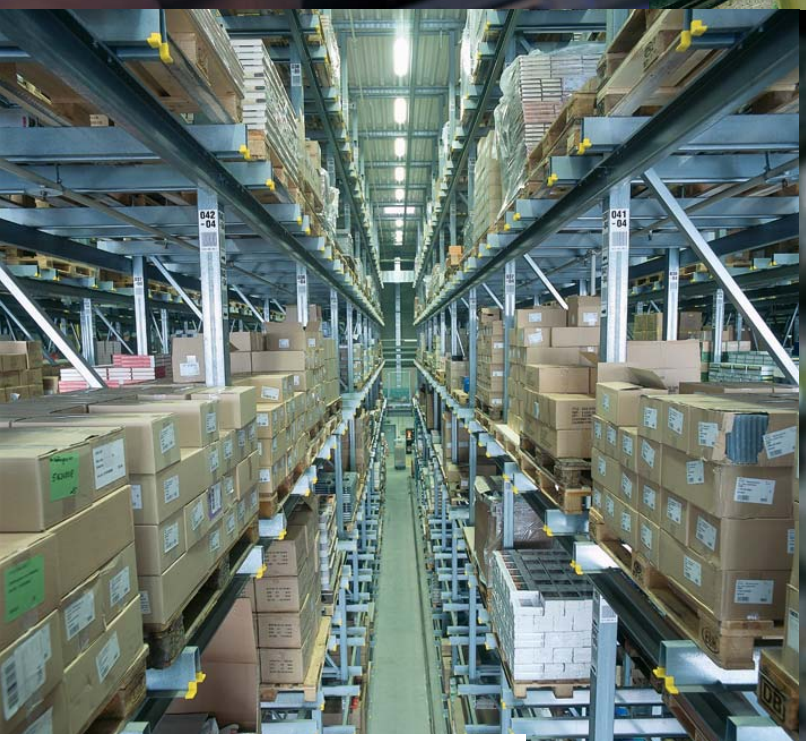
Technologie-Zentrum Informatik

MES

Fraunhofer Institut Sichere Informations-Technologie



RFID-Studie 2007

Technologieintegrierte Datensicherheit bei RFID-Systemen

Diese Studie wurde im Rahmenprogramm Mikrosysteme 2004-2009 durch das Bundesministerium für Bildung und Forschung gefördert.

Bundesministerium für Bildung und Forschung

Folgende Autoren waren an der Erstellung dieser Studie beteiligt:

Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt
Ulrich Waldmann, ulrich.waldmann@sit.fraunhofer.de
Unter Mitwirkung von: Christa Paule und Dr. Dirk Scheuermann

Fachgebiet Mikroelektronische Systeme (MES) der Technischen Universität Darmstadt
Dr. Thomas Hollstein, thomas@mes.tu-darmstadt.de
Unter Mitwirkung von: Frank Harlacher und Oliver Soffke

Technologie-Zentrum Informatik (TZI) der Universität Bremen
Dr. Karsten Sohr, sohr@informatik.uni-bremen.de
Unter Mitwirkung von: Henk Birkholz, Silke Schäfer und Gerhard Stampe

Betreuung: Projektträger Mikrosystemtechnik VDI/VDE Innovation + Technik GmbH, Berlin

Stand: April 2007

Management Summary

Die vorliegende Studie bestimmt Verfahren für eine sichere Anwendung von RFID-Technologien. Auf Grundlage von drei konkreten Anwendungsszenarien ermitteln die Verfasser anwendungsabhängige Bedrohungs- und Risikofaktoren und beschreiben, wie und mit welchem Aufwand Unternehmen diesen Herausforderungen begegnen können. Die Szenarien sind:

- Unternehmensübergreifende Werkstückidentifikation und Supply Chain (Automobilproduktion)
- Auszeichnung und Warenverfolgung von Konsumgütern (Handel)
- Fälschungssicherheit von Medikamenten (Pharmazeutische Lieferkette)

Dort wo Verfahren und Technologien derzeit noch keine ausreichende Sicherheit bieten, identifiziert die Studie offene Fragen in Forschung und Entwicklung, deren Beantwortung die Grundlage für einen breiten und offenen Einsatz der RFID-Technologien sein wird.

Noch fehlt es an Konzepten, Verfahren und allgemeingültigen Standards, damit Unternehmen RFID in unterschiedlichen Bereichen und in großem Umfang sicher und effizient einsetzen können. Die Luftschnittstelle zwischen Tag und Lesegerät und die Tags sind vielfältigen Angriffen ausgesetzt (z.B. Sniffing, Spoofing, Cloning und Tracking). Notwendige Sicherheitsmechanismen lassen sich jedoch nicht mit allen RFID-Systemen umsetzen. So eignen sich preisgünstige Sensoren (Low-Cost-Tags) beispielsweise nicht für kryptographische Verfahren, wie sie zur Authentisierung, Verschlüsselung, Pseudonymisierung und zum Integritäts- und Zugriffsschutz in offenen Lieferketten nötig sind.

In den Insellösungen und Pilotprojekten der **Automobilproduktion** konzentrieren Unternehmen derzeit auf Industrietauglichkeit und Funktionssicherheit. Bei einer tieferen Integration der RFID-Technologie in den Produktionsprozess und einem lieferketten-übergreifenden Einsatz von RFID wird der Aspekt der Informationssicherheit aber mehr in den Vordergrund rücken. Denn um empfindliche Störungen der Produktionsprozesse zu vermeiden, sind hier entsprechend hohe Anforderungen an Datenintegrität und Verfügbarkeit zu erfüllen. Der erfolgreiche RFID-Einsatz in der Automobilindustrie wird unter anderem davon abhängen, wie gut es gelingt, kryptogaphische Verfahren zur Authentisierung und Verschlüsselung zu entwickeln und gleichzeitig Sensorkosten zu minimieren. Eine sichere Verwendung von RFID-Systemen in Lieferketten des **Handels** hingegen wird nur möglich sein, wenn hardwarebasierte Sicherungsverfahren für die Kommunikation zwischen Tag und Lesegerät sowie Lightweigt-Kryptoverfahren und fälschungssichere Schlüssel gefunden werden. Bei der Konzeption des Gesamtsystems von RFID-basierten Supply-Chain-Anwendungen bildet die Funktionssicherheit einen wesentlichen Bestandteil des Sicherheitskonzepts. Aus Akzeptanzgründen gilt es zudem, Fragen des Datenschutzes zu adressieren. In der **pharmazeutischen Lieferkette** bildet die Verwendung eindeutiger schreibgeschützter Tag-Kennungen die Basis für Echtheitsprüfung, Erkennung von Duplikaten und das Abrufen von Produktinformationen. Geeignete effiziente Verfahren, die sich auf Low-Cost Tags und in einer offenen Lieferkette implementieren lassen, ohne Schlüsselmanagement und Synchronisationsmenachismen zu erfordern, existieren jedoch noch nicht. Für die notwendige Produktauthentisierung fehlen zudem einheitliche automatisierbare Verfahren, welche sich in die RFID-Systeme integrieren lassen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

AES	Advanced Encryption Standard
ALE	Application Level Event
API	Application Programming Interface
ASN.1	Abstract Systax Notation One
B2B	Business-To-Business
B2C	Business-To-Customer
BDSG	Bundesdatenschutzgesetz
BFArM	Bundesinstitut für Arzneimittel und Medizinprodukte
CC	Communication Control
CHA	Certification Holder Authority
CMS	Cryptographic Message Syntax
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRPoSDM	Customer-Related PoS Data Management System
CV	Card Verifiable (Zertifikat)
DEC	Decipherment
DES	Data Encryption Standard
DES3	Triple-DES
DESL	Lightweight Data Encryption Standard
DSA	Digital Signature Algorithm
EAN	European Article Number
ECC	Elliptic Curve Cryptography
EDI	Electronical Data Interchange
EEPROM	Electrically Erasable Programmable Read-Only Memory
EIRP	Effective (Equivalent) Isotropically Radiated Power
ElektroG	Elektro- und Elektronikgerätegesetz
EMEA	Europäische Arzneimittelagentur
ENC(x, y)	Encipherment of data x with key y
EPC	Electronic Product Code
EPCIS	EPC Information Services
ERP	1. Enterprise Resource Planning, 2. Effective Radiated Power
ETL	Extract Transform Load
ETSI	European Telecommunications Standards Institute
FDA	Food and Drug Administration
FIB	Focused Ion Beam
FTDMA	Frequency and Time Division Multiple Access
GID	General Identifier
GSM	Global System for Mobile Communication
GPS	Global Positioning System
GS1	Global Standards 1
HF	High Frequency
ICC	Integrated Circuit Card
ID	Identifier
IDM	Identitätsmanagement
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMPACT	International Medical Product Anti-Counterfeiting Taskforce
IP	Ingress Protection
ISO	International Organization for Standardization
JIS	just-in-sequence
JIT	just-in-time
kbit/s	Kilobits per second

kHz	Kilohertz
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDL	Logistik-Dienstleister
LF	Low Frequency
LFSR	Linar Feedback Shift Register
LMAP	Lightweight Mutual Authentication Protocol
LS	Local System
LT	Ladungsträger
MA	Media Adaption
MD5	Message Digest Algorithm 5
MES	Manufacturing Execution System
MHz	Megahertz
MW	Microwave
NFC	Near Field Communication
NSI	Numbering System Identifier
OEM	Original Equipment Manufacturer
ONS	Object Naming Service
PC	Protocol Control
PDA	Personal Digital Assistant
PHAGRO	Pharmagroßhandel
PK	Public Key
PKI	Public Key Infrastructure
PMID	Product Manufacturer Idenitifier
PML	Physical Markup Language
PoS	Point of Sale
POWF	Physical One Way Function
PUF	Physical Unclonable Function
PZN	PharmaZentralNummer
RAM	Random Access Memory
RF	Radio Frequency
RFID	Radio Frequency Identification
RND	Random Number
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adleman
SAML	Security Assertion Markup Language
SHA-1	Secure Hash Algorithmus 1
SCM	Supply Chain Managements
SGTIN	Serialized Global Trade Item Number
SQL	Structured Query Language
SSL	Secure Socket Layer
TDT	Tag Data Translation
TEA	Tiny Encryption Algorithm
TID	Tag Identification
TLS	Transport Layer Security
UCC	Universal Code Council
UID	Unique Identifier
UHF	Ultra High Frequency
UII	Unique Item Identifier
VDA	Verband der Automobilindustrie
VPD	Variable Produktdaten
WEP	Wired Equivalent Privacy
WHO	Welthandelsorganisation
WLAN	Wireless Local Area Network
WORM	Write-Once Read-Many
WMS	Warehouse Management System
XML	Extensible Markup Language

1 Ziel der Untersuchung

Ziel der Untersuchung ist es, anhand von mittelfristig zu erwartenden RFID-Anwendungen verschiedener Kernbranchen der deutschen Wirtschaft die Anforderungen an die technologieintegrierte Datensicherheit von RFID-Systemen zu analysieren und offene technologische Fragestellungen zu thematisieren. Da die technische Einbindung der RFID-Technologie stark von Branche und Einsatzgebiet abhängt, zeigen sich manche realen Sicherheitsbedrohungen erst im Zusammenhang mit konkreten Anwendungsszenarien. Anhand der Szenarien "Unternehmensübergreifende Werkstückidentifikation und Supply Chain (Produktion)", "Auszeichnung von Konsumgütern (Handel)", und "Fälschungssicherheit von Medikamenten" definiert die Studie Sicherheitsanforderungen und leitet konkrete Sicherheitsmaßnahmen ab. Anschließend werden diese mit den bisherigen technischen Umsetzungen verglichen, um offene FuE-Fragestellungen zu identifizieren und FuE-Empfehlungen zu geben. Die in der Untersuchung identifizierten offenen FuE-Fragestellungen sollen der deutschen Forschung und Industrie helfen, zielgerichtet die derzeitigen technologischen Engpässe zu überwinden und die führende Position der Bundesrepublik in der Entwicklung und Anwendung von RFID-Systemen weiter auszubauen.

2 RFID-Technologie

2.1 Technische Grundlagen

RFID steht für "Radio Frequency Identification" und bezeichnet Verfahren zur automatischen Identifizierung von Objekten über Funk, also berührungslos und ohne Sichtkontakt (Line of Sight). RFID-Systeme bestehen aus mindestens drei Komponenten: RFID-Tag (auch: RFID-Transponder, Label, Funk-Etikett), Sende-Empfangseinheit (RFID-Leser) und Softwaresystem, z.B. RFID-Middleware und Server mit Datenbank als Backend. In Abb. 1 sind die Hardwarekomponenten eines RFID-Systems schematisch dargestellt. Die technischen Einzelheiten sind in [finkenzeller06] ausführlich beschrieben.

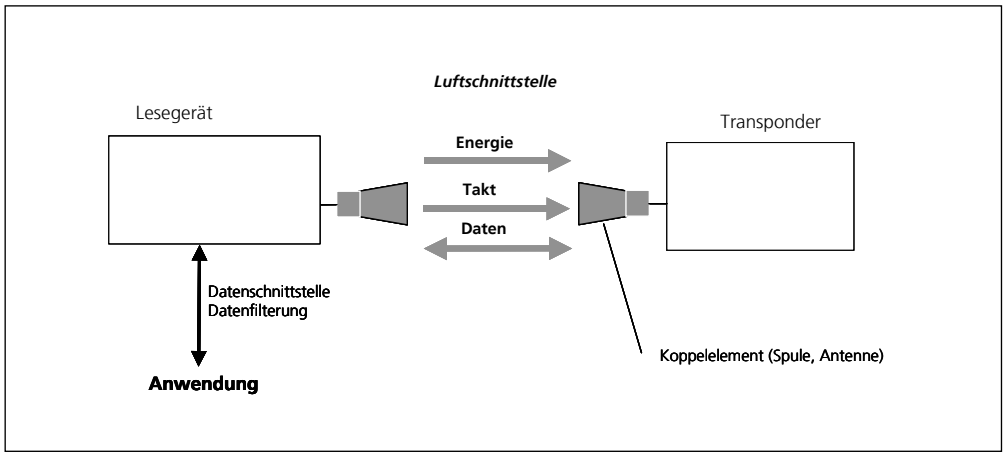


Abb. 1 – Hardwarekomponenten eines RFID-Systems

Das Tag ist der mobile Teil des RFID-Systems. Es nimmt die von der Leseeinheit gesendete Signale auf und antwortet automatisch darauf. Tags stellen die eigentlichen Datenträger eines RFID-Systems dar. Das Lesegerät versorgt das Tag über die Luftschnittstelle mit Energie für die Datenübertragung. Sobald ein Tag in die Nähe – den Empfangsbereich – eines passenden Lesegerätes kommt, liest das Lesegerät die gespeicherten Daten kontaktlos aus. Über eine Datenschnittstelle können RFID-Systeme mit Anwendungen kommunizieren und in andere IT-Systeme eingebunden werden, siehe 2.1.3.

2.1.1 Charakterisierung von RFID-Tags

Die existierende RFID-Technologie ist sehr facettenreich: Über 500 verschiedene Typen von RFID-Tags sind auf dem Markt erhältlich, darunter:

- passive Tags ohne eigene Stromversorgung
- semi-passive Tags mit eigener Stromversorgung für den Chip, während das Senden der Daten durch den Leser induziert werden muss
- aktive Tags mit eigener Stromversorgung, die auch dem Senden der Daten dient

Tags sind für verschiedene Frequenzbereiche erhältlich, vor allem für die Niederfrequenz (LF 100-135 kHz), Hochfrequenz (HF 13,56 MHz), Ultrahochfrequenz (UHF 433 MHz, 865-

868 MHz in Europa, 902-928 MHz in den USA) und für den Mikrowellenbereich (MW 2,45 und 5,8 GHz). Die zulässigen Frequenzbereiche werden durch nationale und internationale Institutionen festgelegt. Dabei werden mit der Frequenz auch die zulässigen Bandbreiten, Sendeleistungen, Sendedauern, Modulationsverfahren und Arbeitsweisen der Lesegeräte vorgeschrieben. Beispielsweise sind für den UHF-Bereich in den USA 4 W (EIRP), in Europa dagegen nur 2 W (ERP; entspricht 3,28 Watt EIRP) maximale Strahlungsleistung zugelassen. Im HF-Bereich ist die maximale magnetische Feldstärke im Abstand von 10 m festgelegt. In den USA dürfen dabei 42 dBμA/m, in Europa 60 dBμA/m nicht überschritten werden.

RFID-Chips realisieren in Abhängigkeit von ihrer Verwendung verschiedene Zugriffsarten: Nur Auslesen (Read-Only), einmaliges Beschreiben (Write-Once-Read-Many) oder auch oftmaliges Wieder-Beschreiben (Read-Write). Es gibt Tags mit einfachen Speicherchips bis hin zu Mikroprozessorkarten mit RFID-Funkschnittstelle. Je nach Intelligenz des Chips besitzen Tags die Fähigkeit zu komplexeren Protokollen wie etwa Authentisierung oder Verschlüsselung. Die Standardisierung der physikalischen Luftschnittstellen und der Übertragungsprotokolle ist mit rund 70 Normen entsprechend mannigfaltig und orientiert sich grob an den Frequenzen und Einsatzbereichen. Eine Auswahl der wichtigsten Standards zeigt Abb. 2.

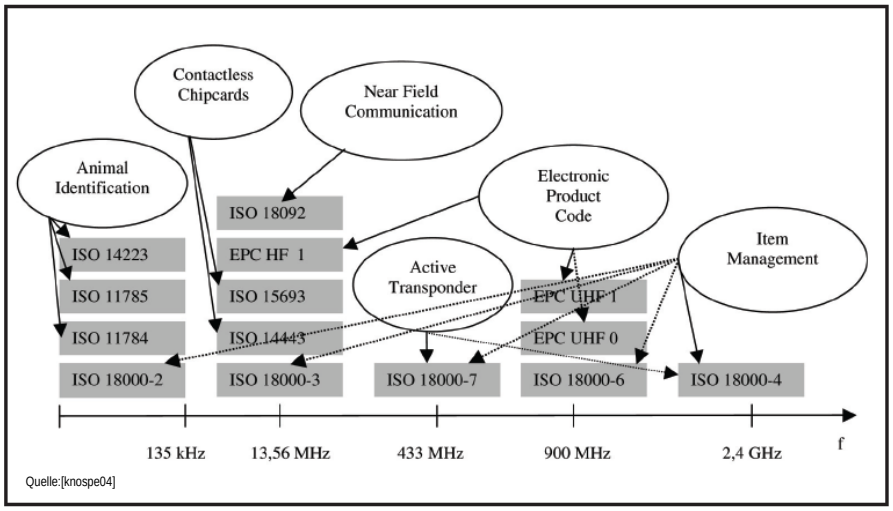


Abb. 2 – RFID-Standards

2.1.2 Physikalische Lesereichweiten

Unterschiedliche Frequenzen, Bandbreiten und Sendeleistungen führen zu unterschiedlichen Lesereichweiten. Ein wesentliches frequenzabhängiges Kriterium für die Kommunikation an der Luftschnittstelle ist die Unterscheidung von Nah- und Fernfeld. Im Nahfeld der Antenne hat sich ein elektromagnetisches Feld noch nicht ausgebildet, d.h. Energie wird nicht weitergetragen, sondern ist in einem magnetischen Feld gespeichert. Tags im Nahfeld können durch induktive Kopplung ihre Energie aus dem Feld beziehen, wobei die resultierende Schwächung des Feldes direkt von der Sendeantenne gemessen werden kann. Im Fernfeld wird dagegen Energie weitergetragen und es gibt keine Rückwirkung auf die Sendeantenne mehr. Das Tag muss daher die Daten entweder aktiv an das Lesegerät

senden oder nach dem so genannten Backscatter-Prinzip die Reflexionseigenschaften seiner Antenne entsprechend den Daten modulieren, so dass der Leser aus der reflektierten Welle die Informationen erhält. Die Grenze zwischen Nah- und Fernfeld ist proportional zur Wellenlänge λ, welche über die Lichtgeschwindigkeit c mit der Frequenz ν gekoppelt ist:

Nahfeld-Radius $r = \lambda / 2\pi$ mit $\lambda = c / \nu$

Tab. 1 zeigt die Grenzen zwischen Nah- und Fernfeld für die unterschiedlichen Frequenzbereiche. Die meisten RFID-Systeme verwenden passive Tags, welche durch induktive Kopplung im magnetischen Feld LF- bzw. HF-Bereich arbeiten. Die induktive Kopplung funktioniert im Nahfeld am besten, weil nur dort das Magnetfeld stark genug ist, um im Chip ein elektrisches Feld für die Energieversorgung und für die Lastmodulation zur Datenübertragung zu induzieren. Der praktische Leseabstand liegt aber noch weit unter dem Nahfeld-Radius, da die magnetische Feldstärke im Nahfeld proportional zur dritten Potenz der Entfernung abnimmt. Als Faustregel kann für den Leseabstand der Durchmesser der Spule des Lesegeräts gelten [lampe05]. Tags im UHF-Bereich arbeiten meist mit elektromagnetischer Backscatter-Kopplung, da das Nahfeld nur einen sehr kleinen Radius hat. Passive UHF-Tags und aktive Tags sind demnach nicht auf das Nahfeld angewiesen [thornton06].

Tab. 1 – Grenze zwischen Nah- und Fernfeld

Sendefrequenz	Wellenlänge	Nahfeld-Radius
125 kHz (LF)	2400,00 m	382,00 m
13,56 MHz (HF)	22,00 m	3,50 m
868 MHz (UHF)	0,35 m	0,06 m
2,45 GHz (MW)	0,12 m	0,02 m

Bei der Betrachtung der Reichweiten, in der RFID-Signale empfangen werden, muss zwischen dem Forward-Channel und dem Backward-Channel unterschieden werden. Im Forward-Channel erfolgt die Datenübertragung vom Leser zum Tag. Diese Übetragung ist von der Reichweite der Energieübertragung abhängig. Die Datenübertragung vom Tag zum Leser erfolgt im Backward-Channel und ist von der Reichweite der Lastmodulation abhängig. Der normale Betriebsabstand (Operating Range), bei dem eine zuverlässige Kommunikation zwischen Tag und Leser gewährleistet ist, liegt weit unterhalb der maximalen Reichweiten beider Übertragungskanäle. Er ist abhängig von der Anwendung, der physikalischen Anwendungsumgebung und den gesetzlichen Regelungen zur Nutzung der Frequenzen. Beide Kommunikationskanäle können aber durch Angreifer abgehört werden, die sich nicht an die gesetzlichen Grenzwerte halten und leistungsfähigere Leser und Antennen einsetzen. Daher muss mit größeren Abhörreichweiten gerechnet werden, welche sich wie folgt klassifizieren lassen [ranasinghe06], siehe Abb. 3.

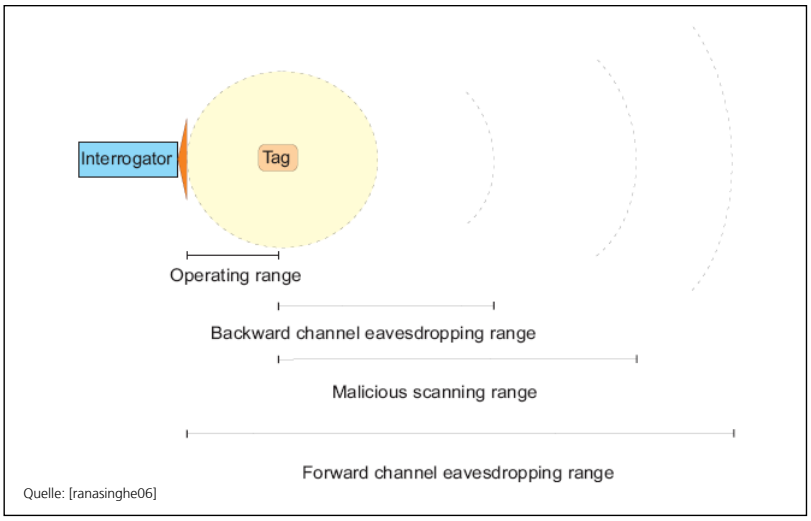


Abb. 3 – Klassifikation von Lesereichweiten

Die Abhörgrenze des Backward-Channels ist bei passiven RFID-Tags im Vergleich zum Forward-Channel relativ gering, kann aber von Angreifern weit über den Betriebsbereich erweitert werden, indem empfindlichere passive Abhörgeräte eingesetzt werden. Ein Angreifer kann aber auch aktiv abhören, d.h. die Tags durch ein eigenes Lesegerät mit Leistung versorgen und dabei auch unterschiedliche Antennen zum Senden und Empfangen einsetzen, die zum Abhören optimiert sind. Damit kann ein Angreifer die Reichweite des Backward-Channels zur "Malicious Scanning Range" erweitern [kasper06, kirschenbaum06].

Wird die Sendeleistung von Lesegerät und Tag betrachtet, so lässt sich das magnetische Wechselfeld des Forward-Channels bei 135 KHz und 13,56 MHz (Leseabstand 10-15 cm) theoretisch bis zu einigen 10 m abhören, der viel schwächere Backward-Channel (ca. 1% der Sendeleistung) aber nur etwa bis zum 5-fachen des Leseabstands [finke04]. In folgender Tabelle finden sich praktische Grenzwerte für die Kommunikation im Backward-Channel eines HF-Tags gemäß [kvir05].

Tab. 2 – Maßnahmen zur Erhöhung der Kommunikationsreichweite

Methode	Max. Reichweite	Zusätzliche Kosten	Verfügbarkeit	Notwendiges Know-How
Standard-Lesegerät	10 cm	0 $	Hoch	Niedrig
Strom + Antenne	40 cm	< 100 $	Hoch	Mittel
Strom + Antenne + optimierte Software	50 cm	< 100 $	Mittel	Hoch
Strom + Antenne + optimierte Signalverarbeitung	55 cm	> 5000 $	Niedrig	Sehr hoch

Zum Abhören aus größeren Entfernungen sind spezielle Lesegeräte mit höherer Leistung, also mit größerem Durchmesser und größerer Leistung der Sendeantenne, erforderlich. Bei zunehmendem Antennendurchmesser nimmt aber im Lesegerät die magnetische Gegeninduktivität und damit der Pegel des Lastmodulationssignals ab und das Rauschen verstärkt sich, so dass sehr schnell eine Grenze erreicht wird, bei der der technische Aufwand des Signalempfangs sehr groß wird. Unter Optimierung aller Parameter (z.B. Sendeleistung und Empfangssensitivität des Kartenlesers, Antennengewinn des Lesers und des Tags, Stromverbrauch und Modulationseffizienz des Tags) liegt bei 13,56 MHz die maximale theoretische

Abhörgrenze zwischen 40 und 100 cm [finkenzeller06]. Allerdings gibt es auch Berichte, nach denen sich der Forward-Channel eines 915-MHz-Systems, dessen Kommunikationsreichweite normalerweise maximal 3 m beträgt, aus einer Entfernung von bis zu 100 m abhören lässt und unter idealen Bedingungen Reichweiten bis zu 1 km denkbar sind [weis03b].

2.1.3 Systemstruktur von RFID-Anwendungen

RFID-Technologie findet heute in vielen Bereichen Anwendung, z.B. in der Logistik zur Kennzeichnung von Handelsobjekten wie einzelne Produkteinheiten, Sammelgebinden, Paletten und Container. Das bedeutet, dass RFID-Systeme in unterschiedliche, oft unternehmensübergreifende Geschäftsprozesse eingebunden werden müssen. Häufig befinden sich viele Tags im Lesebereich eines Lesegerätes und das Lesegerät muss erkennen, welche Daten zu welchem Tag gehören. Neben der automatisierten Identifizierung von einzelnen Objekten durch das RFID-System spielen daher die Datenfilterung, die Organisation und Verwaltung der mit den Objekten verbundenen Daten (z.B. Bearbeitungszustand, Qualitätsdaten) in den dahinter liegenden IT-Anwendungen eine wichtige Rolle. Deshalb ist eine umfassende IT-Architektur notwendig, welche die RFID-Systeme stabil einbettet und einen zuverlässigen Betrieb gewährleistet.

Die Systemarchitektur für RFID-Anwendungen kann als Schichtenmodell dargestellt werden (siehe Abb. 4). Die unterste Ebene enthält die RFID-Hardwarekomponenten RFID-Reader, und RFID-Tags. Die gelesenen Rohdaten werden in der Edgeware-Ebene gefiltert. Dies kann im Lesegerät selbst oder z.B. auf einem Server geschehen. Von dort werden die gefilterten Daten als Events & Alerts an die Middleware übertragen. Die Middleware schlägt die Brücke zu den Geschäftsanwendungen im Backend [bitkom05].

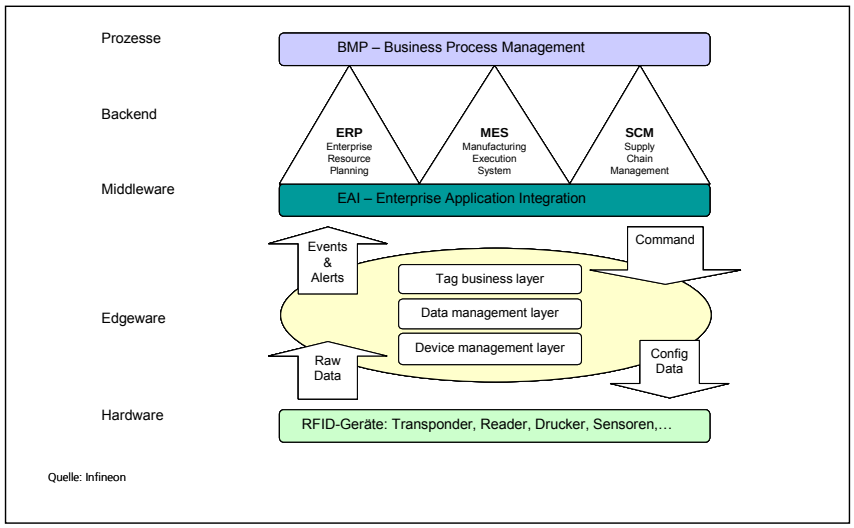


Abb. 4 – Systemarchitektur für RFID-Anwendungen

RFID-Lösungen müssen sachgerecht in das Geschäftsumfeld eingebettet, Verantwortlichkeiten klar zugeordnet und Schnittstellen genau definiert werden. So ist eine wesentliche Voraussetzung für eine weite Verbreitung von RFID die Anwendung einheitlicher und unternehmensübergreifender Standards. Es sind vor allem die Organisationen ISO und EPCglobal,

die RFID-Standards entwickeln. Die Standards kommen auf den unterschiedlichen Ebenen zum Tragen und können entsprechend in Technologie-, Daten- und Anwendungsstandards unterschieden werden. ISO und EPCglobal unterstützen die Spezifikationen der European Article Numbering Association (EAN) und des Universal Code Council (UCC), welche die Datenstrukturen der weit verbreiteten Barcodesysteme definieren. EPCglobal hat sich dabei ein globales Netzwerk von unternehmensübergreifenden Produktinformationen zum Ziel gesetzt (siehe 2.2.2).

2.2 Relevante Spezifikationen

2.2.1 ISO-Standards

Zum Thema Güter- und Warenwirtschaft mit RFID (Item-Management) gibt es eine ganze Reihe von ISO-Standards, die sich nahtlos in ältere Normen einfügen, die auf Basis des Barcodes entwickelt wurden. Da die Infrastruktur für Barcodes in den Betrieben und Logistikketten bereits sehr gut funktioniert, ist eine Migration von gedruckten Barcodedaten auf RFID-Technik ohne große Systemanpassung möglich. Dies wurde bei der Spezifikation der Datenprotokolle berücksichtigt. Tab. 3 führt einige ISO-Standards auf, welche für diese Studie relevant sind und im Folgenden kurz vorgestellt werden.

Tab. 3 – ISO-Standards für die Güter- und Warenwirtschaft mit RFID

Nummer	Titel
ISO 15693	Vicinity cards
ISO 15961	Data protocol: application interface
ISO 15962	Data protocol: data encoding rules and logical memory functions
ISO 15963	Unique identification for RF tags
ISO 18000-1	Reference architecture and definition of parameters to be standardized
ISO 18000-3	Parameters for air interface communications at 13,56 MHz
ISO 18000-6	Parameters for air interface communications at 870 to 930 MHz (UHF)

ISO 15693

Dieser Standard definiert Vicinity Cards, d.h. kontaktlose Chipkarten mit einer Reichweite bis 1,5 m. In drei Teilstandards werden die physikalischen Eigenschaften, die Luftschnittstelle und Initialisierung, Antikollisions- und Übertragungsprotokolle beschrieben. Die Frequenz des Operationsfeldes beträgt 13,56 MHz. Das Antikollisionsverfahren, das Übertragungsprotokoll, die zwei definierten Datenübertragungsmodi (1,65 kbits/s und 26,48 kbits/s) und weitere Definitionen wurden Grundlage von ISO 18000-3 Mode 1 (siehe unten).

ISO 15961 und 15962

ISO 15961 und ISO 15962 spezifizieren ein Datenprotokoll zum Austausch von RFID-Informationen für das Item Management. Der Zugriff auf die Daten im Tag ist nur durch das passende in ISO 18000 spezifizierte Luftschnittstellenprotokoll möglich. Unterschiedliche Anwendungsstandards können eigene Datensets und Datenverzeichnisse haben, müssen aber dafür sorgen, dass die Daten in einer eindeutigen Weise verarbeitet werden. Das definierte Datenprotokoll ist unabhängig von den verschiedenen Protokollen an der Luftschnittstelle, die in ISO 18000 spezifiziert sind. So können neue Luftschnittstellen in ISO 18000 definiert

werden, ohne dass das Datenprotokoll geändert werden muss. Die Unabhängigkeit wird durch die Implementation in unterschiedlichen Ebenen der Protokollhierarchie erreicht. Das Datenprotokoll bezieht sich vorwiegend auf die höheren Ebenen, siehe Abb. 5.

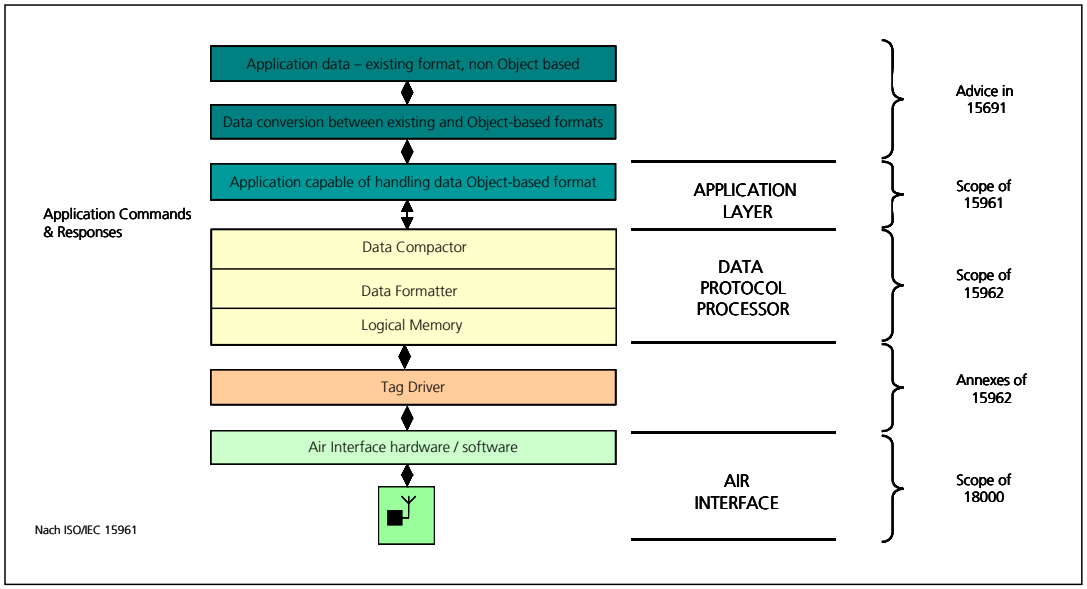


Abb. 5 – RFID-Protokollebenen für Item Management nach ISO 15961 und 15962

Abb. 6 zeigt das Schema einer Implementation, bei der das Datenprotokoll im Leser (Interrogator) abläuft.

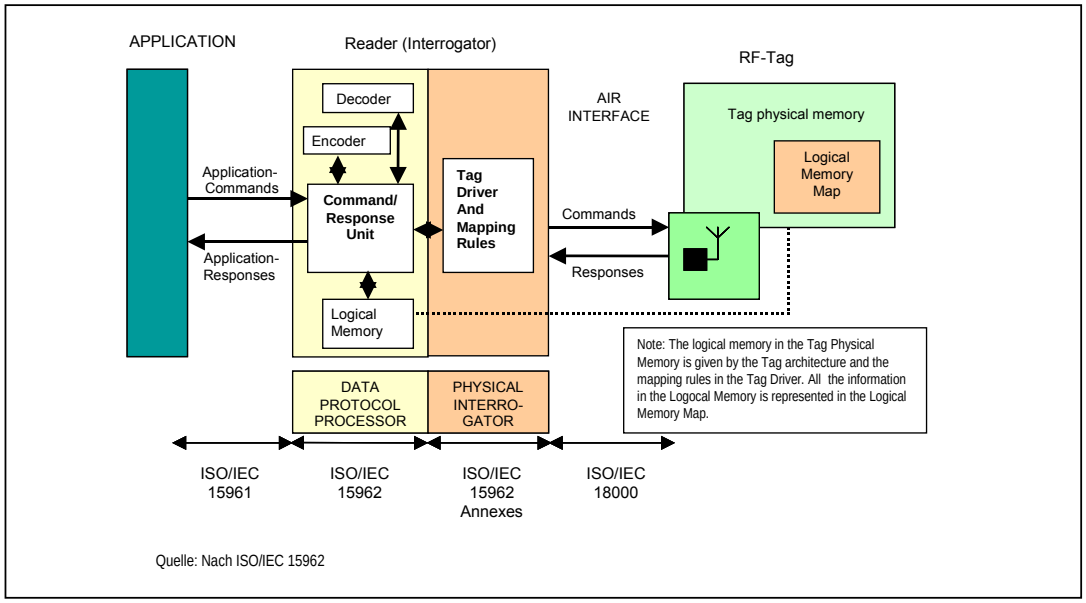


Abb. 6 – Schnittstellen und Funktionen einer ISO-konformen RFID-Implementation

Die Anwendung kann z.B. aus einer Datenbank und der Anwendungssoftware des Benutzers bestehen. Zwischen einer RFID-Anwendung und einem RFID-Leser werden Daten übertragen, die entsprechend ISO 15961 formatiert sind. Da viele Anwendungssysteme mit jeweils unterschiedlichen Datenformaten, z.B. entsprechend der Barcodesyntax, existieren, ist

ein Schnittstellenmodul sinnvoll, welches die Daten von und in diese Anwendungsformate konvertiert. Dieser Bereich wird von ISO 15962 abgedeckt. Der Interrogator ist ein Modul, das eine Schnittstelle zum Tag besitzt und eine erste Bearbeitung gelesener Tag-Daten vornimmt. Die Daten der Anwendung werden im Logical Memory zwischengespeichert, über Mapping Rules im Tagdriver in tagspezifische Kommandos umwandelt und an das Tag gesendet. Umgekehrt wird eine Antwort des Tags im Tagdriver in eine anwendungsspezifische Antwort konvertiert und die Daten entsprechend der MappingRules ins LogicalMemory geschrieben, bevor sie an die Anwendung weitergegeben werden.

ISO 15961 definiert eine Datenschnittstelle zwischen RFID-Leser und einem Anwendungssystem. Die Spezifikation umfasst die Übertragungssyntax, die Anwendungskommandos und Antworten zwischen Anwendung und RFID-Tag. Sie enthält eine formale Beschreibung aller Prozesse unter Verwendung von ASN.1. Der Standard definiert keine Maßnahmen zur Datensicherheit, gibt aber Empfehlungen zur Ablage verschlüsselter Daten im Tag. Die Anwendung ist in diesem Fall für die Verschlüsselung und Entschlüsselung verantwortlich.

ISO 15962 behandelt die Schnittstelle zwischen RFID-Leser und Tag. Allgemeine Kodierungsregeln und Funktionen des logischen Speichers werden spezifiziert, z.B. wie die Daten dem Tag präsentiert und wie umgekehrt die aus dem Tag gelesenen Daten im Leser verarbeitet werden. Dieser Standard spezifiziert dazu Kommandos an den Tagtreiber (z.B. zur Sperrung von Daten auf dem Tag) und Regeln zur Kodierung, Formatierung und Komprimierung von Daten.

ISO 15963

Dieser Standard legt ein Schema für eindeutige Identifikationsnummern (Unique Identifier, Tag-ID) der Tags fest und unterstützt u.a. die EAN-UCC-Spezifikationen. Jeder Herausgeber einer Identifikationsnummer muss selbst eindeutig identifizierbar sein. Es sind dazu fünf Klassen von Herausgebern definiert – eine Erweiterung ist möglich. Eine permanente UID besteht aus drei Feldern. Das erste Feld gibt die Klasse des Herausgebers an. Darauf folgt die Registrierungsnummer des Herausgebers und die von ihm vergebene eindeutige Seriennummer.

ISO 18000

Diese Multipart-Norm enthält Standards für die RFID-Luftschnittstelle des Item Managements für verschiedene international nutzbare RFID-Frequenzen. Für diese Frequenzen sind Parameter der Kommunikationsprotokolle an der Luftschnittstelle in einer Weise definiert, dass für alle Frequenzen weitgehend dasselbe Protokoll genutzt werden kann. Im Rahmen dieser Studie sind vor allem die Teile 1, 3 und 6 relevant, da sie sich auf die in den Anwendungsszenarien verwendeten Frequenzen beziehen. Nationale Regelungen können die Energie-, Frequenz- oder Bandbreitenzuteilung begrenzen, was zu einer Reduzierung der Leistungsfähigkeit eines Systems führen kann. Verantwortlich für die Einhaltung der Vorschriften sind die Nutzer.

ISO 18000-1

ISO 18000-1 beschreibt generische Architekturkonzepte für die Identifikation von Objekten, wie sie beispielsweise in der Logistik gebraucht werden. Es werden Parameter definiert, die in jedem der folgenden Teile von ISO 18000 mit spezifischen Werten belegt werden. Der

Teil 1 enthält allgemeine Definitionen für den Datenaustausch an der Luftschnittstelle zwischen Tag und Reader am Referenzpunkt DELTA (siehe Abb. 7).

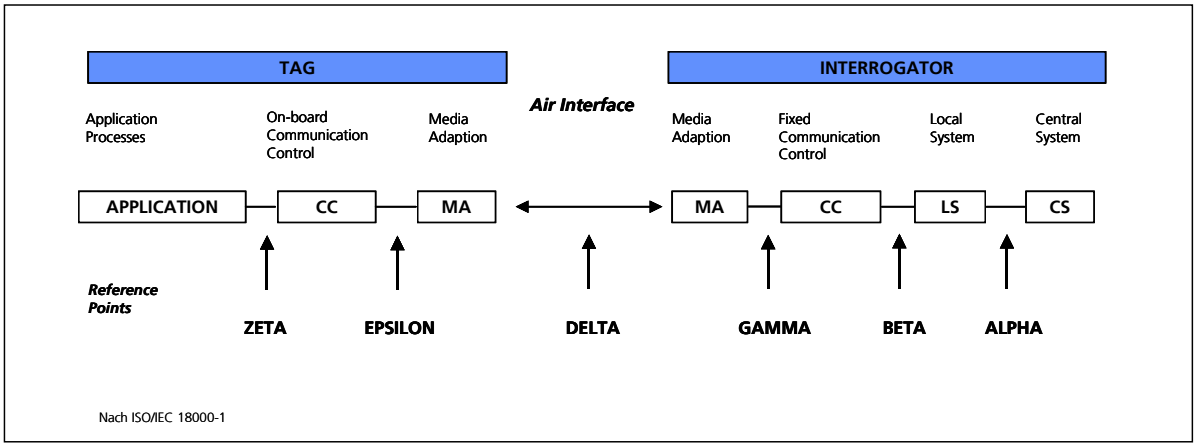


Abb. 7 – RFID- Kommunikationsarchitektur nach ISO 18000-1

ISO 18000-3

ISO/IEC 18000-3 definiert die Luftschnittstelle für RFID-Systeme, die mit der weltweit zugelassenen Frequenz 13,56 MHz arbeiten. Im Hinblick auf verschiedene Anwendungen sind zwei Modi definiert, die nicht interoperabel sind, aber sich nicht wesentlich gegenseitig stören. Beide Modi arbeiten mit der ReaderTalksFirst-Technik und mit passiven Tags. Beide sind für Identifizierungssysteme in Produktion, Logistik, Handel, Transport und für die Fluggepäckabfertigung definiert worden, wobei sich der Mode 2 besser für Förderbandsysteme eignet, bei denen es auf schnelle Datenerfassung ankommt.
Mode 1 basiert auf ISO 15693 (Vicinity Cards) und erweitert diesen Standard, um besondere Anforderungen des Item-Managements zu berücksichtigen und die Kompatibilität zu verbessern. Eine Protokollerweiterung sieht zusätzliche Features und ein alternatives Verfahren zur Kollisionsbehandlung vor. Die Datenrate ist aber relativ gering, siehe Tab. 4.

Mode 2 bietet eine Hochgeschwindigkeitsschnittstelle mit einem effizienteren Anti-Kollisionsverfahren. Kommandos werden mit Frequenzmodulierung kodiert und vom Leser zum Tag mit 423,75 kbit/s bei 13,56 MHz übertragen. Die Tags können unter 8 verschiedenen Kanälen mit Frequenzen zwischen 969 kHz und 3013 kHz (d.h. 13,56 MHz geteilt durch acht verschiedene Werte) wählen. Der Tag-Speicher ist virtuell in drei Bereiche eingeteilt: die Manufacturing System Memory Area für den Identifier des Chip-Herstellers, die User System Memory Area für die Konfigurationsdaten einer Anwendung und die User Memory Area für benutzer-definierte Anwendungsdaten. Der Speicher kann gegen Überschreiben geschützt werden. Die Tags können so konfiguriert werden, dass für die Schreib- und Lese-Kommandos ein Passwort erforderlich ist. Damit ein Kommando im Tag ausgeführt werden kann, muss das Passwort im Kommando mitgeführt werden und mit dem im Tag gespeicherten lesegeschützten Passwort übereinstimmen.

ISO 18000-6

ISO 18000-6 spezifiziert die physikalischen und logischen Anforderungen für passive ReaderTalksFirst-Systeme, die mit einer Frequenz von 860-960 MHz arbeiten und hohe Datenübertragungsraten ermöglichen. Der Standard spezifiziert die physikalischen Parame-

ter für die Kommunikation, die Kommandos und Anti-Kollisionsverfahren, welche in [finkenzeller06] dargestellt sind. Der Standard definiert drei Typen eines Übertragungsmodus:

- Typ A benutzt Pulse Interval Encoding und einen angepassten ALOHA-Algorithmus als Anti-Kollisionsverfahren,
- Typ B verwendet die Manchester-Kodierung und einen angepassten binären Suchalgorithmus (Tree Walking-Verfahren),
- Typ C entspricht den EPCglobal Class 1 Generation 2-Tags (siehe unten), benutzt Pulse Interval Encoding und einen slotted ALOHA-Algorithmus

In Tab. 4 sind die Datenübertragungsraten der wichtigsten in ISO 18000 definierten Luftschnittstellen gegenüber gestellt.

Tab. 4 – Datenübertragungsraten im HF- und UHF-Bereich

Luftschnittstelle	Frequenz	Forward-Link	Backward-Link
ISO 18000-3 Mode 1	13,56 MHz	1,65 oder 26,48 kbit/s	105,94 kbit/s
ISO 18000-3 Mode 2	13,56 MHz	423,75 kbit/s	105,94 kbit/s
ISO 18000-6 Typ A	860-960 MHz	33 kbit/s	40 oder 160 kbit/s
ISO 18000-6 Typ B	860-960 MHz	10 oder 40 kbit/s	40 oder 160 kbit/s
ISO 18000-6 Typ C	860-960 MHz	26,7 bis 128 kbit/s	40 bis 640 kbit/s

2.2.2 Spezifikationen von EPCglobal

EPCglobal entwickelt Standards für die einheitliche Nutzung der RFID-Technologie für Identifikationszwecke entlang der gesamten Versorgungskette über Länder- und Branchengrenzen hinweg. Dem liegt die Idee einer weltweit eindeutigen Kennzeichnung von Objekten in der Lieferkette zugrunde. Allgemeine Darstellungen des EPCglobal-Ansatzes geben [bitkom05, fleisch05, garfinkel05, epc-arch]. Tab. 5 nennt die wichtigsten Spezifikationen von EPCglobal.

Die Anwendung von ISO- oder EPC-Standards ist vom konkreten Einsatzbereich abhängig. Während sich der EPC dem Handel durch seine Verwandtschaft mit dem EAN-Standard und als zukünftige Mehrwertleistung für eine externe Datenbank-Referenzierung anbietet, ist für Einsätze in anderen Branchen auch die ISO-Normung erwägenswert. Denn diese erlaubt es, eigene Nummernsysteme mit einer größeren Anzahl von Stellen abzubilden. Darüber hinaus ist ein Referenzsystem mit dahinter liegender Datenbank in manchen Fällen nicht erforderlich und würde zu einer unnötigen Komplexitätssteigerung führen. Der EPC-Standard für EPC Class1 Gen2-Tags [epc-gen2] ist inzwischen als ISO 18000-6c in die ISO-Normung eingeflossen. GS1 (vormals EAN International, eine Standardisierungsorganisation im Bereich von Lieferketten) empfiehlt nun die Nutzung von ISO 18000-6c für alle UHF-Systeme [sander06].

Tab. 5 – Spezifikationen von EPCglobal

Titel	Inhalt
The EPCglobal Architecture Framework, Final Version, Juli 2005 [epc-arch]	Architekturübersicht
EPC™ Generation 1 Tag Data Standards Version 1.1 Rev.1.27 [epc-gen1data]	EPC-Tag-Datenstandard für Generation 1 Tags
EPCglobal Tag Data Standard Version 1.3 [epc-gen2data]	EPC-Tag-Datenstandard für Generation 2 Tags
EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz –960 MHz, Version 1.0.9 [epc-gen2]	EPC-Luftschnittstellen-Beschreibung
The Application Level Events (ALE) Specification Version 1.0 [epc-ale]	Schnittstelle für Ereignisse auf Anwendungsebene
Object Naming Service (ONS) EPCglobal Ratified Specification Version 1.0 [epc-ons]	Objekt Naming Service
EPCglobal Tag Data Translation (TDT) Ratified Standard Specification Version 1.0	Tag-Datenübersetzung
EPCglobal Certificate Profile Ratified Specification 1.0 [epc-cert]	X.509 Zertifikatsprofil für EPCglobal Network
Reader Protocol (RP) Standard, Version 1.1	Schnittstellen und Mindestfunktionsumfang EPC-kompatibler Reader
Reader Management (RM) Standard, Version 1.0	Schnittstellen und Mindestfunktionsumfang zur Überwachung EPC-kompatibler Reader

Der Electronic Product Code (EPC)

Mit dem Nummerierungsschema des EPC [epc-gen2data] können Produkte eindeutig identifiziert und die Kommunikation zwischen Lesegerät und Tag standardisiert werden. Der EPC basiert auf einer Erweiterung der weltweit verbreiteten EAN-Standards, der für Barcodedaten gebräuchlich ist. Das erleichtert die Migration von gedruckten Barcodes zu RFID. Mit dem EPC erhält jedes Objekt eine individuelle Seriennummer. Verschiedene EPC-Strukturen wurden definiert, insbesondere die 96-Bit-Strukturen General Identifier (GID) und Serialized Global Trade Item Number (SGTIN-96), welche die Barcodestruktur EAN/UCC um eine Seriennummer erweitert. Vereinfacht hat der EPC die folgende Struktur (siehe auch Abb. 8):

- Der Header gibt EPC-Version und die Kodierung an, z.B. SGTIN-96
- Der EPC-Manager stellt die Kennung des Nummernherausgebers (des Herstellers) dar
- Die Objektklasse bezeichnet die Objektnummer, z.B. die Artikelnummer des Produkts
- Die Seriennummer dient der eindeutigen Identifikation des Objektes

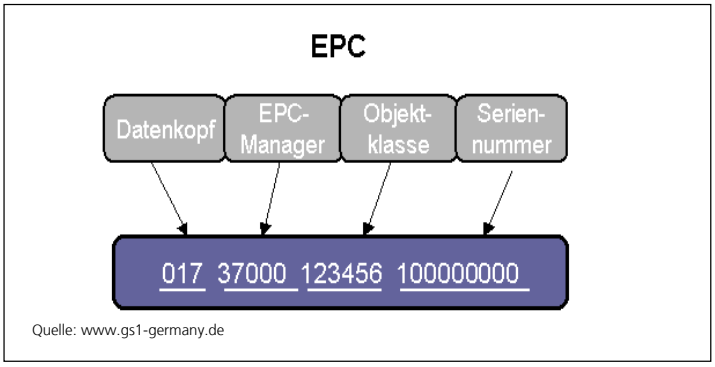


Abb. 8 – Struktur des Electronic Product Code (EPC)

Die EPC-Nummer enthält keine weiteren anwendungsspezifischen Daten. Produktinformationen, wie z. B. wo und wann das Produkt gefertigt wurde, wohin es versendet wird etc. werden von den Anwendungen verwaltet und gesondert über die EPC Information Services gespeichert. EPCglobal geht davon aus, dass in Zukunft jedes Objekt mit seiner EPC Informationen referenziert, die über das EPCglobal-Netzwerk den Herstellern, dem Handel und den Verbrauchern zur Verfügung gestellt werden. Die Informationen können Produktdaten enthalten, z.B. Konstruktions- und Produktionsdaten, Versand- und Verkaufsdaten, Wartung- und Verfallsdaten, Echtheitszertifikate, Gebrauchanweisungen und Lieferdaten.

Funktionsweise des EPCglobal-Systems

Das EPCglobal-Netzwerk umfasst die Komponenten [gs1]:

- **EPC Information Services (EPCIS)**: Der EPCIS stellt die Verbindung zwischen einem Unternehmen und dem EPCglobal-Netzwerk dar. EPC-Informationen werden im EPCIS gespeichert und den Teilnehmern des Netzwerks zur Verfügung gestellt.
- **Object Naming Service (ONS)**: Der ONS ist vergleichbar mit dem Domain Name Service (DNS) aus dem Internet und dient dem Auffinden des EPCIS des Herstellers eines Objektes anhand eines EPC. DerRoot ONS ist ein Dienst von EPCglobal und wird gegenwärtig von der Firma VeriSign betrieben, die auch den DNS verwaltet.
- **EPC Discovery Services**: Die EPC Discovery Services sollen das Auffinden von Produktinformationen zu einem bestimmten EPC ermöglichen. Im Gegensatz zu ONS verweisen die EPC Discovery Services auf alle Datenquellen (EPCIS), die Informationen zu einem bestimmten EPC gespeichert haben. Die Dienste werden zurzeit spezifiziert und können von EPCglobal-zertifizierten externen Dienstleistern bereitgestellt werden.

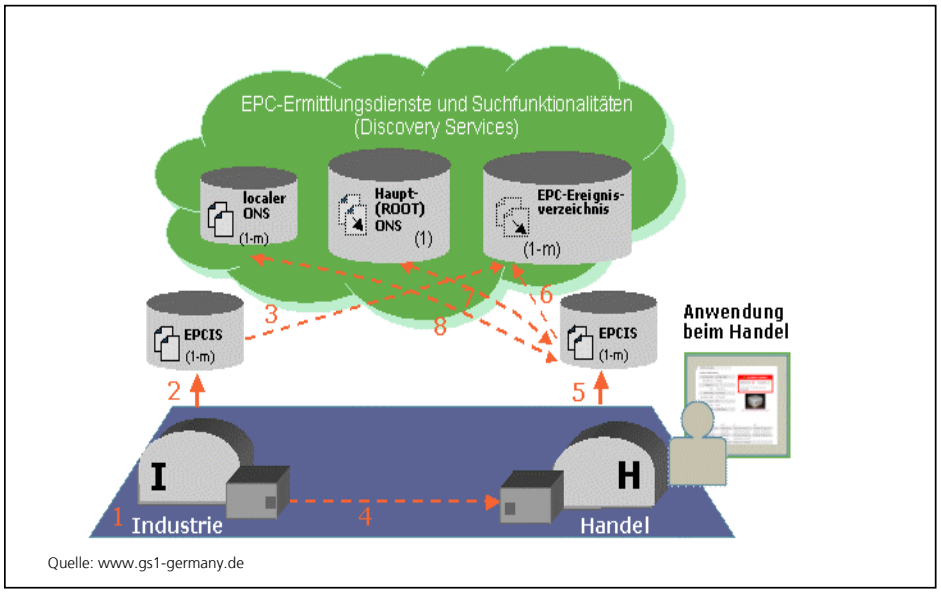


Abb. 9 – EPCglobal-Netzwerk Komponenten

Der Lebenszyklus eines EPC beginnt mit der Kennzeichnung des Objektes beim Hersteller, d.h. durch die Anbringung des EPC-Tags an das Produkt. Die EPC Discovery Services steuern z.B. über eine Authentisierung und Prüfung der Zugangsberechtigung den Zugriff auf Daten im EPCglobal-Netzwerk. Das folgende Beispiel einer EPC-Nutzung ist den GS1-Webseiten [gs1] entnommen, siehe auch Abb. 9:

1. Der Hersteller weist einem bestimmten Produkt einen EPC zu.
2. Der Hersteller speichert die entsprechenden Produktinformationen in seinem EPCIS.
3. Der EPCIS meldet dem EPCglobal-Netzwerk das EPC-Wissen mit Hilfe der EPC Discovery Services.
4. Das mit dem EPC gekennzeichnete Produkt wird an den Warenempfänger versendet.
5. Der Empfänger zeichnet den Empfang des Produktes in seinem EPCIS auf.
6. Der EPCIS des Empfängers meldet dem EPCglobal-Netzwerk über die Discovery Services den Empfang des Produktes.
7. Falls der Empfänger Produktinformationen benötigt, ermittelt er über die Discovery Services und den Root-ONS den lokalen ONS und den EPCIS des Herstellers.
8. Der Empfänger ruft über die Discovery Services die gewünschten Produktinformationen (z. B. Fertigungsdatum, Mindesthaltbarkeitsdatum) vom EPCIS des Herstellers ab.

Zusammenfassung Kapitel 2: RFID-Technologie

RFID steht für "Radio Frequency Identification" und bezeichnet Verfahren zur automatischen Identifizierung von Objekten über Funk. Dazu wird ein so genanntes Tag an ein zu identifizierendes Objekt angebracht. Passive Tags haben keine eigene Energieversorgung, sondern erhalten ihre Betriebsenergie von einem RFID-Lesegerät, sobald sie in dessen Reichweite kommen. Tags sind die mobilen Datenträger eines RFID-Systems und enthalten Informationen bezüglich der Objekte. Diese Informationen können von einem entsprechenden RFID-Lesegerät über eine Luftschnittstelle ausgelesen und verarbeitet werden, indem sie z.B. über eine Schnittstelle an Anwendungen in einem IT-System weitergereicht werden.
Die Technologie bietet sich besonders in Produktion und Handel und in der Lieferkette an, um Produkte eindeutig zu kennzeichnen und wiederzuerkennen. Damit RFID in verschiedenen Bereichen und in großem Umfang eingesetzt werden kann, sind allgemeingültige Standards nötig. ISO und EPCglobal haben z.B. Standards zur Datenstruktur der auf dem Tag gespeicherten Daten und zur Kommunikation über die Luftschnittstelle spezifiziert.

3 Sicherheit von RFID-Systemen

In diesem Kapitel werden die Bedrohungen von RFID-Systemen und die sich daraus ergebenen Anforderungen benannt. RFID-Tags und die Luftschnittstelle stehen dabei im Mittelpunkt. Hinsichtlich des Backend (z.B. Datenbanken, Serverkomponenten mit Datenaustausch über das Internet) werden nur RFID-spezifische Sicherheitsaspekte betrachtet. Die technischen Angriffe und Sicherheitsmaßnahmen werden definiert, die in den späteren Kapiteln auf ihre Bedeutung für die einzelnen Anwendungsszenarien untersucht werden sollen. Umfassende Darstellungen der RFID-Sicherheitsthematik finden sich in [bsi04, thornton06, garfinkel06, finkenzeller06]. Anwendungsspezifische Sicherheitsaspekte werden z.B. in [rand06, taucis06] thematisiert.

3.1 Allgemeine Sicherheitsaspekte

3.1.1 Angriffsmethoden

Die möglichen Bedrohungen und Angriffsmethoden bei RFID-Systemen sind sehr vielfältig, siehe z.B. [garfinkel05, bsi04]. Ein Angreifer kann verschiedene Absichten verfolgen, wenn er versucht, ein RFID-System zu stören, zu missbrauchen oder seine Sicherheitsmechanismen zu überwinden. Im Hinblick auf Datensicherheit kann es ein Angreifer auf die Gewinnung geheimer bzw. vertraulicher Daten abgesehen haben, zu deren sicheren Speicherung oder Übermittlung RFID-Technik eingesetzt wird. Zu den konkreten Angriffsszenarien zählt beispielsweise Industriespionage. Eine andere mögliche Absicht ist die Fälschung von Produkten (deren Echtheit z.B. mit Hilfe von RFID-Tags sichergestellt werden soll) oder die Manipulation gespeicherter oder übertragener Daten.

Unter dem Gesichtspunkt des Datenschutzes stellt die Überwachung von Personen mit Hilfe von RFID-Technik eine mögliche Bedrohung dar. Dies kann z.B. Kunden betreffen (von denen man sich unbemerkt ein Profil erstellen möchte) oder auch Mitarbeiter im eigenen Betrieb. Des Weiteren kann ein Angreifer das Ziel verfolgen, Systeme unbrauchbar zu machen oder ihre korrekte Funktionsweise zu stören, ohne dadurch selbst einen direkten materiellen oder informellen Gewinn zu erhalten. Im letzten Fall erhofft sich der Angreifer oftmals einen indirekten Vorteil, z.B. durch Störung von Produktionsprozessen eines Konkurrenzunternehmens. Zur Verfolgung dieser grundlegenden Ziele eines Angreifers kommen bei RFID-Systemen die nachfolgend beschriebenen generischen Angriffsmethoden in Betracht.

Sniffing

Beim Sniffing verfolgt ein Angreifer das Ziel, sich unbefugt in den Besitz von Daten zu bringen, die auf dem RFID-Chip gespeichert sind oder zwischen Chip und Lesegerät versendet werden. Zur Durchführung des Angriffs gibt es zwei grundlegende Ansätze: Die eine Möglichkeit besteht im heimlichen Abhören einer laufenden Kommunikation zwischen einem Chip und einem Lesegerät mit Hilfe eines entsprechenden Empfängers (Eavesdropping). Eine weitere Strategie besteht im unbefugten Auslesen des Chips mit einem eigenen, ggf. gefälschten Lesegerät (Unauthorised Reading). Die Praxis-Relevanz des Angriffs (insbesondere die Frage, ob es sich für einen Angreifer lohnt) hängt sehr von der Art der Daten, insbesondere ihrer Vertraulichkeit ab.

Spoofing & Replay-Attacken

Ein weiterreichendes Ziel eines Angreifers kann darin bestehen, Daten nicht nur unbefugt abzuhören, sondern auch zu manipulieren bzw. zu fälschen. Diese Angriffsart wird allgemein als Spoofing bezeichnet. Konkrete Angriffziele können hierbei die Kennnummer eines RFID-Chips, weitere auf dem Chip gespeicherte Inhalte oder auch zwischen einem Chip und einem Lesegerät ausgetauschte Informationen sein. Zur Ausführung des Angriffs kann entweder eine direkte Manipulation von Daten auf einem Chip oder eine Absendung manipulierter Daten an einen Chip (z.B. zur Vortäuschung eines vorhandenen autorisierten Lesegerätes) versucht werden.
Die sogenannten Replay-Attacken stellen hierbei eine besondere Angriffsstrategie dar: Hier werden die Daten aus einer echten Kommunikation vorher abgehört und zu einem späteren Zeitpunkt erneut eingespielt. Auf diese Weise wird dann z.B. einem RFID-Chip zu einem späteren Zeitpunkt die erneute Präsenz eines vorher verwendeten autorisierten Lesegerätes vorgetäuscht.

Man-in-the-Middle-Attacken

Bei einem Man-in-theMiddle-Angriff geht es dem Angreifer ebenfalls um das Fälschen von Daten. Die besondere Strategie besteht hierbei in der Zwischenschaltung des Angreifers in eine laufende Kommunikation: Die von der einen Seite abgesendeten Daten werden vom Angreifer abgefangen, und manipulierte oder gefälschte Daten werden an die andere Seite weitergereicht. Beide Seiten – der RFID-Chip und das Lesegerät – haben dabei fälschlicherweise den Eindruck, mit der echten, vertrauenswürdigen Gegenseite zu kommunizieren und bemerken nicht den "in der Mitte sitzenden Angreifer".

Cloning & Emulation

Ein weiteres mögliches Ziel eines Angreifers besteht im unbefugten Nachbauen bzw. Duplizieren von RFID-Chips mit bestimmtem Dateninhalt. Solche Angriffsszenarien werden als Cloning oder Emulation bezeichnet. Die Daten können dabei entweder selbst erzeugt worden sein oder aus einem erfolgreichen Sniffing stammen.

Denial of Service

Ein sogenannter Denial-of-Service-Angriff verfolgt nicht das Ziel einer unbefugten Gewinnung oder Manipulation von Daten. Vielmehr geht es dem Angreifer darum, die Funktion des RFID-Systems zu stören bzw. das System unbrauchbar zu machen. Hierzu gibt es die unterschiedlichsten Strategien:
Eine mögliche Art von Denial-of-Service-Angriffen, welche ohne aufwändige IT-Technik auskommen, sind mechanische Angriffe. Diese können z.B. in Form von mechanischer Zerstörung von RFID-Chips oder dem Entfernen des RFID-Chips vom zu schützenden Gegenstand bestehen. Allerdings sind solche Angriffe in der Regel nicht unbemerkt durchführbar und daher in vielen Anwendungsumgebungen nicht praktikabel.
Eine weitere Möglichkeit, RFID-Chips auf Dauer unbrauchbar zu machen, ist die Verwendung unbefugter Operationen zum Deaktivieren von Chips oder Löschen von Anwendungen auf dem Chip (Kill-Kommandos). Dies erfordert jedoch die Vortäuschung eines autorisierten Lese- oder Schreibgerätes und ist meist nur unter Labor-Bedingungen möglich.
Größere Praxisrelevanz für reale Anwendungsumgebungen haben Angriffe in Form einer temporären Störung der Kommunikation zwischen dem RFID-Chip und dem Lesegerät, die auch unbemerkt mit kleinen, versteckten Geräten durchgeführt werden können. Die einfach-

ste Art der Störung der Kommunikation ist ein gegenseitiges Abschirmen von Sender und Empfänger durch mechanische Unterbrechung des Übertragungsmediums mit Hilfe geeigneter Materialien (Shielding). Des Weiteren kann ein Angreifer z.B. einen aktiven Störsender verwenden oder ein Gerät, welches in sonstiger Weise die elektronmagnetischen Felder beeinflusst (z.B. Frequenzfilterung). Auch die Verwendung sogenannter Blocker-Tags ist möglich, welche dem Lesegerät die Präsenz verschiedener (passiver) RFID-Chips vortäuschen und so die Erfassung des eigentlichen Chips verhindern.

Tracking

Beim sogenannten Tracking hat es ein Angreifer auf eine unbemerkte Überwachung von Personen abgesehen. Die Strategie besteht darin, durch die Zuordnung von RFID-Chip-Nummern und den Zeitpunkten der Verwendung des Chips an einem bestimmten Terminal so genannte Bewegungsprofile zu erstellen.
Diese Angriffe sind naturgemäß besonders bei Verwendung von RFID-Chips für personenbezogene Ausweise relevant, sind aber auch in den RFID-Anwendungsszenarien im Hinblick auf die Sicherung von Produkten zu betrachten.

Relay-Angriffe

Sinn und Zweck der sogenannten Relay-Angriffe (Mafia Fraud Attacks) ist die unbemerkte Erhöhung der Lese-Reichweite eines RFID-Chips. Zur Durchführung benötigt der Angreifer zwei zusätzliche Geräte: ein sogenannter "Ghost" zur Kommunikation mit dem RFID-Chip und ein so genannter "Leech" zur Kommunikation mit dem Lesegerät. Beide Geräte sind auf größere Reichweiten ausgelegt und tauschen die jeweils empfangenen Signale gegenseitig aus. Auf diese Weise wird eine längere Übertragungsstrecke zwischen RFID-Chip und Lesegerät überbrückt, welche dann beide in derselben Weise wie bei unmittelbarer physikalischer Nähe reagieren. Ziel des Angreifers ist hierbei nicht die Fälschung von Daten, Lesegeräten oder RFID-Chips, sondern die gegenseitige Vortäuschung der für einen normalen Betrieb geforderten physikalischen Präsenz, was eine Art Man-in-the-Middle-Attacke darstellt. RFID-Chip und Lesegerät sollen so zu einer vom echten Systembenutzer unerwünschten gegenseitigen Kommunikation und entsprechenden (möglicherweise sicherheitskritischen) Aktionen angeregt werden, für welche eine physikalische Präsenz des RFID-Chips gefordert ist.

RFID-Malware

RFID-Systeme können auch Angriffen durch Malware ausgesetzt sein. Rieback et al. beschreiben beispielsweise einen Angriff, bei dem durch speziell konstruierte Daten eines RFID-Tags Buffer-Overflow- und SQL-Injection-Angriffe möglich sind [rieback06]. Hierdurch können beispielsweise Einträge in Datenbanken des Backend-Systems unautorisiert manipuliert werden. Evtl. kann auch in den Backend-Systemen beliebiger Programmcode ausgeführt werden, wenn ein Buffer-Overflow im Backend-System ausgenutzt wird.
Auch RFID-Lesegeräte können als Ursprung von Buffer-Overflow-Angriffen dienen. Da es sich hier gerade häufig um neuere, oft noch nicht umfassend analysierte Technologien handelt, ist die Wahrscheinlichkeit, dass hier Schwachstellen existieren, nicht zu unterschätzen. Gelingt es einem Angreifer Lesegeräte zu kompromittieren, so kann dies auch eine Bedrohung für die Backend-Systeme darstellen.

3.1.2 Sicherheitsanforderungen

Abb. 10 zeigt den abstrakten Aufbau eines RFID-Systems mit denjenigen Schnittstellen, an denen Sicherheitsanforderungen zur Abwehr der im voran gegangenen Kapitel genannten Angriffsmethoden erhoben werden können. Die Definition von Sicherheitsanforderungen ist umso wichtiger, je offener die Anwendung und das zugrunde liegende RFID-System konzipiert ist. Ein offenes RFID-System lässt heterogene Hardware- und Software-Komponenten verschiedener Hersteller zu. Die Systemkomponenten sind oftmals physisch verteilt und untereinander vernetzt. Es gibt unter Umständen keine zentrale Verwaltung und der Teilnehmerkreis ist nicht von vornherein bekannt oder begrenzt. Dann treten Anforderungen an die Datensicherheit insbesondere bei der Übertragung von Daten an den Schnittstellen der technischen Systemkomponenten auf (rot-schraffierte Schnittstellen). Datenschutzanforderungen bestehen dann, wenn Tags mit Personen und Personendaten physisch oder logisch verbunden sind (Schnittstellen in Blau). Sobald die Tag-Daten mit firmenspezifischen und persönlichen Daten verlinkt sind, kann die Einhaltung von Sicherheitsanforderungen bereits eine komplexe Aufgabe sein.

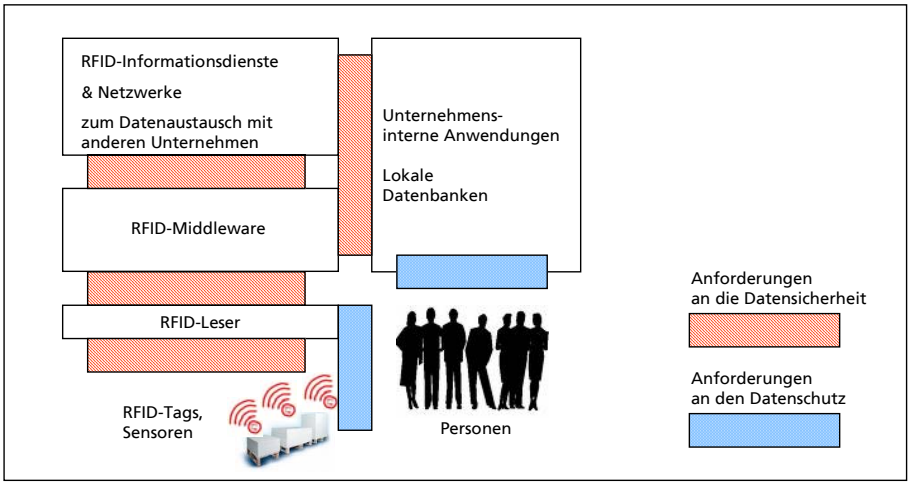


Abb. 10 – Lokalisation von Sicherheitsanforderungen in einem RFID-System

In offenen RFID-Systemen können die folgenden Sicherheitsanforderungen eine Rolle spielen: Funktionssicherheit, Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, und Verbindlichkeit (Nicht-Abstreitbarkeit).

Funktionssicherheit

Die Systemkomponenten sollten ihre Funktionen verlässlich zur Verfügung stellen und keine unzulässigen Zustände annehmen. Gefragt sind Maßnahmen, welche das technische Fehlverhalten einzelner Komponenten verhindern oder ausgleichen, um das Gesamtsystem und die erwarteten Ergebnisse von innen heraus konsistent zu halten. Dazu gehören eine ausreichende Validierung des Programmcodes und eine Fehlertoleranz gegenüber den Umweltbedingungen im Produktionsbetrieb. Beispielsweise sollte eine Tag-Leserate von unter 100% oder auch das unvermeidbare mehrmalige Auslesen einzelner Tags an einem Punkt der Lieferkette nicht dazu führen, dass Herkunftsnachweise unvollständig oder inkonsistent sind oder firmen-spezifische Anwendungen mit unnötigen Fehlermeldungen blockiert werden.

Authentizität

Die Verfahren sollten sicherstellen, dass sowohl die Systemkomponenten (insbesondere die RFID-Tags) als auch die gespeicherten und übertragenen Daten eine gesicherte Herkunft besitzen, d.h. durch charakteristische Eigenschaften und einer eindeutigen Identität nachweislich authentisch und vertrauenswürdig sind. Gefälschte Komponenten oder Daten dürfen nicht akzeptiert werden, sondern sollten Fehlermeldungen auslösen.

Vertraulichkeit

An den Schnittstellen der Datenübertragung sollte sichergestellt sein, dass nur autorisierte Instanzen auf sensitive Daten zugreifen oder diese entschlüsseln können, z.B. nur nach einer erfolgreichen Authentisierung. Die Daten sollten also zugriffsgeschützt in einer sicheren Umgebung abgelegt sein und in unsicheren Umgebungen kryptographisch verschlüsselt übertragen werden. Mit der Komplexität der Systeme verstärkt sich die Anforderung, unzulässige Informationsflüsse zu identifizieren und zu kontrollieren. So könnten z.B. berechtigte Teilnehmer geschützte Informationen abrufen und an unberechtigte Teilnehmer weitergeben.

Integrität

Die Mechanismen zur Datenübertragung sollten sicherstellen, dass Daten nach Verlassen ihrer Quelle (z.B. nach dem Beschreiben oder Auslesen eines Tags, nach dem Speichern oder Abfragen eines EPCIS) unverändert sind und nicht zufällig oder böswillig modifiziert oder gelöscht wurden. Die Daten müssen korrekt und vollständig übertragen und gespeichert werden. Sensitiven Daten dürfen nicht unautorisiert und unbemerkt manipulierbar sein.

Verfügbarkeit

Die Verfügbarkeit von Diensten ist für viele Anwendungsbereiche sicherheitsrelevant. Zugriffs- und Zugangskontrollen sind Beispiele von Systemdiensten, die stets gewährleistet sein sollten, um einerseits berechtigten Teilnehmer den Zugang zur Information zu sichern, andererseits aber unberechtigten Instanzen jegliche Nutzung und Beeinträchtigung der Dienste zu verwehren.

Verbindlichkeit

Die Verfahren müssen sicher stellen, dass eine Aktion nachweislich mit dem Urheber verbunden ist, z.B. dass ein Benutzer die Durchführung einer Aktion oder der Empfänger von Daten ihren Erhalt nicht abstreiten kann. Dies ist nicht nur im Bereich rechtsverbindlicher geschäftlicher Transaktionen (z.B. elektronischer Lieferschein oder Herkunftsnachweis) wichtig, sondern auch bei der Nutzung von Systemressourcen in Mehrbenutzersystemen (z.B. zur Abrechnung von Nutzungskosten). Eine Protokollierung einzelner Benutzeraktivitäten kann allerdings den Anforderungen des Datenschutzes entgegen stehen.

Datenschutz

Besondere Anforderungen an den Datenschutz kommen durch die mögliche Verknüpfung von Personen zu RFID-Daten auf, insbesondere an der Luftschnittstelle zwischen Tag und RFID-Leser. Der Datenschutz ist durchaus nicht nur am Ende der Lieferkette (Endkunden mit Tags in der Öffentlichkeit) ein Thema, sondern besonders dort, wo RFID-Systeme rechtmäßig installiert sind und Personen beruflich mit getaggten Objekten umgehen müssen, z.B. innerhalb der Lieferkette an Produktionsstätten, Lagerhäusern und an Verkaufsplätzen. Angestellte müssen ebenso vor unrechtmäßiger Profilbildung geschützt werden. RFID-Daten von

bewegten Objekten sollten z.B. nicht dazu verwendet werden, die Arbeitsleistung von Angestellten zu messen.

Rechtliche Aspekte in Bezug auf Datenschutz und RFID werden in [holznagel06] betrachtet. Die Speicherung und Verarbeitung personenbezogener Daten ist durch das Bundesdatenschutzgesetz (BDSG) geregelt. Wichtige Grundsätze sind darin das Recht auf informationelle Selbstbestimmung, das Recht auf Offenlegung der gespeicherten Daten, die Zweckbindung der Daten, das Prinzip der Erforderlichkeit (z.B. wenn es der Zweckbestimmung eines Vertragsverhältnisses dient) und die Erfordernis der Einwilligung des Betroffenen. Bei mobilen Speichermedien mit automatischer Verarbeitung ist grundsätzlich die Auskunft und Aufklärung des Betroffenen notwendig.
Die auf RFID-Tags gespeicherte Kennnummern wie der EPC stellen allein noch keine personenbezogenen Daten dar. Vielmehr muss die Verknüpfung dieser Kennnummer mit personenbezogenen Daten im Backend eines RFID-Systems betrachtet werden. Sofern nur die Tag-IDs und EPCs von Tags erfasst werden, ohne einen Bezug zur Person herzustellen, die mit den Tags umgeht, ist die Speicherung der Tag-Daten ohne Einwilligung des Betroffenen vom BDSG aus nicht verboten, da nämlich allein aus den Kennnummern kein Rückschluss auf die Person gezogen werden kann. Sobald jedoch die Kennnummern mit Daten verknüpft werden, die den Rückschluss auf eine bestimmte Person zulassen, fällt die Erfassung und Verarbeitung in den Anwendungsbereich des BDSG und erfordert damit die Information und Einwilligung des Betroffenen. Eine solche Verknüpfung könnte technisch etwa dadurch erfolgen, dass als Identifikationsmerkmal eine Kundenkarte (Payback, Happy Digits, Webmiles etc.), ein bargeldloses Zahlungsmittel (EC-, Kreditkarte) oder ein biometrisches Merkmal (Videoaufnahme einer der zahlreichen Überwachungskameras im Geschäft) herangezogen würde.

Für den Schutz der Persönlichkeitsrechte Betroffener haben die Datenschutzbeauftragten des Bundes und der Länder verbindliche Regelungen aufgezeigt. Diese fordern neben den aufgeführten Regelungen vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Auf der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26.-27. Oktober 2006 in Naumburg wurden u.a. die folgenden Forderungen zum Schutz der Persönlichkeitsrechte Betroffener aufgestellt [naumburg06]:

- Transparenz: Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- Kennzeichnungspflicht: Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- Keine heimliche Profilbildung: Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- Vermeidung der unbefugten Kenntnisnahme: Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.
- Deaktivierung: Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

3.1.3 Sicherheitsmaßnahmen

Authentisierung

Grundsätzlich besteht die Möglichkeit, auf einem RFID-Chip gespeicherte Daten oder vorhandene Applikationen durch Authentisierungsmechanismen zu schützen. Der Zugriff auf Datenobjekte ist dann nur noch nach einer erfolgreichen Authentisierung möglich, welche den Sicherheitsstatus zur Ausführung bestimmter Kommandos setzt. Als Authentisierungsmethoden können entweder eine passwort-basierte oder eine kryptographische Authentisierung zwischen RFID-Chip und Lesegerät verwendet werden. Letztgenannte Methoden erfolgen meist in Form eines Challenge-Response-Verfahrens mit einer vorher von der Gegenseite angeforderten Zufallszahl.
Mit Hilfe einer Authentisierung können unautorisierte Lese- und Schreibzugriffe (Spoofing-Attacken mit direkter Manipulation der Daten auf dem Chip), missbräuchliche Verwendungen von Kill-Kommandos und ggf. auch Cloning-Angriffe abgewehrt werden (letztere z.B. durch möglichst frühzeitige Präparierung von RFID-Rohlingen für bestimmte Anwendungen). Die oben genannte Challenge-Response-Methode dient auch der Verhinderung von Replay-Angriffen, da eine Zufallszahl immer nur für einen Authentisierungsvorgang gültig ist und somit derselbe Vorgang nicht durch erneutes Einspielen der vorher abgehörten Daten wiederholt werden kann.

Verschlüsselung

Zur Sicherung der Vertraulichkeit von Daten ist es sinnvoll, die Daten entsprechend zu verschlüsseln. Hier besteht zunächst die Möglichkeit, Daten in verschlüsselter Form auf dem Chip zu speichern und dann auch in der verschlüsselten Form aus dem Chip auszulesen.
Darüber hinaus bieten zahlreiche RFID-Chips auch die Möglichkeit an, die Datenübertragungsstrecke zwischen dem Chip und dem Lesegerät zu verschlüsseln. Dieser Schutzmechanismus dient vorrangig der Abwehr von Eavesdropping-Angriffen.

Integritätsschutz

Je nach Anwendung spielt weniger die Vertraulichkeit der Daten, sondern eher ihre Unversehrtheit und Unverfälschtheit eine Rolle. Zu diesem Zweck lassen sich mit ähnlichen Kryptomechanismen wie zur Verschlüsselung der Datenübertragung die Daten auch mit einer kryptographischen Prüfsumme versehen, welche eine authentische Datenübertragung – mit der Überprüfbarkeit der Herkunft der Daten und der Garantie ihrer Manipulationsfreiheit – sicherstellt. Hiermit können Replay- und Man-in-the-middle-Angriffe verhindert werden.

Zugriffsschutz

Wie auch andere Funktionen auf dem RFID-Chip kann der Lese- und Schreibzugriff auf Datenobjekte durch entsprechende Authentisierungsmechanismen geschützt werden (s.o.). Darüber hinaus gibt es auch die Möglichkeit, Daten auf dem Chip (die nicht dazu bestimmt sind, jemals wieder verändert oder aus dem Chip ausgelesen zu werden – z.B. kryptographische Schlüssel) komplett gegen Lese- oder Schreibzugriffe zu sperren. Hierauf aufbauend kann auch das weitere Aufbringen zusätzlicher Daten auf einen RFID-Chip unterbunden werden, indem man den gesamten von einer Applikation nicht benötigten Speicherbereich mit schreibgeschützten Dummy-Objekten versieht. Werden auf einem RFID-Chip ausschließlich Daten gespeichert, die während seiner Lebensdauer unverändert bleiben sollen und wird der Chip zu diesem Zweck komplett gegen jeglichen Schreibzugriff gesperrt, so spricht man auch von einem Read-Only-Tag.
Bei jeglichen Datenobjekten, bei denen auf das nachträgliche Auslesen bzw. Abändern verzichtet werden kann, bieten diese Schutzmechanismen eine ideale Abwehr der Sniffing- und Spoofing-Angriffe unter direktem Zugriff auf den Chip.

Kontrollmechanismen außerhalb des Chips

Neben den unmittelbaren Sicherheitsmechanismen auf dem RFID-Chip können bestimmte Angriffe auch durch geeignete Maßnahmen bzw. Vorrichtungen außerhalb des Chips detektiert bzw. unterbunden werden. Zur Verhinderung ungewollter Auslesevorgänge gibt es Detektoren, die auf ein vorhandenes Auslesegerät reagieren und ein entsprechendes Signal von sich geben. Zur Detektierung von Denial-of-Service-Angriffen, die auf der Manipulation des elektromagnetischen Feldes beruhen, können auf Seiten des Lesegerätes entsprechende Mechanismen zur Kontrolle der korrekten Feldparameter (Frequenz, Amplitude etc.) vorhanden sein.

Pseudonymisierung und dynamische IDs

Für bestimmte Anwendungen macht es Sinn, die Identität von RFID-Tags für einen Außenstehenden zu verschleiern. Möchte man ohne aufwändige kryptographische Schutzmechanismen auskommen, so bietet sich die Verwendung sogenannter "Pseudonyme" an, d.h. aus der wahren Identität abgeleitete Kennnummern, die eine eindeutige Wiedererkennung von RFID-Tags ermöglichen, jedoch nur von autorisierten Instanzen der ursprünglichen Identität wieder zugeordnet werden können.
Eine mögliche Strategie zur Verschleierung von Identitäten von RFID-Chips ist die Verwendung dynamischer ID-Nummern. Ein RFID-Chip besitzt dann zwar bei jedem Vorgang eine Kennung, die aber jedes Mal unterschiedlich ist, so dass sich z.B. durch ihr Zusammentragen aus verschiedenen Lesevorgängen für einen Außenstehenden kein Bewegungsprofil ergibt. Diese Sicherheitsmechanismen dienen vorrangig zur Abwehr von Tracking-Angriffen.

Deaktivierung und Verhindern des Auslesens

Einige Strategien zur Durchführung von Denial-of-Service-Angriffen können im positiven Sinne verwendet werden, wenn das Auslesen von Daten aus einem RFID-Chip entweder vorübergehend oder dauerhaft unterbunden werden soll. So kann ein Chip durch das gewollte Absenden eines Deaktivierungsbefehls dauerhaft unbrauchbar gemacht werden, wenn eine weitere Nutzung nicht mehr vorgesehen ist. Durch Verwendung von Blocker-Tags oder durch Shielding kann das ungewollte Auslesen des Chips temporär verhindert werden, z.B. solange er sich in einer möglicherweise unsicheren Umgebung befindet.

Neben einer totalen Deaktivierung des Chips besteht für den Benutzer (eine geeignete Bauart vorausgesetzt) auch die Möglichkeit, einen Teil des Empfangsbereiches abzutrennen und so die Reichweite des Chips (unter Beibehaltung seiner Grundfunktion) zu vermindern. Eine erste Lösung in dieser Richtung wurde jüngst mit den perforierten Clipped Tags von IBM entwickelt, siehe 3.2.7.

Abhörsichere Antikollisionsprotokolle

Zur zuverlässigen Unterscheidung verschiedener RFID-Chips, die sich im Bereich eines Lesegerätes befinden, gibt es verschiedene Arten von Antikollisionsprotokollen. Ein möglicher Schwachpunkt ist hierbei die Aussendung von bestimmten (z.B. den von einem Lesegerät erwarteten) ID-Nummern vom Lesegerät an eventuell vorhandene RFID-Chips, da der Forward-Link wegen seiner höheren Signalstärke leichter aus größerer Entfernung abhörbar ist. Abhörsichere Antikollisionsprotokolle zeichnen sich deshalb dadurch aus, dass entsprechende Aussendungen kompletter, von einen Angreifer nachvollziehbarer Kennungen durch das Lesegerät vermieden werden.

Verwendung kleinerer Reichweiten

Verschiedene RFID-Systeme können auf unterschiedliche Leseabstände zwischen Chip und Lesegerät ausgelegt sein. Grundsätzlich sind RFID-Chips auch noch außerhalb des normalen Leseabstandes abhörbar, vorausgesetzt man besitzt ein geeignetes Abhörgerät mit der entsprechenden Messempfindlichkeit. Im Hinblick auf Abhörsicherheit haben Systeme mit einem kleineren Leseabstand (für Normalbetrieb) den Vorteil, dass ein Angreifer dann zum Abhören aus größerer Entfernung ein entsprechend teureres und aufwändigeres Lesegerät benötigt als die für den Normalbetrieb des Systems vorgesehenen Geräte.

Vereinbarung kurzer Timeout-Zeiten

Auch wenn ein Man-in-the-middle- oder Relay-Angriff prinzipiell erfolgreich verläuft (d.h. die Daten kommen auf der Gegenseite an wie bei einer Versendung durch eine physikalisch präsente autorisierte Instanz), kann es beim Übertragungsweg über die zwischengeschalteten Geräte zu Verzögerungen bei der Signal-Übertragung kommen. Hier kann die Verwendung geeigneter Übertragungsprotokolle mit kurzen Timeout-Zeiten – welche für den normalen Leseabstand genügen, jedoch bei Man-in-the-middle- oder Relay-Angriffen ggf. überschritten werden – helfen, solche Angriffe zu erschweren.

Mechanische Sicherheitsmaßnahmen

Mechanische Denial-of-Service-Angriffe können bei passiven RFID-Chips (d.h. solche ohne eigene Stromversorgung) lediglich durch mechanische Schutzmaßnahmen unterbunden werden – z.B. zurückbleibende Beschädigungen an der Ware bei Entfernung des Chips. Weitergehende Maßnahmen wie z.B. automatische Alarmauslösung sind bisher nur bei aktiven Chips mit eigener Stromversorgung möglich.

3.2 Tag-integrierte Sicherheitsverfahren

Im Folgenden werden die Implementierungsbedingungen für Sicherheitsverfahren auf Low-Cost Tags und die Sicherheit der Low-Cost EPC-Tags skizziert. Danach werden Sicherheitsverfahren für die Kommunikation zwischen Tag und Lesegerät vorgestellt. Diese sind nach

den wichtigsten Sicherheitsmaßnahmen aus dem letzten Kapitel geordnet und bieten je nach Preisniveau geringen bis hohen Schutz. Einige der vorgestellten Verfahren sind noch nicht auf Tags implementiert worden oder erfordern den Einsatz kostenintensiver Mikroprozessoren, die in 3.2.8 vorgestellt werden. In den Kapiteln der Anwendungsszenarien kann auf dieser Grundlage besser abgeschätzt werden, welches Sicherheitsniveau und welcher Aufwand zum Schutz der Sachgüter und Personen gerechtfertigt ist.

3.2.1 Einschränkungen bei Low-Cost Tags

Die Forderung nach Low-Cost RFID-Tags stellt besondere Herausforderungen an die Auswahl von Sicherheitsmaßnahmen [ranasinghe06]. Die Kommunikation zwischen Tag und RFID-Leser ist grundsätzlich ungeschützt, d.h. die Tags können durch jeden Leser ausgelesen werden, der das entsprechende Protokoll an der Luftschnittstelle unterstützt. Die Chips sind einfach im Design, begrenzt in ihrer Funktionalität und nicht manipulationsgeschützt. Die Logik von Low-Cost Tags beschränkt sich meist auf die Bit-Operationen XOR, AND, OR, auf einfache Additionen und die Pseudo-Zufallszahlengenerierung. Auch die RFID-Leser sind aus Kostengründen meist einfach gehalten. Neben der einfach gehaltenen Hardwareausstattung setzen auch die folgenden Faktoren der Implementierung kryptographischer Mechanismen auf RFID-Tags enge Grenzen [ranasinghe06]:

- Gesetzliche Vorschriften: Obergrenzen der Leistungsübertragung, Spektralmasken, Frequenzen, Bandbreiten und die zur Verfügung stehenden Rechenzeiten
- Stromverbrauch: Eine kryptographische Einheit weist, verglichen mit den anderen Komponenten eines passiven Tags, den größten Stromverbrauch auf und vermindert daher die Performanz und Lesereichweite.
- Leistung des RFID-Systems: Die angestrebte Gesamtleistung des Systems (z.B. hohe Leseraten, zuverlässige Pulkerfassung, Datensicherheit) schränkt das Zeitfenster ein, in dem kryptographische Operationen beendet sein müssen. Müssen kryptographische Schlüssel oder Zertifikate in einer Datenbank aus einem Netzwerk abgerufen werden, so muss in jedem Fall mit Verzögerungen gerechnet werden.
- Stromunterbrechungen: Plötzliche Stromunterbrechungen sind eher die Regel als die Ausnahme und sollten den Chip mit kryptographischer Einheit nicht in einen undefinierten Zustand bringen

Als Faustregel für eine akzeptable Obergrenze des Stromverbrauchs kann gelten, dass die Kryptographie nicht mehr Strom verbrauchen sollte als das Schreiben von Daten in die passiven Tags. Zwischen Stromverbrauch und Chip-Architektur muss ein Kompromiss realisiert werden: Parallele Architekturen verbrauchen weniger Strom, sind aber teurer in der Herstellung. Die Reduzierung des Stromverbrauchs durch ein verbessertes Chip-Design ist seit langem ein Forschungsgebiet [rabaey96]. Als einfaches Maß für die Komplexität der Chips kann die Anzahl elektronischer Gatter gelten. Heutige Low-Cost Tags haben 5.000-10.000 Gatter, wobei maximal 3.000 Gatter für Sicherheitsmechanismen zur Verfügung stehen [peris-lopez06]. Hier gibt es Schätzungen, nach denen 1000 zusätzliche Gatter die Kosten des Tags jeweils um etwa 1 US cent erhöhen [lehtonen06a]. Tab. 6 zeigt an einer Auswahl

kryptographischer Algorithmen, wie viele Gatter diese jeweils benötigen [yu06]. Einen einfachen Kriterienkatalog mit Kenngrößen (z.B. Speicherbedarf, Anzahl der Gatter, Stromverbrauch) für die Auswahl von kryptographischen Algorithmen bietet [kaiser05].

Tab. 6 – Implementierung kryptographischer Funktionen

Implementierung	Mindestanzahl Gatter
Stream-Cipher Linear Feedback Shift Register (LFSR)	685
Low-Cost Hashing	1.700
Tiny Encryption Algorithm (TEA)	2.355
DES	3.400
Anvanced Encryption Standard (AES-128) mit RAM-Nutzung	3.595
Hashing SHA-1	4.244
Elliptic Curve Cryptography (ECC) [batina07]	8.000-11.000
Hashing MD5	16.000
Fast Hashing SHA-1 (Helion Technology)	20.000
Anvanced Encryption Standard (AES-128) in Hardware	20.000 – 30.000
RSA 1024 Bit	67.000

3.2.2 Sicherheitsmerkmale der EPC-Tags

In der bisherigen Entwicklung der EPC-Standards wurden kryptographische Mechanismen für die Datensicherheit und den Datenschutz bewusst auf ein Minimum beschränkt, um die Kosten der Tags und die Zeiten zum Erfassen und Auslesen der Tags gering zu halten. Die Architektur sieht bisher kein umfassendes Sicherheits- und Datenschutzkonzept vor, lässt aber Erweiterungen zu [epc-arch]. EPCglobal sieht für die Zukunft eine Tag-Hierarchie vor (siehe Tab. 7), in der jede höhere Tag-Klasse unter Nutzung der gleichen Luftschnittstelle mehr Funktionalität (und Sicherheit) aufweist als die darunter liegende Klasse.

Bisher sind nur Tags der Class 1 und Class 1 Generation 2 definiert, während die Eigenschaften der oberen Klassen lediglich informativ aufgelistet sind. Normativ ist bereits festgelegt, dass die höheren Tags die Funktion und Performanz von Class 1-Tags in derselben RFID-Umgebung nicht beeinträchtigen dürfen.

Die Spezifikation der Class 1 Gen 2-Tags [epc-gen2] gwinnt als Defacto-Standard für kostengünstige Tags immer mehr an Bedeutung. Die UHF-Luftschnittstelle in [epc-gen2] ist grundsätzlich ungeschützt, aber besser an hohe Geschwindigkeiten, ungünstige Lesebedingungen und die Pulkerfassung angepasst. Außer den einfachen Protokollen zur Berechnung von 16-Bit Prüfsummen, den so genannten Cyclic Redundany Checks (CRC), zur Sicherung der Datenübertragung weisen die EPC-Tags vor allem die folgenden Sicherheitsmerkmale auf: Das Kill-Kommando (mandatory), ein kontrollierter passwort-geschützter Lese- und Schreibzugriff (optional) und das Lock-Kommando (optional).

Tab. 7 – Tag-Klassen nach Auto-ID und EPCglobal

Tag-Klasse	Eigenschaften
CLASS 4	Aktive Tags mit folgenden zusätzlichen Merkmalen gegenüber CLASS 3-Tags: - Tag-to-Tag-Kommunikation - Aktive Kommunikation - Adhoc Netzwerktauglichkeit
CLASS 3	Semi-passive Tags mit folgenden zusätzlichen Merkmalen gegenüber CLASS 2-Tags: - Integrierte Energieversorgung (z.B. Batterie) - Integrated sensing circuitry (Sensoren)
CLASS 2	Passive Tags mit folgenden zusätzlichen Eigenschaften gegenüber CLASS 1-Tags: - Erweiterte Tag-ID - Erweiterter Benutzerspeicher - Authentifizierte Zugriffskontrolle
CLASS 1 GENERATION 2	**Definiert die EPCglobal Basisklasse und ein UHF-Protokoll [epc-gen2]; Ein HF-Protokoll ist in Entwicklung; Passive, mehrfach beschreibbare Tags mit folgenden Merkmalen:** **- EPC** **- Tag-ID** **- Pseudo-Zufallszahlengenerator** **- Kill-Funktion mit optionalem 32-Bit Kill-Passwort** **- Optionale 32-Bit Passwort-geschützte Zugangskontrolle** **- Optionaler Speicher für benutzerspezifische Daten**
CLASS 1	Spezifiziert von Auto-ID; Passive, einmal beschreibbare Tags, HF- und UHF-Protokoll
CLASS 0	Spezifiziert von Auto-ID; Passive, nur lesbare Tags; UHF-Protokoll (die Programmierung erfolgt beim Chip-Hersteller)

Kill-Kommando

Das Tag kann mit dem Kill-Kommando dauerhaft deaktiviert werden, wonach es auf kein Lesersignal mehr reagieren darf. Das Kommando selbst kann durch ein tag-spezifisches 32-Bit Passwort geschützt werden, welches mit übergeben werden muss. Das Sicherheitsziel ist die Privatsphäre des Kunden nach dem Kauf eines getaggten Produktes (siehe Tracking und Datenschutz in 3.1.2). Der Leser sendet dazu zwei Kill-Kommandos nacheinander; das erste enthält die 16 höherwertigen Bits des Kill-Passworts verknüpft durch XOR mit einer 16-stelligen Zufallszahl, die der Leser zuvor mit Hilfe des Req_RN-Kommandos vom Tag angefordert hat; das zweite Kill-Kommando enthält die 16 niederwertigen Bits, die auf gleicher Weise mit einer anderen Zufallszahl verdeckt sind.

Passwort-geschützter Lese- und Schreibzugriff

Mit einem weiteren 32-Bit Passwort lassen sich zugriffsgeschützte Speicherbereiche (Benutzerspeicher) vor unberechtigtem Auslesen oder Schreiben schützen. Die Zugriffskommandos Read, Write, BlockWrite und BlockErase werden bei zugriffsgeschützten (locked) Speicherbereichen nur im Secured-Zustand ausgeführt, ebenso das Lock-Kommando. Ein Tag kann ein Access-Passwort implementieren. In diesem Fall kann es erst nach erfolgreichem Access-Kommando in den Secured-Zustand übergehen. Wie beim Kill-Kommando sind dazu mehrere Schritte erforderlich: Der Leser fordert mit Req_RN eine Zufallszahl vom Tag an und schickt ein Access-Kommando mit den 16 höherwertigen Bits des Access-Passwortes verknüpft durch XOR mit dieser Zufallszahl. Das Tag antwortet mit dem Handle und dem CRC. Der Leser fordert eine weitere Zufallszahl vom Tag an und sendet in einem zweiten Access-Kommando, die niederwertigen 16 Bits des Access-Passwortes XOR verknüpft mit der zweiten Zufallszahl.

Lock-Kommando

Mit dem Lock-Kommando können Passwörter und individuelle Speicherbereiche gesperrt oder freigegeben werden. EPC, Tag-ID und Benutzerdaten sind im Locked-Zustand schreibgeschützt, Passwörter zusätzlich auch lesegeschützt. Jeder Speicherbereich kann auch permanent gelockt werden, so dass z.B. Tag-ID bzw. EPC nach ihrem Eintrag vor Änderungen durch einen nicht-autorisierten Leser geschützt sind.

Definierte Tag-Zustände

Das Tag befindet sich zu jedem Zeitpunkt in einem der Zustände Ready, Arbitrate, Reply, Acknowledge, Open, Secured oder Killed, in denen jeweils unterschiedliche Kommandos und daraus resultierende Aktionen erlaubt sind. Beispielsweise versetzen Zugriffkommandos mit korrektem Access-Passwort das Tag vom Open in den Secured-Status, das Kill-Kommando von Secured in den Killed-Status.

Geschützte Speicherbereiche

Für EPC-Tags sind vier Speicherbereiche definiert, die sich unabhängig voneinander schützen lassen: Reserved Memory, EPC Memory, TID Memory und User Memory. Das Reserved Memory ist für das 32-bit-lange Kill- und ein ebenso langes Access-Passwort vorgesehen, die bei den entsprechenden Kommandos vom Leser angegeben werden müssen. Wenn ein Tag kein Kill-Passwort implementiert, soll es sich so verhalten, als wenn das Passwort den Wert 0 hat und dauerhaft lese- und schreibgeschützt ist. Der korrespondierende Bereich im Reserved Memory muss nicht existieren. Entsprechendes gilt für das Access-Passwort. Wenn das Kill-Passwort 0 ist, soll das Tag keine Kill-Operation ausführen.
Das EPC Memory soll einen 16-bit-langen Cyclic-Redundancy-Check (CRC-16), Protocol Control (PC) Bits und den EPC enthalten. Das Tag Identification Memory soll einen 8-bit-langen ISO/IEC 15963 Allocation-Class-Identifier (z.B:11100010 für EPCglobal) enthalten und weitere Information, die den Leser über die zulässigen Benutzerkommandos und die optionale Eigenschaften des Tag unterrichtet. Tags können auch Tag- und Anbieter-spezifische Daten (z.B. eine Tag-Seriennummer) im TID Memory enthalten. Das User Memory kann für anwendungsspezifische Daten genutzt werden.

Geschützte Datenübertragung

Die Passwörter im Reserved Memory und alle Daten, die in das Tag geschrieben werden, sind bei der Übertragung vom Leser zum Tag durch die XOR-Verknüpfung einer Zufallszahl geschützt. Dieser Schutz entspräche einer idealen Verschlüsselung, wenn die verwendete Zahl eine wirkliche Zufallszahl ist, wenn sie geheim und niemals ein zweites Mal verwendet wird (siehe One-Time-Codes in 3.2.4). Allerdings treffen die Bedingungen nicht auf die EPC-Tags zu, welche meist nur Pseudo-Zufallszahlen generieren und diese im Klartext an den Leser übertragen. Ein Angreifer, der die Kommunikation in beide Richtungen mitzuhören imstande ist, kann die Klartextdaten direkt aus der Zufallszahl und der XOR-geschützten Übertragung berechnen. Ein gewisser Schutz ist aber dadurch gewährleistet, dass die Datenübertragung vom Tag zum Leser viel schwerer abhörbar ist als die Übertragung vom Leser zum Tag (siehe 2.1.2).

Zufällige Adressierung

Ein zusätzlicher Schutz liegt darin begründet, dass Kennungen wie der EPC oder die Tag-ID nicht zur Adressierung von Tags verwendet werden. Sobald das Tag vom Leser identifiziert

und zum Lesen vereinzelt wurde, sendet es eine 16-Bit Zufallszahl (Handle), die der Leser für die weitere Kommunikation zur Adressierung des Tags verwendet. Da der EPC aber zum Aufbau der Kommunikation einmal ungeschützt übertragen wird, sind Angriffe denkbar, welche die EPC-Information über den Hersteller, das Produkt und die eindeutige Kennung des getaggten Objekts z.B. zum Klonen von Tags für Produktfälschungen nutzen (siehe 6.2.1 im Szenario Fälschungssicherheit).

3.2.3 Authentisierungsverfahren

Einen Überblick zum Stand der Forschung geben beispielsweise [juels05, lehtonen06a]. Neueste Forschungsartikel finden sich unter [avoine07]. In [ecrypt06] werden aktuelle kryptographische Algorithmen unter dem Aspekt der Sicherheit diskutiert. Neue Authentisierungsverfahren werden auch für kontaktlose elektronische Ausweisdokumente entwickelt, z.B. die Protokolle Password Authenticated Connection Establishment (PACE) und Extended Access Control (EAC), siehe [bsi06]. Solche Verfahren setzen allerdings kryptographiefähige Mikroprozessorchips voraus (siehe 3.2.8).

Passwort-basierte Verfahren

Passwörter können nicht nur zum Zugriffsschutz auf Tags, sondern auch zur direkten Authentisierung von Tags verwendet werden. Eine Echtheitsprüfung mittels statischer Passwörter ist allerdings nur eine schwache Authentisierung, da die Passwörter in irgendeiner Weise während der Authentisierungsprozedur übertragen werden müssen und folglich die Gefahr des Abhörens besteht. Auch kann aufgrund der meist geringen Passwortlängen ein Angreifer durch Ausprobieren aller möglichen Werte meist schneller um Ziel kommen als das mit kryptographischen Schlüsseln möglich wäre.
In [juels04] wird ein Verfahren vorgeschlagen, in dem das Kill-Passwort der EPC-Tags zur Tag-Authentisierung herangezogen wird. Hintergrund bildet die Vorschrift, dass das Tag die Kill-Prozedur mit einer Fehlermeldung abbricht, wenn das Passwort richtig ist, aber die aufgenommene Leistung nicht ausreicht, um das Tag zu deaktivieren. Bei einem falschen Passwort gibt das Tag dagegen keine Antwort. So kann die Fehlermeldung vom RFID-Leser derart interpretiert werden, dass das Passwort richtig und das Tag echt ist. Die Funktion muss allerdings so implementiert sein, dass das Tag die aufgenommene Leistung immer als unzureichend deklariert, damit eine ungewollte Deaktivierung unterbleibt.

Challenge-Response-Verfahren

Challenge-Response beschreibt eine Authentisierungstechnik, in der eine Seite eine zufällige (und jedes Mal andere) Nachricht an die andere Seite sendet und diese dazu auffordert, die Nachricht nach einer ausschließlich beiden Seiten bekannten Vorschrift (z.B. Chiffrierung der Nachricht mit einem bestimmten geheimen Schlüssel) zu beantworten. Diese Authentisierung wird als stark bezeichnet, da das Geheimnis während der Prozedur nicht übertragen wird und damit nicht abgehört werden kann. Die Technik lässt sich in verschiedene Verfahren integrieren [harlacher07, finkenzeller06], die grob in drei Klassen eingeteilt werden können:

1. Bei Verfahren zur Authentisierung des Tags sendet das Lesegerät eine Zufallszahl an das Tag. Dieser verschlüsselt die Zufallszahl mit einem Schlüssel S und sendet das Er-

gebnis zurück an das Lesegerät. Da der Schlüssel S ein gemeinsames Geheimnis zwischen Tag und Lesegerät darstellt, kann das Lesegerät die Richtigkeit des Ergebnisses und damit die Identität des Tags überprüfen. Voraussetzung ist, dass das Tag eine entsprechende kryptographische Funktion ausführen kann.

2. Verfahren zur Authentisierung des Lesegerätes funktionieren genau umgekehrt wie das oben erklärte Verfahren. Allerdings ist es hier notwendig, dass das Tag neben der Ausführung einer kryptographischen Funktion auch dazu in der Lage ist, Zufallszahlen zu generieren. Da die Rechenkapazität auf dem Lesegerät im Gegensatz zu der Rechenkapazität auf dem Tag kein Problem darstellt, bietet es sich hier an, Verfahren zur gegenseitigen Authentisierung zu verwenden.

3. Verfahren zur gegenseitigen Authentisierung werden u.a. in ISO 9798 definiert. Ein dort genanntes Verfahren ist das Tree-Pass Mutual Authentication Protocol, das in Abb. 11 dargestellt wird. Die aufgeführten Berechnungsschritte stellen einen erheblichen Aufwand dar, den der RFID-Leser und das Tag leisten müssen.

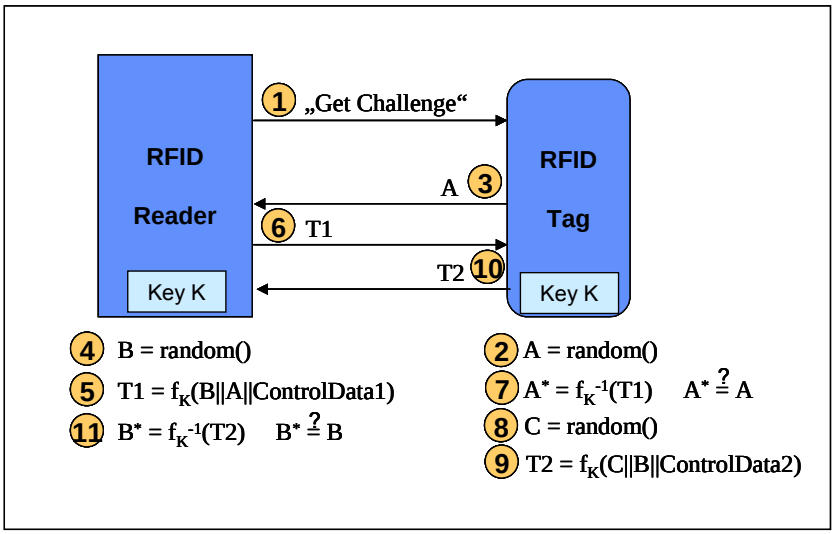


Abb. 11 – Challenge-Response-Verfahren (gegenseitige Authentisierung)

Die Sicherheit beruht auf der Geheimhaltung des kryptographischen Schlüssels. Meist werden symmetrische Verschlüsselungsverfahren verwendet, die effizienter sind als asymmetrische Verfahren. Nachteil der symmetrischen Verfahren ist das komplexe Schlüsselmanagement, d.h. die Verteilung des Schlüssels in alle betroffenen Tags und Backend-Systeme. Wenn alle Tags und Leser den gleichen Schlüssel verwenden, sind alle Komponenten kompromittiert, wenn der Schlüssel einmal bekannt wird. Daher ist gerade in offenen Systemen die Nutzung tag-individueller Schlüssel wichtig. Diese können aus einem Master-Key und einer individuellen Tag-Kennung abgeleitet und im Tag gespeichert werden. Der Master-Key wird nur im Leser oder im Backend hinterlegt, wo er besser geschützt werden kann. Während der Authentisierung wird jeweils der individuellen Tag-Schlüssel berechnet, dessen Kompromittierung nicht das gesamte System unsicher macht. Andere Verfahren verwenden asymmetrische Schlüssel, um in der Authentisierungsprozedur symmetrische Sitzungsschlüssel zu vereinbaren und diese für die weitere Kommunikation zu nutzen.

Asymmetrische Verfahren sind sehr zeit- und rechenintensiv und setzen zudem eine Public Key Infrastructure (PKI) zur Verteilung der öffentlichen Schlüssel voraus.

Die Sicherheit kann erhöht werden, indem kryptographische Operationen von den vielen exponierten RFID-Lesern in die Middleware oder ins Backend-System verlegt werden. Ein Lösungsvorschlag, sieht die Speicherung eines symmetrischen Authentisierungsschlüssels sowohl im Tag als auch in einer Datenbank vor [staake05], siehe Abb. 12. Nachdem das Tag seine Kennung gesendet hat, erzeugt ein kryptographischer Service (integriert in die Middleware bzw. den EPCIS) eine Zufallszahl, welche an das Tag gesendet wird. Das Tag verschlüsselt die Zufallszahl mit dem geheimen Authentisierungsschlüssel. Die kryptographische Einheit empfängt diese Antwort, erfragt von einer Datenbank mit Angabe der Kennung den entsprechenden Authentisierungsschlüssel, und verifiziert damit die Authentisierungsdaten, die nur das Tag im Besitz des geheimen Schlüssel erzeugt haben konnte. Der RFID-Leser reicht die Daten in beide Richtungen weiter, wobei eine Datenmanipulation durch den Leser auf Seiten des Tags bzw. der Middleware auffallen würde.

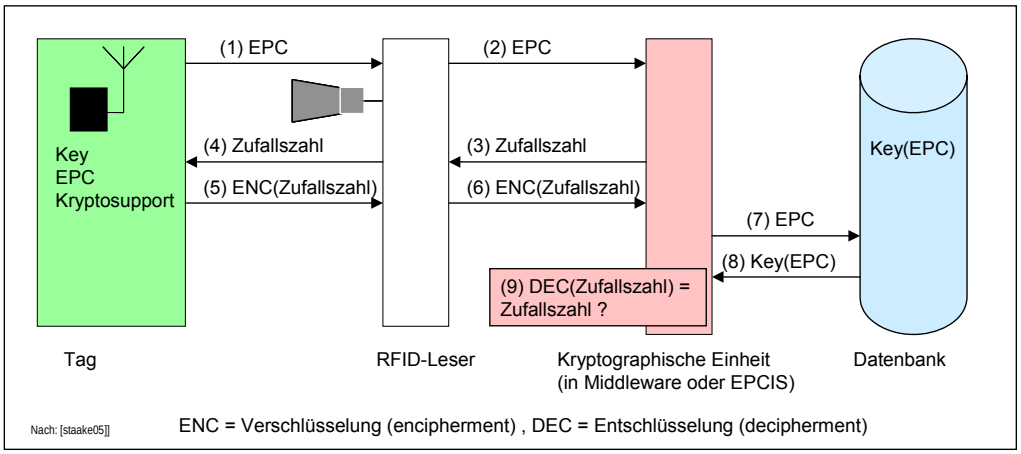


Abb. 12 – Sichere Authentisierung mit kryptographischem Schlüssel auf dem Tag

Bailey und Juels beschreiben in [bailey06], wie in EPC-konformen RFID-Systemen ein solches Challenge-Response-Verfahren durch die erweiterte Nutzung der EPC-Befehle und des Benutzerspeichers gestaltet werden könnte. Sie empfehlen das folgende Verfahren als Grundlage für einen zukünftigen EPC Class2-Standard. Der RFID-Leser schreibt eine Challenge (z.B. eine 16-Bit Zufallszahl) in den Benutzerspeicher des Tags. Die interne Logik des Tags greift intern auf diesen Speicher zu, verschlüsselt die Zufallszahl mit einem symmetrischen Schlüssel, z.B. in einem AES-Verfahren nach [feldhofer04, feldhofer04a], und schreibt die Antwort ENC(Zufallszahl) wiederum in den Speicher. Diese Antwort wird dann zusammen mit dem EPC ausgelesen. Der Leser kann mit dem entsprechenden Schlüssel die Challenge entschlüsseln und damit die Authentizität des Tags verifizieren. Die allgemeinen EPC-Befehle Read und BlockWrite werden auf höherer Ebene zur Implementierung des Sicherheitsverfahrens verwendet. Für einen flexibleren Einsatz verschiedener Algorithmen wird zudem die Einführung von vereinfachten [iso7816-4]-Befehlen und Sicherheitsfeatures für die zukünftigen Class 2-Tags empfohlen.

Wichtig ist die Schaffung standardisierter RFID-Produkt-Authentisierungsprotokolle bzw. eines standardisierten Prozesses für den Low-Cost-Bereich. In der Literatur finden sich viele weitere Authentisierungsverfahren, von denen sich einige parallel etablieren könnten. Dann wäre ein Prozess zur Identifizierung des verwendeten Authentisierungsprotokolls gefragt. Dieser könnte aus den folgenden Schritten bestehen [lehtonen06]: Identifizieren des Produktes anhand des EPC, die Ermittlung der Netzwerkadresse des autorisierten Servers, der Aufbau einer sicheren Verbindung zum autorisierten Server und die Ermittlung des anzuwendenden Protokolls zur Produktauthentisierung. Schließlich würde das ausgewählte Verfahren z.B. im Backend-Server durchgeführt und das Ergebnis an den RFID-Leser kommuniziert.

Verfahren der Lightweight-Cryptography

Ziel der Lightweight-Cryptography ist die Entwicklung effizienter kryptographische Protokolle für Umgebungen mit sehr begrenzten Ressourcen, wie sie insbesondere in Low-Cost Tags vorliegen. Viele Protokolle verwenden ausschließlich Bit-Operationen (XOR) auf Schlüssel und Pseudo-Zufallszahlen. Abb. 13 zeigt ein solches Protokoll, das speziell für EPC-Tags entwickelt wurde [yu06].

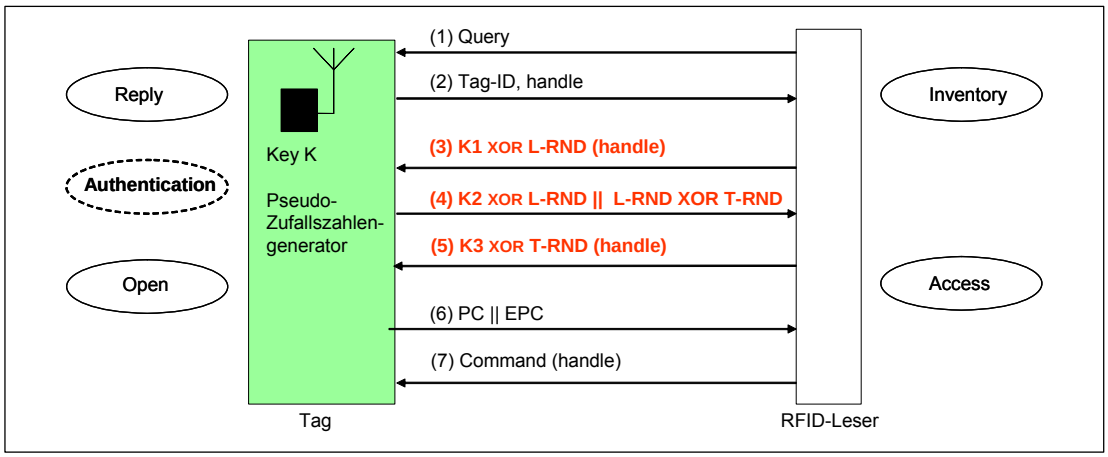


Abb. 13 – Beispiel eines Lightweigth-Cryptography-Protokolls

Hier wird derselbe Schlüssel bestehend aus den Teilschlüsseln K1, K2 und K3 im Tag und im Backend benötigt. Das Lesegerät ruft mit der Tag-ID den Schlüssel vom Backend-Server ab. Anstelle des EPC-spezifizierten Zustands "Acknowledge" wurde ein neuer Zustand "Authentication" eingeführt, für den im Falle einer Integration ins EPC-Protokoll nur wenige Mikrosekunden zur Verfügung stehen. Die Teilschlüssel werden mit Zufallszahlen beider Seiten XOR-verknüpft, so dass von außen weder Schlüssel noch Zufallszahlen erkannt werden können. In Schritt 4 kann sich auf diese Weise das Tag gegenüber dem Leser, in Schritt 5 der Leser gegenüber dem Tag authentisieren. Die verwendeten Zufallszahlen (RNDs) bilden den nächsten Schlüssel für den Fall einer erneuten Authentisierung.
Dieses Beispiel macht deutlich, dass außerhalb der beschränkten Komponente die Protokolle komplex sein können und ebenfalls Zugriffe auf Datenbanken und Server benötigen. Ein anderes Protokoll verwendet symmetrische Sitzungsschlüssel im Tag und Lesegerät. Damit diese auf beiden Seiten denselben Wert besitzen vorliegen, soll im Tag und im Server der gleiche Pseudo-Zufallszahlenalgorithmus zum Einsatz kommen, der auf beiden Seiten mit demselben Wert initialisiert und anschließend synchron gehalten werden muss [duc06]. Der-

artige Protokolle können für die Prüfung vieler Tags einen hohen Rechenaufwand bedeuten. Die Sicherheit der Protokolle ist schwierig nachzuweisen und ist in vielen Fällen widerlegt worden. Die Lightweight-Cryptography ist dennoch ein viel versprechendes Forschungsgebiet.

Verfahren der Minimalist-Cryptography

Die so genannte Minimalist-Cryptography schlägt ähnliche Verfahren für Low-Cost Tags vor wie die Lightweight-Cryptography, verlegt aber weitere Operationen ins Lesegerät oder Backend, so dass das Tag ganz ohne Kryptographie auskommen kann. Eine Übersicht der aktuellen Diskussion bietet [ranasinghe06]. Ein Beispiel ist die Nutzung von gleichen Pseudonymlisten auf Tag und Server, deren Werte bei nachfolgenden Authentisierungsprozeduren rotierend zum Einsatz kommen. Der minimalistische Ansatz geht davon aus, dass ein Angreifer nur wenige Male die Kommunikation zwischen bestimmten Tags und Lesegeräten abhören kann. Protokolle werden z.B. dadurch sicherer, dass das Tag auf bestimmte Challenges mit bestimmten (auf beiden Seiten hinterlegten) Authentisierungsschlüsseln antwortet. Ein Sequenzzähler kann den gültigen Satz von Zufallszahlen für die nächste Abfrage festlegen. Die meisten Verfahren setzen eine aufwändige Datensuche, Aktualisierung oder Synchronisation voraus und führen zu hohen Kommunikationskosten.
Weitere Verfahren versuchen, diese Nachteile zu umgehen. Ein Beispiel sind so genannte Noisy Tags, die ähnlich den Blocker-Tags Störsignale aussenden, aber vom Betreiber des RFID-Systems eingesetzt werden. Dadurch wird verhindert, dass ein Angreifer die eigentliche Kommunikation zwischen Tag und Leser überhaupt identifizieren kann. So lassen sich z.B. einfachere Authentisierungsprotokolle wie ein direkter Schlüsselaustausch an der Luftschnittstelle gegen Abhören schützen.

Physical Uncloneable Functions

Die Erforschung Physical Unclonable Functions (PUFs) ist ein weiteres Forschungsgebiet, welche zukünftig effiziente und kopiergeschützte Sicherheitsfunktionen für Low-Cost Tags bereitstellen könnte. Ein Beispiel dafür ist eine Schaltung mit Verzögerungspfaden, welche durch unkontrollierbare Fabrikationsunterschiede bei der Chip-Herstellung entsteht. Eine solche Schaltung gibt für den betreffenden Chip charakteristische Antworten auf jede eingegebene Bit-Sequenz und wirkt daher wie ein symmetrischer Schlüssel [ranasinghe06a]. Eine 64-stufige PUF kann mit üblicher CMOS-Technologie in weniger als 1000 Gatter implementiert werden und ist damit hardware-effizienter als die meisten kryptographischen Algorithmen. Zudem lassen sich die entscheidenden Funktionsgrößen im Gegensatz zu kryptographischen Schlüsseln weder mit physikalischen Attacken auslesen noch nachbauen. Ein Angreifer kann keine erschöpfende Suche nach gültigen Input-Output-Paaren durchführen. Zur Nutzung der Funktion muss auf dem Server für jedes Tag eine begrenzte Auswahl von Challenge-Response-Paaren gespeichert werden, die möglichst geheim gehalten werden sollte. Gibt das Tag auf einen bestimmten Input die erwartete Antwort, so kann es als authentisiert gelten.
Es können vermutlich viele weitere unklonbare Funktionen gefunden werden, da auf Molekülebene unregelmäßige Materialeigenschaften eher die Regel als die Ausnahme sind. So könnten für den Einsatz von kryptographischen Schlüsseln in unsicheren Hardwarekomponenten Alternativen geschaffen werden. Allerdings müssen die physikalischen Eigenschaften und Toleranzwerte solcher Funktionen weiter verbessert werden, da Temperaturunterschie-

de und Spannungsänderungen die Ergebnisse teilweise unzuverlässig werden lassen. Auch ist eine Definition geeigneter kryptographischer Protokolle notwendig. In [tuyls06] ist ein solches Protokoll beschrieben. Darin ruft der Produkthersteller bei der Produktion mit einigen Zufallszahlen (Challenges) individuelle Antworten der PUF ab, verknüpft diese mit weiteren individuellen Tag-Daten (z.B. EPC) und signiert diese so genannten Fingerprints mit einem geheimen Schlüssel. Die verwendeten Zufallszahlen werden zusammen mit den Fingerprints und den Signaturen auf die Verpackung gedruckt und/oder in einer Datenbank gespeichert. Jedes autorisierte Lesegerät besitzt den öffentlichen Signaturschlüssel und kann damit prüfen, ob die gedruckten Daten authentisch sind. Zur Produktprüfung liest der Leser die Zufallszahlen, ruft mit einer von ihnen die PUF des Tags auf und generiert daraus den Fingerprint. Stimmt der Fingerprint mit den gedruckten Daten überein und ist die Signatur authentisch, so kann das gesamte Produkt als authentisch gelten.

Physical One-Way Functions

Als eine weitere Alternative zur Speicherung kryptographischen Schlüssel in unsicherer Hardware könnte der Einsatz von Physical One-Way Functions (POWFs) auf Tags und Produktpackungen dienen [ravikanth01]. Dabei werden statt numerischer und algorithmischer Einwegsfunktionen physikalische Systeme verwendet, welche kostengünstig und nicht kopierbar sind und auf bestimmte physikalische Eingaben durch ihren charakteristischen physikalischen Zustand deterministische nicht invertierbare Ergebnisse analog zu den herkömmlichen kryptographischen Funktionen (z.B. Hash-Funktionen, Generierung von Zufallszahlen) liefern können. Eine entsprechende manipulationssichere Lösung sieht einen durchsichtigen optischen Datenträger mit eingeschlossener einmaliger und nicht reproduzierbarer 3D-Mikrostruktur vor, welche mittels Laserlicht und Messung des Interferenzmusters in eine Bitsequenz übersetzt werden kann. Derartige Verfahren werden als zukünftige Maßnahmen gegen Kloning und Produktfälschungen empfohlen [ranasinghe06a], wobei der für jedes Produkt einmalige POWF-Wert gemessen und mit dem in einer Datenbank gespeicherten oder auf die Verpackung gedruckten Wert verglichen werden muss. Weitere Untersuchungen zur Anwendbarkeit sind nötig. Ein mögliches Forschungsthema wäre die Schaffung geeigneter Verfahren, welche POWFs zusammen mit entsprechenden Sensoren in RFID-Systeme integrieren. Mittelfristig sind manuelle stichprobenartige Tests für Produktprüfungen denkbar.

Zero-Knowledge-Protokolle

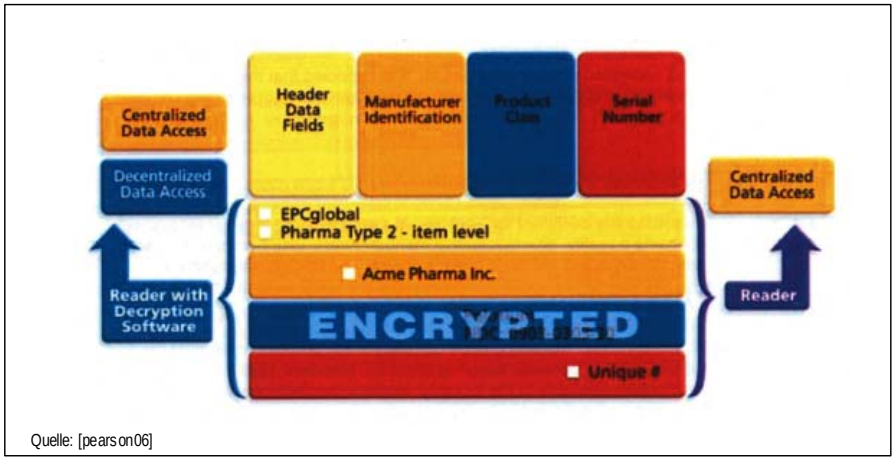
In einem Zero-Knowledge-Beweis oder Zero-Knowledge-Protokoll [goldreich86] kommunizieren zwei Parteien (der Beweiser und der Verifizierer) miteinander. Zero-Knowledge-Protokolle sind eine Erweiterung von interaktiven Beweissystemen. Der Beweiser überzeugt dabei in den Verifizierer mit einer gewissen Wahrscheinlichkeit davon, dass er ein Geheimnis kennt, ohne dabei Informationen über das Geheimnis selbst bekannt zu geben. Zero-Knowledge-Protokolle dienen der Authentisierung und können mithin als Alternative zu Challenge-Response-Protokollen betrachtet werden. Ein Beispiel für ein Zero-Knowledge-Protokoll ist das Fiat-Shamir-Protokoll [Fiat87]. Auch im Kontext von RFID existieren bereits erste Ansätze für den Einsatz von Zero-Knowledge-Protokollen zur Authentisierung wie z.B. ein Prototyp-Tag für EPC Class1 Gen2-Tags [khan05].

3.2.4 Verschlüsselungsverfahren

Für die Verschlüsselung kommen asymmetrische und symmetrische Verfahren in Betracht. In RFID-Systemen werden meist die symmetrischen DES oder 3DES-Algorithmen verwendet, weil sie relativ leicht zu implementieren und effizient in der Ausführung sind. Beide Kommunikationspartner müssen über den gemeinsamen, geheimen Schlüssel verfügen, um miteinander kommunizieren zu können. Das Hauptproblem der symmetrischen Verfahren besteht in dem hierfür notwendigen aufwändigen Schlüsselmanagement. Asymmetrische Verfahren wie RSA und Elliptische-Kurven-Kryptographie (ECC) beruhen darauf, dass jeder Kommunikationspartner über ein Schlüsselpaar bestehend aus einem privaten geheimen Schlüssel und einem öffentlichen allgemein zugänglichen Schlüssel verfügt. Nachrichten werden jeweils mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und von diesem mit dem privaten Schlüssel wieder entschlüsselt. Die asymmetrischen Verfahren gelten als sehr sicher, wenn ausreichend hohe Schlüssellängen verwendet werden. Als Nachteil gilt jedoch der höhere Rechenaufwand im Vergleich zu symmetrischen Verfahren.

Statische Verschlüsselung

Sollen kryptographischen Operationen vollständig vom Tag in den Leser oder ins Backend verlegt werden, so können statische Verschlüsselungsverfahren zum Einsatz kommen. Die Daten werden beispielsweise verschlüsselt im Tag gespeichert, ebenso ausgelesen und erst außerhalb des Tags wieder entschlüsselt. Allerdings kann die Kommunikation nicht vollständig verschlüsselt sein, da das Tag die Befehle verstehen muss. Passworte und andere Daten zur Zugriffssteuerung müssen also weiterhin unverschlüsselt übertragen werden, wenn das Tag auf eine dynamische Dechiffrierung der Kommunikationsdaten verzichten soll. Für eine statische Verschlüsselung von EPC-Daten schlägt Texas Instruments in [pearson06] die Schaffung einer industrieweit standardisierten “Tag Data Security Infrastructure” vor, um kompatible zentrale (online) und dezentrale (offline) Sicherheitsmechanismen außerhalb der Tags zu ermöglichen. Ein erweitertes EPC-Nummerierungssystem sieht vor, dass allein die Produktinformation des EPC verschlüsselt bzw. mit einem privaten Schlüssel elektronisch signiert ist (siehe Abb. 14).



Quelle: [pearson06]

Abb. 14 – EPC-Datenstruktur mit verschlüsselter Produktkennung

Die Produktdaten liegen in einer zentralen Datenbank und können mit dem entschlüsselten EPC abgerufen werden. Da der teilverschlüsselte EPC ebenso eindeutig ist, kann dieser auch direkt in anderen Anwendungen (z.B. für den Herkunftsnachweis) genutzt werden. Daher sind sowohl RFID-Leser mit Entschlüsselungssoftware und öffentlichem Schlüssel als auch einfache Leser ohne Kryptographie einsetzbar. Als Verschlüsselungs- und Signatur-Algorithmus wird ECC vorgeschlagen, da die Berechnung Elliptischer Kurven effizienter als RSA ist und die Signatur weniger Speicherplatz braucht. Die verschlüsselte Produktkennung kommt dem Datenschutz entgegen, weil ein Angreifer über die EPC-Daten den Produkttyp nicht unmittelbar bestimmen kann. Sie kann aber nicht eine Authentisierung des Tags ersetzen. Statisch verschlüsselte Daten bleiben weiterhin kopierbar und könnten in geklonten Tags verwendet werden. Gültige verschlüsselte Daten könnten auch von einem Angreifer zwischen verschiedenen gültigen Tags ausgetauscht werden (Swapping-Attacke), wenn keine weiteren Sicherheitsmechanismen vorhanden sind.

Dynamische Verschlüsselung

Eine dynamische Verschlüsselung wird dadurch erreicht, dass die Kommunikation zwischen den kommunizierenden Komponenten direkt mit symmetrischen Sitzungsschlüsseln chiffriert und dechiffriert wird. Die gemeinsamen Schlüssel könnten beispielsweise in einer Authentisierungsprozedur vereinbart werden. Damit die Daten nicht in Replay-Attacken wieder verwendbar sind, sollte zudem eine Prüfsumme mitgeliefert werden, in deren Berechnung eine Art Sequenzzähler eingeflossen ist. So sind die chiffrierten Daten auch bei wiederholt gleichem Klartext immer unterschiedlich. Die Implementierung dynamischer Verfahren ist aufwändig und eigentlich den Mikroprozessorchips vorbehalten (siehe 3.2.8).

One-Time-Codes

Kryptographische Verfahren mit One-Time-Codes (One-Time-Pad, Vernam Cipher) verwenden zufällige Bitsequenzen, welche die gleiche Länge besitzen wie die zu verschlüsselnden Klartexte. Sie gelten als unübertreffbar sicher, solange der Code wirklich zufällig, geheim und nur ein einziges Mal genutzt wird. Da zur Verschlüsselung und Entschlüsselung nur die einfache bit-weise XOR-Operation benötigt wird, wären solche Verfahren ideal für Low-Cost Tags. Schwierigkeiten bereitet jedoch die Notwendigkeit, dass auf beiden Kommunikationsseiten der gleiche Schlüssel vorliegen muss. Zukünftige Lösungen könnte die Quanten-Kryptographie liefern, welche auf subatomare Zustände von Elektronen und Photonen basiert und wahre Zufallszahlen generieren kann. Andere Quellen für Zufallszahlen sind z.B. kosmologische Radiowellen, welche auf beiden Seiten gemessen und mittels Synchronisationsverfahren verwendet werden können oder 2-Faktoren-Authentisierungsverfahren, welche statische Passwörter zusammen mit variablen Größen (z.B. die synchronisierte Uhrzeit) benutzen. [ghosal06] gibt eine Übersicht zum Thema und analysiert die Anwendbarkeit von One-Time-Codes und Zufallszahlen für RFID-Systeme. Ein einfaches Protokoll für Verschlüsselung und Authentisierung sieht 5 Zufallszahlen (Codes) vor, die sowohl im Tag als auch im Backend gespeichert werden, siehe Abb. 15.

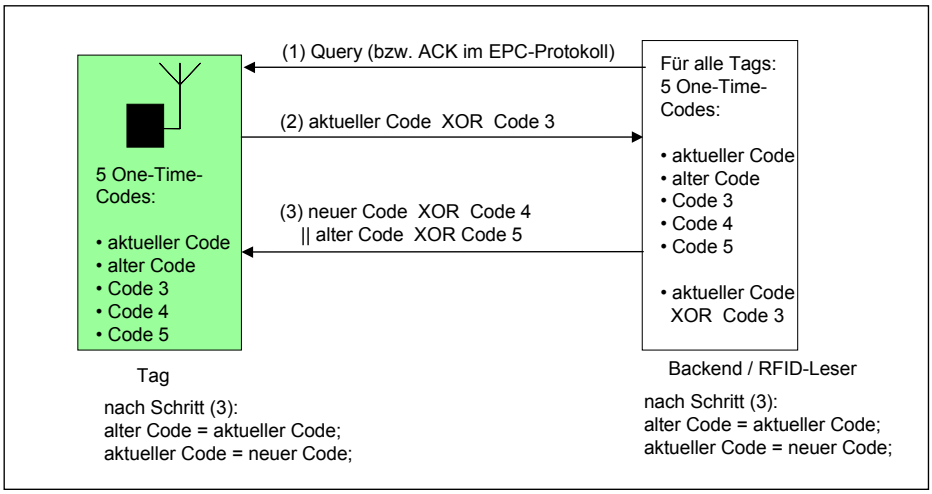


Abb. 15 – Authentisierungsprotokoll mit One-Time-Codes

Die erste Zahl ist der aktuelle One-Time-Code, die zweite repräsentiert den beim letzten Mal verwendeten Code. Die übrigen drei Zahlen werden jeweils zum Verschlüsseln des aktuellen, des neuen bzw. des alten Codes einsetzt, ähnlich wie im Lightweight-Cryptography Protokoll der Abb. 13, so dass die Sequenzen äußerlich nur als wahllose Zufallszahlen erscheinen. Für ein schnelles Auffinden des aktuellen Codes wird für jedes Tag neben den 5 Codes auch der jeweilige verschlüsselte aktuelle Code in der Datenbank gespeichert. In Schritt (2) authentisiert sich das Tag durch den Präsentation des aktuellen Codes. In Schritt (3) authentisiert sich der Leser durch die Präsentation des alten Codes, so dass die im Tag gespeicherten Codes nur durch autorisierte Leser geändert werden. Allerdings bestehen hier ähnlich wie bei vielen anderen Protokollen Sicherheitslücken. Weil z.B. jeder Code (als neuer, aktueller und alter Code) dreimal verwendet wird, kann er nach dem Abhören von drei Authentisierungszyklen berechnet werden.
Die Forschung befasst sich mit der Generierung, Synchronisation zur zeitlich exakten Erfassung von gemeinsam beobachtbaren Ereignissen, möglichen Recovery-Methoden von One-Time-Codes, Ersatz von verbreiteten Stromchiffren durch One-Time-Codes bis hin zur Generierung der Codes in der Quantenkryptographie.

3.2.5 Verfahren zum Integritäts- und Zugriffsschutz

Wenn lediglich die Integrität der auf dem Tag gespeicherten Daten gesichert werden muss, so genügt es, die Daten mit einem Passwort zu schützen oder die Datenbereiche auf dem Tag permanent gegen das Überschreiben zu sperren, wie es auf Low-Cost Tags möglich ist. Da die Kommunikation zwischen Tags und Lesegeräten für Störungen der Datenübertragung anfällig ist, haben sich selbst auf Low-Cost Tags zusätzlich einfache Prüfsummenverfahren (Paritätsprüfung, Längssummenprüfung, CRC etc.) etabliert, welche meist ohne Fehlerkorrektur auskommen. Im Fehlerfall wird einfach die erneute Übertragung der Datenblöcke eingeleitet. Die Verfahren können sich allerdings nicht gegen mutwillige Manipulation der Datenübertragung richten, da ein Angreifer leicht die Prüfsummen manipulierter Daten selbst berechnen und mitliefern kann. Die aufwändigere hash-basierte Berechnung von Prüfsummen bietet aus dem gleichen Grund wenig Schutz gegen Manipulation.

Echten Schutz der Datenübertragung bieten nur starke Integritätsverfahren, d.h. Verfahren, in denen kryptographische Schlüssel zur Prüfsummenberechnung eingesetzt werden. Soll zusätzlich die Herkunft der Daten überprüfbar sein, so können mit einem privaten Schlüssel eines asymmetrischen Verfahrens die Daten signiert werden und die Signatur zusammen mit den Daten übertragen werden. Um den Einsatz teurer leistungsfähiger Tags zu vermeiden, kann die jeweilige Prüfsumme bzw. Signatur außerhalb des Tags erzeugt und mit den zu schützenden Daten im Tag gespeichert werden. In [pearson05] wird ein solches Konzept zum Integritätsschutz mit autorisierten RFID-Lesern beschrieben, mit denen die Teilnehmer von pharmazeutischen Lieferketten ausgestattet werden sollen (siehe Abb. 16).

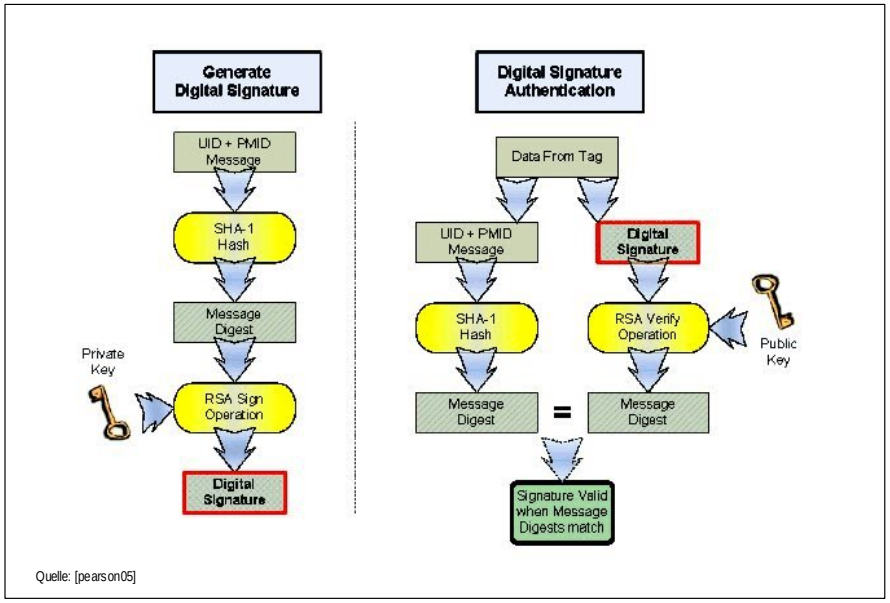


Abb. 16 – Generierung und Prüfung der Tag-Signatur

Die manipulationsgeschützten Leser erhalten über eine PKI öffentliche und private RSA-Schlüssel, mit denen sie RSA-Signaturen erzeugen bzw. verifizieren können. Bestandteile des Konzept sind zwei Kennungen, die vom Tag-Hersteller unveränderbar in den Tag-Speicher geschrieben werden: Die Tag-ID und eine Kennung des Produkt-Herstellers (PMID). Die beiden Kennungen werden vom Leser signiert. Diese Signatur wird zusätzlich in den Tag-Speicher geschrieben. Jeder autorisierte Leser in der Lieferkette kann nun die Daten auslesen und mit dem entsprechenden öffentlichen Schlüssel die Signatur verifizieren. Entgegen der Darstellung im White Paper handelt es sich nicht um eine Authentisierung des Tags, sondern lediglich um eine Prüfung, ob die Tag-Daten authentisch sind und nicht nachträglich verändert wurden. Ein Angreifer könnte die Kennungen einschließlich der Signaturen auslesen und unverändert für gefälschte Tags verwenden, so dass das Verfahren nur wenig mehr Sicherheit bietet als eine Online-Überprüfung der Tag-Kennungen (siehe 6.1.5).

3.2.6 Verfahren zur Pseudonymisierung

Gegen das unberechtigte Auslesen von Tag-Kennungen wurden hash-basierte Verfahren entwickelt, die möglichst wenig Tag-Ressourcen benötigen. Gleichzeitig wird damit Pseudonymität erreicht, indem das Lesegerät die richtige Tag-Kennung präsentieren muss, um Tag-Daten lesen zu können. Unberechtigten Lesergeräten bleibt damit die Identität des Tags ver-

borgen. Weil diese Verfahren große Bedeutung für Low-Cost Tags haben können, seien die wichtigsten von ihnen hier dargestellt. Ein Nachteil der Verfahren ist, dass das RFID-System die Kennungen aller Tags, die in Lesereichweite kommen können, kennen oder aus bereits vorhandenen Daten berechnen muss, um die Tags identifizieren zu können. Das erfordert viele Datenbankzugriffe und begrenzt die Anwendbarkeit der Verfahren auf Systeme mit maximal einigen Tausend Tags.

Hash-Lock-Verfahren

Das Hash-Lock-Verfahren zum Sperren von Low-Cost Tags gegen das unberechtigte Lesen von Daten ist ein einfacher Sicherheitsmechanismus auf Basis bekannter Hash-Funktionen [weis03]. Zur Anwendung des Verfahrens müssen die Tags so leistungsstark ausgelegt sein, dass auf ihnen die Berechnung eines Hash-Wertes durchgeführt werden kann. Kern des Verfahrens ist eine temporäre Meta-ID, die in einem reservierten Bereich des Tags abgelegt wird. Zudem gibt es zwei Zustände, in denen die Tags operieren:
Im Unlocked-State stehen sämtliche Funktionen des Tags für ein beliebiges Erfassungsgerät zur Verfügung. Im Locked-State hingegen antwortet das Tag auf alle Anfragen nur mit seiner Meta-ID und stellt keine sonstigen Funktionen zur Verfügung. Um ein Tag in den Locked-State zu bringen, müssen folgende Operationen durchgeführt werden (Abb. 17):

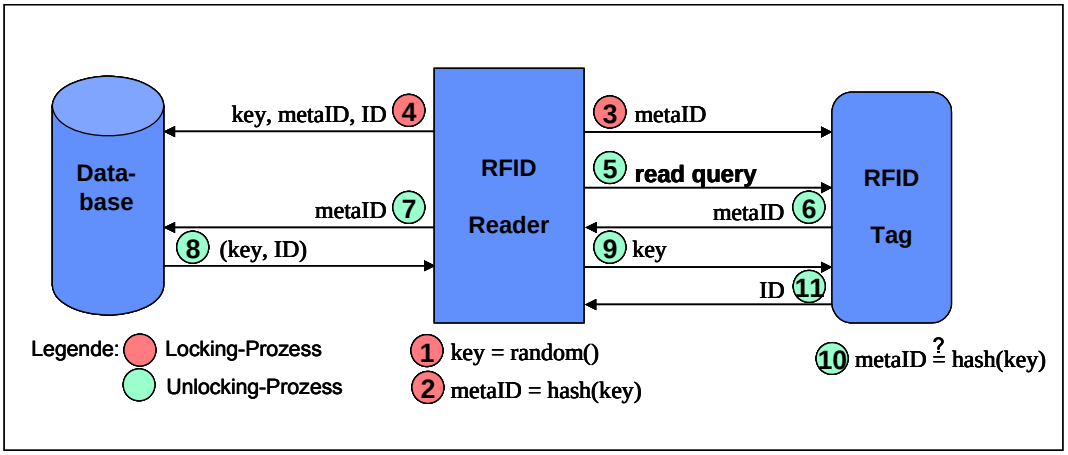


Abb. 17 – Hash-Lock-Verfahren

Das Lesegerät bestimmt eine Zufallszahl als Schlüssel und rechnet deren Hash-Wert aus. Dieser Hash-Wert wird im Folgenden als Meta-ID für das Tag verwendet. Das Lesegerät schreibt die Meta-ID auf das Tag. Dies kann entweder über die Luftschnittstelle geschehen, oder zur Erhöhung der Sicherheit über eine zusätzliche, kontaktbasierte Kommunikationsschnittstelle. Nach dem Empfang der Meta-ID wechselt das Tag automatisch in den Locked-State. Das Lesegerät speichert den Schlüssel (die Zufallszahl) und die Meta-ID (den Hash-Wert der Zufallszahl) in einer sicheren Datenbank im Backend.

In dem nun erreichten Locked-State antwortet das Tag auf alle Anfragen nur mit seiner Meta-ID und bearbeitet keine sonstigen Befehle. Um das Tag wieder mit allen seinen Funktionen nutzen zu können, muss er in den Unlocked-State wechseln. Dazu fragt das Lesegerät zunächst die Meta-ID des Tags ab. In einem zweiten Schritt führt das Lesegerät eine Abfrage der Datenbank im Backend durch, um den zur Meta-ID passenden Schlüssel in Erfah-

rung zu bringen. Das Lesegerät sendet den Schlüssel an das Tag. Das Tag berechnet den Hash-Wert des Schlüssels. Wenn der Hash-Wert der Meta-ID entspricht, wechselt das Tag in den Unlocked-State.

Da es praktisch unmöglich ist, eine Hash-Funktion umzukehren und aus dem Hash-Wert dessen Schlüssel zu berechnen, verhindert das Hash-Lock verfahren, dass unautorisierte Erfassungsgeräte das Tag auslesen können. Allerdings kann umgekehrt nicht verhindert werden, dass ein gelocktes Tag mit seiner Meta-ID geklont wird. Ein gelocktes Tag kann nach seiner Meta-ID gefragt werden, die auf den Klon geschrieben wird. Lediglich das Entdecken eines solchen Angriffes ist möglich, wenn die auf dem geklonten Tag gespeicherten Informationen, z.B. die Seriennummer, nicht denen entsprechen, die das Erfassungsgerät erwartet. Da das originale Tag nur im Unlocked-State Informationen preisgibt, sind diese von einem Angreifer schwierig zu kopieren.

Ein kritischer Punkt dieses Verfahrens ist jedoch, dass Tags im Unlocked-State zur Durchführung eines DoS-Angriffes von einem nicht autorisierten Lesegerät in den Locked-State geschaltet werden und dadurch funktionsunfähig gemacht werden könnten. Das Verbleiben von Tags im Unlocked-State stellt somit ein Sicherheitsrisiko für das RFID-System dar und sollte somit vermieden werden. Tags sollten daher nur in den Unlocked-State gebracht werden, wenn dies z.B. zum Durchführen einer Operation notwendig ist. Direkt nach Abschluss einer Operation sollten Tags wieder in den sicheren Locked-State wechseln. Ein zweiter kritischer Punkt ist, dass der Schlüssel zum Entsperren des Tags im Forward-Link übertragen wird, damit relativ leicht abhörbar ist und in Replay-Attacken verwendet werden könnte. Es ist daher wichtig, dass die Meta-ID gewechselt wird, am besten nach jedem Auslesen durch ein autorisiertes Lesegerät.
Ein weiterer Nachteil des Hash-Lock-Verfahrens ist, dass die Meta-ID des gelockten Tags eine Identifikationsmöglichkeit bietet und dadurch ein Tracking bzw. das Erstellen von Bewegungsprofilen von Konsumenten theoretisch möglich wäre. Hier setzt das Randomized-Hash-Lock-Verfahren an, eine Weiterentwicklung des Hash-Lock-Verfahrens an, die diese Schwachstelle vermeidet.

Randomized Hash-Lock

Um ein mögliches Tracking zu verhindern, wird der Locked-State der Tags modifiziert [harlacher07]. In diesem Zustand ist die Antwort der Tags auf Anfragen zufallsbestimmt, jedoch sind die Tags weiterhin von legitimierten Lesegeräten identifizierbar. Um diese Funktionen realisieren zu können, müssen die Tags über einen Zufallsgenerator verfügen. Diesen zu implementieren kann relativ aufwändig sein. Das Wechseln in den Locked-State geschieht durch einen direkten Befehl (Abb. 18).

Um in den Unlocked-State zu wechseln, sind folgende Schritte notwendig [weis03b]: Das Lesegerät sendet eine Abfrage an das Tag. Das Tag bestimmt daraufhin per Zufallszahlgenerator eine Zufallszahl R. Anschließend berechnet es den Hash-Wert X seiner um R verlängerten Seriennummer. Das Tag sendet R sowie den berechneten Hash-Wert aus Seriennummer und R an das Lesegerät. Das Lesegerät wendet nun eine Brute-Force-Methode an: Es berechnet Hash-Werte von allen bekannten, im Backend gespeicherten Seriennummern verlängert um das vom Tag empfangene R. Die Berechnung kann alternativ auch im

Backend stattfinden. Sobald das Lesegerät eine Übereinstimmung zwischen einem der berechneten Hash-Werte und dem empfangen Hash-Wert feststellt, sendet es die dazu passende Seriennummer an das Tag. Das Tag wechselt in den Unlocked-State, wenn die empfangene ID mit der eigenen ID übereinstimmt.

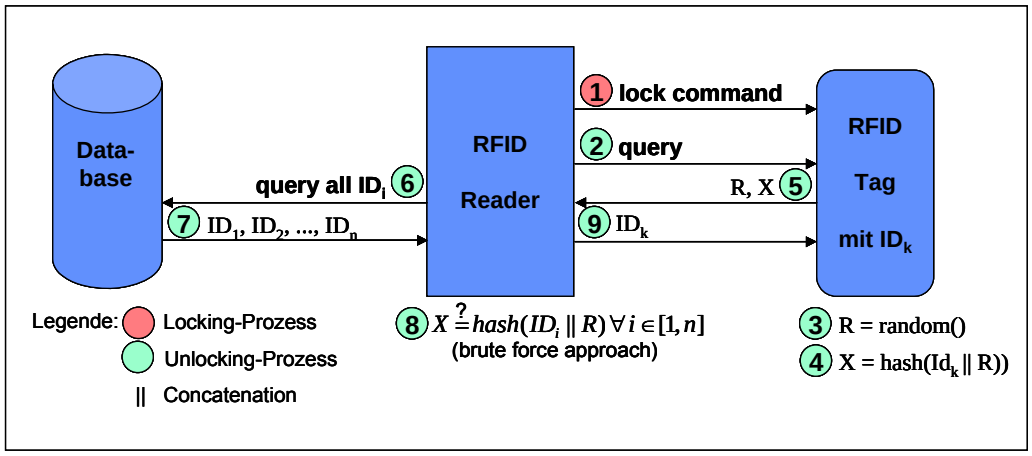


Abb. 18 – Randomisiertes Hash-Lock-Verfahren

Das auf diese Weise verhinderbare Tracking bzw. Erstellen von Bewegungsprofilen ist grundsätzlich eine Bedrohung für die passive Partei, z.B. den Konsumenten, während die aktive Partei, z.B. ein Supermarkt, hiervon nicht direkt betroffen wird. Daher gibt es auch die Überlegung, vor dem Verkauf eines Produktes ein gewöhnliches Hash-Lock-Verfahren einzusetzen und beim Kauf das Tag auf ein Randomized-Hash-Lock-Verfahren umzustellen. Durch die große Anzahl an durchzuführenden Hash-Funktionen eignet sich das Randomized-Hash-Lock-Verfahren allerdings eher für RFID-Systeme mit geringer Tagzahl [harlacher07].
Ein weiterer Schwachpunkt des Randomized-Hash-Lock-Verfahrens ist, dass die originale Seriennummer über die unsichere Luftschnittstelle übertragen wird (letzter Schritt zum Wechsel in den Unlocked-State). Diese Seriennummer genügt, um das Tag in den Unlocked-Mode zu versetzen. Hört ein Angreifer also diese Seriennummer ab, kann er in einer späterer Replay-Attacke mit dieser Seriennummer das Tag ohne Berechtigung in den Unlocked-Mode versetzen und dadurch Auslesen. Das Abhören wird zudem dadurch erleichtert, dass die Übertragung der ID im “lauteren” Forward-Link geschieht. Das Modified-Randomized-Hash-Lock-Verfahren vermeidet das Übertragen der Seriennummer.

Modifizierter radomisierter Hash-Lock

Im Modified-Randomized-Hash-Lock-Verfahren wird statt der Seriennummer eine temporäre Meta-ID an das Tag gesendet [harlacher07]. Abb. 19 zeigt den Ablauf des Verfahrens. Wenn das Lesegerät das Tag in den Locked-State versetzt, sendet es wie beim normalen Hash-Lock den Hash-Wert einer Zufallszahl R an das Tag, welches diesen Hash-Wert als Meta-ID verwendet. Das Lesegerät speichert die Zufallszahl R zusammen mit dessen Hash-Wert und der Tag-Seriennummer im Backend.

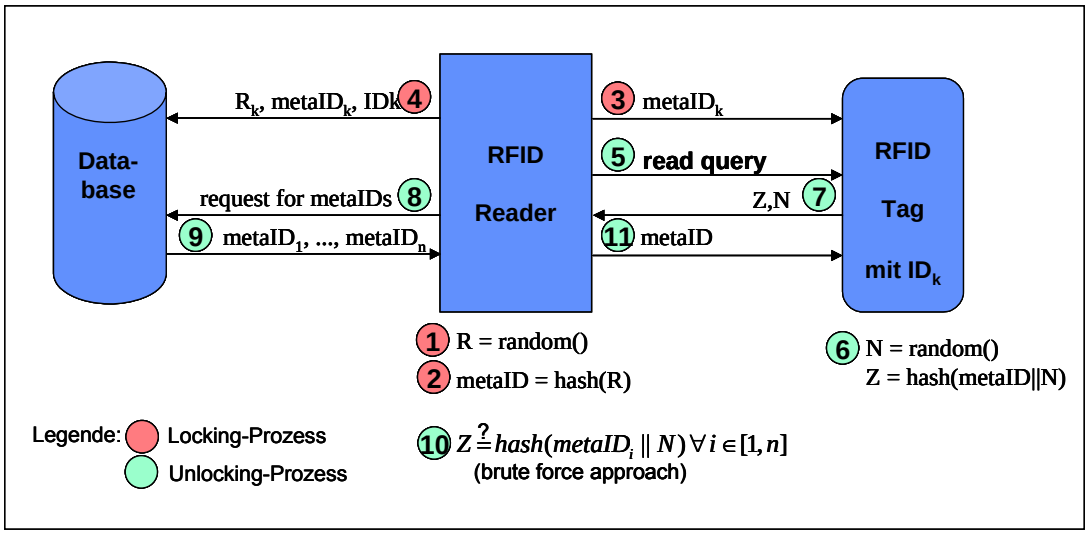


Abb. 19 – Modifiziertes randomisiertes Hash-Lock-Verfahren

Wird das Tag im Locked-State von einem Lesegerät angesprochen, sendet es den Hash-Wert der Meta-ID verlängert um eine eigene Zufallszahl N sowie die Zufallszahl N selbst. Das Lesegerät berechnet nun die Hash-Werte für alle im Backend gespeicherten Meta-IDs verlängert um die Zufallszahl N. Findet das Lesegerät eine Übereinstimmung, sendet es die passende Meta-ID an das Tag. Das Tag geht daraufhin in den Unlocked-State über. Vorteil des Verfahrens ist, dass es das erwähnte Abhörrisiko vermeidet. Auch wenn im letzten Übertragungsschritt die Meta-ID abgehört wird gibt es kein Sicherheitsrisiko, da sich deren Wert beim nächsten Übergang in den Locked-Mode ändert.

Hash-Based ID Variation

Henrici und Müller haben in [henrici04] ein umfassendes Verfahren zur gegenseitigen Authentisierung, Verschlüsselung der Kommunikation und Sicherstellung der Location Privacy vorgestellt. Voraussetzung für das Verfahren ist, dass die Tags in der Lage sind, Hash-Funktionen zu berechnen. Außerdem müssen die Tags eine Reihe von Werten abspeichern können. Vorteil des Verfahrens ist, dass die Tag-Kennung bei jedem Lesevorgang geändert wird. Zudem ist Protokoll unempfindlich gegenüber dem Verlust von Nachrichten aufgrund von Kommunikationsstörungen oder Angriffen.

3.2.7 Verfahren zum Verhindern des Auslesens

Mechanismen zur Verhinderung des Auslesens werden insbesondere dann eingesetzt, wenn sich das getaggte Produkt nach Verkauf an die Endkunden am Ende der offenen Lieferkette befindet und die automatische Identifikation nicht mehr gefragt ist. Dann kann eine Deaktivierung des Tags aus Gründen des Datenschutzes geboten sein. Gegen ein unberechtigtes Auslesen innerhalb geschlossener Kreisläufe oder innerhalb der Lieferkette sind dagegen Verfahren der Pseudonymisierung und des Zugriffsschutzes gebräuchlich. Es wurden Alternativen zur dauerhaften Deaktivierung mittels Kill-Befehl entwickelt, welche der Verbrauchers selbst kontrollieren kann, z.B. eine Disable/Enable-Funktionalität [spiekermann04], perforierte Tags und Blocker-Tags (siehe unten). Eine Übersicht der kryptographischen Verfahren geben [juels05-2, juels06, calmels06, ohkubo05]. Zum gezielten Schutz gegen ungewolltes Auslesen von Tags ist immer auch das Umhüllen der getaggten Produkte

mit Metallfolie wirksam, welche als Faradayscher Käfig gegen magnetische oder elektromagnetische Felder abschirmt.

Dauerhafte Deaktivierung

Der in EPC-Tags vorgeschriebene Kill-Befehl ist ein Mechanismus, der das Auslesen von Daten auf EPC-Tags dauerhaft unterbindet. Allerdings bleibt es den Tag-Herstellern überlassen, wie sie diese Deaktivierung implementieren. Ein bloßes Überschreiben des EPC mit Nullen erscheint ungenügend, da auch andere Tag-Daten und Funktionen zum unberechtigten Tracking & Tracking verwendet werden können. So kann die ungelöschte Tag-ID allein ebenso eindeutig das getaggte Objekt identifizieren, wenn die Produktinformation in Datenbanken neben dem EPC auch die Tag-ID enthält, was zum Zweck der Duplikatsprüfungen gängige Praxis ist. Oftmals wird aus Kostengründen der Kill-Befehl als reine Softwarelösung implementiert, so dass die Tags unter Umständen wieder reaktiviert werden können.

Clipped Tags

Clipped Tags als Alternative zum Kill-Befehl des EPC-Tag werden von IBM zur Verbesserung des Datenschutzes propagiert und inzwischen von der kanadischen Firma Labels Marnlen hergestellt [ibm06]. Abb. 20 zeigt den schematischen Aufbau eines solchen Tags mit abtrennbaren UHF-Antennen. Der Endkunde kann eigenverantwortlich die Perforierungen des gekauften Medikaments durchtrennen und damit die Reichweite der Tags von etwa 10 m auf wenige cm verkürzen. Diese Maßnahme ist zudem per Augenschein überprüfbar. Das Tag kann weiterhin für eine Rückgabe und den Rückruf des Medikaments verwendet werden, ist aber vor unberechtigtem Auslesen viel besser geschützt als normale UHF-Tags.

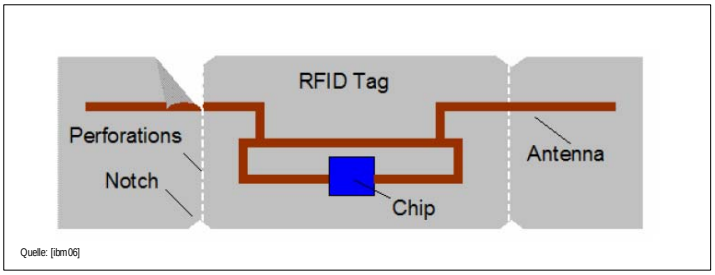


Abb. 20 – Clipped UHF-Tag

Blocker-Tags

Blocker-Tags wurden von den RSA Laboratories zum Schutz der Privatsphäre vorgeschlagen [juels03], können aber auch für Denial of Service-Angriffe verwendet werden (siehe 3). Diese passiven Tags stören das Auslesen aller anderen Tags in der Umgebung, indem sie viele andere Tags simulieren und damit jeden RFID-Leser blockieren. Ein Blocker-Tag sendet z.B. EPCs im gesamten EPC-Zahlenraum aus und veranlasst einen RFID-Leser dazu, den gesamten Nummernraum (nach dem Tree Walking Protokoll) zu durchsuchen. Andere Tags können somit nicht mehr erfasst und zum Lesen vereinzelt werden. Es ist aber auch möglich, nur bestimmte Bereiche von Seriennummern zu blockieren, so dass ein Lesen bestimmter Seriennummern (falls gewünscht) weiterhin möglich ist.
Es ist auch denkbar, dass Kennnummern beim Verkauf eines Medikaments an der Kasse mit einem anderen Präfix (eine Art Privacy-Bit) überschrieben werden, welches durch Blocker-Tags geschützt wird. Damit könnte sowohl die Funktionssicherheit von RFID-Lesern in Ver-

kaufsräumen als auch die Privatsphäre von Endkunden geschützt werden. Blocker-Tags müssten von den Personen, die ihre Privatsphäre schützen möchten, allerdings dauernd mitgeführt werden. Außerdem müssen für verschiedene Antikollisions-Mechanismen (Tree Walking, ALOHA) verschiedene Blocker-Mechanismen eingesetzt werden.

3.2.8 Sicherheit von Mikroprozessor-Tags

Können höherwertige Tags eingesetzt werden, z.B. in geschlossenen Behälterkreisläufen oder für sehr hochwertige Produkte, so bieten sich dafür Mikroprozessorkarten mit einer kontaktlosen Schnittstelle z.B. Proximity Cards nach [iso14443] oder Vicinity Cards nach [iso15693] an. Einfache Mikroprozessorkarten, z.B. LF-Tags der Firma Legic oder HITAG- und MIFARE-Tags von NXP mit HF-Schnittstellen, werden vor allem zur Identifikation von Personen in Zutrittssystemen eingesetzt. Sie besitzen mehr anwendungsspezifischen Speicherplatz als Low-Cost Tags und haben meist einfache kryptographische Verfahren (DES, 3DES) und proprietäre Authentisierungsmechanismen implementiert. Auch das Schlüssel- und Applikationsmanagement ist meist proprietär, so dass die Tags schlecht in offenen Systemen eingesetzt werden können. Höherwertige Smart Cards besitzen dagegen eine standardisierte Kommandoschnittstelle und eine Sicherheitsarchitektur, welche zu [iso7816-4] konform ist. Im Folgenden werden einige Sicherheitsmerkmale dieser interoperablen Smart Cards skizziert.

Kryptographische Algorithmen

Auf Smart Cards stehen die wichtigsten kryptographischen Mechanismen zur Verfügung. Die Karten sind zumeist mit Co-Prozessoren für symmetrische (3DES, AES) und asymmetrische kryptographische Verfahren (RSA, ECC) ausgestattet und unterstützen die Generierung von Schlüsseln direkt in der Karte, so dass ein privater Schlüssel niemals übertragen werden muss. Die Ausführungszeiten für symmetrische kryptographische Berechnungen liegt heute bei etwa 50 µs, für asymmetrische noch bei einigen 10 ms. Proximity Cards mit einem Leseabstand von ca. 10 cm finden auch zur persönlichen Identifikation in Reisepässen oder in Mitarbeiterausweisen Verwendung und eignen sich besonders dann zur Identifizierung von Objekten, wenn diese einzeln und mit ausreichendem Zeitabstand dem Lesegerät präsentiert werden können. Vicinity Cards nach [iso15693] mit größerem Leseabstand eignen sich nur beschränkt für höherwertige Sicherheitsprotokolle, da sie für die Implementierung kryptograhischer Sicherheitsfunktionen eine zu geringe Leistungskopplung aufweisen.

Betriebssystem-kontrollierter Zugriffsschutz

Smart Cards verfügen über ein eigenes Betriebssystem (meist im ROM), das eine für alle installierten Kartenanwendungen einheitliche Sicherheitsarchitektur implementiert. Damit ist der Zugriff auf schützenwerte Daten über die CPU unter Einbeziehung der Co-Prozessoren kontrollierbar. Die Kartenkommandos, Sicherheitsarchitektur und das Dateisystem sind meist nach den Vorgaben in [iso7816-4, -8] gestaltet und erlauben die Speicherung und Nutzung anwendungsspezifischer Daten. Für jede Datei, jedes Kartenkommando oder kryptographische Objekt können eigene Sicherheitsattribute (Zugriffsregeln) installiert werden. Das Betriebssystem prüft auf Basis der Zugriffsregeln die Zulässigkeit jedes Kartenbefehls und führt eine Operation folglich nur dann aus, wenn die Sicherheitsbedingungen erfüllt sind. Beispielsweise kann in den Zugriffsregeln eine Echtheitsprüfung und die Authentisierung einer

zugreifenden Instanz gefordert werden, z.B. eine Benutzerauthentisierung mit PIN oder Biometrie oder eine Geräte-Authentisierung auf Basis symmetrischer oder asymmetrischer Protokolle.

Authentisierungsverfahren auf Basis von CV-Zertifikaten

Bestandteil der asymmetrischen Geräte-Authentisierung sind so genannte Card Verifiable Certificates (CV-Zertifikate), die in beglaubigter Form den öffentlichen RSA-Schlüssel und die so genannte Certificate Holder Authorization (CHA) enthalten. Für eine gegenseitige Authentisierung von Tag und Lesegerät müssen beide Seiten auf gesicherte Weise den öffentlichen Schlüssels der jeweils anderen Seite importieren, um anschließend deren Authentisierungsdaten verifizieren zu können. Der Challenge-Response-Mechanismus ist in [iso7816-8] genormt und ausführlich in [cwa14890-1] beschrieben. Das CV-Zertifikat einer externen Instanz (z.B. eines autorisierten RFID-Lesers mit integrierter Sicherheitsmodulkarte) weist mit der CHA eine bestimmte anwendungsspezifische Rollenkennung auf, deren Präsentation in den Zugriffsregeln der geschützten Daten gefordert werden kann. Nach erfolgreicher Authentisierung wird im Tag ein Sicherheitszustand gesetzt, der besagt, dass die externe Einheit sich nachweislich mit ihrer Rollenkennung präsentiert hat. Dann wird der Zugriff auf bestimmte Daten im Tag, deren Zugriff mit der Rollenkennung geschützt ist, ermöglicht. Neben den asymmetrischen Verfahren könnte das smarte Tag auch symmetrische Authentisierungsverfahren unterstützen, was z.B. bei Interaktionen mit einem Datenserver genutzt werden kann. Generell gilt, dass bei 1:n-Beziehungen (z.B. Karte – Autorisierte Lesegerät eines Zulieferers) die Nutzung asymmetrischer Verfahren sinnvoll ist, bei 1:1-Beziehungen (z.B. Karte – Produktionsdatenserver des Herstellers) jedoch sich die Nutzung eines symmetrischer Verfahrens anbietet.

Sichere Datenübertragung

Als weiteres Element der Sicherheitsarchitektur von [iso7816-4] könnte das Konzept des Trusted-Channels unterstützt werden. Während der Card-to-Card-Authentisierung werden dabei zwischen zwei Instanzen (z.B. Tag / Sicherheitsmodul auf Seiten des Lesegeräts) symmetrische Schlüssel vereinbart, die nur für die Dauer der Sitzung gültig sind. Mit diesen Schlüsseln können dann alle Daten, die von und zum Tag übertragen werden, kryptographisch geschützt werden (Secure-Messaging). Jedes Kommando und jede Antwort wird dabei mit einer kryptographischen Prüfsumme versehen. In den Zugriffsregeln kann zusätzlich auch eine verschlüsselte Übertragung der Daten gefordert werden.

PKI-Dienste

Smarte Tags sind technisch in der Lage, die X.509-basierten PKI-Dienste zu unterstützen, z.B. die Erstellung und Prüfung von digitalen Signaturen, die Dokumenten-Verschlüsselung / Entschlüsselung und Verfahren der Client/Server-Authentisierung. Die Dokumenten-Verschlüsselung / Entschlüsselung wäre z.B. für die chiffrierte Übertragung von Produktionsdaten in einem Netzwerk einsetzbar. Die Funktion Client/Server-Authentisierung kann z.B. für die Erzeugung von Autorisierungstoken genutzt werden und das im Internet gebräuchliche SSL/TLS-Verfahren auf Basis von RSA oder ECC verwenden. Dabei könnte das Tag den Aufbau eines sicheren Kanals zwischen Lesegerät und Datenserver unterstützen, indem seine Signaturen im Protokoll verwendet werden, z.B.:

- Das Lesegerät liest das X.509-Zertifikat für den Client/Server-Authentisierungsschlüssel aus dem Tag und sendet das Zertifikat an den Datenserver, der den öffentlichen Authentisierungsschlüssel des Tags extrahiert.
- Der Server sendet eine Challenge an das Lesegerät, das dieses vom Tag mit dem geheimen Authentisierungsschlüssel signieren lässt und an den Server zurücksendet.
- Der Server prüft die Signatur mit dem öffentlichen Schlüssel des Tags. Schließlich wird ein sicherer Kanal zwischen dem Server und dem Lesegerät (nicht zwischen Server und Tag) aufgebaut.

Dabei ist das Tag selbst an diesem Protokoll nicht weiter beteiligt, dient aber als sicherer Datenspeicher und Sicherheitskomponente, um Missbrauch in den Lesegeräten und Anwendungen zu verhindern. X.509-basierte Authentisierungsverfahren sind kein Ersatz für ein Card-to-Card-Authentisierungsverfahren, da Smart Cards heutiger Technologien keinen entsprechenden Decoder für X.509-Zertifikate besitzen. Die X.509-Zertifikate sind um ein Vielfaches größer als CV-Zertifikate und weisen auch keine Rollenkennung auf, welche direkt für rollenbasierte Zugriffsregeln in der Karte verwendet werden könnte.

Beide Authentisierungsprotokolle mit CV- bzw. X.509-Zertifikaten setzen jeweils das Vorhandensein einer eigenen PKI voraus, welche die Kosten des Tageinsatzes weiter erhöht. Dadurch muss ihre Verwendung vermutlich auf Tags in geschlossenen Kreisläufen oder auf das Tagging sehr teurer Produkte mit langem Life Cycle (z.B. Automobile) beschränkt bleiben. Der Einsatz von Tags in Smart Card-Qualität ist besonders dann sinnvoll, wenn die eigentlichen schützenswerten Daten statt im Backend im Tag selbst gespeichert werden sollen.

Zusammenfassung Kapitel 3: Sicherheit von RFID-Systemen

Die Luftschnittstelle zwischen Tag und Lesegerät und die Tags selbst sind vielfältigen Angriffen ausgesetzt wie z.B. Sniffing, Spoofing, Cloning und Tracking. Die Bedingungen für Low-Cost Tags schränken allerdings den Einsatz notwendiger kryptographischer Sicherheitsmechanismen stark ein. Auch EPC-konforme Tags, welche zunehmend als Low-Cost Tags eingesetzt werden, haben nur wenige Sicherheitsmerkmale und sind kaum in ein umfassendes Sicherheitskonzept integrierbar, weil die meisten Verfahren zur Authentisierung, Verschlüsselung, Pseudonymisierung, zum Integritäts- und Zugriffsschutz die Tag-Ressourcen übersteigen.

Ansätze der Lightweight und Minimalist Cryptography versuchen diese Einschränkungen zu beachten, führen aber außerhalb der Tags meist zu erhöhtem Aufwand wie Synchronisation kryptographischer Daten, Aktualisierung von Schlüsseln und Datenbanksuchen. Diese sind bei Echtzeitsanforderungen und hohen Tag-Stückzahlen zumindest in offenen Lieferketten kaum praktikabel. Für Low-Cost Tags sollten Alternativen gefunden werden, welche die Sicherheit ohne Effizienzverlust verbessern. Wichtige Forschungsgebiete sind Physical-One-Way-Functions, Physical-Uncloneable-Functions für die Authentisierung und One-Time-Codes für die Verschlüsselung. In geschlossenen Kreisläufen oder für sehr hochwertige Produkte könnten Tags mit Mikroprozessorchips eingesetzt werden, die über großen Speicherplatz und eine eigene Sicherheitsarchitektur verfügen.

4 RFID-Anwendungsszenario: Produktion

Das Anwendungsszenario „Produktion“ befasst sich mit der Lieferkette der Automobilindustrie, die aufgrund des durchgängigen Waren- und Informationsflusses in Kombination mit geschlossenen Behälterkreisläufen für die Nutzung von RFID besonders geeignet erscheint [strassner05, taucis06]. In dem beschriebenen Szenario werden Konzepte zur Online-Steuerung der unternehmensübergreifenden Produktion und der Supply Chain über RFID-Systeme betrachtet. Dabei werden die abgeleiteten sicherheitsrelevanten Anforderungen den Erwartungen und Einschätzungen der Anwendungspartner im Bereich Produktion gegenübergestellt.

4.1 Das Szenario der Automobilproduktion

Für diese Studie wurden mehrere Interviews geführt, die den Einsatz von RFID in einer Produktionsumgebung anhand von konkreten Anwendungen thematisieren. Interviewpartner waren die folgenden Anwender:

- der DaimlerChrysler AG, Bremen und ergänzend das LogDynamics Lab [logdynamic06]
- der BLG Logistics Group, Bremen,
- der DaimlerChrysler AG, Rastatt.

Jeder der Anwendungspartner hat RFID in einer in sich geschlossenen Produktionsumgebung im Einsatz. Es werden an dieser Stelle zwei konkrete Szenarien ausführlicher thematisiert, weil diese beiden Einsatzszenarien jeweils ein bestimmtes Einsatzgebiet der RFID-Technologie in der Automobilproduktion widerspiegeln (Kontrolle eines Produktionsprozesses sowie automatische Bereitstellung von Produktdaten für die Dokumentation und Archivierung). Zunächst wird in 4.1.1 das Einsatzszenario des DaimlerChrysler-Werks in Bremen im Detail beschrieben. Anschließend wird in Abschnitt 4.1.2 das RFID-Einsatzszenario des DaimlerChrysler-Werkes in Rastatt erläutert. Darüber hinaus wird auch eine Erweiterung dieses Szenarios in Richtung virtuelle Baukarte beschrieben.
Bei den betrachteten Szenarien handelt es sich nicht um lieferketten-übergreifende, sondern um begrenzte, geschlossene Kreisläufe. Um jedoch auch die Sicherheitsanforderungen an lieferketten-übergreifende Prozesse zu verdeutlichen, wird in 4.1.3 eine generische Lieferkette vorgestellt. In dieses Szenario sind insbesondere Einsatzszenarien der BLG Logistics Group eingeflossen.

4.1.1 Kontrolle des Produktionsprozesses

Just-in-Sequence-Produktion

Die Herstellung und Auslieferung der Sitze der Fahrzeugreihe Mercedes SLK an das DaimlerChrysler-Werk Bremen erfolgt Just-in-Sequence (JIS) durch den Zulieferer Lear Corporation. Der Versand der Sitze durch Lear sowie ihre Verbringung an den Verbauort im DaimlerChrysler-Werk erfolgen in speziellen Ladungsträgern (LT), die nach ihrer Entladung an der Produktionsstätte zur erneuten Verwendung an die Lear Corporation zurückgeführt werden.

Jeder LT verfügt über einen Barcode, der seine Identifikation ermöglicht, und zwei identische Warenanhänger. Sie bezeichnen die im Ladungsträger enthaltenen Sitze und enthalten folgende Informationen in Anlehnung an [vda4902]:

- Kontaktdaten des Zulieferers,
- kleinste Schichtnummer der enthaltenen Sitze,
- größte Schichtnummer der enthaltenen Sitze,
- Sitzmerkmal linke bzw. rechte Fahrzeugseite (L/R),
- Ladungsträger-Nummer.

Ausstattung von Ladungsträgern mit Tags

Für das RFID-Pilotprojekt zum Ladungsträgermanagement wurden insgesamt 54 Ladungsträger zusätzlich zu Barcodes und Warenanhängern auf zwei Seiten mit einem passiven Tag versehen. Sie enthalten neben einer weltweit einmaligen 64-Bit-ID-Nummer keine zusätzlichen Daten. Zum Einsatz kommen Tags der ReadAll GmbH (RAAT-5590-3.1 L/D). Diese beruhen auf dem Chip ATMEL TagIDU 5590 und können im Pulk erfasst werden. Der Chip unterstützt den EPC gemäß ISO 15961.
Im Testbetrieb kommt ein Lesegerät der Firma deister electronic (LogIdent UDL 500) zum Einsatz, das über eine Schreib-/Leseeinheit und integrierte Antennen verfügt. Es unterstützt laut Herstellerangaben die UHF-Protokolle ISO 18000-6 C, EPC Class1 Gen2 sowie ATMEL ATA 5590 und EM 4022, 4222, 4422.

Ziel des RFID-Pilotprojektes

Das Projekt soll insbesondere die technische Funktionsfähigkeit der ausgewählten Hardwarekomponenten im Ladungsträgermanagement zeigen [ulrich05]. Darüber hinaus gibt DaimlerChrysler neben dem zusätzlichen Informationsgewinn die Optimierung der Ladungsträgersteuerung als wichtigstes Kriterium für den Einsatz der RFID-Technologie an. Dazu dienen zwei wesentliche Punkte:

1. **Sicherstellung der Variantentreue.** Als Variantentreue wird die korrekte Platzierung der zu verbauenden Sitze bezeichnet, d.h. dass linke Sitze auf der linken und rechte Sitze dementsprechend auf der rechten Seite eines Fahrzeugs neben dem Band abgestellt werden müssen.
2. **Sicherstellung der Sequenztreue.** Als Sequenztreue wird die reihenfolgetreue Bereitstellung der Komponenten entsprechend dem JIS-Prinzip bezeichnet.

Die Sequenztreue wird beim Zulieferer durch den Einsatz eines Barcode-Systems umgesetzt, so dass dort zurzeit keine RFID-Hardware zum Einsatz kommt. Im Gegensatz dazu erfolgt die Bereitstellung der Ladungsträger bei DaimlerChrysler RFID-gestützt, um so die Variantentreue sicherzustellen. Dazu werden unterstützend Bestückungs- und Versanddaten zu den Ladungsträgern und den darin enthaltenen Sitzen benötigt, die als Solldaten im Vergleich zu den bei DaimlerChrysler ermittelten RFID-Istdaten dienen. Zu diesem Zweck erfolgt beim Warenausgang eine Übertragung der Daten, die sich auch auf dem Warenanhänger befinden, aus den operativen Systemen des Zulieferers an DaimlerChrysler. Anhand dieser Daten kann der Verbauort der im LT enthaltenen Sitze im Werk bestimmt und beim Transport an den Verbauort eine Kontrolle der Sequenz- und Variantentreue durchgeführt werden.

Der Transportvorgang lässt sich in die zwei Teilschritte „Bereitstellung der Ladungsträger im Staplerpfad“ und „Bereitstellung der Ladungsträger am Verbauort“ untergliedern, die im Folgenden beschrieben werden. Einen schematischen Überblick über den Ladungsträgerkreislauf zwischen Lear Corporation und DaimlerChrysler bietet dabei Abb. 21 [ulrich05].

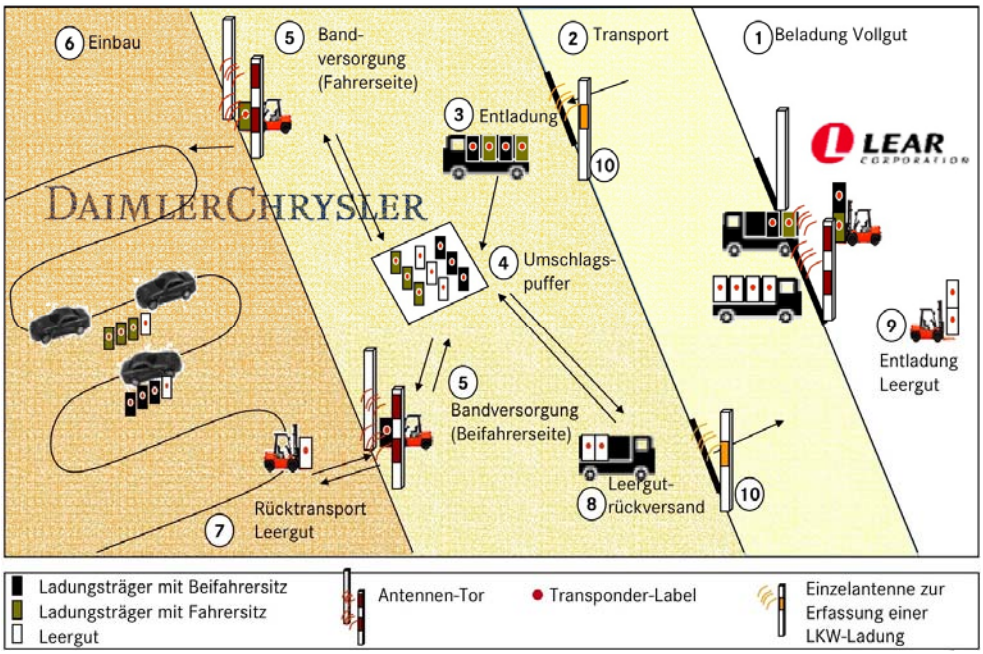


Abb. 21 – Prozess “Ladungsträger-Management bei DaimlerChrysler in Bremen”

Bereitstellung der Ladungsträger im Staplerpfad

Das Ziel des Prozessschrittes „Bereitstellung der Ladungsträger im Staplerpfad“ ist die Verbringung der Ladungsträger in der korrekten Reihenfolge in den Staplerpfad auf der richtigen Bandseite (rechts/links). Die dazu nötigen Arbeitsschritte lassen sich in vier sequentielle Teilaufgaben aufschlüsseln:

1. Der Gabelstaplerfahrer nimmt am Verbauort einen geleerten Ladungsträger auf und transportiert ihn zum Puffer für leere Ladungsträger (Schritt 7 in Abb. 21). Bei der Ausfahrt aus dem Staplerpfad wird der LT von den dort montierten Lesegeräten erfasst und als „entladen“ registriert. Dabei kann eine Unterscheidung zu einem in den Staplerpfad einfahrenden, beladenen LT getroffen werden, da nur die nun leeren Ladungsträger bereits vorab am Verbauort registriert worden sind.
2. Der Staplerfahrer entnimmt einen bestückten LT aus dem Umschlagspuffer für volle Ladungsträger und fährt mit diesem in den Staplerpfad ein, in dem sich ein RFID-Lesegerät befindet (Schritt 5).
3. Der Ladungsträger wird durch Auslesen seiner Tags eindeutig identifiziert.
4. Der identifizierte Ladungsträger wird den von Lear übermittelten Sitz- und Ladungsträgerdaten zugeordnet. An diesem Punkt erfolgt eine Kontrolle, ob der Staplerfahrer mit dem LT in den Staplerpfad auf der richtigen Bandseite einfährt und die Sequenz eingehalten wird. Der Fahrer erhält dazu eine optische Rückmeldung, so dass er bei Nichteinhaltung der Variantentreue auf der anderen Bandseite weiterfahren bzw. beim Auftreten eines

Reihenfolgefehlers den richtigen LT aus dem Umschlagspuffer entnehmen kann. Die Fehlerursache ermittelt er dazu mit einer visuellen Kontrolle des Warenanhängers.

Bereitstellung der Ladungsträger am Verbauort

Der korrekte Ladungsträger wird nun in einem zweiten Prozessschritt am Verbauort zur Entnahme der Sitze bereitgestellt, so dass diese in ein Fahrzeug eingebaut werden können:

1. Der Gabelstaplerfahrer fährt mit dem LT zum Drehteller am Verbauort. Über diesem befindet sich ein weiteres Lesegerät.
2. Beim Abstellen des vollen Ladungsträgers auf dem Drehteller werden die beiden Tags ausgelesen und die Datensätze in einer Archivierungskomponente abgelegt. Auf einem Drehteller haben zwei Ladungsträger Platz (ein voller und ein leerer zur Entnahme). Sie werden an dieser Position auf das Vorhandensein von je zwei Tags geprüft, um einen eventuellen Verlust frühzeitig zu bemerken. Ein Ladungsträger, dessen Tag beschädigt werden oder verloren gehen und der somit nicht mehr zugeordnet werden kann, hat erhebliche negative Auswirkungen auf den Produktionsprozess, da das Wiederauffinden bzw. die Zuordnung zu den richtigen Fahrzeugen zu teuer ist oder länger dauern kann, als der Bandtakt von 4,5 Minuten es zulässt.
3. Der korrekt identifizierte Ladungsträger wird den Sitz- und Ladungsträgerdaten zugeordnet. Es erfolgt erneut eine Kontrolle auf den richtigen Verbauort und die Einhaltung der Sequenz. Ist kein Fehler aufgetreten, wird der LT auf dem Drehteller abgestellt und mit der Aufnahme des entleerten Ladungsträgers vom Drehteller und dem Rücktransport zum Puffer für leere Ladungsträger ist der Prozesszyklus abgeschlossen. Andernfalls erfolgt die Fehlerbehandlung wie beim ersten Prozessschritt dargestellt.

Die zweite Fehlerprüfung ist erforderlich, da die Gabelstaplerfahrer teilweise die Lesegeräte am Staplerpfad und somit die erste Prüfung auf Sequenz- und Links-Rechts-Fehler umgehen können. Das Gesamtsystem muss also in der Lage sein, den Datensatz eines Tags korrekt zu verarbeiten, das erst am Verbauort registriert wird, ohne bereits im Staplerpfad erfasst worden zu sein.

4.1.2 Dokumentation von Produkt- und Produktionsdaten

Im Rahmen der Cockpit-Vormontage bei DaimlerChrysler in Rastatt werden beispielsweise das Bremsmodul oder eine Klimaanlage ins Cockpit eingebaut. Dazu werden die Fahrzeugnummer und so genannte Variable Produktdaten (VPD) benötigt, die mit Hilfe von Funk-Barcode-Scannern erfasst werden. Die VPD sind dokumentationspflichtige Produktionsdaten, die in Verbindung mit einem Fahrzeug für die Dauer von zehn Jahren archiviert werden. Ohne eine vollständige Erfassung darf ein Fahrzeug nicht freigegeben werden. Im Fall der Cockpit-Vormontage handelt es sich bei den VPD um eine Produktions- und eine Sachnummer. Letztere dokumentiert die Airbagnaht, d.h. die Sollbruchstelle des Airbags. Diese Naht muss fachgerecht verarbeitet sein und farblich zur Instrumententafel passen.

Prozessoptimierung durch den Einsatz von RFID

Häufige Defekte an den Barcode-Scannern machen einen größeren Aufwand an Reparaturleistung und Nacharbeit erforderlich. Um dem entgegenzuwirken, ist eine vorbeugende War-

tung etwa alle zwei Wochen nötig. Darüber hinaus entstehen durch den Einsatz von Barcode-Scannern erhöhte Wegezeiten, wenn sich mehrere Mitarbeiter einen Scanner teilen müssen. Eine automatisierte Erfassung mittels RFID mit einer sehr guten Erfassungsrate könnte hier zu einer Prozessoptimierung führen. Aus diesen Gründen führt das DaimlerChrysler Werk in Rastatt eine Machbarkeitsstudie durch, in der zusätzlich zu den etablierten Prozessen Barcodes durch RFID-Tags ergänzt werden. Die Studie soll auch die Wirtschaftlichkeit des RFID-Einsatzes untersuchen.

Einsatz von Smartlabels

Zum Einsatz kommen passive Tags der Firma Philips (ICODE SLI SL2 ICS20). Diese Tags basieren auf [iso15693] und arbeiten im 13,56 MHz-Bereich. Sie verfügen entsprechend [iso15693-3] über eine eindeutige 64-Bit-Kennung sowie über 896 Bit frei nutzbaren Speicher, der in 28 Blöcke unterteilt ist. Jeder dieser Blöcke kann mit einem permanenten Schreibschutz versehen werden [philips02]. Die Tags befinden sich auf Klebe-Etiketten in Rollenform, die mit einem Barcode und weiteren Informationen bedruckt werden können (Smartlabel). Da die Instrumententafel aus Kunststoff besteht, kommen aus Kostengründen Tags zum Einsatz, die nur in nicht-metallischen Umgebungen benutzt werden können. Sie verbleiben auch nach dem Ende des Produktionsprozesses am Objekt, ohne dass eine Löschung der enthaltenen Daten stattgefunden hat. Diese Tags werden im DaimlerChrysler-Werk mit Hilfe von Antennen der Firma SICK ausgelesen.

Die Prozessschritte im Einzelnen

Die Ausstattung der Instrumententafeln mit RFID-Tags beim Zulieferer sowie die Cockpit-Vormontage im DaimlerChrysler-Werk lassen sich in vier Einzelschritte untergliedern, die im Folgenden beschrieben werden. Abb. 22 zeigt dieses Szenario im Überblick. Es laufen folgende Prozessschritte ab:

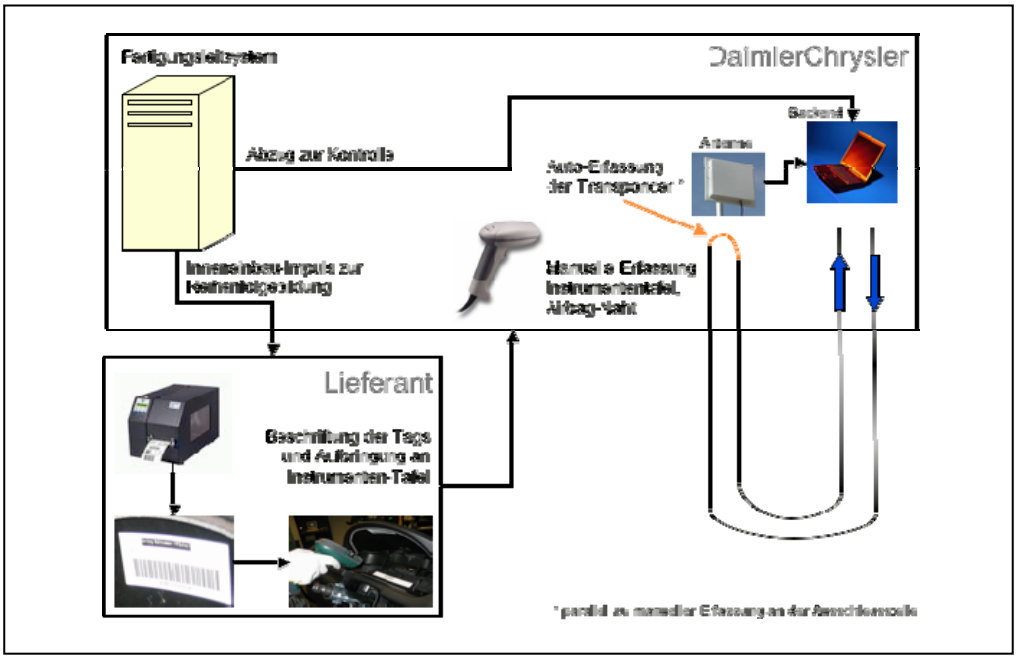


Abb. 22 – Datenerfassung nahe der Cockpit-Ausschleusstelle

1. Aus dem Fertigungsleitsystem bei DaimlerChrysler erfolgt ein Inneneinbauimpuls an den Zulieferer, der über die Reihenfolge der nächsten zu liefernden Instrumententafeln Aufschluss gibt.
2. Beim Zulieferer werden die Klebe-Etiketten mit Hilfe eines Thermotransfer-Druckers mit RFID-Lese-/Schreibeinheit mit den relevanten Daten versehen. Dazu wird zunächst die Tag-ID ausgelesen und das Tag im Klartext mit den VPD beschrieben. Die Tag-ID wird von nun an nicht mehr zur Identifikation verwendet; dazu dient ausschließlich die Produktionsnummer. Aus diesem Grund werden alle nun auf dem Tag befindlichen Daten sicherheitshalber noch einmal ausgelesen. War der Lesevorgang erfolgreich, wird das Etikett mit dem Barcode bedruckt und in die Instrumententafel geklebt.
3. Nach der Lieferung der Instrumententafel erfolgt im DaimlerChrysler-Werk der Einbau weiterer Teile wie Bremsmodul oder Klimaanlage. Die Instrumententafel hängt während dieses Vorgangs an einer Halterung, mit deren Hilfe sie am Arbeitsplatz vorbeibewegt wird. Der Mitarbeiter kann seine notwendigen Arbeiten somit nur in einem begrenzten Bereich vornehmen, indem er sich ggf. mit der Instrumententafel mitbewegt.
4. An die Montage, wenn die Instrumententafel also den Arbeitsbereich des Mitarbeiters passiert hat, schließt sich eine automatische Erfassung des Tags an. Dieser Schritt erfolgt erst zu diesem späten Punkt im Prozess, da die Instrumententafel sich während des Einbaus weiterer Teile bewegt. Damit lässt sich der exakte Verbauort des Cockpits nicht voraussagen, da die Mitarbeiter nicht mit konstanter Geschwindigkeit arbeiten. Die Antennen der Lesegeräte können aus baulichen Gründen nicht an einem früheren Punkt montiert werden, da sie die Mitarbeiter sonst evtl. in ihrer Arbeit behindern würden. Eine Erfassung schon vor der Montage, die auch eine Koinzidenzprüfung mit den Daten im Fertigungsleitsystem ermöglichen würde, ist aus baulichen Gründen ebenfalls nicht möglich. Während der Testphase wird die Erfassung des Tags durch eine Lichtschranke ausgelöst, die die Antennen aktiviert. Mit dieser Vorgehensweise lässt sich zusätzlich die Funktionsfähigkeit des Lesegeräts testen, da unmittelbar auf das Signal der Lichtschranke ein Lesevorgang erfolgen muss. Der Mitarbeiter erhält dazu eine optische Rückmeldung.

Ein großes Problem in diesem Szenario sind fehlende Tags, die beim Zulieferer nicht eingeklebt wurden. Darüber hinaus treten auch übereinander geklebte Etiketten auf. Um einem Bandstopp, der Kosten in siebenstelliger Höhe verursachen kann, vorzubeugen, behilft sich DaimlerChrysler mit einem einfachen Lösungsansatz. An der Stelle, an der die Tags nach der Montage ausgelesen werden, ist eine Kamera montiert. Diese nimmt ein Bild der Instrumententafel auf, das einen Plausibilitätscheck für den Fall erlaubt, dass nach dem Auslösen der Lichtschranke kein erfolgreicher Lesevorgang durchgeführt werden kann.

Während der Machbarkeitsstudie ist die RFID-Technik noch nicht an bestehende Prozesse angebunden. Die mittels RFID erfassten Daten werden ausschließlich an einen dedizierten Rechner weitergeleitet, der ein Backend simuliert und über den eine Auswertung erfolgen kann. In einer späteren Phase des Projekts ist eine Weiterleitung der Daten an das Fertigungsleitsystem sowie eine dauerhafte Archivierung geplant. Darüber hinaus sollen in einem späteren Schritt zusätzliche VPD erfasst und weitere Vorlieferanten eingebunden werden.

Die virtuelle Baukarte

Wenn auch bislang noch nicht vorgesehen, so könnte man sich als Erweiterung sogar eine virtuelle Baukarte (Fahrzeug-Kontrollkarte) vorstellen, die auf ein Tag abgebildet wird. Auf einer Baukarte (vgl. Tab. 8) befinden sich üblicherweise die dokumentations- und archivierungspflichtigen Produktionsdaten eines Automobils. Diese geben Auskunft über die verbauten Teile und dokumentieren den Produktionsweg. Auch werden Verbaufehler vermerkt. Mit Hilfe der Baukarte lassen sich während der Produktion regulär vorgenommene Arbeiten ebenso nachvollziehen wie nachträgliche Fehlerkorrekturen. Bei sicherheitskritischen Teilen ist jeder Arbeitsschritt mittels Baukarte auf einen Mitarbeiter rückführbar. Insbesondere wird jeder Arbeitsschritt derzeit manuell per Stempel durch den entsprechenden Mitarbeiter bestätigt.

Tab. 8 – Beispiele für Baukarteneinträge

Identifikationsdaten	Produktdaten	Prozessdaten (Einbauschritte)	Qualitätsdaten
Halle	Motoraufrüstung	Batterie	Beanstandungen
Tag	Bremsgerät	Lenkungskupplung	Endabnahme (z.B. Motor)
Schichtnummer	Hinterachse	Motorlager hinten	Motortest
Fahrgestellnummer	Airbag Naht Beifahrer	Kraftstoffleitung hinten	Regenprobe
Ausstattung	Radio/Navigationssystem	Klimarohr	Abgaszentrum
Lack	Elektronische Schließungsnummer	Cockpitverschraubung	Elektronik-Test

Abhängig vom verfügbaren Speicherplatz können Teile der auf der Baukarte eingetragenen Informationen nun auf ein RFID-Tag ausgelagert werden wie z.B.:

- **Daten zur Prozessunterstützung**: Auf dem RFID-Tag können die Verarbeitungsschritte festgehalten werden, so dass die Qualitätssicherung durch automatische Prozesse unterstützt werden kann. Mit Hilfe eines Werksausweises könnten sogar einzelne Arbeitsschritte automatisch bestätigt werden (Abstempeln). Der Werksausweis würde in diesem Fall also das Tag mit der virtuellen Baukarte beschreiben. Durch die Automatisierung des Abstempelns der Baukarte wird der eigentliche Effizienzgewinn erwartet. Zudem können die Entscheidungen im Prozess – z.B. zur Gewährleistung der Variantentreue der Sitze im Anwendungsszenario „DaimlerChrysler Bremen“ – auch durch auf den RFID-Tags gespeicherte Informationen unterstützt werden, immer eine entsprechende Verlässlichkeit vorausgesetzt.
- **Informationen für das Recycling**: Da eine Baukarte den Herstellungszyklus eines Fahrzeugs dokumentiert, können in diesem Zusammenhang für ein effizientes Recycling benötigte Informationen miteinbezogen werden. Dieses vereinfacht die Einhaltung von Gesetzen und Richtlinien [vda5501, eu2000, elektrog05].
- **Für die Wartung relevante Daten**: Beispielsweise wird die Schichtnummer gespeichert, über die sich bei Bedarf auch die für den Einbau verantwortliche Person ermitteln lässt.

Durch den Einsatz einer virtuellen Baukarte könnten Fertigungszeiten (Endmontage) vermindert werden.

4.1.3 Absicherung der gesamten Lieferkette

Von Insellösungen zu einem lieferketten-übergreifenden Einsatz von RFID

Die in Abschnitt 4.1.1 und 4.1.2 beschriebenen Szenarien stellen einen von den Anwendungspartnern umgesetzten realen Einsatz von RFID-Technologien dar. Beide haben gemein, dass sie nur in einem Teil einer lieferketten-übergreifenden Prozesskette eingesetzt werden und somit Insellösungen darstellen. Diese Tatsache nimmt Einfluss auf die Bedrohungen und Sicherheitsanforderungen, die sich in geschlossenen und lieferketten-übergreifenden Anwendungen unterscheiden können. Es ist anzunehmen, dass sich mit der Verbreitung der RFID-Technologie auch die Gewichtung der Bedrohungen und der Sicherheitsanforderungen verändert. Wird die Schwelle von Insellösungen zu lieferketten-übergreifenden Lösungen überschritten, so sind auch die Prozessketten, in welchen die RFID-Technologie heutzutage schon eingesetzt wird, nicht mehr geschlossen. Die Konsequenzen dieser Entwicklung und die heute herrschenden Ausgangsbedingungen müssen frühzeitig bei der Entwicklung von Daten- und Kommunikationsstandards berücksichtigt werden. Aus diesem Grund wird in diesem Abschnitt eine übergreifende Lieferkette beschrieben, die in dieser Vollständigkeit noch nicht umgesetzt worden ist, an der aber Bedrohungen und Sicherheitsanforderungen erörtert werden können, die in einer geschlossenen Prozesskette selten vorkommen.

Nutzen eines lieferketten-übergreifenden Einsatzes von RFID

Bei einem durchgängigen Waren- und Informationsfluss in Kombination mit einem geschlossenen Behälterkreislauf ist die Nutzung von RFID besonders vielversprechend. Wenn auch bei den meisten Fahrzeugherstellern derzeit kein übergreifender Einsatz der RFID-Technologie existiert, so soll in diesem Szenario die gesamte Lieferkette vom Zulieferer bis hin zu Händler und Werkstatt betrachtet werden. Des Weiteren wird ein Fokus auf den After-Sales-Bereich (also nach Auslieferung des Fahrzeuges) gelegt, der Rückrufe durch den Fahrzeughersteller, Wartung und Reparaturen in Werkstätten sowie Recycling und Entsorgung am Ende des Produktlebenszyklus umfasst. Darüber hinaus beinhaltet das Szenario verschiedene Einsatzgebiete von RFID in der unternehmensübergreifenden Produktion und Lieferkette. Hierzu gehören beispielsweise die prozessübergreifende Verfolgung von Lieferungen, die Bereitstellung von Daten über die Qualität der Einzelteile, das Werkzeug- und Behältermanagement während der Produktion, sowie der Echtheits- und Diebstahlschutz.

Ein lieferketten-übergreifendes RFID-Szenario ermöglicht den beteiligten Unternehmen eine synchrone Darstellung des Material- und Informationsflusses. Dabei steht genau dann, wenn ein Objekt mit Tag verfügbar ist, auch die zugehörige Information zur Verfügung und umgekehrt [vda5501]. Um dieser Anforderung gerecht zu werden, wird im Folgenden davon ausgegangen, dass alle Bauteile eines Fahrzeugs mit RFID-Tags ausgestattet sind, die während des gesamten Lebenszyklus am Objekt verbleiben. Die Kennzeichnung jedes Objekts erfolgt dabei schon während seiner Produktion durch den jeweiligen Zulieferer. Das Szenario betrachtet beispielhaft den Weg eines Motorblocks vom Zulieferer über Fahrzeughersteller (Original Equipment Manufacturer, OEM), Logistikdienstleister (LDL), Händler und Werkstätten bis hin zu Recycling- und Entsorgungsbetrieben. Es wird stark vereinfachend angenommen, dass der Motor im Ganzen von einem einzigen Automobil-Zulieferer hergestellt und mit einem RFID-Tag versehen wird.

Speicherung von Produkt- und Produktionsdaten auf den Tags

Die in den verschiedenen Stufen des Wertschöpfungsnetzwerks erforderlichen Daten können auf den RFID-Tags selbst abgelegt werden, sofern diese über eine ausreichende Speicherkapazität verfügen. Diese Lösung, die verschiedene Sichten auf die Tagdaten erforderlich macht, wird im Produktionsumfeld zurzeit favorisiert. Alternativ kommt die Ablage in einem Backend in Frage, das eine zentrale Sicht auf die Daten für alle Wertschöpfungspartner ermöglicht. Beide Möglichkeiten unterscheiden sich in ihren Sicherheitsanforderungen und -risiken und ermöglichen unterschiedliche Angriffe. Auf diese Aspekte wird in Abschnitt 4.2 ausführlich eingegangen. Für die Lösung, die Daten im Backend vorzuhalten, ist für das Backend ein entsprechendes Identitätsmanagement (IDM) und rollenbasiertes Berechtigungsmanagement einzurichten (Bildung von Föderationen [erdos05, chandramouli05]). Näheres dazu ist in Abschnitt 4.3 zu finden.

Die Tag-Datenstruktur

In diesem Szenario gehen wir vereinfachend davon aus, dass die relevanten Informationen auf Tags gespeichert werden, die über Speicherplatz verfügen, der im gesamten Lebenszyklus des Objekts beschrieben, ausgelesen oder verändert werden kann. Das nötige Datemodell wird entsprechend Abb. 23 wie folgt angenommen [vda5501]:

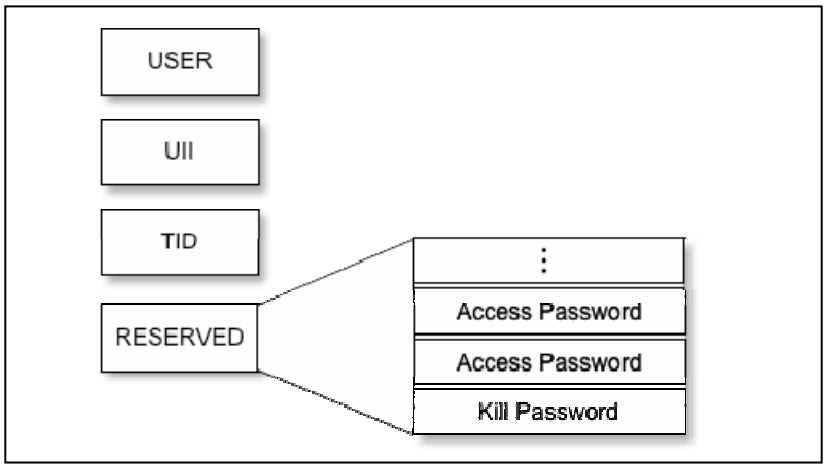


Abb. 23 – Tag-Datenstruktur

Jedes Tag verfügt über einen Unique Item Identifier (UII), der weltweit eindeutig ist. Dabei kann es sich beispielsweise um einen EPC handeln – dies ist aber nicht zwingend vorgeschrieben. Zusätzlich dazu besitzt das Tag einen Speicherbereich, der eine eindeutige Teile- und Seriennummer (TID, Tag-ID) trägt, die vom Hersteller gegen ein Überschreiben geschützt wird. Das Tag-Segment RESERVED wird für die Passwort-Verwaltung verwendet. Es enthält ein Kill-Passwort und weitere Zugriffspasswörter, die für den Zugriff auf die Nutzdaten (USER) benötigt werden. Mit Hilfe der verschiedenen Access-Passwörter lässt sich zum jetzigen Stand jedoch kein differenzierter Schreibzugriff auf den USER-Bereich (etwa gemäß einem Rollenkonzept) umsetzen. Das Kill-Passwort kommt nicht zum Einsatz, da das Tag über den gesamten Lebenszyklus des Objekts im Einsatz bleibt. Der USER-Bereich kann frei organisiert und beschrieben werden. Er enthält folgende Datenfelder:

- Qualitätsstatus/Fehlercode: Dieses Feld kann variabel beschrieben werden. Es ermöglicht, Sperrungen eines defekten Objekts dezentral vorzunehmen.

- Produktionsdatum (schreibgeschützt)
- Zeitstempel: Dieses Datenelement gibt den Zeitpunkt der letzten Datenänderung an
- Gewicht (schreibgeschützt)
- Fahrzeugidentifikationsnummer (schreibgeschützt)
- Recycling-Informationen gemäß EU-Richtlinie über Altfahrzeuge [eu2000]
- freier Block

Mit Ausnahme des freien Blocks sind alle Felder von den an der Lieferkette beteiligten Partnern frei zugreifbar. Der freie Block ist so unterteilt, dass jeder Partner einen verschlüsselten und mit Schreib-/Leserechten versehenen Bereich erhält, in dem sensible Daten geschützt abgelegt werden können. Dieser Zugriffsschutz wird durch die im RESERVED-Feld abgelegten Zugriffspasswörter realisiert. Durch diese Datenstruktur ist ein gezielter Zugriff auf einzelne Datenbereiche möglich, so dass die zum Lesegerät[1] übertragenen Datenmengen und damit auch die Schreib-/Lesezeiten minimiert werden.
Unabhängig von dieser Vorgehensweise ist eine darüber hinausgehende Datenerfassung und -speicherung im Backend eines jeden Wertschöpfungspartners oder in einer föderativ genutzten Datenbank denkbar oder sogar erforderlich [erdos05]. Beispielhaft soll dazu die Nutzung von zusätzlichen EDI-Datenströmen genannt werden, die der Ware „vorauseilen“ [vda5501]. Diese Informationen können mit den Daten auf den RFID-Tags abgeglichen werden und ermöglichen beispielsweise eine Plausibilitätsprüfung beim Wareneingang: Der Empfänger kann mithilfe der EDI-Daten überprüfen, ob er die richtigen Objekte vollzählig erhalten hat, und gegebenenfalls Fehler beim Lieferanten und/oder Spediteur melden.

Einsatz von RFID bei den einzelnen Partnern der Lieferkette

Für das übergreifende Szenario wird die in Abb. 24 dargestellte Lieferkette angenommen:

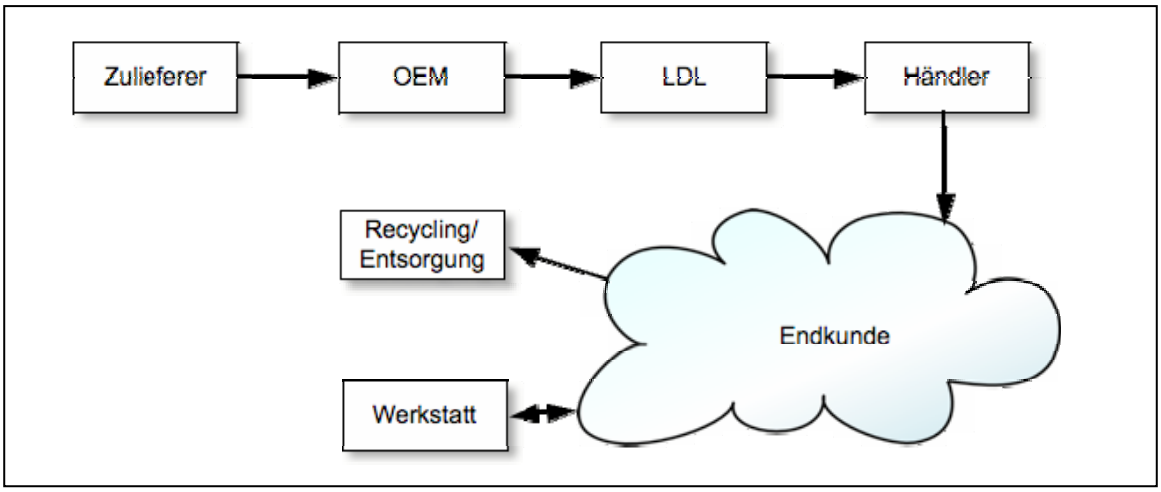


Abb. 24 – Die Lieferkette in der Automobilindustrie

[1] Im Folgenden wird auch die Bezeichnung „RFID-Lesegerät“ verwendet, wenn eine Schreibfunktionalität vorhanden ist.

- **Zulieferer**: Der Zulieferer stellt den Motorblock her und versieht ihn mit einem RFID-Tag, dessen USER-Segment initial mit den Produktdaten beschrieben wird. Er dokumentiert zusätzlich die Produktentstehung in seinem USER-Segment; anhand dieser Daten kann vor der Auslieferung eine Qualitätskontrolle stattfinden. Da die fertigen Motoren anhand ihrer Tags leicht identifiziert werden können, verwendet der Zulieferer diese Informationen zur Sicherstellung der Sequenztreue (vgl. dazu 4.1.1) und kündigt die Lieferung beim Fahrzeughersteller mittels EDI an.
  Weiterhin kann der Zulieferer bei der Warenausgangskontrolle vom RFID-Einsatz profitieren. Hier wird der korrekte Versand an die nächste Stufe der Lieferkette sichergestellt, indem beim Warenausgang ein Abgleich der RFID-Istdaten mit den OEM-Bestelldaten erfolgt. Obwohl dieser Nutzen allein die Mehrkosten durch das Tag nicht für alle Fahrzeugbauteile rechtfertigt, ist dennoch eine wirtschaftliche Legitimierung dieser Vorgehensweise möglich, indem die Kosten zwischen allen Partnern der Lieferkette, die Nutzen aus dem RFID-Einsatz ziehen, so aufgeteilt werden, dass alle profitieren [strassner05a].

- **Fahrzeughersteller**: Der Fahrzeughersteller nutzt beim Eintreffen des zu verbauenden Motors die RFID-Istdaten im Vergleich zu den EDI-Solldaten des Zulieferers zur Wareneingangskontrolle. Diese Vorgehensweise stellt insofern eine Prozessoptimierung dar, als dass ohne RFID-Unterstützung die Wareneingangskontrolle nur implizit über den Verbau des gelieferten Objekts erfolgt, so dass Fehler erst spät entdeckt werden. Auch die Rechnungslegung durch den Zulieferer kann so eher erfolgen.
  Der Fahrzeughersteller verbaut den angelieferten Motor sequenztreu in das richtige Automobil. Dazu kann er die Verbringung des Motors an den Verbauort mithilfe der Daten auf dem Tag steuern, ähnlich wie in 4.1.1 für Sitz-Ladungsträger beschrieben. Er dokumentiert den Einbau des Motors auf dessen Tag (Verbaudokumentation). Diese Daten können in späteren Schritten zum Echtheitsnachweis und zur Qualitätssicherung genutzt werden.
  Neben der Fertigung von Neufahrzeugen organisieren Zulieferer, Fahrzeughersteller und Händler auch die Ersatzteildistribution. Diese umfasst eine große Zahl an Produktvarianten, die teilweise eine kundenindividuelle Konfiguration erforderlich machen. Hier kann RFID zur Lieferzusammenstellung beim OEM Einsatz finden, indem beim Warenausgang ein automatisierter Abgleich mit den Bestelldaten erfolgt [strassner05a].
  Die Ersatzteildistribution bietet ein weiteres Einsatzgebiet für die RFID-Technologie in der Automobilindustrie, da „es sich bei 10% aller als Originalersatzteile vertriebenen Teile in Wirklichkeit um Fälschungen“ [strassner05a] handelt. Aus der Sicht des Fahrzeugherstellers gelten einerseits Plagiate als Fälschungen, also nachgebildete Produkte von teilweise minderer Qualität. Darüber hinaus gelangen auch Ersatzteile auf den Markt, die zwar von einem Vertragpartner produziert wurden, aber nicht den offiziellen Vertriebsweg nehmen. Diese Produkte weisen dieselbe Qualität wie Originalersatzteile auf, da sie zu diesen baugleich sind. Sie führen jedoch zu Umsatzeinbußen des Fahrzeugherstellers. Beide Arten von Fälschungen erhöhen für den OEM das Risiko von Klagen und einem daraus resultierenden Imageverlust. In Verbindung mit einer ausführlichen Produkthistorie kann RFID hier wirtschaftlich sinnvolle Kontrollen ermöglichen, wenn Objekte anhand des fehlenden Originaltags eindeutig als Fälschung identifiziert werden können. Ähnliches gilt für den Diebstahl von Originalteilen, die anhand ihrer Seriennummer eindeutig als gestohlen erkannt werden können.

- **Logistikdienstleister**: Der Logistikdienstleister führt den Transport des fertigen Fahrzeugs vom Fahrzeughersteller zum Händler durch. Die Fahrzeugdaten werden vorab vom OEM avisiert, so dass schon bei der Übernahme des Fahrzeugs eine Plausibilitätsprüfung mittels RFID-Istdaten erfolgen kann, um Folgefehler zu vermeiden. Der LDL setzt die RFID-Technologie verstärkt zur Prozesssteuerung ein. Dazu werden neben der Fahrgestellnummer auch weitere fahrzeugspezifische Daten wie z.B. Modellcode, Farbcode, Schlüsselnummer, Fahrzeugtyp (Kundenfahrzeug, Technikfahrzeug, Lagerfahrzeug) sowie Informationen über den logistischen Prozess wie z.B. vorzunehmende Umbauten (Sitze tauschen), Lieferung (an Kunden, Händler), Lieferdatum, Priorität und der aktuelle Prozesszustand auf den Tags hinterlegt. Diese Daten ermöglichen nicht nur eine effiziente Prozessabwicklung, sondern im Vergleich zu nicht-RFID-gestützten Prozessen auch genauere Prognosen des Auslieferungszeitpunkts an den Endkunden.
  Die RFID-Technologie erlaubt dem LDL in Verbindung mit GPS-Daten darüber hinaus eine ständige Fahrzeuglokalisierung auf seinem Betriebsgelände. Die Ermittlung des genauen Fahrzeugstandorts stellt eine wichtige Voraussetzung für ein effizientes Fahrzeugmanagement dar, wenn das Fahrzeug im Zuge des logistischen Prozesses mehrmals bewegt werden muss.
- **Händler**: Der Händler erzeugt beim Eintreffen der Lieferung eine Online-Anlieferungsmeldung und übermittelt sie an den Fahrzeughersteller. Dies ermöglicht eine frühzeitige Rechnungslegung. Es schließt sich die Übergabe des Fahrzeugs an den Endkunden an.
- **Werkstatt**: In einer Werkstatt werden Wartungen und Reparaturen des Motors und anderer Bauteile vorgenommen. Im Rahmen der Wartung können die Werkstattangestellten vom RFID-Einsatz zur Kennzeichnung aller Bauteile profitieren, da sie so eine genaue Kenntnis der Fahrzeugkonfiguration besitzen. Dies ermöglicht u.a. eine genaue Altersbestimmung sicherheitsrelevanter Bauteile, so dass diese ggf. ausgetauscht werden können, bevor Verschleißerscheinungen auftreten. Weiterhin können die Werkstattmitarbeiter überprüfen, ob es sich um Originalbauteile handelt. Jeder Wartungseingriff wird durch eine Aktualisierung der Daten auf dem Tag des betreffenden Objekts abgeschlossen.
- **Recycling- und Entsorgungsbetriebe**: Als letzte Stufe der Wertschöpfungskette sorgen Recycling- und Entsorgungsbetriebe dafür, dass die verwendeten Rohstoffe einer ordnungsgemäßen Entsorgung zugeführt werden. Auch hier kann aus der RFID-Technologie Nutzen gezogen werden: Der Hersteller des Motorblocks hat dessen Tag mit den Informationen versehen, die nötig sind, um eine stoffliche Identifikation zum sortenreinen Trennen zu ermöglichen. Er trägt damit der EU-Richtlinie 2000/53/EG Rechnung, die besagt, dass „bei der Konstruktion und Produktion von neuen Fahrzeugen der Demontage, Wiederverwendung und Verwertung, insbesondere dem Recycling, von Altfahrzeugen, ihren Bauteilen und Werkstoffen umfassend Rechnung getragen wird und diese Tätigkeiten erleichtert werden“ [eu2000]. Ziel nach Artikel 8 ist eine Wiederverwendungs- und Verwertungsquote bei allen Altfahrzeugen von mindestens 85% ab 2006 und 95% im Jahr 2015.

Bislang handelt es sich beim RFID-Einsatz in der Automobilindustrie nur um Insellösungen entweder innerhalb eines OEMs oder zwischen einem OEM und einem Zulieferer. Ein Szenario, das alle Teilnehmer der Lieferkette abdeckt, ist bisher nicht umgesetzt worden. Aus diesem Grunde werden noch einmal die wesentlichen Voraussetzungen für den liefer-

ketten-übergreifenden Einsatz der RFID-Technologie zusammengefasst, um anschließend die fehlenden Voraussetzungen zu nennen, die einen lieferketten-übergreifenden Einsatz der RFID-Technologie derzeit noch verhindern.

Voraussetzungen für einen umfassenden Einsatz der RFID-Technologie

Gemeinsame Daten- und Kommunikationsstandards sind eine wesentliche Grundlage für einen effizienten Informationsaustausch zwischen den einzelnen Gliedern der Lieferkette. Die Anforderungen an Kompatibilität und Interoperabilität sind abhängig von dem Speicherort der prozessrelevanten Daten. Werden diese auf dem RFID-Tag selbst gespeichert (eine ausreichende Speicherkapazität vorausgesetzt), stellen sich deutlich andere Anforderungen an den Prozessaufbau als bei der Speicherung der korrespondierenden Daten in einem Backend-System. So ist neben der Zusammenarbeit von verschiedenen RFID-Tags und Lesegeräten auch das Verfahren für die Speicherung und Verarbeitung der betroffenen Daten festzulegen (technische Umsetzungen, unterschiedliche schon vorhandene Nummerierungssysteme). Entsprechende Vorgaben für die Einführung und Standardisierung der RFID-Technologie in der Automobilindustrie könnten von den OEMs bzw. von den internationalen und nationalen Automobilverbänden kommen. Ein aktuelles Beispiel für eine solche Vorgabe ist die obengenannte VDA-Empfehlung [vda5501].

Der Erfüllung dieser Voraussetzungen stehen bislang zwei Hindernisse entgegen:

1. Die betrachteten Anwendungsszenarien (4.1.1 und 4.1.2) spiegeln den Stand der Verbreitung der RFID-Technologie in der Automobilproduktion wider. Jedes dieser Szenarien stellt eine Insellösung dar, und dies ist repräsentativ für den generellen Einsatz von RFID-Technologie in der Automobilproduktion. In diesen Insellösungen wird eine spezielle, für die Prozesse ausgewählte, proprietäre RFID-Hardware verwendet. Diese ist an die individuellen Bedingungen der Prozesse gut angepasst, die Interoperabilität zu anderen Systemen wurde bei der Auswahl in den einzelnen Szenarien jedoch so gut wie nicht berücksichtigt. Für die Anforderungen einer Insellösung ist dies auch nicht von prozesskritischer Bedeutung.
2. Gerade Logistikdienstleister mit ihrer Erfahrung aus der Praxis und in diesem Bereich tätige Forschungsgruppen gehen weder von einer Konvergenz der eingesetzten Technologien noch von der Bildung eines einheitlichen oder gar standardisierten Informationsaustausches aus [uckelmann06]. Dies ist umso überraschender, da gerade die Automobilhersteller in der Vergangenheit neue Standards rasch eingeführt und umgesetzt haben (Beispiel: Spezifikation von Versandetiketten nach GM 1724 [gm2001]). Schon heute befinden sich große Mengen (50-100) verschiedener Variationen des Barcodes im Einsatz. Diese sind alle mit derselben Lesegerät-Hardware lesbar, jedoch unterscheiden sie sich beispielsweise in ihrer Datenstruktur, dem Nummerierungssystem und dem Identifikationssystem. Bei der Entwicklung der RFID-Technologie wird erwartet, dass zu der Datenstruktur-Vielfalt, die bereits erfahrungsgemäß auftreten kann, eine vergleichbare Vielfalt an RFID-Tags kommt, die den lieferketten-übergreifenden Einsatz durch inkompatible RFID-Komponenten erschweren wird.

4.2 Sicherheitsanforderungen der Automobilproduktion

Bevor auf die Sicherheitsanforderungen an RFID-Systeme in der Automobilindustrie eingegangen wird, werden zunächst verschiedene Angriffszenarien beschrieben, die für einen Einsatz der RFID-Technologie in der Automobilproduktion charakteristisch sind. Hierfür wird auf die in den Abschnitten 4.1.1 und 4.1.2 beschriebenen Einsatzszenarien sowie auf das lieferketten-übergreifende Szenario Bezug genommen. Die beschriebenen Einsatzszenarien stellen insbesondere einen praktischen Ausschnitt aus einer Lieferkette und einem Fertigungsprozess in der Automobilindustrie dar. Weiterhin ist hier zu beachten, dass sich die in Abschnitt 3.1.1 aufgeführten generischen Angriffsmethoden in unterschiedlichem Maße auf ein Szenario aus dem Gebiet „Produktion“ anwenden lassen.

4.2.1 Anwendungsspezifische Angriffsszenarien

Angriffsszenario 1: Frequenzbandstörung des RF-Mediums

Die Verbindung über die Luftschnittstelle kann absichtlich oder unabsichtlich gestört werden.
Problem: Es besteht die Möglichkeit, dass ein Angreifer die Funktionsfähigkeit des Funkmediums, über das die Lesegeräte und Tags miteinander kommunizieren, aktiv durch einen Störsender zu beeinflussen versucht. Dabei sind insbesondere passive Tags mit ihrer eingeschränkten Leistungsfähigkeit bedroht. Bereits ein genügend starkes White Noise Signal kann in bestimmten Anwendungsgebieten die RFID-Infrastruktur zum Erliegen bringen. Ein Beispiel dafür ist die Lokalisierung von Fahrzeugen auf einem Lagerplatz unter freiem Himmel, wie es bei DaimlerChrysler in Rastatt der Fall ist. Die zugrunde liegenden Motivationen können dabei von reiner Zerstörungslust (Vandalismus) bis hin zur zeitlich gezielten Unterbrechung von Produktionsprozessen reichen (Sabotage). Als Angreifer könnten sowohl externe Personen als auch interne Mitarbeiter in Frage kommen. Sich umfassend gegen einen solchen Angriff zu schützen ist mit einem hohen Aufwand verbunden.
Lösungsansatz: In der Regel gilt, dass eine entsprechende Abschirmung der Einsatzgebiete vor externen Störquellen schützen kann. Interne Sicherheitskontrollen, u.a. auch durch eine kontinuierlich unterstützende Qualitätssicherung, können Störquellen im Inneren der Einsatzgebiete schon im Vorfeld bzw. frühzeitig nach dem Auftreten erkennen. Entsprechende Kontrollmechanismen können bereits in die RFID-Hardware integriert sein.

Angriffsszenario 2: Verfälschen von prozessinternen Informationen

Ein Angreifer könnte beispielsweise sein eigenes Lese-/Schreibgerät in einen RFID-gestützten Produktionsprozess einbringen und eine virtuelle Baukarte mit manipulierten, aber vermeintlich plausiblen Produktdaten (Bremsentest ok, obwohl der Test nicht bestanden wurde) beschreiben. Auch könnte ein Angreifer in einem JIS-Prozess eigene manipulierte Daten einschleusen und so eine unerwünschte Vertauschung der Reihenfolge der Bauteile erzwingen (vgl. DaimlerChrysler-Szenario in Bremen). Dies führt dann letztendlich zu einem Verbaufehler (Sabotage).
Problem: Es fehlen geeignete Methoden für die Authentisierung.

Lösungsansatz: Weil im Falle der virtuellen Baukarte prozesskritische Daten auf den Tags gespeichert werden, sind starke Verfahren zur Authentisierung von Lesegeräten wie z.B. Challenge-Response-Protokolle (siehe Abschnitt 3.2.3) einzusetzen.

Angriffsszenario 3: Unautorisiertes Lesen von Produktdaten in der Lieferkette

Auf einem Tag könnten z.B. für das Recycling relevante Produktdaten gespeichert sein. Andererseits dürfen die Mitarbeiter des Logistikdienstleisters nicht unautorisiert lesenden Zugriff auf diese Daten haben.
Problem: Partner der Lieferkette erhalten unautorisiert Zugriff auf Tagdaten.
Lösungsansatz: Es sind geeignete (starke) Verfahren für die Authentisierung gegenüber dem Tag erforderlich. Darüber hinaus ist im Rahmen einer Lieferkette ein differenzierbarer Zugriffsschutz notwendig.

Angriffsszenario 4: Nutzen von Sicherheitslücken in Betriebssystem und Middleware

In einer Produktionshalle sind alle RFID-Lesegeräte mit der gleichen Systemsoftware ausgestattet. Das Betriebssystem besitzt eine Sicherheitslücke (Pufferüberlauf). Ein Angreifer nutzt diese Sicherheitslücke für einen Zugriff auf das Backend aus.
Problem: Die Betriebssysteme der eingesetzten RFID-Hardware (wie z.B. RFID-Lesegeräte, Gate-Controller), aber auch die RFID-Middleware können Ziele von Angriffen werden; dies wird umso wichtiger, wenn standardisierte RFID-Systeme eine immer weitere Verbreitung finden. Insbesondere können solche Betriebssysteme ebenso wie die auf gebräuchlichen PCs verwendeten Betriebssysteme und die RFID-Middleware Sicherheitslücken aufweisen. Das Problem verstärkt sich dadurch, dass sich Angriffe auch ungezielt gegen ein RFID-System richten können, indem durch Malware automatische Verbreitungsroutinen verwendet werden. Potentielle Angriffsziele dieser Malware könnten auch die im Einsatz befindlichen Betriebssysteme der RFID-Hardware sein.
Lösungsansatz: Durch die Anbindung an ein Backend-System über ein (möglicherweise auch drahtloses) Datennetz sollten RFID-Lesegeräte den gleichen oder restriktiveren Sicherheitsrichtlinien unterliegen wie Arbeitsplatzsysteme. Da die interne Kommunikation des RFID-Systems gezielt auf die verwendeten Protokollschichten eingegrenzt werden kann, sollten entsprechende Filtersysteme auf Netzebene eingesetzt werden. Es empfiehlt sich auch für den Betrieb von Betriebssystem-Software eine Qualitätssicherung durchzuführen, die den Ist-Zustand des Schutzgrades vor aktuellen Angriffsmethoden prüft und analog neue Softwareversionen im Vorfeld auf Verwundbarkeiten testet.
Für die RFID-Middleware gelten ähnliche Bemerkungen wie für die Betriebssysteme, d.h. es muss eine entsprechende Qualitätssicherung der Middleware gewährleistet sein. Dies gilt insbesondere, wenn eine spezielle Middleware für den Einsatz in der Automobilproduktion entwickelt werden sollte.

Angriffsszenario 5: Ablösen oder Zerstören von RFID-Tags

Ein RFID-Tag, das außen an einem Objekt angebracht wurde, kann sowohl vorsätzlich als auch unbeabsichtigt abgelöst werden, so dass die Funktionssicherheit des RFID-Systems nicht mehr gewährleistet werden kann.

Problem: Ein Tag, das sich unbemerkt vom Objekt löst kann zu Störungen im Prozessablauf führen. Das Verhindern eines vorsätzlichen Ablösens impliziert automatisch das Verhindern eines unbeabsichtigten Ablösens eines RFID-Tags, ist jedoch auch ungleich aufwendiger.
Abhängig vom Typ eines RFID-Tags kann es schwierig sein, ihn vor Zerstörung zu schützen: So müssen Smartlabels, die auch einen Barcode tragen, an einem visuell ablesbaren Punkt auf dem Objekt angebracht sein. Diese Notwendigkeit macht ein Smartlabel für Bedrohungen und Gefährdungen gleichermaßen verwundbar. So kann ein oberflächlicher Schnitt oder Kratzer ein Smartlabel bereits zerstören.
Lösungsansatz: Je geschützter ein RFID-Tag in ein Objekt integriert ist, desto geringer ist die Verwundbarkeit. Dem steht die gewünschte Erfassungsreichweite entgegen, die für die Funktionsfähigkeit des RFID-Systems vorausgesetzt wird. Im Gegensatz zu einem Smartlabel wäre damit eine Integration von RFID-Tags in Plastikelemente oder sogar metallene Gussteile deutlich sicherer. Um ein RFID-Tag aus einem Objekt zu entfernen, muss dabei je nach Integrationsart das Objekt beschädigt oder sogar zerstört werden. RFID-Tags, die auf diese Weise in ein Objekt eingearbeitet werden, müssen also eine entsprechende Lebensdauer und Verfügbarkeit gewährleisten. Ein Verhältnis von Schutzgrad vor Ablösung bzw. Zerstörung zu Reichweite der RFID-Tags ist je nach Einsatzgebiet abzuwägen.

Angriffsszenario 6: DoS-Angriff durch Blocker-Tags

Ein Angreifer könnte den Produktionsprozess durch Blocker-Tags (siehe Abschnitt 3.2.7) stören. Darüber hinaus könnte ein solcher DoS-Angriff verdeckt durchgeführt werden, so dass dieser in manchen Fällen erst spät erkannt werden kann.
Problem: Vor allem für das Tree-Walking-Antokollisionsverfahren, aber auch für andere Antikollisionsverfahren (z.B. Aloha) können Blocker-Tags entwickelt werden, so dass es grundsätzlich innerhalb eines gegebenen Antikollisionsprotokolles keinen Schutz vor einem solchen Angriff gibt [bsi04].
Lösungsansatz: In jedem Fall sollte als Fail-safe Default eine manuelle Datenerfassung innerhalb des Produktionsprozesses vorgesehen werden (vgl. virtuelle Baukarte in 4.1.2). Ein auf diesen Angriff ausgerichtetes Erkennungssystem könnte den Einsatz von Blocker-Tags zumindest erkennen.

Angriffsszenario 7: Heimliches Tracking von RFID-Tags

In einem PKW befindet sich der in 4.1.3 beschriebene Motorblock mit RFID-Tag, dessen ID sich von Dritten auslesen lassen könnte. Ohne die korrespondierenden Informationen zu der ID lässt sich keine wesentliche Information über den PKW selbst gewinnen. Hat man aber in Erfahrung gebracht, wem der PKW gehört bzw. wer ihn in der Regel fährt, so ist es möglich, über diese ID diese Person(engruppe) implizit zu verfolgen. Bei einer flächendeckenden Verbreitung der RFID-Technologie – gerade von RFID-Lesegeräten – stellt dies eine signifikante Bedrohung dar.
Problem: Bei dem eben geschilderten Szenario handelt es sich um Tracking. Gemäß 3.1.1 versteht man unter dem Begriff „Tracking“ das unbemerkte Auslesen von RFID-Tags mit dem Zweck der heimlichen Profil-Bildung über Meta-Informationen wie z.B. Bewegungsmuster oder Aufenthaltswahrscheinlichkeiten. Ein RFID-Tag, das an ein spezifisches Objekt

gebunden ist, kann implizit nach dem Einbau oder Verkauf auch an andere Objekte gebunden sein, die evtl. kein eigenes RFID-Tag besitzen.
Lösungsansatz: Bei einem lierferketten-übergreifenden Einsatz der RFID-Technologie muss die Verwendung eines Tags im After-Sales-Bereich berücksichtigt werden. Das Auslesen der Tag-ID sollte beschränkt werden, um eine ungewollte Erfassung zu verhindern.

Angriffsszenario 8: Fälschung von Bauteilen/Ersatzteilen

Die RFID-Technologie soll zum Schutz vor Fälschungen von qualitativ hochwertigen Bauteilen verwendet werden. Hierbei wird das Tag fest mit dem Bauteil integriert. Ein Angreifer liest nun mit einem Lesegerät die Tag-ID aus und erzeugt einen Klon dieses Tags. Das Tag wird dann in ein gefälschtes Bauteil eingebaut, das nun als Originalteil angesehen wird.
Problem: Eine physikalische Integration des Tags mit dem Bauteil reicht für einen Echtheitsnachweis von Bauteilen nicht aus.
Lösungsansatz: Es sind auf dem Tag zusätzlich digitale Signaturen zum Nachweis der Authentizität zu verwenden.

Angriffsszenario 9: Man-in-the-middle Attack

Ein RFID-Tag wird unbefugt ausgelesen, und die gewonnenen Daten werden einem RFID-Lesegerät übermittelt, so dass dieses die scheinbar korrekte Auslesung des entsprechenden Tags feststellt. Dies könnte insbesondere in Szenario DC Bremen dazu führen, dass bei der Bereitstellung der Ladungsträger im Staplerpfad ein beladener Ladungsträger als entladen registriert wird. Ein potentieller Angreifer könnte dies evtl. mit sehr geringem Aufwand erreichen, indem er einfach durch geschickte Forcierung von Reflektionen und/oder Verstärkungseffekte geeignete False-Reads provoziert.
Problem: Ein geschicktes Abfangen und späteres Wiedergeben von übertragenen Daten an der Luftschnittstelle kann einem RFID-Lesegerät authentische RFID-Tags vortäuschen.
Lösungsansatz: Eine mögliche Gegenmaßnahme wäre ähnlich wie bei False-Reads die Kombination der RFID-Lesegeräte mit anderen Sensoren (z.B. Drucksensoren, Scanner etc.), die andere Identifikationsmerkmale erfassen.

4.2.2 Anwendungsspezifische Anforderungen

Erkenntnisse aus den zuvor beschriebenen Anwendungsszenarien – einschließlich dem lieferketten-übergreifenden Szenario – und die Lösungsansätze der im vorangegangen Abschnitt beschriebenen Angriffsszenarien führen zu den folgenden Sicherheitsanforderungen. Neben Sicherheitsanforderungen sind in den durchgeführten Interviews durch die Anwendungspartner auch darüber hinausgehende Anforderungen genannt worden. Die Erfahrungen der Anwendungspartner in dieser Studie lassen dabei einheitliche Anforderungen an die einzusetzende Hardware erkennen.

Funktionssicherheit der Tags

Für den automatischen Einsatz ist die Funktionssicherheit des gesamten Systems kritisch. Dabei ist dem Auftreten von Fehlern möglichst vorzubeugen bzw. das Auftreten von Fehlfunktionen frühzeitig zu erkennen. Ansonsten könnte es evtl. zu einem Bandstopp kommen.

Ein automatisches Auslesen von RFID-Tags setzt die vollständige Funktionsfähigkeit aller sich im Einsatz befindlichen RFID-Tags voraus. Diese Notwendigkeit lässt sich an einem einfachen Beispiel verdeutlichen: Passiert ein mit einem Tag versehener Ladungsträger einen Kontrollpunkt mit einem RFID-Lesegerät (Gate), so soll das Tag an diesem Punkt ausgelesen werden können. Ist das Tag jedoch defekt oder wird durch einen internen Funktionsfehler nicht als ein solches erkannt, wird der entsprechende Ladungsträger nicht mehr beim Passieren eines Gates erfasst. Um die Funktionsfähigkeit der RFID-Tags zu gewährleisten, sind Plausibilitätsprüfungen notwendig.
Im DaimlerChrysler-Werk in Bremen werden an einem Ladungsträger zwei RFID-Tags angebracht – ähnlich wie es in der VDA-Empfehlung [vda5501] vorgeschlagen wird. Diese haben jeweils individuelle IDs, jedoch identische User-Daten bzw. sind mit denselben Prozess-Daten im Backend-System verknüpft. Durch diese Redundanz lässt sich der Ausfall eines RFID-Tags kompensieren. Für die Prüfung der Funktionsfähigkeit müssen Punkte innerhalb des Prozessverlaufs identifiziert werden, an denen eine gleichzeitige Erfassung beider Tags möglich ist. Bei zuverlässiger Erfassung können so automatisch Prozessentscheidungen gefällt werden, die den Austausch eines fehlerhaften Tags einleiten.
Konventionelle Durchfahrtserfassungen wie Lichtschranken, Induktions- oder Drucksensoren können je nach Prozessgestaltung ebenfalls das Erkennen eines Tagausfalls unterstützen.

Funktionssicherheit der Lesegeräte

Häufig sind an die Erfassung von Tags durch die Lesegeräte Prozesssteuerungsentscheidungen gebunden, die z.B. Staplerfahrer in Form von Ampeln oder akustischen Signalen im Prozessverlauf unterstützen (DaimlerChrysler-Werk in Bremen). Um diese Anforderung zu erfüllen, sind ebenfalls die schon zuvor erwähnten Kontrollmechanismen zur Durchfahrtserfassung hilfreich. Eine weitere Möglichkeit, die Funktionsfähigkeit der Lesegeräte zu überprüfen, besteht darin, in einen automatischen Prozesskreislauf Kontroll-Tags zu integrieren. Diese Kontroll-Tags durchlaufen wie andere Objekte den Prozess, jedoch mit dem Unterschied, dass sie nicht an prozessrelevante Objekte gebunden sind. Bleibt die Erfassung eines Kontroll-Tags zu einem definierten Zeitpunkt oder Intervall aus, so liegt ein Fehler vor. In der Praxis konnte darüber hinaus festgestellt werden, dass der Energieverbrauch eines Lesegerätes vor dem Versagen signifikant ansteigt. Dies ließe sich als Indikator für Wartungen verwenden [uckelmann06].

Industrietauglichkeit der Lesegeräte

Um für den Einsatz im Produktions- und Logistikumfeld einsetzbar zu sein, müssen die RFID-Lesegeräte industrietauglich sein. Bei einer festen Installation muss die Gestaltung der Lesegeräte eine sichere Installationsmöglichkeit für Strom- und Datennetze bieten. Dabei dürfen keinesfalls externe Netzteile erforderlich sein. Die Gehäuse der Lesegeräte müssen den jeweiligen Bedingungen gerecht werden: So sollten die Lesegeräte auf Staplerpfaden auch vereinzelten Kollisionen standhalten. Dies bezieht sich insbesondere auf die Verankerung.

Ein weiterer Aspekt der Industrietauglichkeit ist die Geschwindigkeit, mit der auf einem RFID-Tag gespeicherte Daten ausgelesen werden können. Analog gilt dies für die Schreibgeschwindigkeit. Den Angaben der VDA-Empfehlung 5501 [vda5501] nach ist eine Übertragungsgeschwindigkeit von 50-80 KBit/Sekunde (UHF) realistisch. Diese Angaben beziehen

sich auf eine Durchfahrtsgeschwindigkeit von 0-6 m/s. Ist die Durchfahrtsgeschwindigkeit höher, können Lesefehler durch frequenzbedingte Erfassungslücken entstehen. In der Praxis variiert die Dauer des Auslesens und kann unter den Werten liegen, die in der VDA-Empfehlungen angenommen werden (so kamen in einem Einzelfall 3-5 Sekunden Auslesedauer bei 10KBit Daten zustande [uckelmann06]). Aufgrund der schnellen Entwicklung in diesem Sektor lassen sich nur schwierig Aussagen über die Qualität einzelner Produkte fällen, da z.B. auf der Seite des Lesegerätes schon eine neuere Version der Firmware sowohl zu Verbesserungen als auch zu Verschlechterungen führen kann. Daher sollte die verwendete Hardware einer ständigen Qualitätssicherung unterliegen, die die Auswirkungen von Software-Updates und Hardware-Upgrades auf die Funktionssicherheit im Vorfeld untersucht.

Für einen flexiblen Einsatz von RFID-Lesegeräten, wieder unter der besonderen Ausgangslage der Integration in bestehende Prozesse, ist auch eine sichere Anbindung der Lesegeräte (sowohl transportabel als auch fest installiert) an das Backend notwendig. Dies gilt umso mehr, wenn eine kabellose Datenübertragung z.B. WLAN verwendet wird. Hier ist (ebenso wie bei der generellen Störanfälligkeit der Funkverbindung) auf eine überschneidungsfreie Integration mit bereits vorhandenen Funknetzen zu achten, um eine angemessene Verfügbarkeit gewährleisten zu können.

Vermeidung von False-Reads

Unter „False-Reads“ versteht man das unbeabsichtigte Auslesen von RFID-Tags. Reflektionen und Verstärkungseffekte durch metallische Oberflächen können dazu führen, dass auch räumlich weit entfernte Tags durch ein Lesegerät unbeabsichtigt erfasst werden. Da gerade die räumliche Nähe ein wesentliches Kriterium für die Erfassung von RFID-Tags ist, kann ein solches Phänomen den Prozessablauf stören. Gerade wenn keine einheitliche Störquelle für auftretende False-Reads identifizierbar ist, ist eine gute Abschirmung der Lesegeräte empfehlenswert. Auch eine Anpassung der Sende- bzw. Empfangsleistung der Antennen kann ein solches Problem reduzieren.

Geringe Störanfälligkeit der Funkverbindung

Abhängig vom eingesetzten Frequenzband sind Störquellen für die eingesetzte RFID-Technik zu identifizieren und ggf. entsprechend zu schirmen. Ein typischer Einsatzort für RFID-Gates sind z.B. Durchfahrtstore. Diese werden häufig von schnell öffnenden Rolltoren geschlossen, die durch Elektromotoren angetrieben werden. Sensoren erkennen dabei sich nähernde Fahrzeuge oder Personen und öffnen das entsprechende Tor. Bei der Durchfahrt sollen schließlich RFID-Tags ausgelesen werden. Jedoch ist es möglich, dass eine schlecht abgeschirmte Elektrik in den Motoren oder die eingesetzte Sensortechnik das Frequenzband des RFID-Mediums stört. Dies geschieht nur dann, wenn ein Tag das Tor passiert, und ist daher leichter bei der Erfassung von Störquellen zu übersehen.

Bei kabellosen Übertragungsmedien wie WLAN (z.B. nach den Standards IEEE 802.11b/g) oder Bluetooth (nach IEEE 802.15.1) ist darauf zu achten, dass Kanäle zu wählen sind, die sich möglichst nicht mit den eingesetzten RFID-Frequenzen überschneiden. Ist eine Überschneidung nicht zu vermeiden, sollten alternative Technologien in einem weniger genutzten Frequenzband in Erwägung gezogen werden wie z.B. IEEE 802.11a/h mit dem Frequenzband 5 GHz. Eine räumliche Trennung liefert keinen zuverlässigen Schutz vor Störungen, da gerade die im Produktionssektor häufig anzutreffenden metallischen

Oberflächen zu unvorhersehbaren Reflektionen oder sogar Verstärkungseffekten führen können.

Ausreichende Datenübertragungsrate

Die Datenübertragungsrate über das Funkmedium ist von zahlreichen Faktoren abhängig:

- Lesen oder Schreiben von Daten,
- Durchfahrtsgeschwindigkeit,
- Anzahl der Tags, die das Gate pro Sekunde passieren (Pulk),
- Anordnung der Tags auf den Objekten,
- Gegenseitige Beeinflussung der Tags,
- Größe der zu übertragenen Datenmenge,
- Entfernung der Tags zu den Lesegeräten,
- Zahl der Lesegeräte an einem Gate,
- potentielle Störungen des Funkmediums,
- Beschaffenheit des Objekts.

Aus diesem Grund gibt es verschiedene Möglichkeiten, eine für den Prozessablauf ausreichende Datenübertragungsrate sicherzustellen. Durch eine gezielte Veränderung einiger dieser Faktoren können schon mit geringem Aufwand die gewünschten Anforderungen erfüllt werden. Ebenso kann jedoch eine Veränderung bereits eines dieser Faktoren zu einer signifikanten Verschlechterung führen, so dass auch hier eine kontinuierliche Qualitätssicherung empfehlenswert wäre.

Zugriffskontrolle

Sichten und Rollen [Sandhu96] sind zusammen mit entsprechenden Mechanismen für die Authentisierung ein wichtiges Instrument, um Sicherheits- und Datenschutzanforderungen umzusetzen. Zur Veranschaulichung wird dies im Folgenden an einem Beispiel verdeutlicht: Seit dem 24. März 2005 gilt das neue Elektro- und Elektronikgerätegesetz (ElektroG) [bmu05]. Komponenten wie GPS-Displays oder auch Motorenelektronik können bis zu einem bestimmten Grad unter dieses Gesetz fallen. Dafür müssen produktspezifische Daten nachgewiesen und der Lebenszyklus von entsprechenden Einzelteilen dokumentiert werden. Diese Informationen können ebenso wie die Nutzdaten im USER-Bereich eines RFID-Tags gespeichert werden (siehe Abschnitt 4.1.3) [vda5501], wobei ein Teil des USER-Bereichs fest vordefiniert und ein freier Block für individuelle unter den Prozess-Partnern abgestimmte Daten vorgesehen ist. Anders als bei den Recycling-Informationen für Altfahrzeuge [eu2000] gibt es also für Daten, die das ElektroG betreffen, im USER-Bereich keinen vordefinierten Block, so dass diese im freien Block des USER-Bereichs gespeichert werden müssten.
Je nach Anwendungsfall können Daten wie die das ElektroG betreffende Informationen vertraulich sein, so dass manche Prozess-Teilnehmer diese Daten nicht auslesen dürfen. Für andere Prozess-Teilnehmer dienen diese Daten aber gerade zur Unterstützung des Prozessablaufs, so dass ein Zugriff auf diese Daten hier erforderlich ist. Für den Zugriff auf den USER-Block ist jedoch bislang kein Rollenkonzept realisiert. Eine differenzierbare Zugriffskontrolle wäre also an dieser Stelle wünschenswert.
Die in [vda5501] vorgeschlagenen Daten im USER-Block sind nur über ein Access-Passwort zugreifbar. Jedoch ist der Inhalt dieser individuellen Datenfelder nicht weiter differenzierbar. Das Prinzip der Vertraulichkeit ist insofern erfüllt, als dass bei entsprechender Verschlüsselung und der Wahl eines als sicher geltenden Access-Passwortes nur autorisierte Prozess-

partner auf den USER-Bereich zugreifen können. Es ist dagegen nicht möglich, auf Sichten oder Rollen basierende Zugriffe auf das RFID-Tag durchzuführen, so dass weitere Prozesspartner z.B. nicht auf das ElektroG betreffende Informationen im Einzelnen zugreifen können. Es gibt nur die Möglichkeit, den gesamten Inhalt des USER-Blocks offenzulegen oder den Block zu sperren (Schwarz-Weiß-Zugriffsrechte). Dies kann gerade dann eine Bedrohung darstellen, wenn aus Flexibilitätsgründen neben vertraulichen Daten auch öffentliche Daten in dem freien Block abgelegt werden sollen.

Vertraulichkeit als Schutz vor Spionage

Auf den RFID-Tags selbst werden keine vertraulichen Daten gespeichert. Erst die Assoziation der RFID-Tags mit den entsprechenden Datagrammen der Firma Lear stellt eine gewisse vertrauliche Information dar. Die Informationen dienen der Steuerung und Kontrolle innerhalb des geschlossenen Kreislaufs von Ladungsträgern, die Just-In-Time (bzw. Just-In-Sequence) bestückt werden. Dabei sind sowohl die Daten selbst als auch die daraus möglicherweise ableitbaren Informationen (Inferenz) unkritisch.
Werden bei einem komplexen lieferketten-übergreifenden Datenaustausch auch vertrauliche Daten übertragen, so sind angemessene Authentisierungs- und Verschlüsselungsmechanismen notwendig. Dies gilt, wenn das Übertragungsmedium abgehört werden kann (Kommunikation über das Backend- oder RF-Medium), aber auch, wenn das Speicherungsmedium in den Besitz eines Angreifers kommen kann (RFID-Tag). Ein erfolgreicher Spionage-Angriff lässt sich nur schwierig entdecken; aber schon ein Sicherheitskonzept mit verhältnismäßig geringem Aufwand, das dafür ganzheitlich umgesetzt ist, reduziert die Angriffsfläche für eine Spionage signifikant.
Im Gegensatz dazu lassen sich Sabotage-Angriffe besser identifizieren, aber auch schwieriger verhindern. Der Aufwand, sich gegen Sabotage, zu schützen ist nur schwer kalkulierbar und widerspricht der aus den bisherigen Erfahrungen gewonnenen Wahrscheinlichkeit einer Bedrohung. Diese wird von den Anwendungspartnern als gering eingeschätzt.

Integrität der Daten

Ohne Gewährleistung der Datenintegrität kann es geschehen, dass Ladungsträger nicht den betreffenden Prozesszyklen zugeordnet werden könnten oder unbemerkt in einer falschen Sequenz laufen. Da die Verbauprozesse zeitkritisch ablaufen, können aus der Sequenz gefallene Ladungsträger nur schwer wieder integriert werden. Im Fall des Szenarios bei DaimlerChrysler in Rastatt könnte falsche Qualitätsdaten über die Airbag-Naht in das RFID-System eingespielt werden, so dass die Datenintegrität auch hier zu gewährleisten ist. Für die Speicherung von Prozessdaten gibt es zwei mögliche Orte:

- auf dem RFID-Tag, wenn auf diesen User-Daten geschrieben werden können, z.B. in den Speicherbereich MB 11 nach [vda5501] und
- im Backend-System über eine Assoziation mit der ID des Tags.

Die Integrität der Daten ist ein prozesskritischer Faktor, da nicht-integre Daten in JIS- und JIT-Prozessen zu Verbaufehlern, Verzögerungen und Ausschleusungen führen können. Die Integrität auf dem RFID-Tag ist besonders durch die Alterung des Tags und durch Umwelteinflüsse, denen das Tag ausgesetzt ist, gefährdet. Die Speicherung von falsch erfassten oder eingepflegten Daten ist dagegen unabhängig vom verwendeten Medium und daher kein RFID spezifisches Problem. Um zu gewährleisten, dass nicht von vornherein

fehlerhafte Tags mit nicht-integren Daten in den Prozess eingeschleust werden, müssen nach dem Beschreiben eines Tags die soeben geschriebenen Daten auf ihre Integrität geprüft werden. Diese Prüfung sollte durch eine entsprechende Prozessanordnung unterstützt und ganzheitlich im Prozessverlauf vorgesehen sein. So wird im DaimlerChrysler-Werk in Rastatt ein integriertes Gerät verwendet, in dem in einem atomaren Ablauf die RFID-Komponenten von Smartlabels beschrieben werden, die geschriebenen Daten wieder gelesen und verifiziert werden und erst nach dieser Prüfung mit dem korrespondierenden Barcode bedruckt werden.

Eine absichtliche Korruption der Daten mit dem Ziel, den Prozessablauf zu stören (z.B. Vertauschen der Reihenfolge bei JIS-Prozessen), ist dagegen deutlich schwieriger zu erkennen. Werden die auf einem Tag gespeicherten Daten auf eine Art und Weise verfälscht, die durch die eingesetzten Kontrollmechanismen als plausibel eingestuft werden, kann so eine proaktive Erkennung untergraben und der Prozessablauf gestört werden. Die Sicherstellung der Datenintegrität ist insbesondere auch beim Einsatz einer virtuellen Baukarte wichtig, die archivierungspflichtige Produktionsdaten verwaltet. Werden beispielsweise Daten über eine fehlerhafte Verbauung (vgl. Tab. 8) auf dem Tag unautorisiert manipuliert oder später beim Archivierungsvorgang manipulierte Daten in das Backend eingespielt, so fällt dieser Angriff möglicherweise nicht sofort auf. Die Auswirkungen eines solchen Angriffs können sich evtl. erst viel später z.B. bei Wartungsarbeiten an einem ausgelieferten Auto bemerkbar machen, wenn auf die archivierungspflichtigen Daten zugegriffen werden soll.
Jeder Schreibzugriff auf Daten darf nur nach einer erfolgreichen Authentisierung erlaubt werden. Daten, die sich im Prozessverlauf nicht mehr ändern oder wiederverwendet werden können, sollten darüber hinaus nicht mehr veränderbar auf das RFID-Tag geschrieben werden können. Je nachdem, an welchem Ort prozessrelevante Informationen gespeichert werden, können unterschiedliche Sicherheitsmaßnahmen einer Verfälschung vorbeugen oder eine Verfälschung frühzeitig erkennen. Bei RFID-Tags sollten neben der Feststellung der korrekten Übertragung der Daten über das Funkmedium auch CRC-Prüfsummen durchgängig zusätzlich zu den Daten gespeichert werden, so dass bei jedem Auslesen automatisch eine Konsistenzprüfung stattfindet. Einen Schutz vor vorsätzlicher Verfälschung kann eine Prüfsumme jedoch nicht gewährleisten, so dass eine vorgeschaltete Authentisierung notwendig ist.
Eine unabhängig im Backend-System geführte Versionskontrolle kann unbemerkte Veränderungen auf den RFID-Tags ebenfalls erschweren, da hier analog zu den eigentlichen Daten auch die getrennt gespeicherten Protokolldaten manipuliert werden müssen. Auf diese Weise lässt sich die Flexibilität der auf dem RFID-Tag gespeicherten Daten mit der Sicherheit der im Backend-System gespeicherten Daten kombinieren.

Plausibilitäts-Prüfungen im Prozessverlauf

Die Integration der RFID-Technologie in bereits bestehende Prozesse könnte durch Eigenschaften der physischen Umgebung Fehler in der Erfassung begünstigen. So wäre es möglich, dass auf den Staplerpfaden oder an Stationen installierte Gates auch umfahren werden können, so dass eine entsprechende Erfassung ausbleibt. Eine neue Strukturierung der Prozesse kann dem entgegenwirken: Einzelne fehlende Erfassungen an Gates dürfen nicht zu einer Prozessverzögerung führen, sondern müssen durch eine angemessene Toleranz und implizite logische Prüfung kompensiert werden. Steht die Funktionsfähigkeit

des Gates nicht in Frage, kann durch weitere Erfassungen geschlossen werden, dass ein Gate umgangen worden ist.
Das Anbringen eines Tags kann bereits durch einen Zulieferer vorgenommen worden sein. In diesem Fall muss prüfbar sein, ob ein RFID-Tag tatsächlich an jedem Objekt (Einzel- oder Pulkerkennung) oder an einem Ladungsträger angebracht ist. Ebenso kann es sein, dass sich mehr als ein RFID-Tag auf dem Objekt befindet. Im Anwendungsszenario im DaimlerChrysler-Werk in Rastatt kam es z.B. vor, dass sich keine oder mehrere übereinander geklebte Smartlabels an dem Objekt befanden. Beides führt zu einer Beeinträchtigung des Prozesses. Da in dem Szenario nachvollzogen werden kann, wann ein Objekt das Lesegerät passiert, ist in diesem Zusammenhang geplant, das Objekt – nachdem es das Lesegerät passiert hat und kein RFID-Tag erkannt worden ist – visuell (per Kamera) auf das Vorhandensein eines Smartlabels zu überprüfen und ggf. auszuschleusen.

Sichere physische Verbindung des Tags mit dem Objekt

In einem Produktionsprozess kann eine Gefährdung darin bestehen, dass sich ein RFID-Tag unabsichtlich vom Objekt ablöst. Gerade bei hoher mechanischer Belastung müssen die RFID-Tags entsprechend sicher an oder in den Objekten angebracht werden. Weitere wichtige Faktoren sind die Oberflächenbeschaffenheit und Umwelteinflüsse. Die Ladungsträger im Anwendungsszenario „DaimlerChrysler, Bremen“ werden mit Staplern von Station zu Station transportiert. Bei diesem Transportprozess können Tags unbeabsichtigt durch Kollisionen, welche die Ladungsträger selbst unbeeinträchtigt überstehen, vom Ladungsträger getrennt werden. Potentielle Kollisionspunkte sollten daher bei der Wahl der Anbringungspunkte berücksichtigt werden.
Um ein RFID-Tag den gesamten Lebenszyklus über mit einem Motorblock zu verbinden, wird bereits an der Einbettung von RFID-Tags in Gussobjekte geforscht. Diese lassen sich nicht wieder ohne invasive Eingriffe aus dem Motorblock entfernen und stellen daher besondere Anforderungen an die Funktionssicherheit [uckelmann06].

Gehärtete Betriebssysteme

Sogenannte speziell gehärtete Betriebssysteme können die Angriffsfläche auf Betriebssystem-Ebene verringern. Sie stellen darum eine geeignete Basis für sensible produktionskritische Systeme mit hohen Schutzanforderungen dar. Die Qualitätssicherung, die die Funktions- und Datensicherheit solcher Betriebssysteme kontinuierlich sicherstellt, wird hierbei meist durch den Anbieter des gehärteten Betriebssystems übernommen und in Form von zeitnahen Sicherheits-Updates über geschützte Kanäle zur Verfügung gestellt.

Bestandsprüfung und Lokalisierung als Schutz vor Diebstahl

Eine durch die RFID-Technologie gestützte Lagerverwaltung ermöglicht eine präzisere Erfassung des Ist-Zustandes und eine Erhöhung der Granularität bei der Erfassung von Events[2] [strassner05]. Mit Hilfe von aktiven RFID-Tags, wie sie z.B. bei der BLG Logistics Group zur Lokalisierung von Fahrzeugen eingesetzt werden, kann darüber hinaus eine unautorisierte Bewegung von Objekten festgestellt werden. Eine automatische Verfolgung von Objekten kann mit passiven RFID-Tags auch abschnittsweise geschehen, wenn dafür eine entsprechende Anzahl von Kontrollpunkten (Gates) vorhanden ist. Eine aktive Lokalisierung ist gerade bei der Auffindung von Werkzeugen hilfreich. Denn sie verringert so die Wegzeiten

[2] Ereignisse, die mit einer Zustandsveränderung assoziiert sind

und erhöht damit die Verlässlichkeit des Prozessablaufs. Die datenschutzrechtlichen Konsequenzen, die sich aus der Verwendung von RFID für die Lokalisierung ergeben, werden weiter unten erörtert.
Bei ungesteuerten Prozessen wie z.B. dem Transport mit Lastkraftwagen kann das Auftreten von Verlusten oder Diebstählen besser eingegrenzt werden, wobei auch hier wieder generelle Lösungsansätze vorbeugen können: Bei einer Kennzeichnung der Ladungsträger statt der Objekte selbst hilft schon eine Versiegelung der Ladungsträger, die Vollständigkeit einer Lieferung schlüssig nachvollziehen zu können.

Schutz vor ungewolltem Tracking

Um einem Tracking von RFID-Tags vorzubeugen, gibt es zwei Ansätze. Der flexiblere, aber auch kostenintensivere Ansatz ist es, das Auslesen einer RFID nur nach einer dem RFID-Tag gegenüber zuvor erfolgreich durchgeführten Authentisierung zuzulassen. Um einem Replay-Angriff vorzubeugen, müssen dazu geeignete Verschlüsselungsmechanismen in den RFID-Komponenten integriert sein. Dieser Vorgang muss bei jedem Erfassen durchgeführt werden, was gerade bei Pulkerfassungen höhere Anforderungen an die Leistung der Hardware stellt.
Ein einfacherer, aber dafür weniger flexibler Ansatz ist das gezielte Deaktivieren eines RFID-Tags. Der Zugriff auf die Tag-ID ist dabei ähnlich der Erfassung eines herkömmlichen RFID-Tags. Der Unterschied besteht darin, dass dem RFID-Tag ein speziell zu autorisierendes Disable-Kommando (ähnlich dem KILL-Kommando) übermittelt wird. Nach Erhalt dieses Kommandos lässt sich das RFID-Tag nicht mehr auslesen. Nur mit Hilfe eines komplementären Enable-Kommandos kann das RFID-Tag wieder aktiviert werden, damit dieses wie zuvor benutzt werden kann [spiekermann04]. Diese Funktion könnte gerade im After-Sale Bereich eingesetzt werden. Wird ein Objekt wieder aus Recycling- oder Wartungsgründen zurückgeführt, lässt sich das RFID-Tag zu diesem Zwecke wieder aktivieren.
Beide Möglichkeiten beugen auch einem heimlichen Profiling durch RFID-Lesegeräte Dritter vor, die ein verbautes Tag für ihren eigenen Nutzen zweckentfremden könnten.

Datenschutz

In den beiden Anwendungsszenarien werden keine personenbezogenen Daten erhoben oder verarbeitet. Jedoch sind die Möglichkeiten der heimlichen Profilerstellung durch Data-Mining auf Prozessdaten, die per RFID in hoher Granularität erhoben wurden, in Assoziation mit den prozessbeteiligten Personen zu prüfen (Wahrung der Transparenz) und entsprechend zu behandeln (z.B. Datentrennung). Im Regelfall gilt, dass betroffene Personen über eine Erhebung und Weiterverarbeitung von personenbezogenen Daten im Vorfeld zu informieren sind. Da die Löschung von auf RFID-Tags gespeicherten personenbezogenen Daten schwierig sicherzustellen ist, sollte ein solches Verfahren vermieden werden.
Das Lokalisieren von Werkzeugen im Zusammenhang mit der Erfassung von Arbeitszeiten kann ebenfalls der Profilbildung dienen und darf nur im Rahmen der Vorgaben durch das Bundesdatenschutzgesetz geschehen. Entsprechende Datenschutzkonzepte sind in Zusammenarbeit mit dem Betriebsrat [bvg06] gemeinsam mit dem verantwortlichen Datenschutzbeauftragten zu entwickeln.

Angemessene Dimensionierung der verwendeten Hardware

Sollen RFID-Lesegeräte in die räumlichen Begebenheiten bestehender Prozesse integriert werden, so müssen sie teilweise hohe Ansprüche an ihren Platzbedarf erfüllen. Da der Auf-

bau vieler Prozesse die Orte für eine RFID-Erfassung einschränkt, wird dies erfahrungsgemäß zu einem Problem. Ist die Dimensionierung eines Lesegerätes zu groß für den Einsatz in einem beengten Bereich, ist dieser bauliche Grund ein Hindernis für den Einsatz von RFID-Technologie. RFID-Lesegeräte sollten sich daher gerade durch ein schlankes Design auszeichnen, das bei auf dem Boden montierten Lesegeräten auch wenig Fläche einnehmen soll. Darüber hinaus sollten sie flexibel einsetzbar oder sogar an individuelle Begebenheiten anpassbar sein, um eine Erfassung des vollständigen Prozesses sicher gewährleisten zu können.

Gewährleistung der Resistenz gegenüber Umwelteinflüssen

Die eingesetzte RFID-Hardware muss gerade im Anwendungsbereich Produktion oftmals beanspruchenden Umwelteinflüssen standhalten. Diese Anforderung bezieht sich sowohl auf die RFID-Lesegeräte als auch auf die RFID-Tags. Da sich die Lesegeräte jedoch durch geschickte Positionierung meist in weniger kritischen Bereichen aufstellen lassen, fällt auf, dass gerade die Tags extremen Umwelteinflüssen ausgesetzt sein können. Um einen Schutzstandard gegen das Eindringen von Fremdkörpern in ein Gerät zu definieren, gibt es die Schutzarten nach EN 60529/IEC 529. Für den Einsatz im RFID-Bereich sind die Schutzarten IP67 und IP69K interessant. Erstere wird auch von der VDA 5501 empfohlen. ‚IP' steht in diesem Zusammenhang für „Ingress Protection", die erste Ziffer für den Schutzgrad gegenüber dem Eindringen von Fremdkörpern und die zweite Ziffer für den Schutzgrad gegen das Eindringen von Wasser:

- Schutz gegen das Eindringen von Fremdkörpern:
  - Niedrigster Grad: 0 (kein Schutz)
  - Höchster Grad: 6 (kein Eindringen von Staub bei einem Unterdruck von 20 mbar im Gehäuse)
- Schutzart im Hinblick auf schädliche Einflüsse von Wasser:
  - Niedrigster Grad: 0 (kein Schutz)
  - Mittlere Grade: 7 (Schutz vor Wirkungen beim zeitweiligen Untertauchen in Wasser bei einer Eintauchtiefe von 0,15 - 1m und einer Eintauchzeit von einer Minute), 8 (zeitlich unbegrenzter Betrieb unter Wasser)
  - Höchster Grad: 9K (Schutz vor Wasser bei Hochdruck und Dampfstrahlreinigung).

Als deutsche Entsprechung dieser Schutzarten ist die DIN 40050 zu verstehen. Wichtig ist auch zu beachten, dass Schutzarten einander nicht implizieren. So gilt für ein nach IP69K geschütztes Gehäuse nicht implizit der Schutz nach IP68. Hierfür müssten beide Schutzarten unabhängig voneinander gewährleistet sein.
Die zuvor erwähnten Schutzarten beziehen sich nur auf den schädlichen Einfluss von Wasser. Der Schutzgrad gegen chemischen Lösungs- und Reinigungsmitteln ist über sie nicht definiert.
Bei der Beständigkeit gegen extreme Temperaturen ist zu berücksichtigen, dass auch die durch ein Gehäuse geschützte Elektronik die im Innenraum eines RFID-Tags herrschenden Temperaturen übersteht. Unter Umständen ist eine maximale Zeitspanne zu definieren, der ein Tag einer extremen Umweltbedingung ausgesetzt sein darf, um eine Mindestlebensdauer zu gewährleisten. Die Belastung durch kontinuierliche zyklische Temperaturwechsel, wie es z.B. bei der Durchfahrt eines Ladungsträgers durch einen Ofen für die Trocknung des Karosserielacks der Fall ist, kann die Lebensdauer eines Tags signifikant verkürzen. Gerade für solche Umweltbedingungen ausgelegte RFID-Tags zeichnen sich jedoch durch hohe An-

schaffungskosten aus, die einem regelmäßigen prophylaktischen Austausch entgegenstehen.

4.2.3 Einschätzungen der Anwendungspartner

Die praktischen Erfahrungen der Anwendungspartner im Betrieb der RFID-Technologie haben zu einer einheitlichen Einschätzung der Bedrohungen und der Sicherheitsanforderungen geführt. Die Anforderungen an die Sicherheit sind dabei aber unterschiedlich stark gewichtet.

Funktionssicherheit

Eine hohe Bedeutung wird der Funktionssicherheit beigemessen: der Gewährleistung des ungestörten und erwartungskonformen Ablaufs aller Produktionsprozesse (die Ist-Funktionalität entspricht der Soll-Funktionalität [eckert04]). Diese ist gerade in der stark effizienzorientierten Automobilproduktion ein primäres Leitziel. Der Nutzen des Einsatzes der RFID-Technologie wird daher kontinuierlich an bereits stark optimierten Prozessabläufen gemessen. Zum einen muss die eingesetzte RFID-Technologie die bestehenden Sicherheitsstandards erfüllen, zum anderen eine Verbesserung der Prozessabläufe garantieren, die die Investitionen in die RFID-Technologie stützt. Dabei ist auch der kurzfristige Nutzen von entscheidender Bedeutung. Die Annahme, dass langfristig die Verbreitung des Einsatzes der RFID-Technolgie die Investitionen rentabel macht, wird eher verhalten aufgenommen. Vielmehr steht bislang die von Fall zu Fall individuelle Verbesserung von Prozessabläufen im Vordergrund. So machen menschliche Fehler einen wesentlichen Teil der in einem Prozess bekannten Fehlerquellen aus. Diese verspricht man sich durch den Einsatz von RFID-Systemen zu reduzieren, da durch die RFID-Technologie eine umfassende automatische Prüfung der Prozessabschnitte ermöglicht werden kann. Um diese Fehlerquelle zu verringern, wird allerdings eine entsprechende Schulung des an einem Prozess beteiligten Personals durchaus als Alternative erachtet.
Eine vollständige Automatisierung einzelner Prozesse ist langfristig ebenfalls von Interesse. Diese wird aber von den Befragten bislang noch als unrealistisch erachtet. In vielen Fällen stehen dieser die Sicherheitsanforderungen internationaler Zertifizierungen entgegen. Diese fordern für jeden automatischen Prozess eine entsprechende nicht-automatische Ausweichlösung, die die Aufrechterhaltung der Prozesse im Notfall gewährleistet.

Informationssicherheit

Im Gegensatz dazu wird der Bereich der Informationssicherheit (in Bezug auf eine unautorisierte Daten- und Informationsgewinnung sowie Informationsveränderung) deutlich geringer gewichtet. Der Nutzen eines potentiellen Angriffs auf das durch die RFID-Technologie gestützte System ist für die Anwendungspartner nur schwer ersichtlich: Da es sich um eine geschlossene Prozesskette mit geringer Angriffsfläche handelt, sind die bislang auf dem RFID-Tag oder über das Backend verarbeiteten Daten laut Anwendungspartner kaum durch externe Angreifer gefährdet. Die verbleibende Angriffsmöglichkeit aus dem Inneren heraus wird durch die fehlende Relevanz der Dateninhalte abgeschwächt. So gelten prozessinterne Daten zwar als kritisch für die Funktionssicherheit des Prozessablaufs, jedoch inhaltlich als wenig geheimhaltungswürdig. So verbleiben RFID-Tags teilweise über

den Prozess hinaus ohne weitere geplante prozessrelevante Verwendung innerhalb eines Automobilteils. Die Tags werden dabei nicht unbrauchbar gemacht und enthalten auch nach der Auslieferung an den Handel noch die prozessinternen Informationen (siehe 4.1.2).
Generell gehen die Anwendungspartner davon aus, dass es für einen Angreifer deutlich attraktivere Ziele als die durch RFID-Technologie gestützten Prozesse gibt. Vandalismus ist dabei eine Bedrohung, die von den Anwendungspartnern wahrgenommen wird. Es handelt sich dabei aber nicht um ein RFID-spezifisches Problem und wird in seiner Priorität den Erfahrungswerten in anderen Bereichen entsprechend niedrig angesiedelt. Dabei wird die gezielte Informationsveränderung durch Sabotage oder Vandalismus zurzeit im Wesentlichen für die signifikante Bedrohung gehalten.
Es ist an dieser Stelle zu berücksichtigen, dass es sich bei den untersuchten Einsatzszenarien bei DaimlerChrysler noch um Pilotprojekte mit dem Ziel handelt, den Nutzen, aber auch die Risiken und Kosten des Einsatzes der RFID-Technologie in der Automobilproduktion besser verstehen zu können. In zukünftigen Projekten größeren Ausmaßes wird sich diese Situation aber ändern, so dass im Rahmen einer tieferen Integration in die Produktionsprozesse auch als vertraulich eingestufte Daten auf den RFID-Tags gespeichert werden. Dies gilt insbesondere, wenn es sich um ein lieferketten-übergreifendes Szenario handelt, in dem die verschiedenen Partner der Lieferkette Zugriff auf bestimmte durch die RFID-Technologie bereitgestellte Produktions- und Fahrzeugdaten erhalten. Bei einem Anschluss des RFID-Systemes an Produktionssysteme wie z.B. an ein Fertigungsleitsystem sind des Weiteren auch die Integrität und die Verfügbarkeit der Daten von hoher Wichtigkeit.

4.3 Sicherheitsmaßnahmen der Automobilindustrie

Aus den zuvor behandelten Angriffen und den daraus resultierenden Sicherheitsanforderungen für den Einsatz von RFID in der Automobilproduktion werden in diesem Abschnitt konkrete Sicherheitsmaßnahmen abgeleitet. Anschließend wird eine kurze Einschätzung der bisherigen Umsetzung dieser Maßnahmen gegeben. Aus bisherigen Defiziten bei der Umsetzung wird dann der Forschungsbedarf im Themengebiet „RFID-Sicherheit in der Automobilproduktion“ identifiziert.

4.3.1 Empfohlene Sicherheitsmaßnahmen

Notfall-Prozeduren

Zurzeit ist für die Gewährleistung der Funktionssicherheit eine Fallback-Möglichkeit von automatischer Prozesssteuerung über RFID-Systeme zu manuellen Methoden zwingend notwendig (fail-safe default). Insbesondere internationale Zertifizierungen setzen dies voraus.
Betrachtet man beispielsweise das Szenario aus dem Werk Bremen, so können falsche oder in einer falschen Reihenfolge eingespielte Tag-IDs zu zusätzlichen manuellen Kontrollen führen. Dies kann die Ausführung des Prozesses verlangsamen. Im Falle der virtuellen Baukarte könnte es in dem Produktionsprozess Abhängigkeiten geben, die den korrekten Eintrag von Daten in die Baukarte voraussetzen. Fehlen diese Informationen, so kann der aktuelle Arbeitsschritt nicht ausgeführt werden, und der Produktionsprozess wird gestört. Die Auswirkung der RFID-Technologie auf die Sicherheit des Produktionsprozesses ist ein wesentlicher, heutzutage noch nicht ausreichend untersuchter Aspekt.

Verschlüsselung und Passwörter

Bei verschlüsselten Daten sollten sich die Zugangsinformationen, die für einen autorisierten Zugriff notwendig sind, nicht auf dem RFID-Tag selbst befinden [bsi04]. Da ein Angreifer, der sich im Besitz eines RFID-Tags befindet, nicht nur die Daten selbst als sein Angriffsziel wählen kann, sondern z.B. auch die auf dem RFID-Tag gespeicherten Access-Passwortes, wie sie der VDA 5501 nach auf dem Tag gespeichert werden.
Zugangsschlüssel sollten in einem entsprechenden Backend-System hinterlegt sein, auf die man nur nach entsprechender Authentisierung zugreifen kann.
Um den nach VDA 5501 definierten freien Block im USER-Bereich flexibler nutzen zu können, sollten dort gespeicherte vertrauliche Daten separat verschlüsselt werden. Der Schlüssel und der Zugriff darauf können von der Middleware des jeweiligen Prozessbeteiligten verwaltet werden (statische Verschlüsselung, siehe Abschnitt 3.2.4). So können über den freien Block auch lieferketten-übergreifend Prozessdaten ausgetauscht werden. Vertrauliche prozessspezifische Daten sind jedoch trotzdem vor einem unerlaubten Zugriff gesichert.
Die Speicherung von verschlüsselten Daten auf einem RFID-Tag, ohne diese über das Tag selbst entschlüsseln zu lassen, bringt dabei einen generellen Vorteil. Die eingesetzte RFID-Hardware benötigt keine kostenintensiven Verschlüsselungskomponenten. Alle Ver- und Entschlüsselungsvorgänge werden dabei durch die Middleware oder das Backend-System durchgeführt.

Sichten und Rollen im Backend-System

Im Regelfall unterstützen die im Produktionsumfeld verwendeten Datenbanken und die Middleware bereits ein Sichten- und Rollenmodell. Die Verlagerung von Daten in die Backend-Systeme stellt dadurch im ersten Schritt selten eine Hürde dar. Um für alle Prozess-Teilnehmer einen einheitlichen Zugriff auf das Backend-System zu gewährleisten, muss sich das (rollenbasierte) Zugriffskontrollkonzept über die gesamte Lieferkette erstrecken und zugänglich sein. Sichten und Rollen sind für verschiedene RFID-gestützte Prozesse zu etablieren, deren Zahl in Zukunft höchstwahrscheinlich steigen wird, so dass die Verwaltung von Identitäten, Rollen und Berechtigungen immer aufwändiger wird. Die dabei auftretende – vielleicht zu Beginn noch nicht existierende – Komplexität muss bereits frühzeitig beim Design eines lieferketten-übergreifenden Backend-Systems berücksichtigt werden. Ist das System nicht in dem Maße skalierbar, wie es für ein lieferketten-übergreifendes Modell notwendig wäre, kann der Aufwand für den Betrieb auf Lange Sicht für die Nutzer und die Betreiber des Systems eine zu hohe Belastung mit sich bringen [erdos05].

Authentisierung in der Föderation

In einer komplexen Lieferkette ist eine große Zahl von Entitäten und Nutzer aus verschiedenen Unternehmen/Organisationen an dem Betrieb eines RFID-Systems beteiligt. Beispiele hierfür sind sowohl die einzelnen produzierenden Unternehmen als auch die individuellen Transportdienstleister. Jede Entität innerhalb des lieferketten-übergreifenden Prozesses benötigt einen Zugriff auf die im Backend befindliche Datenbank. Ein Backend-System, das nur im Rahmen eines einzelnen Unternehmens eingesetzt wird, kann im Regelfall nur registrierte Nutzer authentisieren. Wird ein Backend-System nach diesem Modell lieferketten-übergreifend zur Verfügung gestellt, so müssen verschiedene heterogene Entitäten (aus verschiedenen Unternehmen) registriert und auch gepflegt werden. Dieser

Aufwand skaliert bei steigender Nutzerzahl zunehmend schlecht, da die damit verbundene Belastung auf Seite des Betreibers deutlich steigt. Jedoch bedeutet ein einheitliches Backend-System nicht gleichzeitig, dass es nur eine Single-point-of-Authentication gibt. Vielmehr kann es auch in einem lieferketten-übergreifenden Backend-System viele verschiedene Instanzen geben, die für unterschiedliche Ströme in der Lieferkette verantwortlich sind. So kommt es auch auf der Seite der Nutzer zu einer hohen Belastung, indem die Zahl der unterschiedlichen Systeme steigt, an denen man sich authentisieren muss.
Abhilfe kann hier ein föderatives Identitätsmanagement schaffen. Der föderative Ansatz für ein Identitätsmanagement teilt die Authentisierung in zwei Schichten auf. Zum einen registrieren sich die beteiligten Unternehmen untereinander. Zum anderen registrieren sich die einzelnen Entitäten/Nutzer der Unternehmen wiederum nur bei den Unternehmen, denen sie angehören. Einander registrierte Unternehmen vertrauen den Entitäten, die sich wiederum bei den jeweiligen Unternehmen selbst registriert haben. So wird der Aufwand für die Pflege der Authentisierungsdaten auf die einzelnen Unternehmen aufgeteilt und ähnelt so dem Aufwand für die Authentisierung eines einzelnen Unternehmens ohne lieferketten-übergreifendes Backend. Analog lassen sich auch die Berechtigungen und Rollen unternehmensübergreifend verwalten, so dass entsprechende Rollenkonzepte aufzustellen und umzusetzen sind (Autorisierung, vgl. auch Abschnitt über Rollen und Sichten).

Differenzierbare Zugriffskontrolle auf den Tags

Gerade bei einem lieferkettenübergreifenden Einsatz der RFID-Technologie und einer Abspeicherung der Daten auf einem Tag (wie von der Automobilindustrie derzeit bevorzugt), sollte eine differenzierbare Zugriffskontrolle ermöglicht werden. In Abschnitt 3.2.8 werden Verfahren angegeben, um eine solche differenzierbare Zugriffskontrolle auf höherwertigen Tags umzusetzen.

Authentisierung zwischen Tag und Lesegerät

Wie bereits in Abschnitt 4.2.2 erwähnt, wird bei den Einsatzszenarien ein höherer Anspruch an die Integrität der Daten gestellt. Eine Voraussetzung ist hier, dass die Daten (bei wiederbeschreibbaren) Tags nicht unautorisiert verändert werden können. Mithin sollten sich Lesegeräte gegenüber Tags authentisieren. Wie stark das Authentisierungsverfahren ist, hängt von der RFID-Anwendung ab. Bei dem Szenario „DaimlerChrysler, Bremen“ würde ein einfacher Passwort-Schutz ausreichen, da eine manuelle Kontrolle vorgenommen wird, wenn die Daten des Zulieferers und des ausgelesenen Tags nicht übereinstimmen. Bei einer virtuellen Baukarte besteht sicherlich ein höherer Schutzbedarf, so dass Challenge-Response-Protokolle (siehe Abschnitt 3.2.3) und kein einfacher Passwort-Schutz eingesetzt werden sollten. Bei einer virtuellen Baukarte besteht zudem die Gefahr, dass ein Angreifer ein Tag mit fehlerhaften Daten in das RFID-System bringt. Mithin ist hier eine wechselseitige Authentisierung sinnvoll.

Authentisierung zwischen Lesegerät und Backend

Weiterhin ist eine Authentisierung zwischen Lesegeräten und Backend (bzw. im Falle eines Einsatzes von WLAN gegenüber der WLAN-Infrastruktur) erforderlich. Anderenfalls könnten durch die Lesegeräte fehlerhafte Daten in das Backend-System eingespielt werden. Für die Authentisierung sind Standardverfahren einzusetzen wie z.B. Challenge-Response-Verfahren.

Digitale Signaturen zur Sicherstellung der Authentizität von Bauteilen

Neben einer Integration der Tags mit den Bauteilen muss auch sichergestellt werden, dass die Tags nicht geklont werden können. Hierfür können z.B. digitale Signaturen, die auf asymmetrischer Kryptographie beruhen, verwendet werden. Letztlich können z.B. produktspezifische Daten signiert werden [nochta06]. Nähere Informationen zu asymmetrischer Kryptographie (inkl. digitaler Signaturen) gibt Abschnitt 3.2.5.

4.3.2 Bewertung der bisherigen technischen Umsetzung

Für die Bewertung der bisherigen technischen Umsetzung von RFID-Sicherheitsmaßnahmen in der Automobilindustrie wird die Beobachtung zugrunde gelegt, dass in der Automobilproduktion und ihrer Wertschöpfungskette eine Speicherung von Produktdaten auf RFID-Tags einer Speicherung im Backend vorgezogen wird – im Gegensatz zu den Empfehlungen von Sicherheitsexperten [bsi04]. Dies spiegelt sich auch in den offiziellen Dokumenten des VDA wider [vda5501].

Für die mittel- bis langfristige Zukunft zeichnet sich darüber hinaus eine tiefe Integration der RFID-Technologie in wirtschaftliche Wertschöpfungsprozesse als wichtiger Trend ab. Im Rahmen einer gelungenen tiefen Integration der RFID-Technologie in wirtschaftliche Wertschöpfungs- bzw. Produktionsprozesse erhält diese eine Bedeutung, die weit über den Ersatz von Barcode als Identifikationsmerkmal hinausgeht (vgl. virtuelle Baukarte). Womöglich könnten solche Tagdaten in Zukunft auch mit in ein Produkt integrierter Software verknüpft sein. Der zu einem solchen Produktionsprozess gehörende Workflow würde sich dann wesentlich auf die im RFID-Tag gespeicherte Information und ihre Veränderung stützen. Dies erfordert dann evtl. globale Identitäten für firmenübergreifende Lieferketten und/oder ein fortgeschrittenes Berechtigungsmanagement (evtl. unter Einschluss des Backend-Systems).

Zum Beispiel könnte das Tag eines zu entsorgenden Autos nach evtl. Reaktivierung und Kontaktaufnahme zum Backend-System des Herstellers die Daten freigeben, aus denen alle im Auto verbauten Materialien hervorgehen (inklusive aktueller Hinweise des Herstellers für den Recycling-Prozess). Tag und Backend-System müssten in diesem Fall natürlich geeignete Mechanismen für ein solches fortgeschrittenes rollenbasiertes Berechtigungsmanagement bereitstellen.

Da in der Automobilindustrie Daten eher auf den Tags gespeichert werden sollen, sind zudem fortgeschrittene Konzepte zur Authentisierung zwischen Tags und Lesegeräten und ein angemessener Zugriffschutz erforderlich. Hierfür müssen kryptographische Verfahren (Verschlüsselung, Hash-Verfahren, digitale Signaturen) entwickelt werden, die mit einer möglichst geringen Zahl an Gattern auskommen. Auch wenn in der Automobilproduktion voraussichtlich eher höherwertige Tags eingesetzt werden (vgl. die Menge und die Art der Daten auf einer virtuellen Baukarte), so ist jede Verringerung der Tagkosten wichtig. Dies zeigt die folgende Beispielrechnung: Nimmt man an, dass ein High-End-Tag mit Kryptoprozessor derzeit ca. 5 € kostet und dass im DaimlerChrysler-Werk in Bremen pro Jahr ca. 200.000 Autos produziert werden, so entstehen jährlich ca. 1 Mio. € an Kosten nur für Tags. Diese Kosten müssen sich erst einmal amortisieren. Derzeit fehlen aber noch effiziente

kryptographische Verfahren, die eine geringe Zahl an Gattern verwenden und gleichzeitig aber auch einer mit angemessenem Aufwand durchgeführten Kryptoanalyse standhalten.
Ähnliche Bemerkungen gelten des Weiteren für einen Zugriffsschutz auf den Tags selbst. Hier fehlen geeignete und kostengünstige Mechanismen, um eine differenzierbare Zugriffskontrolle für die auf den Tags gespeicherten Daten zu ermöglichen.

4.3.3 Identifizierter Forschungs- und Entwicklungsbedarf

Im Folgenden wird der Forschungsbedarf hinsichtlich der Sicherheit von RFID-Systemen in der Automobilproduktion thematisiert. Dieser ergibt sich aus den oben genannten Sicherheitsanforderungen, Bedrohungen und Maßnahmen und der eben vorgenommenen Bewertung der technischen Umsetzung.

Entwicklung von robuster, überall einsetzbarer RFID-Hardware

Abhängig vom Grad der Integration und abhängig von der Integration in bestehende oder neue Prozessstrukturen erfüllen heutige RFID-Lösungen nicht alle Anforderungen der Anwender. Für eine flexible Integration in bestehende Prozesse sind kompakte, robuste RFID-Gates interessant, die sich bei einer übersichtlichen Modellvariation in unterschiedlichen Konstellationen einsetzen lassen. Dabei sind im Besonderen der Bedarf an Stellfläche bzw. Wand oder Deckenmontagefläche, Raumausfüllung und belastbare Anschlussschnittstellen von Bedeutung, die den schon beschriebenen Umgebungskonditionen und geforderten Schutzgraden entsprechen. Der Einsatz von WLAN bei der Anbindung von RFID-Gates (ggf. ebenfalls im 802.11b/g Frequenzbereich arbeitend) an ein Backend-System würde eine flexible Integration an ein vorhandenes Backend vereinfachen.
Die Anforderungen an die RFID-Tags gleichen in Bezug auf Dimensionierung und Haltbarkeit denen der Lesegeraäte, können darüber hinaus jedoch oft wechselnden extremen Umweltbedingungen ausgesetzt sein. Ein flexibler Einsatz auch bei unterschiedlichsten Bedingungen ist daher wünschenswert.
Werden neue Prozesse ganzheitlich unter Berücksichtigung des Einsatzes von RFID-Systemen entworfen, so ist eine individuell an spezielle Umgebungsbedingungen angepasste Integration von RFID-Gates interessant. Der Einsatz von anpassbaren Gehäusen, die Integration in Bausubstanz oder ein modularer Aufbau aus einzelnen speziell angepassten kombinierbaren Komponenten wäre dabei zu untersuchen.

Konsolidierung von RFID-Hardware

Für einen erfolgreichen flächendeckenden Einsatz von RFID-Tags ist eine Zusammenführung der Funktionen unterschiedlicher RFID-Lesegeräte anzustreben. Ein integriertes Lesegerät sollte auf verschiedenen Frequenzbereichen und bei unterschiedlichen Trägermaterialien einsetzbar sein. Vergleichend lässt sich die Entwicklung von WLAN-Adaptern betrachten, deren Entwicklungsstand heute Kombi-Geräte zeigt, die mit unterschiedlichen Frequenzen und Standards arbeiten können. Die beim RFID-Einsatz erschwerend hinzukommende Reichweitenbegrenzung und heterogene Ausbreitungscharakteristik ist dabei ein wesentlicher Forschungsschwerpunkt für die Entwicklung von Kombi-Geräten.
Neben der Konsolidierung der Geräte ist auch eine Standardisierung der RFID-Hardware und der auszutauschenden Daten notwendig. Beispielsweise werden in den oben beschriebenen Insellösungen verschiedene Tagtypen (z.B. unterschiedliche Standards, Frequenzen)

eingesetzt. Bei einem lieferketten-übergreifenden Anwendungsszenario sollten auch die auszutauschenden Daten vereinheitlicht werden.

Effiziente symmetrische Kryptoverfahren für kostengünstige Tags

Auch wenn die Vertraulichkeit der auf den Tags gespeicherten Daten gemäß den Gesprächen mit den Anwendungspartnern derzeit nicht im Vordergrund steht (siehe Abschnitt 4.2.2), so kann sich diese Situation bei einer tieferen Integration von RFID in die Prozesse der Automobilproduktion ändern. Beispielsweise können auf einer virtuellen Baukarte durchaus auch vertrauliche Produktionsdaten gespeichert werden, wie 4.1.2 zeigt. Um den Zugriff auf eine solche Baukarte zu regeln, sind des Weiteren geeignete Authentisierungsverfahren wie z.B. Challenge-Response-Protokolle (siehe Abschnitt 3.2.3) einzusetzen; eine einfache Passwort-Abfrage ist hier zu schwach, weil das Passwort im Klartext über die Luftschnittstelle versendet werden kann. Für die Authentisierung werden aus diesem Grunde angemessen starke symmetrische Verschlüsselungsverfahren oder Zero-Knowledge-Authentisierungsprotokolle benötigt. Letztere stellen eine Alternative zu Authentisierungsverfahren dar, die auf Verschlüsselung beruhen.
Andererseits müssen die Tags kostengünstig bleiben, wie bereits in Abschnitt 3.2.1 ausgeführt. Der Speicherbedarf und die Zahl der Gatter auf einem RFID-Tag sind in diesem Zusammenhang zu optimieren. Dabei helfen Verfahren der Lightweight-Cryptography wie das Lightweight Mutual Authentication Protocol (LMAP) oder der Lightweight Data Encryption Standard (DESL) [peres-lopez06, poschmann06]. An die Anforderungen eines RFID-Einsatzes angepasste sichere Authentisierungsverfahren können ebenso die notwendige Interaktion mit dem Backend verringern und damit die Verarbeitungsgeschwindigkeit (gerade bei Pulkerfassungen) optimieren [peres-lopez06].

RFID-freundliches Design des Produktionsprozesses

Wahrscheinliche, durch RFID-Fehlfunktionen bzw. -störungen bedingte Ausfälle müssen beim Design des Produktionsprozesses berücksichtigt werden, da in der Automobilproduktion die Prozesssicherheit einen hohen Stellenwert und ein Produktionsstillstand hohe Kosten mit sich bringen kann. Auch können verfälschte Produktionsdaten, die in das RFID-System eingeschleust werden, zu einer Störung des Prozesses führen. Aus diesem Grunde müssen Verfahren entwickelt werden, wie systematisch auftretende Störungen des Prozesses erkannt und behoben werden können (Plausibilitätsprüfungen, Redundanz). Im Idealfall sollten diese Verfahren automatisch solche Fehler erkennen können und angemessen reagieren können. Insbesondere sollten die Auswirkungen kleinster Ausfälle auf ein komplexes dynamisches System, wie es z.B. eine RFID-gestützte lieferketten-übergreifende Warenkette darstellt, untersucht werden. Dabei bieten sowohl speziell darauf eingestellte Pilotprojekte als auch auf formalen Beschreibungen basierende mathematischen Methoden, die die Prozessabläufe in entsprechende Modelle fassen, geeignete Forschungsansätze. Ein Beispiel für einen solchen auf mathematischen Modellen beruhenden Analyseansatz für Prozessbeschreibungen wird von Fu et al. angegeben [fu02]. Dieser Analyseansatz verwendet einen Modellprüfer (*model checker*) als Verifikationswerkzeug. Eine Übertragung dieses oder ähnlicher Verfahren auf RFID-gestützte Prozesse ist ein offenenes Forschungsgebiet.

Verfahren zur sicheren Deaktivierung und Reaktivierung von Tags

In einem lieferketten-übergreifenden Szenario ist gerade für Rückrufaktionen und auch im Falle eines Recyclings ein Zugriff auf Daten über Bauteile erforderlich. Hierfür sind Verfahren für eine sichere Deaktivierung und Reaktivierung von Tags zu entwickeln wie z.B. in [spiekermann04] vorgeschlagen.

Schwachstellenanalyse von RFID-Middleware und Betriebssystemen

Sollten in der Logistikkette der Automobilindustrie in Zukunft standardisierte RFID-Lösungen eingesetzt werden, so ist beispielsweise von einer weiteren Verbreitung der Betriebssysteme der RFID-Lesegeräte und auch der RFID-Middleware auszugehen. Da es sich zudem um relativ neue Systeme handelt, sind Schwachstellen nicht auszuschließen. Mithin können solche RFID-Systeme ein lohnendes Ziel für einen Angreifer sein. Aus diesem Grunde sollten (automatische) Testverfahren entwickelt werden, um RFID-Systeme rechtzeitig auf Schwachstellen (z.B. im Pufferüberläufe im Betriebssystem) hin zu analysieren. Auch muss es einfache Möglichkeiten zum Einspielen von Sicherheitspatches für einzelne RFID-Komponenten geben. Als Negativbeispiel kann hier die Einführung der WLAN-Technologie dienen, bei der fehlerhafte Sicherheitsprotokolle (WEP) entwickelt worden sind und letztlich eine Änderung der Firmware erforderlich gewesen wäre, um die fehlerhaften Sicherheitsprotokolle zu ersetzen.

Sicheres und skalierbares Schlüsselmanagement im Backend

Werden auf einem Tag nur verschlüsselte Daten gespeichert, so dass die eigentliche Entschlüsselung der Daten erst im Backend stattfindet, so ist ein sicheres und vor allem skalierbares Schlüsselmanagement erforderlich. Hierbei ist zu beachten, dass pro Jahr ca. 200.000 Autos im DaimlerChrysler-Werk in Bremen produziert werden und mithin mindestens 200.000 Tags mit geeigneten Schlüsseln auszustatten sind.

Effiziente Public-Key-Kryptographie für digitale Signaturen

Digitale Signaturen können auch im Zusammenhang mit der RFID-Technologie an Bedeutung gewinnen. Insbesondere lassen sich diese für einen Echtheitsnachweis von qualitativ hochwertigen und sicherheitskritischen Bauteilen eines Fahrzeuges einsetzen. Batina et al. geben beispielsweise verschiedene auf High-end Tags zugeschnittene Public-Key-Verfahren für digitale Signaturen an [batina07]. In diesem Zusammenhang formulieren sie auch: *The suitability of Public-Key (PK) algorithms for RFID is an open research problem as limitations in costs, area and power are quite severe*. Mithin ist die Entwicklung von effizienten Public-Key-Verfahren für RFID-Systeme ein interessantes und offenes Forschungsfeld. Besonders die Untersuchung von Verfahren, die auf elliptischen Kurven basieren, erscheint wegen der höheren Effizienz und kompakteren Implementierung gegenüber Verfahren, die auf der Potenzierung natürlicher Zahlen beruhen, wie z.B. RSA Erfolg versprechend.

Sicherstellung der Authentizität von Bauteilen

Um die Authentizität von Bauteilen zu sichern, ist nicht nur das Fälschen (Klonen) von RFID-Tags zu verhindern, was z.B. mit Hilfe von digitalen Signaturen geschehen kann [nochta06]. Es müssen zudem die Tags in die Bauteile integriert werden, damit ein Angreifer die Tags nicht ohne Beschädigung des Bauteiles entfernen kann.

Lieferketten-übergreifendes Identitäts- und Berechtigungsmanagement

Durch einen verstärkten Einsatz der RFID-Technologie in Lieferketten (vgl. Abschnitt 4.1.3 und Bemerkungen weiter oben) sind auch angemessene Mechanismen für ein lieferketten-übergreifendes Identitäts- und Berechtigungsmanagement im Backend erforderlich. Letztlich muss von verschiedenen Partnern die Lieferkette (Zulieferer, Logistikunternehmen, Händler) auf Produktdaten wie z.B. Fahrgestellnummer und Qualitätsdaten zugegriffen werden ohne aufwändige Prozeduren zur Authentisierung. Für eine solche Lieferkette bietet sich zur Vereinfachung des Identitätsmangements die Bildung von Föderationen an; Standards wie z.B. Liberty, Shibboleth und SAML existieren hier bereits [erdos05]. Als wesentliche Forschungsfrage ergibt sich mithin, wie man die RFID-Middleware mit föderativen Identitätsmanagementsystemen verbinden kann. Wichtig ist in diesem Zusammenhang insbesondere, welche Attribute in einer Föderation für die einzelnen Identitäten definiert werden müssen.

Wesentliche Attribute sind vor allem Rollen. Diese legen fest, auf welche Daten zugegriffen werden darf. Konsistente und skalierbare Rollenmodelle für eine RFID-gestützte Lieferkette zu entwickeln ist demnach ein weiterer Forschungsaspekt; evtl. müssen die Rollenmodelle auch organisatorische Regeln wie z.B. das Vieraugenprinzip (*separation of duty*) widerspiegeln. Hier kann auf Vorarbeiten aus anderen vom BMBF geförderten Projekten zurückgegriffen, in denen fortgeschrittene Konzepte für ein rollenbasiertes Berechtigungsmanagement entwickelt werden [orka07].

Beispielprojekte für eine tiefe Integration von RFID

In den Projekten, die im Rahmen dieser Studie untersucht worden sind, fand noch keine tiefe Integration der RFID-Technologie in die Produktionsprozesse statt. Es fehlen mithin konkrete Projekte, die eine solche tiefe Integration von RFID zum Ziel haben, wie z.B. eine Anbindung des RFID-Systems an das Fertigungsleitsystem oder an ERP-Systeme. Ein typisches Beispielprojekt wäre die Entwicklung der virtuellen Baukarte inkl. einer Integration mit dem Fertigungsleitsystem in einem Automobilwerk.

Lieferketten-übergreifende Einsatzszenarien für RFID

Eine wesentliche Erkenntnis im Rahmen dieser Studie bestand darin, dass noch kein durchgängiges lieferketten-übergreifendes Szenario für die Automobilindustrie existiert, sondern vielmehr nur Insellösungen vorliegen. Von der BLG Logistics Group gibt es sogar die Aussage, dass ein bei ihr durchgeführtes RFID-Pilotprojekt sich erst amortisiere, wenn der Automobilhersteller auch das RFID-System einsetze (vgl. [strassner05]). Letztendlich müssen also realitätsnahe Einsatzszenarien von RFID über die gesamte Lieferkette bis hin zur Wartung und zum Recycling ausgearbeitet und anschließend umgesetzt werden. Hier würde sich evtl. die Kostenersparnis durch den Einsatz von RFID am ehesten zeigen; genauso würden hier dann viele der oben genannten Sicherheitsmaßnahmen eingesetzt werden.

Zusammenfassung Kapitel 4 RFID-Anwendungsszenario: Produktion

In RFID-Projekten in der Automobilproduktion sind derzeit noch die Aspekte Industrietauglichkeit und Funktionssicherheit im Fokus. Dies liegt großenteils daran, dass es sich meist um Pilotprojekte und mithin um Insellösungen handelt. Bei einer tieferen Integration der RFID-Technologie in den Produktionsprozess und einem lieferketten-übergreifenden Einsatz von RFID wird der Aspekt der Informationssicherheit mehr in den Vordergrund rücken. Hier

sind entsprechende Anforderungen an die Datenintegrität und Verfügbarkeit zu erfüllen, weil sonst beispielsweise Produktionsprozesse gestört werden könnten. Bei einem lieferketten-übergreifenden Einsatz sind auch Vertraulichkeitsanforderungen zu erfüllen.

Da derzeit in der Automobilindustrie die Tendenz vorherrscht, Produkt- und Produktionsdaten auf den Tags und nicht nur im Backend zu speichern, werden voraussichtlich höherwertige Tags zum Einsatz kommen. Diese müssen aber trotzdem kostengünstig sein, weil sich andernfalls die Kosten eines RFID-Einsatzes nicht amortisieren. Da aber Sicherheitsanforderungen erfüllt werden müssen, sind trotzdem sichere kryptographische Verfahren für die Authentisierung und Verschlüsselung zu entwickeln (inkl. einer skalierbaren Schlüsselverwaltung). Bei einem lieferketten-übergreifenden Einsatz von RFID sind auch fortgeschrittene Konzepte des Identitäts- und Berechtigungsmanagements wie z.B. Föderationen umzusetzen. Des Weiteren sollte hier ein differenzierbarer Zugriffsschutz für die auf den RFID-Tags gespeicherten Daten ermöglicht werden, zumal verschiedene Partner der Lieferkette der Automobilindustrie auf die Tags zugreifen.

5 RFID-Anwendungsszenario: Handel

5.1 Das Szenario der Lieferkette von Konsumgütern

5.1.1 Supply Chain Management (SCM) und Wertschöpfungskette

Ziel und Aufgabe eines Supply Chain Managements (SCM) ist eine effiziente Abwicklung von Geschäftsprozessen vom Hersteller über die Distribution bis hin zum Kunden. Abb. 25 stellt eine vereinfachte Gesamtübersicht der Prozesse einer Supply Chain für das Anwendungsszenario “Handel” dar. Letztere besteht aus ”Business-to-Business” (B2B) und ”Business-to-Customer” (B2C) Prozessen.

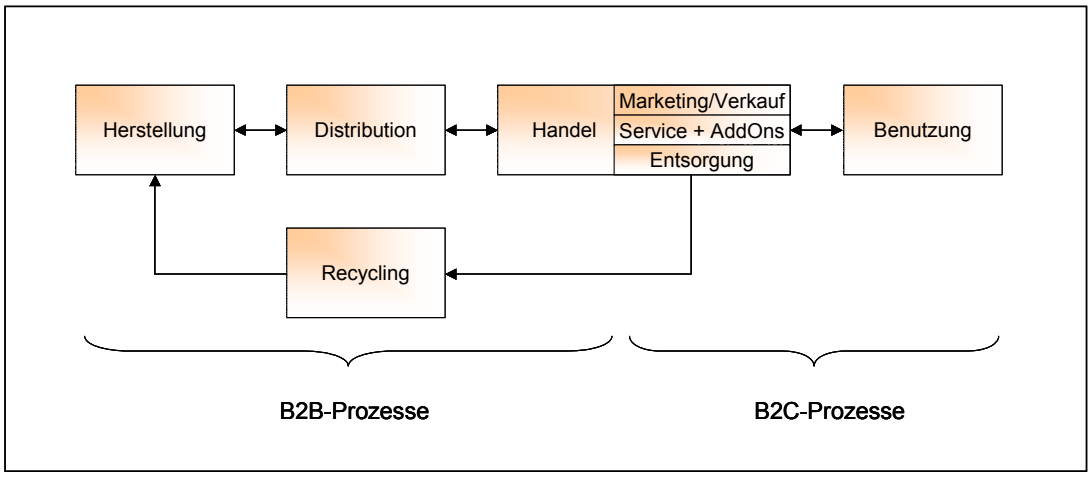


Abb. 25 – Prozessstufen einer Supply Chain

Eine effiziente Realisierung eines SCM setzt voraus, dass Entscheidungen stets auf der Basis genauer Daten und Statistiken getroffen werden können. Hierzu kann der Einsatz von RFID-basierten Systemen einen wesentlichen Beitrag leisten, insbesondere im Hinblick auf die Wettbewerbsfähigkeit der Supply Chain und die Erfüllung von Kundenanforderungen [michael05, levebre06].

5.1.2 Absicherung von Business-to-Business-Prozessen

In Abb. 26 ist ein Modell für Lieferketten im Handel vom Hersteller bis hin zum Endkunden dargestellt.

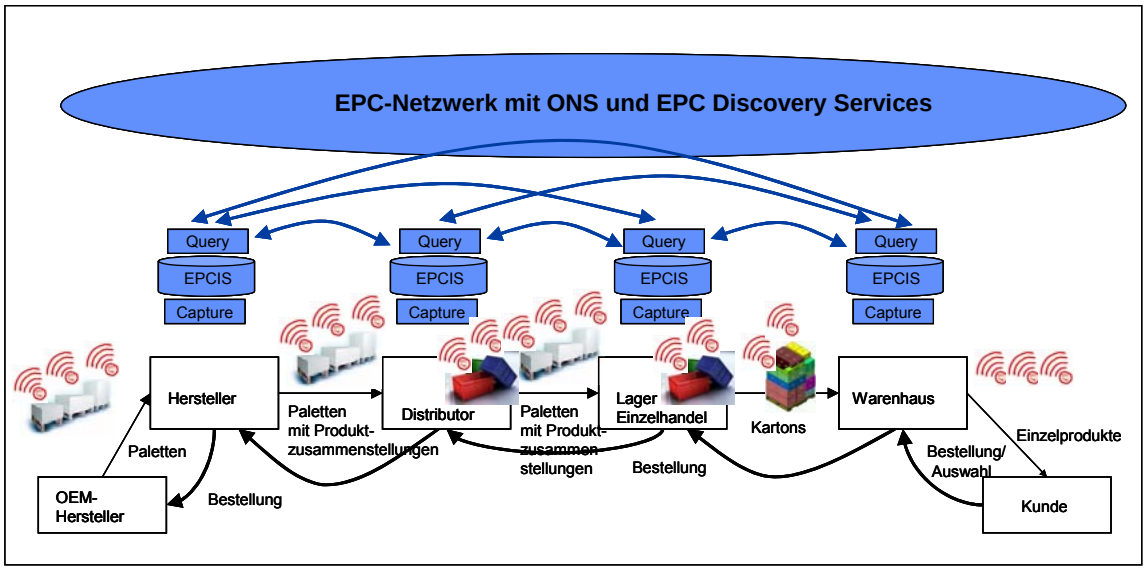


Abb. 26 – Lieferkette des Handels

Schnittstellen zwischen Prozessstufen von Supply Chains sind kritische Punkte, die eine nahtlose Steuerung systemübergreifender Abläufe erschweren. Durch den Einsatz von RFID-Technologien können diese Schnittstellen verbessert und damit eine höhere operative Effizienz erzielt werden. Im Bereich der Warenlogistik lässt sich die operative Effizienz in Bezug auf folgende Aspekte erhöhen [angerer03, kielbassa06]:

- Produktassemblierung aus OEM-Produkten (Hersteller)
- Tracking & Tracing
- Volumenplanung
- Automatische Datenerfassung
- Automatische Sortierung
- Fuhrparksteuerung
- Lieferzuverlässigkeit und Effizienz
- Warenrückverfolgung
- Kontrolle: Mengen, externe Logistik (Effekt: Reduktion von Versicherungskosten)

Durch den Einsatz von RFID-basierten Technologien können genaue Daten über den aktuellen Ist-Stand der Verfügbarkeit von Objekten und Waren gewonnen werden. Zusätzlich können dynamische Modellparameter eines SCM, wie beispielsweise Transportzeiten, einfach erfasst und im Rahmen von Optimierungen im Bereich Lagermanagement verwertet werden. Voraussetzungen für einen aus ökonomischer Sicht erfolgversprechenden Einsatz von RFID-Technologien sind eine zuverlässige und sichere Anwendung der Technologie sowie eine Erhöhung der Zuverlässigkeit und Sicherheit der logistischen Prozesse im Vergleich zu herkömmlichen Verfahren.
Für Distributoren und Handel ergeben sich Effizienzsteigerungen im Bereich der Logistik insbesondere in folgenden Bereichen:

Wareneingang / Kontrolle

- Automatisierte Erfassung der eingegangenen Waren und automatische Übernahme in Warenlager; zuverlässige Feststellung von Fehlmengen und automatisierte Reklamation
- Automatische Übernahme der Daten in Warenwirtschaftssystem

Lagermanagement

- Flexible Zuweisung von Lagerpositionen (Minimierung von Lagerflächen)
- Auffindbarkeit von Waren im Fall von Diskrepanzen zwischen Soll- Und Ist-Position im Lager (Reduktion des von Softwarefehlern verursachten wirtschaftlichen Risikos)
- Schneller Abruf von Waren
- Automatisierte Inventur

Warenausgang / Kommissionierung:

- Automatische Zusammenstellung von Sendungen oder Transporteinheiten für Einzelhandel

Um eine maximale Ausschöpfung des Potentials für Effizienzsteigerungen durch den Einsatz von RFID-Technlogien in den Lieferketten des Handels erzielen zu können, müssen sowohl eine hohe technische Zuverlässigkeit der eingesetzen Systeme als auch deren Sicherheit und Manipulationssicherheit gewährleistet werden.

5.1.3 Absicherung von Business-to-Customer-Prozessen

Kundenservice und Prozesse am Point-of-Sale

Der Einsatz von RFID-Tags auf Item-Level impliziert sowohl für den Retailer als auch den Endkunden gemeinsame wirtschaftliche Vorteile:

- Für hochwertige Produkte kann ein Echtheitsnachweis und ein Herstellernachweis erbracht werden
- In Verbindung mit Kundenkarten kann der Umsatz eines Kunden produktspartenspezifisch ermittelt werden und der Kunde kann personalisierte Rabatte oder Bonusleistungen erhalten. Hierdurch können existierende Bonusprogramme nachhaltig verbessert werden. Für den Einzelhändler ergibt sich der Vorteil einer verbesserten Kundenbindung, für den Kunden der Vorteil einer umsatzangepassten erhöhten Rabattierung.
- Individuelle Kundenbetreuung durch Add-On-Services und gezielte Bewerbung von Zusatzleistungen
- Gezielte Kundenansprache im Fall von herstellerinitiierten Rückrufaktionen
- Effiziente Abwicklung von Garantie und Service (Garantieleistungen können im Zweifelsfall auch ohne Vorlage eines Kassenbelegs schnell und unkompliziert erbracht werden)
- Rücknahme von Altgeräten

Für den Handel ergeben sich weitere Vorzüge hinsichtlich einer effizienten Abwicklung von Geschäftsprozessen:

- Erhöhung der Automatisierung von Kassensystemen
- Diebstahlsicherung von hochwertigen Artikeln
- Vereinfachte Verwaltung des Lagerbestands und vereinfachte Inventur

Für eine sowohl aus Kundensicht als auch der Sicht des Handels erfolgreiche Gestaltung von B2C-Prozessen sind im Kontext eines sicheren und integren Einsatzes von RFID-Technologien die Interessen beider Partner zu berücksichtigen.

Datenschutz

Mit dem Erscheinen von RFID-Tags ist eine heftige öffentliche Diskussion in den Medien bezüglich des Datenschutzes in RFID-basierten Systemen entstanden [langheinrich06]. Die RFID- und die klassischen Barcode-basierten Informationsakquise unterscheiden sich Im Wesentlichen in der Auslesemethode. Bei RFID-basierten Verfahren ist der Auslesevorgang unter Umständen von den Kunden nicht wahrnehmbar. Insbesondere letzteres führt zu der Befürchtung, Personen könnten anhand der Kleidung, Kundenkarten, Reisepass oder anderer mitgeführter Gegenstände jederzeit identifiziert werden. Das Szenario des gläsernen Menschen und dem damit einhergehenden Verlust der Privatsphäre wird vielfach als bedrohlich wahrgenommen. Grundsätzlich liegt der Kernpunkt der Problematik nicht in erster Linie bei den erweiterten technischen Möglichkeiten von RFID-Systemen, sondern in der Verknüpfung von Daten und den daraus abgeleiteten Metadaten. Es handelt sich also nicht primär um ein Problem der Datenerfassung, sondern vielmehr um ein Problem einer sicheren und verantwortungsvollen Datenverwaltung.
In einer vom Informationsforum RFID in Auftrag gegebenen Studie wurden die rechtlichen Rahmenbedingungen für den Einsatz von RFID-Systemen analysiert [holznagel06]. Ergebnis dieser Studie ist, dass der gegenwärtige Stand gesetzlicher Datenschutzbestimmungen grundsätzlich eine hinreichende Absicherung der Privatsphäre gewährleistet.
Basierend auf diesen gesetzlichen Rahmenbedingungen werden häufig im Rahmen von Bonusprogrammen Kundenverträge geschlossen, in denen sich ein Unternehmen durch vertragliche Nebenbedingungen erweiterte Möglichkeiten der Verwendung persönlicher Daten erschließt. Es sei dahingestellt, ob diese Tatsache den Kunden im Einzelnen bewusst ist oder ob diese nicht auch in vielen Fällen Bonusverträge ohne detailliertes Studium der Vertragsbedingungen unterzeichnen.
Verwenden die Unternehmen die Daten innerhalb gesetzlicher Rahmenbedingungen, so sind keine unmittelbaren Gefahren hinsichtlich des Verlustes der Privatsphäre zu befürchten. Dennoch ist zu erwarten, dass es Unternehmen geben wird, die sich über gesetzliche Rahmenbedingungen hinwegsetzen (vgl. Spam, Telefonwerbung).
Probleme hinsichtlich einer durchgängig integren Datenverarbeitung entstehen beispielsweise bei der Auflösung von Firmen: Es ist dann unter Umständen nicht mehr sichergestellt, wer auf welche Daten Zugriff hat und wie diese weiterverwendet werden. Ein weiteres Problemfeld erschließt sich durch die prinzipiell begrenzte Sicherheit von IT-Systemen. Durch den kriminell motivierten Einbruch in Computersysteme können Daten extrahiert und nicht bestimmungsgemäß verwendet und mit anderen existierenden Daten verknüpft werden. Dieses Risiko kann durch eine dezentralisierte Informationsverarbeitung minimiert

werden, was jedoch in vielen Fällen mit höheren Kosten für die betroffenen Unternehmen verbunden ist.
Zentralisierte Datenbestände stehen oft im Fokus von Strafverfolgungsbehörden, da sich diese Daten sehr gut für Rasterverfahren verwenden lassen. Werden auf solchen Datenbeständen ohne richterlichen Beschluss Ermittlungen in einer rechtlichen Grauzone ausgeführt, so birgt dies ein Gefahrenpotenzial für eine demokratische Gesellschaft. Somit sind auch gesamtgesellschaftlich dezentralisierte Datenbestände ein Bestandteil der Sicherung einer Demokratie.

5.2 Sicherheitsanforderungen des Handelsszenarios

5.2.1 Anwendungsspezifische Angriffsszenarien

Prozesse in RFID-basierten Supply-Chains sind einer Bedrohung durch Manipulation von Daten und Prozessen der Informationsbearbeitung ausgesetzt. Möglich ist hier zunächst eine Manipulation der auf RFID-Tags oder in der Middleware gespeicherten Daten. Diese müssen gegen unautorisierten Zugriff (schreibend und/oder lesend) gesichert werden. Weitere kritische Punkte sind in diesem Zusammenhang alle Vorgänge der Datenübermittlung, die sowohl belauscht als auch manipuliert werden können. Besonders gefährdet ist die Schnittstelle zwischen Tag und Lesegerät, da hier ein Angriff bedingt durch das Prinzip der drahtlosen Datenübertragung begünstigt wird. Die nachfolgenden Betrachtungen konzentrieren sich daher auf mögliche Bedrohungen an der Luftschnittstelle. RFID-spezifische Angriffe setzen an verschiedenen Stellen der Lieferkette oder am Point-of-Sale an und lassen sich folgendermaßen klassifizieren [harlacher07]:

- **Unberechtigte Informationserlangung**: Das unberechtigte Auslesen der Daten kann mit einem eigenen Lesegerät und durch das Abhören der Kommunikation zwischen zwei berechtigten Parteien erfolgen. Für das Abhören der Kommunikation ist die Reichweite ein wesentlicher Aspekt (siehe 2.1.2). Um in die Nähe eines originalen Tags zu gelangen, bietet sich für den Angreifer der Einsatz von Lesegeräten an, die sich an einen Personal Digital Assistant (PDA) anschließen lassen und sich ohne Erregung größerer Aufmerksamkeit einsetzen lassen.
  Eine weitere Möglichkeit für eine unberechtigten Informationserlangung ist das physikalische Auslesen der Daten eines Tags, wobei die Speicherzellen des Tags über aufwändige Labortechniken wie “Focused Ion Beam (FIB)” gelesen werden [bsi04].
- **Unberechtigte Informationsvervielfältigung**: Die Informationen auf einem Tag können unberechtigt vervielfältigt werden. Dieses kann entweder über das Klonen einen Tags oder über die Emulation eines beliebigen Tags durch einen universell einsetzbaren Emulator geschehen. Voraussetzung für beide Verfahren ist in der Regel das vorherige unberechtigte Auslesen eines Originaltags.
- **Unberechtigte Informationsveränderung**: Bei dieser Art von Angriffen wird der Dateninhalt eines Tags verändert. Voraussetzung ist, dass es sich um einen Read/Write Tags handelt, bei Read-Only Tags scheidet die Angriffsmöglichkeit von vornherein aus.
- **Verhinderung des Lesevorgangs**: Die Verhinderung eines Lesevorgangs kann durch unautorisierte Deaktivierung (Kill-Kommando) oder durch die Störung der Funkschnitt-

stelle erfolgen. Eine Abschirmung des Tags wird mit Materialien erreicht, die eine hohe Dämpfung des elektromagnetischen Felds verursachen. Eine Zerstörung des Tags kann mechanisch oder elektrisch durch eine hohe Feldeinwirkung erfolgen. So ist z.B. für induktive Tags nach [iso14443] oder [iso15693] eine maximale Feldstärke von 12 A/m definiert [finkenzeller06]. Wird diese Feldstärke erheblich überschritten, dann wird eine zu hohe Spannung in den Tags induziert und der Chip zerstört. Für eine parallele Zerstörung vieler Tags eignet sich ein solcher Angriff jedoch nicht, weil er nur aus nächster Nähe durchführbar ist. Tags lassen sich weiterhin mit einem Mirkowellenherd zerstören, allerdings nicht zuverlässig [bsi04]. Ist das Tag zudem in ein Trägerobjekt bzw. in einen Artikel eingearbeitet, besteht die Gefahr, dass mit dem Tag gleichzeitig das Produkt zerstört oder beschädigt wird [harlacher07].
Eine weitere Möglichkeit, Lesevorgänge zu unterbinden, besteht in der Anwendung von Denial-of-Service-Attacken durch Blocker-Tags oder Störsender.

- **Relay-Angriffe**: Über eine oder mehrere Zwischenstationen wird eine Verbindung zwischen dem Lesegerät am PoS und einem originalen Tag aufgebaut (vgl. Abb. 27 und [hanke05, hanke06]. Dabei wird einem RFID-Lesegerät die Existenz eines Tags vorgetäuscht. In Wirklichkeit existiert jedoch nur ein Frontend, welches die Daten des Lesers entgegennimmt und über eine Kommunikationsmedium mittlerer oder großer Reichweite an eine weitere Station weiterleitet, die sich gegenüber einem dort vorhandenen Tag als Lesegerät ausgibt und die Anfrage des ortsfernen ursprünglichen Lesegerätes an das Tag weitergibt. Die Antwort des Tags wird durch das Zwischenmedium (Relay) wieder an den originären Reader zurück übermittelt.

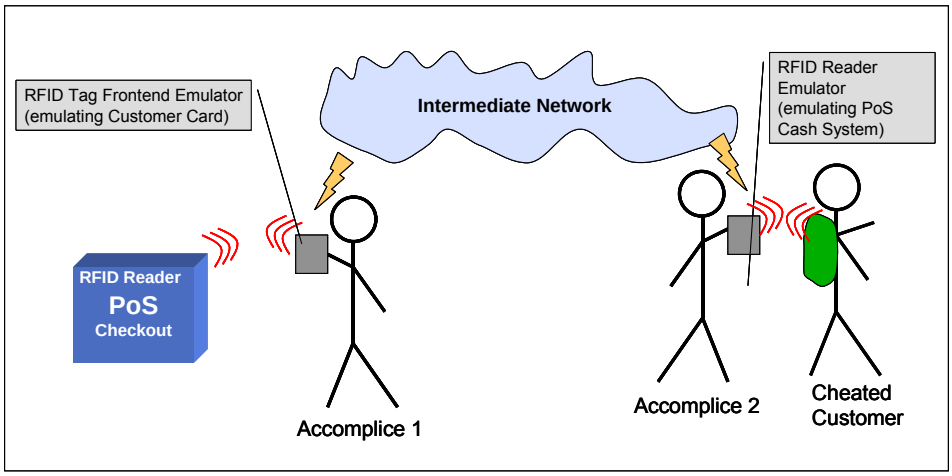


Abb. 27 – Relay-Attacke am Point-of-Sale

Angriffsszenarien für Business-to-Business-Prozesse

In B2B-Prozessen sind Sicherungsmaßnahmen gegen einen Diebstahl von Waren in den einzelnen Prozessstufen der Supply Chain (Warenlager und Kommissionierung) und auf Transportwegen zwischen denselben erforderlich. Durch eine RFID-Datenerfassung im Wareneingang und -ausgang kann der Verlust von Wareneinheiten zeitnah festgestellt werden. Dies setzt voraus, dass weder die eingesetzten Tags noch die verwendete Software (Reader-Firmware, Reader-nahe Middleware und die Middleware) manipuliert oder außer

Kraft gesetzt werden können. Nachfolgend werden einige B2B-Angriffsszenarien beschrieben, aus welchen dann spezifische Sicherheitsanforderungen abgeleitet werden können:

Angriffsszenario 1: Diebstahl mit Deaktivierung des Tags

In einem Lager eines Großhandels oder einem Zwischenlager eines Logistikdienstleisters, werden Waren unautorisiert entnommen, die RFID-Tags werden deaktiviert und die Waren unbemerkt aus dem Lager entfernt.
Problem: Tags können deaktiviert werden
Lösungsansatz: Sicherung der Deaktivierung durch kryptographische Verfahren,
regelmäßige Scans mit Hilfe von stationären Lesegeräten

Angriffsszenario 2: Diebstahl mit Tag-Emulation

In einem Warenlager sind Gegenstände unterschiedlichen Werts in Regalsystemen eingelagert. Ein Angreifer belauscht das Auslesen des Tags durch stationäre Lesegeräte. Das mit RFID-Tag versehene Produkt wird aus dem Regal entwendet und durch einen “Dummy” mit gefälschtem Tag ersetzt (Replay- und Spoofing-Attacke), um einen Verlust des Gegenstands zu verschleiern. Der Original-Tag wird zerstört und die hochwertigen Waren unter Anwendung einer Spoofing-Methode (Vortäuschung des EPC einer niederwertigen Ware) aus dem Gebäude geschleust.
Problem: Tag-Reader-Kommunikation kann belauscht werden
Lösungsansatz: Einsatz kryptographischer Verfahren

Angriffsszenario 3: Diebstahl mit Denial-of-Service-Attacke

Im Bereich des Wareneingangs mit nahe beieinander liegenden Scan-Gates können im UHF-Bereich nur eine mehr oder weniger begrenzte Anzahl interferierender UHF-Lesegeräte betrieben werden (vgl. Dense Reader Mode [iso18000-6]). Mit Hilfe von gezielt eingesetzten Handscannern oder anderen im gleichen Frequenzbereich sendenden Geräten können die Lesevorgänge empfindlich gestört werden. Dies kann dazu führen, dass eine das Scan-Gate passierende Warenpalette nicht ordnungsgemäß erfasst wird. Dieser Zustand kann mit dem Ziel des unbemerkten Ausschleusens von Waren gezielt herbeigeführt werden [weis03].
Problem: Geringe Frequenz-/Kanalressourcen im UHF-Bereich
Lösungsansatz: Zusätzliche Videoüberwachung

Angriffsszenario 4: Einschleusen von RFID-Malware

Einschleusen von schädlichem Code in die Middleware durch manipulierte Daten auf Tags.
Problem und Lösungsansatz: Falls ein Tag beschrieben werden kann, so kann dieser in vielen Fällen mit beliebigen Daten beschrieben werden. Sollten diese Daten ein Stück schädlichen Programmcode darstellen, welcher Sicherheitslücken in der Middleware-Software ausnutzt, dann muss die Aktivierung des Codes im Bereich der Middleware mit Hilfe eines Virenscanners verhindert werden bzw. die Sicherheitslücke der Middleware quellcodeseitig korrigiert werden.

Angriffsszenarien für Business-to-Customer-Prozesse

Im Bereich des Einzelhandels sind Waren gegen Diebstahl durch Kunden oder Personal zu sichern. Weiterhin sind im Bereich automatisierter Kassensysteme die Prozesse der Warenerfassung gegen unsachgemäße oder vorsätzlich manipulierende Handhabung zu schützen. Im Folgenden werden einige Szenarien für mögliche Angriffe auf RFID-basierte Systeme in Warenhäusern exemplarisch erörtert.

Angriffsszenario 5: Mechanische Zerstörung des Tags

Zerstörung von RFID-Tags durch Kunden mit Hilfe von mechanischer oder elektrischer Einwirkung, um einen Lesevorgang in einem automatisierten Kassensystem zu unterbinden.
Probleme: Mechanische Zerstörung ist bei an der Produktoberfläche angebrachten Tags leicht mit geringen Hilfsmitteln (z.B. Messer) durchführbar. Durch Einwirkung mit sehr hohen Feldstärken können die für die Energierückgewinnung zuständigen Komponenten des Tags beschädigt und durch hieraus resultierenden Überspannungen der gesamte Chip des Tags beschädigt werden.
Lösungsansätze: Videoüberwachung, unsichtbare Anbringung des Tags wo möglich;
Gegen elektrische Zerstörung ist der Entwurf robuster Tag-Frontends und die Überwachung und Lokalisierung von Strahlungsquellen im Raum zu erwägen.

Angriffsszenario 6: Unberechtigte Abschirmung des Tags

Abschirmung von Produkten inklusive Tag mit Hilfe einer Hülle, welche die Feldeinwirkung durch das Lesegerät in erheblichem Maße dämpft, um einen Lesevorgang in einem automatisierten Kassensystem zu unterbinden.
Problem: Eine Abschirmung ist bei allen elektromagnetischen Leseverfahren möglich.
Lösungsansatz: Zusätzlicher Einsatz von Metalldetektion beim Lesevorgang und Aktivierung zusätzlicher menschlicher oder automatisierter visueller Überwachung.

Angriffsszenario 7: Manipulation der Tag-Daten

Der Kunde überschreibt den EPC eines Tags mit Hilfe eines mitgebrachten Handlesegeräts um für eine höherwertige Ware einen geringeren Preis zu zahlen oder er deaktiviert das Tag vollständig.
Problem: Wiederbeschreibbare Tags (EPC Class1 Gen2) sind prinzipiell manipulierbar
Lösungsansatz: Kryptographische Verfahren; nur der aktuelle Eigentümer eines Tags, soll die Daten verändern oder den deaktivieren können. Am Point-of-Sale kann mit Hilfe eines kryptographischen Verfahrens das Eigentumsrecht auf den Kunden übertragen werden.

Angriffsszenario 8: Diebstahl mit Denial-of-Service-Attacken

Unbemerktes Ausschleusen von Waren an der Kasse (Checkout) mit Hilfe von Denial-of-Service-Attacken. Der Leser wird durch eine hohe Anzahl von synthetisch erzeugten Lesevorgängen überlastet und ein Auslesen des eigentlichen Tags wird innerhalb des hierfür zur Verfügung stehenden Zeitfensters unterbunden.
Problem: Mögliche Überlastung der RFID-Leser

Lösungsansatz: Redundante Lesevorgänge mit in verschiedenen Richtungen positionierten Readern, DoS-Detektion und systemgesteuerte Verlangsamung des Warentransports, Ergänzung der Warendetektion durch kameragestützte Verfahren der Bildverarbeitung.

Angriffsszenario 9: Relay-Attacken

Eine mögliche Anwendung der Relay-Attacke ist beispielsweise im Bereich bargeldloser RFID-basierter Zahlungsmittel denkbar: Ein Kunde hält am Checkout eines Warenhauses nicht seine wirkliche Kundenkarte vor den dortigen Reader, sondern das Relay-Frontend, welches die Leseanfrage an eine zweite Station übermittelt, welche von einer Kontaktperson unauffällig in der Nähe des RFID-Zahlungsmittels eines anderen Kunden platziert wird. Das Konto des anderen Kunden wird schließlich mit dem Rechnungsbetrag belastet.
Problem: Selbst mit kryptographischen Verfahren können Relay-Attacken nicht unterbunden werden
Lösungsansatz: Zeitbasierte Protokolle, die eine Antwort des Tags innerhalb eines eng gesteckten Zeitfensters erwarten; Verwendung von NFC- oder Close-Coupling-basierten Kundenkarten, welche z.B. im Handy integriert sein können.

Datenschutz-relevante Angriffsszenarien

Durch die Verwendung von RFID-basierten Systemen am Point-of-Sale (Warenhaus) entstehen implizite Bedrohungen der Privatsphäre des Kunden. Im Folgenden werden zwei mögliche Angriffsszenarien exemplarisch skizziert, um existierende Problemstellungen hinsichtlich des Datenschutzes zu illustrieren.

Angriffsszenario 10: Unberechtigte Deaktivierung des Tags

Ein mit einer Unique ID ausgestattetes Tag wird hinter dem Point-of-Sale mit Hilfe eines Kill-Befehls (Überschreiben des EPC-Codes mit 0) deaktiviert. Dann kann zwar nicht mehr der EPC und damit das mit dem Tag verbundene Produkt unmittelbar identifiziert werden; ist jedoch in einer Datenbank die vor Ausführung des Kill-Kommandos bestehende Verknüpfung zwischen Unique ID des Tags hinterlegt, so kann aus einer ausgelesenen Unique ID jederzeit wieder der gelöschte EPC rekonstruiert werden. Der Kill-Befehl ist also nicht unbedingt eine hinreichende Sicherheitsmaßnahme (siehe auch [juels03]).

Angriffsszenario 11: Unberechtigtes Tracking von Personen

Der EPC eines mit einer Unique ID ausgestatteten Tags wurde mit Hilfe eines Kill-Befehls gelöscht und es ist nirgendwo eine Verknüpfung zwischen der Unique ID des Tags und des zuvor auf ihm gespeicherten EPC hinterlegt. Eine Zuordnung des Tags zu einem Produkt ist also nicht mehr möglich. Dennoch kann die Unique ID unter Umständen mit der Person verknüpft werden, die den entsprechenden Gegenstand bei sich trägt. Wird dieselbe Unique ID an anderer Stelle wieder ausgelesen, so kann man den Aufenthaltsort der Person bestimmen unter der Annahme, dass der Gegenstand von der immer gleichen Person verwendet wird. Es handelt sich hier um einen Verlust der “Location Privacy” [sarma03].

5.2.2 Anwendungsspezifische Anforderungen

Das Handelsszenario stellt mit einem hohen Durchsatz an Produkten, welche als Einzelprodukt, Kartonware oder in heterogener Zusammensetzung auf Paletten zu handhaben sind, hohe Anforderung an die Funktionssicherheit RFID-basierter SCM-Systeme und deren Datenintegrität. An verschiedenen Stellen der Lieferkette sind Menschen in die Handhabungsprozesse eingebunden, die sowohl Fehlerquellen im operativen Bereich als auch Initiatoren von Bedrohungen der Sicherheit und Datenintegrität darstellen können. Die Gesamtwirtschaftlichkeit einer Lieferkette wird maßgeblich bestimmt von der operativen Effizienz und der Absicherung der Prozesse gegen Diebstahl und Manipulation. Funktionssicherheit und Datensicherheit sind grundsätzlich in engem Zusammenhang zu betrachten, da Schwachstellen der Funktionssicherheit generell ein Angriffspotenzial im Sinne der zuvor beschriebenen Bedrohungsszenarien generieren. Umgekehrt erhöhen Maßnahmen der Datensicherheit auch die Funktionssicherheit von logistischen Prozessen, da durch zusätzliche Sicherheitsmaßnahmen das Risiko von Fehlinterpretationen und Fehlbearbeitungen minimiert wird.
Die in Lieferketten des Handels zu handhabenden Einheiten unterscheiden sich wesentlich hinsichtlich ihrer Granularität. Die Handhabung und die Nutzung von Tags muss auf den verschiedenen Verpackungsebenen Einzelprodukt, Kartons, Paletten und Container betrachtet werden. Produkte großen Volumens (wie beispielsweise Kühlschränke) sind vom Hersteller über die Distribution auf Palettenebene bis zum Warenhaus aufgrund ihrer Größe als Einzelprodukt zu handhaben. Produkte geringen Volumens (wie beispielsweise Lebensmittel) werden hingegen mehrfach verpackt (Kartons, Paletten) und bei Kommissionierungsvorgängen auf verschiedenen Ebenen neu zusammengestellt.
Weiterhin unterscheiden sich die zu liefernden Produkte in ihrem Wert. Für hochwertige Produkte werden andere Sicherungsmaßnahmen benötigt als für niedrigpreisige Produkte. Sicherheitsanforderungen müssen daher grundsätzlich sowohl dem Risiko der Bedrohung (Eintrittswahrscheinlichkeit) als auch dem Erwartungswert des Schadens angemessen sein. Hieraus resultiert die Notwendigkeit der Differenzierung von Sicherheitsmaßnahmen.

Funktionssicherheit und Verfügbarkeit

Ein wesentlicher Vorteil der Verwendung von RFID-Systemen in Lieferketten des Handels besteht in der Möglichkeit der Umgestaltung von logistischen Vorgängen von einer klassischen zentralistischen zeitverzögerten oder offline durchgeführten Datenverarbeitung hin zu dynamischen Echtzeitprozessen. Die Funktionssicherheit derartiger dynamischer Systeme ist eine Grundvoraussetzung für Datensicherheit und Datenintegrität. Hinsicht der RFID-nahen Middleware impliziert dies die Notwendigkeit einer lokalen Datenverfügbarkeit an jenen Orten, an welchen Schreib- oder Lesevorgänge auf Tags ausgeführt werden müssen.
Für den Zugriff auf ein einzelnes Tag steht im Allgemeinen nur ein sehr beschränktes Zeitfenster zur Verfügung, damit insgesamt eine hinreichende Durchsatzrate erzielt werden kann. Hinsichtlich der Gestaltung der Schnittstelle zwischen Tag und Lesegerät ist hier eine Mindestkommunikationsrate bei gleichzeitiger Minimierung der Fehlerrate zu realisieren. Dies stellt insbesondere Anforderungen an Situationen, in welchen sich beispielsweise mehrere Tags in Reichweite eines Lesegerätes befinden (Pulkerfassung). Das hier für einen einzelnen Tagzugriff zur Verfügung stehende Zeitfenster hängt von der Tagdichte und der Geschwindigkeit ab, mit welcher die Tags an dem Lesegerät vorbeigeführt werden. Durch

gegenseitige Interferenzen von Tags können Schreib- oder Lesevorgänge gestört werden, was die Datenintegrität des Gesamtsystems gefährden kann.

Weitere Herausforderungen hinsichtlich der Kommunikation zwischen Tag und Reader entstehen durch die Materialeigenschaften des etikettierten Produkts (z.B. Metalle, Flüssigkeiten), die vielfach zu einer signifikanten Reichweitenverminderung führen. Funktionssicherheit und Verfügbarkeit sind also insgesamt eine Grundvoraussetzung für die Anwendung Verfahren zur Sicherung der Datenintegrität.
Mangelnde Funktionssicherheit hingegen impliziert Potenzial für die Bedrohung der Datensicherheit und Datenintegrität. Das Ausnutzen von Schwachstellen der Funktionssicherheit von Tag-Reader-Systemen muss unterbunden werden. Hierzu gehören eine Absicherung von Pulkerfassungsvorgängen sowie die Garantie, dass Zeitbedingungen beim Lesevorgang sicher eingehalten werden. Bei UHF-basierten Systemen muss durch Zusatzmaßnahmen eine interferenzfreie Operation gewährleistet werden.

Datensicherheit und Authentizität

Im Bereich der Middleware können für eine Sicherung von RFID-basierten Systemen klassische Verfahren für eine Benutzerauthentisierung und das Management von Zugriffsrechten auf Daten angewendet werden.
Für das RFID-Frontend (Tag-Reader-Kommunikation) ergeben sich zusätzliche Sicherheitsanforderungen in Bezug auf die in Abschnitt 5.2.1 dargestellten Angriffsszenarien:

- **Geschützte Deaktivierung von Tags**: Die Deaktivierung von Tags darf nur nach expliziter Authentisierung durchgeführt werden.
- **Robustheit der Tags**: Zur Reduktion des Risikos der Zerstörung von Tags sollten die analogen Tag-Frontends gegenüber der Einwirkung übermäßig hoher Felder mechanisch robust sein.
- **Authentisierung**: Zur Sicherung gegen unautorisiertes Lesen und/oder Schreiben von Tags sollte eine Authentisierung des Lesegeräts gegenüber dem Tag erfolgen.
- **Schutz gegen Tag-Cloning**: Das Kopieren und Emulieren von Tags für Markenfälschungen muss sicher unterbunden werden. Hierzu müssen Angriffsmethoden wie Sniffing, Spoofing und Replay durch Sicherungsmaßnahmen unmöglich gemacht werden. Diese Bedingung muss auch noch nach dem Point-of-Sale aufrecht erhalten werden, damit keine Serviceleistungen für geklonte Waren erbracht werden müssen.
- **Plausibilitätsprüfungen:** Zur Ergänzung des Lesevorgangs sollten zusätzliche optische Plausibilitätsprüfungen des Produktes durchgeführt werden.
- **Erkennung von DoS-Attacken**: Diese Anforderung sollte insbesondere im Kassenbereich von Warenhäusern erfüllt sein.
- **Verhinderung von Relay-Attacken:** Diese Anforderung kann unter Umständen im Widerspruch zu Anforderungen der Funktionssicherheit stehen.
- **Sichere Übermittlung eines Echtheitsnachweises:** Bei hochwertigen Produkten oder kritischen Lebensmitteln sollte ein Echtheitsnachweis verfügbar sein. Sind in den Tags zusätzliche Sensoren integriert, so ist die Integrität der gespeicherten Sensordaten

sicherzustellen (beispielsweise bei der Überwachung einer unterbrechungsfreien Kühlkette).

Die Notwendigkeit der Realisierung der zuvor genannten Anforderungen hängt im Wesentlichen von den Eigenschaften der etikettierten Produkte und der für diese spezifisch definierten Sicherheitsanforderungen ab. In Abhängigkeit der produktbezogen erforderlichen Sicherungsmaßnahmen stellen sich die Randbedingungen einer technischen Realisierung unterschiedlich dar. Bei Ultra-low-cost-Anwendungen müssen preiswerte Herstellungsverfahren und geringe Tag-Komplexität ohne zusätzliche Sicherungsmaßnahmen auf dem Tag angestrebt werden. Für hochwertige Produkte ist der Einsatz von aufwendigeren Tags mit sicheren Authentisierungs- und Verschlüsselungsverfahren denkbar und realisierbar. Im Hinblick auf Tagging von Einzelprodukten des Handels ist die Beschaffenheit der Produkte und die hiermit verbundene Funktionssicherheit des Tag-Zugriffs zu berücksichtigen. Dies gilt insbesondere für Flüssigkeiten und metallische Oberflächen.

Anforderungen an den Datenschutz

Hinsichtlich des Datenschutzes ist eine durch den Kunden festgelegte Verwendung von Produkt- und Verkaufsdaten notwendig, um dessen Selbstbestimmungsrecht in Bezug auf die Verwendung personenbezogener Daten in vollem Umfang gerecht zu werden.
Um die in Abschnitt 5.2.1 dargelegten Bedrohungen hinsichtlich des Datenschutzes abzuwenden, muss ein Kunde die Möglichkeit haben, Tags dauerhaft oder vorübergehend für Auslesevorgänge zu sperren. Dies impliziert auch die technische Notwendigkeit, dass eine Aktivierung eines vorübergehend gesperrten Tags nur unter Einwirkung des Kunden möglich sein darf. Weiterhin sollte ein Verbraucher differenzierte Möglichkeiten der Beeinflussung der Weiterverarbeitung personenbezogener Daten haben, was insbesondere bei Einkäufen im Rahmen von Bonusprogrammen von Bedeutung ist. Hier ist eine kundengesteuerte differenzierte Datenspeicherung notwendig, bei der beispielsweise bei Lebensmitteln und Produkten niedriger Preiskategorien keine Einzeldaten gespeichert werden. Bei hochwertigen Produkten ist eine Zuordnung eines Produkts mit einer Seriennummer zu einem bestimmten Kunden unter Umständen sinnvoll, weil hiermit von Seiten des Verkäufers bzw. Warenhauses verbesserte Serviceleistungen und für den Kunden interessante Zusatzleistungen angeboten werden können.

5.3 Sicherheitsmaßnahmen des Handelsszenarios

5.3.1 Empfohlene Sicherheitsmaßnahmen

Sicherheitsmaßnahmen der Middleware

Auf der Ebene der Middleware sind Sicherheitsmechanismen anzubringen, die eine Authentisierung und Autorisierung beim Zugriff auf EPC-Sicherheitsdienste steuern die Zugangsrechte zum EPCglobal™-Netzwerk regeln [popova05].
Durch eine restriktive Verteilung von Informationen und eine minimierte Speicherung von Informationen auf Tags (im Idealfall nur eine “Unique ID”) kann die Übermittlung der diesem Tag zugeordneten Daten selektiv basierend auf der Authentifizierung des Benutzers und einer benutzerspezifisch erteilten Autorisierung durch die Middleware erfolgen. Mit dieser

Methode ist eine Zuordnung einer gelesenen ID zu einem Produkt ohne Kenntnis der Datenverknüpfung in der Middleware nicht möglich. Allerdings können Lauschangriffe ohne eine kryptographische Sicherung der Luftschnittstelle nicht unterbunden werden. Somit besteht die Möglichkeit der Herstellung von gefälschten Tags und der Einsatz derselben im Rahmen von Replay-Attacken.

Sicherheitsmaßnahmen für Tags und Lesegeräte

Grundsätzlich ist einer Kostenminimierung beim Einsatz von RFID-basierten Systemen von großer Bedeutung. Insbesondere die Kosten der in großen Stückzahlen hergestellten Tags fallen hier wesentlich ins Gewicht und sind ein entscheidender Faktor für die Markteinführung dieser Technologie. Die in Abschnitt 3.2 vorgestellten kryptographischen Sicherungsverfahren und Authentisierungsverfahren erfordern teilweise einen erheblichen Hardwareaufwand auf der Tag-Seite. Daher ist die Entwicklung und Standardisierung von vereinfachten effizient hardwareimplementierbaren Verfahren in Form von minimalistischen kryptographischen Verfahren (Lightweight-Cryptography) ein wesentlicher Aspekt. Ansätze in dieser Richtung werden beispielsweise in [zongwei05] (Hash-Chain-basiertes Verfahren) und [juels04] (symmetrisches Verschlüsselungsverfahren) vorgestellt.
Bei der Sicherung von niedrigpreisigen Waren wird man aus Kostengründen auf den Einsatz von kryptographischen Sicherungsverfahren verzichten. Hier stehen andere Entwicklungen, wie beispielsweise Printed RFID Tags an, die einen Masseneinsatz von RFID-Technologien wesentlich vorantreiben werden. Letztere werden zunächst zusätzlich zu Barcodes auf Verpackungen aufgedruckt werden und Product Codes werden hier für ganze Produktionschargen gleicher Waren (beispielsweise Lebensmittel) vergeben.

Datenschutz: Customer-Related PoS Data Management

Verfahren zur Deaktivierung eines Tags nach Erfassung des Zahlungsvorgangs am Point-of-Sale können das Problem der Bedrohung der Privatsphäre durch die Verwendung von RFID-Tags wesentlich entschärfen. Dennoch ist zumindest in Verbindung mit einer Kundenkarte eine Profilierung des Kunden über Zeit und Art der gekauften Waren nach wie vor möglich. Daher sind zusätzliche Maßnahmen für eine kundenindividuelle Gestaltung der Speicherung von kundenbezogenen Verkaufsdaten und Profilen notwendig. Diese Maßnahmen müssen so gestaltet werden, dass für den Handel durch deren Umsetzung keine unzumutbar hohen Kosten entstehen. Hierzu werden neue Verfahren für ein kundenbezogenes Datenmanagement im Handel benötigt.
Durch Verwendung einer an den Bedürfnissen des Kunden ausgerichteten Software am Point-of-Sale könnten folgende wegweisende und kundenfreundliche Funktionalitäten zur Verfügung gestellt werden:

- Der Kunde legt fest, welche Verkaufsdaten auf dem System des Anbieters gespeichert bleiben und welche nicht. Sollen Daten nicht gespeichert bleiben, so können diese nur mit Hilfe eines beim Kunden vorhandenen geheimen Schlüssels auf dessen Wunsch beim Anbieter wieder sichtbar gemacht werden, um beispielsweise eine Serviceleistung in Anspruch zu nehmen.

- Für alle Kunden wird ein Standardprofil angelegt, in welchem die Kunden festlegen können, welche Verkaufsdaten (beispielsweise Preiskategorien oder Produktkategorien) mit welchen Attributen beim Anbieter standardmäßig gespeichert werden sollen.
- Über ein passwortgesichertes Web-Interface können Kunden jederzeit die auf sie bezogenen gespeicherten Daten einsehen und bei Bedarf auch löschen oder reaktivieren.

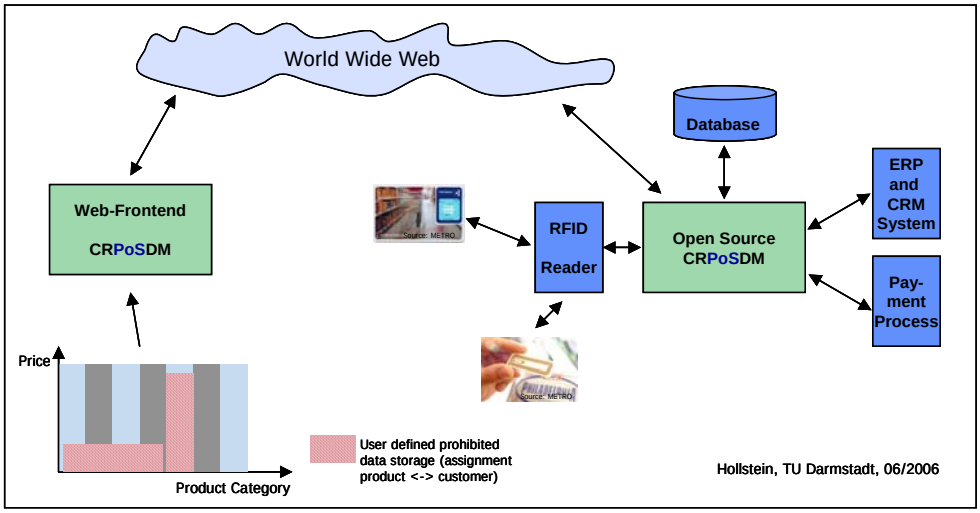


Abb. 28 – Kundendefinierte Datenspeicherung am Point-of-Sale

Um eine Standardisierung von Customer-Related PoS Data Management-Systemen (CRPoSDM) und ein hohes Niveau an Vertraulichkeit zu erreichen, wäre eine Implementation als zertifiziertes Open-Source-System (minimale Zusatzkosten für das Handelsunternehmen) sinnvoll.

5.3.2 Bewertung der bisherigen technischen Umsetzung

Bisherige standardisierte Tags verfügen nur über sehr vereinfachte Sicherungsmaßnahmen. So wird beispielsweise für HF-Tags in ISO 15962 definiert, dass bestimmte EEPROM-Speicherwörter gegen Löschen und erneutes Überschreiben gesichert werden können. Ebenso wird in dem Standard ISO 18000-6 (EPC Class1 Gen2) ein einfaches Einweg-Locking-Verfahren beim Tag-Hersteller oder durch den Anwender vorgesehen. Authentisierungsverfahren sind bei EPCGlobal erst für Tags der Kategorie EPC-Class2 vorgesehen. Eine Implementation aufwendiger Hash-Lock-Verfahren bietet sich hier als Lösung der Zukunft nicht unmittelbar an, da die hierfür notwendigen Verfahren zur Ausführung der notwendigen Brute-Force-Verfahren eine nach oben nicht begrenzten Datenmenge im Reader-Frontend verarbeiten müssten, was die mit gewünschten engen Zeitfenstern für Zugriffsvorgänge auf den Tags nicht konform ist.
Insbesondere im Szenario der Lieferketten des Handels mit einer hohen Anzahl von Produkteinheiten und hohen Anforderungen an die Dynamik der eingesetzen RFID-Systeme sind daher Hash-basierte Verfahren nicht adäquat. Challenge-Response-Verfahren, auch indirekte Verfahren mit abgeleiteten Schlüsseln, sind hier wegen der Notwendigkeit der Existenz eines geheimen Schlüssels ebenfalls nicht geeignet. Zum einen muss hier ein sehr aufwändiges

Schlüsselmanagement betrieben werden. Zum anderen besteht die prinzipielle Gefährdung dass aufgrund der hohen Anzahl der sich im Umlauf befindlichen Tags mit einer hohen Wahrscheinlichkeit irgendwann der geheime Schlüssel mit Hilfe von Reverse-Engineering enttarnt werden kann, womit das gesamte Sicherungssystem hinfällig wird.
In der Literatur werden einige vereinfachte Sicherungsverfahren für die Authentisierung der Tag-Reader-Kommunikation (z.B. [defend07, dimitriou05, peres-lopez06]) vorgestellt. Durch eine Entwicklung neuer Verfahren basierend auf einer Kombination erweiterter Lightweight-Verfahren mit Physical-Unclonable-Functions könnten die offenstehenden Problemstellungen angegangen werden mit dem Ziel der Realisierung kostenverträglicher Sicherungsverfahren für Anwendungen in den Lieferketten des Handels.
Erweiterte Konzepte für eine kundenindividuelle Gestaltung des Datenschutzes existieren bislang noch nicht. Hierfür werden Konzepte und Standards auf europäischer oder internationaler Ebene benötigt.

5.3.3 Identifizierter Forschungs- und Entwicklungsbedarf

Basierend auf den ermittelten Sicherheitsanforderungen des Handels ergibt sich ein Forschungsbedarf sowohl im Bereich neuer Sicherungskonzepte als auch im Bereich neuer effizienter Technologien für Tags und Lesegeräte. Konzepte für eine technologieintegrierte Datensicherheit von RFID-Systemen bieten ein hohes Potential für die Realisierung von Maßnahmen des Datenschutzes, da hier gegebenenfalls auf vorhandene Sicherheitsmechanismen zurückgegriffen werden kann. Im Folgenden werden die im Kontext der Lieferketten des Handels offenen und zukünftig zu betrachteten Fragestellungen zusammenfassend erläutert.

Integrierte und virtualisierbare Sicherungskonzepte

Für in Lieferketten des Handels eingesetzte HF- und UHF-Tagsysteme werden standardisierte Sicherungskonzepte mit produktwertgerechten Sicherungsmaßnahmen benötigt. Diese Konzepte sollten eine modulare Struktur aufweisen und von der physikalischen Ebene der Kommunikation (HF, UHF) abstrahiert angewandt werden können (Virtualisierung der Tag-Hardware). Weiterhin werden multistandard-fähige Lesegeräte mit effizienter Identifikation des Tagtyps und der angewandten Sicherheitsstandards benötigt. Grundsätzlich ist bei einer Virtualisierung von Sicherheitskonzepten auch zu untersuchen, welche Daten auf dem Tag und welche in der Middleware zu speichern sind und wie Redundanzen zur Erhöhung einer Gesamtsicherheit anzuwenden sind. Hierbei ist auch zu berücksichtigen, dass die Nummernvergabe von Unique IDs für Tags bei verschiedenen Registrierungsstellen erfolgen kann und Konzepte systemübergreifend standardisiert funktionieren müssen.

Effiziente hardwareorientierte kryptographische Verfahren

Es werden neue effizient hardwareimplementierbare Verfahren benötigt. Diese müssen eine Umsetzung von Zufallszahlengeneratoren, Hash-Funktionen und symmetrischen und Public-Key-Verfahren bei minimaler Chipfläche und minimiertem Leistungsverbrauch ermöglichen (beispielsweise unter Verwendung von „Physical Unclonable Functions“). Eine weitere Anforderung an derartige Verfahren ist, dass die Dauer der Gesamtkommunikation zwischen Lesegerät und Tag minimiert werden muss. Zusätzlich müssen die Kommunikation und die

Verfahren so robust ausgelegt werden, dass Signalstörungen und vorübergehende Spannungseinbrüche (bedingt durch variable Empfangsbedingungen des Tags) nicht zum Abbruch eines Kommunikationsvorgangs führen.

Maßnahmen zur Verhinderung von Relay-Attacken

Wie bereits zuvor beschrieben, können Relay-Attacken nicht ohne weiteres durch kryptographische Verfahren unmöglich gemacht werden und sind daher als gesonderte Problemstellung zu betrachten. Daher ist eine Entwicklung neuer Verfahren für Detektion und Abwehr von Relay-Attacken notwendig. Die Verfahren werden auf eine Einschränkung des Zeitfensters für einen Lesevorgang hinauslaufen und es ist zu untersuchen, welche kontraproduktiven Zusammenhänge sich im Hinblick auf Verfahren der Pulkerfassung von Tags ergeben.

Weiterentwicklung der Tagtechnologien

Da eine funktionelle Zuverlässigkeit eine wesentliche Voraussetzung für die Sicherheit eines Gesamtsystems darstellt, ist eine robuste Auslegung der Tag-Hardware eine Grundvoraussetzung für RFID Systemsicherheit. Hier wird zum einen die Reduktion des Risikos einer drahtlosen Zerstörung durch Einwirkung hoher Feldstärken ein Gegenstand weiterer Untersuchungen sein und zum anderen eine kosteneffiziente Sicherung von Tags gegen mechanische Zerstörung.
Im Hinblick auf die zukünftige Möglichkeit der Herstellung von Low-Cost-RFIDs im HF-Bereich mit Hilfe von kostengünstigen Druckverfahren, wird zunächst für den Bereich niedrigpreisiger Produkte kein Weg an einer Verwendung von HF-Tags vorbeiführen. Gedruckte HF-Tags werden jedoch auf absehbare Zeit noch keine Sicherungsverfahren für Zugriff und Datenintegrität enthalten können. Für höherwertige Produkte werden HF- oder UHF-Tags mit integrierten Authentisierungs- oder Verschlüsselungsverfahren benötigt. Für kosteneffiziente Implementationen werden hier neue effiziente Verfahren der Lightweight-Cryptography benötigt. Durch Verwendung von Physical Unclonable Functions ist eine effiziente Implementation bei vertretbarem Hardwareaufwand zu erwarten.
Ein weiteres Forschungsfeld bietet die Anforderung der Herstellung kostengünstiger Tags für niedrigpreisige Massengüter. Hier bieten sich neuartige Herstellungsverfahren wie beispielsweise „Printed Electronics“ an. Im Kontext alternativer Herstellungsverfahren sind neue Sicherungstechniken zu erforschen, die eine effiziente Implementation durch Ausnutzung technologiespezifischer Eigenschaften ermöglichen.

Multistandardfähige Lesegeräte mit optimierter Nutzung von Frequenzressourcen

In Zukunft werden im Kontext von RFID-Applikationen im Bereich der Lieferketten des Handels sowohl HF-Technologien als auch UHF-Systeme zum Einsatz kommen, um den Anwendungsanforderungen auf verschiedenen Verpackungsebenen (Einzelprodukt, Kartons, Paletten, Container) gerecht werden zu können. Hierfür wird es spezialisierte Lesegeräte geben, deren Operation sich auf den UHF-Bereich beschränkt (z.B. in Paletten-Gates im Wareneingang oder -ausgang) und mehrbereichsfähige Handgeräte zur Verwendung im Warenlager und Warenhaus. Hieraus ergibt sich für zukünftige Lesegeräte die Anforderung, dass diese in mehreren Frequenzbereichen und innerhalb dieser wieder mit Sicherheitsstandards unterschiedlicher Komplexität in einheitlicher Weise umgehen müssen.
Weiterhin sind neue Verfahren für eine abgesicherte interferenzfreie Operation, beispielsweise im Dense Reader Mode nach [iso18000-6], von Lesegeräten in Multi-Reader-Umgebungen zu entwickeln. Dies ist aufgrund der in Europa begrenzten Frequenzressourcen und der

großen Lesereichweiten im UHF-Bereich ein wichtiger Aspekt hinsichtlich der Gesamtzuverlässigkeit und damit auch der Gesamtsicherheit eines RFID-basierten Logistiksystems.

Echtheits- und Herkunftsnachweise

Grundsätzlich können Anwender von RFID-Technologien Identifikationsnummern für Unternehmen bei verschiedenen Registraren (CEFIC, DUN, GS1, EDIFICE, EHIBCC, ODETTE, UPU) beantragen. Hier werden Verfahren und Standards benötigt, wie Echtheits- und Herkunftsnachweise branchenübergreifend sicher kommuniziert werden können.

Sicherer Checkout am Point-of-Sale

Für eine zuverlässige und sichere Erfassung von Waren mit Hilfe von automatisierten Kassensystemen ist eine Kombination von Verfahren der Bildverarbeitung mit RFID-basierten Verfahren (Abwehr von Low-Tech-Attacken) in zukünftigen anwendungsorientierten Forschungsprojekten zu untersuchen

Datenschutzkonzepte

Hinsichtlich des Datenschutzes werden über existierende Kill-Konzepte oder eine mechanische Zerstörung eines Tags hinausgehende Verfahren für eine verbraucherinitiierte vorübergehende Deaktivierung von Tags benötigt. Hier können insbesondere auch kryptographische Verfahren für einen sicheren Nachweis des Eigentums eines Tags und des zugehörigen Produkts zur Anwendung kommen. Denkbar sind Verfahren, in denen mit einem Eigentumsübertrag auch das Sicherheitsmanagement für das Tag in die Verantwortung des Kunden übergeben wird. Letzterer kann dann im Falle der Notwendigkeit der Inanspruchnahme einer Serviceleistung dem Verkäufer wieder vorübergehende Leseberechtigungen erteilen, um die Berechtigung der Leistungsbeanspruchung nachzuweisen.
Um eine kundenorientierte und kundenbestimmte Verwaltung von personenbezogenen Daten am Point-of-Sale zu ermöglichen, welche sowohl Kunden als auch den Lieferanten flexible Möglichkeiten hinsichtlich der Ausgestaltung von Geschäftsbeziehungen ermöglicht, sind Forschungsprojekte hinsichtlich der Entwicklung von Open-Source-Software für vertrauenswürdiges und genormtes Customer Privacy Management notwendig. Ein Open-Source-Ansatz würde hier die Vorzüge garantierter Vertraulichkeit und wirtschaftlich realistischer Randbedingungen für die Umsetzung vereinen und eine Standardisierung vereinfachen.
Um unautorisierte Lesevorgänge und unautorisierte Verfolgung von Gegenständen zu verhindern (Location Privacy) werden neue Verfahren zur Randomisierung von Tag-Antworten [sarma03] benötigt, die auf neue Autorisierungs- und Authentisierungskonzepte mit unterschiedlichem Sicherheitsniveau abzustimmen sind.

Zusammenfassung Kapitel 5: RFID-Anwendungsszenario: Handel

Eine sichere Verwendung von RFID-Systemen in Lieferketten des Handels für Produkte unterschiedlicher Preiskategorien benötigt als Grundlage effizient hardware-implementierbare Sicherungsverfahren für die Kommunikation zwischen Tag und Lesegerät. Der Vertrieb von Markenfälschungen kann nur durch Verwendung von kryptographischen Sicherungsverfahren unterbunden werden. Bei der Konzeption des Gesamtsystems von RFID-basierten Supply-Chain-Anwendungen ist die Funktionssicherheit ein wesentlicher Bestandteil des Sicherheitskonzepts. Hierbei ist zu berücksichtigen, dass für den Zugriff auf Tags nur ein

begrenztes Zeitfenster zur Verfügung steht und stehen darf. Hieraus resultiert der Bedarf für neue Verfahren der Lightweight-Cryptography mit fälschungssicheren Schlüsseln. Hinsichtlich des Datenschutzes besteht ein Bedarf an neuen Verfahren, die die Interessen von Kunden und Lieferanten auf individueller Basis angleichen und eine automatisierte Datenverarbeitung basierend auf einem durch den Kunden festgelegten spezifischen Profil ermöglichen. Hierfür bietet sich die Entwicklung vertrauenswürdiger Open-Source-Softwarekonzepte an.

6 RFID-Anwendungsszenario Fälschungssicherheit

Im Anwendungsszenario Fälschungssicherheit wird der RFID-Einsatz im Pharma- und Gesundheitssektor betrachtet. Dort sollen RFID-Lösungen nicht nur die Effizienz der Lieferkette verbessern, sondern auch für mehr Medikamentensicherheit sorgen. Bei allgemeinen Aspekten des Handelsszenarios kann auf das vorangegangene Kapitel verwiesen werden.
Nach optimistischen Schätzungen der WHO sind 10-30% aller in Entwicklungsländern angebotenen Arzneimittel Fälschungen. In den Nachfolgestaaten der Sowjetunion liegt der Anteil bei 20%, in den Industriestaaten etwa bei 1%, wobei die Tendenz u.a. durch die zunehmende Nutzung des Versandhandels steigt [korzilius06]. In den Entwicklungsländern sind vor allem Malariamittel, Antibiotika und HIV-Medikamente betroffen, während in den reichen Ländern eher Fälschungen von Lifestylepräparaten (z.B. Mittel für Potenz, Haarwuchs, Muskelaufbau) angeboten werden. Die WHO möchte mit der International Medical Product Anti-Counterfeiting Taskforce (IMPACT) das Problem systematisch angehen. Allerdings wird in Europa bisher nur wenig über Fälschungen berichtet und diskutiert, u.a. weil die europäischen Pharmahersteller fürchten, dass ihre Medikamente in der Öffentlichkeit mit dem Problem in Verbindung gebracht werden.

6.1 Das Szenario der pharmazeutischen Lieferkette

6.1.1 Aufbau der Medikamenten-Lieferkette

Im Folgenden sind die konventionellen Arbeitsabläufe beim Warenstrom von der Industrie zum Kunden über den deutschen Großhandel dargestellt, um einige Rahmenbedingungen für eine mögliche Migration zu RFID-Systemen zu verdeutlichen. Eine Übersicht bietet die Webseite des deutschen Pharmazeutischen Großhandels [phagro06]. In Deutschland dürfen nur Arzneimittel in Verkehr gebracht werden, welche vom Bundesinstitut für Arzneimittel und Medizinprodukte oder dem Paul-Ehrlich-Institut für den Arzneimittelverkehr zugelassen wurden oder aber über eine EU-weite Zulassung bei der europäischen Arzneimittelagentur EMEA verfügen. Medikamente lassen sich nach ihrer Erhältlichkeit unterscheiden, was Auswirkungen auf die Art und Weise des Vertriebes hat:

- Frei verkäufliche Arzneimittel (auch außerhalb der Apotheke)
- Apothekenpflichtige Arzneimittel (Abgabe nur in Apotheken)
- Verschreibungspflichtige Arzneimittel (nur in Apotheken gegen Vorlage eines Rezeptes)
- Verkehrsfähiges Betäubungsmittel (nur in Apotheken gegen Vorlage eines Betäubungsmittelrezeptes)

Abb. 29 stellt die wichtigsten Vertriebswege für apothekenpflichtige Medikamente in Deutschland zusammenfassend dar. Für die Bestellungen wird meist die PZN verwendet, ein bundeseinheitlicher 7-stelliger Identifikationsschlüssel, der in Klarschrift und als Barcode (Code 39) auf jede Arzneimittelpackung gedruckt ist. Die PZN vereinfacht sowohl den Be-

stellprozess als auch den Abrechnungsprozess für Apotheken. Die öffentlichen Apotheken bestellen via PZN beim Großhandel meist kleinere (evt. auch nur Einzelpackungen). Der Großhandel bestellt via PZN entsprechend größere Mengen beim Pharmahersteller. Der Pharmahersteller führt die PZN zusätzlich zu seiner hausinternen Artikelnummer. Bei Bestellungen der Klinikapotheken und der klinikversorgenden Apotheken direkt beim Pharmahersteller bildet der Hersteller die PZN auf die hausinternen Artikelnummern ab. Die Medikamente werden mit den folgenden Angaben bezeichnet: Produktbezeichnung, Darreichungsform (z.B. Tabletten, Filmtabletten, Brausetabletten), Wirkstoffstärke, Packungsgröße, Pharmazeutischer Hersteller (Inverkehrbringer), PZN, Verfallsdatum und Chargenbezeichnung.

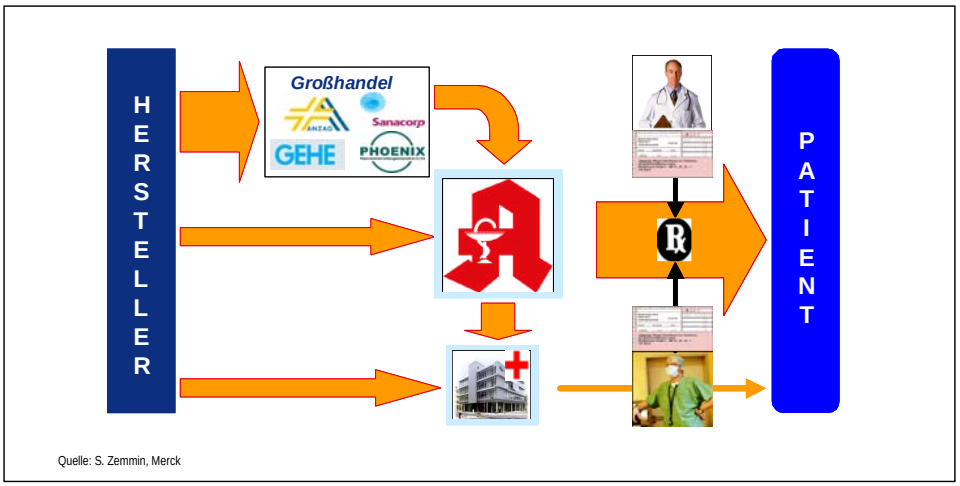


Abb. 29 – Vertriebswege von Medikamenten in Deutschland

Die Abb. 30 zeigt vereinfacht die Warenwirtschaftskette von Medikamenten, die mit den Chemielieferanten beginnt und in der die Kommunikation meist ausschließlich zwischen den benachbarten Teilnehmern der Lieferkette erfolgt.

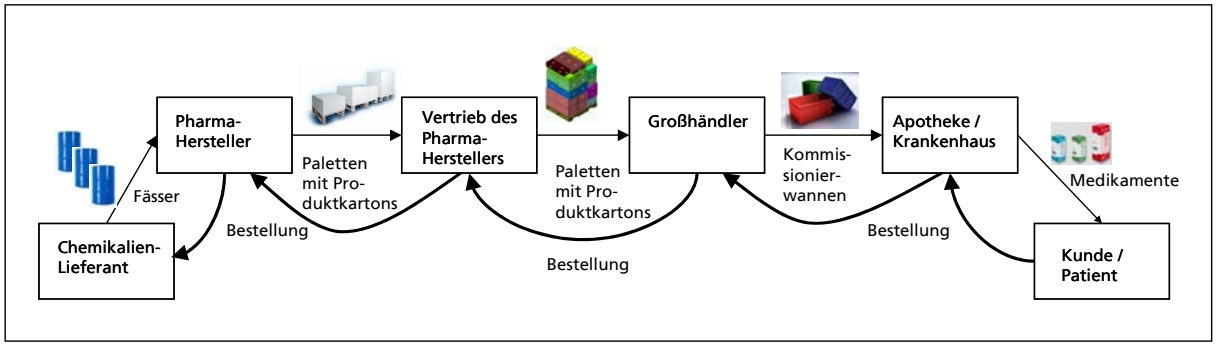


Abb. 30 – Medikamenten-Lieferkette ohne RFID (vereinfacht)

Vom Chemikalienlieferanten zum Pharmahersteller

Die chemische Industrie liefert die Rohstoffe und Grundbestandteile, die in der Pharmaindustrie zu Medikamenten verarbeitet werden.

Vom Pharmahersteller zum Großhandel

Die Pharmaindustrie liefert im Regelfall ihre Medikamente zunächst an ihre eigenen Tochterunternehmen, die jeweils innerhalb einer bestimmten Region (z.B. Staat, Land) für den Vertrieb der Medikamente zuständig sind. Der deutsche Pharmagroßhandel hält ca. 120.000 unterschiedliche Packungen für die Arzneimittelversorgung vorrätig und bestellt die Medikamente elektronisch bei den Vertriebsunternehmen der Industrie. Die Lieferung vom Vertriebslager an den Großhändler erfolgt zumeist per LKW. Beim Wareneingang im Großhandelsunternehmen wird die Ware evtl. gescannt und dann den Lagerplätzen zugeordnet.

Vom Großhandel in die Apotheken

Der Großhandel ruft die Warenwirtschaftssysteme der Apotheken zu festen Zeiten automatisiert an. Die Bestellung und ihre Bestätigung erfolgen weitgehend automatisch. Nur ein kleiner Anteil der Apotheken (ca. 5%) bestellt telefonisch. Eine Apotheke wird im Normalfall von zwei Großhandlungen beliefert und kann mit jedem Großhändler elektronisch kommunizieren. Alle bestellten Artikel werden pro Liefervorgang auf einem Lieferschein dokumentiert. Zu jeder Bestellung ordnet ein zentraler Server des Großhandelunternehmens einer Warenkiste aus Kunststoff (einer so genannten Kommissionierwanne) einen Barcode zu, der sich auch auf dem Lieferschein findet.

Die Warenkiste rollt auf Förderbändern durch das Großlager und wird, dem Barcode der Bestellung entsprechend, automatisiert oder per Hand befüllt. Viele Medikamente, z. B. Impfstoffe, benötigen eine spezielle Lagerung in Kühlschränken und einen besonderen Transport ohne Unterbrechung der Kühlkette. Für Medikamente, die unter das Betäubungsmittelgesetz fallen, gelten besondere Sicherheits- und Dokumentationsvorschriften, so der Schutz vor Diebstahl und Schwund und die Verwaltung durch besonders geschulte Mitarbeiter. Die gesetzlichen Vorschriften regeln, dass alle Arzneimittellieferungen nur in geschlossenen Behältnissen durchgeführt werden dürfen. Deshalb erhalten die gefüllten Warenkisten einen Deckel, der den Inhalt vor unbefugtem Zugriff schützt.

Die befüllten Warenkisten, die für ein Lieferfahrzeug vorgesehen sind, werden im Warenausgang zusammengestellt und den Fahrzeugen zugeordnet. Boten holen die Kisten ab und liefern sie an die Apotheken. Jeder Fahrer ist für die Beladung selbst verantwortlich. In Ballungsräumen kann die Belieferung meist binnen 60 Min. nach Eingang der Bestellung erfolgen. So können die Apotheken ihre Bevorratung optimieren und die Lagerung selten verkaufter Artikel weitestgehend auf den Großhandel übertragen. Die Lieferscheine befinden sich in den verschlossenen Kisten, um in der Apotheke die gesetzlich vorgeschriebene Prüfung und Dokumentation vornehmen zu können. Die Kiste selbst trägt die Anschrift der empfangenden Apotheke. Dort wird die Übereinstimmung von Lieferschein und gelieferter Ware vom Personal überprüft und die Ware ins Lager einsortiert. Die Fehlerquote bei der konventionellen Großhandelskommissionierung liegt im Promille-Bereich.

Von der Apotheke zum Endkunden

Der Kunde übergibt in der Apotheke das Rezept oder besorgt sich seine Medikamente im Rahmen der Selbstmedikation. Mittels Warenwirtschaftssystem wird geprüft, ob das Arzneimittel im Lager ist, ggf. im Warenwirtschaftssystem durch Scannen des Barcode als „abgegeben“ gekennzeichnet und dem Kunden ausgehändigt.

6.1.2 Maßnahmen gegen Medikamentenfälschungen

Die zunehmende Vielfalt an Vertriebswegen mit Parallelimporten und Re-Importen von zugelassenen Medikamenten aus dem Ausland und nicht zuletzt der Internethandel erschweren eine wirksame Kontrolle des Arzneimittelhandels und damit das Erkennen von Fälschungen. In Deutschland ist der Versandhandel (Internet-Apotheke) seit 2004 auch für apothekenpflichtige Medikamente zugelassen, d.h. Kunden dürfen apothekenpflichtige Medikamente online bestellen und über den Versand beziehen. Abb. 31 deutet die Komplexität der pharmazeutischen Lieferketten an. Eine ausführliche Analyse des Arzneimittelmarktes und der Fälschungsbekämpfung bietet [platzen06].

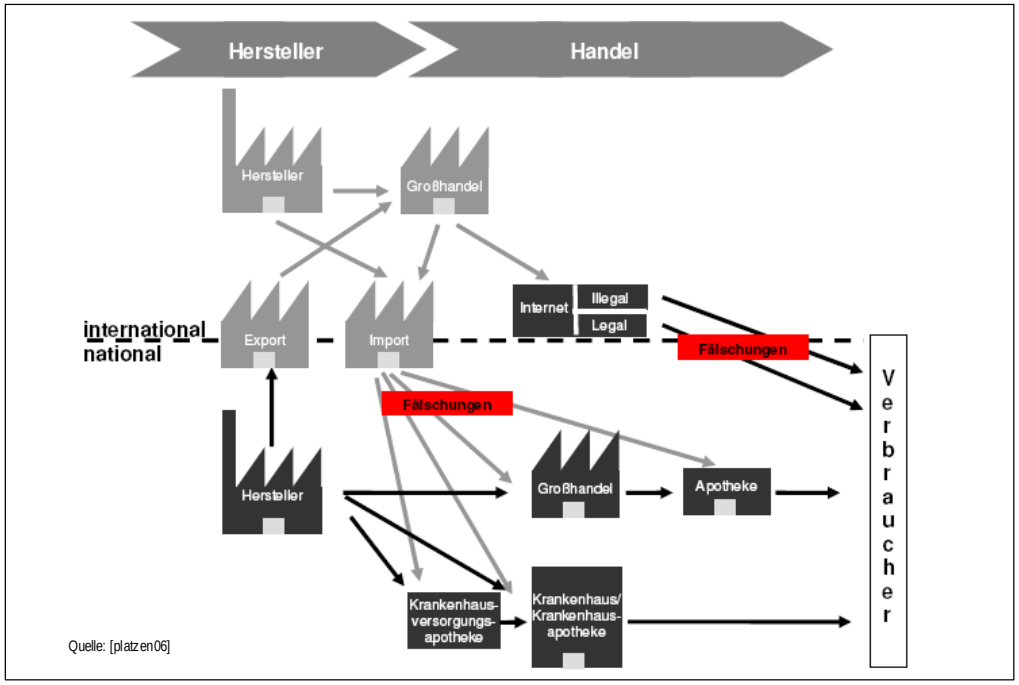


Abb. 31 – Komplexität der pharmazeutischen Lieferkette

Die bisherigen Ansätze gegen gefälschte Pharmazeutika beruhen auf Verfahren der Informationsstrategien (d.h. Aufklärung der Hersteller und Händler und Sensibilisierung der Endkunden, Warnungen und Rückrufaktionen) und Materialtechnologien wie chemische Verfahren und aufwändige Verpackungstechniken. Zu den chemischen Verfahren gehört das Hinzufügen von charakteristischen für den Menschen wirkungslosen biochemischen Markierungen in Medikamente (Intra-Rezeptur), deren Vorhandensein z.B. mit einem Immuntest nachweisbar ist. Auf Verpackungsebene können ein kompliziertes oder wechselndes Design, Wasserzeichen, digitale Wasserzeichen, integrierte Fasern, reaktive Tinte, Hologramme und Barcode verwendet werden. Alle genannten Verfahren sind statisch und bieten nur solange einen Schutz, bis ihre Nachahmung gelingt. Wichtig wären dynamische Verfahren, welche dem Produkt aktuelle und einzigartige Informationen (z.B. Seriennummer, Datum & Uhrzeit) hinzufügen und eine automatische Verifikation zulassen. Dies wird in großem Umfang erst durch die RFID-Technologie ermöglicht.

Die US-amerikanische Behörde Food and Drug Administration (FDA) empfiehlt daher den Einsatz von RFID-Chips und vollständigen Herkunftsnachweisen, um Medikamentenfälschungen zu verhindern [fda05]. Ab 2007 sollen Pharmahersteller und –händler zumindest in einigen US-Staaten wie Florida und Kalifornien RFID-Technologien einsetzen [büchel06]. Das betrifft auch die europäischen Unternehmen, die ihre Produkte dort vertreiben wollen. In Folge dieser Empfehlung wurden erste gesetzliche Initiativen (USA, Italien) angestoßen, welche eine Dokumentation des gesamten Herstellungs- und Vertriebsprozesses und den Herkunftsnachweis jeder Einzelpackung fordern. Mehrere Pharmaunternehmen wie GlaxoSmith-Kline, Purdue Pharma, Pfizer und Aventis setzen bereits entsprechende Technologie von IBM, Siemens, 7iD Technologies und anderen Herstellern ein oder bereiten deren Einsatz vor. In Europa gibt es bisher nur vereinzelt Pilotprojekte, z.B. eine Testimplementierung des finnischen Pharma-Herstellers Orion zusammen mit dem Verpackungshersteller Stora Enso zum RFID-Schutz von Medikamenten.

Neue Lösungen, wie die RFID-Technologie sie bietet, sind gerade im Pharma- und Gesundheitssektor gefragt, wenn es um anspruchsvolle Ziele wie lückenlose Datenerfassung und Fälschungssicherheit geht. Das Verhältnis von Produktwert zu Tag-Preis ist im Pharmasektor besonders günstig, und es spielen zudem höhere Werte wie Gesundheit (Safety) eine große Rolle [bercelon05]. Den RFID-Konzepten von EPCglobal [fleisch05] werden für eine vereinheitlichte Realisierung große Chancen eingeräumt [hdma03, hdma04, büchel06, platzen06].

6.1.3 Position des pharmazeutischen Großhandels zu RFID

RFID-Lösungen werden vom deutschen Bundesverband des pharmazeutischen Großhandels (PHAGRO) und seinen Mitgliedsunternehmen bisher abgelehnt. Der PHAGRO setzt stattdessen auf optische maschinenlesbare Packungsangaben und auf EAN 128 (statt Code 39), worin er sich mit den europäischen Großhandelsunternehmen einig ist. Hersteller wie Sanofi-Aventis entwickeln Technologien, welche der EAN zum Durchbruch verhelfen sollen. Der europäische Pharmaverband EFPIA hat sich im November 2006 für eine europaweite Einführung eines zweidimensionalen Codes ausgesprochen, der die EAN-Daten optisch lesbar abbildet. Mit dieser Technologie erhält jede Einzelpackung eines in Europa vertriebenen Arzneimittels ebenfalls eine eigene Seriennummer. In einer persönlichen Stellungnahme der PHAGRO-Geschäftsführung (vom 18.12.2006) zu RFID und EAN heißt es:

„Der pharmazeutische Großhandel lehnt RFID in der Logistikkette ab, da er der wichtigsten Anforderung nicht gerecht wird, Packungsangaben (z. B. Pharma-Zentral-Nummer, Charge, Verfalldatum) direkt am Lagerplatz verfügbar zu haben. Dies gewährleistet maschinenlesbar auf im Regelfall „kleinen“ Arzneimittelpackungen nur ein zweidimensionaler Code mit den Angaben in der Struktur des EAN 128. Dieser Vorteil optischer Verfahren ist im Pharma-Großhandel unverzichtbar, da zunehmend immer weniger Zeit für die Auftragsbearbeitung zur Verfügung steht. Auch sind nach unserer Kenntnis die verwendeten Frequenzen zu schwach, um bestimmte, für Arzneimittel typische Verpackungsmaterialien (z. B. Glas oder

Aluminium) zu durchdringen. Andere Frequenzen können sich negativ auf das Arzneimittel selbst auswirken. [3]

Neben dem Nachteil, dass bei der RFID-Technik Packungsdaten aus Datenbanken abgefragt werden müssen und dadurch Verzögerungen im Arbeitsablauf entstehen, stellt sich uns auch die Frage, wer solche Datenbanken aufbaut, pflegt und den Zugang kontrolliert. (...)
Uns liegen keine aktuellen Informationen darüber vor, welche deutschen Pharmafirmen den RFID vorantreiben. Unsere Arbeit im Zusammenhang mit dem zweidimensionalen Code und der EAN-128-Struktur ist gekoppelt mit entsprechenden technischen Lösungen des deutschen Pharmamarktführers Sanofi-Aventis. Wir begrüßen jede Maßnahme zur Abwehr von Arzneimittelfälschungen. Ob RFID hierzu geeignet ist, wurde von unseren technischen Ausschüssen nicht geprüft."
RFID-Systemlösungen werden also noch nicht als ein effizienter Schutz gegen Arzneimittelfälschungen wahrgenommen. Führende deutsche Pharmahersteller wie Bayer und Boehringer Ingelheim engagieren sich allerdings inzwischen bei EPCglobal und könnten sich dafür einsetzen, die in Deutschland etablierte Pharmazentralnummer (PZN) in das EPC-System aufzunehmen, um der Einführung von RFID in Deutschland Vorschub zu leisten [büchel06]. Die Kennzeichnung pharmazeutischer Produkte kann (und wird auch teilweise bereits) mit EAN 13 erfolgen. Dies muss aber IFA (Informationsstelle für Arzneispezialitäten GmbH) gemeldet werden, die EAN 13 auf die PZN abbildet. Vorteile der EAN 13 sind neben der Internationalität auch die Integration in das EPC-Nummerierungsschema.

6.1.4 Mögliche Einsatzbereiche von RFID

RFID-Lösungen im Pharmasektor können nicht nur die Effizienz der Lieferkette verbessern, sondern auch für mehr Medikamentensicherheit gegen Plagiate sorgen und die Erkennung von minderwertigen Fälschungen ermöglichen. Eine Einführung zur RFID-Nutzung in der Lieferkette der Pharmaindustrie bietet [koh03]. Die RFID-Technologie kann zwei Maßnahmen unterstützen, um gefälschte Medikamente zu identifizieren: Durch Anfrage an einen Service können alle echten Einheiten eines Medikaments identifiziert werden, falls jede Medikamenteneinheit eine einzigartige Kennung (z.B. EPC) besitzt und das System deren Verifizierung unterstützt. Die zweite Maßnahme ist das dynamische Tracking und Tracing, d.h. die Verfolgung von Produkten entlang der Lieferkette. Das Tracking ermöglicht die aktuelle Lokalisierung des Medikaments und die Ermittlung des Lieferstatus. Das Tracing kann den bisherigen Sendungsverlauf komplett darstellen. Das Tracking und Tracing ermöglicht z.B. die Beantwortung folgender Fragen, welche an verschiedenen Stellen der Lieferkette auftreten können:

- Welche Produkte enthalten die Rohstoffe bestimmter Chargen?
- Wo befindet sich die Medikamentenlieferung gerade?
- Wohin sollte das fehlgeleitete Medikament eigentlich geliefert werden?
- Welche Apotheken wurden mit der Medikamenten-Charge beliefert?

[3] Anmerkung der Autoren: Dies ist ein offenes Forschungsfeld – es gibt unseres Wissens keine Untersuchungen, die diese Aussage stützen.

- Welcher Hersteller steht hinter diesem Medikament?
- Woher stammt der Inhalt dieser Medikamentenpackung ursprünglich?
- Enthält das Medikament dieses bestimmte Allergen?

Mittels einer eindeutigen Kennung jeder Medikamentenpackung können produktbezogene Daten („Worum handelt es sich?“), Lokalisierungsdaten („Wo wurde es erfasst?“), Zeitdaten („Wann wurde es erfasst?“) und Prozessdaten („Warum und von wem wurde es erfasst?“) mit der Kennung verlinkt werden. Für fehlgeleitete Medikamente kann auch nachträglich die Ursache nachvollzogen werden. Anwendungsbeispiele für Recherchen sind die Prüfung der Echtheit von Medikamenten, die Ursachensuche bei Fehlleitung von Medikamenten und die Informationsbeschaffung zur Durchführung von gezielten Rückruf-Aktionen. Das Tracking & Tracing eignet sich evt. sogar für die Strafverfolgung, da nicht nur Fälschungen identifiziert werden können, sondern bis zu einem gewissen Rahmen auch deren Eintritt in die pharmazeutische Lieferkette.

Abb. 32 zeigt mögliche RFID-Einsatzbereiche in der pharmazeutischen Lieferkette über die bloße Lieferkette hinaus. Dazu gehört der Einsatz von Sensoren (z.B. in der Kühlkette von Medikamenten), die Detektion von EPC-Fehlern und Tag-Duplikaten zur Identifizierung möglicher Medikamentenfälschungen, der Vergleich von Verordnungsdaten mit den EPCs der ausgegebenen Medikamente in Apotheken und Krankenhäusern und schließlich die Erfassung von Tags beim Recycling und Entsorgen von alten Medikamenten. Die folgenden Kapitel beschränken sich aber auf das grundlegende Szenario, den RFID-Einsatz in der Lieferkette bis zum Verkauf des Medikaments an den Endkunden.

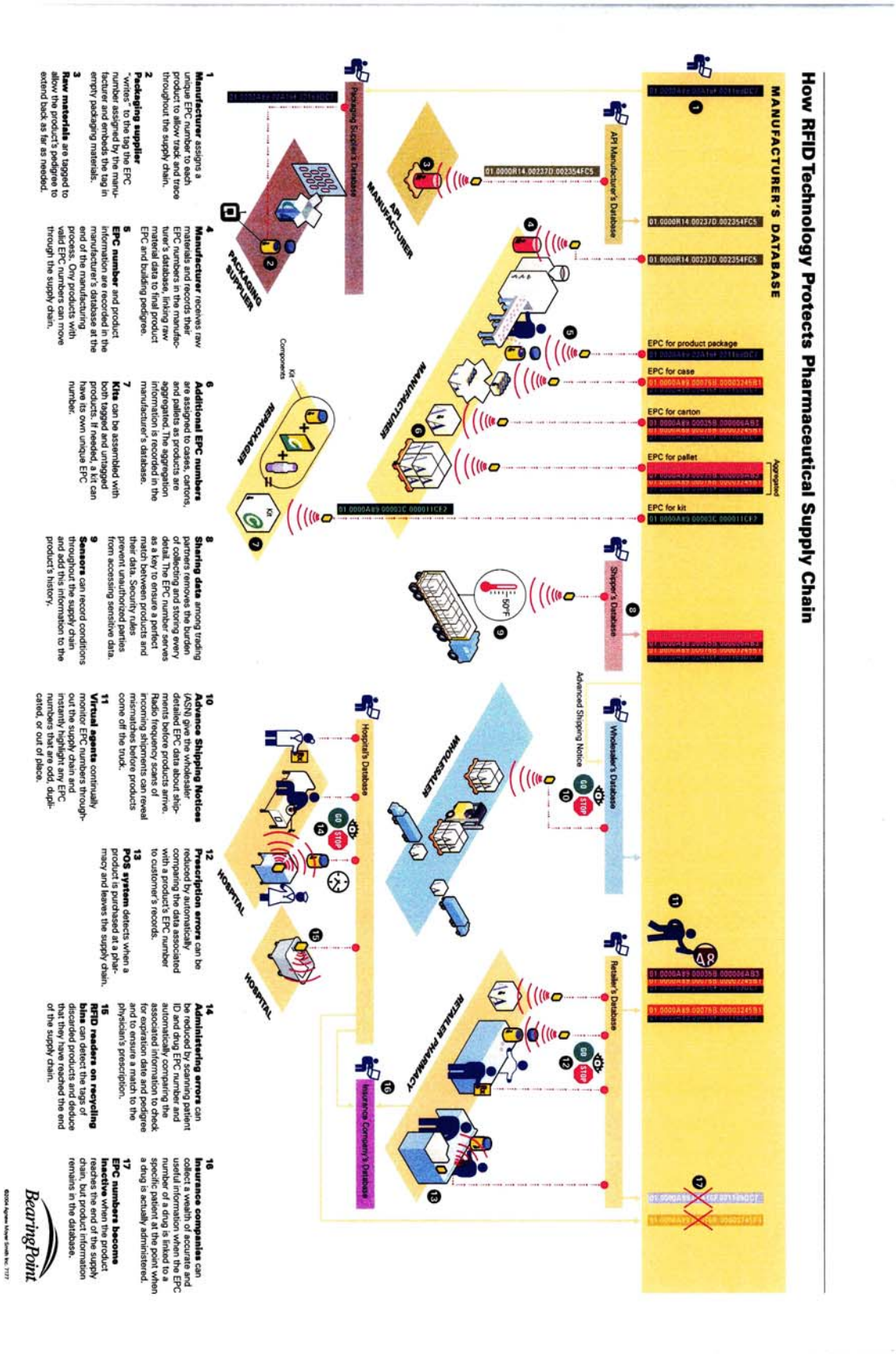


Abb. 32 – Nutzungsmöglichkeiten des EPC in der pharmazeutischen Lieferkette
Quelle: [bearingpoint04]

6.1.5 Absicherung der Medikamenten-Lieferkette

Für diese Studie konnten in Deutschland keine Pilotprojekte zum Medikamentenschutz mit RFID ausfindig gemacht werden. Daher wurde über IBM Deutschland Kontakt zu IBM USA aufgenommen, um Informationen über die dortigen Projekte zu bekommen. Im Folgenden wird das von IBM speziell für den Pharmabereich entwickeltes RFID-System skizziert, das in Pilotprogrammen in den USA bereits im Einsatz ist, und auf Basis des EPC den elektronischen Herkunftsnachweis (electronic pedigree) und die Produktauthentisierung unterstützt. Die dargestellten Informationen über das implementierte RFID-System stammen direkt vom Technologieanbieter IBM. Über die Anwender des Systems, die IBM-Kunden in der US-amerikanischen pharmazeutischen Industrie, werden im Rahmen dieser Studie auf Wunsch von IBM keine Aussagen gemacht.

Lieferkette mit RFID-Systemen von IBM

In Abb. 33 ist die IBM-Lösung skizziert, welche die Medikamenten-Lieferkette mit RFID-Systemen und einem EPCglobal-konformen Netzwerk zum Informationsaustausch zwischen den teilnehmenden Instanzen umfasst. Der individuelle EPC auf dem RFID-Tag jeder Einzelverpackung und die EPC Information Services (EPCIS) mit dem EPC-Protokoll für den Datenaustausch der beteiligten Instanzen über das EPCglobal Network bilden die Basis der Entwicklung. Das System integriert RFID-Hardware und die RFID-Middleware von IBM, welche die Daten der pharmazeutischen Lieferkette synchron zum parallelen Warenfluss erfasst. Mit der Übermittlung des EPC werden die Daten auf lokalen EPCIS-Servern abgelegt und können von berechtigten Teilnehmern über das Netzwerk abgerufen werden.

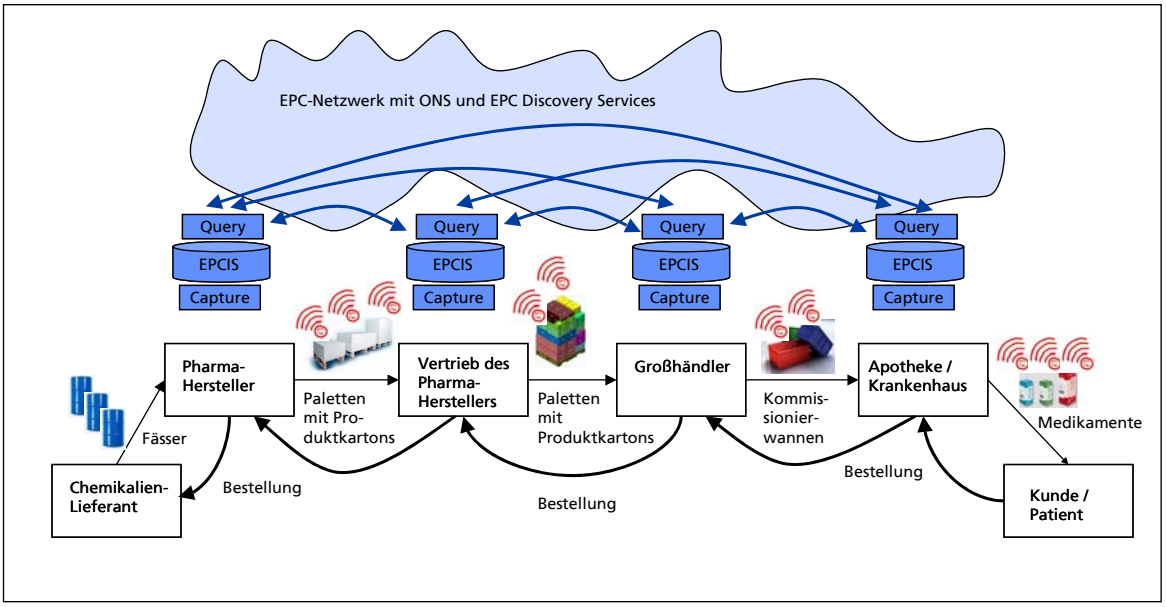


Abb. 33 – Medikamenten-Lieferkette mit EPC-basierten RFID-Systemen (vereinfacht)

Zur Prüfung der Echtheit kann der EPC an jeder Stelle der Lieferkette verifiziert werden. Dazu dienen Anfragen an einen Service, der alle echten Produkteinheiten identifizieren kann. Der EPC verweist auf Informationen z.B. über den aktuellen Standort, die bisher durchlaufenen Standorte, die jeweilige Aufenthaltsdauer, Aufzeichnungen der Besitzer und die Produktzusammensetzung. Die Bestellungen der Produkte erfolgt grundsätzlich außerhalb des Sys-

tems (unter Beibehaltung der konventionellen Abläufe), doch unterstützt das System sowohl Links auf Bestellungen in Warenwirtschaftssystemen als auch Funktionen zur Überwachung von Logistikprozessen. Grundsätzlich könnte jeder Teilnehmer der Lieferkette die von IBM realisierten RFID-unterstützten Prozesse nutzen. Die Chemikalienlieferanten sind jedoch bisher nicht in die RFID-unterstützte Lieferkette integriert. Nach Auskunft von IBM haben Chemieunternehmen durchaus Interesse an RFID-Lösungen, werden darin aber nicht von den Pharmaherstellern unterstützt.

RFID-Systemarchitektur von IBM

Abb. 34 zeigt die EPC-konforme RFID-Systemarchitektur von IBM, die lokal bei jedem Teilnehmer der Lieferkette implementiert werden kann. Die „WebSphere RFID Device Infrastructure“ ist die Middleware von IBM, welche die Schnittstelle zur RFID-Hardware bildet. Sie nimmt die RFID-Daten entgegen und filtert z.B. redundant aufgezeichnete Daten heraus. Der darüber liegende „WebSphere RFID Premises Server“ generiert aus den gefilterten Daten RFID-Events, welche über das Capture-Interface an das „WebSphere RFID Information Center“ weiter gegeben werden. Diese ist die zentrale Komponente des IBM-Systems zur Bereitstellung von EPC-Informationen und entspricht dem EPCIS bei EPCglobal. Das darüber liegende Query-Interface zum EPC-Netzwerk ermöglicht den Informationsaustausch mit den anderen Teilnehmern der Lieferkette. Die EPCIS-Spezifikation definiert vier verschiedene XML-basierte Events (so genannte Object-, Aggregation-, Quantity- und Transaction-Events), mit denen die Ereignisse des RFID-Systems und der Produktions- und Verwaltungssysteme des Unternehmens kommuniziert werden können.

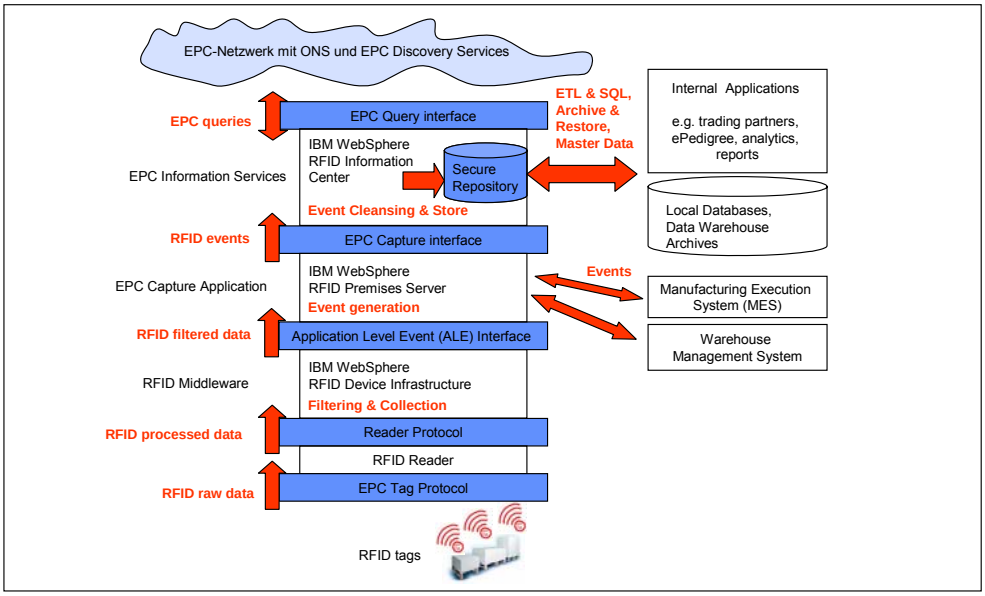


Abb. 34 – EPC-Architektur des RFID-Systems von IBM

RFID-unterstützte Prozesse

Die IBM-Lösung unterstützt neben EPC-basierten HF- und UHF-Tags auch die Verwendung von Barcodes, die ggf. beim Empfang einer Lieferung zusätzlich zur automatischen Erfas-

sung der Tag-Daten mit tragbaren Barcode-Scannern eingelesen werden müssen. Jede Produktlieferung kann mittels automatisierter EPCIS-Anfragen sowohl vom Absender als auch vom Empfänger hinsichtlich Inhalts, Lieferstatus, Lieferzeitraum, Zielort etc. überwacht werden. EPCIS-Reports informieren über Ereignisse und auftretende Fehler. Die wichtigsten Schritte der RFID-gestützten Produktion und Lieferung sind die folgenden:

1. **Zuordnen der Seriennummern**
   Der Chiphersteller liefert die Tags mit jeweils eindeutiger Seriennummer (Tag-ID) als Burnt-In-Code an den Verpackungshersteller, welcher die Tags (noch ohne EPC) in die Verpackungen bzw. Produktbehälter integriert. Der Pharmahersteller weist den verschiedenen Produkten die Objektklassen der EPCs und schließlich den einzelnen Produkteinheiten die Produktseriennummern der EPCs zu.
2. **Verpacken der Produkteinheiten**
   Der Pharmahersteller schreibt die individuellen EPCs in die Tags. Bei der Abfüllung und Verpackung der Produkte werden die EPCs aus den HF- und UHF-Tags gelesen und zusammen mit der Produktinformation gespeichert. Die Anwendung zur EPC-Erfassung generiert im Zusammenspiel mit dem Manufacturing Execution System (MES) entsprechende Events und speichert sie für spätere Abfragen im EPCIS. Die Gebinde mit mehreren Produkteinheiten des gleichen Typs werden mit UHF-Tags gekennzeichnet. Zusätzlich können auch Paletten mit UHF-Tags ausgezeichnet und erfasst werden. Die EPCs der Produkte, Bündelverpackungen und Paletten werden im EPCIS zusammengeführt. Ausschließlich Produkte mit funktionsfähigen Tags werden für die Lieferkette freigegeben.
3. **Versenden der Lieferung an ein Vertriebsunternehmen**
   Die Lieferung bestellter Produkte erfolgt auf Basis von Paletten oder Gebinden. Diese werden am Transportband oder am Hallentor mittels RFID erfasst und zum Herkunftsnachweis als Event im EPCIS gespeichert.
4. **Empfangen der Lieferung im Vertriebsunternehmen**
   Im Vertriebszentrum wird der Empfang der Lieferung auf Basis von Einzelprodukten, Gebinden oder Paletten erfasst und für den Herkunftsnachweis im lokalen EPCIS gespeichert. Die Echtheit der gelieferten Produkte wird durch Anfrage beim EPCIS des Herstellers überprüft (siehe unten).
5. **Bewegen der Produkte im Vertriebsunternehmen**
   Nach dem Empfang der Produkte kann auch die Lagerung, das Auffüllen von Kommissionierungsgeräten, das Auftrennen von Gebinden und Paletten etc. durch Events kontrolliert und protokolliert werden.
6. **Kommissionieren im Vertriebsunternehmen**
   Aufgrund bestehender Verweise auf Bestellungen in den Verwaltungssystemen unterstützt das RFID-System das automatische Packen der bestellten Produkte (Kommissionierung) und speichert den Vorgang als Event im EPCIS.
7. **Versenden der Lieferung an eine Apotheke**
   Aufgrund bestehender Verweise auf Lieferungen in den Verwaltungssystemen werden die bestellten Produkte in Gebinden oder als Einzelprodukte versendet. Die Sendung wird am Transportband oder am Hallentor mittels RFID erfasst und als Event im EPCIS gespeichert.

8. **Empfangen der Lieferung in der Apotheke**
   In der Apotheke wird der Empfang der Lieferung auf Basis von Einzelprodukten erfasst und für den Herkunftsnachweis im lokalen EPCIS gespeichert. Die Echtheit der gelieferten Produkte wird durch Anfrage beim EPCIS des Herstellers überprüft.

Verwendete RFID-Hardware

Zum Tagging einzelner Produkteinheiten setzen die Anwender der IBM-Technologie HF-Tags der Hersteller Symbol, TI, Alien, Impinj und Intermec ein, welche konform zu ISO 15693 (der Grundlage von ISO 18000-3 Mode 1) und ISO 18000-3 Mode 2 sind. Letzterer Standard ermöglicht sehr hohe Datenraten, d.h. 424 kbit/s vom Leser zum Tag bzw. 106 kbit/s vom Tag zum Leser, wobei letztere Datenrate durch Frequenzsprünge und die parallele Nutzung von acht Kanälen bis auf 848 kbit/s gesteigert werden kann (siehe 2.2.1). Dadurch können bis zu 1200 Tags pro Sekunde identifiziert werden [magellan06]. Zur Kennzeichnung von Gebinden und Paletten dienen ISO 18000-6c-konforme UHF-Tags der Hersteller TI, Tagsys und Raflatec.

Verwendete RFID-Middleware

Das eingesetzte RFID Solution Framework von IBM ermöglicht eine flexible Integration von RFID durch separate funktionale Domänen [schollenberger06]. Abb. 35 stellt eine logische Sicht auf die Architektur dar.

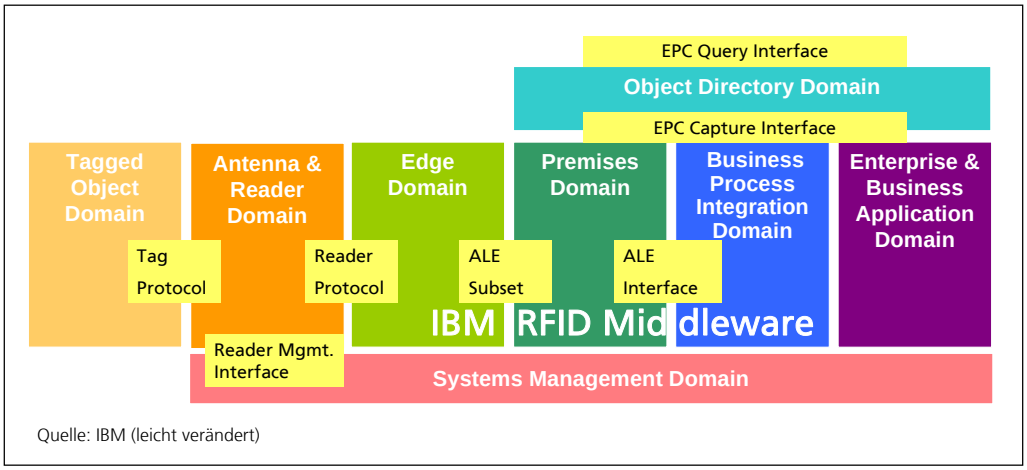


Abb. 35 – IBM RFID Domain Architecture

Die Middleware umfasst die Edge-, Premises- und Business Process Integration-Dömänen und das RFID-System-Management. Sie verbindet damit in drei Schritten (Geräteadaption, Logik und Adaption an die Unternehmensanwendungen) die RFID-Geräte mit den Unternehmenssystemen, wobei zur Kommunikation der gefilterten Daten die EPC-Schnittstelle der Application Level Events (ALE) implementiert ist [epc-ale]. Die Sicherheit und der Datenschutz werden zentral vom System-Management gesteuert. Die IBM WebSphere-Produkte decken die gesamte RFID-Funktionalität ab (vgl. Abb. 34).

Anbindung an das EPC-Netzwerk

Die Schnittstelle zum EPC-Netzwerk liegt in der Object Directory-Domäne, welche die EPC-Daten verwaltet und diese über ein EPC Query Interface anderen Unternehmen zur Verfügung stellt. Diese Domäne entspricht einem lokalen EPCIS. Eingesetzt werden aktuelle Sicherheitstechnologien für Internet und Datenbanken zur Autorisierung und Authentisierung der zugreifenden Instanzen, z.B.:

- Gegenseitige Authentisierung auf Anwendungsebene mit SSL unter Verwendung von X.509-Zertifikaten der Teilnehmer
- Web-Security von LDAP-Servern mit Registrierung und der Vergabe sowohl von rollenbasierten als auch von individuellen Zugriffsrechten
- Bearbeitung der XML-basierten Anfragen auf Basis der eingestellten Zugriffsrechte für eine selektive individuelle Datensichtbarkeit

Abb. 36 zeigt das zugrunde liegende EPC-Modell für den sicheren Austausch von EPC-bezogenen Produktdaten. Jedes Unternehmen ist für die RFID-Hardware, die Konfiguration der EPC-fähigen Middleware, die Datenhaltung und die Rechtevergabe auf Daten im lokalen EPCIS verantwortlich.

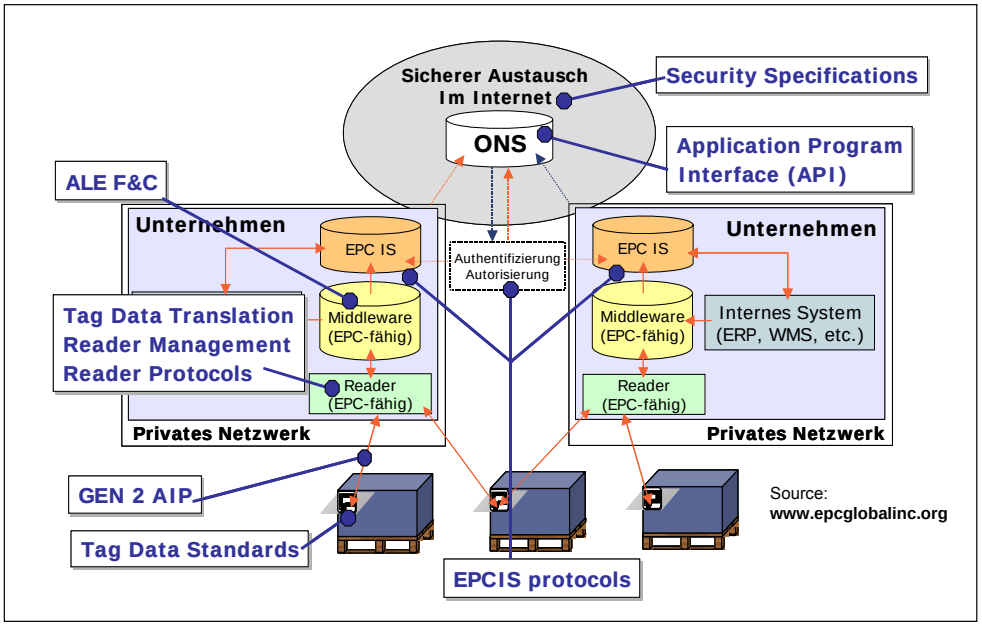


Abb. 36 – EPC-Modell zur sicheren Verknüpfung lokaler RFID-Systeme

Prinzipien der Informationsverwaltung

Grundsätzlich kann jeder (auch der Endkunde oder eine unbeteiligte Instanz) mittels der ihm vorliegenden EPC-Daten die zugehörigen Produktinformationen anfordern. Die jeweilige Antwort hängt von derjenigen Instanz ab, die für die EPCIS-Informationen verantwortlich ist. Sie entscheidet durch das Setzen von Zugriffsrechten, welche Informationen überhaupt zur Verfügung gestellt werden und welche Sicherheitseinstellungen (Autorisierung, Authentisierung)

die Daten im EPCIS schützen. Die Default-Einstellungen des IBM-Produktes erlauben keinen Zugriff auf irgendwelche Daten. Zusammenfassend kommen in der IBM-Systemarchitektur die folgenden Prinzipien der Datenhaltung und Kommunikation zur Anwendung:

- **Minimale Tag-Daten**: Verwendet werden passive RFID-Tags, welche einen Unique Identifier (UID, Tag-ID) und den EPC enthalten. Die statische Tag-ID wird vom Chipherstellers als Burnt-In-Code eingetragen und enthält eine Kennung des Chipherstellers und eine eindeutige Seriennummer des Chips. Der EPC wird vom Pharmahersteller in den Tag geschrieben. Jede weitere Nutzung des Tags erfolgt im Read-Only-Modus. Anwendungsdaten werden nicht im Tag gespeichert.
- **Trennung von Datenerfassung und Datennutzung**: Die RFID-Middleware und die Funktionen der Object Directory-Domäne realisieren eine strikte Trennung von Datenerfassung und Datennutzung. Von außen ist die EPCIS-Komponente nur durch XML-parametrisierte Abfragen zugänglich, ohne dass Daten innerhalb des EPCIS geändert werden können. Die Middleware schützt die RFID-Hardwarekomponenten gegen äußere Einflüsse aus dem EPC-Netzwerk. Es gibt weder einen direkten Zugriff auf die geschützte Datenbank, noch auf die Komponenten der Datenerfassung.
- **Lokale Informationshaltung**: Die EPC-bezogenen Produktdaten werden lokal gehalten und nur auf Anfrage nach erfolgter Authentisierung freigegeben. Die Information verbleibt also grundsätzlich bei demjenigen Teilnehmer, bei dem sie entsteht, d.h. es gibt keine zentrale Datenhaltung, nur lokale EPCIS mit eingebetteter Datenbank. Ausgewählte Informationen werden nur auf Anfrage weiter gegeben, d.h. es gibt kein automatisches Pushing und keine Verteilung oder ineffiziente Synchronisation von Daten.
- **Automatisierte Anfragen**: Die Teilnehmer der Lieferkette können Informationen über zukünftige Ereignisse (Lieferung, Empfang) abonnieren, damit die Informationen bereits zu dem Zeitpunkt vorliegen, wenn die EPCs der erhaltenen Produkte eingelesen werden. Damit können Unstimmigkeiten (falsche Lieferung, Duplikate etc.) bereits bei der Annahme der Produkte erkannt werden.
- **Elektronischer Herkunftsnachweis**: Unterstützt wird der elektronische Herkunftsnachweis auf der Ebene jeder einzelnen Produktpackung. Für einen gesamten Nachweis müssen zurzeit noch alle beteiligten EPCIS der Lieferkette direkt abgefragt werden. Zukünftig soll eine Abfrage beim letzten EPCIS in der Lieferkette ausreichen, wobei die zurückliegenden EPCIS-Informationen automatisch im Hintergrund abgerufen werden. Auch die Einführung von digitalen Signaturen als Teil des Herkunftsnachweises ist geplant.

Echtheitsprüfung des Medikaments

Die Empfänger von Medikamentenlieferungen können die Echtheit jeder empfangenen Produkteinheit beim Hersteller überprüfen. Dazu wird die Kommunikation zwischen dem Produkthersteller und den anderen Teilnehmern der Lieferkette durch SSL gesichert. Jede Seite stellt mit einem Zertifikat ihren öffentlichen Schlüssel zur Verfügung. Der Hersteller und jeder Teilnehmer können für die anderen Teilnehmer bestimmte Informationsattribute festlegen und bestimmen damit, welche Daten den anderen Teilnehmern sichtbar sind. Die Echtheitsprüfung läuft in den folgenden Schritten ab:

1. **Lesen der Tag-Daten**
   Während des Produktempfangs werden die Tag-ID und der EPC aus dem Tag des Einzelprodukts gelesen. Alternativ kann das Tag eines Gebindes gelesen und die Tag-Daten der Einzelpackungen als Look-Up-Tabelle erfragt werden.
2. **Ermitteln des EPCIS**
   Mit dem Hersteller-Präfix des EPC wird beim ONS der EPCIS des Herstellers erfragt.
3. **Senden der Echtheits-Anfrage**
   Mit Tag-ID und EPC wird beim EPCIS des Herstellers erfragt, ob das Produkt bekannt ist.
4. **Empfangen und Auswerten der Antwort**
   Der EPCIS des Herstellers antwortet mit einem Nachweis des Auftrags, falls das Produkt echt ist, oder mit einer Fehlermeldung, falls Tag-ID und EPC unbekannt, nicht glaubhaft oder fehlgeleitet sind. Alle Anfragen und Antworten werden protokolliert. Im Falle einer Fehlermeldung kann der Empfänger z.B. eine Qualitätssicherung oder die Rücksendung des Gebindes an den Absender veranlassen.

Die Echtheitsprüfung beruht auf einem Vergleich der Tag-ID (Burnt-In-Code) und des EPC in der Anfrage mit den beim Hersteller hinterlegten Daten und geht davon aus, dass identische Daten nicht ein zweites Mal vorkommen bzw. aufgrund der Protokollierung auffallen würden. Das System unterstützt nach Angaben von IBM die Erkennung von Duplikaten, Authentisierungsfehlern und unechten Events. Einerseits würden zwar Duplikate auffallen, andererseits kann das System die Angabe des Tagtyps nicht verifizieren, d.h. kann nicht ohne Weiteres feststellen, welches Tag das Original und welches die Fälschung ist. Bei dem Burnt-In-Code handelt es sich vielmehr um einen zusätzlichen Schritt, welcher das Klonen erschweren kann.

6.2 Sicherheitsanforderungen der pharmazeutischen Lieferkette

6.2.1 Anwendungsspezifische Angriffsszenarien

Das Fälschen getaggter Medikamente kann grob betrachtet den folgenden Strategien folgen, welche auch für andere Produktfälschungen angewandt werden:

- Das Auslassen der Sicherheitsmerkmale, d.h. Medikamentenfälschungen ohne Tags
- Das Nachahmen von Sicherheitsmerkmalen, d.h. Medikamentenfälschungen mit beliebigen falschen Tags („Billige Fälschung“)
- Das Entfernen und Wiedereinsetzen von Sicherheitsmerkmalen, d.h. Medikamentenfälschungen mit gültigen Tags
- Das Klonen und professionelle Imitieren von Sicherheitsmerkmalen, d.h. Medikamentenfälschungen mit Tag-Duplikaten („Professionelle Fälschung“)

Bei Medikamentenfälschungen ist es dagegen eher unwahrscheinlich, dass Fälscher direkt die RFID-Systeme der rechtmäßigen Pharmaherstellern und Teilnehmer der Lieferkette stören, da gefälschte Produkte (zumindest was die Situation in Deutschland betrifft) durch Importe in die Lieferketten einschleust werden. Fälscher kommen selbst vermutlich kaum mit den originalen Produktionsstätten in Kontakt. Wahrscheinlicher ist aber, dass sich Vertriebsunternehmen der Lieferkette indirekt an den Fälschungen beteiligen, indem sie die Herkunft der Medikamente unzureichend kontrollieren oder bewusst gefälschte Produkte importieren, umdeklarieren und unter die Originalprodukte mischen. Dazu wäre eine direkte Manipulation der eigenen lokalen Produktdaten in den Backend-Systemen und den EPC Information Services vermutlich leichter als im eigenen Betrieb aktive Angriffe wie Spoofing, Replay-, Relay- und andere Man-in-the-Middle-Attacken an der Luftschnittstelle des RFID-Systems durchzuführen.
Als Ziel der Fälscher und an Fälschungen Beteiligter wird angenommen, dass sich die gefälschten Produkte möglichst unauffällig in der Lieferkette bewegen sollen, ohne die Erfassung der originalen Produkte zu stören. Daher sind Denial-of-Service-Attacken und Angriffe mit RFID-Malware eher unwahrscheinlich. Auch der Bedrohung der Privatsphäre durch das Tracking von Medikamenten wird im Kontext von Fälschungen keine Bedeutung zugemessen. Die wichtigsten Bedrohungen sollen im Folgenden an vier Angriffsszenarien, welche die oben genannten Fälschungsstrategien repräsentieren, deutlich werden.

Angriffsszenario 1: Medikamentenfälschungen ohne Tags

Die Fälscher schleusen wie bisher gefälschte Medikamente ohne Tags in die Lieferketten ein und verlassen sich darauf, dass diese neben getaggten Originalprodukten innerhalb der Lieferkette nicht auffallen.
Problem: Teilnehmer der Lieferkette könnten Produktfälschungen unterstützen, diese auch ohne Tags als echte Medikamente deklarieren und an die nächste Instanz der Lieferkette oder an die Endkunden weitergeben.
Lösungsansätze: Neben der notwendigen Aufklärung aller Teilnehmer der Lieferkette und der Endkunden über getaggte Medikamente und Echtheitsprüfungen sollten automatische Prozesse etabliert werden, welche ein Durchgehen von ungetaggten Produkten verhindern. Produkte mit schadhaften oder fehlenden Tags gehören ausgesondert und einer Qualitätskontrolle unterzogen. Die sicherste Lösung bietet der elektronische Herkunftsnachweis, welcher in jedem Abschnitt der Lieferkette abgerufen werden kann und einen lückenlosen Nachweis aller bisher durchlaufenen Instanzen enthält. Dieser Nachweis könnte auch auf Basis optisch sichtbarer Daten (z.B. mit einem aufgedruckten Produktcode) abrufbar sein. Spätestens am Ende der Lieferkette vor Abgabe an den Endkunden sollte die Echtheit des Produkts überprüft werden.

Angriffsszenario 2: Medikamentenfälschungen mit billigen Tags

Fälscher imitieren vor allem die äußeren Sicherheitsmerkmale der Originalmedikamente. Sie bringen zudem programmierbare Tags an, tragen darin Produktcodes mit Angaben des Pharmaherstellers und Produkttyps der originalen Medikamente und dazu frei erfundene Seriennummern ein. Die Medikamentenfälschungen sehen schließlich dem Original äußerlich

sehr ähnlich und antworten auf Anfrage rechtmäßiger RFID-Leser mit zunächst plausibel aussehenden Daten.
Probleme: Programmierbare Tags sind auf dem Markt erhältlich und können mit gültig erscheinenden Daten ausgestattet werden. Rechtmäßig eingesetzte Tags sind in der Praxis meist ohne vorherige Prüfung ihrer Echtheit frei auslesbar, so dass unrechtmäßige Tags aus anderen Quellen nicht unbedingt auffallen.
Lösungsansätze: Eine erste Maßnahme ist die zufällige oder nach geheimem Verfahren Vergabe von Seriennummern, so dass gültige Werte für Angreifer schwierig zu erraten sind. Eine weitere Maßnahme ist die Verwendung von einmaligen Kennungen (z.B. Tag-ID und EPC) für jedes Produkt und die automatische Prüfung dieser Tag-Kennungen auf gültige Kombinationen. Damit verbunden ist die Prüfung, ob das Produkt überhaupt beim Hersteller registriert ist oder ob der Produktcode unzulässigerweise mehrfach im Umlauf ist. Ein elektronischer Herkunftsnachweis auf Basis des Produktcodes müsste eine Plausibilitätsprüfung einschließen, ob die gemachten Angaben grundsätzlich auf das vorliegende Produkt zutreffen können. Zusätzlich oder als Alternative zur Online-Abfrage wäre eine kryptographische Echtheitsprüfung des Tags sinnvoll.

Angriffsszenario 3: Medikamentenfälschungen mit originalen Tags

Fälscher besorgen sich gültige Tags oder getaggte Verpackungen (evt. vom gleichen Verpackungshersteller wie der rechtmäßige Pharmahersteller oder aus dem Recycling) und verwenden diese Tags für Medikamentenfälschungen, die in die Lieferkette geschleust werden. Bei den Fälschungen könnte es sich auch um Medikamente abgelaufenen Datums (Recycling) oder aus Rückrufaktionen handeln, die von den Fälschern umdeklariert werden. Tags werden dazu von Originalverpackungen entfernt und in neue Verpackungen integriert, welche aktuellere oder scheinbar gültige Daten aufgedruckt haben. Die Daten der originalen Tags (z.B. der Produkttyp) werden bei Bedarf durch Spoofing manipuliert, um mit den Informationen der neuen Verpackung überein zu stimmen.
Probleme: Angreifer könnten leicht Zugang zu Tags und Verpackungen bekommen. Tags enthalten evt. schon vor der Produktion alle Kennungen oder sind im Gegenteil noch frei programmierbar. Die Tags von alten oder zurückgerufenen Medikamenten sind unter Umständen nicht deaktiviert und sind damit nochmals verwendbar oder sogar wieder beschreibbar.
Lösungsansätze: Das Tag sollte eine einmalige Chip-Kennung besitzen, die nach der Chip-Herstellung gegen Überschreiben gesperrt ist. Die Programmierung der EPCs sollte zugriffsgeschützt erst beim Pharmahersteller erfolgen, der während der Produktion die Kennungen registriert. Es ist wichtig, dass die Tags die permanente Sperrung von Speicherbereichen unterstützen und deaktiviert werden können. Die wichtigste Maßnahme ist der elektronische Herkunftsnachweis, der möglichst einen Produktstatus mit Werten wie z.B. „im Vertrieb“, „verkauft“, „abgelaufen“ oder „zurückgerufen“ enthalten und folglich auch nach dem Verkauf oder Ablauf des Medikaments abrufbar bleiben sollte. Nach der Authentisierung des Tags ist eine physische oder optische Produktauthentisierung sinnvoll, um die Korrelation der Tag-Daten mit realen Produkteigenschaften sicherzustellen.

Angriffsszenario 4: Medikamentenfälschungen mit Tag-Duplikaten

Die Fälscher ermitteln durch Sniffing rechtmäßiger RFID-gestützter Abläufe oder durch aktives Auslesen gültige Tag-Daten, um diese für Medikamentenfälschungen zu verwenden. Tags werden einschließlich gültiger Daten professionell dupliziert (Cloning) und auf Medikamentenfälschungen aufgebracht, um deren Echtheit vorzutäuschen.

Probleme: Dieses Angriffsszenario wird dadurch ermöglicht, dass mit geeigneten RFID-Lesern frei auslesbare Tag-Daten (Tag-ID, EPC) relativ einfach passiv abgehört oder aktiv ermittelt werden können. Denkbar ist außerdem, dass Angreifer Zugang zur Chip-Herstellung oder zu frei programmierbaren Tags auf dem Markt haben und Sicherheitsmerkmale realisieren, welche mit denen der originalen Tags übereinstimmen. Das unberechtigte Kopieren einfacher passiver RFID-Tags wird auf Dauer kostengünstig möglich sein.

Lösungsansätze: Eine wichtige Maßnahme ist ebenfalls die Verwendung einmaliger Kombinationen von chip-eigener Tag-ID und produkteigenem EPC. Diese Tag-Kennungen sollten auf gültige Kombinationen und das Vorhandensein von Duplikaten geprüft werden. Darüber hinaus ist der fälschungssichere elektronische Herkunftsnachweis wichtig, mit dem der Weg des Medikaments durch die Lieferkette zurückverfolgt werden kann. Ein sicherer Nachweis, dass das vorliegende Tag echt ist, wird aber erst durch eine Authentisierung des Tags auf Basis von geheimen kryptographischen Schlüsseln erbracht, welche das Tag niemals verlassen und nicht kopierbar sind.

6.2.2 Anwendungsspezifische Anforderungen

Echtheitsprüfungen

Aus den Angriffsszenarien wird deutlich, dass RFID-Lösungen auf Dauer nur dann gegen Medikamentenfälschungen wirksam sein werden, wenn die Herstellung von Tag-Duplikaten (Cloning), das physische Entfernen und Wiederverwenden von Tags, das Manipulieren von Tag-Daten (Spoofing) und nicht zuletzt das Abhören der Luftschnittstelle (Sniffing) erfolgreich unterbunden werden können. Gegen Fälschungen erscheinen daher die folgenden Echtheitsprüfungen notwendig:

- Echtheitsprüfung des EPC und der Kombination von Tag-ID und EPC, um nachzuweisen, dass der EPC vom entsprechenden Hersteller für das Produkt vergeben und in das individuelle Tag geschrieben wurde. Auch die Prüfung auf Duplikate ist sinnvoll.
- Echtheitsprüfung des Herkunftsnachweises mit Überprüfung von enthaltenen digitalen Signaturen und Kennungen, um nachzuweisen, dass die Angaben über das Produkt (z.B. Produktstatus „lieferbar“ oder „verkauft“) und die Lieferkette plausibel sind.
- Echtheitsprüfung des Tags, z.B. durch ein geeignetes kryptographisches Authentisierungsverfahren
- Echtheitsprüfung des Produkts, d.h. der physischen Umgebung, in der das Tag integriert ist, um die Zugehörigkeit des Tags zum Medikament sicherzustellen. Dazu können auch äußere Sicherheitsmerkmale (z.B. Hologramm, intakter Verschluss, Tag-Inlay) dienen, die allerdings nicht in jedem Fall automatisch überprüfbar sind.

Die ausschließliche Verschlüsselung der Daten würde dagegen wenig Schutz gegen Fälschungen bieten, kann aber aus Datenschutzgründen wichtig sein.

Funktionssicherheit

Das Pharma-Szenario stellt mit seinen physikalischen Bedingungen hohe Anforderungen an die Funktionssicherheit der RFID-Systeme. Diese spielt insbesondere an der Luftschnittstelle zwischen Tag und Lesegeräten und in der RFID-Middleware eine Rolle, während sie bei den anderen Systemkomponenten (Datenbanken, Netzwerkkomponenten, Internet) als ausreichend gegeben gelten kann. An der Luftschnittstelle existieren die folgenden spezifischen Anforderungen:

- Heterogene Lesebedingungen: Auf dem Förderband (auf der Ebene der Verpackungslinien von Produkten), im Lager (Bündelverpackungen) und auf der Laderampe (Paletten)
- Hohe Durchsatzgeschwindigkeiten von Produkteinheiten (z.B. 100-200 Flaschen pro Sekunde) und Gebinden (z.B. 1 Gebinde mit 48 Flaschen alle 5 Sekunden)
- Hohe Aggregatdichte (teilweise sehr kleine dicht gepackte Produkteinheiten in Gebinden), bei der die Ausrichtung der Tags zum Leser und die Nähe der Tags untereinander nur eine geringe Rolle spielen darf
- Heterogene Materialien: Mögliche Probleme durch Wechselwirkungen der RFID-Prozesse mit Produktinhalten (z.B. Flüssigkeiten) und Verpackungen (z.B. Metallverschlüsse, Aluminiumfolien auf der Rückseite von Blister-Verpackungen, die Antennen selbst innerhalb von Paletten)
- Heterogene Verpackungsformen: Die Tags sollen auch auf sehr kleinen Produkteinheiten (Ampullen, Fläschchen) und gekrümmten Oberflächen funktionieren. Eine weitere Herausforderung stellen die gemischten Warenkisten in der Kommissionierung dar, in der die Verpackungsformen und Materialien sehr unterschiedlich sind.
- Hohe Erwartung bezüglich der Genauigkeit & Verfügbarkeit, welche die bisherigen Verfahren ohne RFID erreicht haben (z.B. automatische Kommissionierung auf Barcode-Basis mit einer maximalen Fehlerrate im Promillebereich). Von RFID wird erwartet, dass alle Produkteinheiten in Gebinden und gemischten Warenkisten ohne Entpacken und manuelle Kontrolle automatisch erkannt werden.

Die RFID-Middleware stellt die zentrale Komponente der sicheren Integration von RFID-Systemen in ein Unternehmen dar. Sie muss die Funktionen an der Luftschnittstelle absichern und dazu mindestens die folgenden Eigenschaften besitzen [schollenberger06]:

- Sichere Steuerung und Anbindung der physikalischen RFID-Komponenten in die Unternehmensanwendungen, z.B. Echtzeitverarbeitung und Synchronisation der RFID-Daten mit den ERP-Systemen
- RFID-Prozessmanagement mit effizienter Datenfilterung, z.B. Verwerfen von nichtsinnvollen, fehlerhaften und unwichtigen Daten, RFID-Eventgenerierung, inhaltsbezogenes Routing der RFID-Daten, damit die Anwendungsebene (z.B. die ERP-Systeme der Unternehmen) nicht mit einer Datenflut konfrontiert wird
- Anwendungsspezifisches skalierbares Systemmanagement mit guter Konfigurierbarkeit, um die heterogenen Umgebungen zum Erfassen von Medikamenten, Gebinden und

Paletten abzubilden und einen entsprechenden Zugriffs- und Datenschutzes zu realisieren

- Schutz der Hintergrundsysteme gegen RFID-Malware und Implementierung notwendiger Sicherheitsmechanismen, welche für die Tags und RFID-Leser zu kostenintensiv bzw. zu aufwändig wären

Authentizität und Integrität

Damit jeder Teilnehmer der Lieferkette die Integrität und Authentizität der Informationen und des Produktes selbst überprüfen kann, sollte ein elektronischer Herkunftsnachweis jede Medikamentenpackung in der Lieferkette begleiten. Eine detaillierte Beschreibung von Anforderungen an den elektronischen Herkunftsnachweis, seine Echtheit und Verknüpfung mit dem Produkt gibt [harrison06]. Wer ein Produkt empfängt, muss imstande sein, die Zugehörigkeit des Herkunftsnachweises zum empfangenen Produkt sicherzustellen. Wer das Produkt (weiter) liefert, sollte die Information aktualisieren und dabei die gleichen Maßnahmen zur Integrität und Authentizität unterstützen, welche dem nächsten Teilnehmer der Lieferkette eine Überprüfung ermöglichen.
Zum Echtheitsnachweis des Produkts muss die Identität des Produktes mit dem Herkunftsnachweis verknüpft werden. Dazu muss das Produkt nach einem erfolgreichen Authentisierungsverfahren seine Daten (z.B. hartkodierte Tag-Kennung und EPC) mitteilen. Diese sollten dann mit den Daten des Herstellers im Herkunftsnachweis verglichen werden. Weitere Informationen wie Herstellungsdatum, Verfallsdatum und individuelle (von einer bestimmten Kennung abhängige) Sicherheitsmerkmale ermöglichen Plausibilitätschecks und erschweren Produktfälschungen mit bloßen Kopien von Kennungen.
Der sichere Herkunftsnachweis reicht allerdings allein nicht aus. Es kann zwar ohne Authentisierung des Tags nachgewiesen werden, dass die Informationen echt, also nicht von einem Angreifer erzeugt oder verändert wurden, aber es kann sich dabei um eine Datenkopie handeln, die mit einem gefälschten Medikament verknüpft ist. Die für sich authentische Information passt also evt. nicht zum getaggten Objekt (Medikament, Gebinde, Palette). Erst wenn die Echtheit des Tags und die korrekte physische Umgebung des Tags verifiziert ist, kann die Information als wahr gelten.
Weitere Anforderungen bestehen an der Schnittstelle zu den RFID-Informationsdiensten im Netzwerk. Jeder Kommunikationspartner, der Informationen ins EPCIS stellt und anderen zugänglich macht, sollte dazu autorisiert sein. Für den Zugriff auf geschützte Daten muss sich die anfragende Instanz authentisieren.

Vertraulichkeit

Eine ungesicherte Luftschnittstelle kann von einem Angreifer abgehört werden, um daraus gültige Kombinationen von Tag-IDs und EPCs, Passwörter und andere sicherheitssensitive Informationen zu gewinnen. Konkurrierende legale und illegale Pharmahersteller und Vertriebe können auf diese Weise Produktinformationen, Warenbewegungen und Vertriebswege eines Pharmaherstellers oder Vertriebs gewinnen. Trotz unterschiedlicher Lesereichweiten besteht bei allen Frequenzen grundsätzlich die Gefahr des Abhörens an der Luftschnittstelle, da diese exponiert ist und durch Angreifer emuliert werden kann. Da die Schnittstelle dem Sniffing und Spoofing ausgesetzt ist, sollten die Daten zugriffsgeschützt sein. Das freie Aus-

lesen der Tags sollte auch deshalb verhindert werden, um gezielte Diebstähle (z.B. von Betäubungsmitteln) zu erschweren.
Eine statische Verschlüsselung von Tag-Daten (ohne Authentisierung der Komponenten und dynamisch wechselnder Verschlüsselung bei jeder Abfrage) bietet jedoch keinen ausreichenden Schutz, da die verschlüsselten Daten wiederum eine Art eindeutige Kennung darstellen und dem Angreifer ein Tracking ermöglichen. Die Verschlüsselung allein löst auch nicht das Problem der Datenkopien und ihre Verwendung in gefälschten Tags und Produkten. Auch kopierte verschlüsselte Daten auf geklonten Tags erscheinen dem rechtmäßigen RFID-System zunächst als sinnvolle Daten.
Für die Kommunikationskanäle zu den RFID-Informationsdiensten (EPCIS) zum Datenaustausch zwischen Unternehmen über unsichere Netzwerke sollte eine vertrauliche Übermittlung sicherheitssensitiver Daten vorgeschrieben sein. Für die unternehmensinternen Anwendungen und Datenbanken wird dagegen angenommen, dass sie sich in einer sichereren Umgebung befinden bzw. ohnehin der intern geltenden Sicherheits-Policy folgen.

Verfügbarkeit

Die Verfügbarkeit des EPCglobal-Netzwerkes kann für viele Sicherheitsmaßnahmen (z.B. Austausch von kryptographischen Schlüsseln, Zugriffskontrolle, Überprüfung des Herkunftsnachweises und des Produktstatus in Echtzeit) wichtig sein. Bei der Komplexität der Medikamenten-Lieferkette muss aber davon ausgegangen werden, dass die Daten aller Teilnehmer nicht jederzeit über das Netzwerk zugänglich sind. Daher sollte die Abhängigkeit vom Netzwerk so gering wie möglich gestaltet und produktbezogene Daten der Lieferkette möglichst im lokalen EPCIS gehalten werden.

Verbindlichkeit

Der elektronische Herkunftsnachweis kann neben der Integrität und Authentizität auch die Verbindlichkeit von Transaktionen sicherstellen. Dazu muss er eine oder mehrere digitale Signaturen enthalten, welche vom Empfänger auf der Basis zertifizierter öffentlicher Schlüssel geprüft werden können. Die Rechtsverbindlichkeit von so genannten elektronischen Signaturen, die bestimmten Personen zugeordnet sind, wird durch staatliche Gesetze geregelt, in Deutschland durch das Signaturgesetz [sigG01] und die Signaturverordnung [sigV01]. Sie erfordert aber eine Identifikation des Schlüsselinhabers durch Besitz (z.B. Signaturkarte) und Wissen (z.B. Eingabe einer PIN), was für den Herkunftsnachweis kaum durchführbar ist. organisations- oder systembezogene Client/Server-Signaturen sind ausreichend, wenn sie mit zertifizierten Komponenten (z.B. einem Sicherheitsmodul) erzeugt werden und der Organisationsname im Zertifikat hinterlegt ist.

Datenschutz

Für den Datenschutz gelten im Prinzip die für das Handelsszenario beschriebenen Anforderungen. Verglichen mit anderen täglichen Konsumgütern sind Medikamente allerdings sehr persönliche und daher datenschutzrelevante Objekten. Produkt-Tags sollten nach dem Verkauf an den Endkunden gegen das freie Auslesen der Tag-Daten geschützt sein, um die Privatsphäre von Patienten zu schützen. Angreifern darf es nicht möglich sein, unbemerkt die Medikamente, die eine Person bei sich trägt, anhand ihrer RFID-Tags zu identifizieren und etwa auf Krankheiten und den Lifestyle der Person zu schließen. Ohne Schutz wäre das Tracking von Personen auch aufgrund von Tag-Kombinationen am Körper möglich. Anonymität und Location Privacy können durch die endgültige Deaktivierung des Tags beim Ver-

kauf erreicht werden. Wenn der Zugriff auf die Tag-Daten (EPC) geschützt ist und nur den Teilnehmern der Lieferkette oder berechtigten Dritten (z.B. Ärzten) erlaubt ist, sollte das Tag beim Verkauf nicht deaktiviert werden, um weiterhin zum kontrollierten Abruf von Produktinformationen, Rückrufaktionen oder zum Recycling bzw. zur Entsorgung des Medikaments zur Verfügung zu stehen. Der Datenschutz nach Verkauf des Produktes an den Kunden muss dann mit anderen Mittel gewährleistet werden.

6.3 Sicherheitsmaßnahmen der pharmazeutischen Lieferkette

Eine kurze Zusammenfassung des EPC-Ansatzes zur Fälschungssicherheit bietet [gs1-06]. Neuere White Paper der Auto-ID-Labs haben die Datensicherheit EPC-gestützter Lieferketten [harrison06, inaba06, jantscher06] und die Fälschungssicherheit von EPC-Tags [lehtonen06, lehtonen06a, grasso06, ranasinghe06, ranasinghe06a, duc06, yu06] auch mit Blick auf die pharmazeutische Lieferkette zum Gegenstand. In [inaba06] werden als Maßnahmen erstens die eindeutige Identifizierung der kleinsten gehandelten Produkteinheiten, zweitens der elektronische Herkunftsnachweis an jeder Stelle der Lieferkette (Tracking & Tracing) und drittens die Detektion physischer Zerstörung oder Manipulation mit Meldung an das RFID-System empfohlen.
Allerdings besteht im Pharmavertrieb der wirtschaftliche Druck, die Kosten von Tags und RFID-Infrastruktur auf ein Minimum zu beschränken, so dass die Auswahl der Tags im Grunde auf den Low-Cost-Bereich begrenzt ist. Das macht evt. auch die Festlegung auf eine einzige Frequenz und ein Protokoll für Einzelprodukte, Gebinde und Paletten in der gesamten Lieferkette notwendig. Die Anforderungen an die Informationssicherheit (Authentizität, Integrität und Vertraulichkeit der Daten) und an den Datenschutz spielen bisher in der Diskussion und bei der praktischen RFID-Implementierung zum Medikamentenschutz nur eine untergeordnete Rolle. Stattdessen stehen bei den Technologieanbietern und Anwendern Maßnahmen zur Verbesserung der Funktionssicherheit der RFID-Systeme im Zentrum der Aufmerksamkeit.

6.3.1 Empfohlene Sicherheitsmaßnahmen

Funktionssicherheit an der Luftschnittstelle

Als entscheidender Engpass der Funktionssicherheit gilt noch immer das Erfassen und Auslesen der Tags an der Luftschnittstelle mit der richtigen Wahl der Frequenz, hohen Tag-Leseraten und einer zuverlässigen Pulkerfassung. In White Papern, welche den RFID-Einsatz im pharmazeutischen Umfeld zum Gegenstand haben [z.B. philips04, adt06, odin06] werden besonders die Anforderungen an die Tag-Leseraten, die Wechselwirkungen mit Metallen und Flüssigkeiten, die Argumente für die Nutzung von HF- bzw. UHF-Tags und (im Falle von HF) die Auswahl des geeigneten HF-Protokolls diskutiert. Die Festlegung auf eine bestimmte Frequenz (HF oder UHF) hat große Auswirkungen auf die Hardware-Implementierung und die Funktionssicherheit. Tab. 9 fasst einige Eigenschaften von HF- und UHF-Tags zusammen.

Tab. 9 – Funktionssicherheit von passiven HF- und UHF-Tags

	HF-Tags	UHF-Tags
Frequenz	13,56 MHz (weltweit)	860-960 MHz (reglementierte Nutzung in Europa)
Absolute Bandbreite (Europa)	13.553-13.567 = 14 kHz	865-868 MHz = 3.000 kHz
Standard	ISO 18000-3 Mode 2	ISO 18000-6 Type C (EPC Gen 2 Tag)
Bitrate Leser ->Tag	424 kbits/s	26,7 bis 128 kbit/s
Bitrate Tag -> Leser	106 kbits/s	40 bis 640 kbit/s
Zahl der Antwortkanäle	8	1
CRC Error Checking	Kommando: 16 bit; Antwort: 32 bit	Kommando: 5 bis 16 bit; Antwort:: 16 bit
Performanz bei Inline-Geschwindigkeit [odin06] (ISO 15693 HF-Tags)	Aufgrund niedrigerer Leserate nur bis 4,5 m/s gut	Noch bei 7,5 m/s gut
Reichweite	0 bis 1,5 m (räumlich homogenes magnetisches Feld)	0 bis 10 m (elektromagnetisches Feld)
Hohe Leserdichte	Kein Problem	Evt. problematisch (gegenseitige Störungen, empfindlich gegen Nebenbandgeräusche)
Anti-Kollision	Frequency and Time Division Multiple Access (FTDMA); schnell & zuverlässig	Slotted Terminating Adaptive Collection; relativ langsam
Pulkerfassung	Max. 1200 Tags / s	Ja, bis 1000 Tags / s, wenn Tags gut separiert
Dichte Stapelung, Aggregation zu Gebinden	Ja, auch bei Berührung der Tags	Ja, wenn Tags mindestens ein Viertel der Wellenlänge (von 34 cm) separiert und nicht gleich im Raum verteilt (sonst evt. Bildung von Antennen-Arrays)
Fähigkeit, dynamische Tagpulks zu lesen	Ja	Begrenzt, da alle Tags während des Antikollisionsverfahrens im Feld des Lesers bleiben müssen.
Einfluss von Flüssigkeiten	Weniger anfällig gegen Absorption	Stark beeinflusst durch flüssige Inhalte und andere Dielektrika, welche durch Absorption erwärmt werden. Weniger stark im Nahbereich (wenige cm)
Einfluss von Metallen	Abschirmung	Abschirmung, Reflexion, Interferenzen mit Feldauslöschungen im Raum; Luftraum zwischen Metall und Tag nötig
Unbeabsichtigtes Lesen von entfernten Tags	Nicht möglich	Ja, aufgrund von unregelmäßiger Ausbreitung des Feldes („Hot Spots“) und „Spill Over“ von Antennen; Gegenmaßnahme: Frequency Hopping
Weitere Einflüsse	Leistungsfähigkeit von Tags weniger abhängig vom Design, aber empfindlicher in Bezug auf Antennenorientierung zwischen Tag und Leser	Störung durch GSM Mobile (850 und 900 MHz) und evt. andere Telefonsysteme; Leistung abhängiger von Krümmungen und Biegungen der (verglichen mit HF-Tags) größeren Antennen.

Die Eignung einer Frequenz hängt entschieden von den Umgebungsbedingungen der Tags und Leser ab. Bisher gilt HF, dessen Nutzung auf das Nahfeld beschränkt ist, als geeigneter und zuverlässiger für die Kennzeichnung der Produkteinheiten. Da keine elektrische Energie transportiert wird, sondern im Tag durch das magnetische Feld induziert wird, treten weniger Störungen auf. UHF dagegen transportiert Energie und ist leistungsfähiger für die Fernfeld-Anwendungen, also für die Kennzeichnung von Gebinden und Paletten. UHF ist deshalb aber auch anfälliger für elektromagnetische Interferenzen und gegenüber Materialien wie Flüssigkeiten und Metalle. Die White Paper [philips04], [magellan06] und [odin06] sprechen sich daher für HF-Tags auf Item Level aus. [adt06] versucht mit den folgenden Argumenten den Nachweis zu erbringen, dass der ausschließliche Einsatz von UHF-Tags machbar und sinnvoll ist:

- **UHF-Verhalten im Nahbereich**: UHF wird im Nahfeld (unter 5,2 cm) nicht durch Flüssigkeiten absorbiert und kann daher auch an oder sogar in Behältern mit Flüssigkeiten gelesen werden. Die UHF-Antennen können so entworfen werden, dass Metall die

elektromagnetische Kopplung unterstützt. Auch bei größeren Abständen können Störungen durch ein geeignetes System-Design vermieden werden.

- **UHF-Antennendesign**: Der Lesebereich ist nicht so sehr von der Frequenz abhängig, sondern vom Antennen-Design im Tag und Leser und von der eingesetzten Leistung. Antennen lassen sich so entwerfen, dass sie sowohl magnetische als auch elektromagnetische Kopplung unterstützen und damit flexibel für verschiedene Leseabstände (zwischen 5 cm – 10 m für UHF) einsetzbar sind. UHF-Tags haben aufgrund der einfacheren Dipol-Antennen weniger Masse als HF-Tags und können daher sehr dicht nebeneinander liegen.
- **UHF-Antennengröße**: Die erforderliche Tag-Größe ist davon abhängig, wie groß der Leseabstand sein soll. Je geringer der Abstand, desto kleiner darf die Tagantenne sein. Daher sind zum nahen Lesen von Produkteinheiten auch sehr kleine UHF-Antennen (z.B. 25 mm) möglich. Zum Erfassen von Bündelverpackungen und Paletten sind dagegen UHF-Tag von 10 – 15 cm Größe üblich.
- **Absolute UHF-Bandbreite**: Die absolute Bandbreite ist bei UHF (3.000 kHz) um den Faktor 214 größer als bei HF (14 kHz), so dass mit UHF grundsätzlich höhere Datenübertragung erreicht werden kann.
- **UHF-Leserate**: EPC Class1 Gen 2-Spezifikation [epc-gen2] erlaubt ein schnelles und zuverlässiges Auslesen von bis zu 1000 Tag pro Sekunde.
- **UHF-Energieaufnahme**: Die magnetische Kopplung ist umso höher, je höher die Frequenz ist. Daher brauchen HF-Antennen mehr Windungen und bessere Materialien (z.B. Kupfer). UHF-Tags kommen mit einer Windung (Dipol) und kostengünstigeren Materialien aus.
- **UHF-Kosten**: Die einfacheren UHF-Antennen reduzieren die Kosten ungefähr auf die Hälfte (durchschnittlich 10 – 15 Cents). Im unteren Performanzbereich sind HF-Leser zwar billiger (ab $ 50) als UHF-Leser (ab $ 500), im oberen Bereich kehrt sich das Verhältnis aber um: HF-Leser für $ 3000-15000, UHF-Leser für $ 2000-3000 mit sinkender Tendenz.

Die White Paper können aber nicht als wirklich unabhängig gelten, da die durchgeführten Nachweise offensichtlich Herstellerinteressen untermauern sollen. Unabhängige Untersuchungen verschiedener RFID-Frequenzen in anwendungsspezifischen Umgebungen wären daher hilfreich. Unternehmen führen oftmals eigene Tests durch und implementieren mehr als eine Technologie, wenn mehrere Anwendungsebenen abgedeckt werden sollen. Technologielieferanten wie IBM bieten Produkte an, welche sowohl UHF- als auch HF-Techniken unterstützen bzw. von den RFID-Frequenzen unabhängig sind, um die Vorteile mehrerer Frequenzen nutzen zu können.
HF-Tags sind seit langem im Gebrauch (kommerziell erhältlich seit 1995) und haben eine technologische Reife erreicht, die nur noch schwer zu optimieren ist. Bei UHF-Systemen scheinen dagegen noch durchgreifende Optimierungen möglich, z.B. in Bezug auf das Antennendesign, eine verbesserte Feldausbreitung, die Vermeidung von Absorption und Reflexion (z.B. durch Integration von Metalloberflächen in die Antennenfunktion) und die Reduzierung von Kosten. Im Vergleich zu den USA ist die Nutzung von UHF in Europa allerdings

durch die Spezifikationen ETSI EN 300 220 und 302 208 stärker reglementiert. Die eingeschränkte Bandbreite lässt ein Frequency Hopping nicht zu und beschränkt die Effizienz von Antikollisionsverfahren. RFID-Leser müssen jeden Kanal zunächst abhören und freie Kanäle finden, auf denen sie Tags ansprechen („Listen Before Talk“). Diese Auflage vermindert ebenfalls die Leistung von Systemen, wird aber von ETSI auf Alternativen (z.B. Zulassung von UHF-Bändern ohne „Listen Before Talk“) hin untersucht. Danach muss auf nationaler Ebene eine Umsetzung in die Frequenznutzungspläne erfolgen. In Deutschland ist dafür die Bundesnetzagentur zuständig. Zeitnah zu technologischen Optimierungen von UHF-Tags, Synchronisation von Lesegeräten und verbesserten Abschirmmaßnahmen müssen also ggf. die gesetzlichen Vorschriften angepasst werden.

Eindeutige schreibgeschützte Tag-Kennungen

Die eindeutige Kennzeichnung jeder Produkteinheit mittels der Kombination aus einer chipindividuellen Kennung (Tag-ID) und einer Kennung des Produkts (z.B. EPC) ist nach der Funktionssicherheit die wichtigste Sicherheitsmaßnahme. Ein geheimes Zuordnungsschema von Tag-Kennung und EPC zu Produkteinheiten erschwert Angreifern zudem eine einfache schematische Generierung oder Zuordnung von Kennungskombinationen zu Produkten. Mit Hilfe von Echtheits-, Duplikats- und Statusprüfungen können Tags mit kopierten Daten und Tags gestohlener oder ausgemusterter Produkte erkannt werden. Die Vergabe und Registrierung dieser Kennungen beim Pharmahersteller ist auch eine Voraussetzung für die Einführung eines sicheren elektronischen Herkunftsnachweises.

Sicherer elektronischer Herkunftsnachweis

Der elektronische Herkunftsnachweis dient der Sicherstellung der Integrität, Authentizität und Verbindlichkeit der Produktinformationen und sollte zu diesem Zweck digitale Signaturen erhalten, welche von jedem Absender des Produktes erzeugt und von jedem Empfänger geprüft werden können. Eine strukturierte Datenübermittlung einschließlich Signaturen und Zertifikaten zur Übermittlung der öffentlichen Schlüssel kann z.B. durch standardisierte XML-Verfahren erfolgen. Der Herkunftsnachweis kann grundsätzlich als verteilte Einzelnachweise oder als erweiterbares einzelnes Dokument gestaltet sein [harrison06], wie im Folgenden beschrieben.

Nach dem Prinzip des verteilten Herkunftsnachweises signiert jede Instanz der Lieferkette ihre Daten für den Herkunftsnachweis und speichert sie in einer lokalen Datenbank, auf die andere Instanzen der Lieferkette über ein Netzwerk Zugriff haben (z.B. lokale EPCIS im EPCglobal-Netwerk). Die Informationen werden also nicht in der Lieferkette weitergereicht, sondern über Links bekannt gemacht und abgerufen. Der Vorteil dieses Prinzips ist die geringere Datenmenge, die zudem auf die Fälle aktiver Nachfrage beschränkt werden kann. Allerdings müssen für einen lückenlosen Herkunftsnachweis alle beteiligten Instanzen einzeln abgefragt werden, was evt. zu mehr Datenverkehr, Wartezeiten, Datenausfällen und allgemein zu geringerer Robustheit führt. Der verteilte Herkunftsnachweis ist damit eher für stichprobenartige Prüfungen und für Prüfung auf gesonderte Anfrage geeignet.

Eine bedeutende Sicherheitslücke besteht darin, dass die Daten jeweils nur unter Kontrolle eines einzelnen Teilnehmers stehen, und nachträglich durch diesen verändert oder gelöscht werden könnten. Einzelne unzuverlässige Teilnehmer könnten gefälschte Medikamente mit technisch einwandfreien Teilnachweisen in die Lieferkette einschleusen. Gegen nachträgliche Fälschungen müsste zumindest das Signieren der ursprünglichen Daten und das Ver-

wahren dieser Signaturen zusammen mit den Links bei unabhängigen vertrauenswürdigen Dienstleistern (z.B. als Teil der EPCglobal Discovery Services) gefordert werden, bei denen jeder Teilnehmer für ein bestimmtes Produkt nur ein einmaliges Schreibrecht besitzt. Empfänger würden zunächst neben dem Link auf den Herkunftsnachweis auch die entsprechenden Signaturen abrufen und verifizieren.
Nach dem Prinzip des erweiterten Herkunftsnachweises werden die Informationen, die auf dem Weg des Produktes durch die Lieferkette anfallen, in einem Dokument vereinigt und jeweils vollständig an den nächsten Teilnehmer weiter gegeben. Jeder Teilnehmer der Lieferkette verifiziert das Dokument anhand der letzten Signatur, fügt Informationen hinzu und signiert wiederum die gesamte Information, also auch die bereits signierten Daten der voran gegangenen Teilnehmer. Die Größe des Dokuments nimmt dabei mit der Zahl der Teilnehmer zu und kann mit den enthaltenen Signaturen und PKI-Zertifikaten schnell in den Bereich von MBytes kommen, so dass eine Speicherung auf den Tags nicht in Frage kommt.
Der Sicherheitsvorteil dieses erweiterten Herkunftsnachweises besteht darin, dass Teilinformationen vielfach kopiert vorliegen und dadurch robust gegen Ausfälle von Instanzen und gegen nachträgliche Verfälschungen von Daten bei einzelnen Instanzen sind. Ein solcher Herkunftsnachweis könnte aber statt bei den einzelnen Instanzen der Lieferkette auch in einer zentralen Datenbank abgelegt sein und dort von allen Teilnehmern aktualisiert und gelesen werden, wie in [koh05] vorgeschlagen (siehe Abb. 37). Die Produktdaten sind dabei einheitlich in der XML-basierten Physical Markup Language (PML) formatiert.

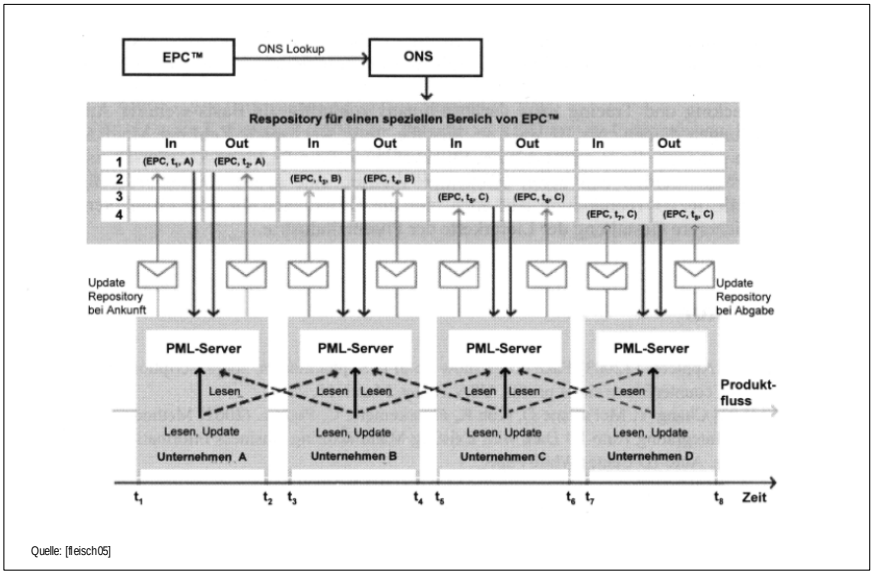


Abb. 37 – Zentrale Repository-Datenbank mit Herkunftsnachweis

EPCglobal hat sich gemäß der gesetzlichen Regelungen in den USA für den pharmazeutischen Handel auf den erweiterbaren Herkunftsnachweis festgelegt und eine XML-basierte Struktur definiert [epc-pedigree]. Die Herkunftsnachweise sollen als rechtsgültige Dokumente von jedem Teilnehmer der Lieferkette elektronisch signiert und an den nächsten Empfänger des Produktes weitergereicht werden. Vorgesehen sind digitale Signaturen auf RSA-Basis und eine zugehörige Public Key Infrastruktur (PKI) mit X.509-Zertifikaten eigenen Profils [epc-cert]. Abb. 38 zeigt beispielhaft die Struktur eines Herkunftsnachweises mit insgesamt vier Signaturen: eine Signatur vom Produkthersteller, Signaturen von zwei Großhändlern und

einem Einzelhändler (z.B. Apotheker). An den Herkunftsnachweis können auch andere Dateien angehängt sein, wie z.B. MIME-Dokumente, pdf-Dateien oder Bilder für die manuelle Produktauthentisierung. Der Herkunftsnachweis ist nicht auf den Pharma-Bereich beschränkt, sondern kann auch für andere Bereiche zum Tracking & Tracing von Produkten verwendet werden. Der Einsatz von EPC und RFID ist keine Voraussetzung, so dass der Herkunftsnachweis auch mit anderen Methoden wie Barcodes oder Papierdokumenten vereinbar ist.

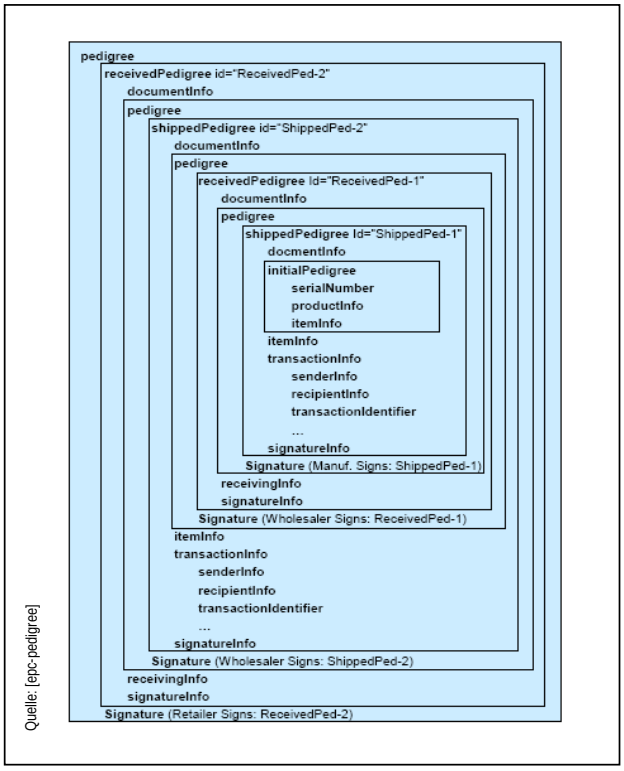


Abb. 38 – Struktur eines EPC-Herkunftnachweises (Beispiel)

Leider sieht der EPC-Herkunftsnachweis keinen Eintrag eines Produktstatus wie „Haltbarkeit abgelaufen“ oder „An Endkunden verkauft“ vor, wenn das Medikament das Ende der Lieferkette erreicht hat. Ein entsprechender Eintrag würde eine unrechtmäßige Wiederverwendung von Daten beim Einschleusen von Produktfälschungen in die Lieferkette zumindest erschweren. Da der Herkunftsnachweis auch nach dem Verkauf für Anfragen der Endkunden und für Rückrufaktionen wichtig sein könnte, sollte die Information in jedem Fall auch nach dem Verkauf abrufbar sein. Der vollständige Herkunftsnachweis könnte im EPCIS des Herstellers oder der Apotheke oder in den EPC Discovery Services abgelegt werden. Ein entsprechendes Konzept existiert bei EPCglobal noch nicht. Die Apotheken/ Krankenhäuser würden vermutlich nicht ohne zwingende gesetzliche Regelungen solche Dienste übernehmen [harrison06].
Ein erweiterter Herkunftsnachweis würde der Apotheke oder dem Endkunden Plausibilitätsprüfungen ermöglichen: Ein EPC, der auf die Lagerung bei einem Großhändler in den USA hinweist, ist wahrscheinlich eine Fälschung, wenn das Produkt zeitgleich in Deutschland angeboten wird. Da einfache EPC-Tags allerdings leicht kopierbar sind, könnte ein Händler den

Tag mehrfach kopieren und auf Produktfälschungen aufbringen. Wenn der Händler die zentrale Datenbank nicht aktualisiert und auch der Kunde den Kauf nicht registrieren lässt, dann fällt die Vervielfältigung des Tags nicht auf, weil jede Fälschung mit Tag-Kopie auf Anfrage denselben plausiblen Herkunftsnachweis bietet. Über Tracking & Tracing durch Herkunftsnachweise hinaus ist daher eine sichere Authentisierung eines nicht-kopierbaren Tags sinnvoll [staake05].

Authentisierung des Tags

Der Startpunkt zur Produktauthentisierung mit RFID ist das Anbringen oder Einlassen des Tags in die Verpackung bzw. in den Medikamentenbehälter. Allein die Existenz des Tags ist eine Hürde für den Angreifer, da dieser für getaggte Produktfälschungen Zugang zur Halbleiter-Industrie haben, gültige Tag Identifier und individuelle EPCs in die Tags schreiben und die Tags in die Verpackungen / Produkte (als Inlay oder Label) integrieren muss. Das wird aber mittelfristig für einen Angreifer durchführbar sein. Neben dem sicheren Herkunftsnachweis ist daher auch eine Authentisierung des Tags sinnvoll.
Die entscheidende Sicherheitsmaßnahme zur Verhinderung geklonter Tags auf Produktfälschungen ist eine starke Authentisierung des Tags auf Basis nicht-kopierbarer kryptographischer Schlüssel im Tag selbst. Das Tag braucht aber allerdings dazu eine kryptographische Einheit ähnlich wie sie Mikroprozessorkarten besitzen, welche mit [iso7816-4] konform sind und eine [iso14443]-Luftschnittstelle besitzen, siehe 3.2.8. Damit würde das Tag nicht mehr im Low-Cost-Bereich liegen. Für die Echtheitsprüfung des Tags werden daher geeignete kryptographische Authentisierungsverfahren gesucht (siehe siehe 3.2.3), die auch auf Low-Cost Tags implementiert werden können.

Authentisierung des Produkts

Neben der Echtheit des Tags sollte sicher gestellt werden, dass das Tag physisch an der zugehörigen Produkteinheit befestigt ist. Die Verpackung muss unbeschädigt sein und den Originalinhalt des Medikaments schützen. EPC Class1- oder Class2-Tags könnten dazu beispielsweise in spritzgussgeformten Kunststoffverschlüssen eingegossen sein, welche das Produkt derart versiegeln, dass ein Öffnen oder Austauschen des Verschlusses nicht unbemerkt bleiben kann [philips04]. Auch können Tags als Inlays also von außen physisch unzugänglich in Flaschen oder Blisterverpackungen eingelassen sein.
Bei der Ausgabe des Medikaments an den Endkunden könnte schließlich ein manueller oder optisch-maschinenlesbarer Vergleich der EPC-verlinkten Daten mit den aufgedruckten Daten und äußeren Produktmerkmalen (z.B. Barcode, aufgedruckte Seriennummer, Hologramm) erfolgen. Dazu können Produktbilder oder andere Zusatzinformationen dienen, die zusammen mit dem elektronischen Herkunftsnachweis abrufbar sind. Dazu müssen einheitliche effiziente Verfahren entwickelt werden.

Zugriffsgeschützte Datenhaltung

Die US-amerikanische Behörde FDA vertritt den Standpunkt, dass RFID-unterstützte Produktinformationen entweder verschlüsselt auf dem Tag oder zugriffsgeschützt verlinkt sein müssen. Statisch verschlüsselte Daten auf dem Tag schützen allerdings nicht vor Sniffing, Datenkopien oder Tracking, selbst wenn dabei dem Angreifer die Bedeutung der Daten verborgen bliebe. Die gängigen Verschlüsselungsmechanismen der kontaktlosen Mikroprozessorkarten nach [iso14443] stehen den einfachen EPCglobal-Tags ohnehin nicht zur Verfügung. Die Daten könnten aber zusätzlich zu den Mechanismen der Authentisierung und Da-

tenintegrität im RFID-Leser, in der RFID-Middleware oder im Backend verschlüsselt und in dieser Form auf dem Tag abgelegt und später ausgelesen werden, da die Daten für das Tag transparent sind, also nicht durch das Tag selbst ausgewertet werden müssen. Die Verschlüsselung der Kennungen (EPC) auf dem Tag ohne Sinngehalt für einen Angreifer kann zudem für den Datenschutz wichtig sein.
Für die Bereitstellung von lokalen Produktinformationen im EPC-Netzwerk sind in jedem Fall Autorisierungs- und Authentisierungstechniken notwendig wie sie im Internet für zugriffsgeschützte Web-Server eingesetzt werden.

Offline-Verfügbarkeit

Möchte der Großhandel eine effiziente von Zugriffen auf die Backend-Systeme unabhängige Lagerhaltung, so reicht es nicht aus, auf dem Tag nur Kennungen wie Tag-ID und EPC zu speichern. Gemäß [epc-gen2] steht auf dem Tag neben reserviertem Speicher, EPC und Tag-ID auch frei verwendbarer Anwendungsspeicher zur Verfügung, der die Abhängigkeit vom Netzwerk vermindern könnte. Dazu sollten allerdings einheitliche Regeln zur Speicherzuteilung und zum Zugriffsschutz spezifiziert werden. Dann könnten neben dem EPC z.B. auch die Chargennummer und das Haltbarkeitsdatum interoperabel auf dem Tag gespeichert werden und direkt durch das Auslesen aller Tag-Daten zur Verfügung stehen. In dem Fall wäre es aber wichtig, dass die Sicherheitsmechanismen an der Luftschnittstelle nicht von kryptographischen Daten im Backend abhängig sind. Dazu müssten effiziente Offline-Authentisierungverfahren entwickelt werden. Eine Alternative wäre es, die Tag-Authentisierung ausschließlich zur Echtheitsprüfung des Tags zu verwenden und nicht zur Bedingung für das Auslesen der Tag-Daten zu machen. Unter der Annahme, dass die Tag-Daten der Lagerhaltung für Angreifer zumindest im Kontext von Medikamentenfälschungen relativ uninteressant sind, könnten diese Daten frei auslesbar aber schreibgeschützt auf den Tags gespeichert sein.

Nutzung eines Datenschutzmechanismus

Für den Datenschutz reicht einer der in 3.2.7 genannten Mechanismen zum Verhindern des Auslesens völlig aus. Der Kill-Befehl zur endgültigen Deaktivierung des Tags ist für die Logistik der Medikamentenlieferkette relativ ungeeignet und würde nach dem Verkauf in der Apotheke ein Abrufen von Produktinformationen (z.B. als Teil von Rückrufaktionen) erschweren. Die dafür relevanten Daten einschließlich EPC könnten aber zusätzlich auf die Medikamentenpackung oder beim Verkauf auf die Quittung gedruckt werden, so dass sie für eine spätere Anfrage an das Informationssystem optisch eingelesen oder manuell eingegeben werden können. Als Alternative zum Kill-Befehl scheinen Clipped Tags besonders geeignet, weil der Mechanismus von Kunden selbst durchführbar und überprüfbar ist. Zudem wären Informationen auf kontrollierte Weise weiterhin abrufbar.

6.3.2 Bewertung der bisherigen technischen Umsetzung

Leider konnten die Anwender des von IBM angebotenen RFID-Systems nicht direkt befragt werden, so dass deren Erfahrungen zur Funktionssicherheit für diese Studie nicht vorliegen. Die Auswahl der RFID-Hardware, insbesondere der HF-Tags auf Produktebene bleibt nach IBM-Angaben den Technologiekunden überlassen. Die von IBM implementierte Funktionalität setzt nur voraus, dass alle Tags eine vom Chiphersteller eingetragene eindeutige Tag-ID besitzen. Die im Einsatz befindlichen Tags sind Class1-Tags mit Write-Once und Read-Many

Memory, d.h. passive Tags ohne Möglichkeit einer gegenseitigen Authentisierung von Tag und Leser und ohne Verschlüsselung der Kommunikation an der Luftschnittstelle. Die eingesetzten UHF-Tags sind konform zu EPC Class1 Gen2 und verfügen damit über ein Passwort-geschütztes Kill-Kommando. Kryptographische Tag-Funktionalität wurde von den Anwendern nicht gewünscht, da die Funktionssicherheit und die Low-Cost-Forderung weiterhin höchste Priorität haben.

Teil des IBM-Konzeptes für Tracking & Tracing ist ein verteilter elektronischer Herkunftsnachweis, bei dem nur Teilnachweise lokal bei den Teilnehmern der Lieferkette gespeichert werden und von dort abgerufen werden müssen. Höhere Sicherheit ließe sich mit einem erweiterten Herkunftsnachweis erreichen, da die Daten nach der Versendung des Herkunftsnachweises parallel zur Ware nicht mehr vom Ersteller verändert werden können, siehe 6.3.1. Auch sollten digitale Signaturen zur Echtheits- und Integritätsprüfung der Daten unbedingt Teil des Herkunftsnachweises sein, was großen Aufwand (z.B. den Aufbau einer PKI) erfordert und bisher nur in Planung ist. Der Forschungsbedarfs ist hier gering, da die notwendigen Technologien bereits vorhanden und in den EPC-Spezifikationen [epc-pedigree, epc-cert] vorgesehen sind.
Die Online-Prüfung der Tag-Kennungen wird von IBM und den Anwendern als wesentlich und ausreichend zur Erkennung von Fälschungen angesehen. Über die physische Verbindung der Tags zu den verschiedenen Produktenverpackungen und mögliche Sicherheitsmerkmale zur Authentisierung des Produkts liegen keine Informationen zur Veröffentlichung in dieser Studie vor. Die im IBM-System realisierte zugriffsgeschützte Datenhaltung im EPCIS entspricht dem heutigen Stand der Internet-Technologien. Allerdings wurde von IBM der Bedarf an einheitlichen Sicherheitsmechanismen für ONS und EPC Discovery Services geäußert, da die meisten Technologieanbieter einschließlich IBM bisher proprietäre Lösungen vorsehen. Bis jetzt verfügt der ONS über keine Authentisierungsmechanismen für die Clients. Eine solche Funktionalität wurde daher in den lokalen EPCIS-Servern eingerichtet, unterliegt aber damit der lokalen Sicherheitskonfiguration der Unternehmen. Wünschenswert wären Lookup-Services auf Produktebene mit sicherer Zugriffskontrolle und Authentisierung, die einheitlich für die EPC Discovery Services festgelegt werden sollten [inaba06].
Maßnahmen für die Offline-Verfügbarkeit liegen im Ermessen der Anwender und wurden in den prototypischen Implementierungen in den USA vermutlich nicht umgesetzt. Gleiches gilt für die technischen Maßnahmen des Datenschutzes. Den Kill-Befehl unterstützen die eingesetzten UHF-Tags, welche aber nicht zum Taggen der Produkteinheiten, sondern zur Kennzeichnung von Gebinden und Paletten eingesetzt werden. Ihre Datenschutzrelevanz ist entsprechend gering.

6.3.3 Identifizierter Forschungs- und Entwicklungsbedarf

Der Pharmaindustrie gilt als Vorreiter bei der Einführung von RFID auf der Ebene einzelner Produktpackungen (Item-Level) für die Lieferketten des Handels. Gemäß einer Wirtschaftsumfrage warten 65% der US-amerikanischen Anwender in den Bereichen Verbrauchsgüter, Einzelhandel und Gesundheit die Entwicklung im Pharmabereich ab [vdc06]. Insbesondere in den USA laufen im Pharmabereich zahlreiche RFID-Pilotprogramme zur Testung und Identifizierung von Entwicklungsbedarf. Es werden vor allem die folgenden fünf Hindernisse genannt, die einer breiten Einführung von RFID entgegenstehen:

- **Hohe Kosten:** Hardware, Software und Dienste; Sicherheit zum Schutz gegen Produktfälschungen; kundenspezifische Formfaktoren der Tags
- **Mehrere mögliche Frequenzen**: UFH versus HF auf Item-Level
- **Mangelnde Funktionssicherheit**: Lesereichweite, Leseraten, Interoperabilität etc.
- **Undefinierte Use-Cases**: Verwendung und Vorteile der RFID-Infrastruktur und Daten für den Hersteller und die Teilnehmer der Lieferkette
- **Unbekannte Effekte**: Mögliche Auswirkungen der RF-Energie auf organische Inhaltsstoffe sind bisher nicht systematisch untersucht worden

Eine gemischte Palette mit getaggten Arzneimittelpackungen stellt eine extreme Herausforderung für die Funktionssicherheit dar, die sich kaum im Voraus berechnen lässt. Es kann immer Materialien und Konstellationen geben, bei denen einzelne Tags nicht erfasst werden. Viele zugrunde liegende Faktoren scheinen nur durch interdisziplinäre Forschung und Entwicklung lösbar. In der Praxis fällt jedoch das Fehlen von technischen RFID-Richtlinien und einheitlichen Spezifikationen viel stärker ins Gewicht als die notwendigen technischen Verbesserungen aufgrund von Forschungsarbeiten [li06]. Daher stehen weiterhin prototypische Pilotprojekte und intensive Tests von RFID-Produkten am Anfang jeder kommerziellen Implementierung. Für den Pharmabereich ist zudem eine branchenübergreifende Standardisierung wichtig, da zumindest bei frei verkäuflichen Arzneimitteln Überschneidungen mit Einzelhandelssortimenten (z.B. bei Wal-Mart) bestehen.
Vermutlich wird EPCglobal in der pharmazeutischen Industrie eine große Bedeutung erlangen, sobald neben dem Kommunikationsprotokoll für UHF-Tags [epc-gen2] auch das entsprechende Protokoll für HF-Tags vorliegt, welches zurzeit erarbeitet wird. Damit würden zwei weltweit einsetzbare Protokolle vorliegen, die auf Low-Cost Tags implementiert und in einem globalen Netzwerk eingesetzt werden können. Die Forschung sollte die Weiterentwicklung von Low-Cost Tags zum Ziel haben, auch wenn sie sich nicht auf die bei EPCglobal gemachten Vorgaben beschränken darf. Mögliche Forschungsfelder betreffen die Vereinheitlichung von RFID-Komponenten, die Verbesserung der Hardware, die Entwicklung angepasster kryptographischer Mechanismen und anwendungsspezifischer Sicherheitsprotokolle zur Produktauthentisierung.

Spezifikation und Weiterentwicklung von RFID-Komponenten

Die Integration von RFID-Systemkomponenten in bestehende Anwendungen und Datenbanken wird von Technologieanbietern und Anwendern als vordringliche Aufgabe angesehen [li06]. Wichtig wäre z.B. eine Standardisierung der RFID-Leser und der Schnittstelle zur RFID-Middleware, da zurzeit viele unterschiedliche Protokolle und Treiber existieren. Nahezu jeder Lesertyp und Treiber muss gesondert mit der Middleware bzw. der Anwendungssoftware verbunden werden. Große ERP-Anbieter wie SAP, Oracle, Microsoft und IBM bieten eine Integration von RFID-Systemen an, die meist jedoch in proprietäre Lösungen enthält. Eine einheitliche Anbindung und Integration von RFID-Systemen in ERP-Systeme könnte die Einführung von RFID-Systemen voranbringen.
Für das EPCglobal-System besteht mit Blick auf das Pharma-Szenario der folgende Spezifikationsbedarf: Es fehlen einheitliche Nutzungskonzepte für Benutzerspeicher auf den EPC

Class1 Gen2-Tags, z.B. für die Offline-Nutzung in einer effizienten Lagerhaltung oder zur Nutzung für Sicherheitsmechanismen. Es fehlen Sicherheitsmechanismen für den ONS. Die EPC Discovery Services zum Abrufen der Produktinformationen und der Herkunftsnachweise sollten einheitlich und skalierbar sein. Bis jetzt existieren zudem keine einheitlichen Konzepte für die Verwaltung und Finanzierung komplexer EPC Discovery Services, so dass viele Technologieanbieter ihre eigenen proprietären Lösungen entwickeln.
Sinnvoll wäre eine Erweiterung der EPC-Dienste um das Management von Produktstatus und Lifcycle der Kennungen [inaba06]: Wenn Kennungen nicht durch Verschlüsselung und Zugriffskontrolle auf den Tags gesichert sind, könnte eine effiziente Identifizierung von Duplikaten und Überprüfung des Medikamentenstatus (z.B. „verkauft“, „abgelaufen“, „entsorgt“) die Sicherheit der Lieferkette gegen gestohlene oder gefälschte Medikamente erhöhen.

Verbesserung der RFID-Hardware

Die Funktionssicherheit von Tags und Lesern ist von zahlreichen Faktoren (z.B. Frequenz, Antennendesign, dielektrische Eigenschaften der getaggten Objekte, Wechselwirkungen zwischen Tags) abhängig, so dass es umfangreiche wissenschaftliche Untersuchungen bedarf, um die Leseraten der Systeme zu optimieren. Dabei erscheinen unabhängige vergleichende Tests von HF- und UHF-Tags mit modifizierter Hardware und Verbindung des Tags an unterschiedlichen Verpackungsmaterialien notwendig. Zur Erforschung der Feldunregelmäßigkeiten im UHF-Bereich wäre es dienlich, Referenzmodelle für verschiedene Stapel dielektrischer Objekte und Leseanordnungen zu entwickeln, um vereinfachte Modellrechnungen durchzuführen zu können. Weitere Entwicklungsarbeiten sollten zudem über die reine RFID-Hardware hinausgehen und z.B. RFID-freundliche Verpackungen zum Ziel haben.
Bei ungeordneten Produktgemischen lassen sich vermutlich auch bei optimierter Hardware keine hundertprozentigen Leseraten erreichen. Daher sollten einheitliche Verfahren entwickelt werden, um defekte oder nicht gelesene Tags zu identifizieren. Eine Echtzeit-Verknüpfung von RFID-Daten der unterschiedlichen Verpackungsebenen könnte als Ansatz dienen: Wird z.B. auf der Ebene der Produktkartons gemeldet, dass 12 Einzelpackungen enthalten sein müssen, dann sollte das System auf das Ereignis reagieren können, dass nur 11 Packungen gelesen werden konnten [li06].
Medikamentenfälschungen kommen auch auf Ebene der so genannten Blisterverpackungen vor, also auf Ebene der Primärverpackung [platzen06]. Meist sind mehrere Blisterverpackungen in einem gemeinsamen Umkarton enthalten. Einzelne originale Blisterverpackungen könnten mit gefälschten Verpackungen getauscht sein, so dass im originalen Umkarton echte und gefälschte Medikamente vorkommen können. Eine Integration von Tags in Blisterverpackungen stellt nicht nur durch die erhöhte Anzahl und Dichte der Tags eine Herausforderung dar, sondern vor allem dadurch, dass die Verpackung bevorzugt aus Aluminium oder anderen Metallen besteht. Die Möglichkeit, Blisterverpackungen als Antennen zur RFID-Signalverstärkung zu nutzen, sollte untersucht werden.

Entwicklung von kryptographischen Mechanismen

Die Entwicklung hardware-effizienter Krypto-Verfahren für Low-Cost Tags ist eine Voraussetzung für die Implementierung von Sicherheitsprotokollen gegen Medikamentenfälschungen. Die üblichen Algorithmen wie AES und RSA zur Verschlüsselungs- und gegenseitigen Authentisierung können nicht auf Low-Cost Tags implementiert werden. Geeigneter erscheinen Algorithmen, die viele Male hintereinander einfache Berechnungen durchführen und nur we-

nig Overhead zum Lesen der Tags hinzufügen wie Hash-basierte Verfahren (siehe 3.2.6), in deren Berechnung aber ein kryptographisches Geheimnis zur Authentisierung eingehen sollte. Um ein flexibles Schlüsselmanagement ohne ständige Serverzugriffe realisieren zu können, erscheint die Erweiterung von RFID-Lesern um Sicherheitsfunktionalität notwendig, die ein Nachladen und Aktualisieren von Schlüsseln erlauben. Ein guter Ansatz kann die Integration eines Trusted Platform Module (TPM) in den Leser sein, wie er in [molnar05] vorgeschlagen wird. Sinnvoll wäre auch die Entwicklung effizienter Offline-Authentisierungsverfahren [lehtonen06], z.B. eine Batch Mode Authentisierung wie in [tsudik06]. Dort initiiert ein RFID-Leser Authentisierungprozeduren im Offline-Modus und beendet sie, sobald die Netzverbindung wieder besteht.

Entwicklung von Sicherheitsprotokollen gegen Produktfälschungen

Ein wichtiges Entwicklungsziel sind spezielle Sicherheitsprotokolle zur Produktauthentisierung. Die Verknüpfung des RFID-Tags mit den Produkten bzw. der Verpackung muss fälschungssicher gestaltet werden, so dass das Tag integraler Bestandteil des Medikaments wird und der Produktauthentisierung dienen kann. Darüber hinaus werden langfristig Maßnahmen zur automatischen Detektion von physischen Manipulationen an Tag, Verpackung und Produktinhalten benötigt. Idealerweise sollten die Sensoren bei fehlerhaften Verbindungen zwischen Tag und Produkt oder beim Öffnen der Verpackung automatische Warnungen generieren, die als Events im RFID-System verarbeitet werden [inaba06]. Entsprechende Sensoren sind heute bestenfalls auf Basis aktiver Tags realisierbar und entsprechend kostspielig. Ein langfristiges Ziel wäre es, eine entsprechende Sensorik auf passiven Tags zu entwickeln, welche z.B. auf der Basis von Energy Harvesting (Bewegung, Licht, Temperaturunterschiede, Piezoeffekt unter Druck etc.) arbeitet, Veränderungen an der Packung registriert und diese auf Anfrage dem System mitteilt.
Sicherheitsprotokolle zur Produktauthentisierung könnten eine Verknüpfung von aufgedruckten Produktdaten mit einer Physical Uncloneable Function (PUF, siehe 3.2.3) des Chips vorsehen. Dabei werden Verfahren benötigt, die auch offline durchführbar sind, evtl. auch eine manuelle Eingabe von Produktdaten zulassen oder mit Barcode-Daten kombiniert werden können. Eine vielversprechende Kombination von physikalischen Fingerprints (auf Grundlage von PUFs) und kryptographischen Methoden der digitalen Signatur und Authentisierung auf Basis von ECC wird in [tuyls06] vorgestellt.

7 Technologie-Roadmap

7.1 Forschungs- und Entwicklungsbedarf

Ein großes Hindernis für die Einführung von RFID-Systemen ist das Fehlen von technischen Richtlinien und anwendungsspezifischen Standardlösungen (Best Practice Scenarios). RFID-Anwendungen müssen auf ihren spezifischen Anwendungskontext zugeschnitten sein, was die Definition von Anwendungsfällen und die Durchführung umfangreicher Tests erfordert. Damit sind potentielle Anwender schnell überfordert. Wichtig ist die Entwicklung einheitlicher Nutzungskonzepte für RFID-Ressourcen, z.B. für den Benutzerspeicher auf Tags.

Verbesserte RFID-Hardware

Eine wesentliche Voraussetzung für die sichere Anwendung von RFID-Systemen ist eine auf physikalischer Ebene zuverlässige Funktion von Tags. RFID-Technologien sollten auf ihre Robustheit hinsichtlich von Temperatureinwirkungen, elektrischen Einwirkungen (unmittelbar oder durch übergroße Feldstärken) sowie mechanische Beanspruchung untersucht und optimiert werden.

Eine dauerhafte Integration (Einbettung) von Tags in die Bauteile industrieller Fertigungsprozesse oder Produkte erfordern neue Verfahren für eine sichere produktintegrierte Verarbeitung (z.B. Gussintegration) von RFID-Tags. Für extreme Low-Cost-Anwendungen sind die Potentiale neuartiger Herstellungsverfahren, wie beispielsweise Druckverfahren, zu berücksichtigen. In vielen Anwendungsgebieten ist zukünftig eine gemischte Verwendung von in verschiedenen Frequenzbereichen arbeitenden Tags zu erwarten. Daher werden in Zukunft vermehrt multi-standardfähige Lesegeräte benötigt (Abstraktion von der „Physik“) Neue Sicherheitskonzepte sollten mit einem an die jeweilige Anwendung angepassten Sicherheitsniveau unabhängig auf Tags verschiedener Frequenzen (HF, UHF) implementierbar sein und von Lesegeräten verarbeitet werden können.

Für einen interferenzfreien Betrieb von RFID-Lesegeräten bei eingeschränkten Frequenzressourcen (insbesondere im UHF-Bereich) werden neue Verfahren für die sichere Steuerung von Lesegeräten in Multireader-Umgebungen und eine sichere Detektion von Leseausfällen durch Interferenzen benötigt. Eine Vielzahl von Anwendungsfällen benötigt neue Verfahren zur Integration von Sensoren (Bildverarbeitung, Manipulationserkennung) in RFID-Systeme, um die Systemzuverlässigkeit und Systemsicherheit zu verbessern. So könnte eine automatische Detektion und Behebung von durch RFID-Fehlfunktionen erzielt werden. Letzteres kann dazu beitragen, Systemausfälle in RFID-gestützten Prozessen zu vermeiden oder zumindest zu reduzieren. Bei sicherheitskritischen oder auch hochwertigen Produkten (Bauteilen) sind geeignete Verfahren für die physikalische Integration von Tags mit den Produkten gefragt. Anderenfalls könnten die Tags einfach entfernt werden und mit anderen, gefälschten Produkten verknüpft werden. Eine Möglichkeit ist die Gussintegration, wobei jedoch ein zu starker Abschirmungseffekt bzw. eine große Verringerung der Lesereichweite zu verhindern ist. Somit sind Industrietaugliche Verfahren für eine solche Gussintegration zu entwickeln.

Effiziente Kryptoverfahren

Die Entwicklung hardware-effizienter kryptographischer Verfahren ist eine Voraussetzung für die Realisierung von Sicherheitsverfahren auf Low-Cost Tags. Herkömmliche Algorithmen müssen für die begrenzten Ressourcen optimiert werden. Ein mittel- und langfristig aussichtsreiches Forschungsfeld ist der Ersatz von kryptographischen Schlüsseln durch preisgünstige physische und technologie-integrierte Fingerprints (z.B. auf Basis von PUFs, POWs und One-Time-Codes), welche Teile des Produkts oder der Verpackung werden bzw. untrennbar mit dem Chip verbunden sind. Fingerprints sind auch für Ultra-Low-Cost Tags denkbar, welche auf Basis von leitenden Polymeren entwickelt werden und idealerweise direkt auf die Verpackung gedruckt oder in die Produktmaterialien integriert werden. Verglichen mit schwer kopierbaren kryptographischen Schlüsseln haben PUFs und POWs-basierte Fingerprints verstärkte Anti-Cloning Eigenschaften, weil das integrierte Geheimnis durch Manipulationen zerstört wird und selbst durch Reverse Engineering oder Side-Channel-Attacken nicht ermittelt werden kann. Die Sicherheitsanalyse von veröffentlichten Verfahren und proprietären Protokollen kommerziell erhältlicher RFID-Hardware sind weitere notwendige Forschungsthemen.

Des Weiteren werden Verfahren für eine sichere Deaktivierung und Reaktivierung von Tags benötigt. Dies ist nicht nur im Einzelhandel zur Umsetzung von Datenschutzanforderungen der Fall, sondern beispielsweise auch in der Automobillogistik, zumal auf den RFID-Tags evtl. vertrauliche Produkt- bzw. Produktionsdaten gespeichert werden. Ein einfacher Passwortschutz zur Absicherung der Enable- und Disable-Befehle für die Tags ist unter Umständen zu unflexibel und unsicher, so dass hier noch Forschungsbedarf besteht. Auch sind die bisher vorgeschlagenen Verfahren meist einseitig auf Datenschutzanforderungen zugeschnitten, ohne die weiteren Ziele der Datensicherheit zu berücksichtigen.

Identitäts- und Berechtigungsmanagement

Neben der Entwicklung von effizienten kryptographischen Verfahren existieren jedoch auch Forschungsfragen im Bereich der organisatorischen Sicherheit bzw. des Sicherheitsmanagements von RFID-Systemen. So sind insbesondere Verfahren zu entwickeln, die ein sicheres, aber auch skalierbares Management für Access- und Kill-Passwörter sowie für kryptographische Schlüssel erlauben. Der Aufwand für die Schlüsselverwaltung kann bereits in einem Automobilwerk sehr hoch werden, wenn beispielsweise pro Jahr 200.000 Fahrzeuge produziert werden, die mit Tags und somit mit kryptographischen Schlüsseln ausgestattet sind. Noch komplexer wird das Schlüsselmanagement in den RFID-Anwendungsszenarien der Massenkonsumgüter. Wenn zudem eine differenzierbare Zugriffskontrolle für Tags eingesetzt werden soll, sind pro Tag verschiedene kryptographische Schlüssel zu erzeugen und zu verwalten.

Ferner wird in der Taucis-Studie [taucis06] zum Aspekt des Schlüsselmanagements in RFID-Systemen formuliert: *Für geschlossene Systeme mit einem kleinen, vorher bekannten Teilnehmerkreis und einer begrenzten Anzahl von Tags zeichnen sich Lösungen ab. Nicht jedoch für offene Systeme, die z.B. auch Dienste nach dem Verlauf eines Objektes („Post-Sale Services“) anbieten und dabei etwa auch das geplante globale EPC-Netzwerk einbinden. Alle Verfahren müssen um ein sicheres Verfahren zum Schlüsselmanagement ergänzt werden – ein Problem, das derzeit noch nicht einmal theoretisch gelöst ist.* Dies zeigt noch einmal, dass das Schlüsselmanagement ein ungelöstes Problem im Bereich der RFID-Sicherheit ist.

Darüber hinaus ist eine differenzierte Zugriffskontrolle für die Tags erforderlich, wenn wie z.B. in der Automobilindustrie die Tendenz besteht, Produktdaten auf den Tags und nicht im Backend zu speichern. Heutzutage erlauben (meist höherwertige) Tags nur eine Rechtevergabe mit zwei verschiedenen Schlüsseln. Bei einem lieferketten-übergreifenden Einsatz von RFID sind jedoch oftmals mehr als zwei Partner wie z.B. Lieferant, Produzent, Logistiker, Händler und Kunde beteiligt. Auch wenn solche Tags recht komplex werden können, müssen diese dennoch möglichst kostengünstig bleiben, damit sich der Einsatz von RFID amortisiert. Die Entwicklung von möglichst kostengünstigen Tags mit einer differenzierbaren Zugriffskontrolle ist mithin ein weiteres Forschungsgebiet.

In allen Szenarien, die in dieser Studie behandelt worden sind, spielt die lieferketten-übergreifende Verfolgung von mit RFID-Tags bestückten Produkten eine Rolle. Hierfür müssen verschiedene Partner der Lieferkette auch auf im Backend gespeicherte Daten zugreifen, wobei diese Partner unterschiedliche Zugriffsberechtigungen besitzen sollten. Aus diesem Grunde ist ein skalierbares und effektives lieferketten-übergreifendes Identitäts- und Berechtigungsmanagement zu etablieren (föderiertes Identitätsmanagement). Ein solches föderiertes Identitätsmanagement soll eine transparente lieferketten-übergreifende Authentisierung der einzelnen Partner an dem Backend-System ermöglichen. Welche Informationen (Attribute) dabei für die einzelnen Identitäten einer RFID-gestützten Lieferkette benötigt werden, ist derzeit ein offenes Problem. Insbesondere sind Verfahren zu entwickeln, um geeignete Rollen und Berechtigungen für die verschiedenen Lieferkettenpartner zu definieren.
Darüber hinaus sollte auch bei einer tiefen Integration der RFID-Technologie in Produktionsprozesse (innerhalb eines Unternehmens) ein geeignetes rollenbasiertes Berechtigungsmanagement etabliert werden, um den Zugriff auf Produktionsdaten und einzelne Arbeitsschritte zu regeln.

Verbesserte Systemintegration und Sicherheit

Interoperabilität ist eine wesentliche Voraussetzung für eine unternehmensübergreifende Realisierung technologieintegrierter Datensicherheit von RFID-basierten Systemen. Unter dem Aspekt der Systemintegration besteht hier zunächst Klärungs- und Standardisierungsbedarf hinsichtlich der Organisation der Datenspeicherung (ob nur in Middleware, ob nur auf dem Tag oder sowohl in Middleware als auch auf dem Tag). Weiterhin besteht ein Bedarf der Entwicklung vereinheitlichter Datenstrukturen für Produktdaten und Sicherheitsinformationen auf dem Tag und in der Middleware. Eine einheitliche Anbindung von RFID-Systemen an ERP-Anwendungen ist ebenso notwendig wie eine Service-Interoperabilität verschiedener Registrierungsorganisationen (Second Source Prinzip).

Zukünftige Forschungsvorhaben sollten auch eine Schwachstellenanalyse von Softwarekomponenten eines RFID-basierten Gesamtsystems (Betriebssysteme für Lesegeräte, RFID-Middleware) adressieren, um Sicherheitslücken schließen zu können. Eine Erarbeitung von IT-Sicherheitsstandards bzw. IT-Sicherheitskriterien für RFID-Technologien wird ein wesentlicher Schritt auf dem Weg zu sicheren Gesamtsystemen sein.

Nicht zuletzt werden integrierte Konzepte für Datensicherheit und Datenschutz benötigt, da Systemsicherheit eine wesentliche Voraussetzung für eine verantwortliche und geregelte Verarbeitung personenbezogener Daten ist. Technische Konzepte wie kryptographische Verfahren und Authentisierungsverfahren können hier synergetisch und aufwandsoptimiert Hand in Hand mit der Entwicklung neuer Konzepte für den Datenschutz integriert werden.

Da sich durch den Einsatz der RFID-Technologie die Komplexität von Prozessen erhöhen kann, werden zur Validierung und Verifikation der Sicherheit eines RFID-Systems Methoden für eine formale Beschreibung komplexer RFID-gestützter Prozesse benötigt, die in zukünftigen Forschungsprojekten entwickelt werden müssen. Diese Verfahren sollen automatisch und systematisch die auftretenden Prozessstörungen erkennen und ggf. beheben. Insbesondere sollten die Auswirkungen kleinster Ausfälle auf ein komplexes dynamisches System, wie es z.B. eine RFID-gestützte lieferketten-übergreifende Warenkette darstellt, untersucht werden. Ein interessantes offenes Forschungsgebiet besteht beispielsweise darin, RFID-gestützte Prozesse in einem mathematischen Modell zu erfassen und dieses Modell anschließend mit Hilfe von geeigneten Verifikationswerkzeugen wie z.B. Modellprüfern zu analysieren, um auf diese Weise Schwachstellen und unerwartete Abhängigkeiten innerhalb des Prozesses zu ermitteln.

7.2 Einschätzung der Förderungswürdigkeit

Hardware. Der Forschungsbedarf im Bereich Hardware bezieht sich im Wesentlichen auf die Themen Funktionssicherheit, Robustheit und Einsetzbarkeit. Es handelt sich also vorwiegend um kurz- bis mittelfristige anwendungsbezogene Forschung. Da in dieser Frage sowohl ein hohes Problembewusstsein als auch entsprechende Kompetenzen in der Wirtschaft bestehen, ist der Bedarf an Forschungsförderung durch öffentliche Mittel als vergleichsweise moderat einzustufen.

Software. Hier ist mittel- bis langfristig ein gewisser Bedarf für die Forschungsförderung durch die öffentliche Hand zu erwarten. Das möglichst fehlerfreie Design entsprechender Software erfordert genaue Kenntnis der zu verwendenden Protokolle sowie einen ausreichenden theoretischen Hintergrund in aktuellen Entwicklungsmethoden. Daher empfiehlt sich hier die Beauftragung von Forschungsinstitutionen.

Kryptographie. Hier geht es um die Anpassung vorhandener kryptographischer Methoden bzw. Sicherheitsprotokolle oder eventuell auch die Neuentwicklung für die RFID-Technologie. Dies erfordert einen sehr guten wissenschaftlichen Hintergrund. Daher scheint ein nicht zu vernachlässigender mittel- bis langfristiger Förderungsbedarf durch die öffentliche Hand auf jeden Fall gegeben zu sein.

IT-Sicherheitsstandards. Im Bereich der IT-Sicherheitsstandards für RFID-Technologie sollten Forschungsinstitutionen sowie das BSI die Führung übernehmen. Das BMBF sollte sein Vorgehen in diesem Gebiet mit dem BSI koordinieren. Die mittel- bis langfristige Förderungswürdigkeit aus Sicht der öffentlichen Hand ist als durchaus bedeutend einzustufen.

Formale Beschreibungen von Prozessen. Die Untersuchung der speziellen Eigenschaften RFID-gestützter Prozesse kann die langfristige Skalierbarkeit sich entwickelnder Prozesse gewährleisten. Mit Hilfe der Darstellung durch formale Methoden lassen sich kritische Prozessschritte und Schwellen schon im Vorfeld identifizieren.

Fortgeschrittenes Identitäts- und Berechtigungsmanagement. Dieser Bereich betrifft im Wesentlichen die Zugriffskontrolle und die Verwaltung von Identitäten für die durch den Einsatz der RFID-Technologie verfügbaren Daten im Kontext von Produktionsprozessen bzw. von Lieferketten. Dabei sind organisatorische Richtlinien, Datenschutzanforderungen, Konsumenten- und Firmeninteressen zu beachten. Ferner erfordert eine Zertifizierung nach IT-Sicherheitsstandards wie den Common Criteria formale Nachweise der Erfüllung von Sicherheitsanforderungen. Die Forschung auf dem Gebiet des fortgeschrittenen Berechtigungsmanagements befindet sich noch in den Anfängen. Ferner ist das Problembewusstsein der Wirtschaft in diesem Bereich noch gering. Aus den oben genannten Gründen ist dieser Themenbereich in der langfristigen Perspektive als besonders förderungswürdig einzustufen.

Glossar

Abstract Syntax Notation One (ASN.1)	Formale Regeln zur flexiblen Notation von Datenstrukturen zur Präsentation, Kodierung und Übertragung von Daten unabhängig von maschinenspezifischen Kodierungen.
Authentisierung (Authentication)	Der Entscheidungsprozess darüber, ob eine Person oder ein Objekt tatsächlich die Identität besitzt, welche behauptet wird. Für Personen werden z.B. der Besitz einer Sache (z.B. Ausweis), wissensbasierte oder biometrische Verfahren eingesetzt. Objekte authentisieren sich kryptographisch z.B. durch die nachweisliche Verwendung eines geheimen Schlüssels.
Authentizität (Authenticity)	Die Eigenschaft von Verfahren, sicherzustellen, dass Objekte oder Daten eine gesicherte Herkunft besitzen. Die Eigenschaft von Objekten oder Daten, authentisch, vertrauenswürdig und keine Fälschungen zu sein.
Auto-Id Labs	Führender Forschungsverbund auf dem Gebiet der Nutzung von RFID in einem globalen Netzwerk. Auto-Id Labs arbeitet EPCglobal zu.
Autorisierung (Authorization)	Der Prozess, bestimmte Zugriffs- und Nutzungsrechte an Personen oder Objekte zu vergeben. Damit wird festgelegt, welche Aktionen (z.B. Anfragen) eine Instanz durchführen darf und welche ihr verwehrt sind. Die Prüfung dieser Rechte erfolgt gewöhnlich während einer Authentisierung, die in vielen Fällen gegenseitig erfolgt.
Electronic Product Code (EPC)	Nummernschema, mit dem Objekte (Logistikeinheiten, Transportbehälter, Produkte aller Art) eindeutig gekennzeichnet und identifiziert werden können. Er basiert auf einer Erweiterung der weltweit verbreiteten EAN-Nummernstandards. Beim EPC erhält jeder einzelne Artikel, jedes Objekt eine individuelle Seriennummer. Der EPC wurde von Auto-ID-Labs und EPCglobal entwickelt und im EPCglobal Tag Data Standard spezifiziert.
EPC Discovery Services	EPC-Ermittlungsdienste, welche das Auffinden von Informationen über einen bestimmten EPC ermöglichen. Im Gegensatz zu ONS verweisen die EPC Discovery Services auf alle Datenquellen (EPCIS), die Informationen zu einem bestimmten EPC gespeichert haben.
EPCglobal	Die Non-Profit-Organisation EPCglobal Inc. entwickelt Standards für die einheitliche Nutzung der RFIDTechnologie entlang der gesamten Versorgungskette über Länder- und Branchengrenzen hinweg.
EPC Information Services (EPCIS)	Der EPC-Informationsservice stellt die Verbindung zwischen einem Unternehmen und dem EPCglobal Netzwerk dar. EPC-Informationen werden im EPC-Informationservice gespeichert und den Netzwerkmitgliedern zur Verfügung gestellt.
EAN (European Article Number)	EAN steht für International Article Number (früher European Article Number) und ist ein weltweit verwendetes Nummerierungssystem zur automatischen Identifikation von Produkten und logistischen Einheiten. Die EAN wird in der Regel als Barcode auf die Warenpackung aufgedruckt.
European Article Numbering Association	Organisation, die die EAN-Standards seit 1977 entwickelte und später in EAN International umbenannt wurde.
EAN International	Globale Organisation, die die EAN.UCC-Standards entwickelt. Seit 2005 GS1.
EAN.UCC	Zusammenführung von EAN und UCC (siehe unten) zu einem Nummernsystem.
Föderation (Federation)	Um Identitäten unternehmensübergreifend zu verwalten, werden mehrere unternehmensinterne IDM-Systeme zu einer Föderation zusammengeschlossen. Zwischen den einzelnen Unternehmen wird auf diese Weise eine entsprechende Vertrauensbeziehung aufgebaut.

Funktionssicherheit	Die Eigenschaft eines Systems keine unzulässigen sicherheitskritischen Zustände einzunehmen, sondern zu gewährleisten, dass die spezifizierten Funktionen zuverlässig erbracht werden.
GS1	GS1 (Globals Standard 1) ist eine globale Organisation (vormals EAN International), die globale Standards entwickelt, um die Effizienz und Transparenz von Lieferketten auf verschiedenen Gebieten (wie Gesundheitswesen, Transport und Logistik) weltweit zu verbessern. GS1 hat in über 100 Ländern Mitgliedsorganisationen (wie z.B. GS1 Germany). GS1 arbeitet eng mit anderen Internationalen Standardisierungsorganisationen zusammen.
GS1 Germany	GS1 Germany (vormals CCG) ist das Dienstleistungs- und Kompetenzzentrum für unternehmensübergreifende Geschäftsabläufe in der deutschen Konsumgüterwirtschaft und ihren angrenzenden Wirtschaftsbereichen. Sie ist Gründungsmitglied der internationalen EAN-Organisation, deren Standards heute in 129 Ländern eingesetzt werden.
Insellösung	Einsatz von RFID-Technologie nur in einem Teil der lieferketten-übergreifenden Prozesskette.
Integrität (Integrity)	Die Eigenschaft von Verfahren, sicherzustellen, dass Daten seit Verlassen ihrer Quelle unverändert sind und nicht zufällig oder böswillig modifiziert oder gelöscht wurden. Die Eigenschaft der Daten, korrekt und vollständig zu sein und der Absicht ihres Urhebers zu entsprechen.
International Organization for Standards	Die ISO ist eine internationale Vereinigung der Standardisierungsgremien von 151 Ländern. Sie verabschiedet internationale Standards in allen Bereichen. Deutschland ist durch das Deutsche Institut für Normung (DIN) in der ISO vertreten.
Identitätsmanagement (Identity Management)	Je größer ein Unternehmen ist, desto mehr Identitäten und Berechtigungen müssen für die einzelnen Benutzer verwaltet werden. Dazu werden so genannte Identitätsmanagement-Systeme (IDM-Systeme) eingesetzt. Dabei handelt es sich um Software-Komponenten, welche die Identitäten und deren Berechtigungen verwalten.
Item-Management	Kennzeichnung von Objekten in der Güter- und Warenwirtschaft mit RFID
Just-in-Sequence-Produktion	Unter JIS-Produktion wird der Einbau von Bauteilen in der Reihenfolge, wie sie von den Lieferanten bereitgestellt werden, verstanden.
Nicht-Abstreitbarkeit (Non-Repudiation)	Die Eigenschaft von Verfahren, sicherzustellen, dass eine Aktion nachweislich mit dem Urheber verbunden ist, z.B. dass ein Benutzer die Durchführung einer Aktion oder der Empfänger von Daten ihren Erhalt nicht abstreiten kann.
Object Naming Service (ONS)	Der ONS ist vergleichbar mit dem Domain Name Service (DNS) des Internet und dient dem Auffinden des EPCIS des Herstellers eines Objektes anhand eines EPC. Der Root ONS ist ein Dienst von EPCglobal und wird gegenwärtig von der Firma VeriSign betrieben, die auch den DNS verwaltet.
Offenes System	Eine Betriebsumgebung, die Interoperabilität und Portabilität durch offene Schnittstellen und Spezifikationen sichert.
Radio Frequency Identification (RFID)	RFID ist ein Verfahren zur kontaktlosen Identifizierung und Lokalisierung von Gegenständen und Lebewesen und zur automatischen Erfassung und Speicherung von Daten.
RFID-System	Prinzipiell umfasst ein RFID-System ein Tag, das ein Objekt kennzeichnet, ein Lesegerät zum Auslesen der Tagdaten und eine RFID-Middleware mit Schnittstellen zu weiteren EDV-Systemen und Datenbanken.
RFID-Transponder	Ein RFID-Transponder (oft auch als Tag, bezeichnet) besteht aus: Mikrochip, Antenne, Träger oder Gehäuse und Energiequelle (bei aktiven Transpondern). Der Begriff Transponder ist zusammengesetzt aus den Begriffen Transmitter und Responder. Transponder können passiv oder aktiv sein.

Rollenbasiertes Berechtigungsmanagement (Role-based Access Control)	Beim rollenbasierten Berechtigungsmanagement werden Berechtigungen nicht direkt an einzelne Benutzer gebunden, sondern Benutzern über Rollen zugewiesen, welche die Benutzer im Unternehmen innehaben.
Sequenztreue	Als Sequenztreue wird die reihenfolgetreue Bereitstellung der Komponenten entsprechend dem JIS-Prinzip bezeichnet.
Smartlabel	Etikett mit aufgedrucktem Barcode, in das ein RFID-Transponder eingebracht ist
Tag Identifier (Tag-ID)	Ein Unique Identifier (UID) zur eindeutigen Identifizierung von RF-Tags während der Datenübertragung. Die Kennung ist nicht mit dem EPC zu verwechseln, der das getaggte Produkt kennzeichnet.
Uniform Code Council (UCC)	Eine weltweit einflussreiche Organisationen, die sich auf Globalisierung und Standardisierung spezialisiert hat und z.B. den Barcode Universal Product Code (auch UPC genannt) entwickelte. Der UCC ist eine Mitgliedsorganisation von EAN International. 2005 änderte das UCC seinen Namen in GS1 US.
Unique Identifier (UID)	In [iso15961] definierter Code, der in permanente UID und dynamische UID unterschieden wird. Eine permanente UID besteht aus drei Feldern. Das erste Feld gibt die Klasse des Herausgebers an. Darauf folgt die Registrierungsnummer des Herausgebers und die von ihm vergebene eindeutige Seriennummer. Der UID wird - wenn erforderlich - zur Identifizierung von RFID-Tags bei Lese- und Schreiboperationen verwendet.
Unique Item Identifier	In [iso15961] definierter Code, der einen Gegenstand (z.B. ein Produkt, eine Transporteinheit) bezeichnet, welcher innerhalb einer Domäne oder Bereichs eines Codesystems einmalig ist. Bei EPCglobal ist das der EPC.
Vertraulichkeit (Confidentiality)	Die Eigenschaft von Verfahren, sicher zu stellen, dass nur autorisierte Instanzen auf die Daten zugreifen oder diese entschlüsseln können, z.B. nur nach einer erfolgreichen Authentisierung. Die Eigenschaft der Daten, zugriffsgeschützt oder kryptographisch verschlüsselt zu sein.
Variantentreue	Korrekte Platzierung von einzubauenden Objekten in der Produktion, z.B.. dass linke Sitze auf der linken und rechte Sitze dementsprechend auf der rechten Seite eines Fahrzeugs neben dem Band abgestellt und anschließend korrekt eingebaut werden.
Virtuelle Baukarte	Auf einer Baukarte befinden sich üblicherweise die dokumentations- und archivierungspflichtigen Produktionsdaten eines Automobils. Diese geben Auskunft über die verbauten Teile und dokumentieren den Produktionsweg; auch werden Verbaufehler vermerkt. Mit Hilfe der Baukarte lassen sich während der Produktion regulär vorgenommene Arbeiten und nachträgliche Fehlerkorrekturen nachvollziehen. Die Baukarte liegt derzeit noch in Papierform vor. Unter einer virtuellen Baukarte versteht man dann die Abbildung der Baukarte auf elektronische Systeme wie z.B. RFID-Tag.

Literatur

[adt06] ADT/Tyco Fire & Security, Alien Technology, Impinj, Intel, Symbol, Xterprise: RFID and UHF: A prescription for RFID success in the pharmaceutical industry, White Paper, June 2006

[angerer03] A. Angerer, L. Dittmann: Einsatzfelder von RFID in der Logistik am Beispiel der Warenrückverfolgung, Kühne-Institut für Logistik, St. Gallen, 2003. Online verfügbar unter: www.klog.unisg.ch

[avoine07] G. Avoine: Security and privacy in RFID systems, bibliography web page: http://lasecwww.epfl.ch/~gavoine/rfid/

[bailey06] D. V. Bailey, A. Juels: Shoehorning Security into the EPC Standard, RSA Laboratories, January 2006

[barber05] G. Barber, E. Tsibertzopoulos: An Analysis of Using EPCglobal Class-1 Generation-2 RFID Technology for Wireless Asset Management, Booz Allen Hamilton, 2005

[batina07] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede: Public-Key Cryptography for RFID-Tags, PerSec Conference, 2007

[bearingpoint04] How RFID Technology protects the Pharmaceutical Supply Chain, BearingPoint, Agnew Moyer Smith Inc., 2004

[bercelon05] A. Stiehler, T. Wichmann: RFID im Pharma- und Gesundheitssektor, Berlecon Report, Berlin 2005

[bitkom05] White Paper RFID – Technologie, Systeme und Anwendungen, BITKOM Projektgruppe RFID, Berlin, August 2005

[bitkom06] BITKOM RFID Guide 2006, BITKOM Projektgruppe RFID, Berlin, 2006

[bmu05] Bundesumweltministerium: Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten (Elektro- und Elektronikgerätegesetz – ElektroG)*), Bundesgesetzblatt Jahrgang 2005 Teil I Nr. 17, Bonn, 23. März 2005, http://www.bmu.de/files/pdfs/allgemein/application/pdf/elektrog.pdf

[bsi04] Bundesamt für Sicherheit in der Informationstechnik – BSI: Risiken und Chancen des Einsatzes von RFID-Systemen, 2004.

[bsi06] Bundesamt für Sicherheit in der Informationstechnik – BSI: Extended Access Control (EAC), http://www.bsi.bund.de/fachthem/epass/eac.htm

[büchel06] P. B. Büchel, O. Platzen: RFID-Technologie zur Verhinderung von Arzneimittelfälschungen, Pharm. Ind. 68, Nr. 10, 1153-1157, 2006

[bvg2006] Betriebsverfassungsgesetz, Stand 30.10.2006

[calmels06] B. Calmels, S. Canard, M. Girault, H. Sibert: Low-Cost Cryptography for Privacy in RFID Systems, CARDIS 2006, LNCS 3928, pp. 237-251, 2006

[chandramouli05] R. Chandramouli, T. Grance, R. Kuhn: Security Standards for the RFID Market, IEEE Security & Privacy, 2005

[cwa14890-1] CEN Workshop Agreement 14890: Application Interface for SmartCards used as Secure Signature Creation Devices, Part 1: Basic Requirements, 2004

[defend07] B. Defend, K. Fu, A. Juels: Cryptanalysis of Two Lightweight RFID Authentication Scheme

[dimitriou05] T. Dimitriou: A lightweight RFID Protocol to protect against Traceability and Cloning attacks, IEEE, 2005

[duc06] D. N. Duc, H. Lee, K. Kim: Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning, Auto-ID Labs Information and Communication University, White Paper, 2006

[eckert04] C. Eckert: IT-Sicherheit – Konzepte, Verfahren, Protokolle, Oldenbourg Verlag München Wien, 3. Auflage, 2004

[ecrypt06]	European Network of Excellence in Cryptology (ECRYPT): Yearly Report on Algorithms and Keysizes (2005), January 2006, online abrufbar unter: http://www.ecrypt.eu.org/documents/D.SPA.16-1.0.pdf
[elektrog05]	Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten, BGBl I 2005
[epc-ale]	EPCglobal: The Application Level Events (ALE) Specification,Version 1.0, Ratified Specification, September 2005
[epc-arch]	EPCglobal: The EPCglobal Architecture Framework, Final Version, July 2005
[epc-cert]	EPCglobal: Certificate profile, Ratified Specification, Version 1.0, March 2006
[epc-gen1data]	EPCglobal: EPC Generation 1 Tag Data Standards Version 1.1 Rev.1.27, May 2005
[epc-gen2data]	EPCglobal: EPCglobal Tag Data Standard Version 1.3, March 2006
[epc-gen2]	EPCglobal: EPC Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz – 960 MHz, Version 1.0.9, January 2005
[epc-ons]	EPCglobal: Object Naming Service (ONS), Version 1.0, October 2005
[epc-pedigree]	EPCglobal: Pedigree Ratified Standard, Version 1.0, January 2007
[erdos05]	M. Erdos: RFID and Authenticity of Goods, In: [garfinkel05]
[eu2000]	Richtlinie 2000/53/EG des europäischen Parlaments und des Rates vom 18. September 2000 über Altfahrzeuge, veröffentlicht in Amtsblatt der Europäischen Gemeinschaften am 21.10.2000
[fda05]	Combating Counterfeiting Drugs: A Report of the Food and Drug Administration Annual Update, US Department of Health and Human Services, 2005
[feldhofer04]	M. Feldhofer: An Authentication Protocol in a Security Layer for RFID Smart Tags, IEEE MELECON 2004, May 2004
[feldhofer04a]	M. Feldhofer, S. Dominikus, J. Wolkerstorfer: Strong authentication for RFID systems using the AES algorithm, Lecture Notes in Computer Science, Vol. 3156, pp 357-370, 2004
[fiat87]	A. Fiat, A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Proceedings on Advances in Cryptology - *CRYPTO '86.* Springer-Verlag, S. 186–194, 1987
[finke04]	T. Finke, H. Kelter: Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, 2004
[finkenzeller06]	K. Finkenzeller: RFID Handbuch, 4. Auflage, Hanser Verlag, 2006
[fleisch05]	E. Fleisch, F. Mattern: Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Springer-Verlag, Berlin 2005.
[fu02]	X. Fu, T. Bultan, J. Su: Formal Verification of e-Services and Workflows. WES 2002: 188-202
[garfinkel05]	S. L. Garfinkel, A. Juels, R. Pappu: RFID Privacy: An Overview of Problems and Proposed Solutions, 2005
[garfinkel06]	S. Garfinkel, B. Rosenberg (Hrsg.): RFID – Applications, Security, and Privacy, Addison-Wesley, 2006
[ghosal06]	R. Ghosal, M. Jantscher, A. R. Grasso, P. H. Cole: One time codes, Auto-ID Labs University of Adelaide, White Paper, 2006
[gm2001]	GM Vehicle Supply Operations – Material Business Process Group: GM 1724-A – Label Template For Individual Containers, 2001
[goldreich86]	O. Goldreich, S. Micali, A. Widgerson: Proofs that yiels nothing but their validity nad a methodology of cryptographic protocol design. Proc. 27. FOCS, S. 171-185, 1986

[grasso06] A. R. Grasso, P. H. Cole: Definition of terms used by the Auto-ID Labs in the anti-counterfeiting white paper series, Auto-ID Labs University of Adelaide, White Paper, 2006

[gs1] GS1-Germany: www.gs1-germany.de

[gs1-06] GS1 Germany: Fälschungssicherheit per EPC, Über EPC und EPCglobal-Netzwerk Warenechtheit gewährleisten, März 2006, Online verfügbar: [gs1]

[hanke05] G. Hanke: A Practical Relay Attack on ISO 14443 Proximity Cards, 2005, online verfügbar unter http://www.cl.cam.ac.uk/~gh275/relay.pdf, Zugriff am 06.12.2006

[hancke06] G. Hancke: Practical Relay Attacks on Proximity Identification Systems, Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06), Short Paper, 2006

[harlacher07] Harlacher, F.: Untersuchung der Sicherheit von RFID-Technologien und –Systemen, Studienarbeit, TU Darmstadt, FG Mikroelektronische Systeme, 2007 .

[harrison06] M. Harrison, T. Inaba: Improving the safety and security of the pharmaceutical supply chain, Auto-ID Labs, White Paper, 2006

[henrici 04] D. Henrici, P. Müller: Hash-Based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers, Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications, S. 149-153, März 2004, online verfügbar unter:

http://dspace.icsy.de:12000/dspace/bitstream/123456789/124/1/DPArchiv.0080.pdf, Zugriff am 15.12.2006

[hdma03] Healthcare Distribution Management Association (HDMA): Protecting safety and improving efficiencies in the health care supply chain – using Electronic Product Codes, White Paper, November 2003

[hdma04] Healthcare Distribution Management Association (HDMA): EPC and Healthcare Distribution: Current State of the Industry, White Paper, November 2004

[höfling05] Jürgen Höfling: Ungelöste Sicherheitsfragen bei Transponder-Etiketten, informationweek.de, Short Paper, 2005

[holznagel06] B. Holznagel, M. Bonnekoh: RFID – Rechtliche Dimensionen der Radiofrequenz-Identifikation, Informationsforum RFID, Berlin, 2006

[ibm06] IBM, Printronix, Marlen RFID: Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag, White Paper, May 2006, Online verfügbar unter: www.marnlen.com

[inaba06] T. Inaba: EPC System for safe & secure supply chain and How it is applied, Auto-ID Labs Keio University, White Paper, 2006

[iso14443-1] ISO/IEC 14443-1: 2000 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics

[iso14443-2] ISO/IEC 14443-2: 2001 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface

[iso14443-3] ISO/IEC 14443-3: 2001 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision

[iso14443-4] ISO/IEC 14443-4: 2001 – Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol

[iso15693-1] ISO/IEC 15693-1:2000 – Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 1: Physical characteristics

[iso15693-2] ISO/IEC 15693-2:2006 – Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 2: Air interface and initialization

[iso15693-3] ISO/IEC 15693-3:2001– Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 3: Anticollision and transmission protocol

[iso15961]	ISO/IEC 15961:2004 – Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface
[iso15962]	ISO/IEC 15962:2004 – Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions
[iso15963]	ISO/IEC 15963:2004 – Information technology – Radio frequency identification for item management – Unique identification for RF tags
[iso18000-1]	ISO/IEC 18000-1:2004 – Information technology – Radio frequency identification for item management – Part 1: Reference architecture and definition of parameters to be standardized
[iso18000-3]	ISO/IEC 18000-3:2004 – Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz
[iso18000-6]	ISO/IEC 18000-6: 2004 – Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz
[iso7816-3]	ISO/IEC 7816-3: 2006 – Identification cards – Integrated circuit cards with contacts – Part 3: Electrical interface and transmission protocols
[iso7816-4]	ISO/IEC 7816-4:2005 – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange
[iso7816-8]	ISO/IEC 7816-8: 2004 – Identification cards – Integrated circuit cards – Part 8: Commands for security operations
[jantscher06]	M. Jantscher, P. H. Cole: Security and authentication primer, Auto-ID Labs University of Adelaide, White Paper, 2006
[juels03]	R. Juels, R. L. Rivest, M. Szydlo: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, ACM 2003, online verfügbar unter http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/ blocker/blocker.pdf, Zugriff am 18.12.2006
[juels04]	A. Juels: Minimalist cryptography for low-cost RFID tags. The Fourth International Conference on Security in Communication Networks (SCN 2004). Springer-Verlag, LNCS 3352, 2004
[juels05]	A. Juels: RFID Security and Privacy: A research Survey, RSA Laboratories, IEEE Journal on Selected Areas in Communications; Volume 24; Issue 2; S. 381-394; Feb. 2006, online verfügbar unter http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf, Zugriff am 30.10.2006
[juels05-2]	A. Juels: RFID Privacy: A Technical Primer for the Non-Technical Reader, RSA Laboratories, 2005
[juels06]	A. Juels, S. A. Weis: Defining Strong Privacy for RFID, RSA Laboratories & MIT, April 2006
[kaiser05]	U. Kaiser, C. Paar, J. Pelzl, et al.: Auswahlkriterien für kryptographische Algorithmen bei Low-Cost-RFID-Systemen, DACH Security 2005
[kasper06]	T. Kasper, D. Carluccio, C. Paar: Entwicklung und Realisierung eines Werkzeugs zur Sicherheitsanalyse von ISO 14443 RFID Systemen, 2006
[khan05]	F. Khan. Can Zero-Knowledge Tags Protect Privacy? RFID Journal, September 2005.
[kielbassa06]	M. Kielbassa: RFID im Supply Chain Management und in der Produktion, Studienarbeit, TU Darmstadt, FG Mikroelektronische Systeme, 2006.
[kirschenbaum06]	I. Kirschenbaum, A. Wool: How to Build a Low-Cost, Extended-Range RFID Skimmer, 2006
[knospe04]	H. Knospe, H. Pohl: RFID Security. Information Security Technical Report. Vol. 9, No. 4 (30-41), 2004

[koh03] R. Koh, E. W. Schuster, I. Chackrabarti, A. Bellmann: Securing the Pharmaceutical Supply Chain, Auto-ID Center MIT, White Paper, September 2003

[koh05] R. Koh, T. Staake: Nutzen von RFID zur Sicherung der Supply Chain der Pharmaindustrie, in [fleisch05]

[korzilius06] H. Korzilius: Arzneimittelfälschungen: Globale Lösung für ein globales System, Deutsches Ärzteblatt 103, Ausgabe 48 vom 01.12.2006

[kvir05] Z. Kvir, A. Wool: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, 2005, online verfügbar unter http://eprint.iacr.org/2005/052.pdf, Zugriff am 30.10.2006

[lampe05] M. Lampe, C. Flörkemeyer, S. Haller: Einführung in die RFID-Technologie, In: [fleisch05]

[langheinrich06] M. Langheinrich: RFID and Privacy, In: M. Petkovic; W. Jonker (Eds.): Security, Privacy, and Trust in Modern Data Management; Springer Verlag, 2006, online verfügbar unter: http://www.vs.inf.ethz.ch/res/papers/langhein2006rfidprivacy.pdf, Zugriff am 23.01.2007

[lefebvre06] L. A. Levebvre, E. Levebvre, Y. Bendavid, S. F. Wamba, H. Boeck: RFID as an Enabler of B-to-B e-Commerce and its Impact on Business Processes: A Pilot Study of a Supply Chain in the Retail Industry, Proc. of the 39th Annual Hawaii International Conferences on System Sciences (HICSS) 2006, S. 104a, Hawaii, Jan. 2006.

[lehtonen06] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch: The potential of RFID and NFC in anti-counterfeiting, Auto-ID Labs ETH Zürich und Uni St. Gallen, White Paper, 2006

[lehtonen06a] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch: From identification to authentication, Auto-ID Labs ETH Zürich und Uni St. Gallen, White Paper, 2006

[li06] S. Li, J. K. Visich, B. M. Khumawals, C. Zhang: Radio Frequency Identification Technology: Applications, technical challenges and strategies, Sensor Review 26/03 193-202, 2006

[logdynamic06] Webseite des LogDynamics Lab: http://logdynamics.biba.uni-bremen.de/lab.html

[magellan06] Magellan technology: A comparison of RFID frequencies and protocols, White Paper, March 2006

[michael05] K. Michael, L. McCathie: The Pros and Cons of RFID in Supply Chain Management, Proc. of the International Conference on Mobile Business 2005; S. 623-629; July, 2005.

[molnar05] D. Molnar, A, Soppera, D. Wagner: Privacy for RFID through Trusted Computing, ACM, Short Paper, 2005

[naumburg06] Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Verbindliche Regelungen für den Einsatz von RFID-Technologien, Naumburg, Oktober 2006

[nochta06] Z. Nochta, T. Staake, E. Fleisch: Product specific security features based on RFID technology, Auto-ID Lab ETH Zürich, Uni St.Gallen, White Paper, 2006

[odin06] ODIN technologies laboratories: Pharmaceutical item level RFID: Battle of the frequencies, White Paper, March 2006

[ohkubo05] M. Ohkubo, K. Suzuki, A. Kinoshita: RFID Privacy Issues and Technical Challenges, Communications of the ACM 48/09, September 2005

[orka07] Webseite ORKA: ORKA – Organisatorische Kontrolle: Der Weg von einem statischen Berechtigungsmanagement hin zu dynamischer organisationsbasierter Kontrolle, 2007, http://www.orka-projekt.de/index.htm

[pappu02] R. Pappu, B. Recht, J. Taylor, N. Gershen-Feld: Physical one-way functions, Science, Vol. 297, pp. 2026-2030, 2002

[pearson05] J. Pearson: Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies, TI White Paper, 2005

[pearson06] J. Pearson: RFID Tag Data Security Infrastructure: A Common Ground Approach for Pharmaceutical Supply Chain Safety, TI White Paper, 2006

[peres-lopez06] P. Peres-Lopez, J. C. Hernandez-Castro, et al.: LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags, RFIDSec 2006 Graz

[phagro06] PHAGRO-Webseite: www.phagro.de und www.phagro.de/Rundgang/1.aspx

[philips02] Philips Semiconductors: ICODE SLI SL2 ICS20 Short Form Specification. Revision 1.1. April 2002. http://www.nxp.com/acrobat_download/other/identification/SFS052611.pdf

[philips04] Philips, TAGSYS, Texas Instruments: Item-level visibility in the pharmaceutical supply chain: A comparison of the HF and UHF RFID technologies, White Paper, July 2004

[platzen06] Oliver Platzen: Die Eignung eines Auto-ID-Systems zur Reduzierung von Arzneimittelfälschung im Auftragsabwicklungsprozess zwischen Hersteller und Handel in Deutschland, Diplomarbeit Uni Regensburg, 3.2.2006

[popova05] Popova, T.: Internet der Dinge – Management- Information, GS1 Germany, Köln, 2005. Online verfügbar unter: www.gs1-germany.de

[poschmann06] A. Poschmann, G. Leander, K. Schramm, C. Paar: A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications, RFIDSec 2006, Graz

[rabaey96] J. Rabaey, M. Pedram: Low-Power Design Methodologies, Kulwer Academic Publishers, 1996

[ranasinghe06] D. C. Ranasinghe, P. H. Cole: Security in low cost RFID, Auto-ID Labs University of Adelaide, White Paper, 2006

[ranasinghe06a] D. C. Ranasinghe, P. H. Cole: A low cost solution to authentication in passive RFID systems, Auto-ID Labs University of Adelaide, White Paper, 2006

[rand06] RAND Europe: Security Challenges to the Use and Deployment of Disruptive Technologies, TR-406-EC, Final Report (D4), September 2006

[ravikanth01] P. S. Ravikanth: Physical One-Way Functions, Massachusetts Institute of Technology, March 2001

[rieback06] M. Rieback, B. Crispo, A. S. Tanenbaum: Is your cat infected with a Comuter Virus?, 2006

[rieback06a] M. Rieback, B. Crispo, A. S. Tanenbaum: The Evolution of RFID Security, IEEE 2006

[sander06] M. Sander, K. Stieler: RFID Geschäftsprozesse mit Funktechnologie unterstützen, hessen-media Band 54, 2006

[sandhu96] R.S. Sandhu, E.J. Coyle, H.L. Feinstein, C.E. Youman. Role-based access control models, IEEE Computer 29(2), 38-47, 1996.

[sarma03] S. E. Sarma, S. A. Weis, D. W. Engels: Radio Frequency Identification: Security Risks and Challenges, RSA Laboratories Cryptobytes; Vol. 6, No. 1, Spring 2003.

[schollenberger06] W. Schollenberger, N. Goetz, G. Schmidt: The role of EPC/RFID middleware – What's in the gap between physics and business applications?, Busiuness Action Group of EPCglobal, V0.4.1, April 2006

[sigG01] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Bundesgesetzblatt Nr. 22, 2001, S. 876

[sigV01] Verordnung zur elektronischen Signatur – SigV, 2001, Bundesgesetzblatt Nr. 509, 2001, S. 3074

[spiekermann04] S. Spiekermann, O. Berthold: Maintaining Privacy in RFID Enabled Environments, 2004

[staake05]	T. Staake, F. Thiesse, E. Fleisch: Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting, ACM Symposium on Applied Computing, 2005
[strassner05]	M. Strassner: RFID im Supply Chain Management, Deutscher Universitäts-Verlag, 2005
[strassner05a]	M. Strassner: Potentiale der RFID-Technologie für das Supply Chain Management in der Automobilindustrie, In: [fleisch05]
[taucis06]	TAUCIS, Technologieabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung, Studie im Auftrag des BMBF, www.taucis.de, 2006
[thornton06]	F. Thornton, B. Haines et al.: RFID Security, Syngress Publishing, 2006
[tsudik06]	G. Tsudik: YA-TRAP: Yet another trivial RFID authentication protocol, IEEE conference paper, March 2006
[tuyls06]	P. Tuyls, L. Batina: RFID-Tags for Anti-counterfeiting, CT-RSA 2006, LNCS 3860, pp. 115-131, Springer-Verlag, 2006
[uckelmann06]	D. Uckelmann. Persönliche Kommunikation, LogDynamics Lab, 2006
[ulrich05]	R. Ulrich, G. Wetzel: Case Study: RFID in der Lieferkette der Automobilindustrie. 8. VDEB-Infotag und Anwendertag RFID, Bremen 2005.
[vda4902]	Verband der Automobilindustrie: VDA-4902 Warenanhänger, 2006
[vda5501]	Verband der Automobilindustrie: VDA-5501 RFID im Behältermanagement der Supply-Chain, November 2006
[yu06]	Y. Yu, Y. Yang, Y. Fan, H. Min: Security scheme for RFID tag, Auto-ID Labs Fudan University, White Paper, 2006
[vdc06]	VDC: Pharma Item-Level RFID to Set Precedent, RFID Update, www.rfidupdate.com/articles/index.php?id=1222, October 2006
[weis03]	Weis, S.A.; Sarma, S. E.; Rivest, R. L.;Engels, D. W.: Security and Privacy Aspects of Low Cost Radio Frequency Identification Systems, online verfügbar unter http://theory.lcs.mit.edu/~sweis/pdfs/spc-rfid.pdf, Zugriff am 17.01.2007
[weis03b]	S. A. Weis: Security and Privacy in Radio-Frequency Identification, 2003, online verfügbar unter http://theory.lcs.mit.edu/%7Ecis/theses/weis-masters.pdf, Zugriff am 18.12.2006
[zongwei05]	L. Zonwei, T. Chan, J. S. Li: A lightweight mutual authentication protocol for RFID networks; Proc. of the IEEE International Conference on e-Business Engineering, S. 620-625, Okt. 2005