sicherstellen (2011) und damit für eine Inventarisierung oder eine Kontrolle der Vollständigkeit ungeeignet.

Wenn im Lesevorgang kein Anti-Kollisionsverfahren und keine Stummschaltung wirken, ist die geometrische Vereinzelung außerhalb des Lesebereichs und die Beschränkung auf jeweils ein Tag im Lesebereich die Verfahrensweise mit generell besserer Erkennungsquote.

2.8 Antikollisions- oder Multi-Zugangsverfahren (Anti-collision)

Die Antikollision beschreibt eine Menge von Prozeduren, die den Tags ermöglichen, gleichzeitig zu kommunizieren, also das Überlagern mehrerer verschiedener Signale ausschließen sollen. Das Antikollisionsverfahren regelt die Einhaltung der Reihenfolge bzw. Abstände der Antworten, beispielsweise durch zufällig verteiltes Senden dieser Responses, so dass der Empfänger jedes Tag einzeln auslesen kann. Die Leistung der Antikollisionsverfahren wird in der Einheit „Tags/s“ gemessen. Es gibt vier Grundarten für Antikollisions- oder Multi-Zugangsverfahren:

- **Space Division Multiple Access (SDMA)**: Abstände, Reichweite, Antennenart und Positionierung werden eingestellt
- **Time Division Multiple Access (TDMA)**: die Zugangszeit wird zwischen den Teilnehmern aufgeteilt
- **Frequency Division Multiple Access (FDMA)**: verschiedene Frequenzen werden verwendet
- **Code Division Multiple Access (CDMA)**

Typische Antikollisionsverfahren im RFID-Bereich sind:

- **Slotted ALOHA**: eine Variante des **ALOHA**-Verfahrens aus den 1970er-Jahren (Aloha Networks, Hawaii). Aloha war die Inspiration für das **Ethernet**-Protokoll und ist ein TDMA-Verfahren.
- **Adaptive Binary Tree**: Dieses Verfahren verwendet eine binäre Suche, um einen bestimmten Tag in einer Masse zu finden.
- **Slotted Terminal Adaptive Collection (STAC)**: hat Ähnlichkeiten mit dem ALOHA-Verfahren, ist aber erheblich komplexer.
- **EPC UHF Class I Gen 2**: ist ein Singulationsverfahren.

2.9 Identität (Identity)

Alle RFID-Tags müssen eindeutig gekennzeichnet sein, damit der Empfänger Responses/Requests aller Tags erkennen kann.^[10] RFID-Tags, in denen diese Kennzeichnung geändert werden kann, sind für eine sichere Prozessführung in einem offenen System ohne praktischen Wert (Beispiel: EPC Generation 1).

2.10 Unterscheidungsmerkmale von RFID-Systemen

Mindestmerkmale eines RFID-Systems sind:

- ein Nummernsystem für RFID-Tags und für die zu kennzeichnenden Gegenstände^[11]
- eine Verfahrensbeschreibung für das Kennzeichnen und für das Beschreiben und das Lesen der Kennzeichen^[12]
- ein an Gegenständen oder Lebewesen angebrachtes RFID-Tag, das elektronisch und berührungslos eine seriell auszulesende Information bereitstellt
- ein dazu passendes RFID-Lesegerät

2.10.1 Zusatzfunktionen

Viele Tags unterstützen auch eine oder mehrere der folgenden Operationen:

- Die Tags können über einen sogenannten „kill code“ oder z. B. durch ein **Magnetfeld** permanent deaktiviert werden (engl. *kill, disable*).
- Die Tags erlauben ein einmaliges Schreiben von **Daten** (engl. *write once*).
- Die Tags können mehrmals mit Daten beschrieben werden (engl. *write many*).
- Antikollision: Die Tags wissen, wann sie warten oder Anfragen beantworten müssen.
- Sicherheit: Die Tags können (auch verschlüsselt) ein geheimes **Password** verlangen, bevor sie kommunizieren.

2.10.2 Datenstrom-Betriebsarten

RFID kann im **Duplexbetrieb** oder **sequentiell** Daten mit dem Lesegerät austauschen. Man unterscheidet:

- *full duplex system* (FDX)
- *half duplex system* (HDX)
- *sequential system* (SEQ)

2.10.3 Speicherkapazität

Die Kapazität des beschreibbaren Speichers eines RFID-Chips reicht von wenigen Bit bis zu mehreren **KBytes**. Die 1-Bit-Transponder sind beispielsweise in **Waresicherungsetiketten** und lassen nur die Unterscheidung „da“ oder „nicht da“ zu.

Der Datensatz des **Transponders** wird bei dessen Herstellung fest in ihm als laufende eindeutige Zahl (inhärente Identität) oder bei dessen Applikation als nicht einmalige Daten (z. B. Chargennummer) abgelegt. Moderne Tags können auch später geändert oder mit weiteren Daten beschrieben werden.

2.10.4 Beschreibbarkeit

Beschreibbare Transponder verwenden derzeit meist folgende Speichertechnologien:

- nicht-flüchtige Speicher (Daten bleiben ohne Stromversorgung erhalten, daher geeignet für induktiv versorgte RFID):
 - **EEPROM**
 - **FRAM**
- flüchtige Speicher (benötigen eine ununterbrochene Stromversorgung, um die Daten zu behalten):
 - **SRAM**

2.10.5 Energieversorgung

Passive Transponder entnehmen ihre Betriebsspannung dem (elektromagnetischen) Feld und speichern sie für den Antwortvorgang in Kapazitäten im Chip. Das Lesegerät beleuchtet den Chip und dieser reflektiert einen geringen Teil der Energie. Die eingestrahlte Energie muss etwa 1.000 mal größer sein als die für den Antwortvorgang verfügbare Energie. Damit benötigen passive Transponder das mit Abstand energiereichste Lesefeld.

Semi-passive (auch genannt semi-aktive) Transponder besitzen eine (Stütz-)Batterie für den volatilen (flüchtigen) Speicher und zum Betrieb angeschlossener Sensoren, nicht jedoch für die Datenübertragung. Das Energieverhältnis zwischen Beleuchtung und Rückstrahlung entspricht dem passiver Tags.

Aktive Transponder nutzen Batterien für den Prozessor und auch für den Datentransfer, sind mit einem eigenen Sender ausgestattet und erreichen so eine höhere Reichweite. Das Abfragesignal des Lesegeräts ist etwa so gering wie das Sendesignal des Transponders, somit ist der Lesevorgang für aktive Transponder verglichen mit passiven Transpondern besonders störungsarm.

Baken-Transmitter, die fortlaufend intermittierend senden und nicht auf eine Anregung reagieren, arbeiten immer mit Batterien (Primärbatterien oder Akkus). Das Energieverhältnis zwischen Abfrage und Antwortsignal entspricht dem aktiver Tags. Der Sendevorgang für Baken-Transponder ist ungeachtet der steten Sendefunktion verglichen mit passiven Transpondern besonders störungsarm.

In Deutschland werden aktive Transponder auch als Telemetriegeräte (siehe unten) klassifiziert. Auch Telemetrie-SRD (Funkverbindungen über kurze Entfernungen, z. B. von Sensoren) werden teilweise als RFID bezeichnet, sie benutzen einen aktiven Sender, der beispielsweise mit Solarzellen oder der Bewegung des Gegenstandes (z. B. Reifendrucksensor) mit Energie versorgt wird. Bei warmblütigen Lebewesen ist auch die Versorgung aus einer Temperaturdifferenz in Entwicklung.^[13]

2.10.6 Betriebsfrequenz

2.10.7 Reichweiten und typische Anwendungen



Flag-Tag-Etikett mit integriertem RFID-Chip

Nach dem englischen Sprachgebrauch haben sich folgende Unterscheidungen etabliert:^[14]

- *Close coupling*: 0...1 cm (ISO 10536)
- *Remote coupling* (auch *proximity coupling*): 0...0,1 m (ISO 14443, ISO 18000-3)
- *Remote coupling* (auch *vicinity coupling*): 0...1 m (ISO 15693, ISO 18000-3)
- *Long range coupling*: mehr als 1 m (ISO 18000-4, ISO 18000-5, ISO 18000-7)

Technisch können größere Distanzen erreicht werden, typisch sind jedoch lediglich die angegebenen Reichweiten bei zugelassenen Sendefeldstärken. Dabei ist die Beleuchtungsfeldstärke für passive Tags (Abfrage durch Lesegeräte) etwa um den Faktor 1.000 höher als die Sendefeldstärke aktiver Tags (Empfang durch Lesegeräte).

2.10.8 Frequenzbeeinflussung

- Reflexion / gerichtete bzw. ungerichtete Streuung (*backscatter*): Frequenz der reflektierten Welle ist die Sendefrequenz des Lesegerätes
- Dämpfungsmodulation: durch den Transponder wird das Feld des Lesegerätes beeinflusst (Frequenzverhältnis 1:1)
- subharmonische Welle (Frequenzverhältnis 1:n)

- Erzeugung von Oberwellen (n-fache) im Transponder

2.10.9 Kopplungsmethoden

- elektrostatische Felder in **kapazitiver Kopplung** (für RFID eher die Ausnahme, kein Standard)
- magnetische Felder für **induktive Kopplung** oder **Nahfeldkopplung (NFC)**: Datenübertragung und meist auch Energieversorgung erfolgen über das magnetische Nahfeld der Spulen im Lesegerät und im Tag (üblich sind **Rahmenantennen** oder **Ferritantennen**). Diese Kopplung ist üblich bei Frequenzen von 135 kHz (ISO 18000-2) und 13,56 MHz (ISO 18000-3) sowie für 13,56 MHz NFC (ISO 22536).
- **elektromagnetische Dipolfelder** für **Fernfeldkopplung**: Datenübertragung und oft auch Energieversorgung erfolgen mit Antennen (üblich sind **Dipolantennen** oder **Spiralantennen**). Diese Kopplung ist üblich bei Frequenzen von 433 MHz (ISO 18000-7), bei 868 MHz (ISO 18000-6) und bei 2,45 GHz (ISO 18000-4).

3 Einsatz

Generell ist die **Logistik** die Hauptüberschrift für das Einsatzgebiet. Logistische Problemstellungen gehen quer durch alle Branchen. Hier gibt es ein riesiges **Rationalisierungspotential** auszuschöpfen. Der Durchbruch zu allgemeiner Ausbreitung scheitert in der Regel an Problemen, den Geschäftsfall (business case) über Unternehmensgrenzen hinweg zu budgetieren (s.a. **Zählpunkt (Logistik)**).

Manche Institutionen erhoffen sich darüber hinaus eine verbesserte Überwachung im Personen- und Warenverkehr. Der technische Aufwand und die Kosten auf der RFID-Seite sind überschaubar. Die zu erwartenden riesigen Datenmengen begrenzen die praktische Ausführung.

Der Begriff „fälschungssicher“ in diesem Zusammenhang wird sich nach kurzer Zeit relativieren.

Die folgende Aufzählung enthält nur einige, derzeit (2013) wichtige Gebiete:

3.1 Fahrzeugidentifikation

Die **e-Plate**-Nummernschilder identifizieren sich automatisch an Lesegeräten. Dadurch sind Zugangskontrollen, **Innenstadtmautsysteme** und auch **Section-Control**-Geschwindigkeitsmessungen möglich. Bei entsprechend dichtem Sensorennetz lassen sich auch Wegeprofile erstellen. In einem Großversuch hat das britische Verkehrsministerium im April/Mai 2006 etwa 50.000 Kennzei-



Electronic Road Pricing System in Singapur

chenschilder mit RFID-Funkchips ausstatten lassen. Ziel ist die Informationssammlung über die Fälschungsquote sowie die Gültigkeit von Zulassung und Versicherungsschutz. Bei erfolgreicher Erprobung ist eine flächendeckende Einführung geplant. Die Erfassung erfolgt im Abstand von weniger als zehn Metern. Eine Verwertung der Geschwindigkeitsmessung mit Hilfe dieser Technik ist durch die britische Rechtsprechung derzeit stark eingeschränkt. Mit Stand 2006 sind Waggonen und Lokomotiven in den USA und Kanada an beiden Seiten mit je einem etwa BxHxT 25x5x1 cm großen RFID-Tag markiert, das an etwa 500 Stationen von der Seite während der Fahrt abgelesen wird.^[15]

3.2 Elektronische Bauzustandsdokumentation

Die Automobilindustrie verwendet RFID für die automatisierte Bauzustandsdokumentation von Versuchsfahrzeugen und Prototypenteilen (Projekt Gläserner Prototyp).

3.3 Banknoten

Bereits im Jahr 2003 wurde bekannt, dass die Europäische Zentralbank mit dem japanischen Elektronikkonzern Hitachi über eine Integration von RFID-Transpondern in Euro-Banknoten verhandelte.^[16] Auf dem sogenannten μ -Chip ($0,16 \text{ mm}^2 \times 0,064 \text{ mm}$ dick) ist eine eindeutige 38-stellige Ziffernfolge (128 Bit) gespeichert.^[17] Mit einem solchen RFID-Chip gekennzeichnete Banknoten sollen besser gegen Fälschung geschützt sein. Vorstellbar wäre aber auch eine lückenlose Dokumentation des Umlaufs. Aufgrund der mit der Implementierung verbundenen Kosten sowie datenschutzrechtlicher Probleme ist die Einführung bislang nicht vorgesehen.

3.4 Bezahlkarten

Debit- und Kreditkarten mit Funk-Bezahlsystem^[18] erlauben auch eine Identifizierung. Dem Sicherheitsrisiko, das durch möglicherweise unbemerktes Auslesen und Abbuchen entstehen könnte, wird dabei durch Begrenzung der Zahlungsbeträge auf einen Maximalbetrag oder auf ein gewisses Guthaben begegnet. Beispiele sind hier das Paypass-System von Mastercard.

3.5 Identifizierung von Personen

RFID-Chips sind in allen seit dem 1. November 2005 ausgestellten deutschen Reisepässen sowie ab dem 1. November 2010 in allen Personalausweisen enthalten. Im November 2004 genehmigte die US-amerikanische Gesundheitsbehörde (FDA) den Einsatz des „VeriChip“ am Menschen.^[19] Der Transponder der US-amerikanischen Firma Applied Digital Solutions wird unter der Haut eingepflanzt. Geworben wird mit einfacher Verfügbarkeit lebenswichtiger Informationen im Notfall. Andere Lösungen arbeiten dagegen mit Patientenarmbändern und koppeln diese Daten über den PDA des medizinischen Personals mit dem Patienteninformationssystem im Krankenhaus.^[20]

3.6 Identifizierung von Tieren



Glastransponder zur Tieridentifikation (rechts) mit zugehörigem Applikationsgerät (links)

Seit den 1970er-Jahren kommen RFID-Transponder bei Nutztieren zum Einsatz. Außer der Kennzeichnung von Nutztieren mit Halsbändern, Ohrmarken und Boli werden Implantate bei Haustieren (EU-Heimtierausweis, ISO/IEC 11784 und ISO/IEC 11785) verwendet. Auch die Tiere im Zoo erhalten solche Implantate.

- 125 kHz – international für Zootierhaltung, Nutztieridentifikation, Meeresschildkröten-Erfassung, Forschung.
- ISO 134,2 kHz – (ursprünglich europäischer) internationaler Standard in der Nutztieridentifikation, Implantate bei Haustieren.^[21]

3.7 Echtheitsmerkmal für Medikamente

Die US-Arzneimittelbehörde FDA empfiehlt den Einsatz von RFID-Technik im Kampf gegen gefälschte Medikamente. Bisher werden jedoch überwiegend optische Verfahren eingesetzt, da deren materieller Aufwand wirtschaftlich vertretbar ist. Für den Transport temperaturempfindlicher Medizinprodukte werden vielfach RFID-Tags mit Sensorfunktionen an den Transportbehältern eingesetzt. Die Aufzeichnung dokumentiert eine Verletzung von Transportbedingungen und unterstützt den Schutz der Patienten durch qualifiziertes Verwerfen eines falsch transportierten Gutes.

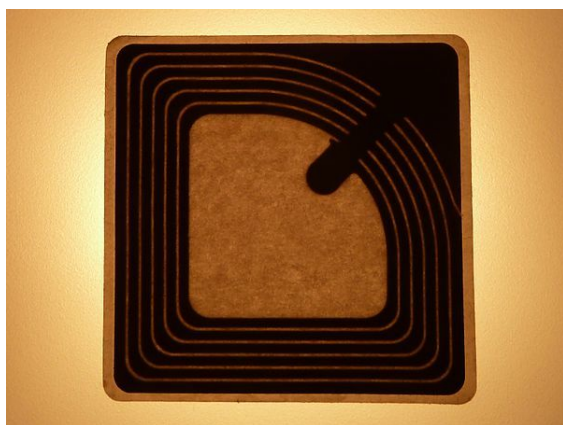
3.8 Schlauchbahnhöfe und Abfüllanlagen

Im industriellen Einsatz zur prozesssicheren Steuerung und elektronischen Überwachung von Um- und Füllvorgängen. Die RFID-Antenne befindet sich in der anlagenseitigen Kupplungshälfte, der RFID-Transponder in der beweglichen Kupplungshälfte, z. B. schlauchseitig an einem Kesselwagen. In gekuppeltem Zustand werden so alle benötigten Informationen kontaktlos übertragen. Die Anlagensteuerung kann dann automatisch nachfolgende Prozessschritte starten.

3.9 Leiterplatten mit RFID-Tags

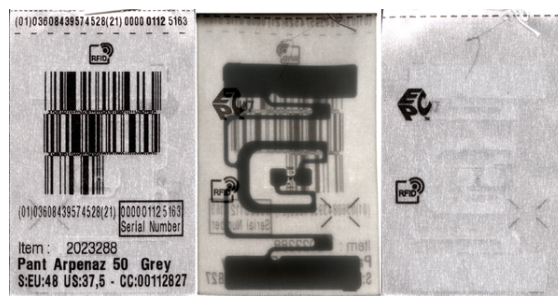
RFID-Tags werden eingesetzt, um Leiterplatten oder andere Bauteile rückverfolgbar zu machen.^[22] Leiterplatten wurden bislang häufig mit Barcodes gekennzeichnet.

3.10 Textilien und Bekleidung



RFID-Etikett eines Kleidungsstücks

In der Textil- und Bekleidungsindustrie ist ein zunehmend flächendeckender Einsatz von RFID aufgrund einer im Vergleich zu anderen Branchen höheren Marge sehr wahrscheinlich. Als weltweit erstes Unternehmen hat Lemmi Fashion (Kindermode) die komplette



Eingenähtes RFID-Etikett in einem Kleidungsstück des französischen Sportausstatters Decathlon. Vorder- und Rückseite sowie Durchlichtscan.

Lieferkette auf RFID umgerüstet und eine weitreichende Integration mit der Warenwirtschaft umgesetzt. Die Firma Levi Strauss & Co. hat ebenfalls begonnen, ihre Jeans mit RFID-Etiketten auszustatten.^[23] Ein weiterer RFID-Pionier ist die Firma Gerry Weber, die sich seit 2004 in diversen Projekten mit der Technologie beschäftigte und seit 2010 in alle Bekleidungsstücke einen RFID-Tag integriert, der gleichzeitig als Warensicherung fungiert.^{[24][25][26]} Seit 2012 wird RFID vom Modeunternehmen C&A verwendet^[27], seit 2013/2014 durch die Adler Modemärkte^{[28][29]}. Die Sportartikel-Kette Decathlon näht seit 2013 RFID-Etiketten in Textilien ihrer Hausmarken ein und bringt diese an Drittprodukten an.^[30]

3.11 Container-Siegel

Für See-Container sind spezielle mechanische Siegel mit zusätzlichen RFID-Tags entworfen worden, die in Einzelfällen bereits benutzt werden. Sie werden entweder wiederholt genutzt (semi-aktive RFID-Tags nach ISO/IEC 17363, ab 2007) oder einmalig eingesetzt (passive RFID-Tags nach ISO/IEC 18185, ab 2007). Bisher gibt es keine Verpflichtung zur Verwendung solcher elektronischen Siegel.

3.12 Automobile Wegfahrsperre

Als Bestandteil des Fahrzeugschlüssels bilden Transponder das Rückgrat der elektronischen Wegfahrsperren. Der Transponder wird dabei im eingesteckten Zustand über eine Zündschloss-Lesespule ausgelesen und stellt mit seinem abgespeicherten Code das ergänzende Schlüsselement des Fahrzeugschlüssels dar. Für diesen Zweck werden üblicherweise Crypto-Transponder eingesetzt, deren Inhalt nicht ohne deren Zerstörung manipuliert werden kann.

Die Diebstahlsicherung erkaufte man sich mit dem hohen Aufwand von in der Praxis 200 € für den Ersatz eines verlorenen Schlüssels, samt Codierung, zu deren Durchführung alle in Zukunft gültigen Schlüssel, das Fahrzeug und das Gerät des Markenhändlers zusammenge-

führt werden müssen.

3.13 Kontaktlose Chipkarten

In Asien sowie größeren Städten weit verbreitet sind berührungslose, wiederaufladbare Fahrkarten. Weltweiter Marktführer für das sogenannte **Ticketing** ist **NXP** (hervorgegangen aus Philips) mit seinem **Mifare**-System. In den USA und in Europa werden Systeme zur **Zutrittskontrolle** und **Zeiterfassung** bereits häufig mit RFID-Technik realisiert. Hier werden weltweit meist Mifare oder HiD bzw. iClass5 und in Europa hauptsächlich **Legic**, Mifare und teilweise unterschiedliche 125-kHz-Verfahren (Hitag, Miro usw.) eingesetzt. Manche **Kreditkarten**-Anbieter setzen RFID-Chips bereits als Nachfolger von Magnetstreifen bzw. Kontakt-Chips ein. 2006 kam die RFID-Technik in Deutschland bei den **Eintrittskarten der Fußball-Weltmeisterschaft** zum Einsatz. Ziel ist es, den Ticketschwarzhandel durch Bindung der Karte an den Käufer zu reduzieren. Bei **Bayer 04 Leverkusen**, **VfL Wolfsburg** und **Alemannia Aachen** kommt diese Technologie bereits bei Bundesliga-Spielen zum Einsatz. Fast alle größeren Skigebiete der Alpen verwenden heutzutage nur noch kontaktlose Skipässe. Der Deutsche Golf Verband e.V. stellt seinen Mitgliedern bereits seit 2007 den optionalen DGV-AusweisPlus mit optionalem Mifare-Chip zur Verfügung. Im Ausweisjahr 2016 wurden über 240.000 DGV-AusweisPlus (Jahresausweise) ausgegeben.

3.14 Waren- und Bestandsmanagement

In Bibliotheken jeder Größe und Typs wird RFID zur Medienverbuchung und Sicherung verwendet. Prominente Installationen sind die **Münchener Stadtbibliothek**, die **Hamburger Öffentlichen Bücherhallen**, die **Wiener Hauptbücherei**, die **Stadtbücherei Stuttgart** und die **Hauptbibliotheken der Technischen Universität Graz** und des **Karlsruher Instituts für Technologie**. 2013 wird auch der **Verbund der Öffentlichen Bibliotheken Berlins** die Umstellung seines Medienmanagements auf RFID abschließen. Auch die **Bibliothek der Universität Konstanz** stattet ihre Medien im Rahmen der Sanierung mit der RFID-Technologie aus.

Die RFID-Lesegeräte sind in der Lage, spezielle RFID-Transponder stapelweise und berührungslos zu lesen. Dieses Leistungsmerkmal bezeichnet man mit **Pulklesung**. Das bedeutet bei der Entleihe und Rückgabe, dass die Bücher, Zeitschriften und audiovisuellen Medien nicht einzeln aufgelegt und gescannt werden müssen. Der Bibliotheksbenutzer kann auf diese Weise an RFID-Selbstverbuchungsterminals alle Medien selbstständig ausleihen. Auch die Medienrückgabe kann automatisiert werden: Eigens entwickelte RFID-Rückgabeautomaten ermöglichen eine Rückgabe außerhalb der Öffnungszeiten. An den Türen und Aufgängen befinden sich Lese-

geräte, die wie Sicherheitsschranken in den Kaufhäusern aussehen. Sie kontrollieren die korrekte Entleihe. Mit speziellen RFID-Lesegeräten wird die Inventarisierung des Bestandes und das Auffinden vermisster Medien spürbar einfacher und schneller.

Große Einzelhandelsketten wie **Metro**, **Rewe**, **Tesco** und **Walmart** sind an der Verwendung von RFID bei der Kontrolle des Warenflusses im Verkaufsraum interessiert. Dieser Einsatz hat in letzter Zeit zu Diskussionen geführt. Der Vereinfachung für den Kunden (z. B. Automatisierung des Bezahlvorganges) stehen Datenschutzbedenken gegenüber.

3.15 Positionsbestimmung

Im industriellen Einsatz in geschlossenen Arealen sind **fahrerlose Transportsysteme** im Einsatz, bei der die Position mit Hilfe von in geringen Abstand zueinander im Boden eingelassenen Transpondern aufgrund von deren bekannter Position über die gelesene Identität und über Interpolation bestimmt wird. Solche Systeme sind davon abhängig, dass ausschließlich zuvor bestimmte Trassen und Routen befahren werden. Für Schienenfahrzeuge kommt die magnetisch gekoppelte **Eurobalise** zum Einsatz.

3.16 Müllentsorgung



RFID-Chip auf Mülltonne

In den österreichischen Bezirken Kufstein und Kitzbühel wurde bereits im Jahr 1993 ein auf RFID basierendes Müllmesssystem nach Volumenmessung in Litern entwickelt und flächendeckend eingeführt; sämtliche Transponder der Erstausgabe (AEGID Trovan ID200 125 kHz) aus dem Jahr 1993 sind dort trotz erneuerter Abfahrzeuge (und Reader-Einheiten) bis heute in der Originalbestückung unverändert im Einsatz. Eine Müllverschreibung erfolgt bei diesem System nach tatsächlich gemessenen Litern (laufende Abrechnung je Quartal). Das System verknüpft über die Adresselemente Straße,

Hausnummer, Türe und Top, automatisiert eine Personenanzahl (Datenabfrage aus dem zentralen Melderegister Österreichs) mit jedem Müllgefäß und summiert unabhängig von einer tatsächlich abgeführten Müllmenge diese virtuell errechnete Mindestmüllmenge auf die Müllgefäßkonten. Zur Vermeidung eines sonst unweigerlichen Missbrauchs einer aufkommensgerechten Abfallvergebühung durch **Littering** vergleicht das System am Jahresende eine tatsächlich abgeführte Jahresmüllmenge je Gefäß mit einer virtuell aus der Personenanzahl errechneten Mindestmüllmenge (je Gemeinde 2–3 Liter je Woche und Person) und schreibt bei einer Unterschreitung der bemessenen Müllmenge eine Differenz am Jahresabschluss jedenfalls vor. Das beschriebene System befindet sich seit mehr als 14 Jahren konfliktfrei und ohne technisch bedingten Datenverlust im Einsatz. Datenschutzrechtlich relevante Abläufe finden ausnahmslos innerhalb der kommunalen Gemeindeverwaltung statt, jeder Bürger kann auf Verlangen in seine Müllmessdaten in seiner Heimatgemeinde Einsicht nehmen.



RFID-Chip in Mülltonne eingebaut

Im deutschen **Landkreis Celle** werden Mülltonnen seit etwa 1993^[31] mit Chips gekennzeichnet. Im Sommer 2013 wurden die alten Chips, die mittlerweile nicht mehr hergestellt werden, durch Chips in Form eines Stiftsockelstifts ersetzt. Alle Restmüll-, Bio- und Papiertonnen werden damit ausgestattet. Der Zweckverband Abfallwirtschaft Celle erfasst die Anzahl der Leerungen im Kalenderjahr und erstellt für Restmüll und Bioabfall Gebührenbescheide unter Berücksichtigung der Leerungsanzahl. Bei Unterschreitung einer Mindestanzahl Leerungen wird der Bescheid über eine leerungsanzahlunabhängige Grundgebühr ausgestellt. Das Gewicht oder Volumen wird nicht registriert, es gilt die Anzahl der Leerungen. Für Papiertonnen wird eine Statistik über die Zahl der gebührenfreien Leerungen geführt. Die **Gelben Ton-**

nen haben keine elektronische Kennzeichnung und werden gebührenfrei geleert.

In den deutschen Städten **Bremen** und **Dresden** sind **Mülltonnen** für die gebührenpflichtige Abfuhr ebenfalls mit RFID-Transpondern versehen. Die gebührenfreie Abfuhr von Papier, Grünabfall und Verpackung wird hingegen nicht erfasst. Bei der Leerung erfassen die **Abfuhrfahrzeuge** mittels geeichter Waagen das **Gewicht** jeder einzelnen Tonne. Über RFID ist die Zuordnung des Abholgewichts jeder Tonne zu einem individuellen Haushalt möglich; die Bürger erhalten in Dresden eine Abrechnung, die auf dem tatsächlich geleerten Gewicht (und nicht, wie sonst üblich, auf einer Volumenpauschale) basiert, bzw. in Bremen über die Anzahl der über die Pauschale hinaus erfolgten tatsächlichen Leerungen (und nicht, wie sonst üblich, allein auf einer pauschalen Anzahl).

In **Großbritannien** wurden mehrere hunderttausend Mülltonnen ohne Wissen der Bürger mit RFID-Transpondern versehen.^[32] Hintergrund soll die Absicht der britischen Kommunen sein, das Recyclingverhalten der Bürger zu erfassen.^[33]

3.17 Zugriffskontrolle

Transponder am oder im Schlüssel dienen zur Kontrolle, wenn **Workstations** mit entsprechenden Lesegeräten ausgestattet sind, ebenso zur Benutzerauthentifizierung für spezielle externe mobile Sicherheitsfestplatten, wenn diese im Gehäuse mit entsprechenden Lesegeräten ausgestattet sind.

3.18 Zutrittskontrolle

Transponder am oder im Schlüssel dienen zur Zutrittskontrolle, wenn die Türen mit entsprechenden Lesegeräten oder mit entsprechenden Schließzylindern mit Leseoption ausgestattet sind.

3.19 Zeiterfassung

Transponder dienen am Schuh(band) oder in der Startnummer eines Läufers bzw. am oder im Rahmen eines Rennrades als digitales Identifikationsmerkmal in Sportwettkämpfen (Produktbeispiele: **ChampionChip**, **Bibchip**, **DigiChip**)

An **Terminals** werden die Zeiten des Kommens und Gehens, evtl. auch der Pausenzeiten erfasst, wenn der Nutzer sein RFID-Medium (meist Chipkarte oder Schlüsselanhänger) in Lesereichweite bringt.



Zeiterfassungsterminal mit RFID

3.20 RFID in Ladehilfsmitteln

Einige Hersteller von Ladehilfsmitteln bieten Lösungen mit integrierten RFID-Transpondern nach ISO/IEC 18000-6C an. Beispiele sind Transportpaletten aus Kunststoff oder Holz sowie Kleinladungsträger.^{[34][35][36]} Die integrierten Transponder können bspw. für das Ladungsträger- bzw. Behältermanagement oder nach der temporären Verheirathung des Hilfsmittels mit dem zu transportierenden Gut als Identifikationsmerkmal der Ladeeinheit im Rahmen des Supply Chain Event Managements eingesetzt werden.^[37]

4 Verbreitung und Kosten

Kumuliert wurden in den Jahren von 1944 bis 2005 insgesamt 2,397 Milliarden RFID-Chips verkauft.^[38] Die genaue Verbreitung nach Anwendung sieht wie folgt aus:

Im Jahr 2005 wurden 565 Millionen Hochfrequenz-RFID-Tags (nach ISO/IEC 14443) abgesetzt, was insbesondere auf die erhöhte Nachfrage im Logistik-Bereich zurückzuführen ist.^[39] Für das Jahr 2006 erwartete man einen weltweiten Absatz von 1,3 Milliarden RFID-Tags.^[40] U. a. wegen der zunehmenden Vereinheitlichung von RFID-Lösungen sowie dem gewachsenen Austausch der Interessenten untereinander mussten Marktforscher ihre Prognose für das Marktwachstum im Jahr 2007 um 15 % senken. So wurde erwartet, dass man im Jahr 2007 mit rund 3,7 Milliarden US-Dollar für RFID-Services

und -Lösungen weniger Umsatz machte.^[41]

In industriellen Anwendungsfällen stellen die Kosten für die Chips und deren zu erwartende Degression nicht den entscheidenden Faktor dar. Viel mehr ins Gewicht fallen Installationskosten für banal Erscheinendes wie Verkabelungen, Steckdosen, Übertrager und Antennen und so weiter, die in konventioneller Handwerksleistung installiert werden und bei denen deswegen kaum eine Kostendegression zu erwarten ist. Bei Wirtschaftlichkeitsvergleichen von RFID zu zum Beispiel Barcode waren und blieben es diese Infrastrukturkosten, die durch die erwartbaren Rationalisierungserträge eines RFID-Systems nicht auszugleichen waren.^{[42][43]}

Die Kosten für die Transponder (also die RFID-Chips) liegen zwischen 35 Euro pro Stück für aktive Transponder in kleinen Stückzahlen und absehbar 5 bis 10 Cent pro Stück für einfache passive Transponder bei Abnahme von mehreren Milliarden.^{[44][45]}

5 Studienmöglichkeiten

Eine Reihe von Hochschulen bietet Kurse zum Fachgebiet *RFID* innerhalb bestehender Ausbildungen an. Seit dem Sommersemester 2009 besteht beispielsweise die Möglichkeit, ein Masterstudium an der Hochschule Magdeburg-Stendal abzuschließen.

6 Normen

- Verband der Automobilindustrie (VDA)
 - VDA 5500: Grundlagen für den RFID-Einsatz in der Automobilindustrie
 - VDA 5501: RFID Einsatz im Behältermanagement
 - VDA 5509: AutoID/RFID-Einsatz und Datentransfer zur Verfolgung von Bauteilen und Komponenten in der Fahrzeugentwicklung
 - VDA 5510: RFID zur Verfolgung von Teilen und Baugruppen
 - VDA 5520: RFID-Einsatz in der Fahrzeugdistribution
- Müllentsorgung
 - Trovan
 - BDE VKI (Abwandlung ISO 11784 / 11785)^[46]
- Tier-Identifizierung
 - ISO 11784
 - ISO 11785: FDX, HDX, SEQ
 - ISO 14223: advanced transponders

- Contactless Smartcards
 - ISO/IEC 10536: close coupling Smartcards (Reichweite bis 1 cm)
 - **ISO/IEC 14443**: proximity coupling Smartcards (Reichweite bis 10 cm)
 - ISO/IEC 15693: vicinity Smartcards (Reichweite bis 1 m)
 - ISO/IEC 10373: Testmethoden für Smartcards
- ISO 69873: für den Werkzeugbereich
- Container-Identifizierung (Logistikbereich)
 - ISO 10374: Container-Identifizierung (Logistikbereich)
 - ISO 10374.2: „Freight Container – Automatic Identification“ das sog. licence plate
 - ISO 17363: „Supply Chain application of RFID – Freight Containers“ das sog. shipment tag
 - ISO 18185: „Freight Container – Electronic Seals“ das sog. eSeal (elektronische Siegel)
- VDI 4470: Diebstahlsicherung für Waren (**EAS**)
- VDI 4472: Anforderungen an Transpondersysteme zum Einsatz in der Supply Chain
 - Blatt 1: Einsatz der Transpondertechnologie (Allgemeiner Teil)
 - Blatt 2: Einsatz der Transpondertechnologie in der textilen Kette (HF-Systeme)
 - Blatt 4: Kosten-Nutzenbewertung von RFID-Systemen in der Logistik
 - Blatt 5: Einsatz der Transpondertechnologie in der Mehrweglogistik
 - Blatt 8: Leitfaden für das Management von RFID-Projekten
 - Blatt 10: Abnahmeverfahren zur Überprüfung der Leistungsfähigkeit von RFID-Systemenbereich
 - Blatt 12: Einsatz der Transpondertechnologie zur Unterstützung der Rückverfolgbarkeit am Beispiel der automobilen Supply-Chain
- Item Management (Verwaltung von Gegenständen)
 - **ISO/IEC 18000** Information technology — Radio frequency identification for item management:
 - Part 1: Reference architecture and definition of parameters to be standardized
 - Part 2: Parameters for air interface communications below 135 kHz

- Part 3: Parameters for air interface communications at 13,56 MHz
- Part 4: Parameters for air interface communications at 2,45 GHz
- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz
- Part 7: Parameters for active air interface communications at 433 MHz

- Datenstrukturen und Reader-Kommunikationsprotokolle

- EPCglobal (**Electronic Product Code**)
- ISO/IEC 15961 AIDC RFID Data Protocol – Application interface
- ISO/IEC 15962 AIDC RFID Data Protocol – Encoding Rules

7 Bedenken und Kritik

Ein RFID-Kennzeichen ist zunächst ein offenes – also für alle mit der nötigen Technik Ausgerüsteten lesbares – individuelles Kennzeichen. Im Zusammenhang mit Bedenken zu RFID-Chips wird daher von „Spychips“ gesprochen.^[47]

7.1 Technische Begrenzungen

Die Beschränkung der RFID-**Technik** ist in der technisch nutzbaren Reichweite und in der ausgewählten festen Information zu erkennen. RFID-Chips liefern keine Information über den genauen Ort (Position), die Orientierung (Richtung) und Bewegung (Geschwindigkeit), sondern die Identität des Kennzeichens ohne weitere Information über den Träger des Kennzeichens.

7.2 Bewegungsprofil

Ortsinformationen erhält man aber immer indirekt über die Kenntnis des Standorts des Lesegerätes. An tragbaren Gegenständen angebrachte und so von Personen mit sich geführte RFIDs sind eine Gefahr für die informationelle Selbstbestimmung, da die ausgelesenen Daten bei Kenntnis des Zusammenhangs personenbeziehbar sind (siehe unten). In dieser Hinsicht gleichen RFID einem eingeschalteten **Mobiltelefon**, dessen Standort ungefähr anhand der nächstgelegenen **Funkzelle** ermittelt werden kann. Aufgrund der vergleichsweise geringen Reichweite von wenigen Metern bei passiven RFID-Chips ist die Standortbestimmung in dem Moment des Auslesens aber wesentlich genauer, sogar noch genauer als bei ziviler Nutzung von **GPS**. Anhand strategisch geschickter Platzierung von mehreren Lesegeräten an diversen Verkehrsknotenpunkten, Engpässen, Türen und dergleichen ließe

sich auch ein zeitlich und räumlich relativ genaues Bewegungsprofil erstellen. Dabei besteht die Gefahr für die informationelle Selbstbestimmung insbesondere aus dem Umstand, dass viele RFID versteckt angebracht sind, der Träger also nicht weiß, dass er sie mitführt, in Kombination mit einem völlig unbemerkten Auslesevorgang.

7.3 Gefahren des Verlustes der informationellen Selbstbestimmung



Logo der StopRFID-Kampagne

Die Gefahr der RFID-Technik liegt zum Beispiel im Verlust der informationellen Selbstbestimmung, d. h. die einzelne Person hat durch die „versteckten“ Sender keinen Einfluss mehr darauf, welche Informationen preisgegeben werden. Deshalb ist der bevorstehende massenhafte Einsatz von RFID-Transpondern unter Datenschutz-Gesichtspunkten problematisch. Um dem zu entgehen, schlagen manche Kritiker die Zerstörung der RFID-Transponder nach dem Kauf vor. Dies könnte (ähnlich wie bei der Deaktivierung der Diebstahlsicherung) an der Kasse geschehen. Ein Nachweis, dass ein Transponder wirklich zerstört bzw. sein Speicher wirklich gelöscht wurde, ist für den Verbraucher in der Regel nicht möglich.^[48] Deshalb wird die Technik häufig auch als Schnüffelchip oder Schnüffel-Chip abwertend bezeichnet.^{[49][50]}

Weiterhin ist die Integration zusätzlicher, nicht dokumentierter Speicherzellen oder Transponder denkbar. Für den Verbraucher wird ein RFID-Transponder so zur Black Box, weshalb manche eine lückenlose Überwachung des gesamten Produktionsprozesses fordern.

2003 hatte der Metro-Konzern einen Teil seiner Kundenkarten mit RFID-Transpondern ausgestattet, ohne seine Kunden darauf hinzuweisen. Der Konzern wurde daraufhin mit der Negativ-Auszeichnung Big Brother Award bedacht. Metro setzt seine RFID-Versuche in seinem Future

Store zwar fort, tauschte die betreffenden Kundenkarten jedoch um. Dies bewerten Datenschutz-Aktivistinnen als Folge ihrer Proteste. Generell kann sich ein Kunde gegen solche Praktiken erfolgreich wehren, wenn sie nicht heimlich geschehen. 2007 erhielt die Deutsche Bahn AG den genannten Big Brother Award, weil sie weiterhin – ohne die Kunden zu informieren – die BahnCard 100 mit RFID-Chips ausstattete.

7.4 Angriffs- bzw. Schutzszenarien

- Man kann versuchen zu verhindern, dass die RFID-Transponder ihre Energie erhalten. Dazu kann man beispielsweise die Batterie herausnehmen oder die RFID-Transponder in einen Faradayschen Käfig stecken. Wenn RFID-Transponder induktiv auf tiefen Frequenzen um 100 kHz ankoppeln, kann eine Abschirmung aus magnetisierbaren Materialien wie Eisen oder Mu-Metall verwendet werden. Bei hohen Frequenzen über 1 MHz genügt Umwickeln mit dünner Alufolie.
- Bei größeren RFID-Transpondern kann man im Röntgenbild die Spiralen der Antenne deutlich erkennen. Wird sie an einer Stelle durchtrennt, funktioniert der RFID-Transponder nicht mehr.
- Die Induktivität einer Spulenantenne ist meist mit einem integrierten Kondensator auf die Arbeitsfrequenz abgestimmt (Schwingkreis). Durch Überkleben mit Alufolie wird die Resonanzfrequenz sehr deutlich erhöht und die Reichweite entsprechend verringert.
- Ein elektromagnetischer Impuls auf Transponder und Antenne zerstört diese ebenfalls und macht sie unbrauchbar. Als Beispiel dafür wurde auf dem Chaos Communication Congress 2005 der RFID-Zapper vorgestellt. Hierbei handelt es sich um ein Gerät, welches RFID-Transponder mittels eines elektromagnetischen Impulses deaktiviert. Auch die hohe Feldstärke eines Mikrowellenherds zerstört die Elektronik, allerdings unter dem Risiko der Beschädigung des Trägermaterials (z. B. einer Kundenkarte).
- Aufwändig: Durch Aussendung eines Störsignals – bevorzugt auf der Frequenz, auf der auch der RFID-Transponder sendet – können die recht schwachen Signale des RFID-Transponders nicht mehr empfangen werden. Dieser Störsender kann aber seinerseits geortet werden.
- Die Übertragung kann auch gestört werden, indem man eine große Zahl (mehrere hundert bis tausend) RFID-Transponder auf einen gemeinsamen Träger (Gehäuse) setzt. Wird das dadurch entstehende Gerät („Jamming-Device“) in den Lesebereich eines

Lesegeräts gebracht, antworten die Tags alle gleichzeitig. Selbst wenn das Lesegerät mit Antikollisionsverfahren arbeitet, ist es bei einer derart großen Zahl von Transpondern doch überfordert und auch nicht mehr in der Lage, „echte“ RFID-Tags (z. B. an Waren) zu erkennen. Solche Jamming-Vorrichtungen können als MP3-Player, Mobiltelefone usw. getarnt sein.

- Kaum effektiv: Wie beim Telefon (per Draht oder drahtlos) kann man auch RFID-Signale ausspähen. Auf diese Weise kann man bestenfalls mitlesen, was der RFID gerade zurücksendet.
- Extrem aufwändig: RFID-Signale können manipuliert werden. Bei einem Speicherchip zur Authentifizierung werden daher auch Verschlüsselungsmethoden eingesetzt.
- Auf der IEEE Conference of Pervasive computing 2006 (*Percom*) in Pisa stellten Wissenschaftler um Andrew S. Tanenbaum eine Methode vor, wie mit Hilfe von manipulierten RFID-Chips die Back-end-Datenbanken von RFID-Systemen kompromittiert werden können. Sie bezeichnen ihre Arbeit selbst als weltweit ersten RFID-Virus seiner Art.^[51] Diese Darstellung wird allerdings mittlerweile von verschiedenen Stellen als zu theoretisch konstruiert angesehen.^[52]

7.5 Umwelt und Recycling

Auf Umverpackungen aufgebrachte RFID-Tags können nach derzeitigem Kenntnisstand nicht so gut recycelt werden wie Umverpackungen ohne RFID-Tags. Sortenreines Verpackungsmaterial wie Altglas, Altpapier oder Kunststoff kann durch die schwierig abzutrennenden RFID-Chips aus Kupfer und weiteren Metallen verunreinigt werden. Mögliche Risiken von Verunreinigungen des Recyclingmaterials durch RFID-Chips können aufwändigeres Recycling oder mindere Qualität der entstehenden Rohstoffe bedeuten.^{[53][54]}

Derzeit gibt es keine Regeln zur Entsorgung der Transponder als Elektronikschrott beim Masseneinsatz wie beispielsweise bei Supermarktartikeln. Unter anderem wird an neuen Materialien (z. B. auf Polymerbasis) geforscht, was zur weiteren Senkung der Herstellungskosten sowie der Erschließung neuer Einsatzgebiete (z. B. in Ausweisen und Kleidung eingearbeitete Transponder)^[55] dienen soll.

Ein weiterer Punkt ist der Ressourcenverbrauch von RFID-Transpondern. Kostbare Edelmetalle gehen mit ihnen diffus auf Deponien und in Müllverbrennungsanlagen verloren. Obwohl ein einziger Transponder nur eine geringe Menge Edelmetall enthält, würde durch eine große Anzahl von Chips (z. B. in Lebensmittelverpackungen) der Ressourcenverbrauch erheblich steigen.

7.6 Störung der Medizintechnik durch RFID

Im *Journal of the American Medical Association* wurde im Juni 2008 eine Studie^[56] veröffentlicht, die nachweist, dass zahlreiche diagnostische Messungen durch die zur Auslesung erforderlichen elektromagnetischen Wellen von RFID verfälscht werden.^[57] Geräte der Medizintechnik, die in jeder gut ausgestatteten Intensivmedizin-Station vorhanden sind, reagierten unterschiedlich empfindlich mit Messwert-Verzerrungen. „In einer Entfernung von einem Zentimeter bis sechs Metern kam es bei 34 von 123 Tests zu einer Fehlfunktion der medizinischen Geräte. In 22 Fällen wurden diese Störungen als gefährlich beurteilt, weil Beatmungsgeräte ausfielen oder selbsttätig die Atemfrequenz veränderten, weil Infusionspumpen stoppten oder externe Schrittmacher den Dienst versagten, weil ein Dialysegerät ausfiel oder der EKG-Monitor eine nicht vorhandene Rhythmusstörung anzeigte.“^[58]

8 Siehe auch

- Auto-ID
- Chipkarte
- Data-Mining
- Organische Elektronik
- Near Field Communication
- Ubiquitous computing
- Internet der Dinge
- Sekundärradar

9 Literatur

9.1 Übersicht

- Himanshu Bhatt, Bill Glover: *RFID Essentials*. O'Reilly & Associates, Sebastopol, CA 2005, ISBN 0-596-00944-5.
- Klaus Finkenzeller, Michael Gebhart: *RFID-Handbuch. Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC* 6. Auflage, Hanser, München 2012, ISBN 978-3-446-42992-5.
- Patrick Sweeney: *RFID für Dummies* (Originaltitel: *RFID for Dummies*, übersetzt von Werner Niemeyer-Stein. Fachkorrektur von Heinrich Oehlmann und Michael Wernle). Wiley-VCH, Weinheim 2006, ISBN 3-527-70263-6 (mit Radio frequency

identification - RFID Produktions- und Distributionsketten verfolgen und führen; mit smarten Etiketten Informationen in Echtzeit, die Vorteile der RFID-Technik nutzen; die Physik und die Organisationen dahinter verstehen; mit RFID alle Prozesse sicher führen).



- Gerrit Tamm, Christoph Tribowski: *RFID*. Springer, Berlin / Heidelberg 2010, ISBN 978-3-642-11459-5.

9.2 Monographien

- N. Bartneck, V. Klaas, H. Schönherr: *Prozesse optimieren mit RFID und Auto-ID*. ISBN 978-3-89578-319-7.
- Thorsten Blecker, George Q. Huang (Hrsg.): *RFID in Operations and Supply Chain Management*. Erich Schmidt Verlag, Berlin 2008, ISBN 978-3-503-10088-0.
- D. Dreher: *Der Einsatz von Radio Frequency Identification in der Logistik*. ISBN 3-638-65794-9.
- F. Gillert, W. Hansen: *RFID – für die Optimierung von Geschäftsprozessen*. ISBN 3-446-40507-0.
- Markus Hansen, Sebastian Meissner: *Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFID Tags*. (PDF; 56 kB) IFIP Summer School, Karlstad 2007. Folien (PDF; 294 kB)
- W. Franke, W. Dangelmaier: *RFID – Leitfaden für die Logistik*. ISBN 3-8349-0303-5.
- C. Kern: *Anwendung von RFID-Systemen*. 2. Auflage. 2006, ISBN 3-540-27725-0.
- C. Köster: *Radio Frequency Identification. Einführung, Trends, gesellschaftliche Implikationen*. ISBN 3-8364-0162-2.
- S. Kummer, M. Einbock, C. Westerheide: *RFID in der Logistik. Handbuch für die Praxis*. ISBN 3-901983-59-7.
- B. Lietke, M. Boslau, S. Kraus: *RFID-Technologie in der Wertschöpfungskette*. In: *Wirtschaftswissenschaftliches Studium (WiSt) – Zeitschrift für Ausbildung und Hochschulkontakt*. (ISSN 0340-1650), Verlage C.H. Beck/Vahlen, 35. Jg., Nr. 12, S. 690–692
- Christoph Rosol: *RFID. Vom Ursprung einer (all)gegenwärtigen Kulturtechnologie*. ISBN 978-3-86599-041-9.
- R. Schoblick: *RFID*. ISBN 3-7723-5920-5.

- E. Schuster, S. Allen, D. Brock: *Global RFID. The Value of the EPCglobal Network for Supply Chain Management*. ISBN 3-540-35654-1.
- W. Seifert, J. Decker (Hrsg.): *RFID in der Logistik*. ISBN 3-87154-322-5.
- Klaus Finkenzeller: *RFID-Handbuch: Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC*. 5. Auflage. München 2008, ISBN 978-3-446-41200-2.

10 Weblinks

 **Commons: RFID** – Sammlung von Bildern, Videos und Audiodateien
 **Wikibooks: RFID-Technologie** – Lern- und Lehrmaterialien

- Film über RFID – Auf Nummer sicher (avi 463 MB)
- Auto-ID Labs Forschungsverbund
- StopRFID-Kampagne von Digitalcourage e. V.
- Die Spychip-Seiten der US-amerikanischen Verbraucherorganisation C.A.S.P.I.A.N.
- Animation: So funktioniert RFID in der Logistik
- Studie: Risiken und Chancen des Einsatzes von RFID-Systemen – Bundesamt für Sicherheit in der Informationstechnik
- Grundlegende Sicherheit von RFID
- Angriffsmethoden auf RFID-Systeme

11 Einzelnachweise

- [1] *RFID-Chips aus dem Drucker*. zdn.net.de, 9. Februar 2005.
- [2] Harvey Lehpamer: *RFID Design Principles*, Second Edition. 2nd ed. Artech House, Boston 2012, ISBN 978-1-60807-470-9, S. 363.
- [3] Christoph Rosol: *RFID. Vom Ursprung einer (all)gegenwärtigen Kulturtechnologie*.
- [4] Bundestag: *Funkchips – Die Radio Frequency Identification (RFID)*. 24. Mai 2007
- [5] AIM Global: *Shrouds of Time – The History of RFID* oder *Shrouds of Time – The History of RFID* (Memento vom 8. Juli 2009 im Internet Archive)
- [6] Auto-ID Center (Memento vom 14. April 2004 im Internet Archive)

- [7] <https://www.fraunhofer.de/de/presse/presseinformationen/2011/februar/chirurgische-instrumente-mit-elektronischer-seriennummer.html>
- [8] *Miniaturisierte HF-Transponder in metallischer und rauer Umgebung*. Abgerufen am 28. November 2014.
- [9] *Funketiketten steuern die Fertigung – RFID-Systeme nach dem EPCglobal-Standard erobern die Produktion*. Siemens A&D Compendium 2009/2010, abgerufen am 20. Oktober 2010
- [10] *ISO/IEC 18000-1:2008 Information technology – Radio frequency identification for item management – Part 1: Reference architecture and definition of parameters to be standardized*
- [11] *ISO/IEC 15459-3:2006 Information technology – Unique identifiers – Part 3: Common rules for unique identifiers*
- [12] *ISO/IEC 15459-4:2008 Information technology – Unique identifiers – Part 4: Individual items*
- [13] „Forschung aktuell“, Deutschlandfunk
- [14] z. B. Finkenzyler 2008, S. 273.
- [15] World Geographic Channel: *The Largest Rail Yards In The World - Freight Trains History* youtube.com, Video 42:49 min, A&E Television Networks, 2006, 9. Juni 2016, abgerufen 6. Februar 2017. (Englisch) – (38:48–40:04) *RFID Intermodal and Rail Tag* an den Seiten von Waggon und Loks in Nordamerika, Bahngesellschaft BNSF, USA.
- [16] tecCHANNEL.de: *RFID-Chip soll Euro-Blüten verhindern*, 23. Mai 2003
- [17] Hitachi: *μ-Chip – The World's Smallest RFID IC*. Stand: August 2006
- [18] Süddeutsche: *Funk Bezahlssystem*, 19. Juni 2011
- [19] heise online: *Patientenidentifikation mit RFID-Chips*. 27. August 2006
- [20] *RFID-Einsatz im Gesundheitswesen* (PDF, 634 KB)
- [21] *ISO 134,2 und der proprietäre historische 125-kHz-RFID-Standard (Memento vom 14. Oktober 2007 im Internet Archive)* (englisch)
- [22] RFID Journal: <http://www.rfidjournal.com/article/articleview/2032/1/1/>
- [23] heise online: *Erste RFID-Markierungen auf Levi's Jeans*. 28. April 2006
- [24] Vgl. C. Goebel, R. Tröger, C. Tribowski, O. Günther, R. Nickerl: *RFID in the Supply Chain: How to obtain a positive ROI. The case of Gerry Weber*. In: *Proceedings of the International Conference on Enterprise Information Systems (ICEIS)*. Mailand 2009
- [25] Vgl. J. Müller, R. Tröger, R. Alt, A. Zeier: *Gain in Transparency vs. Investment in the EPC Network – Analysis and Results of a Discrete Event Simulation Based on a Case Study in the Fashion Industry*. In: *Proceedings of the 7th International Joint Conference on Service Oriented Computing, SOC-LOG Workshop*, Stockholm 2009
- [26] Vgl. RFID Journal: *Gerry Weber sews in RFID's Benefits*. 2009
- [27] *C&A startet RFID-Projekt an fünf Standorten*. Pressemitteilung C&A vom 1. Juni 2012 (pdf), abgerufen am 27. Januar 2014
- [28] *Adler hebt mit RFID ab* Meldung von TextilWirtschaft vom 12. Dezember 2013, abgerufen am 23. April 2014
- [29] *Adler platziert RFID-Hardware in Modemärkten*. Meldung des EHI Retail Institute e.V. vom 26. März 2014, abgerufen am 23. April 2014
- [30] *Decathlon Sees Sales Rise and Shrinkage Drop, Aided by RFID*. RFID Journal, 7. Dezember 2015, abgerufen am 21. April 2016
- [31] <http://www.zacelle.de/privatkunden/chiptausch/faqs-chiptausch>
- [32] *Briten empört: 500.000 Mülltonnen heimlich verwandt*. Spiegel Online, 26. August 2006
- [33] *Germans plant bugs in our wheelee bins*. Mail on Sunday, 26. August 2006
- [34] Vgl. RFID im Blick: *Der Palette auf der Spur mittels RFID* 2009
- [35] Vgl. RFID im Blick: *RFID-Angebot gering – Nachfrage steigend?* (PDF; 465 kB) 2011
- [36] Vgl. MM Logistik: *Erste RFID-Tauschpalette aus Holz* 2012
- [37] Vgl. VDA 5501: *RFID im Behältermanagement der Supply Chain* 2008
- [38] *RFID tag sales in 2005 – how many and where*. IDTechEx, 21. Dezember 2005
- [39] *SCM – Es funkt im RFID-Markt*. CIO Online, 25. September 2006
- [40] *Der RFID-Boom hat gerade erst begonnen*. Computerwoche, 24. Juli 2006
- [41] *Marktforscher sieht 2007 weniger RFID-Wachstum*. sili-con.de, 11. August 2006
- [42] Mira Schnell: *Einsatzmöglichkeiten der RFID-Technologie innerhalb der Materiallogistik am Beispiel der Fahrzeugfertigung der Ford-Werke GmbH in Köln*. FH Aachen, Aachen 2006.
- [43] Michael Tegelkamp: *Möglichkeiten des RFID-Einsatzes im internen Warenfluss eines mittelständischen Süßwarenherstellers*. FH Aachen, Aachen 2005.
- [44] *Kosten laut RFID-Basis.de*
- [45] *Kosten laut RFID-Journal.de*
- [46] BDE-Transponder
- [47] Katherine Albrecht und Liz McIntyre: *SPYCHIPS – How Major Corporations and Government Plan to Track Your Every Move with RFID*. Veröffentlicht von Nelson Current, A Subsidiary of Thomas Nelson, Inc., 501 Nelson Place, Nashville, TN, USA, 2005

- [48] Kritik aus Sicht der Verbraucher: *Die StopRFID-Seiten des FoeBuD e. V.*
- [49] Christian Sprenger, Frank Wecker: *RFID - Leitfaden für die Logistik*, S. 6, Gabler Verlag, 2006, ISBN 978-3-8349-0303-7
- [50] Helmut Martin-Jung: *Warum Funketiketten eine Gefahr für Verbraucher sind* Süddeutsche Zeitung, 18. Januar 2012
- [51] *Is Your Cat Infected with a Computer Virus?* (PDF; 199 kB), Website des RFID-Virus
- [52] *Roaming charges: Pet-embedded RFID chips bring down Las Vegas!* (Memento vom 2. Mai 2006 im Internet Archive), Larry Loeb, 18. April 2006
- [53] *Problem-Müll Funkchip*, wissenschaft.de, 5. Februar 2008
- [54] *Studie: Massenhafter RFID-Einsatz könnte Recycling verschlechtern*, heise.de, 9. November 2007
- [55] *Übersehene Gefahr: RFID-Chips verseuchen das Trinkwasser*. ZDNet.de, 5. Dezember 2005
- [56] Zusammenfassung der JAMA-Studie
- [57] *JAMA* Band 299, 2008. S. 2884–2890.
- [58] *Studie: RFID-Etikette können medizinische Geräte empfindlich stören*. Deutsches Ärzteblatt, 25. Juni 2008

Normdaten (Sachbegriff): GND: 4509863-3

12 Text- und Bildquellen, Autoren und Lizenzen

12.1 Text

- **RFID Quelle:** <https://de.wikipedia.org/wiki/RFID?oldid=167640398> **Autoren:** Walter Koch, RobertLechner, Nerd, Kku, Gnu1742, Aka, Stefan Kühn, Hafenbar, Ilja Lorek, Head, Fab, StephanKetz, Mathias Schindler, Markobr, Fusslkopp, Katharina, Okrumnow, Maurice-KA, Herrick, Ce2, Casandro, HenrikHolke, Karl Gruber, EricPoehlsen, Akl, Tzeh, GDK, Zwobot, D, Kdwnv, HaeB, ArtMechanic, Stern, Ernesto, FelixKaiser, S.ludwig, Bernhard55, Bmr, Anton, Gunnar Eberlein, *g, NetReaper, Mwka, Zinnmann, Asdert, MartinWoelker, Ed.dunkel, Sinn, Peter200, Svebert, Zaubermann, Grimsel, Harry20, Priwo, Mvb, André Schneider, Das Ohr, Sol1, PhHertzog, Plp, Mnh, Ot, Aloiswuest, P. Birken, Ahellwig, Supaari, Pischdi, Aineias, Bdk, Kubrick, Timekeeper, Philipendula, Frubi, Unscheinbar, PeeCee, Kingruedi, Idler, J. 'mach' wust, Sina Eetezadi, Ri st, LimboDancer, Chrisfrenzel, Niemeyerstein, Esher, Conny, ChristophDemmer, Thors-tenS, Darian, Leshonai, Stefan h, DasBee, King, Saint Etienne, Historiograf, Panama01, Mjk-dewiki, Forevermore, RiFID, Captaingrog, Pylon, BWBot, Spauli, Polarlys, Botteler, Simon04, Mps, Garak76, Nicor, Polluks, Kmb, WikipediaMaster, ElRaki, Biedimpfl, M.L., Rosenzweig, Sippel2707, Diba, Padeluun, Horgner, Jpkoester1, C.Löser, SchorSch, Jergen, Emgo, Ejfis, FlaBot, Ulfbastel, Code, Modusvivendi, Musik-chris, Bepeppered, Zum, Hubertl, Avobert, Mareikus, Capriccio, AngMo, Tonk, Bigbang, Kalinka-dewiki, AF666, Arbeo, Luiscantero, Manorainjan, TdL, Tuxo, Badenserbub, Kolja21, GS, Itti, Micha99, Zerberus, Zaphiro, FriedhelmW, GünniX, Millbart, Ju-Ta, Prometeus, Wernfried, BjKa, BLUcoder, Cerno, KaiMartin, PSS, Robote, MB-one, Werner von Basil, Uwe W., Mkaiser30, Ra'ike, Saehrimnir, Chobot, STBR, Ephraim33, Hydro, Spaetabends, Mehrleisealslaut, RobotQuistnix, Elvaube, Tsca.bot, Euku, YurikBot, Nuuk, UdoWDoege, Masegand, WikiMax, Lütke, Bahnemann, Chaddy, Shelmtom-dewiki, DerHexer, Botulph, Tomcat0815, WikiBasti, Staro1, TheReincarnator, Eskimbot, Wikipit, Liberaler Humanist, Lipsianer, Kaisersoft, Na204, Dontworry, Justus Nussbaum, Nightflyer, No-CultureIcons, Okfm, Phantom, Tomreplay, PortalBot, LKD, Knbinnerer, MoLa, Maprie, Shadak, Guenson, Pblanc, Stowasser, Kunobert, Saemon-dewiki, Hundehalter, Guizza, Gripweed, Colognese, Coaster J, Kungfuman, Authentic, Dschanz, Kölscher Pitter, Miwu, 08-15, Biberl, IgorPodolskiy, Sargoth, Charly Whisky, Toolmaker, Ninjagame, Kai Burghardt, Slobot, BJ Axel, .:bÄr, Wdwd, Franz Halac, Pendulin, SeL, ZDragon, Ruppert, Doudo, Kgfleischmann, HAH, Gerrit Tamm, Tönjes, Karsten11, Cleverboy, Graphikus, Graukappe, Kunigunda, BesondereUmstaende, Thomas Schultz, Rufus46, Till.niermann, Spuk968, Thijs!bot, Dr.cueppers, Mbssch, Summ, S.Didam, Büchsenöff-ner, YMS, FBE2005, Rainald62, PsY.cHo, Belabls, Dugong, Cholo Aleman, Arno Matthias, Jakob Schulze, Horst Gräbner, Gohnarch, Patrickdu, Hedwig in Washington, Reijnders, JAnDbot, Kalinko-dewiki, Herbertweidner, Matthiasb, Staycoolandbegood, AviationEx-pert, Wehe00, YourEyesOnly, Kickof, Kraete, Clasen, ComillaBot, Satmap, Tom md, Rissa, Zardo28, Goldmember1603, Nolispanmo, Bildungsbürger, ZweiBein, Kuebi, Numbo3, Primus von Quack, MADE, Ijbond, Giftmischer, FunkelFeuer, Brork, Don Magnifico, Bern-hard Wallisch, Euphoriceyes, BravoOne, Wosch21149, SashatoBot, GerritR, Ncornelius, Complex, VolkovBot, Fjunky, Mideal, Repat, Maschinenjunge, Tristram, Wesener, TXiKiBoT, Hans Eo, Membeth, Jorabo, DanielHerzberg, Chipmeup, Regi51, Ole62, Hannes Röst, Polarbear24, Noogle, Realfoasis, Färber, Krawi, Netpilots, SieBot, Crazy1880, Backwoods, DaBot, Yoky, Fipptehler, Der.Traeumer, Tasma3197, Aleks-ger, T5b6 de, Trustable, Oms, Umherirrender, Rdennis, Dachbewohner, Wikiner-dewiki, Alpha dino, Shimba, Usaro-ber, Alnilam, Sven.petersen, Pittimann, Xyox, Zulu55, Rasieel, Se4598, Giftpflanze, Woches, UlrichAAB, Steak, Kein Einstein, Vernetzung, Inkowik, BunnyUsagi, Xeph, DumZiBoT, Leuchtschnabelbeutelschabe, Donkelmann, SchroedingersKatze, LogoX, Grumm1, Anka Friedrich, Rnawrocki, JoePP, TobbiM, LinkFA-Bot, Schotterebene, MagnusA.Bot, Goiken, LaaknorBot, Tanhabot, MikeCGN-1, Biezl, Hoo man, Drahtloser, Mrlabs, Rosa Schlagfertig, PM3, Schwarzschilding, Hammertom, 6BL-A504, Sarang, KamikazeBot, Reinraum, Gregorgross1055, Bwbuz, Null Drei Null, GrouchoBot, Krd, Anton Sevarius, Rubinbot, Bananenfalter, Powerpille, ChenzwBot, Pfreppi, Obersachsebot, Xqbot, Serol1971-dewiki, Henrik A., Bye Bei, Itu, Pentachlorphenol, Alblefter, Oehhar, GhalyBot, Quartl, Rr2000, Quiemiec, Gonzosft, Nanahara, Ralf König, S3r0, Jivee Blau, MorbZ-Bot, Serols, Susanne und Stefanie, LepoRello, Ahti333, Bpatgibliothek, WTW11980, TobeBot, Coffeesandy, Mabschaaf, Krassotkin, Jo.Fruechtnicht, Md-rfid, Helium4, Dynamik-bot, Bootz, Laserjones, DO6PAT, Wassertraeger, EmausBot, XchrissyX, Mag-elektronik, U11-82-2, Hubert.voney, Smarty9002, Didym, MaddZ, Ne discere ces-sa!, Centovalli, Gelli63, RöntgenTechniker, WikitanvirBot, Randolph33, Conscius, Ptolusque, Stündle, ReneDens, Trigonometrie, CocuBot, Krdbot, Diega92, Temporarity, SchalkG, Leezu, Mlasaj, FrauAva89, Dateientlinkerbot, Staubteufel, Frequent, Ajv39, Rfid123, Dexbot, Steinsplitter, Exoport, H174de, Rmcharb, Asturius, Meisterschiff, UweFried, Wilmjacob, Studi321, Holmium, Derbai, Addbot, Janoschkr, XXnickiXx, Akliesing, Natsu Dragoneel, Srleppal, Blutdurst, Digitoolsoftware, Luke081515Bot, TannoT., FNDE, Lukas House, Hgzh, Gridditsch, Rfid.automobile, Wolf2556, Siwibegewp, Bartolo Bernoulli, Zahnputzbecher, Kasuru21 und Anonyme: 660

12.2 Bilder

- **Datei:134_2khz_rfid_animal_tag.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/a/a9/134_2khz_rfid_animal_tag.jpg *Lizenz:* Public domain *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Reinraum
- **Datei:Commons-logo.svg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/4/4a/Commons-logo.svg> *Lizenz:* Public domain *Autoren:* This version created by Pumbaa, using a proper partial circle and SVG geometry features. (Former versions used to be slightly warped.) *Ursprünglicher Schöpfer:* SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.
- **Datei:ERPBugis.JPG** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/7/7a/ERPBugis.JPG> *Lizenz:* CC BY-SA 3.0 *Autoren:* Self-taken (Unmodified) *Ursprünglicher Schöpfer:* mailer_diablo
- **Datei:FlagTag.jpg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/b/b9/FlagTag.jpg> *Lizenz:* Public domain *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Usarobert
- **Datei:HLG_H5.png** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/a/ac/HLG_H5.png *Lizenz:* Public domain *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* --Satmap 17:31, 11 January 2008 (UTC)
- **Datei:LogiScan.jpg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/2/2c/LogiScan.jpg> *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Bartolo Bernoulli
- **Datei:Medea_UHF_RFID_Reader_from_Nordic_ID.png** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/5/57/Medea_UHF_RFID_Reader_from_Nordic_ID.png *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Srleppal
- **Datei:QSicon_rot_Uhr.svg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/2/20/QSicon_rot_Uhr.svg *Lizenz:* Public domain *Autoren:* abgeleitet von File:QS icon orange abwartend.svg *Ursprünglicher Schöpfer:* AleXXw, Zesal

- **Datei:RFID-Chip_an_Cellex-Abfallbehälter_2013_09.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/8/88/RFID-Chip_an_Cellex-Abfallbehälter_2013_09.jpg *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Hundehalter
- **Datei:RFID-Chip_an_Cellex-Abfallbehälter_2013_14.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/9/9c/RFID-Chip_an_Cellex-Abfallbehälter_2013_14.jpg *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Hundehalter
- **Datei:RFID_125_KHz_Glass_Tag.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/3/36/RFID_125_kHz_Glass_Tag_1.jpg *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Flollie
- **Datei:RFID_Bluetooth_Reader_for_NeoTAG_-_KTS.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/1/19/RFID_Bluetooth_Reader_for_NeoTAG_-_KTS.jpg *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Sraleppal
- **Datei:RFID_Tags.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/e/e3/RFID_Tags.jpg *Lizenz:* CC BY 2.5 *Autoren:* Selbst fotografiert *Ursprünglicher Schöpfer:* Grika in der Wikipedia auf Englisch
- **Datei:RFID_Tags_ISO15693.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/e/ed/RFID_Tags_ISO15693.jpg *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* wdw
- **Datei:RFID_tag_of_a_garment.JPG** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/9/9e/RFID_tag_of_a_garment.JPG *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Conscius
- **Datei:RFID_tag_textile_front-through-back.png** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/5/57/RFID_tag_textile_front-through-back.png *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Polarbear24
- **Datei:Schraube_mit_NeoTAG_plug_13,56MHz_RFID_transponder.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/5/53/Schraube_mit_NeoTAG_plug_13%2C56MHz_RFID_transponder.jpg *Lizenz:* CC BY-SA 4.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* Sraleppal
- **Datei:Stoprfid-logo.svg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/a/af/Stoprfid-logo.svg> *Lizenz:* Public domain *Autoren:* <http://commons.wikimedia.org/wiki/Image:Stoprfid-logo.jpg> *Ursprünglicher Schöpfer:* (Gemeinschaftarbeit des FoeBuD e.V. mit einer Umsetzung von Peter Ehrentaut, zu finden auf www.StopRFID.de. Das Logo ist von uns zur Nutzung freigegeben.)
- **Datei:Transponder2.jpg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/6/6f/Transponder2.jpg> *Lizenz:* CC-BY-SA-3.0 *Autoren:* Transponder selbst gescannt *Ursprünglicher Schöpfer:* Kalinko in der Wikipedia auf Deutsch
- **Datei:Wikibooks-logo.svg** *Quelle:* <https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg> *Lizenz:* CC BY-SA 3.0 *Autoren:* Eigenes Werk *Ursprünglicher Schöpfer:* User:Bastique, User:Ramac et al.
- **Datei:Zeiterfassungsterminal_mit_RFID.jpg** *Quelle:* https://upload.wikimedia.org/wikipedia/commons/f/f8/Zeiterfassungsterminal_mit_RFID.jpg *Lizenz:* Public domain *Autoren:* AHB Electronic GmbH *Ursprünglicher Schöpfer:* ?

12.3 Inhaltslizenz

- Creative Commons Attribution-Share Alike 3.0