



■ **White Paper RFID Technologie, Systeme und Anwendungen**

Ein Überblick für Unternehmen, die ihre IT-Systeme direkt mit der „realen“ Welt verbinden möchten und dafür den Einsatz von RFID-Technologie planen

■ Impressum

Herausgeber:

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 – 0

Fax: 030/27 576 – 400

bitkom@bitkom.org

www.bitkom.org

Eine Arbeit der Projektgruppe RFID (Radio Frequency Identification)

Herausgegeben im August 2005

Ansprechpartner:

Dr. Birgit Heinz, BITKOM e.V.

Tel: +49 (0)30 / 27576 – 243

E-Mail: b.heinz@bitkom.org

Inhaltsverzeichnis

1	Vorwort.....	5
2	Einleitung	7
3	Management-Architektur für RFID-Lösungen	9
4	RFID-System-Architektur und Standards.....	11
4.1	Markttrends und Nutzungsformen	11
4.2	Architektur von RFID-Systemen	12
4.3	Das Internet der Dinge aus EPCglobal-Sicht	15
4.4	RFID-Standards.....	19
4.5	Ausblick	20
5	RFID-System-Komponenten.....	21
5.1	RFID-Tags: Chip und Antenne	21
5.1.1	Aufbau eines RFID-Tags bzw. -Transponders	21
5.1.2	Tag-Antenne.....	23
5.2	Air Interface und Pulkerfassung	24
5.3	Reader und Antenne	26
5.3.1	Reader-Aufbau	26
5.3.2	Reader-Antenne	28
6	IT-Infrastruktur	30
6.1	Middleware und serviceorientierte Architektur (SOA).....	30
6.2	Schichtenmodell für das Real-time Enterprise	31
6.3	Event-Architektur	32
6.4	Das Middleware-Konzept Savant von EPCglobal	35
6.5	Datenbanken	36
7	RFID-Sicherheitsaspekte	38
8	Anwendungsbeispiele	41
8.1	Fallstudie: Logistik-Prozesse bei Hewlett-Packard GmbH	41
8.2	Fallstudie: Flexible Produktionsprozesse in der Automobilfertigung bei BMW	42
8.3	Fallstudie: Mobile Wartungslösung bei Fraport AG	43
8.4	Fallstudie: RFID-Flächen-Rollout in der Logistik bei Metro AG	45
9	Glossar.....	48
10	Weitere Informationsquellen	50

Abbildungen

Abbildung 1: Schichten und Komponenten einer RFID-Management-Architektur.....	9
Abbildung 2: Systemarchitektur für RFID-Anwendungen.....	12
Abbildung 3: Die wichtigsten RFID-Frequenzbereiche und ihre Anwendungen	14
Abbildung 4: Beispiel und Struktur einer EPC-Nummer.....	15
Abbildung 5: Struktur des EPCglobal-Netzwerkes im Vergleich zum Web.....	16
Abbildung 6: Fragen, die zukünftig über das EPCglobal-Netzwerk beantwortet werden.....	17
Abbildung 7: EPCIS-Service von Gillette.....	18
Abbildung 8: Standards des EPCglobal-Netzwerkes	19
Abbildung 9: ISO- und EPCglobal-Standards	20
Abbildung 10: Inlays für RFID-Tags mit 13,56 MHz (HF).....	21
Abbildung 11: Inlays für RFID-Tags mit 868 MHz (UHF)	22
Abbildung 12: Reflexionen im Bereich der Reader-Antenne.....	24
Abbildung 13: Das Anti-Kollisions-Protokoll des RFID-Readers	25
Abbildung 14: Typisches Anschluss-Schema eines Readers mit RFID-Antennen	27
Abbildung 15: Pulk-Erkennung und Multi-Tag-Handling	28
Abbildung 16: Überlagerung der Felder von RFID-Readern	28
Abbildung 17: Reader-Antenne mit Antennen-Array und Feldregionen.....	29
Abbildung 18: Ebenen einer Software-Architektur für das Real-time Enterprise	31
Abbildung 19: Implementierung der Global Data Synchronization (GDS)	32
Abbildung 20: Auto-ID-Event-Architektur.....	33
Abbildung 21: Event-Informationen in einer Automotive-Prozesskette	35
Abbildung 22: EPCglobal-orientierte RFID-Anwendungs- und Kommunikationsstruktur.....	36
Abbildung 23: Warenausgang mit RFID-Antennen im HP-Werk Chester	41
Abbildung 24: Prinzipielle Architektur für RFID in der industriellen Fertigung.....	42
Abbildung 25: RFID-Transponder mit Datenspeicher an der Karosserieplatte bei BMW	43
Abbildung 26: Papierloses mit RFID optimiertes Wartungsszenario am Flughafen Frankfurt	44
Abbildung 27: Schichtenmodell einer umfassenden Auto-ID-Anwendungsarchitektur	46
Abbildung 28: Konfiguration der RFID-Antennen an den Toren im Metro-Lager.....	47

1 Vorwort



Sehr geehrte Leserinnen und Leser,

ich möchte mit Ihnen eine kurze Zeitreise wagen – und zwar rund 2400 Jahre zurück ins griechische Abdera. Dort stellt soeben der Philosoph Demokrit seine erkenntnistheoretischen Überlegungen an.

Nach seiner Überzeugung gehen von den Dingen dieser Welt Bildchen aus, so genannte Eidola – heute sagen wir Idole, oder kurz: IDs. Erst durch die Wahrnehmung dieser Idole seien die Menschen in der Lage, den Dingen Eigenschaften und Wechselwirkungen zuzuordnen. So entstehen überhaupt Denken und Erkenntnis. Mit anderen Worten: Ohne ID – also ohne die Bildchen, die von den Dingen ausgehen – kein Denken.

Meiner Meinung nach beschreibt Demokrit ziemlich genau, was RFID eigentlich anstrebt: Die Dinge und Waren geben Informationen über ihre Herkunft, ihre Bestimmung, ihren Status preis – eben ihre Identität, ihre ID. Und dank dieser Informationen können Menschen,

Maschinen und Transportmittel erkennen, was mit den Dingen und Waren zu geschehen hat. Heute suchen sich im Internet die virtuellen Bits- und Bytes auf Datenleitungen ihren eigenen Weg zum anderen Ende des World Wide Web. Morgen suchen sich im „Internet der Dinge“, wie RFID auch genannt wird, reale Container, Paletten und Päckchen auf Frachtschiffen und LKWs ihren Weg zum anderen Ende der Welt.

Schon heute bezahlen Touristen per RFID-Chip ihre Kurtaxe, werden Skipässe, Parkscheine und – im kommenden Jahr – die Eintrittskarten zur Fußball-WM damit ausgestattet und Bälle werden selbst wissen, dass sie ein Tor gemacht haben. Doch trotz dieser Allgegenwart dieser faszinierenden Technologie gibt es noch großen Erklärungs- und Wissensnachholbedarf in Staat, Wirtschaft und Gesellschaft. Nur wenige wissen, was Radio-Frequency Identification eigentlich bedeutet, was diese Technologie leistet und was sie alles (noch) nicht leisten kann. Dementsprechend gilt mein großer Dank der Projektgruppe innerhalb unseres Verbandes: Sie hat sich – aus den verschiedensten Blickwinkeln – diesem Thema genähert und erleichtert damit auch kleinen Unternehmen sich mit RFID-Unterstützung richtig in die Wertschöpfungskette zum Beispiel von Handel und Logistik einzuhängen.

Die konkreten Fallbeispiele zeigen, dass RFID den Anwendern konkreten Nutzen bringen kann. Laut dem Düsseldorfer Handelskonzern Metro könnten in Zukunft dank der Chips bis zu 20 Prozent der Kosten eingespart werden. Doch, und dies ist mir als Mittelständler besonders wichtig, RFID ist auch eine Öffnung intelligenter Logistik für alle Marktteilnehmer. RFID senkt die wirtschaftlichen Zugangsschranken und lässt eben auch mittelständische Firmen an allen Vorteilen einer effizienten Logistik teilhaben. Somit können sich bald nicht nur Großunternehmen aufwändige Waren-Verfolgungssysteme leisten. Allein die Warenlaufzeiten zu verkürzen, senkt die Kapitalbindung für Hersteller enorm – gerade für Mittelständler ein wichtiger „Zu-Gewinn“. Es ist also nicht überraschend, dass RFID vor allem im Zusammenhang mit Transport und Lagerhaltung diskutiert wird.

Die RFID-Technologie ist eine großartige Chance für Deutschland. Wir sind in der Handhabung, Entwicklung und Forschung ganz weit vorne, wenn nicht sogar Weltklasse. Der BITKOM fordert seit längerem die Politik, die Wirtschaft und die Gesellschaft auf, RFID zu unterstützen. Wichtig ist uns, dass diese Technologie nicht durch eine typisch deutsche

Regelungswut erstickt wird und wir wieder einmal – denken Sie nur an das PAL-Fernsehen oder mp3 – Technologien erfinden und ihre Verwertung dem Ausland überlassen.

RFID wird unsere Arbeitswelt, unsere Umwelt verbessern. Da bin ich mir trotz der Bedenken einiger Datenschützer, die eine zusätzliche Form der Überwachung befürchten, ganz sicher. Bislang gab es eine Lücke zwischen der realen Welt der physikalischen Dinge und Personen auf der einen Seite und der virtuellen Welt der Informationen. RFID schließt diese Lücke!

Wenn der Philosoph Demokrit vor 2400 Jahren sagte: „Ohne ID kein Denken“, so behaupte ich „Ohne RFID kein erfolgreicher Handel.“

Vielen Dank

BITKOM Vizepräsident Heinz Paul Bonn

2 Einleitung

Die Abkürzung RFID (Radiofrequenz-Identifikation) ist eine Art Leitbegriff für Systemlösungen für globales und lokales Tracking und Tracing mit Hilfe von Funketiketten (RFID-Tags). RFID gehört zusammen mit anderen Technologien zu den Auto-ID-Verfahren, also Verfahren zur automatischen Identifikation von Objekten. Es schließt die Lücken zu IT-Systemen, die bisher durch manuelle Dateneingaben überbrückt werden mussten.

Der Trend, Auto-ID-Verfahren einzusetzen, breitet sich besonders in den Lieferketten (Supply Chains) der Unternehmen aus. Dabei überschreiten RFID-Lösungen meist die Grenzen einzelner Unternehmen und müssen in die umfassenden IT-Systeme integriert werden. Deswegen positionieren sich fast alle IT-Anbieter, egal ob Produkt- oder Dienstleistungsanbieter, zu dem Thema.

Bürger nutzen bereits RFID beispielsweise für die Zentralverriegelung ihrer Autos und Skipässe. Auch Reisepässe und Gesundheitskarten werden zukünftig mit RFID-Funktionen ausgestattet. Bis Yoghurt-Becher und andere kleinere Verbraucherartikel in Supermärkten mit RFID-Etiketten versehen sein werden, wird es allerdings noch Jahre dauern – sofern es überhaupt soweit kommt.

Realität geworden sind RFID-Etiketten z.B. für das Management von Behältern in der Produktionslogistik bei Automobilherstellern sowie für die Kennzeichnung von Paletten und Kartons in der Handelslogistik. Diese industriellen Einsatzbereiche, die bereits solche Prozesse maßgeblich verbessert haben, kommen in der öffentlichen Diskussion oft zu kurz, weil hier meist über das Tagging von Konsumartikeln gesprochen wird. Die damit verbundenen Bedrohungsszenarien für den Bürger führen zu emotionalen Wogen, obwohl eine Etikettierung dieser Artikel noch gar nicht aktuell ist (s.o.) Natürlich sind Unternehmen, die RFID-Lösungen einsetzen, gefordert, das Bedürfnis der Bürger auf Schutz ihrer Privatsphäre zu respektieren und so das informationelle Selbstbestimmungsrecht der Bürger zu respektieren.

Dieses White Paper bietet einen Überblick über zahlreiche anwendungsbezogene und technische Aspekte von RFID-Systemen. Es zeigt, dass auch in dem wettbewerbsintensiven IT-Markt grundsätzliche Strukturen dargestellt werden können, auf die sich die verschiedenen Anbieter einigen können. Das ist hilfreich für die Unternehmen, die RFID-Verfahren nutzen möchten und dafür Komponenten unterschiedlicher Anbieter zu umfassenden, stabilen und unternehmensübergreifenden IT-Infrastrukturen verbinden müssen. Dies kann mit der Arbeit eines Architekten verglichen werden, der die Pläne zeichnet, die einzelnen Gewerke werden jedoch von unterschiedlichen Fachleuten erstellt.

Mehr als zehn Autoren haben zu diesem Papier beigetragen. Sie gehören zu ganz verschiedenen Unternehmen des ITK-Sektors, die im Markt sowohl als Partner als auch als Konkurrenten auftreten. Gleichwohl sind sie sich in der hier gegebenen Darstellung und dem Ziel dieses White Papers einig. Die technischen Ausführungen sind auf einem Verständnisniveau gehalten, das Unternehmensleitern – besonders Mittelständlern – oder Managern in Fachabteilungen die Möglichkeit gibt, die Zusammenhänge von RFID-Systemen zu verstehen, auch wenn sie keine IT-Fachleute oder Spezialisten für elektrodynamische Antennenfelder sind. Ihnen soll geholfen werden, die Brücke von den fachlichen Anforderungen, die durch die gewünschten Geschäftsprozesse vorgegeben werden, zu den IT-Systemen zu schlagen, die für die Unterstützung von RFID-Lösungen beschafft, entwickelt oder integriert werden müssen. Schließlich werden im Kapitel „Anwendungsbeispiele“ RFID-Lösungen beschrieben, die sich in der industriellen Praxis bereits bewährt haben.

Dem interessierten Leser werden zusätzliche Literaturangaben und Adressen im Internet zur eigenen Recherche geboten. Die Themen Auto-ID und RFID entwickeln sich weltweit sehr

dynamisch, so dass täglich neue Informationen besonders im Internet erscheinen. Es lohnt sich, diese zu verfolgen.

Auch wenn es in Bezug auf die bevorstehende Ausbreitung von Auto-ID-Verfahren viele skeptische Stimmen gibt, so überwiegt doch der Tenor, dass diese Verfahren einen ähnlichen Siegeszug antreten werden wie der Barcode. Besonders Unternehmen, die in unternehmensübergreifende Lieferketten eingebunden sind, sollten sich deswegen intensiv mit diesem Thema befassen.

Das vorliegende White Paper ist ein Gemeinschaftswerk der BITKOM-Projektgruppe RFID, das im ersten Halbjahr 2005 erstellt wurde.

Berlin, den 30. Juli 2005

3 Management-Architektur für RFID-Lösungen

Die störungsfreie Funktion von Geschäftsanwendungen ist eine Überlebensfrage für Unternehmen. Ausfälle von IT-Systemen beeinträchtigen nicht nur das eigene Unternehmen, sondern können auch die Beziehungen zu Kunden und Geschäftspartnern schmerzhaft belasten. Deshalb ist es wichtig, dass unternehmensübergreifende Geschäftsprozesse zuverlässig strukturiert werden. Dies erfordert eine durchgehende Management-Infrastruktur, die von den strategischen Zielen eines Unternehmens bis hin zu einzelnen Komponenten der IT-Systeme zu gestalten ist. Gerade Auto-ID- und RFID-Lösungen müssen sachgerecht in ein solches Umfeld eingebettet werden. Verantwortlichkeiten müssen klar zugeordnet und Schnittstellen genau definiert werden. Das steigert die Transparenz und senkt die Kosten.

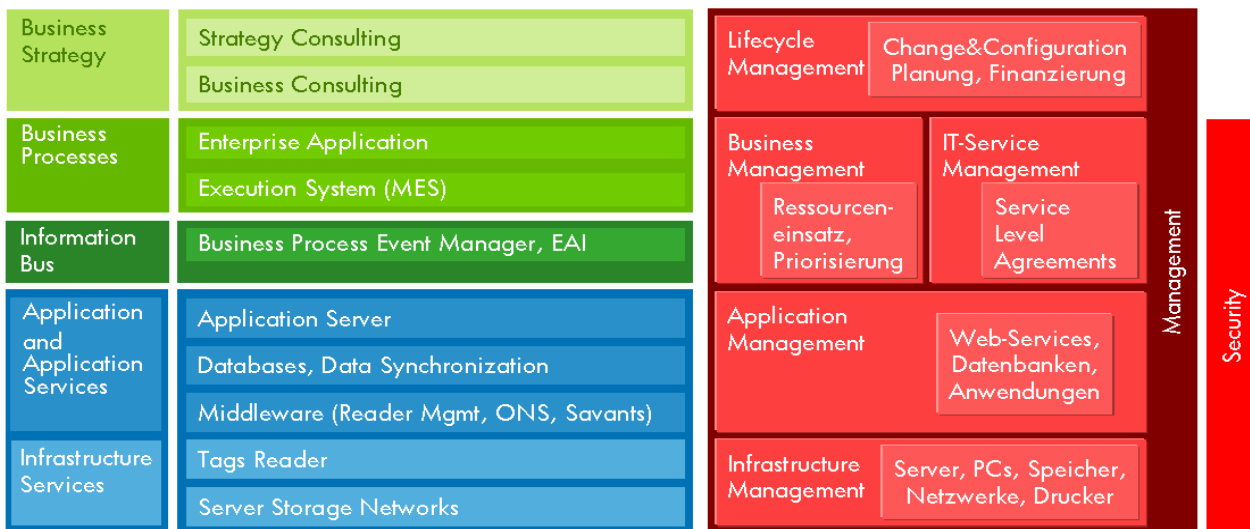


Abbildung 1: Schichten und Komponenten einer RFID-Management-Architektur
Quelle: Hewlett-Packard

Komponenten einer RFID-Management-Architektur

In der Abbildung 1 sind die Management- und Funktionsbausteine einer umfassenden IT-Architektur dargestellt. In der linken Spalte sind die Ebenen bezeichnet. Die Bausteine in der mittleren und rechten Spalte müssen sachgemäß miteinander verzahnt sein, um einen ordnungsgemäßen IT-Betrieb sicherzustellen. Der rechte Block (rot) bezieht sich dabei auf die Management-Disziplinen, der mittlere untere (blau) auf die Anwendungs-, Hardware- und Software-Infrastruktur und die darüber liegenden Blöcke (grün) vornehmlich auf Anwendungssysteme (z.B. ERP) und Dienstleistungsaufgaben. Natürlich muss das Gesamtkonstrukt mit angemessenen Sicherheitsstrukturen unterlegt sein (Security). Auf der zweituntersten blauen Ebene finden sich die RFID-Tags und die RFID-Reader. Es folgen nähere Ausführungen zu den Management-Disziplinen.

- IT Infrastructure Management – Optimierung geschäftskritischer Komponenten**
 Damit wird die IT-Infrastruktur verwaltet und gesteuert, also Komponenten wie Server, Datenspeicher, Netzwerke, PCs und Drucker. Das verbessert die Verfügbarkeit des Gesamtsystems, erhöht den Systemdurchsatz und unterstützt den kostengünstigen Betrieb.
- Application Management – Verfügbarkeit der Anwendungen**
 Application Management überwacht und steuert komplexe geschäftskritische Anwendungsumgebungen. Performance, Verfügbarkeit und Qualität von Standardanwendungen und unternehmensspezifischen Applikationen werden verbessert. Probleme werden so schnell erkannt, lokalisiert und zeitnah behoben.

■ **IT Service Management – IT als Service**

IT Service Management optimiert IT als Dienstleistung im Unternehmen. So werden Auswirkungen einer Störung auf Geschäftsprozesse in Kennzahlen wie Umsatzverlust oder erhöhtem Personalbedarf erfasst und SLAs (Service Level Agreements) definiert. Durch Einsatz von Best Practices und ITIL (IT Infrastructure Library) kann die Service-Qualität erheblich verbessert werden. Solche Standards ermöglichen darüber hinaus das Benchmarking mit vergleichbaren Unternehmensbereichen oder Mitbewerbern.

■ **Business Management – Verknüpfung mit den Geschäftsprozessen**

Business Management verbindet die IT-Ressourcen mit den Geschäftszielen und -prioritäten. Sämtliche Geschäftsprozesse sowie die Zusammenhänge zwischen Geschäftsprozessen und IT-Applikationen bzw. IT-Infrastrukturen werden anhand von Key-Performance-Indikatoren (KPI) überwacht, die die strategischen Ziele eines Unternehmens repräsentieren. Entsprechend der Relevanz für die geschäftlichen Abläufe werden IT-Ressourcen besser zugeordnet, Problemlösungen priorisiert und die Performance von Geschäftsprozessen optimiert.

■ **Lifecycle Management – den Wandel vorausschauend planen**

Mit Lifecycle Management planen Unternehmen ihre Geschäftsprozesse strategisch im Voraus. Hier werden die zukünftigen Anforderungen der Geschäftsprozesse mit den lang- und mittelfristigen Zielen des Unternehmens verknüpft. Just-in-time-Erweiterung der Systeme durch Capacity-Management vermeidet Überkapazitäten und leistet damit einen hohen Beitrag zur Kosteneinsparung.

Der Markt bietet eine Vielfalt von Software-Produkten, die die Management-Disziplinen unterstützen. Für die Auswahl geeigneter Produkte und für den wirtschaftlichen Einsatz, d.h. für die Bestimmung des erzielbaren Return-of-Investment (ROI), sind die folgenden Maßstäbe zu berücksichtigen:

- Höhere Verfügbarkeit der Anwendung
- Reduzierung ungeplanter Ausfälle, Minimierung geplanter Stillstandszeiten zur Installation weiterer Komponenten, Aufrüstung von Hardware und Software (Updates und Release-Wechsel) usw.
- Auswirkungen auf die Kundenbeziehungen (Service Level Agreements)
- Mögliche Produktivitätssteigerungen der Mitarbeiter
- Kosteneinsparungen durch schnellere Anpassung von Geschäftsprozessen

Die Einführung von Auto-ID- bzw. RFID-Verfahren hat großen Einfluss auf viele Bereiche wie etwa auf die Steuerung einer Supply Chain, auf das Product Lifecycle Management (PLM) oder auf den Produktionsprozess. Heute gibt es innerhalb der Prozesse diverse Dateninseln, Datenquellen und Medienbrüche. Dokumente werden ausgedruckt und in andere Systeme wieder manuell eingegeben. Dadurch kommt es zu Fehlern und Verzögerungen, zur Beeinträchtigung der Anlagenauslastung (Return of Net Asset) und zu Unflexibilitäten innerhalb der Prozesse. Mit RFID ist eine Maschine-zu-Maschine-Kommunikation also eine automatische eventgesteuerte Kommunikation möglich. Dabei werden Daten real-time und medienübergreifend zur Verfügung gestellt und verarbeitet.

4 RFID-System-Architektur und Standards

4.1 Markttrends und Nutzungsformen

Radiofrequenz-Identifikation (RFID) bezeichnet eine Technologie, die der Identifikation von Objekten dient, ohne dass diese berührt werden oder deren Funketiketten (RFID-Tags) sichtbar sein müssen. Die RFID-Technologie ist in vielen Bereichen bereits eingeführt, so z.B. für Skipässe, für die Fernbedienung der Zentralverriegelung von Autos, für den Diebstahlschutz in Warenhäusern, für die Logistik von Handelsobjekten wie z.B. Paletten, Container, Kleidungsstücken sowie für die Identifizierung von Haus- und Schlachttieren. RFID-Technologie wird den Barcode in vielen Marktsektoren ablösen, aber besonders im Supermarkt, also bei Verbraucherartikeln, wird der Barcode noch auf Jahre hinaus eine dominante Rolle spielen.

In den vergangenen Jahren wurde viel darüber geschrieben, wie sich die RFID-Technologie im Retail-Bereich auswirken wird, dies besonders am Beispiel der Warenhausketten Metro (Deutschland), Tesco (UK) und Wal-Mart (USA). Dabei entstand oft der Eindruck, dass die Verbrauchermärkte dieser Firmen kurz davor stehen, alle ihre Produkte mit RFID-Tags zu versehen, den Nachschub in den Regalen vollständig zu automatisieren und die Kassivorgänge vollkommen autonom von den Kunden selbst abwickeln zu lassen. Bis Mitte 2005 sind erst marginale einstellige Prozentsätze der Artikel mit RFID-Tags ausgestattet, und die umfassende, RFID-gestützte Selbstbedienung an den Kassen ist noch Zukunft. Barcodes sind hier weiterhin das dominante und weltweit akzeptierte Medium für die Produktidentifikation.

Gleichwohl sind Metro und Wal-Mart Innovatoren beim Einsatz von RFID-Tags in der Lieferkette (Supply Chain). Kartons und Paletten werden von ihren Lieferanten zunehmend mit RFID-Tags ausgestattet, die meist auf der Rückseite konventioneller Barcode-Etiketten aufweisen, so dass beide Verfahren komplementär eingesetzt werden können. Es ist zu erwarten, dass diese Ebene sich in der Logistik in den nächsten Jahren sehr stark ausbreiten wird.

Zurzeit ist die Mehrheit der RFID-Anwendungen in „geschlossenen“ Prozessen zu finden, bei denen die Tags immer wieder verwendet werden und die Anwendung innerhalb einer Organisation bzw. Firma stattfindet, z.B. in Bibliotheken für die Ausleihe von Büchern sowie in den Bereichen Asset- und Dokumentenmanagement. Man spricht hier von „geschlossenen Schleifen“ bzw. „**closed loops**“. Im Retail-Bereich geht es meist um „offene“ Systeme mit Etiketten an der Verpackung, die am Ende zusammen mit den RFID-Tags weggeworfen werden, so genannte „offene Schleifen“ bzw. „**open loops**“. Da bisher die untere Preisgrenze von RFID-Tags bei 10 bis 30 Cent liegt, ist das Tagging für Konsumartikel wie Yoghurtbecher, die selbst auf diesem Preisniveau liegen, bislang unwirtschaftlich.

Es werden auch Paletten und Container verwendet, an denen RFID-Tags fest montiert sind. Sie werden entsprechend der Wiederverwendung der Paletten immer wieder neu mit Daten beschriftet. Deswegen können hier auch teurere Tags wirtschaftlich sinnvoll eingesetzt werden. Auch das ist eine „closed loop“, denn die Paletten bewegen sich im Kreislauf.

Eine weitere Form der Nutzung von RFID-Tags liegt z.B. bei Ersatzteilen vor. Deren Tags können nach dem Einbau in Anlagen, Flugzeugen oder Autos am Teil verbleiben und so zu jedem Zeitpunkt zur Identifikation des Teils dienen. Zusätzliche Daten könnten auf solchen Tags gespeichert und jederzeit abgefragt werden, etwa Daten über Einbau, Lebensdauer oder Wartungsintervalle. Dies ist z. B. bei Airbus und Boeing für Flugzeugteile geplant.

Mit Tracking und Tracing wird die automatische Verfolgung und Lokalisierung von Produkten in Lieferketten bezeichnet. Der Nutzen der RFID-Technologie dafür ist an das Vorhandensein von RFID-Antennen und Readern gebunden, z.B. an Lagerzugängen und Logistik-Hubs.

Natürlich können die Antennen auch an mobilen Geräten angeschlossen werden, so bietet z.B. Nokia als erster Anbieter ein Mobiltelefon mit RFID-Reader, was zukünftig sowohl für Konsumenten- wie für Industrie-Anwendungen interessant sein wird.

Soll der Lauf von Containern oder anderer mobiler Objekte verfolgt werden, dann kommt eine weitere Auto-ID-Technologie zum Tragen, nämlich GPS (General Positioning System) bzw. das in der Entwicklung befindliche europäische Galileo-System. Diese Technologie ist bekannt durch die Navigationssysteme in Kraftfahrzeugen. Sie dient der weltweiten Lokalisierung von Objekten und wird hier nicht weiter vertieft.

Für die Übertragung von Lokalisierungs- oder RFID-Daten bei mobilen Geräten wird GSM, GPRS, UMTS oder der Satellitenfunk INMARSAT verwendet. Fest installierte RFID-Antennen werden über Kabel oder drahtlos über WLAN an sog. Backend-Systeme zur weiteren Verarbeitung der empfangenen Daten angeschlossen. (Natürlich können auch andere Technologien wie GPS oder Location Based Services für solche Zwecke genutzt werden.)

4.2 Architektur von RFID-Systemen

Eine umfassende IT-Architektur ist notwendig, um die RFID-Systeme darin stabil einzubetten und einen zuverlässigen Betrieb sicher zu stellen. In einer solchen Architektur werden typischer Weise die System- und Anwendungsfunktionen in Ebenen angeordnet, zwischen denen Daten ausgetauscht werden.

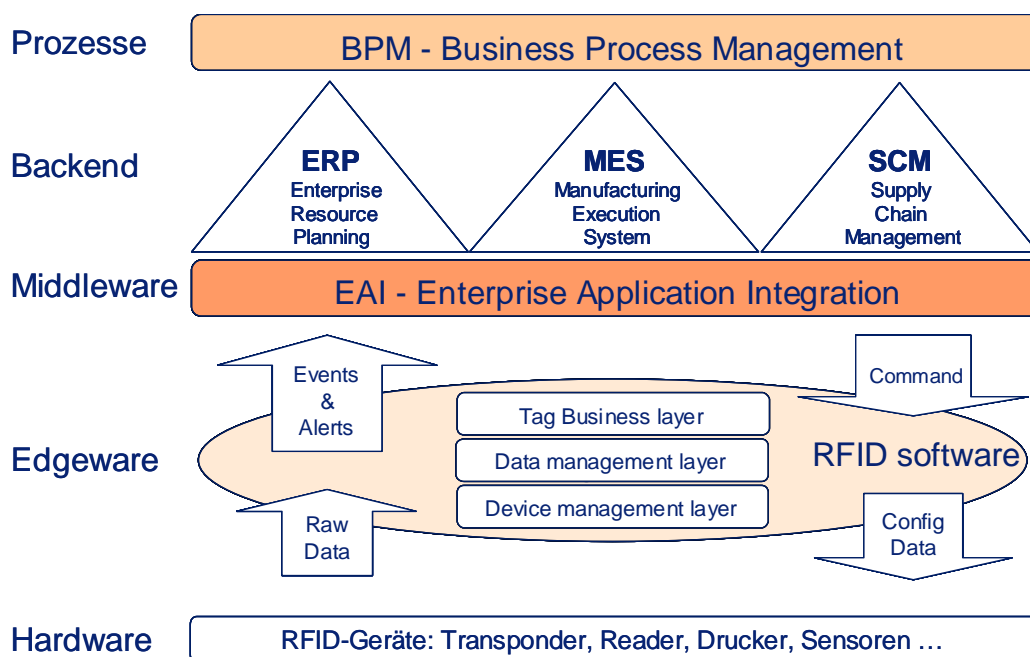


Abbildung 2: Systemarchitektur für RFID-Anwendungen

Quelle: Infineon

In der Abbildung 2 sind die RFID-Reader, die die RFID-Tags lesen, in der unteren Hardware-Ebene angeordnet. Die gelesenen Daten ("raw data") werden in die Ebene "Edgware" übertragen. Diese ist z.B. auf einem Server im Lagerhaus implementiert. Hier werden die Daten gefiltert und nur die Daten ("Events" oder "Alerts") weiter zur Middleware übertragen, die für die darüber liegenden Ebenen wichtig sind. Die Middleware ist typischer Weise im Rechenzentrum installiert.

Eine solche Architektur erleichtert den Entwicklungsprozess, die Installation, den Betrieb und die Wartung von RFID-Systemen. Middleware schlägt die Brücke zu den vorhandenen

Geschäftsapplikation im „Backend“. Unterstützt wird dieses Modell von einer Infrastruktur, die für Überwachung und Update der Komponenten und für die Kommunikation zwischen den Komponenten verantwortlich ist.

Nachfolgend werden im Kontext mit der Abbildung 2 einige Komponenten beschrieben. Ausführlichere Darstellungen folgen im Kapitel „RFID-Systemkomponenten“.

■ **RFID-Tag bzw. RFID-Transponder**

Im einfachsten Fall handelt es sich hier um ein Etikett, das aus einem Chip und einer Antenne besteht. In Form eines Klebe-Etiketts kann es auf Teile aufgeklebt werden. Als Glaszylinder werden RFID-Tags Tieren und Menschen unter der Haut implantiert. Die entsprechende Zulassung ist in USA bereits erfolgt. RFID-Tags können auch in Kunstharz eingegossen werden, um schwierigen Umgebungsbedingungen Stand zu halten.

Einfache Tags sind passiv, d.h. sie können ihre Information nur abgeben, wenn ihnen elektromagnetische Wellen von Lesegeräten Energie zuführen. Aktive Tags verfügen über eine eigene Energiequelle und eigene Sendefähigkeit.

In ihrer einfachsten Form tragen RFID-Tags nur eine Tag-ID, eine weltweite eindeutige Seriennummer, und geben diese bei Bedarf ab. Tags können aber auch über beschreibbare Speicherbereiche verfügen, so dass auf einem Paletten-Tag z. B. der elektronische Lieferschein gespeichert werden kann. Dies ist dann wichtig, wenn Sendungen an Orten überprüft werden sollen, an denen kein Zugriff auf das Internet bzw. das EPCglobal-Netzwerk möglich ist.

Die Anbringung von Tags ist kritisch für ihre elektronische Erkennbarkeit. So müssen Tags auf Metalloberflächen mit speziellen Kunststoffunterlagen versehen werden. Unter Flüssigkeiten (Behältern, Flaschen) verborgene Tags können wenn überhaupt nur bei einigen Technologien (125 KHz, 13.56 MHz) verwendet werden.

■ **RFID – Reader / Writer bzw. Antennen**

Antennen sind an elektronische Steuergeräte angeschlossen: die Reader. Sie erzeugen elektromagnetische Felder, über die Daten von RFID-Tags empfangen bzw. an diese übertragen werden. Die Übertragung erfolgt ohne Sichtkontakt zum Tag. Allerdings ist zu beachten, dass ungünstige Bedingungen bei bestimmten Technologien zu Übertragungsproblemen führen können, z.B. metallische Umgebungen oder Flüssigkeiten. Tags und Reader / Writer müssen hinsichtlich der Frequenzen aufeinander abgestimmt sein. Abbildung 3 zeigt die wichtigsten Frequenzen und ihre Einsatzbereiche.

Neben der Frequenz kommt es auf Antennenform und -reichweite, also auf den maximalen Abstand zwischen RFID-Tag und Antenne, sowie auf die Sendeleistung an. Die erforderliche Geometrie der Antennen muss immer vor Ort ermittelt und verifiziert werden, d. h. dort, wo die Lesevorgänge stattfinden sollen. Weitere Ausführungen dazu folgen im Kapitel „RFID-Systemkomponenten“.

RFID-Frequenz	Kommentar
125 KHz (LF)	Weltweit standardisierte und freigegebene Frequenz, vor allem für preiswerte, passive RFID-Tags für die Tieridentifikation.
13,56 MHz (HF)	Weltweit standardisierte und freigegebene Frequenz, vor allem für preiswerte, passive RFID-Tags zur Kennzeichnung von einzelnen Objekten.
400 MHz	Fernbedienung für die Zentralverriegelung von Kfz
868 MHz (UHF)	In Europa standardisierte Frequenz für aktive und passive RFID-Tags in der Logistik.
915 MHz (UHF)	Analog verwendete Frequenz in USA. Die Tags unterstützen in der Regel den gesamten Frequenzkanal von 850 bis 950 MHz und können so für globale Logistik-Prozesse verwendet werden.
2,45 GHz	Weltweit freigegebenes lizenz- und anmeldefreies ISM-Band (ISM = Industrial, Scientific, Medical). Aktive Transponder, z.B. mit Temperatursensoren oder GPS-Ortsbestimmung.

Abbildung 3: Die wichtigsten RFID-Frequenzbereiche und ihre Anwendungen

■ **Middleware und Edgeware**

Eine besondere Eigenart des Tracking und Tracing mit Auto-ID-Verfahren ist, dass die Daten eventorientiert anfallen, d.h. sie müssen dann übernommen werden, wenn sie von irgendeiner Antenne erkannt und übertragen werden. Weiterhin fallen viel mehr Daten an, als von den nach gelagerten kaufmännischen Systemen im Backend benötigt werden. Deswegen sind für solche IT-Systeme eine oder mehrere spezielle Funktionsschichten notwendig. In der Abbildung 2 sind das die Middleware und die Edgeware. Die Edgeware bereinigt die Daten von Lesefehlern und Mehrfachlesungen, soweit das nicht bereits von den Readern erledigt wird, und puffert sie in einer Datenbank. Dann werden sie entsprechend den Anforderungen der Geschäftsprozesse gefiltert und an die ERP-Systeme übertragen. Diese Übertragung muss auch zeitnah erfolgen, da ja die ERP-Systeme daraufhin bei Bedarf weitere Aktionen anstoßen müssen. Mit der Pufferung wird erreicht, dass die Daten für weitere Auswertungs- oder Revisionszwecke bereit stehen.

Die Übertragung der Event-Daten von den Antennen / Readern zur Edgeware bzw. zur Middleware erfolgt über Ethernet oder WLAN bei fest installierten Antennen/Readern bzw. über GSM, GPRS oder INMARSAT bei mobilen Geräten. Unabhängig von RFID-Aspekten hat Middleware auch die Aufgabe, unternehmensweit verteilte Anwendungssysteme zu integrieren. Deswegen spricht man hier auch von Enterprise Application Integration (EAI). Das Management der Geschäftsprozesse ("Business Process Management") kann innerhalb der ERP-Module stattfinden oder, wenn es modulübergreifend funktionieren muss, auch in der Middleware.

■ **ERP bzw. kaufmännische IT-Systeme (Backend)**

Dies ist üblicher Weise die oberste Ebene in einer Systemarchitektur. Hier sind die IT-Systeme gemeint, die von Standardsoftware-Herstellern wie SAP, Oracle, Retek oder Microsoft (Navision) stammen oder individuell programmiert sind. Sie verwenden die empfangenen Daten für die Unterstützung der Geschäftsprozesse. ERP (Enterprise Resource Planning) ist der Oberbegriff dafür. Entsprechend den spezifischen Anwendungsaspekten gibt es ergänzende Systeme wie MES (Manufacturing Execution System) oder SCM (Supply Chain Management).

4.3 Das Internet der Dinge aus EPCglobal-Sicht

Der EPC (Electronic Product Code) auf RFID-Tags wird zunehmend die Rolle des bekannten EAN-Code auf Barcode-Etiketten übernehmen. EPC ist ein Nummernschema, das alle Objekte weltweit eindeutig identifizieren kann und von EPCglobal Inc., New Jersey (USA) und Brüssel (Belgien), herausgegeben wird. EPCglobal Inc. ist eine internationale Organisation, die aus der Vereinigung von EAN International und dem Uniform Code Council, Inc. (UCC) hervorgegangen ist: www.EPCglobalinc.org.

Die EPC-Nummer hat einen festen Aufbau, der in der Tabelle in Abbildung 4 dargestellt ist.

Gillette Venus Cartridge: 00.47400.114008.9780. (Struktur laut EPCTM Tag Data Standards Version 1.1 Rev.1.24)		
Feldbezeichnung	Länge (Bytes)	Kommentar
Datenkopf	2	Für netzwerk-interne Steuerungszwecke, Versionsbezeichnungen, Formatangaben
Hersteller (EPC Manager)	7-9	Nummer wird in Deutschland von GS1 vergeben.
Teilenummer. (Objektklasse)	6	Produzent- und Teilenummer entsprechen der EAN aus dem EAN.UCC-System; pro EPC besteht eine Kapazität für 1 Million Artikel
Seriennummer	9	Diese Nummer dient der ein-eindeutigen Bezeichnung individueller Teile; Kapazität pro Hersteller: 100 Milliarden Artikel.

Abbildung 4: Beispiel und Struktur einer EPC-Nummer

EPCglobal betreibt das EPCglobal™ Network. Es stellt die standardisierten Mittel für den Einsatz der RFID-Technologie in der globalen Wertschöpfungskette – besonders im Handel - zur Verfügung. Das EPCglobal-Szenario geht davon aus, dass zukünftig jedes individuelle Objekt seine eigene Homepage hat und dass diese über das EPCglobal-Netzwerk erreicht werden kann. Sie wird irgendwo im Internet liegen und typischer Weise vom Produzenten des Objektes betrieben. Diese Homepage stellt u.a. folgende Angaben zum gewünschten Produkt zur Verfügung:

- Daten über Konstruktion, Produktion, Versand, Verkauf, Wartungs- bzw. Verfallsdaten
- Echtheitszertifikat, Gebrauchsanweisung
- Auslieferung des Objektes auf bestimmten Paletten sowie sein Verbleib in der Lieferkette

In konstruktiven Bereichen wird damit auch das Product Lifecycle Management (PLM) unterstützt. Die Summe dieser Homepages ergibt das häufig zitierte und auch in die Literatur eingegangene „**Internet der Dinge**“. „Dinge“ sind dabei Artikel, Kartons, Paletten, Ersatzteile und andere Objekte.

Der wissenschaftliche Ansatz für das EPCglobal-Netzwerk wurde vom Auto-ID Center entwickelt, einem Projekt des Massachusetts Institute of Technology (MIT) in Boston (USA). Daraus entstand das Netzwerk der Auto-ID-Labs, in dem weltweit verteilte Universitätsinstitute mitarbeiten, so in St. Gallen (Schweiz) und Cambridge (UK). Das MIT hat nach Abschluss der Grundlagenforschung zu RFID die weitere Arbeit am EPCglobal-Projekt und die Förderung seiner Marktausbreitung an die EPCglobal Inc. übertragen. EPC-Repräsentant in Deutschland ist GS1 Germany GmbH (vormals CCG) in Köln:

www.gs1-germany.de

Der Darstellung des EPCglobal-Netzwerkes wird in diesem White Paper relativ viel Raum gewidmet, weil es sich dabei um eine wissenschaftlich fundierte Struktur mit weltweiter Ausprägung handelt. Natürlich können RFID-Tags besonders in geschlossenen Kreisläufen auch völlig unabhängig von EPCglobal genutzt werden.

Der EPC-Datenstandard ist branchenübergreifend einsetzbar. Spezifische Branchenbedürfnisse werden über Anwendergruppen eingebracht. Derzeit gibt es die Expertenkreise "Fast Moving Consumer Goods", "Gesundheitswesen / Pharma" sowie "Transport / Logistik". Bedarfsgerecht ist die Einrichtung weiterer Gruppen geplant. Die Interessen klein- und mittelständischer Unternehmen sowie noch nicht vertretener Länder/Regionen werden in diesem Standardisierungsprozess über die nationalen GS1-Mitgliedsorganisationen abgedeckt. Sie sorgen für die generelle Ausgewogenheit von Interessen und Umsetzbarkeit der Ergebnisse als offene, globale Standards.

Das EPCglobal-Netzwerk verbindet dezentrale Server, die die Homepages der Objekte enthalten. Der Zugang wird mittels Internet realisiert. Die Steuerung dieser Server sowie die Autorisierung und der Zugang zu den Informationen übernehmen verschiedene Service-Komponenten des Netzwerkes. Zentrales Element des EPCglobal-Netzwerkes wird der Object Name Service (ONS) sein. Er arbeitet nach dem Muster des bekannten Domain Name Service (DNS), der URL-Adressen (www) in maschinenlesbare IP-Adressen zur Lokalisierung im Internet umsetzt.

World Wide Web	EPCglobal-Netzwerk
<p>DNS Zentrales System, das die Abfrage von Webseiten und E-Mails steuert.</p>	<p>ONS Zentrales Verzeichnis der bei EPC registrierten Hersteller, das Anfragen nach Produktinformationen steuert.</p>
<p>Web Sites Ort (Ressource), an dem sich Informationen zu einem bestimmten Thema befinden.</p>	<p>EPC Information Services Ort (Ressource), an dem sich Informationen über ein Produkt befinden.</p>
<p>Search Engines Instrument für das Auffinden von Web-Seiten.</p>	<p>EPC Discovery Services Instrument für das Auffinden von EPC-Informationen.</p>
<p>SSL Sicherheitsstandard für Webseiten.</p>	<p>EPC Security Services Instrument für den sicheren Zugang in Anhängigkeit von Rechten.</p>

Abbildung 5: Struktur des EPCglobal-Netzwerkes im Vergleich zum Web

■ **Der ONS-Server**

wird alle EPC-Nummern und die zugehörigen IP-Adressen enthalten, unter denen die Homepages einzelner Objekte im Internet erreicht werden können. Auf diese Services können von EPCglobal autorisierte Teilnehmer zugreifen. Betriebswirtschaftliche Fragen, die zukünftig über das EPCglobal-Netzwerk beantwortet werden können, sind in der Abbildung 6 aufgelistet.

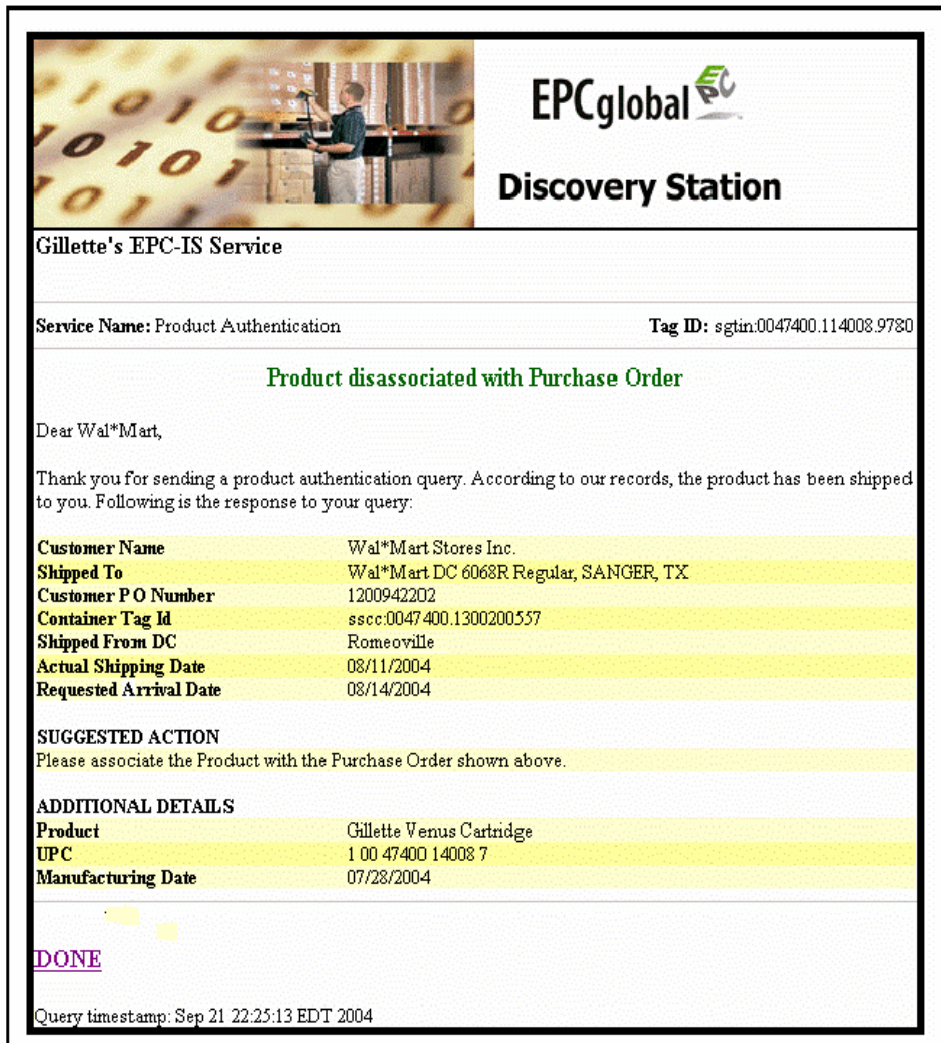
Anwendungsbereich	Frage an das EPCglobal Network
Produktion	Wir müssen 1000 Teile wegen Produktionsfehlern zurückrufen. Wo sind diese Teile?
Marketing	Die Produktpromotion läuft sehr gut in der Nordost-Region. In welchen Regionen haben wir Produkte auf Lager, die wir nach Nordost verschieben können?
Retail	Wir brauchen schnell eine Nachlieferung zu Produkt xy. Woher können wir sie erhalten?
Distribution	Der Lastwagen ist bei Kunde xy, aber ein Karton fehlt. Wo ist der Karton?
Wartung	Wann wurde dieses Teil eingebaut? Wann muss es ausgetauscht werden?


Abbildung 6: Fragen, die zukünftig über das EPCglobal-Netzwerk beantwortet werden

■ **EPCIS: EPC Information Service**

Die Kommunikation einzelner Unternehmen mit dem EPCglobal-Netzwerk und dem ONS-Server erfolgt über die Software-Komponente EPCIS, eine Interface-Software bzw. ein Gateway, der von EPCglobal definiert ist. Über EPCIS können Unternehmen EPC-Nummern an den ONS-Server schicken und so die IP-Adressen der Homepages der Objekte ermitteln. EPCIS unterstützt auch den Austausch von Daten zwischen den Unternehmen. Die EPC-Nummer dient dann zum Auffinden des entsprechenden Kommunikationspartners.

Die Abbildung 7 zeigt einen typischen Datenabruf von einer Objekt-Homepage über EPCIS. Gillette informiert hier Wal-Mart darüber, dass ein Produkt in der Lieferkette von einer Gesamtlieferung getrennt wurde und empfiehlt die passende Aktion.



EPCglobal 
Discovery Station

Gillette's EPC-IS Service

Service Name: Product Authentication **Tag ID:** sgtin:0047400.114008.9780

Product disassociated with Purchase Order

Dear Wal*Mart,

Thank you for sending a product authentication query. According to our records, the product has been shipped to you. Following is the response to your query:

Customer Name	Wal*Mart Stores Inc.
Shipped To	Wal*Mart DC 6068R Regular, SANGER, TX
Customer P O Number	1200942202
Container Tag Id	sccc:0047400.1300200557
Shipped From DC	Romeoville
Actual Shipping Date	08/11/2004
Requested Arrival Date	08/14/2004

SUGGESTED ACTION
Please associate the Product with the Purchase Order shown above.

ADDITIONAL DETAILS

Product	Gillette Venus Cartridge
UPC	1 00 47400 14008 7
Manufacturing Date	07/28/2004

DONE

Query timestamp: Sep 21 22:25:13 EDT 2004

Abbildung 7: EPCIS-Service von Gillette
Quelle: GS1 Germany / EPCglobal

■ RFID-Standardisierungsaktivitäten bei EPCglobal

Der Einsatz von RFID in offenen Systemen über Unternehmensgrenzen hinweg erfordert eine standardisierte Infrastruktur, wie sie z. B. in der Abbildung 8 dargestellt ist. Das EPC-Konzept beschreibt die standardisierte Gewinnung bzw. Erfassung, das Speichern und den Austausch von EPC-Informationen in offenen Systemen. Zur Zeit werden unter dem Dach von EPCglobal die folgenden Standards für ein EPC-fähiges RFID-System entwickelt bzw. definiert:

- Tag Data Standards (der Datenstandard)
Dieser Datenstandard regelt, wie die verschiedenen Identifikationsstandards (z.B. SGTIN, NVE) als EPC-Tag-Information kodiert werden.
- Protokoll für die Luftschnittstelle (GEN 2 AIP)
Das auch als „Generation 2“ bekannte Protokoll für die Luftschnittstelle regelt die Kommunikation zwischen Reader und Tag.
- Reader-Protokoll
Beschreibung des Datenaustausches und der Befehlsstruktur zwischen einer EPC-fähigen Middleware und dem Reader.
- Reader-Management-Spezifikation
Standardfunktionen zur individuellen Konfiguration von EPC-fähigen Readern und die Steuerung einer multiplen Reader-Umgebung.

- Tag Data Translation
Konvertierung der EPC-Informationen aus dem TAG in ein Internet-kompatibles Format.
- Filter and Collection ALE (F & C ALE)
Art und Weise, wie die EPCs in einer Reader-Umgebung nach verschiedenen Kriterien ausgelesen und gezählt werden
- ONS Application Layer Interface
Auskunft darüber, wo in dem EPCglobal-Netzwerk Informationen über eine bestimmte EPC-Nummer zu finden sind.
- EPCIS-Protokolle
Beschreibung, wie die EPC-Informationen gespeichert und über das EPCglobal-Netzwerk aufgerufen werden können.
- Security-Spezifikation
Anforderungen an einen sicheren Informationsaustausch zwischen den Teilnehmern des EPCglobal-Netzwerks.

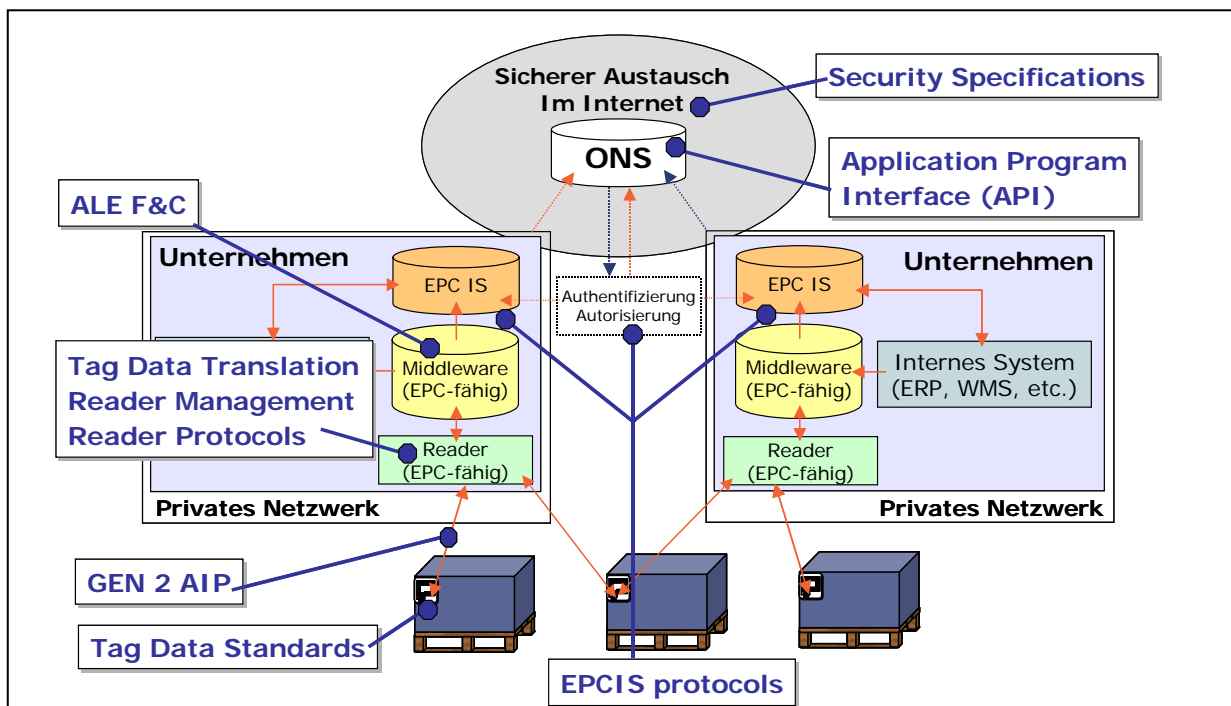


Abbildung 8: Standards des EPCglobal-Netzwerkes

Quelle: GS1 Germany / EPCglobal

Die EPCglobal-Standards stellen technische Spezifikationen und funktionale Beschreibungen dar. Jeder IT-Dienstleister kann diese Standards in seine Lösungen (Hard- und Software) integrieren und den Anwendern zur Verfügung stellen. Die Mehrzahl der Spezifikationen wird zur Zeit erarbeitet. Das Protokoll für die Luftschnittstelle (GEN 2 AIP) und der Datenstandard sind bereits fertig gestellt. Erste Entwürfe der anderen Spezifikationen sind Ende 2005 zu erwarten.

4.4 RFID-Standards

Technologie-Standards beschreiben die technische Basis von RFID-Systemen. Sie legen Frequenzen, Übertragungsgeschwindigkeiten, Kodierungen, (Antikollisions-)Protokolle und andere Faktoren fest. Maßgebliche Standards gibt es von Seiten der ISO (International

Standards Organisation), aber auch von EPCglobal bzw. den Auto-ID-Labs. Natürlich ist es erstrebenswert, dass die EPC-Standards auch von ISO bestätigt werden. Deswegen hat EPCglobal den neuen Standard Generation 2 (Gen 2) bei der ISO eingereicht. Mit der Normung kann bis Anfang 2006 gerechnet werden. Hier eine Auswahl wichtiger Standards:

Standard	Gegenstand des Standards	Frequenzen
Auto-ID Class 0	Parameter für die Air Interface Communication	860 - 930 MHz
Auto-ID Class 1	Parameter für die Air Interface Communication	860 - 930 MHz
EPCglobal Gen 2	Parameter für die Air Interface Communication, als Ablösung für Class 0 und 1 vorgesehen, wurde Anfang 2005 bei ISO eingereicht.	860 - 930 MHz
ISO 14443	Air Interface und Initialisierung für Identifikationskarten, Kundenkarten.	13,56 MHz
ISO 15693	Regelung für eindeutige Ident-Nummern („Unique Identifier“) für Transponder bzw. Tags	
ISO 15993-2	Air Interface und Initialisierung für Identifikationskarten, Kundenkarten.	13,56 MHz
ISO 15993-3	Air Interface, Initialisierung, Antikollisions- und Übertragungsprotokoll für Identifikations- und Kundenkarten.	13,56 MHz
ISO 18000	RFID Air Interface Standard.	alle

Abbildung 9: ISO- und EPCglobal-Standards

Die Ident-Nummer aus ISO 15693 ist zu unterscheiden von dem EPC, der zur Identifikation des den RFID-Transponder tragenden Objektes dient. Die Ident-Nummern werden den verschiedenen Herstellern so zugeteilt, dass sie sich nicht überschneiden und eine eindeutige Identifikation erlauben. Die zugehörigen Produktdaten (z.B. EPC) können auf den Transpondern oder auf externen Datenbanken abgelegt sein. Die 18000-Standards beschreiben Messverfahren zur Überprüfung von RFID-Strukturen. Hier geht es um Feldstärken, Modulationsgrade, Reichweiten und Bearbeitungszeiten.

4.5 Ausblick

Die RFID-Technologie ist im Kontext mit EPCglobal und der Vision "Internet der Dinge" auf dem Weg, viele Bereiche von Industrie, Logistik und Verbrauchenumfeld zu durchdringen. Jetzt geht es darum, betriebswirtschaftlich sinnvolle Lösungen zu finden und diese so zu gestalten, dass sie sich in ein globales Netzwerk für Tracking und Tracing einbinden lassen. Der Schutz der Verbraucher vor Missbrauch und der Schutz von Patenten und "Intellectual Property" sind dabei wichtige Randbedingungen, die es zu wahren gilt.

5 RFID-System-Komponenten

5.1 RFID-Tags: Chip und Antenne

5.1.1 Aufbau eines RFID-Tags bzw. -Transponders

RFID-Tags, auch RFID-Transponder genannt, bestehen aus einem Speicher-Chip und einer Antenne. Sie können in vielerlei Hinsicht unterschieden werden. Ein wesentliches Kriterium ist die Frequenz, die sich nach heutigem Stand zwischen 125 kHz im LF-Bereich und 5,8 GHz im UHF-Bereich bewegt und einen wesentlichen Einfluss auf die Bauform der Antenne hat. Die folgende Betrachtung bezieht sich vor allem auf Transponder mit Frequenzen von 13,56 MHz (HF) bzw. zwischen 860 und 960 MHz (UHF). Diese werden hauptsächlich in Handel und Logistik eingesetzt und können als hochvolumige Einwegtransponder hergestellt werden.

Leistungsparameter eines Tags sind die Lesereichweite, die Übertragungsgeschwindigkeit (Datenrate), die Pulklesefähigkeit und die Beeinflussung durch umgebende Objekte. Die Frequenz, die Ausrichtung zum Reader-Feld sowie Form und Größe der Antenne bestimmen die Lesereichweite, die Robustheit gegenüber Umweltbeeinflussung sowie die Pulkfähigkeit der RFID-Tags. Die Frequenz und das entsprechende Übertragungsprotokoll (Antikollisionsalgorithmus) entscheiden über die grundsätzliche Datenübertragungsrate bzw. Auslesegeschwindigkeit im Pulk. Man unterscheidet aktive, semi-aktive und passive Transponder. Aktive Transponder können mithilfe einer Batterie Radiosignale erzeugen, semi-aktive könne nach Anregung durch das Lesefeld die Feldbeeinflussung verstärken, oder Sensordaten puffern (z. B. für die Kühlkettenverfolgung), während passive Transponder lediglich das vom Reader ausgesendete Feld zur Datenübermittlung modulieren.

Beispiele von RFID-Inlays für passive RFID-Tags sind in den Abbildungen 10 und 11 dargestellt. An den Spulenantennen erkennt man den Frequenzbereich von 13,56 MHz (HF). Die Abb. 11 zeigt Inlays, die im Bereich 860 bis 960 MHz (UHF) arbeiten. In diesem Fall haben die Antennen die Form von Dipolen. Der abgebildete Tripol ist die Variante eines Dipols. Die bizarren Formen der Dipol-Antennen dienen dazu, in speziellen Arbeitsumgebungen optimale Empfangsverhältnisse herzustellen. Die Inlays werden z. B. zu Etiketten oder Ausweiskarten verarbeitet.

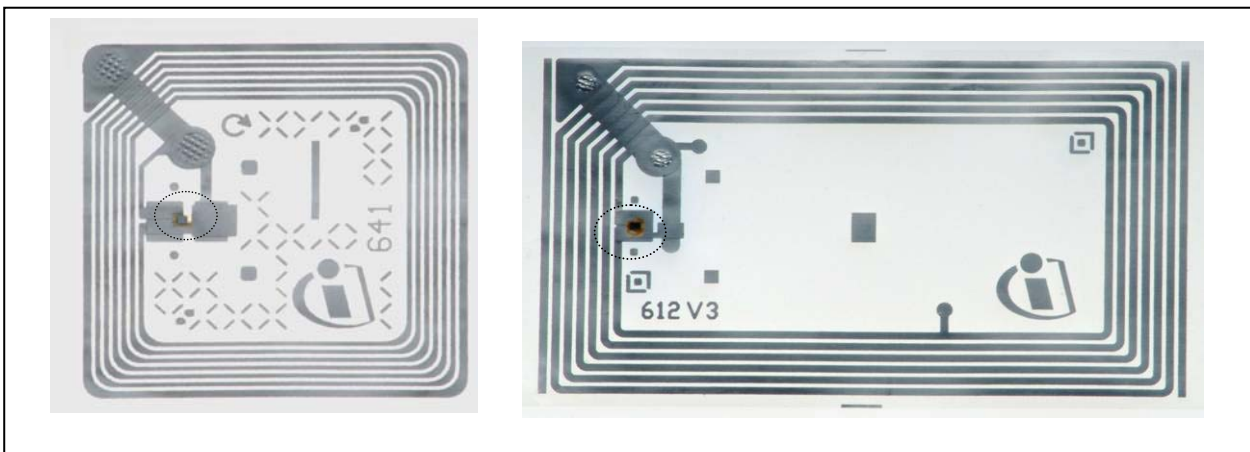


Abbildung 10: Inlays für RFID-Tags mit 13,56 MHz (HF)

Quelle: Infineon

Ein weiteres Unterscheidungsmerkmal ist die Schreib-/Lesefähigkeit der Transponder. Hier gibt es drei Typen:

- Read-only Tags
erhalten bei der Herstellung eine n Bit große eindeutige Seriennummer zur Identifikation. Die Informationsverknüpfung mit den Objekten, auf denen sie angebracht werden, erfolgt über zentrale Datenbanken.
- WORM Tags (Write once – Read many)
erlauben eine einmalige unveränderliche Codierung der Information auf dem Tag, die nahezu beliebig oft (> 100.000 mal) gelesen werden kann.
- Read/Write Tags
verfügen über individuell beschreibbare Speicherbereiche. Die Information kann geschrieben und verändert werden. Nutzdaten, Handlungsanweisungen oder Prozessdaten können hinterlegt werden. Ebenso können die Daten verschlüsselt werden. Beschreibbare Tags können Schnittstellendaten zwischen Anwendungen transportieren und helfen, Medienbrüche zu vermeiden.

Das Kernstück eines Tags ist der Chip auf dem die Informationen gespeichert werden. Er besteht im Wesentlichen aus drei Komponenten:

- Hochfrequenz-Teil zur Signalverarbeitung und zur Gewinnung der notwendigen Energie aus dem elektrischen Feld.
- Kontrolleinheit zur Verarbeitung der empfangenen Kommandos.
- Speichereinheit.

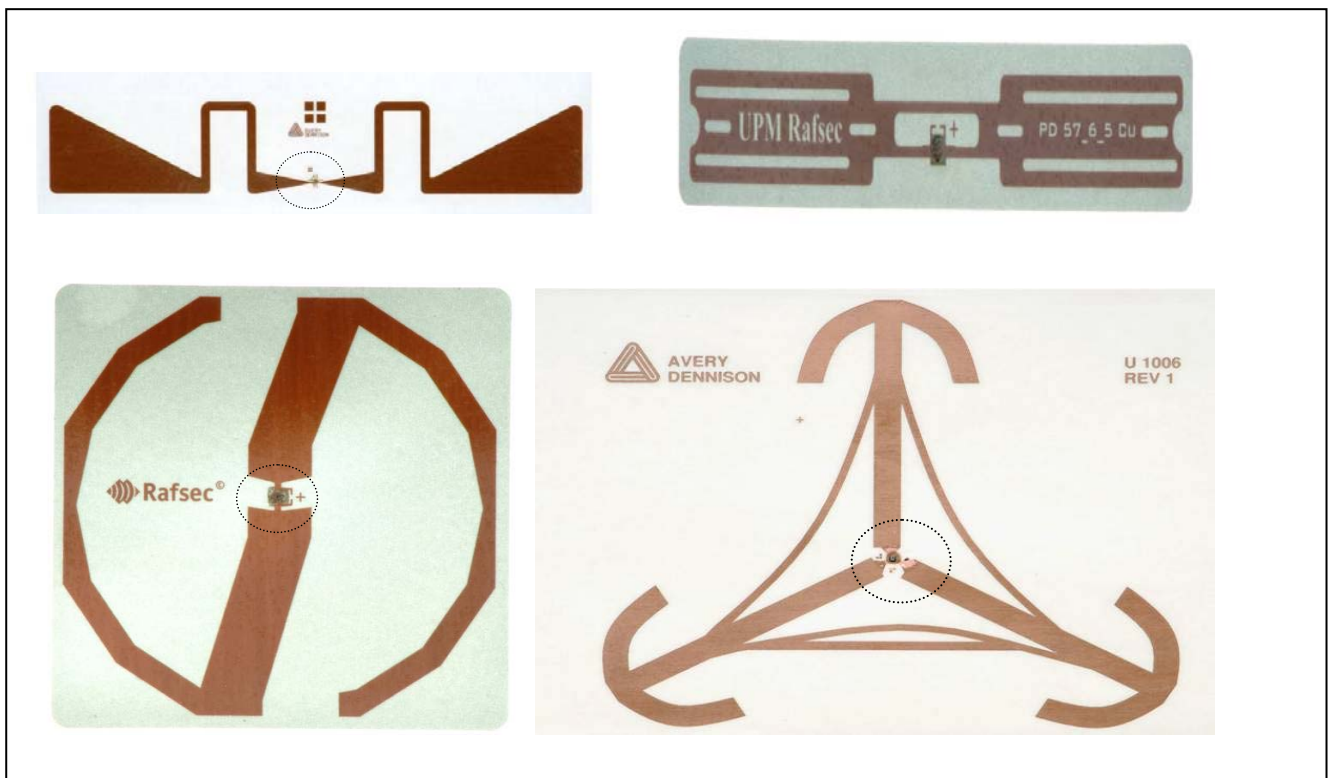


Abbildung 11: Inlays für RFID-Tags mit 868 MHz (UHF)

Quelle: Avery Dennison und Rafsec.

Der wesentlichste Parameter für den Einsatz der Chips ist die Größe des verfügbaren Speichers, auch Datenbreite genannt. Hier wird unterschieden in den Anwender-Speicher (z. B. 96 Bit bei EPC-kompatiblen Chips) und weiteren Speicherzellen zur Status-Steuerung (z. B. Sperren einzelner Speicherzellen, Kill-Befehl zur permanenten Deaktivierung) und

Datenkontrolle (Speicherung von Prüfsummen). Der größte, derzeit verfügbare Chip im UHF-Bereich bietet 2048 Bit, wobei der Anwender 1728 Bit frei nutzen kann.

Die einfachsten Tags verfügen über eine Datenbreite von einem Bit und enthalten keinen Chip. Diese 1-Bit-Tags werden im Einzelhandel zum Diebstahlschutz genutzt (EAS – Electronic Article Surveillance). Sie enthalten lediglich eine veränderbare Ja/Nein-Information (bezahlt/nicht bezahlt): Sind sie noch an der Ware, wenn der Kunde den Ausgang des Warenhauses und die dort angebrachten RFID-Antennen passiert, dann wird ein Warnton erzeugt der besagt, dass die Ware entweder nicht bezahlt oder dass vergessen wurde, den Tag an der Kasse zu entfernen. Über den Artikel sagen diese Tags nichts aus.

5.1.2 Tag-Antenne

Die Antenne des RFID-Tags hat die Aufgabe, die Verbindung zwischen der elektromagnetischen Welle des Raumes, die vom RFID-Reader erzeugt wird, und dem Chip herzustellen. Auf Tags werden möglichst kleine Antennen eingesetzt.

Im Bereich niedriger Frequenzen (HF) mit kurzen Leseabständen befindet sich der Tag im Nahfeld der Reader-Antenne. Hier wird für die Energie- bzw. Signalübertragung eine magnetische Kopplung mittels Induktivitäten verwendet. Die Tag-Antenne besteht daher im HF-Bereich aus einer Spule (induktive Schleifen), an die der Chip angeschlossen wird.

Im UHF-Bereich befindet sich der Tag bei größeren Leseabständen im Fernfeld der Reader-Antenne. Die Verkopplung von Reader und Tag erfolgt damit über die elektromagnetische Welle des freien Raumes, an die Reader und Tag über geeignete Antennenkonstruktionen angeschlossen werden. Die Tag-Antenne sollte möglichst klein und leicht zu fertigen sein. Die damit verbundenen Anforderungen werden weiter unten erläutert.

Recht einfach zu fertigen sind gedruckte Antennen, bei denen die Antenne als flache Struktur auf ein Trägermaterial aufgebracht wird. Häufig wird im nächsten Fertigungsschritt der Chip auf das Trägermaterial aufgebracht und mit der Antenne verbunden. Diese Konstruktion wird als Inlay bezeichnet. Ein Inlay wird zum Tag bzw. Transponder, indem es auf ein Klebeetikett oder eine Smart Card aufgebracht. Dabei muss berücksichtigt werden, dass die elektromagnetischen Eigenschaften der das Inlay umgebenden Materialien Einfluss auf die Kommunikationsfähigkeit des Tags hat. Im Extremfall kann die falsche Wahl einer Reader-Antenne dazu führen, dass ein Tag nicht gelesen werden kann.

Eine andere Verwendungsart ist die Integration in das zu kennzeichnende Objekt. Dabei können Teile des Objekts zu einer Antenne geformt und die Antenne optimal auf das Objekt abgestimmt werden. Das führt zu einer wesentlichen Verbesserung der Lesbarkeit und dient auch der Fälschungssicherheit.

Im UHF-Bereich werden bevorzugt Dipolantennen eingesetzt. Allerdings besitzen sehr kleine gerade Dipolantennen ungünstige Anschlussimpedanzen und lassen sich daher nicht ohne hohe Verluste an den Chip anpassen. Daher werden Dipole oft zu Mäandern oder fraktalen Strukturen gefaltet, womit sich gute Kompromisse bezüglich der elektrischen Eigenschaften ergeben. Ähnliches gilt für einfache Schleifen- oder Loop-Antennen.

Dipole und Loop-Antennen lassen sich sehr gut in gedruckter Form herstellen, womit sich preisgünstige flache Tags produzieren lassen. Jedoch besteht hierbei der Nachteil, dass die Antennenparameter stark durch das in unmittelbarer Umgebung befindliche Material, insbesondere durch das zu kennzeichnende Objekt, verändert werden. So ist ein Dipol auf einer Metallfläche wirkungslos und auf Glas besitzt er andere Eigenschaften als auf Papier.

Die Struktur und Dicke des hinter dem Dipol befindlichen Materials hat Einfluss auf die Eigenschaften der Tag-Antenne. Eine im Abstand einer halben Wellenlänge hinter einem Dipol befindliche große Metallfläche kann das Readersignal derart reflektieren, dass am Ort des

Tags eine Auslöschung der Welle stattfindet und damit der Tag vom Reader nicht mehr gelesen werden kann. Ähnliche Effekte können auch durch nicht leitende Materialien hervorgerufen werden.

Konstruktion und Auswahl der Tag-Antennen ist also sehr bestimmend für den Erfolg der angestrebten Auto-ID-Funktionen.

5.2 Air Interface und Pulkerfassung

Das Air Interface beschreibt die Verbindung zwischen Reader und Tag. Dabei werden verschiedene Ebenen der Verbindung unterschieden. Physikalisch werden Reader und Tag über eine elektromagnetische Welle verbunden. Damit Reader und Tag kommunizieren können und Informationen übertragen werden, muss die Welle moduliert werden. Die Art der Modulation sowie die Form des aufmodulierten Signals gehören ebenso zur Air-Interface-Spezifikation wie die Struktur der übertragenen Kommandos, während die Kommandos selbst nicht mehr Bestandteil des Air Interfaces sind.

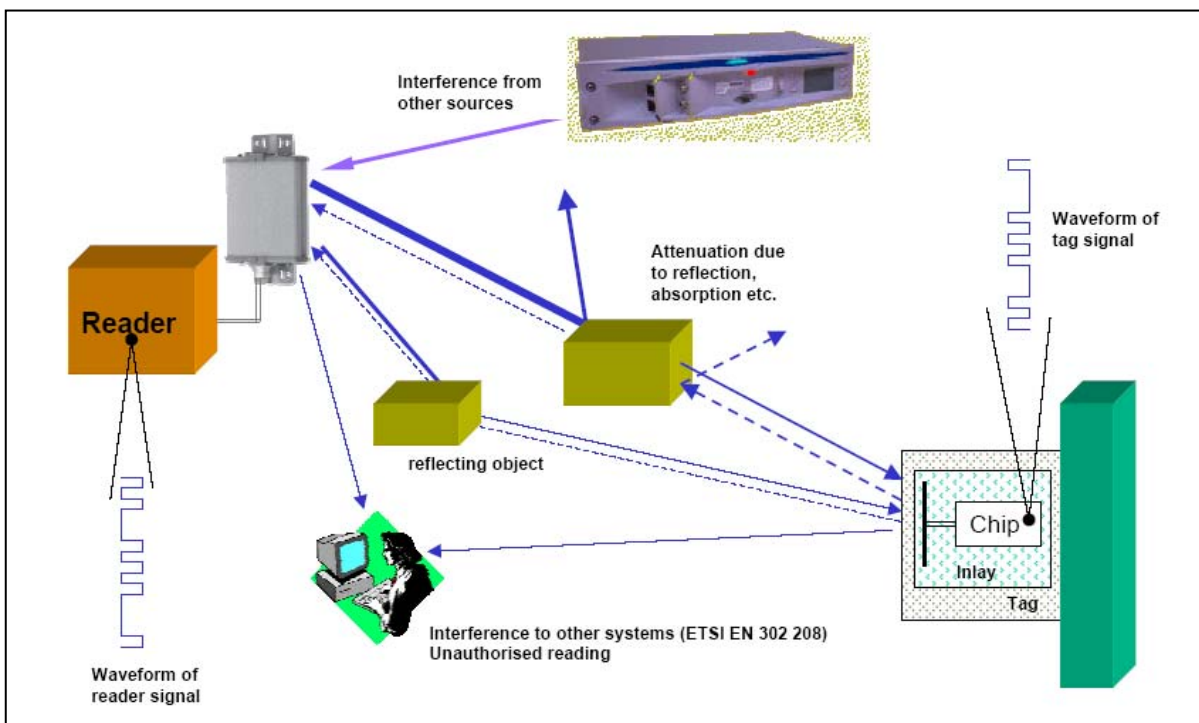


Abbildung 12: Reflexionen im Bereich der Reader-Antenne

Quelle: Kathrein

Damit Tags in offenen RFID-Systemen weltweit gelesen werden können, ist es notwendig, dass nicht nur globale Standards für das Air Interface existieren, sondern auch für die Frequenzbereiche, in denen die RFID-Systeme arbeiten. Diese müssen von den Regulierungsbehörden harmonisiert und für die entsprechende Nutzung freigegeben sein. Im HF-Bereich ist die Frequenz 13,56 MHz weltweit verfügbar. Im UHF-Bereich wird in Europa die Frequenz 868 MHz verwendet, in den USA dagegen 915 MHz. Einer Harmonisierung stehen die jeweiligen Mobilfunk-Frequenzen entgegen.

Da Reader Sendeantennen sind, dürfen sie nur in den jeweils zugewiesenen Frequenzbändern arbeiten. Daher müssen UHF-Tags für die weltweite Nutzung so beschaffen sein, dass sie im gesamten Frequenzbereich von 860 bis 960 MHz arbeiten können. Das stellt hohe Anforderungen an die Tag-Antenne und erhöht den Preis der Tags. Im HF-Bereich wird bei geringem Leseabstand üblicherweise das Nahfeld-Verfahren für die Kommunikation zwischen Reader und Tag angewandt. Die elektromagnetische Verbindung besteht daher aus einer

relativ einfachen magnetischen Kopplung. Objekte in der näheren Umgebung haben nur einen geringen Einfluss auf die Kopplung. Die Stärke der Kopplung wird im Wesentlichen durch den Abstand zwischen Reader- und Tag-Antenne sowie Lage und Orientierung der beiden Antennen bzw. Spulen zueinander bestimmt.

Im UHF-Bereich mit den gewünschten großen Lesereichweiten sind die Verhältnisse wesentlich komplexer. Fremdobjekte hinter dem Tag Objekte oder stärker noch im Messfeld beeinflussen das gesamte System Reader-Tag. Die Effekte reichen von einfacher Dämpfung über Reflexion und Brechung bis hin zur Streuung der elektromagnetischen Welle. Die Vielfalt der möglichen Störeffekte verlangt, dass sich während der Lesevorgänge keine Objekte zwischen Reader und Tag befinden. Ausnahmen sind dünne nicht leitende Schichten sowie Materialien mit geringer Dämpfung und niedriger Dielektrizitätskonstante wie Papier, lockere Stoffe, geschäumtes Polystyrol u.ä. Weiterhin kann es passieren, dass Tags gelesen werden, wenn sie sich unter einer trockenen Plane befinden. Ist dieselbe Plane aber nass, so ist die Wahrscheinlichkeit hoch, dass die Tags nicht mehr gelesen werden.

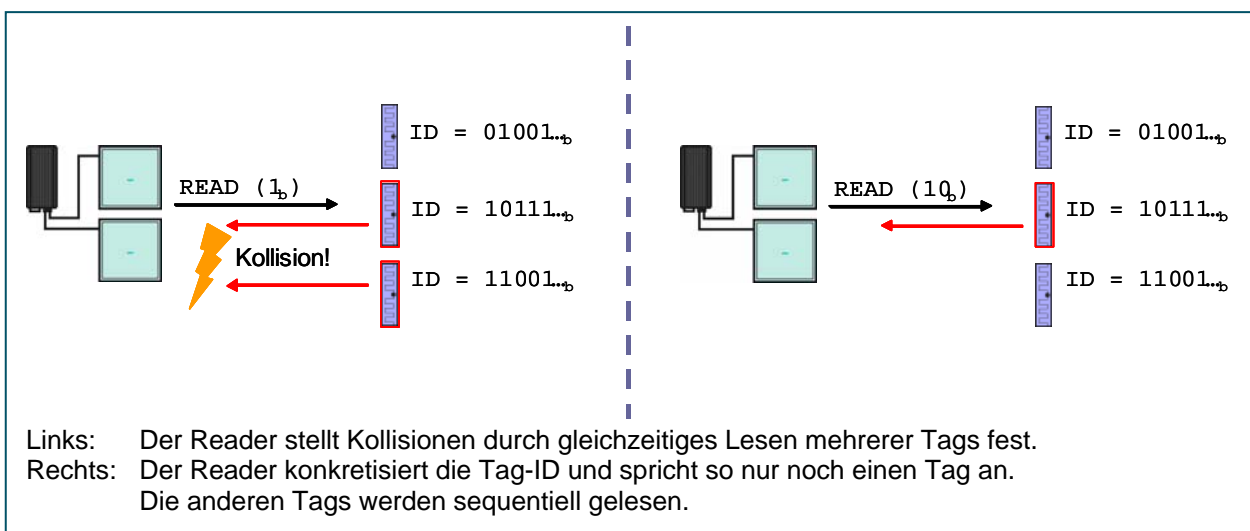


Abbildung 13: Das Anti-Kollisions-Protokoll des RFID-Readers

Quelle: Siemens

Kritisch ist auch die Lage von Reader- und Tag-Antenne zueinander beim Lesevorgang. Die optimale Konfiguration und Justierung der Reader-Antenne zum Beispiel am Lagertor muss deswegen jeweils ermittelt werden.

Die Kommunikation zwischen Reader und Tag erfolgt über die Antennen und einen definierten Befehlssatz (Command Set). Das Kommunikationsprotokoll ist so definiert, dass zuerst der Reader ein Kommando schickt, auf das der Chip antwortet. Das Command Set umfasst Befehle zum Lesen und Schreiben, zur Steuerung des Anti-Kollisionsprotokolls, zum Sperren einzelner Speicherzellen und zum Deaktivieren des Chips (Kill-Befehl).

Pulkerfassung bedeutet, dass sich eine Vielzahl von Tags zur selben Zeit im Messfeld befinden und nahezu gleichzeitig gelesen werden. Dafür dient das Anti-Kollisionsprotokoll. Es sorgt dafür, dass beim Lesen ein Teil der Tag-ID vom Reader im Read-Kommando vorgegeben wird. Solange mehr als ein Tag antwortet, erweitert der Reader die ID um weitere Stellen, bis schließlich nur noch ein einzelner Tag reagiert. Der identifizierte Tag wird dann abgeschaltet. Dieses Protokoll erlaubt die Bearbeitung von bis zu 100 Tags pro Sekunde.

Die Lesbarkeit der Tags hängt stark von den Materialien, der Struktur und den Orten ab, an denen sie sich befinden. So ist es unmöglich einen UHF-Tag zu lesen, der von metallischen Gegenständen, Flüssigkeiten oder anderen stark leitenden oder stark reflektierenden Materialien umgeben ist. Ein Tag muss daher immer außen am Pulk – z. B. an einer Palette -

angebracht werden. Er darf höchstens von Papier, von geschäumtem Polystyrol oder ähnlichen Materialien abgedeckt werden.

5.3 Reader und Antenne

5.3.1 Reader-Aufbau

Zum Schreiben und Lesen der Tag-Informationen wird eine RFID-Reader-Antennen-Einheit benötigt. Dazu gehören die Antennen sowie das eigentliche Schreib-Lesegerät. Zur besseren Erkennung der Tags können an ein Gerät oftmals mehrere Antennen angeschlossen werden. Die Reader unterscheiden sich je nach Anwendungszweck und Umgebungsbedingungen in ihrer funktionalen und technischen Ausprägung:

- **Gate Reader**
Montage an Verladetoren oder Durchfahrten von Lastwagen oder Gabelstaplern. Hier kommt es auf die zuverlässige Erkennung bei großen Abständen oder unterschiedlichen Positionierungen der Tags an. Gate Reader arbeiten in der Regel mit mehreren Antennen.
- **Compact Reader**
Antenne und Schreib-Lesegerät sind in einem kompakten Gehäuse kombiniert. Dieser Reader-Typ bildet eine kostengünstige Alternative zum Gate Reader, wenn kürzere Abstände zu den Tags und unproblematische Bedingungen vorliegen
- **Fahrzeuggebundene Reader**
zur Montage an Fahrzeugen, z.B. Gabelstaplern
- **Mobile Reader**
Handgeräte zur mobilen Verwendung. Diese Geräte übertragen entweder die gelesenen Tag-Daten sofort über eine Funkverbindung (z.B. WLAN) oder sammeln die Daten in einem eingebauten Speicher. Von dort werden die Daten nach dem Einsetzen des Gerätes in eine Docking-Station z. B. zu einem PC übertragen. Aus dem Anwendungszweck ergeben sich weitere Anforderungen, z. B. an die Schutzart der Geräte. So benötigen Reader und Antennen an Verladetoren eine hohe Temperaturtoleranz und Schutz gegen Staub und Feuchtigkeit. Zur Integration in die höheren (Software-) Schichten der RFID-Architektur, zur Konfiguration und zur Diagnose müssen die RFID-Reader geeignete Schnittstellen unterstützen, z.B.:
 - Für WLAN und Internet (über Ethernet und TCP/IP).
 - Für Punkt-zu-Punkt-Verbindungen: RS422 zur Anbindung an speicher-programmierbare Steuerungen (SPS) oder RS232.
 - Für die mobile Kommunikation: GSM, GPRS oder UMTS.

Daneben gibt es bei einigen Readern Anschlussmöglichkeiten, um einfache Prozess-Steuerungen vorzunehmen, z. B. digitale Ein- und Ausgänge mit 24 V. Diese können zur Ansteuerung von Ampeln oder Schranken verwendet werden, die zur Freigabe nach Prüfung der Tag-Daten am Warenein- oder -ausgang dienen. Auch einfache SPS-Kopplungen sind damit realisierbar. Höheren Protokollschichten sind derzeit noch nicht standardisiert, das hat zusätzlichen Aufwand bei der herstellerübergreifenden Integration der Reader zur Folge hat. Hier ist eine gemeinsame Initiative der RFID-Anbieter wünschenswert.

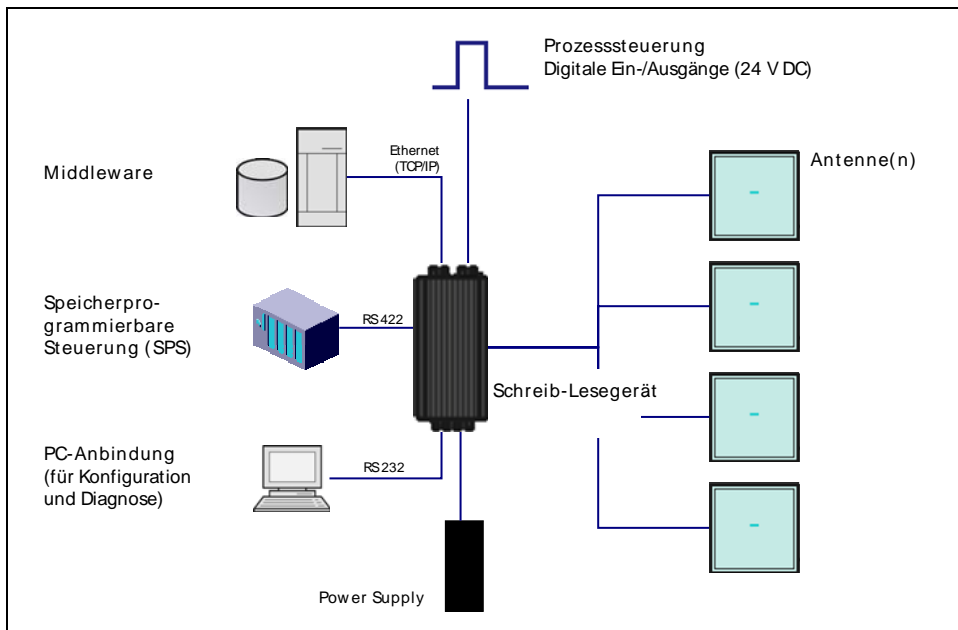


Abbildung 14: Typisches Anschluss-Schema eines Readers mit RFID-Antennen
Quelle: Siemens

■ Funktionale Anforderungen

Funktional besteht zunächst die Anforderung, eine ausreichend hohe Leserate und Lesezuverlässigkeit zu bieten. Dies hängt von Parametern ab wie Anzahl und Ausrichtung der Antennen, Art der verwendeten Tags, Menge der gespeicherten Daten, Positionierung der Tags usw. Unter guten Bedingungen können bis ca. 100 Tags pro Sekunde erkannt werden.

Werden mehrere Tags gleichzeitig in das Feld eingebracht, wird zunächst die Pulkerkennung eingesetzt, die den Datenstrom sequenzialisiert und so kollisionsfrei die Tag-IDs erkennen kann. Beim Lesen größerer Datenmengen, aber vor allem beim Schreibzugriff, wird das Multi-Tag-Handling eingesetzt, das die gezielte Ansprache einzelner Tags erlaubt.

Werden mehrere Reader eingesetzt, kann es durch Über-Reichweiten und Reflexionen zu wechselseitigen Störungen kommen. Die Abbildung 16 zeigt ein einfaches Beispiel, bei dem sich jeweils die Felder zweier nebeneinander aufgebauter Reader überlagern. In der Praxis können aufgrund von Reflexionen an Gebäudeteilen jedoch erheblich komplexere Szenarien auftreten. Diese Störungen haben ebenfalls Erkennungsfehler zur Folge. Über die Device-Managementfunktion der überlagerten Software-Schicht müssen die Reader deshalb synchronisiert werden.

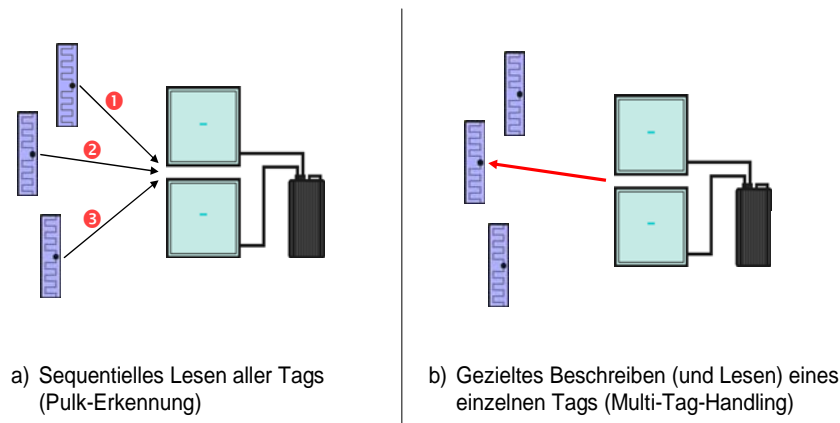


Abbildung 15: Pulk-Erkennung und Multi-Tag-Handling

Quelle: Siemens

Je nach der genauen System-Auslegung kann in den Readern bereits eine Vorverarbeitung der Daten stattfinden. Dabei können Tag-Daten nach vorgegebenen Mustern gefiltert werden, um z. B. nur die an Paletten angebrachten Tags zu lesen, nicht aber Tags an den einzelnen Produkten. Auch die Filterung über eine gewisse Zeitspanne ist denkbar, so dass die Tag-Informationen nur einmal in einem definierten Zeitfenster übertragen werden. Damit können „Löcher“ im Feld ausgeglichen werden, die andernfalls zur Mehrfach-Erkennung führen. Beide Funktionen dienen dazu, die Datenmenge auf dem Netzwerk zu reduzieren.

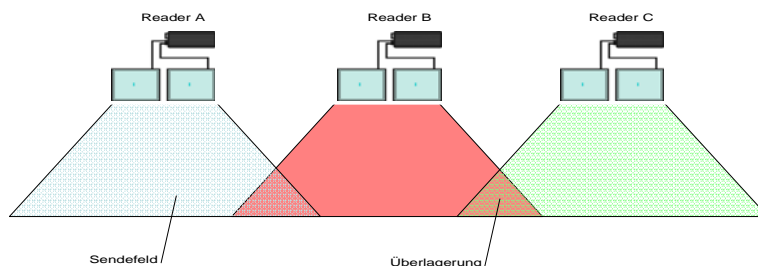


Abbildung 16: Überlagerung der Felder von RFID-Readern

Quelle: Siemens

Schließlich bieten einige Reader die Software-gestützte Konfiguration verschiedener Parameter, z. B. der Sendestärke (zur Begrenzung der Reichweite). Diese Parameter werden im Reader gespeichert.

5.3.2 Reader-Antenne

Die Reader-Antenne stellt die Verbindung zwischen der Readerelektronik und der elektromagnetischen Welle des Raumes her. Im HF-Bereich handelt es sich wie beim Tag um eine Spule. Diese wird so gestaltet, dass eine möglichst starke Kopplung mit der Antenne des Tags erzielt werden kann.

Im UHF-Bereich gibt es wie beim Tag eine Vielzahl von möglichen Antennenkonstruktionen. Für große Leseabstände setzt man stark bündelnde Antennen mit hohem Gewinn ein. Da üblicherweise die Sendeleistung zuzüglich Antennengewinn, d. h. die in eine bestimmte Richtung abgestrahlte Maximalleistung, durch die Regulierungsbehörden begrenzt wird, muss die vom Reader an die Antenne abgebenen Sendeleistung entsprechend geregelt werden. Für

stark bündelnde Antennen spricht, dass es oft notwendig ist, die Leistung des Readers nur in die Raumbereiche abzustrahlen, in denen sich die zu lesenden Tags befinden.

Im Allgemeinen ist der Gewinn einer Antenne aufgrund physikalischer Zusammenhänge mit der Größe der Antenne verknüpft. Je größer der Gewinn bzw. je kleiner der Raumwinkel, in den die Antenne abstrahlt, umso größer wird die mechanische Konstruktion der Antenne. Stark bündelnde Antennen kommen daher bei Handheld-Readern nicht zum Einsatz. Typische Antennen die bei Handheld-Readern zum Einsatz kommen, sind Patch-Antennen, Halbwellen-Dipole oder Wendelantennen.

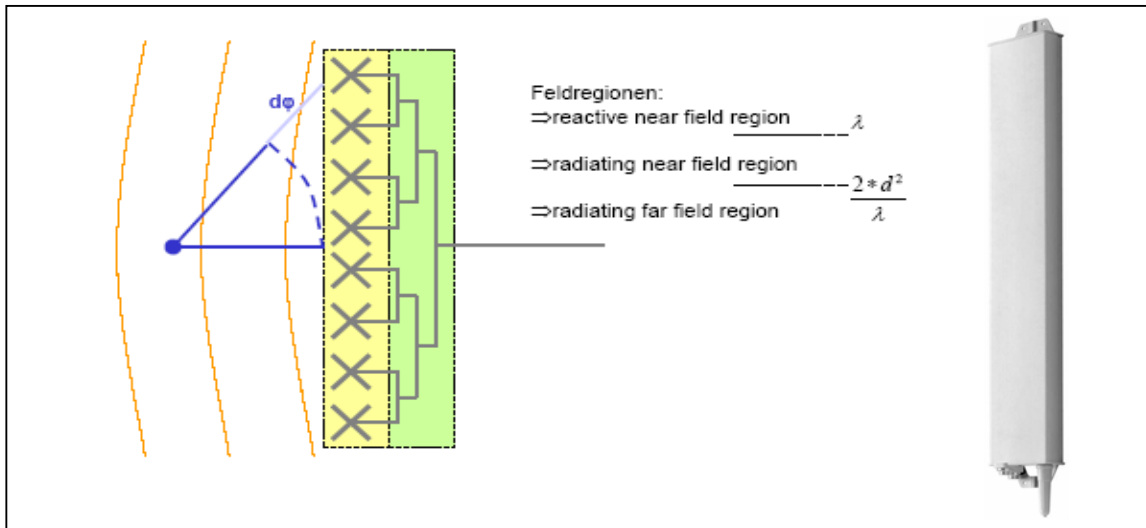


Abbildung 17: Reader-Antenne mit Antennen-Array und Feldregionen

Quelle: Kathrein

Bei stationären Readern können größere Antennenkonstruktionen eingesetzt werden. Diese werden im UHF-Bereich üblicherweise als Arrays ausgeführt (s. Abb. 17), d. h. mehrere kleine Strahlerelemente werden so zusammen geschaltet, dass sich in der gewünschten Richtung eine Aufsummierung der Wellenanteile ergibt. Das Fernfeld dieser Antennen hängt von der Größe ab. Erst wenn der Abstand zur Antenne so groß ist, dass die Differenzen der Wege von den einzelnen Strahlern im Vergleich zur Wellenlänge vernachlässigbar sind, wirkt das Fernfeld.

Nahe an der Antenne ist das Feld nicht mehr homogen und es kann vorkommen, dass ein Tag nicht gelesen wird, weil er sich im Bereich sehr niedriger Feldstärke befindet. Insbesondere bei Lagertoren, die mit Reader-Antennen ausgerüstet werden, ist ein Einsatz stark bündelnder Antennen nicht in jedem Fall angebracht. Besser sind speziell adaptierte Antennen, die ein möglichst homogenes Messfeld generieren.

6 IT-Infrastruktur

6.1 Middleware und serviceorientierte Architektur (SOA)

Der Begriff SOA (Serviceorientierte Architektur) hat in den letzten Jahren an Bedeutung gewonnen. SOA hat das Ziel, dem Anwender flexibel und aufgabengerecht strukturierte IT-Systeme und IT-Dienste zur Verfügung zu stellen, die kostengünstig gewartet werden können. Sie werden die Geschäftsprozesse optimal und unternehmensweit integriert unterstützen und für eine möglichst umfassende Interoperabilität der beteiligten IT-Systeme sorgen. Die Verarbeitung von Events, also Real-time-Informationen, die z. B. durch RFID-Lesevorgänge ins System gelangen, ist dabei ebenso einzubeziehen wie die Nutzung des Internets als globales Kommunikationsnetzwerk. Eines der bekannten Instrumente für die Realisierung von SOA ist der Internet-Standard XML (Extended Markup Language), der der durchgängigen Strukturierung von Informationen dient, gleichgültig wie sie medial dargestellt werden.

In einer SOA-Umgebung erfolgt die Kommunikation der operativen Anwendungssysteme über Service Interfaces und nicht über bidirektional vereinbarte Schnittstellen. So können Änderungen an den einzelnen Software-Komponenten flexibel vorgenommen werden (z. B. Software Updates oder die Verlagerung dezentraler Services in ein zentrales Rechenzentrum), ohne dass diese sich auf andere Systeme auswirken und ohne dass jedes Mal umfangreiche Integrationstests vorgenommen werden müssen.

Klassische Middleware funktioniert auch ohne SOA, kann aber dann nicht auf die oben beschriebene Flexibilität zurückgreifen und macht die Systeme folglich unflexibler und wartungsaufwändiger.

RFID-Middleware verbindet die RFID-Reader-Ebene mit den Geschäftsanwendungen. Sie muss RFID-Events verarbeiten und den Geschäftsanwendungen so präsentieren, dass diese dort weiter verarbeitet werden können. Im Falle eines bisher nicht RFID-fähigen Anwendungssystems für Lagerverwaltung bedeutet das z. B., dass die Aggregation von individuellen Items (z. B. viele Artikel in einem Karton) zu Gruppen (Anzahl gleichartiger Kartons) und umgekehrt vollzogen wird, ehe die Events an die Anwendung weitergegeben werden.

Weiterhin ist die Middleware verantwortlich für die Kontrolle über die RFID-Physik (Reader, Antennen etc.). Es geht dabei um Rückmeldungen an die Feedback-Geber und Überwachung der Sensoren (Lichtschranken, Zeitgeber, Bewegungsmelder), da dies mit der ursächlichen Prozesslogik zunächst nicht zu verbinden ist. Die Middleware synchronisiert diese Events mit den RFID-Leseergebnissen und sorgt dafür, dass Doppellesungen entsprechend der Fachspezifikationen entweder zugelassen oder eliminiert werden. Die Zahl der erzeugten Nachrichten im LAN oder WAN muss dabei auf einem Minimum gehalten werden. Nicht alle RFID-Leseergebnisse müssen an das Warenwirtschaftssystem übertragen werden.

SOA dient also auch der vereinfachten Konfiguration und Anpassung der Software an unterschiedliche Einsatzgebiete. Mit Software-Entwicklungswerkzeugen können die einzelnen Services entsprechend den Prozesserfordernissen orchestriert werden. Webservices, XML, Message Queuing und Workflow sind Elemente einer serviceorientierten Architektur und einer RFID-Middleware, die für die Kopplung verschiedener Services Verwendung finden.

6.2 Schichtenmodell für das Real-time Enterprise

Im letzten Abschnitt wurde der Begriff SOA kommentiert. Eine umfassende Software-Architektur zur Einbeziehung von RFID-Lösungen besteht z. B. aus fünf Schichten (Layer 0 bis 4), wie sie in Abb. 18 dargestellt sind.

Je nach Erfahrungshintergrund der Verfasser werden in diesem Kontext eine Reihe verschiedener Begriffe verwendet, die letztlich Aspekte eines gemeinsamen Gesamtbildes sind. So auch der Begriff "Real-time Enterprise", der auf der obersten Ebene (Layer 4: Anwendungsebene) der o. a. Abbildung eingeordnet ist. Auch die Anzahl der Ebenen, in die Systemarchitekturen aufgegliedert werden, differiert. Gleichwohl besteht ein hoher Grad der Kongruenz, wenn man die einzelnen Funktionsbausteine der Ebenen vergleicht. Solche Schichtenmodelle sind sinnvoll, um eine Ordnung in die Architektur von Informationssystemen zu bringen, die aus Komponenten ganz verschiedener Hersteller zusammengesetzt sind. Den Schichten sind folgende Funktionsbausteine zuzuordnen:

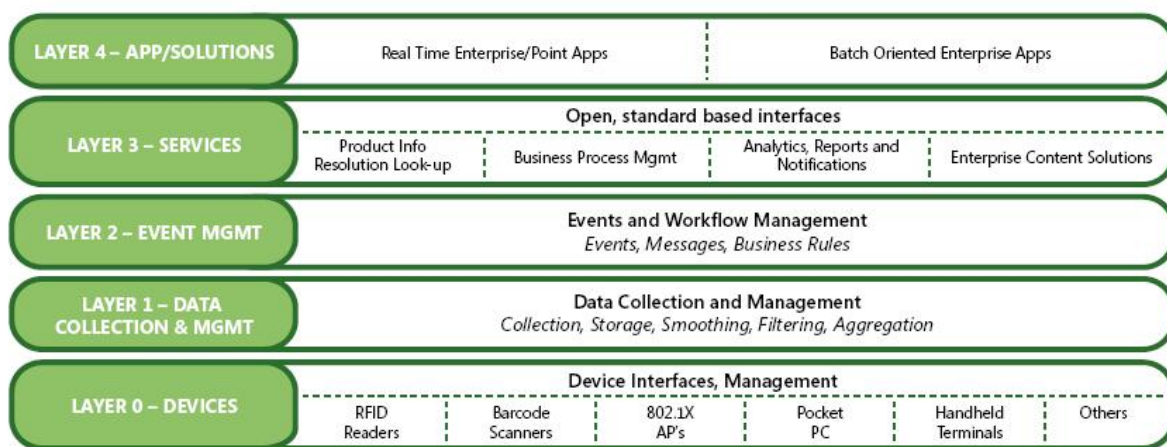


Abbildung 18: Ebenen einer Software-Architektur für das Real-time Enterprise

Quelle: Microsoft

- Schicht 0: Geräte
Hardware: Endgeräte wie RFID-Reader, Printer, Handheld Terminals u.a.
- Schicht 1: Datensammlung und –management
Die gesamte Hardwareinfrastruktur, Betriebssysteme, Netzwerke, und andere Komponenten dienen dazu, RFID zu unterstützen. Filtermechanismen, die mehrfach gelesene RFID-Tags erkennen und unerwünschte Daten filtern.
- Schicht 2: Event-Management
Diese und die darüber liegenden Schichten ermöglichen den Geschäftsprozessen und -Lösungen die Nutzung der real-time erzeugten RFID-Informationen. Hier findet die Integration mit anderen Services, Geschäftspartnern und dem EPCglobal-Netzwerk statt.
- Schicht 3: Services
Diese Schicht kann als Anwendungsprogramm-Schnittstelle (API) oder als auf offenen Standards basierender XML-Webservice ausgeführt werden, z.B. für den Look-up-Service zur Gewinnung von Produktinformationen aus Produktkatalogdatenbanken, die in Schicht 2 gelegen sind. Weitere hier angesiedelte Services: Business Intelligence, Analyse und Reports sowie Ereignis-Benachrichtigungen (Alerts).

- Schicht 4: Anwendungen
Spezifischen Unternehmensanwendungen bzw. ERP-Systeme mit dem strategischen Ziel, das Real-time Enterprise zu unterstützen.

XML Web Services ist ein wichtiger Middleware-Standard für die Interoperabilität verschiedener Systeme, der in Schicht 2 angeordnet ist. Er basiert auf dem XML-Standard. Die Komponenten Web Services Description Language (WSDL) für die Beschreibung solcher Services und das Simple Object Access Protocol (SOAP) für die Kommunikation stehen auf nahezu allen Systemplattformen zur Verfügung. Gleichwohl ist XML Web Services ein noch fließender Standard. Es müssen noch weitere Funktionsbereiche standardisiert werden, um die herstellerübergreifende Kompatibilität sicher zu stellen: Quality-of-Services für die RFID-Integration, Skalierbarkeit, zuverlässige Nachrichtenlieferung, Load-Balancing, Fehlertoleranz, Sicherheit u. a. Dies ist jedoch ein Sachverhalt, der immer mit aufkommenden neuen Technologiefeldern einhergeht. Er sollte die Anwender nicht daran hindern, schon jetzt innovative Anwendungen zur Nutzung von RFID-Verfahren zu implementieren.



Abbildung 19: Implementierung der Global Data Synchronization (GDS)

Quelle: Microsoft

Die Integration mit dem EPCglobal-Netzwerk und die damit verbundene Global Data Synchronization (GDS) finden in Schicht 2 statt. Die dafür notwendige Kommunikation erfolgt auch über XML und Web Services.

6.3 Event-Architektur

Mithilfe von Auto-ID/RFID ist die Maschine-zu-Maschine-Kommunikation möglich, also die automatische eventgesteuerte Kommunikation. Daten werden hier real-time zur Verfügung gestellt und verarbeitet. Auto-ID bzw. RFID hat starken Einfluss auf die Gestaltung von Prozessen. Diese müssen optimiert werden, um den Ansprüchen an Transparenz, Flexibilität, Produktivität, Agilität und Effizienz zu entsprechen. Mithilfe einer Event-Architektur werden die Daten dynamisch erfasst und ggf. verdichtet, die Informationen dargestellt und event-getrieben an die entsprechenden Applikationen zur Verarbeitung weitergegeben. Dies soll schnell, mit geringen Integrationsaufwand und kostentransparent möglich sein.

Über die Maschine-zu-Maschine-Kommunikation und das automatische Erfassen von Item-Informationen werden Events und aus dem Prozess erzeugte Statusmeldungen automatisch weitergeleitet oder stoßen weitere Aktionen an. Hierzu wird eine entsprechende Infrastruktur und Architektur benötigt. Die nachfolgend beschriebene Architektur bezieht sich auf ein Outsourcing-Modell, also auf den Betrieb der IT-Systeme bei einem Service-Rechenzentrum. Die gleichen Komponenten können natürlich auch vor Ort im eigenen Unternehmen betrieben werden. Bei der Implementierung der Event-Steuerung gibt es immer zwei Möglichkeiten:

- Die Middleware übernimmt die Event-Steuerung und reduziert damit den Integrationsaufwand und den Zeitaufwand für die Implementierung (nachfolgend beschrieben). Von diesem Modell wird hier ausgegangen.
- Die Event-Steuerung wird von bestehenden ERP-Applikationen (Legacy Applications) übernommen. Dafür müssen bestehende Prozesse innerhalb vorhandener Applikationen mit hohem Aufwand geändert und den optimierten Prozessen angepasst werden. Funktionen aus Schicht 2, nämlich die Managed Auto-ID-Services, müssten in Systeme der Schicht 3 integriert werden. Diese Vorgehensweise ist nicht zu empfehlen und wird hier nicht weiter beschrieben.

Auf jeden Fall sollte zur Entscheidungsfindung eine Kosten-Nutzen-Analyse durchgeführt werden.

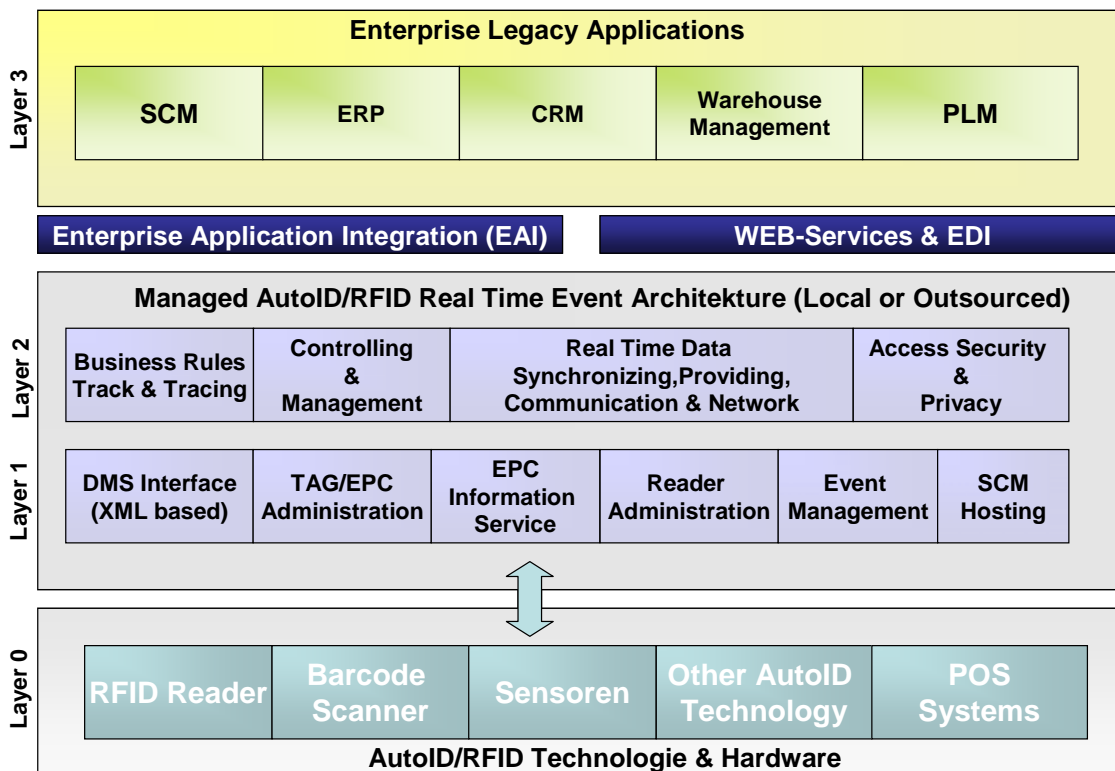


Abbildung 20: Auto-ID-Event-Architektur
Quelle: T-Systems

Es folgt die Beschreibung der Schichten (Layer) und Elemente der abgebildeten Event-Architektur:

- **Schicht 0**
Erfassungsgeräte für Auto-ID-Informationen.
- **Schicht 1 und 2**
Managed Auto-ID / RFID-Real-Time-Event-Architecture
 - DMS Interface
Informationen liegen oft nicht als reine Daten vor, sondern als Dokumente. Ein XML Interface ermöglicht die Anbindung an ein Dokument-Management- (DMS) oder Archivsystem, um diese Dokumente nach vorgegeben Kriterien zu speichern,
 - TAG/EPC Administration
Administration der eingesetzten Auto-ID-Komponenten und EPC-

Verzeichnisdienste, ggf. Verbindung zu dezentralen EPC-Verzeichnissen, -Diensten oder -Datenbanken (z. B. für Food Safety / Warenrückverfolgung)

- EPC Information Service (EPCIS)
Speicherung der Produktdaten (z.B. Herstellungsdatum, Verfallsdatum etc.) in einer Datenbank.
- Reader Administration
Administration der eingesetzten Auto-ID-Reader (RFID, Barcode, Biometrie etc.) und deren Interfaces
- Event Management
Scripting Engine zur Erstellung, Verwaltung und Durchführung automatischer Events (Input/Output).
- SCM Hosting
Hosting bzw. Outsourcing einer Supply-Chain-Management-Umgebung für dezentrale Standorte oder mittelständische Unternehmen.
- Geschäftsregeln / Tracking & Tracing
Abbildung der Geschäftsregeln (Festlegung der Aktionen zu einem Event) und Berichtsfunktion für das Suchen und Verfolgen der Objekte mit RFID-Tags.
- Controlling und Management
Bereitstellung von Controlling-Funktionen zur Auswertung der abgebildeten Prozesse (Key Performance Indicators / KPI) und vollständiges Management von Architektur und Plattform.
- Real-time Data Synchronizing, Providing, Communication & Network
Bereitstellung und Synchronisierung der Informationen, aufgrund der auf die Events bezogenen Geschäftsregeln. Communication Interface zu Anwendungen und Netzwerken, z. B: Festnetz, Mobilfunknetz, Internet / IP.
- Access Security & Privacy
Festlegung der Zugriffsrechte und Abhängigkeiten für Nutzer und Anwendungen (innerhalb der M2M-Kommunikation). Abgrenzung der einzelnen Mandanten und deren Daten und Informationen.

■ Layer 3: Enterprise Legacy Applications

Betriebswirtschaftliche Anwendungen (ERP). Diese kommunizieren direkt mit der Event-Architektur. Dadurch, dass die Event-Informationen und Prozesse in der Middleware abgelegt und abgearbeitet werden, ist hier der Aufwand der Systemintegration minimiert. Die Optimierung des betriebswirtschaftlichen Prozesses in dieser Schicht entfällt natürlich nicht.

In der Abbildung 21 wird ein umfassender Produktionsprozess im Automotive-Sektor gezeigt: von der Produktion von Teilen über die Montage von Fahrzeugen bis zum Verkauf. Dieser Prozess überspannt mehrere Unternehmensbereiche bzw. mehrere Unternehmen (verschiedene Farben). Jedes Glied in dieser Prozesskette muss optimal funktionieren, damit das Ganze zielgerecht arbeiten kann. Damit die Überwachung der einzelnen Prozessschritte real-time – also eventorientiert – stattfinden kann, werden entsprechende Daten künftig durch RFID- oder andere Auto-ID-Verfahren automatisch erhoben und dem System zur Kontrolle der Prozesse zugeleitet (Stichworte mit gestrichelten Verbindungen). Die mit bisherigen manuellen Verfahren verbundene Zeitverzögerung der Datenverfügbarkeit und ihre Unvollständigkeiten entfallen damit. Dies ist ein wesentlicher Schritt zum Real-time- Enterprise.

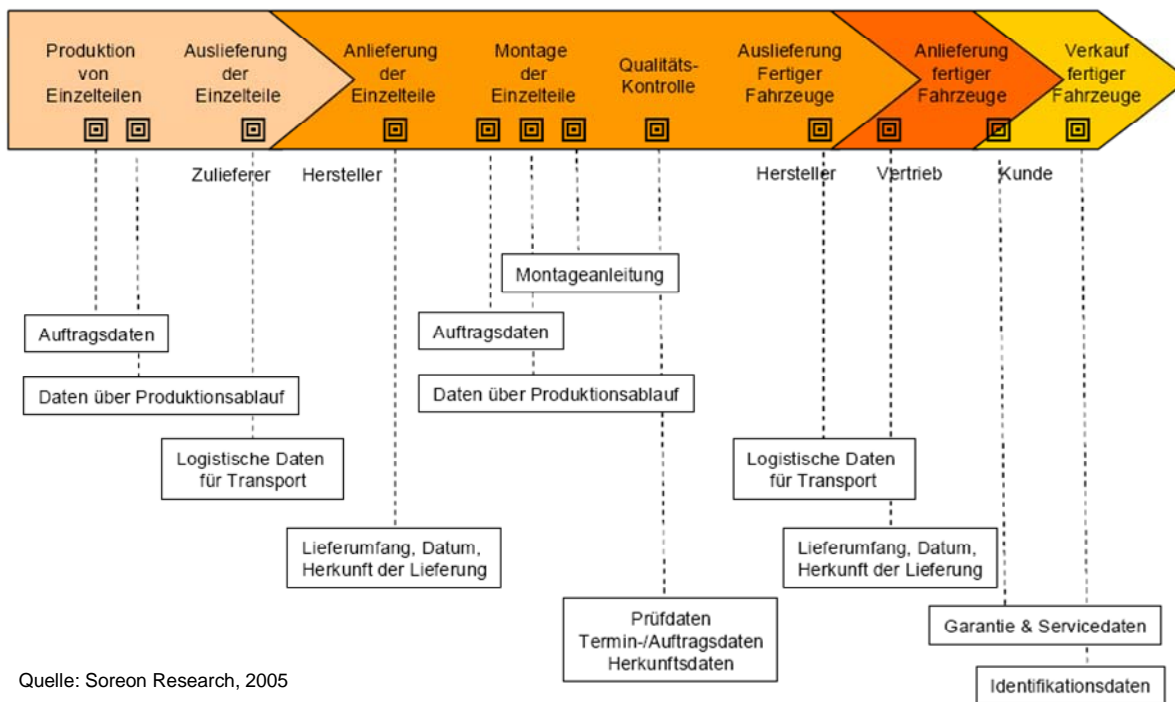


Abbildung 21: Event-Informationen in einer Automotive-Prozesskette

6.4 Das Middleware-Konzept Savant von EPCglobal

Die Savant-Software war ursprünglich die eigentliche Middleware-Komponente des EPCglobal-Netzwerkes. Ihre Hauptaufgabe sollte sein, die Datenströme von den Readern und anderen Sensoren zu verarbeiten und an die entsprechenden Anwendungen weiterzuleiten. Savant sollte auch die von den Readern generierten Datenmengen filtern, aggregieren und den entsprechenden Unternehmenssoftwaresystemen zur Verfügung stellen, ohne diese mit großen Datenmengen zu überlasten.

Die Savant-Software sollte als Open Source zur Verfügung gestellt werden. Diese Pläne wurden jedoch nicht weiter verfolgt. Vielmehr hat EPCglobal sich dazu entschlossen, keine Referenzimplementation oder Softwarespezifikation zu liefern, sondern lediglich die Schnittstelle zwischen RFID-Middleware und Anwendungssoftware zu normieren. Wie RFID-Middleware die einzelnen Funktionen, z.B. das Filtern der EPC-Daten, implementiert, bleibt damit den jeweiligen Software-Anbietern überlassen.

Die Schnittstelle zwischen RFID-Middleware und Applikation wird von EPCglobal als Application Level Events Specification (ALE) bezeichnet. Diese enthält Funktionalität, die das einfache Filtern und Bündeln der aggregierten Daten unterstützt. So können Filter spezifiziert werden, die nur EPCs mit bestimmten Bitmustern weiterleiten. Außerdem sind Filter angedacht, die die mehrfache Erkennung eines RFID-Transponders in einem kurzen Zeitraum zu einem einzigen Eingangsereignis bündeln. Durch eine Verknüpfung solcher Filter sollten die Daten, die von den verschiedenen angeschlossenen Readern geliefert werden, aufbereitet und in die entsprechenden Ereignisse für die Anwendung umgewandelt werden. So könnte beispielsweise eine Vielzahl von Transpondererkennungen an einem Lesegerät in ein einziges Wareneingangsereignis für eine Lieferung zusammengefasst werden.

Auch wenn die Savant-Software von EPCglobal nicht lieferbar ist, so sind doch entsprechende Software-Komponenten im Markt verfügbar, die eine sinnvolle Behandlung dieser Auto-ID-Vorgänge ermöglichen.

6.5 Datenbanken

Mit RFID können Unternehmen ihre Vermögenswerte genauer verfolgen und überwachen, größere Transparenz in ihren Betrieben und Real-time-Information für die Entscheidungsfindung gewinnen. Eine Voraussetzung dafür ist, dass die durch RFID-Verfahren gewonnenen Daten sachgerecht gespeichert und zuverlässig für die Nutzung bereitgestellt werden.

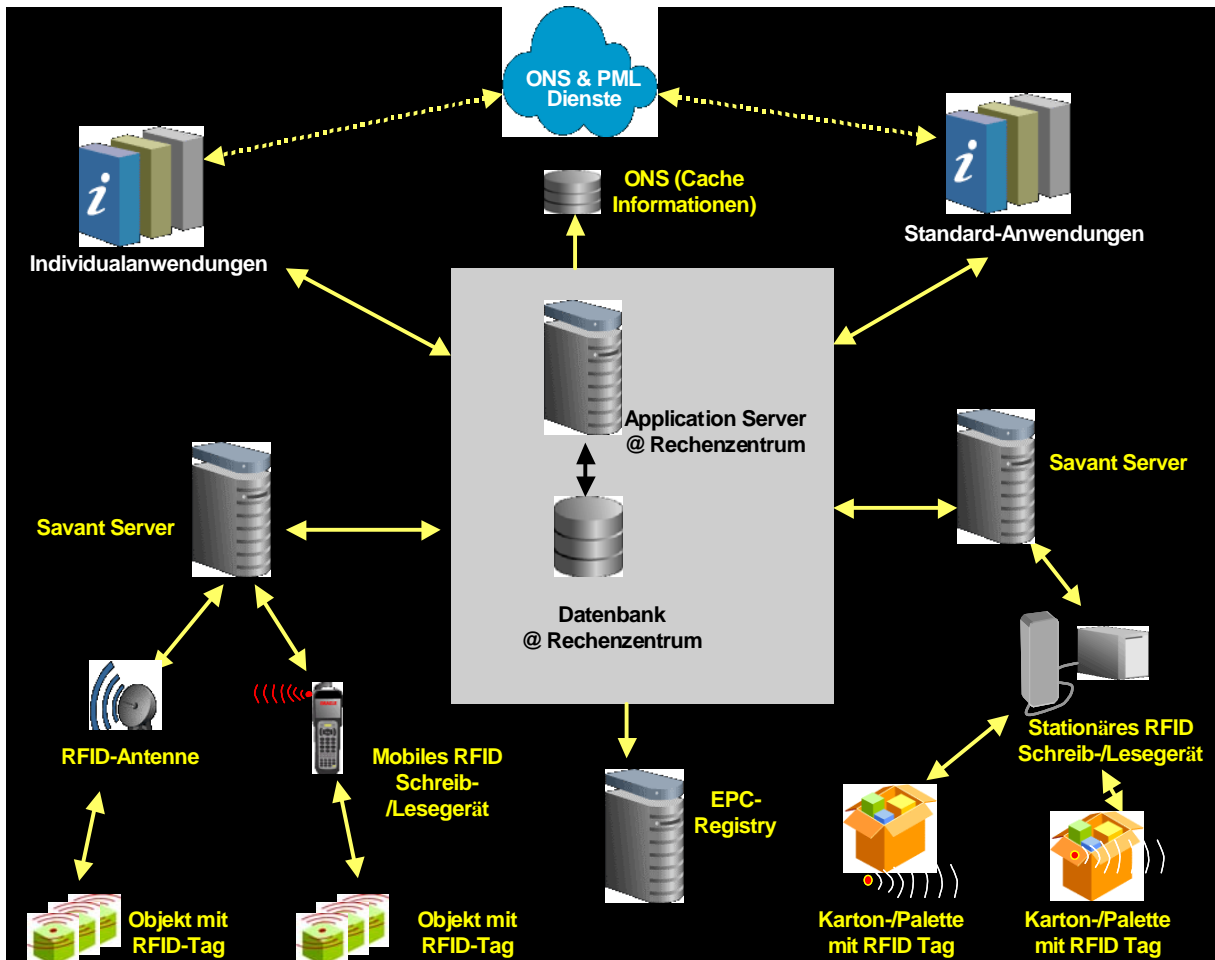


Abbildung 22: EPCglobal-orientierte RFID-Anwendungs- und Kommunikationsstruktur
Quelle: Oracle / GS1 Germany / EPCglobal

Die Abbildung 22 zeigt am Beispiel einer EPC-orientierten Architektur, wie komplex der Lauf der Daten durch IT-Systeme sein kann, die mit RFID-Verfahren arbeiten. RFID-Daten werden hier über RFID-Middleware-Server dem zentralen Rechenzentrum eines Unternehmens zugeleitet. Im Rechenzentrum werden die klassischen Geschäftsanwendungen betrieben. Dabei ist generell zwischen zentralem und dezentralem Datenmanagement zu unterscheiden. Beim zentralen Datenmanagement wird lediglich eine Identifikationsnummer eines Objekts übertragen (Information auf dem Tag). Alle weiteren mit dem Objekt verbundenen Daten werden in zentralen Datenbanken hinterlegt.

Beim dezentralen Datenmanagement werden die relevanten Daten direkt auf dem Tag hinterlegt, um die Prozesslaufzeit zu optimieren. Um diese Daten ggf. zu verifizieren, ist eine Anbindung an eine Datenbank notwendig. Bei den typischen dezentralen (autarken) Abläufen wird dies jedoch nicht benötigt.

Welches dieser beiden Datenmanagementmodelle sinnvoller ist, kann pauschal nicht beantwortet werden und hängt von der konkreten Anwendungsumgebung ab. Im

Konsumgüterbereich entwickelt sich unter Nutzung des EPC ein zentrales Datenmanagementmodell.

Das dem Datenmanagement zugrunde liegende Datenbanksystem ist als Bestandteil des EPC-Netzwerkes zu verstehen bzw. als angebundene Komponente (Object Directory Domain). Da nicht alle Geschäftsanwendungen in der Lage sind, die RFID-Daten zu verarbeiten, müssen diese Rohdaten in dem Datenbanksystem vorgehalten werden. An das Datenbanksystem sind folgende Anforderungen zu stellen:

- Schnelle Zugriffsmöglichkeit auf Einzeldaten (Indexierung)
- Individuelle Datenfilterung
- Langzeitspeicherung von Prozessdaten; ggf. Überführung in ein Datawarehouse
- Zugriffssicherheit und Hochverfügbarkeit

Datenbanken helfen auch, unterschiedliche Sicherheits- und Geheimhaltungsanforderungen zu lösen. Dazu dienen interne Verfahren, Verschlüsselungstechniken, Auditing und Zugriffseinschränkungen, die auch für RFID-relevante Daten verwendet werden können. Weitere Sicherheitsaspekte sind im folgenden Kapitel dargestellt.

Mit der Einführung von RFID-Verfahren, der Zentralisierung der Daten und zunehmenden Real-time-Zugriffen gelangt die sog. Hochverfügbarkeit der Daten massiv in den Vordergrund. Je nach Sensibilität der Daten können unterschiedliche technische Konzepte für Hochverfügbarkeit benutzt werden, z. B. Cluster-Systeme, Standby- oder Replikationsdatenbanken. Die geeignete Wahl ist abhängig von den Systembedingungen bzw. von den Prozessen, die unterstützt werden sollen.

7 RFID-Sicherheitsaspekte

Die Nutzung von RFID-Daten muss unter klaren Regularien für IT-Sicherheit sowie Verbraucher- und Datenschutz erfolgen. Die Ängste der Verbraucher vor einer generellen Transparenz ihres Verhaltens sind ernst zu nehmen. Hier kann es durchaus zu Konflikten kommen, deren Lösung eine Einschränkung der Systeme zur Folge hat. So wird es zukünftig möglich sein, RFID-Tags an Kleidungsstücken und anderen Konsumartikeln an der Kasse zu zerstören (Kill-Befehl), zu entfernen oder unlesbar zu machen. Aufgeregte Diskussionen zum Verbraucherschutz hat es auch gegeben, als sich die Mobiltelefonnetze ausbreiteten. Heute scheut kaum noch ein Konsument davor zurück, sein Mobiltelefon ständig bei sich zu tragen, obwohl bekannt ist, dass damit ein recht genaues Tracking und Tracing seiner Bewegungen möglich ist.

Gleichwohl muss der Betrieb von RFID-Systemen mit außerordentlichem Verantwortungsbewusstsein und Transparenz für den Verbraucher erfolgen, so dass auch das gesellschaftliche Ziel der informationellen Selbstbestimmung der Bürger unterstützt wird. Dies gilt für alle Systeme, in denen – auch bisher schon - Verbraucherdaten gesammelt werden. So dienen heute häufig Bezahlvorgänge mit Kredit-, Bank- oder Loyalty-Karten zur Gewinnung von Verbraucherdaten, was von den Verbrauchern in großem Umfang unterstützt wird.

Eine umfassende Darstellung der Sicherheitsfragen im Kontext mit RFID-Systemen liefert die Studie des BSI (Bundesamt für Sicherheit in der Informationstechnik): siehe Abschnitt „Weitere Informationsquellen“. Hier sollen deswegen nur einige Aspekte behandelt werden.

RFID-Systeme und deren Sicherheitsaspekte wurden lange vor der Einführung erster Industrieanwendungen in der Presse und in der Öffentlichkeit diskutiert. Ein Großteil dieser Diskussionen bezog sich jedoch auf die nur möglicherweise zum Missbrauch geeignete Korrelation von Informationen auf den RFID-Tags und Personeninformation bzw. auf die Sammlung von personenbezogenen Daten und deren anschließende missbräuchliche Nutzung – also eine eher für den Verbraucher in Frage kommende Problemstellung.

Die heute in Pilotprojekten zur Anwendung und zur Berichterstattung herangezogenen Systeme zeigen zwar einen hohen Bedarf an Kundenaufklärung und Offenlegung der Nutzung potenziell personenbezogener Daten (vgl. hier die BSI Studie S.41 und S.46 ff.), jedoch können direkte Bedrohungen bzw. Verletzungen der datenschutzrechtlichen Bestimmungen durch diese Industrie- bzw. Logistikanwendungen nahezu ausgeschlossen werden.

Im Folgenden werden die zurzeit relevanten technischen Sicherheitskriterien angesprochen, die sich primär auf die Sicherung firmenkritischer Daten bzw. deren Missbrauch beziehen. Sicher sind auch hier unter Umständen personenbezogene Daten zu schützen (z.B. bei der Verwendung von RFID als Medium in Firmenausweisen, Zutrittsschutz etc.), das Hauptaugenmerk wird jedoch auf die Systemsicherheit von RFID z.B. in der Logistik oder anderen Industrieanwendungen gelegt.

Wie in allen Bereichen der IT-Sicherheit so ist auch bei RFID eine Unterscheidung der Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit sinnvoll. Entsprechend der Architektur sollte man diese jeweils für die Betreiber der RFID-Systeme und deren Nutzer getrennt betrachten.

In Anlehnung an ganzheitliche Sichtweisen der IT-Sicherheit muss im Vorwege einer solchen Diskussion eine Abgrenzung erfolgen. Ein RFID-System begrenzt sich typischerweise auf die RFID-Tags, den Reader und die in diesem Raum übertragenen Daten (Luftschnittstelle), ggf. noch den Grenzbereich zwischen dem Reader und der Middleware, die die erfassten Daten weiter verarbeitet. Deshalb ist bei der Einführung eines RFID-Systems und dem Design des

entsprechenden Sicherheitskonzeptes auf eine ausreichende Absicherung der Middleware und Backendsysteme zu achten (Vgl. BSI-Studie S. 45).

■ **RFID-Sicherheit für Anwender**

Für die Anwender und Nutzer (seien diese wissentlich oder unwissentlich in ein RFID-System eingebunden) sind Aspekte der Vertraulichkeit und Verbindlichkeit als oberste Schutzziele zu nennen. Einige besondere Fälle, z.B. die Verwendung von RFID-Firmenausweisen, -Reisedokumenten oder -Zahlungsmitteln generieren zudem Probleme im Bereich Lokalisierung der Anwender („Location Privacy“). Gerade die Anwendung von Türzutrittssystemen setzt auf die genaue Zuordnung von Personen (Nutzern) und RFID-Tags um Berechtigungen zu prüfen. Im Rahmen einer eindeutigen Identifikation und Authentisierung (etwa an Vereinzelungsschleusen) werden eine Vielzahl personenbezogener Daten erhoben, die in sich hohen Schutzbedarf haben. Darüber hinaus können mit versteckten RFID-Sensoren zusätzliche Positionsdaten erhoben werden, die zur Erstellung von sehr genauen Bewegungsprofilen missbräuchlich genutzt werden könnten. Deswegen ist es erforderlich, den Zugriff auf und das Auslesen von RFID-Daten entsprechend zu schützen und dem Grundsatz der Datensparsamkeit zu entsprechen.

Darüber hinaus kommt es durch die Architektur der RFID-Systeme (Luftschnittstelle!) inhärent zu einer Beeinträchtigung der Vertraulichkeit von Daten. Alle während einer RFID-Systemaktivität übertragenen Daten (die Aktivierung des Tags durch den Reader und die vom Tag ausgesandten Informationen) sind potenziell einfach abzuhören, wenn die Übertragung (wie derzeit noch üblich) unverschlüsselt abläuft. Hierbei ist jedoch einschränkend zu bedenken, dass durch die Vielzahl der Systeme, Frequenzen und Codierungen eine hohe Systemkenntnis und ein nicht unerheblicher technischer Aufwand betrieben werden muss, um aus den Übertragungen sinnvolle Daten zu generieren. Erst die Kombination aus Kenntnis des verwendeten Systems, der Verfügbarkeit eines geeigneten manipulierten Readers bzw. Empfängers und dessen unbeobachtete Positionierung in Reichweite der legitimierten Reader-Tag-Kommunikation ermöglichen einen solchen Angriff.

Zusammenfassend lässt sich für den Anwenderteil der RFID-Sicherheit darstellen, dass eine Kombination aus Aufklärung über die Verwendung personenbezogener Daten (Ausweise, Geldnoten etc.) und der Sicherung der systeminternen Kommunikation (etwa durch Abschirmung, vgl. BSI Studie S. 51 ff.) für den grundlegenden Schutz unabdingbar sind. Darüber hinaus muss je nach Anwendungsfall (insbesondere wenn statt einfacher Tag-Daten komplexere Informationen im RFID-System übertragen werden) entschieden werden, welche zusätzlichen Maßnahmen zu treffen sind.

■ **RFID-Sicherheit für Betreiber**

Die Betreiber eines RFID-Systems bilden oftmals unternehmenskritische Prozesse wie Logistikketten oder Ersatzteilidentifizierung über RFID ab. Der grundlegende Schutzbedarf ist somit als extrem hoch anzusiedeln, da der Unternehmenserfolg direkt oder indirekt von der Verfügbarkeit der RFID-Daten sowie deren Integrität und Verbindlichkeit abhängt. Zudem haben die Betreiber ein hohes Interesse daran, dass Dritte keinen Zugriff auf die Systemdaten erhalten, da dies tief greifende Rückschlüsse auf die Unternehmensabläufe zuließe. Vor diesem Hintergrund sind folgende Aspekte der RFID-Sicherheit zu betrachten:

- RFID-Systeme müssen ausreichend verfügbar sein und verlässlich arbeiten.
- Übertragenen Daten sollten nicht trivial veränderbar sein.
- Es sollen keine falschen Daten in die Systeme eingespeist werden können.

Da RFID als drahtloses System inhärent leicht zu beeinflussen ist (etwa Denial-of-Service durch Überschwemmung des elektromagnetischen Feldes), ist schon beim Design der Lösung auf eine ausreichende Kapselung und Schirmung der Reader-Tag-Kommunikation zu achten. Eingehende Tests unter wechselnden Bedingungen bieten hier die einzig verlässliche Informationsquelle für ein sicheres und verfügbares Design.

Um eine Veränderung der Daten bzw. eine Täuschung des Systems zu vermeiden, bieten sich bei Verwendung einfacher RFID-Tags nur nachgelagerte Plausibilitätschecks in der Middleware oder im Backend-System an. Diese Limitierung kann jedoch durch die Verwendung leistungsfähigerer Tags der neueren Generation überwunden werden. Der Einsatz von Kryptofunktionen zur einseitigen oder beidseitigen Identifikation und Authentisierung versetzt diese RFID-Systeme in die Lage, Tags und Reader als zum System gehörend zu identifizieren und teilweise sogar die Kommunikation im RFID-System zu verschlüsseln. Generell gilt jedoch, dass einfache RFID-Systeme nur minimale Informationen speichern und übertragen sollten und die „Intelligenz“ der Anwendung durch die Verknüpfung der RFID-Daten in den Backend-Systemen entsteht.

Diverse Probleme der Sicherheit für RFID-Betreiber können somit nur durch komplexere Chips und Reader vollständig gelöst werden. Diese Systeme eignen sich wegen ihrer höheren Kosten nur für hochwertige Produkte und Prozesse sowie für sogenannte „Closed-Loop-Anwendungen, in denen die Tags immer wieder verwendet werden. Weitere Informationen zu Gegenmaßnahmen finden sich detailliert in der BSI Studie ab Seite 47, Abschnitt 7.7.

Für die allgemeine Sicherheitsbetrachtung von RFID-Systemen gilt: Es gibt keine generell anwendbare Sicherheitsarchitektur. Eine eindeutige Klärung der beteiligten Parteien (Stakeholder) und deren Schutzbedarfe ist notwendig, um ein sicheres Design einer RFID-Lösung zu ermöglichen. Basierend auf den Anforderungen der unterstützten Geschäftsprozesse, der beteiligten Stakeholder und der Ausdehnung des RFID-Systems (sowohl geografisch als auch logisch) müssen individuell die zur Anwendung kommenden Sicherheitsmaßnahmen bestimmt werden.

Solange nur Hersteller- und Seriennummern übertragen werden und diese nur durch die Kombination mit Detailinformationen aus den Backend-Systemen zu verwertbaren Informationen ergänzt werden können, ist das Sicherheitsrisiko durch den Einsatz von RFID, etwa in der betriebsinternen Logistikkette, als vernachlässigbar einzuschätzen.

■ **Fälschungssicherheit ("Anti Counterfeiting")**

Ein anderer Sicherheitsaspekt ist die Fälschungssicherheit von RFID-Tags - auch unter dem Begriff "Anti Counterfeiting" bekannt - und deren Eindeutigkeit. Hier ist noch Grundlagenarbeit zu leisten. So können originale Ersatzteile nur dann sicher von gefälschten Teilen unterschieden werden, wenn auch die Tags fälschungssicher also z.B. durch eine Signatur geschützt sind. An diesem Thema arbeitet auch eine Special Interest Group des Auto-ID Lab an der Universität St. Gallen: www.autoidlabs.ch/sigac

8 Anwendungsbeispiele

8.1 Fallstudie: Logistik-Prozesse bei Hewlett-Packard GmbH



Mit einer Produktpalette von über 23.000 verschiedenen Produkten und Handelsbeziehungen zu mehr als 110.000 Lieferanten nutzt HP bereits seit geraumer Zeit RFID-Verfahren. Damit werden die Kosten der Lagerhaltung und des Versands in der eigenen Lieferkette wie auch bei Handels- und Vertriebspartnern reduziert.

Derzeit wird RFID in 30 HP-Werken und Logistikzentren vor allem in China, Süd-Ost-Asien, USA und Brasilien eingesetzt. RFID wurde bei HP ursprünglich eingeführt, um die eigenen Logistikprozesse zu optimieren. Als Wal-Mart ebenfalls das Auszeichnen mit RFID-Tags forderte, war HP als einer der ersten Lieferanten in der Lage, diesen Anforderungen nachzukommen.

Abbildung 23: Warenausgang mit RFID-Antennen im HP-Werk Chester
Quelle: Hewlett-Packard

RFID-Tagging wird auf Verpackungseinheits- und Palettenebene im Werk Sao Paulo (Brasilien) und in den beiden HP-Logistikzentren Chester und Memphis (USA) eingesetzt. An den drei Standorten wird RFID unterschiedlich genutzt: Das Werk in Sao Paulo ist für die Produktion von Druckern und deren Versand zu verschiedenen Logistikzentren verantwortlich. In Chester werden Tintenpatronen verpackt, zwischengelagert und zum Logistikzentrum in Memphis versandt. Dort wird RFID bei Endverpackung, Lagerung und Versand von hochwertigen Druckern benutzt.

Dank RFID reduzierte sich die Dauer des logistischen Dispositionsprozesses von Paletten in Memphis von Minuten auf Sekunden, weil die umständliche Nutzung von Barcode-Lesern entfällt. In Chester konnten bei der Handhabung der Verpackungseinheiten und Paletten innerhalb der Distributionszentren die Kosten erheblich gesenkt werden, indem Kostentreiber, Verluste und Fehler in der manuellen Handhabung vermieden wurden. Dabei sind weitere Möglichkeiten, wie z.B. die Nutzung zusätzlicher Information über die EPC-Standard-Informationen hinaus, noch nicht einmal voll ausgenutzt.

Der weltweite Einsatz von RFID in der Supply Chain von Hewlett-Packard wird in Zusammenarbeit mit Logistik-Unternehmen, Handelspartnern und Großkunden systematisch weiter entwickelt und implementiert. Zu den bislang 30 HP-Werken und Logistikzentren, die RFID einsetzen, werden im Jahr 2005 weitere Standorte aber auch die Implementierung von RFID-Transpondern der zweiten EPC-Generation hinzukommen.

8.2 Fallstudie: Flexible Produktionsprozesse in der Automobilfertigung bei BMW

RFID ist für die industrielle Fertigung eine wichtige Technologie, um flexible Produktionskonzepte zu realisieren. Dabei wird vor allem die geringe Empfindlichkeit der Datenträger (Tags) gegen raue Umgebungsbedingungen und Verschmutzung geschätzt – spezielle Industrie-Tags können bei über 200°C eingesetzt werden. Die Möglichkeit zur dynamischen Datenspeicherung erlaubt zudem interessante, dezentrale Systemarchitekturen.

Eine häufige Anwendung von RFID ist die Kennzeichnung von Trägermodulen, die in verschiedenen Ausführungen zum innerbetrieblichen Transport von der einzelnen Leiterplatte bis zur Autokarosserie eingesetzt werden. An diesen Trägern wird ein RFID-Tag befestigt, das gemeinsam mit dem zu produzierenden Gut den kompletten Fertigungsweg durchläuft. Da Trägermodul und Tag anschließend immer wieder für erneute Produktionsdurchläufe einsetzbar sind, spricht man von geschlossenen Kreisläufen (closed loop).

Im einfachsten Fall kann auf den Datenspeichern die Identifikationsnummer eines Fertigungsauftrages abgelegt werden. An den einzelnen Bearbeitungsstationen wird dann das Gut automatisch identifiziert. Eine Fertigungssteuerungs-Software (Manufacturing Execution System, MES) legt anhand dieser Nummer fest, welcher Produktionsschritt an dieser speziellen Station zu erfolgen hat.

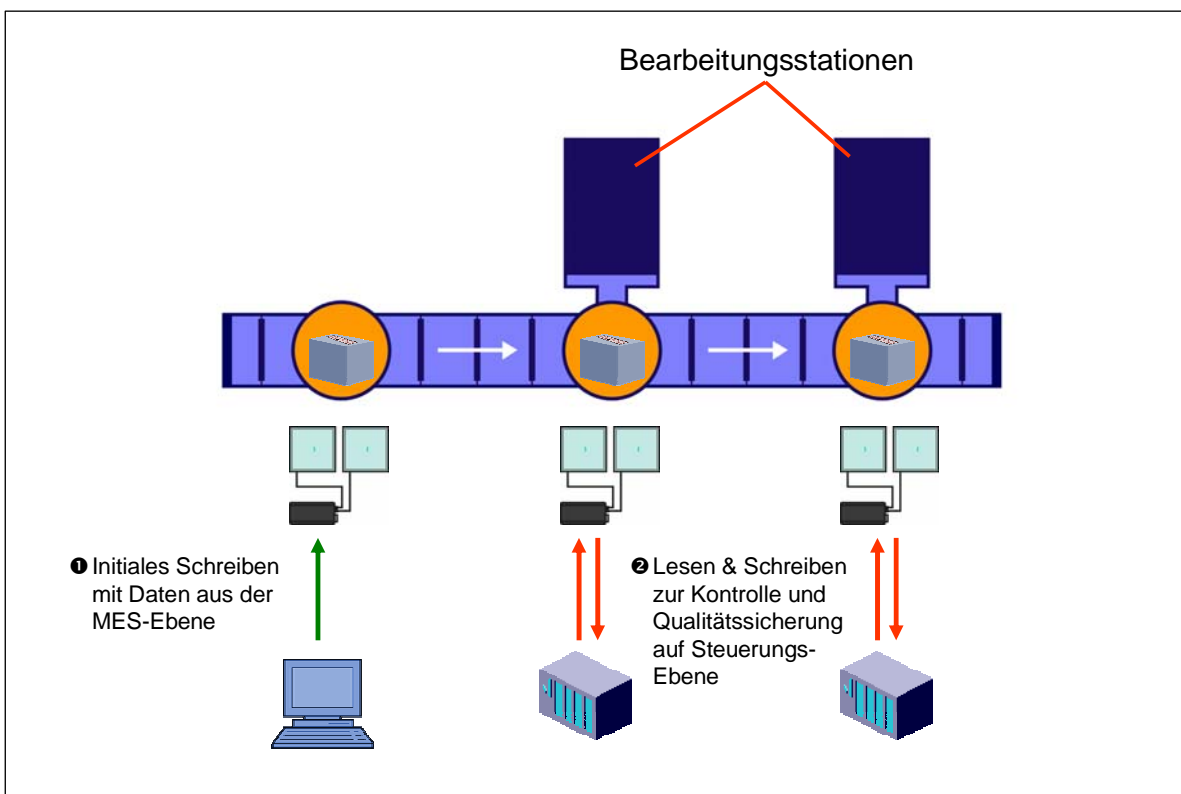


Abbildung 24: Prinzipielle Architektur für RFID in der industriellen Fertigung

Quelle: Siemens AG

Bei weiter reichenden Konzepten werden diese Produktionsanweisungen direkt auf dem Datenträger gespeichert. Dies hat den Vorteil, dass die Linie zumindest die eingeschleusten Güter autark, d.h. ohne Zugriff auf höhere Systemkomponenten, produzieren kann. Damit führt der Einsatz von RFID zu einer höheren Verfügbarkeit der Anlage.

Ein solches Konzept wird z.B. bei BMW erfolgreich genutzt. Im Zuge einer Modernisierung und Erweiterung des BMW-Werks 1 in München wurde die neue Schubpalettenanlage für die Karosseriemontage der 3er-Serie mit RFID-Datenträgern und Schreib-Lesegeräten ausgestattet. Auf jedem Karosserieträger befindet sich ein RFID-Datenträger, der alle für die

Produktion des Fahrzeugs relevanten Daten speichert, so dass die Karosserie jederzeit identifiziert werden kann. Dies ist bei BMW wichtig für die Produktionssteuerung, Dokumentation und Qualitätssicherung.



Abbildung 25: RFID-Transponder mit Datenspeicher an der Karosserieplatte bei BMW
Foto: Siemens AG

Weitere Vorteile: Aufgrund der autarken Intelligenz auf jeder Platte und der nahtlosen Integration des Systems in die Simatic-Automatisierungslandschaft besitzt die Anlage eine maximale Flexibilität. Damit können auf der Linie gleichzeitig mehrere Modelle gefertigt und neue Modelle sukzessive eingespeist werden.

8.3 Fallstudie: Mobile Wartungslösung bei Fraport AG

Die Fraport AG mit einem weltweiten Umsatz von 1,8 Mrd. Euro nimmt eine führende Rolle im internationalen Airport Business ein. Sie ist auch die Eigentümerin und Betreiberin des Flughafens in Frankfurt. Die Geschäftsbereiche Bodenverkehrsdienste, Verkehrs- und Terminalmanagement, Kommunikationsdienstleistungen sowie Immobilien und Facility Management decken die gesamte Bandbreite an Produkten und Dienstleistungen im Flughafengeschäft ab.

Unter der Federführung von SAP Consulting wurde ein ehrgeiziges mobiles RFID-Wartungsszenario für die Fraport AG realisiert: Durch die Verknüpfung der Software SAP Mobile Asset Management mit mobilen Handheld-Computern und RFID-Technologie erhielt Fraport ein innovatives Gesamtsystem für die gerichts feste Organisation von Wartungsarbeiten an unterschiedlichsten Technikkomponenten auf dem Flughafengelände, z.B. an Brandschutzklappen.

Das mobile RFID-Wartungsszenario basiert auf der Software-Lösung Mobile Asset Management und erhöht die Sicherheit am Frankfurter Flughafen. Sie ersetzt Arbeitspapiere, übermittelt detaillierte Real-time-Daten und schließt die Informationslücke zwischen Backend-Systemen und dem Vor-Ort-Geschehen.

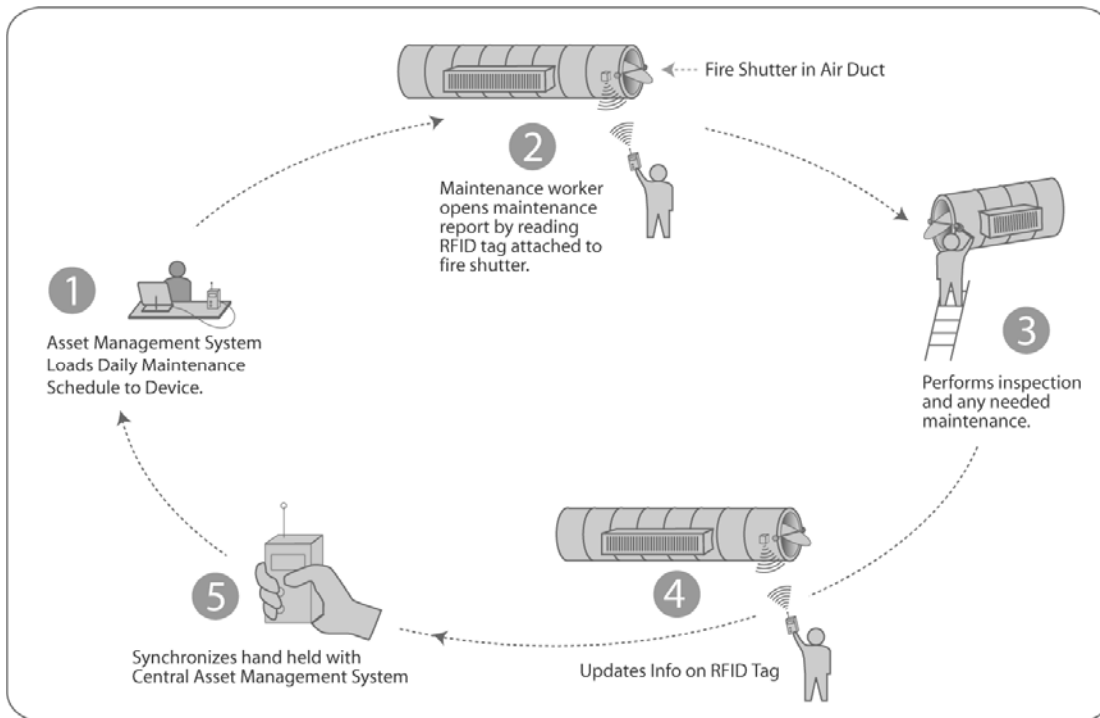


Abbildung 26: Papierloses mit RFID optimiertes Wartungsszenario am Flughafen Frankfurt
 Quelle: Claus Heinrich (SAP): RFID and Beyond (s. Informationsquellen)

■ **Optimierte papierlose Wartungsabläufe**

Im Rahmen des Immobilien und Facility Managements betreut die Fraport AG rund 420 Gebäude und Anlagen am Flughafen Frankfurt. Eine der zentralen Aufgaben ist die regelmäßige Instandhaltung und Kontrolle von technischen Komponenten mit gesetzlich vorgeschriebener Wartung. Dabei steht Fraport als Betreiber des Flughafens in der Nachweispflicht. Zur Steuerung seiner Wartungsaktivitäten nutzt das Unternehmen die leistungsfähige SAP-Lösung Plant Maintenance. Diese Applikation wurde um eine mobile Lösung, das Mobile Asset Management, erweitert. Nahtlos greifen hier Transponder mit innovativer RFID-Technologie sowie robuste Handheld-Computer als effektives Gesamtsystem ineinander.

■ **Erfolgreiche Kombination innovativer Technologien**

Statt papiergebundener Arbeitsanweisungen nutzen die Wartungsmonteure heute das widerstandsfähige Frontend, das den Chip der RFID-Transponder lesen und beschreiben kann und mit der Mobile-Asset-Management-Anwendung kommuniziert. Die mobilen Endgeräte werden zentral von Fraport mit den fälligen Wartungsaufträgen aus dem SAP-System bestückt. Nach der Legitimation und dem Log-in beginnt ein kontrollierter Schritt-für-Schritt-Dialog zwischen der Mobile-Asset-Management-Anwendung, dem Monteur und den an den lufttechnischen Anlagen installierten RFID-Etiketten. Dieses Vorgehen stellt sicher, dass die Wartung der Anlagen in genau definierten Prozessschritten durchgeführt wird. Etwaige Fehlerfälle werden über umfangreiche Schadenscodes protokolliert.

Damit sind der Verlauf jeder Wartungsaktivität und der Zustand vor Ort lückenlos dokumentiert und elektronisch festgehalten. Nach Abschluss der Wartungsarbeiten werden die mobilen Endgeräte ausgelesen und die Informationen elektronisch an das Backend-System übertragen. In Summe hat Mobile Asset Management die Wartungsabläufe wesentlich beschleunigt, die Qualität und Sicherheit der Daten deutlich erhöht sowie neue Möglichkeiten für Berichte über Störungen und Lebensdauer der Produkte geschaffen.

Mit der SAP-Lösung hat die Fraport AG eine zukunftssichere, moderne und mobile Wartungslösung erhalten, die an jede beliebige Aufgabenstellung innerhalb der Instandhaltung adaptiert werden kann. Seit Mai 2005 ist bei der Fraport AG die SAP Mobile Asset Management Lösung in der neuesten Version 2.5 produktiv im Einsatz, welche die RFID-Funktionalität standardmäßig beinhaltet.

■ **Sechsstelliges Einsparpotential realisiert**

Fraport gewann einen lückenlosen elektronischen Wartungsprozess, mit dem die korrekte Wartungsdurchführung an den Anlagen gewährleistet ist. Durch die Nutzung innovativer Technologien können die Wartungsaktivitäten schneller als früher durchgeführt werden. Und jeglicher Prozessschritt kann heute auf Knopfdruck exakt nachvollzogen werden. Damit wurde größtmögliche Transparenz für die Nachweispflicht gegenüber Revisionsorganen und dem Gesetzgeber geschaffen.

Fraport hat an 22.000 Brandschutzklappen des Flughafens RFID-Tags angebracht. Dafür fielen bisher im Rahmen der Wartung jährlich 88.000 Auftragsdatenblätter an. „Dank des Einsatzes von RFID sparen wir in der für uns wichtigen Dokumentation rund 450.000 Euro im Jahr“, sagt Dr. Roland Krieg, CIO der Fraport AG, im Interview. (Computerwoche 25 vom 24.06.2005, Seite 24). Demgegenüber beziffert er die einmaligen Kosten für die RFID-Tags und RFID-Lesegeräte auf unter 100 000 Euro. Das ergibt einen überzeugenden Return on Investment von weniger als einem Jahr.

8.4 Fallstudie: RFID-Flächen-Rollout in der Logistik bei Metro AG

Die METRO AG beabsichtigt die Einführung von RFID in ihren logistischen Prozessen bis hin zu Verräumungsprozessen in den Einzelhandelsmärkten. Dazu ist es notwendig, dass eine RFID-Implementierung in vielen Märkten und angeschlossenen Warenverteilzentren vollzogen wird. Aufgrund der unterschiedlichen IT-Anwendungen, die an die RFID-Physik angeschlossen werden müssen, empfiehlt sich die Nutzung einer Standard-Middleware. Deren Aufgabe ist es, den Status der RFID-Reader zu kontrollieren, die Feedback-Geber zu steuern und die prozessbasierten Aufgaben der RFID-Reader, Writer und Printer zu unterstützen. Die entsprechenden Daten werden an die Geschäftsanwendungen übertragen. Die Software basiert auf dem von IBM entwickelten RFID-Domänenmodell für die Verarbeitung von RFID-Events und deren Anbindung an Geschäftsanwendungen.

Die Metro AG hat sich im Jahr 2005 entschieden, für den Flächenrollout in ihren Märkten und Warenverteilzentren durch die RFID-Middleware von IBM – Produktfamilie WebSphere – zu verwenden. Diese bildet das Rückgrat der Versorgung der Anwendungssysteme mit RFID-Events und der Einbindung in das vorhandene Werkzeug für Systemmanagement.

Für das Future-Store-Projekt der Metro hat sich die UHF-Technologie als geeignet erwiesen. Die RFID-Tags werden bei den Produzenten von Einzelhandelsware an die logistischen Einheiten (z.B. an Paletten) angebracht. Im Rahmen einer standardisierten EDI-Nachricht werden der Metro diese Details übermittelt. An den Wareneingängen in den Warenverteilzentren oder bei Direct Shipments in den Supermärkten kann der erwartete Wareneingang und mit dem am RFID-Reader ermittelten tatsächlichen Lieferumfang verglichen werden. Mit einem entsprechenden Signal kann das Vergleichsergebnis an den Disponenten übermittelt werden, so dass er bei Abweichungen sofort tätig werden kann. Die weitere Verbuchung der Lieferungen findet in den Warenwirtschaftssystemen statt.

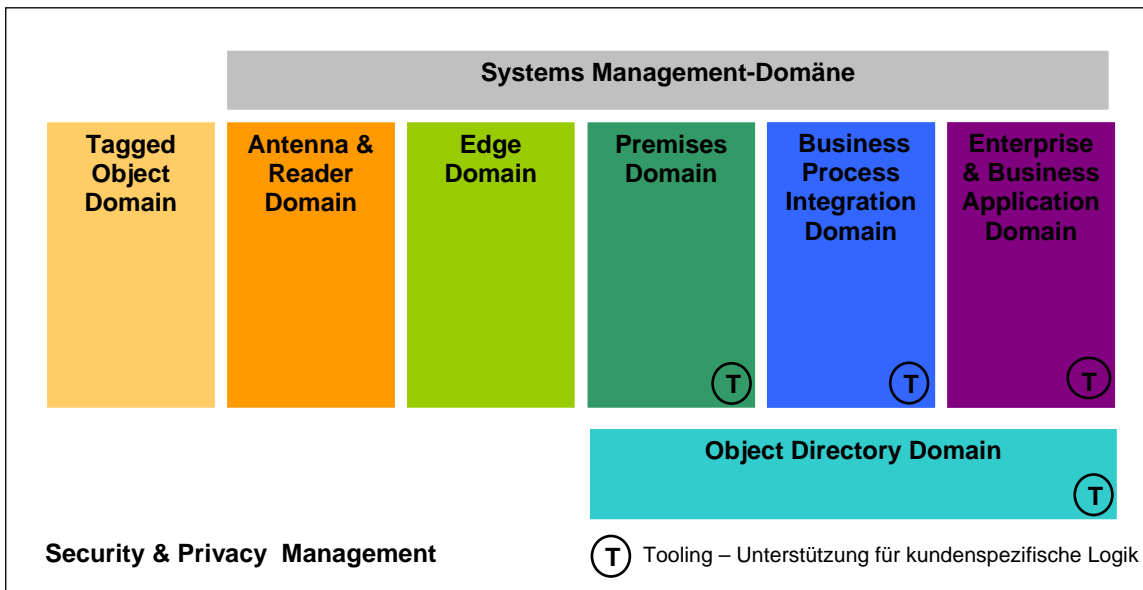


Abbildung 27: Schichtenmodell einer umfassenden Auto-ID-Anwendungsarchitektur
Quelle: IBM

Der typische Systemaufbau ist wie folgt: Die Edge Domain, die in den Märkten installierte Software, kontrolliert die Physik der RFID-Reader. Über eine Kommunikationsverbindung (Uplink) werden die Daten zum „WebSphere Premises Server“ übertragen, der das Kernstück der RFID-Systemintegration darstellt. Die nächsthöhere Anwendungsintegration wird im Integration Layer vollzogen, der wie die Premises-Infrastruktur zentral im Rechenzentrum betrieben wird. Dieser zentrale Integration Layer bietet die Möglichkeit, verschiedene Anwendungen direkt mit den RFID-Daten zu versorgen.

Die Anbindung der „WebSphere RFID-Middleware“ an die unterschiedlichen Geschäftsapplikationen erfolgt über einen Process Integration Layer, um die Anzahl der IT-Schnittstellen zu optimieren. Ebenso ist der Pflege- und Betriebsaufwand dieser Schnittstellen deutlich geringer als Punkt-zu-Punkt-Kopplungen der Middleware mit einzelnen Zielanwendungen.

Der Vorteil der RFID-Technologie besteht darin, dass die Entlade- und Beladeprozesse (z. B. in den Warenverteilzentren) schneller durchgeführt werden können, und eine Verbuchung in den Geschäftsanwendungen wesentlich präziser vollzogen werden kann. In den Altverfahren, die Barcode basiert sind, hängt sehr viel von der Zuverlässigkeit der Mitarbeiter beim Lesen der Etiketten ab. Weiterhin sind die Probleme, die von verschmutzten Barcodes ausgehen, gelöst. Ein weiterer Vorteil ist die Vermeidung bzw. Reduktion von Fehllieferungen, da dem Mitarbeiter zwangsweise eine Rückmeldung über die korrekte Verladung gegeben werden kann.

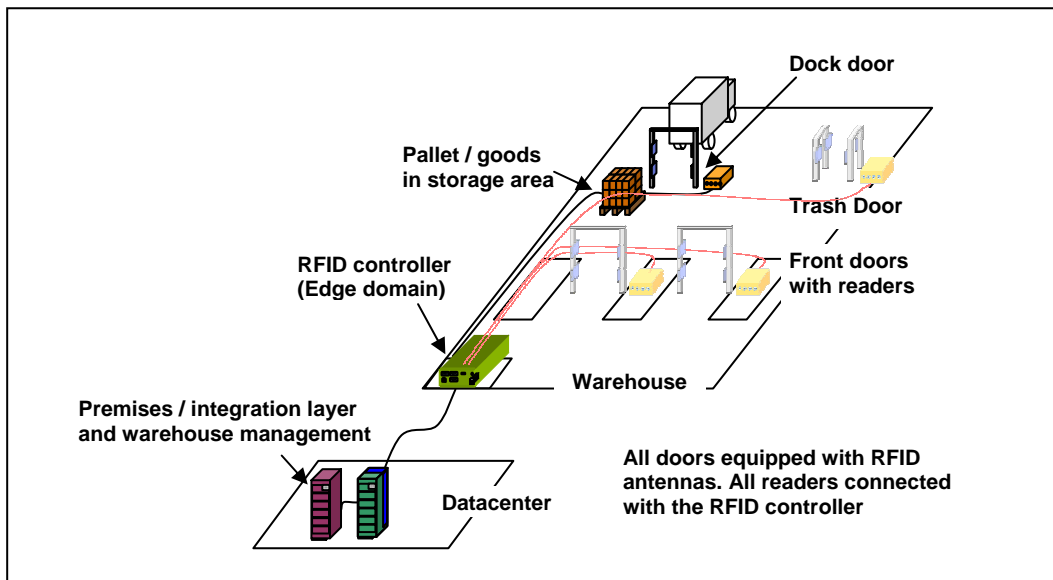


Abbildung 28: Konfiguration der RFID-Antennen an den Toren im Metro-Lager.
Quelle: IBM

Dazu wurde von Kurt Salmon Associates eine Analyse von Verbesserungen durchgeführt. Diese ergab, dass die Verluste auf dem Transportweg durch RFID-Technologie um 11 bis 14 Prozent reduziert werden konnten. Die Verfügbarkeit von Waren in den Märkten wurde um bis zu 14 Prozent gesteigert. Die Kostenreduktion in den Warenverteilzentren lag bei ca. 11 Prozent. Die Analyse zeige auch, dass die Migration auf eine neue Technologie durch Prozessveränderungen unterstützt werden sollte. Dadurch sind signifikante Einsparungen realisierbar.

Insgesamt plant die Metro die Ausstattung von 250 Märkten mit dieser Technologie. Schrittweise werden dabei die Lieferanten über das Paletten-Tagging zum Case bzw. Item Tagging herangeführt. Die Gesamtimplementierung wurde durch IBM Global Services vollzogen. Dazu wurden folgende Teilprojekte durchgeführt: Prozessanalyse, Beschreibung des neuen Prozessablaufes, Basistests zur Auswahl der notwendigen Hard- und Software, Überprüfung (Dokumentation) der Umgebungsbedingungen in den Zielmärkten, Aufbau der RFID-Physik in den Zielmärkten, Konfiguration und Integration der WebSphere RFID-Middleware. Das System ist seit November 2004 im Betrieb und wird täglich genutzt.

9 Glossar

Air Interface	Luftschnittstelle, Bereich zwischen Reader- und Tag-Antenne und Kommunikations-Interface, das hier benötigt wird.
ALE	Application Level Events Specification: Schnittstelle zwischen RFID-Middleware und Applikation, von EPCglobal definiert.
Auto-ID	Automatisch, berührungslose Identifikation von Objekten, Überbegriff für Verfahren wie Barcode und RFID-Forschungsgebiet der Auto-ID Labs beim MIT, in St. Gallen, Cambridge usw.
Chip	Datenträger im Tag.
DNS	Denic Name Server, Adressverzeichnis für Internet-Adressen, Umsetzung von WWW- in IP-Adressen.
EICAR	European Institute for Computer Anti-Virus Research - betreibt auch eine RFID-Taskforce.
EPCIS	Middleware-Komponente für den Zugriff auf das EPCglobal-Netzwerk.
EPC	Electronic Product Code: Hersteller-, Produkt- und Seriennr., vergeben von EPCglobal.
ERP	Enterprise Resource Planning (-System)
ETSI	European Telecommunications Standards Institute
Event	Ereignis im Auto-ID-Umfeld, z. B. das Lesen eines RFID-Tags.
GDS	Global Data Synchronisation: Maßnahmen zum Abgleich von Artikelstammdaten zwischen Handelspartnern nach globalen Standards, die durch die GS1 (vormals EAN.UCC) entwickelt wurden.
GTIN	Global Trade Item Number, ein EAN/UCC-Standard.
Inlay	Rohversion eines RFID-Tags zur Aufbringung auf Etiketten bzw. zur Einbettung in eine Smart Card.
Inlay	Verbindung einer Antennenstruktur mit einem Chip zu einer Transponderfunktionseinheit. Durch Verbindung mit dem endgültigen Träger oder Etikett entsteht aus einem Inlay ein Tag.
ISO	International Standards Organisation
ITIL	IT Infrastructure Library: Im Auftrag der britischen Regierung entwickelter Leitfadent ITIL. Weltweiter De-facto-Standard für das Service Management.
KPI	Key performance indicators
M2M	Maschine-zu-Maschine-Kommunikation
MES	Manufacturing Execution System
Middleware	Software-Komponente in der mittleren Schicht in einer hierarchischen Software-Architektur.
NVE	Nummer der Versandeinheit für die Identifikation von Paletten, Versandkartons, Pakete, Päckchen etc.
ONS	Object Name Server: Zentrales Verzeichnis der EPC-Nummern im EPCglobal-Netzwerk
PLM	Product Lifecycle Management

RCS	Radar Cross Section, eine fiktive Fläche, die in der Radartechnik zur Charakterisierung des Reflexionsvermögens von Objekten verwendet wird. Im RFID-Bereich wird damit das Reflexionsvermögens von Tags spezifiziert.
RFID	Radio Frequency Identification
Savant	Von EPCglobal konzipiertes Middleware-Konzept für RFID-Systeme. Der ursprüngliche Plan, daraus ein marktfähiges Produkt zu machen, wurde aufgegeben. (s. Kapitel Infrastruktur).
SCM	Supply Chain Management (-System)
SGTIN	Serialized Global Trade Identification Number: GTIN-Nummer kombiniert mit einer Seriennummer zur eindeutigen Identifizierung von Objekten, ein EAN/UCC-Standard.
SKU	Stock-keeping Unit: Verpackungseinheit im Lager, die einen RFID-Tag trägt.
SLA	Service Level Agreement: Vertrag über Dienstleistungen und zugehörige Messkriterien.
SOA	Service Oriented Architecture, insbesondere eine Eigenschaft flexibler Middleware.
SOAP	Simple Object Access Protocol
Tag	(Elektronisches) RFID-Etikett bestehend aus einem Chip mit Datenspeicher und einer Antenne für die Übertragung über Radiofrequenzen (RF), angebracht auf Klebeetiketten, in Smart Cards, in Glaszylindern oder in einem Kunststoffgehäuse.
Transponder	Synonym für Tag.
WSDL	Web Services Description Language
XML	Extended Markup Language, Internet-Standard für die Formatierung von Informationen und Dokumenten.

10 Weitere Informationsquellen

Bücher

- Elgar Fleisch /
Friedemann Mattern Das Internet der Dinge, Springer Verlag, Berlin, Juni 2005,
ISBN: 3540240039
- Klaus Finkenzeller RFID-Handbuch, 3. Auflage, 2002, Carl Hanser Verlag München,
ISBN 3-446-22071-2.
- Claus Heinrich Adapt or Die: Transforming Your Supply Chain into an Adaptive
Business Network. 2003, John Wiley & Sons, Inc.
ISBN 0-471-26543-8
- Claus Heinrich RFID and Beyond: Growing Your Business Through Real World
Awareness, 2005 John Wiley & Sons, Inc.
ISBN 0-7645-8335-2
- BSI-Studie Risiken und Chancen des Einsatzes von RFID-Systemen, Trends und
Entwicklungen in Technologien, Anwendungen und Sicherheit., 2004,
Bundesamt für Sicherheit in der Informationstechnik (BSI),
ISBN 3-922746-r56-x. <http://www.bsi.bund.de/fachthem/rfid/studie.htm>

Internet-Adressen

Universitäten, Verbände, Gremien, Hersteller-übergreifende Internet-Seiten

www.aim-de.de	AIM e.V.
www.airlines.org	ATA : Air Transport Association
www.autoidlabs.org	Weltweites Netzwerk der Auto-ID-Center
www.bitkom.org	Größter europäischer Verband der IT-Industrie
www.bme.de	Bundesverbandes Materialwirtschaft, Einkauf und Logistik (BME)
www.bsi.bund.de	Bundesamt für Sicherheit in der Informationstechnik
www.chep.com	Weltweite Paletten- und Verpackungslogistik
www.bvl.de	Bundesvereinigung Logistik
www.gs1-germany.de	GS1 Germany GmbH (ehemals CCG)
www.epcglobal.de	GS1 Germany GmbH (ehemals CCG)
www.epcglobalinc.org	EPCglobal Inc.
www.future-store.org	Metro Future Store Initiative
www.item.ch	Institute of Technology Management, Uni St. Gallen
www.licon-logistics.de	Logistik-Verband, getragen von Kühne + Nagel, Siemens u.a.
www.logistics.about.com	Informationen
www.logistik-lexikon.de	Online-Lexikon
www.m-lab.ch	M-Lab (Uni St. Gallen und der ETH Zürich)
www.myLogistics.net	Logistik-Portal der AXIT AG. gute Stichwortsuche.
www.rfid-handbook.de	Internetseite zum RFID-Handbuch von Klaus Finkenzeller (s.o.)
www.uc-council.org	Uniform Code Council, USA

Medien

www.dvz.de
www.logistra-net.de
www.eweek.com
www.funkschau.de
www.ipm-scm.com
www.ident.de
www.logistik-heute.de
www.rfid-im-blick.de
www.logistik-inside.de
www.rfidforum.de
www.rfid-forum.de
www.rfidjournal.com
www.themanufacturer.com

Deutsche Verkehrszeitung / Deutsche Logistik-Zeitung
Fachmagazin
Fachmagazin mit RFID-Schwerpunkt
Fachmagazin
Fachmagazin Supply Chain Management
Fachmagazin
Magazin des BVL
Fachmagazin in Deutschland
Fachmagazin, ausführliche RFID-Dokumentation
Fachmagazin / Smart Card Forum
Presseorgan vom AIM, Titel: „ident“
Fachmagazin USA, auch Konferenzveranstalter
Fachmagazin USA

Danksagung

Das vorliegende White Paper „RFID – Technologie, Systeme und Anwendungen“ entstand in Abstimmung mit der BITKOM-Projektgruppe RFID (Radio Frequency Identification). Das Autorenteam bestehend aus Vertretern namhafter Unternehmen der unterschiedlichen ITK-Technologiefelder, hat damit eine hervorragende Zusammenarbeit von Playern der ITK-Wertschöpfungskette geleistet, die das Zusammenspiel der Technologiefelder und einiger Anwendungsfelder hervorragend widerspiegelt.

Wir bedanken uns herzlich bei den Autoren, Dr. Norbert Ephan, Kathrein Werke KG, Jens Gerecke, Microsoft Deutschland GmbH, Wolf Rüdiger Hansen, Diamond Systems GmbH, Dr. Frank Gillert, Infineon AG, Michael Hegenbarth, Infineon AG, Tanja Popova, GS1 Germany GmbH, Georg Raabe, Hewlett Packert GmbH, Sebastian Rohr, Computer Associates GmbH, Tamara Sass, Oracle Deutschland GmbH, Thomas Schuh, T-Systems GmbH, Peter Sommerfeld, Fujitsu Siemens Computer GmbH, Markus Weinländer, Siemens AG, Wolfgang Weyand, IBM Deutschland GmbH und Dr. Alexander Zeier, SAP AG für ihre engagierte Mitarbeit und die kreativen Diskussionen. Dank geht auch an die anderen Mitglieder der Projektgruppe, die die Arbeiten aufmerksam verfolgt und Kommentiert haben.

Die Abbildungen wurden uns weitgehend von den Unternehmen zur Verfügung gestellt und das Autorenteam hat jeweils die aus seiner Sicht beste Darstellung ausgewählt und der Veröffentlichung in diesem BITKOM-White-Paper zugestimmt.

Besonderen Dank richten wir an den Projektleiter und Redakteur, Wolf Rüdiger Hansen, Diamond Systems GmbH, der die zahlreichen Autorenbeiträge aufeinander abstimmt. Besonderer Dank gilt auch den stellvertretenden Projektleitern, Georg Raabe, Hewlett Packert GmbH und Dr. Alexander Zeier, SAP AG, die wesentlich zur Verfeinerung und Harmonisierung des finalen White Papers beigetragen haben.

Dr. Birgit Heinz, BITKOM e.V., redigierte den Gesamttext und steht für Rückfragen unter b.heinz@bitkom.org zur Verfügung.

Berlin, den 30. Juli 2005

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder mit etwa 120 Mrd. Euro Umsatz und etwa 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org