



HINTERGRUNDINFORMATIONEN DER GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

ZU

RFID – RADIO FREQUENCY IDENTIFICATION

Transponder (RFID tags) bestehen aus Computerchips mit Prozessor und Betriebssystem und derzeit bis zu mehreren 100 Bit Speicher sowie einem Sender und Empfänger mit Antenne zum berührungslosen Auslesen; die Bauweise der Chips wird bei reduzierter Dicke (kleiner als 100 µm) tendenziell immer kleinflächiger (kleiner als 0,5 mm²). Sie können – im Gegensatz zu Barcodes – auch ohne Sichtkontakt ausgelesen werden. Wegen dieser äußerst geringen Größe werden Transponder für die Bürger in der Regel überhaupt nicht mehr erkennbar und ihre Aktivität nicht mehr bemerkbar sein. Dementsprechend ist ein Schutz vor diesen Geräten kaum möglich.

Angesichts der mit Hilfe von Transpondern erstellbaren personalisierten Einkaufs-, Nutzungs-, Verhaltens- und Bewegungsprofile betont die GI das Recht des Individuums z.B. darauf, nicht in Geschäften und nach dem Kauf eines Gegenstands weiter verfolgt zu werden, wenn Transponder in Waren wie in Kleidungsstücke (Blusen, Hosen, Unterhosen, ...) oder Geldscheine eingewebt ('smart labels' oder 'smart tags') oder in Schlüssel oder Dosen integriert sind.

Die mit den Transpondern möglichen Datenerhebungen sind nach § 86 TKG unzulässig, sofern die Inhalte nicht ausdrücklich für den Empfänger bestimmt sind.

Um die potenziellen Gefahren von Transpondern für die Bürger und die Gesellschaft auf ein Minimum zu reduzieren, fordert die GI:

- 1 Eine formelle technologische Untersuchung und Bewertung der RFID-Technologie vor einer breiten Verwendung (z.B. in Simulationsstudien) unter Einbeziehung aller Interessengruppen einschließlich der Verbraucher – z.B. durch das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB). Weiterhin datenschutzrechtliche Erforschung des Einsatzes von Transpondern. Eine Sachverständigenkommission der Bundesregierung sollte notwendig werdende gesetzliche Regelungen überprüfen.
- 2 Die Einhaltung spezifischer Datenschutzregelungen durch alle Nutzer der RFID-Technologie. Veröffentlichung der jeweiligen Datenschutz-Praxis.
 - Einfache (ohne besondere Geräte) Erkennbarkeit von Transpondern und Lesegeräten (mit den gespeicherten und gelesenen Daten inkl. der technischen Spezifikationen) durch optische und andere Markierungen. Einfache Erkennbarkeit des aktuellen Leseprozesses eines Transponders. Angabe des Nutzungszwecks.
 - Benutzerfreundliches, leichtes Auslesen und Korrigieren der gespeicherten Daten.
 - Anspruch des Käufers auf Entfernung, Deaktivierung oder Zerstörung der Transponder durch den Verkäufer – ohne nachteilige Folgen für den Käufer. (Nicht markierte) Transponder dürfen gesucht und außer Betrieb gesetzt werden.
 - Ein unverzichtbares Auskunftsrecht darf nicht auf das mobile Medium beschränkt werden, sondern muss sich auf alle involvierten Informations- und Kommunikationssysteme erstrecken.

Auch wenn die ausgelesenen Daten (noch) nicht den Begriff der personenbezogenen Daten erfüllen, sollten im Sinn der Vorsorge dennoch die Grundsätze der Vermeidung des Personenbezugs, der Erforderlichkeit und der Zweckbindung auf sie Anwendung finden, wenn zu erwarten ist, dass ein Personenbezug hergestellt wird oder werden kann. Dürften diese Daten frei gesammelt, gespeichert, verbreitet oder



veröffentlicht werden, könnte der nachträglich hergestellte Personenbezug zu großen Benachteiligungen führen.

3 Ein gesetzliches Verbot bestimmter Anwendungen von Transpondern:

- Transponder dürfen in keinem Fall zur Verfolgung von Bürgern genutzt werden können – auch nicht indirekt durch Kleidung, Konsumgüter oder andere Gegenstände wie Pkws. Transponder dürfen generell nicht benutzt werden, um Anonymität zu verringern oder zu verhindern.
- Transponder dürfen nicht an Zahlungsmitteln wie Geldscheinen oder Münzen angebracht werden.

Anderenfalls befürchtet die GI erhebliche Widerstände gegen RFID-Verfahren allein aufgrund der unbeschränkten Überwachungsmöglichkeiten breiter Bevölkerungskreise. Daran kann keiner der beteiligten Hersteller und Anwender ein Interesse haben.

Die Gesellschaft für Informatik (GI) tritt ausdrücklich ein für die Entwicklung, die Herstellung und den Einsatz zukunftssträchtiger Technologien. Sie unterstützt das wirtschaftliche Interesse an der Verfolgung von Objekten z.B. innerhalb einer Logistikkette mit (kontaktlosen) Transpondern (RFID tags). Allerdings kann dies nicht schrankenlos geschehen; vielmehr müssen auch die gesellschaftlichen Folgen berücksichtigt werden.



Technische und organisatorische Erläuterungen

Inhaltsverzeichnis:

1	Funktionsweise und Technik	3
1.1	Passive Transponder	3
1.2	Aktive Transponder	4
2	Erste Bewertung der Transponder-Technik	4
2.1	Nachteile	4
2.2	Vorteile	4
3	Mögliche Angriffe	4
3.1	Angriffe auf die Transponder	4
3.2	Indirekte Angriffe	5
3.3	Überwachung Betroffener	5
3.4	Kommunikation zwischen mobilen Lesegeräten und Transpondern sowie zwischen Transpondern	6
4	Sicherheitsmaßnahmen	6
5	Beispielhafte Anwendungen und Szenarien	6
5.1	Handel, Waren-Logistik	6
5.2	Andere Bereiche	7
6	Literatur	7

1 Funktionsweise und Technik

RFID ist eine Warenmarkierungstechnologie (Transponder) zur Kennzeichnung physischer Objekte, die u.a. den Barcode (Strichcode) auf Waren ersetzen soll. Es werden passive und - zusätzlich mit einer Stromversorgung (Batterie) ausgestattete - aktive Transponder unterschieden.

Zur Kommunikation werden folgende Frequenzen benutzt: Niedrigfrequenz-Bereich (125 KHz und 134.2 kHz), Hochfrequenz-Bereich (13,56 MHz) und UHF-Bereich (868-928 MHz) sowie 2,45 GHz. Höhere Frequenzen ermöglichen geringere Herstellungskosten, eine höhere Schreib-/Lese-Geschwindigkeit sowie eine flachere Form; dies sind Voraussetzungen für die Anwendung von Transpondern im Masseneinsatz.

1.1 Passive Transponder

Gibt ein RFID-Lesegerät ein Funksignal ab, so antworten alle empfangenden Transponder, indem sie ihre gespeicherten Daten an das Lesegerät senden. Bei passiven RFID-Systemen (ohne eigene Stromversorgung) kann die Leseentfernung von ca. einem Zentimeter bis etwa fünf oder zehn Meter betragen. RFID-Leser können 200 Transponder pro Sekunde auslesen – und das bei einer Fahrgeschwindigkeit bis zu 300 km/Std.

Die Transponder werden an Gegenständen angebracht oder integriert (eingewoben). In passiven Transpondern findet keinerlei Verarbeitung von Daten statt. Ob im gesamten Transpondersystem (mit Lesegerät) personenbezogene Daten verarbeitet werden, hängt von den Umständen ab. Die in jedem Transponder enthaltene Kennung kann personenbezogen sein, wenn es eine Zuordnungsmöglichkeit für denjenigen gibt, der die gespeicherten Daten ausliest. Ob es diese gibt, ist unabhängig vom Transponder und den auf ihm befindlichen Daten. Der Gebrauch der Transponder kann von den Betroffenen nicht beeinflusst werden, da es keine verantwortliche Stelle gibt, die sowohl das Medium ausgibt oder verkauft und alle Anwendungen verantwortet.



1.2 Aktive Transponder

Der Prozessor aktiver (mit einer eigenen Stromversorgung) Transponder kann u.U. die Daten verschlüsseln. An aktive Transponder können Sensoren, Displays und Tastaturen angeschlossen werden. Diese RFID-Systeme ermöglichen eine Leseentfernung von bis zu 30 m.

2 Bewertung der Transponder-Technik

2.1 Nachteile

- Derzeit noch relativ hohe Etikettpreise – allerdings werden die Preise für Transponder aufgrund der Massenproduktion in naher Zukunft erheblich sinken – für 2005 wird ein Preis von 1 Cent pro passivem Transponder angestrebt.
- Die Funktionalität der Transponder kann von Metallgegenständen beeinflusst werden.
- Die gesundheitlichen Risiken der elektromagnetischen Strahlung sind nicht vollständig untersucht.
- Derzeit können 200 Transponder mit hoher Geschwindigkeit parallel gelesen werden. Zur Fehlerquote liegen allerdings unterschiedliche Aussagen vor.

2.2 Vorteile

- Es wird keine (platzraubende) Sichtverbindung zwischen Transponder und Leser benötigt (im Gegensatz zu Barcode).
- Lokalisierbarkeit der Transponder bei Einsatz mehrerer Lesegeräte (Ortung).
- Deaktivierung der Transponder-Inhalte möglich.

PASSIVE TRANSPONDER

- Es kann mehr Information gespeichert werden als auf Barcode-Etiketten und sie kann mit dem Leser verändert werden.
- Der Datenaustausch zwischen Tag und Leser kann mit fehlererkennenden Übertragungsprotokollen durchgeführt werden.
- Unabhängig gegenüber Verschmutzung oder Verschleiß, da mechanische Kontakte fehlen. Wartungsfrei. Transponder sind langlebig und resistent gegen physische Einwirkungen.

AKTIVE TRANSPONDER

- Der integrierte Prozessor aktiver Transponder kann Daten verarbeiten – z.B. verschlüsseln.
- Hohe (read/write) Speicherkapazität der Transponder (derzeit bis zu 256 k Byte).

3 Mögliche Angriffe

RFID-Systeme bestehen wie oben dargestellt aus einem (kleinen) Computer mit Betriebssystem und Anwendungssoftware; insoweit sind sie also angreifbar wie alle anderen Computer auch.

3.1 Angriffe auf die Transponder

Auf Betriebssystemebene:

- Unberechtigtes Lesen der gespeicherten Information, unberechtigtes Schreiben oder Ändern (Fälschung), Löschen.



- Ablösbarkeit der Transponder von der Ware/Karte: Diebstahl.
- Lokalisierbarkeit des Eigentümers.
- 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, ist es möglich, RFID-Etiketten auszulesen, die z.B. in die Kleidung eingenäht oder auf Objekten angebracht sind, die sich in Geldbörsen und Brieftaschen befinden, in Einkaufstaschen, Koffern etc. Eine Zuordnung zum Eigentümer ist über Transponder in Kreditkarten o.ä. möglich.
- Einzigartige Identifikationsmerkmale für alle Objekte weltweit: Der elektronische Produktcode ermöglicht es, dass jeder einzelne Gegenstand auf der Erde seine eigene, einzigartige ID bekommt. Der Gebrauch von einzigartigen ID-Nummern könnte zur Errichtung eines globalen Registrierungssystems 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 großer Datenbanken, die die individuellen Daten eines Etiketts enthalten. Diese Datensammlungen könnten mit Personenidentifikationsdaten verbunden werden.
- Versteckte Lesegeräte: Die Etiketten können aus einiger Entfernung ausgelesen werden, auch durch Sichtbarrieren hindurch und von Lesegeräten, die unsichtbar angebracht sind: Z.B. in Fußböden, Teppichen, Bodenmatten, Türrahmen, Einzelhandelsregalen, Schaltern.

3.2 Indirekte Angriffe

Individuelle Verfolgung und Profilierung: Wenn persönliche Identität mit einer RFID-Etikettennummer verbunden wird, können Personen verfolgt und Bewegungs- und andere Profile von ihnen erstellt werden - ohne dass dieser Erfassungsvorgang von den Betroffenen bemerkt wird. Zum Beispiel könnte mit einem an einem Schuh angebrachten RFID-Etikett eine Person identifiziert werden. Selbst wenn die Identifikation auf Objekt- oder Produktniveau beschränkt bleibt, könnte die Identifikation eines getragenen oder mitgeführten Gegenstands mit der Person und speziellen Ereignissen wie Windowshopping, Kaufdatum oder eine gleichzeitig am Ort stattfindende Demonstration in Verbindung gebracht werden.

- Getragene Kleidung bewerten, zählen, Geld zählen.
- Gezielte Umwegsteuerung.
- (Persönliche) Schreib-/Lesegeräte (lesen dann auch 'fremde' Transponder).
- Diebe, Einbrecher erkennen jüngere Geräte und Geld bei Wohnungseinbrüchen, Überfall und Diebstahl leichter.

3.3 Überwachung Betroffener

Minutiöse Überwachung von Personen, Kunden, Mitarbeitern durch Transponder in der Kleidung, Berufskleidung: Häufigkeit und Dauer von Toilettengängen, 'Sie tragen einen Brioni-Anzug und einen Zimmerli-Slip aus ägyptischer Baumwolle – dazu, mein Herr passt aber nun wirklich nicht das Nylon-Hemd von Woolworth, wir haben hier etwas für Sie ...'. Überwachung in der Öffentlichkeit.

Transponder können mit anderen Geräten wie Uhren und GPS-Empfängern gekoppelt werden.



3.4 Kommunikation zwischen Transpondern und zu mobilen Lesegeräten

Transponder können mit Lesegeräten verbunden werden. Damit können Transponder Daten austauschen.

4 Sicherheitsmaßnahmen

Unberechtigte Zugriffe auf die gespeicherten Informationen:

- Zerstören der Transponder 'an der Ladenkasse', wenn die Ware in die Hände von Endverbrauchern übergeht.
- (Persönliche) Schreib-/Lesegeräte (die lesen dann aber auch 'fremde' Transponder).
- Ein-/Aus-Schalter auf dem Transponder.
- Blocker Chips: Gezielte Unterbrechung der Datenübertragung.
- Jammer: Störsender.
- Zugriffskontrolle im Transponder-Betriebssystem.

5 Beispielhafte Anwendungen und Szenarien

Transponder können folgende Funktionen erfüllen:

- Identifizierung (Lagerverwaltung), Authentifizierung: Zugangskontrolle.
- Ortsverfolgung (Zugangskontrolle, Tierkennzeichnung) und Steuerung.
- (Zustands-)Überwachung, Diebstahlsschutz (Wegfahrsperrung).
- Notifikation.

Beispielhafte Bereiche

- Transport und Logistik.
- Industrie: Herstellung und Verarbeitung:
Global Trade Item Number (GTIN), Electronic Product Code (EPC).

Genutzt werden derzeit meist Anwendungen in denen der Mikrochip nur eine Electronic Product Code (EPC) codierte Information über das Produkt und die individuelle Ware enthält; in anderen Anwendungen werden auch Messwerte erfasst und gespeichert.

Im Einzelnen können die folgenden Leistungen erbracht werden:

5.1 Handel, Warenlogistik

Identifizierung, persönliche Begrüßung, Kombination mit vorhandenen Daten 'Einkaufszettel', 'was Sie sonst noch kauften' (persönliche Vorlieben), optimale Wegeberechnung und Steuerung im Supermarkt (Vermeidung von Suchzeiten), vollautomatische Check-Outs an der Kasse (programmgesteuertes Auslesen/Rechnungsschreiben, 'Verschieben' gekaufter Waren auf dem Kassensband durch Kassiererinnen entfällt), Produktverfolgung/Nachvollziehbarkeit: Kauf, Aufbewahrungsdauer, automatische Warenbestandskontrolle, Warennachbestellung, Vermeidung von Out-of-Stock Situationen, elektronische Artikelsicherung, Inventur, Nachbestellen, keine Preisauszeichnung – Anzeige, individuelle Preise/Rabatte, Herkunftsland etc., individuelle Bewerbung, Verfallsdatum, Nachbestellen durch den Kühlschrank, Abfallmanagement (Straßenverschmutzung).

Mit Transpondern versehen werden können z.B. Paletten und Transportverpackungen aber auch jede Ware im Einzelnen wie Joghurtbecher, Weinflaschen, Pullover – jedes Teil hat eine eigene Nummer, die ohne Berührungs- oder Sichtkontakt ausgelesen



werden kann. Mit dem Lesegerät vernetzt können Informationen zu diesem speziellen Gegenstand aufgerufen werden, z.B. der Preis, die Herkunft. Da auch Kunden-, Kredit- oder Payback-Karten zukünftig mit diesen kleinen Chips ausgerüstet werden können, können auch Kunden eindeutig identifiziert werden. Weiterhin sind elektronische Fahrkarten und Ausweise geplant. Die Europäische Zentralbank prüft, 200-Euro-Scheine mit Transpondern auszurüsten.

Bisher sind Rasierklingen, CDs, Lebensmittel und Kosmetik mit dieser Technik ausgestattet: Metro Cash&Carry - 'Future Store' Rheinberg der Metro AG (erhielt Big Brother Award 2003), Kaufhoffilialen Münster und Wesel. "Real", "Extra" und "Galeria-Kaufhof" sowie 10 Vertriebszentren sollen ebenfalls mit der neuen Technik ausgestattet werden. Metro arbeitet mit Intel und SAP zusammen. Durch die RFID-Technik erwartet der Konzern bei den Lagerhaltungskosten Einsparungen um 20 Prozent, also mehreren Milliarden US-Dollar.

Indem Etikettenlesegeräte auf den Regalen von Buchhandlungen angebracht werden, erlaubt das neue System Buchhändlern, Informationen zu sammeln wie zum Beispiel die Bandbreite an Titeln, die ein Käufer durchgeblättert hat, wie oft ein bestimmter Titel angefasst wurde und sogar die Zeit, wie lange in jedem Buch herumgeblättert wurde.

Das US-amerikanische Unternehmen ADS hat einen Transponder namens "Veripay" vorgestellt, den sich die Nutzer unter ihrer Haut einpflanzen können. Das Unternehmen sucht nun nach Partnern in der Finanzbranche wie Banken und Kreditkartenunternehmen, die den Transponder als Zahlungsmittel nutzen wollen. Als Vorteil gegenüber Karten als Identifikationsmittel wird gesehen, dass Transponder nicht verloren und missbraucht werden können.

Rückverfolgung von Medikamenten und anderen industriell hergestellten Gütern vom Punkt der Herstellung bis zum Punkt der Ausgabe: RFID-Etiketten können Fälschungen wichtiger Produkte verhindern, sicherzustellen, dass Produkte nicht verloren gehen oder gestohlen werden, sachgemäßen Umgang (Regal) kontrollieren und korrekte Ausgabe erreichen.

Auffindung von Gegenständen, die toxische Substanzen enthalten, wenn sie bei der Mülldeponie angeliefert werden: Wenn zum Beispiel ein PC zu einer Mülldeponie gebracht wird, kann ein Kurzstanz-RFID-Etikett die Existenz giftiger Inhaltsstoffe an ein Lesegerät bei der Deponie übermitteln.

5.2 Andere Anwendungsbereiche

- Tierkennzeichnung.
- Paketverfolgung, Gepäckverfolgung (Flughafen).
- PKW-Überwachung. Maut - Road Toll Management: Vehicle Identification Number (VIN).
- Personenüberwachung: Hauseingänge, strategische Punkte.
- (In-)Direkte Ortung durch Satelliten.

6 Literatur

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) (Ed.):
Position Statement on the Use of RFID on Consumer Products. 2003
<http://www.privacyrights.org/ar/RFIDposition.htm>

Electronic Privacy Information Center (EPIC): Radio Frequency Identification (RFID)
Systems. Washington 2004 <http://www.epic.org/privacy/rfid/>



- Finkenzeller, K.: RFID-Handbuch. Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktlose Chipkarten. 2. Aufl. München 2000
- Garfinkel, S.L.: Adopting Fair Information Practices to Low Cost RFID Systems. Cambridge 2002 <http://www.simson.net>
- Hansen, M.; Wiese, M.: RFID – Radio Frequency Identification. Datenschutz und Datensicherung 28, 2, 2004, S. 109
- Hilty, L.; Behrendt, S.; Binswanger, M.; Bruinink, A.; Erdmann, L.; Fröhlich, J.; Köhler, A.; Kuster, N.; Claudia Som, C.; Würtenberger, F.: Das Vorsorgeprinzip in der Informationsgesellschaft. Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Bern 2003
- Roßnagel, A.; Pfitzmann, A.; Garstka, H.: Modernisierung des Datenschutzrechts. Berlin 2001
- ISO SG3 18000: Information Technology AIDC Techniques RFID - Air Interface. Genf 2003
- Weis, S.A.; Sarma, S.E.; Rivest, R.L.; Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems

Kontakt:

Gesellschaft für Informatik e.V. (GI)
Ahrstraße 45
53175 Bonn

Tel.: 0228-302145
Fax: 0228-302167
E-Mail: gs@gi-ev.de
Web: <http://www.gi-ev.de>