SEMINARARBEIT ZUM
INTEGRIERTEN SEMINAR:
GRUNDLAGEN WEBBASIERTER INFORMATIONSSYSTEME

Sommersemester 2004

RFID

(Radio Frequency IDentification)

Dipl.-Inf. (FH) Joachim Klein

Angewandte Informatik (BI)

AG Heterogene Informationssysteme
Technische Universität Kaiserslautern

Betreuer: Dipl.-Inf. Jürgen Göres

Freitag, 23. Juli 2004

Inhaltsverzeichnis

1 Einleitung

Die Entwicklungen in der RFID-Technologie (Radio Frequency IDentification) wurden in den letzten Jahren mit großer Kraft vorangetrieben. Die Technik als solche ist zwar nicht neu, doch viele Software- und Hardwarehersteller arbeiten fieberhaft an der Umsetzung einheitlicher Lösungen für Handel und Industrie. Den vielfältigen Einsatzmöglichkeiten dieser Technologie sind dabei kaum Grenzen gesetzt. Sie reichen vom Einsatz in Logistikketten bis zu Anwendungen in der Tierhaltung. Ein besonderes Problem stellt heutzutage jedoch immer noch die globale Umsetzung einer einheitlichen informationstechnischen Infrastruktur und ihre Integration in bestehende Systeme dar. Insbesondere für den Einsatz in der Logistik ist dies von besonderer Bedeutung. Die heutige Herausforderung besteht darin, eine Architektur zu entwickeln, welche es ermöglicht, Produktdaten über ein WAN (Wide Area Network; großräumiges Netzwerk) zwischen hunderttausenden gleichzeitig arbeitenden Benutzern auszutauschen. Heutzutage benutzen Einzelhändler und Lieferanten meist das Electronic-Data-Interchange-Protokoll (EDI[1]) um Daten bzw. Produktinformationen untereinander zu verteilen. Benutzen Firmen dieses oder andere Protokolle können nur die untereinander verbundenen Partner die Informationen interpretieren, ein eventuell betroffener Drittanbieter kann nicht dynamisch eingebunden werden.

Im vorliegenden Dokument werden zunächst die Grundlagen der neuen Technologie und der damit verbundenen Hardwarekomponenten erklärt, anschließend werden informationstechnische Software-Infrastrukturen vorgestellt. In einigen Anwendungsbeispielen wird gezeigt, wie und wofür die RFID-Technologie eingesetzt werden kann. Trotz zahlreicher Vorteile ist dieser weit reichende Einsatz der Technologie durchaus nicht unbedenklich. Die Möglichkeit, Personen und Gegenstände zu orten, berührt ein wichtiges Teilgebiet des Datenschutzes. Meinungen und Forderungen von Datenschützern sowie die Aussagen der Unternehmen, welche RFID-Technologie herstellen, werden im vorliegenden Dokument kritisch hinterfragt.

2 Grundlagen

2.1 Auto-ID-Systeme

Die Abkürzung Auto-ID steht für automatische Identifikationsverfahren, wie sie vor allem im Handel, in der Beschaffungs- und Distributionslogik und anderen Bereichen zu finden sind. Sie werden dazu verwendet, Informationen über Objekte wie z.B. Güter und Waren, aber auch Personen, bereitzustellen. Am weitesten verbreitet und hinlänglich bekannt sind sicher die Barcode-Aufdrucke, wie sie an jeder Milchpackung hierzulande zu finden sind. Andere automatische Identifikationsverfahren sind z.B. die automatische optische Zeichenerkennung (engl. Optical Character Recognition, OCR), welche die automatische Texterkennung von einer gedruckten Vorlage beschreibt, Chip-Karten beziehungsweise biometrische Identifikationssysteme (Fingerabdruck, Sprachidentifikation). Eine weitere wichtige Methode hierbei stellt die Radio Frequency Identification (RFID) dar.

2.2 RFID

Radio Frequency Identification (RFID, engl. für Identifizierung per Funk) ist eine Methode, um kontaktlos Daten lesen und speichern zu können. Die Daten werden auf so genannten RFID-Tags - oft auch als Transponder bezeichnet - gespeichert. Die gespeicherten Daten werden über elektromagnetische Wellen gelesen. Die Entfernung, über die ein Tag ausgelesen werden kann, schwankt aufgrund der Ausführung (aktiv/passiv), genutztem Frequenzband, Sendestärke und

[1] Electronic Data Interchange bezeichnet als Sammelbegriff alle elektronischen Verfahren zum *asynchronen* und *vollautomatischen* Versand von *strukturierten Nachrichten* zwischen *Anwendungssystemen unterschiedlicher Institutionen.* Typische verwendete Nachrichtenstandards sind: UN/EDIFACT, ANSI X.12, VDA, EANCON, ODETTE, GALIA, ebXML, XBRL.

Umwelteinflüssen zwischen wenigen Zentimetern und mehreren Metern. Ist der Chip selbst auch sehr klein, so wird die Baugröße maßgeblich durch die Antenne (ist abhängig von der Frequenz beziehungsweise Wellenlänge) und das Gehäuse bestimmt. Dadurch werden die möglichen Einbauorte und Anwendungen stark beschränkt [wikirfid].

2.3 Grundlegendes Modell für ein RFID-System

Ein RFID-System besteht stets aus den folgenden Komponenten:

- den Transpondern, welche an den zu identifizierenden Objekten angebracht sind,
- den Erfassungs- oder Lesegeräten und
- einer informationstechnischen Applikation, meist mit Anbindung an ein Datenbanksystem, welche die eingelesenen Daten verwaltet.

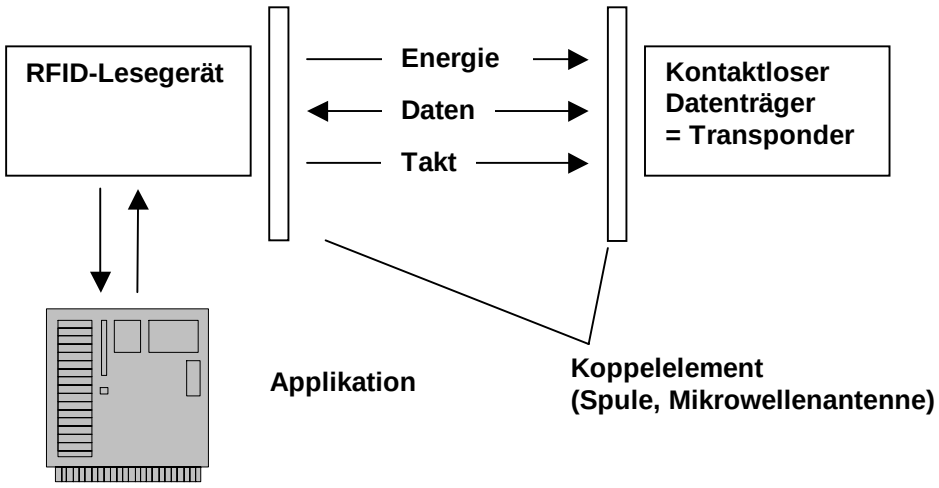

Abbildung 1: Lesegerät, Transponder und informationstechnische Applikation sind Grundbestandteile jedes RFID-Systems [Fink2002].

2.4 Stärken und Schwächen von RFID-Systemen

Der besondere Erfolg von RFID-Systemen gründet sich nicht nur auf der Möglichkeit, kontaktlos Daten zu übertragen. Die typische Datenmenge, welche derzeit in einem RFID-Chip gespeichert werden kann, liegt zwischen einem Bit und bis zu 64 kByte. Dies übertrifft die typische Größe für Barcodes bei weitem, welche nur auf 1 ~ 100 Bit kommen. Vergleichbar sind hier nur Chipkarten, welche eine ähnliche Datenmenge wie RFID-Chips erreichen. Ein weiterer Vorteil dieser Technologie ist, dass Einflüsse wie Nässe, Verschmutzung und Verschleiß aufgrund der kontaktlosen Kommunikation kaum eine Rolle spielen. Anschaffungs- und Betriebskosten sind vergleichsweise günstig und die Auslesegeschwindigkeit der Chips ist sehr hoch. (<0,3s).

Der kontaktlose Datentransfer führt allerdings dazu, dass Daten während der Kommunikation durch äußere Einflüsse leicht verfälscht werden können. Entsprechend aufwendige Verfahren zur Fehlererkennung und Korrektur können diesen Nachteil zwar mindern, aber Fehler doch nie ganz ausschließen. Ein weiterer weniger gravierender Nachteil ist sicherlich auch die Tatsache, dass die Lesbarkeit der Daten durch Personen ohne weitere Hilfsmittel nicht gewährleistet ist, was z.B. bei OCR sehr einfach ist.

2.5 Unterscheidungsmerkmale für RFID-Systeme

Da es unzählige verschiedene Varianten von RFID-Systemen gibt, ist es sinnvoll, Unterscheidungsmerkmale festzulegen, anhand derer man die verschiedenen Systeme kategorisieren kann.

Außerdem stellen diese Unterscheidungsmerkmale eine wichtige Entscheidungsgrundlage für die Auswahl eines RFID-Systems dar. Einen Überblick über wichtige Unterscheidungsparameter gibt das folgende Diagramm (Abbildung 2).

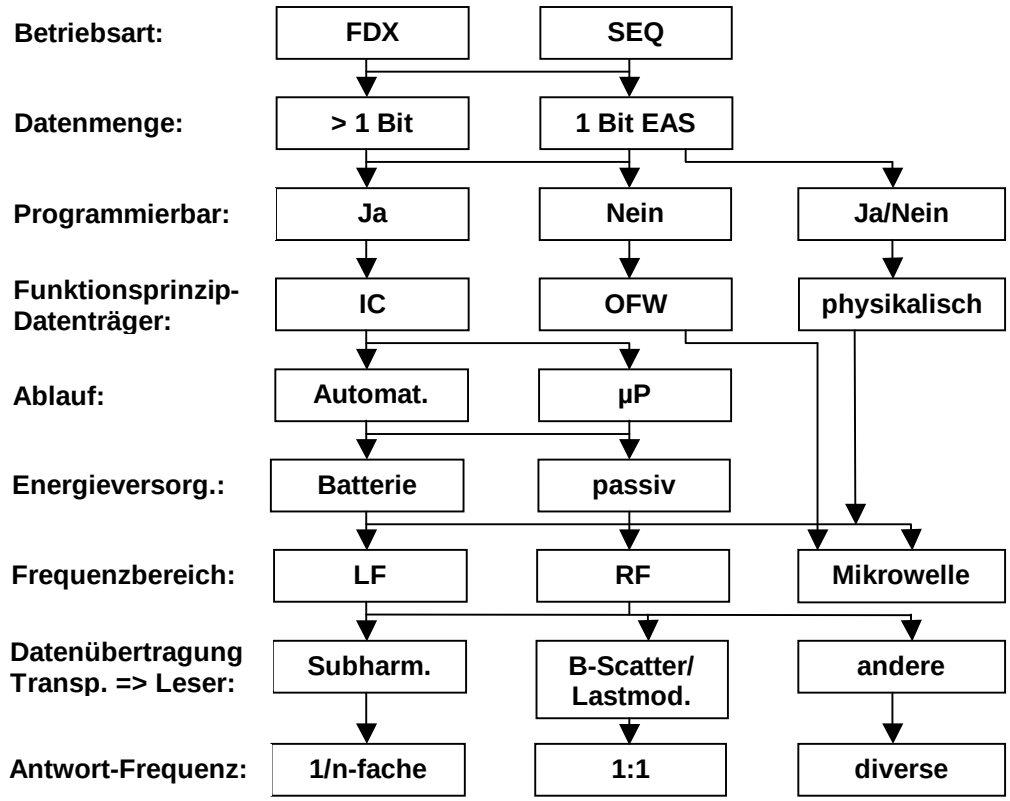

Abbildung 2: Verschiedene Unterscheidungsmerkmale von RFID-Systemen [Fink2002].

Kopplung

Ein im Diagramm nicht eingeordnetes aber grundlegendes Unterscheidungsmerkmal für alle RFID-Systeme ist die Art der Kopplung. Diese kann *induktiv* durch Spulenstrukturen, welche als Antennen wirken oder *kapazitiv* durch flächige Kondensatoren realisiert werden. Induktive Systeme verfügen über einen besonders guten Kopplungseffekt, erfordern allerdings den Einbau einer unverletzten Antenne, welche aus verhältnismäßig teurem Kupfer gefertigt ist. Kapazitive Systeme sind demgegenüber sehr leicht zu fertigen, z.B. durch den Aufdruck leitender Tinte und somit auch kostengünstiger. Allerdings besitzen sie eine schlechtere Kopplung und somit auch eine geringere Ausleseentfernung.

Betriebsart

Bei der Betriebsart werden *simultane* und *sequentielle* Systeme voneinander unterschieden. Simultane Systeme, welche wiederum in Voll- (full duplex, FDX) und Halbduplex-Systeme (half duplex, HDX) eingeteilt werden, übertragen die Antwort des Transponders bei eingeschaltetem Hochfrequenz-Feld. Hierbei ist es notwendig, die Signale des Lesers von denen der Labels unterscheiden zu können, z.B. durch Verwendung unterschiedlicher Frequenzen beziehungsweise Modulationsarten. Bei *sequentiellen Verfahren* hingegen wird das Feld des Lesegerätes periodisch für kurze Zeit ausgeschaltet. Dies setzt allerdings voraus, dass die Labels entweder mit einer eigenen Spannungsversorgung ausgestattet sind oder mit einer Spannungspufferung z.B. über einen Kondensator agieren.

Datenmenge

In Bezug auf die Datenmenge, die ein Transponder speichern kann, unterscheidet man grundsätzlich zwischen *1-Bit*-Systemen und *n-Bit*-Systemen, wobei letztere sogar mehrere kBytes übertragen können. Für viele Anwendungen wie einfache Überwachungs- oder Signalisierungsaufgaben sind 1-Bit-Systeme völlig ausreichend, welche zusätzlich den Vorteil besitzen, dass für einen 1-Bit-Transponder kein integrierter Schaltkreis benötigt wird, was die Herstellung besonders günstig macht.

Programmierbarkeit

RFID-Systeme werden oft auch einfach in Bezug auf die Beschreibbarkeit der Labels unterschieden. Hier unterscheidet man zwischen Read-Only- und Read-Write-Tags. Read-Only-Transponder werden schon während der Herstellung beschrieben, z.B. mit einer einfachen Seriennummer, auf die dann nur noch lesend zugegriffen werden kann. Bei Read-Write-Systemen lassen sich die Labels mehrfach mit Daten überschreiben. Diese Systeme werden meist mit EEPROMs[2], FRAMs[3] oder auch SRAMs[4] bei Mikrowellensystemen zur Datenspeicherung realisiert.

Funktionsprinzip Datenträger beziehungsweise Ablauf

Vor allem bei programmierbaren RFID-Labels kommt der Realisierung des Datenträgers eine besondere Bedeutung zu. Die verschiedenen Schreib- und Lesezugriffe müssen durch logische Bausteine abgebildet werden. Am einfachsten kann diese Abbildung durch einen einfachen Zustandsautomaten mit Hilfe eines integrierten Schaltkreises (IC) realisiert werden. Dies bedeutet allerdings eine geringe Flexibilität bei Änderungen, da diese ein Neudesign des ICs erfordern. Besser ist unter diesem Aspekt die Verwendung eines Mikroprozessors (µP), welcher ein eigenes Betriebssystem zur Verwaltung von Applikationsdaten erhält. Änderungen können so kostengünstiger durch eine Softwarelösung eingebracht werden. Bei der Verwendung von Chipkarten spricht man diesbezüglich auch von *Speicherkarten* (für IC) und *Prozessorkarten* (für µP).

Es gibt aber auch Transponder die Daten aufgrund von physikalischen Zusammenhängen speichern können. Hierunter fallen die Read-only-Oberflächenwellen-Transponder sowie 1-Bit-Transponder, die durch ein beschreiben mit „0“ deaktiviert bzw. mit „1“ aktiviert werden können.

Energieversorgung

Eines der wichtigsten Merkmale zur Unterscheidung von RFID-Systemen ist die Art der Stromversorgung für die Transponder. Es gibt Tags, welche keine Stromquelle benötigen und somit komplett von der durch das Hochfrequenzfeld des Lesers erzeugten Energie abhängig sind. Sie werden als *passive Transponder* bezeichnet. Im Gegensatz dazu enthalten *aktive Transponder* eine Stromquelle welche die Energie zum Betrieb des Mikrochips und zum Senden der Antwort zur Verfügung stellt.

---

[2] EEPROM steht für Electrically Eraseable Programmable Read Only Memory. Im Gegensatz zu einem EPROM kann der Inhalt eines EEPROMs elektrisch (electrically) gelöscht werden. Bei EPROMs ist zum Löschen eine UV-Lampe nötig, EEPROMs können in einem Programmiergerät gelöscht werden. Der Löschvorgang dauert deshalb nur einige Sekunden - verglichen mit 5 bis 10 Minuten beim EPROM.

[3] Als Ferroelectric Random Access Memory (FRAM oder FeRAM) bezeichnet man einen elektronischen Speichertyp auf der Basis von Kristallen mit ferroelektrischen Eigenschaften (ferroelektrische Kristalle ähneln in ihrem Verhalten Ferromagneten).

[4] Statisches RAM (engl. Static Random Access Memory, abgekürzt SRAM) bezeichnet einen Typ von Speicherbausteinen. Im Gegensatz zu DRAMs (dynamisches RAM) müssen, um die Daten zu erhalten, außer der Betriebsspannung keine Signale zum Auffrischen erzeugt werden, die Daten bleiben also auch bei statischer Ansteuerung erhalten.

Frequenzbereich

Das wichtigste Unterscheidungsmerkmal für ein RFID-System ist der Frequenzbereich, oft auch als Betriebsfrequenz bezeichnet, welcher entscheidenden Einfluss auf die Reichweite des Systems hat. Als Betriebsfrequenz wird dabei die Sendefrequenz des Lesegerätes bezeichnet. Die Sendefrequenz der Transponder wird nicht berücksichtigt. Die Systeme werden unterteilt in

- LF-Systeme (low frequency), 30 kHz – 300 kHz,
- HF- (high frequency) beziehungsweise RF-Systeme (radio frequency), 3 MHz – 30 MHz und
- UHF-Systeme (ultra high frequency), 300 MHz – 3 GHz.

Nach Reichweite wird unterschieden in

- Close coupling (0 – 1 cm), so genannte *proximity labels*,
- Remote coupling (0 – 1 m) und
- Long range Systeme (über 1 m).

Datenübertragung und Antwort-Frequenz

In Bezug auf die Datenübertragung vom Transponder zum Lesegerät und der dafür verwendeten Frequenz, werden drei grundlegende Verfahren unterschieden:

- Transponder, die die gleiche Frequenz wie das Lesegerät verwenden (Frequenzverhältnis 1:1). Sie können realisiert sein als
  Backscatter, die unter Anwendung von Reflexion arbeiten, wobei die Frequenz der reflektierten Welle der Sendefrequenz des Lesegerätes entspricht oder Transponder mit Lastmodulation, bei denen das Sendefeld des Lesegerätes durch den Transponder beeinflusst wird
- *subharmonische* Transponder, welche mit 1/n–tel der Abfragefrequenz antworten
- *Oberwellen*-Transpondern welche auf n-facher Abfragefrequenz antworten.

2.6 Transponder

2.6.1 Bauformen von Transpondern

An dieser Stelle soll kurz auf die grundlegenden unterschiedlichen Bauformen hingewiesen werden. Viele dieser Bauformen wurden speziell für eine bestimmte Anwendung neu entwickelt, wie z.B. induktiv gekoppelte Transponder zur Werkzeug- und Glasflaschenidentifikation. Es wurden aber auch spezielle Bauformen für Schlüsselanhänger, Uhren und Chipkarten entwickelt. Eine der wichtigsten Bauformen sind die papierdünnen *Smart Labels*. Die verschiedenen Vor- und Nachteile der Bauformen lassen sich in [Fink2002] genau nachlesen.

2.6.2 Realisierungen elektronischer Datenträger

In Kapitel 2.5 wurde schon auf die Vielzahl der Realisierungsmöglichkeiten für Transponder hingewiesen. Als elektronische Datenträger werden Transponder bezeichnet, welche auf der Grundlage integrierter Schaltungen realisiert sind. Ihnen gegenüber werden Transponder unterschieden, welche ihre Daten rein durch Ausnutzung physikalischer Effekte speichern. Zu ihnen gehören z.B. 1-Bit-Transponder. Letztere reichen für einfache Anwendungen, wie die Positionserfassung von Gegenständen bereits aus. In komplexen logistischen Anwendungen sind erweiterte Eigenschaften erforderlich. Beim Transport von Gütern und Waren müssen die Tags von verschiedenen Partnern eingelesen werden, welche auch neue Daten auf den Datenträger schreiben wollen. Damit dies nur für berechtigte Instanzen möglich ist, braucht der Transponder ein Betriebssystem zum Einlesen und Schreiben neuer Daten und zur Durchführung einer Zugangskontrolle. Er sollte

auch über ein Verschlüsselungsmodul verfügen, welches sicherstellt, dass nur befugte Instanzen den Transponder auslesen können. In manchen Fällen soll sogar eine Speicherung mehrerer Anwendungen auf dem Datenträger möglich sein. Die grundlegenden Bausteine solcher Datenträger werden nun näher betrachtet (siehe Abbildung 3).

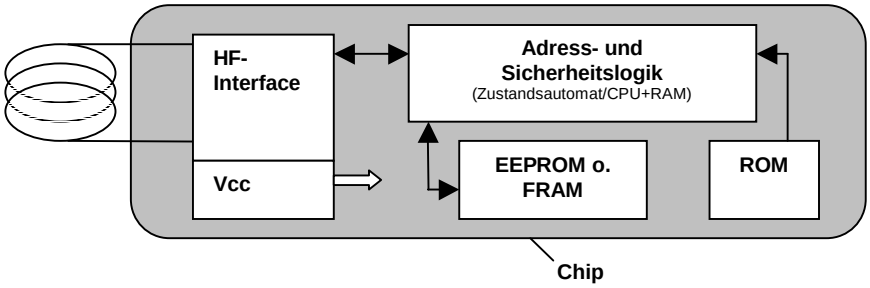

Abbildung 3: Blockschaltbild eines RFID-Datenträgers mit Speicherfunktion [Fink2002]

Hochfrequenz-Interface des Transponders

Das HF-Interface bildet die Schnittstelle zwischen dem analogen, hochfrequenten Übertragungskanal vom Lesegerät zum Transponder und den digitalen Schaltungselementen des Transponders. Das HF-Interface entspricht daher in seiner Aufgabe dem klassischen Modem, wie es zur analogen Datenübertragung über Telefonleitungen eingesetzt wird. Passive Transponder werden über das HF-Interface zudem mit Energie versorgt. Hierzu wird der vom HF-Feld induzierte Strom gleichgerichtet und dem Chip als Versorgungsspannung (siehe Abbildung 3. „Vcc“) zur Verfügung gestellt. Um Daten an das Lesegerät zurücksenden zu können, verfügt das HF-Interface über einen Last- oder Backscatter-Modulator (oder andere Verfahren, z.B. Frequenzteiler), welcher das Antwortsignal entsprechend den digitalen Sendedaten moduliert. [fink2002].

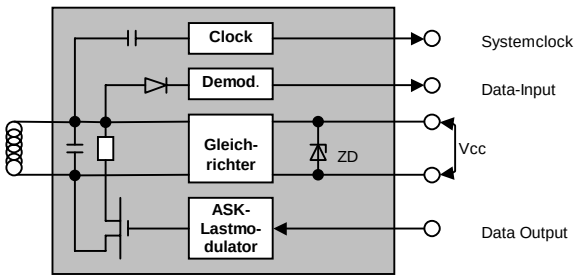

Abbildung 4: Blockschaltbild des HF-Interfaces eines induktiv gekoppelten Transponders mit Lastmodulator [fink2002]

Adress- und Sicherheitslogik

Die *Adress- und Sicherheitslogik* ist der Kern des Datenträgers und steuert alle Vorgänge auf dem Chip.

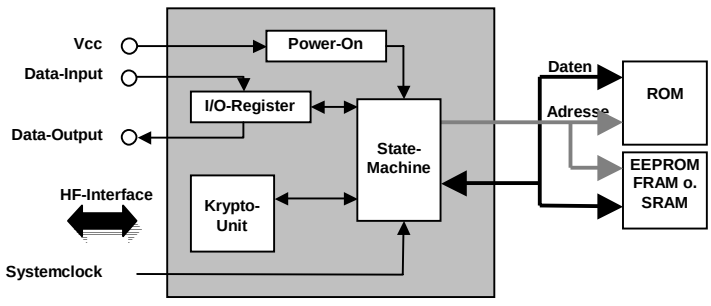

Abbildung 5: Blockschaltbild der Adress- und Sicherheitslogik [fink2002]

Durch eine *Power-On-Logik* wird der Datenträger bei Eintritt in ein HF-Feld in einen definierten Anfangszustand überführt. Ähnlich wie in einem Prozessor dienen spezielle I/O-Register dem Datenaustausch mit dem Lesegerät. Optional kann auch noch eine *Krypto-Unit* zur Authentifizierung, Datenverschlüsselung und Schlüsselverwaltung hinzugefügt werden. Über einen Adress- und Datenbus sind die Datenspeicher, ein ROM für unveränderliche Daten und EEPROM oder FRAM für sich ändernde Daten angebunden. Der zur Ablaufsteuerung und Systemsynchronisation benötigte *Takt* (Systemtakt) wird durch das HF-Interface der Adress- und Sicherheitslogik zugeführt.

Die zustandsabhängige Steuerung aller Vorgänge übernimmt ein Zustandsautomat (*State Machine*, *hard wired Software*). Die durch State Machines erreichbare Komplexität reicht durchaus an die Leistung von Mikroprozessoren heran. Allerdings ist der „Programmablauf" dieser Automaten durch das Chipdesign festgelegt und nicht programmierbar. Eine Änderung oder Anpassung an spezielle Systemanforderungen kann nur durch ein geändertes Chipdesign verwirklicht werden.

Die komplette Steuerung der Adress- und Sicherheitslogik kann auf dem Chip auch durch eine CPU und zusätzliches RAM umgesetzt werden. Auf dem angeschlossenen ROM wird dann das Betriebssystem für den Transponder abgelegt, welches die benötigten Funktionen bereitstellt. Dies hat den Vorteil, dass der Chip in seinem Funktionsumfang dynamisch erweitert werden kann [fink2002].

Speicherarchitektur

Neben dem Zustandsautomaten oder Mikroprozessor ist der Speicher einer der wichtigsten Bestandteile. Auf dem nach der Herstellung nicht mehr beschreibbaren ROM-Speicher sind Daten wie z.B. Unikatsnummern (einmal vergebene Seriennummer, EPC-Daten (siehe Kapitel 3)) oder auch Programmdaten zum Auslesen dauerhaft abgelegt.

Sollen auch neue Daten auf dem Transponder abgelegt werden, so werden auch RAM-, EEPROM- und FRAM-Zellen auf dem Tag aufgebracht. EEPROM- und FRAM-Zellen sind erforderlich, wenn die geschriebenen Daten ohne Spannungsversorgung über lange Zeit (ca. 10 Jahre) gespeichert werden müssen. Weitere detaillierte Informationen sind in [fink2002] zu finden.

2.7 Lesegeräte

Auch in diesem Abschnitt wird nur auf die grundlegenden Eigenschaften der Lesegeräte eingegangen. Es wird nicht das Ziel verfolgt die genaue technische Realisierung dieser Geräte zu erklären. Einen guten Überblick bildet auch hier das Standardwerk zur RFID-Technologie [fink2002].

2.7.1 Datenfluss in einer Applikation

Eine Softwareanwendung (Applikationssoftware), welche Daten von einem kontaktlosen Datenträger (Transponder) lesen oder schreiben möchte, benötigt als Schnittstelle das Lesegerät. Aus Sicht der Applikationssoftware sollte der Zugriff dabei möglichst transparent erfolgen. Die einzelnen Komponenten Applikation, Lesegerät und Transponder stehen hierbei in einer Master-Slave-Beziehung zueinander. Dabei werden alle durchzuführenden Operationen durch die Applikationssoftware angestoßen. Auch der Transponder antwortet ausschließlich auf Befehle des Lesegerätes und wird nie selbständig aktiv (ausgenommen einfachste Read-only-Transponder). Es ist also insbesondere auch die Aufgabe der Applikationssoftware bzw. des Lesegerätes abzufragen, ob und wie viele Transponder sich im Feld befinden.

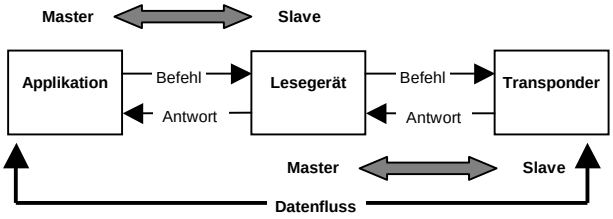

Abbildung 6: Master-Slave-Prinzip zwischen Applikationssoftware (Applikation), Lesegerät und Transponder [fink2002]

2.7.2 Komponenten eines Lesegerätes

Lesegeräte aller Systeme können auf zwei grundsätzliche Funktionsblöcke reduziert werden: die *Steuerung* und das *HF-Interface*, bestehend aus Sender und Empfänger. Die Lesegeräte werden mit dem Computer meist über die serielle Schnittstelle verbunden. Im Folgenden werden die Aufgaben der beiden Funktionsblöcke kurz erläutert.

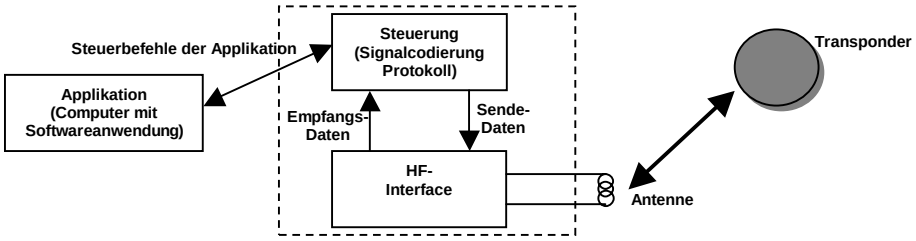

Abbildung 7: Blockschaltbild eines Lesegerätes [fink2002]

HF-Interface des Lesegerätes

Das HF-Interface stellt die Schnittstelle zwischen dem Lesegerät und dem kontaktlosen Transponder dar und übernimmt folgende Aufgaben:

- Erzeugung einer hochfrequenten Sendeleistung zur Aktivierung und Energieversorgung eines Transponders.
- Modulation des Sendersignals zur Übertragung der Daten zum Transponder.
- Empfang und Demodulation von HF-Signalen, ausgehend von einem Transponder.

Steuerung

Die Steuerung eines Lesegerätes übernimmt mindestens die folgenden Aufgaben:

- Kommunikation mit der Applikationssoftware,
- Steuerung des Kommunikationsablaufs mit einem Transponder (Master-Slave-Prinzip) und
- Signalkodierung und –decodierung

Komplexere Systeme verfügen zusätzlich meist über folgende Funktionen:

- Ausführen eines Applikationsalgorithmus, z.B. zum Filtern von Daten
- Ver- und Entschlüsselung der zwischen Transponder und Lesegerät zu übertragenden Daten
- Abwicklung einer Authentifizierung zwischen Transponder und Lesegerät

Die voran stehenden Aufgaben werden durch einen Mikroprozessor übernommen. Rechenintensive Funktionen, wie z.B. die Verschlüsselung der Daten während der Kommunikation zwischen

Lesegerät und Transponder, werden durch einen speziellen Zusatzchip (ASIC[5]) übernommen. Das Lesegerät ist über eine serielle Schnittstelle (RS232, RS485 oder USB) mit dem Computer verbunden. Als Codierung wird auf diesem Übertragungsweg meist, wie in der PC-Welt üblich, eine NRZ-Codierung verwendet. Als Kommunikationsprotokoll werden heute noch oft selbst definierte Protokolle eingesetzt. In Kapitel 3 werden wir sehen, dass für einen globalen Einsatz einheitliche Protokolle unerlässlich sind.

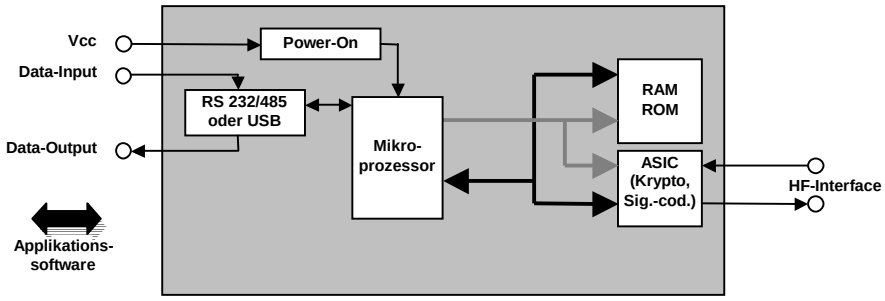

Abbildung 8: Blockschaltbild der Steuerung eines Lesegerätes [fink2002]

3 Kommunikationsarchitekturen

In der Folge wollen wir uns damit beschäftigen, wie Produktdaten, welche von Lesegeräten erfasst werden, anderen Partnern zur Verfügung gestellt werden können. Diese Fragestellung ist Gegenstand aktueller Forschung und unterliegt noch einem steten Wandel. Vor allem in der Logistik ist eine lokal gebundene Lösung wenig sinnvoll. Standards, welche eine Kommunikation der verschiedenen Systeme über Firmengrenzen hinweg ermöglichen, sind notwendig, um Lieferketten und die Kommunikation zwischen beliebig vielen Partnern zu optimieren.

3.1 Der EPC-Standard

EPC (Electronic Product Code) ist der Standard mit welchem dieses geleistet werden soll. Ziel ist es, in Echtzeit Daten zu Produkten über das Internet zugänglich zu machen. Hierzu wurde vom Auto-ID Center des *Massachusetts Institute of Technology* (M.I.T.) die *Web Services WAN Special Interest Group* (SIG) gebildet, welche einen ersten Prototypen zur Verteilung von EPC-Daten über WANs (Wide Area Networks) mit Hilfe von Web Services realisieren soll. Aus dieser Initiative entstand die EPC-Netzwerk-Architektur.

Der Standard wird unterstützt durch EPCGlobal, eine Gemeinschaftsunternehmung von *EAN International*[6] und dem *Uniform Code Council*[7] (UCC). In Verbindung mit Vertretern der Industrie[8] verfolgt sie das Ziel, die EPC-Netzwerk-Architektur als globalen Standard zur direkten, automati-

[5] Unter Application Specific Integrated Circuit (ASIC), auch Custom-Chip, versteht man eine anwendungsspezifische integrierte Schaltung. Diese integriert z.B. eine große Zahl von Logik-Funktionen, für die sonst aus diversen Standardbausteinen wie CPUs, Logikfamilien (z.B. AND-Gatter, OR-Gatter, bipolaren Schaltungen der Serie 74xxx, usw.) oder ähnlichen Bausteinen zusammengestellt werden müssten.

[6] Die EAN (**E**uropäische **A**rtikel-**N**ummer) ist eine ursprüngliche europaweite, heute weltweite eindeutige Produktkennzeichnung für Handelswaren. Sie ist ein wichtiger Bestandteil jeder modernen Warenwirtschaft und hat 13 (bzw. 8) Stellen. Meist ist sie als Strichcode (Barcode) auf die Warenverpackung aufgebracht. Die EAN wurde von der Organisation „EAN International" entwickelt.

[7] Die Abkürzung **UCC** steht für das **Uniform Code Council**. Hierbei handelt es sich um eine der weltweit einflussreichsten Organisationen, die sich auf Globalisierung und Standardisierung spezialisiert hat. Sie ist eine gemeinnützige Mitgliedsorganisation der EAN International.

[8] einige wichtige Vertreter sind: WalMart, Boehringer Ingelheim International GmbH, DHL Logistics GmbH, FEIG ELECTRONIC GmbH, Hermos Informatik GmbH, Infineon Technologies AG, METRO AG, PolyIC GmbH & Co. KG, …

schen und akkuraten Identifikation aller Gegenstände in einer Lieferkette, für jede Firma und jeden beliebigen Industriezweig, durchzusetzen [EPCG].

Es gibt noch eine Vielzahl anderer Programme welche die Verbreitung und Einführung dieser Technik unterstützen. Ein wichtiges in Europa ist das EAP (European Adoption Program), eine Arbeitsgruppe der „CPG Business Action Group[9]“ [EANat].

3.1.1 Die EPC Netzwerk Architektur

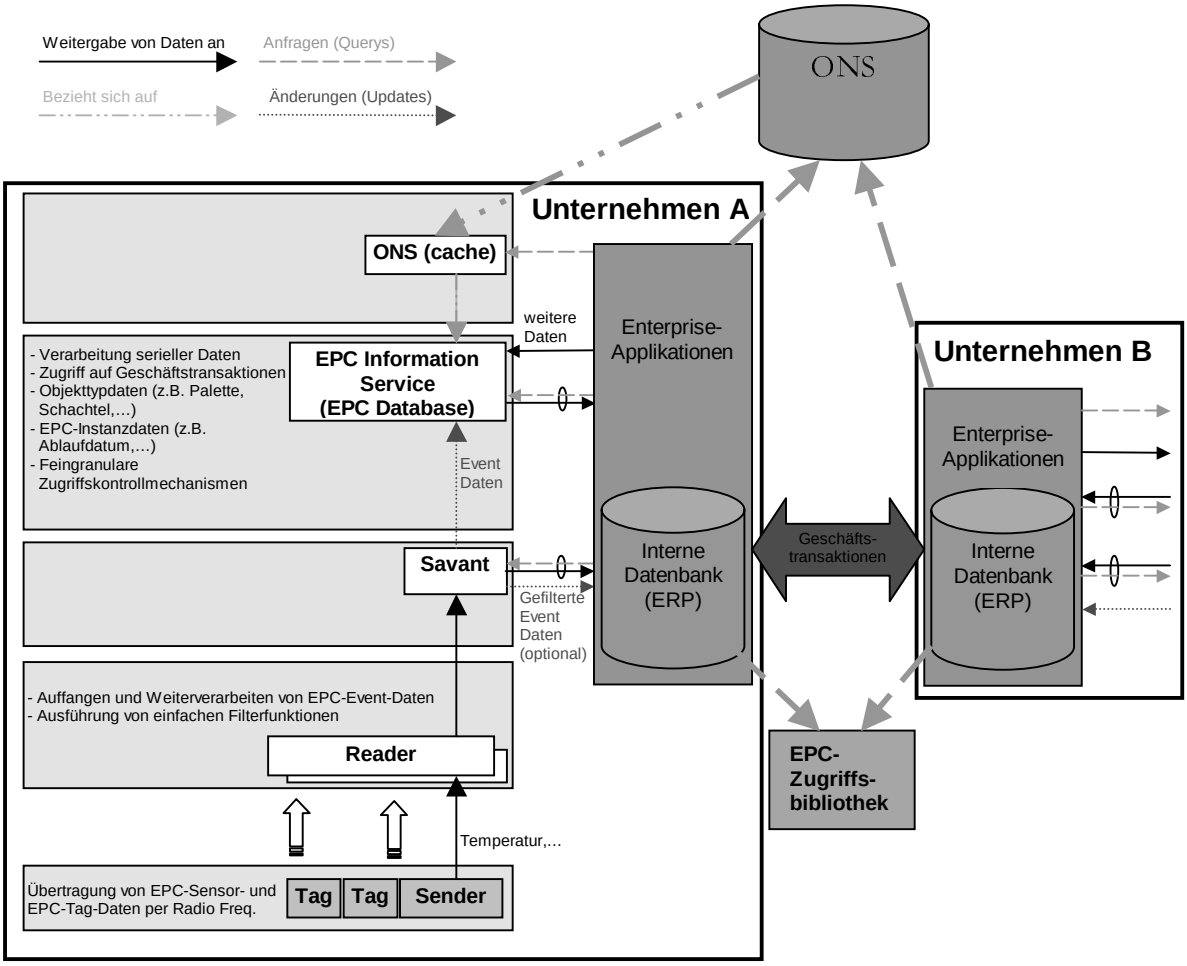

Abbildung 9: Die EPC-Netzwerk-Architektur über Firmengrenzen hinweg [EPCGsav]

Abbildung 9 beschreibt, die Verarbeitung der EPC-Daten über die verschiedenen Bearbeitungspunkte (Schichten) des EPC-Netzwerks hinweg. Damit die Daten eines EPC-Tags, die von den entsprechenden Lesegeräten eingelesen werden, von allen Herstellern auf gleiche Art und Weise verwendet und auf das Tag aufgebracht werden, wurde eine entsprechende EPC-Tag-Daten-Spezifikation entwickelt. In ihr werden eindeutige Formate für die EPC-Identifikationsnummer festgelegt. Gleichzeitig wird gezeigt, auf welche Art und Weise es für eine Applikationssoftware möglich wird, standardisiert auf die EPC-Daten Zugriff zu nehmen. Hier wird ein einheitlicher Zugriff durch Anwendungsprogramme auf die verschiedenen Lesegeräte und umgekehrt über die neu entwickelte Middleware *Savant* gewährleistet. Um Handelspartnern einen einheitlichen Zugriff auf mit EPC-Daten verbundene Dienste und Informationen zu gewähren, werden Web Services in Verbindung mit den Standards *ONS* (Object Name Service) und *PML* (Physical Markup Language) benutzt. Der ONS basiert auf dem DNS (Domain Name Service) und liefert zu einer EPC-

[9] CPG steht für Consumer Packaged Goods

Identifikationsnummer eine oder mehrere Internetadressen zurück an denen weitere Informationen abrufbar sind. Die PML ist eine XML-basiserte Auszeichnung für EPC-Daten. Eine global zugreifbare EPC-Zugriffsbibliothek beschreibt die Schnittstellen der EPC Web Services der verschiedenen Anbieter.

3.1.2 EPC-Tag-Daten-Spezifikation

Der EPC (Electronic Product Code) [EPCGtag] ist ein Identifikationsschema zur weltweit eindeutigen Kennzeichnung von physischen Objekten mit Hilfe der Radiofrequenzidentifikation. Die Tag-Daten-Spezifikation beschreibt, wie dieser Code auf einem Transponder kodiert wird. Außerdem wird die Art und Weise der Verarbeitung dieser Daten über die verschieden Schichten des EPC-Netzwerks hinweg normiert. Ein Beispiel hierfür sind die EPC-URI-Kodierungen (Uniform Resource Identifier Encodings), welche im Folgenden nur noch mit EPC-URI bezeichnet werden.

Der EPC gliedert sich in einen Kopf (*Header*) gefolgt von einem oder mehreren Wertefeldern (*Value-Fields*). Der Kopf beschreibt die Gesamtlänge des Codes und das Format der Wertefelder. In einem Wertefeld ist die eindeutige EPC-Identifikationsnummer (EPC-Id) enthalten und optional ein Filterwert, falls eine Dekodierung auf dem Transponder selbst nötig beziehungsweise gewünscht ist. Diese Option wird meist zur effizienteren Verarbeitung der Daten benutzt. Durch einen Filterwert, können beispielsweise einzelne Artikel von Paletten unterschieden werden. Zusätzlich zu diesen standardisierten Daten können auch benutzerdefinierte Daten in weiteren Wertefeldern abgelegt werden.

Die EPC-URIs stellen Hilfsmittel für die Verarbeitung der EPC-Daten bereit. Einerseits auf Bit-Level und andererseits für die verschiedenen Schichten der semantischen Abstraktionsebenen, welche unabhängig von der physischen Ablage sind. Es werden vier Kategorien von URIs unterschieden:

1. URIs für echte Entitäten (pure Identities), welche auch *canonical forms* genannt werden. Diese beinhalten nur die eindeutige Information (die EPC-Id) zur Identifikation eines Objektes, die noch unabhängig von der physischen Ablage sind.
2. URIs welche spezielle Transponderkodierungen repräsentieren. Diese werden in der Applikationssoftware an den Stellen verwendet, an denen das Kodierungsschema relevant ist, z.B. beim Beschreiben eines Tags.
3. URIs welche Muster oder ganze Mengen von EPC-Tags repräsentieren. Diese werden benutzt, zum Filtern von Informationen aus den EPC-Daten.
4. URIs welche die Rohdaten der EPC-Tags repräsentieren. Diese werden normalerweise nur zur Fehlerbehandlung eingesetzt.

Im Folgenden werden zunächst die Konzepte zur Kodierung der EPC-Id betrachtet. Danach werden die EPC-URIs noch etwas genauer betrachtet. Eine komplette Übersicht über die verschiedenen Kodierungsschemata findet man in der EPC-Tag-Daten-Spezifikation der EPCGlobal [EPCGtag].

Die EPC-Identifikationsnummer (EPC Identifier, EPC-Id)

Die EPC-Id ist ein Meta-Schema zur Kodierung, welches entwickelt wurde, um die Anforderungen der verschiedenen Industriezweige an eine eindeutige Kennzeichnung ihrer Objekte zu erfüllen. Zusätzlich zu den existierenden Kodierungen können wenn erforderlich auch weitere auf diesem Schema definiert werden. Die verschiedenen Kodierungsarten sind je nach unterstützter Domäne benannt, z.B. nach einem speziellen Industriezweig oder Handelgruppen.

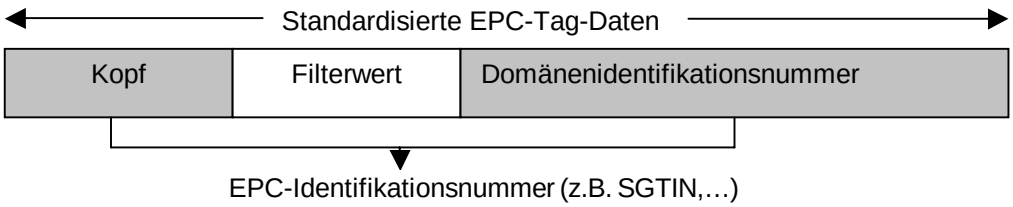

Abbildung 10: Aufbau der EPC-Tag-Daten

In der aktuellen EPC-Tag-Daten-Spezifikation sind folgende Kodierungsschemata definiert:

- Generell Identifier (GID)
- eine serialisierte Version der EAN.UCC Global Trade Item Number (GTIN)
- EAN.UCC Serial Shipping Container Code (SSCC®)
- EAN.UCC Global Location Number (GLN®)
- EAN.UCC Global Returnable Asset Identifier (GRAI®)
- EAN.UCC Global Individual Asset Identifier (GIAI®)

definiert. Der GID beschreibt das ursprüngliche EPC-Format. Zu diesem wurden die durch die Organisationen EAN und UCC weit verbreiteten Nummernformate mit aufgenommen. Das EPC-Format SGTIN-96, wurde speziell für die General Trade Item Number (GTIN) – den UPC (Universal Product Code) und die EAN (European Article Number) – entwickelt. Da der UPC und die EAN über keine Produktseriennummer verfügen, wurden die in diesen Codes typischen Felder für den Herstellercode und den Produkttyp in diesen EPC-Typ übernommen und durch eine Produktseriennummer ergänzt [flör2004].

Nachfolgend betrachten wir das diesen speziellen Kodierungen gemeinsame Framework zur Kodierung der EPC-Daten. Es ist sinnvoll, die drei folgenden Ebenen der Identifikation zu unterscheiden (siehe Abb. 11).

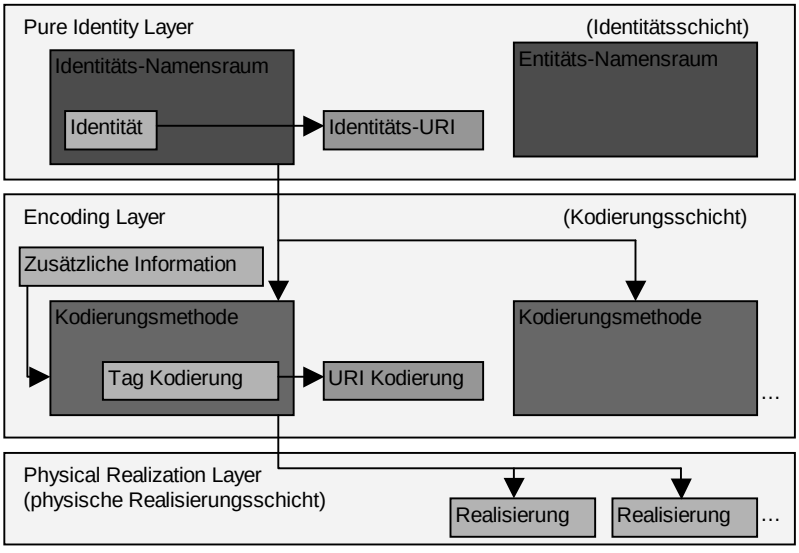

Abbildung 11: Die Unterscheidung in Identitätsschicht, Kodierungsschicht und physische Realisierungsschicht [EPCGtag]

Die (echte) Identität (pure identity) bezeichnet die Beziehung zu einer physischen oder logischen Entität unabhängig von dem verwendeten Speicherort oder Kodierungssystem, wie z.B. einem RFID-Tag, einem Barcode oder einem Datenbankfeld. Eine *pure indentity* ist demnach ein abstrakter Name oder eine Nummer, welche eine Entität eindeutig identifiziert. Sie enthält darüber hinaus

keine weiteren Informationen. Der Uniform Resource Identifier (URI) einer pure identity ist eine eindeutige Zeichenkette, welche im Allgemeinen dazu benutzt wird, Identitätsdaten zwischen Softwarekomponenten größerer Systeme auszutauschen und referenzieren zu können.

In der Kodierungsschicht wird die unabhängige Identitätsinformation, zusammen mit zusätzlicher Information, wie z.B. dem optionalen Filterwert, in eine spezielle Syntax überführt. Eine pure identity kann auf mehreren verschiedenen Kodierungsarten kodiert werden, wie z.B. mit einer Barcode-Kodierung, verschiedenen Transponderkodierungen oder verschiedenen URI-Kodierungen. Kodierungsschemata können neben der Identität auch andere Daten enthalten, wie z.B. der schon erwähnte Filterwert, wobei in diesem Fall das Kodierungsschema festlegt, welche zusätzlichen Daten dies sein dürfen.

In der Realisierungsschicht wird die kodierte Information in eine entsprechende plattformabhängige Kodierung überführt. Dies kann z.B. für eine bestimmte Art von RFID-Tags geschehen oder ein bestimmtes Datenbankfeld. Eine Kodierung kann mehrere Möglichkeiten der physischen Realisierung besitzen.

Beispielhaft wird eine Kodierung über die 3 Schichten hinweg gezeigt. Hierbei wird die Kodierung einer SGTIN (Serialized Global Trade Item Number) verwendet. Die im Beispiel verwendete GTIN ist die 10614141007346.

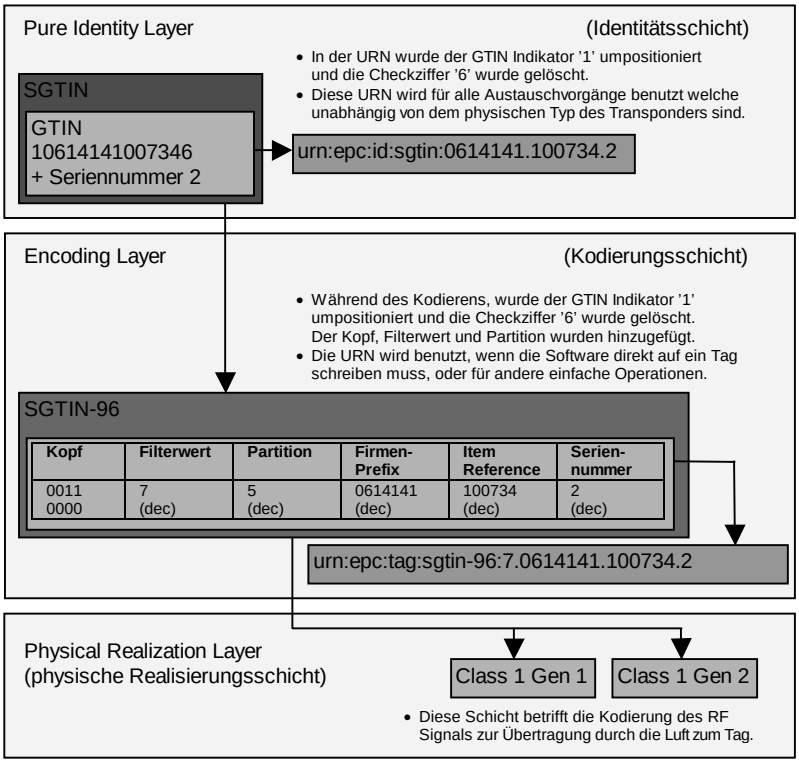

Abbildung 12: Beispiel für eine bestimmte Art der Kodierung [EPCGtag]

3.1.3 Das Auto-ID-Protokoll für Lesegeräte

Das Auto-ID-Protokoll für Lesegeräte 1.0 (Auto-ID Reader Protocol 1.0) [EPCGread], welches zurzeit erst als „Working Draft" vorliegt, spezifiziert die Schnittstelle zwischen einem Lesegerät beziehungsweise Lese/Schreibgerät für Auto-ID-Systeme und einer Applikationssoftware. Diese beiden Teile werden in diesem Zusammenhang oft nur als *Reader* und *Host* bezeichnet. Als Host kann z.B. die Middleware Savant zum Einsatz kommen, dies wird aber durch diese Spezifikation nicht vorgeschrieben. Das Protokoll beschreibt nicht die Art und Weise des Zugriffs auf bestimmte RF-Tags, wie z.B. [EPCGhf1], [EPCGuhf0] oder [EPCGuhf1], welche hier nicht genauer betrach-

tet werden. Das Ziel des Protokolls besteht darin, von der detaillierten Realisierung des Lesegeräts zu abstrahieren, so dass ein einheitlicher Zugriff ermöglicht wird. So ist es z.B. möglich, dass ein Lesegerät mehrere verschiedene Protokolle zum Zugriff auf unterschiedliche RFID-Tags unterstützt oder sogar eine andere Technik, wie z.B. das Einlesen von Barcodes.

In der Version 1.0 wird explizit darauf hingewiesen, dass zurzeit nur ein Framework zur Realisierung dieser Schnittstelle beschrieben ist. Viele Optionen sind im Detail noch nicht beschrieben.

Auch in diesem Protokoll werden 3 Schichten unterschieden:

Abbildung 13: Übersicht der Schichtenarchitektur im Auto-ID-Protokoll für Lesegeräte (Reader) [EPCGread]

- **Reader-Schicht**
  Diese Schicht spezifiziert den Inhalt und das Format der Nachrichten, welche zwischen Reader und Host ausgetauscht werden. Die Schicht ist das Herz des Protokolls für Lesegeräte. Sie definiert die unterstützten Nachrichten und was sie bedeuten.

- **Nachrichtenschicht**
  In dieser Schicht wird definiert wie die Nachrichten für einen bestimmten Netzwerktransport aufgeteilt, verändert und übertragen werden. Darüber hinaus werden falls vorhanden Sicherheitsdienste hinzugefügt. Beispiele hierfür sind Authentisierung, Autorisierung oder die Unterstützung vertraulicher und gegen Veränderungen gesicherter Nachrichten. Die Nachrichtenschicht legt fest, wie eine Kommunikationsverbindung aufgebaut wird, wie eine Synchronisation zur Initialisierung der Sicherheitsdienste gewährleistet wird und auf welche Art und Weise Dienste realisiert sind, die für alle Nachrichten auf gleiche Art und Weise durchgeführt werden, wie z.B. bei einer Verschlüsselung von Nachrichten.

- **Transportschicht**
  Die Transportschicht korrespondiert zu den in Betriebssystemen unterstützten Protokollen und wird auch nur dort definiert.

Das Auto-ID-Protokoll für Lesegeräte sieht mehrere verschiedene Implementierungen der Nachrichtenschicht vor. Jede dieser Implementierungen wird als *Messaging/Transport Binding* (MTB) bezeichnet und unterstützt dabei eine bestimmte Transportart, wie z.B. TCP/IP oder Bluetooth. Jede dieser MTB kann verschiedene Sicherheitsdienste unterstützen, z.B. für den Aufbau einer Verbindung oder für die Beschaffung von Konfigurationsdaten.

Unabhängig davon welche Art MTB benutzt wird, ist jedes Lesegerät zusammen mit höchstens einem Host in einer Session gekapselt. In dieser Spezifikation wird auch noch keine synchrone Übertragung von Nachrichten zwischen mehreren Hosts unterstützt [EPCGread].

3.1.4 Savant

Savant [EPCGsav] ist eine vom Auto-ID Center entwickelte Software, welche als Middleware zwischen den Lesegeräten und den Enterprise-Applikationen sitzt. Sie ist dazu gedacht, die

einheitlichen Verarbeitungsmethoden, welche von EPC-Applikationen angefordert werden, zu realisieren. Dabei soll die Software insbesondere die Datenmengen filtern und bündeln, damit sie dann den entsprechenden Unternehmenssoftwaresystemen zur Verfügung gestellt werden können, ohne diese mit den entstehenden großen Datenmengen zu überlasten.

Die Savant Spezifikation 1.0, von der auch eine Referenzimplementierung existiert, beschreibt die Savant-Software als einen Container für so genannte *processing modules*, die einerseits über eine Schnittstelle auf die verschiedenen Lesegeräte zugreifen können und andererseits auch über eine Schnittstelle mit den verschiedenen Anwendungen, welche die Dienste der Savant-Software in Anspruch nehmen wollen, kommunizieren können. Es ist geplant, dass zukünftige Versionen den Zugriff auf die anderen Systemkomponenten wie z. B. das ONS-System spezifizieren.

Bei den verschiedenen Processing Modules wird zwischen User-Defined- und Standard-Processing-Modulen unterschieden. In der Version 1.0 werden dabei nur zwei Standard Processing Modules vorgeschrieben: *core* und *readerproxy*. Während das core-Modul ein minimales Kommandoset zur Verfügung stellt, um Informationen zur jeweiligen Savant-Instanz abzurufen, wie z.B. die Identifikationsnummer, erlaubt das readerproxy-Modul Anfragen zu den angeschlossenen Lesegeräten und die Ansteuerung dieser Geräte. Als Kommunikationsschnittstelle werden dabei sowohl XML-RPC als auch SOAP-RPC über HTTP unterstützt [flör2004].

Es ist geplant, dass die Savant-Software auch Funktionalitäten enthält, die das einfache Filtern und Bündeln der aggregierten Daten innerhalb einer EPC-Id unterstützten. So sollten beispielsweise Filter spezifiziert werden können, die nur EPCs mit bestimmten Bitmustern weiterleiten. Außerdem sind Filter angedacht, welche die mehrfache Erkennung eines Transponders in einem kurzen Zeitraum zu einem einzigen Eingangsereignis bündeln. Durch eine Verknüpfung solcher Filter sollten die Daten, die von den verschiedenen angeschlossenen Lesegeräten geliefert werden, aufbereitet und in die entsprechenden Ereignisse für die Anwendung umgewandelt werden. So könnten beispielsweise eine Vielzahl von Transpondererkennungen an einem Lesegerät in ein einziges Wareneingangsereignis für eine Lieferung zusammengefasst werden. Es bleibt abzuwarten, ob diese Filterfunktionen in die nächste Version der Savant-Spezifikation aufgenommen werden.

3.1.5 EPC Information Services

Der *EPC Information Service* wurde ursprünglich unter dem Namen *PML Service* (Physikal Markup Language Service) entwickelt. Er soll die EPC-Daten der Transponder zur globalen Weiterverarbeitung mit Hilfe der PML verfügbar machen [EPCGsav]. Die Daten werden im Hinblick auf eine spätere Objektverfolgung mit der Historie entsprechender Transpondererkennungen erweitert (Track&Trace). Außerdem sollen instanzenbezogene Daten von allgemeinem Interesse wie z.B. Herstellungs- und Mindesthaltbarkeitsdatum verfügbar gemacht werden. Der EPC Information Service soll dabei nicht nur auf selbst erfasste Daten zurückgreifen können, sondern auch Informationen aus anderen Datenquellen anbieten, die unternehmensweit zur Verfügung gestellt werden, wie z.B. Produktkataloge [EPCGsav].

Eine detaillierte Spezifikation des EPC Information Service liegt zurzeit noch nicht vor [flör2004].

3.1.6 Physical Markup Language (PML)

Das Ziel bei der Entwicklung der XML-basierten Auszeichnungssprache PML [EPCGpml] war es, eine Menge von gemeinsamen, standardisierten Vokabularien zu definieren, um auf das EPC-Netzwerk bezogene Informationen zu repräsentieren und zu verteilen. Es sollen z.B. Überwachungen von Sensoren (z.B. von RFID-Lesegeräten), Konfigurationsbeschreibungen oder e-Commerce-Dokumente welche EPC-Daten enthalten, unterstützt werden (vgl. Abb. 14).

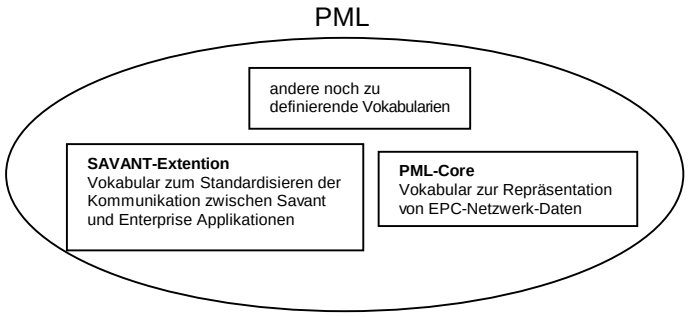

Abbildung 14: PML ist eine Menge von gemeinsamen standardisierten Vokabularien [EPCGsav]

Da sich die Entwicklung einer anwendungsunabhängigen Beschreibungssprache, die aber trotzdem den Anforderungen verschiedener Anwendungsgebiete gerecht wird, als schwierig herausstellte, wurde zunächst unter dem Namen *PML Core* ein Vokabular entwickelt, das den Austausch von Daten, die von den Lesegeräten und anderen Sensoren im EPC-Netzwerk geliefert werden, standardisiert. Die in Abbildung 14 als Beispiel aufgeführte SAVANT-Extention ist ebenfalls noch in der Planung und nicht komplett spezifiziert.

Beispiel 1 zeigt eine PML-Core-XML-Datei, welche die Informationen eines Lesevorgangs eines Sensors, der 2 Transponder ausgelesen hat, enthält.

```
<pmlcore: Sensor>
        <pmluid:ID>urn:epc:1:4.16.36</pmluid:ID>
        <pmlcore:Observation>
                <pmlcore:DateTime>2002-11-06T13:04:34-06:00</pmlcore:DateTime>
                <pmlcore:Tag>
                        <pmluid:ID>urn:epc:1:2.24.400</pmluid:ID>
                </pmlcore:Tag>
                <pmlcore:Tag>
                        <pmluid:ID>urn:epc:1:2.24.401</pmluid:ID>
                </pmlcore:Tag>
        </pmlcore:Observation>
</pmlcore:Sensor>
```

Beispiel 1: PML-Core-Datei

3.1.7 Object Name Service (ONS)

Um Datenquellen mit weiteren Informationen zu der EPC-Identifikationsnummer im Internet zu finden, ist es notwendig, einen Lookup-Mechanismus anzubieten, indem diese registriert und so auffindbar sind. Im EPC-Netzwerk wird diese Lookup-Funktion vom *Object Naming Service* (ONS) bereitgestellt. Unter Angabe eines EPC liefert der ONS eine oder mehrere Internetadressen (URLs) zurück. Diese Internetadressen können dabei auf einen EPC Information Service oder auch auf anderen Datenquellen wie zum Beispiel eine einfache Web-Seite im HTML-Format zeigen. Das ONS-System basiert auf dem Domain Name Service (DNS). Aus diesem Grund werden bei Anfragen an den ONS die EPC-Daten auch erst in gültige Domänennamen umgewandelt, bevor sie als DNS-Anfrage weitergeleitet werden. Die Antwort des DNS ist dann dementsprechend ein gültiger DNS Resource Record. Ein typischer Anfrageablauf könnte folgendermaßen aussehen [EPCGons]:

1. Eine Bit-Sequenz, die einen EPC beinhaltet, wird vom Transponder durch das Lesegerät gelesen.

2. Das Lesegerät sendet diese Sequenz an einen lokalen Server, der sie in das EPC-URI-Format umwandelt und zur ONS-Auflösungsinstanz schickt.

3. Die ONS-Auflösungsinstanz übersetzt den URI in einen DNS Namen, schickt eine DNS Anfrage ab und erhält einen DNS Resource Record als Antwort, in der die zugehörigen Internetadressen enthalten sind.

Die Version 1.0 der ONS-Spezifikation [EPCGons] erlaubt keine Anfragen für einzelne EPCs, sondern nur für um die Seriennummer verkürzte EPCs. Anfragen zu Informationen für einen einzelnen EPC sollen von den jeweiligen Applikationsservern aufgelöst werden, die nach Angabe des um die Seriennummer verkürzten EPC vom ONS System aufgelistet werden. Eine Anfrage, die auch die Seriennummer beinhaltet, soll in zukünftigen Versionen der Spezifikation ermöglicht werden, sobald die Architektur- und Skalierungsfragen, die sich aus der erheblichen Größe des Adressraumes ergeben, geklärt sind. Abschließend wäre noch zu betonen, dass es sich bei dem ONS-System um einen reinen Lookup-Service handelt, dessen Aufgabe darin besteht, die Internetadresse einer Datenquelle anzugeben. Die Funktion eines globalen Track&Trace-Systems beispielsweise, das die Positionsbestimmung über Länder- und Unternehmensgrenzen möglich machen würde, kann das ONS-System daher nicht selbst erfüllen [flör2004].

3.2 EPC-Netzwerk-Architektur von Sun

Im Februar 2004 [SUNtw] stellte die Firma *Sun* erstmals ihre Konzepte zur Realisierung der EPC-Netzwerk-Architektur vor. Im Kern basiert die Architektur auf dem *Sun EPC Event Manager* und dem *Sun EPC Information Server* (siehe Abb. 15).

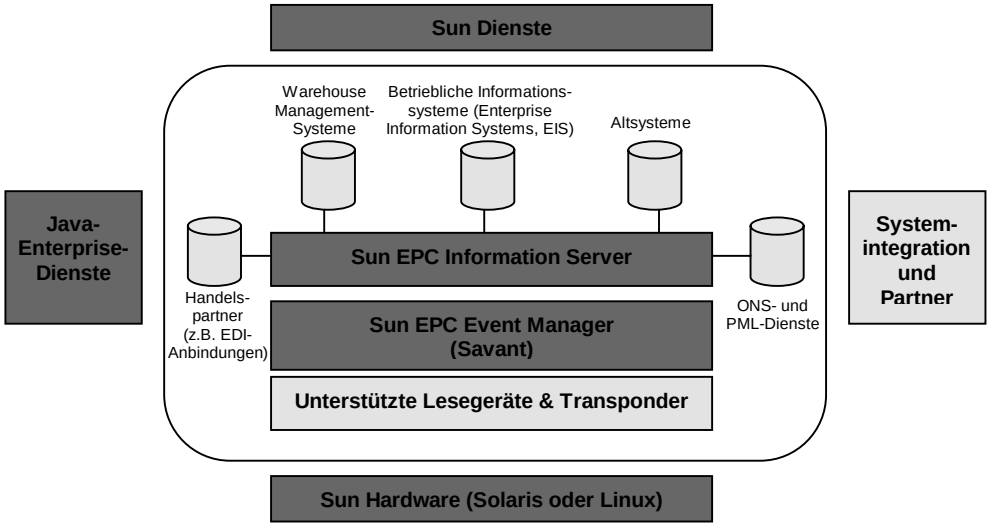

Abbildung 15: Sun-EPC-Netzwerk-Architektur [SunTw04]

Wie auch in Kapitel 3.1.1. gezeigt basiert die Architektur auf so genannten *EPC-compliant* Transpondern und Lesegeräten, welche den EPC-Standard unterstützen. Hier kommen vor allem die bereits im EPC-Standard spezifizierten 13.56 MHz ISM Band Class-1-RFID-Tags [EPCGhf1], 900 MHz Class-0-RFID-Tags [EPCGuhf1] und 860MHz–930MHz Class-1-RFID-Tags [EPCGuhf1] zum Einsatz. Die verwendeten Lesegeräte müssen die Befehlsschnittstelle der Savant Middleware unterstützen.

Der Sun EPC Event Manager ist eine Umsetzung der Savant Middleware mittels J2EE (Java 2 Enterprise Edition). Die von einem Transponder ausgelesenen Daten werden hierbei oft als EPC-Events bezeichnet, weil durch das Eintreffen neuer EPC-Datenströme weitere Prozesse angestoßen werden. Sun spricht im Durchschnitt von 200 ausgelesenen Tags pro Sekunde [SUNtw] für jedes angeschlossene Lesegerät. Der von Sun entwickelte EPC Event Manager verfügt insbesondere über Filter- und Aggregatsfunktionen, um die in EPC-Daten kodierte Information geeignet aufbereitet an Applikationen weiterzuleiten (vgl. auch Kapitel 3.1.1., Filterwert). Aggregatsfunktio-

nalität wird benötigt, um z.B. Daten von Tags, welche ohne bewegt zu werden längere Zeit im HF-Feld eines Lesegerätes verbleiben, nicht mehrfach an eine Applikation zu melden. Entsprechend dem in Kapitel 3.1.1. vorgestellten Konzept, können auch vom Sun EPC Event Manager mehrere Instanzen gebildet werden, um geographisch zusammen liegende Lesegeräte mit gleichen Aufgaben, wie z.B. in Verkaufsräumen, in der Warenannahme oder der Warenausgabe, getrennt voneinander zu behandeln.

Auf der dritten Schicht über dem Sun EPC Event Manager befindet sich der Sun EPC Information Server. Sun tritt dafür ein, dass auf dieser Ebene Integrationstechniken benutzt werden, um die EPC-Event-Manager-Schicht mit betrieblichen Informationssystemen (Enterprise Information Systems, EIS), wie z.B. Altsysteme, ERP-Systeme (Enterprise Resource Planning Systems), WMS-Systeme (Warehouse Managment Systems), SCM-Systeme (Supply Chain Management Systems), CRM-Systeme (Customer Relationship Management Systeme) oder andere Systeme welche EPC-Tag-Informationen benötigen, zu verbinden [SUNtw]. Dies umfasst auch die Verwendung von Komponenten und Techniken welche bereits im *Java Enterprise System* enthalten sind, wie z.B. Web-, Kommunikation-, Applikations- und Sicherheitsdienste oder Java-Technologien wie das *Java Messaging System* (JMS) oder die *J2EE Connector Architecture* (CA) zur Anbindung betrieblicher Informationssysteme. Um Daten und Dienste für andere Partner zur Verfügung zu stellen, ist es möglich, basierend auf der *Sun Java System Application Server Platform* spezielle Webdienste, z.B. *Session Beans* oder *Servlets,* zu entwickeln. Ebenso ist es notwendig, Daten von anderen Anbietern in das eigene System zu integrieren. In Anlehnung an die von Auto-ID-Center vorgestellte Architektur ist es geplant EPC Information Server (IS) einzusetzen, welche Produktdaten mittels PML zugänglich machen und verbreiten. Hierfür setzt Sun auf die schon bewährten Dienste aus ihrer J2EE Framework Architektur.

Um die von Sun vorgestellten Konzepte zu testen, wurde das *Sun RFID Test Center* in Dallas (Texas) ins Leben gerufen [SUNtc]. Sun ermöglicht es dort Firmen, die neue Technologie zu testen und Anwendungen zu entwickeln. Eine Firma, die dies dort bereits getan hat, ist Goodyear [SUNtcVi]. Als Hardwarehersteller für Transponder und Lesegeräte wird Sun vor allem durch die Firma Texas Instruments unterstützt [SUNtcVi].

Im Nachfolgenden werden die Vorstellungen von Sun bezüglich des Sun EPC Event Managers und des Sun EPC Information Servers noch näher vorgestellt.

3.2.1 Sun EPC Event Manager

Die Realisierung des Sun EPC Event Managers basiert auf der Version 1.0 der Savant-Spezifikation. Sun hält sich an diese und stellt darüber hinaus Funktionalitäten bereit, welche speziell für die Unterstützung und Anbindung großer betriebswirtschaftlicher Anwendungen entwickelt wurden [SUNTw]. Da in Kapitel 3.1.1. schon die standardisierte Funktionalität der Savant Middleware eingegangen wurde, wird hier nur noch die zusätzliche Funktionalität vorgestellt.

Der Sun EPC Event Manager wurde mit dem Ziel entwickelt, flexible Entwicklungsmöglichkeiten zu garantieren, ohne Erreichbarkeit, Erweiterbarkeit oder Benutzbarkeit einzubüßen [SUNtw]. Sun will dies durch eine verteilte Architektur erreichen. Ein Grundsatz für verteilte Systeme ist, dass sie anpassungsfähig an sich ändernde Bedingungen in einem Netzwerk reagieren können. Netzwerkkomponenten und Dienste wie z.B. Webserver oder andere Mailserver können Fehler produzieren oder ausfallen. Manchmal werden auch neue Komponenten beziehungsweise Dienste in das Netzwerk eingebracht. Sind die Komponenten nicht redundant und verteilt ausgelegt, kann es im Fehlerfall zum Stillstand eines ganzen Systems kommen. Aus diesen Gründen wurde der Sun EPC Event Manager als föderierte Dienstarchitektur entwickelt, welche flexibel auf Ereignisse und Störungen reagiert, z.B. auf Ausfälle von Lesegeräten oder einzelnen Servern.

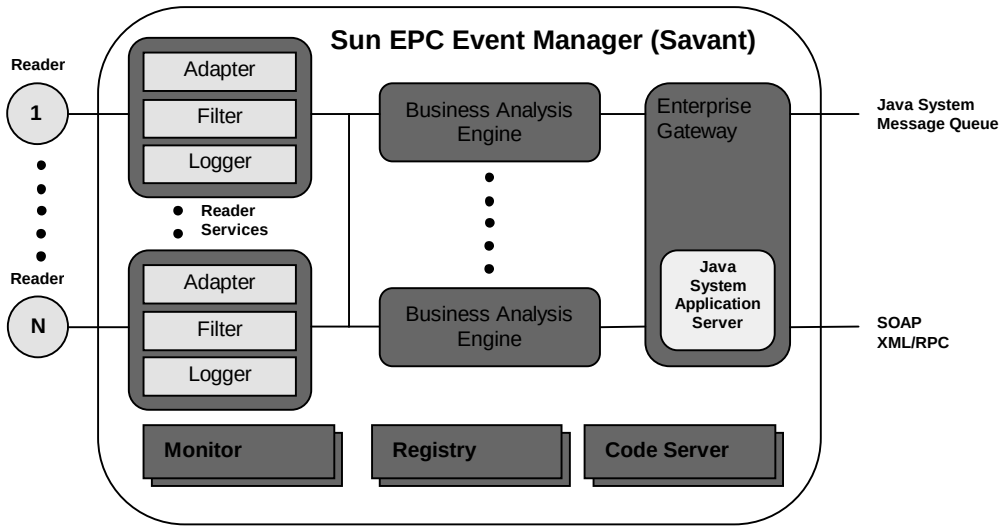

Abbildung 16: Die Sun-EPC-Event-Manager-Architektur [SUNtw].

Jedes Lesegerät wird über einen *Reader Service* angeschlossen. Die Daten, welche diese einsammeln werden an ein Netzwerk aus *Business Analysis Engines* weitergeleitet, welches z.B. als Lastverbund realisiert sein kann. Auf diese Weise ist es möglich, Ausfälle zu tolerieren und zusätzliche Komponenten leicht hinzuzufügen. Das *Enterprise Gateway* stellt eine einheitliche Schnittstelle bereit, über die Applikationen Informationen zu Event-Daten abrufen können [SUNtw].

Die Reader Dienste bestehen aus einem *Device Adapter*, *Filtern* und *Loggern*. Device Adapter annektieren verschiedene Geräte wie z.B. RFID-Lesegeräte oder Barcodeleser. Filter helfen beim Entziffern der nützlichen Daten aus den verschiedenen kodierten Informationen eines EPC-Tags. Filter können auch kleine Teile von Prozess- oder Geschäftslogik enthalten. Für gewisse Aufgaben gibt es Standardfilter, wie z.B. für *event smoothing* (z.B. das Aggregieren mehrerer aufeinander folgender gleicher Events zu einem). Logger sind dafür geeignet, externe Systeme über RFID- oder non-RFID-Event-Daten zu benachrichtigen. Der Sun EPC Event Manager unterstützt das Logging in Dateien, in eine JMS-Queue oder durch XML-, http- oder SOAP-Nachrichten [SUNtw].

3.2.2 Sun EPC Information Server

Der Sun EPC Information Server sammelt die vom Sun EPC Event Manager generierten Daten und macht sie für andere Applikationen konsistent und einheitlich zugreifbar. Das Konzept von Sun sieht vor, dass auf dieser Ebene eine Anpassung und Integration für im Betrieb schon vorhandene Systeme stattfindet. Sun bietet drei Arten der Anbindung dieser Systeme an [SUNtw]:

- J2EE Connector Architecture
- Java Messaging Service
- native Unterstützung für Web Services

4 Sicherheit und Datenschutz

Mit dem Einsatz von RFID-Technik ist eine Vielzahl von datenschutzrechtlichen und sicherheitsbezogenen Bedenken verbunden. Durch die kontaktlose Kommunikation zwischen RFID-Tags und Lesegeräten besteht die Möglichkeit, dass unberechtigte Personen Informationen lesen, weiterverarbeiten oder sogar manipulieren. Darüber hinaus ist es möglich, RFID-Systeme durch in das System unberechtigterweise eingebrachte Tags zu manipulieren. Angriffe auf Lesegeräte oder sogar Applikationen durch solche Transponder könnten durch Ausnutzen von Sicherheitslücken,

wie Buffer-Overflows, ähnliche Wirkungen hervorrufen wie solche, die von Computerviren ausgehen. Große Bedenken von Seiten der Datenschützer bestehen auch im Bezug darauf, dass durch die globale Verflechtung von Informationen (wie z.B. bei EPC-Tags) Firmen und andere Nutzer in der Lage sind, Querbezüge zwischen diesen Daten zu generieren, welche im Rahmen der Bundesdatenschutzgesetze nicht zulässig sind. Die aufgezeigten Gefahrenpunkte zeigen, dass die Anforderungen an die Sicherheit der eingesetzten Systeme sehr hoch sind. Datenschützer und die Gegner der RFID-Technologie fordern neue Gesetze und Regeln für den Einsatz der Technologie. Ein großes Problem ist hierbei, wie auf vielen anderen Gebieten auch, die uneinheitliche Gesetzgebung in den verschiedenen Ländern. Im Folgenden werden einige wichtige Forderungen in Bezug auf Sicherheit und Datenschutz aufgeführt und kritisch hinterfragt.

Eine große Forderung besteht darin, gewisse Anwendungen ganz und gar zu verbieten. Dies umfasst z.B. das Verfolgen von Personen, Verringerung oder Verhinderung von Anonymität oder das Anbringen von RFID-Tags an Münzen oder Geldscheinen [GIrfid]. Es ist sicher ein Problem, zu zeigen, wann bei einer Verringerung von Anonymität die Grenze überschritten wird. Hier ist der Gesetzgeber in der Pflicht, entsprechende Gesetze zu erlassen bzw. die Folgen durch den globalen Einsatz der Technologie richtig einzuschätzen.

Eine weitere Forderung ist es, die verwendeten RFID-Tags und Lesegeräte sowie einzelne Lesevorgänge so zu markieren, dass eine absolute Transparenz der Handelsunternehmen gewährleistet ist. Des Weiteren soll beim Kauf eines Gutes der Anspruch bestehen, das RFID-Tag durch den Verkäufer entfernen oder zerstören zu lassen, ohne dass für den Käufer ein Nachteil entsteht. Generell wird darauf hingewiesen, dass nur sehr wenige Daten auf den Transponder aufgebracht werden sollen. Dies soll die Gefahr mindern, dass sich auf einem Transponder befindliche Daten zu einem späteren Zeitpunkt mit einer Person in Verbindung bringen lassen. Die global eindeutigen Identifikationen und die Möglichkeit, nachträglich Daten über das Internet abzufragen, hebeln diese Forderung allerdings teilweise aus.

5 Einsatzgebiete und Anwendungsbeispiele

Die Einsatzgebiete der RFID-Technologie sind sehr zahlreich. Eines der größten Anwendungsgebiete ist der Einsatz in kontaktlosen Chipkarten. Diese werden bisher vor allem im öffentlichen Nahverkehr (ÖPNV) verwendet. Im Bereich der Logistik ist die Firma *WalMart* einer der wichtigsten Vorreiter beim Einsatz der RFID-Technologie. Sie verwendet die zuvor vorgestellte EPC-Netzwerk-Architektur. Andere Anwendungsbereiche, in denen die RFID-Technologie bereits eingesetzt wird, sind z.B. die Zugriffs- beziehungsweise Zutrittskontrolle, der Einsatz in Verkehrssystemen, der Einsatz zur Tieridentifikation, zur Realisierung elektronischer Wegfahrsperren, zur Unterstützung bei der Abfallentsorgung, zur Positionsermittlung bei sportlichen Veranstaltungen, der Einsatz zur Industrieautomation oder in medizinischen Anwendungen. Im Folgenden werden die Pläne und Umsetzungen des Metro-Konzerns, der ebenfalls den Einsatz von RFID-Technologie befürwortet, näher betrachtet.

5.1 Der Metro Future Store

Seit April 2003 testet die METRO Group in ihrem Future Store in Rheinberg bei Duisburg, gemeinsam mit Partnern der Future-Store-Initiative neue Technologien im Handel. Unterstützt wird sie dabei vor allem durch SAP, Intel und IBM sowie weitere Partnerunternehmen aus den Bereichen Informationstechnologie und Konsumgüterindustrie.

Momentan testet die METRO Group den Einsatz der RFID-Technologie vorrangig im Lagermanagement des Future Stores.

Insgesamt wird RFID dort in folgenden Bereichen eingesetzt [MGfs]:

- **Warenanlieferung im Markt:**
  Mit Hilfe von RFID wird kontrolliert, ob die eintreffenden Lieferungen mit der Bestellung übereinstimmen.

- **Lagermanagement:**
  Im Warenflusssystem ist genau vermerkt, welche Produkte sich im Lager befinden.

- **Transport der Waren in den Verkaufsraum:**
  Das Warenflusssystem identifiziert dank RFID die Produkte als "in den Markt verräumt".

- **Intelligente Regale im Markt:**
  Einige Produkte im Future Store sind bereits mit Smart Chips versehen. In den Regalen von „Philadelphia"-Frischkäse, „Pantene"-Shampoo und „Mach 3 Turbo"-Rasierklingen befinden sich Lesegeräte, die dem Personal des Future Stores melden, wenn Ware einsortiert werden muss.

- **Tags auf CDs, DVDs und Videos:**
  RFID ermöglicht das Ansehen von Trailern zu einzelnen Filmen sowie das Anhören von Musik-CDs.

- **De-Activator:**
  Nach dem Bezahlvorgang kann der Kunde die auf dem Smart Chip gespeicherten Informationen überschreiben und somit den Chip deaktivieren.

Über das Lagermanagement hinaus wird die RFID-Technologie auch zur Verbesserung des Informationsmanagements eingesetzt. Der persönliche Einkaufsberater, Info-Terminals und Werbedisplays helfen Kunden bei der Suche nach Produkten und beraten durch umfassende Informationen bei der Auswahl der Waren. Die Informationssysteme gestalten zudem die Arbeitsprozesse effizienter. Beispielsweise erkennt das Personal schneller, wenn die Produkte in den Regalen zur Neige gehen.

Im Bereich des Kassiervorganges kann der Kunde die Produkte mit dem persönlichen Einkaufsberater scannen oder die Selbstzahlerkasse benutzen. Die Wartezeiten an den Kassen und der Arbeitsaufwand für das Personal reduzieren sich dadurch deutlich. Wer diese neuen Technologien nicht nutzen möchte, kann seine Waren im Future Store aber auch wie in jedem anderen Supermarkt an der Kasse bezahlen.

Die durch den Einsatz von RFID im Future Store in Rheinberg bisher gesammelten Erfahrungen zeigen, dass diese Zukunftstechnologie große Vorteile für den Handel und seine Kunden bietet. Daher wird der Einsatz von RFID entlang der gesamten Prozesskette in den kommenden Jahren systematisch weiter ausgeweitet. In diesen Prozess werden die Lieferanten und Partner der METRO Group miteinbezogen. Nur durch eine partnerschaftliche Kooperation ist RFID als Zukunftstechnologie für Handel und Industrie zu verwirklichen.

Die METRO Group möchte langfristiges Vertrauen in die RFID-Technologie schaffen und weltweit gültige Standards für RFID festlegen. Deshalb arbeitet sie auf internationaler Ebene in der Initiative EPCGlobal mit anderen Unternehmen aus der IT- und Konsumgüterindustrie sowie anderen Handelsunternehmen zusammen.

Die METRO Group informiert ihre Kunden offen und transparent über den Einsatz der RFID-Technologie: Überall dort, wo RFID im Future Store eingesetzt wird, ist dies gekennzeichnet.

Darüber hinaus klären Informationsmaterial und ein Info-Terminal den Kunden umfangreich über das Thema RFID auf.

RFID Net

Künftig wird die METRO Group die RFID-Technologie entlang der gesamten Prozesskette einsetzen. Mit einem ausgewählten Kreis von Partnern startet dieses Projekt ab November 2004. Die weiteren Schritte wurden am 14. Mai 2004 auf dem Fachkongress RFID im Kongresszentrum West der Kölnmesse vorgestellt. Dort berichteten die Vertriebslinien Kaufhof, Metro Cash & Carry, Real und Extra von ihren ersten Erfahrungen mit RFID und präsentierten ihren Fahrplan für die Zukunft. Außerdem erläuterten ausgewählte Partner aus der IT-Branche und der Konsumgüterindustrie die technischen Anforderungen und beantworteten Fragen zum Einsatz von RFID in den Unternehmen [MGfs].

RFID Innovation Centers

Mit der Eröffnung des RFID Innovation Centers am 7. Juli 2004 in Neuss-Norf legt die METRO Group einen weiteren Grundstein. Ziel des Innovation Centers ist es den geplanten Rollout der RFID-Technologie innerhalb des Unternehmens mit den Partnern der METRO Group intensiv vorzubereiten. Darüber hinaus sollen im Innovation Center innovative RFID Anwendungen gezeigt werden, die das Einkaufen der Zukunft erleichtern [MGic].

6 Ausblick

Die RFID-Technologie als solche ist nicht neu. Aber sie erfährt in den letzten Jahren, unterstützt durch die Entwicklung von neuen Internettechnologien (XML, Web-Services) und den damit verbundenen Möglichkeiten eine überproportional wachsende Nutzung durch Industrie und Handel. Die in den aktuellen Fassungen noch nicht endgültigen Standards für eine globale Kommunikationsarchitektur haben allerdings einen Entwicklungsstand erreicht, der den weltweiten Einsatz der Technik ermöglicht. Aus diesem Grund ist zu erwarten, dass die Einrichtung und Inbetriebnahme neuer RFID-Systeme in allen Bereichen des Handels stark voranschreitet. Nicht ohne Grund warnen Datenschützer vor den Gefahren für die Privatsphäre der Verbraucher. In Deutschland setzt sich unter anderem die Gesellschaft der Informatik dafür ein, dass diese Problematik nicht übersehen wird. Doch auch eine Berücksichtigung durch entsprechende Gesetze kann den Missbrauch der Technologie nicht völlig ausschließen.

Quellenangaben

[fink2002] Klaus Finkenzeller, *RFID-Handbuch*, 3. Auflage, 2002, Hanser Verlag

[flör2004] Christian Flörkemeyer, *Die Technologiestandards des Auto-ID Centers*, 2004, Institut für Pervasive Computing, ETH Zürich

[EPCG] EPCGlobal, http://www.epcglobalinc.org

[EPCGtag] EPCGlobal, *EPC Tag Data Standards Version 1.1 Rev.1.24*, Standard Specification, 1. April 2004, http://www.epcglobalinc.org/standards_technology/EPCTagDataSpecification11rev124.pdf

[EPCGread] EPCGlobal, *Auto-ID Reader Protocol 1.0*, Working Draft Version of 5. September 2003, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/WD-reader-protocol-200309051.doc

[EPCGsav] EPCGlobal, *Auto-ID Savant Specification 1.0*, Version of 1 September 2003, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/WD-savant-1_0-20030911.doc

[EPCGpml] EPCGlobal, *PML Core Specification 1.0*, Auto-ID Center Recommendation 15. September 2003, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/PML_Core_Specification_v1.0.pdf

[EPCGons] EPCGlobal, *Auto-ID Object Name Service (ONS) 1.0*, Auto-ID Center Working Draft, 12. August 2003, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/WD-ons-1.0-20030930.pdf

[EPCGhf1] EPCGlobal, *13.56 MHz ISM Band Class 1Radio Frequency Identification Tag Interface Specification*, Auto-ID Center Candidate Recommendation, Version 1.0.0, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf

[EPCGuhf0] EPCGlobal, *Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag*, 23. Februar 2003, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

[EPCGuhf1] EPCGlobal, *860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification*, Auto-ID Center Candidate Recommendation, Version 1.0.1, http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

[SUNtw] Sun Microsystems, *The Sun EPC Network Architecture*, A Technical White Paper, Februar 2004, http://wwws.sun.com/software/solutions/rfid/EPCNetArch_wp021304a.pdf

[SUNsoft] Sun Microsystems, *Sun Java System RFID Software*, http://wwws.sun.com/software/solutions/rfid/ds/rfid_ds.pdf

[SUNtc] Sun Microsystems, *The Sun RFID Test Center*, http://wwws.sun.com/software/solutions/rfid/ds/RFIDTestCtr.pdf

[SUNtcVi] *Video of Sun's Dallas RFID Test Center* http://webcast-east.sun.com/archives/GSN-1665/GSN-1665_01_096.rm

[wikirfid] Wikipedia, http://de.wikipedia.org/wiki/rfid

[MGfs] Metro Group Future Store, http://www.future-store.org

[MGic] Metro Group Innovation Center, http://www.innovation-center.metrogroup.de

[EANat] European Adoption Program, http://www.ean.co.at/eep/html/eap.html

[GIrfid] Gesellschaft für Informatik, *Hintergrundinformationen der Gesellschaft für Informatik e.V. (GI) zu RFID*, http://www.gi-ev.de/download/RFID-GI040608.pdf