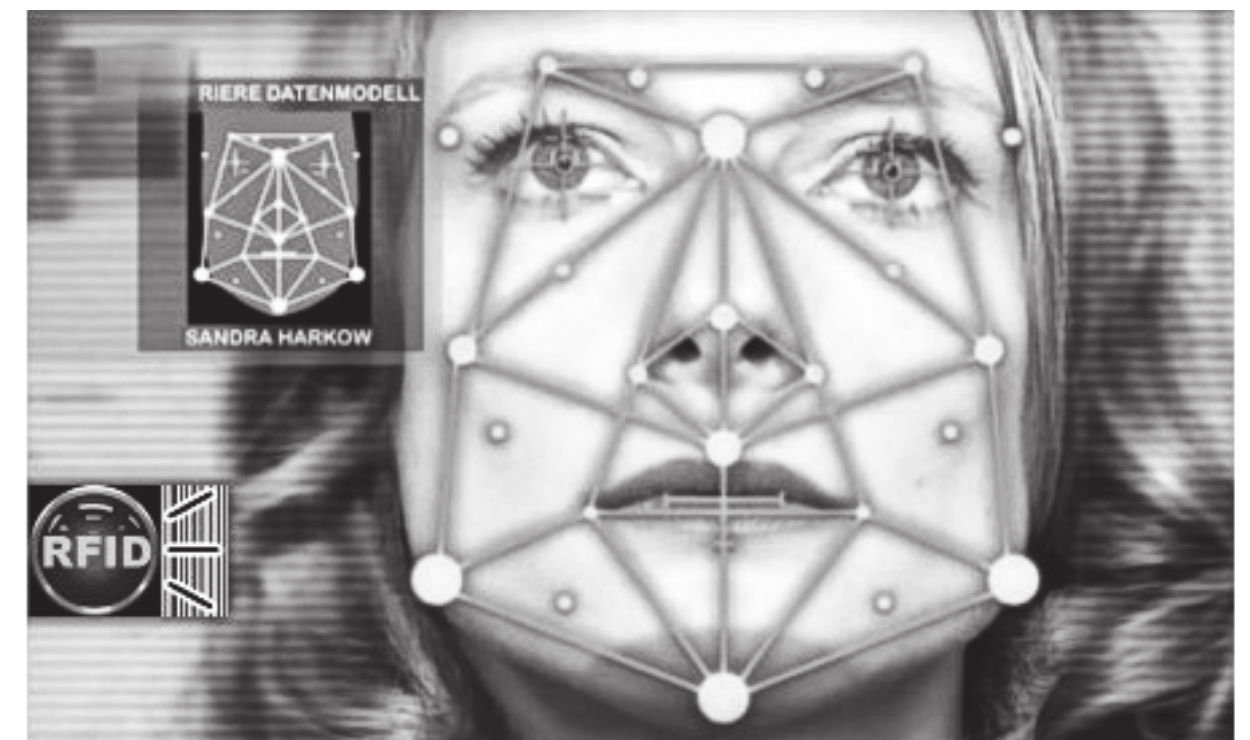




# Inhaltsangaben

- **Die Kontrollgesellschaft und ihre neuen Technologien ... 4**
- **Geschichte von RFID..... 8**
- **Grundlagen der RFID-Technologie..... 10**
- **Ausführungen und Bauformen von RFID-Systemen ..... 13**
- **Anwendung ..... 18**
- **RFID und Datensicherheit..... 26**
- **Sicherheit von RFID-Systemen ..... 27**
- **Möglichkeiten, um die korrekte Funktionsweise  
eines RFID-Systems zu beeinträchtigen ..... 31**
- **Quellenangaben ..... 32**
- **Weiterführende Links ..... 33**



# Die Kontrollgesellschaft und ihre neuen Technologien

„Wer weiss, dass die Chips, die sich die Spasskultur-besessenen Kunden der „Baja-Beach-Club“-Disco-Kette europaweit für 180 Euro spritzen lassen können damit sie auch beim Nackt-Tanzen bargeldlos bezahlen können, dass ebendiese Chips dazu dienen, High-Tech-Waffen an ihre eingetragenen Benutzer zu lizensieren? Wenn der gechipte Polizist seine „nicht-tödliche Wuchtgeschoss“-Waffe verliert, ist sie für den Finder nutzlos. Man kann sie nur abfeuern, wenn man den Griff auf die Hautpartie über den eingepflanzten Chip legt. Wer heute beim Supermarktriesen WalMart Rasierklingen oder bei Benetton Pullover kauft, wird längst-auch nach der Entfernung der Diebstahlsicherung- noch gescannt. Eingebaute hauchdünne Markierfolien registrieren die Kundenprofile selbst nach Verlassen der wunderbaren Warenwelt. Die Mittel der Kontrolle kommen uns körperlich nahe, wachsen in uns hinein: bei den Kontrollierten wie bei den Kontrolleuren.“  
(aus einer Beschreibung des Projektes Crowd CTRL der Gruppe BBM)

Nachdem alle Hunde einer Chip-Pflicht unterliegen, nachdem ganze Produktions-und Verarbeitungsprozesse RFID-gesteuert ablaufen, nachdem zuerst die Dementen, dann Gefängnisinsassen, dann Kleinkinder, dann Leichenteile, dann ganze Belegschaften, dann wer-auch-immer gechipt werden, nachdem RFID in Bibliotheken, in Supermärkten, als Zugangssicherung und Identifikationsmittel zur Normalität geworden ist, müssen wir uns also der Realität stellen, dass diese Technologie bis auf weiteres unsere gesamten Lebensbereiche eingenommen hat und einnehmen wird. Wie wir damit umgehen, hängt sehr davon ab, welches Wissen oder besser; welche Ohnmacht wir dem Zutagetreten dieser minimen aber doch frappanten Erscheinung auf der Käseverpackung entgegenbringen. Um der biopolitischen Invasion unseres Alltags defensiv gegenüberzutreten, müssen wir uns ein Grundwissen aneignen, um zumindest minimale Gegenstrategien zu entwickeln.

Die Einheiten werden kleiner, der Blick der Kontrolle bricht durch die Oberfläche (Fingerabdruck) hindurch, bemächtigt sich der kleinsten körpereigenen Bauteile (DNA), Technologie und Körper bilden endlich eine Einheit; Cyborgphantasien werden wahr; Hobbybastler implantieren sich selbst Chips, um ihr Auto, ihren Computer, ihre Wohnung per Handballen zu öffnen. Wo die Euphorie nicht überwiegt, trägt die Sicherheits – und Terrorismusdebatte ihre Früchte; Eltern erkennen die Notwendigkeit der Verfolgbarkeit ihrer Kinder im Falle einer Entführung; andere chippen sich, um im Falle einer Hospitalisierung die eigenen Krankheitsbilder und Blutgruppen zugänglich in sich zu tragen. Was die Expansion der Kontrollmechanismen in unserem Alltag wirklich bedeutet, werden wir wohl in ihrer ganzen Tragweite erst in einigen Jahren zu spüren kriegen; dann nämlich, wenn die Unmengen an Daten, die über uns gesammelt werden, auch ausgewertet und zugänglich gemacht werden. Schliesst man nämlich

## Weiterführende Links

- **Technische Aspekte der biometrischen Ausweise der Schweiz**  
<http://www.biometrische-ausweise.ch/>
- **No Verichip Inside Movement**  
<http://www.wethepeoplewillnotbechipped.com>
- **FoeBuD e.V. ; Deutsche Datenschützerplattform**  
Passtaschen und RFID-Armreifen und Buttons und sonstige Gadgets erhältlich  
<http://www.foebud.org/>
- **RFIDIOT**  
an open source python library for exploring RFID devices  
<http://rfidiot.org/>
- **RFDump**  
backend GPL tool to directly interoperate with any RFID ISO-Reader  
<http://www.rf-dump.org/>
- **«Leben mit neuen Ideen»**  
<http://rfidabc.de/>
- **RFID Weblog**  
«immer auf Sendung...»  
<http://www.rfidweblog.de>
- **Hack a Day**  
serves up fresh hacks each day  
<http://hackaday.com/?s=rfid>

### Mit CCTV und RFID gegen Fahrraddiebe

In Portsmouth, England, werden Fahrräder mit einer Kombination von CCTV, Funkchips und Bewegungssensoren geschützt. Mit dem WASP Cycle Monitoring System der Firma SOS Response können Radfahrer ihren Drahtesel an speziellen, kameraüberwachten Parkplätzen abstellen und anmelden. Wird das Rad bewegt, aktivieren Sensoren die nächste Kamera, die daraufhin auf den Standort des Rades zoomen. Per SMS wird ein Alarm ausgelöst. Die Sicherheitsbeamten können anhand der Live-Übertragung entscheiden, ob ein Beamter losgeschickt wird.





# Quellenangabe

- **WikiBook «RFID-Technologie»**  
<http://de.wikibooks.org/wiki/RFID-Technologie>
- **Verichip**  
<http://de.wikipedia.org/wiki/VeriChip>
- **RFID – Zapper**  
[http://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper\\_de61.html](http://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper_de61.html)
- **Warcart**  
<http://web.mit.edu/zacka/www/warcart.html>
- **RFID Hacks**  
<http://www.heise.de/newsticker/classic/>  
<http://www.golem.de/ticker/>

die Überwachungskamera mit dem Handy mit den Kleidern mit dem Pass mit der Fahrkarte mit dem Einkauf mit dem Laptop kurz, so ergibt sich die Möglichkeit einer völlig verfolgbaren, kontrollierbaren, nachvollziehbaren und wiedererkennbaren Existenz. Die Kontrolle fächert sich auf, verschwindet sozusagen aus dem Sichtbaren, die Instanzen werden kleiner, unauffindbarer, und mit ihrem scheinbaren Verschwinden erscheint die Kontrolle allmächtiger denn zuvor. Sie tritt sozusagen nur noch im Falle der Abweichung aus ihrem Schattendasein hervor; solange die Existenz in ihrer Legalität gesichert ist, hat sie nichts zu befürchten. Was eben nicht heisst, dass der wunderbare Spruch all der unbescholtenen Bürger; welche „nichts zu verbergen haben“, und sich deswegen gerne zum gläsernen Menschen machen, auch aufgeht. Niemand bewegt sich völlig legal, und je mehr Daten gesammelt werden, desto mehr Abweichungen werden auch ersichtlich.

Das Erscheinen der Tags ist bedenklich, solange die Entwicklung so fortschreitet wie bisher; ein grosser Teil der Bevölkerung bedient sich oder wird bedient mit einer Technologie, derer sie sich nicht ermächtigt fühlt und sich auch nicht ermächtigt. Die Identifizierung der Autos auf den zahlungspflichtigen Autobahnstrecken, die Verfolgbarkeit der Gepäckstücke am Flughafen, die Metrokarten, die durch die Handtasche hindurch gelesen werden, all dies sind schon fast mythische Vorgänge, welche einem gewissen Zauber nicht entbehren. Schlussendlich jedoch ebenso unterbrechbar und angreifbar wie es die Lochkarte auch war; ein RFID-Chip an ein Zugangs-Lesegerät geklebt, und es wird garantiert

## Japanische Schüler bekommen RFID-Chips

RFID wird jetzt von den Schulen in Osaka, Japan, zur Überwachung von Schülern eingesetzt. Für die Schulbehörde der Stadt überwiegen die Vorteile der erzielbaren Kontrolle deutlich die Bedenken von Menschenrechtlern und Verbraucherschützern.

Die winzigen Tags sollen in Schulranzen, Namensschilder oder – im Fall einer Grundschule – Schuluniformen der Kinder integriert werden. Ausgelesen werden sie durch Lesegeräte an den Toren und an anderen Schlüsselstellen, etwa am Rand des Schulgeländes, um die Bewegungen der Schüler nachvollziehen zu können. Eine ähnliche RFID-Implementation hatte das dänische Legoland vergangenen Monat eingeführt, um Kinder wieder zu finden, die ihre Eltern verloren oder sich verlaufen haben.



**Niederlande:** Biometrie-Pass erfolgreich gehackt. 01.02.2006. Fortschritt der Technik: Nun lassen sich Pässe berührungslos kopieren und fälschen. Der Vorteil von RFID ist, dass es Daten berührungslos und auf Entfernung auslesen kann. Die Chips in den neuen Biometrie-Pässen sind zwar nur für begrenzte Entfernungen ausgelegt, doch mithören lässt sich die drahtlose Kommunikation zwischen Pass und Lesegerät auch über größere Entfernungen. Und knacken sowieso. Das niederländische Fernsehmagazin Nieuwslicht verkündet, dass die dortigen Biometrie-Pässe bereits erfolgreich geknackt wurden. Die Hacker waren dabei vom Smartcard-Sicherheitsspezialisten Riscure aus Delft, der schon vor einem halben Jahr ausführlich erläuterte, dass die Kommunikation zwischen Biometrie-Pass und Lesegerät auf einer Entfernung von bis zu 10 Metern belauscht und aufgezeichnet werden kann. In etwa zwei Stunden kann dann der zuvor aufgezeichnete Code geknackt werden, so dass Geburtsdatum, Foto und Fingerabdruck des belauschten

Passbesitzers im Klartext vorliegen. Passfälscher müssen zukünftig also gar nicht mehr Pässe stehlen oder ausleihen und kopieren; es reicht vielmehr völlig, wenn sie sich mit Notebook und RFID-Empfänger in 10 Meter Umkreis einer Passkontrolle beispielsweise am Flughafen auf die Lauer legen. ... Die Sicherheitslücken sollen zwar verringert werden, sodass es etwas länger dauert, den Code zu knacken – das drahtlose Mitlesen selbst lässt sich jedoch nicht verhindern. Update: Deutscher und österreichischer Biometrie-Pass ebenfalls unsicher. Wie viele der anderen EU-Staaten ebenfalls unsichere Biometrie-Pässe haben, ist noch nicht bekannt. Zumindest der deutsche und der österreichische Pass sind jedoch in der gegenwärtigen Version ebenso unsicher wie der niederländische. Und im Gegensatz zum niederländischen und österreichischen Biometrie-Pass, welche noch nicht ausgegeben wurden, ist die bundesdeutsche unsichere Variante bereits im Umlauf.



keinen Zugang mehr gewähren bis nicht jemand den Störsender entdeckt. Eine Alufolie in der Tasche oder um den Pass ermöglicht einen ungestörten Diebstahl oder schützt vor „unautorisiertem“ Auslesen. Natürlich werden auch schon konsumentenschützende Störtags produziert, welche permanent Daten senden und so den Reader überlasten und ausser Gefecht setzen. Sobald die Spezialisierung durchbrochen ist, erweist sich ein Verichip eventuell sogar als unsicherer als andere Formen der Identitätssicherung; wenn eine Person auf offener Strasse im Vorbeigehen ausgelesen und ihr Chip geklont werden kann, könnte dies einem nicht nur Zugang zum Baja Beach Club verschaffen....

Die Kontrollgesellschaft setzt sich in den Körpern fest, macht sich der Dinge habhaft, so dass zu jedem Einzelnen jeweils eine zweite Ebene; diejenige der Beschreibung, der Daten, existiert. Alles existiert in einem Doppel, einmal objekthaft, und einmal virtuell. Der Abgleich dieser beiden Informationsströme rückt immer näher zueinander hin und ist nun schon fast zu einer Ebene verschmolzen. Die paranoide Warengesellschaft hat ihre Kontrolldispositive auf den Plan gerückt; die Vision der globalen Infrastruktur zur Identifikation jeglichen Objekts an jeglichem Ort; das Internet der Dinge, rückt in den Bereich des Möglichen. Die Inkorporierung der Kontrolle, das Dispositiv-werden der Subjekte, wurde beim Wort genommen.

## **Möglichkeiten, um die korrekte Funktionsweise eines RFID-Systems zu beeinträchtigen**

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

je nach Sicherheitsverfahren, auch von Passwörtern oder Schlüsseln Kenntnis haben.

Das Tag wird vom Trägerobjekt losgelöst, um dessen Bewegungen vor dem Lesegerät zu verbergen oder ein anderes Objekt als das ursprüngliche Trägerobjekt auszugeben.

**Vorwerk präsentiert  
RFID «smart floor»**

Mit dem weltweit ersten textilen Underlay zur automatischen Steuerung von Robotern eröffnen die Vorwerk Teppichwerke völlig neue Dimensionen für zukunftsorientiertes Gebäudemanagement. Teppichboden und andere Bodenbeläge werden künftig zum Navigationssystem. Nach mehr als drei Jahren Forschungsarbeit ist es den Vorwerk Teppichwerken aus Hameln jetzt gelungen, den ersten serienreifen «smart floor» zu entwickeln. Der «smart floor», eine textile Unterlage, ist mit RFID-Chips bestückt und kann unter nahezu allen geeigneten Bodenbelägen installiert werden. Anhand der auf den elektronischen Chips gespeicherten Informationen können sich RFID-Roboter auf der Bodenfläche zielgenau orientieren und zum Beispiel automatisierte Reinigungs – oder Transportfunktionen in Gebäuden übernehmen.



**Pan/Tilt Mechanism**  
attachments include antennas or a smoke *grenade launcher*

**Two Laptops**  
for control and data logging

**Scanner**  
to pick up various communications

**Control Box**  
w/ key switch for activation

**Antenna Switch Box**  
To toggle between antennas and radios

**Flash Drive Dropper**  
for U3 hacksaws

**900 MHz Antenna**  
directional, great for cordless phones

**19dBi WiFi Antenna**  
directional

**12dBi WiFi Antenna**  
omnidirectional

**25-1300 MHz Antenna**  
general coverage, great for picking up the police

**CCD Camera**  
trip documentation

**Lights**  
2M candlepower for night operations

**PA Speaker**  
For announcements and intimidating music

**Der ultimative  
Kommunikationsempfänger**

Um den Warcart zu verstehen muss man zuerst ein wenig Geschichte kennen. Wardriving, das heisst, mit einem Laptop Auto fahren und WiFi-Zugänge suchen, wurde erstmals populär um das Jahr 2001. Innert kürzester Zeit erfanden Leute warwalking und Millionen bewanderten die Strasse mit einem Laptop und einer WiFi Karte in der Hand. Dann ging es richtig los als jemand ein Cessna Flugzeug mit einem Laptop flog und der erste warflyer wurde. Sehr schnell berichtete die Presse und viele Internetblogs über die neusten war-irgendwas Interventionen. Es gab warrocketing, warballooning,

warbiking und warboating. Es gab Podien und Seminare, neue Geschichten und Blogs, Fernseh-und Radioberichte, alles über die neusten WiFi-Trackings. Schnell wurde es offensichtlich, dass viele dieser Methoden sehr elitär sind. Es gibt das Autofahren, die Privatflugzeuge, Heissluftballonflüge, Yachtbesitzer, alle mit Laptops ausgerüstet. Was die Welt brauchte, war eine funktionierende low-cost Alternative.





# Geschichte von RFID

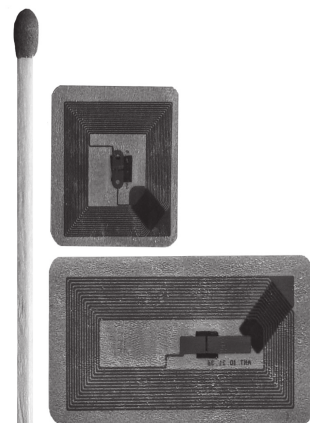
Radio Frequency IDentification (engl. für Funkfrequenz-Identifizierung) ist eine Methode, um Daten berührungslos und ohne Sichtkontakt lesen und speichern zu können. RFID-Systeme eignen sich grundsätzlich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss.

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

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

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

Zur Jahrtausendwende hin erlebte die RFID-Technologie einen weiteren Schub, als zwei Professoren, David Brock und Sanjay Sarma, preisgünstige RFID-Chips entwickelten, um jedes Produkt damit auszustatten. Außerdem nutzten sie die Chips als mobile Datenbanken, um alle Informationen über das Produkt und alle Produktbewegungen



**03.02.2009.** US-Hacker kopiert unbemerkt RFID-Ausweise.

Notwendiges Zubehör ist für 250 US-Dollar zu haben. Dem US-Hacker und Sicherheitsspezialisten Chris Paget ist es in den USA gelungen, unbemerkt und auf Entfernung RFID-Tags von Ausweisen zu kopieren. Alles, was er dafür benötigte, ließ sich günstig auf Auktionsplattformen beschaffen. Mit einfachen Mitteln ist es dem US-Hacker Chris Paget gelungen, RFID-Ausweise von US-Bürgern unbemerkt zu kopieren. Dafür genügte Hardware im Wert von 250 US-Dollar, die Paget auf der Auktionsplattform eBay ersteigert hatte, berichtet The Register. Mit der Hardware erreichte Paget eine Reichweite von rund 9 Metern. Mit weiteren Verbesserungen sollen sogar 1,6 Kilometer möglich sein. Die Hardware bestand aus dem Lesegerät Symbol XR400 RFID, einer Motorola-AN400-Antenne und einem Notebook. Paget platzierte sie in einem Auto und nutzte sie, um in San Francisco 20 Minuten lang nach Personalausweisen oder Führerscheinen mit RFID-Tags zu suchen. Pagets Angaben zufolge gelang es, die Daten von zwei Ausweisen auszulesen und zu kopieren. Die betroffenen Inhaber bemerkten von dem Kopiervorgang nichts. Ziel der Machbarkeitsstudie ist, die Öffentlichkeit auf die Sicherheitsprobleme aufmerksam zu machen, die hinter der RFID-Technik stecken. Außerdem hofft Paget, Verwaltungen dazu zu bewegen, auf die Technik zu verzichten.



## Ausspähen von Daten

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

Die Kommunikation zwischen Tags und Lesegeräten wird vom Angreifer mit einem eigenen Empfänger abgehört. Dabei kann die Entfernung größer sein als die standardmäßig vorgesehene Lesedistanz.

Die Daten aus den Tags werden vom Angreifer mit einem eigenen Lesegerät auslesen. Dabei kann das Lesegerät versteckt installiert sein oder auch mobil eingesetzt werden. Darüber hinaus muss der Angreifer die Identität des Lesegeräts fälschen können, für den Fall dass eine Authentifizierung des Lesegeräts vorgesehen ist.

## Einspeisen falscher Daten (Täuschen)

Folgende Angriffe können vom Angreifer in Täuschungsabsicht durchgeführt werden:

Der Inhalt eines Tags wird vom Angreifer verändert. Diese Art des Angriffs ist jedoch nur möglich, wenn die der ID zugeordneten Daten auf den Tags selbst (und nicht im Backend) gespeichert werden. In den meisten Anwendungen ist dies aber nicht der Fall.

Tags werden vom Angreifer emuliert oder dupliziert (Cloning). Um die Identität gegenüber dem Lesegerät vortäuschen zu können, muss der Angreifer hierzu mindestens von der ID (Seriennummer) und,



Tags nicht mehr feststellen oder die Anwesenheit des Tags im Lesebereich nicht mehr erkennen.

#### Ablösen

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

#### Angriffe auf die Luftschnittstelle

##### Abhören

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

##### Blocken

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

##### Stören

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

##### Identität fälschen (Lesegerät)

In einem sicheren RFID-System muss das Lesegerät seine Berechtigung gegenüber dem Tag nachweisen. Damit ein Angreifer die Daten mit einem eigenen Lesegerät auslesen kann, muss dieses die Identität eines autorisierten Lesegeräts vortäuschen. Diese Art von Angriff reicht auf der Skala der Durchführbarkeit von „sehr einfach“ bis „praktisch unmöglich“, in Abhängigkeit von den verwendeten Sicherheitsmaßnahmen.

zu dokumentieren. Damit war es beispielsweise möglich, Warenbewegungen nicht nur für den Lieferanten, sondern auch für den Kunden so transparent zu gestalten, dass jederzeit der Status der Lieferung überwacht werden konnte.

#### Auto-ID-Systeme

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

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

Eine Hauptaufgabe solcher Systeme besteht, wie es die Bezeichnung Auto-ID-Systeme bereits vermuten lässt, darin, automatisiert Objekte (bspw. Personen, Tiere, Güter, Waren, Gegenstände, ...) zu identifizieren und sie für Maschinen lesbar zu machen.

#### EU fördert Internet der Dinge in Unternehmensumgebungen

Das Arbeitsprogramm Objective 1.3 der Europäischen Union (EU) soll pervasive und sichere Netzwerk – und Servicestrukturen beim Internet der Dinge bereitstellen.

„Wir wollen den breit angelegten Austausch auf der Ebene von Best Practices zwischen den Unternehmen insbesondere bei der Nutzung von RFID-Technologien umfassend fördern“, sagt Florent Frederix, Head of Sector DG Infso, bei der Europäischen Kommission. Dazu haben die Experten in Brüssel ein für die kommenden beiden Jahre umfassendes Rahmenprogramm ausgearbeitet.

Das Programm sieht in zwei Tranchen ein Volumen von insgesamt 557 Millionen Euro vor. „Die unvorhersehbare Nutzung der ursprünglichen internet-basierten Netzwerkstruktur ist an ihre Grenze gestoßen, was den Bedarf von neuen technolo-

gischen Architekturen nach sich zieht“, sagt Frederix.

Da das Internet der Dinge sich jedoch vielerorts noch in der Forschung und Entwicklung befindet, setzt man in Brüssel vor allem auf die mobile Vernetzung von Gegenständen und Prozessen. Besonders ersichtlich wird dieser Trend gerade bei den weltweit vernetzten Lieferketten. Als Schlüsseltechnologie beziehungsweise klares Zuggpferd gilt die Radio Frequency Identification (RFID).

Um die Ansätze auf eine breite Grundlage zu stellen, sind neben europäischen Ländern auch Drittstaaten wie USA, Japan, Südkorea, China und Indien mit in das Rahmenprogramm integriert. Ein besonderes Augenmerk legt die EU nach Aussage von Florent Frederix auf die Entwicklung von globalen Business Standards, und zwar gemeinsam im Zuge der europäisch-transatlantischen Lighthouse Initiative (Transatlantic Economic Council (TEC) Lighthouse Project on RFID).



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

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

## Grundlagen der RFID-Technologie

### Systembestandteile

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

### RFID-Datenträger

Der RFID-Datenträger wird meist unter dem Begriff Transponder (transmit und response) verwendet. Ein RFID-Transponder besteht aus einem Mikrochip. Dieser Chip ist mit einer Antenne (Spule oder Dipol) versehen, die mit dem entsprechenden Lesegerät kommuniziert. Über ein elektronisches Kopplungsverfahren werden alle Daten per Modulation ausgetauscht. Die Energieversorgung der Transponderchips wird bei vielen RFID-Systemen ebenfalls über die Kopplung realisiert. Bei den RFID-Transpondern wird auch häufig von RFID-Chips, – tags, – labeln oder – etiketten gesprochen.

In biometrischen Authentifikationssystemen werden die RFID-Transponder als Datenspeicher für technische Abbilder von persönlichen Körpermerkmalen genutzt. Sie werden als Schlüssel bei den autorisierten Personen getragen. Diese Arten von Transpondern können in Plastikkarten, z.B. kontaktlosen Chipkarten einlaminiert werden.

Bei der Art der Informationsverarbeitung im Transponder gibt es ein breites Spektrum zwischen Low-End – und High-End-Systemen:

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

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

## Sicherheit von RFID-Systemen

Die Datensicherheit spielt beim Einsatz von RFID eine große Rolle. Dabei ist entscheidend, ob die Daten auf dem Chip gespeichert sind oder der Chip nur eine Nummer trägt, zu der Daten im System hinterlegt sind. Daten auf einem Transponder kann prinzipiell jeder abrufen, der mit einem Lesegerät Kontakt zum Transponder aufbauen kann. Um die Daten vor fremdem Auslesen zu schützen, können der Zugriff oder die Daten beispielsweise durch Passwörter oder Chiffrierung gesichert werden. Allerdings benötigen kryptologische Verfahren Speicherplatz und Rechenleistung und machen so den Transponder teurer. Im System hinterlegte Daten können auf herkömmliche Weise gesichert werden, beispielsweise mit einer Firewall.

### Angriffe auf den Transponder

Inhalt fälschen

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

Identität fälschen (Transponder)

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

Deaktivieren

Durch unautorisierten Gebrauch von Lösch – oder Kill-Befehlen oder durch physische Zerstörung wird der Transponder unbrauchbar gemacht. Als Folge dieses Angriffs kann das Lesegerät die Identität des



# RFID und Datensicherheit

Durch die Speicherung personenbezogener Daten in einem RFID-System kann die Datensicherheit der passiven Partei bedroht sein:

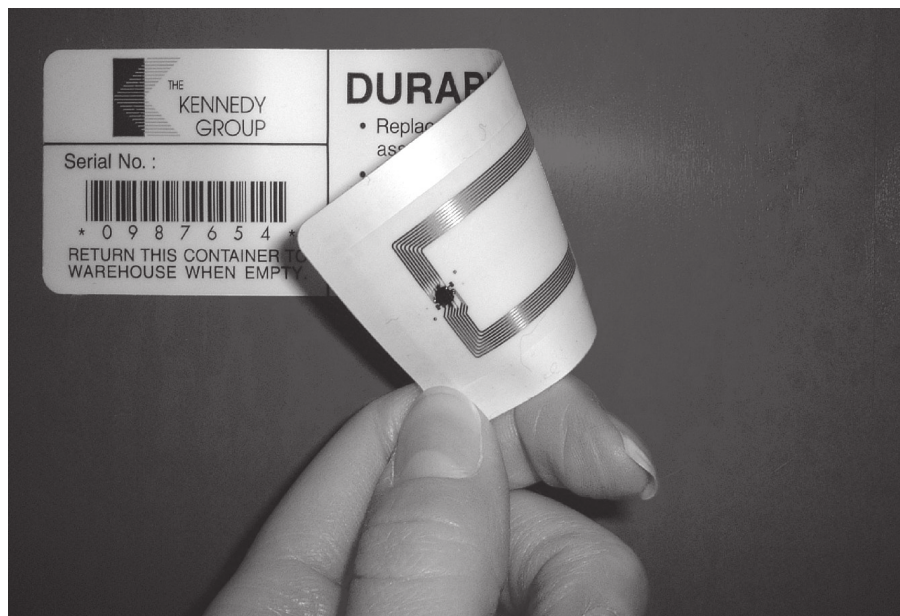
Ein potenzieller Angreifer kann sich durch Abhören der Luftschnittstelle oder unautorisiertes Auslesen von Tags unberechtigt Zugang zu Daten verschaffen.

Aufgrund der zunehmenden Dichte der von Personen hinterlassenen Datenspuren könnten neben personenbezogenen Daten auch potenziell personenbezogene Daten zu einem Angriffsziel werden. Potenziell personenbezogene Daten sind anonymisierte Daten, die durch Kombination von Daten mit hoher Wahrscheinlichkeit treffend einzelnen Personen zugeordnet werden können.

Mit der steigenden Verfügbarkeit der Daten steigt auch das Risiko, dass die Datenbestände ohne Wissen der Betroffenen zu nicht bestimmungsgemäßen Zwecken ausgewertet werden. Insbesondere kann ein neuer Bedarf an Auswertungen der Daten entstehen (bei der aktiven Partei oder bei einer Drittpartei, z. B. auch bei staatlichen Kontrollinstanzen), die möglicherweise nicht im Interesse der passiven Partei liegen.

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

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



## 1-Bit-Transponder

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

## Read-only-Transponder

Diese Transponder sind mit einem Mikrochip ausgestattet, auf dem eine eindeutige Seriennummer gespeichert ist. Diese wird in der Regel bereits bei der Produktion des Transponders generiert. Sobald sich ein solcher Transponder im Empfangsbereich eines Erfassungsgerätes befindet, beginnt dieser ständig seine Seriennummer zu senden (unidirektionaler Datenfluss). Diese Verfahrensweise ist überall dort

gut geeignet, wo es auf die eindeutige Identifizierung von Objekten ankommt (z.B. Tieridentifikation, Sendungsverfolgung).

## Transponder mit beschreibbarem Speicher

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

## kontaktlose Chipkarten mit Betriebssystem

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

## RFID-Lesegerät

Das Lesegerät besteht je nach eingesetzter Technologie aus einer Lese – bzw. einer Schreib-/ Leseinheit. Die Einheit liest somit Daten vom Transponder und weist diesen gegebenenfalls an, weitere Daten zu speichern. Darüber hinaus kontrolliert das Lesegerät die Qualität der Datenübermittlung. Die Lesegeräte sind typischerweise mit einer zusätzlichen Schnittstelle ausgestattet, um die empfangenen Daten an ein anderes System (z.B. PC, Automatensteuerung oder Authentifikationssystem) weiterzuleiten und dort zu verarbeiten.

Das RFID-Lesegerät, welches die RFID-Transponder in seiner Reichweite erkennt startet die Kommunikation die einem bestimmten Protokoll unterliegt. Diese Informationen werden auf Energiewellen ausgetauscht, wobei das zu übertragende Nutzsignal in ein so genanntes Trägersignal umgewandelt wird. Das zur Kommunikation erzeugte Feld wird auch als RF-Feld (Radio-Frequenz-Feld) bezeichnet.



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

**03.08.2006.** Sicherheitsexperte führt Klonen von RFID-Reisepässen vor. Folgt man den Ausführungen von Unternehmen und Behörden, sind die neuen elektronischen Reisepässe, bei denen Daten auf RFID-Chips gespeichert werden, sicher. Offensichtlich ist dies aber nicht der Fall: Nachdem bereits Anfang des Jahres Mitarbeiter einer niederländischen Sicherheitsfirma im Fernsehen gezeigt hatten, wie sich die zwischen Ausweisdokument und RFID-Lesegerät übertragenen Daten abhören und innerhalb weniger Stunden entschlüsseln lassen, führt ein deutscher Sicherheitsexperte derzeit auf der "Black Hat Briefings and Training USA 2006" in Las Vegas vor, wie die auf den RFID-Chips hinterlegten Daten kopiert und in ein anderes elektronisches Ausweisdokument eingelesen werden können. "Die derzeitige ePass-Architektur ist ein einziger Hirnschaden", echauffiert sich Lukas Grunwald gegenüber dem Online-Magazin Wired News. "Aus meiner Sicht sind RFID-Pässe eine riesige Geldverschwendung, da sie in keinerlei Hinsicht die Sicherheit erhöhen", erklärt der Geschäftsführer der Hildesheimer DN-Systems, ein auf IT-Sicherheitsprodukte und – Dienstleistungen spezialisiertes Beratungsunternehmen.

Grunwald benötigte eigenen Angaben zufolge lediglich zwei Wochen, um herauszufinden, wie sich

die elektronischen Daten eines RFID-Passes auslesen, klonen und auf einen anderen Chip übertragen lassen – auch auf Smartcards, die dann für Zutrittsberechtigungen genutzt werden könnten. Grunwald bediente sich bei seinen Recherchen vor allem aus offiziellen Dokumenten der internationalen Luftfahrtbehörde ICAO, in denen die Systemstandards für ePässe beschrieben sind. Als Lese – und Schreibgerät nutzt der Sicherheitsexperte einen für Grenzkontrollen offiziell zugelassenen RFID-Reader der deutschen ACG Identification Technologies. Als Software kommt das "Golden Reader Tool" (GRT) zum Einsatz, das den Anforderungen der ICAO entspricht. Nachdem Grunwald die Daten eines RFID-Passes mittels dieser Hard – und Software ausgelesen hat, brennt er zunächst das ICAO-Layout auf einen neuen RFID-Tag, sodass die Basisstruktur des Chips den offiziellen Anforderungen entspricht. In einem nächsten Schritt wird der Chip dann über das selbst entwickelte Programm RFDump mit den kopierten Daten gefüttert. Laut Grunwald erhält man so ein Dokument, das elektronische Pass-Lesegeräte nicht vom Original unterscheiden können.

Die häufigsten Verfahren Nutztiere mit RFID-Chips zu kennzeichnen funktionieren mittels Halsbandtranspondern, Ohrmarken und injizierbaren Transpondern.

### Objektidentifikation (Produktionsgüter, Waren, Gegenstände)

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

Einer der wichtigsten und vielseitigsten Anwendungsgebiete von RFID-Systemen ist deshalb genau dieser Bereich, angefangen beim RFID-Einsatz zur Kontrolle des Warenflusses (Ein – und Ausgangskontrollen an jedem Glied der Lieferkette) bis zur RFID-System gestützten Fälschungs – und Diebstahlsicherung.

- Durch die Kennzeichnung jeder einzelnen Ware („item level tagging“) ergeben sich im Verkauf ein großes Potential für Rationalisierungen sowie vollkommen neue Möglichkeiten, z.B. durch:
- Bezahlung an Selbstbedienungsterminals bzw. bezahlen durch einfaches Vorbeiführen des gefüllten Einkaufswagens an einer entsprechenden RFID-Kassenstation, welche alle Waren direkt im Einkaufswagen erfasst und automatisch die Rechnung erstellt oder den Betrag gleich vom Konto des Kunden einbezieht

- Elektronische Preisauszeichnung, d.h. der Artikel sendet seinen Preis an ein Display am Regal, welches diesen darstellt (Preisänderungen würden dann nicht mehr manuell durch den Austausch der Preisschilder erfolgen, sondern bspw. durch Neuprogrammierung der Transponder)angepasste
- Spezialangebote, bspw. können einem Kunden, der in einer Umkleidekabine ein bestimmtes Kleidungsstück anprobiert auf einem Bildschirm dazu passende weitere Kleidungsstücke oder Accessoires präsentiert werden.

**30.09.2008.** Sicherheitsprüfung für elektronische Reisepässe überlistet. Elvis lebt, zumindest wenn man den Scannern für elektronische Reisepässe am Flughafen Amsterdam Glauben schenken darf. In einem Video ( <http://freeworld.thc.org/thc-epassport> ) des Sicherheitsspezialisten Jeroen van Beek (auch als vonJeek bekannt) ist zu sehen, wie der Pass-Scanner einen nachgemachten ePassport ausliest und die Daten des verstorbenen Elvis Aaron Presley nebst Foto auf dem Bildschirm anzeigt. Gelungen ist der Trick laut Beschreibung durch den Einsatz einer Java Card und einem darauf laufendem ePassport-Emulator-Applet sowie durch Ausnutzung von Schwachstellen bei der Verifikation der Daten. Offenbar prüfen die Scanner nicht alle definierten Sicherheitsmerkmale einer Karte, sodass manipulierte Pässe oder solche mit komplett neuen Daten keine Warnung oder einen Alarm auslösen. ... Im derzeitigen Stadium gäben die ePassports seiner Ansicht nach ein falsches Gefühl von Sicherheit.

gen auch in der Nutztierhaltung, qualitativ und quantitativ, sind der Grund, dass bereits seit fast 20 Jahren mehr und mehr auch elektronische Kennzeichnungssysteme in diesem Bereich zum Einsatz kommen. Die Tieridentifikation war und ist eine der wichtigsten Triebfedern für die Entwicklung moderner RFID-Systeme.

### RFID Zapper

RFID Zapper können dazu verwendet werden, einen starken elektromagnetischen Puls (EMP) zu erzeugen. Dadurch können RFID-Chips gewaltsam (aber im Gegensatz zur Zerstörung in einer Mikrowelle ohne sichtbare Spuren) zerstört werden. Da kein physischer Kontakt zum RFID-Chip notwendig ist, ist es auch denkbar, dass ein RFID-Zapper ohne das Wissen und gegen

den Willen des Besitzers eines Passes verwendet wird.

Ein RFID Zapper arbeitet ähnlich dem Prinzip eines Mikrowellenherdes: Durch eine Spule wird kurzzeitig ein starkes elektromagnetisches Feld erzeugt, ähnlich wie bei einem EMP. Dieses Feld induziert wiederum eine Spannung in der Spule des RFID-Tags, die so hoch sein soll, dass ein Bauelement der Schaltung im RFID-Chip durchbrennt.



Hierzu verwenden wir einen hochkapazitiven und hochvoltigen Blitzkondensator, wie wir ihn in einer billigen Einwegkamera finden, die wir mit einer Spule aus lackiertem Kupferdraht nachrüsten. (Ein zusätzlicher Schalter erwies sich auch als notwendig.) Und schon haben wir ein batteriebetriebenes, handliches Gerät zum Zerstören von RFID-Tags. Die Ziele des Projekts sind ein Proof-of-Concept, der Bau eines funktionsfähigen und optisch ansprechenden Gerätes, sowie eine Dokumentation, so dass jeder sich einen eigenen RFID-Zapper bauen kann. Da das Projekt

bisher so viel positive Resonanz gefunden hat, werden wir wohl auch noch an anderen Umsetzungen des Konzeptes arbeiten, zum Beispiel am Bau eines RFID-Zappers von Grund auf, ohne uns einer Einwegkamera zu bedienen.

## Ausführungen und Bauformen von RFID-Systemen

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

1. Elektronische Identifikation: Das System ermöglicht eine eindeutige Kennzeichnung von Objekten durch elektronisch gespeicherte Daten.
2. Kontaktlose Datenübertragung: Die Daten können zur Identifikation des Objekts drahtlos über einen Funkfrequenzkanal ausgelesen werden.
3. Senden auf Abruf (on call): Ein gekennzeichnetes Objekt sendet seine Daten nur dann, wenn ein dafür vorgesehenes Lesegerät diesen Vorgang abrufen. RFID-Systeme zählen zu den Funkanlagen. Durch die elektronische Identifikation sowie die Eigenschaft, dass Transponder nur auf Abruf Daten übermitteln, grenzen sich RFID-Systeme von anderen digitalen Funktechnologien wie Mobilfunk, W-LAN oder Bluetooth ab.

„Denken sie an den Fall Jakob Boeskov und seine Pseudofirma Empire North, die 2002 als einziger dänischer Aussteller auf der China Police 2002 registriert war, der ersten internationalen Polizeimesse in der Volksrepublik China. Das ungewöhnliche Produkt von Empire North war ein mit einem Werbeplakat beworbener Prototyp namens ID Sniper. Auf dem Poster an dem sonst leeren Ausstellungsstand, den Boeskov doch mit einem mulmigen Gefühl in Beschlag nahm, stand zu lesen: Mit dem Scharfschützengewehr ID Sniper kann ein Projektil mit einem eingebauten GPS-Mikrochip aus sicherer Entfernung in den Körper eines Menschen implantiert werden. (...) Gleichzeitig nimmt ein in das Zielfernrohr eingebauter digitaler Camcorder mit Zoomlinse ein hochauflösendes Bild des Ziels auf. Das Bild wird zur späteren Bildanalyse auf einer Speicherkarte abgelegt. (...)“

Aus GOODBYE PRIVACY,  
Ars Electronica 2007,  
Hatje Cantz



RFID-Systeme müssen mindestens die folgenden Leistungen erbringen:

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

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

Ein RFID-Tag kann in Form und Größe variieren, je nach Modell und Ausführung von wenigen Millimetern bis einigen Zentimetern. Das Aussehen kann von rund und massiv, bis flach und flexibel beliebig angepasst werden. Je nach Anwendungsgebiet unterscheiden sich auch die sonstigen Kennzahlen wie z.B. Funkfrequenz, Übertragungs-



geschwindigkeit, Lebensdauer, Kosten pro Einheit, Speicherplatz und Funktionsumfang. Maßgeblich für die Baugröße sind die Antenne und das Gehäuse. Die Form und Größe der Antenne ist abhängig von der Frequenz bzw. Wellenlänge. Je nach geforderter Anwendung werden Transponder in unterschiedlichen Bauformen, Größen und Schutzklassen angeboten. Im folgenden Abschnitt soll auf die geläufigsten Bauformen von RFID-Transpondern eingegangen werden:

### Disks und Münzen

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

### Glasgehäuse

Die Glastransponder wurden vor allem für die Identifizierung von Tieren entwickelt, denn dieses RFID-Gehäuse kann unter die Haut des Tieres implantiert werden. Das Glasgehäuse ist lediglich 10 bis 32mm lang. Innerhalb des Glasgehäuses befinden sich ein Microchip und ein Chipkondensator zur Glättung der gewonnenen Versorgungsspannung. Die Transponderspule besteht aus nur 0,03mm dickem Draht, welcher auf einen Ferritkern gewickelt ist. Alle Transponderkomponenten sind in einem Weichkleber eingebettet. Nur so kann die mechanische Stabilität und die Haltbarkeit des Transponders gewährleistet werden.

### Schlüssel und Schlüsselanhänger

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

### Kontaktlose Chipkarten

Diese Bauform erlangt immer größere Bedeutung, denn sie hat den Vorteil der hohen Reichweite, welche aus einer großen Spulenfläche resultiert. Für die Herstellung einer kontaktlosen Chipkarte wird ein Transponder z.B. zwischen vier PVC-Folien einlaminiert. Temperaturen von über 100°C und ein hoher Druck lässt die Einzelfolien zu einer unlöslichen Einheit werden. Die kontaktlose Chipkarte basiert häufig auf der Bauform ID-1 (85,72mm x 54,03mm x 0,76mm ± Toleranzen), welche von Kredit – und Telefonkarten bekannt ist.

### Smart Label

Bei der Bauform "Smart Label" handelt es sich um eine papierdünne Transponderbauform. Grundlage für diese Bauform ist eine 0,1mm dicke Plastikfolie, auf welche die Transponderspule durch Siebdruck oder Ätztechnik aufgebracht wird. Die Folie kann anschließend lami-

des Dritten Reiches über seine Tochtergesellschaft DEHOMAG mit dem Hitlerregime zusammengearbeitet zu haben und so durch die Lieferungen der Hollerith-Rechner und der Lochkartentechnik den Holocaust logistisch möglich gemacht zu haben.

### SOMARK

SOMARK Innovations hat eine passive RFID-Technik entwickelt, mit der sich Tiere – und auch Menschen – markieren lassen. Der wichtigste Bestandteil ist eine unsichtbare »RFID-Tinte«, die auf die Haut aufgetragen wird. Die Tinte dringt nur in die obersten Hautschichten ein. Die Informationen, die in der Markierung gespeichert sind, lassen sich mit einem Lesegerät erfassen. Dabei beträgt die Reichweite etwa 120 Zentimeter. Wie viele Informationen sich in einem »Tattoo« speichern lassen, hängt von der Größe der Fläche ab, auf welche die Markierung aufgebracht wird. Angeblich können derzeit 15-stellige Zahlen gespeichert werden. Einsatzgebiete der Technik sind laut Somark die Landwirtschaft und der Lebensmittelhandel. So lassen sich mit der Tinte beispielsweise Schlachttiere markieren. Anwendbar sind die Tattoos auf „lebendem Gewebe“, Metall, Glas, Plastik, Papier, Holz, Karton und Flüssigkeitsverpackungen. Aber auch das Militär kommt als Nutzer in Frage: So könnten Soldaten mit einer RFID-Kennung versehen werden, statt der üblichen Erkennungsmarke aus Metall, auf der Name, Blutgruppe und ID-Nummer eingepägt sind.

Nachdem SOMARK 2008 zum „Young Entrepreneur Of The Year“ erklärt wurde, schlossen sie im Februar 2009 einen Finanzierungsvertrag mit Finistere Ventures und T2 venture capital. Andere Investoren sind Med-Pharmex Animal Health und St. Louis Arch Angels. Es geht um die Weiterentwicklung und Patentierung einer chiplosen Tätowierung für

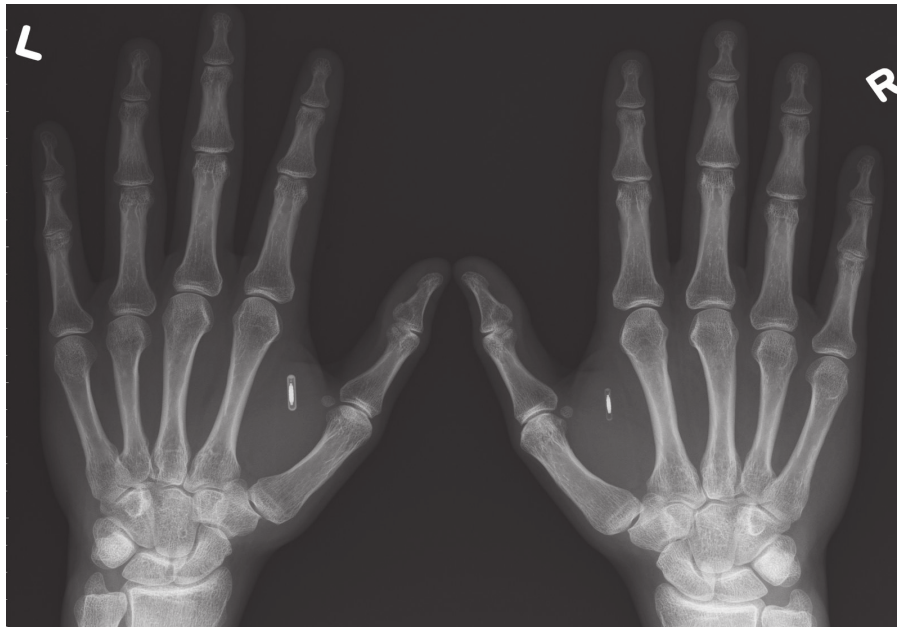
ein Tier-Identifikationssystem, welches vorläufig zur besseren Kontrolle und Identifikation von Lab Animals angewendet werden soll:

“This financing will enable the product development of our lab-animal identification system that will improve drug development processes. The goals of our lab-animal product are to decrease the costs of drug development and to increase the accuracy of pre-clinical data.” Mark C. Pydynowski, SOMARK President.

### Tieridentifikation

Die visuell lesbaren Ohrmarken sind die am weitesten verbreitete Art und Weise der Kennzeichnung bei Nutztieren (Rinder, Schweine, Schafe und Ziegen). Wachsende Anforderun-



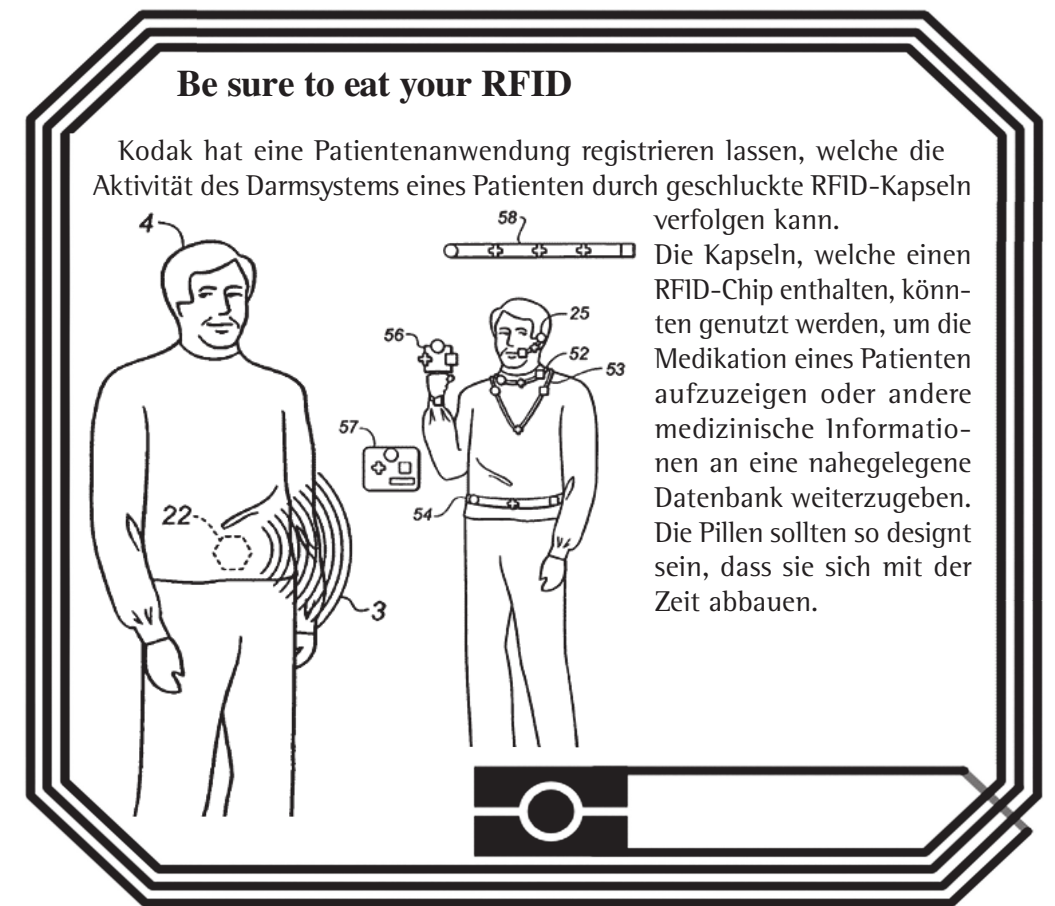


### Verichip Corporation

„The roots of VeriChip trace back to the events of September 11, 2001 when New York firemen were writing their badge ID numbers on their chests in case they were found injured or unconscious. It was evident there was a desperate need for personal information in emergency situations and that an injectable RFID microchip could help patients.“ So beginnt die Geschichtsschreibung der Verichip Corporation selbst. Inzwischen sind ihre Dienstleistungen unterteilt in Veri-Med, die Verichip-Anwendung zur Patientenkontrolle, und VeriTrace, vielversprechend „emergency management“ genannt. VeriTrace wird da zum Beispiel für die Vereinfachung des Leichenerkennungsprozesses während des Hurricane Catrina gelobt; die einzelnen Körperteile wurden gechipt, und waren einfacher verfolgbar. Ausserdem ist Verichip natürlich auch als „infant protection“, „wander prevention“, „tool & equipment monitoring“, „asset tracking“ und „vibration monitoring“ anwendbar.

Die „We the people will not be chipped“-„No Verichip inside“ – Bewegung, welche eine Homepage führt und vor allem Aufklärungsarbeit in Sachen Verichip leistet, weist auf die Verknüpfung der Verichip Corporation mit IBM hin. Das Verichip Patent hält Digital Angel, die 75% ige Tochterfirma von Applied Digital Solutions (ADSX). Diese Tochterfirma wäre 2003 fast in die Hände des Computerriesen IBM gefallen, da ADSX 77 Millionen Schulden bei IBM zu begleichen hatte, von welchen 46 Millionen überfällig waren. IBM hielt Digital Angel dazumals als Pfand. Um das Patent zu behalten, verkaufte ADSX flugs 25 Millionen Aktien. Danach stiegen die Aktien um 37%.

Das Interesse von IBM am Verichip wird von „we the people will not be chipped“ mit IBM`s langer Geschichte der Entwicklung von Massenkontroll- und Identifikationstechnologie in Verbindung gebracht. Im Februar 2001 veröffentlichte der amerikanische Autor Edwin Black das Buch IBM und der Holocaust. In diesem wirft er IBM vor, während



niert und mit einem Kleber beschichtet werden und so als Selbstklebeetiketten in verschiedenen Bereichen zum Einsatz kommen (z.B. Gepäckstücke, Pakete und Waren aller Art). Vorteil dieser Transponder ist, dass nachträglich weitere Daten mit bereits gespeicherten Daten verknüpft werden können, da die Klebeetiketten auf der Vorderseite bedruckbar sind (z.B. Barcode).

## Funktionsweise

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





Dieser Armreif leuchtet rot auf, wenn er ein RFID-Scanner-induktionsfeld entdeckt. Er besteht aus Kupferdraht, Kondensator und LED. In einem Eingang z.B. zu einem Kaufhaus leuchtet er rot auf, wenn es sich bei den am Eingang aufgestellten Induktions-Systemen nicht um herkömmlichen Diebstahlschutz, sondern um RFID-Lesegeräte (im Bereich 13,56 MHz) handelt.

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

### Reichweite

Grundsätzlich kann gesagt werden, dass eine größere Reichweite auch mit größeren Aufwand verbunden ist, denn je größer die Reichweite, desto mehr potentielle Störquellen können auf das RFID-System einwirken.

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

Bei Close-Coupling-Systemen liegt die Reichweite im Bereich bis zu einem Zentimeter. Close-Coupling-Systeme können in Abhängigkeit von der Kopplung auf nahezu beliebigen Frequenzbändern (von Niederfrequenz bis 30MHz) betrieben werden. Die Datenübertragung erfolgt bei Close-Coupling-Systemen entweder über eine induktive oder – möglich bei einer sehr geringen Entfernung zwischen Transponder und Lesegerät – über eine kapazitive Kopplung. Diese RFID-Systeme werden in Bereichen mit hohen Sicherheitsanforderungen eingesetzt,



**1. August 2007.** RFID-Pass. Hack den Chip, lass RFID-Reader abstürzen. ... Daher dürfte es die Entwickler der teuren Technologie interessieren, dass RFID-Experte Lukas Grunwald eine Methode gefunden hat, mit der man mittels manipuliertem Chip die Lesegeräte zum Abstürzen bringen kann. Und was man abstürzen lassen kann, kann man auch exploiten, so Grunwald. Bereits letztes Jahr demonstrierte Grunwald, wie RFID-Pässe unautorisiert ausgelesen werden können – die Schwachstellen im Design ermöglichen auch das Klonen der gespeicherten Daten. Und eben auch, um die Lesegeräte zum Abstürzen zu bringen. Zu diesem Zweck spielte Grunwald ein manipuliertes JPEG-Bild auf den Chip. Beim Versuch, das Passbild elektronisch auszulesen, stürzten zwei unterschiedliche Lesegeräte für RFID-Pässe ab. Wenn mit manipulierten Bilddaten ein Lesegerät zum Absturz gebracht werden kann, bestehen auch Möglichkeiten, über Code-Injections die Geräte “nur” zu manipulieren, schlussfolgert Grunwald. Damit könnten die Geräte beispielsweise dazu gebracht werden, abgelaufene oder ungültige Pässe dennoch zu akzeptieren. Grunwald geht davon aus, dass die meisten Lesegeräte Standardbibliotheken zum Auslesen der JPEG-Daten verwenden und die Anfälligkeit bei den meisten Readern gegeben ist. Grundsätzliche Sicherheitsprinzipien fehlen bei den RFID-Pässen, so Grunwald. Möglich ist auch das Klonen der Chips, theoretisch wäre durch den JPEG-Exploit vielleicht sogar ein Angriff auf den (Windows)-Rechner möglich, an dem das RFID-Lesegerät angeschlossen ist. Einmal mehr wird eine “Sicherheits”-Technologie damit zur Quelle von größerer Unsicherheit.

Auge von außen nicht sichtbar. Der Chip kann auch außerhalb des Körpers, als Bestandteil von Uhren oder Schmuck, getragen werden; so ist er im Bedarfsfall leicht abzulegen. Da der Transponder mittels Induktion mit Energie versorgt wird, benötigt er keine Batterien. Wird der Chip auf der richtigen Frequenz angesprochen, antwortet er mit einer eindeutigen sechzehnstelligen Nummernfolge, die den Träger des Chips in einer Datenbank identifizieren kann. So können beispielsweise Zugangsberechtigungen abgefragt werden oder auf medizinische oder andere Unterlagen zur Person zugegriffen werden. Der VeriChip ist der erste RFID-Chip, der von der US-amerikanischen Food and Drug Administration für den Implantationseinsatz am Menschen zugelassen wurde. Die FDA-Zulassung erfolgte 2002. Bis zum Januar 2006 hatten 68 Krankenhäuser in den Vereinigten Staaten Verträge unterzeichnet, um die neue Technologie in ihren Notfallaufnahmen nutzen zu können. Allerdings haben einige von ihnen ihre Versuche wegen mangelnder Akzeptanz auf Patientenseite und wegen der möglichen Verletzung der Privatsphäre bereits wieder aufgegeben. Das Unternehmen schätzt, dass weltweit etwa 2000 Personen einen VeriChip tragen. Am 10. Februar 2006 verwendete erstmals ein Überwachungsunternehmen in Cincinnati VeriChips, um den Zugang zu ihrem Rechenzentrum zu steuern.



Neben Accenture hoffen Konzerne wie EADS, BAE Systems oder Sagem Sécurité auf lukrative Aufträge aus den Mitgliedsstaaten.

Im vergangenen Jahr betrug der Umsatz mit elektronischen Grenzkontrollsystemen in der EU 250 Mio. Euro. Für 2015 rechnen Analysten mit 400 Mio. Euro. Das ist vorsichtig geschätzt: Den USA war die elektronische Aufrüstung ihrer Grenzen 2004 über fünf Jahre immerhin 10 Mrd. \$ wert.

Die wichtigsten Abnehmer von Iris – oder Fingerabdruckscannern sind Flughäfen. Schon heute stecken sie rund vier Fünftel ihrer Sicherheitsbudgets in Anschaffung und Unterhalt biometrischer Kontrollsysteme. Die EU mag sich davon einen Rückgang illegaler Einwanderung erhoffen, den Flughafenbetreibern geht es vor allem um eins: Zeit – und damit Kostenersparnis beim Abfertigen der Reisenden.

### Krankenhäuser

Passive, wieder verwendbare Transponder (geschlossenes System), vor allem in Form RFID-Chip versehener Armbänder oder Armbanduhren, RFID-Etiketten oder kontaktlose ISO Karten werden verwendet, um Patienten zu „kennzeichnen“ und zu identifizieren und Patienten-daten bspw. über den Personal Digital Assistant (PDA) des Arztes mit dem Patienteninformationssystem im Krankenhaus zu koppeln. Im einfachsten Fall erfolgt diese Kopplung über eine auf dem Chip gespeicherte eindeutige ID. Darüber hinaus können allerdings auch weitere Daten wie Blutgruppe, Allergien u.ä. hinterlegt werden.

### Verichip

Der VeriChip (Produktbezeichnung: VeriMed) ist ein passiver RFID-Transponder, der sich zur Implantierung in Menschen und

Tiere eignet. Hergestellt wird er von der VeriChip Corporation, einem 100%igen Tochterunternehmen von Applied Digital Solutions in Delray Beach, Florida. Der Transponder befindet sich in einem etwa 12 mm langen und 2 mm dicken Glaszylinder, der beim Menschen üblicherweise oberhalb des Trizeps unter die Haut des rechten Armes eingepflanzt wird. Ebenfalls gebräuchlich ist die Einpflanzung in die Hautfalte zwischen Daumen und Zeigefinger. Das Ein – und Herausoperieren geschieht unter lokaler Betäubung und kann problemlos ambulant erfolgen. Der Chip ist mit bloßem

Annalee Newitz und Jonathan Westhues hackten an der HOPE Number Six conference in New York den Verichip. Newitz implantierte sich den Verichip in ihren rechten Oberarm, woraufhin Westhues ihn mit einem handelsüblichen RFID Reader auslas. Dann scannte er ihn nochmals mit einer selbstgebastelten Antenne, welche mit seinem Laptop verbunden war, der das Signal des Chips aufnahm. Dann las er mit demselben Reader das Signal vom Laptop und prompt spuckte der Newitz's eindeutige ID Nummer aus. Verichip antwortete darauf mit der Aussage, es sei immer noch sehr schwierig, einen Verichip zu klonen. John Procter, Verichip-Pressesprecher: 'We can't verify what they may or may not have done....We haven't seen any first-hand evidence other than what's been reported in the media.' (Sat Jul 22, 2006) und: «VeriChip is an excellent security system, but it shouldn't be used as a stand-alone,“ er empfiehlt, auch gleich noch die ID-Karte zu kontrollieren.

Annalee Newitz ist Autorin und Journalistin, sie schrieb einen Artikel namens „the RFID hacking underground“, in welchem sie mit Jonathan Westhues den verschiedenen möglichen RFID-Hacks nachging.



beispielsweise bei Chipkarten mit Zahlungsfunktion oder im Bereich der Zutrittskontrolle.

Remote-Coupling-Systeme verfügen über eine Reichweite von bis zu ca. einem Meter. Sie arbeiten typischerweise im Frequenzbereich unter 135 kHz sowie bei 13,56MHz. Die Kopplung zwischen Lesegerät und Transponder erfolgt induktiv.

Als Long-Range-Systeme werden RFID-Systeme mit Reichweiten von über 1,5 bis typischerweise zehn Metern bezeichnet. In Ausnahmefällen sind auch höhere Reichweiten möglich: etwa 100 Meter oder sogar 1 Kilometer, wie sie im Frequenzspektrum um 5,8 GHz, das sich derzeit in einem sehr frühen Entwicklungsstadium befindet, erreicht werden können. Die Reichweiten von Long-Range-Systemen werden im Mikrowellenbereich, im 868/915-MHz – Bereich sowie im 2,45-GHz-Bereich erreicht. Long-Range-Systeme unterscheiden sich von den beiden zuvor Genannten durch die Energieversorgung der Transponder (aktiv) und der Datenübertragungsverfahren (Backscatter).

### Speichertechnologie

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

Read-only-Transponder: Diese Transponder können nach dem Programmiervorgang beim Hersteller vom Lesegerät nur gelesen werden. Sie sind kostengünstiger in der Herstellung. Die variable Information, die mit dem Tag assoziiert werden soll, muss in einer Datenbank im Backend des RFID-Systems abgelegt werden. Beim Auslesen des Tags wird diese Information anhand der ID-Nummer (Seriennummer) des Tags aus der Datenbank abgerufen.

Read-write-Transponder: Diese Transponder beinhalten einen Speicher und sind daher teurer in der Herstellung. Es können leistungsfähige Sicherheitsmechanismen implementiert und auch variable Informationen auf dem Transponder durch das Anwendungssystem neu gespeichert werden.

### Energieversorgung der Transponder

Grundsätzlich gibt es zwei Transpondertypen sowie Mischformen beider Typen:

Aktive Transponder haben eine eigene Energiequelle zur Erzeugung elektromagnetischer Wellen. Sie sind batteriebetrieben, befinden sie sich jedoch solange im Ruhezustand bis sie von einem Lesegerät ein Aktivierungssignal empfangen. Dadurch kann die Lebensdauer der Energiequelle erhöht werden. Aktuell sind Transpondertypen mit internem Speicher bis zu 1 Million Bytes erhältlich.

Passive Transponder werden dagegen bei Lesevorgängen über Funkwellen durch die Lesegeräte mit Energie versorgt. Sie haben eine geringere Reichweite als die aktiven Transponder. Für die Energieversorgung

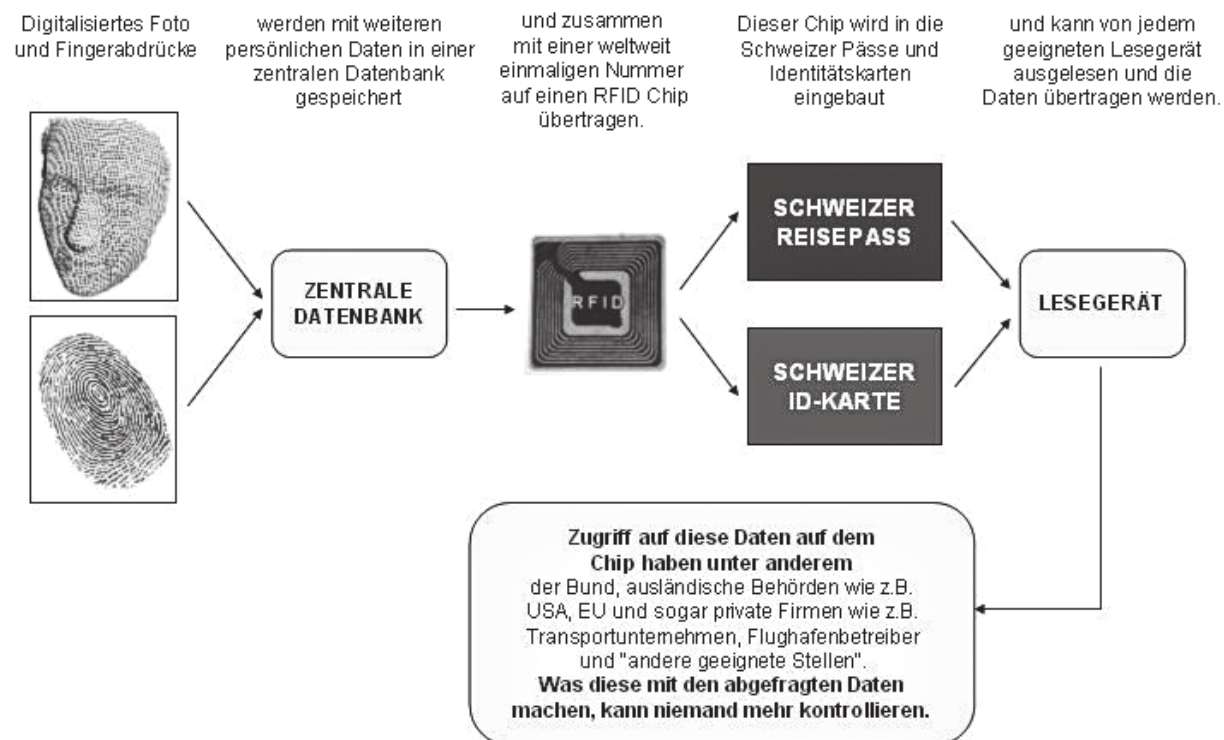
des passiven RFID-Transponders sind besonders leistungsstarke Lesegeräte als aktive RFID-Systeme notwendig. Es können deutlich weniger Informationen als bei aktiven Tags gespeichert werden.

## Anwendung

### Personenidentifikation (Personenbezug)

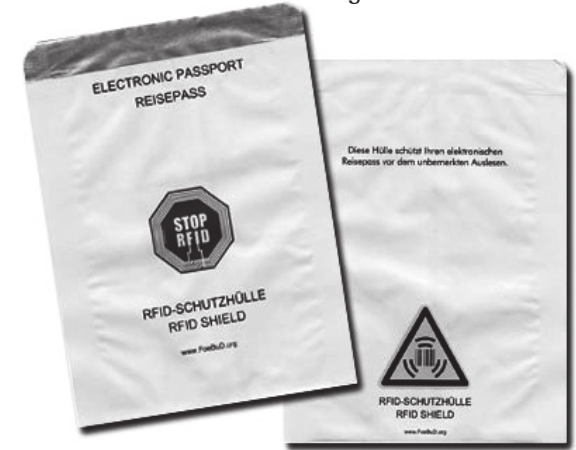
Seit 1997 befasste sich die ICAO, eine Unterorganisation der Vereinten Nationen, mit der Einführung von elektronisch auswertbaren biometrischen Merkmalen in Reisedokumenten. Im Jahre 2003 führte dies zur Vorstellung einer unter der Bezeichnung „Blueprint“ bekannt gewordenen Empfehlung. Sie hält die UN-Mitgliedsstaaten dazu an, zukünftig biometrische Merkmale der Inhaber elektronisch auf dem Reisedokument zu speichern. Die Kriterien für die Auswahl der zu verwendenden Techniken sind weltweite Interoperabilität, Einheitlichkeit, technische Zuverlässigkeit, Praktikabilität und Haltbarkeit. Die vier zentralen Punkte des „Blueprint“ sind die Verwendung von kontaktlosen Chips (RFID), die digitale Speicherung des Lichtbilds auf diesen Chips, wobei weitere Merkmale wie Fingerabdrücke oder Irismuster ergänzt werden können, die Verwendung einer definierten logischen Datenstruktur (Logical Data Structure, LDS) und ein Verfahren zur Verwaltung von digitalen Zugangsschlüsseln (Public Key Infrastructure, PKI). Die Vorgaben wurden in der Weiterentwicklung des Standards 9303 der ICAO zusammengefasst.

Am 13. Dezember 2004 beschloss der Rat der Europäischen Union auf politischen Druck der USA, die mit dem Wegfall der Visumsfreiheit für europäische Reisende drohten, die Pässe der Mitgliedsstaaten gemäß diesem Standard mit maschinenlesbaren biometrischen Daten des Inhabers auszustatten.



### Schützen Sie Ihre persönlichen Daten, die auf einem RFID-Chip im neuen Reisepass gespeichert sind, vor unbefugtem Zugriff.

Unser Gag, die 'RFID-Schutzfolie', die ja nur ein kleiner Sarkasmus sein sollte, ist nun in funktionierende Wirklichkeit umgesetzt: Tatsächlich steckt in dieser Hülle Technologie, die wirklich und ernsthaft verhindert, dass Schnüffelflips ausgelesen werden können. Die Planung der Herstellerfirma ist, dass damit einmal Geldbörsen und Lederhüllen für ePässe und RFID-Karten ausgestattet werden. Die Passschutzhülle besteht aus einer mit Metall beschichteten Folie. Auch im Innenministerium wird diese Folie zum Schutz von Pässen und Hausausweisen verwendet!



### Europäischer ePass

Der Europapass besteht aus einem bordeauxroten Umschlagdeckel mit goldfarbener Prägung, den eigentlichen Inhaltsseiten sowie der Datenseite, die die persönlichen Daten des Antragstellers enthält. Im Falle des deutschen PASSES ist die Datenseite eine Kunststoffkarte (die Reisepasskarte), in der sich das Papier-Inlett sowie das Identigramm®-Merkmal befinden.

### Schweizer ePass

Der Pass 06 wird bereits seit 2006 für visumsfreie Reisen in die USA ausgestellt. Nachdem am 17. Mai 2009 die definitive Einführung des PASSES 10 und die zentrale Speicherung der Fingerabdruckdaten an der Urne mit einem Mehr von 50.1% knapp bestätigt wurden, soll der Pass 06 mit der definitiven Einführung biometrischer ePässe durch den Pass 10 abgelöst werden, der auf dem Funkchip zusätzlich zwei Fingerabdrücke speichert. Ob die Versprechen, dass die ID weiterhin ohne Chip erhältlich sein wird, und die Fingerabdruckdaten nicht zur Fahndung verwendet werden, gehalten werden, wird die Zukunft zeigen.

### Grenzübertritt mit dem biometrischen Ausweis in Europa

Bis 2015 will Europa ein ähnliches Register wie die USA schaffen, in dem sich Ausländer bei der Einreise mit Fingerabdruck und Foto identifizieren müssen. Auch EU-Bürger sollen ermuntert werden, die biometrischen Daten ihres PASSES bei der Abfertigung zu nutzen. Dafür müssen rund 1800 Kontrollposten in der Union umgerüstet werden.