

RFID-Chips

**Sie sind im neuen Reisepass,
sie wurden schon heimlich in
Payback-Karten eingesetzt.
Vielleicht gibt es sie bald überall...**

Was ist RFID?

RFID-Etiketten sind winzige Computerchips mit Miniantennen, die an physischen Objekten angebracht werden



RFID-Etikett im „Future Store“ der Metro AG

können. Bei den am meisten beworbenen Anwendungen von RFIDs enthält der Mikrochip einen elektronischen Produktcode (Electronic Product Code, EPC), der lang genug ist, jedes weltweit hergestellte Produkt eindeutig zu identifizieren. Wenn ein RFID-Lesegerät ein Funksignal abgibt, antworten in der Nähe befindliche Chips, indem sie die auf ihnen gespeicherten Daten an das Lesegerät übermitteln. Bei passiven (batterielosen) RFID-Etiketten kann

die Leseentfernung von ca. einem Zentimeter bis ungefähr fünf oder zehn Meter variieren, während aktive, mit einer eigenen Energiequelle ausgerüstete Etiketten eine weit größere Leseentfernung haben können. Typischerweise werden die Daten an ein System von vernetzten Computern gesandt, die zum Beispiel im Management von Versorgungsketten oder bei der Inventarkontrolle eines Lagers eingesetzt werden.

Gefahren für Privatsphäre und Bürgerrechte

Obwohl es sinnvolle Einsatzmöglichkeiten für RFID gibt, können Eigenschaften dieser Technologie so genutzt werden, daß Privatsphäre, Bürgerrechte und Datenschutz gefährdet sind.

- Versteckte Anbringung von Etiketten: RFID-Etiketten können in oder an Objekten und Dokumenten angebracht werden, ohne dass die Person, die diese Objekte erwirbt, davon Kenntnis hat oder erhält. Da Funkwellen ganz leicht und geräuschlos durch Gewebe, Plastik und andere Materialien dringen können, ist es möglich, RFID-Etiketten auszulesen, die in die Kleidung eingenäht oder auf Objekten angebracht sind, die sich in Geldbörsen und Brieftaschen befinden, in Einkaufstaschen, Koffern und anderes mehr.
- Einzigartige Identifikationsmerkmale für alle Objekte weltweit: Der elektronische Produktcode ermöglicht es potentiell, dass jeder einzelne Gegenstand auf der Erde seine eigene, einzigartige ID bekommt. Der Gebrauch von einzigartigen ID-Nummern könnte zur Errichtung eines globalen Re-

gistrierungssystems führen, in dem jedes physische Objekt identifiziert und auf seinen Käufer oder Besitzer zum Zeitpunkt eines Kaufs oder einer Übergabe zurückgeführt werden kann.

- Massenhafte Datenzusammenführung: Der Einsatz von RFID erfordert die Errichtung riesiger Datenbanken, die die individuellen, einzigartigen Daten eines Etiketts enthalten. Diese Datensammlungen könnten verbunden werden mit Personenidentifikationsdaten, insbesondere mit den immer weiter steigenden Speicherkapazitäten und Prozessorleistungen.
- Versteckte Lesegeräte: Die Etiketten können aus einiger Entfernung ausgelesen werden, auch durch Sichtbarrieren hindurch, und von Lesegeräten, die unsichtbar in nahezu jeder Umgebung, in der menschliche

Wesen oder irgendwelche Gegenstände versammelt sind, angebracht werden können. Man hat schon testweise RFID-Lesegeräte in Fußbodenbretter eingebaut, in Teppiche und Bodenmatten eingewebt, in Türrahmen ver-

steckt und nahtlos an Einzelhandelsregalen und Schaltern angebracht, womit es für den Verbraucher nahezu unmöglich wurde, zu erfahren, wann oder ob er oder sie „gescannt“ wurde.

- Individuelle Verfolgung und Profilierung: Wenn persönliche Identität mit einer eindeutigen RFID-Etikettennummer verbunden würde, könnten Personen verfolgt und Bewegungs- und andere Profile von ihnen erstellt werden, ohne dass die Individuen davon wissen oder ihre Zustimmung dazu gegeben haben. Zum Beispiel könnte ein RFID-Etikett, das an einem Schuh angebracht ist, de facto als ein Identifikator der Person dienen, die diesen Schuh trägt. Selbst wenn die Identifikation auf Objekt- oder Produkt-Niveau beschränkt bleibt, könnte die Identifikation eines Gegenstands, den jemand an hat oder bei sich trägt, ihn zum Beispiel mit speziellen Ereignissen wie etwa Demonstrationen in Verbindung bringen.

Aus: RFID-Positionspapier des FoeBud e. V.

Wo gibt es RFID?

Einzelhandel

Erklärtes Ziel der RFID-Lobby ist es, in den kommenden Jahren alles, jede Steckdose, jede Hose, jeden Schuh und jeden Joghurtbecher mit RFID auszustatten. Und jedes Produkt, das mit RFID verkauft wird, ist ein Schritt in diese Richtung. Folgerichtig ist der Handel der wichtigste Partner bei der Einführung der Schnüffelchips. In verschiedenen Ländern werden schon jetzt Bewegungsprofile von Kunden

- Am 22. Februar 2005 gibt die Metro-Gruppe in Düsseldorf bekannt, dass sie bis Ende des Jahres bundesweit in 250 Filialen von Metro-Töchtern wie Real oder Saturn RFID-Technik installieren will. Die Zahl der Lieferanten von entsprechend ausgestatteter Ware solle von derzeit 22 auf 100 erhöht werden, sagte Metro-Vorstandsmitglied Zygmunt Mierdorf in Düsseldorf. (Quelle: dpa) Bis 2007 will die Metro AG alle 800 Warenhäuser und Vertriebscenter mit RFID ausgestattet haben. (Quelle: Chip 03/2004) RFID-Chips sollen laut einer Studie von Forrester Research die Strichcodes bis 2008 weltweit aus den Läden verbannt haben. (Quelle: Chip 02/2004)
- März 2004, Neuss: Angeblich testet

mit RFID erstellt oder es wird erfasst, ob Werbe-Displays, an denen jemand vorbei gegangen ist, direkten Einfluss auf das Kaufverhalten haben (Marktkauf). Wenn die Chips mit dem Kunden den Laden verlassen, sind sie allerdings keineswegs Müll: Sie bleiben aktiv bzw. sie werden weiterhin ihre Daten preis geben, sobald sie angefunkt werden, egal von wem. Noch ist das kein wirklich großes Problem

- ein Textilkaufhaus RFID, die in die Kleidung, z.B. in den Kragensaum eingenäht sind und vom Endverbraucher nicht wie ein Preisetikett einfach entfernt werden können. Wer das ist, konnte bislang nicht in Erfahrung gebracht werden. (Quelle: Eigenrecherche FoeBuD e.V.)
- Als erster Händler weltweit (unbestätigte Einschätzung von Katherine Albrecht) hat die Metro AG ihre Payback-Kundenkarte mit einem RFID-Chip versehen. Nach Protesten des FoeBuD e.V. im Februar 2004 bietet der Konzern 10.000 Kunden an, die Karte gegen eine ohne RFID umzutauschen.
- In Rheinberg bei Duisburg testet die Metro AG seit April 2003 im "Ex-

tra Future Store" an verschiedenen Stellen RFID-Chips: Erstens unter den Preisetiketten von "Philadelphia Frischkäse" (Hersteller: Kraft) und "Pantene Pro V Shampoo"-Flaschen (Procter&Gamble). Zweitens werden im Future Store Tests mit RFID in "Gillette Mach 3" Rasierklingen-Verpackungen durchgeführt. Auf den CDs und DVDs im Future Store befinden sich drittens RFID-Etiketten, die preisgeben, ob eine CD/DVD bezahlt wurde oder nicht. Und viertens werden RFID im Lager des Future Store getestet, diese erreichen aber nicht den Endverbraucher. (Quelle: Metro AG 2004)

tra Future Store" an verschiedenen Stellen RFID-Chips: Erstens unter den Preisetiketten von "Philadelphia Frischkäse" (Hersteller: Kraft) und "Pantene Pro V Shampoo"-Flaschen (Procter&Gamble). Zweitens werden im Future Store Tests mit RFID in "Gillette Mach 3" Rasierklingen-Verpackungen durchgeführt. Auf den CDs und DVDs im Future Store befinden sich drittens RFID-Etiketten, die preisgeben, ob eine CD/DVD bezahlt wurde oder nicht. Und viertens werden RFID im Lager des Future Store getestet, diese erreichen aber nicht den Endverbraucher. (Quelle: Metro AG 2004)

Ausweise und andere Identitätspapiere

RFID in Ausweisen sind für Überwachungs-Trolle besonders effektiv, denn: Das Erfassen eines Menschen über die Gegenstände, die er bei sich trägt (Schuhe, Jacken, Kaugummipackungen) ist recht aufwendig. Schließlich muss zur Zeit noch bei jedem erfassten Schnüffelchip eine Rück-

- Seit November 2005 enthalten die neuen elektronischen und mit biometrischen Merkmalen versehenen EU-Reisepässe (ePässe) in Deutschland einen RFID-Chip. Darauf ist unter anderem das digitale Foto und der digitale Fingerabdruck gespeichert. Das in Deutschland umstrittene Konzept (Lesen Sie die Laudatio zu den BigBrotherAwards 2005) wird inzwischen von der Bundesdruckerei ins Ausland exportiert, zum Beispiel nach Paris und Abu Dhabi und nach Luxemburg. (Quelle: Bundesdruckerei) Die ARD-Sendung "Monitor" stellte am 24.2.2005 in einem Beitrag dar, wie unsicher diese Technologie in neuen Reisepässen ist. Eine zentrale Datenbank der Pässe und Ausweise der EU solle nicht geschaffen

fragen an mehrere Datenbanken gestellt werden: "Wer hat diese Schuhe damals wo mit Kunden-/Kreditkarte gekauft?" Bei Ausweisen ist der Weg direkt: "Wem gehört dieses Ausweispapier?" Auf den ersten Blick erscheint es sinnvoll, dass z.B. die Polizei die Chips in den Ausweisen entschlüs-

werden, heißt es im EU-Einführungs-Beschluss. Was allerdings die Staaten, in die man einreisen will, mit den erfassten Daten machen, entzieht sich jeder Kontrolle. Aber alle Stellen, die Zugriff auf den Chip haben, sollen in ein Register aufgenommen werden, um eine Zweckentfremdung der sensiblen Informationen zu verhindern. Der neue Reisepass ist trotz Bezuschussung durch den Staat etwa doppelt so teuer wie die herkömmlichen Pässe. Das Bundesamt für Sicherheit in der Informationstechnik verweist auf eine Studie, nach der ein Test der "International Biometric Group" Fehlerquoten von bis zu 23 Prozent bei aktuellen RFID-Produkten ergeben hat. "Die Einführungsstrategie ist: erstmal das Visaverfahren, da haben wir in Deutschland schon biometrische Merkmale, und da die technischen Strukturen bei den Einwohnermeldeämtern dann ohnehin vorgehalten werden müssen, werden wohl auch die Personalausweise kommen", sagte der Bundesdatenschutzbeauftragte Peter Schaar. (Quelle: AP, ct und WDR)

- Immer mehr Universitäten und Fachhochschulen spicken ihren Studierendenausweise mit RFID. Ausgelesen werden die Chips meist in den Bibliotheken und in der Mensa, wenn die Studi-Ausweise in die Nähe des Lesegerätes gehalten werden. Fehlen nur noch die RFID-Lese-Antennen in den Türrahmen, dann

seln kann – was auf den zweiten Blick allerdings bedeutet, dass ein Lesegerät neben einer Demonstration innerhalb von Sekunden alle Teilnehmer/innen erfassen kann, ohne dass diese das überhaupt merken. Eine besondere Gefahr für die Wahrnehmung demokratischer Grundrechte!

heißt es "Ich weiß, welches Buch Du liest" - "Den Schein kriegst Du nicht, Du warst ja immer zu spät bei der Vorlesung" - "Ernähr Dich mal gesünder, dann schaffst Du auch Deine Prüfung..." usw.

- Haben Sie auch kürzlich einen neuen Mitarbeiter-Ausweis Ihrer Firma bekommen, den Sie nicht mehr durch einen Schlitz ziehen müssen, sondern der auch von der Jackentasche aus die Türen öffnen kann? Dann können Sie sicher sein: Dieser Ausweis enthält einen RFID-Funkchip. Ist dieser neue Ausweis mit Ihrem betrieblichen Datenschutzbeauftragten und - ganz wichtig - Ihrem Betriebs-/Personalrat abgesprochen worden? Wurden Sie über die Konsequenzen für Ihre Privatsphäre informiert? Die können erheblich sein: "Eines Tages könnten diese Geräte dem Management mitteilen, mit wem Sie sich beim Kaffeeautomaten unterhalten und wie lange Sie auf der Toilette waren – und sogar, ob Sie sich hinterher die Hände gewaschen haben. Es gibt schon ein Produkt mit dem Namen iHygiene, das die Händewaschgewohnheiten von RFID-behafteten Angestellten beim Gang auf die Toilette überwacht." (zitiert aus unserer Übersetzung des ersten Kapitels des Buches "Spychips" von Katherine Albrecht und Liz McIntyre)



Die Kennzeichnung für elektronische Pässe.

Erkennungsdienstliche Behandlung auf den Meldeämtern

Pressemitteilung des Chaos Computer Club e.V. zur Einführung biometrischer Reisepässe vom 04. Oktober 2005

Ab 1. November 2005 wird in Deutschland ein neuer Reisepass (ePass) eingeführt. Er enthält erstmals als biometrisches Datum das Bild des Passinhabers in elektronischer Form. Diese Information wird auf einem Funk-Mikrochip (RFID) gespeichert. Ab dem Jahr 2007 wird zusätzlich der elektronische Fingerabdruck aufgenommen.

Nach einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die neue Technologie weder praxistauglich noch ausgereift. Zudem eröff-



Der Fingerabdruck von Bundesinnenminister Wolfgang Schäuble

net sie neue Formen der Überwachung. Das Ganze muss der Bürger über Steuer-gelder und erhöhte Passgebühren auch noch bezahlen.

Nach und nach werden in den nächsten Jahren alle deutschen Passinhaber auf den Meldeämtern einer Prozedur unterzogen, die der erkennungsdienstlichen Behandlung von Kriminellen gleicht. Ein Bild ihres Gesichtes und ihrer Fingerabdrücke werden aufgezeichnet. In Folge der Einführung der biometrischen Ausweisdokumente wird das Grundrecht auf Informationelle Selbstbestimmung verletzt, denn die im ePass gespeicherten Daten können an internationalen Grenzen ausgelesen und in Datenbanken gespeichert werden. Niemand weiß, wer Zugriff darauf hat und was mit den sensiblen biometrischen Daten weiter passiert.

Es ist nicht erkenntlich, welche Vorteile der ePass bringt. Um Ausweisdokumente fälschungssicherer zu machen, ist die Speicherung neuer personenbezogener Daten nicht nötig. Soll die Überprüfung der Zusammengehörigkeit von Ausweisträger und Ausweis verbessert werden, ist die Erfassung der Fingerabdrücke aller deutschen Staatsbürger unverhältnismäßig. Professionelle Straftäter oder gar Terroristen können weiterhin auf Ausweisdokumente anderer Staaten ausweichen.

Nach Auffassung der Humanistischen Union (HU), des Chaos Computer Clubs (CCC), des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF), der JungdemokratInnen/Junge Linke und des Netzwerk Neue Medien wird hier ein Sicherheitsplacebo mit inakzeptablen bürgerrechtlichen Nebenwirkungen zwangsverabreicht. "Kein Bürger sollte glauben, durch die Biometrie in Ausweisen könnten Terroristen gefangen werden. Schließlich haben die Täter in der Vergangenheit immer einen gültigen Pass besessen," sagt Andy Müller-Maguhn, Sprecher des CCC. Zudem bleibt der Reisepass gültig, wenn der Chip nicht mehr funktioniert.

Doch der ePass ist erst der Anfang. Der nächste Schritt ist der biometrische Personalausweis. "Ohne erkennbaren Sicherheitsgewinn baut die Bundesregierung eine Überwachungsinfrastruktur mit hohem Missbrauchspotential auf. Das entspricht nicht unserem Demokratieverständnis," erklärt Dr. Christoph Bruch, Mitglied des Bundesvorstandes der HU. Biometrische Verfahren und die eingesetzten Funkchips bieten mannigfaltige Möglichkeiten zur Überwachung von Menschen. Und dass einmal installierte Technologien zur Identifizierung und Überwachung die Begehrlichkeiten von Geheimdiensten, Ermittlungsbehörden,

aber auch kommerziellen Unternehmen wecken werden, ist kein neues Phänomen.

Mit dem Argument, die neuen Dokumente seien ein Werkzeug gegen den Terrorismus, findet eine gigantische Verschwendung von finanziellen Ressourcen statt, die weit sinnvoller zur tatsächlichen Terrorismusprävention verwendet werden könnten. Die Kosten von 59 bzw. 91 Euro, die der Passinhaber tragen muss, decken die finanziellen Aufwendungen für die Einführung der biometrischen Pässe dabei nicht einmal.

Wozu also die praxisuntaugliche Technologie, über deren Einführung ohne gesellschaftliche Debatte über die Köpfe der Bürger und des Parlaments hinweg entschieden wurde? Weshalb die überstürzte Einführung? Der Verdacht liegt nahe, dass hier Lobbyisten ganze Arbeit geleistet haben und wirtschaftliche Interessen massiv unterstützt werden sollen. Die marode Bundesdruckerei mit ihren undurchsichtigen Eigentumsverhältnissen und die auf ein Riesengeschäft lauende Biometrieindustrie erwarten blendende Umsätze. Der Bürger hingegen darf sich auf mehr Überwachung, neue digitale Datensammlungen und eine Technik, die nachweislich noch nicht einsatzreif ist, freuen.