

Oliver Grimm
Hauptstraße 5
98554 Benshausen
e-Mail: post ,at' olivergrimm.com

**RFID-Technologie -
Aufbau, Funktionsweise und technische Anwendungen**

**Hauptseminar
an der Fakultät für Informatik und Automatisierung
der Technischen Universität Ilmenau**

**Fachgebiet Rechnerarchitekturen
Betreuer: Dr.-Ing. Jürgen Nützel**

Inhaltsverzeichnis

1 Einleitung	5
1.1 Problemstellung.....	5
1.2 Zielsetzung	5
1.3 Vorgehensweise und Aufbau	5
2 Funktionsweise und technische Umsetzung.....	6
2.1 Bestandteile eines RFID-Systems	7
2.2 Funktionsweise.....	7
2.2.1 Transponder	7
2.2.2 Erfassungsgeräte	9
2.3 Frequenzbereiche	10
3 Sicherheit und Datenschutz	11
3.1 Integrität	11
3.2 Verfügbarkeit	12
3.2.1 Raummultiplex – SDMA	12
3.2.2 Frequenzmultiplex – FDMA.....	13
3.2.3 Zeitmultiplex – TDMA.....	13
3.3 Authentizität.....	14
3.4 Vertraulichkeit.....	15
3.5 Anonymität und Datenschutz.....	15
3.5.1 RFID-Blocker	17
3.5.2 Stellungnahme der Bundesregierung.....	18
4 Praktische Anwendungsbeispiele	18
4.1 Tieridentifikation.....	18
4.2 Metro-Future-Store	20
4.3 Sport	21
5 Resümee und Ausblick	22
6 Literaturverzeichnis / Quellenangaben.....	23

Abkürzungsverzeichnis

ASIC	Application Specific Integrated Circuit
CDMA	Code Division Multiple Access
CRC	Cycling Redundancy Check
DIN	Deutsche Industrienorm
EAS	Electronic Article Surveillance
EEPROM	Electric Erasable and Programmable Read only Memory
EPC	Electronic Product Code
FDMA	Frequency Domain Multiple Access
FDTMA	Frequency and Time Division Multiple Access
FoeBuD e.V.	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.
HF	High Frequency
ISO	International Standardization Organization
LF	Low Frequency
LRC	Longitudinal Redundancy Check
MDL	Metro-Group Distribution Logistic
OCR	Optical Character Recognition
ÖPNV	Öffentlicher Personennahverkehr
OS	Operating System
PPS	Produktionsplanung und -steuerung
RFID	Radio Frequency Identification
SAM	Security Authentication Module
SDMA	Space Division Multiple Access
SRAM	Static Random Access Memory
TDMA	Time Domain Multiple Access
UHF	Ultra-High Frequency
WLAN	Wireless Local Area Network

Abbildungsverzeichnis

Abbildung 2-1: Bestandteile eines RFID-Systems.....	7
Abbildung 2-2: Master-Slave-Prinzip	9
Abbildung 3-1: Raummultiplex mit steuerbarer Richtantenne.....	13
Abbildung 4-1: RFID-Einsatz im Motorsport	22

Tabellenverzeichnis

Tabelle 2-1: Vergleich verschiedener ID-Systeme.....	6
Tabelle 2-2: RFID-Frequenzbereiche.....	10
Tabelle 4-1: Anwendungsbeispiele in verschiedenen Frequenzbereichen.....	18

1 Einleitung

1.1 Problemstellung

„RFID“ (Radio Frequency Identification) ist mit Sicherheit eines der Schlagworte der aktuellen Technologiebranche. Vielseitige Einsatzmöglichkeiten wie in der Logistik, in Bibliotheken, der Abfallwirtschaft, Wegfahrsperrern für Kraftfahrzeuge und viele mehr, machen die RFID-Systeme für viele Bereiche interessant.¹

Bisher erfolgte Identifikation von Objekten meist über Barcodesysteme. Engpaß dabei ist allerdings die geringe Speicherfähigkeit, die Unmöglichkeit der Umprogrammierung der enthaltenen Daten und das Auslesen des Barcodes.² Ein Siliziumchip zur Speicherung von Daten soll diese Probleme lösen. Unter Verwendung eines Senders und eines Empfängers (Funktechnologie) können Gegenstände, Tiere und Menschen eindeutig identifiziert werden. Diese Identifikationssysteme haben sich in den letzten Jahren immer weiter verbreitet.

1.2 Zielsetzung

Ziel der Hauptseminararbeit soll es sein, Aufbau, die Funktionsweise und die technische Anwendung von RFID Systemen anhand von Beispielen aus der Praxis zu beschreiben. Dabei soll auch auf bestimmte Sicherheitsaspekte und den Datenschutz bei der Benutzung dieser Technologie eingegangen werden.

1.3 Vorgehensweise und Aufbau

Nachdem die einzelnen Bestandteile eines RFID-Systems genannt wurden, sollen diese und deren Funktionsweise näher erläutert werden. Im Anschluß daran werden die zu verfolgenden Sicherheitsziele erklärt und dargestellt, welche Ansatzpunkte zu deren Umsetzung es in der RFID-Technologie gibt. Abschließend sollen einige praktische Anwendungsbeispiele aufgezeigt werden.

¹ Vgl. c't 03/2004, Seite 46: RFID

² Vgl. Finkenzeller / RFID-Handbuch / S. 1

2 Funktionsweise und technische Umsetzung

Bei RFID handelt es sich um ein Identifikationssystem auf der Basis der Funktechnologie. Die Erfindung der RFID-Technologie erfolgte 1948 durch Harry Stockman (Veröffentlichung „Communication by means of reflected power“).³ In den 60er Jahren wurde diese, noch theoretische Technologie, in die Wirklichkeit umgesetzt. Die ersten 1-bit-Transponder wurden für die Produktsicherung verwendet (EAS, Electronic Article Surveillance). Der Durchbruch setzte ab dem Jahr 2000 ein, als die Stückkosten für die Produktion der Transponder stark gesunken sind.

Da es sich um eine kontaktlose Übertragung handelt, bietet RFID gegenüber anderen Identifikationstechnologien einige Vorteile. Ein Vergleich einer Auswahl von solchen ID-Systemen ist in der Tabelle 2-1 dargestellt.

Parameter	Barcode	OCR	Chipkarte	RFID
typische Datenmenge	1-100 Byte	1-100 Byte	16 Byte-64 kB	16 Byte-64 kB
Datendichte	gering	gering	sehr hoch	sehr hoch
Lesbarkeit durch Menschen	bedingt	einfach	unmöglich	unmöglich
Einfluß von Schutz/Nässe	sehr stark	sehr stark	möglich	kein Einfluß
Anschaffungskosten Elektronik	sehr gering	mittel	gering	mittel
Lesegeschwindigkeit	gering (~4s)	gering (~3s)	gering (~4s)	sehr schnell (~0,5s)
max. Entfernung zw. Datenträger und Erfassungsgerät	0...50 cm	<1 cm	direkter Kontakt	0...5m

Tabelle 2-1: Vergleich verschiedener ID-Systeme⁴

³ Vgl. AIM / Shrouds of Time: The history of RFID / S. 4

⁴ Vgl. Finkenzeller / RFID-Handbuch / S. 8

2.1 Bestandteile eines RFID-Systems

Für die RFID-Technologie sind zwei Komponenten erforderlich: ein Transponder und ein Erfassungsgerät.⁵ Der Begriff Transponder stammt von den Worten transmit und response.⁶ Er besteht aus einem Mikrochip sowie einer Antenne (Spule oder Dipol). Mit Hilfe des Erfassungsgerätes, welches aus einem Hochfrequenzmodul, einem Controller und einer Antenne besteht, kann man die Daten des Transponders auslesen und ggf. auch auf diesen schreiben. Über eine Schnittstelle (z.B. seriell oder WLAN) können die Daten vom Erfassungsgerät an andere Geräte zur Auswertung weitergeleitet werden (PC, PPS-System). Alle Komponenten sind in der Abbildung 2-1 dargestellt.

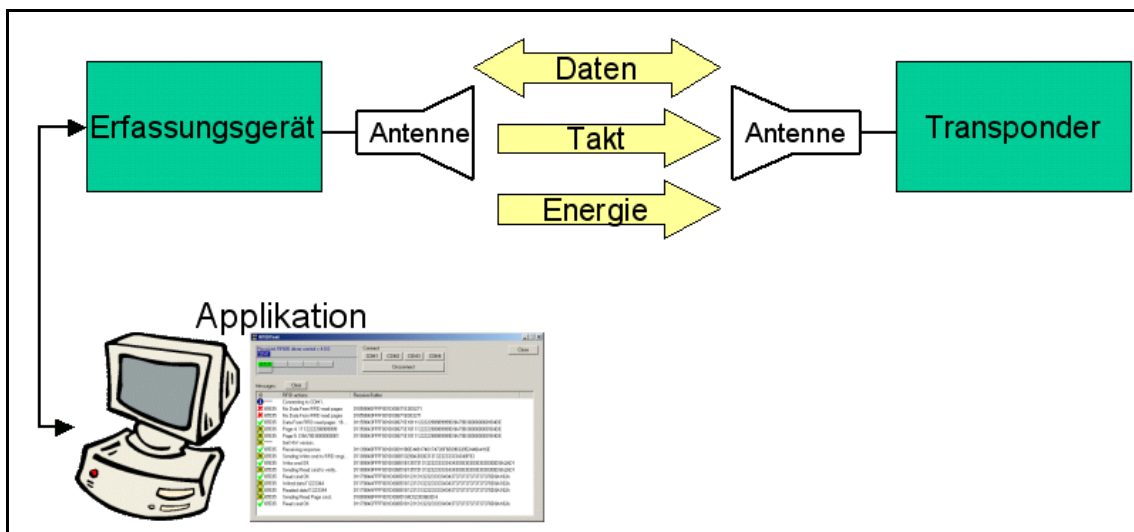


Abbildung 2-1: Bestandteile eines RFID-Systems⁷

2.2 Funktionsweise

2.2.1 Transponder

Man kann zwei verschiedene Arten von Transponder unterscheiden: aktive und passive.⁸ Bei der aktiven Bauweise erfolgt die Energieversorgung für den Mikrochip über eine eingebaute Batterie. Die passiven Systeme verfügen nicht über eine eigene Ener-

⁵ Vgl. Finkenzeller / RFID-Handbuch / S. 7

⁶ Vgl. Meyer, Schüler / Mitteilbare Etiketten (c't 2004 Heft 9; S. 122ff)

⁷ Vgl. Finkenzeller / RFID-Handbuch / S. 7

⁸ Vgl. Finkenzeller / RFID-Handbuch / S. 13

giequelle. Bei diesen wird das elektromagnetische Feld des Erfassungsgerätes genutzt, um die nötige Stromversorgung des Mikrochips zu gewährleisten (siehe auch Abb. 2-1).

Bei der Art der Informationsverarbeitung im Transponder gibt es ein breites Spektrum zwischen Low-end und High-end-Systemen⁹:

- 1-bit-Transponder
Diese sogenannten 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 beschreibbaren 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.

⁹ Vgl. Finkenzeller / RFID-Handbuch / S. 23ff

- Dual-face-Chipkarten

Diese Chipkarten sind zusätzlich mit einem kryptographischen Coprozessor ausgestattet und bieten somit eine höhere Sicherheit bei der Verschlüsselung.

2.2.2 Erfassungsgeräte

Alle Schreib- und Leseoperationen im RFID-System erfolgen nach dem hierarchischen Master-Slave-Prinzip (siehe Abbildung 2-2).¹⁰ An oberster Stelle steht hierbei die Applikationssoftware, von der alle Operationen ausgehen. Das Erfassungsgerät wirkt dabei als Interface zwischen Applikation und Transponder. In diesem werden auch alle Besonderheiten der kontaktlosen RFID-Technologie, wie zum Beispiel Antikollisionsverfahren oder Authentifizierung, durchgeführt.

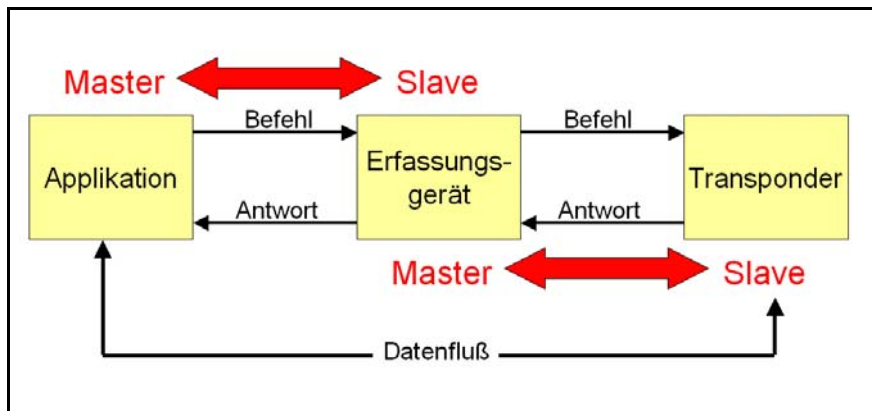


Abbildung 2-2: Master-Slave-Prinzip

Grundsätzlich besteht ein Erfassungsgerät aus zwei Bestandteilen, dem HF-Interface sowie der Steuerung. 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:¹¹

¹⁰ Vgl. Finkenzeller / RFID-Handbuch / S. 319ff

¹¹ Vgl. Finkenzeller / RFID-Handbuch / S. 326

- 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

Dazu enthält die Steuerung in den meisten Fällen einen Mikroprozessor sowie ggf. einen ASIC-Baustein, um den Prozessor bei rechenintensiven Operationen, wie Verschlüsselung oder Signalcodierung, zu entlasten.

2.3 Frequenzbereiche

In der Tabelle 2-2 sind die unterschiedlichen Frequenzbereiche der RFID-Technologie sowie einige Merkmale dargestellt.

	RFID-Frequenzbereiche		
	100 - 135 Khz (Langwellen, LF)	13,56 Mhz (Kurzwellen, HF)	2,45 Ghz (Dezimeterwellen, UHF)
Reichweite*	bis 120 cm	bis 100 cm	bis 12 m
Energieversorgung	passiv	passiv	(semi-)passiv, aktiv
Geschwindigkeit	3 m/s	3 m/s	20 m/s
Material-durchdringung	hohe Eindringungstiefe	hohe Eindringungstiefe	materialabhängig
Einsatz auf Metall	beschränkt	beschränkt	sehr gut (fördernd)
*Reichweite abhängig von Datenträger-, Antennenbauform, Übertragungsart, Sendeleistung			

Tabelle 2-2: RFID-Frequenzbereiche¹²

¹² Vgl. <http://www.idsystems-ag.de/de/rfid-kategorien.php> (Abruf: 2004-05-26)

3 Sicherheit und Datenschutz

Zu den Sicherheitsaspekten in der IT zählen Integrität, Verfügbarkeit und Vertraulichkeit.¹³ Diese drei Grundsicherheitsziele können durch die Authentizität sowie die Anonymität in diesem Zusammenhang erweitert werden.

Unter **Integrität** versteht man die Forderung, daß sicherheitsrelevante Elemente nicht unautorisiert verändert werden können. Die Integrität ist gewährleistet, wenn das entsprechende Element vollständig, unverfälscht und korrekt sind. Es muß gesichert werden, daß unerwünschte Veränderungen sowohl durch Datendefekte, als auch durch mutwillige Verfälschung, eindeutig erkennbar werden. Der Begriff **Verfügbarkeit** beschreibt den Zustand einer Ressource vorhanden zu sein, wenn diese benötigt wird. Die Verfügbarkeit ist gewährleistet, wenn die Betriebsbereitschaft und die Funktionalität jederzeit gegeben ist, d.h., wenn keine negative Beeinträchtigung der Funktionalität stattfindet. Von **Vertraulichkeit** spricht man, wenn man gewährleisten kann, daß bestimmte Daten und Informationen nur den Personen zur Verfügung stehen, die zu deren Nutzung befugt sind, d.h., wenn man unbefugten Informationsgewinn verhindern kann. Dies kann durch die Zugriffskontrolle (**Authentizität** aller Beteiligten) gewährleistet werden (Sicherstellung der Identität eines Subjektes). In den folgenden Kapiteln wird die Umsetzung dieser Sicherheitsziele bei der Nutzung der RFID-Technologie erläutert.

3.1 Integrität

Um die Datenintegrität während der kontaktlosen Übertragung zwischen dem Transponder und dem Erfassungsgerät zu gewährleisten, werden Prüfsummenverfahren angewendet. Dazu zählen beispielsweise die Paritätsprüfung, das LRC- sowie das CRC-Verfahren. Finkenzeller sieht aufgrund der hohen Fehlererkennung das CRC-Verfahren für die RFID-Technologie am geeignetsten.¹⁴ Hierbei handelt es sich um ein zyklisches Verfahren. Bei dessen Berechnung des CRC-Wertes gehen sowohl der CRC-Wert des aktuell zu berechnenden Datenbytes, als auch die CRC-Werte aller vorhergehenden ein. Dadurch wird gewährleistet, daß jedes einzelne Byte des Datenblocks geprüft wird.

¹³ Vgl. BSI / Grundschriftbuch / S. 19

¹⁴ Vgl. Finkenzeller / RFID-Handbuch / S. 200ff

3.2 Verfügbarkeit¹⁵

Ein Problem bei der Anwendung von RFID-Systemen stellt die Tatsache dar, daß sich mehrere Transponder gleichzeitig im Empfangsbereich des Erfassungsgerätes befinden können. Hierbei kann es zu Datenkollisionen kommen. Um dies zu verhindern kommen sogenannte Vielfachzugriffsverfahren zum Einsatz. Grundsätzlich sind zwei Problembereiche zu lösen: Einerseits die Übertragung von Daten vom Erfassungsgerät zu den Transpondern (Broadcast), andererseits der Datenstrom von einem der anwesenden Transponder zum Erfassungsgerät (Vielfachzugriff). Um das Problem des Vielfachzugriffs zu lösen stehen eine Reihe von Verfahren zur Verfügung:

- Raummultiplexverfahren (SDMA)
- Frequenzmultiplexverfahren (FDMA)
- Zeitmultiplexverfahren (TDMA)
- Codemultiplexverfahren (CDMA)

Ein Problem der RFID-Technologie besteht darin, daß ein Datenstrom von einem Transponder zum Erfassungsgerät durch andere Transponder im Empfangsbereich nicht mitgelesen werden kann. Dadurch bleibt diesem die Anwesenheit weiterer Geräte im Empfangsbereich verborgen. Wie das Problem des Vielfachzugriffs gelöst wird ist je nach Hersteller unterschiedlich und wird von diesen in der Regel nicht veröffentlicht. Dadurch ist selbst in der Fachliteratur zu diesem Thema wenig Informationsmaterial zu finden.¹⁶

3.2.1 Raummultiplex – SDMA

Eine Möglichkeit die Kollision von Datenströmen zu verhindern besteht darin, die Reichweite eines Erfassungsgerätes drastisch zu reduzieren und dafür eine Vielzahl solcher Geräte flächendeckend in der Form eines Arrays anzuordnen. Dadurch wird es ermöglicht, eine hohe Anzahl räumlich verteilter Transponder gleichzeitig auszulesen. Weiterhin besteht die Möglichkeit der Verwendung einer elektronisch steuerbaren Richtantenne (Abb. 3-1).

¹⁵ Die Ausführungen dieses Kapitels sind folgender Quelle entnommen:
Finkenzeller / RFID-Handbuch / S. 203ff

¹⁶ Vgl. Finkenzeller / RFID-Handbuch / S. 205

Aufgrund des hohen Implementierungsaufwandes für Raummultiplexverfahren beschränkt sich die Anwendung dieser auf wenige Spezialgebiete.

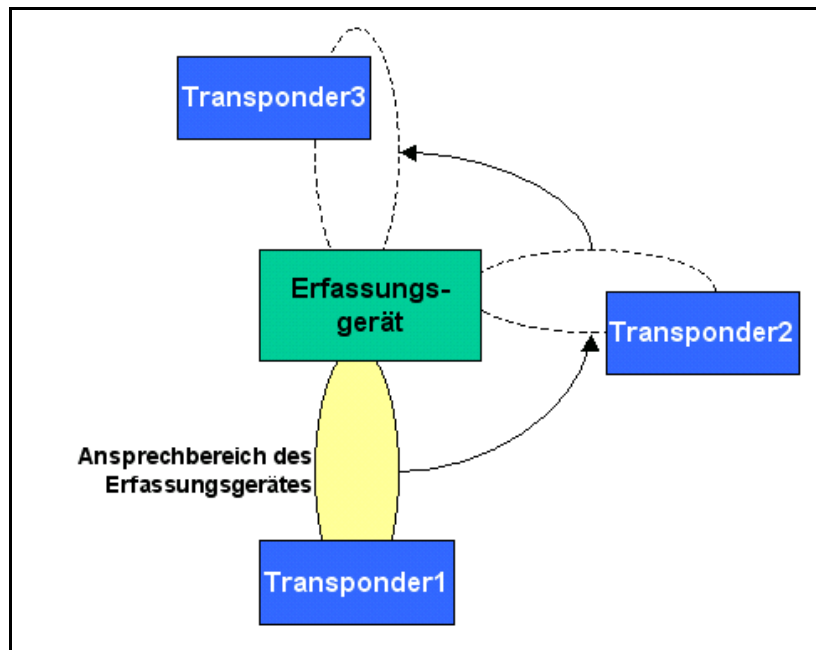


Abbildung 3-1: Raummultiplex mit steuerbarer Richtantenne

3.2.2 Frequenzmultiplex – FDMA

Bei den Frequenzmultiplexverfahren werden den einzelnen Kommunikationspartnern mehrere Übertragungsfrequenzen zur Verfügung gestellt. Zu diesem Zwecke kommen Transponder mit frei einstellbaren Sendefrequenzen zum Einsatz. Nachteil dieser Verfahren ist der hohe technische Aufwand in den Erfassungsgeräten, da für jeden Empfangskanal ein eigener Empfänger bereitgestellt werden muß.

3.2.3 Zeitmultiplex – TDMA

Das gebräuchlichste Antikollisionsverfahren ist das Zeitmultiplexverfahren. Man unterscheidet hier weiter in transpondergesteuerte (transponder driven) und empfangsgerätgesteuerte Verfahren (interrogator driven). Die transpondergesteuerten Verfahren arbeiten asynchron und sind aufgrund dessen sehr langsam und unflexibel. Ein Beispiel dafür ist das ALOHA-Verfahren. Dieses wird vor allem in Europa zur Kennzeichnung einzelner Produkte genutzt.¹⁷ Bei diesem Verfahren weist das Erfassungsgerät den Transponder an, mit einer unvorhersehbaren Zeitverzögerung zu antworten. Dazu sendet es ein

¹⁷ Vgl. Schüler / RFID-Blocker / c't 06-2004 S. 40

Request mit der Angabe einer Fenstergröße, in der der Transponder antworten kann (slotted Aloha).

Wesentlich häufiger kommen die empfangsgerätgesteuerten Verfahren zum Einsatz. Bei diesem synchronen Verfahren werden alle Transponder im Empfangsbereich vom Erfassungsgeräten gesteuert. Dabei selektiert das Erfassungsgerät zunächst genau einen Transponder im Erfassungsbereich, kommuniziert mit diesem und baut letztlich die Verbindung wieder ab. Da zu einem Zeitpunkt immer nur eine Kommunikationsbeziehung mit einem Transponder bestehen kann, und die einzelnen Geräte nacheinander selektiert werden, kann man dieses Verfahren als Zeitmultiplexing bezeichnen. Ein Beispiel für ein empfangsgerätgesteuertes Verfahren ist der „Tree-Walking-Algorithmus“ (binärer Suchbaum).¹⁸ Dabei wird vom Erfassungsgerät bewußt solange eine Datenkollision herbeigeführt, bis nur noch ein einziger Transponder zur Kommunikation zur Verfügung steht. Das Erfassungsgerät fordert zunächst alle Transponder, die mit der (binären) Seriennummer „1“ beginnen, auf, ihre Daten zu senden. Kommt es zu einer Kollision, weiß das Gerät, daß sich mehrere solche Seriennummern im Empfangsbereich befinden. Deshalb wird der Bereich weiter eingeschränkt, und es werden nun alle Transponder, die mit der Seriennummer „11“ beginnen, aufgefordert. Diese Verfahrensweise wird solange wiederholt, bis nur noch ein Transponder antwortet.

3.3 Authentizität

Die Authentifizierung von Erfassungsgerät und Transponder beruht auf der „Three Pass Mutual Authentication“ nach ISO 9798-2.¹⁹ Dabei handelt es sich um eine symmetrische Verschlüsselung. Der geheime Schlüssel ist in Besitz aller an einem System beteiligten Erfassungsgeräte und Transponder. Mit diesem Challenge-and-Response-Verfahren kann sichergestellt werden, daß kein unberechtigtes Erfassungsgerät die Daten eines zum System gehörenden Transponders ausliest und daß das Erfassungsgerät keine gefälschten Daten von fremden Transpondern erhält. Ein Nachteil besteht darin, daß alle beteiligten Geräte des Systems im Besitz des geheimen Schlüssels sein müssen. Dies kann bei Einsatzgebieten, bei denen viele Transponder frei zugänglich sind (Ticke-

¹⁸ Vgl. Sarma, Weis, Engels / RFID Systems and Security and Privacy Implications

¹⁹ Vgl. Finkenzeller / RFID-Handbuch / S. 225

ting im ÖPNV), zu einem Sicherheitsrisiko führen. Der geheime Schlüssel könnte von unberechtigten Personen ermittelt und mißbräuchlich eingesetzt werden. Um dieses Sicherheitsrisiko zu vermeiden, kann eine Authentifizierung mit abgeleiteten Schlüsseln eingesetzt werden.²⁰ Dazu wird bei der Produktion des Transponders mit Hilfe dessen eindeutiger Seriennummer, eines kryptographischen Algorithmus und eines Masterschlüssels ein Schlüssel für den Transponder abgeleitet. Bei der Authentifizierung der Geräte wird zunächst durch das Erfassungsgerät die Seriennummer des Transponders angefordert. Mit Hilfe des Masterschlüssels wird dann daraus in einem besonderen Sicherheitsmodul des Erfassungsgerätes (SAM) der spezifische Schlüssel des beteiligten Transponders abgeleitet. Dieser ist nun sowohl dem Erfassungsgerät, als auch dem Transponder bekannt. Mit diesem spezifischen Schlüssel wird nun das Challenge-and-Response-Verfahren abgewickelt. Als SAM kommen in der Regel kontaktbehaftete Chipkarten mit einem Kryptoprozessor zum Einsatz.

3.4 Vertraulichkeit

Bei RFID-Systemen kann man grundsätzlich zwei Arten von Angriffen auf die Vertraulichkeit von Daten unterscheiden²¹. Einerseits die aktiven Angriffe, bei denen die übertragenen Daten manipuliert werden (Integritätsverlust) und andererseits die passiven Angriffe, bei denen der Datenstrom lediglich ausgelesen wird und diese erfaßten Daten evtl. mißbräuchlich benutzt werden. Um diese Arten von Angriffen zu verhindern, können die übertragenen Daten verschlüsselt werden. Bei RFID-Systemen werden bisher ausschließlich symmetrische Verschlüsselungsverfahren eingesetzt. Aufgrund der hohen Rechenleistung, die für symmetrische Blockverfahren benötigt wird, kommt in der Regel nur eine symmetrische Stromverschlüsselung in Frage (Streamcipher).

3.5 Anonymität und Datenschutz

Ein großes Problem mit viel Diskussionen in der Öffentlichkeit stellen die Anonymität und der Datenschutz dar.²² Durch den Einsatz der RFID-Technologie in der Logistik (Supply Chain Management) und dadurch teilweise auch im Einzelhandel (siehe auch

²⁰ Vgl. Finkenzeller / RFID-Handbuch / S. 227

²¹ Vgl. Finkenzeller / RFID-Handbuch / S. 228

²² siehe hierzu auch: <http://www.foebud.org/texte/aktion/rfid/demo/index.htm>
(Abruf: 2004-05-26)

Kapitel 4.2 Metro-Future-Store) ist es möglich festzustellen, welche Waren der Kunde in seinem Einkaufskorb hat, und das, ohne daß dieser etwas davon bemerkt (im Gegensatz zum Einsatz von Barcode, der erst offensichtlich eingescannt werden muß), da durch die zunehmende Miniaturisierung kaum feststellbar ist, wo sich ein solches RFID-Etikett befindet und aufgrund der Funktechnologie die Erkennung der Datenübertragung zwischen dem Transponder und dem Erfassungsgerät ohne technische Hilfsmittel nicht möglich ist. In Zusammenwirken mit einer RFID-Kundenkarte wäre es möglich, genaue Bewegungs- und Kundenprofile zu erstellen.²³ Bei dem gegenwärtigen ID-System im Einzelhandel (Barcodeverfahren EAN13) kann nur darauf geschlossen werden, um welchen Artikel es sich handelt, d.h., alle identischen Artikel eines Herstellers haben die gleiche 13-stellige Nummer. Bei Produkten, die mit Hilfe der RFID-Technologie mit dem Electronic Product Code (EPC) gekennzeichnet sind, ist es möglich, jeden einzelnen Artikel weltweit eindeutig zu identifizieren, da jeder einzelne Artikel einer Produktreihe eines Herstellers eine andere, eindeutige Seriennummer hat.²⁴ Mit Hilfe der EPC ist es möglich, 68 Milliarden Stück jedes registrierten Artikels individuell zu kennzeichnen.

Der FoeBuD e.V. stellt in einem Positionspapier folgende Gefahren für die Privatsphäre und Bürgerrechte auf²⁵:

- versteckte Anbringung von Etiketten
- einzigartige ID-Merkmale für Objekte (weltweit)
- massenhafte Datenzusammenführung
- versteckte Lesegeräte
- individuelle Verfolgung und Profilierung

²³ Vgl. Meyer / RFID / c't 03-2004 S. 46

²⁴ Vgl. Kuri, Meyer, Schüler / PC-Trends: Datenschutz und RFID / c't 06-2004 S. 138

²⁵ Vgl. FoeBud e.V. / Positionspapier

Es gibt verschiedene Ansatzpunkte zur Lösung der Probleme beim Schutz der Privatsphäre des Nutzers:²⁶

- Transponder mit einem Schutznetz oder einer Schutzfolie umhüllen
- Transponder vernichten / unbrauchbar machen
- Active Jamming (Aussenden von RF-Signalen mit Hilfe eines leistungsstarken Störsenders)
- Smart-Tag-Lösung (Datenschutz mit Hilfe kryptographischer Lösungen)
- Einsatz von Blocker-Tags

3.5.1 RFID-Blocker

Die Firma RSA (<http://www.rsasecurity.com>) hat eine Technologie entwickelt, bei der die RFID-Technologie mit einer Schutzzone für die Privatsphäre umgeben werden kann.²⁷ Durch den Blocker-Tag werden alle möglichen Seriennummern simuliert („full-blocker“), sodaß es für das Erfassungsgerät nicht möglich ist, die Daten der übrigen Transponder im Empfangsbereich auszulesen. Allerdings ist dieses Verfahren nur bei dem sogenannten „Tree-Walking-Protokoll“ wirksam (siehe Kapitel 3.2.3, Zeitmultiplex). Bei jeder Anfrage des Erfassungsgerätes nach der Seriennummer meldet sich der Blocker-Tag.²⁸ Dadurch wird es immer zu einer Datenkollision mit einem anderen anwesenden Transponder im Empfangsbereich kommen, sodaß von diesem keine Daten ausgelesen werden können. Falls genügend Zeit und Rechenleistung im Erfassungsgerät zur Verfügung steht, dann wird so der komplette Binärbaum durchsucht, was bei einfachen Systemen immerhin schon 2^{64} (also 18.446.744.073.709.600.000) Möglichkeiten sind. Weiterhin ist eine Implementation eines „Partial Blockers“ möglich, der beispielsweise nur die rechte Seite des Binärbaums betrifft, sodaß alle Seriennummern, die mit „1“ beginnen, blockiert würden. Diese Vorgehensweise ist für beliebige Teilbäume möglich.

²⁶ Vgl. Rivest, Szydlo, Jules / The Blocker Tag

²⁷ Vgl. Schüler / Schnüffeltechnik ausgetrickst / c't 06-2004 S. 40

²⁸ Vgl. Rivest, Szydlo, Jules / The Blocker Tag

3.5.2 Stellungnahme der Bundesregierung

Die Bundesregierung hat am 26.05.2004 auf ein Anfrage der FDP-Bundestagsabgeordneten Gisela Piltz²⁹ bezüglich des Datenschutzes bei der RFID-Technologie festgestellt, daß kein ergänzender datenschutzrechtlicher Regelungsbedarf erkennbar ist.³⁰ Begründet wird dies mit der Tatsache, daß beispielsweise bei Zutrittsystemen personenbezogene Daten gespeichert und übertragen werden, aber ein unbewußtes Auslesen der Daten ausgeschlossen werden kann, da aufgrund der geringen Reichweite der Nutzer den Transponder bewußt an das Erfassungsgerät halten muß.³¹ RFID-Systeme mit höheren Reichweiten, zum Beispiel beim Einsatz in der Logistik, enthalten i.d.R. keine personenbezogenen Daten, sodaß auch hier kein Handlungsbedarf besteht. Selbst wenn personenbezogene Daten mit Hilfe der RFID-Technologie erfaßt würden, beispielsweise im Einzelhandel durch die Kombination von Produktdaten (EPC) und Daten aus einer RFID-Kundenkarte, regelt das Bundesdatenschutzgesetz bereits den Umgang mit solchen Daten.

4 Praktische Anwendungsbeispiele

Je nach Betriebsfrequenz ergeben sich verschiedene Einsatzgebiete. Beispiele dafür die unterschiedlichen Frequenzbereiche sind in der Tabelle 4-1 dargestellt.

100 kHz – 135 kHz	13,56 MHz	2,45 GHz
Wegfahrsperren	Ski-Ticketing	Mehrweggebinde/Pfand
Zutrittskontrolle	Dokumentenverfolgung	Mauterfassung
Tieridentifikation	ÖPNV	Wechselbrückenverfolgung

Tabelle 4-1: Anwendungsbeispiele in verschiedenen Frequenzbereichen

4.1 Tieridentifikation

Mit den ISO-Normen 11784, 11785 und 14223 ist ein internationaler Standard zur Tierkennzeichnung festgelegt.³² RFID-Systeme werden beispielsweise bei der Rinderhal-

²⁹ Vgl. Piltz / Anfrage Bundesregierung

³⁰ Vgl. Bundesregierung / Antwort auf FDP-Anfrage

³¹ Vgl. Heise News / <http://www.heise.de/newsticker/meldung/47743>
(Abruf: 2004-05-28)

³² Vgl. Finkenzeller / RFID-Handbuch / S. 233

tung und bei Brieftaubenpreisflügen eingesetzt. Dadurch ist eine Herkunftssicherung sowie eine individuelle Futterzuteilung möglich. Dabei erhält jedes Tier eine eindeutige Seriennummer. Dazu können folgende Transponderarten genutzt werden:³³

- injizierbare Transponder
Der Transponder befindet sich hierbei in einer Glashülle, die unter die Haut oder in einen Muskel des Tieres injiziert wird.
- Bolustransponder
Bei dem Bolus handelt es sich um einen Keramikzylinder (Durchmesser 20mm, Länge 70mm) in dem sich der Transponder befindet. Der Bolus wird m.H. einer Sonde in den Magen des Tieres verbracht (nur bei Wiederkäuern möglich).
- elektronische Ohrmarken
Diese entsprechen in Form und Anwendung den bisher verwendeten Ohrmarken, nur, daß diese mit einem Transponder ausgestattet ist.

Die Teilnahme an Preisflügen ist ein wesentlicher Bestandteil der Brieftaubenzucht.³⁴ Ähnlich wie bei Marathonläufen (siehe Kapitel 4.3) werden hier Hunderte von Individuen zur gleichen Zeit am gleichen Ort starten. Ziel ist es, daß die Brieftauben den Schlag in ihrer Heimat schnellstmöglich erreichen. Für eine genaue Bewertung ist es nötig, die genaue Ankunftszeit jeder Taube zu erfassen. Bisher wurde das mit einer sog. mechanischen Konstatieruhr vorgenommen. Eine technisch bessere Lösung stellt das Anbringen von Read-only-Transpondern (Glastransponder die in Kunststoffringe eingegossen werden). Zu Beginn eines Preisfluges werden die Transponderdaten ausgelesen, und somit die Taube registriert. Sobald diese im Heimatschlag angekommen ist, wird der Transponder erneut erfaßt, und zusätzlich die Ankunftszeit der Taube gespeichert, sodaß eine genaue Auswertung möglich ist. Aufgrund von Betrugsversuchen der Züchter (Vortäuschen der Seriennummer mit einem Simulationsgerät) kam es zur Einführung eines zusätzlichen, beschreibbaren EEPROM-Speichers auf dem Transponder. Vor dem Start wird eine Zufallszahl auf dem Chip gespeichert. Nun muß sichergestellt werden, daß die Züchter keinen Zugriff mehr auf die Tiere haben, um ggf. die Zufallszahl auslesen zu können.

³³ Vgl. Texas-Trading / Elektronische Tiererkennung

³⁴ Vgl. Finkenzeller / RFID-Handbuch / S. 282ff

4.2 Metro-Future-Store

Bei dem Metro-Future-Store handelt es sich um eine gemeinsame Initiative der Metro-Group mit SAP, Intel, IBM und weiteren Unternehmen mit dem Ziel der technischen und prozessualen Modernisierung im Handel.³⁵ Repräsentiert wird das Projekt durch ein Einzelhandelsgeschäft der Kette EXTRA in Rheinberg (Nordrhein-Westfalen). Metro nennt folgende Einsatzgebiete der RFID-Technologie im Future-Store:³⁶

- Warenanlieferung im Markt
- Lagermanagement
- Transport der Waren in den Verkaufsraum
- intelligente Regale im Markt
- Tags auf CDs, DVDs und Videos

Alle Transporteinheiten (Paletten, Kartons) für den Metro-Future-Store werden im Lager der METRO Group Distribution Logistic (MDL) per Hand mit einem RFID-Label versehen. Mit Hilfe dieser wird kontrolliert, ob die Lieferungen im Wareneingang des Future-Stores mit den Bestellungen übereinstimmen. Zusätzlich ist an jedem Lagerplatz ein Transponder angebracht, der bei der Einlagerung der Ware zusammen mit den Daten der Kartons eingelesen wird. Dadurch ist im Warenflußsystem genau vermerkt, welche Produkte sich wo im Lager befinden, wodurch keine Inventur „per Hand“ mehr nötig ist. Das Warenflußsystem erkennt auch automatisch, wenn Ware vom Lager in den Ladenraum geschafft wird. Dadurch ist ein einfacheres Auslösen einer Nachbestellung möglich, wenn die Waren im Lager den Meldebestand unterschreiten. Einige wenige Produkte sind bereits auf der Stückerbene mit RFID-Transpondern ausgerüstet (bei Metro derzeit 3 Produkte) und in den Regalen dieser Artikeln befinden sich Lesegeräte, die dem Personal melden, wenn Ware nachgefüllt werden muß. Mit Hilfe von Transpondern (Tags) auf CD's, DVD's und Videos kann man sich Trailer zu den Filmen ansehen oder die Musik-CD hören.

Aber auch das Konzept von Metro ist nicht unumstritten. So erhielt die Metro-Group 2003 den „Big-Brother-Award“ des FoeBud e.V.:

³⁵ Vgl. Metro-Group / Hintergrundinformationen

³⁶ Vgl. Metro-Group / Future-Store: Technische Komponenten / S. 17

„Den BigBrotherAward in der Kategorie Verbraucherschutz erhält die Metro AG für das Projekt "future store", mit dem die RFID-Technik in Deutschland propagiert werden soll. Der berührungslos auszulesende Chip, der zukünftig den Barcode auf Waren ersetzen soll, birgt große Gefahren für die Privatsphäre der Verbraucher.“³⁷

4.3 Sport

Bei großen Marathonveranstaltungen, wie dem Berlin-Marathon (über 30.000 Teilnehmer), kann es nach dem Startsignal mehrere Minuten dauern, bis auch der letzte Läufer über die Startlinie gelaufen ist. Ohne eine individuelle Zeitnahme würden die Läufer in den hinteren Startreihen stark benachteiligt.³⁸ Deshalb wird von jedem Teilnehmer ein Transponder mitgeführt. So kann genau ermittelt werden, wann dieser die Startlinie überschritten hat. Der Chip mit dem Transporter wird an einem Schuh befestigt. Die Antennen der Erfassungsgeräte befinden sich in einer Matte, die auf dem Boden über der Startlinie bzw. der Ziellinie ausgerollt wird. Dadurch kann die genaue Startzeit und Zielankunftszeit jedem Teilnehmer individuell zugeordnet werden, wodurch eine sofortige elektronische Auswertung nach der Zielankunft möglich ist.

Ein anderes Einsatzgebiet sind Sportveranstaltungen, bei denen es gilt, eine festgelegte Runde in einer bestimmten Zeit so oft wie möglich zu absolvieren. Ein Beispiel ist die German-Cross-Country-Championship. Dabei handelt es sich um einen Wettkampf mit Enduro- und Moto-Cross-Motorrädern. Bevor RFID-Technologie zum Einsatz kam, mußten die Nummern der Fahrer nach jeder Runde durch Mitarbeiter in einer Kontrollstation erkannt und notiert werden, was aufgrund von Verschmutzungen häufig nicht eindeutig möglich war. Vor jedem Rennen bekommt jeder Fahrer einen Transponder, den er in der Regel mit einem Gummiband am rechten Handgelenk befestigt. An einem Punkt der Strecke ist eine Zählstelle mit mehreren Erfassungsgeräten, an der der Fahrer kurz anhält und den Transponder in den Erfassungsbereich des Gerätes hält (Abb. 4-1),

³⁷ Vgl. <http://www.bigbrotherawards.de/2003/.cop/> (Abruf: 2004-05-26)

³⁸ Vgl. Finkenzeller / RFID-Handbuch / S.393ff

wodurch die angeschlossene Applikation die Information erhält, daß dieser Fahrer eine weitere Runde absolviert hat.



Abbildung 4-1: RFID-Einsatz im Motorsport³⁹

5 Resümee und Ausblick

Die RFID-Technologie bietet aufgrund der vielen Vorteile gegenüber herkömmlichen Identifikationssystemen, eine große Vielfalt von Anwendungsmöglichkeiten. Durch sinkenden Stückkosten für die Herstellung der Transponder ist ein effizienterer Einsatz dieser Technik möglich. Allerdings darf man bei den zukünftigen Einsatzgebieten die Datenschutz- und Sicherheitsaspekte nicht vernachlässigen, um einen Datenmißbrauch zu verhindern. Zwar werden einige Sicherheitsaspekte in den RFID-Systemen bereits umgesetzt, dennoch sollte man dem Einsatz dieser Technologie immer kritisch gegenüberstehen, und Vor- und Nachteile genau abwägen.

³⁹ Quelle: <http://www.enduroteam.de> (Abruf: 2004-05-19)

6 Literaturverzeichnis / Quellenangaben

AIM / Shrouds of Time: The history of RFID

AIM (The Association of Automatic Identification and Data Capture Technologies): Shrouds of Time: The history of RFID

http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf

Abruf: 2004-06-01

BSI / Grundschutzhandbuch /

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch

Stand: 4.Ergänzungslieferung, Mai 2002

Bundesregierung / Antwort auf FDP-Anfrage

Antwort der Bundesregierung auf die Anfrage der FDP-Bundestagsabgeordneten

Gisela Piltz

http://marvin.unique.de/piltz/front_single/pdf/1503025_Antwort.pdf

Abruf: 2004-05-28

FoeBud e.V. / Positionspapier

<http://www.foebud.org/rfid/positionspapier.pdf>

Abruf: 2004-04-01

Kuri, Meyer, Schüler / PC-Trends: Datenschutz und RFID / c't 06-2004 S. 138

Jürgen Kuri, Angela Meyer, Peter Schüler

c't 6/2004, S. 138: PC-Trends: Datenschutz und RFID

Abruf: 2004-03-31

Metro-Group / Future-Store: Technische Komponenten

<http://www.future-store.org/servlet/PB/-/1vtk46wfsu629149x59d54gxr8yjvh5b/show/1001848/RZV%20D-Technik-02-10-03.pdf>

Abruf: 2004-05-26

Metro-Group / Hintergrundinformationen

http://www.future-store.org/servlet/PB/-s/1vtk46wfsu629149x59d54gxr8yjvh5b/show/1002055/Backgroundinfos%20FS_L_dt.pdf

Abruf: 2004-05-26

Meyer / RFID / c't 03-2004 S. 46

Angela Meyer; c't 3/2004, S. 46: RFID

Piltz / Anfrage Bundesregierung

Gisela Piltz / Anfrage an die Bundesregierung: Technologie der Radio Frequency Identification

<http://dip.bundestag.de/btd/15/030/1503025.pdf>

Abruf: 2004-05-28

Rivest, Szydlo, Jules / The Blocker Tag

Ari Juels, Ronald L Rivest, Michael Szydlo: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy

<http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf> (Abruf: 2004-05-26)

Sarma, Weis, Engels / RFID Systems and Security and Privacy Implications

RFID Systems and Security and Privacy Implications

Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels

Massachusetts Institute of Technology

<http://www.springerlink.com/media/3L93GJQRTL5QADHWRH5U/Contributions/7/M/D/K/7MDKKQVGWVA88QXQ.pdf>

Abruf: 2004-05-26

Schüler / RFID-Blocker

Peter Schüler

RFID-Blocker : Schnüffeltechnik ausgetrickst

c't 06-2004; S.40

Texas-Trading / Elektronische Tiererkennung

http://www.texas-trading.de/pdf/elektronische_tiererkennung_03-04.pdf

Abruf: 2004-05-26