

**Semesterarbeit**

**Lehrveranstaltung „Nachrichtenverkehrssysteme“**

**Thema:** Daten- und Nutzersicherheit bei RFID-Systemen

**Aufgabenstellung:** Erarbeiten Sie eine Übersicht über wesentliche Verfahren zur Datensicherheit bei RFID-Systemen, insbesondere bei der Datenspeicherung und Datenübertragung und über die Sicherheit des Nutzers von RFID-Systemen von der über die direkte RFID-Anwendung hinausgehende Verwendung dieser Daten.

**Betreuer:** Dr. Ing. Stephan Baumann

**Bearbeitet von:** Kristin Reinhardt

**Abgabe:** 06.02.2006

# Inhaltsverzeichnis

<b>ABBILDUNGSVERZEICHNIS .....</b>	<b>III</b>
<b>1 VORWORT .....</b>	<b>1</b>
<b>2 TECHNISCHER HINTERGRUND .....</b>	<b>2</b>
2.1 AUFBAU .....	2
2.2 KOMMUNIKATION .....	3
2.3 DATENSPEICHERUNG .....	4
<b>3 DATENSICHERHEIT .....</b>	<b>5</b>
3.1 RECHTLICHE GRUNDLAGEN .....	5
3.2 MÖGLICHE ANGRIFFE AUF RFID-SYSTEME .....	7
3.2.1 Unerwünschtes Auslesen der Daten .....	7
3.2.2 Abhören am Chip .....	8
3.2.3 Buffer Overflows .....	8
3.2.4 Unwissentliches Senden von Daten .....	8
3.3. UNTERBINDUNG UNERWÜNSCHTER DATENÜBERTRAGUNG .....	9
3.3.1 Deaktivierung der RFID-Chips .....	9
3.3.2 Abschirmung der RFID-Chips .....	9
3.3.3 Frequenzhopping .....	9
3.3.4 Passwortschutz .....	9
3.3.5 Blockieren der RFID-Chips .....	10
3.3.6 Verwendung einer angeschlossenen Datenbank .....	10
3.4 SICHERE DATENÜBERTRAGUNG .....	10
3.4.1 Symmetrische Verschlüsselung .....	11
3.4.2 Asymmetrische Verschlüsselung .....	13
3.4.3 Hybridverfahren .....	13
3.4.4 Verschlüsselungsalgorithmen im Detail .....	14
3.4.4.1 DES - Data Encryption Standard 1974 .....	14
3.4.4.2 Triple-DES .....	14
3.4.4.3 RSA - Rivest, Shamir und Adleman 1977 .....	15
3.4.4.4 RC4 1987 .....	15
3.4.4.5 IDEA 1990 .....	15
3.4.4.6 Blowfish 1993 .....	16
3.4.4.7 Cast 1996 .....	16
3.4.4.8 Cayley-Purser-Algorithmus 1999 .....	16
3.4.4.9 AES – Advanced Encryption Standard 2000 .....	16
3.4.5 Digitale Signaturverfahren .....	17
3.4.5.1 S/MIME - Secure MIME – Trusted Mime .....	17
3.4.5.2 Digital Signature Algorithmus (DSA) .....	17
3.4.5.3 Elliptic Curve Digital Signature Algorithmus (ECDSA) .....	18
3.5 DATENSICHERHEIT BEI DER WEITERGEHENDEN VERWENDUNG DER DATEN .....	18
<b>4 PRAXIS – BEISPIELE .....</b>	<b>20</b>
4.1 IMMOBILIZER .....	20
4.2 EINZELHANDEL .....	20
4.3 ZUTRITTSKONTROLLE .....	21
4.4 BEZAHLSYSTEME .....	22
4.5 DEUTSCHER REISEPASS (SEIT 2005) .....	23
4.6 IDENTIFIKATION .....	25
<b>5 FAZIT .....</b>	<b>27</b>
<b>LITERATUR .....</b>	<b>28</b>
<b>WEBLINKS .....</b>	<b>29</b>

## Abbildungsverzeichnis

Abbildung 1: Beispiele für RFID-Tags von Texas Instruments .....	1
Abbildung 2: Grundbestandteile von RFID-Systemen.....	2
Abbildung 3: Aktive vs. Passive Transponder .....	2
Abbildung 4: Größenvorstellung von RFID-Chips.....	2
Abbildung 5: Grundlegende Funktionsweise der Kommunikation zwischen Lesegerät und RFID-Transponder.....	3
Abbildung 6: Prinzip des asymmetrischen Verfahrens.....	13
Abbildung 7: Symmetrische vs. Asymmetrische vs. Hybridverfahren .....	14
Abbildung 8: Elektronische Signatur.....	17
Abbildung 9: Basic Access Control.....	24

## 1 Vorwort

Die wesentliche Eigenschaft von Radio Frequency Identification (RFID) liegt in der berührungslosen Übertragung von Daten<sup>1</sup>. Bereits in den 60er Jahren wurden Vorläufer von RFID in einfacher Form als Diebstahlsicherungen im Einzelhandel eingesetzt<sup>2</sup>. Weiterentwicklungen und daraus resultierende weitere Einsatzmöglichkeiten dieser Technologie führten zu einer verstärkten Nutzung in der Landwirtschaft, zum Beispiel bei der Kennzeichnung von Nutztieren. Mehrere amerikanische Bundesstaaten sowie Norwegen entschieden sich in den 80er Jahren für den Einsatz von RFID im Straßenverkehr, womit die USA im Folgenden Mautsysteme installierte. Weitere Anwendung fand die Technologie beispielsweise bei der Realisation von Zugangskontrollen, Verfahren zum bargeldlosen Bezahlen, Skipässen, Tankkarten, elektronischen Wegfahrsperrern und hält nun auch Einzug in die Logistikkette vom Rohstoff bis zum fertigen Produkt beim Endverbraucher. Viele weitere mögliche Einsatzbereiche werden derzeit erprobt, so beispielsweise der Einsatz zur Identifikation in Krankenhäusern, Schulen und Unternehmen. Auch der neue deutsche Reisepass ist mit RFID ausgestattet, so dass sich die Fragen nach dem Schutz sensibler Daten mehren.

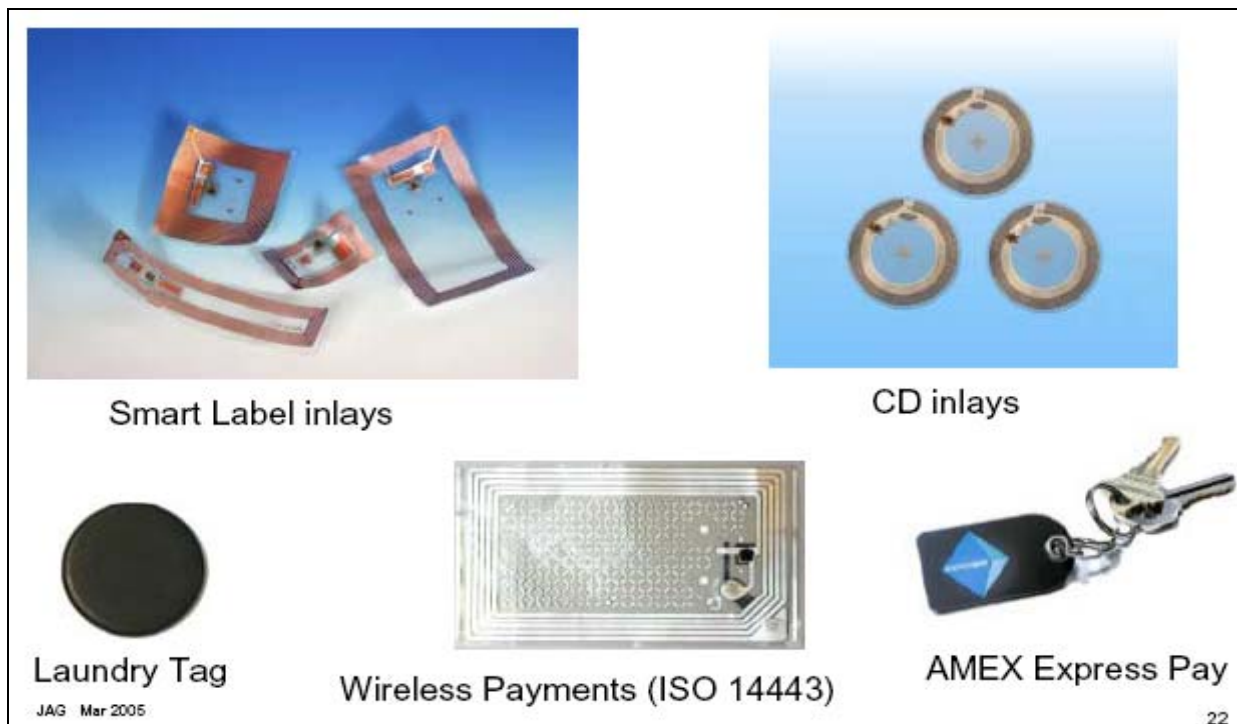


Abbildung 1: Beispiele für RFID-Tags von Texas Instruments<sup>3</sup>

<sup>1</sup> Quelle: RFID-Journal: „RFID“; <http://www.rfid-journal.de/rfid.html>

<sup>2</sup> Quelle: Geschichte Lexikon: „Radio Frequency Identification“;  
<http://www.geschichteboard.de/lexikon/RFID,information.htm>

<sup>3</sup> Quelle: „RFID 101 - The Basics, Texas Instruments' RFID Systems“; zu beziehen über Texas Instruments

## 2 Technischer Hintergrund <sup>4</sup>

### 2.1 Aufbau

Der Transponder selbst besteht aus einer Kombination von Mikrochip und Antenne. Einfache passive 1-Bit-Tags können durch einen Speicher für eine eindeutige ID, Read-only- bzw. Read/Write-Speicher erweitert werden.

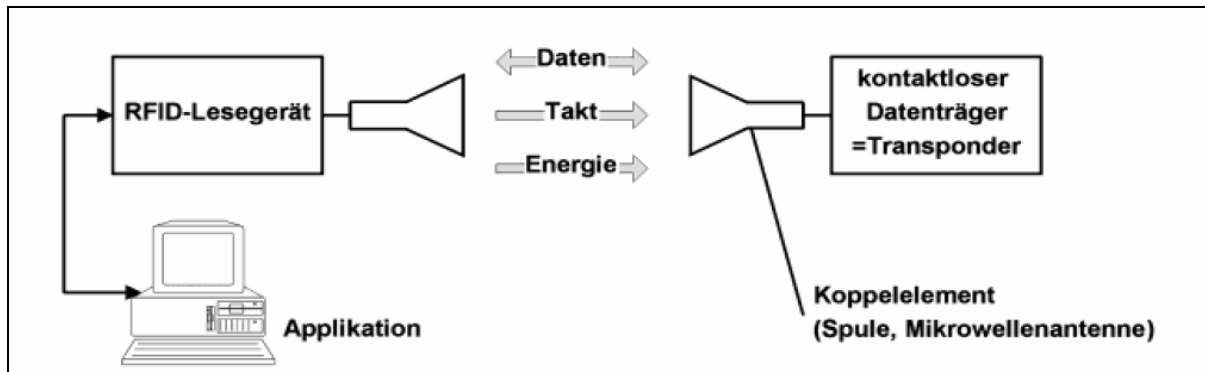


Abbildung 2: Lesegerät und T ransponder sind die Grundbestandteile jedes RFID-Systems. RFID-Handbuch, S.9

Die Energieversorgung erfolgt durch die vom Lesegerät ausgestrahlten Funkwellen<sup>5</sup>. Daneben gibt es auch aktive Tags mit einer eigenen Energieversorgung, womit längere Aktivitäten im und mit dem Chip möglich sind, und größere Reichweiten erzielt werden können. Diese aktiven Tags können neben der ID und dem RW-Speicher mit einem Prozessor ausgestattet sein. Außerdem können in RFIDs Sensoren zur Protokollierung von Umgebungsbedingungen und kryptographische Coprozessoren, die noch komplexere Sicherheitsalgorithmen ermöglichen, integriert sein. Die Kryptofunktionen ermöglichen komplexe Authentifizierungs- und Verschlüsselungsverfahren.

Eigenschaft	AKTIV	PASSIV
Bauform	Groß	Klein
Gewicht	Groß	Gering
Sendereichweite	Groß	Gering
Speicherplatz	Groß	Gering
Anschaffungspreis	Hoch	Gering
Wartungsaufwand	Hoch	Gering
Mehrfach beschreibbar	Ja	Evt.

Abbildung 3: Aktive vs. Passive Transponder



Abbildung 4: Größenvorstellung: 50 kleine RFID-Chips; Quelle: <http://2004clcc.blogspot.com>

<sup>4</sup> Quelle: „RFID-Handbuch“, Klaus Finkenzeller und „Studie 6: Prozessoptimierung durch eingebettete Technologien für Endprodukte“, FH Salzburg

<sup>5</sup> Quelle: RFID-Journal: „RFID Energieversorgung“; <http://www.rfid-journal.de/rfid-energieversorgung.html>

## 2.2 Kommunikation <sup>6</sup>

Die Kommunikation erfolgt per Funk, wobei das Lesegerät die Existenz des Tags durch eine Veränderung im Feld detektiert und gegebenenfalls Daten abfragt oder andere Vorgänge anweist. Bei RFIDs für niedrige Frequenzbereiche ab 125 KHz stehen lange Übertragungszeiten und geringe Reichweiten einem vergleichsweise günstigen Anschaffungspreis und der Einbindung einer „Sollbruchstelle“ mittels eines starken Magnetfeldes zur Deaktivierung gegenüber. In hohen Frequenzbereichen (bis etwa 2,4 GHz) steigt neben Reichweite (bis zu 30 Meter) und Lesegeschwindigkeit auch der Preis.<sup>7</sup>

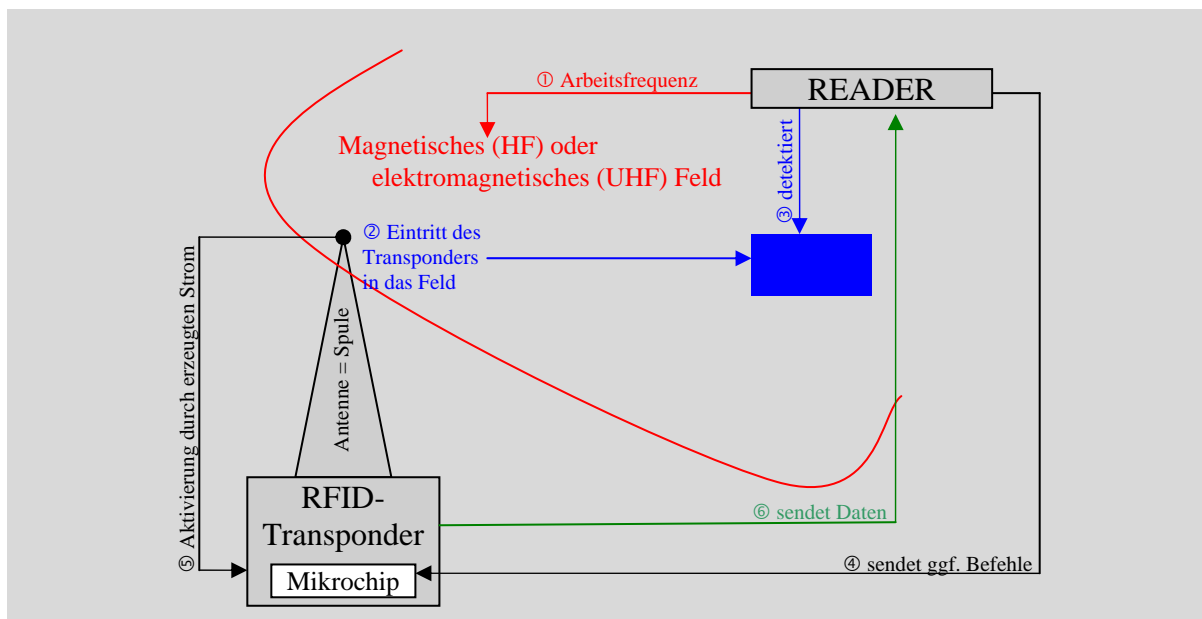


Abbildung 5: Grundlegende Funktionsweise der Kommunikation zwischen Lesegerät und RFID-Transponder

Das Lesegerät startet den Auslesevorgang durch das Ausstrahlen einer Hochfrequenz der passenden Wellenlänge, die von der Antenne des RFID empfangen, und somit eine Spannung induziert wird. Passive Tags nutzen diese Spannung, um die Antwort zu senden. Aktive RFID hingegen können mit größerer Leistung antworten und längere Operationen im Chip ablaufen lassen. Befinden sich mehrere RFIDs im Lesebereich, können Kollisionen der Antworten durch das Tree-Walking-, Aloha- oder Slotted Aloha-Verfahren vermieden werden<sup>8</sup>.

Beim Tree-Walking-Verfahren erfolgt eine Teilung und Abfrage des möglichen Wertebereiches der Nummern solange bis jedes Intervall kollisionsfrei ist. Das Aloha-Verfahren basiert auf der Anweisung, mit unterschiedlicher Zeitverzögerung zu antworten, bis das Lesegerät den erfolgreichen Empfang bestätigt und der Chip schweigt. Beim Slotted-Aloha-Verfahren teilt das Lesegerät auch eine Anzahl von gleichgroßen zeitlichen Slots mit,

<sup>6</sup> Quelle: RFID-Journal: „RFID-Technik“; <http://www.rfid-journal.de/rfid-technik.html>, „Übertragungsfrequenzen“; <http://www.rfid-journal.de/rfid-uebertragungsfrequenzen.html>

<sup>7</sup> Quelle: Geschichte Lexikon: „Radio Frequency Identification“; <http://www.geschichteboard.de/lexikon/RFID,information.htm>

<sup>8</sup> Quelle: Klaus Finkenzeller: „RFID Handbuch“

von denen jeweils einer für die Antwort genutzt und somit die Überlappung von Antworten vermieden wird. Wenn es sich um einfache Tags handelt, die keine eigenen Operationen ausführen können, sind diese Verfahren allerdings nicht anwendbar, da diese kontinuierlich ihre gespeicherten Daten senden, sobald und solange die dafür nötige Energie durch das vom Lesegerät ausgestrahlte Feld verfügbar ist, und nicht auf konkrete Anweisungen des Lesegerätes reagieren können.

### **2.3 Datenspeicherung**<sup>9</sup>

Die Speicherkapazität im Chip beginnt bei einfachen Transpondern bei 1 Bit, wobei allerdings nur deren Anwesenheit detektiert werden kann. Weitere Daten können entweder in einem zusätzlichen Speicher auf dem Chip selbst gespeichert werden, so dass diese jederzeit und überall offline verfügbar sind, oder es erfolgt eine externe Speicherung in einer angeschlossenen Datenbank.

Beim ROMs, die in der Regel über 96 oder mehr Bit Kapazität verfügen, werden die Daten bei der Herstellung der Chips integriert und können im Nachhinein nicht mehr verändert werden. Eine Erweiterung stellen die so genannten Write-Once-Read-Many-Tags (WORM) dar, die vom Nutzer einmalig mit Hilfe des Lesegerätes beschrieben, die Daten danach aber ebenfalls nicht mehr verändert werden können.

RW-Tags verfügen über einen bis zu 100.000fach wiederbeschreibbaren Electrically Erasable Programmable Read Only Memory (EEPROM) und unterstützen neben Antikollisions- auch einfache Authentifizierungs- und Verschlüsselungsverfahren. Verfügt der Chip über ein Betriebssystem, so ist dieses vom Hersteller fest eingebracht worden. Die Implementierung der entsprechenden Anwendungen kann später flexibel vom Nutzer durchgeführt werden.

---

<sup>9</sup> Quellen: „Studie 6: Prozessoptimierung durch eingebettete Technologien für Endprodukte“, FH Salzburg, <http://esycs.salzburgresearch.at/doc/rfid-studie-final.pdf>;

Claus Mauricio Lahner: „Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen“, Abschlussarbeit zur Erlangung des Grades LL.M. (Master of Laws), Universität Hannover  
<http://www.rechtsanwaltlahner.de/web-content/RFID.pdf> (16.07.2004)

## 3 Datensicherheit

### 3.1 Rechtliche Grundlagen

Der Schutz der Daten ist bei der Möglichkeit des berührungslosen Auslesens natürlich sowohl für Hersteller und Anwender als auch für diejenigen, deren Daten gespeichert werden von großer Bedeutung. Grundlage dafür sind neben dem Recht auf informationelle Selbstbestimmung<sup>10</sup> das Bundesdatenschutzgesetz sowie die ergänzenden Datenschutzgesetze der einzelnen Bundesländer, deren Ziel es ist, „den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“<sup>11</sup>. Diese Gesetze finden immer dann Anwendung, wenn personenbezogene Daten durch öffentliche Stellen des Bundes oder der Länder bzw. nicht-öffentliche Stellen zu gewerblichen Zwecken erhoben, verarbeitet oder genutzt werden. Dabei sind personenbezogene Daten im Sinne des §3 dieses Gesetzes solche Daten, die „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmaren natürlichen Person“ sind. Das Verarbeiten wird im §2 BDSG als „Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten“ definiert, was nach §4 BDSG nur dann zulässig ist, wenn „dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat“. Nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen ist es gestattet, Daten zu übermitteln oder zu nutzen, „wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel, akademische Grade, Anschrift, Geburtsjahr beschränken“<sup>12</sup> und der Betroffene dem nicht widersprochen hat. In der Anlage zu §9 werden weiterhin Regelungen zur automatisierten Verarbeitung personenbezogener Daten und die entsprechende Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags-, Transport- und Organisationskontrolle getroffen. Entsprechend müssen bei der Nutzung von RFID-Systemen die folgenden Punkte beachtet werden, wenn eine Verarbeitung personenbezogener Daten stattfindet:

Zugangskontrolle:                   Kein Unbefugter darf Zugang zu den entsprechenden Datenverarbeitungsanlagen erhalten. Das heißt, die dem RFID-

---

<sup>10</sup> Teil des allgemeinen Persönlichkeitsrechts, das nicht explizit im Grundgesetz Erwähnung findet

<sup>11</sup> §1 BDSG

<sup>12</sup> § 28(2) BDSG

- System zugrunde liegende Technik (z.B. Lesegerät bei der Passkontrolle) darf physisch nur für Autorisierte zugänglich sein.
- Datenträgerkontrolle:** Die Datenträger sind so zu schützen, dass sie nicht „unbefugt gelesen, kopiert, verändert oder entfernt werden können“. Die RFID-Tags und eine gegebenenfalls angeschlossene Datenbank sind mit Hilfe geeigneter Methoden vor missbräuchlicher Nutzung zu schützen.
- Speicherkontrolle:** Unbefugte dürfen keinen Zugriff auf den Speicher erhalten, um Daten einzugeben, zu verändern oder zu löschen. Der Zugriff auf die Daten muss generell unterbunden werden, wenn keine Berechtigung dafür vorliegt, was insbesondere bei der berührungslosen Kommunikation der RFID-Systeme von großer Bedeutung ist.
- Benutzerkontrolle:** Die Datenverarbeitungssysteme dürfen auch „mit Hilfe von Einrichtungen zur Datenübertragung [nicht] von Unbefugten genutzt werden können“. Das System darf nur von Befugten benutzt werden. Eine unerwünschte, unter Umständen sogar unbemerkte Kommunikation ist auszuschließen.
- Zugriffskontrolle:** Zur Benutzung der Datenverarbeitungssysteme Berechtigte dürfen nur entsprechend ihrer Zugriffsberechtigung auf die Daten zugreifen können. Die Einrichtung von nutzerabhängigen Zugriffsprofilen (z.B. für verschiedene Lesegeräte) muss möglich sein, um zu differenzieren, wer auf welche Daten zugreifen kann.
- Übermittlungskontrolle:** Eine Kontrolle, wohin Daten übermittelt werden können, muss möglich sein. Werden Daten wie bei RFID-Systemen berührungslos übertragen, muss festgestellt werden können, wohin sie übermittelt werden.
- Eingabekontrolle:** Es muss im Nachhinein nachvollzogen werden können, wann welche Daten eingegeben hat. Bei wiederbeschreibbaren RFID-Chips und den angeschlossenen Datenbanken muss

- kontrolliert werden können, wer (Schreibgerät, Person bei Datenbank) wann welche Daten geändert hat.
- Auftragskontrolle:** Wenn personenbezogenen Daten im Auftrag verarbeitet werden, müssen die Anweisungen des Auftraggebers befolgt werden.
- Transportkontrolle:** Werden personenbezogenen Daten übermittelt oder das Speichermedium transportiert, muss unbefugtes Lesen, Kopieren, Verändern oder Löschen verhindert werden. Da RFID-Tags (zumeist) permanenten Ortsveränderungen unterliegen und baulich dafür geschaffen sind, Daten zu übermitteln, muss insbesondere auf die Transportkontrolle geachtet werden, wenn personenbezogene Daten gespeichert wurden.
- Organisationskontrolle:** Die Organisation von Daten verarbeitenden Behörden und Betrieben ist „so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird“. Die Organisationskontrolle zielt insbesondere darauf, Strukturen zu schaffen, die einen möglichen Missbrauch personenbezogener Daten verhindern.

Weltweit geltende Standards zum Datenschutz bei RFID-Systemen existieren derzeit nicht.

## **3.2 Mögliche Angriffe auf RFID-Systeme**

### **3.2.1 Unerwünschtes Auslesen der Daten**

Da RFID-Systeme berührungslos kommunizieren, kann es theoretisch jederzeit zu einer Abfrage der auf dem Chip gespeicherten Daten kommen. Eine Lösung für dieses Problem stellt einerseits eine ausschließlich authentifizierte und verschlüsselte Datenübertragung dar. Dabei kommt es allerdings im Wesentlichen auf die Sicherheit der verwendeten Verfahren an. Problematisch ist auch eine mögliche Unwissenheit über angebrachte RFIDs – beispielsweise an Konsumgütern, beziehungsweise eine nicht erfolgreiche Deaktivierung, so dass (weiterhin) Daten gesendet werden können, ohne dass der „Träger“ dies bemerkt.

### 3.2.2 Abhören am Chip <sup>13</sup>

Die Strahlung des RFID-Chips abzuhören, stellt ein weiteres Angriffsszenario dar, bei dem Daten womöglich im Klartext mitgehört oder woraus Rückschlüsse über den verwendeten Schlüssel gezogen werden könnten. Damit kann es möglich sein, diesen leichter ausfindig zu machen. In ihrem Versuch konnten Thomas Finke und Harald Kelter die Kommunikation zwischen Transponder und Lesegerät in einigen Metern Entfernung passiv mithören. Um das System gegen solche Angriffe zu schützen, können Detektoren eingesetzt werden, die derartige Attacken melden und die Daten gegebenenfalls löschen.

### 3.2.3 Buffer Overflows <sup>14</sup>

Beim Pufferüberlauf werden Datenmengen in einen dafür zu kleinen Speicher geschrieben. Infolge dessen kommt es zum Überschreiben der originären Daten. Diese Sicherheitslücke kann zum Beispiel dafür genutzt werden, einen Zugang zum System zu erhalten und auf die gespeicherten Daten zugreifen zu können. Um solche „Buffer Overflows“ zu vermeiden, muss bei der Programmierung auf die Überwachung der Speicherbereichsgrenzen geachtet werden.

### 3.2.4 Unwissentliches Senden von Daten

Da RFID-Chips mittlerweile sehr klein sind und problemlos in verschiedenste Güter integriert werden können<sup>15</sup>, kann man sie unter Umständen unbemerkt mit sich herumtragen<sup>16</sup>. Dieser Aspekt darf keinesfalls vernachlässigt werden, insbesondere da diese Technologie immer stärker Einzug in die Warenketten hält. Einen Schutz davor gibt es im eigentlichen Sinn nicht: Ein Nachfragen an der Kasse beispielsweise ist möglich, erfordert aber Personal, das mit dieser Thematik vertraut ist. Auch ein „Absuchen“ mit den entsprechenden (kompatiblen!) Lesegeräten<sup>17</sup> kann erfolgen, allerdings erfordert das einen nicht zu unterschätzenden Aufwand, da die Reichweite insbesondere der im Handel eingesetzten passiven Tags sehr gering ist.

---

<sup>13</sup> Quelle: Thomas Finke, Harald Kelter: „Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems“  
[http://www.bsi.de/fachthem/rfid/Abh\\_RFID.pdf](http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf)

<sup>14</sup> Quelle: Stephan Kallnik, Daniel Pape, Daniel Schröter, Stefan Strobel: „Das Sicherheitsloch. Buffer-Overflows und wie man sich davor schützt“; c't 23/2001, S. 216 - 218

<sup>15</sup> z.B. textile Etiketten: dünne waschbare Tags von Texas Instruments

<sup>16</sup> Quelle: RFID-Journal: „RFID Datenschutz“, <http://www.rfid-journal.de/rfid-bedenken.html>

<sup>17</sup> RFID-Reader sind mittlerweile z.B. als Handyzusatzmodul (Siemens, Nokia) erhältlich;

Quelle: Susanne Schwonbeck: „Chipmania. Wirtschaftlichkeit contra Datenschutz“; iX 05/2004, S.12 – 14

### **3.3. Unterbindung unerwünschter Datenübertragung**

#### **3.3.1 Deaktivierung der RFID-Chips<sup>18</sup>**

Um ein (unerwünschtes) Auslesen der RFID-Tags zu unterbinden, können diese nach der Nutzung – so zum Beispiel nach dem Zahlungsvorgang an der Kasse – deaktiviert werden. Mithilfe eines HF-Feldes können vorhandene Sollbruchstellen im Tag durchgebrannt werden. Es besteht außerdem die Möglichkeit, den Chip durch Überschreibung zu deaktivieren. Beides ist im Nachhinein – zum Beispiel vom Käufer – allerdings nicht nachvollziehbar.

#### **3.3.2 Abschirmung der RFID-Chips**

Eine Abschirmung der Tags erfolgt entweder durch metallische Gegenstände – zum Beispiel Metallfolie<sup>19</sup> – oder durch Störsignale, die von so genannten „Blockade RFIDs“<sup>20</sup> ausgesendet werden und die Antwort des abgefragten Tags stören. Dabei kommt entweder das Tree-Walking-Verfahren, bei dem die Blockade RFIDs bei jedem Nummernbereich antworten und so zu Milliarden von möglichen Abfragen führen, oder das Aloha-Verfahren zum Einsatz, das in diesem Fall nicht zu einem bestimmten Zeitpunkt sondern im kompletten Zeitfenster für mögliche Antworten sendet, somit allerdings auch sehr viel mehr Energie benötigt.

#### **3.3.3 Frequenzhopping**

Eine größere Sicherheit bietet auch das Frequenzhopping, also das Wechseln der Kommunikationsfrequenz während der Datenübertragung, was ein Abhören erschwert. Allerdings müssen sowohl der RFID-Chip selbst als auch das Lesegerät dafür ausgelegt sein.

#### **3.3.4 Passwortschutz<sup>21</sup>**

Der Schreib- bzw. Lesezugriff kann gegebenenfalls erst nach Übermittlung eines Passwortes ermöglicht werden. Wenn die Kommunikation dieses Passwortes unverschlüsselt erfolgt, sollte es aber vom Chip zum Lesegerät gesendet werden, da aufgrund der geringeren Leistung

---

<sup>18</sup> Quelle: Bundesamt für Sicherheit in der Informationstechnik: „Risiken und Chancen des Einsatzes von RFID-Systemen Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit“  
<http://www.bsi.de/fachthem/rfid/RIKCHA.pdf>

<sup>19</sup> Quelle: „Studie 6: Prozessoptimierung durch eingebettete Technologien für Endprodukte“, FH Salzburg,  
<http://esycs.salzburgresearch.at/doc/rfid-studie-final.pdf>

<sup>20</sup> z.B. Blocker Tag von RSA Security; [http://www.rsasecurity.com/press\\_release.asp?doc\\_id=4233&id=2675](http://www.rsasecurity.com/press_release.asp?doc_id=4233&id=2675)

<sup>21</sup> vgl. Kapitel 3.4

nur eine kürzere Reichweite erzielt wird und somit die ungewollte Kenntnisnahme Dritter zumindest erschwert wird.

### 3.3.5 Blockieren der RFID-Chips

RFIDs können so konfiguriert werden, dass es bei der Übermittlung eines falschen Passwortes zum Blockieren des Schreibzugriffs kommt<sup>22</sup>. In ähnlicher Weise kann ein „Kill“-Befehl<sup>23</sup> implementiert werden, nach dessen Ausführung ein Transponder keine weiteren Aktionen durchführt.

### 3.3.6 Verwendung einer angeschlossenen Datenbank

Eine andere Möglichkeit bietet die externe Speicherung der Daten in einer separaten Datenbank, auf die nur bestimmte Nutzer differenzierte Zugriffsrechte haben. Damit kann erst mit Hilfe der Chip-ID und ggf. nach erfolgreicher Authentifizierung auf die entsprechenden Daten zugegriffen werden. Ohne verschlüsselte Kommunikation könnte allerdings trotzdem die weltweit einmalige ID des Chips mitgehört oder unwissentlich ausgelesen werden, und unter Umständen Rückschlüsse auf sensible Daten zulassen.

## 3.4 Sichere Datenübertragung<sup>24</sup>

Bei den meisten RFID-Systemen werden die Daten heute noch unverschlüsselt übertragen<sup>25</sup>. Es gibt aber einige Möglichkeiten, diese Daten zu schützen:

Einerseits ist die Speicherung von ausschließlich verschlüsselten Daten möglich. Dabei besteht allerdings das Problem, dass die Kommunikation zwischen Chip und Lesegerät belauscht und damit die Steuerbefehle abgehört werden können. Schutz vor Manipulation der gesendeten Daten bietet die Übermittlung eines so genannten Fingerabdrucks, einer Zahl, die aus der Nachricht selbst erstellt wird.

Eine weiteres Verfahren der Datensicherheit bei der Datenübertragung stellt „Challenge Response“, ein symmetrisches Authentifizierungsverfahren, dar. Dabei wird zunächst eine

---

<sup>22</sup> Quelle: Torsten Roth: „Informationssicherheitsverfahren von RFID-Transpondern“, [http://www.sigs.de/publications/os/2005/rfid/roth\\_OS\\_rfid\\_05.pdf](http://www.sigs.de/publications/os/2005/rfid/roth_OS_rfid_05.pdf) (2005)

<sup>23</sup> Quelle: Heise online: „Metro zeigt RFID auf der CeBIT“, <http://www.heise.de/newsticker/meldung/68313> (13.01.2006)

<sup>24</sup> Quelle: Torsten Roth: „Informationssicherheitsverfahren von RFID-Transpondern“, [http://www.sigs.de/publications/os/2005/rfid/roth\\_OS\\_rfid\\_05.pdf](http://www.sigs.de/publications/os/2005/rfid/roth_OS_rfid_05.pdf) (2005)

<sup>25</sup> Quelle: „Studie 6: Prozessoptimierung durch eingebettete Technologien für Endprodukte“, FH Salzburg, <http://esyics.salzburgresearch.at/doc/rfid-studie-final.pdf>

Zufallszahl im Klartext übertragen und gemeinsam mit einer weiteren Zufallszahl verschlüsselt zurückgesendet. Wird der Schlüssel als korrekt erkannt, muss nur noch die zweite Zufallszahl übermittelt werden, um sich so für die Kommunikation zu autorisieren. Da die Enthüllung dieses Schlüssels das gesamte System gefährden würde, kann im Chip ein aus der Transponder-ID und Masterschlüssel abgeleiteter Schlüssel gespeichert werden, den das Lesegerät beim Zugriff selbst errechnet und somit während der Kommunikation die einzige Quelle des Masterschlüssels ist.

Möglich ist auch die Nutzung von Meta-IDs, was die Verfolgung von Transpondern verhindern soll: Dabei sendet der Chip eine von seiner eigentlichen ID abgewandelte – im Idealfall bei jedem Auslesevorgang verschiedene – Meta-ID an das Lesegerät, das wiederum alle im Lesebereich möglichen IDs kennt und aufgrund der Meta-ID darauf zurück schließen kann. Wegen des großen Datenvolumens sollte dieses Verfahren allerdings nur bei Systemen mit einer ausreichend kleinen Anzahl an Transpondern angewandt werden.

Bei allen Verschlüsselungsverfahren ist der Schlüssel die schwächste Stelle des Systems und muss dementsprechend sorgfältig ausgewählt und sicher verwahrt werden.

### 3.4.1 Symmetrische Verschlüsselung <sup>26</sup>

Bei der symmetrischen Verschlüsselung, die bei RFID-Systemen am weitesten verbreitet ist, benutzen Sender und Empfänger den gleichen Schlüssel, um daraus einen Schlüssel zur Ver- und Entschlüsselung zu generieren, so dass die Übertragung einerseits sehr schnell erfolgen kann, andererseits das Problem der sicheren Kommunikation des Schlüssels und der Ableitbarkeit des Dechiffrier- aus dem Chiffrierschlüssel selbst besteht. Am weitesten verbreitet sind dabei DES bzw. 3DES.

Bei *Monoalphabetischen Substitutionschiffren* wird je ein Zeichen des Klartextes durch ein Geheimzeichen ersetzt. Der Schlüssel kann frei gestaltet werden, muss aber eindeutig sein, also jedem (möglichen) Klartextzeichen genau ein Geheimzeichen zuordnen. Die Entschlüsselung kann mithilfe einer Häufigkeitsanalyse sehr schnell erfolgreich verlaufen. Beispiele für monoalphabetische Substitutionschiffren sind Atbash, Caesar-Chiffre, Nomenklatur, Polybioschiffre und der so genannte TELWA-Code, der im Zweiten Weltkrieg von den Alliierten eingesetzt und von deutschen Kryptoanalytikern entschlüsselt wurde.

---

<sup>26</sup> Quelle: BSI: „Verschlüsselungsverfahren“; [http://www.bsi-fuer-buerger.de/schuetzen/07\\_0301.htm](http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm)

Die ***Polyalphabetische Substitution*** verwendet mehrere Geheimentextalphabete, wobei die Positionen der einzelnen Buchstaben des Schlüssels im Alphabet die Verschiebung der Klartextbuchstaben bestimmen. Dieses Verfahren stellt eine erweiterte Caesar-Chiffrierung dar und findet Anwendung bei der Vigenère- und Autokeyverschlüsselung, aber auch die im Zweiten Weltkrieg eingesetzte Enigma bediente sich der Polyalphabetischen Substitution.

Im Gegensatz dazu werden die Zeichen bei der ***Transposition*** nicht umgewandelt sondern lediglich in ihrer Position vertauscht, indem der Text nach einer durch den Schlüssel bestimmten Anzahl von Zeichen umgebrochen und untereinander geschrieben wird, und das Auslesen der Spalten den Geheimtext ergibt. Die Skytale ist das wohl älteste militärische Verschlüsselungsverfahren, bei dem sich schon die Spartaner eines Holzstabes – der so genannten Skytale – bedienten, um den ein Lederstreifen spiralförmig gewickelt und entlang des Stabes beschrieben wurde. In diesem Fall stellte der Skytale-Durchmesser den Schlüssel zur Entschlüsselung der Geheimnachricht dar.

Bei der ***Blockverschlüsselung*** werden die zu verschlüsselnden Daten in gleich große Blöcke geteilt – der letzte muss gegebenenfalls aufgefüllt werden, um die entsprechende Länge zu erreichen – und dann nacheinander verschlüsselt, wobei das Ergebnis der Verschlüsselung in den Schlüssel des nächsten Blocks mit einfließen kann. Heute finden häufig 64- und 128-Bit Blöcke mit einem 128- oder 256-Bit-Schlüssel Anwendung, zum Beispiel beim Data Encryption Standard und Advanced Encryption Standard<sup>27</sup>.

Im Gegensatz zur Blockverschlüsselung arbeitet die ***Stromverschlüsselung*** kontinuierlich und „übersetzt“ jedes einzelne übertragene Bit. Da nicht gewartet werden muss, bis ein entsprechend großer Block zu ver- bzw. entschlüsseln ist, bietet dieses Verfahren eine sehr schnelle Arbeitsweise. Dabei wird der Geheimtext durch eine XOR-Verknüpfung von Klartext und eines aus dem geheimen Schlüssel erzeugten Schlüsselstroms generiert und auf Empfängerseite durch eine erneute XOR-Verknüpfung wieder dechiffriert. Der Schlüsselstrom sollte eine Pseudozufallsfolge mit einer möglichst geringen Systematik sein, um eine entsprechende Sicherheit bieten zu können. Im Idealfall ist der Schlüssel ein One-Time-Pad, der keinerlei statistischen Abhängigkeiten aufweist und nur einmal verwendet wird. Dabei stellt sich aber wiederum das Problem der sicheren Übertragung des Schlüssels, da beide Kommunikationspartner denselben, aber bei jeder Kommunikation neuen Schlüssel verwenden müssen.

---

<sup>27</sup> Nähere Erläuterung im Kapitel 3.4.4

### 3.4.2 Asymmetrische Verschlüsselung<sup>28</sup>

Bei den asymmetrischen Verfahren werden die Daten mit einem bekannten öffentlichen Schlüssel verschlüsselt, um dann mithilfe des korrespondierenden (geheimen) privaten Schlüssels wieder decodiert zu werden. Somit erfordern diese Vorgänge mehr Zeit als die symmetrische Verschlüsselung, weswegen diese Verfahren selten bei RFID-Systemen zum Einsatz kommen. Beispiele dafür sind RSA und ECC<sup>29</sup>.

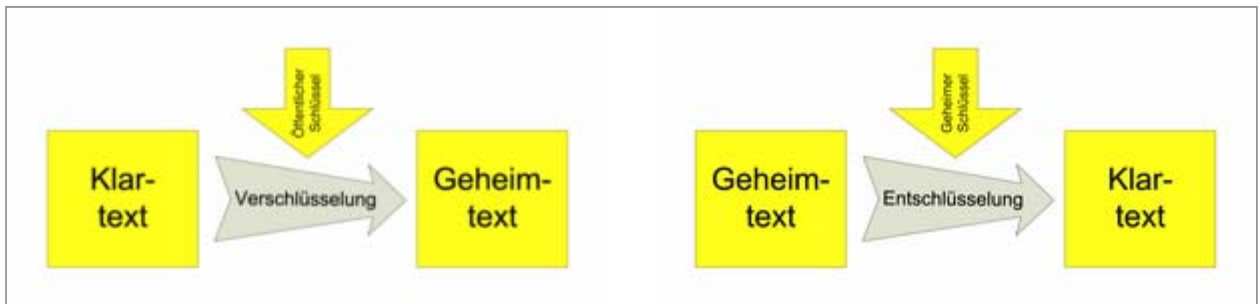


Abbildung 6: Prinzip des asymmetrischen Verfahrens. [www.wikipedia.de](http://www.wikipedia.de); Asymmetrisches Kryptosystem

### 3.4.3 Hybridverfahren<sup>30</sup>

Einen Kompromiss zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren stellen die Hybriden Verschlüsselungsverfahren dar, die den Schlüssel asymmetrisch übertragen, um diesen bei einer symmetrisch verschlüsselten Datenübertragung zu verwenden und somit die Vorteile der beiden Verschlüsselungsverfahren zu vereinen.

Ein Verfahren, um den Schlüssel über unsichere Medien zu übertragen, ist der 1976 veröffentlichte Diffie-Hellman-Schlüsselaustausch, bei dem zunächst eine Primzahl und eine Primitivwurzel, die über unsichere Kanäle kommuniziert werden können, sowie von jedem der beiden Kommunikationsteilnehmer jeweils eine geheim zu haltende Zufallszahl festgelegt werden. Berechnungen mit diesen Variablen führen auf beiden Seiten zu verschiedenen Ergebnissen, die wiederum (unsicher) übertragen werden und mithilfe weiterer Berechnungen mit den (geheimen) Zufallszahlen auf beiden Seiten zum gleichen Resultat führen, das letztendlich als Schlüssel für die weitere Kommunikation verwendet wird. Gegen passives Abhören gilt dieses Verfahren als sicher, da der Schlüssel nicht aus den (im Klartext) verschickten Informationen abgeleitet werden kann. Der Grund dafür ist die aufwändige Berechnung des diskreten Logarithmus einer (in der Praxis) sehr großen Zahl, die hier durch das Potenzieren der Variablen entsteht.

<sup>28</sup> Quelle: BSI: „Verschlüsselungsverfahren“; [http://www.bsi-fuer-buerger.de/schuetzen/07\\_0301.htm](http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm)

<sup>29</sup> vgl. Kapitel 3.4

<sup>30</sup> Quelle: BSI: „Verschlüsselungsverfahren“; [http://www.bsi-fuer-buerger.de/schuetzen/07\\_0301.htm](http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm)

	Symmetrisch	Hybrid	Asymmetrisch
Schlüssel Sender → Verschlüsseln	nur 1 Schlüssel	nur 1 Schlüssel	Öffentlicher Schlüssel
Schlüssel Empfänger → Entschlüsseln			Privater Schlüssel
Geheimzuhaltende Schlüssel	für jeden Teilnehmer	Private Schlüssel	Privater Schlüssel
Übertragung Schlüssel	sicher	asynchron	Privater: sicher Öffentlicher ist zugänglich
Ver-/Entschlüsselungs- geschwindigkeit	schnell	schnell	langsam
Angriffsmöglichkeiten	Brute-Force-Attack		Mittelsmann-Angriff
Lösungsmöglichkeit	Längerer Schlüssel ohne logischen Zusammenhang zwischen den einzelnen Zeichen		Authentifizierung, Signieren, Kontrolle des öffentlichen Schlüssels durch Nachfrage bei einer zentralen Schlüsselverwaltung

Abbildung 7: Symmetrische vs. Asymmetrische vs. Hybridverfahren

### 3.4.4 Verschlüsselungsalgorithmen im Detail <sup>31</sup>

#### 3.4.4.1 DES - Data Encryption Standard 1974

Beim 1974 von IBM entwickelten Data Encryption Standard handelt es sich um ein symmetrisches blockweises (64 Bits) Verfahren mit einem 56-Bit-langen Schlüssel. DES wurde für eine öffentliche Ausschreibung entwickelt, deren Ziel ein einheitlicher Standardverschlüsselungsalgorithmus war. Nachdem DES bereits 1977 als offizieller Standard für die Bundesbehörden der USA eingeführt wurde, folgte die Anerkennung für den privaten Sektor im Jahr 1981. Bei GOST handelt es sich um das in der ehemaligen Sowjetunion entwickelte Pendant zu DES. Nachdem Zweifel über die Sicherheit des Standards aufkamen und bereits am Nachfolger EAS gearbeitet wurde, konnte die Electronic Frontier Foundation 1998 mit Hilfe eines Brute-Force-Angriffs binnen weniger Stunden einen Schlüssel berechnen<sup>32</sup>.

DES wird vor allem bei Geldautomaten, aber auch bei RFID-Systemen eingesetzt.

#### 3.4.4.2 Triple-DES

Hierbei handelt es sich um eine Ableitung des DES-Verfahrens, das auch Encrypt-Decrypt-Encrypt (EDE) oder 3DES genannt wird. Die Schlüssellänge beträgt  $3 \cdot 56 = 168$  Bit. Offiziell wurde DES im Oktober 2000 aber durch AES ersetzt, das sich in einem neuerlichen

<sup>31</sup> Quelle: WIKIPEDIA: „Kryptologie“; [http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt\\_Kryptologie](http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie)

<sup>32</sup> Quelle: Heise online: „Data Encryption Standard hat ausgedient“ (15.09.2001)

Wettbewerb durchsetzen konnte. Trotzdem gehört 3DES zu den bei RFID-Systemen gebräuchlichsten Verschlüsselungsalgorithmen.

#### **3.4.4.3 RSA - Rivest, Shamir und Adleman 1977**

Aus dem Problem der sicheren Übertragung des Schlüssels zwischen den teilweise weit entfernten Kommunikationspartnern, entwickelten sich asymmetrische Verschlüsselungssysteme, zu denen auch RSA gezählt wird. Da diese Verfahren aber relativ langsam arbeiten, werden zur Verschlüsselung größerer Datenmengen hauptsächlich symmetrische Verfahren eingesetzt, die – als Hybridverfahren – gegebenenfalls durch asymmetrische Verfahren initialisiert werden. RSA bedient sich eines Produkts aus zwei (genügend großen) Primzahlen als Teil des öffentlichen Schlüssels, von dem aus weder mit dem heutigen mathematischen Wissensstand noch mithilfe der heute verfügbaren Technik in ausreichender Zeit auf die originären Primzahlen zu schließen ist. Anwendung findet RSA beispielsweise bei verschiedensten technischen Kommunikationsformen (Internet, Telefonie, Email) und bei der Authentifizierung französischer Telefonkarten.

#### **3.4.4.4 RC4 1987**

Bei RC4 handelt es sich um einen Stromchiffrierer, dessen Algorithmus bis 1994 geheim war. RC4 verfügt über eine variable Schlüssellänge (bis 2048 Bit), so dass er sicherer als DES ist. Seine Kompaktheit lässt es außerdem sehr viel schneller als DES arbeiten. Ein Beispiel für RC4 ist Wired Equivalent Privacy (WEP), das für WLAN genutzt, aber wegen seiner Schwachstellen durch Wi-Fi Protected Access (WPA) abgelöst wurde.

#### **3.4.4.5 IDEA 1990**

Der International Data Encryption Algorithm ist ein Blockchiffre mit einem 128-Bit-Schlüssel, der den symmetrischen Algorithmen zuzuordnen ist. Das Verfahren bedient sich der Kombination von drei verschiedenen Operationen und gilt somit als hinreichend sicher. Nur schwache Schlüssel stellen ein Sicherheitsrisiko dar, da sie mit relativ geringem Aufwand berechnet werden können. Die an der Entwicklung beteiligte Ascom Systec AG hält für diesen Algorithmus noch bis 2011 den Patentschutz in Europa.

#### **3.4.4.6 Blowfish 1993**

Der Blowfish-Algorithmus gehört ebenfalls zu den symmetrischen Blockchiffren und gilt als Ersatz für DES und IDEA. Das Verfahren ist sehr schnell und bietet eine variable Schlüssellänge zwischen 32 und 448 Bit. Nachdem der Blowfish-Algorithmus veröffentlicht wurde, konnten bis auf einige schwache Schlüssel keine weiteren Schwachstellen nachgewiesen werden. Eine Erweiterung stellt der 1996 entwickelte Cobra 128-Algorithmus dar, der eine variable Blocklänge und eine größere Anzahl an Verschlüsselungsrunden bietet.

#### **3.4.4.7 Cast 1996**

Cast gehört ebenfalls zu den symmetrischen Blockchiffren, arbeitet mit variablen Schlüssellängen von 40 – 128 Bits und ist zwei- bis dreimal schneller als DES, so dass dieser Algorithmus auch bei Echtzeitanwendungen eingesetzt werden kann. Cast konnte bis heute noch nicht gebrochen werden.

#### **3.4.4.8 Cayley-Purser-Algorithmus 1999**

Dieser Algorithmus benutzt einen 256-Bit langen Schlüssel und basiert auf der matrix-basierten Multiplikation und soll somit 22-mal schneller sein als RSA. Bisher konnten keine Schwachstellen dieses Algorithmus entdeckt werden.

#### **3.4.4.9 AES – Advanced Encryption Standard 2000**

Der Advanced Encryption Standard gehört ebenso zu den symmetrischen Blockchiffren und hat Ende 2000 DES, die Standard-Verschlüsselung in den USA, abgelöst, weil er aufgrund seiner Einfachheit und überdurchschnittlichen Performance überzeugen konnte. Sowohl die Blockgröße als auch die Schlüssellänge sind mit jeweils 128, 192 oder 256 Bit variabel.

Anwendung findet AES zum Beispiel beim Standard 802.11i für WLAN, Secure Shell und Skype.

### 3.4.5 Digitale Signaturverfahren

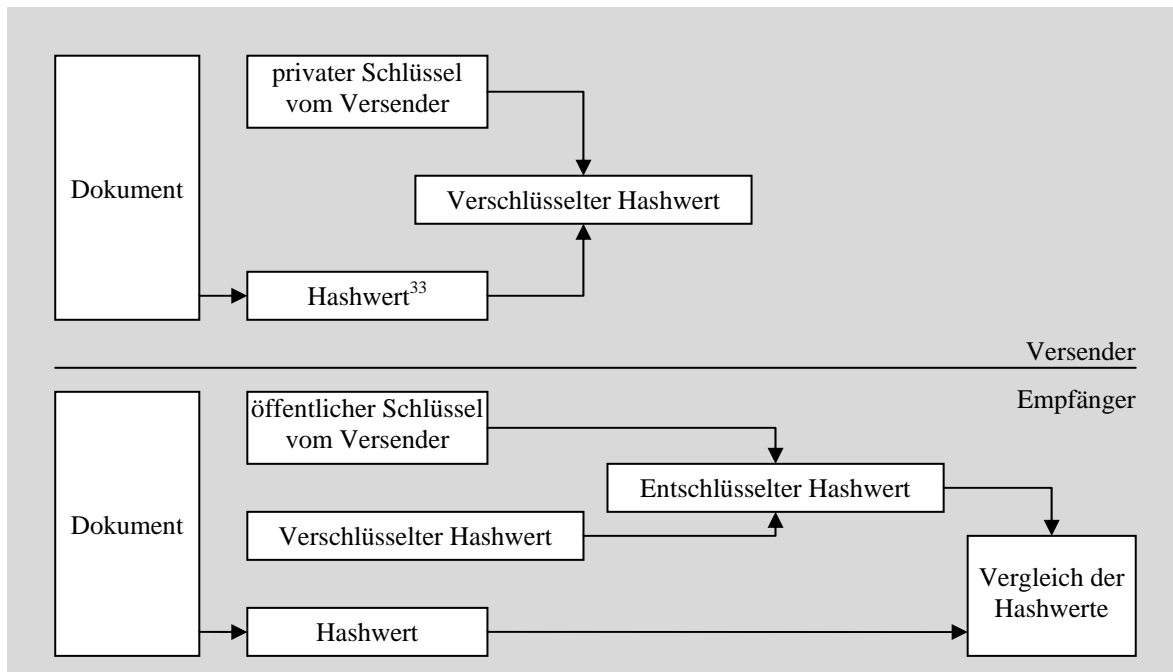


Abbildung 8: Elektronische Signatur; in Anlehnung an [www.wikipedia.de](http://www.wikipedia.de)

#### 3.4.5.1 S/MIME - Secure MIME – Trusted Mime <sup>34</sup>

MIME ist eine elektronische Unterschrift, die auf asymmetrischen Kryptoverfahren beruht, und stellt eine Ergänzung zu den gängigen Verschlüsselungsalgorithmen dar, um elektronische Informationen mit Hilfe einer digitalen Signatur abzusichern. Neben der Authentizität und der Integrität dieser Daten kann damit auch die Identität des Senders sichergestellt werden. Dabei wird die mit dem geheimen Schlüssel erzeugte Signatur mit dem öffentlichen Schlüssel kontrolliert.

#### 3.4.5.2 Digital Signature Algorithmus (DSA) <sup>35</sup>

DSA sollte hochsichere Signaturen anbieten, wenn bei einer Kommunikation keine Verschlüsselung angewendet werden kann oder darf. Allerdings hat sich das Verfahren aufgrund seiner geringen Geschwindigkeit als praxisuntauglich herausgestellt.

<sup>33</sup> Der Hashwert stellt den Fingerabdruck von Dateien bzw. Dateifragmenten dar, um diese eindeutig identifizieren zu können.

<sup>34</sup> Quelle: WIKIPEDIA: „Kryptologie“; [http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt\\_Kryptologie](http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie)

<sup>35</sup> Quelle: WIKIPEDIA: „Data Encryption Standard“; [http://de.wikipedia.org/wiki/Data\\_Encryption\\_Standard](http://de.wikipedia.org/wiki/Data_Encryption_Standard)

### 3.4.5.3 Elliptic Curve Digital Signature Algorithmus (ECDSA) <sup>36</sup>

ECDSA ist ein asymmetrisches digitales Signaturverfahren, bei dem der Nutzer authentische Kopien seines öffentlichen Schlüssels zur Verfügung stellt, mit denen seine mit dem privaten Schlüssel erstellten Signaturen verifiziert werden. Die zugrunde liegenden Algorithmen beruhen auf dem mathematischen Prinzip elliptischer Kurven, so dass wesentlich kürzere Schlüssel hinreichend sicher sind.

## 3.5 Datensicherheit bei der weitergehenden Verwendung der Daten

Die weitergehende Verwendung der gespeicherten und kommunizierten Daten stellt einen Sicherheitsaspekt dar, der nicht nur bei RFID-Systemen zu beachten ist, und insbesondere Anforderungen an die Benutzer stellt. In Deutschland ist dies nur rechtlich relevant, wenn diese Daten als personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes gelten<sup>37</sup>.

Fraglich ist hierbei, inwieweit eine weltweit einmalige ID zu den personenbezogenen Daten zu zählen ist, da sich damit beispielsweise bei Kundenkarten oder Zutrittskontrollsystemen Bewegungsprofile<sup>38</sup> generieren lassen könnten, Solche Profile widersprechen aber dem Grundsatz der informationellen Selbstbestimmung. Im Einzelhandel ist auch eine Verknüpfung der Daten zu Kundenprofilen<sup>39</sup> möglich, mit denen die Kunden im Folgenden individuell beworben werden könnten. Notwendig dafür sind lediglich mit RFID-Tags ausgestattete Produkte und das Bezahlen mit EC-Karte oder die Vorlage einer Kundenkarte.

Um die entsprechende Sicherheit von personenbezogenen Daten zu gewährleisten, muss bei der Implementierung von RFID-Systemen, bei denen solche Daten verarbeitet werden, insbesondere die Anlage zum §9 des Bundesdatenschutzgesetzes mit den Regelungen zur Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags-, Transport- und Organisationskontrolle Beachtung finden.

Die Hardware darf nur Befugten zugänglich sein und muss entsprechend sicher verwahrt werden. Der Zugang zu speziellen Lesegeräten, mit denen personenbezogene Daten spezieller RFID-Chips ausgelesen werden können, muss folglich kontrolliert und geschützt werden. Außerdem müssen diese Datenträger so beschaffen beziehungsweise geschützt sein, dass Unbefugte die Daten nicht verarbeiten können. Weiterhin sind abhängig von den einzelnen Aufgaben differenzierte Zugriffsberechtigungen zu vergeben und Veränderungen und

---

<sup>36</sup> Quelle: WIKIPEDIA: „Elliptische-Kurven-Kryptosystem“;  
<http://de.wikipedia.org/wiki/Elliptische-Kurven-Kryptosystem>

<sup>37</sup> vgl. Kapitel 3.1

<sup>38</sup> Quelle: RFID-Journal: “RFID Datenschutz” <http://www.rfid-journal.de/rfid-bedenken.html>

<sup>39</sup> Quelle: Susanne Schwonbeck: „Chipmania. Wirtschaftlichkeit contra Datenschutz“; iX 05/2004, S.12 – 14

Eingaben von Daten zu protokollieren, um diese nachvollziehbar zu gestalten. Die Zugriffsrechte sollten nach dem Minimalprinzip vergeben werden. Werden Daten durch Dritte verarbeitet, muss sichergestellt werden, dass diese ausschließlich gemäß den Anweisungen des Auftraggebers handeln. Auch die Organisation der Behörden und Betriebe, die personenbezogene Daten verarbeiten, müssen so gestaltet werden, dass sie diesen Anforderungen an den Datenschutz entsprechen. Personal, das mit der Verarbeitung personenbezogener Daten betraut ist, muss über die Aspekte zum Datenschutz unterwiesen werden. Wenn RFID-Systeme Anwendung finden, sollte auch auf die Verfahrensweise und die möglichen Gefahren hingewiesen werden, um einen fahrlässigen Umgang damit zu verhindern.

Die weitergehende Verwendung nicht-personenbezogener Daten bleibt rechtlich unberührt, insofern keine Verknüpfung zu personenbezogenen Daten hergestellt wird.

Neueste Entwicklungen zeigen aber datenschutzrechtlich bedenkliche Tendenzen auf:

Noch im Februar 2005 hat der deutsche Bundestag eine Vorratsdatenspeicherung abgelehnt, da die damit verbundene vorrätige Speicherung personenbezogener Daten dem Erforderlichkeitsgrundsatz widerspricht<sup>40</sup>. Trotzdem hat Deutschland im Dezember 2005 im EU-Parlament entgegen der Anträge der Opposition<sup>41</sup> für die Europäische Richtlinie zur Vorratsdatenspeicherung gestimmt<sup>42</sup> und erachtet die vorrätige Speicherung der Daten nun für verfassungskonform<sup>43</sup>. Insofern bleibt abzuwarten, inwieweit dies auch in Deutschland weitere mögliche Überwachungsszenarien wie die im Kapitel 4.4 vorgestellten Verkehrsüberwachungssysteme nach sich zieht.

---

<sup>40</sup> Quelle: Heise online: „Absprachen über Vorratsdatenspeicherung lösen Empörung aus“;  
<http://www.heise.de/newsticker/meldung/57507> (14.03.2005)

<sup>41</sup> Quelle: „Antrag. Freiheit des Telefonverkehrs vor Zwangsspeicherungen“;  
<http://dip.bundestag.de/btd/16/002/1600237.pdf> (14.12.2005)

<sup>42</sup> Quelle: Heise online: „EU-Parlament beschließt massive Überwachung der Telekommunikation“;  
<http://www.heise.de/newsticker/meldung/67358> (14.12.2005)

<sup>43</sup> Quelle: Heise online: „Große Koalition sieht Vorratsdatenspeicherung im Einklang mit der Verfassung“;  
<http://www.heise.de/newsticker/meldung/68951> (27.01.2006)

## 4 Praxis – Beispiele

### 4.1 Immobilizer

Bereits heute werden allein im Bereich der Wegfahrsperrungen Millionen von passiven RFID-Transpondern eingesetzt. Der geheime Verschlüsselungsalgorithmus im als „Immobilizer“ bezeichneten System von Texas Instruments konnte allerdings bereits im Januar 2005 von Forschern der John Hopkins University und RSA Security geknackt werden<sup>44</sup>. Der Hersteller reagierte drauf gelassen, da es in diesem Anwendungsbereich vor allem um niedrige Kosten und kurze Operationszeiten gehe. Eine Alternative, die für den Vorgang 3s statt 250ms benötigt sei deswegen von der Automobilindustrie nicht tragbar. Obwohl in die Entscheidung über die Nutzung von Alternativen auch wirtschaftliche Gründe hineinspielen, ist es fraglich inwieweit diese Meinung auch von den Nutzern geteilt wird.

### 4.2 Einzelhandel

Der derzeitige Weg führt in Richtung lückenloses Warenmanagement vom Zulieferer bis zum Konsumenten, um alle Vorgänge überwachen und ein optimiertes Bestandsmanagement realisieren zu können. Die dabei zum Einsatz kommenden RFID-Chips sollen nach dem Bezahlvorgang deaktiviert werden, was vom Käufer aber nicht (ohne Hilfsmittel) nachvollziehbar ist. Der Metrokonzern nimmt bei der Einführung der neuen Technologie eine Vorreiterrolle ein und will die bisher auf Palettenebene integrierten Chips bis 2007 auf Kartonebene zum Einsatz bringen<sup>45</sup>. Damit wird es möglich sein, den Warenbestand zum Beispiel mit Hilfe in den Boden eingelassener Lesegeräte zu überwachen. Bis die RFID-Tags allerdings den bekannten Barcode ablösen, wird es nach Schätzung von Gerd Wolfram, Geschäftsführer der Metro Group Information Technology (MGI), aber noch 5 bis 10 Jahre dauern. Bereits im Frühjahr 2004 hatte der Metrokonzern einen Vorstoß gewagt und Kundenkarten, die mit RFID-Chips ausgestattet waren, ausgegeben. Allerdings wurden diese auf Drängen vieler Datenschützer hin wieder zurückgenommen<sup>46</sup>. Problematisch erscheint in diesem Zusammenhang insbesondere die Möglichkeit, verschiedene personenbezogene Daten zusammenzuführen und Kundenprofile zu erstellen, wenngleich Metro dieses Vorhaben

---

<sup>44</sup> Quellen: Heise security: „Auto-Schlüssel mit unsicherem Schlüssel“, <http://www.heise.de/security/news/meldung/55729> (30.01.2005); „Hersteller: geknackte RFID-Verschlüsselung derzeit kein Problem“, <http://www.heise.de/security/news/meldung/57890> (24.03.2005)

<sup>45</sup> Quelle: Henry Steinhilber: „In der Standardisierungsfalle“ iX 03/2005, S.24

<sup>46</sup> Quelle: Heise online: „Metro zieht RFID-Karte zurück“; <http://www.heise.de/newsticker/meldung/45062> (27.02.2004)

zumindest derzeit von sich weist<sup>47</sup>. Auch die Kaufhof Warenhaus AG führt gemeinsam mit dem Zulieferer Gerry Weber ein Pilotprojekt zum RFID-Einsatz durch, wonach Prozesskosten von bis zu 11%<sup>48</sup> eingespart werden könnten.

### **4.3 Zutrittskontrolle**

Karten, die mit RFID ausgestattet sind, können vom Lesegerät – gegebenenfalls mit Hilfe der ID und einer entsprechenden Datenbankabfrage – in zu akzeptierende und abzuweisende Anfragen unterschieden werden. Damit lassen sich zum Beispiel Kontrollen für Mitarbeiter realisieren, die nur zu bestimmten Bereichen zutrittsberechtigt sind. Auch Skipässe sind zum Teil mit RFID-Chips bestückt, die die Nutzung der einzelnen Skilifte ermöglicht bzw. verweigert. Die Tickets werden dabei wieder verwendet und die jeweiligen Zugangsrechte und Zeiträume anhand der ID in einer Datenbank gespeichert. Bei Verlust kann die entsprechende ID in der Datenbank gesperrt und eine neue Karte ausgegeben werden.

Eine besondere Stellung nimmt die RFID-Technologie auch im Bereich des Eventmanagements ein, um das Einlassen der Teilnehmer effektiver zu gestalten. Allerdings sorgte zum Beispiel die Ausstattung der Tickets für die Fußball-Weltmeisterschaft 2006 mit RFID bereits im Vorfeld für zahlreiche Diskussionen um den Datenschutz. Von Vorteil ist dabei die (zumindest theoretische) Unfälschbarkeit der Tickets, da sie über einmalige IDs verfügen. Allerdings kommt auch bei dieser Anwendung einer sicheren Verschlüsselung eine grundlegende Bedeutung zu. Bei der Bestellung von Tickets für die Fußballweltmeisterschaft 2006 muss neben Name, Vorname, Adresse, Nationalität, Geschlecht, Geburtsdatum, Ausweisnummer und Zahlungsverbindung auch angegeben werden, welcher Mannschaft man die Daumen drücken wird. Diese Daten werden nicht direkt auf dem Chip sondern in einer angeschlossenen Datenbank gespeichert, so dass diese auch bei Verlust des Tickets nicht ausgelesen werden können. Nur der Name des Inhabers wird im Klartext auf das Ticket gedruckt. Eine Änderung der Daten kann folglich direkt in der Datenbank durchgeführt werden. Bei der Weitergabe eines Tickets, der nur auf Antrag und „in besonderen Fällen (Hochzeit, Tod oder Krankheit innerhalb der Familie)“<sup>49</sup> zugestimmt werden muss, bedarf es allerdings der Neuausstellung, um den Namensaufdruck zu ändern. Personenbezogene Daten können also nicht ungewollt ausgelesen werden, solange kein Unbefugter Zugriff auf die Datenbank erhält, in der die Daten bis Oktober 2006 gespeichert sein werden. Kritischer ist

---

<sup>47</sup> Quelle: Heise online: „RFID-Kundenkarten kein Thema?“; <http://www.heise.de/newsticker/meldung/44352> (05.02.2004)

<sup>48</sup> Quelle: Henry Steinhilber: „In der Standardisierungsfalle“ iX 03/2005, S.24

<sup>49</sup> Quelle: 2006 FIFA World Cup™ Ticketing Center (FWCTC): „FAQs zum Kartenkauf FIFA WM 2006“

eine mögliche Verknüpfung der Daten: Eine Lokalisation der einzelnen Besucher im Stadion ist jederzeit möglich und könnte mit Hilfe der Bezahlungsfunktion der Tickets und im Vorfeld erhobener Daten gezielt eingesetzt werden, um Verbraucherprofile für die Sponsoren zu erstellen. Bedenklich ist auch die Weitergabe der vom Besucher erhobenen, teilweise personenbezogenen Daten an die Sponsoren der WM, die teilweise in Ländern ansässig sind, deren Datenschutzgesetze keinesfalls den deutschen entsprechen.

#### **4.4 Bezahlssysteme**

Auch Kreditkartenunternehmen setzen in verstärktem Maß auf den Einsatz von RFID: So wollte Mastercard bis Ende 2005 mehrere Millionen Karten ausgeben, die mit RFID-Chips ausgestattet sind.<sup>50</sup>

Im öffentlichen Nahverkehr werden die Vorteile der RFID-Technik ebenfalls genutzt, indem sie als wiederaufladbare Fahrkarte eingesetzt werden. In Hong Kong hat sich eine solche Karte als „Octopus-Karte“<sup>51</sup> durchgesetzt, mit der man zum Beispiel auch in Läden und Restaurants bargeldlos bezahlen kann. Bei dieser Anwendung muss insbesondere auf eine sichere Kommunikation Wert gelegt werden, um einen Missbrauch zu verhindern.

Weiterhin kommen die Chips in elektronischen Mautsystemen zum Einsatz, bei denen einerseits die Route als auch die Nutzungsdauer dokumentieren lassen. Das britische Verkehrsministerium<sup>52</sup> hat nach dem Test mit RFID-Tags versehener Nummernschilder<sup>53</sup> an Polizeiwagen mit der Installation eines umfassenden Verkehrsüberwachungssystems begonnen. Die so genannten e-Plates können im ruhenden und bewegten Verkehr aus bis zu 100 Metern Entfernung identifiziert werden. Trotz des permanenten Sendens der gespeicherten Informationen, wird die Lebensdauer der Schilder mit zehn Jahren angegeben. Auch in den Vereinigten Arabischen Emiraten soll ein solches System eingeführt werden<sup>54</sup>. Der Chip im Führerschein wird vom Bordcomputer in der so genannten Smartbox des Fahrzeugs automatisch in der Verkehrsüberwachungszentrale eingebucht. Damit sollen neben

---

<sup>50</sup> Quelle: Netzeitung.de: „Mastercard will Funkchips in Kreditkarten“;

<http://www.netzeitung.de/internet/358795.html> (20.09.2005)

<sup>51</sup> Quelle: Heise online: „Erste Geräte für Near Field Communication bereits Ende 2004“;

<http://www.netzeitung.de/internet/358795.html> (29.07.2004)

<sup>52</sup> Quelle: Heise online: „Britisches Verkehrsministerium testet RFID-Nummernschilder“

<http://www.heise.de/newsticker/meldung/62666> (10.08.2005)

<sup>53</sup> Hills Numberplates stattet seine Nummernschilder mit aktiven RFID-Tags von Identec Solutions aus.

Quelle: [www.e-plate.com](http://www.e-plate.com)

<sup>54</sup> Quelle: Peter Welchering: „Wüstenraser an der kurzen Leine“; Financial Times Deutschland,

<http://www.ftd.de/rd/17652.html> (10.08.2005)

Geschwindigkeit<sup>55</sup> auch die Fahrerdaten übertragen, sowie etwaige Verkehrsverstöße gemeldet und gegebenenfalls Strafzettel verschickt werden. Ziel ist es, die Verkehrssicherheit zu erhöhen, wenngleich das Vorhaben eine flächendeckende Überwachung der Fahrer darstellt, mit der sich weitflächige Bewegungsprofile erstellen lassen. Auch deutsche Politiker – zum Beispiel Otto Schily und Günther Beckstein – fordern vermehrt eine derartige Verkehrsüberwachung zur Terroristenabwehr<sup>56</sup>.

#### **4.5 Deutscher Reisepass (seit 2005) <sup>57</sup>**

Nach einem Beschluss des EU-Rates vom 13. Dezember 2004<sup>58</sup>, werden EU-Pässe mit einem RF-Chip<sup>59</sup> ausgestattet, auf dem neben den bisherigen Passdaten – Geburtsdatum, Augenfarbe, Körpergröße, ein Gesichtsbild sowie die Unterschrift – später auch die Fingerabdrücke in digitaler Form gespeichert werden. Damit soll die Fälschungssicherheit der Reisepässe erhöht und die Zuordnung zum Besitzer erleichtert werden. In der Verordnung werden aber keine Regelungen getroffen, was die Sicherheit der Daten im Pass selbst angeht. Im Vordergrund steht also der Schutz der personenbezogenen Daten<sup>60</sup>, da keine Datenbank zugrunde gelegt werden kann, wenn die Daten weltweit verfügbar sein sollen. Die theoretische Auslesedistanz von rund 10 Zentimetern kann durch entsprechende Hilfsmittel ausgedehnt werden. Um dennoch die Datensicherheit zu gewährleisten, müssen folglich entsprechende Sicherheitsmechanismen implementiert werden<sup>61</sup>. In den USA sieht man aus diesem Grund das Einbringen von Metallfolien vor, was aber keinen ausreichenden Schutz bietet.

Die New Technologies Working Group der Internationalen Zivilluftfahrtbehörde ICAO, in der auch Deutschland involviert ist, hat Empfehlungen zum Datenschutz erarbeitet, die beim deutschen Reisepass umgesetzt werden<sup>62</sup>. Diese orientieren sich am Minimalprinzip, damit auch verschiedene Systeme miteinander kooperieren können. Dabei muss eine digitale

---

<sup>55</sup> Die aktuelle Geschwindigkeit soll über GPS übertragen werden, um Falschdaten aufgrund von Tachomanipulationen auszuschließen.

<sup>56</sup> Quelle: Peter Welcherling: „Wüstenraser an der kurzen Leine“; Financial Times Deutschland, <http://www.ftd.de/rd/17652.html> (10.08.2005)

<sup>57</sup> Quelle: Schulzki-Haddouti, Christiane: „Untrügliche Zeichen“; c't 18/2004, S. 80 – 82

<sup>58</sup> Verordnung (EG) Nr. 2252/2004 DES RATES vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten; Quelle: Amtsblatt der Europäischen Union L 385, 29.12.2004

<sup>59</sup> Die in deutschen Reisepässen verwendeten Chips werden von Phillips und Infineon hergestellt. Quelle: Heise online: „Deutschland setzt internationale Standards bei Biometrie-Reisepässen“ (12.05.2005)

<sup>60</sup> Quelle: Ute Ross: „Interessenskonflikte“; iX 05/2005, S.20

<sup>61</sup> Quelle: Heise online: „Scharfe Kritik an der geplanten Einführung neuer Pässe und Ausweise“ <http://www.heise.de/newsticker/meldung/55233> (17.01.2005)

<sup>62</sup> Quelle: Bundesamt für Sicherheit in der Informationstechnik: „Digitale Sicherheitsmerkmale im ePass“; <http://www.bsi.de/fachthem/epass/Sicherheitsmerkmale.pdf> (01.06.2005)



Die eigentliche Kommunikation zwischen Reisepass und Lesegerät wird mit 112-3DES verschlüsselt, was nach Auffassung des Bundesamtes für Sicherheit in der Informationstechnik zusammen Basic Access Control ausreichend ist, da die „Daten relativ öffentlich sind und auf anderem Wege wesentlich einfacher gesammelt werden könnten“<sup>63</sup>.

Die zugrunde liegenden Daten zur Erstellung des Reisepasses werden nur für den Produktionszeitraum gespeichert und im Anschluss – kontrolliert durch den Bundesdatenschutzbeauftragten – gelöscht. Eine weitere Verwendung in einer zentralen Datenbank wird vom Bundespassgesetz ausgeschlossen<sup>64</sup>. Klärungsbedarf besteht weiterhin darüber, was mit abgelaufenen bzw. zerstörten Pässen passieren soll.

#### **4.6 Identifikation**

Mit RFID-Chips können Gegenstände, Tiere und sogar Menschen gekennzeichnet und identifiziert werden. Einen großen Einsatzbereich haben die Chips in Bibliotheken, die den Bücherbestand mit RFID-Tags bestücken. Damit können zum einen relevante Daten gespeichert werden, andererseits bietet das System eine Möglichkeit der Diebstahlskontrolle, wie sie im Einzelhandel in einfacherer Form bereits seit den 60er Jahren<sup>65</sup> angewendet wird.

In den USA kommt der etwa reiskorngroße so genannte „Verichip“<sup>66</sup> zum Einsatz, der beim Menschen unter der Haut eingepflanzt wird und im Notfall lebenswichtige Informationen bereitstellen kann. Das Klinikum Saarbrücken ist auf diesem Gebiet Vorreiter in Deutschland und erprobt den Einsatz gemeinsam mit Intel, Siemens Business Services und Fujitsu Siemens<sup>67</sup>. Der Chip ist dabei in ein Armband integriert und kann mit Hilfe von Tablet PCs, PDAs oder an Infoterminals von befugten Mitarbeitern und Patienten ausgelesen werden.

Mit Hilfe der RFID-Technologie können Gegenstände auch individualisiert und somit fälschungssicher gemacht werden. Dieser Aspekt wird einerseits bei dem neuen deutschen Reisepass (vgl. Kapitel 4.5) in den Vordergrund gestellt, aber auch die Europäische Zentralbank denkt über eine mögliche Anwendung in den Euro-Banknoten nach<sup>68</sup>. Demnach müsste man sich umso mehr Gedanken machen, inwieweit die gespeicherten Daten geschützt werden können. Denn obwohl es sich nicht um personenbezogene Daten im Sinne des

---

<sup>63</sup> Bundesamt für Sicherheit in der Informationstechnik: „Digitale Sicherheitsmerkmale im ePass“, 01.06.2005

<sup>64</sup> Quelle: Dr. Thilo Weichert: „Angriff auf den Datenschutz?“, c't 11/2005, S. 94 – 99

<sup>65</sup> Quelle: RFID-Journal: „RFID“; <http://www.rfid-journal.de/rfid.html>

<sup>66</sup> Quelle: Heise online: „Implantierbare RFID-Chips breiten sich aus“, <http://www.heise.de/newsticker/meldung/53789> (30.11.2004)

<sup>67</sup> Quelle: Heise online: „RFID jetzt auch in deutschem Krankenhaus“, <http://www.heise.de/newsticker/meldung/58777> (20.04.2005)

<sup>68</sup> Quelle: Heise online: „Euro-Banknoten mit Identifikationschips“, <http://www.heise.de/newsticker/meldung/37063> (23.05.2003)

Bundesdatenschutzgesetzes handelt, ist es ersichtlich, dass ein unerwünschtes Auslesen beispielsweise des Wertes in jedem Fall zu unterbinden ist. Eine vergleichbare Sicherheitsstruktur wie beim neuen deutschen Reisepass wäre zwar denkbar, allerdings rein aus Kostengründen kaum realisierbar. Dennoch könnte eine Zugriffsverweigerung bei fehlendem Sichtkontakt einen Lösungsansatz bieten.

## 5 Fazit

Von vielen unbemerkt werden RFID-Systeme in weiten Bereichen des täglichen Lebens implementiert. Sei es der Immobilizer im Autoschlüssel, der Tag in den Bibliotheksbüchern, oder das Ticket zur Fußballweltmeisterschaft, RFID ist bereits heute allgegenwärtig.

Dass damit Informationen preisgegeben werden, über Interessengebiete und Kaufverhalten zum Beispiel, ist dem Einzelnen meist nicht bewusst. Deswegen sollte mit dem verstärkten Einsatz von RFID-Systemen auch eine Information der Betroffenen erfolgen, um diesen die möglichen Konsequenzen zu verdeutlichen.

Werden RFID-Systeme in Verbindung mit personenbezogenen Daten verwendet, ist – zumindest derzeit bei den in dieser Arbeit gewählten Beispielen – ein nach deutschem Recht hinreichender Schutz gegeben. Erfahrungsgemäß wird es aber immer Anstrengungen geben, diese Mechanismen zu brechen oder zu umgehen, wie das Beispiel des Immobilizers im Kapitel 4.1 zeigte. Bedenklich ist damit auch die Speicherung von biometrischen Daten wie dem Fingerabdruck ab 2007 auf dem zehn Jahre gültigen deutschen Reisepass.

Das Auslesen des Warenkorbes, möglicherweise sogar der Geldscheine in der Tasche und die Verknüpfung mit den Daten der Kundenkarte sind im Moment noch Fiktion. Dennoch müssen die weiteren Entwicklungen kritisch beobachtet werden, insbesondere wenn man die Entwicklung weltweit, aber auch die datenschutzrechtliche Aufweichung in Deutschland bedenkt. So ist das unter 4.4 vorgestellte Mautsystem der Vereinigten Arabischen Emirate auch bei deutschen Politikern im Gespräch, um es als wichtigen Faktor bei der Terrorabwehr einzusetzen. Wenngleich eine Einführung in Deutschland analog zur in Kapitel 3.5 angesprochenen Vorratsdatenspeicherung rechtlich äußerst bedenklich ist, bleibt abzuwarten, ob sich Datenschutz oder „innere Sicherheit“ in Deutschland durchsetzen wird.

Dabei werden wohl juristische Experten die Frage klären müssen, inwieweit derartige Maßnahmen und insbesondere die damit verbundene Datenverarbeitung mit der deutschen Verfassung vereinbar sind. Die gesammelten Daten könnten somit über den eigentlichen Zweck hinaus, beispielsweise zur Strafverfolgung benutzt werden.

RFID kann viele Verfahren und Abläufe vereinfachen und effizienter gestalten, dennoch muss der Einsatz immer genau bedacht und konzipiert werden, um dem Datenschutz die erforderliche Bedeutung zukommen zu lassen.

## Literatur

- Finkenzeller, Klaus                      RFID-Handbuch  
ISBN 3446220712
- Haar, Tobias                                „Erfasst“  
iX 03/2005, S. 82 – 84
- Kallnik, Stephan;  
Pape, Daniel;  
Schröter, Daniel;  
Strobel, Stefan                        „Das Sicherheitsloch. Buffer-Overflows und wie man sich davor schützt“  
c't 23/2001, S. 216 - 218
- Kaufmann, Thomas                    „Die üblichen Verdächtigen“  
iX 02/2005, S. 10 – 12
- Kügler, Dr. Dennis                    „Risiko Reisepass“  
c't 05/2005, S. 84 – 89
- Kuri, Jürgen;  
Meyer, Angela;  
Schüler, Peter                        „Im Fadenkreuz“  
c't 06/2004, S. 138
- Meyer, Angela;  
Schüler, Peter                        „Mitteilsame Etiketten“  
c't 09/2004. S. 122
- Roos, Ute                                „Interessenskonflikte“  
iX 02/2005, S. 20
- Schoblick, Robert                    RFID  
ISBN 3772359205
- Schulzki-Haddouti, Christiane        „Untrügliche Zeichen“  
c't 18/2004, S. 80 – 82
- Schwonbeck, Susanne                „Chipmania. Wirtschaftlichkeit contra Datenschutz“  
iX 05/2004, S.12 – 14
- Steinhau, Henry                        „In der Standardisierungsfalle“  
iX 03/2005, S.24
- Tolmein, Dr. Oliver                    „Nichts zu verbergen?“  
c't 01/2005; S. 74 – 79
- Weichert, Dr. Thilo                    „Angriff auf den Datenschutz?“  
c't 11/2005, S. 94 – 99

## Weblinks

Stand: 02.02.2006

- |   |  |
|---|--|
| Bundesamt für Sicherheit in der Informationstechnik | <p>„Digitale Sicherheitsmerkmale im ePass“<br/> <a href="http://www.bsi.de/fachthem/epass/Sicherheitsmerkmale.pdf">http://www.bsi.de/fachthem/epass/Sicherheitsmerkmale.pdf</a> (01.06.2005)</p> <p>„Risiken und Chancen des Einsatzes von RFID-Systemen Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit“<br/> <a href="http://www.bsi.de/fachthem/rfid/RIKCHA.pdf">http://www.bsi.de/fachthem/rfid/RIKCHA.pdf</a></p> <p>„Verschlüsselungsverfahren“<br/> <a href="http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm">http://www.bsi-fuer-buerger.de/schuetzen/07_0301.htm</a></p>  |
| Bündnis 90/Die Grünen                               | <p>„Antrag. Freiheit des Telefonverkehrs vor Zwangsspeicherungen“<br/> <a href="http://dip.bundestag.de/btd/16/002/1600237.pdf">http://dip.bundestag.de/btd/16/002/1600237.pdf</a> (14.12.2005)</p>  |
| DAFU Datenfunk                                      | <p>RFID - Radio-Frequency Identification<br/> <a href="http://www.dafu.de/praxis/rfid.html">http://www.dafu.de/praxis/rfid.html</a></p>  |
| FH Salzburg   | <p>„Studie 6: Prozessoptimierung durch eingebettete Technologien für Endprodukte“<br/> <a href="http://esyys.salzburgresearch.at/doc/rfid-studie-final.pdf">http://esyys.salzburgresearch.at/doc/rfid-studie-final.pdf</a></p>   |
| Finke, Thomas;<br>Kelter, Harald                    | <p>“Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems“<br/> <a href="http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf">http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf</a></p>  |
| FWCTC: 2006 FIFA World Cup™ Ticketing Center        | <p>„FAQs zum Kartenkauf FIFA WM 2006“<br/> <a href="http://www.dfb.de/tickets/wm2006/FAQs.pdf">http://www.dfb.de/tickets/wm2006/FAQs.pdf</a></p>   |
| Garstka, Prof. Dr. Hansjürgen                       | <p>„Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2004“<br/> <a href="http://www.datenschutz-berlin.de/infomat/dateien/jb/jb04.pdf">http://www.datenschutz-berlin.de/infomat/dateien/jb/jb04.pdf</a> (15.03.2005)</p>  |
| Geschichte Lexikon                                  | <p>„Radio Frequency Identification“<br/> <a href="http://www.geschichteboard.de/lexikon/RFID,information.htm">http://www.geschichteboard.de/lexikon/RFID,information.htm</a></p>   |
| Heise online  | <p>„Absprachen über Vorratsdatenspeicherung lösen Empörung aus“<br/> <a href="http://www.heise.de/newsticker/meldung/57507">http://www.heise.de/newsticker/meldung/57507</a> (14.03.2005)</p> <p>„Britisches Verkehrsministerium testet RFID-Nummernschilder“<br/> <a href="http://www.heise.de/newsticker/meldung/62666">http://www.heise.de/newsticker/meldung/62666</a> (10.08.2005)</p> <p>„Data Encryption Standard hat ausgedient“<br/> <a href="http://www.heise.de/newsticker/meldung/21083">http://www.heise.de/newsticker/meldung/21083</a> (15.09.2001)</p> <p>„Deutschland setzt internationale Standards bei Biometrie-Reisepässen“<br/> <a href="http://www.heise.de/newsticker/meldung/66273">http://www.heise.de/newsticker/meldung/66273</a> (12.05.2005)</p> <p>„Erste Geräte für Near Field Communication bereits Ende 2004“<br/> <a href="http://www.netzeitung.de/internet/358795.html">http://www.netzeitung.de/internet/358795.html</a> (29.07.2004)</p> <p>„EU-Parlament beschließt massive Überwachung der Telekommunikation“<br/> <a href="http://www.heise.de/newsticker/meldung/67358">http://www.heise.de/newsticker/meldung/67358</a> (14.12.2005)</p> |

- „Große Koalition sieht Vorratsdatenspeicherung im Einklang mit der Verfassung“  
<http://www.heise.de/newsticker/meldung/68951> (27.01.2006)
- „Identitätssicherung von Biometriepässen in der Diskussion“  
<http://www.heise.de/newsticker/meldung/66273> (16.11.2005)
- „Implantierbare RFID-Chips breiten sich aus“  
<http://www.heise.de/newsticker/meldung/53789> (30.11.2004)
- „Metro zeigt RFID auf der CeBIT“  
<http://www.heise.de/newsticker/meldung/68313> (13.01.2006)
- „Metro zieht RFID-Karte zurück“  
<http://www.heise.de/newsticker/meldung/45062> (27.02.2004)
- „RFID jetzt auch in deutschem Krankenhaus“  
<http://www.heise.de/newsticker/meldung/58777> (20.04.2005)
- „RFID-Kundenkarten kein Thema?“  
<http://www.heise.de/newsticker/meldung/44352> (05.02.2004)
- „Scharfe Kritik an der geplanten Einführung neuer Pässe und Ausweise“  
<http://www.heise.de/newsticker/meldung/55233> (17.01.2005)
- Heise security „Auto-Schlüssel mit unsicherem Schlüssel“  
<http://www.heise.de/security/news/meldung/55729> (30.01.2005)
- „Hersteller: geknackte RFID-Verschlüsselung derzeit kein Problem“  
<http://www.heise.de/security/news/meldung/57890> (24.03.2005)
- Hills Numberplates Ltd [www.e-plate.com](http://www.e-plate.com)
- Lahner, Claus Mauricio „Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen“  
 Abschlussarbeit zur Erlangung des Grades LL.M. (Master of Laws),  
 Universität Hannover  
<http://www.rechtsanwaltlahner.de/web-content/RFID.pdf> (16.07.2004)
- Netzeitung.de „Mastercard will Funkchips in Kreditkarten“  
<http://www.netzeitung.de/internet/358795.html> (20.09.2005)
- RFID-Journal „RFID“  
<http://www.rfid-journal.de/rfid.html>
- „RFID Datenschutz“  
<http://www.rfid-journal.de/rfid-bedenken.html>
- „RFID Energieversorgung“  
<http://www.rfid-journal.de/rfid-energieversorgung.html>
- „RFID-Systeme“  
<http://www.rfid-journal.de/rfid-systeme.html>
- „RFID-Technik“  
<http://www.rfid-journal.de/rfid-technik.html>
- „Übertragungsfrequenzen“

- 
- <http://www.rfid-journal.de/rfid-uebertragungsfrequenzen.html>
- Roth, Torsten      „Informationssicherheitsverfahren von RFID-Transpondern“  
[http://www.sigs.de/publications/os/2005/rfid/roth\\_OS\\_rfid\\_05.pdf](http://www.sigs.de/publications/os/2005/rfid/roth_OS_rfid_05.pdf) (2005)
- Texas Instruments      „RFID 101 - The Basics, Texas Instruments' RFID Systems“  
Diese Broschüre wurde auf Anfrage hin von Texas Instruments zugesandt und kann unter [http://www.wingine.net/dok/rfid\\_ti.pdf](http://www.wingine.net/dok/rfid_ti.pdf) eingesehen werden.
- Viruelles Datenschutzbüro      „RFID-Chips“  
<http://www.datenschutz.de/feature/detail/?featid=2>
- Welchering, Peter      „Wüstenraser an der kurzen Leine“  
Financial Times Deutschland  
<http://www.ftd.de/rd/17652.html> (10.08.2005)
- WIKIPEDIA      „RFID“  
Die freie Enzyklopädie      <http://de.wikipedia.org/wiki/Rfid>
- „Kryptologie“  
[http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt\\_Kryptologie](http://de.wikipedia.org/wiki/Wikipedia:WikiProjekt_Kryptologie)