



# Management-Leitfaden für den Einsatz von RFID-Systemen



herausgegeben vom VDEB  
in Zusammenarbeit mit AIM Deutschland

Management-Leitfaden für den Einsatz von RFID-Systemen, herausgegeben von der RFID-Fachgruppe des Verband der EDV-Software- und -Beratungsunternehmen e.V. (VDEB) in Zusammenarbeit mit dem Industrieverband für Automatische Identifikation, Datenerfassung und Mobile Datenkommunikation (AIM Deutschland).

Version 1.07, Stand Dezember 2006

## Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Eigenschaften der Frequenzbereiche</b>	<b>4</b>
2.1	Überblick und grundsätzliche Aspekte	4
2.2	Gerichtete Ausbreitung	5
2.3	Übertragungsraten	5
2.4	Reflexionen und Interferenzen	5
2.5	Wirbelstromverluste in leitenden Flächen	5
2.6	Absorption bei Nichtleitern	5
2.7	Interferenzen vermeiden	6
<b>3</b>	<b>Die Parameter der Frequenzbereiche im Einzelnen</b>	<b>7</b>
3.1	LF-Bereich (119...148,5 kHz)	7
3.2	HF-Bereich (13,56 MHz)	7
3.3	UHF-Bereich	8
3.4	GHz-Bereich (2,4...2,5 GHz)	9
<b>4</b>	<b>Standards</b>	<b>10</b>
4.1	Luftschnittstellenstandards	10
4.2	Standards zum Datenmanagement	11
4.3	Kontaktlose Chipkarten	12
4.4	Testmethoden	12
4.5	Funkvorschriften	13
4.6	Einsatzempfehlungen	14
4.7	Anwendungsstandards	14
4.8	Spezifikationen zum EPC-Netzwerk	16
<b>5</b>	<b>Technik</b>	<b>17</b>
5.1	Transponder	17
5.2	Speichertypen	17
5.2.1	Read-Only-Transponder	17
5.2.2	Schreib-/Lese-Transponder	17
5.2.3	Speicherkapazität	17
5.3	Schreib-/Lesegeräte, Antennen und mobile Terminals	18

<b>6</b>	<b>Physikalische Aspekte</b>	<b>19</b>
6.1	Auslegung von bewegten Systemen	19
6.2	Lesereichweiten in der Praxis	19
6.3	Umgebungsparameter	20
<b>7</b>	<b>Eigenschaften einer RFID-Middleware und Kriterien für die Architektur und die Implementierung</b>	<b>21</b>
7.1	Beschreibung	21
7.2	Definition	22
7.3	Herausforderung Datenmanagement	23
7.4	Architekturprinzipien	23
7.5	Komponenten	24
7.5.1	Allgemeines	24
7.5.2	Event Engine	24
7.5.3	Event Datenbank	25
7.5.4	Event Server	25
7.5.5	Event Cache	25
7.5.6	Reporting	25
7.6	Kriterien	25
7.7	Fallbeispiele	26
<b>8</b>	<b>Datenschutz</b>	<b>28</b>
8.1	Allgemein	28
8.2	Datenschutz-Kriterienkatalog	29
8.2.1	Personenbezogene Daten werden verarbeitet	29
8.2.2	Einsatz von RFID-Tags	29
8.2.3	Einschaltung des betrieblichen Datenschutzbeauftragten	30
<b>9</b>	<b>Ein Blick in die Kristallkugel</b>	<b>31</b>
<b>10</b>	<b>Zusammenfassung</b>	<b>33</b>
<b>11</b>	<b>Literatur</b>	<b>34</b>

**Anlage 1: Kriterien für die RFID-Hardware (Physik und Technik)**

**Anlage 2: Kriterien für eine RFID-Middleware**

**Anlage 3: Implementierte Lösungen**

**Profil VDEB**

**Profil AIM**

## 1 Einführung

Obwohl die öffentliche Aufmerksamkeit für RFID durch verschiedene Pilotprojekte der multinationalen Handelskonzerne, wie Metro und Walmart, relativ neu ist, kann RFID als Identifikationstechnologie auf mehr als 20 Jahre Existenz zurückblicken. Anwendungen wie Tieridentifikation, Wegfahrsperre, berührungslose Zutrittskontrolle für Skilifte, Identifikation von Müllbehältern basieren seit vielen Jahren auf einem Transponder in einer Verpackung aus Glas, Epoxy oder PVC.

Das Verpacken des Transponders als Papierlabel und die damit verbundenen Möglichkeiten zur Massenfertigung sowie die Einführung von neuen passiven Tags mit der Frequenz 868 MHz mit einer größeren Reichweite lassen viele Unternehmen und Marketingspezialisten von einem Einsatz entlang der gesamten globalen Wertschöpfungskette träumen. Wenn diese „Chips“ dann auch bald weniger als einen Cent kosten sollen, gibt es kein Halten mehr und wir können uns endlich vom Barcode verabschieden. Beim Verlassen des Supermarktes wird uns von einem freundlichen Mitarbeiter unser Einkaufsbeleg ausgehändigt und wir können jederzeit im Internet nachschauen, wann und wo die gekaufte Ketchupflasche produziert wurde.



Innovation wird auch durch Träume vorangetrieben, trotzdem brauchen wir in der ganzen Diskussion um das Thema RFID ein Stück Realismus: Faraday lässt grüßen und Smart Labels (HF) von 2 cm Länge, die auf eine Verpackung Frischkäse passen, erzielen keine Lesereichweite von 1 Meter. Ohne Zweifel aber bieten RFID-Systeme wirtschaftliche Lösungen im Bereich des hochwertigen inner- und außerbetrieblichen Materialflusses. Hier liegen bereits viele Chancen für Unternehmen diese Technologie einzusetzen, und damit sollte man eher heute als morgen anfangen. Die Technik ist reif wie die vielen tausend implementierten Anwendungen Tag für Tag belegen. Dieses Papier möchte Sie dabei begleiten, sich mit RFID vertrauter zu machen.

## 2 Eigenschaften der Frequenzbereiche

Von Dipl.-Ing. Erwin Schmidt, Pepperl und Fuchs GmbH

### 2.1 Überblick und grundsätzliche Aspekte

Für RFID-Systeme sind nur bestimmte Frequenzbereiche zugänglich, die von internationalen und nationalen Institutionen dafür freigegeben werden. Diese Freigaben legen nicht nur die Frequenzen fest, sondern auch die zulässigen Bandbreiten, Sendeleistungen, Sendedauern, Modulationsverfahren und Arbeitsweisen der Schreib-/Lesegeräte. Für länderübergreifende Anwendungen sind natürlich weltweite Zulassungen wünschenswert, was aber leider nicht für alle Frequenzbereiche gegeben ist.

Unterschiedliche Frequenzen haben unterschiedliche Ausbreitungseigenschaften. Die zulässigen Bandbreiten und Sendeleistungen sind ebenfalls für die Systemeigenschaften relevant. Ein wesentliches Kriterium für die Arbeitsweise der Kommunikation ist die Unterscheidung von Nah- und Fernfeld. Im Nahfeld hat sich die elektromagnetische Welle noch nicht von der Antenne gelöst. Dadurch kann eine Feldschwächung direkt an der Sendeantenne detektiert werden. Im Fernfeld gibt es keine detektierbare Rückwirkungen auf die Sendeantenne mehr. Die Grenze zwischen Nah- und Fernfeld ist von der Wellenlänge abhängig und liegt bei  $\lambda/2\pi$ . Damit ergeben sich die folgenden Werte:

Frequenz	Wellenlänge	Grenze zwischen Nah- und Fernfeld
125 kHz	2400,00 m	382,00 m
13,56 MHz	22,00 m	3,50 m
868 MHz	0,35 m	0,06 m
2,45 GHz	0,12 m	0,02 m

Im LF-Bereich (125 kHz, 134,2 kHz) und im HF-Bereich (13,56 MHz) arbeitet man im Nahfeld mit einer induktiven Kopplung. Die Belastungsmodulation durch den Transponder kann an der Readerantenne ausgewertet werden. Die damit erreichbaren typischen Reichweiten liegen im Bereich von 0...1 m. Im UHF-Bereich (z. B. 868 MHz) und im Mikrowellen-Bereich (2,4...2,5 GHz) ist das Nahfeld so klein, dass nur über das Fernfeld gearbeitet werden kann. Entweder sendet der Transponder seine Informationen aktiv zurück (z.B. bei den meisten Transpondern im Mikrowellenbereich) oder er arbeitet nach dem sogenannten Backscatter-

Prinzip. Dabei werden die Reflexionseigenschaften der Transponderantenne durch Anpassung und Fehlanpassung verändert und die reflektierte Welle, die zum Reader zurückwandert, verstärkt oder abgeschwächt. Die erzielbaren Reichweiten liegen bei einigen Metern.

## **2.2 Gerichtete Ausbreitung**

Je höher die Frequenz ist, um so besser kann durch geeignete Antennen eine gerichtete Ausbreitung erreicht werden. Mit dieser Fokussierung können im UHF- und GHz-Bereich Lesebereiche gezielter abgedeckt werden.

## **2.3 Übertragungsraten**

Die mögliche Datenübertragungsrate ist mit der Frequenz direkt gekoppelt. Je höher die Frequenz ist, desto schneller können Daten übertragen werden. Insbesondere bei Antikollisionsverfahren (wenn mehrere Transponder gleichzeitig gelesen oder beschrieben werden müssen) ist eine schnelle Datenübertragung wichtig, da ein intensiver Datenaustausch notwendig ist, um die Transponder elektronisch zu vereinzeln. Dazu kommt noch, dass oft sehr viele Transponder gelesen werden sollen. Es ist andererseits aber zu beachten, dass hohe Datenübertragungsraten und eine damit verbundene starke Modulation der Trägerfrequenz entsprechend breite Seitenbänder erzeugt, die die zulässige Bandbreite nicht überschreiten dürfen.

## **2.4 Reflexionen und Interferenzen**

Durch die Überlagerung der gesendeten elektromagnetischen Welle mit reflektierten Wellen kommt es zu Interferenzen, d. h. zu Feldverstärkungen und -auslöschungen. Dieser Effekt macht sich bei höheren Frequenzen verstärkt bemerkbar. Bei UHF und im GHz-Bereich lassen sich solche Nullstellen im Feld praktisch nicht vermeiden, da in einer realen Anwendung immer Reflexionen auftreten. Nur im freien Raum wäre eine nullstellenfreie Ausbreitung der elektromagnetischen Felder denkbar.

## **2.5 Wirbelstromverluste in leitenden Flächen**

Wenn elektromagnetische Wellen auf Metallflächen auftreffen, werden Wirbelströme induziert, d. h. es entstehen Energieverluste an der Metalloberfläche oder allgemeiner an jeder elektrisch leitenden Fläche. Je höher die Frequenz ist, desto höher sind die Wirbelstromverluste. Das ist einer der Gründe, warum man in einer Umgebung mit vielen Metallflächen bevorzugt LF-Systeme einsetzt.

## **2.6 Absorption bei Nichtleitern**

Während bei niedrigen Frequenzen Nichtleiter und schlecht leitende Materialien keinen Einfluss haben, sind bei hohen Frequenzen Absorptionen zu berücksichtigen, die durch Stoffe mit hoher Dielektrizitätskonstante  $\epsilon$  verursacht werden. Besonders im Lebensmittelbereich und bei der Tieridentifikation sind Absorptionen durch Wasser zu berücksichtigen. Deshalb ist für diese Anwendungen der Einsatz von hochfrequenten Systemen stark eingeschränkt.

## 2.7 Interferenzen vermeiden

Es gibt eine Reihe von Maßnahmen, die die oben aufgeführten Nachteile zu vermeiden helfen und auch den Betrieb mehrerer Systeme im selben Frequenzband ermöglichen. Eine manuelle oder automatische Kanalwahl (Frequenzmultiplex) kann eingesetzt werden, wenn die Bandbreite des Frequenzbandes es zulässt. Gegebenenfalls kann ein Schreib-/Lesegerät erkennen, ob auf einem Frequenzkanal bereits gesendet wird und erst dann senden, wenn der Kanal frei ist (Listen-before-talk). Es gibt Verfahren, wie Frequency Hopping Spread Spectrum (FHSS) und Direct Sequence Spread Spectrum (DSSS), die direkt eine größere Bandbreite belegen und damit die Kommunikation sicherer machen, aber andere Systeme stärker stören können.

Neben diesen Frequenzmultiplex-Verfahren kann man auch Reader im Zeitmultiplex betreiben (Duty Cycle), d. h. das Schreib-/Lesegerät ist nur für eine kurze Zeit aktiv und schaltet sich dann wieder ab. Man muss natürlich sicherstellen, dass ein Transponder lange genug im Lesebereich verbleibt.

Neuere Ansätze nutzen sehr breite Frequenzbereiche mit wesentlich verringerter Sendeleistung, die im Bereich der üblichen Rauschpegel liegt. Dazu gehören „Ultra Wide Band“ (nur ca. 3...10 GHz) und der Einsatz von Chirp-Impulsen. Ein Chirp-Impuls ist eine Signalform, die innerhalb einer vorgegebenen Zeit einen bestimmten Frequenzbereich überstreicht ("Wobbel-Impuls").



### 3 Die Parameter der Frequenzbereiche im Einzelnen

Von Dipl.-Ing. Erwin Schmidt, Pepperl und Fuchs GmbH

Die folgenden Angaben können nur einen Überblick geben. Weitere Details und gegebenenfalls aktuellere Angaben zu diesen Frequenzen findet man in dem Dokumenten CEPT/ERC 70-03, ETSI EN 300 330, EN 300 220, EN 300 440 und EN 302 208. (siehe Kapitel 4.5 und [www.ero.dk](http://www.ero.dk), [www.etsi.org](http://www.etsi.org)).

#### 3.1 LF-Bereich (119...148,5 kHz)

Eigenschaften:

- induktive Kopplung, Nahfeld
- bündiger Einbau in Metall möglich
- kugelförmiges Lesefeld
- geringe Reichweiten
- niedrige Datenübertragungsraten
- Antikollision hat geringe Bedeutung

Frequenzzulassungen:

Europa

- bis 135 kHz: 65 dB $\mu$ A/m @ 10m
- 135...140 kHz: 42 dB $\mu$ A/m @ 10m
- 140...148,5 kHz: 37,5 dB $\mu$ A/m @ 10m

USA/Kanada

- 2400/f [kHz]  $\mu$ V/m @ 300m

Japan

- 30V/m @ 3m

China

- P<sub>peak</sub> < 1W

#### 3.2 HF-Bereich (13,56 MHz)

Eigenschaften:

- induktive Kopplung, Nahfeld
- Transponderspulen mit wenigen Windungen (niedriger Preis, flache Label)
- höhere Datenübertragungsrate
- Antikollision wichtig für bestimmte Anwendungen

Frequenzzulassungen:

Europa

- 13,553...13,567 MHz 60 dB $\mu$ A/m @ 10m

13,410...13,710 MHz 9 dB $\mu$ A/m @ 10m  
außerhalb -3,5 dB $\mu$ A/m @ 10m

USA/Kanada

wie Europa (nur max. 42 dB $\mu$ A/m)  
außerhalb 13,560...14,010 MHz -12,4 dB $\mu$ A/m @ 10m

Japan

13,56 MHz  $\pm$ 7 kHz 42 dB $\mu$ A/m  
13,56 MHz  $\pm$ 150 kHz 9 dB $\mu$ A/m  
13,56 MHz  $\pm$ 450 kHz -3,5 dB $\mu$ A/m  
13,56 MHz  $\pm$ 900 kHz -10 dB $\mu$ A/m

China

13,553...13,567 MHz 42 dB $\mu$ A/m @ 10m

### 3.3 UHF-Bereich

Eigenschaften:

- hohe Reichweiten
- hohe Datenübertragungsraten
- schnelle Antikollision möglich
- keine weltweit überlappenden Frequenzbereiche
- schlechte Energieversorgung durch das Feld  
→ optional: Transponder mit Batterie für hohe Reichweiten
- unklare Patentsituation durch ca. 1500...2000 Patente

Frequenzzulassungen:

Europa (200kHz-Kanäle, Listen-before-talk/Carrier sense)

865,0...868,0 MHz Perp = +20 dBm (100 mW)

865,6...868,0 MHz Perp = +27 dBm (500 mW)

865,6...867,6 MHz Perp = +33 dBm (2 W)

USA/Kanada

902...928 MHz Peirp = 4 W (equivalent isotropic radiated power)

Japan (200kHz-Kanäle, Listen-before-talk/Carrier sense)

952...955 MHz Perp = 1 W, +6dB Antennengewinn = 4 W

China (200kHz-Kanäle, Listen-before-talk/Carrier sense)

(917...925 MHz geplant)

Korea (200kHz-Kanäle, Listen-before-talk/Carrier sense)

908,5...914 MHz Perp = 4 W

Singapur (200kHz-Kanäle, Listen-before-talk/Carrier sense)

923...925 MHz P = 2 W

(920...925 MHz geplant)

Indien

wie Europa

### 3.4 GHz-Bereich (2,4...2,5 GHz)

- Backscatter, Fernfeld
- hohe Reichweiten
- hohe Datenübertragungsraten
- schlechte Energieversorgung durch das Feld  
→ optional: Transponder mit Batterie
- breites ISM-Band  
→ effektive Verfahren zur Interferenzvermeidung

Frequenzzulassungen:

Europa

2,446...2,454 GHz Peirp = 500 mW, 4 W indoor

USA/Kanada

2,400...2,483 GHz Peirp = 4 W

Japan

2,400...2,4835 GHz 3 mW/MHz (Peirp = 1 W)

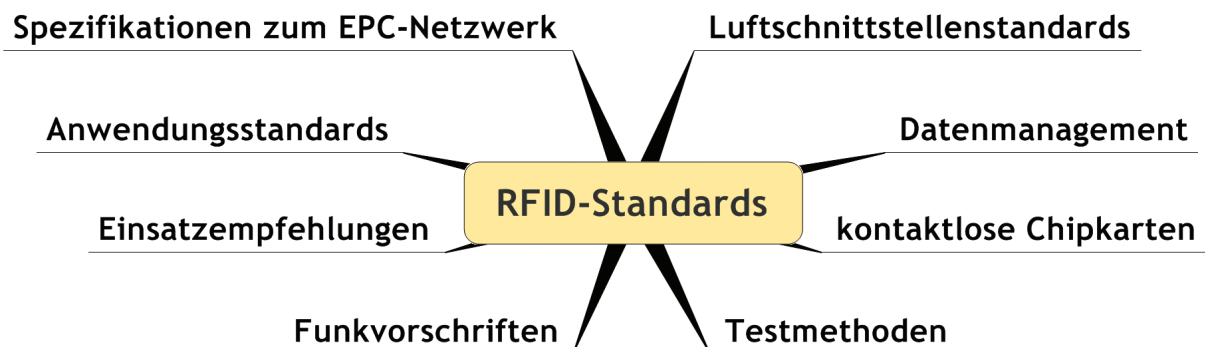
China

2,400...2,425 GHz 250 mW/m @ 3 m (Peirp = 21 mW)

## 4 Standards

Von Dipl.-Wirt.-Ing. Jan Hustadt, Fachgebiet Logistik der Universität Dortmund

Standards sind ein wichtiger Aspekt bei der Einführung neuer Technologien wie der RFID-Technologie und können als Innovationsmotor begriffen werden. Erst wenn entsprechende Vereinbarungen über Hardware, Software oder die Prozessgestaltung vorliegen, wird es für die breite Masse von insbesondere mittelständischen Unternehmen interessant, sich mit einer neuen Technologie auseinanderzusetzen. In dem Fall sinken zum einen die Investitionskosten gegenüber proprietären Lösungen, zum anderen besteht – sicher entscheidender – Investitionssicherheit hinsichtlich der gewählten Lösung. Hinzu kommt, dass in einer heute stark vernetzten Welt und zusätzlich offenen Systemen eine Nutzung über Unternehmensgrenzen hinweg nur über standardisierte Lösungen sinnvoll möglich ist.



**Abb. 1: Standardisierung im Bereich RFID**

### 4.1 Luftschnittstellenstandards

Zentrales Element eines jeden RFID-Systems ist die Luftschnittstelle zwischen Transponder und Schreib-/Lesegerät (Reader). Spezifiziert werden technisch relevante Angaben die Signalübertragung betreffend. Dies gilt z. B. für die Betriebsfrequenz, die Bandbreite, Modulation, Datenkodierung und Datenrate. Die ISO/IEC 18000er Reihe nimmt hierbei einen zentralen Platz ein. Ihre einzelnen Blätter werden derzeit hinsichtlich Sensorfunktionen, batteriegestützter Transponder, allgemeiner Verbesserungen und einer Einbindung von EPC Class 1 Generation 2 (siehe Tab.1) überarbeitet.

**Tab. 1: Luftschnittstellenstandards**

Titel	Inhalt	Status
ISO/IEC 18000-1	Referenz-Architektur und allgemeine Parameterbeschreibung	Veröffentlicht (in Überarbeitung)
ISO/IEC 18000-2	Parameter für Frequenzen unterhalb 135 kHz (passiv)	Veröffentlicht (in Überarbeitung)
ISO/IEC 18000-3	Parameter für 13,56 MHz (passiv)	Veröffentlicht (in Überarbeitung)
ISO/IEC 18000-4	Parameter für 2,45 GHz (passiv, aktiv)	Veröffentlicht (in Überarbeitung)
ISO/IEC 18000-6	Parameter für 860 bis 960 MHz (passiv; integriert im Teil C EPC Class 1 Generation 2, in Entwicklung)	Veröffentlicht (in Überarbeitung)
ISO/IEC 18000-7	Parameter für 433 MHz (aktiv)	Veröffentlicht (in Überarbeitung)
ISO/IEC TR 24710	Auf ISO/IEC 18000 basierender Elementartransponder	Veröffentlicht
EPC Class 1 Generation 2	UHF Air Interface Protocol Standard	Veröffentlicht

## 4.2 Standards zum Datenmanagement

Datenprotokolle beschreiben den Austausch von Daten in einem RFID-System. ISO/IEC 15961 und ISO/IEC 15962 spezifizieren im Verbund zum einen die Schnittstelle des Readers zum Anwendungssystem und zum anderen die Schnittstelle vom Reader zum Transponder mit einem Abbild der Transponderdaten im Reader und Angaben zur Basisverarbeitung der Transponderdaten. Beide Normen werden derzeit in Bezug auf Speichersegmentierung, Sicherheit und Authentifikation überarbeitet und erweitert. In Ergänzung beschreibt z. B. ISO/IEC 24752 das Systemmanagement von Reader-Infrastrukturen.

**Tab. 2: Standards zum Datenmanagement – Datenprotokoll**

Titel	Inhalt	Status
ISO/IEC 15961	Anwendungsinterface	Veröffentlicht
ISO/IEC 15961-1	Anwendungsinterface	In Entwicklung
ISO/IEC 15961-2	Registrierung von Datenelementen	In Entwicklung
ISO/IEC 15961-3	Datenelemente	In Entwicklung
ISO/IEC 15962	Transponderinterface	Veröffentlicht
ISO/IEC 15962-1	Transponderinterface	In Entwicklung
ISO/IEC 24752, 1-5	Funktionen zur Steuerung und Überwachung der Schreib-/Lesegeräte	In Entwicklung
ISO/IEC 24753	Funktionen für aktive Transponder und Sensorfunktionen	In Entwicklung
ISO/IEC 15434	Transfersyntax	Veröffentlicht (in Überarbeitung)

Während der Inhalt der auf einem Transponder gespeicherten Daten vom Anwender nach bestimmten Regeln frei wählbar ist, wird der Aufbau dieser Daten in Standards zur Datenstruktur definiert. Über einen hohen Bekanntheitsgrad verfügt die so genannte elektronische Produktnummer EPC (siehe hierzu Abschnitt 4.8). Daneben bietet ISO/IEC 15963 ein Kennzeichnungssystem zur eindeutigen Identifizierung von Transpondern, angefangen bei einer Nutzung für Mechanismen zur Pulkerfassung bis hin zur Verfolgung gekennzeichnete Artikel

in der Supply Chain. Standards, die bisher vornehmlich mit existierenden Barcode-Anwendungen in Verbindung gebracht worden sind, werden an neue rechtliche und qualitative Anforderungen bezüglich der Rückverfolgbarkeit von Produkten im Sinne einer Unverwechselbarkeit bis hin zu kleinsten Einheiten/Objekten angepasst. Entsprechend ist ISO/IEC 15459 ausgehend von einem Schwerpunkt bei der Transportlogistik erweitert worden.

**Tab. 3: Standards zum Datenmanagement – Datenstruktur**

Titel	Inhalt	Status
ISO/IEC 15963	Eindeutige Identifizierung	Veröffentlicht
ISO/IEC 15418	Datenidentifikatoren	Veröffentlicht
ISO/IEC 9834-1	Objektidentifikatoren	Veröffentlicht
ISO/IEC 15459-1	Unique identifiers for item management – Unique identification of transport units	Veröffentlicht
ISO/IEC 15459-2	Registration procedures	Veröffentlicht
ISO/IEC 15459-3	Common rules for unique identification	Veröffentlicht
ISO/IEC 15459-4	Unique item identification for supply chain management	Veröffentlicht
ISO/IEC 15459-5	Unique identification of returnable transport items	In Entwicklung
ISO/IEC 15459-6	Unique identification for product groupings in material lifecycle management	In Entwicklung
DIN V 66401	Unverwechselbare Identifikations-Marke	Veröffentlicht
DIN V 66403	Systemidentifikatoren für Datenstrukturen	Veröffentlicht
EPC Tag Data Standard	Eindeutige Identifizierung	Veröffentlicht

### 4.3 Kontaktlose Chipkarten

Kontaktlose Chipkarten stellen immer noch ein Haupteinsatzgebiet für RFID-Anwendungen dar. Sie unterscheiden sich hinsichtlich ihrer Reichweite und decken anwendungsunabhängig alle relevanten Bereiche zum Einsatz der Chipkarten ab – angefangen bei den physikalischen Eigenschaften über die Luftschnittstelle bis hin zum Datenprotokoll.

**Tab. 4: Kontaktlose Chipkarten**

Titel	Inhalt	Status
ISO 10536, 1-3	Close-Coupling-Chipkarten	Veröffentlicht
ISO 14443, 1-4	Proximity-Coupling-Chipkarten	Veröffentlicht
ISO 15693, 1-3	Vicinity-Coupling-Chipkarten	Veröffentlicht

### 4.4 Testmethoden

Insbesondere die ISO/IEC 18000er Reihe ist als Sollbestimmung zu verstehen. Zur Überprüfung der Einhaltung ihrer Vorgaben stehen mit ISO/IEC 18046 und der ISO/IEC 18047er Reihe entsprechende Prüfverfahren zur Verfügung. Erstere konzentriert sich auf die Leistungsfähigkeit, letztere auf die Konformität. VDI 4472 Blatt 10 soll in Ergänzung dazu für den Anwender leicht verständlich und nachvollziehbar die Leistungsfähigkeit von RFID-Systemen oder einzelner Systemkomponenten hinsichtlich bestimmter Herstellerangaben und/oder konkreter Einsatzszenarien nachweisen. Labore der verschiedenen Universitäten und Institu-

te garantieren in diesem Zusammenhang für eine herstellerunabhängige und neutrale Expertise.

**Tab. 5: Testmethoden**

Titel	Inhalt	Status
ISO/IEC TR 18046	Leistungsfähigkeit von RFID-Systemen	Veröffentlicht
ISO/IEC TR 18047-2	Konformität der Luftschnittstelle bei Frequenzen unterhalb 135 kHz	In Entwicklung
ISO/IEC TR 18047-3	Konformität der Luftschnittstelle bei 13,56 MHz	Veröffentlicht
ISO/IEC TR 18047-4	Konformität der Luftschnittstelle bei 2,45 GHz	Veröffentlicht
ISO/IEC TR 18047-6	Konformität der Luftschnittstelle bei 860 bis 960 MHz	In Entwicklung
ISO/IEC TR 18047-7	Konformität der Luftschnittstelle bei 433 MHz	Veröffentlicht
ISO/IEC 10373-1	Allgemeine Prüfungen zu Identifikationskarten	Veröffentlicht (in Überarbeitung)
ISO/IEC 10373-6	Proximity-Coupling-Chipkarten	Veröffentlicht (in Überarbeitung)
ISO/IEC 10373-7	Vicinity-Coupling-Chipkarten	Veröffentlicht
VDI 4472-10	Abnahmeverfahren zur Leistungsfähigkeit von RFID-Systemen	In Entwicklung

## 4.5 Funkvorschriften

RFID-Systeme sind rein rechtlich mit Funkanlagen gleichzusetzen und dementsprechend sind Funkvorschriften zu beachten. Um den z. B. im Zusammenhang mit ETSI EN 300220 existierenden Leistungsrückstand bei RFID-Anwendungen im für die Logistik besonders interessanten Bereich der Ultrahochfrequenz gegenüber den Möglichkeiten, die in den USA herrschen, auszugleichen, wurde Ende 2005 ETSI EN 302208 veröffentlicht. Diese Norm ermöglicht und regelt den Einsatz von bis zu zwei Watt (ERP) starken Readern im Bereich zwischen 865 und 868 MHz auf allerdings insgesamt nur zehn Kanälen. Der Inhalt der ETSI EN 302208 ist zudem noch nicht von allen Ländern der EU in nationales Recht überführt worden.

**Tab. 6: Funkvorschriften**

Titel	Inhalt	Status
ETSI EN 300220, 1-3	Funkparameter 25 bis 1000 MHz	Veröffentlicht
ETSI EN 300330, 1-2	Funkparameter 9 kHz bis 25 MHz	Veröffentlicht
ETSI EN 300440, 1-2	Funkparameter 1 bis 40 GHz	Veröffentlicht
ETSI EN 302208, 1-2	Funkparameter 865 bis 868 MHz	Veröffentlicht
ETSI EN 301489	Elektromagnetische Kompatibilität	Veröffentlicht
EN 50357	Ermittlung der Exposition von Personen gegenüber elektromagnetischen Feldern	Veröffentlicht
EN 50364	Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern	Veröffentlicht

## 4.6 Einsatzempfehlungen

Als Zwischenschritt zwischen technologieorientierten Standards einerseits und Anwendungsstandards andererseits bieten Einsatzempfehlungen Anleitungen zum Einsatz, zur Installation oder zur Inbetriebnahme von RFID-Systemen.

**Tab. 7: Einsatzempfehlungen und Begriffe**

Titel	Inhalt	Status
ISO/IEC TR 18001	Profile für Anforderungserfordernisse	Veröffentlicht
ISO/IEC TR 24729-1	Einsatzempfehlungen für RFID-Label	In Entwicklung
ISO/IEC TR 24729-2	Hinweise zur Recyclingfähigkeit	In Entwicklung
ISO/IEC TR 24729-3	Installation von Readern und Antennen	In Entwicklung
ETSI TR 101445	Referenzdokument und Konditionen zu Anwendungen im Bereich UHF	Veröffentlicht
ETSI TR 102436	Installation und Inbetriebnahme von UHF-RFID-Systemen	Veröffentlicht
ISO/IEC 19762-1	Allgemeine Begriffe zur automatischen Datenerfassung	Veröffentlicht
ISO/IEC 19762-3	RFID-Begriffe	Veröffentlicht

## 4.7 Anwendungsstandards

Anwendungsstandards empfehlen eine bestimmte technische Lösung für einzelne Anwendungen und greifen dabei auf andere existierende technologieorientierte Standards z. B. zur Luftschnittstelle oder zum Datenmanagement zurück. Erarbeitet werden in diesem Zusammenhang aus Sicht der Logistik im Wesentlichen die ISO-Normen 17363 bis 17367, die sich auf alle Ebenen einer Lieferkette beziehen und hinsichtlich der RFID-Technologie u. a. auf die ISO/IEC 18000er Reihe zurückgreifen. Abgesehen von diesem Projekt findet man entsprechende und veröffentlichte Standards immer noch selten. Als Ausnahmen sind u. a. die sich mit der Identifikation von Tieren im niederfrequenten Bereich befassenden ISO-Normen 11784, 11785 und 14223 zu nennen, die darüber hinaus z. B. als Basis für Systeme aus dem Bereich der Entsorgungswirtschaft dienen.

**Tab. 8: Anwendungsstandards (international)**

Titel	Inhalt	Status
ISO 11784	Tieridentifikation, Codestruktur	Veröffentlicht
ISO 11785	Tieridentifikation, technisches Konzept	Veröffentlicht
ISO 14223	Tieridentifikation, weiterentwickelte Transponder	Veröffentlicht
ISO 17363	Frachtcontainer	In Entwicklung
ISO 17364	Wiederverwendbare Transporteinheiten	In Entwicklung
ISO 17365	Transporteinheiten	In Entwicklung
ISO 17366	Produktverpackungen	In Entwicklung
ISO 17367	Artikelkennzeichnung	In Entwicklung
ISO 10374	Automatische Identifikation von Frachtcontainern	Veröffentlicht (in Überarbeitung)
ISO 18185, 1-4 u. 6-7	Elektronisches Siegel von Frachtcontainern	In Entwicklung
ISO 21007, 1-2	Kennzeichnung von Gasflaschen	Veröffentlicht
ISO/IEC 24730, 1-4	Ortungssysteme, Real-time locating systems (RTLS)	In Entwicklung (Blatt 1 veröffentlicht)



Auf nationaler Ebene schreitet die Standardisierung im Bereich RFID nicht in dem Maße voran wie international. Es werden insbesondere anwendungsbezogene Standards formuliert. Dies liegt aber vor allem auch daran, dass Deutschland aufgrund von länderübergreifenden Vereinbarungen und Regeln internationale Normen übernimmt sowie in unterschiedlichster Art und Weise deutsche Interessen bereits in internationalen Gremien und Organisationen vertreten sind, z. B. durch den DIN Unterausschuss NI-31.4.

**Tab. 9: Anwendungsstandards (national)**

Titel	Inhalt	Status
DIN V 30745	Elektronische Identifizierung von Abfallsammelbehältern durch RFID	Veröffentlicht
DIN EN 14803, 1-3	Identifizierung und Mengenbestimmung von Abfall	Veröffentlicht
VDI 2515-2	Identträger für Stückgutfördersysteme	Veröffentlicht
VDI 3964	Mobile Datenspeicher für Großladungsträger	Veröffentlicht
VDI 4472, 1-11	Transpondereinsatz in der Supply Chain	In Entwicklung (Bl. 1 u. 2 veröffentlicht)

Obwohl die RFID-Technologie bereits seit vielen Jahren in unterschiedlichen Anwendungsgebieten erfolgreich eingesetzt wird, befinden sich entsprechende Standardisierungsprojekte mit logistischem Schwerpunkt – wie beschrieben, soweit vorgesehen und/oder betrieben – in der Regel noch in der Entwicklung. Insbesondere anwendungsbezogene und branchenspezifische Richtlinien werden jedoch vom VDI z. B. mit der Richtlinie 4472 als Stand der Technik erarbeitet und stellen technologische, logistische und konzeptionelle Orientierungshilfen zur Verfügung. Der Vorteil derartiger Richtlinien liegt in der Einbindung aller interessierten Kreise und in einer kurzfristig möglichen Zielerreichung. Dabei haben VDI-Richtlinien auf Grund vertraglicher Regeln mit dem DIN national den Rang einer Norm.

**Tab. 10: VDI-Richtlinienprojekt 4472**

VDI	VDI 4472 – Anforderungen an Transpondersysteme zum Einsatz in der Supply Chain	
Blatt 1:	Einsatz der Transpondertechnologie (Allgemeiner Teil)	veröffentlicht
Blatt 2:	Einsatz der Transpondertechnologie in der textilen Kette (HF-Systeme)	veröffentlicht
Blatt 3:	Einsatz der Transpondertechnologie in der textilen Kette (UHF-Systeme)	in Bearbeitung
Blatt 4:	Kostenbewertung von RFID-Systemen	in Bearbeitung
Blatt 5:	Einsatz der Transpondertechnologie in der Mehrweglogistik	in Bearbeitung
Blatt 6:	Einsatz der Transpondertechnologie in der Kühlkette	in Planung
Blatt 7:	Einsatz der Transpondertechnologie in der Entsorgungslogistik	in Bearbeitung
Blatt 8:	Leitfaden für das Management von RFID-Projekten	in Bearbeitung
Blatt 9:	Einsatz der Transpondertechnologie in der Getränke-logistik	in Planung
Blatt 10:	Abnahmeverfahren zur Überprüfung der Leistungsfähigkeit von RFID-Systemen	in Bearbeitung
Blatt 11:	Leitfaden zur Transpondertechnologie unter Sicherheitsaspekten	in Planung

## 4.8 Spezifikationen zum EPC-Netzwerk

Häufig wird im Zusammenhang mit RFID-Standards im gleichen Atemzug mit RFID der EPC (Electronic Product Code) genannt. Dabei entspricht der EPC einer weltweit eindeutigen Seriennummer, die derart gestaltet ist, dass sie existierende, bewährte Nummerierungsschemata vornehmlich aus dem Bereich des Handels als eine Art Containerformat aufnehmen kann, um Inkompatibilitäten zu vermeiden. Gerade auf der zweiten Generation des EPC von EPCglobal Inc., einer aus dem Auto-ID Center hervorgegangenen Organisation, die in Deutschland durch die GS 1 Germany GmbH vertreten wird, ruhen große Hoffnungen. Doch dabei geht es nicht alleine um eine Nummer, den EPC, sondern auch um die Luftschnittstelle (EPC Class 1 Generation 2) und insbesondere eine ganze Architektur bzw. Infrastruktur, welche die Informationen über die mit den EPCs gekennzeichneten Objekte zum einen erfasst und speichert sowie zum anderen bei Abfragen bereit stellt, das EPC-Netzwerk.

**Tab. 11: Spezifikationen zum EPC-Netzwerk**

Standards   Spezifikationen	Status
EPC-Tag-Datenstandard, Versionen 1.1 Rev. 1.27 und 1.3	Veröffentlicht
EPC-Luftschnittstellenbeschreibung - Class 1 Generation 2 (UHF), Version 1.0.9 - Class 1 Version 1 (UHF), Class 1 Version 1 (HF), Class 0 Version 1 (UHF)	Veröffentlicht
Lesegerät-Protokoll	In Entwicklung
Lesegerät-Management	In Entwicklung
Tag-Datenübersetzung, Tag Data Translation (TDT) Version 1.0	Veröffentlicht
Ereignisse auf Anwendungsebene ALE, Application Level Events (ALE) Specification Version 1.0	Veröffentlicht
EPCIS-Erfassungsschnittstelle	In Entwicklung
EPCIS-Datenspezifikation	In Entwicklung
Objektnamenservice, Object Naming Service (ONS) Specification Version 1.0	Veröffentlicht
EPCIS-Abfrageschnittstelle	In Entwicklung
EPCIS-Ermittlung	In Entwicklung
Teilnehmer-Authentifizierung	In Entwicklung

Für den Fall, dass ein offenes RFID-System konzipiert werden soll, ist der Einsatz von standardisierten Komponenten unumgänglich; aber auch bei geschlossenen Systemen empfiehlt es sich – aus wirtschaftlichen Gründen – ISO-Standards anzuwenden.

## 5 Technik

Von Jos Fransen M.B.A., Euro I.D. Identifikationssysteme GmbH & Co. KG

### 5.1 Transponder

Grundsätzlich sind zwei Typen, sowohl eine Nur-Lese-Version (Read-Only) als auch eine Schreib-Lese-Version (Read/Write), verfügbar. Bei der Auswahl sollte man sich auf die Aufgabenstellung konzentrieren und bedenken, dass die Schreib-Lese-Lösung meistens mehr Zeit bei der Datenübertragung in Anspruch nimmt, weil die geschriebenen Daten, zur Sicherheit, noch einmal zurück gelesen werden sollten. Diese Transponder haben durch das EEPROM auch einen reduzierten Temperaturbereich. Die Lebensdauer passiver Transponder ist im Read-Only-Modus nahezu unendlich. Bei Schreib-/Leseinsatz gibt es eine Grenze bei ca. 100.000 Schreibzyklen. Die maximalen Temperaturen bei Hochtemperaturtranspondern betragen ca. 210 bis 240 °C. Bei aktiven Transpondern werden sowohl Lebensdauer (ca. 7 Jahre) als auch maximale Temperatur (z. B. +70 °C) von der Batterie begrenzt.

### 5.2 Speichertypen

#### 5.2.1 Read-Only-Transponder

Die Kennung ist in einer Diodenmatrix (ROM) auf dem Mikrochip abgelegt. Wegen der größeren Datensicherheit und um eine Änderung bzw. Fälschung der Kennung auszuschließen, werden die entsprechenden Diodenverbindungen nicht elektrisch zerstört, sondern mit einem Laserstrahl ausgebrannt. Aus Gründen des produktionstechnischen Ablaufes ist es nicht möglich, eine Sequenz oder gar eine Programmierung nach Kundenwunsch zu liefern. Es wird aber die absolute Einmaligkeit einer jeden Kennung garantiert.

#### 5.2.2 Schreib-/Lese-Transponder

Beim Schreib-/Lese-Transponder können Daten in einem EEPROM abgelegt werden, das ca. 100.000 mal beschrieben werden kann. Die meisten Schreib-/Lesetransponder bieten neben dem freien Speicherbereich eine unveränderbare einmalige Seriennummer. Es besteht auch die Möglichkeit des One-Time-Programming (OTP). Hierbei wird der Speicher nach Programmierung des gewünschten Codes für weitere Schreibzugriffe gesperrt. Damit können dann, allerdings ohne Garantie der Einmaligkeit, kundenspezifische Programmierungen erstellt werden.

#### 5.2.3 Speicherkapazität

Die meisten Read-Only-Transponder haben eine Speicherkapazität von 64 Bit. Hiervon werden eine Anzahl zur Synchronisation sowie zur Fehlererkennung und Fehlereliminierung benötigt. Read-/Write-Transponder verfügen, je nach Typ, über EEPROMs mit Speicherkapazitäten von 264 Bit bis 2 kBit. Einige aktive Transponder bieten eine Speicherkapazität von

32kByte. Die Read-/Write-Transponder bieten neben extensiver Sicherung vor Fehlprogrammierung eine Aufteilung des Speichers in Blöcke mit einem Schreibschutz je Block. Auf Wunsch kann auch eine zusätzliche Verriegelung über Passwort erfolgen.

### **5.3 Schreib-/Lesegeräte, Antennen und mobile Terminals**

Eine technisch versierte und wirtschaftlich rentable Lösung wird erst dann daraus, wenn das System mit seinen einzelnen Komponenten die jeweilige Anwendung optimal unterstützt und in die EDV-Hierarchie eingebunden werden kann.

Die Kommunikation mit den Rechnern kann über integrierte Schnittstellen erfolgen. Je nach Lesegerät stehen RS 232, RS 485, PROFIBUS, PROFINET, CAN, Interbus, DeviceNet oder TCP/IP-Schnittstellen und neuerdings auch WLAN/Bluetooth zur Verfügung. Für einfache Anwendungen mit Einzelsystemen (RS 232) erfolgt die Kommunikation mittels ASCII-Protokoll mit einfachen Befehlen. Dadurch ist die Softwareschnittstelle Leser/Rechner in einfacher Weise zu programmieren. Zur Kopplung der PROFIBUS-Systeme mit einer Siemens S7 oder Beckhoff-SPS bieten einige Hersteller Funktionsbausteine an, die den Programmieraufwand deutlich reduzieren.

## 6 Physikalische Aspekte

Von Jos Fransen M.B.A., Euro I.D. Identifikationssysteme GmbH & Co. KG

### 6.1 Auslegung von bewegten Systemen

Wenn ein Transponder in Bewegung ausgelesen werden soll, sind die folgenden Punkte zu beachten:

Der gesamte Dateninhalt des Transponders ist während des Durchgangs durch das Feld des Lesegerätes zu lesen.

Hierbei sind die wesentlichen Einflussgrößen:

#### a) Dateninhalt des Transponders

Er bestimmt die zeitliche Länge des Datentelegramms und sollte minimiert werden. Die zur Berechnung notwendigen Informationen, wie Header, Nutzdaten, CRC-Anteil und Übertragungsrate sind den obengenannten ISO-Normen zu entnehmen.

#### b) Lesereichweite Transponder – Lesegerät

Die geometrischen Abmessungen und die elektrischen Eigenschaften der Antennen in Lesegerät und im Transponder bestimmen den Leseabstand ebenso wie die obengenannten physikalischen Bedingungen.

Ein wesentlicher Gesichtspunkt ist auch, ob ein Antikollisionsverfahren eingesetzt werden soll. Die Abfrage mehrerer Transponder im Feld eines Lesegerätes erfordert ein Vielfaches der Summe der Lesezeiten der Einzeltransponder.

### 6.2 Lesereichweiten in der Praxis

Unter Industriebedingungen gibt es einige Einschränkungen, so werden die Lesereichweiten bei LF-Systemen durch elektromagnetische Störung reduziert. Hierzu gehören z. B. frequenzgesteuerte Antriebe, Monitore mit Bildröhren und Leuchtstofflampen, die mit Halbleiter-Drosseln arbeiten. Für den UHF- und GHz-Bereich können Überreichweiten auftreten z. B. durch Reflexionen an Metallflächen („Bouncing-Effekt“).

Bei allen Frequenzbereichen gibt es Einschränkungen, wenn Transponder direkt auf Metall aufgebracht werden (siehe 2.5). Durch geeignete Maßnahmen (Abschirmung, Feldbündelung durch Ferritkerne, Abstimmung) kann das Lesen auf Metall oder sogar bei bündigem Einbau in Metall trotzdem ermöglicht werden. Je nach Maßnahme ist mit einem reduzierten Leseabstand zu rechnen.

Bei Einsatz von mehreren Lesegeräten ist eine sorgfältige Trennung der Arbeitskanäle vorzusehen, beziehungsweise geeignete Maßnahmen der Abschirmung vorzunehmen. Für alle

Frequenzbereiche gilt es, die Synchronisation der Lesegeräte zu beachten (Listen-before-talk).

### **6.3 Umgebungsparameter**

Weitere Umgebungsparameter wie Temperatur, Säuren, Laugen, Lösungsmittel und Feuchtigkeit spielen eine wichtige Rolle bei der Auswahl der Transpondertechnik und -verpackung. Hier gibt es für die verschiedenen Frequenzbereiche eine Vielfalt an Bauformen mit unterschiedlichen Spezifikationen. Für die spezifische Anwendung kann hier eine spezielle Anpassung notwendig sein.

## **7 Eigenschaften einer RFID-Middleware und Kriterien für die Architektur und die Implementierung**

Von Dr. Michael Groß, Dabac integrierte EDV Organisation GmbH

Ziel dieses Kapitels ist es, Anforderungen an die RFID-Middleware zu formulieren und eine Entscheidungs- und Planungshilfe für die Konzeption von RFID-Systemen zu bieten.

Die Verfügbarkeit von RFID-Systemen ist abhängig von allen Komponenten (End2End Availability), wobei der RFID-Middleware eine zentrale Rolle zukommt. Dies betrifft die Zuverlässigkeit der Informationen, die Sicherheit der Informationen, die Verfügbarkeit von Informationen und die Skalierbarkeit der Systeme.

Software stellt in vielen RFID-Lösungen einen wichtigen Bestandteil dar. Die Vielfalt an verfügbarer RFID-Hardware, die stürmische Entwicklung bei Standards und die täglich wachsende Flut an Anwendungsfällen erfordert heute einen beträchtlichen Aufwand bei der Softwareerstellung und profundes Know-How der daran beteiligten Entwickler. Diese Problematik kann durch die Verwendung einer generischen, nicht von einer speziellen Hardware abhängigen Programmierschnittstelle (Abstraktionsinstanz) vereinfacht werden. Zusätzlich kann auf verschiedene Standardmodule zurückgegriffen werden, um beispielsweise eine Anbindung an SAP und andere Systeme zu schaffen.

### **7.1 Beschreibung**

Ein wesentliches Merkmal von RFID-Systemen ist die Echtzeitverarbeitung von Informationen zur Synchronisation der virtuellen Unternehmenswelt (ERP-Systeme, WM-Systeme etc.) mit der realen Welt der Unternehmensprozesse. RFID-Systeme bestehen im Allgemeinen aus den Transpondern, den Lese-/Schreibeinheiten, der Middleware und den Anschlusssystemen an die Unternehmenssoftware (RFID-Gateways). Eine Integration von RFID-Systemen in die Infrastruktur und Prozesse von Unternehmen ist damit erfolgskritisch verbunden mit der Leistungs- und Anpassungsfähigkeit der RFID-Middleware. Die RFID-Middleware stellt das Bindeglied und eine Abstraktionsebene zwischen der RFID-Geräteinfrastruktur und den Systemen der Geschäftsprozesssteuerung dar und muss spezifische Anforderungen erfüllen, um diese Integration zu ermöglichen.

Middleware muss nicht unbedingt notwendige RFID-Daten möglichst nahe an der Quelle überprüfen und filtern, sollte aber diese Funktionalitäten konfigurierbar in verschiedenen Ebenen der Datenstromverarbeitung (Eventstreamprocessing) zur Verfügung stellen können. Sie ist für die Anwendungen unsichtbar und verhindert die Überflutung der angeschlossenen Systeme mit Daten. Einfache Mechanismen zur Steigerung der Leistungsfähigkeit, um grö-

Bere Datenmengen zu bewältigen, sind daher ein wesentlicher Bestandteil einer geeigneten RFID-Middleware.

RFID-Datenströme sind mit der Entwicklung neuer Anwendungsmöglichkeiten und -technologien ebenso wie andere Middlewareanwendungen oder Datenarten aus dem Bereich Ton und Bild einem dynamischen Wachstum unterworfen. Schon heute zeichnet sich ab, dass die Datenmengen und die Anforderungen an die Echtzeitverarbeitung mit der zunehmenden Komplexität der RFID-Systeme exponentiell steigen werden. Eine geeignete Middlewareinfrastruktur hilft damit, die Investitionen in RFID-Netze zukunftsicher zu machen.

Die RFID-Entwicklung bietet neben seriellen Anschlusstechniken direkt an PC basierte Systeme oder seriell über Industriebussysteme vernetzte und proprietäre Verbindungen auch IP basierte Anschlüsse. Die Vernetzung ist damit flexibel an projektindividuelle Gegebenheiten anpassbar und in bestehende Netzwerkstrukturen zu integrieren. Dies erhöht gleichzeitig die Anforderungen an die Interoperabilität mit Geräten und Verarbeitungssystemen verschiedenster Hersteller sowie an die Koexistenz unterschiedlichster Datenströme, die dieselbe Netzwerkinfrastruktur verwenden.

Die Sicherheit der Datenströme stellt einen Aspekt dar, der in der Zukunft immer mehr an Bedeutung gewinnen wird. Die zunehmende Vernetzung und Integration verschiedenster Datenquellen und Datenverarbeitungssysteme wird die Schutzanforderungen stark erhöhen und damit einen kritischen Faktor für die Auswahl geeigneter Middlewaresysteme darstellen. Die Gefahren werden zunehmen, – durch unerlaubten Zugriff auf Daten, nicht erlaubte Modifikation von Daten, Diebstahl und Mißbrauch von Diensten und Vortäuschen einer falschen Identität. Eine Infektion über RFID-Viren ist ebenfalls denkbar und schon mindestens im Labor nachgewiesen worden (Vrije Universiteit Amsterdam, Telepolis 03/2006). Die RFID-Middleware muss dem Rechnung tragen und die Sicherheit in den RFID-Datenströmen gewährleisten.

## **7.2 Definition**

RFID-Middleware, auch als RFID-Manager-Software bezeichnet, stellt die Verbindung zwischen RFID-Lese-/Schreibeinrichtungen (Hardware mit Betriebssystem, Firmware) und den Verwaltungssystemen wie Lager- und Fertigungsplanungssystemen her und transportiert RFID-Leseereignisse und RFID-Schreibbefehle transaktionssicher und in Echtzeit. Man kann Middleware auch als eine Verteilungsplattform, d.h. als ein Protokoll auf einer höheren Schicht als der der gewöhnlichen Rechnerkommunikation, auffassen.

Middleware stellt eine Ebene in einem komplexen Software-System dar, die als „Dienstleister“ anderen ansonsten entkoppelten Softwarekomponenten die Kommunikation untereinander ermöglicht. Middleware arbeitet dabei auf einem hohen Niveau innerhalb des Schichtenmodells: sie organisiert den Transport komplexer Daten (Messaging), vermittelt Funktionsaufrufe zwischen den Komponenten (Remote Procedure Calls), stellt die Transaktionssicherheit über ansonsten unabhängige Teilsysteme her (Funktion als Transaktions-Monitor) etc. Sie stellt damit eine Abstraktionsinstanz zwischen den beteiligten Systemen



unterschiedlichster Hersteller und Technologien dar und besitzt alle Funktionen, um die hersteller-unabhängige Interoperabilität sicherzustellen. Die RFID-Middleware enthält auch Funktionen zur Überwachung, Steuerung und Wartung von RFID-Systemen.

### **7.3 Herausforderung Datenmanagement**

Traditionelle Softwareanwendungen zur Verfolgung und Nachvollziehbarkeit (Tracking und Tracing) wurden dafür entwickelt, während der Lebensdauer eines Objektes, die Standorte und Zustandsänderungen des Objektes zu verfolgen und zu speichern. Diese Anwendungen, egal ob es sich um die Verfolgung von Personen, Produkten, Containern, Fahrzeugen oder Ausrüstung handelt, werden zunehmend von Systemen ersetzt werden, die RFID-Technologien zur Datensammlung einsetzen. Objekte werden in Zukunft auf der kleinstmöglichen Ebene – der individuellen Ebene (Item level) – verfolgt werden und so ein Vielfaches an Daten verglichen mit traditionellen Systemen erzeugen.

Durch den ständigen Rückgang der Kosten für die Komponenten und der Überwindung störender Umwelteinflüsse rückt das „Internet of Things“ immer näher. Die Möglichkeiten jedoch jedes Objekt zu taggen, zu verfolgen und mittels einer eindeutigen Seriennummer (z.B. Electronic Product Code [EPC]) auszulesen, wird eine Anpassung der Firmensoftware an zukünftige Standards verlangen und immer größere Anforderungen an die Systemintegration innerhalb einer Prozesskette stellen.

Die komplexe Eventverarbeitung muss erkennen, dass nicht nur der aktuelle Eventstrom den momentanen Zustand oder die Aktivität bestimmt, sondern die Event Engine muss gleichzeitig Zugriff auf den aktuellen und die bereits in diesem Zusammenhang gespeicherten Eventströme haben, um alle Aktivitäten dauerhaft messen und vergleichen zu können, sowie sie einander gegenüberzustellen.

Existierende Anwendungen interpretieren und verarbeiten für sich allein stehende Transaktionen (z.B. Zahlungsbelege für 30 Kisten von XYZ). RFID verändert die Dynamik. Jetzt müssen diese Anwendungen einen stetigen Strom von Events überwachen, die eine sinnvolle Einsicht in die Leistung, Trends und Ausnahmebedingungen von Prozessen gewährleisten können, sowohl in Echtzeit als auch mit gespeicherten Daten. Dieser traditionelle Ansatz für die Architektur und Funktionalität von Middlewaresystemen wird zunehmend erweitert hin zu der Anforderung eines übergeordneten Systems, welches nicht nur Informationen sammelt und weiterleitet, sondern auch eine Ebene der Verarbeitung und Auswertung bereitstellt. Eine Lösung für diese Herausforderung ist die Einführung komplexer Eventverarbeitung.

### **7.4 Architekturprinzipien**

Eine RFID-Middleware setzt sich aus mehreren Schichten zusammen: Der Kommunikationsschicht, die alle beteiligten Systeme verbindet, der Verarbeitungsschicht, die Daten verarbeitet, und der Datenbankschicht, die alle Daten archiviert und zur Komplexeventsteuerung verfügbar macht. Nicht alle Funktionen einer Middleware sind in allen Anwendungsfällen und

Einsatzgebieten notwendig. Ein modularer und nicht monolithischer Aufbau unterstützt den bedarfsgerechten Einsatz. Dies ermöglicht auch die Verteilung der verschiedenen Komponenten bei wechselnden Anforderungen und erlaubt Skalierungen und Anpassungen, ohne das System insgesamt in Frage zu stellen.

## **7.5 Komponenten**

### **7.5.1 Allgemeines**

Jede aktuelle Business Anwendung bei der RFID-Reader zum Einsatz kommen, die die eingehenden RFID-Daten von vielen Produkten und Verpackungen lesen müssen, hat einen stetigen Datenstrom zu verarbeiten. Jedes einzelne Datenpaket, welches eine Lesung oder einen Schreibvorgang repräsentiert, wird als Event bezeichnet.

#### **Definition Event:**

Um einem RFID-Event, welcher Seriennummer, Daten, Zeit und Reader-ID (zur lokalen Ortung) beinhaltet, Sinn zu geben, muss die Eventverarbeitung in der Lage sein, Ur-Daten wieder abrufen zu können, und dem Lesevorgang damit Bedeutung zu verleihen. Zum Beispiel kann sich diese Bedeutung aus Produktstammdateien, Lieferanten- und Kundenstammdateien sowie aus Bestellungen- oder Vertragsdateien ergeben. Die Fähigkeit, diese Daten in Echtzeit wieder abzurufen, sie einem Event zuzuordnen und eine Geschäftsentscheidung zu treffen, ist entscheidend für den Erfolg der komplexen Eventverarbeitung. Mit der Entwicklung der Eventverarbeitung ergibt sich auch die Fähigkeit, große Mengen dieser Daten zu speichern, was die Synchronisation mit den residenten Stammdateien oder anderen Cache-Vorgängen gewährleistet. Das Zwischenspeichern von Stammdaten direkt am Verarbeitungsort wird im Zuge der Implementierung von CEP (Complex Event Processing) eine immer wichtigere Rolle spielen.

Von diesen Eventströmen werden manche sinnvolle Events beinhalten, aber auch solche, die unwichtig für die Kernverarbeitung der Applikation sind. Die Datenströme können unvollständig oder fehlerhaft sein. Die Verarbeitung dieser eingehenden Daten benötigt die Implementierung einer Verarbeitungsschicht, die solche Datenströme abarbeiten, sinnvolle von den unwichtigen unterscheidet, und damit entsprechend präzisere Event-Daten erzeugen kann. Diese Auswertung ist eines der Kernprinzipien komplexer Eventverarbeitung. Allerdings sind es nicht die Events selbst, die komplex sind, sondern eher deren Interpretation.

Neben der RFID-Standardarchitektur, wie Reader, Tags und RFID-Middleware, besteht eine erfolgreiche, skalierbare CEP (Complex Event Processing) Architektur aus den in Abschnitt 7.5.2 bis 7.5.6 beschriebenen Komponenten.

### **7.5.2 Event Engine**

Sobald Events die Sammelphase durchlaufen, können Sie nach Typ verarbeitet werden. Die Event Engine erstellt Ereignisprozesse (Pipelines); diese kann flexible Filterformen, Aggregationen und Transformationen bereitstellen.

Eine Pipeline ist ein programmatisch strukturierter Aufbau individueller Komponenten. Jede Komponente führt eine Art Verarbeitung (Sammeln, Filtern, Gruppieren und Transformieren) an einem Event durch und sendet das Ergebnis zur nächsten Komponente. Eine Pipeline kann aus einem einzelnen Prozess oder aus vielen Prozessen bestehen, von denen jeder einen einzelnen Schritt in einer komplexen Umwandlung durchführt. Das Ergebnis ist hohe Performance und ein anpassungsfähiges Ereignismodell.

### **7.5.3 Event Datenbank**

Die Event Datenbank ist ein Cache für Events. Ereignisse erlauben jedoch nur einfache flüchtige Einträge. Die Event Engine hat die Fähigkeit, jedes Ereignis in seiner Rohform oder in seiner verarbeiteten Form, in einer skalierbaren Event Datenbank zu speichern. Die Datenbank verfügt über ein Historienobjekt für die Ereignisverarbeitung und für externe Anwendungen zum Überwachen und Messen der Ereignisse über den gesamten Prozessablauf hinweg.

### **7.5.4 Event Server**

Der Event Server unterstützt ein flexibles Interface zur Event Engine, die Integration verschiedener Datensatzformate (GRAI vs. SGTIN vs. UCC-128) und Programme zur Datenbankabfrage. Durch den Event Server kann die Event Engine nicht nur dazu verwendet werden, RFID-Anweisungen zu bearbeiten, sondern auch z.B. für Barcodeleser, Datenbankeingaben und das multiple Bereitstellen von Daten (via JMS subscription model).

### **7.5.5 Event Cache**

Der Event Cache gewährleistet den Echtzeitzugriff für eine Anzahl von Kundenanwendungen, die die Eventdatenbank abfragen wollen. Die Cache-Architektur ermöglicht mehrere Übertragungsarten (point-to-point über Queues oder publish subscriber, abhängig von den benötigten Informationssystem-Integrationen).

### **7.5.6 Reporting**

Die Middleware-Architektur unterstützt externe Anwendungen dabei, Daten aus der Eventdatenbank wieder abzurufen. Sie muss eine Standardschnittstelle für alle Client Anwendungen haben, um die konstante Verwendung des Event-Protokolls zu gewährleisten.

RFID-Systeme müssen folgende Abfragen unterstützen:

- Auflistung der Tags, die pro Reader in einer bestimmten Zeit gelesen werden.
- Auflistung der Reader, die einen bestimmten RFID-Tag in einer bestimmten Zeit ausgelesen haben.
- Anzahl der Events, die sich auf ein bestimmtes Tag, einen bestimmten Reader, eine bestimmte Organisation oder einen bestimmten Zeitraum beziehen.

## **7.6 Kriterien**

Die Kriterien, die an eine RFID-Middleware angelegt werden müssen, sind selbstverständlich abhängig von den gewünschten Leistungsparametern der RFID-Systeme. Nicht jedes RFID-

System muss alle Kriterien erfüllen, da es abhängig von Herstellern und Anforderungen unterschiedliche Strategien der Komponentenarchitektur gibt. In der Anlage 2 finden Sie eine Liste an Kriterien, die von einer RFID-Middleware – abhängig von den Erfordernissen der konkreten Anwendung – erfüllt werden sollten, ohne auf die Zuordnung zu spezifischen Komponenten einzugehen.

## 7.7 Fallbeispiele

Eventverarbeitung mit leistungsfähigen Middlewaresystemen kann in einer Vielzahl von Geschäftsprozessen eingesetzt werden, um die Prozesssicherheit zu verbessern, die Prozessgeschwindigkeit zu erhöhen und neue Prozessschritte einzubinden. Middlewaresysteme werden daher mehr und mehr schon vor den angeschlossenen Verarbeitungssystemen Informationen zur Prozesssteuerung und -analyse bereitstellen können. Zusätzlich zu den unten aufgeführten Beispielen aus der Lagerlogistik finden Sie in der Anlage 3 Beschreibungen über implementierte Lösungen in der Produktionssteuerung, Objektkennzeichnung etc.

### **Beispiel 1: Überwachung der Verteilzentrum-Aktivitäten**

Bei einer aktuellen Arbeitslastüberwachung in einem Lager oder Verteilzentrum geht es um das Management individueller Arbeitslasten (Aufgaben), die rechtzeitig beendet werden müssen.

RFID-Sensordaten werden während verschiedener Aufgaben an einem bestimmten Ort gesammelt und Benutzer können somit eine Hochrechnung des Leistungsgrades der Station anstellen. Zum Beispiel:

- die Anzahl der Tags, die an allen WARENEINGANG-Lesern ankommen,
- die Anzahl der Tags, die an allen VERSAND-Lesern ausgehen,
- die Durchschnittszeit der STAGING Phase (Zeitunterschied zwischen Tageingang und Tagausgang)

### **Beispiel 2: Verfolgen der Produktmenge**

Ein Benutzer möchte herausfinden, wie eine Produktmenge an den falschen Ort des Verteilzentrums gelangen konnte. Das Scannen eines Tags auf einer Verpackung löst ein Abfrageverfahren aus, um alle Reader zu ermitteln, die diesen Tag auf seinem Weg ausgelesen haben.

Das RFID-System gibt nun ein genaues Modell des Weges zurück, den die Verpackung innerhalb des Verteilzentrums genommen hat.

Dies unterscheidet sich von traditionellen ERP- und WMS-Anwendungen, die nur die Bewegungen aufzeichnen, die von einem Anwender zu einer bestimmten Zweck oder Gegebenheit eingegeben wurden (z.B. Entnahme). Dies gilt auch für Barcodesysteme, die zum überwiegenden Teil manuell von einem Mitarbeiter eingesetzt werden. Die Möglichkeit eines Eingabefehlers, z.B. das Eintragen unvollständiger oder falscher Daten, kann nicht ausgeschlossen werden.

### **Beispiel 3: Rückruf**

Im Falle einer Rückrufaktion nach Lieferung aufgrund fehlerhafter Qualitätskontrolle muss das System alle betroffenen Positionen eindeutig identifizieren. Um die einzelnen Positionen, die mit einem eindeutigen Code versehen sind, zu verfolgen, kann das System eine Auflistung aller Reader ausgeben, die diese Tags gelesen haben.

Dies zeigt das letzte Verteilzentrum/Lager aller Positionen, die sich noch im Gebäude befinden, und die letzten Versandinformationen aller ausgelieferten Positionen.

Der Vorteil hiervon gegenüber einer traditionellen ERP-Anwendung ist der, dass eine RFID-Abbildung in Echtzeit erfolgen kann, während eine ERP/WMS-Lösung auf manuelles AbleSEN der Positionen angewiesen ist, wenn die Positionen bewegt oder versendet werden.

### **Beispiel 4: Nachvollziehen von Lagerhausaktivität**

Nachdem ein Fehler im Prozessablauf erkannt wurde, möchte der Benutzer vom System wissen, wie sich die betroffenen Positionen innerhalb des Lagers in den letzten 72 Stunden bewegt haben.

Die ausgegebene Auflistung der Tag-Events zeigt alle Bewegungen seit dem Beginn des Warenzyklus und wo/warum der Fehler aufgetreten ist.

## 8 Datenschutz

Von Jürgen Autor, Innenministerium Baden-Württemberg

### 8.1 Allgemein

Datenschutzrechte müssen beachtet werden, wenn entweder der RFID-Tag selbst personenbezogene Daten enthält oder die nicht personenbezogenen Daten auf dem RFID-Tag mit Hilfe eines EDV-Hintergrundsystems personenbeziehbar sind, also einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können. Für die datenschutzrechtliche Beurteilung des jeweiligen RFID-Systems kommt es damit auf den konkreten Einsatzbereich an.

Damit der Betroffene auch künftig „Herr seiner Daten“ bleibt, darf der Einsatz von RFID in Bezug mit seinen personenbezogenen Daten nicht heimlich erfolgen, sondern muss transparent gemacht werden. Das bedeutet, dass der Betroffene über den Einsatz personenbeziehbarer RFID-Systeme darüber informiert werden muss, was mit seinen personenbezogenen Daten geschieht. Es dürfen keine Daten unbefugt gelesen und verarbeitet werden, zudem sind die Auskunftsrechte zu beachten.

Das Bundesdatenschutzgesetz (BDSG) enthält hierzu Vorschriften. Danach darf die Verarbeitung personenbezogener Daten nur erfolgen, wenn ein Gesetz dies erlaubt oder der Betroffene hierin einwilligt (§ 4 Abs. 1 BDSG). Nicht mehr benötigte Daten sind zu löschen, das heisst, die Daten des RFID-Tags, der für Abrechnungszwecke beispielsweise an der Kasse im Supermarkt benötigt wurde, ist dann nach der erfolgten Abrechnung auf Anforderung des Kunden zu löschen (notfalls durch Zerstören des Chips), wenn damit personenbezogene Daten des Kunden verarbeitet werden sollen. Werden beim Betroffenen Daten erhoben, so ist er außerdem über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Datenverarbeitung und die Kategorien der Empfänger der Daten zu unterrichten.

Bei einem Einsatz von aktiven RFID-Tags mit Speicher- und Verarbeitungsmöglichkeiten ist zusätzlich § 6 c BDSG zu beachten. Diese Vorschrift beinhaltet weitergehende Informationspflichten, beispielsweise welche personenbezogene Daten sich auf dem RFID-Tag befinden und welche Verarbeitungsvorgänge ausgelöst werden.

Das bedeutet, dass Betroffene in die Lage versetzt werden müssen, Waren mit RFID-Technik als solche zu erkennen, die Daten auf den RFID-Tags zu lesen, um dann selbst zu entscheiden, ob sie die RFID-Tags nach dem Kauf effektiv löschen bzw. zerstören wollen. Der Kunde ist auf eventuelle Nachteile hinzuweisen, die mit dem Löschen oder Zerstören des Tags verbunden sein können.

Wesentlich ist die Erarbeitung eines **Datenschutz- und Sicherheitskonzeptes** und zwar vor dem Einsatz des RFID-Systems. Die wesentlichen datenschutzrechtlichen Aspekte, die dabei beachtet werden müssen, sind nachfolgend in einem Kriterienkatalog kurz aufgeführt. Der Kriterienkatalog erhebt keinen Anspruch auf Vollständigkeit, da nicht alle Einsatzgebiete abgedeckt werden können. Deshalb ist es ratsam, den betrieblichen Datenschutzbeauftragten einzuschalten oder die zuständige Datenschutzaufsichtsbehörde um Rat zu fragen.

## **8.2 Datenschutz-Kriterienkatalog**

### **8.2.1 Personenbezogene Daten werden verarbeitet**

Die Bestimmungen des Datenschutzes sind zu beachten, wenn mit Hilfe von RFID-Systemen personenbezogene Daten verarbeitet werden. Datenschutzrechtlich spricht man von personenbezogenen Daten, wenn sie sich auf eine bestimmte oder bestimmbar natürliche Person beziehen. Ersteres ist der Fall, wenn die Daten mit dem Namen des Betroffenen verbunden sind oder sich aus dem Inhalt oder dem Zusammenhang der Bezug direkt herleiten lässt. Ist dies nicht der Fall, sind die Daten nur dann personenbezogen, wenn der Betroffene bestimmbar ist. Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle (z. B. mit Hilfe von EDV-Hintergrundsystemen) an.

### **8.2.2 Einsatz von RFID-Tags**

Bei einem Einsatz von RFID-Tags, mit denen personenbezogene Daten gespeichert und verarbeitet werden, ist auf Folgendes zu achten:

#### **a) Umfassende Information des Betroffenen**

Der Betroffene ist darüber zu informieren, dass er einen RFID-Tag mit der Ware/Dienstleistung erworben hat. Darüber hinaus ist der Betroffene umfassend über den Einsatz, Verarbeitungszweck und Inhalt zu informieren. Das schließt auch die EDV-Hintergrundsysteme mit ein, auf denen dann selbst erst die personenbezogene Verarbeitung und Nutzung durchgeführt wird.

#### **b) Offenlegung der Verarbeitungsvorgänge**

Die Verarbeitungsvorgänge, wie mit den personenbezogenen Daten umgegangen wird, sind für die Betroffenen offen zu legen. Bei aktiven RFID-Tags muss der Betroffene die Möglichkeit haben, diese Vorgänge selbst nachprüfen zu können (am besten mittels Leseterminals).

#### **c) Zweckbestimmung**

Die personenbezogenen Daten dürfen nur für die Zwecke verarbeitet und genutzt werden, für die sie auch erhoben wurden und über die der Betroffene informiert ist. Eine Änderung des Zweckes bedarf der vorherigen Information des Betroffenen und gegebenenfalls seiner Einwilligung.

#### **d) Möglichkeiten zur Deaktivierung**

Es muss dem Betroffenen nach Aufklärung über den beabsichtigten Zweck des Einsatzes des RFID-Tags ermöglicht werden, diesen zu deaktivieren und/oder zu löschen oder mit Nul-

len zu überschreiben. Der Betroffene ist auch darüber zu informieren, was mit einer durch ihn ausgelösten Deaktivierung oder Löschung eventuell verbunden ist.

**e) Vertraulichkeit der Datenübertragung zwischen Sender und Empfänger**

Zur Herstellung der Vertraulichkeit der Datenübertragung zwischen Sende- und Empfangsgerät ist es erforderlich, dass die Übertragungstrecke mit einem schwer entschlüsselbaren Schlüssel (mindestens 128 Bit) verschlüsselt wird.

**f) Zugriffskontrolle auf die Daten**

Es ist zu gewährleisten, dass nur die zur Benutzung des RFID-Tags Berechtigten auf die Daten zugreifen können. Fremde dürfen keinen Zugriff bekommen. (Hierunter ist auch das unbemerkte Auslesen der Daten seitens Dritter zu verstehen). Empfohlen wird in diesem Zusammenhang auch eine verschlüsselte Speicherung der Inhaltsdaten.

**g) Löschung der Daten**

Die personenbezogenen Daten dürfen nur so lange gespeichert bleiben, wie es zur Erreichung des angegebenen Zwecks erforderlich ist. Bei der Information an den Betroffenen sind deshalb die Löschfristen mit anzugeben.

**h) Schutz der Daten vor Verlust oder zufälliger Zerstörung**

Bei RFID-Tags, auf denen die personenbezogenen Daten selbst gespeichert und verarbeitet werden, ist sicherzustellen, dass die Daten gegen zufällige Zerstörung oder Verlust geschützt sind (beispielsweise mittels Back-up-Systeme). Die Schaffung einer Back-up-Möglichkeit ist in Abhängigkeit vom Einsatzzweck zu sehen. Sie muss nicht in allen Fällen geschaffen werden; ist aber bei der Planung mit zu berücksichtigen und zu bewerten.

### **8.2.3 Einschaltung des betrieblichen Datenschutzbeauftragten**

Auf jeden Fall sollte vor jedem Einsatz von RFID-Systemen, bei denen personenbezogene Daten gespeichert und/oder verarbeitet werden, der betriebliche Datenschutzbeauftragte informiert und befragt werden. Der betriebliche Datenschutzbeauftragte kann die jeweils zuständige Datenschutzaufsichtsbehörde einschalten.

Bei kleineren Unternehmen, die keinen betrieblichen Datenschutzbeauftragten bestellen müssen, hilft die zuständige Datenschutzaufsichtsbehörde gerne weiter.



## 9 Ein Blick in die Kristallkugel

Von Dr. Michael Groß, Dabac integrierte EDV Organisation GmbH

Folgende Trends in der Entwicklung von RFID-Systemen zeichnen sich ab:

RFID-Systeme werden zunehmend nur eine weitere Technologie zur Datenerzeugung sein und zusammen mit anderen Technologien gemeinsame Infrastrukturkomponenten zur Kommunikation, Verschlüsselung und Verarbeitung verwenden. RFID-Systeme der Zukunft werden damit in einer allgemeinen Datenplattform zusammengeführt, die die Systemintegration über unterschiedlichste Datentypen ermöglicht. Daraus läßt sich ableiten, dass die Middleware der Zukunft nicht für bestimmte Technologien von Datenquellen geeignet sein muß, sondern technologieübergreifende Integrationsaufgaben wahrnehmen wird.

Die Koexistenz verschiedenster Datenströme auf denselben Kommunikationseinrichtungen wird die Anforderungen an Verschlüsselung, Datensicherheit und Zugriffsschutz extrem erhöhen. Die Gefahr des Missbrauchs wird immens ansteigen und Abwehrkonzepte müssen rechtzeitig, zuverlässig und robust entwickelt werden, wie bei allen EDV-Systemen.

Systemintegration wird verstärkt über Unternehmensgrenzen (systemübergreifend: Supply Chain Integration) und benachbarte Prozesse (prozessübergreifend: Gepäckverfolgung und Passagiertracking) stattfinden und damit die Komplexität der entsprechenden Infrastrukturen exponentiell erhöhen.

Die Einbettung von Autoidsystemen in Dinge des täglichen Lebens und Personen (z.B. Smart Shirt, Assisted Living etc.) werden ganz neue Geschäftsmodelle, Prozesse und soziologische Entwicklungen ermöglichen.

Die zunehmende Vernetzung und die Entwicklung von Prozessmodellen, die durch die Verarbeitung von Komplexevents automatisiert werden können, werden immer größere Anforderungen an die verarbeitende Software (Middleware) stellen. Folgende Fragen rücken zunehmend in den Vordergrund:

- Gibt es einen Entwicklungsbedarf in der Verarbeitung von Geschäftstransaktionen, um dieser neuen Herausforderung im RFID-Datenmanagement und diesen neuen Anforderungen gerecht zu werden?
- Gibt es eine Möglichkeit, um Events sowohl als spezifische Vorfälle zu betrachten, als auch als verwandte Vorgänge, die neue Methoden des Datenmanagements auslösen können?
- Können wichtige zusammenhängende Daten hinter jedem Event in Echtzeit bereitgestellt werden, die hochkomplexes Sortieren ermöglichen, um kritische Geschäftsentcheidungspunkte einzuführen oder zu verbessern?

RFID wird kein sofortiger Ersatz für existierende Identifikations- oder Etikettiersysteme.

Obwohl das erklärte Ziel von EPCglobal und ISO die Definition einer einheitlichen Verschlüsselung ist, ist es wahrscheinlich, dass in einer globalen Versorgungskette mehrere Nummerierungssysteme nebeneinander existieren.

Die Fähigkeit die Kernverarbeitung zu definieren und zu differenzieren, basierend auf Verschlüsselung und Kennzeichnung, ermöglicht eine Verwendung der RFID-Middleware als Mittel, alle automatischen Identifikationssysteme und Events in einer einzigen Schicht zu integrieren. Dies bedeutet, dass die Middleware alle redundanten Daten aus dem System filtert. Durch Plug&Play ist es möglich, definierte RFID-Systeme sofort zu integrieren und in bestehende Applikationen zu implementieren.

Die zentrale Rolle der Middleware ist hierbei, Daten an jede Software in reduzierter Form über eine Direktverbindung zu schicken.

### **Skalierbarkeit & Dezentralisierung**

Mit dem Wachstum von RFID steigt die Größe der benötigten Infrastruktur (Schreiben, Lesen) und das Volumen von Tag-Events exponentiell an. RFID-Middleware und die Architektur der Eventserver muss dafür ausgelegt sein, auch große Projekte der Zukunft zu managen. Dazu müssen sie Folgendes unterstützen:

- Verteilter Einsatz von Collectors- und Query-Adaptern
- Verarbeitung gesammelter Eventdaten in Form von kleinstmöglichen Eventprozessen, die nur in bestimmten Szenarien benötigt werden (Eventtyp, Produkt, Tagtyp)
- Hochskalierbares Caching von kontextbezogenen Informationen
- Optimierte Event Query Language für das Suchen von Tag-Events, Transformieren und Wiederauffinden bestehender Eventdaten
- Eine dahinterliegende objektorientierte Datenbank kann die Eventdaten speichern und abfragen, – entweder als unverarbeitetes Event oder erweitert für eine Unterstützung in einer Serie von relationalen Datenbanken.

## 10 Zusammenfassung

Die Optimierung eines RFID-Systems erfordert ein breites Know-how über die Anwendung, Datenschnittstellen, die Ausführungsformen der Transponder und der Lesegeräte, sowie der elektromagnetischen Verträglichkeit (EMV/EMC). Vor allem im industriellen Umfeld sind RFID-Systeme noch keine „plug and play“-Lösung. Lassen Sie sich kompetent beraten von einem Systemintegrator, der auch über das richtige Knowhow im Bereich der RFID-Hardware verfügt.

## 11 Literatur

[Computer Zeitung, Nr.10/ 6.März 2006]

Computer Zeitung – Die Wochenzeitung für die Informationsgesellschaft: RFID-Integration lenkt Automatisierungsgrad

[Finkenzeller, 2002]:

Finkenzeller, Klaus 2006. RFID-Handbuch, Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. 4. Auflage, München: Carl-Hanser-Verlag, ISBN 3-446-22071-2, [www.rfid-handbook.de](http://www.rfid-handbook.de)

[Fleisch et al, 2005]:

Fleisch, Elgar; Mattern, Friedemann (Hg.) 2005. Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Berlin: Springer.

[Heinrich, 2005]

Heinrich, Claus 2005. RFID and Beyond – Growing Your Business Through Real World Awareness. Indianapolis: Wiley Publishing.

[Kern, 2006]

Kern, Christian 2006. Anwendung von RFID-Systemen. Berlin: Springer.

[Luckham, Wesley 2002]

David Luckham, Addison Wesley: The Power of Events

[Palmer, August 2004]:

Mark Palmer: The 7 Principles of RFID Data Management (Enterprise Systems Journal)

Mark Palmer: Build an Effective RFID Architecture (RFID Journal)

[van Steen et al 1998]:

M. van Steen, A.S. Tanenbaum, I. Kuz, and H.J. Sips: A Scalable Middleware Solution for Advanced Wide-Area Web Services, Proc. Middleware '98, The Lake District, UK, Sept. 1998

[Sweeney, 2006]

Sweeney, Patrick J. 2006. RFID für Dummies. 1. Auflage, Weinheim: Wiley-VCH Verlag GmbH & Co. KG, ISBN-13 978-3-527-70263-3

[B. Trigg, März 2005]

John B. Trigg: Progress for RFID – An Architectural Overview

## Organisationen

### [AIM-D e.V.]

AIM-D e. V. - Verband für Automatische Datenerfassung, Identifikation und Mobilität -  
Deutschland - Österreich – Schweiz - [www.aim-d.de](http://www.aim-d.de)

### [EPC Global]

EPC Global – [www.epcglobal.com](http://www.epcglobal.com)

### [VDEB]

VDEB - Verband der EDV-Software- und -Beratungsunternehmen e.V. -  
<http://www.vdeb.de/>

## Medien

### [ident]

ident - Das führende Anwendermagazin für Automatische Datenerfassung & Identifikation  
ident Verlag & Service GmbH, Rödermark - ISSN 1432-3559 - [www.ident.de](http://www.ident.de)

### [IT Backbones]

IT Backbones – RFID Resellers - [www.rfidreseller.com](http://www.rfidreseller.com)

### [RFID-im-Blick]

Das Medium für kontaktlosen Datentransfer  
Verlag & Freie Medien Anja van Bocxlaer, Amelinghausen - ISSN 1860-5907 [www.rfid-im-blick.de](http://www.rfid-im-blick.de)

### [Wikipedia]

Wikipedia – Die freie Enzyklopädie - [www.Wikipedia.de](http://www.Wikipedia.de)

## Anlage 1

Einige Kriterien für die RFID-Hardware (Physik und Technik)

<b>Frequenzen</b>				
125 kHz				
13,56 MHz				
868 MHz			aktiv o. passiv	
2,4 GHz				
<b>Leistungsgrenzen</b>				
Max. Leseabstand in cm:				
Max. Schreibabstand in cm:				
<b>Umgebungsparameter</b>				
Betriebstemperatur				
Lagertemperatur				
Säure/Laugen				
Feuchtigkeit / IP				
Explosionsgefährdet (Ex)				
Mechanische Belastung				
<b>Erfassungsart</b>				
Einzel				
Pulk			# pro sek.	
Max. Geschwindigkeit des Objektes:				
Zum Zeitpunkt der Ablesung in m/s				
Zum Zeitpunkt des Schreibens in m/s				
<b>Transponder</b>				
Bauform/Größe				
Read-only oder Read-/write			Speichergroße	
Lebensdauer				
Standards				
<b>Stationäre Schreib-/Lesegeräte</b>				
Schnittstelle (RS232, PROFIBUS, TCP/IP)				
Infrastrukturanschluss (max.# der Geräte pro Anlage)				
Austauschbarkeit				
Externe Antennen				
Max. Leitungslänge zwischen RFID-Gerät und Rechner/EDV				
Versorgungsspannung				
<b>Mobile Geräte</b>				
Betriebssystem				
Betriebszeit				
Datensicherheit				
Kommunikationstechnik				
Lokale Funktionalität				
Zugriffssicherheit				

## Anlage 2

### Kriterien für eine RFID-Middleware

<b>Allgemeine Anforderungen</b>	<b>Erfüllt</b>	<b>Bemerkung</b>
Abstraktionsschicht für die RFID-Peripherie (Dynamic Nameservice)		
Verwaltung der angeschlossenen Geräte in Hierarchien und Domänen		
Verschlüsselung der Datenströme (Events)		
Sicherheit mit Zugriffsrechten auf System- und Nutzerebenen		
<b>Standards</b>		
Unterstützung der EPC Global Standards I		
Unterstützung der EPC Global Standards II		
Unterstützung applikationspezifischer Standards (z.B. Eldat)		
Andere		
<b>Datenintegrität, Datenschutz und Fehlertoleranz</b>		
Domänen innerhalb der Sicherheitskonzepte		
<b>Vertraulichkeit</b>		
Nur autorisierte Systemteilnehmer (Nutzer oder Systeme oder Services) erhalten Zugriff auf Komponenten, Dienste und Daten		
<b>Integrität</b>		
Die Modifikation von Daten ist nur autorisierten Systemteilnehmern gestattet und möglich		
<b>Verantwortlichkeit</b>		
Das System ermöglicht Systemteilnehmern entsprechende Sicherheitsstandards einzurichten, zu überwachen und zu verwalten		
<b>Verfügbarkeit</b>		
Single-Sign-On (Das System darf berechtigten Systemteilnehmern den Zugang nicht verweigern.)		
<b>Funktionen zum Ausschleusen von fehlerhaften Nachrichten</b>		
Es müssen Korrekturfunktionen für fehlerhafte Nachrichten verfügbar sein.		
Manuelle Korrekturmöglichkeiten		
Automatische Korrekturfunktionen, regelbasiert		
Fehlerbedingungen definierbar (Errorlevel)		
Errorlevelabhängige Weiterverarbeitung		
Transaktionssicherheit zwischen Dateneingang und Auslieferung		
Garantierte Auslieferung (Persistenz)		
Variable Persistenz (Zeitdauer, Eventtyp, Scenario)		
Vollständige Auslieferung		
Garantierte Reihenfolge der Auslieferung gemäß Dateneingang		
<b>Realtimeprocessing</b>		
Eventcaching (Speichergröße _____)		
Direkte High-Speed-Anschlussmöglichkeit für RFID-Reader (Anzahl Events pro sec: _____)		

High Performance in Memory Caching (Anzahl Events pro sec: _____, max. Anzahl Reader: _____)		
<b>Architekturanforderungen</b>		
Dynamisches Routing		
Redundante Nachrichtenrouten zu einem zentralen Middleware Broker oder einem Cluster von Brokern zur Vermeidung von Verfügbarkeitsproblemen der Middleware		
Schichtenarchitektur mit verschiedenen Leistungsstufen		
Opensource Plattformen (Linux)		
Windows Plattformen		
Unix Plattformen (Solaris, AIX, HPUX)		
<b>Hardware und betriebssystemnahe Komponenten</b>		
Systemverfügbarkeit und Failover Strategien		
24/7 Verfügbarkeit der Systeme auf dem zentralen Rechner des Middlewarebrokers		
Failover: Zentraleinheit nicht verfügbar (locale Zwischenpufferung)		
System Management (lokales Repository)		
Speicherkapazitäten erschöpft (Ressourcenmonitoring)		
Skalierbarkeit der Speichermedien (Hot extension)		
Steigerungsmöglichkeiten der Datenverarbeitungsgeschwindigkeit durch die Integration /Inbetriebnahme neuer Funktionsbereiche		
Verteilung der Funktionseinheiten auf mehrere Systeme		
Verfügbare Bandbreite der Kommunikationswege wird überwacht		
Skalierbarkeit der Verbindungen		
Systemstatusmeldung: Verbindung nicht verfügbar.		
<b>Logikanforderungen</b>		
Universelle standardisierte Adapter		
Standardanschlussmöglichkeiten für WMS (welche)		
Standardanschlussmöglichkeiten für MES (welche)		
Standardanschlussmöglichkeiten für ERPS (welche)		
Sonstige Anschlussmöglichkeiten (welche)		
Validierung nach Bytemuster		
Validierung nach Inhalt		
Validierung nach TagID-Raum		
Definition von Validierungsregeln		
Ebenen der Validierungsregeln (Reihenfolge)		
Echtzeitvalidierung (sofortige Korrekturmaßnahme im Eventcache)		
Korrekturmaßnahme in späteren Prozessschritten		
Korrekturmaßnahme in künftigen Wiederholungen automatisierbar		
Regelarbeitung mit verschiedenen möglichen Strategien		
Realtime (im Eventcache)		
Regeln nach Eventcache abarbeitbar		
Regeln im Eventarchiv abarbeitbar		
Nachrichten bei Dateneingang auf Vollständigkeit prüfen		
Beispiel: Anhand von Attributlisten automatisch Eventtypen überprüfen, ob alle notwendigen Daten enthalten sind. Ist dies nicht der Fall, den Event automatisch an eine Korrekturstelle weiterleiten.		



Nachrichten im Eventcache auf Vollständigkeit prüfen		
Komprimierung gleicher Nachrichten zu Sammelevents		
Dubletten parametrisierbar herausfiltern		
Beispiel: Bleibt ein Transponder im Bereich der Lese/Schreibeinheit während mehrerer Lese/Schreibzyklen stehen, so muß die Middleware entstehende Mehrfachevents herausfiltern.		
<b>Archivierung</b>		
Komprimierte vollständige Speicherung aller Ereignisse		
Recherchegrundlage (Prozessanalyse / Überwachung, Daten in Datenbank verfügbar)		
Mehrstufiges Archivieren (Realtimebestände, Recherchebestände, Historienbestände)		
<b>Formatmapping: Unterstützung verschiedener Ausgabeformate</b>		
Toolbox zur Generierung von Inhouseformaten		
ASCII auf XML		
Eldat		
Umsetzung aller RFID-Events auf Standardnachrichtenformate		
EDI		
<b>Prozesssteuerung</b>		
Events auf mehrere Zielsysteme		
Beispiel: Eine Palette wird beim Wareneingang eines Warenlagers gescannt, das Ereignis wird an das Warenhausmanagement geschickt als Wareneingang, an das Logistiksystem als erfolgte Auslieferung, an das Lieferantensystem als erfolgte Auslieferung		
mehrere Events zusammengefasst auf ein oder mehrere Zielsysteme		
Beispiel: Bei einer Wareneingangskontrolle von Mehrwegbehältern wird eine Pulkerfassung gemacht und neben dem Palettentag auch alle Tags der einzelnen Behälter erfasst. Diese Daten werden zusammengefasst in einem Event an das entsprechende Hauptsystem geschickt und nicht jedes Lesereignis als eigenes Event.		
Komplexevents verarbeiten		
Events in eine Reihenfolge stellen und Abweichungen erkennen		
Businessregeln erstellen, verwalten und abarbeiten (Definitionsumgebung)		
Szenarien definieren und verwalten		
Bi-direktionale Kommunikation		
Lese- und Schreibvorgänge unterstützen		
Schreibvorgänge validieren (RAW Read-after-Write Verification)		
<b>RFID-Management</b>		
BI-Engine für Auswertungen, Analysen und Statistiken		
Mustererkennung, dynamische und persistente Abfragen zur Echtzeit-Analyse		

Monitoring: Engpassanalyse/-überwachung (Dashboard, Global Alerts)		
Systemüberwachung durch Statuskontrolle aller Komponenten		
Grafischer Systemmonitor		
<b>Die Middleware muss einen zentralen Managementservice enthalten:</b>		
dezentrale Applikationskomponenten in Peripheriegeräten verwalten		
Fehleranalysen durchführen		
Softwareaktualisierungen (Updates von Firmware) zentral durchführen		

## Anlage 3

### Implementierte Lösungen

#### **Kennzeichnung von Formen**

Eine Firma fertigt künstliche Zähne für die Erstellung von Teil- und Gesamtprothesen. Hierbei ist sicherzustellen, dass die unteren Formteile immer nur mit dem passenden oberen Formteil abgedeckt werden. Darüber hinaus sind die Reinigungsvorgänge und Standzeiten zu dokumentieren. Die Markierung der einzelnen Formteile mit Transpondern erlaubt eine schnelle, automatische und unverwechselbare Identifikation auch dann, wenn der Datenträger z. B. durch überschüssigen Kunststoff abgedeckt wurde. Die hier eingesetzten Transponder überstehen auch die verschiedenen Temperatur- und Druckwechsel, die während des Fertigungsprozesses auftreten.

#### **Temporäre Kennzeichnung von Paletten**

Ein Traditionsunternehmen aus dem Westerwald verarbeitet hochwertige Gläser für Markengetränke. Um den heutigen Kundenwünschen nachzukommen und den aktuellen Marktentwicklungen und Trends der Getränkebranche gerecht zu werden, muss das Sortiment an Getränkegläsern ständig diversifiziert und ergänzt werden. Zur Erhöhung der Lagerqualität und zur Verkürzung der Durchlaufzeiten wurde ein Hochregallager errichtet, das direkt mit der Produktion verbunden ist. Die Rohware – Gläser ohne Kennzeichnung – wird grundsätzlich auf Europaletten in Schrumpf- oder Wickelfolie angeliefert. Beim Wareneingang werden diese Paletten mit einem Disk-Transponder gekennzeichnet, der zur besseren Erkennung und Handhabung in einen roten Kunststoffclip integriert wurde. Durch den Einsatz verschiedener, schnittstellenkompatibler Antennensysteme in der Förderlinie ist es möglich, mit nur einem Transponder pro Palette zu arbeiten. Dieser wird sowohl in der Längs- als auch in der Querförderung erkannt. Der Transponder wird bei der Kommissionierung entfernt und zur Wiederverwendung an den Wareneingang zurückgeführt.

#### **Prozesssteuerung in der Automobilindustrie**

In einem sehr frühen Fertigungsstadium wird jede Rohkarosserie mit einem Transponder ausgestattet, der am Fahrzeug verbleibt. Über die unverwechselbare Codierung wird der Fertigungsprozess gesteuert (Zuführung der Baugruppen, Farbwahl, Motorvariante etc.). Später kann der Transpondercode für die Identifikation des Fahrzeuges in den Servicestützpunkten, z.B. zur zweifelsfreien Information über die eingesetzten Baugruppenversionen für die Ersatzteilbeschaffung, genutzt werden.

#### **Baumkennzeichnung**

Alle Bäume einer Stadt müssen zweimal pro Jahr auf Ihren Zustand hin begutachtet werden. Daraufhin sind entsprechende Arbeitsaufträge zu erstellen. Als weitere Nutzung kann die Bodenanalyse eines jeden Baumes in einem Bewässerungssystem gespeichert werden. Das Bewässerungssystem mixt dann einen speziellen "Cocktail" aus Wasser, Dünger etc. für jeden Baum.

### **Müllmanagement**

Alle Müllgefäße werden mit einem Transponder gekennzeichnet. Eine Leseeinrichtung befindet sich auf dem Müllsammelfahrzeug. Das Gefäß wird bei jeder Leerung registriert, und dadurch kann aufgezählt werden, wie oft pro Haushalt das Gefäß geleert wurde. Mehr Genauigkeit, ohne eine Änderung der Abfuhrzyklen, ermöglicht die Installation eines Wiege- oder Volumenmesssystems auf dem Müllsammelfahrzeug. Dieses wiegt die Müllgefäße bei jeder Leerung bzw. erfasst deren Füllstand.

### **Probenbehälterkennzeichnung**

Bei der Anlieferung von Zuckerrüben werden an unterschiedlichen Standorten Proben entnommen, die in Plastikkisten zur Zentralanalyse in ein Labor transportiert werden. Die Probenbehälter sind mit einem beschreibbaren Transponder markiert. Die entsprechenden Informationen wie Datum, Probennummer, Probenart etc. werden im Transponder abgelegt. Dadurch ist die zweifelsfreie Zuordnung des ermittelten Zuckergehaltes (maßgeblich für Vergütung) zum Anlieferer möglich.

## Über den VDEB – Der Verband für den IT-Mittelstand

Der Verband der EDV-Software- und -Beratungsunternehmen e.V. (VDEB) vertritt die Interessen des IT-Mittelstands, speziell der kleinen und mittleren Softwarehersteller und EDV-Beratungsunternehmen in Deutschland. Ziel der Arbeit des Verbandes ist die verstärkte Zusammenarbeit der mittelständischen IT-Unternehmen. Die Interessen der Mitglieder werden durch eine gemeinsame Fach- und Öffentlichkeitsarbeit zum Ausdruck gebracht. Der VDEB ist beim Deutschen Bundestag akkreditiert.

Unsere Mitglieder sind mittelständische Soft- und Hardwarehersteller sowie IT-Beratungsunternehmen. Die EDV-Berater, die sich dem VDEB angeschlossen haben, sind wichtige Mittler zwischen IT-Anbietern und Anwendern. Bei uns engagieren sich sowohl Selbständige als auch Unternehmen mit mehreren hundert Mitarbeitern.

Der VDEB bündelt das Know-how und die Kompetenzen seiner Mitglieder. Das Netzwerk untereinander ist eng geknüpft. Sie profitieren vom gegenseitigen Informationsaustausch und von der Zusammenarbeit mit anderen. Stetig werden Anfragen zu IT-Projekten aus der Wirtschaft an unsere Mitglieder vermittelt. Der Verband unterstützt Sie zudem in der täglichen Arbeit und bei der Verfolgung langfristiger Interessen.

Der IT-Mittelstand in Deutschland braucht eine eigene Stimme. Dafür setzt sich der VDEB als IT-Fachverband ein. Der VDEB ist unabhängig von der IT-Industrie, politischen Parteien und staatlichen Einrichtungen. Wir leben das Prinzip "Mittelstand für den Mittelstand". Daher sind im VDEB auch nur Unternehmen mit bis zu 750 Mitarbeitern stimmberechtigt.

Wir brauchen Ihre Unterstützung, denn der VDEB ist Ihre Vertretung. Nur mit anderen mittelständischen Unternehmen zusammen können Sie wirklich Interessen entwickeln und vertreten. Und nur ein Verband wie der VDEB kann diese Interessen wirkungsvoll umsetzen – in der Öffentlichkeit, beim Gesetzgeber, aber auch in gemeinsamen Marketing-Aktionen.

weitere Informationen:

<http://www.vdeb.de/>

Ihr Ansprechpartner beim VDEB

Herr Marc Houben,  
Leiter der Geschäftsstelle des VDEB

E-Mail: [mhouben@vdeb.de](mailto:mhouben@vdeb.de)

## Über AIM Deutschland

AIM Deutschland e.V., Lampertheim, ist ein Industrieverband für Automatische Identifikation (Auto-ID), Datenerfassung und Mobile Datenkommunikation. AIM verfolgt das Ziel, die Marktausbreitung der damit verbundenen Technologien und Verfahren zu fördern. AIM-D ist die deutsche Sektion von AIM Global und repräsentiert über 120 Mitglieder in Deutschland, Österreich und der Schweiz. Weiterhin sind 14 deutsche Universitäts- und Forschungsinstitute als Allianzpartner mit AIM-D verbunden. AIM Mitglieder sind Unternehmen aller Größenordnungen, die Technologien, Systeme und Dienstleistungen anbieten, die der Objekt-Identifikation sowie der mobilen Datenerfassung und -kommunikation dienen. Technologien wie RFID, ein- oder zweidimensionaler Barcode und andere werden dabei gleichermaßen unterstützt.

weitere Informationen:

<http://www.aim-d.de/>

<http://www.kompetenzzentrum-autoid.de/>

Ihr Ansprechpartnern beim AIM Deutschland

Herr Wolf-Ruediger Hansen,  
Geschäftsführer

E-Mail: [wolf-ruediger.hansen@aim-d.de](mailto:wolf-ruediger.hansen@aim-d.de)