

Security und Privacy in RFID v.0.4

1. Inhaltsverzeichnis

<u>1. Inhaltsverzeichnis.....</u>	<u>2</u>
<u>Security und Privacy in RFID v.0.4.....</u>	<u>2</u>
<u>2. Einführung.....</u>	<u>4</u>
<u>2.1 Motivation.....</u>	<u>5</u>
<u>2.2 Überblick über die Firma.....</u>	<u>6</u>
<u>2.3 Ziel.....</u>	<u>7</u>
<u>3. Problemstellung.....</u>	<u>8</u>
<u>3.1 RFID Systeme.....</u>	<u>8</u>
<u>3.1.1 Übersicht über die RFID Technologie /Standards.....</u>	<u>11</u>
<u>3.1.2 Bestandteile eines RFID Systems.....</u>	<u>12</u>
<u>3.1.3 Unterschiede von RFID Systemen.....</u>	<u>13</u>
<u>3.1.3.1 Low Frequency.....</u>	<u>14</u>
<u>3.1.3.2 High Frequency.....</u>	<u>15</u>
<u>3.1.3.3 Ultra High Frequency.....</u>	<u>15</u>
<u>3.1.3.4 Mikrowelle.....</u>	<u>17</u>
<u>3.2 Sicherheit von RFID Systemen.....</u>	<u>19</u>
<u>3.2.1 Datenschutz und Privacy.....</u>	<u>20</u>
<u>3.2.2 Angriffe auf RFID Systeme.....</u>	<u>23</u>
<u>3.2.2.1 Angriffe auf den Transponder.....</u>	<u>24</u>
<u>4. Problemanalyse.....</u>	<u>26</u>
<u>4.1 Kryptographische Maßnahmen.....</u>	<u>26</u>
<u>4.2 Symmetrische Verschlüsselung.....</u>	<u>26</u>
<u>4.3 Asymmetrische Verschlüsselung.....</u>	<u>26</u>
<u>4.4 Authentifizierung.....</u>	<u>26</u>
<u>5. Implementierung.....</u>	<u>27</u>
<u>Projekt Management.....</u>	<u>27</u>
<u>Planner – Gantt Diagramm.....</u>	<u>27</u>
<u>Wasserfall Modell.....</u>	<u>28</u>
<u>User Stories.....</u>	<u>29</u>
<u>Lauf- und Entwicklungs- Umgebung.....</u>	<u>30</u>
<u>Subversion.....</u>	<u>30</u>
<u>Testgetriebene Entwicklung.....</u>	<u>31</u>
<u>JUnit.....</u>	<u>31</u>

Security und Privacy in RFID v.0.4

Javadoc.....	33
Java Entwurfsmuster.....	33
Singleton Entwurfsmuster.....	33
Strategie Entwurfsmuster.....	34
Entwicklung einer Web Anwendung für die Verwaltung von Zertificaten.....	35
6. Zusammenfassung.....	39
7. Übersicht.....	39
7.1 Bewertung von Stärken und Schwächen von dem Produkt.....	39
7.2 Einsatzgebiete.....	39
8. Ausblick.....	39
9. Quellenverzeichnis.....	39
10. Anhänge.....	39
11. Glossar.....	39

2. Einführung

In vielen Dienstleistungsbereichen, in der Beschaffungs- und Distributionslogik, im Handel, in Produktionsbetrieben und Materialflusssystemen haben automatische Identifikationsverfahren („Auto-ID“) in den letzten Jahren große Verbreitung gefunden. Aufgabe und Ziel der Auto-ID ist die Bereitstellung von Informationen zu Personen, Tieren, Gütern und Waren.

Die weit verbreiteten Barcode-Etiketten, die schon vor vielen Jahren eine Revolution bei Identifikationssystemen auslösten, sind heute in zunehmenden Fällen nicht mehr ausreichend. Zwar sind Barcodes äußerst billig, ihr Engpass ist jedoch die geringe Speicherfähigkeit sowie die Unmöglichkeit der Umprogrammierung.

Kreative Anwendungen der Radio Frequency Identification („RFID“) Technologien versprechen viele Vorteile für Konsumenten, die Wirtschaft und die Regierung. Sie beinhalten unter anderem Möglichkeiten zur Kostenreduktion durch besseres Inventarmanagement, zur Verbesserung der Sicherheit bei der Medikamenteneinnahme, zur Hilfe bei der Pflege von Alten und Behinderten, zur Verringerung von Irrtümern in Krankenhäusern sowie für verbesserte Rückverfolgung von Gepäckstücken und Frachtgütern an Flughäfen, die die Sicherheit und den Fluggastservice verbessert.

Darüber hinaus hat sich kontaktlose Identifikation in den letzten Jahren immer mehr zu einem eigenständigen interdisziplinären Fachgebiet entwickelt, das in keine der klassischen Schubladen mehr passt. Es fließen hier Elemente aus den verschiedensten Branchen zusammen: HF-Technik und EMV, Halbleitertechnik, Datenschutz und Kryptographie, Telekommunikation, Fertigungstechnik und viele verwandte Fachgebiete.

Es gibt viele mögliche Anwendungen von RFID, die keine größere Bedenken in Bezug auf die Privatsphäre auslösen. Aber insofern RFID-Geräte mit personenbezogenen Informationen (personally identifiable information, „PII“) verknüpft werden können, eingeschlossen die Fälle, in denen solche Geräte die Standortfeststellung einer bestimmten Person ermöglichen, gibt RFID zu vielen Sorgen bezüglich der Privatsphäre Anlass.

Security und Privacy in RFID v.0.4

2.1 Motivation

RFID ist eine der Schlüsseltechnologien der Zukunft, konkrete Anwendungen in der Wirtschaft entstehen in rasantem Tempo.

In stark wachsendem Umfang werden Waren, aber auch Tiere mit Hilfe von RFID-Transpondern (radio frequency identification) gekennzeichnet. Auch für die Identifikation von Personen, für die Zugangskontrolle, Parkchips oder das bargeldlose Bezahlen, beispielsweise in Erlebnisbädern, oder in der Logistik zur Steuerung von Materialströmen wie automatische Lagerhallen finden die RFID-Transponder Einsatz.

RFID-Tags können heute in den unterschiedlichsten Formen preiswert hergestellt werden: wenig größer als ein Reiskorn zur sicheren Kennzeichnung von Haus- und Nutztieren oder flach als selbstklebende Etiketten für Waren in Großmärkten, oder als Chipkarte, Armband oder Schlüsselanhänger für die Zugangskontrolle.

Die RFID Technologie hat das Potential, Optimierungen und Rationalisierungen im Warenfluss zu erschließen, die in den nächsten Jahren Wettbewerbsrelevant sein werden.

Was aber erwartet und fordert der Handel und die Industrie von dieser Technologie und welche Lösungen bietet der Markt?

Die Ergebnisse der Studie zeigen, dass auf der Ebene Sammel- und Ladeeinheiten der Transponder in den nächsten Jahren erhebliche Marktanteile auf Kosten des Barcode gewinnen wird. Interessant ist hierbei die unterschiedliche Erwartungshaltung bei Industrie und Handel und auch zwischen Konsum- und Investitionsgüterindustrie. Die Chancen: verbesserte Leistung und höhere Qualität der Logistikprozesse und die Hemmnisse: fehlende Standardisierung und Kosten zeigen für die Technikanbieter und Systemintegratoren die Schwerpunkte der zukünftigen Aufgabenfelder auf.

Im Augenblick ist die RFID-Technologie noch zu teuer, um im Handel großflächig eingesetzt zu werden. In der Zukunft könnten jedoch alle im Handel erhältlichen Produkte einen RFID-Chip tragen. Dies würde einige ganz neue Möglichkeiten eröffnen: Kühlschränke könnten etwa automatisch registrieren, welche in ihnen gelagerten Lebensmitteln als nächstes auslaufen oder nachgekauft werden müssen. Ähnliches ist für Regale in Supermärkten vorstellbar. Auch außerhalb des Handels existieren zahlreiche Einsatzmöglichkeiten, z.B. in Büchereien, wo die Ausleihe und Rückgabe mittels RFID automatisiert erfolgen kann, oder in Mautsystemen.

Das Wettbewerb und rechtliche Bestimmung wie das Bundesdatenschutzgesetz begründen das Sicherheitsbedürfnis von vielen Unternehmen. So soll z.B. Verhindert werden, dass Konkurrenten in den Besitz von Betriebsgeheimnissen kommen oder Unbefugte personenbezogene Daten einsehen können.

Security und Privacy in RFID v.0.4

2.2 Überblick über die Firma

Siemens Business Services ist ein führender IT-Service-Anbieter. Als strategischer Partner bei der Lösung unternehmerischer Probleme bietet SBS ihren Kunden in Deutschland Leistungen entlang der gesamten IT-Dienstleistungskette aus einer Hand - vom Consulting über die Systemintegration bis zum Management von IT Infrastrukturen.

Mit umfassendem Know-how und spezifischem Branchenwissen schaffen motivierten und bestausgebildeten Mitarbeiterinnen und Mitarbeiter messbaren Mehrwert für die Kunden. Im Geschäftsjahr von 2004 betrug der Umsatz in Deutschland 2,3 Mrd. Euro. Derzeit werden ca. 15.100 Mitarbeiterinnen und Mitarbeiter in Deutschland beschäftigt.

Die Qualität von Dienstleistungen stellt in enger Zusammenarbeit mit internen und externen Partnern eine Beschleunigung der Geschäftsprozesse sicher und sorgt für eine hohe Wertschöpfung in den Unternehmen ihrer Kunden.

Darstellung des Unternehmens

Wir beraten Sie umfassend entsprechend Ihren Anforderungen und integrieren Ihre Lösung in Ihre bestehende IT-Landschaft. Wenn es um die Beratung, den Entwurf und die Realisierung von Software-, System- oder Kommunikationslösungen geht, wenden Sie sich an uns.

Darstellung im Überblick:

1. • Workshops für die Aufnahme der Kundenanforderungen
2. • Strategiebetrachtungen (Einsatzfeldbetrachtung mit Realisierungsphasen, Migrationskonzepte)
3. • IT-Konzepte, Architekturkonzepte, technische Fachkonzepte einschließlich Software- und Hardwareauswahl
4. • Konzeption, Spezifikation und detaillierte Festlegung des gesamten Funktionsumfangs, der Komponenten sowie sämtlicher Schnittstellen des Gesamtsystems
5. • Softwareentwicklung unternehmenskritischer Anwendungen auf Basis neuester Technologien, Einbindung vorhandener Komponenten/Funktionen und Systeme, Schnittstellenbetrachtungen
6. • Test sowie Integration in die vorhandene Unternehmens-DV (Einbettung in die vorhandenen Verfahren und Systemumgebungen des Anwenders und – bei Bedarf – seiner Partner)
7. • Installations- und Administrationskonzepte
8. • Schulungen
9. • Betreuungskonzepte

Security und Privacy in RFID v.0.4

2.3 Ziel

Im Moment sind alle RFID Lösungen die etwas mehr an Sicherheit bieten noch etwas zu Teuer. Oft ist es auch so das es einen Kunden nur eines Bestimmtes Niveau in Frage Sicherheit schon zufrieden stellen würde.

Das Ziel dieser Arbeit ist auszuarbeiten eine möglichst günstige Lösung für eine zusätzliche Feature für Erhöhung von Sicherheit eines RFID Systems.

Dabei soll die Lösung flexible einsetzbar sein. Sollte leicht in ein RFID System integrierbar sein und keine extra Hardware brauchen.

[noch zu schreiben...]

3. Problemstellung

3.1 RFID Systeme

Radio Frequency Identifikation ist eine Methode, um Daten auf einem Transponder Berührungslos und ohne Sichtkontakt lesen und speichern zu können. Dieser Transponder kann an Objekten angebracht werden, welche dann anhand der darauf gespeicherten Daten automatisch und schnell identifiziert werden können.

Ein RFID-System umfasst

- den Transponder (auch RFID-Etikett, -Chip, -Tag, -Label oder Funketikett genannt),
- die Sende-Empfangs-Einheit (auch Reader genannt) und,
- die Integration mit Servern, Diensten und sonstigen Systemen wie z.B. Kassensystemen oder Warenwirtschaftssystemen.

Die Datenübertragung zwischen Transponder und Lese-Empfangs-Einheit findet dabei mittels elektromagnetischer Wellen statt. Bei niedrigen Frequenzen geschieht dies induktiv über ein Nahfeld, bei höheren über ein elektromagnetisches Fernfeld. Die Entfernung, über die ein RFID-Transponder ausgelesen werden kann, schwankt je nach Ausführung (passiv/aktiv), benutztem Frequenzband, Sendeleistung und Umwelteinflüssen zwischen wenigen Zentimetern und mehr als einem Kilometer.

Transponder bestehen aus Mikrochip, Antenne, Träger oder Gehäuse und einer Energiequelle (bei aktiven Transpondern).

Die RFID-Transponder unterscheiden sich teilweise stark voneinander. Sie können über einen mehrfach beschreibbaren Speicher verfügen, in dem während der Lebensdauer Informationen abgelegt werden können. Nach Anwendungsgebiet unterscheiden sich auch die sonstigen Kennzahlen wie z.B. Funkfrequenz, Übertragungsrate, Lebensdauer, Kosten pro Einheit, Speicherplatz, Lesereichweite und Funktionsumfang. Prinzipiell funktioniert die RFID-Kommunikation so: Der Reader erzeugt ein elektromagnetisches (U)HF-Feld, welches die Antenne des RFID-Transponders empfängt. In der Antennenspule entsteht, sobald sie in die Nähe des elektromagnetischen Feldes kommt, Induktionsstrom. Dieser aktiviert den Mikrochip im RFID-Tag. Durch den induzierten Strom wird bei passiven Tags zudem ein Kondensator aufgeladen, welcher für dauerhafte Stromversorgung des Chips sorgt. Dies übernimmt bei aktiven Tags eine eingebaute Batterie.

Ist der Mikrochip einmal aktiviert, so empfängt er vom Lesegerät Befehle. Indem der Tag eine Antwort in das vom Reader ausgesendete Feld moduliert, sendet er seine Seriennummer oder andere vom Reader abgefragte Daten.

Dabei sendet der Tag selbst kein Feld aus, sondern verändert nur das elektromagnetische Feld des Readers durch so genannte Lastmodulation, indem er die Energie des Feldes „verbraucht“, was wiederum der Reader detektiert. Prinzipienbedingt kann ein 13,56 MHz Tag daher nur im elektromagnetischen Nahfeld gelesen werden, welches eine Reichweite der halben Wellenlänge $\lambda/2$ hat, bei 13,56 MHz also maximal 11,1 Meter.

Security und Privacy in RFID v.0.4

Im UHF Bereich bei 865 – 920 MHz reflektiert die Transponderantenne nach gleichem Prinzip das elektromagnetische Feld oder absorbiert dieses, sodass das Verhältnis der Reflektionsänderung vom Reader wahrgenommen werden kann. Dies nennt man Backscattering. Da Wasser diese Strahlung sehr stark absorbiert und Metall diese Strahlung sehr stark reflektiert, ist klar, dass diese Materialien diesen Vorgang sehr stark beeinflussen, ein Tag auf diesen Materialien also kaum lesbar ist.

Zum Betrieb, insbesondere zur Signalmodulierung, muss der RFID-Mikrochip mit Energie versorgt werden. Hierbei werden zwei Arten von RFID-Transpondern unterschieden:

1. Passive RFID-Transponder beziehen ihre Energie zur Versorgung des Microchips aus den empfangenen Funkwellen, oft als "Continuous Wave" bezeichnet. Mit der Antenne als Spule wird durch Induktion ein Kondensator aufgeladen, welcher den Tag mit Energie versorgt. Die Continuous Wave muss aufgrund der geringen Kapazität des Kondensators durchgehend vom Lesegerät gesendet werden, während der Tag sich im Lesebereich befindet.
2. Aktive RFID-Transponder sind batteriebetrieben, d.h. sie beziehen die Energie zur Versorgung des Mikrochips aus einer eingebauten Batterie. Normalerweise befinden sie sich im Ruhezustand bzw. senden keine Informationen aus, um die Lebensdauer der Energiequelle zu erhöhen. Nur wenn ein spezielles Aktivierungssignal empfangen wird, aktiviert sich der Sender. Nicht genutzt werden kann die Energie der Batterie für das Erzeugen des modulierten Rücksignals, dennoch erreicht man durch höheren Rückstrahlkoeffizienten beim Backscatteringverfahren aufgrund des geringeren Energieverbrauches an Feldenergie eine deutlich höhere Reichweite.

Polymere Transponder (PolyIC)



Auf dem Weg zur Massenproduktion von RFID-Chips aus Kunststoff ist das Unternehmen PolyIC einen großen Schritt vorangekommen: Die Entwickler schufen mit 600 Kilohertz die weltweit schnellste integrierte Schaltung aus organischem Material. Zudem gelang ihnen mit Techniken des Druckens die Herstellung von besonders stabilen Schaltungen aus Polymeren, was nach Angaben des Unternehmens weltweit noch keine andere Forschergruppe schafft. Der Abstand zweier Leiterbahnen ist mit unter 50 Mikrometern etwa so dünn wie ein menschliches Haar. Diese Chips funktionieren noch nach zwei Tagen Lagerung bei 60 Grad Celsius und 100 Prozent Luftfeuchte und geben erst oberhalb 120 Grad auf.

PolyIC setzt auf eine revolutionäre Produktionstechnik. Die Schaltungen sollen auf Folie aufgedruckt werden – wie eine Zeitung auf Papier. Langfristig sollen so Produktionskosten von weniger als einem Cent pro Chip möglich sein. Damit will das Unternehmen sein ehrgeiziges Ziel erreichen, den Barcode, der meist nur eine Typbezeichnung enthält, durch elektronische Chips aus Kunststoff abzulösen. Mit diesen „intelligenten Etiketten“ sollen künftig Produkte einzeln unterscheidbar werden. Diese aufgeklebten Funkchips eröffnen für Lieferung, Lagerhaltung und Kennzeichnung von Waren neue Möglichkeiten, weil sie aus der Ferne auslesbar sind. Denkbar ist zudem eine automatische Kasse: Kunden müssten ihren Einkaufswagen nur an einem Funkscanner vorbeifahren, und alle Waren würden automatisch erfasst.

Security und Privacy in RFID v.0.4

Die Anwendungsmöglichkeiten für die Chips aus Kunststoff sind enorm breit: Erste Produkte, die 2006 erhältlich sein sollen, können als fälschungssichere Etiketten eingesetzt werden, wie das Forschungsmagazin Pictures of the Future kürzlich berichtete. Stufenweise will PolyIC komplexere Schaltungen mit einigen tausend Transistoren und bis zu 128 Bit Speicherkapazität produzieren, die als Barcode-Ersatz dienen können. Ein Barcode kann heute üblicherweise 44 Bit speichern.

Security und Privacy in RFID v.0.4

3.1.1 Standards und Normen

Die Erarbeitung von Normen obliegt den technischen Komitees verschiedener Normungsinstitute. Die ISO (International Organisation for Standardisation) ist eine weltweite Vereinigung nationaler Normungsinstitute, wie DIN (Deutschland) oder ANSI (USA) und mit zahlreichen Committees und Arbeitsgruppen an der Entwicklung von RFID-Normen beteiligt.

Die Darstellung der Normen in diesem Kapitel dient lediglich dem technischen Verständnis der beschriebenen RFID-Anwendungen, ist aber keine vollständige Wiedergabe der zitierten Normen. Außerdem werden Normen von Zeit zu Zeit dem technischen Stand angepasst und unterliegen somit Änderungen.

ISO/IEC 14443 – Proximity-coupling-Chipkarten. Die ISO/IEC-Norm 14443 beschreibt unter dem Titel „Identification cards – Proximity integrated circuit(s) cards“ Funktionsweise und Betriebsparameter kontaktloser Proximity-coupling-Chipkarten. Darunter versteht man kontaktlose Chipkarten mit einer ungefähren Reichweite von 7 ... 15 cm, wie sie überwiegend im Bereich „Ticketing“ eingesetzt werden. Als Datenträger beinhalten diese Chipkarten üblicherweise einen Mikroprozessor und verfügen darüber hinaus häufig über zusätzliche Kontakte.

ISO/IEC 15693 – Vicinity-coupling-Chipkarten. Die ISO/IEC-Norm 15693 beschreibt unter dem Titel „Identification cards – contactless integrated circuit(s) cards – Vicinity Cards“ Funktionsweise und Betriebsparameter kontaktloser Vicinity-coupling-Chipkarten. Darunter versteht man kontaktlose Chipkarten mit einer Reichweite bis zu 1 m, wie sie etwa für die Zutrittskontrolle eingesetzt werden. Als Datenträger werden bei diesen Chipkarten überwiegend kostengünstige Speicherbausteine mit einfacher State-Machine eingesetzt.

Security und Privacy in RFID v.0.4

3.1.2 Bestandteile eines RFID Systems

Ein RFID-System besteht immer aus zwei Komponenten:

- dem Transponder, der an den zu identifizierenden Objekten angebracht wird;
- dem Erfassungs- oder Lesegerät, das je nach Ausführung und eingesetzter Technologie als Lese- oder Schreib/Lese-Einheit erhältlich ist.

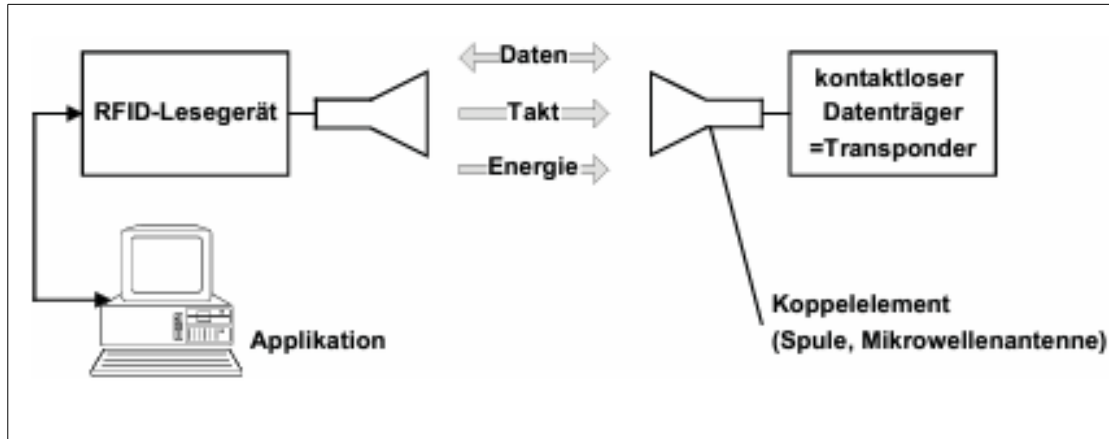


Abb. 1.1 Lesegerät und Transponder sind die Grundbestandteile jedes RFID-Systems.

Ein Lesegerät beinhaltet typischerweise ein Hochfrequenzmodul (Sender und Empfänger), eine Kontrolleinheit sowie ein Koppellement zum Transponder. Daneben sind viele Lesegeräte mit einer zusätzlichen Schnittstelle (RS 232, RS 485, ...) ausgestattet, um die erhaltenen Daten an ein anderes System (PC, Automatensteuerung, ...) weiterzuleiten.

Der Transponder, der den eigentlichen Datenträger eines RFID Systems darstellt, besteht üblicherweise aus einem Koppellement sowie einem elektronischen Mikrochip. Außerhalb des Ansprechbereichs eines Lesegerätes verhält sich der Transponder, der in der Regel keine eigene Spannungsversorgung (Batterie) besitzt, vollkommen passiv. Erst innerhalb des Ansprechbereichs eines Lesegerätes wird der Transponder aktiviert. Die zum Betrieb des Transponders benötigte Energie wird ebenso wie Takt und Daten durch die Koppelheit (kontaktlos) zum Transponder übertragen.

Security und Privacy in RFID v.0.4

3.1.3 Unterschiedsmerkmale von RFID Systemen

RFID Systeme existieren in unzähligen Varianten, von fast ebenso vielen verschiedenen Herstellern. Um den Überblick über RFID Systeme zu behalten, ist es notwendig, Unterscheidungsmerkmale zu finden, nach denen verschiedenste RFID Systeme voneinander unterschieden werden können.

Die Datenmenge von RFID Transpondern reicht üblicherweise von wenigen Bytes bis zu mehreren KBytes. Eine Ausnahme stellen die so genannten 1-bit-Transponder dar: Einer Datenmenge von genau 1 Bit reicht gerade dazu aus, um dem Lesegerät zwei Zustände zu signalisieren: „Transponder im Feld“ oder „keiner Transponder im Feld“. Dies ist jedoch vollkommen ausreichend, um einfache Überwachungs- oder Signalisierungsaufgaben zu erfüllen. Da zur Realisierung eines 1-bit-Transponders kein elektronischer Chip benötigt wird, können diese Transponder in großen Stückzahlen für Bruchteile eines Pfennigs hergestellt werden. Aus diesem Grunde werden 1-bit-Transponder zur Diebstahlsicherung (EAS) von Waren in Kaufhäusern und Geschäften eingesetzt. Beim verlassen des Kaufhauses mit unbezahlter Ware wird das am Ausgang installierte Lesegerät dann den Zustand „Transponder im Feld“ erkennen und entsprechende Reaktionen auslösen. Bei einer ordnungsgemäß bezahlten Ware würde der 1-bit-Transponder an der Kasse entfernt oder deaktiviert werden.

Eine weitere Unterscheidungsmöglichkeit von RFID Systemen ist die Beschreibbarkeit des Transponders mit Daten. Bei sehr einfachen Systemen wird der Datensatz des Transponders, meist eine einfache (Serien-) Nummer, schon zum Zeitpunkt der Chipherstellung aufgebracht und kann dann nicht mehr verändert werden. Im Gegensatz dazu können beschreibbare Transponder durch das Lesegerät mit Daten beschrieben werden. Zu Speicherung der Daten werden vor allem drei Verfahren eingesetzt: Bei induktiv gekoppelten RFID Systemen sind EEPROMs das dominierende Verfahren, jedoch einer Lebensdauer von maximal 100000 Schreibvorgängen. In jüngster Zeit werden vereinzelt auch so genannte FRAMs eingesetzt. Im Vergleich zu EEPROMs ist die Leistungsaufnahme zum Beschreiben von FRAMs etwas um den Faktor 100, die Schreibzeit sogar um den Faktor 1000 geringer, Probleme in der Herstellung der FRAMs haben deren breite Markteinführung bisher jedoch verhindert.

Eines der wichtigsten Merkmale von RFID Systemen ist die Betriebsfrequenz und die daraus resultierte Reichweite des Systems. Als Betriebsfrequenz eines RFID Systems wird dabei die Frequenz bezeichnet, auf der das Lesegerät sendet. Die Sendefrequenz des Transponders wird nicht berücksichtigt. In den meisten Fällen entspricht sie der Sendefrequenz des Lesegerätes (Lastmodulation, Backscatter). Die „Sendeleistung“ des Transponders kann jedoch in jedem Fall um mehrere Zehnerpotenzen niedriger angesetzt werden als die des Lesegeräts.

Security und Privacy in RFID v.0.4

RFID Technologies Overview				
Technology	Low Frequency 100 - 135 kHz	High Frequency 13,56 MHz	UHF EU: 868MHz US: 902-928 MHz	Microwave 2,45 GHz
Communication	Inductive Magnetic Field Coupling		Electromagnetic Field Coupling	
Availability	> 30 Years	> 10 years ISO 15693 since 2002	US: > 2 years EU: relatively new	
Subsurface (except metal)	No Impact	Low Impact	Depends on material	No Impact
Fluids	No Impact	Low Impact	High Impact	High Impact
Readability on Metal	Limited	Bad but special tags available	Good	Good
Bulk Reading	No Implementations	Up to 100 Tags/sec	Up to 50 Tags/sec	No Implementations
Reading Distance (Credit Card Size)	~ 0 - 100 cm	~ 0 - 100 cm	US: ~ 0 - 500+ cm EU: ~ 0 - 300+ cm	> 500 m
Data Transmission Rate	Low	Medium	Fast	Fast
Interference Resistance	High	High	Depends on environment	Susceptible to electronic noise
Typical Applications	Animal Identification Car Anti Theft Devices	Track&Trace, Ski-Ticketing Document Management	Track&Trace Container Management	Toll Collection, Real Time Location Systems

Grundsätzlich werden die verschiedenen Sendefrequenzen den drei Bereichen LF, HF und UHF bzw. Mikrowelle zugeordnet.

3.1.3.1 Low Frequency

Die Low Frequency Technik ist eine der ersten entwickelten RFID-Techniken gewesen. Die Transponder sind read-only, d.h. es wird nur die eindeutige Seriennummer ausgelesen. Auch die Reichweite ist im Vergleich zu anderen, heute verfügbaren RFID-Techniken, kürzer und der Datentransfer auf Grund der niedrigeren Frequenz deutlich langsamer. Die Vorteile der niederfrequenten Technik sind die geringeren Ansprüche an die Bauform der Transponder, die deutlich kleiner sein können als bei den MHz-Transpondern. Die 125/134 kHz-Technik wird heute vor allem für Zugangskontrollsysteme und in der Tieridentifikation genutzt. Die Transponder gibt es daher neben dem Scheckkartenformat oft auch als Schlüsselanhänger und als Glasröhrchen.

Dieser Frequenzbereich gehört nicht zu den ISM-Frequenzbereichen. Deshalb erfolgt hier eine starke Nutzung durch andere Funkdienste. Die Trägerfrequenzen von RFID-Systemen in diesem Bereich liegen, je nach Hersteller, zwischen 120 kHz und 135 kHz. Durch die Verwendung von Spulen mit Ferritkern, ist eine miniaturisierte Transponderbauform möglich. In diesem Bereich finden passive Transponder Einsatz.

Diese Systeme weisen eine geringe Reichweite auf, arbeiten in der am häufigsten verwendeten 64 bit Read Only Technologie einwandfrei und schnell genug für viele Anwendungen. Bei größeren Datenmengen ergeben sich längere Übertragungszeiten. LF-Transponder sind günstig in der Anschaffung, kommen mit hoher (Luft-) Feuchtigkeit und Metall zurecht und werden in vielfältigen Bauformen angeboten. Diese Eigenschaften begünstigen den Einsatz in rauen Industrieumgebungen, sie werden jedoch auch z.B. für Zugangskontrollen, Wegfahrsperrern und

Erstellt von Kulyk Nazar

Security und Privacy in RFID v.0.4

Lagerverwaltung (häufig 125 kHz) verwendet. LF-Versionen eignen sich auch für den Einsatzfall in explosionsgefährdeten Bereichen. Hier können ATEX zertifizierte Versionen eingesetzt werden.

Es haben sich weltweit bislang zwei Standards durchgesetzt, die durch ISO-Normen technologisch vereinheitlicht sind und somit eine länderübergreifende Verwendung der RFID-Tags ermöglichen: das niederfrequente 125 KHz-Band (LF-Bereich) und das hochfrequente 13,56 MHz-Band (HF-Bereich). Für LF-Bereiche wurde seit ihrer Einführung mit großem Erfolg eine Vielzahl spezifischer Einsatzgebiete erschlossen, wie z.B. Zutrittskontrollen oder PKW-Wegfahrsperrren.

Allerdings gibt es im LF -Bereich auch einige Einschränkungen - wie z.B. prinzipielle Kommunikationsreichweiten, Energieübertragung, die Notwendigkeit spezieller Bauformen oder hohe Metallempfindlichkeit - die den breiten Einsatz der RFID-Technologie in einigen industriellen und logistischen Anwendungen erschweren.

3.1.3.2 High Frequency

Der Vorteil dieses Frequenzbereichs ist, daß eine schnelle Datenübertragung (typ. 106 kBits/s) realisierbar ist. Aufgrund der hohen Taktfrequenz ist der Einsatz von Signalver-schlüsselungsverfahren möglich.

Kurze bis mittlere Reichweite, mittlere Übertragungsgeschwindigkeit, mittlere bis günstige Preisklasse. In diesen Frequenzbereich arbeiten die sog. Smart Label.

Der Leser kann Informationen berührungslos auslesen, ohne dass ein optischer Kontakt zum Transponder bestehen muss. Deshalb können Transponder vollständig in Produkte integriert werden. Ein so eingebauter Transponder ist unempfindlich sowohl gegen Nässe und Verschmutzung, als auch gegen mechanische Einflüsse und kann somit auch in widrigen Umgebungen zum Einsatz kommen.

Transponder und Reader im Frequenzbereich von 13,56 MHz haben gegenüber ihren Vorgängern (125 und 134 kHz) folgende Vorteile:

- Pulkerfassung
- Größere Reichweite
- Deutlich schnellere Datenübertragung
- Transponder können auch beschrieben werden

Für HF- Technologie gibt es ein großes Einsatzgebiet insbesondere im Bereich Warenlogistik, Produktionssteuerung oder dem elektronischen Pass.

Allerdings gibt es im HF-Bereich, sowie es auch bei LF-Technologie war auch einige Einschränkungen - prinzipielle Kommunikationsreichweiten, Energieübertragung, die Notwendigkeit spezieller Bauformen oder hohe Metallempfindlichkeit - die den breiten Einsatz der RFID-Technologie in einigen industriellen und logistischen Anwendungen erschweren.

3.1.3.3 Ultra High Frequency

Prinzipiell unterscheidet sich die RFID-UHF-Technologie in den benötigten Komponenten nicht von der 13,56 MHz-Technik. Ein elektronischer Transponder,

Security und Privacy in RFID v.0.4

bestehend aus mindestens einem Speicherchip und einer angeschlossenen Miniantenne, empfängt über eine Luftschnittstelle Impulse von einer Lese-/Schreibereinheit (Reader) und gibt umgekehrt seine gespeicherten Informationen an den Reader zurück. Sofern es sich dabei um passive Transponder ohne eigene Energieversorgung und ohne weitere Bauteile handelt, werden mit den Impulsen der Lese-/Schreibereinheit sowohl die Daten als auch die Energie für den Chip übertragen. Anders als bei den LF- und HF-Anwendungen erfolgt im 868-MHz-Bereich die Koppelung zwischen Transponder und der Lese-/Schreibereinheit nicht induktiv durch ein Magnetfeld, sondern über elektromagnetische Wellen, d.h. als Strahlung. Die Kommunikation zwischen Transponder und Lesegerät erfolgt durch die Modulation der Reflexion des ausgestrahlten Feldes ("Backscatter-Technik").

Die elektromagnetische Koppelung erfordert keine spulenförmigen Antenne, sondern eine einfachen Dipol- oder Flachantennen. Die Lesereichweiten für passive UHF-Transponder betragen bei guten Bedingungen und einer effektiven Sendeleistung von 0,5 Watt ERP (effectiv radiated power) maximal 4 Meter. Seit Anfang 2005 gilt eine erhöhte Obergrenze der Reader-Sendeleistung von 2 Watt ERP im Frequenzbereich zwischen 865,6 und 867,6 MHz. Dies ermöglicht es, künftig noch höhere Reichweiten von theoretisch bis zu 8 Meter zu realisieren.

Wie HF-Systeme, sind auch UHF-Systeme pulklesefähig, d.h. sie sind der Lage bis zu 600 RFID-Tags gleichzeitig zu erkennen und individuell zu unterscheiden, wobei Datentransfer-Raten von bis zu 160 KBit/s erzielt werden. Die 868-MHz-Technologie ist daher sehr gut für Applikationen geeignet, die erhöhte Anforderungen an die Schnelligkeit der Objekterkennung stellen.

Gegenüber 13,56 MHz-Anwendungen zeigt die UHF Transponder-Technologie allerdings auch Schwächen. So sind UHF-Systeme sehr sensibel gegenüber Wasser bzw. wasserhaltigen Stoffen. Da Wasser Strahlung absorbiert, können eine feuchte Umgebung oder Personen, die sich im Strahlungsfeld des Systems befinden, die Lesereichweite deutlich einschränken. Auch die Durchdringung nicht-metallischer Stoffe ist generell stärker vom jeweiligen Material abhängig als bei induktiver Kopplung. Das erfordert eine deutlich präzisere Abstimmung des RFID-System auf den jeweiligen Untergrund und eine exaktere Justierung der Position von Transponder und Reader zueinander.

Die Lesbarkeit auf Metalloberflächen ist bei der UHF-Technologie zwar prinzipiell besser als bei der HF-Technologie, doch die angebotenen RFID-Inlays benötigen trotzdem einen Mindestabstand zum Metall, um arbeiten zu können. Daher sind UHF-Labels nicht als generelles Allheilmittel für metallische Umgebungen anzusehen.

Ein zentraler Einflussfaktor bei der Entwicklung von RFID-Lösungen sind gesetzliche Vorschriften. Da RFID-Systeme in verschiedenen Frequenzbereichen und Reichweiten arbeiten, müssen die Funkvorschriften der jeweiligen Regionen und Länder berücksichtigt werden. Hier existieren für den UHF-Bereich bedauerlicherweise weltweit unterschiedliche gesetzliche Regelungen. Während in Europa für UHF-RFID-Applikationen bisher ein 250-KHz-Band im Bereich von 869,4 bis 869,65 MHz und künftig zehn 200-KHz-Kanäle zwischen 865,6 und 867,6 MHz freigegeben sind, werden in den USA 902 bis 928 MHz mit 50 Kanälen verwendet. In Japan gibt es seit 2003 eine vorläufige Freigabe für Test mit RFID-Anwendungen im Logistikmanagement im Bereich 950 bis 956 MHz, Korea plant ein

Security und Privacy in RFID v.0.4

RFID-Frequenzband von 908,5 bis 914 MHz. Da in Europa und den USA der jeweils andere Frequenzbereich vom Mobilfunk blockiert wird, ist mit einer weltweiten Vereinheitlichung, wie sie im LF- und HF-Bereich realisiert ist, nicht zu rechnen.

Ausnutzen kann man bei UHF den Effekt, dass Wellen reflektiert werden. So können sich durch Reflexion an den Wänden in größerer Entfernung Feldstärken einstellen, die für eine Transponder-Erkennung ausreichen, obwohl dies in direkter Sicht nicht möglich erscheint. Allerdings ergeben sich durch Reflexion und Interferenz mit der direkt ausgestrahlten Welle auch Leselöcher, und dies je nach Umgebungskonfiguration bereits in kleineren Abständen (ab etwa ein bis zwei Metern). Geeignete Systemintegration nutzt die Vorteile und umgeht die Nachteile der Leselöcher durch Mehrfach-Antennen und bewegte Güter.

Hohe Reichweite (3-6 Meter für passive Transponder; 30 Meter und mehr für aktive Transponder) und hohe Lesegeschwindigkeit. Niedrige Preise für passive Transponder, tendenziell hohe Preise für aktive Transponder.

Möglicher Einsatz z.B. im Bereich der automatisierten Mautsysteme und Güterwagen-Erkennung

3.1.3.4 Mikrowelle

Diese Technologie verfügt über einen großzügigen Erfassungsbereich und eignet sich daher besonders für Applikationen, in denen große Lesereichweiten gefordert sind, wie z.B.:

- Zutrittskontrollen
- Container Tracking
- High Speed Detection
- Industrie-Automation
- Parkplatz Management

Die Antikollisionsfunktion erlaubt die Erkennung mehrerer Transponder gleichzeitig. Mit der optionalen Schreibfunktion dieses Systems ergeben sich weitere Anwendungsmöglichkeiten im Industriebereich.

Durch die variable Arbeitsfrequenz lassen sich mehrere Leser auch auf engstem Raum betreiben. Selbst bei sich überschneidenden Feldern kommt es zu keiner Beeinträchtigung der Leseleistung.

Vorteile:

- Servicefreundlich
- Einstellbare Reichweite
- High Speed Erfassung
- Große Reichweite
- Antikollision
- Variable Arbeitsfrequenz
- IP 65 - Hohe Schutzklassen

Security und Privacy in RFID v.0.4

- Robuster Aufbau
- bis zu 32 Leser vernetzbar

Mittels Mikrowellen-RFID Systemen ist es möglich Objekte zu orten.

3.2 Sicherheit von RFID Systemen

Wie jedes andere System der Nachrichten- und Informationstechnik, so sind auch RFID-Systeme potentiell gefährdet, von einem Angreifer ausgespäht oder manipuliert zu werden. Um die möglichen Risiken des Einsatzes von RFID-Systemen etwas besser einschätzen zu können, werden wir daher in Kapitel 3.2.2 einige der gängigen Angriffsarten auf RFID-Systeme etwas genauer betrachten. Im Anschluss daran werden in Kapitel 4.1 kryptographische Verfahren zum Schutz gegen gängige Angriffe vorgestellt.

Ein RFID-System ist darauf angewiesen, dass die vom Lesegerät erfassten Daten über weitere Kommunikationskanäle mit anderen Datenbeständen verknüpft werden. Die Sicherheitsaspekte in diesem so genannten Backend des RFID-Systems sind jedoch nicht spezifisch für RFID [*]. Um den Rahmen dieses Buchs nicht zu sprengen, beschränken wir uns da-her im Wesentlichen auf Angriffe auf die Luftschnittstelle zwischen dem Lesegerät und den Transpondern, sowie Angriffe auf den Transponder selbst. Angriffe auf das Hintergrundsystem, also zum Beispiel auf eine Datenbank, werden an dieser Stelle nicht weiter untersucht. Betrachten wir den Verwendungskontext in einem offenen RFID-System, so fällt auf, dass es in der Regel zwei beteiligte Parteien mit unterschiedlichen Interessen gibt. Der Systembetreiber bildet die aktive Partei und stellt die Infrastruktur, also die Lesegeräte und das Hintergrundsystem, zur Verfügung. Die aktive Partei gibt auch die Transponder aus, und verwertet die mit den Transpondern assoziierten oder abgespeicherten Daten. Damit hat sie alle vom RFID-System erfassten Daten sowie deren Verwendung unter Kontrolle [*]

Auf der anderen Seite stehen die Nutzer des RFID-Systems, in der Regel ein Kunde oder Angestellter des Systembetreibers. Die Nutzer bilden die passive Partei. Zwar ist die passive Partei im Besitz der Transponder (z. B. einem kontaktlosen Ticket oder Fahrschein, einem Ausweisdokument oder dem Warenaufkleber auf einem eben gekauften Produkt), sie hat aber nicht immer Einfluss auf deren Verwendung, bzw. auf die Verwendung der erfassten Daten[*].

In einem geschlossenen System, z. B. bei der Fertigungssteuerung mittels RFID in einem Betrieb, existiert die Trennung zwischen aktiver und passiver Partei nicht. Hier ist der Systembetreiber auch gleichzeitig der Nutzer des Systems.

Daneben kann es auch noch eine dritte Partei geben, zum Beispiel einen Hacker oder Konkurrenten, der versucht, unberechtigterweise an die im Transponder oder System gespeicherten Daten zu gelangen, oder diese sogar zu seinem Vorteil zu verändern.

Die breite Einführung von RFID-Systemen bei Warenaufklebern, Reisepässen und anderen Ausweisdokumenten, kontaktlosen Tickets und Eintrittskarten konfrontiert die breite Öffentlichkeit mit einer neuen und ungewohnten Technologie, deren Funktionsweise, und damit auch deren Grenzen oder Risiken nicht im Detail verstanden werden. Die Vielzahl an verschiedenen RFID-Systemen unterschiedlichster Performance trägt dabei nicht unwesentlich zu einer Verwirrung bei. Wie jeder neuen Technologie wird daher auch der RFID nicht nur mit Neugier,

*Risiken und Chancen des Einsatzes von RFID-Systemen, Studie des Bundesamtes für Sicherheit in der Informationstechnik in Zusammenarbeit mit dem Institut für Zukunftsstudien und Technologiebewertung (IZT) und der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA), November 2004

Security und Privacy in RFID v.0.4

sondern auch mit Ängsten und sogar Ablehnung begegnet. Eine vergleichbare Reaktion war auch Ende der 70er Jahre bei der Einführung von Barcodes zur Produktkennzeichnung, dem EAN-Code oder dem amerikanischen UPC, zu beobachten.

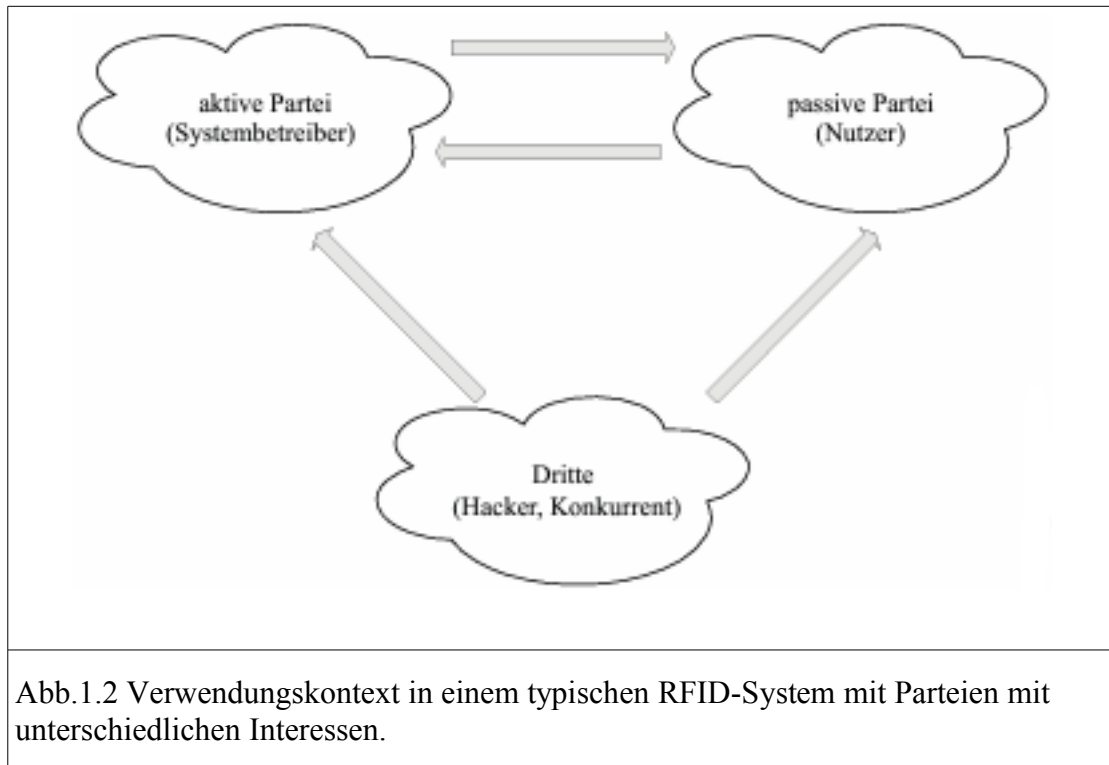


Abb.1.2 Verwendungskontext in einem typischen RFID-System mit Parteien mit unterschiedlichen Interessen.

Ein wichtiger Diskussionspunkt war damals, und ist auch heute wieder der Schutz der Privatsphäre des Einzelnen. Im Vordergrund steht dabei die Angst, die neue Technologie RFID könnte zum unbemerkten und unerwünschten Sammeln von Daten des Einzelnen, also zum Ausspionieren der Privatsphäre durch die aktive Partei, eingesetzt werden. In den letzten Jahren haben sich vermehrt Bürgerverbände und Verbraucherschutzorganisationen darum bemüht, die Öffentlichkeit über die möglichen Risiken eines breiten Einsatzes von RFID-Systemen zu informieren.

In einigen Ländern, insbesondere in den USA, wurde bereits mehrfach die Einführung von Gesetzen zur Regulierung des Einsatzes von RFID gefordert, so etwa im Januar 2004 im US-Bundesstaat Missouri der „RFID Right to Know Act of 2004 (SB 0867)“, der jedoch bisher nicht verabschiedet wurde [1]. Der Entwurf für diese Verordnung fordert unter anderem die eindeutige und sichtbare Kennzeichnung von Produkten, die einen RFID-Chip beinhalten.

3.2.1 Datenschutz und Privacy

Bei der datenschutzrechtlichen Bewertung der RFID-Technik stellt sich zunächst die Frage, inwieweit durch diese Technik personenbezogene Daten berührt sind. Bei einigen Anwendungen wie etwa den biometrischen Reisepässen und Personalausweisen werden die RFID-Tags selbst personenbezogene Daten enthalten. Auch in Krankenhäusern wird RFID-Technik bereits zur Identifizierung der Patienten erprobt. In Patientenarmbänder integrierte RFID-Tags sollen es Ärzten und Pflegepersonal im Notfall ermöglichen, schnell auf die Krankengeschichte und

¹ Lahiri, S. : RFID Sourcebook, IBM Press, Upper Saddle River NJ, 2004

Security und Privacy in RFID v.0.4

Medikamentendosierung zugreifen zu können. Aber auch, wenn ein RFID-Tag selbst keine personenbezogenen Daten enthält, kann dessen Verwendung dazu beitragen, dass personenbezogene Daten über den Inhaber des mit dem RFID-Tag versehenen Gegenstands wesentlich leichter als bisher gesammelt und ausgewertet werden können. Folgende datenschutzrechtliche Risiken gehen mit der Nutzung der RFID-Technik einher[*]:

- **Bewegungsprofile**

Insbesondere wenn Personen bestimmte mit RFID-Tag versehene Gegenstände häufig mit sich führen (z. B. bestimmte Kleidungsstücke, Schuhe, Taschen, Handys), kann jeder, der einmal die Zuordnung zwischen Person und der Produkt-ID vorgenommen hat, ein Bewegungsprofil der Person erstellen. Dies ist umso leichter möglich, je mehr Geräte zum Auslesen der Daten in Behörden, Unternehmen oder öffentlichen Bereichen betrieben werden und je intensiver deren Betreiber die erfassten Daten untereinander austauschen.

- **Nutzungs- und Verhaltensprofile**

Verknüpft man Daten über Personen mit den per RFID bei ihnen nachgewiesenen Waren, lässt dies Rückschlüsse auf Interessen, Vorlieben und andere Persönlichkeitsmerkmale zu. Da beim Einsatz der RFID-Technik zur Warenkennzeichnung vorgesehen ist, jedes einzelne Produkt mit einer individuellen Nummer zu versehen, wird sich unter Umständen für jeden Gegenstand, der künftig irgendwo angetroffen wird, nachvollziehen lassen, wer diesen Gegenstand wann wo gekauft hat. Solche Informationen, die in erster Linie den Verkäufern der Waren zur Verfügung stehen, können bei Vorliegen entsprechender Voraussetzungen aber auch von Strafverfolgungsbehörden oder anderen Sicherheitsbehörden für deren Zwecke genutzt werden.

- **Fehlende Transparenz**

RFID-Tags können versteckt an oder in Waren angebracht sein. Da der Inhaber eines mit RFID-Tag versehenen Gegenstands auch nicht ohne weiteres etwas davon bemerkt, wenn ein RFID-Tag mit einem externen System Daten austauscht, besteht beim Einsatz der RFID-Technik das Risiko, dass unbemerkt Daten über den Inhaber der Gegenstände erhoben werden.

- **Große Datenmengen**

Bei einer systematischen Ausstattung der Alltagsgegenstände mit RFID-Tags und einer systematischen Speicherung der mit Hilfe der RFID-Technik ausgetauschten Daten können riesige Datenbestände entstehen.

- **Komplexe Auswertungen**

Diese Datenmengen können auf vielfältige Weise automatisiert ausgewertet werden. Insbesondere können in diesen Datenbeständen Verfahren des sog. Data Mining zum Einsatz kommen, bei denen - zunächst noch ohne bestimmtes Ziel - diese auf formale Besonderheiten hin untersucht werden können.

* RFID. Auszug aus dem 26. Tätigkeitsbericht 2005 des Landesbeauftragten für Datenschutz Baden-Württemberg. Version 1.0 08.06.2006

Security und Privacy in RFID v.0.4

- „Datenschatten“

Führt jemand mit RFID-Tags versehene Gegenstände in Taschen oder einem Rucksack mit sich, so können diese von einem Dritten, der über ein RFID Lesegerät verfügt, identifiziert werden. Der Einblick in den Tascheninhalt wird damit auch gegen den Willen des Inhabers der Gegenstände möglich. Die dabei gewonnenen Erkenntnisse können zudem mit weiteren, zu der Person bekannten Informationen zusammengeführt werden. Auch wenn auf diese Weise der Name der Person noch nicht direkt ermittelt werden kann, wirft der Einzelne einen „Datenschatten“, der von Dritten wahrgenommen und für deren Zwecke ausgewertet werden kann.

- RFID-Funkverkehr abhörbar

Wenn keine weiteren Schutzmaßnahmen ergriffen werden, können die zwischen einem RFID-Tag und dessen Kommunikationspartnern ausgetauschten Daten von Dritten abgehört werden.

Datenschutzmaßnahmen bei RFID-Systemen, die unmittelbar zur Verarbeitung personenbezogener Daten dienen

Dass Systeme, bei denen personenbezogene Daten in den RFID-Tags gespeichert werden, datenschutzrechtlich sorgsam konzipiert werden müssen, entspricht den auch bislang schon geltenden Regeln des Datenschutzes. Derartige Systeme müssen insbesondere folgenden Anforderungen entsprechen:

- Es ist eine Vorabkontrolle durchzuführen. Dabei ist zu prüfen, welche Gefahren sich bei Realisierung des geplanten Projekts für die Persönlichkeitsrechte der Betroffenen ergeben, was zur Reduzierung dieser Gefahren getan werden soll sowie ob das danach verbleibende Restrisiko tragbar ist.
- Spätestens mit Beginn des Echtbetriebs müssen technisch-organisatorische Datenschutzmaßnahmen ergriffen werden und nachvollziehbar dokumentiert sein.
- Es muss sichergestellt sein, dass die Betroffenen die ihnen zustehenden Rechte ohne unverhältnismäßigen Aufwand wahrnehmen und so etwa Auskunft über die zu ihrer Person gespeicherten Daten erhalten oder die Berichtigung unrichtiger Daten verlangen können.

Datenschutzmaßnahmen bei RFID-Systemen, die nicht unmittelbar zur Verarbeitung personenbezogener Daten dienen sollen

Eine Besonderheit der RFID-Technik liegt darin, dass auch Systeme, die nicht unmittelbar zur Verarbeitung personenbezogener Daten genutzt werden sollen, nachhaltig in die Persönlichkeitsrechte von Bürgerinnen und Bürgern eingreifen können. Denn ein Personenbezug lässt sich mitunter auch in diesen Fällen leicht herstellen, etwa wenn die Identität der Person, die RFID-markierte Waren bei sich trägt, durch Auslesen personenbezogener Daten etwa aus einer Kreditkarte bestimmt werden kann. Werden die aus RFID-Tags ausgelesenen Daten z.B. in zentralen Datenbanken gespeichert, so können Bewegungs-, Nutzungs- und letztlich auch Persönlichkeitsprofile erstellt werden, deren Zustände kommen für den Betroffenen

Security und Privacy in RFID v.0.4

vollkommen intransparent ist und auf deren Entstehen er keinen Einfluss hat. Das bedeutet, dass das Recht des Betroffenen auf informationelle Selbstbestimmung durch diese Technologie erheblich gefährdet ist. Geboten ist daher eine frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen auch bei solchen RFID-Anwendungen, die unmittelbar nur auf die Verarbeitung nicht-personenbezogener Daten gerichtet sind.

Generelle Datenschutzmaßnahmen bei RFID-Systemen

Bei allen datenschutzrechtlich relevanten RFID-Anwendungen ist zu fordern, dass

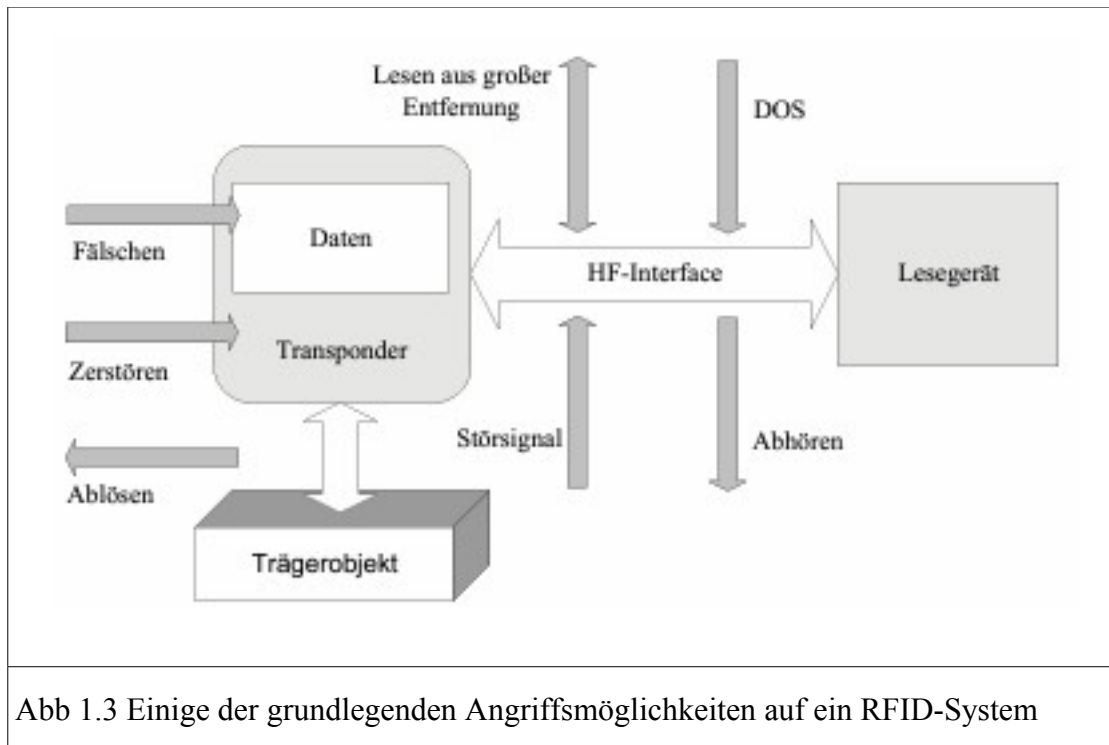
- der Grundsatz der Erforderlichkeit der Datenverarbeitung beachtet wird,
- dem Grundsatz der Datensparsamkeit folgend die Systeme so gestaltet werden, dass so weit wie möglich auf die Verarbeitung personenbezogener Daten verzichtet wird,
- die Bürgerinnen und Bürger stets erkennen können, wenn eine Ware mit dieser Technik ausgestattet ist; ferner muss zu erkennen sein, welche Daten damit verarbeitet werden und welche Art der Datenverarbeitung damit ermöglicht wird,
- technische Maßnahmen gegen das unbefugte Auslesen von auf RFID-Tags gespeicherten Daten und das Abhören der drahtlos übertragenen Daten ergriffen werden,
- den Betroffenen die Möglichkeit geboten werden sollte, die Funktion der RFID-Tags zu deaktivieren, sofern diese ihre Aufgabe erfüllt haben.

Insbesondere hinsichtlich des Umgangs mit RFID-Tags, die nicht unmittelbar der Verarbeitung personenbezogener Daten dienen sollen, bleibt abzuwarten, ob deren Anbieter die hier dargestellten Maßnahmen ergreifen. Sofern dies nicht in ausreichendem Maße geschieht, ist eine entsprechende gesetzliche Verpflichtung zu erwägen.

3.2.2 Angriffe auf RFID Systeme

Ein Blick auf die Abbildung 4.1 zeigt uns verschiedene grundlegende Angriffsarten auf die verschiedenen Komponenten eines RFID-Systems. Grundsätzlich kann ein Angriff dabei auf den Transponder, das Lesegerät oder auch das HF-Interface zwischen Transponder und Lesegerät erfolgen.

Security und Privacy in RFID v.0.4



Die Angriffe können dabei völlig unterschiedlich motiviert sein. Je nach dem Zweck, der hierbei verfolgt wird, lassen sich für die nachfolgend beschriebenen Angriffe vier Angriffs-arten klassifizieren:

- **Ausspähen**: Hier versucht der Angreifer, sich unberechtigten Zugang zu Informationen und Daten der aktiven oder passiven Datei zu verschaffen.
- **Täuschen**: Hierbei versucht der Angreifer, unzutreffende Informationen in das RFID-System einzuspeisen, um die aktive Partei, also den Betreiber eines RFID-Systems, oder die passive Partei, also den Benutzer eines RFID-Systems, zu täuschen.
- **Denial of Service**: Bei diesem Angriff wird die Verfügbarkeit von Funktionen eines RFID-Systems beeinträchtigt.
- **Schutz der Privatsphäre**: Der Angreifer sieht seine eigene Privatsphäre durch das RFID-System bedroht und versucht, diese durch einen entsprechenden Angriff auf das RFID-System zu schützen.

3.2.2.1 Angriffe auf den Transponder

Am leichtesten zugänglich ist in der Regel der Transponder, der auf Waren oder als Ticket für einen Angreifer jederzeit und in den meisten Fällen zeitlich unbegrenzt zur Verfügung steht. Gegenüber dem Transponder existiert daher eine Vielfalt an unterschiedlich wirksamen Angriffen.

Dauerhaftes Zerstören des Transponders. Die einfachste Möglichkeit eines Angriffes auf ein RFID-System besteht in der mechanischen oder chemischen Zerstörung eines Transponders. So kann die Antenne meist mit einfachen Hilfsmitteln durchtrennt oder abgeschnitten werden. Auch der Chip kann durch Knicken oder einen Hammerschlag leicht zerstört werden. Eine weitere Möglichkeit ist die

Security und Privacy in RFID v.0.4

Zerstörung eines Transponders durch eine entsprechend starke Feldeinwirkung. So ist für induktiv gekoppelte Transponder nach ISO/IEC14443 oder ISO/IEC15693 eine maximale Feldstärke von 12A/m bei einer Frequenz von 13,56Mhz spezifiziert. Wird der Transponder bei dieser Frequenz in ein Feld mit deutlich höherer Feldstärke eingebracht, kann schließlich die am Shuntregler auftretende Verlust wärme nicht mehr ausreichend abgeführt werden, so dass der Transponder thermisch zerstört wird. Steht kein ausreichend starker Sender für diesen Frequenzbereich zur Verfügung, so kann der Transponder auch in einen Mikrowellenherd eingebracht werden.

Abschirmen oder Verstimmen des Transponders. Ein sehr effektiver Angriff ist das Abschirmen eines Transponders gegenüber der magnetischen oder elektromagnetischen Strahlung des Lesegerätes durch Metallflächen. Im einfachsten Fall reicht es dabei, einen Transponder in eine metallische Folie, zum Beispiel Alu-Haushaltsfolie, einzuwickeln. Bei induktiv gekoppelten Transpondern wird der Antennenschwingkreis des Transponders durch eine Metalloberfläche in unmittelbarer Nähe stark verstimmt. Zusätzlich wird das magnetische Feld des Lesegerätes durch Wirbelstromverluste in der Metallfolie gedämpft. Häufig reicht es daher schon, einen Transponder auf einer Seite auf einer Metallfläche zu befestigen. Die elektromagnetischen Felder eines UHF-Backscatter-Systems (zum Beispiel auf 868 MHz) werden durch eine Metallfläche reflektiert, und so wirkungsvoll vom Transponder abgehalten. Ein passiver Transponder wird im günstigsten Fall gar nicht erst mit ausreichend Energie zum Betrieb des Chips versorgt. Dieser Angriff ist vor allem dazu geeignet, einen Transponder nur zeitweise außer Betrieb zu setzen. Wird die Abschirmung entfernt, so ist der Transponder wieder uneingeschränkt funktionsfähig. Für den technisch weniger versierten Laien werden mittlerweile auch kommerzielle Produkte zur Abschirmung von Transponder angeboten [*]. Antennen von UHF-Backscatter-Transpondern werden durch das Auf- oder Einbringen in ein Dielektrikum, zum Beispiel Glas oder Kunststoff, verstimmt. Die Verstimmung fällt umso stärker aus, je höher die Dielektrizitätskonstante ϵ_r und Dicke des umgebenden Dielektrikums sind. Durch die auftretende Verstimmung verschlechtert sich die Ansprechempfindlichkeit des Transponders auf der Sendefrequenz des Lesegerätes, so dass die Lesereichweite des derart angegriffenen Transponders verringert wird.

Emulieren und Klonen eines Transponders. Es gibt unterschiedlich komplexe Verfahren zur Informationsspeicherung in einem Transponder. Im einfachsten Fall, dem Read-only-Transponder, verfügt der Transponder lediglich über eine fest programmierte Kennung, die Seriennummer des Transponders.

Gelangt ein Read-only Transponder in ein ausreichend starkes Feld eines Lesegerätes, beginnt er unmittelbar mit der periodischen Aussendung seiner Seriennummer, so dass diese von einem geeigneten Lesegerät problemlos gelesen werden kann. Ein Angreifer könnte nun aus diskreten Bauelementen selbst einen Read-only-Transponder (Transponderklon) aufbauen, und das PROM, das die Seriennummer des Transponders enthält, durch einen mehrfach programmierbaren Speicher (EEPROM) oder, im einfachsten Falle, durch eine Reihe von DIP-Schaltern ersetzen. Liest der Angreifer anschließend die Seriennummer eines beliebigen Transponders aus, kann er diese Seriennummer dann im Transponderklon einprogrammieren. Wird der Transponderklon in das Feld eines Lesegerätes gehalten, kann er nun die zuvor aus dem echten Transponder ausgelesene Seriennummer aussenden, und somit die

* Cloatek™ EMI /RFI Shielding, <http://mobilecloak.com>

Security und Privacy in RFID v.0.4

Anwesenheit des echten Transponders gegenüber dem Lesegerät vortäuschen [^{*1}]. Für das Lesegerät besteht keine Möglichkeit festzustellen ob eine aktuell empfangene Seriennummer von einem echten Transponder oder einem Transponderklon gesendet wurde. Problematisch ist es dabei auch, dass der Angreifer keinen physischen Zugriff auf den Transponder benötigt, sondern sich lediglich mit einem geeigneten Lesegerät unbemerkt bis auf Lesereichweite an den zu klonenden Transponder annähern muss.

Nach dem Read-only-Transponder wird die nächste Stufe der Funktionalität durch Transponder mit beschreibbaren Speichern gebildet. Häufig können die Speicherbereiche völlig frei, d.h. ohne Kenntnis eines geheimen Passwortes oder Schlüssels, gelesen und beschrieben werden. Auch hierbei besteht die Möglichkeit, dass die gespeicherten Daten von einem Angreifer entweder einfach zu dessen Nutzen verändert werden, oder dass Kopien des angegriffenen Transponders hergestellt werden, indem die Daten ausgelesen und auf weitere Transponder kopiert werden. Durch den Einsatz von Authentifizierung und verschlüsselter Datenübertragung kann das Klonen von Transpondern jedoch wirkungsvoll verhindert werden. RFID-Anwendungen, die für einen Angreifer leicht zugänglich sind, zum Beispiel Zutrittssysteme oder Ticketsysteme, sollten daher auf die Anwendung von Read-only-Transpondern oder den unverschlüsselten Zugriff auf Datenbereiche grundsätzlich verzichten.

Angriffe über das HF-Interface. RFID-Systeme sind Funkssysteme und kommunizieren über elektromagnetische Wellen im Nah- und Fernfeld. Für einen Angreifer liegt es daher nahe zu versuchen, ein RFID-System über das HF-Interface anzugreifen. Der besondere Reiz liegt darin, dass bei einem Angriff über das HF-Interface kein physischer Zugriff auf ein Lesegerät oder einen Transponder nötig ist, sondern aus der Entfernung agiert werden kann. Derzeit sind folgende Angriffe bekannt und untersucht:

- Abhören der Kommunikation zwischen Lesegerät und Transponder.
- Stören der Kommunikation zwischen Lesegerät und Transponder mittels Störsender.
- Vergrößern der Lesereichweite zum unbemerkten Auslesen entfernter Transponder.
- Blockieren eines Lesegerätes durch DOS-Attacken.
- Unbemerkte Verwendung eines entfernten Transponders mittels einer Relay-Attacke.

^{*1} Westhues, J. : Hacking the prox card, erschienen in Garfinkel, S., Rosenberg.: RFID Applications, Security, and Privacy, July 2005

4. Problemanalyse

4.1 Kryptographische Maßnahmen

In zunehmendem Maße werden RFID-Systeme auch in sicherheitsrelevanten Anwendungen, wie Zutrittssystemen, oder als Zahlungsmittel und Tickets eingesetzt. Bei diesen Einsatzbereichen muss jedoch immer mit potenziellen Angriffsversuchen gerechnet werden, bei denen versucht wird, RFID-Systeme „auszutricksen“ und sich damit unberechtigten Zutritt zu Gebäuden oder einen unbezahlten Zugriff auf Dienstleistungen (Tickets) zu verschaffen. Die technischen Möglichkeiten hierzu haben wir bereits in Kapitel 3.2.2 „Angriffe auf RFID Systeme“ eingehend untersucht. Schon in den Mythen und Märchen wurde versucht, Sicherheitssysteme zu überlisten. So gelang es zum Beispiel Ali Baba, durch das Ausspähen eines geheimen Passwortes, sich unberechtigten Zutritt in das vermeintlich sichere Warenlager der 40 Räuber zu verschaffen. Auch bei modernen Authentifizierungsprotokollen wird ausnahmslos die Kenntnis eines Geheimnisses (d.h. eines kryptographischen Schlüssels) überprüft. Durch geeignete Algorithmen kann jedoch das Ausspähen der geheimen Schlüssel verhindert werden. Im Einzelnen müssen folgende Angriffsversuche auf sicherheitsrelevante RFID-Systeme abgewehrt werden können:

Unberechtigtes Auslesen eines Datenträgers, um Daten zu duplizieren und/oder zu verändern.

Einbringen eines applikationsfremden Datenträgers in den Lesebereich eines Lesegerätes mit der Absicht, unberechtigten Zutritt oder Leistungen zu erlangen.

Abhören der Funkverbindung und Wiedervorspielen der Daten, um so einen echten Datenträger vorzutäuschen („replay and fraud“). Bei der Auswahl von geeigneten RFID-Systemen sollte den kryptologischen Funktionen der betrachteten Systeme besondere Aufmerksamkeit zukommen. Anwendungen, die keinerlei Sicherheitsfunktionen bedürfen (z.B. Industrieautomation, Werkzeugetkennung), werden durch kryptologische Verfahren nur unnötig verteuert. Im Gegensatz dazu kann sich bei sicherheitsrelevanten Anwendungen (z.B. Ticketing, Kleingeldbörse) der unüberlegte Verzicht auf kryptologische Verfahren durch unberechtigte Inanspruchnahme von Leistungen mittels manipulierter Transponder teuer rächen.

4.2 Symmetrische Verschlüsselung

4.3 Asymmetrische Verschlüsselung

4.4 Authentifizierung

Security und Privacy in RFID v.0.4

5. Implementierung

Zum Anfang dieser Arbeit würde entschieden die Arbeit auf zwei Teilaufgaben zu Teilen. Eine ist die Implementierung einer Erweiterung zu einem RFID Device Handler Software und Erstellung einer Verwaltung Web Applikation.

Entwicklung eines Package für den Device Handler gibt dem RFID System zusätzliche Funktionalität um angegebene Niveau von Sicherheit zu erreichen.

Zertifikate und Kunden Verwaltung Web Applikation ist eine selbständige Web Portal Lösung die als Aufgabe stellt sich eine Umgebung leicht Zertifikate für die Kunden zu verwalten, aber auch eine Zentrale stelle den Device Handler Sicherheitspaket.

Projekt Management

Bevor man mit der Anforderungsdefinition für ein Softwareprojekt beginnt, wird das gesamte Projekt geplant. Eine gute Projektplanung ist das A und O eines jeden Projekts. Um später gute Benutzbarkeit und Wartbarkeit zu gewährleisten, sollten bereits zu Projektbeginn alle erforderlichen Ressourcen eingeplant werden.

Ein guter Projektmanagement ist einer der wichtigsten Faktoren für den Erfolg einer Arbeit. Auch bei einem Einmannprojekt ist das nicht zu unterschätzen. Durch Planung und Strukturierung in diesem Projekt lässt sich vor allem erreichen:

- Besserer Überblick
- Leichtere Steuerbarkeit der Prozesse
- Zeitgewinn

Planner – Gantt Diagramm

Es würde einen Open Source Tool – „Gnome Planner“ verwendet um sich die Aufgaben in eine Klare Struktur zu unterteilen.

Im Gantt-Diagramm werden die Aktivitäten eines Projektes in die erste Spalte einer Tabelle eingetragen. In der ersten Zeile der Tabelle wird die Zeitachse dargestellt.

Die einzelnen Aktivitäten werden dann in den jeweiligen Zeilen mit einem waagerechten Balken visualisiert. Je länger der Balken, desto länger dauert die Aktivität. Sich überschneidende Aktivitäten werden durch überlappende Balken dargestellt. Auch die Visualisierung des kritischen Pfades ist möglich. Häufig wird mit Pfeilen versucht, Abhängigkeiten zwischen den Aktivitäten zu verdeutlichen. Bei einer großen Anzahl an Aktivitäten wird die Darstellung dann schnell unübersichtlich. Das Gantt-Diagramm eignet sich deshalb eher für Projekte mit einer geringen bis mittleren Anzahl an Aktivitäten.

Eine Herausforderung liegt in der Wahl des richtigen Detaillierungsgrades. Eine zu geringe Anzahl an Aktivitäten oder nur die Darstellung von Teilprojekten ermöglicht keine ausreichende Kontrolle der Aktivitäten. Jede einzelne Tätigkeit aufzunehmen, schwächt die Aussagekraft. Die Zusammenfassung von Aktivitäten zu Projektphasen macht das Gantt-Diagramm erheblich übersichtlicher.

Security und Privacy in RFID v.0.4

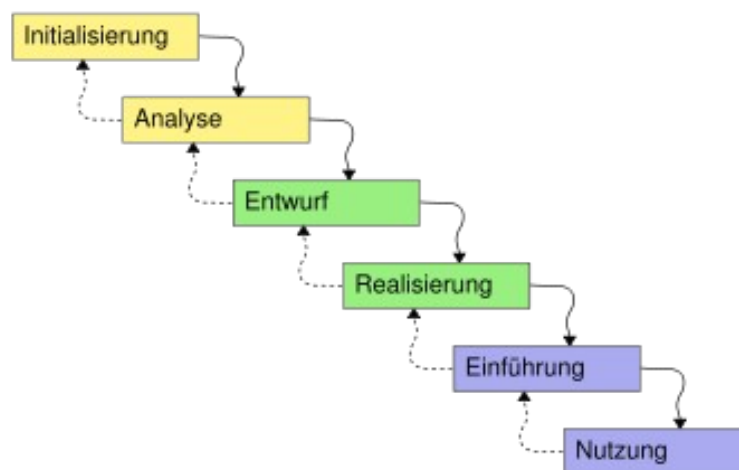
Wasserfall Modell

Es sind alle Anforderungen für die Implementierung erster Iteration schon von Anfang an klar definiert. Das spricht ganz stark für einen Wasserfall Modell als Vorgehensmodell.

Das Wasserfallmodell bezeichnet ein Vorgehensmodell in der Softwareentwicklung, bei dem der Softwareentwicklungsprozess in Phasen organisiert wird. Dabei gehen die Phasenergebnisse wie bei einem Wasserfall immer als bindende Vorgaben für die nächst tiefere Phase ein.

Zuerst vorgeschlagen wurde es in einer Publikation aus dem Jahr 1970 von Winston Royce mit dem Titel Managing the Development of Large Software Systems: Concepts and Techniques. Im Wasserfallmodell hat jede Phase wohldefinierte Start- und Endpunkte mit eindeutig definierten Ergebnissen. In Meilensteinsitzungen am jeweiligen Phasenende werden die Ergebnisdokumente verabschiedet. Zu den wichtigsten Dokumenten zählen dabei das Lastenheft sowie das Pflichtenheft. In der betrieblichen Praxis gibt es viele Varianten des reinen Modells. Es ist aber das traditionell am weitesten verbreitete Vorgehensmodell.

Der Name „Wasserfall“ kommt von der häufig gewählten grafischen Darstellung der fünf bis sechs als Kaskade angeordneten Phasen.



Erweiterungen des einfachen Modells (Wasserfallmodell mit Rücksprung) erlauben ein schrittweises „Aufwärtslaufen“ der Kaskade, sofern in der aktuellen Phase etwas schief laufen sollte, um den Fehler auf der nächsthöheren Stufe ausmerzen zu können.

Das Wasserfallmodell wird allgemein dort vorteilhaft angewendet, wo sich Anforderungen, Leistungen und Abläufe in der Planungsphase relativ präzise beschreiben lassen.

In der Phase Initialisierung und Analyse werden alle User Stories zusammengeschrieben und es wird ein grobes Verhalten überlegt. Alle Anforderungen und Schnittstellen werden festgelegt.

In diesem Projekt ist es sinnvoll Entwurf Phase durch Unit Tests Entwicklung zu ersetzen. Es werden zuerst alle Test Fälle ausgeschrieben um dann das verlaufen von Realisierungsphase zu kontrollieren.

Security und Privacy in RFID v.0.4

Realisierung ist eigentlich Implementierung von funktionalem Code. Es werden alle Klassen implementiert und alle Verschlüsselungsverfahren.

Einführung und Nutzung ist das Testen von dem Sicherheitspaket in einer echten Anwendung mit Device Handler und RFID Reader.

User Stories

„Benutzergeschichte“ ist eine in Alltagssprache formulierte Software-Anforderung. Sie ist bewusst kurz gehalten und umfasst in der Regel nicht mehr als zwei Sätze.

User Stories werden in Extreme Programming (XP) zusammen mit Akzeptanztests zur Spezifikation von Anforderungen eingesetzt. Dabei wird jede User Story auf eine Story-Card geschrieben. Der Autor der Story sollte der Kunde des Software-Projektes sein. Die User Story ist die wichtigste Methode um ein agiles Projekt zu steuern.

Hier sind folgende User Stories:

Anwendung Starten

Die Anwendung startet, es werden alle RFID Reader Initialisiert, dabei wird die Eigenschaften Datei gelesen um alle wichtigen Informationen für den Sicherheit Package. Es wird einen Privat Schlüssel und Publik CA Zertifikat geöffnet. Das Privat Schlüssel wird nach Gültigkeit gegen den Publik CA Zertifikat überprüft. Wenn das Schlüssel noch gültig ist kann die Applikation weiter laufen. Im gegen Fall wird eine Meldung in das Log geschrieben das diese Applikation keine Berechtigung hat.

Anwendung Authentifizieren

Es wird Anwendungsprivatschlüssel eingelesen und das CA Publik Root Zertifikat. Dann findet statt eine Signatures Überprüfung ob das Zertifikat von der Anwendung wirklich mit CA Stelle signiert wurde. Die Echtheit von Root Zertifikat wird mit einer MD5 Hash Funktion wo die MD5 Summe direkt im Code eingetragen ist verifiziert. Wenn das Validierungsdatum immer noch gültig ist wird Anwendung Authentifiziert.

RFID Tag beschreiben

Es wird aus Eigenschaften Datei eine Verschlüsselungsstrategie ausgewählt. Alternative kann man die Strategie über API wechseln. Die Daten werden mit Hilfe von Sicherheitspaket verschlüsselt und zurück und den Device Handler gegeben um dann auf den Chip geschrieben zu werden.

RFID Tag lesen

Es wird eine Strategie für die Verschlüsselung aus Eigenschaften Datei ausgewählt, oder über API bestimmt. Daten von Device Handler, der den RFID Tag gelesen hat werden entschlüsselt und an den Device Handler zurück gegeben.

Bei Entschlüsselung kann erkannt werden ob die Daten mit selbem Verfahren verschlüsselt waren. Falls nicht wird eine Meldung und Device Handler geschickt.

Security und Privacy in RFID v.0.4

Anmeldung auf dem Portal für die Zertifikaten Verwaltung

Verwaltung von Portal Nutzern

Man bekommt eine Login Maske und nach einer erfolgreicher Authentifizierung wird angemeldeter Nutzer einer Rolle auf diesem Portal zugeteilt. Diese Rolle bestimmt Zugriffsberechtigungen von dem Nutzer zu bestimmten Funktionen. Falls Nutzer Rechte auf eine Nutzer Verwaltung hat, kann dies andere Nutzer Eintragen, Sperren oder die Zugriffsrechte verändern.

Verwaltung von Kunden

Nutzer mit Kundenverwaltungsrechten haben Zugriff auf das einsehen und verändern von Kunden Listen. Mann kann neue Kunden eintragen, deren Daten eingeben oder verändern, oder auch löschen.

Verwaltung der Zertifikate

Jeder Kunde hat eine Menge von Zertifikaten. Nutzer mit einer Berechtigung zu dieser Funktion können neue Zertifikate generieren lassen. Es werden keine Zertifiten gelöscht. Für jede Aktion für einen Kunden wird eine History (Geschichte) mit protokolliert. Mann kann alle aktivitäten für einen Kunden nachsehen.

Lauf- und Entwicklungs- Umgebung

Das Sicherheitspaket wird mit Hilfe von Eclipse 3.2 auf Java 1.5 entwickelt. Dabei sind keine zusätzliche Java Pakete mutig.

Die Web Anwendung wird auf einem Development Web Server entwickelt basieren auf einem Gentoo System mit Apache 2.1 als Web Server mit PHP 5.2. Alle Daten werden in einer MySQL Datenbank gehalten.

Für die Datenbank Verwaltung wird SQLyog verwendet.

Für die Source Control Management von Quellcode soll Subversion verwendet werden.

Entwicklung von Sercurity Package soll mit „Testdriven Development“ Technik entwickelt werden.

Subversion

Subversion (SVN) ist eine Open Source Software zur Versionsverwaltung. Sie wurde als Freie Software unter einer Lizenz im Stil der Apache-Lizenz veröffentlicht. Die Benennung „Subversion“ verweist einerseits auf den politisch-soziologischen Begriff der Subversion und greift andererseits die Bedeutung von Subversion im Sinne von Unterversion, früherer Version auf.

Subversion wurde als moderne Ablösung für das mit vielen Schwächen behaftete, in Entwicklerkreisen trotzdem noch sehr verbreitete, Programm CVS entwickelt. Deshalb ist es mit Bedacht in der Bedienung sehr ähnlich gehalten, hat dasselbe zentrale Paradigma und behebt die meisten Schwächen von CVS.

Security und Privacy in RFID v.0.4

Testgetriebene Entwicklung

Es ist sehr wichtig eine sehr hoch Qualitative Code zu schreiben bei solchen Projekten wie dieses. Qualität von Quellcode sehr hoch beeinflusst den Sicherheitsfaktor von einer Anwendung. Dabei würde entschieden die „Testdriven Development“ Technik aus Extreme Programming Umfeld zu verwenden.

Es werden zu erst die Test Fälle geschrieben und dann dazu die Implementierung. Testfälle bedecken auch alle User Stories.

Als testgetriebene Entwicklung (auch testgesteuerte Programmierung, engl. test first development oder test-driven development, Abkürzung TDD, manchmal auch scherzhaft Extreme Testing) bezeichnet man eine Agile Methode zur Entwicklung eines Computerprogramms, bei der die Programmierer Software-Tests vor den zu testenden Komponenten entwickeln. Unit-Tests der testgetriebenen Entwicklung sind Grey-Box-Tests statt White-Box-Tests. Die wohl bekannteste Agile Methode ist die des Extreme Programming.

Klassischerweise werden Tests nach oder parallel unabhängig zum zu testenden System entwickelt. Dies kann unter Umständen dazu führen, dass nicht die gewünschte bzw. erforderliche Testabdeckung erzielt wird. Mögliche Gründe dafür sind unter anderem:

- Akuter Zeitmangel
- Mangelhafte Testbarkeit (das zu testende System besitzt Eigenschaften, die das Testen erschweren)
- Faulheit bzw. mangelnde Disziplin der Programmierer
- Firmenpolitik verbietet Investition in nicht-funktionale Programmteile

Ein weiterer Nachteil klassischer Unit-Tests als White-Box-Tests ist, dass der Entwickler das zu testende System und seine Eigenheiten kennt und dadurch eventuell ungewollt "um Fehler herum" testet.

Die testgetriebene Entwicklung ist ein Ansatz, den Gründen für eine nicht ausreichende Testabdeckung und einigen Nachteilen der White-Box-Tests entgegenzuwirken.

JUnit

JUnit ist ein Framework zum Testen von Java-Programmen, das besonders für automatisierte Unit-Tests einzelner Units (meist Klassen oder Methoden) geeignet ist. Es basiert auf Konzepten, die ursprünglich unter dem Namen SUnit für Smalltalk entwickelt wurden.

Ein JUnit-Test kennt nur zwei Ergebnisse: Entweder der Test gelingt (dann ist er „grün“) oder er misslingt (dann ist er „rot“). Das Misslingen kann als Ursache einen Fehler (Error) oder ein falsches Ergebnis (Failure) haben, die beide per Exception signalisiert werden. Der Unterschied zwischen den beiden Begriffen liegt darin, dass Failures erwartet werden, während Errors eher unerwartet auftreten. Technisch werden Failures mittels einer speziellen Exception namens „AssertionFailedError“ signalisiert, während alle übrigen Exceptions vom JUnit-Framework als Error interpretiert werden. JUnit ist ein wichtiges Hilfsmittel im Extreme Programming und unterstützt in diesem Zusammenhang die Idee des Extreme Testing. Dabei schreibt ein Programmierer zuerst einen automatisch wiederholbaren (JUnit-)Test und dann

Security und Privacy in RFID v.0.4

den zu testenden Code. Der Test ist selbst ein Stück Software und wird ebenso wie der zu testende Code programmiert. Wenn zu einem späteren Zeitpunkt ein anderer Programmierer den so entstandenen Code ändern möchte, so ruft er zuerst alle JUnit-Tests auf, um sich zu vergewissern, dass der Code vor seiner Änderung fehlerfrei ist. Dann führt er die Änderung durch und ruft die JUnit-Tests erneut auf. Misslingen diese, so weiß er, dass er selbst einen Fehler eingebaut hat und muss ihn korrigieren. Dieser Zyklus wiederholt sich solange, bis alle JUnit-Tests wieder „grün“ sind.

Dieses Verfahren wird auch „Testgetriebene Entwicklung“ (englisch test-driven software development) genannt und zählt zu den Agilen Methoden. Die Idee dabei ist, dass Fehlerfreiheit dadurch garantiert wird, dass nichts implementiert wird, was nicht auch getestet wird. Werden Testfälle erst nach dem Code entwickelt, so besteht die Gefahr, einen Testfall zu übersehen. Wenn dagegen die Testfälle bestimmen, was implementiert wird, sind sie per Definition vollständig.

Mittlerweile existieren JUnit-ähnliche Frameworks auch für viele andere Programmiersprachen. Für dieses Projekt ist Junit Version 4 im Einsatz. Mit Hilfe von Eclipse kann man diese Tests sehr leicht in den Implementierungsverlauf mit integrieren.

Es gibt folgende TestCases für dieses Projekt:

- CryptTest
- CryptTestAES
- CryptTestPBE
- CryptTestRSA

CryptTest ist einen allgemeinen Test Case für automatisches Testen von dem Package Schnittstellen und beinhaltet Test Methoden:

testGetInstance – überprüft eine Instantiierung von der Crypt Klasse.

testValidate – Testfall für die Zertifikaten Validieren gegen das Root Zertifikat.

testgetAlgorhythm – Testfall um eine laufende Strategie zu befragen.

testsetAlgorhythm – Festfall überprüft das setzen von einer Strategie.

testgetExpireDate – überprüft das Verfallsdatum von einem Zertifikat.

Weitere Test Cases sind sehr endlich vom Inhalt. Es wird eine Strategie für Verschlüsselungsverfahren ausgewählt und getestet.

testDecryptString – Testfall für das Decodieren einer String Variable.

testDecryptByteByteArray – überprüfen von Decodieren einer ByteArray.

testEncryptString – Testfall für String Verschlüsselung.

testEncryptByteByteArray – Testfall für Verschlüsselung von ByteArray.

Security und Privacy in RFID v.0.4

Javadoc

Alle Schnittstellen und interne Methoden werden mit Hilfe von Javadoc dokumentiert. Das sichert dem Code eine bessere Wartbarkeit in der Zukunft und erleichtert das Dokumentieren von API.

Javadoc ist ein Software-Dokumentationswerkzeug, das aus Java-Quelltexten automatisch HTML-Dokumentationsdateien erstellt. Javadoc wurde ebenso wie Java von Sun Microsystems entwickelt und ist seit Version 2 ein Bestandteil des Java Development Kits.

Die Dokumentation kann somit durch spezielle Kommentare im Quelltext erstellt werden. Dadurch können Beschreibungen für Interfaces, Klassen, Methoden und Felder über spezielle Doclet-Tags definiert werden.

Java ist eine objektorientierte Programmiersprache. Die Kapselung und das Geheimnisprinzip werden als zentrale Elemente objektorientierten Programmierens angesehen, insbesondere in Java. Daraus folgt, dass zur Verwendung eines Symbols, z.B. einer Klasse oder einer Methode, seine öffentliche Schnittstelle und seine Spezifikation herangezogen werden sollten. Sich vor der Verwendung Kenntnisse über die interne Funktionsweise zu verschaffen, verstößt gegen das Geheimnisprinzip und macht außerdem unter Umständen von Änderungen in der Implementierung abhängig. Daher ist es notwendig, die Schnittstelle zu spezifizieren und dokumentieren. Das ist das Haupteinsatzgebiet von Javadoc.

Java Entwurfsmuster

Ein Entwurfsmuster (engl. design pattern) beschreibt eine bewährte Schablone für ein Entwurfsproblem. Es stellt damit eine wiederverwendbare Vorlage zur Problemlösung dar. Entstanden ist der Ausdruck in der Architektur, von der er für die Softwareentwicklung übernommen wurde. In den letzten Jahren hat der Ansatz der Entwurfsmuster auch zunehmendes Interesse im Bereich der Mensch-Computer-Interaktion gefunden. Aber auch in nicht-informatischen Bereichen findet diese Idee immer mehr Eingang.

Ein gutes Muster sollte

- ein oder mehrere Probleme lösen,
- ein erprobtes Konzept bieten,
- über das rein Offensichtliche hinausgehen,
- den Benutzer in den Entwurfsprozess einbinden,
- Beziehungen aufzeigen, die tiefer gehende Strukturen und Mechanismen eines Systems umfassen.

Entwurfsmuster beinhalten Referenzen auf andere Muster. Mithilfe dieser ist es möglich, Mustersprachen zu entwickeln.

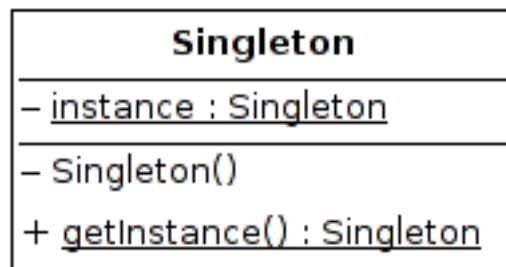
Singleton Entwurfsmuster

Das Einzelstück (engl. Singleton) ist ein in der Softwareentwicklung eingesetztes Entwurfsmuster und gehört zur Kategorie der Erzeugungsmuster (engl. Creational Patterns). Es verhindert, dass von einer Klasse mehr als ein Objekt erzeugt werden

Erstellt von Kulyk Nazar

Security und Privacy in RFID v.0.4

kann. Dieses Einzelstück ist darüber hinaus üblicherweise global verfügbar. Das Muster ist eines der von der so genannten Viererbande (GoF) publizierten Muster.



```
public class Crypt implements ICrypt {  
    /**  
     * Privates Klassenattribut,  
     * wird beim erstmaligen Gebrauch (nicht beim Laden) der Klasse erzeugt  
     */  
    private static final Crypt instance = new Crypt();  
  
    /** Konstruktor ist privat, darf nicht von außen instantiiert werden. */  
    private Crypt() {}  
  
    /**  
     * Statische Methode "getInstance()" liefert die einzige Instanz der Klasse zurück.  
     */  
    public static Crypt getInstance() {  
        if(!ready)  
            return null;  
        return instance;  
    }  
}
```

Ausschnitt aus der Crypt Klasse (Crypt.java)

Strategie Entwurfsmuster

Strategy ist ein Entwurfsmuster aus dem Bereich der Softwareentwicklung und gehört zu der Kategorie der Verhaltensmuster (Behavioural Patterns). Das Muster definiert eine Familie austauschbarer Algorithmen.

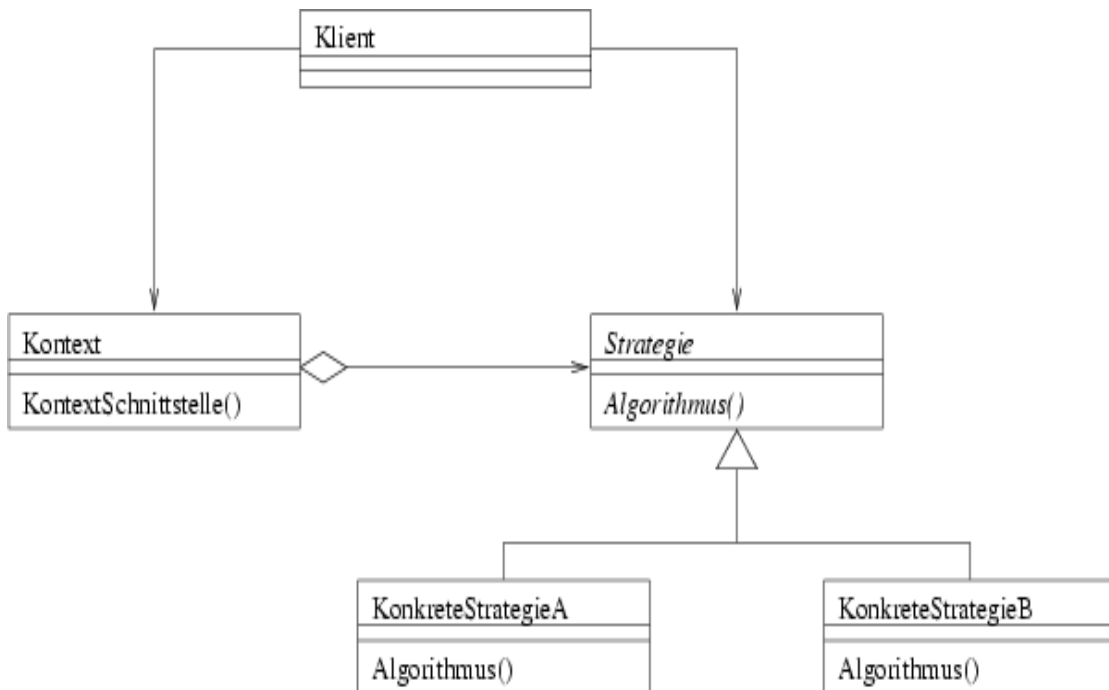
Security und Privacy in RFID v.0.4

Strategie-Objekte werden ähnlich wie Klassenbibliotheken verwendet. Im Gegensatz dazu handelt es sich jedoch nicht um externe Programmteile, die als ein Toolkit genutzt werden können, sondern um integrale Bestandteile des eigentlichen Programms, die deshalb als eigene Objekte definiert wurden, damit sie durch andere Algorithmen ausgetauscht werden können.

Meistens wird eine Strategie durch Klassen umgesetzt, die eine bestimmte Schnittstelle implementieren. In Sprachen wie Smalltalk, in denen auch der Programmcode selbst in Objekten abgelegt werden kann, kann eine Strategie aber auch durch solche Code-Objekte realisiert werden.

Die Verwendung von Strategien bieten sich an, wenn

- viele verwandte Klassen sich nur in ihrem Verhalten unterscheiden.
- unterschiedliche (austauschbare) Varianten eines Algorithmus benötigt werden.
- Daten innerhalb eines Algorithmus vor Klienten verborgen werden sollen.
- verschiedene Verhaltensweisen innerhalb einer Klasse fest integriert sind (meist über Mehrfachverzweigungen) aber
 - die verwendeten Algorithmen wiederverwendet werden sollen bzw
 - die Klasse flexibler gestaltet werden soll.



Wir haben 3 unterschiedliche Strategien zu Verschlüsselung Algorithmus Auswahl in diesem Projekt - RSA, AES und PBE. Die Implementierungsklasse Crypt die implementiert ICrypt Interface ist in unserem Fall das Kontext der beschreibt die Schnittstellen. RFID Device Handler ist ein Klient.

Entwicklung einer Web Anwendung für die Verwaltung von Zertificaten

Für die schnelle Entwicklung einer Web Anwendung kann man sich einen Applikation Server zu Hilfe nehmen. Ich habe eine eigene Implementierung von Applikation Server der sich basiert auf Apache mit PHP als Sprache für diese Aufgabe ausgewählt.

Security und Privacy in RFID v.0.4

Für Verwendung von SSL Zertifikaten bietet PHP sehr viele Möglichkeiten. Es ist auch sehr gut dokumentiert und leicht zu verwenden. Hier ist ein kleiner Überblick über die Methoden die PHP für SSL anbietet:

- `openssl_csr_new` erzeugt einen neuen CSR (Zertifikatssignierungsanfrage) basierend auf den Informationen, die mit dem Parameter `dn` angegeben werden. Dieser bestimmt den Distinguished Name, der im Zertifikat benutzt werden soll.

`privkey` sollte auf einen privaten Schlüssel zeigen, der vorher mit `openssl_pkey_new()` erzeugt wurde (oder den Sie auf andere Weise von der Familie der `openssl_pkey` Funktionen erhalten haben). Der entsprechende öffentliche Teil des Schlüssels wird benutzt um den CSR zu signieren.

`extraattribs` können Sie benutzen um zusätzliche Konfigurationsoptionen für den CSR anzugeben. Sowohl `dn` als auch `extraattribs` sind assoziative Arrays, deren Schlüssel zu OIDs konvertiert und auf den relevanten Teil der Anfrage angewendet werden.

- `openssl_pkey_new` erzeugt ein neues privates und öffentliches Schlüsselpaar.
- `openssl_pkey_export` exportiert `key` als eine PEM kodierte Zeichenkette und speichert diese in `out` (welcher per Referenz übergeben wird). Der Schlüssel kann optional mit einer Passphrase geschützt werden.
- `openssl_x509_export` speichert das x509 Zertifikat in einem PEM kodierten Format in der Zeichenkette `output`. Der optionale Parameter `notext` beeinflusst den Umfang der Ausgabe; ist dieser auf `FALSE` gesetzt werden zusätzliche, für Menschen lesbare, Informationen in der Datei mit ausgegeben. Der Standardwert von `notext` ist `TRUE`.
- `openssl_csr_export` exportiert die mit dem Parameter `csr` angegebene Zertifikatssignierungsanfrage und speichert diese als ASCII-armierten Text in `out`, der per Referenz übergeben wird. Der optionale Parameter `notext` beeinflusst den Umfang der Ausgabe; ist dieser auf `FALSE` gesetzt werden zusätzliche, für Menschen lesbare, Informationen in der Datei mit ausgegeben. Der Standardwert von `notext` ist `TRUE`.
- `openssl_get_publickey` extrahiert den Öffentlichen Schlüssel aus Zertifikate und bereitet ihn für den Gebrauch durch andere Funktionen vor.

```
<?php
// Angabe der Daten für den distinguished name, der in
dem
// Zertifikat benutzt wird. Sie müssen die Werte dieser
Schlüssel
// so anpassen, dass diese ihrem Namen und Firma
entsprechen, oder
// um präziser zu sein, den Namen und die Firma der
Person/Seite
// angeben, für die Sie das Zertifikat erzeugen.
```

Security und Privacy in RFID v.0.4

```
// Für SSL Zertifikate entspricht der commonName
gewöhnlich dem
// Domainnamen, für den das Zertifikat benutzt werden
soll, aber
// bei S/MIME Zertifikaten entspricht der commonName dem
Namen der
// Person, die das Zertifikat nutzen möchte.
$dn = array(
    "countryName" => "UK",
    "stateOrProvinceName" => "Somerset",
    "localityName" => "Glastonbury",
    "organizationName" => "The Brain Room Limited",
    "organizationalUnitName" => "PHP Documentation
Team",
    "commonName" => "Wez Furlong",
    "emailAddress" => "wez@example.com"
);

// Erzeugen eines neuen privaten (und öffentlichen)
Schlüsselpaare
$privkey = openssl_pkey_new();

// Erzeugen einer Zertifikatssignierungsanfrage
$csr = openssl_csr_new($dn, $privkey);

// Gewöhnlicherweise möchten Sie zu diesem Zeitpunkt ein
// selbstsigniertes Zertifikat erzeugen, das Sie
benutzten
// können, bis ihre CA ihre Anfrage im positiven Sinne
bearbeitet
// hat.
// Erzeugen eines selbst signierten Zertifikats, das für
die Dauer
// von 365 Tagen gültig ist.
$sscert = openssl_csr_sign($csr, null, $privkey, 365);

// Jetzt möchten Sie ihren privaten Schlüssel, ihren CSR
und das
// selbstsignierte Zertifikat sichern.
openssl_csr_export($csr, $csrout) and
var_dump($csrout);;
openssl_x509_export($sscert, $certout) and
var_dump($certout);
openssl_pkey_export($privkey, $pkeyout, "mypassword")
and var_dump($pkeyout);

// Anzeigen der möglichen aufgetretenen Fehler
```

Security und Privacy in RFID v.0.4

```
while (($e = openssl_error_string()) !== false) {  
    echo $e . "\n";  
}  
?>
```

Beispiel für eine Verwendung von OpenSSL Integration in PHP

Alle weiteren funktionalen Teile so wie Benutzer Authentifizierung und Verwaltung, Rollen Zugriff, Templates, Daten Bank Aufrufe der Web Anwendung würden dem Applikation Server Framework überlassen.

Security und Privacy in RFID v.0.4

6. Zusammenfassung

7. Übersicht

7.1 Bewertung von Stärken und Schwächen von dem Produkt

7.2 Einsatzgebiete

8. Ausblick

9. Quellenverzeichnis

10. Anhänge

11. Glossar

EEPROM Electric Erasable and Programmable Read Only Memory

EMV Elektro-Magnetische Verträglichkeit

FRAM Ferroelectric Random Access Memory

HF High Frequency (3 ... 30MHz)

PII Personally Identifiable Information

RFID Radio Frequency Identification