RFID als Infrastruktur

Von geschlossenen und offenen Systemen

CAST-Forum RFID/Smartcard – Darmstadt

Frank Pallas, TU Berlin, Informatik und Gesellschaft

http://ig.cs.tu-berlin.de/ma/fp/

15. September 2005

Zusammenfassung

Die Technik der funkbasierten Identifizierung (Remote Frequency IDentification – RFID) ist nicht neu. Sie befindet sich vielmehr bereits seit Jahrzehnten beispielsweise in Bibliotheken oder in der Viehwirtschaft im Einsatz und hat sich bewährt. Aktuelle Entwicklungen gehen jedoch in Richtung einer für unterschiedlichste Zwecke nutzbaren Mehrzwecktechnologie. Die Sekundärnutzung ist dabei ausdrücklich vorgesehen.

Der Artikel geht auf diese Entwicklungen ein und zeigt auf, welche Auswirkungen eine solche, mit einer Infrastruktur vergleichbare, Struktur der Nummeriertheit von Dingen nach sich zieht. Die Unterscheidung von geschlossenen und offenen Systemen steht dabei im Vordergrung und soll als Grundlage zur Strukturierung der anhaltenden Diskussion dienen.

1 Einleitung

RFID: Vier Buchstaben, die einen beachtlichen Teil der Fachwelt unterschiedlichster Disziplinen in höchste Aufregung versetzen. RFID, die „Schnüffelchips“ oder „Mitteilsamen Etiketten“[1], die den Verbraucher schutzlos den Begehrlichkeiten von Handelskonzernen und Datensammlern aussetzen. Die Garanten für Fälschungssicherheit von Medikamenten[2] wie auch Geldscheinen[3]. RFID, die Barcodes der nächsten Generation, die jeden Gegenstand mit einer weltweit eindeutigen Nummer versehen und die die Logistik revolutionieren werden[4]. RFID, die neue Technik zur Sicherung des internationalen Reiseverkehrs[5]. RFID... ja, was eigentlich?

Es scheint an der Zeit zu sein, Luft zu holen und den Blick über die so unterschiedlichen Sichten auf RFID schweifen zu lassen. Ist es vielleicht möglich, eine Ordnung im allgemeinen Durcheinander zu finden? Und lassen sich aus einer nüchternen Betrachtung eventuell neue Schlüsse oder Ansätze entwickeln, die es zumindest wert sind, ebenfalls diskutiert zu werden? Ein Versuch lohnt sich sicherlich.

2 Die technische Sicht: Antennen und Mikrochips

Auch wenn in anderen Bereichen die Meinungen teilweise stark auseinandergehen – in einem Punkt dürften sich alle einig sein: der wesentlichen Technik hinter RFID. Grundsätzlich dient die RFID-Technik der funkbasierten Identifikation (Radio Frequency IDentification). RFID-Systeme bestehen dabei typischerweise aus drei maßgeblichen Bestandteilen: einem Transponder (Chip, Tag) als beweglichen Träger von Daten, einer Sende- und Empfangseinheit (Lesegerät, Reader) sowie aus nachgelagerten datenverarbeitenden Systemen (vgl. Abbildung 1).

Der Identifikationsvorgang folgt nun in nahezu allen RFID-Systemen dem gleichen Schema: Das (meist stationäre) Lesegerät sendet kontinuierlich Funkimpulse aus, die alle in Reichweite befindlichen Transponder zu einer Antwort auffordern. Wird dieser Impuls von einem Transponter empfangen, so sendet dieser die angeforderten Daten an das Lesegerät zurück[6]. Je nach Verfahren kann es sich dabei um unterschiedliche Arten von Daten handeln. In den einfachsten Systemen, die beispielsweise zum Diebstahlschutz in Warenhäusern

[1] Vgl. Meyer und Schüler (2004).

[2] Vgl. dazu Heise Online vom 15. 11. 2004: „Medikamentenpackungen sollen in den USA mit RFID-Chips gekennzeichnet werden“ `http://www.heise.de/newsticker/meldung/53277` [01. 09. 2005].

[3] Entsprechende Gerüchte über die „RFIDisierung“ von Euro-Banknoten kursieren bereits seit geraumer Zeit, wurden von der Europäischen Zentralbank jedoch bislang nicht offiziell bestätigt. Vgl. dazu u. a. EETimes vom 19. 12. 2001: „Euro bank notes to embed RFID chips by 2005“ `http://www.eetimes.com/story/OEG20011219S0016` [01. 09. 2005].

[4] Vgl. Bose und Pal (2005).

[5] Vgl. Kügler (2005).

[6] Auf Unterschiede wie den zwischen aktiven und passiven Tags sowie auf weitere Aspekte wie Antikollisionsprotokolle etc. soll hier nicht genauer eingegangen werden, da sie für die weiteren Betrachtungen weniger relevant sind. Zu diesen und anderen Themen vgl. insb. Finkenzeller (2002) sowie Lampe, Flörkemeier, und Haller (2005) und BSI - Bundesamt für Sicherheit in der Informationstechnik (2004).

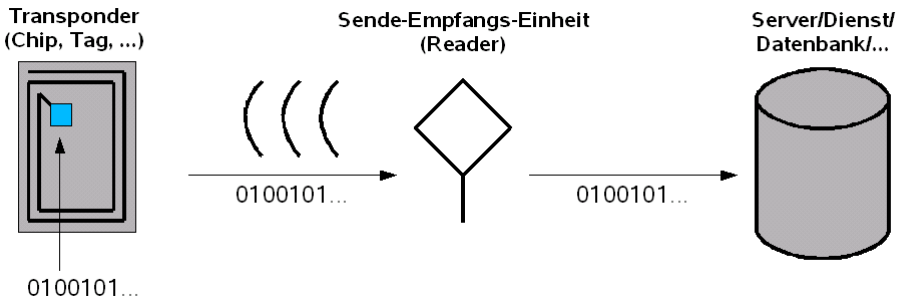

Abbildung 1: RFID-System, bestehend aus Transponder, Sende-/Empfangseinheit und nachgelagertem, datenverarbeitendem System

zum Einsatz kommen, wird lediglich eine binäre Antwort („Ja“ oder „Nein“[7]) übermittelt.

In komplexeren Systemen, die beispielsweise in Bibliotheken zum Einsatz kommen, können aber auch ganze Datensätze (Autor, Titel, Verlag etc.) auf dem Transponder abgelegt und von dort gelesen werden. Die gängigsten Systeme basieren jedoch auf der Übermittlung von in einem definierten System eindeutigen Nummern, den ID's.

Mit diesen wiederum sind in den nachgelagerten Systemen abgelegte Daten verknüpft. Wird nun ein RFID-Tag mit einer bestimmten Nummer von einem Lesegerät erkannt, so können durch die nachgelagerten Systeme vorab festgelegte Aktionen beliebiger Komplexität angestoßen werden. In einer Bibliotheksanwendung kann dies beispielsweise in Form einer „Automatischen Buchrückgabe“ umgesetzt werden, bei der ein Bibliotheksbenutzer lediglich die ausgeliehenen Bücher in ein „Rückgabefach“ legen muss[8]. In einem solchen Fall würde die ID eines Buches per Funk ausgelesen und daraufhin automatisch die Aktion „markiere Buch mit der ID X in der Datenbank als nicht mehr ausgeliehen“ oder aber auch „markiere Buch mit der ID X in der Datenbank als nicht mehr ausgeliehen und buche wegen verspäteter Rückgabe des Buches mit der ID X vom Konto des Bibliotheksbenutzers Y den Betrag Z ab“ ausgeführt[9]. Gleichzeitig können die Tags der Bücher auch zu Zwecken des Diebstahlschutzes eingesetzt werden: Passiert ein Buch, das in der Datenbank als „nicht ausgeliehen“ markiert ist, ein an einer Ausgangsschleuse platziertes Lesegerät, so ließe sich ein Alarm auslösen. Weitere Anwendungen sind ebenfalls möglich.

[7] Genaugenommen wird in solchen Systemen lediglich ausgewertet, *ob* eine Antwort registriert wird. Ist dies der Fall, so wird sie üblicherweise im Sinne von „es existiert ein aktives Tag und damit unbezahlte Ware“ ausgewertet.

[8] Derartige Systeme befinden sich auch in Deutschland bereits im Einsatz. So setzt die Stadtbücherei Stuttgart ein System ein, bei dem auch die selbständige Ausleihe möglich ist. Vgl. dazu: `http://www.stuttgart.de/stadtbuecherei/druck/selbstverbucher.pdf` [06.09.2005]. Auch in der Bibliothek des Vatikans kommen RFID-Chips zum Einsatz. Hier liegt der Schwerpunkt jedoch auf der Beschleunigung der Inventur, für die die Bibliothek bisher einen Monat lang geschlossen werden musste. Vgl. dazu Heise newsticker vom 08.07.2004: RFID im Vatikan `http://www.heise.de/newsticker/meldung/48943` [06.09.2005].

[9] Derartige Anwendungen lassen sich prinzipiell auch unter Verwendung klassischer bibliothekseigener Strichcodes umsetzen. Auch in diesem Fall würde auf Basis einer eindeutigen Kennung und mit dieser Kennung verknüpfter Daten eine Aktion ausgelöst.

Das grundlegende Prinzip derartiger Systeme bleibt dabei immer gleich: Eine eindeutige ID wird von einem bestimmten Lesegerät registriert, welches dies an nachgelagerte Datenverarbeitungssysteme meldet. In Abhängigkeit von jeweils zusätzlichen Kontextinformationen (Lesegerät befindet sich in Rückgabefach, Lesegerät befindet sich an Ausgangsschleuse, Buch ist als „nicht ausgeliehen“ markiert, ...) werden daraufhin bestimmte Aktionen ausgelöst. Die Rolle der RFID-Technik beschränkt sich hierbei lediglich auf einen einzigen Teilaspekt: Das *funkbasierte* Auslesen *eindeutiger* Kennungen und damit die *Identifizierung von Dingen*.

3 Von geschlossenen und offenen Systemen

Diese Identifizierung von Dingen zur kontextbasierten Steuerung von Abläufen oder Aktionen lässt sich auf vielfältige Art und Weise nutzen. So werden bereits seit geraumer Zeit in der Viehwirtschaft Melk- und Fütterungsanlagen dahingehend automatisiert, dass mit RFID-Tags versehene Rinder sowohl beim Melken als auch bei Betreten der Fütterungsanlage eindeutig identifiziert werden. Zusammensetzung und Menge des Futters können dabei ständig an die jeweilige Milchleistung angepasst werden.

Mit den Eintrittskarten für die Fußball-Weltmeisterschaft 2006 verhält es sich ähnlich. Auch sie werden einen RFID-Chip mit eindeutiger Nummer tragen, mit der weitergehende Informationen zum rechtmäßigen Kartenbesitzer verknüpft sind. Die hierbei verfolgten Ziele sind noch nicht vollständig geklärt, von den Veranstaltern werden aber unter Anderem der Ausschluss bekannter Gewalttäter vom Ticketkauf sowie die Möglichkeit zum Sperren gestohlener oder verloren gegangener Tickets genannt[10]. Die Liste existierender Anwendungen ließe sich nahezu beliebig fortsetzen.

3.1 Geschlossene Systeme

Alle bis hierher aufgeführten Szenarien zeichnen sich dadurch aus, dass sie sich auf *geschlossene Systeme* beziehen: Büchereien verwenden RFID-Tags, die nur innerhalb einer Bibliothek – bestenfalls über alle von demselben Hersteller ausgerüsteten Bibliotheken hinweg – gelesen und verarbeitet werden können. Auch die vergebenen IDs müssen nur innerhalb *eines* geschlossenen Systems eindeutig sein. Gleiches gilt für die genannten Anwendungen in der Viewirtschaft oder für die Fußball-Tickets: Auch hier können die verwendeten Tags herstellerspezifisch sein und müssen sich weder mit Lesegeräten anderer Hersteller auslesen lassen noch ist die verwendete ID gezwungenermaßen über Systemgrenzen hinweg eindeutig[11]. Zudem ist in geschlossenen Systemen der Einsatzzweck und damit die Anforderungen

[10] Vgl. Heise Newsticker vom 15. 01. 2004: „Fußball-WM 2006: Nur mit RFID ins Stadion“ `http://www.heise.de/newsticker/meldung/43645` [12.09.2005].

[11] Für die Viehwirtschaft gilt hierbei laut BSI - Bundesamt für Sicherheit in der Informationstechnik (2004, S. 64), dass die zu verwendenden Tags sowohl in Bezug auf die physischen Eigenschaften wie auch in Bezug auf das Nummerierungsschema international normiert sind. Nichtsdestotrotz kommen solche Systeme nur in der Viewirtschaft zum Einsatz. Sie sind somit zwar interoperabel, werden aber weiterhin ausschließlich in der Viehwirtschaft genutzt.

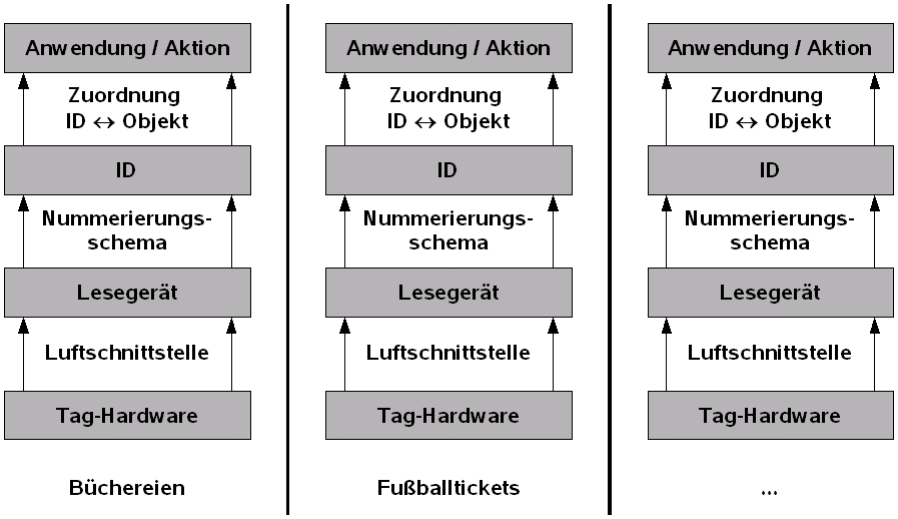

Abbildung 2: Geschlossene, nicht interoperable RFID-Systeme

an das System bereits im Vorhinein bekannt und vergleichsweise klar definiert.

Abstrakt gesprochen unterliegen also RFID-Systeme für geschlossene Anwendungen *keinem Normungs- bzw. Interoperabilitätsdruck*. Büchereisysteme müssen nicht mit Tags anderer Bibliotheken oder gar mit Fußballtickets kommunizieren können. Tags, die auf die besonderen Anforderungen der Viehwirtschaft (Kälte- und Feuchtigkeitsresistenz etc.) zugeschnitten sind, sind in Ihrem Wert für den Anwender absolut unabhängig von der Auslesbarkeit in anderen Systemen. Die zum Einsatz kommende RFID-Technik ist eine *Einzelzwecktechnologie*, bei der die unterschiedlichen Systeme typischerweise strikt voneinander getrennt sind (vgl. Abbildung 2).

Aus diesem Grund lässt sich die jeweils verwendete Technik ohne zu befürchtende Seiteneffekte explizit an den jeweiligen Einsatzzweck anpassen. Was für den jeweiligen, vergleichsweise klar spezifizierten Einsatzzweck sinnvoll erscheint, lässt sich umsetzen. Dies gilt sowohl für die Wahl von Übertragungsfrequenz, Reichweite oder Nummerierungsschema als auch für die Frage, ob ein Antikollisionsprotokoll zum Einsatz kommt oder auch, ob die Kommunikation zwischen Tag und Lesegerät verschlüsselt werden soll oder nicht. Auf dieses Thema wird an späterer Stelle noch genauer eingegangen.

3.2 Der Electronic Product Code

Einen anderen Ansatz verfolgt das aus den Auto-ID-Labs des MIT hervorgegangene Konsortiom EPCglobal[12]. Unter Mitwirkung des Nordamerikanischen Uniform Code Council und des EAN- (European Article Number) Verbandes, die bereits für Normierung und Verwaltung der bekannten Strichcodes auf Konsumgütern verantwortlich sind, definiert EPCglobal weltweit einheitliche Standards für die Verwendung von RFID-Tags. Die Standardisierung

[12]Webseite: `http://www.epcglobalinc.org` [12.09.2005]

bezieht sich dabei sowohl auf die Kommunikation zwischen Lesegerät und Tag (verwendete Funkfrequenzen, Protokolle, etc.) als auch auf die verwendeten Nummerierungsschemata und hier insbesondere den *Electronic Product Code (EPC)*, dessen Spezifikation im Jahr 2003 erfolgte und der gemeinhin als Nachfolger der bekannten Strichcodes angesehen wird (Vgl. Flörkemeier 2004).

Dieser EPC unterscheidet sich in zwei Punkten maßgeblich von den etablierten Nummerierungsschemata für Strichcodes: Zum einen ist der verfügbare Nummernbereich deutlich größer. So sind im EAN-Strichcode für die Herstellerkennung (Landeskennung und länderspezifische Herstellerkennung) sieben Dezimalstellen vorgesehen, was eine Unterscheidung von theoretisch maximal zehn Millionen Herstellern erlauben würde. Im EPC, der insgesamt über 96 Bit verfügt, sind hierfür allein 28 Bit vorgesehen – es können somit ca. 270 Millionen Hersteller unterschieden werden. Ähnliches gilt für die Auszeichnung des Produkt-Typs. Der EAN-Strichcode sieht hierfür fünf Dezimalstellen vor (entspr. 100.000 möglichen Produktlinien *eines* Herstellers), der EPC hingegen 24 Bit (ca. 16 Mio. mögliche Produktlinien je Hersteller).

Zum Anderen – und hier liegt der bedeutendere Unterschied zwischen bekannten Strichcodes und dem EPC – ist im EPC-Nummerierungsschema eine *eindeutige Seriennummer* für jedes einzelne Objekt vorgesehen. Anders als beim etablierten Verfahren werden damit unterschiedliche Gegenstände gleichen Typs eindeutig unterscheid- und identifizierbar. Würden diese weltweit eindeutigen EPC-Kennungen nun wie vorgesehen bereits bei der Fertigung mittels standardisierter RFID-Tags an die jeweiligen Gegenstände angebracht[13], so würde sich über kurz oder lang ein Zustand der mehr oder minder vollständigen *„Nummeriertheit von Dingen“* ergeben[14].

3.3 Offene Systeme

Wie würde sich nun eine derartige Nutzung der RFID-Technik von den oben aufgeführten geschlossenen Systemen unterscheiden? Zentrales Ziel bei der Standardisierung von Funkschnittstelle und Nummerierungsschema durch EPCglobal war es, *Interoperabilität* zu schaffen. Jedes Tag soll mit jedem auf dem gleichen Standard basierenden Lesegerät nutzbar sein. Ein bereits bei der Herstellung in den Deckel eines Buches integriertes, EPC-konformes RFID-Tag könnte damit sowohl innerhalb des weiteren Produktions- und Auslieferungsprozesses (Verpackung, Wareneingangskontrolle in der Buchhandlung, etc.) als auch innerhalb der Buchhandlung (beschleunigte Inventur, Selbstzahlerkassen, etc.) oder eben in einem Bibliothekssystem wie dem oben beschriebenen verwendet werden.

All diese Anwendungsfälle zeichnen sich durch besondere Anforderungen aus, für deren

[13] Bei Kleidungsstücken bietet sich hierzu das Anbringen in Form eingenähter Etiketten an, bei technischen Geräten könnte das Tag im jetzt schon bekannten Seriennummern-Aufkleber integriert sein, usw.

[14] Mit dem „Object Names Service (ONS)“ und der „Physical Markup Language (PML)“ gehen die Pläne sogar noch deutlich weiter. Analog zum aus dem Internet bekannten „Domain Name Service (DNS)“ soll mittels ONS eine Abbildung der EPC-Nummer auf eine Internet-Ressource möglich sein, an der mittels PML formulierte weitere Angaben zum jeweiligen Objekt hinterlegt werden. Am ehesten wäre dies mit einer „Webseite für jeden Gegenstand“ vergleichbar. Auf dieses Konzept geht Flörkemeier (2004) zusammenfassend ein.

Erfüllung im oben dargelegten Modell der geschlossenen Systeme jeweils unterschiedliche Techniken zum Einsatz kämen: interne Strichcodes für die Steuerung des Herstellungsprozesses, manuelles Zählen von Liefermengen, manuelle und damit deutlich teurere Inventur oder eben RFID-basierte Bibliotheksmanagementsysteme. Standardisierte und problemlos nutzbare RFID-Tags bringen all dies auf einen gemeinsamen Nenner, der auf den ersten Blick überraschend simpel klingt: Die prozess- und systemübergreifende Nummeriertheit von Dingen (vgl. Abbildung 3).

Ausgehend von einer solchen Vorstellung ließen sich nahezu unendlich viele weitere Anwendungsmöglichkeiten skizzieren: Der „Smarte Kühlschrank" – er kann mittlerweile guten Gewissens als Klassiker bezeichnet werden – könnte anhand der eindeutigen Seriennummern das Haltbarkeitsdatum der Milch bestimmen und auf dessen Ablauf hinweisen. Die „Smarte Waschmaschine" auf Basis der EPCs der eingelegten Kleidungsstücke das richtige Programm bestimmen[15] und der Kleiderschrank könnte den persönlichen Kleidungsbestand regelmäßig inventarisieren und allmorgendlich eine auf die aktuelle Wettervorhersage abgestimmte Kleidungsempfehlung abgeben[16].

Doch all diese Beispiele sind noch vergleichsweise kurz gegriffen. So lassen sich auch weitaus umfassendere mögliche Szenarien skizzieren, die auf einer einheitlichen Nummeriertheit von Dingen aufbauen. Kang und Cuff (2005) nennen beispielsweise die mögliche Durchsetzung von Bekleidungsrichtlinien anhand der ausgelesenen IDs aller von einem Besucher getragenen Kleidungsstücke oder auch die Möglichkeit des „political shopping" (S. 37 ff)[17].

Bereits hieran wird deutlich, welche Auswirkungen standardisierte, offene und an allen Produkten des täglichen Lebens angebrachte oder gar darin eingebettete RFID-Tags nach sich zögen: Sie würden verschiedenste Anwendungen *ermöglichen*. Der Unterschied zu den klassischen, geschlossenen RFID-Systemen besteht darin, dass es sich nicht mehr um *Systeme* im eigentlichen Sinn handelt, sondern um eine *Mehrzwecktechnologie*. Durch den Ausschluss möglichst vieler Annahmen zum späteren Einsatzweck werden unterschiedlichste Einsatzszenarien erst ermöglicht – insbesondere auch solche, die zum Zeitpunkt des technischen Designs noch nicht absehbar waren. Der Vergleich mit dem Internet oder anderen „Ermöglichungsstrukturen" bzw. „Infrastrukturen" drängt sich geradezu auf.

4 RFID als Infrastruktur

Eine solche Sicht, die allgegenwärtige standardisierte RFID-Tags im Sinne einer Kommunikationsinfrastruktur betrachtet, ist nicht neu. So ist im Zusammenhang mit RFID immer

[15] Vgl. RFIDJournal vom 04. 04. 2003: Merloni Unveils RFID Appliances `http://rfidjournal.com/article/articleview/369/1/1` [06. 09. 2005]

[16] Vgl. hierzu insbesondere Wan (2000).

[17] Unter „political shopping" verstehen die Autoren dabei beispielsweise die Möglichkeit, Informationen zur Umweltpolitik eines Herstellers abzufragen. Weiterhin merken die Autoren an, dass derartige weitergehende Informationen auch in einem peer-to-peer-Prozess durch die Verbraucher selbst erzeugt werden können. Derartige Szenarien werden natürlich nicht allein durch RFID-Technik ermöglicht, können jedoch auf standardisierter RFID-Technik *aufbauen*.

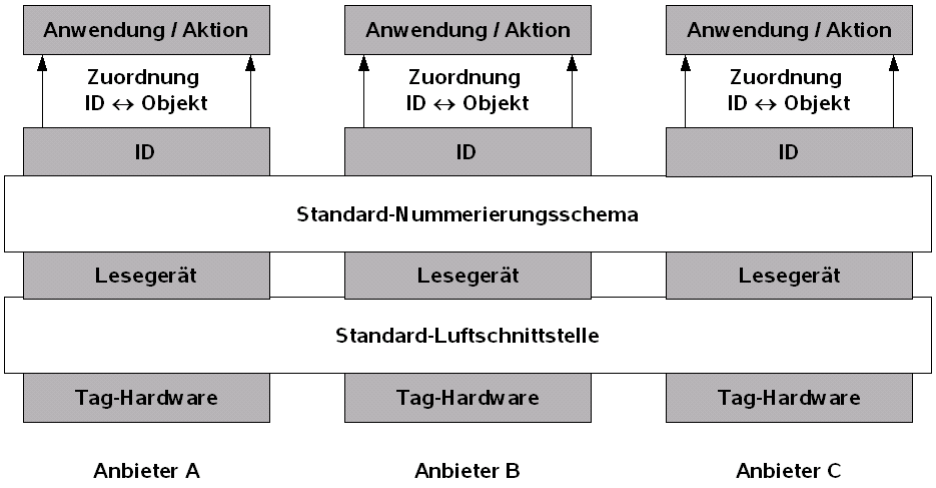

Abbildung 3: Offene, interoperable RFID-Systeme

wieder die Rede von einem „Internet der Dinge“[18] und auch Mark Roberti, Gründer des renommierten RFID Journals, hat dies erst kürzlich in einem Vortrag angemerkt: „RFID is infrastructure; It's an enabling technology; once installed and networked, readers can be used for many different applications; this is similar to the Internet“[19]. Wenn sich aber das Internet und ein möglicher zukünftiger Zustand allgegenwärtiger standardisierter RFID-Tags in zentralen Punkten als vergleichbar erweisen, welche Implikationen hat dann dies für die Gestaltung der allgegenwärtigen Tags?

Isenberg (1997) weist in seinem Artikel „Rise of the Stupid Network“ darauf hin, dass auf bestimmte Anforderungen hin gestaltete Netzwerke nur so lange ihren Zweck erfüllen, wie die getroffenen Annahmen weiterhin gelten[20]. Mit Blick auf das Design von Telekommunikationsnetzwerken führt er hierzu das Beispiel an, dass klassische Vermittlungsstellen des Telefonnetzes schnell an ihre Kapazitätsgrenzen stoßen, sobald durch verstärkte Internetnutzung die angenommene durchschnittliche Verbindungsdauer und damit die angenommene durchschnittliche Auslastung steigt. Insbesondere zieht Isenberg den Schluss, dass sich der Gefahr der Beeinträchtigung durch veränderte Rahmenbedingungen vor Allem durch ein möglichst unspezifisches Design und die Berücksichtigung möglichst weniger Annahmen entgegenwirken ließe.

Ähnlich wird üblicherweise auch in Bezug auf den Zusammenhang von Netzwerkdesign und Innovation argumentiert: Grundlegende Dienste sollen möglichst simpel gestaltet sein, um Innovationen an den Enden zu ermöglichen, anstatt sie zu behindern[21].

Interessant sind diese Ausführungen aus dem Bereich der Telekommunikationsnetze

[18] Vgl. z. B. Bose und Pal (2005) oder Schoenberger (2002).

[19] Vgl. `http://www.misrc.umn.edu/seminars/slides/mark_roberti_rfid.pdf` [06. 09. 2005] S. 45.

[20] Vgl. Isenberg (1997): „Design-by-assumption works as long as assumptions hold.“

[21] Vgl. hierzu beispielsweise Lemley und Lessig (2004, S. 46): „By keeping the network simple, and its interaction general, the Internet has facilitated the design of applications that could not originally have been envisioned.“

besonders in Anbetracht obiger Ausführungen zu geschlossenen und offenen Systemen. Geschlossene RFID-Systeme lassen sich als Einzelzwecktechnologie durchaus mit klassischen Kommunikationsnetzen wie dem Telefon- oder dem Fernsehkabelnetz vergleichen: Der Verwendungszweck wird im Vorhinein als bekannt angenommen und das System wird entsprechend diesem Zweck gestaltet und optimiert. Eine Sekundärnutzung wird durch derartige Optimierungen jedoch zumindest erschwert und lässt sich (z.B. durch den Hersteller) sogar aktiv behindern[22]. Anwendungen, die die Systemgrenzen überschreiten, sind gar nicht oder nur unter hohem Aufwand umsetzbar[23].

Offene RFID-Systeme hingegen sind als Mehrzwecktechnologie zu betrachten und lassen sich daher eher mit dem Internet vergleichen: Durch die bewusste Beschränkung auf minimale Funktionalität (standardisiertes, funkbasiertes Auslesen eindeutiger Seriennummern) wäre die größtmögliche Interoperabilität gewährleistet. Das Auslesen ließe sich nicht durch Hersteller oder Konsortien reglementieren bzw. beschränken und Sekundärnutzungen würden explizit gefördert.

Allerdings haben offene Systeme auch eine Kehrseite: Genauso wie das Internet nicht zwischen „gut“ und „böse“ unterscheidet und sich damit auch zu unerwünschten oder gesetzwidrigen Zwecken nutzen lässt, würde auch durch die Möglichkeit des *unbeschränkten* Auslesens standardisierter RFID-Tags die Gefahr des Missbrauchs erhöht: Die Möglichkeit zur Bildung umfassender Einkaufs- und Bewegungsprofile ist bereits breit diskutiert[24]. Hinzu kommen Verbraucherängste vor Kontrollverlust, Objektverantwortlichkeit oder auch Technologiepaternalismus[25]. Auch dies sind mögliche Auswirkungen des so einfachen Prinzips der Nummeriertheit von Dingen.

Was also soll man tun, um diese unerwünschten Auswirkungen bereits im Vorhinein zu verhindern, ohne gleichzeitig erwünschte Sekundärnutzungen zu unterbinden?

5 Von offenen zu verschlossenen Systemen?

Die Wissenschaft hat sich dieser Fragestellung eingehend gewidmet. Grundsätzlich lassen sich dabei zwei unterschiedliche technische Ansätze unterscheiden: zum Einen das *partielle oder vollständige Löschen* der RFID-Tags und zum Anderen unterschiedliche Arten der *Zugriffskontrolle mit kryptographischen Mitteln*.

Die Idee hinter dem ersten Ansatz des partiellen oder vollständigen Löschens ist dabei

[22] So führte die zumeist unidirektionale Auslegung des Fernsehkabelnetzes in weiten Teilen Deutschlands dazu, dass eine Sekundärnutzung für den breitbandigen Internetzugang nicht möglich war. Zudem wurden Vorwürfe laut, der bidirektionale Ausbau des Kabelfernsehnetzes würde bewusst verzögert. Vgl. dazu Frankfurter Allgemeine Zeitung vom 24. 08. 2004, S. 12: „Kartellamt wirft Kabel Deutschland und Telekom Kungelei vor“

[23] Man denke hier beispielsweise an Eintrittskarten, die sich gleichzeitig als Fahrkarten im öffentlichen Nahverkehr nutzen lassen sollen. Kommen hier unterschiedliche RFID-Systeme zum Einsatz, so wäre der technische Aufwand für eine solche Nutzung vergleichsweise groß

[24] So hat auch die Artikel-29-Gruppe der Europäischen Datenschutzbeauftragten im Januar 2005 ein Arbeitspapier zu diesem Thema vorgelegt. Vgl. Article 29 Data Protection Working Party (2005).

[25] Vgl. Berthold, Günther, und Spiekermann (2005). Zu „Technologipaternalismus“ siehe auch Spiekermann und Pallas (2005).

vergleichsweise simpel. Durch einen einfachen Mechanismus werden die eindeutigen Seriennummern der RFID-Tags beispielsweise an der Supermarktkasse automatisch gelöscht. Dadurch, so die Vorstellung, könne man der negativen Auswirkungen der RFID-Technologie Herr werden. Dass dieser Ansatz jedoch nicht weit trägt ist mittlerweile allgemein akzeptiert: Personen ließen sich auch ohne eindeutige Seriennummern der von Ihnen mitgeführten Gegenstände eindeutig identifizieren, indem „Konstellationen" (Weis 2003, S. 29) dauerhaft mitgeführter Gegenstände ausgewertet würden.

Werden beispielsweise zur gleichen Zeit ein bestimmtes Schuhmodell, ein bestimmtes Modell einer Armbanduhr und beispielsweise ein bestimmter Manteltyp am gleichen Ort erkannt, so lässt sich daraus schließen, dass diese ein und derselben Person zuzuordnen sind. Wird nun zu einem anderen Zeitpunkt die gleiche Kombination aus Schuh-, Mantel- und Uhrenmodell erkannt, so handelt es sich mit großer Wahrscheinlichkeit um die selbe Person[26].

Hinzu kommt, dass bei der *partiellen Löschung* gerade die eindeutige Seriennummer verloren geht, was wiederum auch gewünschte Sekundärnutzungen[27] zumindest in Teilen ausschließt. Gleiches gilt in noch gesteigertem Maße für das *vollständige Löschen* der RFID-Tags: Eine u. U. gewünschte Sekundärnutzung wäre in diesem Fall gänzlich unmöglich. Festzuhalten bleibt: Das Löschen der Seriennummer löst die entstehenden Probleme nicht und verringert den durch Sekundärnutzung möglichen Wert deutlich. Komplettes Löschen der RFID-Tags löst zwar die potentiellen Probleme, macht aber eine Sekundärnutzung gänzlich unmöglich[28].

Der zweite Ansatz, die *Zugriffskontrolle mittels kryptographischer oder vergleichbarer Mechanismen*, erscheint dagegen vielversprechender: Die grundlegende Funktionalität der weltweit eindeutigen und standardisierten Seriennummer bleibt vollständig erhalten, das Auslesen ist jedoch an eine *situatonsspezifische explizite Erlaubnis* hierzu gekoppelt. Diese Erlaubnis kann dabei mittels einfacher Passwort- oder Challenge-Response-Verfahren (Berthold et al. 2005, S. 11 f), „Meta-IDs" (Sarma, Weis, und Engels 2002, S. 13) oder gar mittels aufwändiger Public-Key-Verfahren (NTRU 2005) erteilt werden. In jedem Fall würde so das unerwünschte Auslesen unmöglich gemacht oder zumindest deutlich erschwert.

Neben den oftmals angeführten höheren Kosten für ein einzelnes Tag[29] würden diese Verfahren bei flächendeckendem Einsatz jedoch wiederum die Möglichkeiten zur Sekundärnutzung deutlich beeinträchtigen. Wäre das Auslesen eines Tags beispielsweise erst nach Übermittlung eines Passworts möglich, so müsste dieses Passwort auch innerhalb jedes

[26] Im Regelfall dürfte schon die Kombination aus Schuh und Uhr ausreichen, um eine neu erkannte Jacke ebenfalls der gleichen Person zuzuordnen.

[27] Beispielsweise die eindeutige Identifizierung einer Milchtüte zur Bestimmung des Haltbarkeitsdatums

[28] Hinzu kommt, dass das Prinzip des generellen Löschens nur schwer umzusetzen wäre. Da die Ausstattung nahezu aller produzierten Güter mit RFID erklärtes Ziel ist, müsste folgerichtig jeder Bahnhofskiosk mit Deaktivierungseinrichtungen ausgestattet werden. Vgl. dazu Stapleton-Gray (2003, S. 4).

[29] Für die genannten Verfahren sind unterschiedlich viele zusätzliche schaltkreise auf den in die Tags eingebundenen Mikrochips notwendig. Besonders in der mikrochipindustrie gelten jedoch die „economies of scale", die u. U. dazu führen, dass bei entsprechender Produktionsmenge die Kosten für einen einzelnen erzeugten Chip gegenüber den initialen Entwicklungskosten nahezu vernachlässigbar sind. Dies würde das Argument der gesteigerten Kosten entkräften.

Systems bekannt gemacht werden, welches das Tag auslesen soll. Im Zweifelsfall würde dies beispielsweise bedeuten, dass eine „smarte“ Waschmaschine vor dem Wählen des richtigen Programms ebenso zur Eingabe eines Passwortes auffordern würde wie „smarte“ Mikrowellen, Kleiderschränke usw. Dies würde der von Weiser und Brown (1996) skizzierten Idee des „Calm Computing“, welches ruhig und unbemerkt im Hintergrund seine Arbeit zum Wohle des Menschen verrichtet, geradezu konträr entgegenstehen. Natürlich ließe sich diesem Effekt durch das Einführen weiterer Systeme wie Authentifikationsagenten (Vgl. Spiekermann und Berthold 2005, S. 8 f) entgegenwirken, die Auswirkungen eines solchen Vorgehens liegen jedoch auf der Hand:

Durch das Einführen von Verschlüsselungs- oder Authentifizierungsmechanismen wird die Komplexität der verwendeten RFID-Technik erhöht. Die Tags können nicht mehr zu beliebigen Zwecken sondern erst nach expliziter Erlaubnis ausgelesen werden. Gleiches gilt für die übrigen genannten Ansätze zur Verhinderung unbeschränkten Auslesens: Sie gehen von der Annahme aus, dass nicht explizit zugelassenes Auslesen *grundsätzlich* unerwünscht und damit generell zu verhindern ist.

Nochmals: Für das Netzwerkdesign gilt die allgemein anerkannte Maxime, für das Design grundlegender Dienste möglichst wenige Annahmen zu treffen, um Mehrfach- bzw. Sekundärnutzungen sowie innovative Anwendungen erst zu ermöglichen. Offene Systeme zeichnen sich durch möglichst weit gehendes Befolgen dieser Maxime aus. Geschlossene Systeme hingegen werden – unter Berücksichtigung vergleichsweise vieler Annahmen – auf einen bestimmten Einsatzzweck hin optimiert. Die breite Einführung von Authentifikations-, Anonymisierungs- oder Verschlüssellungsmechanismen auf *allen* Tags wäre somit durchaus als *Verschließen* vormals offen gestalteter Systeme anzusehen – mit allen Vor- und Nachteilen.

Verschlossene RFID-Systeme würden zwar einen vergleichsweise guten Schutz vor unerwünschtem Auslesen bieten, würden aber gleichzeitig auch dem Infrastrukturcharakter einer für verschiedenste Anwendungszwecke nutzbaren *Nummeriertheit von Dingen* entgegenwirken. Entweder die Systeme bleiben den derzeitigen Plänen entsprechend offen gestaltet und erlauben somit die „gute“ wie auch die „böse“ Nutzung, oder aber sie werden deutlich in ihrer Flexibilität beschnitten und schränken damit die Nutzbarkeit durch innovative Sekundäranwendungen ein.

6 Zusammenfassung

Der Artikel hat gezeigt, dass trotz der derzeitigen Medienpräsenz das grundlegende Prinzip hinter RFID keineswegs neu ist. RFID-Systeme befinden sich bereits seit geraumer Zeit – beispielsweise in der Viehwirtschaft oder in Bibliotheken – im Einsatz und haben sich dort durchaus bewährt.

Dennoch zeichnet sich eine bedeutende Änderung ab: Waren bisherige Systeme noch meist „geschlossen“ und der Einsatz entweder auf einzelne Orte (z. B. die Bücherei des Vatikans) oder unterschiedliche Szenarien gleichen Typs (z. B. einheitliche Identifizierung von Vieh) beschränkt, zielen die derzeit geplanten Systeme explizit auf die unternehmens-

und prozessübergreifende Nutzung von Tags ab, die bereits bei der Produktion an nahezu alle Gegenstände angebracht werden. Durch die einheitliche Nutzung dieser standardisierten Tags für unterschiedlichste Produkte würde sich ein Zustand der allgemeinen und für verschiedenste Zwecke nutzbaren „Nummeriertheit von Dingen“ ergeben, der die Sekundärnutzung von Tags für verschiedenste Anwendungen – insbesondere auch für solche, die heute noch nicht vorhergesehen werden – ermöglichen würde.

Nun wird niemand auf die Idee kommen, für alle RFID-Systeme vollkommene Offenheit zu fordern. Vielmehr scheint es notwendig, zwischen besonders kritischen Anwendungen, bei denen das Sicherheits- und Privatheitsbedürfnis eindeutig Vorrang hat, und solchen Anwendungen, bei denen der mögliche Wert durch Sekundärnutzungen überwiegt, zu unterscheiden. Für den Fall, dass eine mögliche Sekundärnutzung eine eher unbedeutende Rolle spielt, erscheint der Aufbau geschlossener oder durch kryptographische Mittel *ver*schlossener Systeme durchaus sinnvoll. Zu nennen wären hier beispielsweise Funkbasierte Einlass- bzw. Schlüsselsysteme wie sie in der Autoindustrie als Schlüsselersatz zum Einsatz kommen[30].

Geradezu konträr verhält es sich jedoch mit den derzeit breit diskutierten elektronischen Etiketten nach dem EPC-Standard. Hier entstehen durch die Möglichkeit unterschiedlichster Sekundärnutzungen Potentiale, die in aktuellen Debatten oftmals untergehen. Nichtsdestotrotz sollten aber Ängste und Befürchtungen der Verbraucher ernstgenommen werden. Die Frage, wie in Zukunft Privatheit im Umfeld von RFID gestaltet werden soll, muss weiterhin diskutiert werden. Letztendlich wird sich vieles auf die Abwägung von Sekundärnutzen und potentiellen Gefahren reduzieren lassen. Die bewusste Unterscheidung zwischen offenen und geschlossenen Systemen jedenfalls scheint dabei hilfreich zu sein, mehr Ordnung in die eingangs erwähnte Unstrukturiertheit der Debatte zu bringen.

[30] Der vielzitierte „RFID-Reisepass“ wird hier bewusst ausgelassen, das es sich hierbei streng genommen nicht um ein Identifikationssystem sondern vielmehr um ein System zur funkbasierten Nahfeldkommunikation handelt.

Literatur

Article 29 Data Protection Working Party (2005). Working document on data protection issues related to RFID technology. Online: `http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf` [12.09.2005].

Berthold, O., O. Günther, und S. Spiekermann (2005). RFID-Technik: Verbraucherängste und Verbraucherschutz – eine Frage der Kontrolle. Online: `http://www.wiwi.hu-berlin.de/~sspiek/RFIDWI.pdf` [25.02.2005].

Bose, I. und R. Pal (2005). Auto-ID: Managing Anything, Anywhere, Anytime in the Supply Chain. *Communications of the ACM 48*(8), 100–106.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2004). *Chancen und Risiken des Einsatzes von RFID-Systemen*. Bonn, Ingelheim: Bundesamt für Sicherheit in der Informationstechnik und SecuMedia Verlags-GmbH.

Finkenzeller, K. (2002). *RFID-Handbuch*. München, Wien: Hanser.

Flörkemeier, C. (2004). EPC-Technologie - vom Auto-ID-Center zu EPCglobal. Online: `http://www.vs.inf.ethz.ch/publ/papers/floerkem-autoid-2004.pdf` [12.09.2005].

Isenberg, D. S. (1997). Rise of the Stupid Network. Online: `http://www.isen.com/stupid.html` [22.08.2005].

Kang, J. und D. Cuff (2005). Pervasive Computing: Embedding the Public Sphere. *Washington and Lee Law Review 62*.

Kügler, D. (2005). Risiko Reisepass? - Schutz der biometrischen Daten im RF-Chip. *c't Magazin für Computertechnik 5/2005*, 84–89.

Lampe, M., C. Flörkemeier, und S. Haller (2005). Einführung in die RFID-Technologie. Online: `http://www.vs.inf.ethz.ch/publ/papers/mlampe-rfid-2005.pdf` [22.08.2005].

Lemley, M. A. und L. Lessig (2004). The End of End-to-End: Preserving the Architecture of the Internet in the Broadband-Era. In: M. N. Cooper (Hrsg.), *Open Architecture as Communications Policy*. Stanford Law School: Center for Internet and Society.

Meyer, A. und P. Schüler (2004). Mitteilsame Etiketten. *c't Magazin für Computertechnik 9/2005*, 122.

NTRU (2005). GenuID. Online: `http://www.ntru.com/products/genuid.htm` [13.09.2005].

Sarma, S. E., S. A. Weis, und D. W. Engels (2002). RFID Systems, Security & Privacy Implications.

Schoenberger, C. R. (2002). RFID: The Internet of Things. *Forbes 18.03.2002*.

Spiekermann, S. und O. Berthold (2005). Maintaining Privacy in RFID Enabled Environments – Proposal for a disable-model. Online: `http://www.wiwi.hu-berlin.de/~sspiek/SPPC_spiekermann-edited.pdf` [21.09.2005].

Spiekermann, S. und F. Pallas (2005). Technology Paternalism - Wider Implications of Ubiquitous Computing. *Poiesis and Praxis*.

Stapleton-Gray, R. (2003). Scanning the Horizon: A Skeptical View of RFIDs on the Shelves. Online: `http://www.stapleton-gray.com/papers/sk-20031113.PDF` [13.09.2005].

Wan, D. (2000). The Magic Wardrobe: Situated Shopping from Your Own Bedroom. Accenture, Online: `http://www.accenture.com/xdoc/en/services/technology/publications/magicwardrobe-huc2000.PDF` [18.07.2005].

Weis, S. A. (2003). Security and Privacy in Radio-Frequency Identification Devices. Online: `http://theory.lcs.mit.edu/~sweis/masters.pdf` [18.07.2005].

Weiser, M. und J. S. Brown (1996). Designing Calm Technology. *PowerGrid Journal 1* (1), 94–100.