der Bundeswehr
Universität München
FAKULTÄT FÜR INFORMATIK

Von der Sicherheit elektronischer Dokumente bis zu digitalen Identitäten

Prof. Gabi Dreo
Dr. Udo Helmbrecht

Volker Eiseler
Frank Eyermann
Matthias Göhner
Iris Hochstatter
Andreas Matheus

(Hrsg.)

Institut für Informationstechnische Systeme, IIS

Bericht 2008-01
Februar 2008

Werner-Heisenberg-Weg 39 • 85577 Neubiberg • Germany

Inhalt

Das Internet bietet heute den Menschen einen globalen elektronischen Kommunikationsraum, der dem Waren-, Dienstleistungs- und Wissensaustausch an virtuellen Orten dient. Behörden, Unternehmen und private Haushalte sind zum großen Teil mit entsprechender Technologie ausgestattet. Einkäufe, Geschäfte mit Banken oder Versicherungen, Diskussionen zu verschiedensten Themen werden zunehmend durch einen virtuellen Besuch in Online-Shops, beim Online-Banking oder in Online-Foren getätigt. Mit dieser Verlagerung von Transaktionen in den virtuellen Raum steigen dort die Bedrohungen zum Beispiel durch Phishing, Identitätsdiebstahl und weitere Formen der Cyber-Kriminalität. Das Bedürfnis nach Sicherheit steigt, doch bisher verfügbare Identifizierungs- und Signaturmechanismen erreichen aufgrund vergleichsweiser komplexer Handhabung und hohen Kosten keine hinreichende Marktdurchdringung. Bei der Dokumentensicherheit ergeben sich durch neue technische Entwicklungen wie die kontaktlose Chiptechnologie und biometrische Verfahren neue Möglichkeiten, das Sicherheitsniveau von Dokumenten anzuheben. Ein sehr erfolgreiches Beispiel für die Anwendung digitaler Sicherheitsmerkmale auf Basis von Biometrie und RFID-Technologie stellt der elektronische Reisepass (ePass) dar, dessen Sicherheitsarchiktektur auch in die Konzeption des künftigen deutschen elektronischen Personalausweises einfliessen soll. Zudem soll dieser Ausweis mit einer optionalen Signaturfunktion ausgestattet sein, Die Sicherheit digitaler Informationen und der Schutz digitaler Identitäten bilden heute große Herausforderungen an die IT-Sicherheit. Diese reichen von der Authentizität digitalisierter Schriftstücke bis zu digitalen Sicherheitsmerkmalen in Reisedokumenten.

Ausgehend von den technischen Möglichkeiten, wie der RFID-Technologie und den biometrischen Authentisierungsverfahren, diskutierte das Seminar "Von der Sicherheit elektronischer Dokumente bis zu digitalen Identitäten" am Institut für Informationstechnische Systeme (IIS) der Universität der Bundeswehr München die Sicherheitsfragen aktueller Anwendungen wie dem elektronischen Reisepass (ePass) und Gesundheitskarte (eGK) und gibt dabei auch einen Ausblick auf zukünftige Entwicklungen des Pervasive Computing.

Dr. Udo Helmbrecht
München, im Februar 2008

Inhaltsverzeichnis

Kapitel 1

RFID — Technische Grundlagen und Sicherheitsaspekte

Florian Sesser, TU München

Moderne elektronische Identifikation beruht oft auf Radio Frequency Identification, kurz RFID. Seit einigen Jahren ist diese junge Technologie auch außerhalb von Lieferketten und Fertigungsstraßen im Einsatz: Elektronische Wegfahrsperren, seit über zehn Jahren in Neuwagen serienmäßig enthalten, funktionieren mit Hilfe der Funk-Chips. Neue Brisanz hat das Thema aufgrund der seit November 2005 ausgestellten Reisepässe erhalten, die ebenfalls einen sogenannten Tag zur automatischen Identifikation enthalten. Stetig fallende Preise und die inzwischen nachgeholte Standardisierung fördern die weitere Verbreitung.

Oft hört man von RFID auch im Kontext der Diskussion um den „Gläsernen Bürger", dessen Konsumverhalten und Bewegungsprofil aufgezeichnet und auf ewig gespeichert wird. Dabei stehen nicht nur Datenschutz- und Bürgerrechtsgruppen der RFID-Technik skeptisch gegenüber. Unternehmen wollen sicherstellen dass Betriebsgeheimnisse auch wirklich geheim bleiben. Die Sicherheit dieser Informationssysteme ist eine also kritische Voraussetzung für deren erfolgreichen Einsatz.

Um auf dieses Problem eingehen zu können, werde ich im folgenden die technischen Grundlagen der Radio Frequency Identification erläutern, einige prominente Anwendungsszenarien vorstellen und im Anschluss daran potentielle Sicherheitsrisiken und passende Gegenmaßnahmen aufzeigen.

Inhaltsverzeichnis

1.1 Einleitung

1.1.1 RFID - Definition

RFID – Radio Frequency IDentification – ist eine relativ junge Technologie für die automatische Identifikation. Andere Technologien in diesem Feld sind zB. Barcode-Systeme, Optical Character Recognition (OCR) sowie Chipkarten [4]. Ähnlich wie Barcode-Systeme kann die RFID-Technik helfen, die reale Welt im Computer besser abzubilden. Deshalb ist im Zusammenhang mit RFID auch immer wieder das Schlagwort „Internet der Dinge“ zu hören. Der große Vorteil von RFID besteht in der Funkübertragung der Daten: Es ist keine Sichtverbindung notwendig, auch größere Distanzen können überwunden werden, und es findet praktisch keine Abnutzung statt.

Ein RFID-System besteht aus einem Lesegerät, auch Reader oder Transmitter genannt, und einem Transponder, auch „Tag“ oder „Chip“.

Das Lesegerät enthält meistens einen Computer sowie eine Anbindung an ein Back-End-System, d.h. eine Datenbank, die Information über die mit RFID-Tags bestückten Objekte enthält. Der Transponder sendet seine Daten nur dann, wenn er vom Lesegerät dazu aufgefordert wird (sogenenntes Senden „on call“).

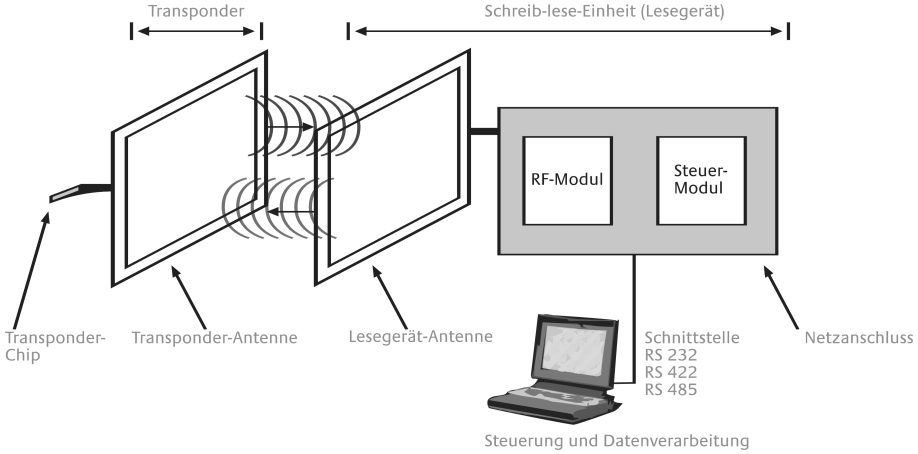

Abbildung 1.1: RFID-System, bestehend aus Transponder und Lesegerät [2]

Das Tag kann im Vergleich zum Lesegerät sehr klein sein, und besteht meistens einfach aus einer Antenne und dem eigentlichen RFID-Chip, aufgebracht z.B. auf einem Aufkleber. Die Chips werden laufend weiterentwickelt: In raschem Tempo wird auf immer weniger Raum – typischerweise weniger als einem Quadratmillimeter – immer mehr Information gespeichert. Seit einigen Jahren sind auch RFID-Tags mit passiver Stromversorgung erhältlich, die eigene Logik enthalten, was z.B. starke Kryptographie ermöglicht.

1.1.2 Kurze Geschichte der RFID-Technik

- Anfänge ca. 1970 (Diebstahlsicherung)
- 1980, 1990 Industrieller Einsatz (z.B. auf Fertigungsstraßen)
- ab 2000: Logik auf den Chips

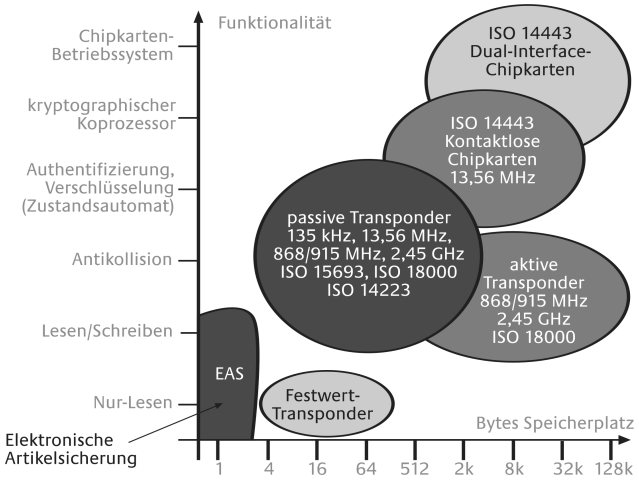

Abbildung 1.2: Klassifizierung unterschiedlicher RFID-Chips nach Fähigkeiten [4]

Die einfachste denkbare RFID Implementierung, die schon seit rund 40 Jahren existiert, sind die zur Diebstahlsicherung eingesetzten „1-Bit-Transponder“ (EAS - Elektronische Artikelsicherung). Derartige Systeme sind inzwischen in allen Kaufhäusern im Einsatz. Die Transponder werden an der Kasse deaktiviert. Das System schlägt Alarm, falls es einen aktiven Tag im Feld Lesegeräts feststellt.

Eine Entwicklungsstufe darüber stehen die Tags, die auf Abfrage eine Seriennummer zurücksenden. Solche RFID-Tags sind am ehesten mit Barcode-Aufklebern vergleichbar und befinden sich seit den späten Achtzigern im Einsatz. Diese Transponder-Bauart ist nach wie vor wohl die verbreitetste: Man bedenke, dass in einem geschlossenen System wie einer Fabrik oder einer Warenlieferungskette alle nötige Information in Datenbanken im Back-End-System gespeichert wird. Große Speicher auf den Tags sind also nicht notwendig, was natürlich auch die Kosten für die einzelnen Transponder minimiert.

Seit der Jahrtausendwende finden Chips, die über große Speicher und sogar Mikroprozessoren verfügen, durch den speziell hier schnell voranschreitenden Preisverfall zunehmende Verbreitung. Solche Tags werden z.B. dann eingesetzt, wenn Daten nicht zentral in einem Back-End-System gespeichert werden sollen oder können, oder wenn besondere Sicherheitsanforderungen herrschen und RFID-Technik einen Teil der Lösung dieser Anforderungen darstellt. Ein gutes Beispiel sind hier die neuen elektronischen Reisepässe. Die schon seit fast einer Dekade existierende Geldkarte wäre wohl das Paradebeispiel, allerdings überträgt sie ihre Daten nicht über Funk. Schlüsselkarten zur Gebäudesicherung wurden bisher auch als einfachere Speicherkarten hergestellt, was einige Sicherheitsrisiken birgt. Hier wird deshalb zunehmend auf „intelligentere“ Kartentypen gesetzt.

1.2 Technische Grundlagen

Zunächst sollen die technischen Grundlagen dieser neuen Technologie erläutert werden. Nach einem kurzen Ausblick in die zugrunde liegende Physik wird schematisch auf die Technik von RFID-Lesegeräten und -Sendern eingegangen. Eine erschöpfende Behandlung der Thematik wie auch eine Marktumschau ist im Rahmen dieser Arbeit leider nicht möglich. Ich möchte daher auf die weiterführende Literatur, besonders auf das Standardwerk im deutschen Sprachraum, dem RFID-Handbuch von Klaus Finkenzeller [4], verweisen.

1.2.1 Physik: Entstehung elektromagnetischer Wellen

Legt man an einen Dipol[1] eine Wechselspannung an, so entsteht ein alternierendes magnetisches Feld. Dieses magnetische Feld induziert ein elektrisches Feld mit in sich geschlossenen Feldlinien (ein sog. *Wirbelfeld*, siehe Abbildung 1.3d sowie 1.3e) [4].

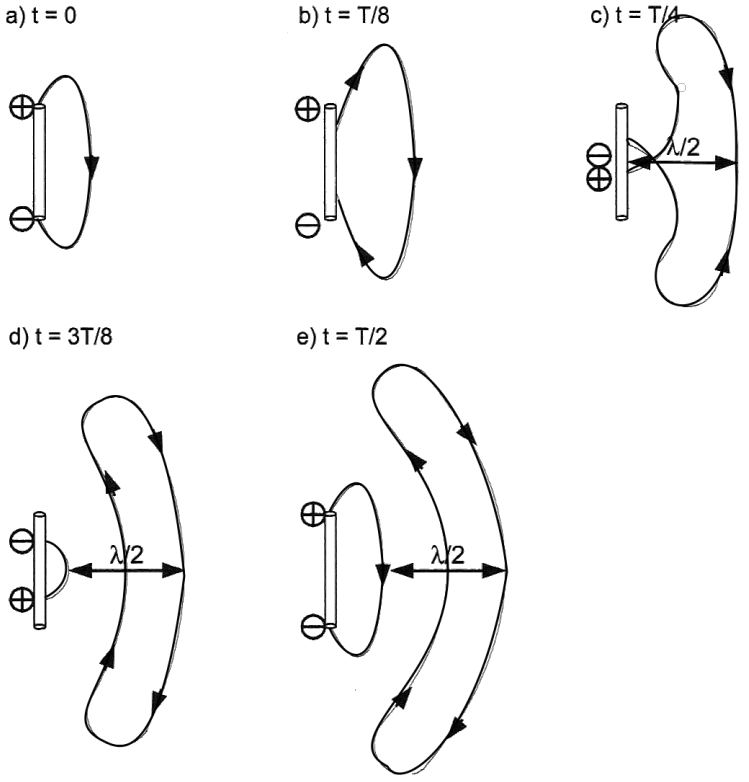

Abbildung 1.3: Entstehung elektomagnetischer Wellen [4]

Wechselt die Polarität am Dipol (Abbildung 1.3c, sog. *Nulldurchgang*), so stößt der Dipol das bisherige Feld in die Ferne (Abbildung 1.3d). Die Feldlinien im Raum schließen dabei durch Bildung abgeschlossener Wirbel in sich selbst (Abbildung 1.3d sowie 1.3e) [4].

Der Grund für die Entstehung elektromagnetischer Wellen aus dem Feld ist die endliche Ausbreitungsgeschwindigkeit[2] des Feldes: Der Änderung der Spannung an der Antenne

[1] Die Antenne unseres Systems

[2] $c \approx 300.000\ km/s$; Lichtgeschwindigkeit

kann das Feld im Raum nicht verzögerungsfrei folgen. Die folgende Halbwelle drängt wegen ihrer umgekehrten Polarität den bereits vorhandenen Wirbel vom Strahler fort [4].

Das elektrische Feld ist an das magnetische gekoppelt und steht (in jeder Dimension) senkrecht auf diesem. Eine sehr anschauliche Erklärung dieses Sachverhaltes findet sich auf der Website von Dr. Michael Komma in seinem Artikel zum Hertzschen Dipol [5].

Das magnetische Feld beginnt unmittelbar an der Antenne. Bei dessen Ausbreitung bildet sich durch Induktion zunehmend auch ein elektrisches Feld aus, so dass das ursprünglich rein magnetische Feld in ein elektromagnetisches Feld übergeht. In der Entfernung $\lambda/2\pi$ beginnt sich das elektromagnetische Feld von der Antenne abzulösen und als Welle durch den Raum zu wandern[3]. Der Bereich bis zur Ablösung der elektromagnetischen Welle wird als *Nahfeld*, der Bereich darüber hinaus als *Fernfeld* bezeichnet [4].

Im Fernfeld kann keine *transformatorische (induktive) Kopplung* mehr stattfinden [4]. Für RFID-Tags, die vom Lesegerät mit Strom versorgt werden, stellt das Nahfeld also eine unüberschreitbare Reichweitengrenze dar [4]. Tabelle 1.1 enthält grobe Richtwerte für die Reichweite des Nahfelds bei unterschiedlichen, oft genutzten Frequenzen.

Frequenz	Wellenlänge	Nahfeld
$<$ 135 kHz (LF)	$>$ 2222 m	$>$ 353 m
13,56 Mhz (HF)	22,1 m	3,5 m
868 MHz (UHF)	0,35 m	0,06 m
2,45 GHz (MW)	0,12 m	0,02 m

Tabelle 1.1: Wellenlänge λ und Nahfeld $\lambda/2\pi$ für Frequenzen f, nach [3]

Die Reichweite von Funkwellen wird noch durch eine Vielzahl weiterer Faktoren begrenzt. An erster Stelle zu nennen sind hier sicher Reflexion und Absorption. Des weiteren nimmt die Strahlungsleistung polynomiell ab (bei isotropen Strahlern[4] quadratisch), was für die Rückstrahlungsleistung bei den weit verbreiteten Backscatter-Systemen[5] eine Leistungsabnahme um die vierte Wurzel bedeutet: Um die beim Lesegerät ankommende (d.h. vom Transponder zurückgestrahlte) Leistung zu verdoppeln, muss die Sendeleistung des Lesegerätes versechzehnfacht werden [4]. Weiterhin sind Polarisationsverluste und Interferenzen zu beachten. Eine eingehende Behandlung würde offensichtlich den Rahmen dieser Arbeit sprengen. Der interessierte Leser sei daher auf das RFID-Handbuch [4] verwiesen.

1.2.2 Lesegeräte (Transmitter)

Unter Lesegeräten (auch: Erfassungsgerät, Transmitter) sind bei RFID-Systemen stationäre oder mobile Geräte zu verstehen, die fast immer einen Computer beinhalten und über sog. *Middleware* mit einer Datenbank (dem *Back-End-System*) verknüpft sind (siehe Abbildung 1.1 auf Seite 7).

[3]Wellenlänge: $\lambda = c/f$; $c :=$ Lichtgeschwindigkeit; $f :=$ Frequenz

[4]Isotrop wir ein Strahler genannt, der in alle Richtungen gleich stark sendet.

[5]Backscatter: Wichtigste Art der Signalmodulation, mehr dazu in Kapitel 1.2.3 – Passive Tags.

Abbildung 1.4: Mobiler RFID-Reader von Gao Research Inc. [11]

Der irreführenden Namensgebung zum Trotz können Lesegeräte auf geeigneten Tags durchaus auch Daten schreiben. Die Erfassungsgeräte kontrollieren die Güte der Datenübermittlung und stellen bei passiven RFID-Tags deren Stromversorgung sicher. Je nach Anwendungszweck kann es sich um handliche, portable Geräte handeln, die ihrerseits via Funk (oft: WLAN) angebunden sind oder die von den Tags gesammelten Daten auf einem internen Speicher zwischenlagern (hier beispielhaft der PT850 von Gao Research Inc. in Abbildung 1.4). In Warenlieferungsketten oder Fertigungsstraßen werden die Lesegeräte oft als stationäre Kontrollpunkte an Fließbändern eingesetzt. Je nach Anwendungszweck ist es möglich, RFID-Systeme zu konzipieren, die auch über große Entfernung hinweg (1 km und darüber hinaus) oder bei hohen Geschwindigkeiten (z.B. Maut-Brücken auf amerikanischen Highways) noch zuverlässig funktionieren.

1.2.3 Tags (Transponder)

Die Tags (auch: Transponder, Label), die an jedem vom RFID-System zu erkennenden Objekt angebracht werden, sind aus der Sicht der *passiven Partei*, also den Konsumenten, Angestellten, etc. sicherlich von höherem Interesse als die Lesegeräte, die im Normalfall nur vom Betreiber des Systems (der *aktiven Partei*) genutzt werden.

Grundsätzlich werden RFID-Transponder nach ihrer Energieversorgung unterschieden: in passive, semi-aktive und aktive Tags.

Passive Tags

Mit Abstand die meiste Verbreitung finden passive RFID-Tags, die ihren Strombedarf komplett aus den elektromagnetischen Wellen des Lesegeräts decken. Gründe hierfür liegen

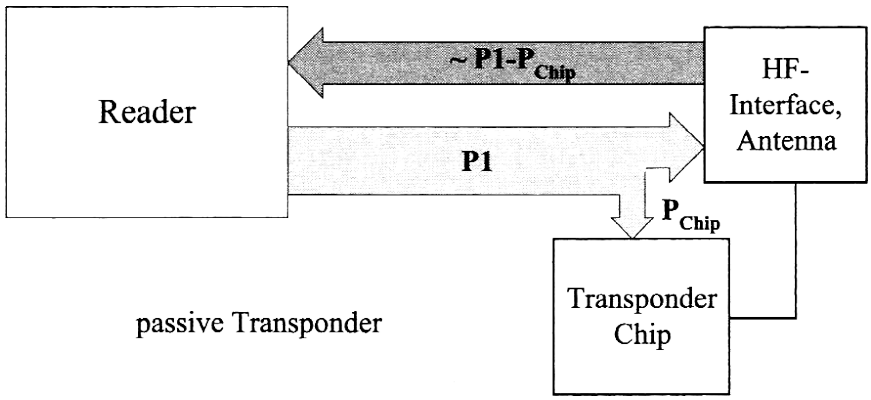

Abbildung 1.5: Modell: Passiver Transponder [4]

in der geringen Baugröße, die sie auch in Etiketten oder Dokumenten einsetzbar machen, sowie der kostengünstigen Herstellung.

Ein passiver Tag besteht im einfachsten Fall aus einem Dipol (die Antenne des Tags), einem Kondensator (der *Eingangskapazität* C_2), einem *Lastwiderstand* R_L sowie einer *Modulationsimpedanz* Z_{mod}. Außer der Antenne werden oft alle Bauteile auf dem Transponderchip vereint (siehe Abbildung 1.6, dargestellt durch das graue, umschließende Rechteck).

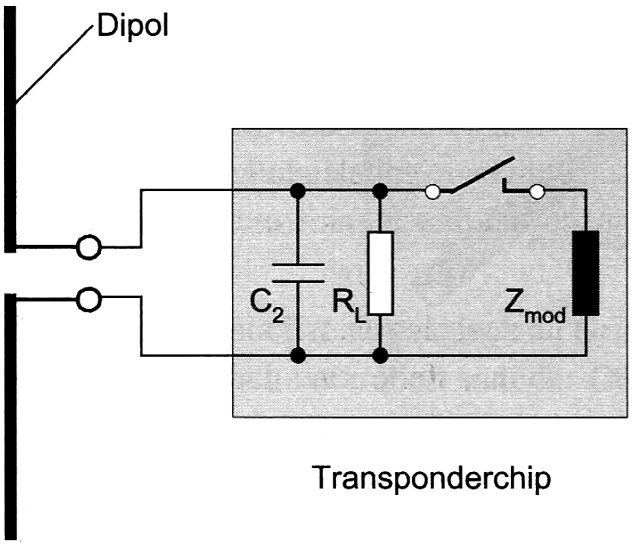

Abbildung 1.6: Ersatzschildbild eines passiven Mikrowellen-RFID-Tags [4]

Auf dem Ersatzschaltbild ist weiterhin ein Schalter zu sehen, der die Modulationsimpedanz Z_{mod} hinzuschaltet oder aus der Schaltung ausschließt. Dieser Schalter wird natürlich nicht von einem Menschen sondern vom RFID-Chip „betätigt“. Auf diese Weise verändert der RFID-Chip den Schwingkreis. Diese Veränderung kann vom Lesegerät erkannt werden. So überträgt der RFID-Transponder seine Daten zum Erfassungsgerät.

Ist Z_{mod} ein zusätzlicher Widerstand, kann der Chip die vom Lesegerät ankommenden elektromagnetischen Wellen entweder reflektieren oder absorbieren. Diese Art der *Modulation*

wird *Backscatter-Modulation*[6] (oder *Lastmodulation*, *Amplitudenmodulation*) genannt und ist in der RFID-Welt die verbreitetste Methode, Daten vom Tag zum Lesegerät zu senden.

Ist Z_{mod} ein Kondensator, so verstimmt der RFID-Chip den Schwingkreis. Die Daten (auch *Payload* genannt) werden dann auf sog. *Seitenbändern* übertragen. So funktioniert im RFID-Bereich *Frequenzmodulation*.

Für tiefere Einblicke in die Themen Modulation und Signalcodierung sei der interessierte Leser auf [4] verwiesen.

Stromversorgung passiver Tags

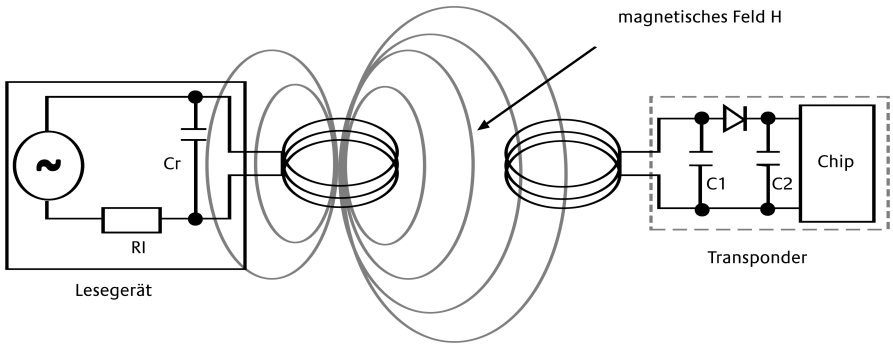

Abbildung 1.7: Energieversorgung passiver Transponder [4]

In nächster Nähe des Lesegeräts[7] ist das Magnetfeld noch ausreichend stark, um in der Antenne des Transponders einen für die Versorgung des RFID-Chips ausreichend starken Stromfluss zu induzieren. Dieser wird mit Hilfe eines Kondensators vom Transponder durch *Resonanzüberhöhung* noch verstärkt. Meist unter Zuhilfenahme einer Zener-Diode wird die induzierte Spannung im Transponder auf ein für den Betrieb des RFID-Chips geeignetes Maß begrenzt. Während man bei in Glas eingeschlossenen Ampullen-Tags diese einzelnen elektronischen Bauteile gut unterscheiden kann, sind sie wegen des geringeren Stromverbrauchs und um die Baugröße weiter zu reduzieren auch oft schon auf dem RFID-Chip selbst integriert.

Semi-Passive Tags

Die Reichweite passiver Tags lässt sich beträchtlich erhöhen, wenn der RFID-Chip seine Energie nicht aus dem elektromagnetischem Feld des Lesegeräts beziehen muss. Genau dies nutzt man bei semi-passiven[8] Transpondern aus.

Die semi-passiven Transponder ähneln technisch den rein passiven Tags sehr. Der einzige Unterschied ist die Stützbatterie, die den RFID-Chip mit Energie versorgt. Um die

[6] Backscatter (engl.): Wörtlich „Rückstreuung“. Wegen des Zurückstrahlens der vom Lesegerät empfangenen Wellen.

[7] In jedem Fall weniger als der Nahfeld-Radius, s.o.

[8] In der Literatur synonym verwandt: Semi-Aktiv

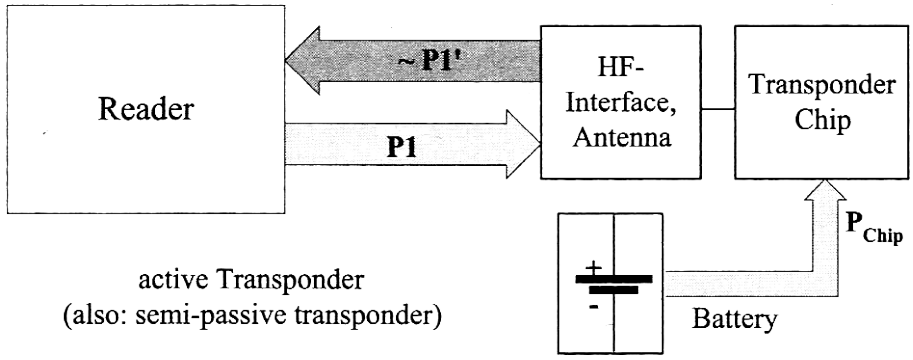

Abbildung 1.8: Modell: Semi-Passiver Transponder [4]

Batterie nicht unnötig zu belasten, wird sie nur hinzugezogen, wenn der RFID-Chip eine Anfrage von einem Lesegerät erhält.

Im gern genutzten Hochfrequenz-Bereich erhöht sich die Reichweite von typischerweise deutlich unter einem Meter auf einige Meter. Jedoch werden die Tags durch die zusätzliche Batterie und das nötige Gehäuse um ein vielfaches teurer.

Aktive Transponder

Aktive RFID-Transponder besitzen eine eigene Stromversorgung für den Chip wie auch für das Sende/Empfangsmodul. Sie können als eigenständige Funkgeräte angesehen werden. Als solche unterliegen sie keinen besonderen Einschränkungen was die mögliche Reichweite anbelangt, fallen aber recht groß aus und sind vor allem teuer.

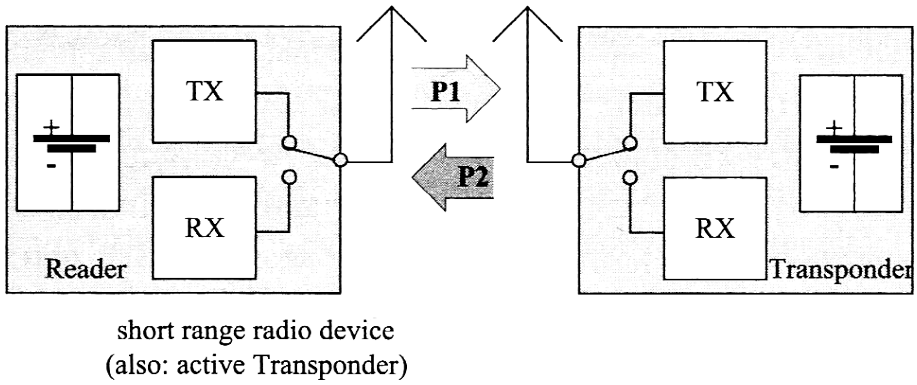

Abbildung 1.9: Modell: Aktiver Transponder [4]

Für manche Zwecke lohnen sie sich dennoch: Straßen- oder Brückenmaut ist zum Beispiel eine denkbares Szenario, indem die Kommunikation über RFID stattfinden kann, die Transponder hohe Sendeleistungen benötigen und der Stückpreis nicht so sehr ins Gewicht fällt, da er vom Kunden oder auch von der Kostenersparnis des Systems getragen wird.

1.3 Anwendungsbeispiele

Um eine Vorstellung zu entwickeln, wo und in welcher Form RFID heute zum Einsatz kommt, hier einige wenige, aber prominente Anwendungsbeispiele.

1.3.1 Handel und Logistik

Schon seit 40 Jahren befinden sich Systeme zur „elektronischen Artikelsicherung“ (EAS) im Einsatz, die schon ein mal – bei der geschichtlichen Betrachtung (Kapitel 1.1.2) – Erwähnung fanden: Simple „1-Bit-Tags“ werden beim Verlassen eines Kaufhauses von der Diebstahlsicherung detektiert, sofern sie nicht vom Kassenpersonal deaktiviert wurden.

Aktuelle RFID-Technik kann jedoch einiges mehr: Der weltweite Standard für Barcodes[9] kann zwei fünfstellige Zahlen[10] speichern und so die *Art* bzw. das *Modell* eines Artikels eines Herstellers festhalten. Auf einem RFID-Chip kann jedoch wesentlich mehr Information gespeichert werden, vor allem: die Seriennummer des Artikels. Das ermöglicht die Verfolgung eines Artikels von seiner Produktion an. Diese Entwicklung ist dabei, das Supply-Chain-Management[11] zu revolutionieren.

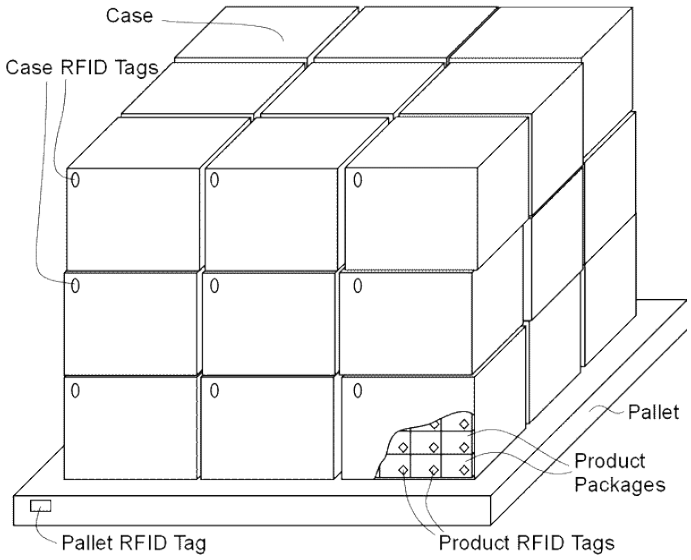

Abbildung 1.10: Unterschiedliche *Packaging Levels*. [12]

Abbildung 1.10 veranschaulicht die verschiedenen *Packaging Levels*, an denen RFID-Tags angebracht werden können. Die Einführung von RFID wird von den Unternehmen meistens schrittweise vollzogen: Erst werden nur die Paletten mit RFID-Tags versehen. Bisher war es immer ein großes Problem, Lieferungen zu überprüfen, die nicht als komplette Palette eingegangen sind. Wenn auch Kartons oder sogar einzelne Verpackungseinheiten mit

[9] EAN - European Article Number. Inzwischen auch ausserhalb Europa anerkanntes System zur Artikelidentifizierung.

[10] Plus zwei Ziffern für das Ursprungsland und eine Prüfziffer

[11] SCM - Das Management von Lieferketten

RFID-Tags gekennzeichnet werden, kann beim Eingang der Ware automatisch geprüft werden, wie viele Einheiten sich auf einer Palette befinden. Differenzen zum Lieferschein werden im Idealfall automatisch aufgedeckt.

Wal-Mart

Seit dem Jahr 2005 nimmt Wal-Mart von seinen 100 größten Zulieferern nur noch mit RFID-Tags bestückte Lieferungen entgegen. Diese Initiative wird von Wal-Mart konsequent fortgesetzt. Wal-Mart ist weltweit für 9 % des Einzelhandelsaufkommens verantwortlich [9], so dass bei der Ankündigung dieses Schrittes die Zulieferer regelrecht aufgerüttelt wurden. Der größte Kostenvorteil liegt für Wal-Mart in der wesentlich schnelleren Wiederbeschaffung vergriffener Artikel. Im Rahmen einer sechsmonatigen Studie wurde geschätzt, dass Wal-Mart durch diesen Schritt acht Mrd. USD jährlich sparen wird, sobald das Projekt komplett umgesetzt ist [9].

Department of Defense

Auch das Departement of Defense (DoD), das jährlich über ein Budget von 425 Mrd. USD verfügt, verlangt seit 2005 von seinen Zulieferern, wenigstens jede Palette mit einem RFID-Tag eindeutig zu unterscheiden. Laut Plan soll ab Januar 2007 jede Lieferung auf *Item*-Ebene mit RFID-Tags ausgestatt sein [9].

1.3.2 Identifikation und Authentifizierung

Auch in sicherheitskritischen Bereichen wird RFID eingesetzt. Der Unterschied zwischen Identifikation und Authentifizierung besteht darin, dass letzteres auch eine Prüfung[12] der Identität bedarf, nicht nur deren Feststellung.

Gebäudesicherung

Da RFID-Tags im Gegensatz zu kontaktbehafteten Chipkarten oder Magnetstreifenkarten kontaktlos arbeiten, sind sie (und vor allem die Lesegeräte!) wesentlich weniger von Abnutzung betroffen. Das sowie die Tatsache, dass die Karten praktisch zu benutzen sind (oft müssen sie nicht mal aus dem Geldbeutel genommen werden) spricht für die Eignung von RFID-Tags im Scheckkartenformat[13] als Zutrittskarten in Gebäuden. Da RFID-Zutrittskarten prinzipiell dem Risiko ausgesetzt sind, ohne das Wissen des Inhabers kopiert zu werden[14], müssen bei besonders hohen Sicherheitsanforderungen zusätzliche Zugangskontrollen (PIN etc.) eingesetzt werden. Ansonsten gelten die selben Vorteile, die auch

[12] Siehe dazu die *Three Factors of Security*, Kapitel 1.5.2
[13] ISO 7810 - Scheckkartenformat 85,60 mm · 53,98 mm
[14] sog. Cloning oder Skimming - Mehr dazu in Kapitel 1.4.

kontaktbehaftete elektronische Gebäudesicherungssysteme haben: Als verloren gemeldete Karten können schnell und einfach gesperrt und neu vergeben werden, der Zutritt zu Büros und Tagungsräumen kann, falls gewünscht, protokolliert werden, Zugangsberechtigungen zu neuen Bereichen können gegeben werden ohne den Schlüssel (d.h. die Karte) auszutauschen, um nur einige zu nennen.

Bezahlsysteme

Die vergleichsweise hohe Robustheit macht RFID-Systeme ideal für die bargeldlose Bezahlung. In vielen Kantinen und Cafeterias ist inzwischen die Zahlung per kontaktloser Wertkarte möglich. Die Wartezeiten an der Kasse verkürzen sich so auf ein Minimum. Speziell in größeren Betrieben, die typischerweise Ausweise an all ihre Angestellten ausgeben, ist es ein Leichtes, diese Karten so mit einem Zusatznutzen auszustatten.

Ein weiteres prominentes Beispiel ist das amerikanische Tunnel- und Brückenmautsystem *EZ-Pass*. Ein aktiver RFID-Tag wird im Inneren des Autos, normalerweise hinter die Windschutzscheibe, angebracht (siehe Abbildung 1.11. An Mautstellen gibt es eine oder mehrere Spuren, die Kunden mit EZ-Pass vorbehalten sind. Schon eine Zeitersparnis von einigen Minuten ist vor allem für Pendler Anreiz genug, sich einen solchen Transponder anzuschaffen. Die relativ hohen Kosten pro Transponder sind durch Zeitersparnis schnell wieder eingespart. Inzwischen ist das System in den meisten Bundesstaaten in den USA Standard [9].

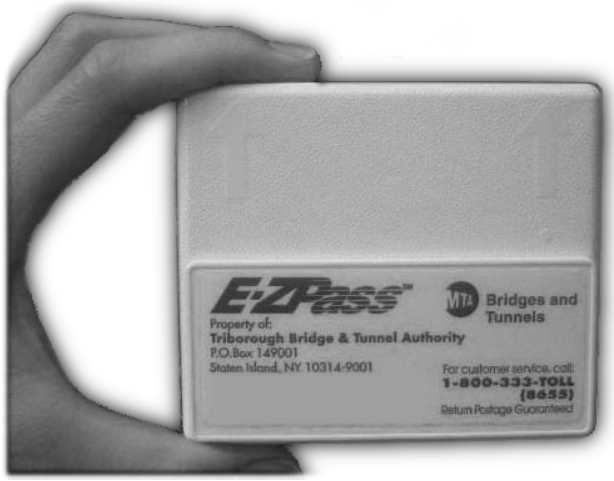

Abbildung 1.11: Aktiver Transponder der Firma EZ-Pass. [13]

Elektronische Wegfahrsperre

Die seit 1995 in praktisch jedem Neuwagen serienmäßig vorhandene *elektronische Wegfahrsperre* funktioniert mittels RFID: Im Plastikgehäuse des Schlüssels befindet sich ein RFID-Transponder, der von der Bordelektronik beim Versuch, den Motor zu starten, überprüft wird. Schlägt die Überprüfung fehl, so lässt sich der Wagen nicht starten. So tragen viele Menschen schon einen RFID-Tag mit sich herum, ohne davon zu wissen.

1.3.3 Ungewöhnliche Beispiele

Tieridentifikation

Die Verwaltung großer Herden in „modernen“ Aufzuchtbetrieben, aber auch das Risiko ansteckender Krankheiten oder die Gefahren durch Tierseuchen sind Gründe für den Einsatz von RFID in der Tieridentifikation. Für diesen Einsatzbereich existieren eine Reihe international anerkannter Standards[15].

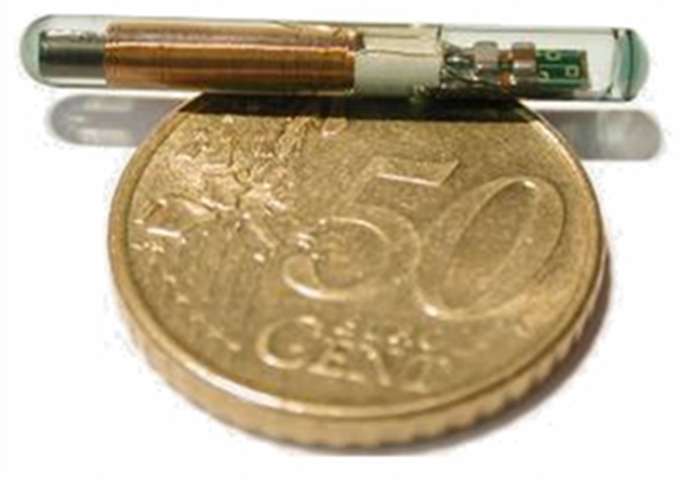

Abbildung 1.12: Glaszylinder zur Tieridentifikation. [14]

Für diesen Zweck geeignete Transponder sind normalerweise in sterile Glaszylinder eingegossen, und werden in das Fettgewebe der Tiere implantiert. In der Abbildung 1.12 zu sehen ist die Spule mit Ferritkern, die als Antenne dient (links im Bild) sowie der zur Resonanzerhöhung eingesetzte Kondensator und Lastwiderstand (rechts im Bild, die beiden Quader auf der Platine). Der RFID-Chip selbst ist nicht sichtbar.

Sportliche Veranstaltungen

Das sogenannte *Chip-Timing* erleichtert die faire Zeitmessung besonders bei großen Sportevents wie öffentlichen Marathonläufen unter Zuhilfenahme von RFID-Technik. Die Abbildung 1.13 zeigt einen in einen Kunststoffträger eingegossenen RFID-Transponder[16], der an den Schnürsenkeln von Laufschuhen oder wie hier an Klettverschlussbändern angebracht wird. Um eine hohe Zuverlässigkeit des Systems zu erreichen, ist es notwendig, dass die Lesegeräte entsprechend ausgelegt werden. Bei Marathonläufen geschieht das normalerweise, indem die Antennen des Erfassungsgerätes unter dünnen, am Boden liegenden Tartanmatten angebracht werden.

[15] ISO 11784, 11785 und 14223. Siehe [4].

[16] Der Transponder ähnelt dem aus Abb. 1.12 und steckt senkrecht in der Mitte des ChampionChips.

Abbildung 1.13: Transponder der Firma ChampionChip. [15]

1.4 Sicherheitsrisiken

Die voranschreitende Einführung von RFID-Technik wird von öffentlichen Protesten begleitet. Es heißt, RFID schaffe den gläsernen Kunden (respektive Bürger). So wird diese neue Technologie von vielen als ein massiver Eingriff in die eigene Privatsphäre angesehen. Die *Datensicherheit* lässt sich hier in zwei Kategorien einteilen: Einerseits steht die *Data Privacy* auf dem Spiel – „Wer darf was von mir wissen?“ Schwer zu schützen ist außerdem die *Location Privacy*, also die Information darüber, wo man sich gerade aufhält. Gegen den eigenen Willen eindeutig identifiziert werden zu können gibt vielen (zu Recht) ein ungutes Gefühl, und ruft Datenschutzverbände sowie Bürgerrechtler auf den Plan.

Abbildung 1.14: Lesegerät-Detektor des Datenschutzverbandes FoeBuD e.V. [16]

In Abbildung 1.14 ist eine Anstecknadel vom Datenschutzverband FoeBuD e.V. zu sehen. Sie dient gleichzeitig als Detektor für RFID-Lesegeräte.

Auch rein technisch gibt es bei der Sicherheit von RFID-Systemen einiges zu beachten. Der wichtigste Vorteil von RFID, die Übertragung der Daten per Funk, ist gleichzeitig ihr größtes Sicherheitsrisiko.

Einerseits ist die *Funktionssicherheit* von RFID stets bedroht: Durch Einsatz eines Störsenders oder das relativ leicht mögliche absichtliche Zerstören von Transpondern haben Saboteure leichtes Spiel.

Wenn ein Angreifer durch Manipulation des Systems, wie dem Einschleusen falscher Daten oder dem Vorspielen einer falschen Identität, einen Vorteil erlangen kann, muss vor allem bei öffentlich zugänglichen Systemen im Vorfeld sichergestellt werden, dass solche Angriffe nicht gelingen oder wenigstens leicht aufgedeckt und zurückverfolgt werden können. Die *Authentizität* der Daten muss sichergestellt werden.

In diesem Kapitel werden zuerst die der Technik innewohnenden Risiken erläutert und die Theorie durch greifbare Beispiele untermauert. Im Anschluss werden einige wirksame Gegenmaßnahmen beschrieben.

Abbildung 1.15 zeigt die grundsätzlichen Angriffsarten auf RFID-Systeme auf. Am wichtigsten ist hier sicherlich die Luftschnittstelle, die RFID von anderen *Auto-ID Systemen* unterscheidet.

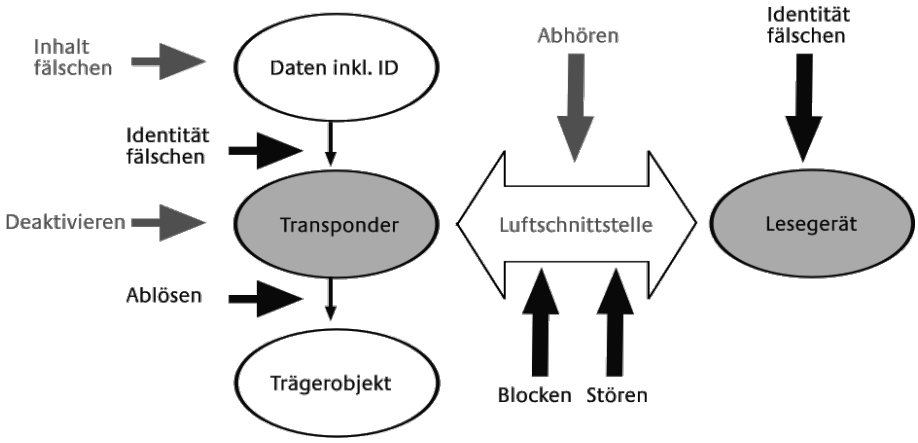

Abbildung 1.15: Grundsätzliche Angriffsarten auf RFID-Systeme. [2]

1.4.1 Denial of Service

Saboteure können RFID-Systeme aus unterschiedlicher Motivation heraus – sei das der Schutz ihrer Privatsphäre, unlauterer Wettbewerb oder ähnliches – in ihrer Funktion beeinträchtigen. Unter dem Sammelbegriff *Denial-Of-Service-Attacken (DoS)* werden alle Angriffe zusammengefasst, die auf die Störung der ordnungsgemäßen Funktion des Systems abzielen.

Einerseits können die der passiven Partei ausgehändigten Transponder durch unterschiedlichste Weise unbrauchbar gemacht werden. Starke Feldeinwirkung (wie das sogenannte „Toasten“ von RFID-Transpondern in einem Mikrowellenherd), mechanische Zerstörung (Durchtrennen der Antenne) oder bösartiges Ausnutzen des in vielen RFID-Tags vorhandenen Kill-Befehls[17] sind die gängigsten Beispiele.

[17]Funktion zum Deaktivieren des Transponders durch den Herausgeber. Laut Spezifikation nicht reversibel, meist nur durch ein einfaches Passwort geschützt.

Andererseits ist die Luftschnittstelle für DoS-Angriffe sehr verwundbar. Störsender oder sogenannte *Blocker-Tags*, die eine Vielzahl von im Feld befindlichen Tags vorspielen und das Lesegerät so temporär unbrauchbar machen, sind leicht zu beschaffen beziehungsweise sogar im Elektro-Fachhandel günstig zu erwerben.

1.4.2 Eavesdropping

Das *Abhören* der Kommunikation zwischen RFID-Transponder und -Erfassungsgerät wird im Fachjargon *Eavesdropping* genannt. Es ermöglicht dem Angreifer das heimliche Ausspähen von Information. Der Angreifer beteiligt sich (noch) nicht aktiv an der Kommunikation. Wichtig ist die Tatsache, dass das Abhören der Kommunikation mit entsprechend empfindlicher Sensorik auch bei RFID-Systemen mit geringer Reichweite weit über deren spezifizierte Betriebsdistanz hinaus möglich ist. Während ISO 14443-gerechte Transponder, wie sie zum Beispiel im elektronischen Reisepass zum Einsatz kommen, normalerweise nur eine Distanz von bis zu 10 cm überbrücken können, gelingt das Abhören der Kommunikation laut der amerikanischen Firma Flexilis über eine Distanz von mindestens 3 m [6]. Der Grund hierfür liegt im Unterschied zwischen der *Energiereichweite*, die beschreibt, bis zu welcher Entfernung passive Transponder genügend Strom für die ordnungsgemäße Funktion beziehen können, und der *Modulationsreichweite*, die die Ausbreitung der Funkwellen (dem *Backscatter-Rauschen*) beschreibt.

1.4.3 Scanning, Skimming, Cloning

Das unautorisierte (und unter Umständen auch unbemerkte) Auslesen, auch *Scanning* genannt, kann im Bereich der spezifizierten Reichweite eines RFID-Transponders von einem Angreifer einfach und mit günstiger Hardware durchgeführt werden. Darüber hinaus steigt der benötigte Aufwand wie auch die Kosten für den Angreifer sehr schnell an [4].

Scanning kann eine Vorstufe zum *Cloning* (Synonym: *Skimming*) sein: Sobald die Daten eines Transponders komplett ausgelesen sind, ist es leicht, diese auf einen leeren Transponder gleicher Bauart aufzuspielen. Der *Täuschung* des Systems durch Verwendung des kopierten Transponders steht nichts mehr im Wege. Bei Identifikationssystemen wird so Impersonifizierung möglich.

Hierzu ein warnendes Szenario: Es gilt, eine sich normalerweise in der Geldbörse befindliche Schlüsselkarte zu kopieren. In beengten Umgebungen, wie einem Fahrstuhl oder an einer Ampel, wird es einem Angreifer leicht fallen, nahe genug an sein Opfer heranzukommen (vor allem wenn er etwas vom *Social Engineering*, dem Ausnutzen sozialer Gegebenheiten, versteht). Zudem reicht es oft aus, nicht den Schlüssel vom Eigentümer der Firma, sondern z.B. den des Reinigungspersonals zu kopieren – das ja auch überall Zugang haben muss. Die Zeit, die ein Händedruck und ein wohlwollendes Kompliment für die gut geleistete Arbeit an den Hausmeister braucht, ist für einen böswilligen Angreifer mehr als ausreichend, um jede Schlüsselkarte zu auszulesen, die dieser mit sich führt – Es sei denn, diese Karten sind ausreichend geschützt[18].

[18] Zu möglichen Schutzmaßnahmen siehe Kapitel 1.5

1.4.4 Spoofing

Ähnlich dem Skimming bzw. Cloning kann *Spoofing* zur Impersonifikation genutzt werden. Der Unterschied besteht darin, dass nicht einfach ein valider Tag kopiert wird. Beim Spoofing werden eher vorhandene Daten modifiziert, um Fehlinformationen ins System einzuschleusen. Ansonsten ähnelt es den bereits beschriebenen Techniken.

1.4.5 Tracking, Hotlisting

Tracking beschreibt das örtliche Verfolgen von RFID-Transpondern. Durch eine derartige Kompromittierung der *Location Privacy* können zum Beispiel Bewegungsprofile erstellt werden.

Hotlisting unterscheidet sich im Zweck der Attacke: Ziel ist die Detektion eines oder mehrerer bestimmter, zuvor auf eine „schwarze Liste“ gesetzten Tags. Ein sehr plakatives, wenn auch überzogenes, Beispiel ist die Idee, schlecht geschützte elektronische Reisedokumente als Auslöser für „Anti-Amerikaner-Bomben“ oder „Anti-Christen-Bomben“ zu verwenden[7]. Eine bestimmte Produktgruppe am Ausgang eines Kaufhauses zu detektieren, und die Einkäufe so einer Rasterfahnung zu unterziehen, ist ein weiteres, weniger marktschreierisches Beispiel für Hotlisting, das trotzdem Aufhorchen lassen sollte.

1.4.6 Angriffe auf das Back-End

Schlecht geschützte RFID-Systeme sind noch anderen Attacken ausgesetzt. So hat Forscherin Melanie Rieback (Vrije Universiteit Amsterdam) einen RFID-Virus kreiert [8]. Der Virus befällt das Back-End-Datenbanksystem (hier: eine Oracle-Installation) beim Auslesen des Tags, und repliziert sich selbstständig. Große Systeme mit standardisierten Schnittstellen, wie z.B. die Gepäckabfertigung auf großen Flughäfen, sind anfällig für derartige Angriffe, und müssen entsprechend geschützt werden.

1.5 Sicherheitsmaßnahmen

Die gute Nachricht ist, dass man RFID-Systeme gegen die meisten dieser potentiellen Sicherheitslöcher schützen kann, wenn man in einem frühen Stadium der Implementierungs- oder noch besser der Planungsphase handelt.

1.5.1 Maßnahmen gegen genannte Risiken

Angriffe auf das Back-End können recht einfach eingegrenzt werden, indem man einige seit vielen Jahren aus der Softwareentwicklung bekannte Techniken wie *Input Sanitizing* und *Boundary Checking* einsetzt. In [8] wird beschrieben, wie man sich vor einem hypothetischen RFID-Virus schützen kann.

Spoofing kann durch das Einbeziehen der Seriennummern, die von Herstellern der RFID-Tags fest auf die Chips gebrannt werden, mit einfachen Mitteln stark erschwert werden. Das System gleicht den Inhalt eines Tags bei jedem Auslesen mit dem in der Back-End Datenbank gespeicherten Eintrag (und der Seriennummer des Tags) ab, und benachrichtigt gegebenenfalls den Betreiber des Systems. Die aktive Partei eines nicht-öffentlichen RFID-Systems sollte außerdem peinlich genau darauf achten, valide Tags, die nicht mehr gebraucht werden, zu zerstören (am besten durch eine sichere Methode, wie den dafür vorgesehenen *Kill-Befehl*). Objekte, die in der Datenbank nicht mehr existieren, sollten in der Realität also auch nicht mehr existieren. Generell wird empfohlen, die Konsistenz zwischen realer und virtueller Welt möglichst hoch zu halten.

Praktisch unmöglich gemacht wird Spoofing durch den Einsatz von *starker Kryptographie*, also durch das Verschlüsseln der Daten, die auf den Chip gebrannt werden. Die Achillesferse solch eines Systems: Die privaten Schlüssel müssen mit allen erdenklichen Mitteln geschützt werden. Sind sie ein mal kompromittiert (z.B. durch einen Mitarbeiter, der das System angreift) ist die Verschlüsselung wertlos geworden. Die Schlüssel können nicht einfach gewechselt werden, da sich viele Tags mit dem alten Schlüssel in Umlauf befinden.

Scanning, Cloning, Skimming Verschlüsselung der Daten schützt zwar gegen das Verändern der Daten auf dem Tag. Valide Tags können jedoch trotzdem noch kopiert werden[19], die Signatur des Systembetreibers bleibt dabei intakt. Das Abschirmen des Transponders durch entsprechende Schutzhüllen hilft der passiven Partei, zu überwachen, wann ein Tag ausgelesen werden kann.

Gegen das für das Cloning essentielle unentdeckte Auslesen kann ein System mithilfe von aktiver Authentifizierung geschützt werden. Ein Challenge-Response-Verfahren wie das „Three-Pass Mutual Authentication Protocol“ wird genutzt, um das Lesegerät gegenüber dem Tag sowie das Tag gegenüber dem Lesegerät zu authentifizieren. Erst dann kann der Inhalt des Tags gelesen werden. Im Gegensatz zur reinen Datenverschlüsselung erhöht dies jedoch die Komplexität des Tags. Es können keine einfachen Speicher-Chips mehr verwendet werden (preislich derzeit im Bereich 0,05 Euro bis 0,10 Euro). Je nach Verfahren werden Mikroprozessorchips, oft mit integriertem Zufallsgenerator, benötigt (die besseren liegen preislich im Bereich 2 - 20 Euro). Für weitere Information zu diesem Thema siehe [2].

Eavesdropping ist bei Tags, auf denen die Daten verschlüsselt gespeichert werden, prinzipiell kein Problem. Außerdem kann ein Systembetreiber durch bauliche Maßnahmen verhindern, dass die Datenübertragung aus großer Entfernung mitgelesen werden kann. Ein Faraday'scher Käfig um das Lesegerät oder Tapeten mit eingearbeiteter Metallfolie können hier helfen.

Tracking und Hotlisting ist technisch schwerer beizukommen als man zuerst meinen könnte. Das Problem besteht in den *Anti-Kollisions-IDs*, die Lesegeräten ermögli-

[19] Beispiel: Schlecht implementierte elektronische Reisepässe. Siehe [10].

chen, einen Tag von mehreren sich im Feld befindlichen auszuwählen und einzeln auszulesen[20]. Starke Authentifizierung und Verschlüsselung schützen hier also nicht, da die Anti-Kollisions-ID zu Beginn der Kommunikation bekannt sein muss. Was allerdings schützen kann, sind *abhörsichere* Anti-Kollisionsalgorithmen[21]. Diese erhöhen unter Umständen den Aufwand für den Betreiber des Systems. Einige der Verfahren benötigen auch einen Zufallsgenerator auf dem Transponder, was die Kosten stark erhöht. Zur weiteren Lektüre sei [2] empfohlen.

Denial of Service ist die Angriffsart, für die am schwersten ein pro-aktiver Schutz gefunden werden kann. Speziell bei einem großen RFID-System, das eine Vielzahl von Feinden hat[22], ist das sehr problematisch. Die einzig denkbare Abhilfe ist hier, sich auf die RFID-Technik nicht ausschließlich zu verlassen – was wie bei jeder Technologie empfohlen wird. Reisepässe sind auch ohne funktionierenden Chip gültig. Ein Klebeetikett, das auf der Rückseite einen RFID-Tag trägt, kann ohne weiteres auf der Vorderseite einen Barcode aufgedruckt bekommen. Dieser trägt die gleiche Information, kann jedoch nicht genauso praktisch und schnell ausgelesen werden[23]. Als *Fall-Back* kann sich solch eine Lösung aber schnell bezahlt machen.

1.5.2 Wichtig bei Authentifizierung

RFID-Systeme mit geringer Reichweite[24] sind an sich schon relativ sicher – kontaktbehaftete Chipkarten oder Schlüssel können schließlich auch gestohlen werden. Anstatt viel Geld für teure Prozessorchipkarten zu investieren, lohnt es sich bedeutend mehr, für die Absicherung kritischer Bereiche noch einen zweiten Weg zur Identifikation zu wählen, der die durch RFID gewonnene Identität absichern kann.

Three Factors of Security

Authentifizierung folgt normalerweise den „Three Factors of Security“ [9]. Geprüft wird:

- Der *Besitz* z.B. einer RFID Schlüsselkarte
- Das *Wissen* z.B. einer PIN oder eines Passworts
- Eine *physische Eigenschaft* einer Person (normalerweise durch Biometrie: Gesichtserkennung, Fingerabdruck, etc)

[20] Mehrere Tags gleichzeitig auszulesen funktioniert nicht, da sie auf der gleichen Frequenz arbeiten und sich die Signale gegenseitig stören würden.

[21] Zum Beispiel *Chained Hashes*, *Randomized Hash-Lock*, *Silent Tree Walking*.

[22] Wie z.B. den elektronischen Reisedokumenten.

[23] Für RFID-Tags mit großen Speicher ist das zwar keine Lösung. Diese werden aber auch eher selten benötigt.

[24] Wie *Close-Coupling* Systeme, Reichweite < 1 cm.

Gemeinsam sind diese Maßnahmen wesentlich sicherer als eine allein. Bei mangelhafter Implementierung oder Kompromittierung einer der Sicherheitsmaßnahmen kann eine andere den Schutz aufrecht erhalten.

1.6 Ausblick

RFID ist eine noch junge, vielversprechende Technik. Wenn sie mit Bedacht eingesetzt wird, bietet sie nicht nur der aktiven, sondern auch der passiven Partei Vorteile. Die fallenden Preise und die sich allmählich heraus kristallisierenden Standards weisen RFID eine gute Zukunft. Ich kann mich der Auffassung des BSI, dass diese Technik ein stetiges, kontinuierliches Wachstum erfahren wird, nur anschließen.

Abbildungen

Literaturverzeichnis

[1] Brewin, Bob. *No silver bullets – Initial DOD RFID hype gets tempered by reality*, Government Computer News (GCN, www.gcn.com) 2005.

[2] BSI - Bundesamt für Sicherheit in der Informationstechnik. *Risiken und Chancen des Einsatzes von RFID-Systemen*, SecuMedia Verlags-GmbH, Ingelheim 2004.

[3] BSI - Bundesamt für Sicherheit in der Informationstechnik. *RFID-Studie 2007 - Technologieintegrierte Datensicherheit bei RFID-Systemen*, Stand April 2007.

[4] Finkenzeller, Klaus. *RFID Handbuch*, Carl Hanser Verlag, München Wien 2006.

[5] Komma, Michael. *Hertzscher Dipol*.
http://www.mikomma.de/fh/eldy/hertz.html – 11. Januar 2008.

[6] Mahaffey, Kevin. *Passive RFID Security*, Juli 2005, BlackHat Conference.
http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-mahaffey.pdf – 13. Januar 2008.

[7] Miller, Paul. *Scaremongers dub RFID passports as potential bomb trigger*, Engadget, 18. August 2006.
http://www.engadget.com/2006/08/18/scaremongers-dub-rfid-passports-as-potential-bomb-trigger/ – 13. Januar 2008.

[8] Rieback, Melanie. *Is Your Cat Infected with a Computer Virus?*, Vrije Universiteit Amsterdam, Computer Systems Group, 2006.
http://www.rfidvirus.org/papers/percom.06.pdf – 13. Januar 2008.

[9] Thornton et al. *RFID Security - Protecting the Supply Chain*, Syngress Publishing Inc, Rockland 2006.

[10] Witteman, Marc. *Attacks on Digital Passports*, 28. Juli 2005, WhatTheHack Conference.
http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf – 13. Januar 2008.

Bildquellen

[11] *http://www.gaorfid.com/* – 11. Januar 2008.

[12] *http://www.jefflindsay.com/rfid3.shtml* – 11. Januar 2008.

[13] *http://www.kayo2u.tv/nyd/archives/cat_oieao.html* – 13. Januar 2008.

[14] *http://www.rotil.nl/communications/products/rfid.nl.php* – 13. Januar 2008.

[15] *http://www.vasaloppet.se/* – 13. Januar 2008.

[16] *http://www.foebud.de/* – 13. Januar 2008.

Kapitel 2

Biometrie

Elmostapha Miliki

Unter Biometrie versteht man die Messungen der Lebewesen und ihrer Eigenschaften. Je nach dem Anwendungsbereich gibt es unterschiedliche Definitionen des Wortes [2].
Dieses Kapitel beschäftigt sich mit biometrischen Erkennungsverfahren und einigen Ihrer vielfältigen Anwendungen im Zusammenhang mit IT Sicherheit. In diesem Bereich definiert man Biomertie als automatisierte Erkennung von Personen, basierend auf ihren biologischen Eigenschaften. Die Verbreitung und der Einsatz von Biomertie bringt wichtige sensible Daten mit sich, welche Verwaltung und Schutz braucht. Deshalb muss das passende System effizient, sicher und zuverlässig sein.
Dieses Kapitel behandelt biometrische Verfahren, ihre Anwendungen, mögliche Angriffe und Gegenmaßnahmen.

Inhaltsverzeichnis

2.1 Einleitung

Die Biometrie nimmt immer mehr Bedeutung ein. Sie spielt eine große Rolle in der Sicherheit, in dem biometrische Systeme sowohl zur Bekämpfung gegen Terrorismus und Verbrechen, die eine Gefahr für die Gesellschaft darstellen, als auch zur Ermöglichung der Zutrittskontrolle in mehrere Firmen und IT-Systeme eingesetzt wurden.

Außerdem können diese Systeme Identitäten speichern und aus einer oder mehrere Kombinationen von biometrischen Daten wird auf einer Person geschlossen[2].Diese Systeme haben die Grenze des lokalen Einsatz überschritten und können via Netzwerke verwaltet werden. Verschiedenste Gefahren müssen mit hilfe von IT-Sicherheitsmaßnahmen verhindert werden.

2.2 Geschichte

Seit langem haben sich Menschen durch unterschiedliche Methoden authentifiziert. Schon 2000 vor Christus kannte man in Ägypten die Unterschrift durch Fingerabdruck. Nach archäologischen Funden wurde schon bei den Assyrern der Fingerabdruck als eine Form der Identifikation eingesetzt. Die Tonvasen wurden mit dem Fingerabdruck des Töpfers gekennzeichnet. In der Tang-Dynastie (618 bis 906) wurden die ersten Fingerabdrücke verwendet, um Verträge zu authentifizieren. In dieser Zeit wurde bei den Pharaonen die Größe des Körpers einer Person zum Nachweis seiner Berechtigung verwendet.

Die ersten Vorschläge zur Nutzung des Fingerabdrucks in der Kriminalistik erfolgen im Jahr 1858. Im gleichen Jahr hat Sir William Herschel zum ersten Mal den Fingerabdruck angewendet, um Verträge mit Handelsreisenden zu authentifizieren.

Nachher im Jahr 1897 wurden die ersten Straftäter durch New ScotlandYard mittels Fingerabdrucks identifiziert. In Deutschland wurde das erste System mit Fingerabdrucken im Jahr 1901 eingesetzt und im Jahr 1903 offiziell eingeführt. seitdem ist die Daktyloskopie in Europa in Gebrauch. Eine Automatisierung erfolgte hingegen erst später. In den sechziger Jahren begannen Arbeiten an der automatisierten Fingerabdrückerkennung auch im nichtforensischen Bereiche für Hochgesichertensysteme. Später in den siebzigen Jahren folgten Entwicklungen von Handgeometrieserkennungssystemen. Mitte der achtziger Jahre wurden Verfahren zur Erkennung von Retina und Iris entwickelt. Danach wurde das erste Verfahren zur Erkennung von John Daugman patentiert. Auf der Grundlage neuronaler Netze werden biometrische Systeme angewendet und seit etwa 1994-1996 erfolgte der erste Wettbewerb von Gesichtserkennungsverfahren, ausgeschrieben und veranstaltet vom US-amerikanischen Verteidigungsministerium. Darauf hin entstand die erste Kommerzialisierungswelle biometrischer Systeme, an die sich die Entwicklung des Marktwettbewerbs entsprechender Produkte anschloss [1].

2.3 Biometrische Erkennungsverfahren

2.3.1 Biometrische Merkmale

Jeder Mensch besitzt Eigenschaften, die biometrische Merkmale darstellen können. Diese Eigenschaften können passiv oder aktiv sein und dienen der Unterscheidung der Personen. Zu den ersten gehören körperliche Merkmale wie Finger, Gesicht, Iris, Retina und Hand. Die aktiven stellen Bewegungen und Verhaltensmuster dar, wie die Schreibdynamik und der Gang.

Beim Einsatz der Biometrie zur automatisierten Erkennung von Personen kommt es darauf an, individuelle biometrische Verhaltens- oder Körpermerkmale zu finden. Diese müssen folgende Eigenschaften besitzen:

- **Erfassbarkeit:** Es sollte eine gute definierbare Messgröße geben, für die es geeignete Sensoren gibt.
- **Universalität:** Jeder Mensch oder fast alle müssen das Merkmal aufweisen.
- **Einzigartigkeit:** Der Messwert ist für jede Person eindeutig.
- **Beständigkeit:** Der Messwert darf nicht von der Messzeit oder vom Alter abhängen.

Als biometrische Merkmale werden auch folgende verwendet:

1. Fingerabdruck
2. Iris
3. Retina
4. Gesichtsgeometrie
5. Handgeometrie
6. Handlinienstruktur
7. Stimme
8. Unterschrift und Handschrift
9. Körpergeruch
10. DNA

2.3.2 Aufbau biometrische Systeme

Die entwickelten Systeme haben denselben Aufbau, sie bestehen aus folgendem:

1. Einem oder mehreren Sensoren für die Aufnahme und die Lebenderkennung.

2. Einer Verarbeitungseinheit um geeignete Informationen zu extrahieren und zum Vergleich vorbereiten.

3. Einer Datenbank um die komprimierten biometrische Daten zu speichern.

4. Einem Vergleicher der die verarbeitete Aufnahme mit der gespeicherten vergleicht (Matching).

5. Einer Ausgabeeinheit; sie gibt das Ergebnis des Vergleichoperation zurück.

2.3.3 Ablauf biometrische Erkennungsverfahren

Das Grundprinzip der biometrischen Verfahren hängt nicht von einem System ab. Das enthält folgende Komponenten: [1]

- **Enrollment:** Personalisierung oder Registrierung des Nutzers im System. und Erfassung relevanter Eigenschaften einer Person und Erstellung von Datensätzen also des Templates.
- **Maching:** Das Vergleichen der aktuellen mit den früher gespeicherten Daten.

Beim ersten Kontakt mit biometrischen Systemen müssen biometrische Merkmale erfasst werden. So entstehen die so genannten Rohdaten woraus das Template generiert wird. Danach kann das Matching ausgeführt werden.
Beim Matching gibt es zwei Möglichkeiten:

- **Verifikation:** In diesem Vorgang wird ein 1:1 Vergleich durchgeführt. Das biometrische Merkmal einer registrierten Person wird mit dem zu dieser Person passende Template verglichen und damit die vorgegebene Identität bestätigt oder widerlegt.
- **Identifikation:** In diesem Vorgang wird ein 1:n Vergleich durchgeführt. Das biometrische Merkmal einer Person wird mit den in der Datenbank gespeicherten Templates verglichen und damit die Zugehörigkeit der Identität zur Datenbank verifizieren. Im Vergleich mit der Verifikation nimmt die Identifikationsphase mehr Zeit in Anspruch,wenn viele Personen in der Datenbank gespeichert sind.

2.3.4 Fingerabdruckerkennung

Die Fingerabdruckerkennung ist eine der ersten entdeckten biometrischen Verfahren. Die Oberfläche des menschlichen Fingers stellt ein Linienmuster dar. Schleifen, Linienenden, Bogen und Wirbel, woraus die so genante Minuzien (siehe Abbildung 2.1) erzeugt werden, unterscheiden sich von Finger zu Finger, auch bei derselben Person.
Unabhängig von der Art der Erfassung des Fingerabdrucks steht dem Verfahren stets ein graustufiges Bild des Fingerabdrucks zur Verfügung. Im Gegensatz zur kriminaltechnischen Methoden, die die graustufigen Bilder benutzt, wobei jedes Bild etwa 250 KBytes im Speicher pro Finger beträgt, verwenden biometrische Verfahren nur die besonderen Punkte (Template 250 bis 1000 Bytes)[5]. Aus praktischem Sicht sind Fingerabdrücke schnell und einfach zu verarbeiten. Außerdem ist die Anschaffung eines Fingerabdrucksystems günstiger als andere Systeme.
Durch unterschiedliche Methoden können die charakteristischen Kennzeichen aus dem Bild extrahiert werden um relevante Teile oder Minuzien aus dem gesamten Bild zu extrahieren.
Für die automatische Erfassung des Fingerabdrucks werden spezielle Sensoren benutzt. Es werden optische, kapazitive thermische und Ultraschalltechnologien genutzt.
Die optische Methode basiert auf optischen Aufnahmen, dabei führt leider Feuchtigkeit des Fingers zu Fehlern.

Die kapazitive Technologie gründet sich auf CMOS Kapazitätsaufnahmen, d.h. Ladungsunterschiede auf dem Finger werden durch CMOS-Halbleiter gemessen. Dabei verursachen auch Feuchtigkeit der Haut und Umgebungsladungen Messfehler.
Das thermische Verfahren ist besser als die beiden ersten, es ist auf die thermische Aufnahme der Haut basiert und deshalb von der Feuchtigkeit unabhängig, aber nicht von der Umgebungswärme.
Das Ultraschall-Verfahren ist das beste Verfahren, weil sein einziger Nachteil der Zeitaufwand ist. [1]. Fingerabducksysteme behalten den Verbrauchsrekord, weil die im Vergleich mit den anderen bequem für den Benutzer sind. Jedoch sind Fingerabdrucksystem relativ leicht zu überwinden. Siehe hierzu auch Abschnitt 2.5.3.

Abbildung 2.1: Fingerabdruck zu Minuzien[5]

2.3.5 Gesichtserkennung

Gesichtserkennungssystem rufen ein geteiltes Echo hervor. Für viele ist Gesichtsaufnahme ohne das Wissen der Person einen Nachteil. Im Gegensatz dazu stellt es für die Regierung und die Hersteller der biometrischen Systeme einen Vorteil dar.

Der entscheidende Faktor hier ist die Gesichtsgeometrie (geometrische Lage der Augen, Mund, Wangenknochen und Nase).Bei der Gesichtserkennung werden 2D und 3D-Verfahre eingesetzt. Dies funktioniert mittels klassischer Bildverarbeitung und Bildanalyse. Dabei wird das Templat aus dem gesamten Bild zu extrahieren und wird entweder gespeichert oder mit einem vorher gespeicherten Template verglichen. Die Templategröße ist ungefähr 2 kBytes[5]. Beim 2D-Verfahren werden zweidimensionale Vermessungen der Gesichtsgeometrie verwendet, besonders auf der vorderen Seite. Heutige Verfahren stützen auf komplexen Berechnungen wie Wellenanalyse (Fourier Transformation) ab, wobei das Bild nach Frequenzanteilen analysiert wird [2].
Jedes Bild hat eine eindeutige Frequenzdarstellung. Der Vorteil ist das diese Frequenzbilder leicht zu vergleichen sind und die Gesichterkennung durch Erhöhung des Anzahl der Frequenzwerte genauer gemacht werden kann[5].

Die dreidimensionale Vermessung der Gesichtsgeometrie basiert auf der Streifenprojektionen [2]. Die Streifenprojektion ist ein technisches Verfahren zur dreidimensionalen digitalen Erfassung von Oberflächenformen anhand optischer Abtastung. Dabei wird das Gesicht im Laufe der Zeit mit Hilfe eines Projektors durch parallelen hellen und dunklen Streifen aus unterschiedlichen Winkeln gestrahlt (Abbildung 2.2) und das Bild mit einer oder zwei Kameras aufgenommen (Abbildung 2.3). Wenn alle Muster aufeinander gelegt werden, entsteht eine zeitliche Folge von Helligkeitswerten, die zur Bestimmung der Oberflächenkoordinaten eingesetzt werden kann (Abbildung 2.4). Die Messgenauigkeit ist proportional zur dritten Wurzel des Volumens.
Allerdings ändert sich das Gesicht mit der Zeit und lässt sich durch Bartwuchs, Verkleidungen, Mimik, Brillen oder Make-up verändern.

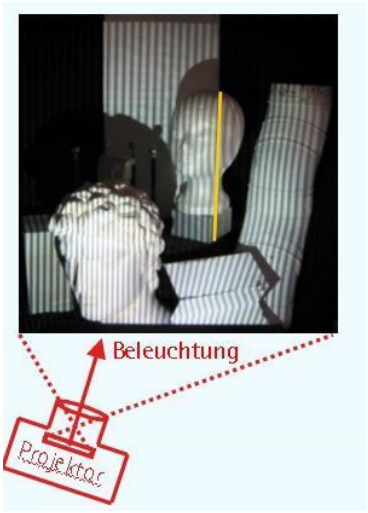

Abbildung 2.2: Gesichtsaufnahme mit Streifenprojektion erster Schritt[7].

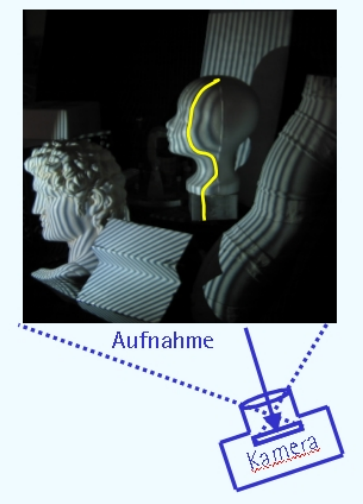

Abbildung 2.3: Gesichtsaufnahme mit Streifenprojektion zweiter Schritt[7].

Abbildung 2.4: Gesichtsaufnahme mit Streifenprojektion Ergebnis[7].

2.3.6 Iriserkennung

Die Iris oder Regenbogenhaut ist die Blende des Auges. Sie ist durch Pigmente gefärbt und liegt zwischen der vorderen und hinteren Augenkammer [2]. Sie stellt bei Menschen eine eindeutige Struktur dar und ist auch bei eineiigen Zwillingen unterschiedlich. Außerdem verändert sie sich sehr wenig während das Leben [1]. Die biometrischen Merkmale der Iris sind Fasern, Flecken, Verflechtungen und Streifen [4]. Bei diesem Verfahren wird das Auge aus einer Entfernung von etwa einem Meter mit einem infraroten Licht beleuchtet und mit einer traditionellen Kamera aufgenommen. Die Aufnahme wird mit geeignete mathematischen Methoden zu einem Template umgewandelt und in einer Datenbank gespeichert [1]. Die Speichergröße beträgt etwa 256 Bytes [5]. Das Verfahren ist nicht geeignet für Blinde oder Menschen deren Augen erkrankt sind. Dabei ist das Betrügen unmöglich weil die Bewegung der Pupillen für Lebenserkennung verwendet wird.

Abbildung 2.5: Iriserkennung mit einem Handgerät[2].

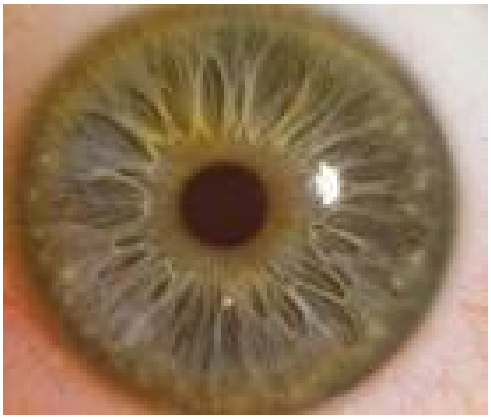

Abbildung 2.6: Irisstrukture[2].

2.4 Anwendungen

Die traditionellen Verfahren sind Verifikation mit Ausweis oder Karte.Man kann aber das Dokument vergessen, zerstören oder verlieren. Die hohe Anzahl an Passwörtern ist für den Benutzer ein Problem. Magnetstreifenkarten sind heute allgemein nicht genug sicher weil sie ohne Mühe kopierbar sind Außerdem ist diese Technik teuer und der Speichermangel verhindert die Verschlüsselung. Dies sind Gründe für die Migration zu biometrischen Systemen. Deshalb gibt es heutzutage viele Anwendungen unterschiedlicher biometrischen Verfahren. Aus Sicht der IT-Sicherheit sind nicht alle Anwendungen erfolgreich, einige davon sind bequem und leisten das Gewünschte, wenn es nicht um Hochsicherheitsbereiche geht. Es handelt sich hier um einen Kompromiss. In dem Maße wie der Komfort steigt, sinkt im Allgemeinen die Sicherheit. Komfort in dem Sinne, dass die Übereinstimung beim Matching jeder einregistrierte Benutzer oft erfolgreich ist. Dieser Punkt wird im Abschnitt 2.5.1 genauer erläutert.

2.4.1 Zutrittskontrolle

Zutrittskontrolle steuert den Zugang und legt fest wer, wann und wohin Zutritt erhält. Sie findet bei Büros, Gebäuden und Gesellschaften wie Regierungsamt, Flughafen und Forschungsabteilungen statt. Die meisten am Markt erhältlichen Managementsysteme für

biometrische Daten sind für die Zutrittskontrolle gedacht. Zutrittskontrollsysteme können entweder kontakthaft oder kontaktlos, je nach dem verwendeten Verfahren, sein. Die Zutrittskontrolle bestehen mindestens aus drei Komponenten:
Ein Sensor führt die Identifikation oder Verifikation und übermittelt das Ergebnis der Zutrittskontrollzentrale, die entscheidet ob der Befehl zum Öffnen der Tür gegeben wird oder nicht. Der Türöffner seinersatz gewährt Zutritt beim Erfolg.

Die Zutrittskontrollzentrale kann zentralisiert sein, wobei alle Sensoren und Türoffner mit einer Zutrittskontrollzentrale direkt verbunden sind, oder dezentralisiert d.h. mehrere häufig miteinander verbundene Zutrittskontrollzentralen an der Verwaltung teilnehmen. Diese können über Ethernet, RS485 oder RS232 vernetzt sein.

2.4.2 PC-Anmeldung

Seit ca.1998 sind auf dem Markt Produkte, die Passwort-Anmeldung am PC beziehungsweise am Firmennetzwerk ersetzt, erhältlich. solche Produkte bestehen meistens aus einem Fingerabducksensor der in der Tastatur oder der Maus eingebaut ist. Da PassWörter hackbar sind, ist es in Zukunft zu erwarten, dass die meisten Notebooks mit biometrische Sensoren ausgestattet sein werden, weil die Streifensensoren sehr günstig sind.

Abbildung 2.7: biometrische Maus [6].

2.4.3 E-Commerce

Bei E-Commerce geht es um elektronischen Handel von Dienstleistungen oder Produkte über Netzwerke (Internet, Intranets, Extranets) via das TCP/IP Protokoll. E-Commece

bietet eine Reihe von Vorteilen zum Beispiel unbegrenzte Öffnungszeiten, keinen Einkaufstress, Parkplatzsuche und lange Schlange. Außerdem bietet E-Commerce die Möglichkeit Web-Suche nach bestimmten Produkten zu führen oder Preise von zu Haus zu vergleichen. Die Nachteil des E-Commerces liegen im Übertragungsweg liegen, wenn die Kommunikation nicht sicher ist. Deswegen stellen die Bedrohungen der IT-Sicherheit (sind genau das Gegenteil der Ziele der IT-sicherheit sehe Abschnitt 1.5.3) die E-Commerce Nachteile dar. Außerdem sind biometrische Merkmale Körperteile und damit nicht übertragbar. Deshalb wird man sich in naher Zukunft für biometrische Systeme zur Authentifizierung bei on Line Banking, E-Goverment, e-bay, Voice over IP, Online-Versicherung oder Flugticketbuchung.

2.4.4 Conveniencebereich

In diesem Bereich geht es nicht um Sicherheit sondern um Bequemlichkeit, Angemessenheit und Übertragbarkeit. Für Besucher einer Sauna oder eines Schwimmbades ist der Schlüssel an der Hand lästig oder einige Mitglieder eines Clubs geben ihre Mitgliedkarte weiter. Der Einsatz von biometrische Erkennungssysteme ist die Lösung für solche Probleme.

2.4.5 Höheitlicher Bereich

Im Frankfurter Flughafen gibt es schon ein Pilot-Projekt, wobei die Reisende sich durch ein Iriserkennungssystem authentifizieren lassen. Andere Beispiele in diesem Bereich sind elektronische Reisepasse, Ausweis und Gesundheitskarte, was in nächsten Kapitelen folgt.

2.5 IT-Sicherheit und Biometrie

Die steigende Abhängigkeit der Bürgern und Institutionen von eingesetzten IT lässt sich klar bemerken. Alle Informationen sind digital gespeichert und werden über Netzen ausgetauscht, was zur selben Frage führt: sind unsere Systeme und die Datenübertragungen wirklich geschützt? Wie oben erwähnt, haben alle Anwendungen noch Schwach-Stellen. IT-Sicherheit und Biometrie sind komplementär, gemeinsam können sie ein sehr großes Sicherheitsniveau erreichen.

2.5.1 Treffer- und Fehlerraten

Die Fehlerquellen bei biometrischen Systeme sind unterschiedlich:
Da biometrische Merkmale sehr sensible sind kann das Matching nie Hundertprozent durchgeführt sondern eine bestimmte Ähnlichkeit zu untersuchen. Dies hat zur Folge, dass die Entscheidung, ob das Matching erfolgreich ist oder nicht, von Toleranzbereich abhängt, der durch den Vergleichswert und die vorher fixierten Parametern bestimmt ist.

Für den Vergleich wird ein Toleranzschwelle festgelegt zum entscheiden ob das Ergebnis positiv oder negativ ist. (z.B. bei 99 Prozent Übereinstimung beim Matching wird das Ergebnis akzeptiert sonst abgelehnt).

Aus Kapazitätsgründen sind nicht die kompletten biometrischen Daten gespeichert sondern nur bestimmte Informationen, was zu Fehlern führen kann. Die Messdaten können fehlerhaft sein, zum einen wegen einer unzureichendne Messungenauigkeit des Sensors, zum anderen wegen Umwelteinflüsse wie Lichtverhältnisse, oder wegen der Veränderung der biometrischen Merkmale durch Verletzung oder andere Ursachen. Dieses hat zur Folge das biometrische Systeme zusätzliche Maßnahmen brauchen, was im nächsten Kapitel aus der Nähe betrachtet wird. Wesentliche Begriffe wie CAR, CRR, FAR, FRR, EER und FER werden auf den nächsten Seiten erläutert.

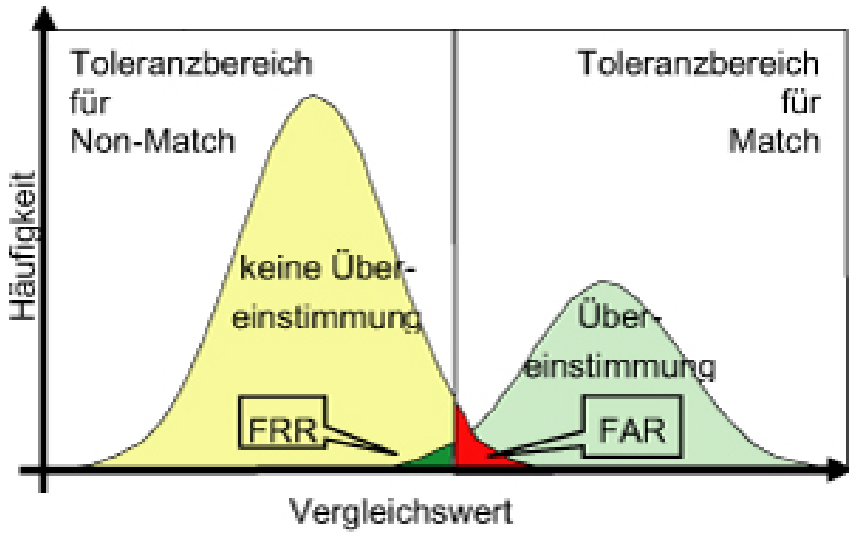

Abbildung 2.8: Toleranzbereich [1]

- **Correct Akzeptanz Rate (CAR):** Die Trefferrate richtiger Akzeptanz registrierter Benutzer [5].
- **Correct Rejection Rate(CRR):** Die Trefferrate richtiger Zurückweisung Unbefügter [5].
- **False Akzeptanz Rate (FAR):** Die Rate der Akzeptanz unbefügter Benutzer. Sie soll sehr klein sein, sonst ist das System nicht ausreichend sicher [5].
- **False Rejection Rate (FRR) :** Die Rate der Zurückweisung registrierter Benutzer. Sie soll klein sein, sonst muss jeder Benutzer, auch befügte, den Versuch mehrmals wiederhollen[5].
- **Equal Error Rate (EER) :** wenn die FAR gleich die FRR [4].
- **False Enrollment Rate (FER) :** Die Rate fehlerhafter Enrollementversuche,d.h. Anzahl an Personen die nicht vermessen werden können. Eine zu hoch FER bedeutet dass kein Benutzer sich registrieren kann und das System nicht mehr einsetzbar ist[4].

Die FAR und FRR hangen von einem einstellbaren Schwellwert und beeinflussen sich gegenseitig, wie man im Abbildung 2.8 sehen kann. Sie sind sogar umgekehrt proportional zu einander. Auf der x-Achse ist die Ähnlichkeit mit dem Template dargestellt, links vom Toleranzwert wird alles abgelehnt und rechts davon wird alles akzeptiert. Verschiebt man die Schwelle nach links wird die FRR kleiner und gleichzeitig die FAR größer, demgegenüber verschiebt man sie nach rechts wird die FAR kleiner und damit das System sicherer, aber auch die FRR wird höher und damit das System strenger und unkomfortabler. Auf der y-Achse ist die Häufigkeit dargestellt.

2.5.2 Angriffe auf biometrische Systeme

Biometrische Systeme haben mehrere Schwachstellen, sowohl der Sensor als auch die Übertragung oder die Template können angegriffen werden. Beim Angriff auf dem Sensor können Benutzermerkmale gestohlen und nachgebildet werden um Systeme zu überleisten.

Beim Angriff auf die Übertragung können Daten unterwegs kopiert und damit zur Nachbildung verwendet oder einfach verfälscht werden. Die Datenbank kann auch angegriffen werden um die Template zu erhalten oder zu manipulieren. Einige biometrische Merkmale sind leicht nachzubilden. Man kann Fingerabdrucke von einem Gegenstand (z.B. eine Flasche oder ein Glas) abnehmen und auf Holzleim bringen und damit sich als Befigter anmelden [3]. Seinerseits können Gesichterkennungssystem durch Bilder überlistet werden. Die einzige Merkmale, die noch nicht nachgebildet wurden, ist die Retina.

Abbildung 2.9: Fingerabdruck Nachbildung[3].

Abbildung 2.10: Finger und Attrappe[3].

2.5.3 IT-Sicherheit Aspekte

Um die Sicherheit in IT-Systeme zu garantieren, muss man folgende Aspekte beachten:

- **Vertraulichkeit:** nur berichtigte Personen dürfen auf die Information zugreifen.
- **Integrität:** nur erlaubte und berchtigte Personen können Änderungen der Informationen in einem IT-Systeme ausführen.
- **Verfügbarkeit:** soll garantieren, dass der Benutzer eines IT-Systems einen Dienst in angemessener Qualität, Form und Zeit nutzen kann.
- **Authentizität:** hat zwei Aspekte. Zum ersten Datenauthentizität d.h. die Daten zwischen oder im System sind echt zum zweiten Teilnehmerauthentizität, Sender und Empfänger sind echt und diejenigen, als die angemeldet haben, sein.
  Beispiel: Der E-Mail Absender und der Inhalt sind echt.
- **Verbindlichkeit:** soll garantieren dass die geforderte Operationen ausgeführt werden.
- **Anonymität:** Die eigne Identität und Daten sind nur soweit, wie der Inhaber erlaubt, verbreitet.

Probleme treten bei PC-Anmeldung , E-Commerce oder Zutrittkontrolle besonders im dezentralisierten Fall auf, genau wenn einer der oberen Aspekte verletzt wird. Um die Angriffe auf biometrische Systeme zu vermeiden und damit die oben genante Ziele (Aspekte) zu erreichen, muss man unterschiedliche Gegenmaßnahmen einsetzen.

2.5.4 Maßnahmen gegen Sensorangriff

- **Sabotageschalter:** Seine Aktivierung bewirkt, dass das Gerät eine Meldung abgibt oder eine Alarm auflöst, sobald der Sabotageschalter geöffnet ist (das Gerät von der Wand genommen ist).
- **Watchdog:** Diese Option sichert das Booten des Geräts, falls innere Fehler festgestellt wird.
- **Überwachungskamera:** Diese Kamera überwacht ein oder mehrere Geräte zum Beispiel im Flughafen oder Hochsicherheitsgebiete.

2.5.5 Maßnahmen gegen Kommunikationsangriff

- **Verschlüsselung:** bietet die Möglichkeit Daten so zu verändern, dass ein Dritter mit diesen nichts anfangen kann. Beispiel dafür sind symmetrische und asymmetrische Verschlüsselung .

- **Digitale Signaturen:** Ermöglicht dem Empfänger einer Nachricht durch Prüfsummen zu überprüfen ob die Nachricht unterwegs geändert wurde oder nicht.
- **Zertifikat:** Der Empfänger muss sicher sein dass der öffentliche Schlüssel wirklich zum richtigen Sender gehört. Dies wird durch Zertifikat erreicht. Neben den Daten, und dem öffentlichen Schlüssel enthält die Nachricht den Namen der Stelle die das Zertifikat ausgestellt hat, eine Serienummer, Angaben zur Gültigkeitsdauer und wieder ein mit privaten Schlüssel erstelltes Zertifikat.

2.5.6 Maßnahmen gegen Datenbankangriff

- **Physikalischer Schutz:** Die Datenbank soll sich in einem sicheren Raum befinden.
- **Verschlüsselung:** Die Daten können auch in der Datenbank verschlüsselt gespeichert. Beispielsweise SSL-Verschlüsselung für MySQL.

2.5.7 Maßnahmen gegen Merkmaldiebstahl

- **Einsatz lebenderkennende Geräte:** Bei kontakthaften Systeme kann durch Wärmesensoren geprüft werden, ob die Temperatur der menschlichen entspricht oder durch Impulssensor ob es überhaupt Impulse gibt.
- **Kombination von einem biometrischen Verfahren und einem Traditionnelen:** Beispielsweise Gesichtserkennung und Passworteingabe.
- **Kombination von mehrere biometrischer Verfahren:** Zum Beispiel in einigen Institutionen wird Fingerabdruck- und Gesichtserkennung verwendet.

2.5.8 Abschließende Bemerkungen

Es ist festzustellen, dass ohne Einsatz biometrische Systeme, bleibt die Anonymität konkurrierend zur Authentizität, Vertraulichkeit und Integrität. Gegen die Sozialengeneering braucht man keine Gegenmaßnahmen wenn biometrische Verfahren verwendet werden, weil biometrische Merkmale nicht weitergegeben werden können.

Sicher können diese Gegenmaßnahmen zusammen mit Antiviren, Firewall und Intrusiondetection-Systeme einen sehr hohen Grad an Sicherheit erreichen. Aber noch sind die Systeme weit von der Perfektion entfernt, weil jedes von den obengenanten Verfahren Vorteile und Nachteile hat. Gelangt ein Böser in das System so kann er große Schaden verursachen. Der Feind ist der Mensch selbst, deshalb gibt es immer wieder neuartige Angriffe die verlangen, dass Schutzmaßnahmen immer weiter verbessert werden müssen.

Abbildungen

Literaturverzeichnis

[1] Bsi-Bund.*http://www.bsi.bund.de/fachthem/biometrie.*

[2] Wikipedia.*http://de.wikipedia.org/wiki/Biometrie.*

[3] Hacken mit Handauflegen.*http://www.trust-us.ch/ds/80/008.htm*

[4] E.Jasinka Biometrie und Datenschutz.*http://www.Jainka.de/uni/biometrie-datenschutz,Stand:23.5.2005*

[5] A.Talaska,O.Münstermann. Üniversität der Bundeswehr München.*Sicherheitsmechanismen I*

[6] Sicherhaits-Check per PC-nager.*http://www.it-im-untrnehmen.de*

[7] Bremer Institut für angewandte Strahltechnik.*http://www.bias.de/Abteilungen/OMT/Systeme/Streifenprojektion*

Kapitel 3

ePass

David Ristow

Mit Eintritt in die zweite Phase der Auslieferung des elektronischen Reisepasses am 1. November 2007, war die Bundesrepublik Deutschland der erste Staat des Schengener Abkommens, welcher sich zur Speicherung des biometrischen Fingerabdrucks auf einem hoheitlichen Dokument verpflichtete. Vater des Grundgedanken war die International Civil Aviation Organization (ICAO), die im Jahr 1997 erstmalig die Empfehlung zur Einbindung von Biometrie in Reisepässen anbrachte. Dieser Prozess wurde von der Europäischen Union in zwei Phasen eingeteilt, die Kombination der schon vorhandenen Machine Readable Zone (MRZ) mit einem digital gespeicherten Gesichtsbild und die Erweiterung durch den biometrischen Fingerabdruck. Der erste Prozessschritt wurde in Deutschland am 1. November 2005 mit der Ausgabe von elektronischen Reisepässen erfolgreich realisiert. Hierzu mussten neue Arbeitswege und Ablaufverfahren eingeführt werden um das sichere Erfassen der biometrischen Daten eines jeden Bürgers zu gewährleisten. Grundlage des neuen Ausweisdokuments ist ein kontaktloser und zertifizierter Radio Frequency Identification (RFID)-Chip, der mit einem Coprozessor und einem dazugehörigen 72kByte Speicher ausgestattet ist. Um die Interoperabilität und Sicherheit, der von der ICAO festgelegten Datengruppen, zu gewährleisten, wurde nun auf verschiedene Zugriffs- und Kodierungsverfahren zurückgegriffen. Ein sicheres Verfahren zum Schutz des abgespeicherten Gesichtsbildes stellt der Basic Access Control (BAC) dar, welcher Anfang 2006 in den deutschen Meldestellen eingeführt wurde. BAC ist ein symmetrisches kryptografisches Protokoll, das vor allem Schutz vor unbemerktem Auslesen des Reisepasses bieten soll. Die Abschirmung gegen unbefugtes Auslesen der Fingerabdruckdaten realisiert das asymmetrische Protokoll Extended Access Control (EAC), welches auf einer Public Key Infrastructure (PKI) arbeitet. EAC setzt eine erfolgreiche Durchführung von BAC voraus und verhindert in erster Linie das Klonen des Reisepasses. Entgegen aller Angst der deutschen Bürger vor Identitätsdiebstahl und Dokumentenfälschung, liefert das ePass-Projekt den derzeit höchsten internationalen Standard im Bereich der Sicherung von hoheitlichen Dokumenten und wird diesem auch in Zukunft gerecht werden.

Inhaltsverzeichnis

3.1 Einleitung

Das deutsche Recht auf Informelle Selbstbestimmung bezeichnet das Recht des einzelnen Bürgers über seine personenbezogenen Daten selbst zu verfügen. Die Billigung der Einschränkung dieses Grundrechts durch den Gesetzgeber fordert meist das überwiegende Allgemeininteresse der Bevölkerung. Die Preisgabe von persönlichen Informationen ist häufig an Datenschutzkriterien gebunden, die im Zeitalter der Digitalisierung den technologischen Standard sehr hoch setzen und den Informanten zum Kritiker der Sicherheit werden lassen. Mit dieser Problemstellung ist der Staat gefordert spezielle Verfahrensvorschriften zu entwickeln, die wiederum den Datenmissbrauch unmöglich machen. Mit Beginn des ePass-Projektes sahen sich die staatlichen Behörden einer großen Masse von Kritikern gegenüber. Beeinflusst durch verschiedene Medien, welche die Schwächen anderer Dokumente mit gleicher Technologie aufzeigten, wurde die Angst des Identitätsdiebstahls gestreut. Die Aufgabe, das technologische Niveau der IT-Sicherheit auf das höchste mögliche Maß anzuheben, wurde von der Bundesregierung erkannt und unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit dem Bundeskriminalamt erfolgreich umgesetzt. In diesem Arbeitsprozess wurden neue Spezifikationen des Zugriffs in der kontaktlosen Datenübertragung, wie Extended Access Control, realisiert. Das folgende Kapitel soll einen Überblick zur allgemeinen Funktionsweise sowie Aufschluss über entwickelte Prozessstrukturen und zertifizierte Zugriffs- und Codierungsverfahren im ePass-Projekt geben.

3.2 Der deutsche ePass

Es folgt ein Einblick in die Grundzüge von ePass, eine zeitliche Einordnung der festgelegten Meilensteine des Projektplans sowie ein Überblick zum gesetzlichen Rahmen. Anschließend stehen die technischen und sicherheitsspezifischen Merkmale des elektronischen Reisepasses im Mittelpunkt der Betrachtungen.

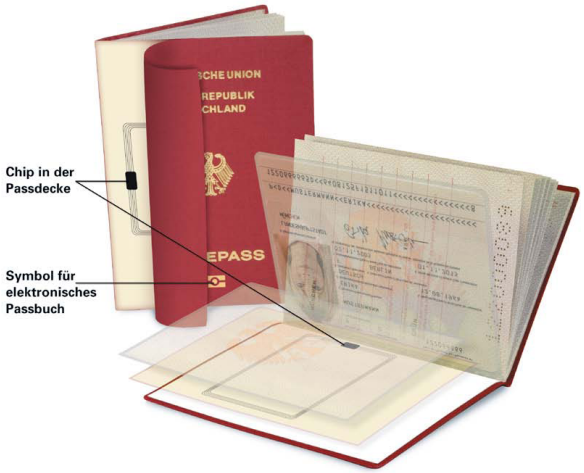

Abbildung 3.1: Elektronischer Reisepass [1]

3.2.1 Der Weg des elektronischen Reisepasses

Beginnend mit der New Orleans Resolution, die im März 2003 durch die International Civil Aviation Organization (ICAO) verfasst wurde, gelang die Festlegung des Gesichtsbildes als primäres biometrisches Merkmal für maschinenlesbare Reisedokumente. Das digital gespeicherte Lichtbild sollte später, durch die Aufnahme des Fingerabdrucks oder der Iris für die maschinengestützte Identifikation, erweitert werden. Im Oktober 2004 spezifizierte die ICAO ihre technischen Richtlinien zur Nutzung einer Public Key Infrastructure (PKI) sowie die Entwicklung des Standards 9303 in Zusammenarbeit mit der International Organization for Standardization (ISO). Mit dem Inkrafttreten der EG-Verordnung über *Normen für Sicherheitsmerkmale und biometrische Daten in den von den Mitgliedstaaten ausgestellten Pässen* folgte die EU der Empfehlung der ICAO 18 Monate später. Die EU-Richtlinie definierte technische Vorschläge als Standard und erklärte das digitale Gesichtsbild in Kombination mit dem Fingerabdruck zum Pflichtkriterium Europäischer Reisepässe. Für die technologische Realisierung der neuen Generation von Reisepässen in Deutschland und Europa, wurde unter Initiative des Bundesinnenministerium, des BSI und deutscher Unternehmen die *Essen Group* gegründet, welche fortan Empfehlungen für Fachausschüsse und Expertengremien gab. Am 8. Juli 2005 bestätigte schließlich der Bundesrat die Abänderung der deutschen Passverordnung zum 1. November 2005. Dies startete die Probezeit des ePass-Projektes, welche ihr Ende mit der Einführung und Vervollständigung durch den biometrischen Fingerabdruck 2 Jahre später haben sollte.

3.2.2 Aktueller Stand

Der deutsche Reisepass gehört, seit Beginn im November 2007, zu den sichersten Reisedokumenten weltweit. Grundlegende Pfeiler dieser Sicherheitsarchitektur ist sowohl die Integration, als auch die Kombination von Gesichtsbiometrie und Fingerabdruckdaten in einem Dokument. Die von der ICAO standardisierten Methoden zur softwarebasierten Auswertung von Passbildern, welche mit Hilfe einer Fotomustertabelle erstellt wurden, dienen hierbei nur der internationalen Einheitlichkeit. Die Sicherheit hingegen wird durch den Schutzmechanismus Basic Access Control (BAC) gewährleistet. Das äquivalente Verfahren zum Abschirmen der biometrischen Fingerabdruckdaten ist Extended Access Control (EAC). Beide Verfahren bilden den Schwerpunkt dieser Seminararbeit und werden im weiteren Verlauf detailiert beschrieben. Es folgt eine technische Beschreibung des elektronischen Reisepasses.

Nicht das Setzen eines neuen Grundsteines sollte den Angriff auf die schwindende Integrität der Sicherheit hoheitlicher, europäischer Reisedokumente verhindern. Eine Transformation bestehender Strukturen sollte den gewünschten Erfolg bringen. Diese weitreichende Überlegung begründete auch das Bewahren der alten Passstruktur, mit allen der in Abbildung 3.2 gezeigten klassischen Sicherheitsmerkmale. Komplett neu hingegen ist die Einbettung eines 72kByte Mikroprozessors mit kryptografischen Coprozessor in der Hinterseite der Deckelklappe. Dieser zertifizierte Radio Frequency Identification (RFID)-Chip bildet das neue technologische Herz des ePass-Projektes. Die Datenübertragung zwischen

dem Chip und dem Lesegerät erfolgt gemäß des Standards ISO/IEC 14443 mit einer Frequenz von 13.56 Megahertz kontaktlos über Funk. Hierfür kann der Abstand zwischen den beiden technischen Einheiten, Chip und Lesegerät, von einigen Millimetern bis zu maximal 25 Zentimetern variieren. Der Chip generiert aus den Funkwellen des Terminals seine Betriebsspannung. Über die durch den Chip gesteuerte Modulation der Feldstärke werden Informationen zum Lesegerät übertragen. Dieses induktive Verfahren auf Basis von Drahtspulen als Antennen ermöglicht Datenübertragungsraten von ca. 100 bis 850 Kilobit pro Sekunde. Der deutsche ePass arbeitet heute mit einer Übertragungsrate von etwa 424 Kilobit pro Sekunde und ermöglicht so die schnelle Übermittlung der auf dem Chip gespeicherten Daten[1].

Abbildung 3.2: Klassische Sicherheitsmerkmale des dt. Reisepass: 1)Holografisches Portrait, 2)Bundesadler, 3)Kinematischen Bewegungsstrukturen, 4)Makro- und Mikroschriften, 5)Kontrastumkehr, 6)Holografische Wiedergabe der Machine Readable Zone (MRZ), 7)Maschinell prüfbare Struktur, 8)Oberflächenprägung, 9)Mehrfarbiger Sicherheitsdruck, 10)Laserbeschriftung, 11)Wasserzeichen [1]

3.2.3 Der elektronische Personalausweis

Der Vorschlag von *E-Goverment 2.0* im September 2006 durch das Bundesinnenministerium sollte in erster Linie einfache und schnelle Kommunikationswege sowie integrierte und standardisierte Prozesse im Verwaltungsapparat der deutschen Behörden einführen. Sowohl die elektronische Zusammenarbeit zwischen Wirtschaft und Verwaltung, als auch die Bündelung gleichartiger Dienstleistungen verschiedener Behörden in großen Servicezentren, war Grundgedanke dieses Vorhabens. Das Kernelement von *E-Goverment 2.0* stellt der elektronische Personalausweis dar, der mit Starttermin 2008 angekündigt wurde. Der neue Ausweis soll die Personenidentifikation (analog zum ePass) sicherer und komfortabler machen, und darüber hinaus den Anwendungsbereich des heutigen Papierdokuments um die Identifikation im Internet ergänzen. Hierzu ist ein Scheckkartenformat (Abb. 3.3) angedacht, welches einen qualifizierten RFID Chip mit elektronischer Signatur enthält. Die staatliche Vergabe von Zertifikaten durch zentrale Organe ermöglicht dann einen einfach zu handhabenden Identifizierungsmechanismus für Online-Dienstleistungen oder andere organisationsübergreifende Geschäftsprozesse. Wie in der Verwendung der RFID-Technologie, sollen auch bei den Richtlinien zur Produktionsdatenerfassung und Qualitätsprüfung die Synergien zwischen elektronischem Reisepass und Personalausweis

genutzt werden. Die technischen Richtlinien werden zurzeit unter Federführung des BSI erarbeitet.

Abbildung 3.3: Erster Entwurf für den elektronischen Personalausweis von der Firma Giesecke u. Devrient [Quelle: sueddeutsche.de]

3.3 Prozessschritte in ePass bei der biometrischen Datenerfassung

Mit der Digitalisierung des deutschen Passsystems wurde auch die Forderung nach neuen Prozessstrukturen laut. Sowohl die technischen, als auch qualitativen Richtlinien zur diskreten Speicherung von biometrischen Informationen, deren Verifizierung und die Übertragung an den Passproduzenten, stellen das zentrale Thema dieses Kapitels dar.

3.3.1 Datentransfermodell

Bei starker Abstraktion des Kommunikationsmodells kristallisieren sich lediglich zwei Endpunkte heraus. Die Richtlinie beschreibt daher die austellende Passbehörde als Quelle und den Passproduzenten als Senke. Erstere nimmt die Erfassung der biometrischen Daten vor und führt anschließend eine lokale Qualitätsbewertung durch, welche bei unzufriedenem Ergebnis beliebig wiederholt wird. Es folgt eine Zusammenfassung aller aufgenommenen Daten einer Person in sogenannte Antragsdatensätze und die anschließende Einbettung in ein Kommunikationsmodul das den, im Folgenden beschriebenen, Datentransfer regelt. Nach Ankunft der Informationen beim Passproduzenten erfolgt, vor der Produktion, eine letzte zentrale Qualitätsprüfung und deren Aufzeichnung.

Basis der Datenkommunikation in ePass ist ein speziell entwickelter Datentyp mit dem Namen XPass, ein XML-basiertes Datenaustauschformat, das aufgrund seiner Unabhängigkeit gegenüber Betriebssystemen oder Anwendersoftware große Vorteile in dokumentorientierten Geschäftsprozessen liefert. Die flexible Implementierung ermöglicht jedoch auch den Übertrag in andere Prozessarten, wie dem elektronischen Personalausweis. Die

XPass-Daten werden zur Übertragung mit einer digitalen Signatur versehen. Dabei handelt sich nicht um eine qualifizierte Signatur im Sinne des Signaturgesetzes, sondern um Authentisierung des Senders und der Integritätssicherung durch XML-Signature, einer XML-Schreibweise für digitale Signaturen. Die Verwaltung der Zertifikate zur Erzeugung der Signaturen wird durch die Verwaltungs-PKI des Bundes und der Länder, die in Abschnitt 3.4 noch einmal ausführlich beschrieben wird, realisiert. Um die Vertraulichkeit der bereits signierten Daten zu schützen, erfolgt vor dem Transport der XPass-Daten eine zusätzliche Verschlüsselung durch XML-Encryption. Um die authentische Datenübermittlung zwischen Passbehörde bzw. Vermittlungsstelle und Passhersteller zu gewährleisten, wird auf geeignete Transportprotokolle zurückgegriffen. Das im Rahmen von *E-Government* verwendete *Online Services Computer Interface* (OSCI) wurde hier als Standard gewählt. Für Passbehörden, welche die elektronische Datenübermittlung OSCI nicht unterstützten, wurde eine Kombination aus *Web Service Description Language* (WSDL) und *Simple Object Access Protocol* (SOAP) gewählt. Dieses alternative Ersatzverfahren verwendet *Hypertext Transfer Protocol Secure* (HTTPS) mit der Grundlage von XML.

Wie bereits beschrieben, erfordert die Kommunikation zwischen Passbehörde und Passhersteller die allgemeinen Richtlinien der Datensicherheit. Der Schutz der Integrität durch elektronische Signaturen, die kryptografische Verschlüsselung zum Wahren der Vertraulichkeit und eine gegenseitige Authentisierung von Sender und Empfänger bilden das Sicherheitskonzept von XPass, das in Abbildung 3.4 nochmals zusammengefasst wird. Die Vergabe von Signaturzertifikaten zum Schutz der Integrität erfolgt in Deutschland durch das BSI in Form von SmartCards seitens der Passbehörde und als Softwarezertifikate für die Passhersteller. Um der inhaltlichen Manipulation der Passdaten zu entgehen, erzeugt der Sender der Daten mit Hilfe seines privaten Schlüssels aus dem Signaturzertifikat eine XML-Signatur. Die Überprüfung der Signatur erfolgt dann durch einen öffentlichen Schlüssel des Zertifikats vom Passhersteller. Zur Gewährleistung der Vertraulichkeit der Daten bedient sich die sendende Passbehörde eines öffentlichen Schlüssels ihres ausgestellten Verschlüsselungszertifikats, das wiederum auf der Seite des Konsumenten zur Dekodierung mittels eines privaten Schlüssels dient. Neben allen verwendeten Zertifikaten auf der Anwenderebene zur Verschlüsselung und Signierung, werden selbige auch auf der Transportebene eingesetzt. In der Variante des OSCI Transports spielt das Intermediär, ein vermittelndes Serversystem, das Dienste wie die Authentisierung mittels elektronischem Zertifikat erbringt, ein große Rolle. Hierbei verfügt jeder OSCI-Client und Intermediär über sein eigenes Authentisierungszertifikat sowie einen öffentlichen Schlüssel. Das gleiche Prinzip findet auch in der Variante WSDL/SOAP, mit dem Unterschied der Kommunikation der Passbehörde mit einem Webserver, seine Anwendung. In beiden Fällen erfolgt eine Echtheitsüberprüfung seitens des Clients und analog umgekehrt durch den Server vor der Datenübertragung. Die Garantie des authentisierten Zugriffs auf die Passdaten ist somit gewährleistet.

3.3.2 Erfassung der Lichtbilder als biometrisches Merkmal

Die Forderung der Interoperabilität des biometrischen Gesichtsbildes im weltweiten Passverkehr brachte neue Prozesse in der Datenerfassung zum Vorschein. Eine einheitliche Quali-

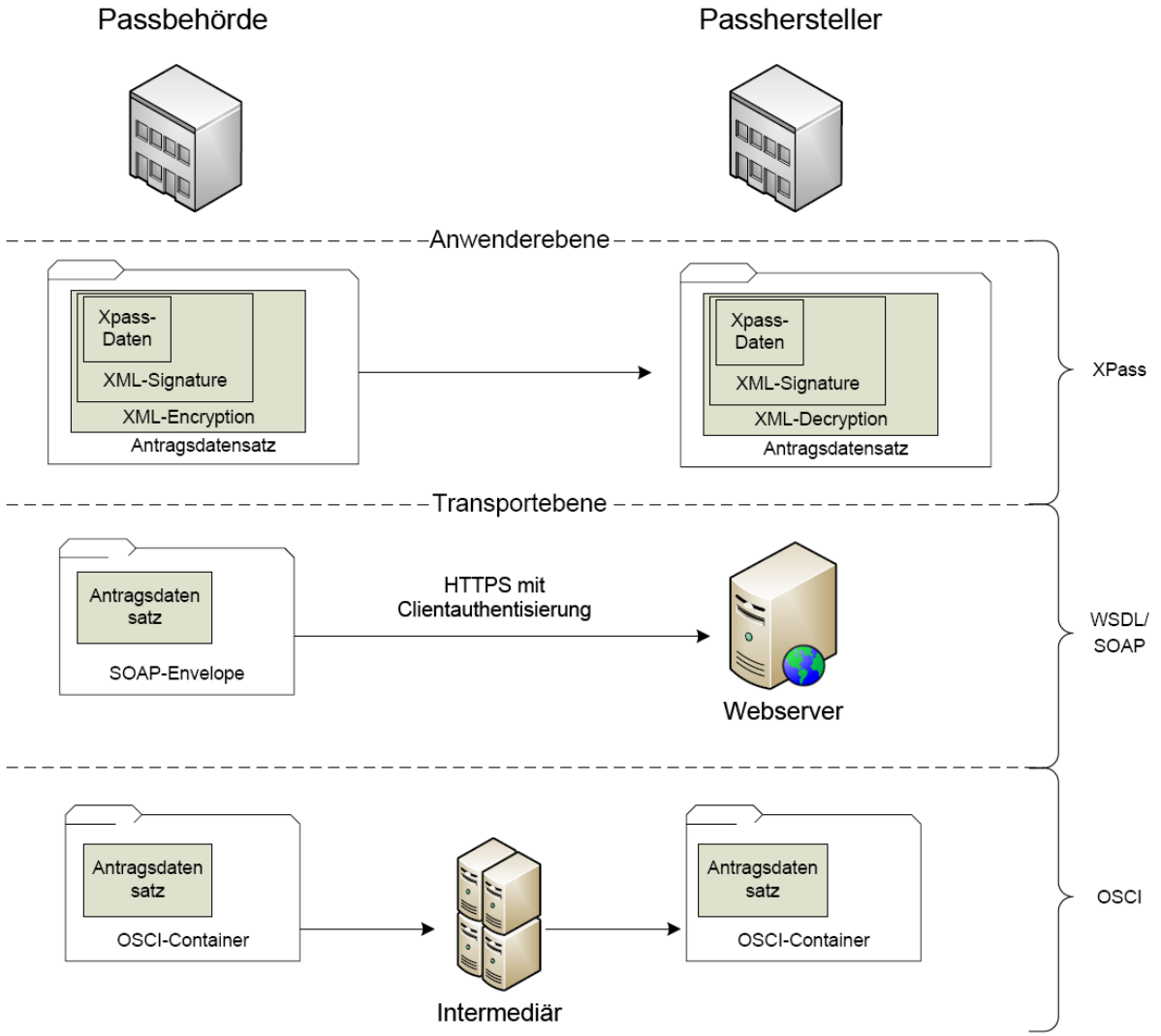

Abbildung 3.4: Datentransfermodell XPass

tätssicherung (QS) als Referenzgrundlage in der Passbildererstellung war der einzige Weg um in internationalen Verifikationsverfahren jeweils die gleichen digitalen Ergebnisse zu erzielen. Genaue Eingrenzung der Richtlinien des Antragsverfahrens, der Erstellung der Lichtbilder und der Produktion der Dokumente fließen dabei in den Gesamtprozess ein. Die Qualitätssicherung im Falle der Gesichtsbildaufnahme und der Fingerabdruckdaten wird in die dezentrale Prüfung in der Passbehörde, als auch in die zentrale Kontrolle seitens des Passhersteller unterteilt.

Die Art der dezentralen Prüfung der Lichtbildaufnahme unterscheidet sich jeweils in welcher Form das Passbild angefertigt wurde. Bei analoger Fotografie der Person ist zunächst eine visuelle Prüfung vorzunehmen, welche bei positivem Ergebnis den Scanvorgang nach sich zieht, um das Bild zu digitalisieren. Die visuelle Prüfung erfolgt anhand einer Fotomustertafel, die zum Beispiel das definierte Verhältnis zwischen Gesichtsfeld und Gesamtbild

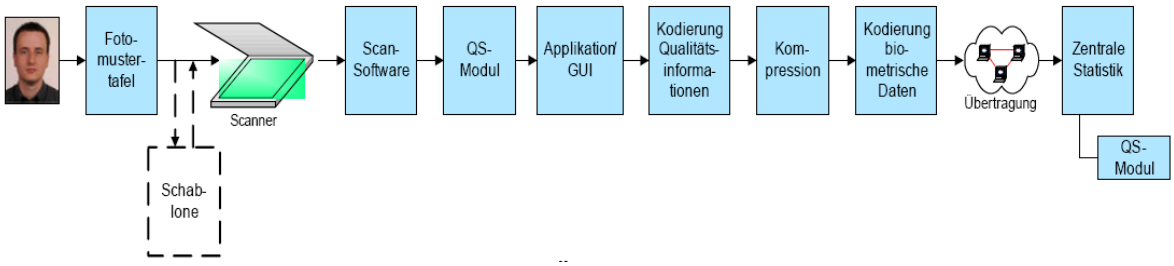

Abbildung 3.5: Analoge Erfassung von Bilddaten bei Passbehörden mit Digitaler Übermittlung [5]

oder einen neutralen Gesichtsausdruck vorgibt. Technisch wird das Bild auf Größe und Farbtiefe (hier 24 Bit) untersucht. Die nach dem Scanvorgang folgende Kontrolle durch ein QS-Modul, beschreibt das softwaregestützte Verifizieren der Bilddaten. Diese Software prüft erneut alle Kriterien der ICAO-Vorgaben für Lichtbilder, berechnet die Qualität der Merkmale und gibt diese mittels einer Applikation auf dem Bildschirm aus (Abb. 3.6).

Abbildung 3.6: Applikation(GUI) zur Qualitätssicherung[2]

Einsatzgebiet des QS-Moduls ist die Passbehörde zur Passfertigung und der Passhersteller für statistische Erhebungen. Nach der anschließenden Kodierung, der vom QS-Modul bereitgestellten Qualitätsinformationen, folgt die einmalige verlustbehaftete Kompression der Bilddaten durch JPEG 2000 auf eine feste Dateigröße von 15kByte. Die darauf folgen-

de Kodierung der biometrischen Daten unterliegt dem ISO-konformen Standard *Common Biometric Exchange Format Framework* (CBEFF) und wird in Abbildung 3.7 erläutert.

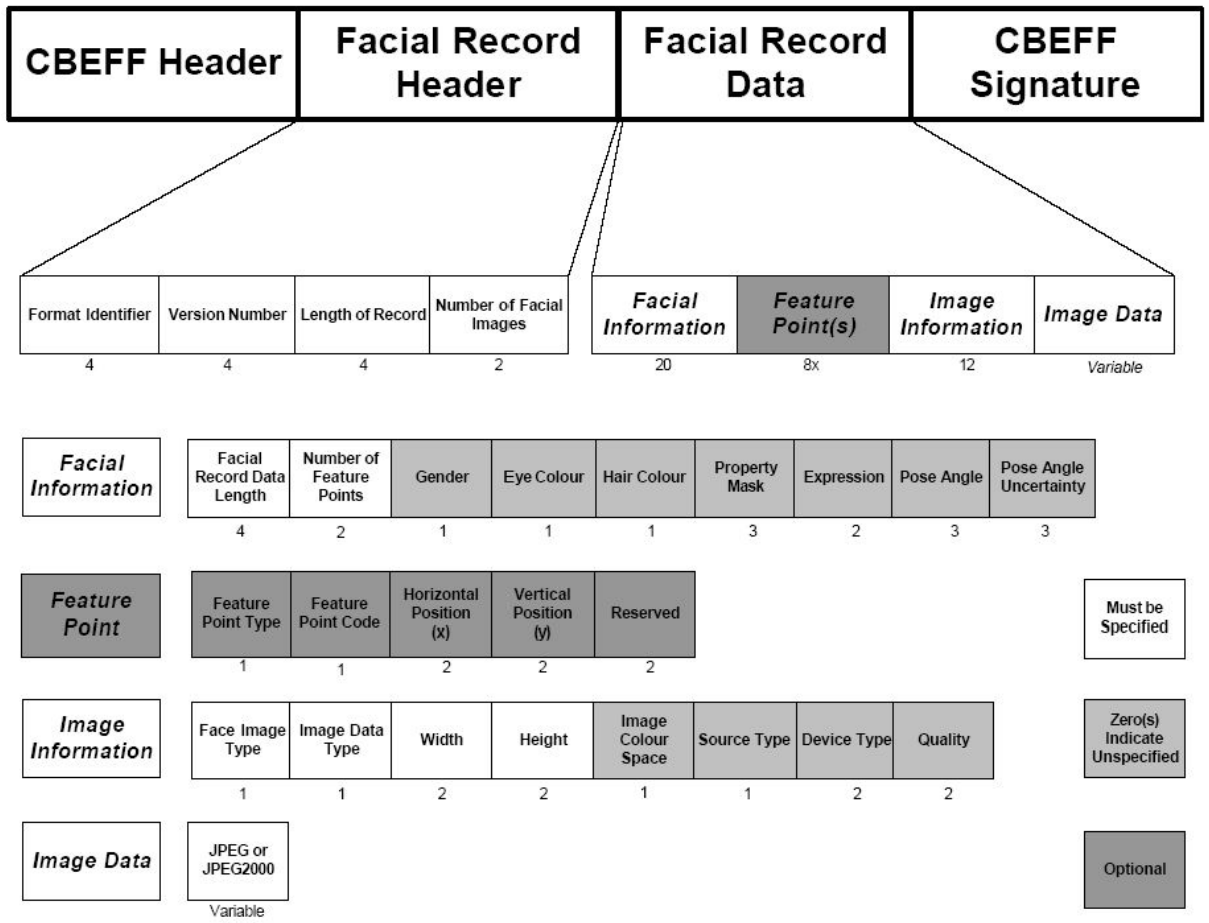

Abbildung 3.7: Face Record Format [3]

3.3.3 Erfassung der Fingerabdruckdaten als biometrisches Merkmal

Äquivalent zur Gesichtsbilderfassung, werden auch bei der Speicherung von Fingerabdruckdaten Anforderungen bezüglich der Qualität, des Erfassungsprozesses sowie der Kodierung und Kompression gestellt. Die international festgelegten ISO-konformen Bestimmung der ICAO entscheiden hierbei über die Grenzen der einzuhaltenden Qualitätsanforderungen.

Der technische Erfassungsprozess (Abb. 3.8) beginnt mit der Vorqualifizierung der einzelnen Finger jeder Hand durch die entsprechende Sensorapplikation. Somit wird vor dem eigentlichem Beginn der Fingerabdruckaufnahme definiert, welche Finger nicht zur Verfügung stehen. Grundlegend besteht die Erfassung der Fingerabdrücke aus der Aufnahme eines Fingers der rechten sowie der linken Hand. Steht eine Hand durch mögliche Verletzungen oder Amputation nicht zur Verfügung, tritt ein abweichender Aufnahmeprozess in

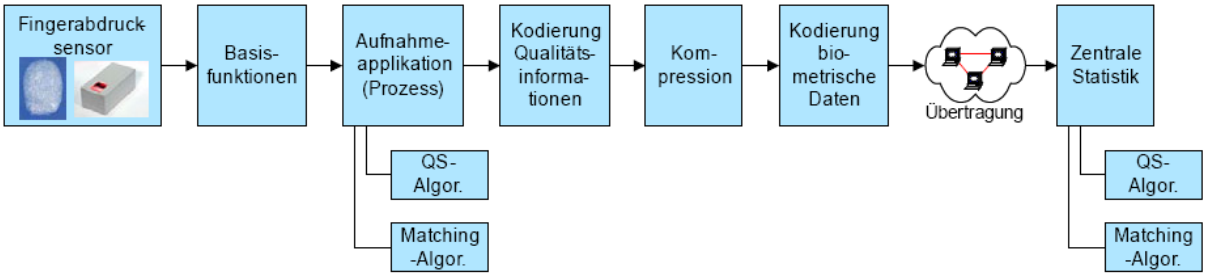

Abbildung 3.8: Erfassung und Übertragung der Fingerabdruckdaten [5]

Kraft, der durch den Sachbearbeiter vor Ort entschieden wird. Nach der optischen Digitalisierung des Fingerabdrucks realisieren die Basisfunktionen des Sensors das Segmentieren der aufgenommenen Daten. Das bekannte QS-Modul unterzieht die empfangenen Daten, anhand der mitgelieferten Parametersätze, einer Qualitätsprüfung. Anschließend erfolgt eine Testverifikation der qualifizierten Daten. Bewertungs- und Verifikationsalgorithmus entstammen beide der *NIST Biometric Image Software* (NBIS) vom *National Institute of Standards and Technology* (NIST), einer Bundesbehörde der Vereinigten Staaten, aus der schon die bekannten Verschlüsselungsalgorithmen DES und AES hervorgegangen sind. Der Prozessablauf eines Aufnahmevorgangs für einen Finger (Matching Algorithmus) ist in Abbildung 3.9 nochmals verdeutlicht.

Die oben beschriebene Aufnahme eines Fingers beginnt mit dem Zeigefinger der rechten Hand. Kann eine erfolgreiche Validierung festgestellt werden, so wird die gleiche Reihenfolge an der linken Hand durchgeführt. Bei negativem Ergebnis wird jedoch in der Reihenfolge Daumen, Mittelfinger und Ringfinger der Matching Algorithmus wiederholt. Ist kein erfolgreiches Ergebnis festzustellen wird das bisher beste, aber abgewiesen Ergebnis inklusive Parametersatz, Fingercode und negativer Wertung an den übergeordneten Prozess übergeben.

Nach Abschluss der erfolgreichen Datenerfassung, folgt die nötige Kompression in ein entsprechendes Datenformat. Hierzu kommt *Wavelet Scalar Quantification* (WSQ) zum Einsatz. Das vom *Federal Bureau of Investigation* (FBI) der Vereinigten Staaten lizensierte Format basiert auf der *Gray-Scale Fingerprint Image Compression*, einem Kompressionsverfahren, das die resultierende Bilddatei mit dem Faktor 0,06 verkleinert sodass die Maximalgröße von 18kByte nicht überschritten wird. Sollte eine Dateigröße diesen Grenzwert überschreiten, ist es möglich im Einzelfall eine stärkere Kompression zu verwenden um den Toleranzbereich von 1kByte nicht zu überschreiten.

3.4 Sicherheitsmechanismen in der kontaktlosen Datenkommunikation von ePass

Thema dieses Abschnittes ist es, einen Überblick über die Ziele und die Funktionsweise der Sicherheitsmechanismen zu geben, die im Rahmen des kontaktlosen Informationsaustausches von ePass zur Anwendung kommen. Grundlegend ist das sicherheitstechnische Vermögen der Kommunikationsbeziehung zwischen Reisepass und Lesegerät auf zwei

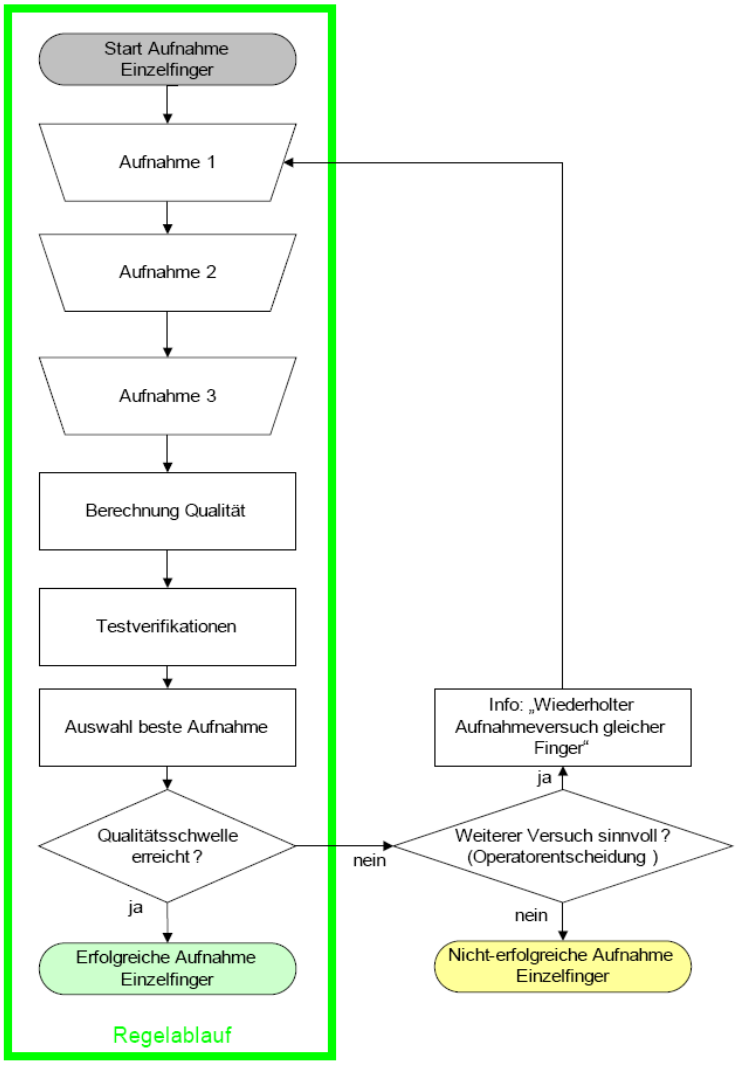

Abbildung 3.9: Aufnahme Einzelfinger(Matching Algorithmus)[6]

Schwerpunkte begrenzt: die Steigerung der Fälschungssicherheit zu garantieren sowie den Missbrauch von persönlichen Daten zu verhindern. Tragende Elemente in der internationalen Standardisierung von Reisepässen sind die technischen Spezifikationen der ICAO. Die Definition der digitalen Speicherung von Name, Geburtsdatum, Geschlecht, Nationalität, Gesichtsbilddaten und Fingerabdruckdaten erfolgt auf dem RFID Chip gemäß logischer Datengruppen. Diese organisatorische Datenstruktur gibt, neben den herkömmlichen Informationen, Auskunft über Hash-Werte der einzelnen Datengruppen, verwendete Zugriffsverfahren und vorhandenen Zertifikate sowie Signaturen. Die Existenz der einzelnen *Datagroups* (DG) in der *Logical Data Structure* (LDS) auf dem Chip ist variabel gestaltet und nur für die ersten zwei Vertreter verpflichtend. DG1 beinhaltet die Informationen der Machine Readable Zone (MRZ) des üblichen Reisedokuments. Das digital gespeicherte Gesichtsbild wird als global festgeschriebenes Merkmal in DG2 abgelegt. Die von der ICAO als optional definierte Datengruppe, welche den biometrischen Fingerabdruck umfasst, wurde später in Europa durch EG-Richtlinien zum Pflichtprogramm erklärt. Auch die Verfahrensweisen zur Erhöhung der Fälschungssicherheit und dem Schutz vor unautorisierten Abhören der Kommunikation sind durch die oberste zi-

vile Luftfahrtbehörde wenig eingeschränkt. Erst das Eingreifen der Europäischen Union definierte standardisierte Sicherheitsrichtlinien, welche in Tabelle 3.2 aufgezeigt werden. Die markierten Sicherheitsmechanismen zur kontaktlosen Datenkommunikation in ePass werden im Folgenden näher beschrieben.

Datengruppe	**Bedeutung**
DG1	personenbezogene Daten (MRZ)
DG2	Gesichtsbild
DG3	Fingerabdrücke
DG14	Chip-Authentisierung öffentlicher Schlüssel
Document Security Objects	Hashwerte aller Datengruppen

Tabelle 3.1: Verwendete ICAO-Datengruppen im ePass (Auszug)

Sicherheitmechanismus	**ICAO-Vorgabe**	**EU-Vorgabe**
MRTD Basic Access Control	optional	vorhanden
Passive Authentisierung	vorgeschrieben	vorhanden
Aktive Authentisierung	Optional	n. vorhanden
Extended Access Control	Optional	vorhanden

Tabelle 3.2: Verwendete ICAO-Sicherheitsvorgaben in ePass

3.4.1 Passive Authentisierung

Um die Integrität der Datengruppen zu gewährleisten, bedient sich die Passive Authentisierung eines einfachen Verifikationsverfahrens, das die Sicherung der *Document Security Objects* (DSO) über digitale Signaturen möglich macht. Die unberechtigte Manipulation der gespeicherten Daten im Reisepass würde die Signatur unbrauchbar machen und somit das kryptografische Kontrollverfahren zu einem negativen Ergebnis zwingen.

Fundament dieses simplen, jedoch aber effizienten Schutzvorgangs, ist eine von der ICAO geforderte und global interoperable Public Key Infrastructure. Diese zweistufige Baumstruktur dient der Zertifikatsvergabe und besteht aus einer Country Signing Certification Authority (CSCA) im Wurzelknoten und mehreren Document Signern (DS). Die Country Signing CA ist die oberste Zertifizierungsstelle eines Landes und wird in der Bundesrepublik Deutschland durch das BSI repräsentiert. International übergeordnet gibt es nichts weiter, so wird sichergestellt, dass jedes Land die Kontrolle über seine Schlüssel zum signieren der Zertifikate besitzt. Die Zertifikate dürfen nur auf diplomatischem Wege weitergereicht werden, müssen aber auch an die ICAO zur Prüfung gegeben werden. Aus dem erzeugten Schlüsselpaar wird der Private Key dazu verwendet um Document Signer zu zertifizieren. Der Public Key wird an die ICAO weitergegeben. Der durch das Zertifikat der CA berechtigte Document Signer, in der Regel vom Passhersteller repräsentiert, ist nun

in der Lage mittels seines eigenen Schlüsselpaars die sicherheitsempfindlichen Daten des Reisedokuments zu signieren. Die Echtheit der Daten kann im Falle einer Grenzkontrolle mit dem entsprechenden öffentlichen Schlüssel verifiziert werden. Aufgrund der langen Verwendungsdauer der Schlüssel (vgl. Tabelle 3.3) muss ein entsprechend starkes Signaturverfahren zum Einsatz kommen. Der deutsche Reisepass verwendet die Systematik des Elliptic Curve Digital Signature Algorithm (ECDSA).

Institution	**Dauer Private Key**	**Dauer Public Key**	**Schlüssellänge**
CSCA	3-5 Jahre	13-15 Jahre	256 Bit
DS	max 3 Monate	10 Jahre 3 Monate	224 Bit

Tabelle 3.3: Verwendungsdauer und Schlüssellänge bei Einsatz von ECDSA und einer Passgültigkeit von 10 Jahren

3.4.2 Zugriffsschutz

Schwerpunkt vom Sicherheitskonzept im Rahmen von ePass ist der Zugriffsschutz. Die Vermeidung des nicht autorisierten Auslesens von digital gespeicherten Gesichtsbild- und Fingerabdruckdaten steht dabei im Vordergrund. Diese Bedrohungslage ist dabei in zwei Problemfelder zu unterteilen. Der versteckte Zugriff auf die Daten im zugeklappten Zustand des Passes wurde dabei als primäre Gefahrenquelle identifiziert und durch den Einsatz von BAC unterbunden. Ein weiteres Szenario beschreibt den offensichtlichen Zugriff auf den Reisepass durch ein gefälschtes Lesegerät. Die im Rahmen von Extended Access Control entwickelte Lesegerät-Authentifizierung garantiert Schutz vor möglichen Angriffen dieser Art. Im Folgenden wird die Funktionsweise beider Zugriffsschutzmechanismen detailiert beschrieben.

Basic Access Control (BAC)

Grundlegender Stützpfeiler für den Schutz gegen das unberechtigte Lesen der auf den Chip gespeicherten Daten ist eine indirekte logische Verknüpfung dieser Daten mit der zugehörigen Datenseite des Reisepasses. Die wichtigsten personenbezogenen Daten sind sowohl auf dem Chip (in der Datengruppe DG1), als auch auf der Datenseite in maschinenlesbarer Form, in der sogenannten Machine Readable Zone (MRZ), abgedruckt. Das optische Einlesen der personenbezogenen Daten wurde bereits vor der Einführung des elektronischen Reisepasses zur Personenidentifikation benutzt. Die Überprüfung der Verknüpfung zwischen MRZ und der digitalen Informationen wird implizit durch den Chip erzwungen, denn ein Zugriff auf die Daten erfordert die Kenntnis der MRZ, die damit selbst als Zugriffschlüssel dient.

Im Einzelnen bedeutet dies, dass das Lesegerät die MRZ optisch ausliest und sich danach mit dem erforderlichen Schlüssel, generiert aus Passnummer und Ablaufdatum des Reisepasses sowie Geburtsdatum des Passinhabers, um sich gegenüber dem Chip auszuweisen. Nach Generierung einer Zufallszahl aus festgelegten Werten, wie Datum und den

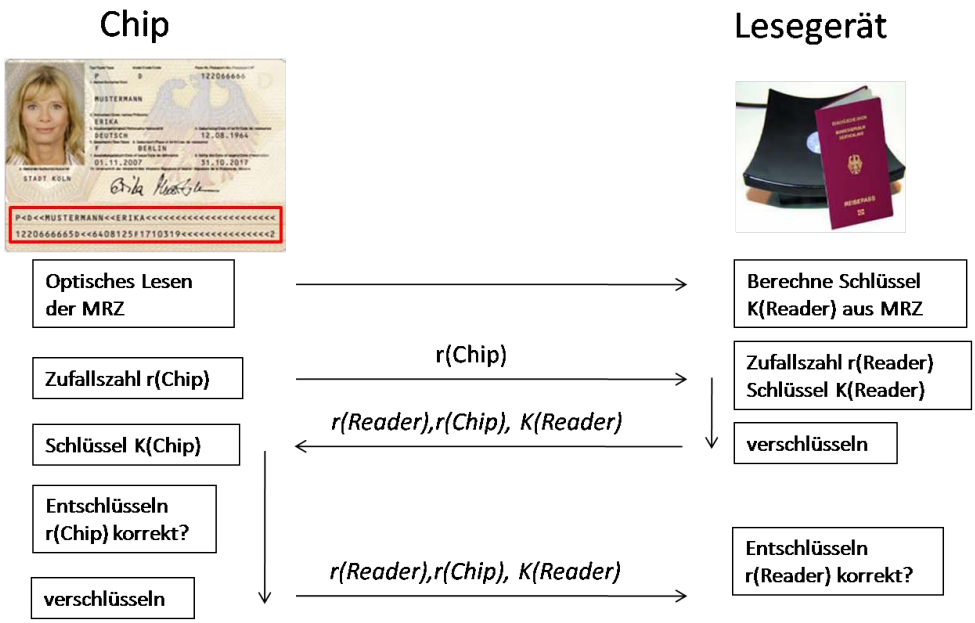

Abbildung 3.10: Einzelschritte in Basic Access Control [1]

gespeicherten Chipinformationen auf beiden Seiten, folgt deren Austausch um somit die Kenntnis über die korrekten Schlüsselhälften zu belegen (vgl. Abb. 3.10).

Die möglichen Schlüssel ergeben sich aus der neunstelligen Passnummer (10^9 Möglichkeiten), der Anzahl von möglichen Geburtstagen (ca. 356×10^2) und der Menge an Passverfallsdaten bei einer Gültigkeit von 10 Jahren (356×10). Somit berechnen sich ca. 2^{56} mögliche Schlüssel ($356^2 \times 10^{12} = 2^{56}$) mit einer resultierenden Schlüsselstärke von 56 Bit.

Nach dem erfolgreichem Abschluss der BAC-Authentisierung gestattet der RFID-Chip den Zugriff auf die personenbezogenen Daten und das Auslesen der einzelnen Datengruppen, um den Weg für weitere Zugriffsmechanismen zu ebnen. Der im Voraus ausgehandelte Sitzungsschlüssel (56 Bit) dient nun der sicheren Schlüsselübertragung im Rahmen von Triple Data Encryption Standard (3DES). Dieser symmetrische Verschlüsselungsalgorithmus stützt sich auf die dreifache Anwendung des weit verbreiteten Kodierungsverfahrens, in der nach der Stückelung des Klartextes zu 64 Bit Blöcken, die Verschlüsselung mit einem 56 Bit Schlüssel mit anschließender Permutation erfolgt. Zur Erhöhung der Sicherheit kann der 56 Bit lange Schlüssel des DES-Verfahrens vergrößert werden, indem das DES-Verfahren mit einem weiteren Schlüssel auf den Chiffre-Text der ersten Verschlüsselung angewendet wird. Das Ergebnis ist eine mit zwei unabhängigen Schlüsseln gesicherte Chiffre, also mit 112 Bit-Schlüsseln. 3DES entspricht als symmetrisches Verfahren einer äquivalent starken Verschlüsselung, wie es ein 2048 Bit RSA-Schlüssel garantieren kann. Abbildung 3.11 verdeutlicht den Ablauf von 3DES.

Extended Access Control (EAC)

Wurde im Rahmen von Basic Access Control noch auf Daten zugegriffen, welche auch aus anderen Quellen einfach zu beschaffen gewesen wären, schützt EAC hingegen sicherheits-

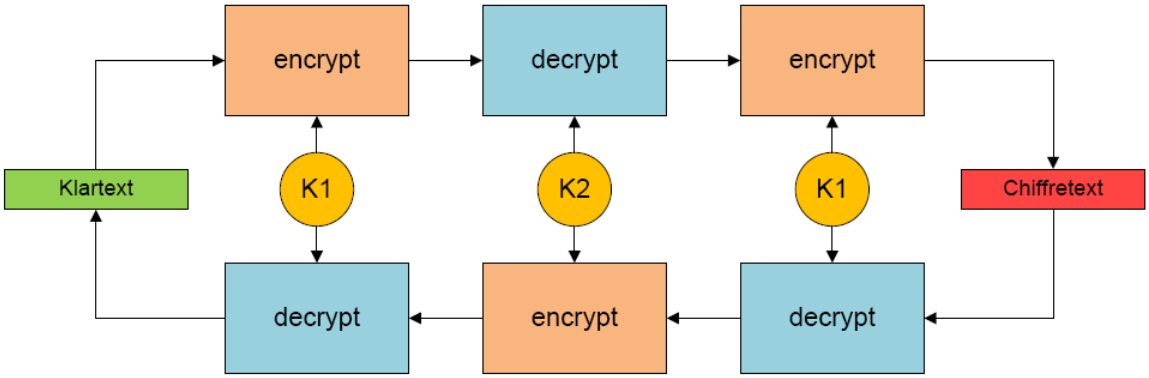

Abbildung 3.11: Triple Data Encryption Standard

empfindliche Informationen, deren Verschluss hohe Priorität hat. Mit der Speicherung der Fingerabdruckdaten in Phase zwei des ePass-Projektes wurde das ursprüngliche Sicherheitskonzept nicht verworfen, sondern nur ein neuer Schutzwall um den inneren Kern geformt. Grundlegend wird EAC in die Chip- beziehungsweise Terminal-Authentisierung unterteilt.

Die Chip-Authentisierung garantiert im Gegensatz zur passiven Authentisierung nicht die Authentizität der gespeicherten Daten, sondern die Echtheit des RFID-Chips. Das Verfahren basiert darauf, dass in einem sicheren, nicht auslesbaren Bereich des Chips ein individueller, privater Schlüssel gespeichert ist. Der zugehörige öffentliche Schlüssel wird hingegen in einer durch passive Authentisierung geschützten Datengruppe verfügbar gemacht. Der private Schlüssel kann somit vom Chip für die Authentisierung verwendet werden. Der Beweis der Echtheit des privaten Schlüssels erfolgt implizit über die Fähigkeit der stark gesicherten Kommunikation durch einen integritätsgesicherten Kanal mittels Schlüsseleinigungsverfahren nach Diffie-Hellman. Die Systematik sieht vor, dass der in Datengruppe DG14 gespeicherte öffentliche Schlüssel auf Seiten des Lesegeräts und der öffentliche Schlüssel des Terminals auf Seiten des Chips zur Schlüsseleinigung verwendet werden. Der deutsche Reisepass ermöglicht im Zuge der Chip-Authentisierung nicht nur den Echtheitsnachweis, er vereinbart gleichermaßen auch die Verwendung eines deutlich stärkeren Sitzungsschlüssels mit einer Stärke von 224 Bit und garantiert somit die sichere Übertragung der sensitiven Daten.

Die Terminal-Authentisierung, welche direkt nach Abschluss der Chip-Authentisierung beginnt, dient in erster Linie der Echtheitsprüfung des Lesegeräts um den folgenden Lesezugriff auf hochsensitive Datengruppen zu gewähren. Vereinfacht ausgedrückt zwingt der RFID-Chip das Lesegerät sich auszuweisen. Die Authentisierung entspricht daher einer Art *Challenge Response Protocol*, in dem der erste Schritt die Übertragung einer Zertifikatskette vom Lesegerät zum RFID-Chip beinhaltet. Grundlage dieses Vorgangs ist eine zweistufige PKI, welche zentral von der Country Verifying Certification Authority (CVCA) als Wurzelinstanz geleitet wird. Die Zertifikatsvergabe an die Lesegeräte erfolgt direkt durch den Document Verifier (DC), der in der Regel auch der Gerätehersteller ist. Die DV-Zertifikate werden wiederum durch die CVCA ausgestellt. Eine wichtige Funktion

der Zertifikatskette ist nicht nur die Verifizierung des Lesesystems als berechtigtes Gerät, es dient ebenso der Festlegung welche sensitiven Daten im internationalen Reiseverkehr durch ein ausländisches Lesegerät ausgelesen werden dürfen. Welche Daten dies im Einzelfall sind, bestimmt immer der Staat, aus dem der Pass stammt. Die zur Verifizierung der Zertifikate notwendigen öffentlichen Schlüssel werden direkt durch das BSI, die deutsche CVCA, vergeben und als eine Art Vertrauensanker auf dem Reisepass-Chip gespeichert. Nun zurück zum Protokollablauf, in dem sich das Lesegerät mithilfe der Zertifikatskette gegenüber dem Chip authentisieren muss, wobei die Kette mit dem, auf dem Chip gespeicherten, öffentlichen Schlüssel der passherstellenden Wurzelinstanz enden muss. Dieser Mechanismus gibt der Bundesrepublik Deutschland die volle Kontrolle welche Staaten auf die sensitiven Daten des deutschen Reisepasses zugreifen dürfen (vgl. Abbildung 3.12). Im Detail geschieht dies dadurch, dass der Chip eine generierte Zufallszahl übermittelt, welche mit dem Hash-Wert des öffentlichen Schlüssels durch das Lesegerät mittels privaten Schlüssel signiert wird. Der RFID-Chip überprüft diese Signatur und gleicht diese mit seinem Hash-Wert des öffentlichen Schlüssels ab. Tritt ein Gleichnis auf, so hat das Lesegerät fortan Lesezugriff auf die sensitiven Daten des Chips, welche im Fall des deutschen Reisepass durch die Fingerabdruckdaten repräsentiert werden.[9]

Zusammenfassung des Ablaufs einer Passkontrolle

Die digitale Kommunikation zwischen Lesegerät und RFID-CHip unterteilt sich in folgende Schritte:

1. **Basic Access Control**
   - Grundlegende Verschlüsselung durch den Triple Data Encryption Standard
   - Lesegerät erhält Zugriffsrechte auf Datengruppen DG1, DG2, DG3 und DG14 (vgl. Tabelle 3.1)
2. **Passive Authentisierung**
   - Verifikation der Echtheit der Daten durch Signaturprüfung
   - Lesegerät erhält Zugriffsrechte auf Document Security Objects (DSO) und öffentlichen Schlüssel aus DG14 in Vorbereitung auf die Chip Authentisierung
3. **Chip Authentisierung (EAC)**
   - Chip ist echt
   - Aufsetzen einer noch stärkern Verschlüsselung mit der Schlüsseleinigung nach Diffie Hellman
4. **Terminal Authentisierung (EAC)**
   - Terminal ist berechtigt auf hoch sensitive Daten zu zugreifen
   - Leserechte auf hoch sensitiven Daten im Falle des Vorhandenseins der korrekten Zertifikate

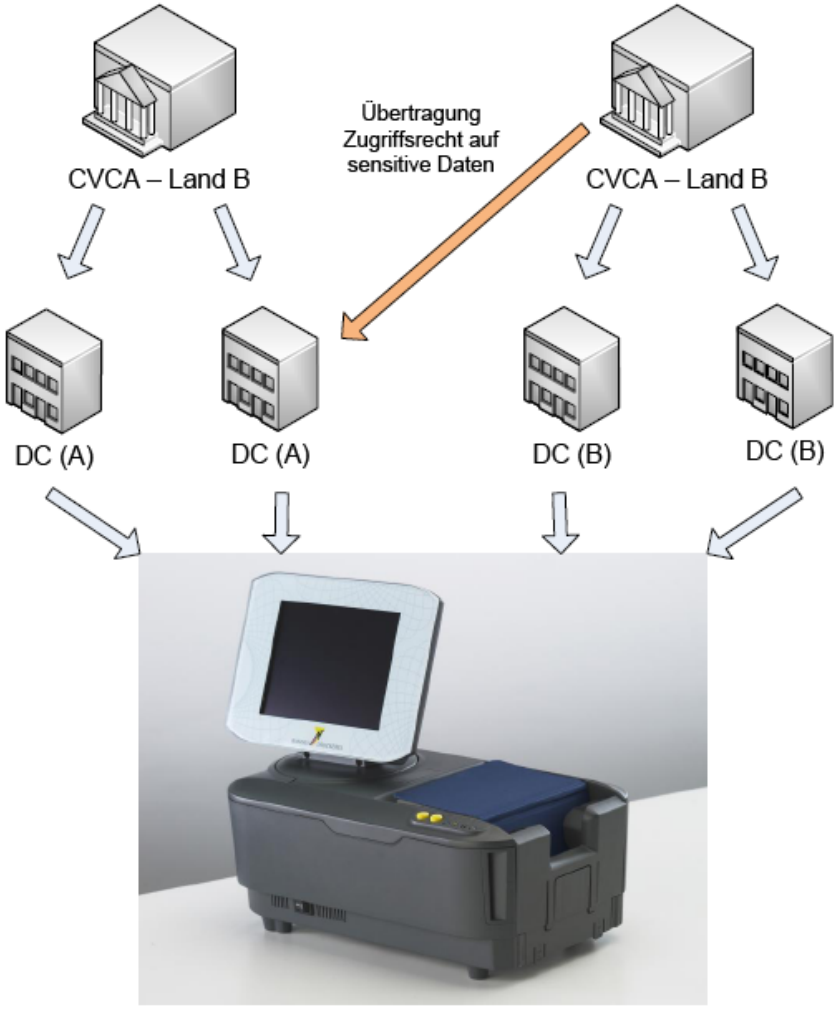

Abbildung 3.12: Zertifikatsvergabe innerhalb der Public Key Infrastructure durch die Country Verifying Certification Authority (CVCA) und den Document Verifyer (DC). Das Foto zeigt das in Deutschland verwendete Lesegerät Visotec E100 der Bundesdruckerei [2]

3.5 Diskussion der Sicherheitsaspekte

Mit dem Entschluss der Europäischen Union, den Vorschlägen der ICAO zu folgen und sicherheitsempfindliche Daten auch digital auf Reisepässen zur Verfügung zu stellen, wurden daraufhin Bedenken geäußert, welche die IT-Sicherheit des ePass-Projekts in Fragen stellten. Datenschützer beschrieben Szenarien des gläsernen Bürgers, der bei Verwendung des neuen ePass zu jeder Zeit Gefahr läuft seine persönlichen Daten preiszugeben und eventuell sogar die digitalen Daten des RFID-Chips einer nicht beabsichtigten Änderung unterzieht. Sei es das Erstellen von aktiven Bewegungsprofilen oder das Abhören der Kommunikation zwischen Lesegerät und Chip, das Modell möglicher Ereignisse hatte meist negativen Charakter. Meist war es jedoch mangelnde Information, die jenes trügerische Bild verbreiten ließ. Die vorgestellten Sicherheitsmechanismen im Schwerpunkt dieser Se-

minararbeit sollen nun auf mögliche Bedrohungssituationen angewandt werden, um deren Vertraulichkeit aufzuzeigen.

3.5.1 Diskutierte Angriffsszenarien

Unberechtigtes Auslesen der Chipinhalte

Grundlegend muss dieses Problemfeld in zwei Situationen unterschieden werden: das nicht autorisierte Auslesen der Passinformationen, während sich der Reisepass geschlossen in der Tasche befindet und der illegale Zugriff auf die Daten während des willentlichen Akts des autorisierten Auslesens mittels gefälschten Lesegeräten an der Passkontrolle).
Um einen Zugriff auf den geschlossen ePass einzuleiten, müsste der Angreifer zunächst den benötigten Mindestabstand zur fehlerfreien Kommunikation unterschreiten. Das Überschreiten dieser physikalischen Grenze zöge einen exponentiellen Anstieg der Leistung nach sich, um die Verbindung zum Reisepass aufrecht zu erhalten. Selbst mit der Annahme der Angreifer hätte diese Barriere überwunden, stünde er immer noch der Suche nach einem geeigneten Zugriffsschlüssel im Rahmen von Basic Access Control gegenüber. Wie in Abschnitt 3.4.2 beschrieben, benötigt dieses Zugriffsverfahren die Passnummer, das Geburtsdatum und das Ablaufdatum um einen korrekten Schlüssel zu ermitteln. Das wahllose Ausprobieren aller möglichen Kombinationen wäre in der kurzen Zeit nicht denkbar, da selbst bei der Möglichkeit das Alter des Passbesitzers oder das Passablaufdatum abzuschätzen, die mögliche Schlüsselanzahl nicht unter ein realistisches Maß fällt (vgl. Abschnitt 3.4.2).
Selbst mit der Annahme, der Angreifer hätte durch längere Nachforschungen die benötigten Informationen beschaffen können, wäre seine Ausbeute mager. Die durch BAC preisgegebenen Daten würden nur das offenbaren was der Angreifer schon weiß, die optisch lesbaren Daten der MRZ des Reispasses. Das digital gespeicherte Passbild würde zwar in der Originalkodierung offenliegen, wäre aber aufgrund der folgenden Signaturprüfung unbrauchbar. Ist der Angreifer hingegen nur an einem Foto interessiert, so stellt dies im Zeitalter der digitalen Fotografie keine Herausforderung dar.
Würde der Angriff auf die digital gespeicherten Fingerabdruckdaten abzielen, so müsste zunächst ein erfolgreicher Abschluss des BAC-Protokolls vorliegen. Im Falle des Vortäuschens einer sicheren Umgebung, sodass die Aushändigung des Reisepasses den vollständigen Zugriff auf alle optisch einlesbaren Daten nach sich zieht, würde ein gefälschtes Lesegerät an den Spezifikationen des EAC-Protokolls scheitern. Die Unterwanderung der in Abschnitt 3.4.2 beschriebenen Zertifikatsvergabe an Lesegeräte durch eine nationale Public Key Infrastructure kann heute aus Sicht der IT-Sicherheit ausgeschlossen werden. Die Verwaltung aller privaten Schlüssel durch eine Wurzelinstanz (BSI) macht es unmöglich eigene Zertifikate auszustellen.

Änderung der digitalen Daten im Pass

Physikalisch würde Versuch, die gespeicherten Chipinformationen zu ändern, daran scheitern, dass jeder Chip nach seiner Fertigung eine Art Versiegelung erhält, die jegliche

Schreibrechte entfernt und nur den Lesezugriff erlaubt. Würde darüber hinaus ein Versuch unternommen die gespeicherten Daten zu manipulieren, würde die bestehende Signatur verfälscht und somit unbrauchbar gemacht werden. Der Aufgabe, die Schlüssel der autorisierten Document Signer zu bestimmen würde selbst bei enorm hoher Rechenkapazität scheitern. Die Kombination des Schutzes vor unberechtigtem Auslesen des Passinhalts und der nicht autorisierten Änderung der Passdaten führt auch zu dem logischen Schluss, dass das Klonen und Übertragen der Passinformationen auf einen anderen Chip nicht möglich wäre.

Erstellung von Bewegungsprofilen

Bewegungsprofile im Allgemeinen beschreiben das periodische Aufzeichnen von Ortskoordinaten über einen gewissen Zeitraum. In gewünschten oder legalen Beispielen dieser Anwendung der RFID Technologie besitzt das aufgezeichnete Objekt eine eindeutige Nummer (ID), die über Datenbanken zweifelsfrei einer Person oder einem Produkt zugeordnet werden können. Neben den oben beschriebenen physikalischen Grenzen und dem sicheren Zugriffsschutz begleitet den deutschen ePass eine stetig wechselnde Unique-ID (UID), die sitzungsabhängig bei jedem neuen Zugriff neu erzeugt wird. Somit entfällt das Erstellen eines Bewegungsprofils zwischen gefälschten Lesegeräten.
Eine andere Lage stellt sich dar, wenn die Informationen der Machine Readable Zone bereits bekannt und somit das BAC-Protokoll selbst für die eindeutige ortsgebundene Identifizierung sorgt. Die physikalischen Lesegrenzen und die benötigte Zeit der Authentisierung im BAC-Protokoll lässt diese Option allerdings für die Praxis untauglich erscheinen.

Abhören der Kommunikation

Dieser Vorgang beschreibt das passive Mitlesen des Informationsaustausches zwischen Lesegerät und RFID-Chip. Um den vollständigen Informationsgehalt der Kommunikation zu erfassen, benötigt der Angreifer nach der Aufzeichnung eine entsprechende Rechenanlage um die mitgeschnittenen Dialoge zu entschlüsseln. Grundlegend sieht sich der Angreifer zwei Problemen gegenüber. Die Überbrückung der Entfernung zum Kommunikationskanal zwischen Chip und Lesegerät und die Stärke der Dialogverschlüsselung. Ersteres ist laut einer BSI-Studie in einer Entfernung von 2 Meter noch möglich und ab einer Distanz von 2,70 Meter undenkbar.
Die Entschlüsselung der Kommunikation führt über die Dechiffrierung des Sitzungsschlüssels im Triple Data Encryption Standard Algorithmus und der Diffie Hellman Schlüsseleinigung. Beide Verfahren werden durch eine hohe effektive Entropie der Schlüssel gestützt und stellen selbst bei unwahrscheinlicher fehlerfreier Übertragung hohe Anforderungen an ausgeähnte Rechenmaschinen. Durch physikalische Beeinträchtigungen im verdeckten Mitschneiden der Kommunikation ist eine gewisse Fehlerhäufigkeit zu erwarten, die das Auswerten des Chiffrats unmöglich macht. Aufgrund des Aufbaus der Chiffretexte beim Schlüsselaustausch, hat ein Bitfehler weitreichende Folgen. Bei einer angenommenen Anzahl von n vermuteten Fehlern würde es circa 196^n Möglichkeiten geben, diese Fehler manuell zu korrigieren.[9]

3.6 Schluss

Schon vor der Einführung von ePass galt der deutsche Reisepass als eines der fälschungssichersten Hoheitsdokumente weltweit. Mit dem Eintritt in die erste Phase des elektronischen Reisepasses, der Speicherung von personenbezogenen Daten auf dem RFID-Chip, gelang es das schon vorhandene Sicherheitsniveau auf eine völlig neue Ebene zu heben. Auch das Einbinden der Fingerabdruckdaten in die Passstruktur erfuhr durch den Schutz von EAC keinerlei Ablass in der IT-Sicherheit. Die oben aufgezeigten Abwehrmechanismen des ePass lassen den Schluss zu, dass die geäußerten Bedenken bezüglich der Datensicherheit nicht berechtigt waren und das Vertrauen in das deutsche Passsystem weiterhin Fortbestand haben sollte. Von den praktischen Erfahrungen des Reisepasses wird mit seiner Einführung im Jahr 2008 auch der elektronische Personalausweis profitieren und so den Fortschritt des ePass-Projektes weiter vorantreiben.

Abbildungen

Literaturverzeichnis

[1] Bundesdruckerei GMBH. *ePass Fibel*, Bundesdruckerei, Berlin 2007.

[2] Bundesdruckerei GMBH. *Innovation für Personaldokumente*, Bundesdruckerei, Berlin 2007.

[3] BSI. *Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe*, BSI, Bonn 2007.

[4] BSI. *Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe(Qualitätssicherung-Gesicht)*, BSI, Bonn 2007.

[5] BSI. *Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe(Konformität)*, BSI, Bonn 2007.

[6] BSI. *Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe(QS-Finger)*, BSI, Bonn 2007.

[7] BSI. *Advanced Security Mechanisms for Machine Readable Travel Documents*, BSI, Bonn 2007.

[8] A. Juels, D. Molnar, D. Wagner. *Security and Privacy Issues in E-passports.*, Bedford, MA, USA 2006.

[9] Dr. Dennis Kügler. *Risiko Reisepass? - Schutz der biometrischen Daten im RF-Chip*, CT - Heise Zeitschriftenverlag, Hannover 2005.

[10] Bundesministerium des Inneren. *www.epass.de*, BMI, Berlin 2005.

Kapitel 4

Pervasive Computing: Anforderungen an die IT Sicherheit

Martin Scheele

Ob es nun das intelligente Haus ist, welches den Haushalt automatisch erledigt und für den Einkauf sorgt, oder ein Kraftfahrzeug, welches ohne menschliche Hilfe von A nach B fährt, die technologische Richtung bleibt die selbe: Eine komplette Vernetzung aller Geräte. Dies ist das Umfeld des Pervasive Computing. Beschäftigt man sich intensiver mit den Rechennetzwerken, wie z.B. dem Internet, so stößt man nach kurzer Zeit auf das Thema Sicherheit. Zu der Zeit, als sich das Internet noch in den Kinderschuhen befand, war der Aspekt Sicherheit, anders als heute, kein wichtiger Faktor. Die Vernachlässigung der Sicherheit wurde später zu einem großen Problem, zumal das Internet immer beliebter wurde. Nicht selten hört man heute noch von Viren, Würmern, oder anderen Schädlingen in den Nachrichten, welche der Wirtschaft schaden. Wären diese Aspekte zu Anfang mit beachtet worden, hätte das Problem sicher viel kleinere Ausmaße gehabt. Vergleicht man schließlich die Anzahl der Computer im Internet mit der Anzahl von vernetzter Elektronik im Pervasive Computing, so stellt man fest, dass das Pervasive Computing auch nur ein Netzwerk ist, welches die Teilnehmeranzahl des Internets um ein vielfaches überschreiten wird. In einem solchen Netzwerk ist die Sicherheit ein zentrales Problem und muss von vornherein betrachtet werden, damit sich die Fehler in Bezug auf die Sicherheit nicht wiederholen. In dieser Seminararbeit werden einige Beispiele der Sicherheit aufgegriffen, näher erläutert und eine, falls vorhanden, Lösungen präsentiert.

Inhaltsverzeichnis

4.1 Pervasive Computing

Der Begriff Pervasive Computing (lat. pervadere = durchdringen) bezeichnet die alles durchdringende Vernetzung von im Alltag befindlichen „intelligenten“ Objekten [5]. Dabei sind mit intelligenten Objekten Gegenstände gemeint, die ihre Umgebung wahrnehmen, mit anderen Objekten kommunizieren, mit den Nutzern interagieren und auf Ereignisse reagieren. Dies wäre z.B. bei einer Kaffeemaschine möglich, nicht aber bei einem Stein. Dabei ist dieser Begriff das industrielle Äquivalent zum Ubiquitous Computing (lat. ubiquitos = allgegenwärtig).
Im Pervasive Computing besitzen viele Objekte Sensoren und sollen durch diese Art der Wahrnehmung selbstständig handeln. So können beispielsweise Lager automatisch aufgefüllt werden, eine Kaffeemaschine kann automatisch starten, wenn der Besitzer morgens aufsteht, oder Objekte können miteinander kommunizieren und gegenseitig die Sensordaten austauschen. Es gibt unzählig viele Szenarien, welche für das Pervasive Computing in Betracht kommen, so dass man sie nicht alle aufzählen kann. Letztendlich sollen alle Gegenstände miteinander vernetzt werden.
Das Pervasive Computing beschreibt einen Ansatz zu einer virtuellen Realität. Dabei wird jedoch nicht die Welt in einem Computer abgebildet und simuliert, sondern die Gegenstände der Realität werden Teil des Informations- und Kommunikationssystem. Pervasive Computing wird zu einem durchgreifenden Wandel im Umgang mit Computern führen. Während heutige Produkte und Dienste der Information und Kommunikation in der Regel bewusst genutzt werden, wird sich dies im Pervasive Computing ändern. Da künftige Computer aufgrund ihrer Integration in Alltagsgegenstände oft gar nicht mehr als solche wahrgenommen werden, entzieht sich auch ihre Nutzung weitgehend der bewussten Wahrnehmung. Vielfältige Prozesse laufen automatisch im Hintergrund ab und interagieren im Sinne des Nutzers, ohne dass dieser explizite Vorgaben macht bzw. Entscheidungen trifft: Im Pervasive Computing denkt die Umgebung mit und wird visionsweise zu einem kooperativen Partner des Menschen.

4.1.1 Entwicklung des Pervasive Computing

Die Integration des Pervasive Computing wird ein andauernder Prozess sein. Dabei spricht man von der zweistufigen Entwicklungsperspektive des Pervasive Computing. In der ersten Stufe (PvC-1) werden innerhalb der nächsten Jahre viele Produkte und Anwendungen etabliert, die von den Entwicklungszielen Mobilität und Ad-hoc-Vernetzung gekennzeichnet sein werden. Trotz der Vernetzung und permanenten Verbindung der intelligenten Geräte werden nur isolierte Lösungen geschaffen. Gleichzeitig werden Alltagsgegenstände vermehrt mit Mikrokontrollern und Sensoren ausgestattet. Durch die Annäherung dieser beiden parallel ablaufenden Trends werden sich in der weiteren Entwicklung Insellösungen herausbilden, die vornehmlich anwendungs- oder herstellerspezifisch sind. Dabei sind diese Insellösungen souverän und mit anderen „Inseln“ nicht kompatibel. Diese Situation führt zu einer Übergangsphase, ub der die bestehenden Medienbrüche und Inkompatibilitäten der Insellösungen überwunden werden, wobei die Grenzen nicht komplett wegfallen. Dies geschieht erst mit der zweiten Stufe des Pervasive Computing (PvC-2), in welcher eine wirklich offene Vernetzungsstruktur ohne Medienbrüche etabliert werden kann. Abbildung

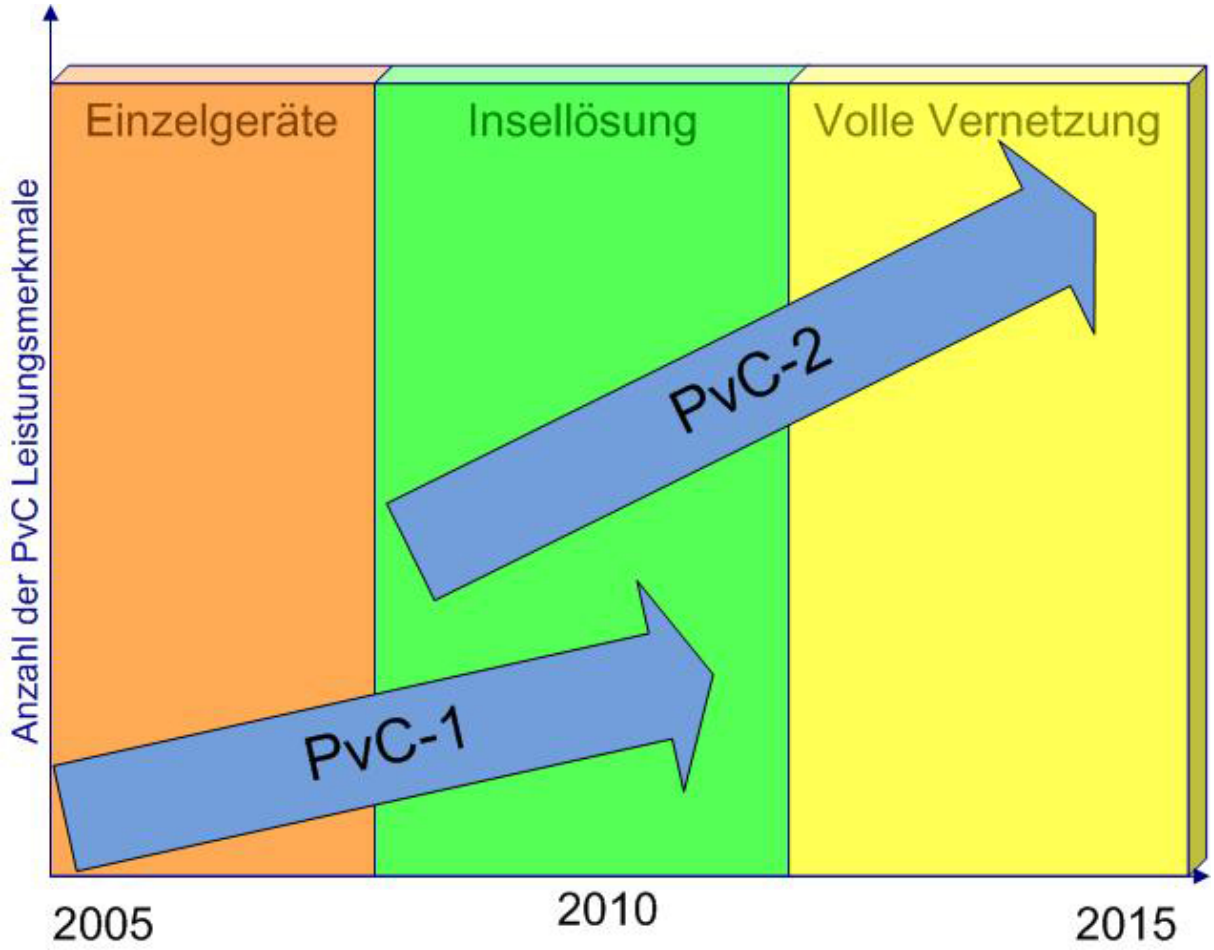

Abbildung 4.1: Zweistufige Entwicklung des Pervasive Computing

4.1 zeigt die Auswirkung der Phasen des Pervasive Computing im ersten und zweiten Entwicklungsbereich, wobei die Einflussfaktoren und Technologien die Basis für die Merkmale und somit auch die Auswirkungen. Dabei kann man die Verbindung mehrerer Technologien und deren Abhängigkeiten sehen.

4.1.2 Die technologischen Grundlagen des Pervasive Computing

Das Pervasive Computing ist keine eigene Technologie, sondern die Anwendung einer Kombination aus vielen Technologien und Forschungsfeldern. Das Pervasive Computing fordert intelligente Gegenstände, welche kaum Platz beanspruchen. Zudem sollen alle Objekte verbunden sein bzw. über ein gemeinsames Netz verfügbar werden. Für diese Anforderung lassen sich acht Technologiefelder charakterisieren, welche Einfluss auf bis zu sechs Leistungsmerkmale haben. Diese sind in der Tabelle auf Bild 4.2 zu sehen.

Aus dieser Tabelle ist zu entnehmen, welche Technologiefelder bestimmte Leistungsmerkmale des Pervasive Computing fördern. Eine Gewichtung ist aus der Tabelle nicht zu entnehmen. Ohne Zweifel sind die Kommunikationstechnologie und die Sensorik einige der wichtigsten Voraussetzungen.

	Mobilität	Einbettung	Ad-Hoc-Netzte	Kontext-Sensitivität	Energie-Autarkie	Autonomie
Mikroelektronik	X	X				
Energieversorgung	X		X		X	X
Sensorik			X	X		X
Kommunikations-Technologie	X			X		X
Lokalisations-Technologie	X			X		X
Sicherheitstechnik		X	X	X		X
Maschine-zu-Maschine Kommunikation		X	X	X		X
Maschine-Mensch Interaktion		X		X		X

Abbildung 4.2: Technik des Pervasive Computing [2]

4.1.3 Anwendungsfelder des Pervasive Computing

Es gibt eine große Anzahl an einzelnen Anwendungsfeldern für das Pervasive Computing. Diese finden sich hauptsächlich in:

- Logistik und Produktion
- Autoverkehr
- Innere und Äußere Sicherheit
- Identifikation
- Medizin

Innerhalb dieser Felder ergeben sich viele Anwendungsmöglichkeiten, bei denen sich eine komplette Vernetzung der Alltagsgegenstände durch das Pervasive Computing als sehr nützlich erweisen würde.
Mögliche Anwendungsszenarien wären hierbei:

1. Die Universelle ID: Dieses Beispiel sieht vor, dass es eine einzelne ID pro Person für alle Institutionen gibt. Es wird im zweiten Anwendungsszenario 4.4 detaillierter beschrieben.

2. Einkaufen ohne Kasse: Die Vision ist hier, dass der Kunde im Kaufhaus oder Supermarkt doe Ware einfach einsteckt und aus dem Geschäft geht. Am Ausgang werden sowohl die Person, als auch die eingekauften Artikel erkannt. Der fällige Betrag wird von dem Konto des Kunden abgebucht. Dieses Beispiel wurde in der Werbung durch IBM geprägt.

3. Das intelligente Haus: Hierbei handelt es sich um ein weit verbreite Zukunftsvision. Dabei soll das Haus so weit wie möglich alle Alltagsaufgaben, wie Reinigungsaufgaben, übernehmen. Zudem besitzt es viele Mechanismen, welche gegen die Vergesslichkeit des Menschen vorgehen. So kann das Haus automatisch Fenster schließen, das Licht ausschalten oder das einlaufende Wasser im Badezimmer abschalten. Außerdem soll das intelligente Haus auch in der Lage sein den Bestand im Kühlschrank automatisch aufzufüllen, indem es bei Warenmangel automatisch eine Bestellung abschickt.

4. Die dezentrale Telematik behandelt die Vernetzung im Verkehr und wird im letzten Anwendungsszenario im Abschnitt 4.5 näher beschrieben.

4.1.4 Motivation

Die vorherigen Dekaden haben gezeigt, dass die Sicherheit im IT-Bereich sehr wichtig ist. Die weltweite Vernetzung durch das Internet hat den Angreifern zahlreiche Möglichkeiten eröffnet. Zur Entwicklungszeit hat sich niemand Gedanken über die Sicherheit gemacht. Mit dem Pervasive Computing geht die weltweite Vernetzung in die nächste Runde. Dabei sollte man aus den Fehlern der Vergangenheit lernen und diesmal die Sicherheit mit beachtrachten, so dass viele unnötige Fehlfunktionen und Sicherheitslücken vermieden werden können.

4.2 Anforderungen an die IT Sicherheit im Pervasive Computing

In diesem Kapitel geht es um die Sicherheitsanforderungen im Bereich des Pervasive Computing. Die IT Sicherheit steht im Pervasive Computing auf drei wesentlichen Sicherheitsaspekten: Der Funktionssicherheit, der Informationssicherheit und dem Datenschutz. Während es bei der Funktionssicherheit eher darum geht, dass die Geräte funktionieren bzw. neue Mechanismen die ursprüngliche Funktion nicht beeinträchtigen, behandelt die Informationssicherheit die Situationen, welche sich mit dem Schutz vor Angreifern beschäftigen. Aber auch der Datenschutz, gerade in Bezug auf die persönlichen Rechte ist nicht zu vernachlässigen.

4.2.1 Funktionssicherheit

Bei der Funktionssicherheit geht es beim Pervasive Computing nicht nur darum, dass die Technik selber funktioniert, sondern vielmehr darum, dass die Integration der intelligenten Gegenstände die ursprüngliche Funktion nicht behindert oder verhindert. Dies ist gerade bei der Erweiterung von Geräten durch zusätzliche Funktionen und Module wichtig, da diese keinen schädigenden Einfluss auf den ursprünglichen Ablauf haben sollten. Die Anforderungen der Funktionssicherheit an das Pervasive Computing sind daher simpel zu

formulieren, aber teilweise komplex zu realisieren. Während einige Erweiterungen keinen Einfluss auf die Funktionssicherheit haben (z.B. ein ID Modul ohne weitere Funktionen) können andere Module ein System komplett zum Absturz bringen oder die Funktion maßgeblich beeinträchtigen, wie es im Szenario zur Objektidentifizierung 4.3 gezeigt wird. In vielen Anwendungsfällen kann das Pervasive Computing die Funktionssicherheit von anderen Anwendungen aber auch erhöhen, da es viel mehr Wahrnehmungsmöglichkeiten durch die große Anzahl der vernetzten Sensoren gibt. Die unsichtbare Anwesenheit der intelligenten Objekten kann ggf. direkt auf Fehlfunktionen reagieren. Außerdem werden viele Funktionen des Pervasive Computing in Zukunft gar nicht mehr wahrgenommen. So z.B. in der Automobilindustrie, wo sich die Scheinwerfer automatisch an die Lichtverhältnisse anpassen, die Scheibenwischer selbstständig anfangen zu wischen, oder eine System zur Stabilitätskontrolle (wie ESP von VW) die Fahrt deutlich sicherer machen. Für die Zukunft wird lediglich die Anforderung bleiben, dass man bei Pervasive Computing Systemen, welche für Leben von Menschen oder auch anderen Lebewesen bei einem Störfall schädlich sein könnten, immer eine Ausweichmöglichkeit beibehalten und die Sicherheit von Lebewesen nicht von der Technik abhängig wird.

4.2.2 Informationssicherheit

Bei der Informationssicherheit geht es um die Sicherheit der Daten vor beabsichtigten Angriffen Dritter. So sollen diese von Dritten nicht verändert oder verfälscht werden. Gerade im Bereich des Pervasive Computing, wo die Systeme viele Informationen beinhalten und/oder transportieren, wird es häufig vorkommen, dass Unbefugte versuchen eine vertrauliche Kommunikationsübertragungen zu verfälschen, zu stören oder abzuhören. Durch die hohe Integration, welche die Gegenstände des Pervasive Computing in Zukunft nahezu unsichtbar macht, fällt ein solcher Angriff auch bei Dienstanbietern und Betreibern von Infrastrukturen eher weniger auf, da die Anzahl der zu überwachenden Geräte durch die große Menge unüberschaubar ist. Die technischen Mittel für die Wahrung von Informationen sind im Pervasive Computing schon heute vorhanden, jedoch fehlt in vielen Fällen eine Anpassung der Sicherheitstechnologie an die Hardware. Dies ist z.B. der Fall, wenn es um das Public-Key-Kryptographieverfahren geht, welches sehr Hardware-lastig ist. Ebenso benötigt dieses Verfahren eine Zertifizierungsstelle. Im Allgemeinen kann man sagen, dass der Grad der Informationssicherheit von dem schwächsten Glied der Sicherheitskette abhängt. Wie bei allen digitalen Netzwerken stehen auch im Pervasive Computing die IT Sicherheitsziele Authenzität und Anonymität in Konkurrenz. Eine sichere Identifikation einer Person impliziert die Freigabe bzw. den Verlust der Anonymität. Dies ist ebenfalls der Fall, wenn eine Transition über Objekte vollzogen werden kann, d.h. ein Objekt sich eindeutig identifiziert und eine bestimmte Person als Benutzer in Frage kommt. Auch wenn dieser Bereich eher zum Datenschutz gehört, so ist gerade die Informationssicherheit eine mögliche Quelle für Datenschutzangriffe. Bei der Personen- und Objektidentifizierung zeigen sich folgende Angriffspunkte bzgl. der Informationssicherheit:

- Identifikationsnummer (ID) und ID-Träger bzw. Sender
- Lesegerät bzw. Empfänger

- Kommunikationsschnittstelle

Dabei sind folgende Angriffsszenarien möglich:

Inhalt fälschen: Angreifer fälscht Inhalt des Identifikationsträgers

ID fälschen: Angreifer erlangt ID eines Objektes und gibt sich als dieses Objekt aus

Klonen: Es wird eine identische Kopie des Objektes erstellt und versucht hiermit Leistungen von anderen Objekten zu erschleichen

Deaktivieren: Das Objekt wird von der Software deaktiviert (Löschen oder Kill-Befehle) oder physisch beschädigt. Der Angreifer erhofft sich dadurch eine Überbrückung durch nicht mögliche Identifizierung

Entfernen: Angreifer trennt ID-Träger vom Trägerobjekt und bringt den Träger auf einem anderen Objekt an

Stören: Angreifer beeinflusst bzw. stört den Datenaustausch (besonders Luft als Kommunikationsmedium)

Blocken: Angreifer verhindert die Identifikation eines Objektes, um so das Auslesen der Daten zu verhindern

Abhören: Die Kommunikation zwischen ID-Träger und Lesegerät wird vom Angreifer mitgehört und dekodiert

Man-in-the-Middle: Dies ist eine Angriffskombination aus Abhören, Blocken und zusätzlicher Fälschung der Kommunikationsdaten. Die Daten des Senders werden vom Angreifer abgefangen, manipuliert und zum Empfänger unter dem Namen des ursprünglichen Absenders geschickt.

ID des Lesegerätes fälschen: Angreifer täuscht nicht vorhandene Leseberechtigung in Form einer Authorisierung bzw. eines Zertifikates vor.

Entfernen bzw. Deaktivieren des Lesegerätes: Angreifer entfernen bzw. deaktiviert das Lesegerät, so dass eine Identifikation nicht statt finden kann

Lesegerät ohne Erlaubnis hinzufügen: Hier versucht der Angreifer ein eigenes Lesegerät (unauthorisiert) zu installieren, um ein Identifikationsverfahren einzuleiten.

Anhand dieser Angriffspunkte können bestimmte Szenarien bezüglich Informationssicherheit bewertet analysiert werden.

4.2.3 Datenschutz

Wie schon an mehreren Stellen angedeutet wurde, haben die Sicherheitsmaßnahmen, die auf die eindeutige Identifizierung/Authentizität setzen, einen Konflikt mit der Anonymität. Denn immer wenn sich eine Person identifiziert oder ein identifiziertes Objekt einem Benutzer zugeordnet werden kann, besteht die Möglichkeit Verhaltensinformationen zu erlangen. Ebenso können bei Universalen ID Systemen, bei welchen alle Informationen an eine ID gebunden sind, mehr Daten abgegeben werden, als es gewollt ist. Dieses Problem besteht in den meisten Anwendungen vom Pervasive Computing. Daher gibt es diesbezüglich keine spezielle Überprüfung zum Datenschutz bei einzelnen Komponenten. Entweder es besteht das Risiko generell bei dem System, oder nicht.
Das Recht auf den Datenschutz bzw. auf die Entscheidung, wer die personenbezogene Daten eines Menschen haben darf und wer nicht, ist nicht direkt im Grundgesetz verankert. Es wurde jedoch durch das Bundesverfassungsgericht nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG im so genannten Volkszählungsurteil von 1983 als informationelles Selbstbestimmungsrecht als Grundrecht anerkannt.
Daher ist es notwenig die Technik und Anwendungsszenarien unter dem Aspekt des Datenschutzes zu analysieren, um festzustellen, ob es Möglichkeiten für den unerlaubten Datenraub bzw. das Herstellen von persönlichen Datenprofilen gibt.

4.3 Szenario 1: Objektidentifikation

Im ersten Szenario geht es um die Objektidentifikation. Diese ist ein wichtiger Bestandteil der Sicherheit im Pervasive Computing, da sichergestellt werden sollte, gegenüber wen man sich als Person identifiziert bzw. welches Objekt etwas verlangt. Andernfalls könnte sich ein Angreifer als Objekt ausgeben und im Vertrauen des Benutzers viele sensible Daten erschleichen, oder anderen Schaden verursachen.

4.3.1 Das Trusted Platform Module

Im Rahmen des Pervasive Computing wird hier häufig das Trusted Platform Module (TPM) genannt. Hierbei handelt es sich um einen Chip, der den Hardware-Teil der Trusted Computing Architecture darstellt. Im Großen und Ganzen bietet das Trusted Platform Module die Funktion einer Smartcard, ist allerdings für Gegenstände vorgesehen. Das TPM bietet viele Funktionen:

- Generierung von asymmetrischen und symmetrischen Schlüsseln unter Nutzung eines Hardware-basierten Zufallsgenerators. Diese werden innerhalb des TPM erzeugt, benutzt und sicher abgelegt. Da die Schlüssel das TPM nicht verlassen müssen, sind sie vor Softwareangriffen in großem Umfang sicher. Der Hardwareschutz ist vergleichbar mit einer Smartcard. TPMs sind dabei so herzustellen, dass eine physische Manipulation und Zerstörung auch die unweigerliche Zerstörung der Daten zur folge hat. Dies geschieht durch die mehrfache Verschlüsselung.

- Die Hash-Berechnung (Bilden einer Prüfsumme) dient der Versiegelung sensibler Daten. Diese werden an einen spezifischen Zustand des TPM gebunden. Eine Entschlüsselung gelingt nur, wenn die Prüfsumme wiederhergestellt werden kann, was bei Zustandsänderung oder Zerstörung des TPM nicht der Fall ist.
- Durch einen überwachten Bootvorgang kann ein Schutz der Hardware entstehen. Dabei muss nach Auslieferung das Gerät bereits in einem vertrauenswürdigem Zustand sein, welcher dann vom TPM zertifiziert werden kann.
- Das Erstellen von signierten Auskünften (Reporting) über die Werte der geschützen Speicher, sofern der Plattformbesitzer diese Auskunftserteilung autorisiert hat, ermöglicht die Zustandsüberwachung.
- Funktion zur Beglaubigung über einen Dritten. Die Attestation Identity Keys (AIK) müssen von einem Trusted Third Party (TTP) signiert werden. Anhand dieser Signierung kann auch eine Erkennung des Systems erfolgen. Daher gibt es zusätzlich eine anonyme Beglaubigung durch das Direct Anonymous Attestation (DAA). Hier wird durch matehmatische Verfahren die TTP ersetzt.
- Funktionen, so dass der Besitzer der Plattform den Chip in Besitz nehmen kann und berechtigt ist, das TPM zu aktivieren oder auch (wieder) zu deaktivieren.
- Ein vertrauenswürdiger Zeitgeber (timer), der z.B. für die Feststellung und Prüfung der Gültigkeitsdaten von Zertifikationen genutzt werden kann.

Wie auch die Smartcard kann das TPM nicht aktiv sein, sondern reagiert nur auf Kommandos. Beim Start des Gerätes muss das TPM zuerst einen Funktionstest durchführen um die Korrektheit zu prüfen. Das TPM ist einer Rechnerplattform zugeordnet und kann durch den Endorsement Key und das Endorsement Key Zertifikat das Gerät, welches mit dem TPM verbunden ist eindeutig identifizieren. Darüber hinaus besitzt es eine Reporting-Funktion, die es anderen Anwendungen erlaubt eine signierte Bestätigung der Plattform mit ihrem Zustand zu bekommen. Jeglicher Datenverkehr, sowohl intern als auch extern ist verschlüsselt und mit Passwörtern oder Hash-Werten geschützt. Das TPM wird dann eingesetzt, wenn eine Anwendung eine Identifizierung des TPM benötigt. Kann sich das Objekt anhand des TPM identifizieren, so kann die Anwendung weiter ausgeführt werden. Sollte die Identifikation und Autorisierung nicht gelingen, so muss die Anwendung den Vorgang beenden.

4.3.2 Architektur des TPM

Die Architektur des Trusted Platform Module wird in Abbildung 4.3 gezeigt.

Die Kommunikation zwischen dem Trusted Platform Module und der Umgebung erfolgt über die **Input/Output-Komponente**. Diese führt die interne Codierung durch, so dass die Kommunikation auf dem internen Bus möglich ist. Das TPM beinhaltet grundlegende kryptographische Dienste. Hierzu gehört der Zufallszahlen-Generator **(Random Number Generator)**, der aber auch von anderen Funktionen des Chips benutzt wird,

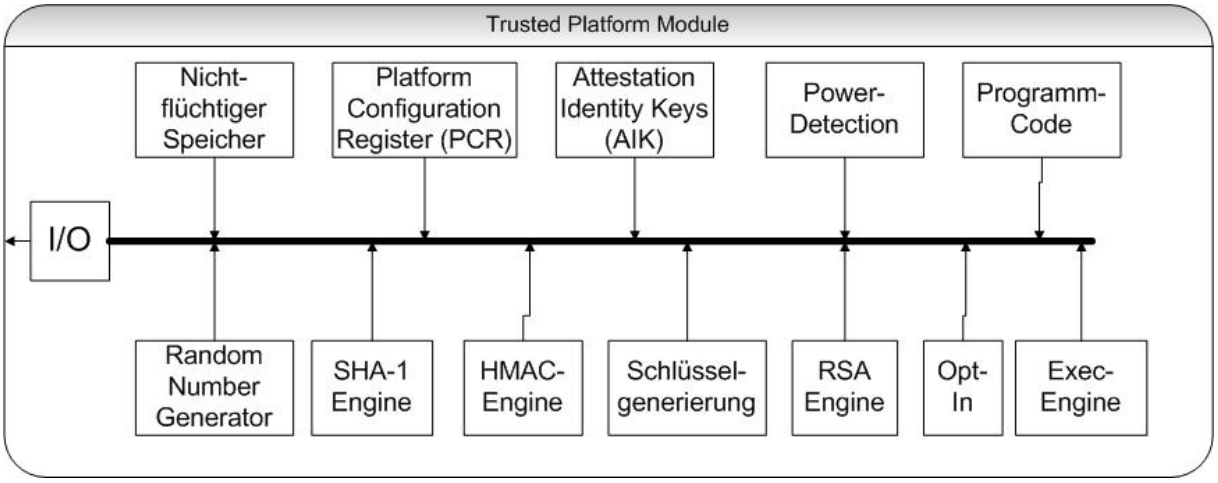

Abbildung 4.3: Architektur des TPM[1]

Desweiteren wird eine Hashfunktion **(SHA-1 Engine)** sowie eine Funktion zur Erzeugung von Message Authetication Codes **(HMAC-Engine)** geboten, wobei der MAC-Schlüssel eine Länge von 160 Bit besitzen muss. Die SHA-1 Funktion mit ebenfalls 160 Bit ist auch von außen nutzbar. Dies ist vor allem deswegen wichtig, damit während des Bootvorganges eines Objektes die Hashwerte von Systemkonfigurationen und Zuständen vertrauenswürdig berechnet werden können. Das TPM enthält ebenso eine Funktion zur Erzeugung asymmetrischer Schlüssel **(RSA Engine)** und eine Funktion für symmetrische Schlüssel **(Schlüsselgenerierung)**. Dabei muss schon bei der Generierung des Schlüssels feststehen, wofür er benutzt werden soll (Verschlüsselung, Signatur). Durch die RSA-Engine erfolgt auch die Ver- und Entschlüsselung mittels asymmetrischer Schlüssel. Die Datenformate und Implementierungsdetails für RSA-Schlüssel auf dem TPM sind durch den PKCS#1-Standard festgelegt. Das symmetrische Verschlüsselungsverfahren darf ausschließlich von internen Operationen verwendet werden, da das Exportieren des Schlüssels nach Außen eine Sicherheitslücke bedeuten könnte. Es wird nur genutzt, um den internen Verkehr zu sichern, so dass ein Abhören der einzelnen Funktions-Module auf sensitive Daten, wie Schlüssel, erheblich erschwert wird. Somit wird jeder Schlüssel wiederum verschlüsselt, was eine Schlüsselhierarchie aufbaut. Da die Spezifikation des TPM kein symmetrisches Verfahren vorschreibt, kann sowohl AES als auch 3DES zum Einsatz kommen. Die **Opt-In** Einheit dient dazu die Funktion des Chips zu aktivieren bzw. zu deaktivieren. Dies kann nur durch den Besitzer geschehen und erfordert somit dessen Autorisierung, die z.B. durch das Drücken von bestimmten Tasten erfolgt. Somit wird sichergestellt, dass die Aktivierung nicht ohne Wissen des Besitzers erfolgt. Das **Platform Configuration Register** (PCR) ist ein flüchtiger Speicher, der zur Speicherung der Hashwerte von 160 Bit Schlüssel dient. Diese werden nach dem „sicheren“ Bootvorganges des Systems berechnet und im PCR abgelegt. Es wird der flüchtige Speicher genommen, so dass ein Herausreißen des Speichers nicht dazu führt, dass die Speicherzellen ausgelesen werden können. Aus diesem Grund werden die Register auch Shielded Register genannt. Jedes TPM muss mindestens 16 dieser Register besitzen. Das TPM bietet neben der internen Verschlüsselung noch eine Art Versiegelung (sealing). Hier wird ein Systemzustand mit den Registerinhalten verschlüsselt bzw. versiegelt und kann nur zurückgewonnen werden, wenn die Schlüssel gleich bleiben, was bedeutet, dass der Systemzustand sich nicht ändern

darf. Der **Power Detection** Block sorgt für die Überwachung der Stromzufuhr für die Plattform. Dabei werden alle Veränderungen bemerkt, um so ggf. Kommandos eines Zustandes beim Wechsel des Zustandes zu stoppen. Ebenfalls sorgt dieser Block dafür, dass beim Bootvorgang der flüchtige Speicher geleert wird und die neuen Hashwerte berechnet werden können. Beim Sleep/ Hibernation Modus muss der Power Detection Block dafür sorgen, dass die Daten des flüchtigen Speichers gesichert werden. Der **Endorsement Key** (EK) ist ein nicht migrierbares RSA-Schlüsselpaar, welches dem TPM eindeutig zugeordnet ist. Es dient zur Identifizierung des TPM nach außen, d.h. es bestätigt, dass das TPM auch ein TPM ist. Das EK ist mit 2048 Bit nach dem RSA Verfahren verschlüsselt. Der EK wird vom Hersteller bei der Erzeugung des TPM generiert. Der private Schlüssel darf das TPM nie verlassen. Ebenfalls signiert das EK die Attestation Identity Keys und wird für die Generierung dieser benötigt. Die **Attestation Identity Keys** (AIK) sind 2048-Bit RSA-Signaturschlüsselpaare. Die AIK werden unter Nutzung des EK generiert. Dabei können beliebig viele erstellt werden. Sie dienen, im Gegensatz zum EK, zur Identifikation der gesamten Plattform, auf welcher der TPM verwendet wird. Dieser Mechanismus ist ein Schutz, so dass man die Objektidentität nicht auf den EK und somit auf den Besitzer zurück schließen kann. Der EK lässt sich auch nicht aus dem AIK ableiten. Da es beliebig viele AIKs geben kann, besteht auch die Möglichkeit die Schlüssel extern zu Speichern. Das **Storage Root Key** Schlüsselpaar (SRK) dient zum Ver- und Entschlüsseln von allen im TPM gespeicherten Daten und Schlüsseln, um sie vor dem Zugriff von unbefugten Personen zu schützen. Durch diese Schlüsselsignierung lassen sich alle später erstellten Schlüssel in der Hierarchie nach oben signieren. Das SRK ist im Auslieferzustand nicht vorhanden. Es wird erst vom Besitzer im TPM mit einem dafür vorgesehenen Kommando generiert, wenn dieser die Besitzübernahme durchgeführt hat. Der zum entschlüsseln benutzte private Schlüssel verlässt das TPM nie, kann aber vom Benutzer wieder gelöscht werden. Immer wenn ein neuer Besitzer gemeldet wird, wird eine neue Schlüsselhierarchie erzeugt. Somit werden alte Werte überschrieben und können nicht von anderen benutzt werden. Die **Execution Engine** führt den Programmcode aus, der von TPM-Befehlen stammt, die wiederum von außen über den I/O-Port übermittelt wurden. Der **Programm-Code** Block enthält die Firmware, mit welcher die Integrität der Geräte der Trusted Computer Group (TCG)-Plattformen bestimmt werden können. Hierbei handelt es sich um die Core Root of Trust for Measurement (CRTM), welche jedoch nicht auf dem TPM implementiert sein müssen, sondern extern angebracht sein können. Während der **flüchtige Speicher** als sicherer Schlüsselspeicher gilt und sowohl die Key-Slots als auch die PCR enthält, beinhaltet der **nicht-flüchtige Speicher** die persistenten Daten, wie den 2048-Bit Endorsement Key oder Storage Root Key und ggf. auch die AIKs, wie es Tabelel 1 zeigt.

Krypto-Funktionen	Nichtflüchtiger Speicher	Flüchtiger Speicher
RNG	DIR0, … (160-Bit)	Key-Slot 0
SHA-1	Endorsement Key (2048 Bit)	….
HMAC	Storage Root Key (2048 Bit)	Key-Slot 9
Schlüsselgenerierung	Owner Authorization Key (160 Bit)	PCR 0
Ver- und Entschlüsselung	Wenn vorhanden: AIKs	…
		PCR 15

Abbildung 4.4: Funktionen, flüchtiger und nicht flüchtiger Speicher des TPM[1]

4.3.3 Funktionsabläufe

Signierung

Wenn Daten versiegelt werden, wird der 160 Bit Hashwert erstellt. Sollte sich der Inhalt der Daten verändern, so würde ein anderer Hashwert entstehen bzw. die Hashwertkontrolle einen Fehler ausgeben. Die Daten inklusive Hashwert werden danach mit dem privaten 2048 Bit RSA-Schlüssel eines AIK verschlüsselt. Zum Lesen wird somit der öffentliche Schlüssel benötigt, welcher bei einer öffentlichen Zertifizierungsstelle verfügbar ist. Damit ist für den Leser durch die Verschlüsselung sicher gestellt, dass es sich um den richtigen Autor der der Daten handelt. Durch die Hashfunktion wird somit die Datenkonsistenz gesichert.

Identifizierung

Bei der Identifizierung fordert die Plattform den Dienst eines Anbieters an. Der Anbieter verlangt eine Bestätigung der Glaubwürdigkeit. Darauf hin signiert die Plattform ihre Systemkonfiguration (anhand der Platform Configuration Register) mit einem AIK. Diese wird dem Anbieter übermittelt, worauf der Anbieter über einen Drittanbieter, dem Trusted Third Party, den öffentlichen AIK erhält. Dieser Drittanbieter führ sowohl eine schwarze Liste mit ungültigen AIKs und öffentlichen EKs als auch eine Liste mit zertifizierten AIKs. Darauf hin wird die Bestätigung an den Anbieter gegeben. Der Anbieter überprüft Systemkonfiguration der Plattform durch die PCR. Darauf hin wird der Dienst des Anbieters der Plattform freigegeben.

4.3.4 Sicherheitskriterien

Funktionssicherheit

Durch die Nutzung des Trusted Pkatform Module ergeben sich Risiken. Gibt es Anwendungen auf der Plattform, welche das TPM benötigen und dieses defekt ist, so ist die Anwendung nicht mehr verfügbar. Zudem können die versiegelten Daten nicht mehr benutzt werden, da diese anhand des TPM Status verschlüsselt werden. Die Daten sind somit unbrauchbar, sowohl für Angreifer, als auch für den Besitzer. Werden persönliche Daten mit dem TPM verschlüsselt bzw. versiegelt, so ist die Funktion des TPM für die Daten unverzichtbar. Setzt nun ein gesamtes System auf das TPM, z.B. Verschlüsselung einer Systemfestplatte durch das TPM, so ist das System bei Ausfall des TPM nicht mehr nutzbar, da wichtige Teile fehlen. Auf diese Art können bestimmte Text- und Bildverarbeitungsprogramme nicht mehr mit anderen Programmen geöffnet werden. Ebenfalls wird auf diesem Weg die Funktionssicherheit von digitalen Dokumenten durch eine Art technisches Monopol beeinflusst werden. Hierbei sollte beachtet werden, dass eine totale Verzahnung von Anwendungen mit einem TPM ggf. keine Rückfallstrategien mehr offen lässt, um den Ausfall des TPM zu kompensieren. Sollte ein TPM Defekt dazu führen, dass Anwendungen, welche für Leib und Leben notwendig sind, nicht mehr funktionieren, so stellt der TPM ein Funktionssicherheitsrisiko für die Plattform dar.

Informationssicherheit

Die Architektur und Funktion des Trusted Platform Module eignet sich somit gut für die Identifikation von Objekten im Pervasive Computing. Die Informationssicherheit, wie sie zu Anfang gezeigt wurde, ist somit in den von den TPM abhängigen Fällen gegeben.

Inhalt fälschen: Ein Angreifer könnte durch unautorisierte Schreibzugriffe auf den TPM-Chip den Versuch starten die Dateien zu verfälschen. Dieser Angriff eignet sich nur, wenn dabei der Endorsement Key und evtl. weitere Sicherheitsinformationen unverändert bleiben, wie z.B. andere Schlüssel. Hierzu müsste der Angreifer die Identität des Besitzers annehmen, was wiederum von der Passwort und Sicherheitswahl des Besitzers abhängig ist.

ID fälschen: Der Angreifer bringt sich in den Besitz der ID und versucht diese mit einem eigenen TPM zu benutzen. Dies ist nur möglich, wenn der Angreifer ein Duplikat des TPM hat bzw. ein Gerät besitzt, das beliebige TPMs emulieren kann. Solche geräte sind bisher nicht existent.

Deaktivieren des TPM: Versucht ein Angreifer durch Lösch-/ Kill-Befehle oder physische Zerstörung das TPM zu deaktivieren, so wird auch der Inhalt nicht mehr brauchbar sein. Daher ist es nicht möglich den Inhalt zum Missbrauch zu nutzen. Jegliche Identifizierung, die das TPM benötig, ist nicht mehr möglich.

Entfernen des TPM: Ein Entfernen des TPM zur Integration in ein anderes Objekt ist nicht möglich, da das TPM fest in ein Objekt integriert ist und ein zerstörungsfreies Entfernen sehr schwer bis unmöglich ist.

Stören, Blocken, Stören: Die Übertragungsleitungen gehören nicht mehr zum TPM und können daher abgehört werden. Gerade bei kabelloser Vernetzung ist dies leichter, als bei kabelgebundenen Übertragunsmedien. Allerdings ist die Kommunikation verschlüsselt, was zumindest das Abhören erschwert.

ID des Lesegerätes fälschen: Ein Angreifer täuscht nicht vorhandene Leseberechtigung in Form einer Authorisierung bzw. eines Zertifikates vor.

ID des Lesegerätes fälschen bzw. unauthirisiertes Lesegerät hinzufügen: In einem System, welches sichere Authentifizierung gewährleistet, muss das Lesegerät gegenüber dem Objekt ebenfalls seine Berechtigung nachweisen. Somit muss ein Angreifer die entsprechenden Sicherheitsmaßnahmen überwinden, um ein Lesegerät zu fälschen oder unbefugt zu integrieren. Idealerweise verfügt auch ein Lesegerät über ein TPM.

Lesegerät deaktivieren oder entfernen: Das TPM eines zu identifizierenden Objektes hat keinen Einfluss auf den Status des Lesegerätes.

Auch wenn der Informationsgehalt nicht immer gesichert ist, so sorgt die komplexe Ver- und Entschlüsselungshierarchie für ein sicheres System, indem durch reine Abhörfunktionen die Daten schwer beziehbar sind. Sollte sich ein Angreifer als ein Objekt ausgeben, so

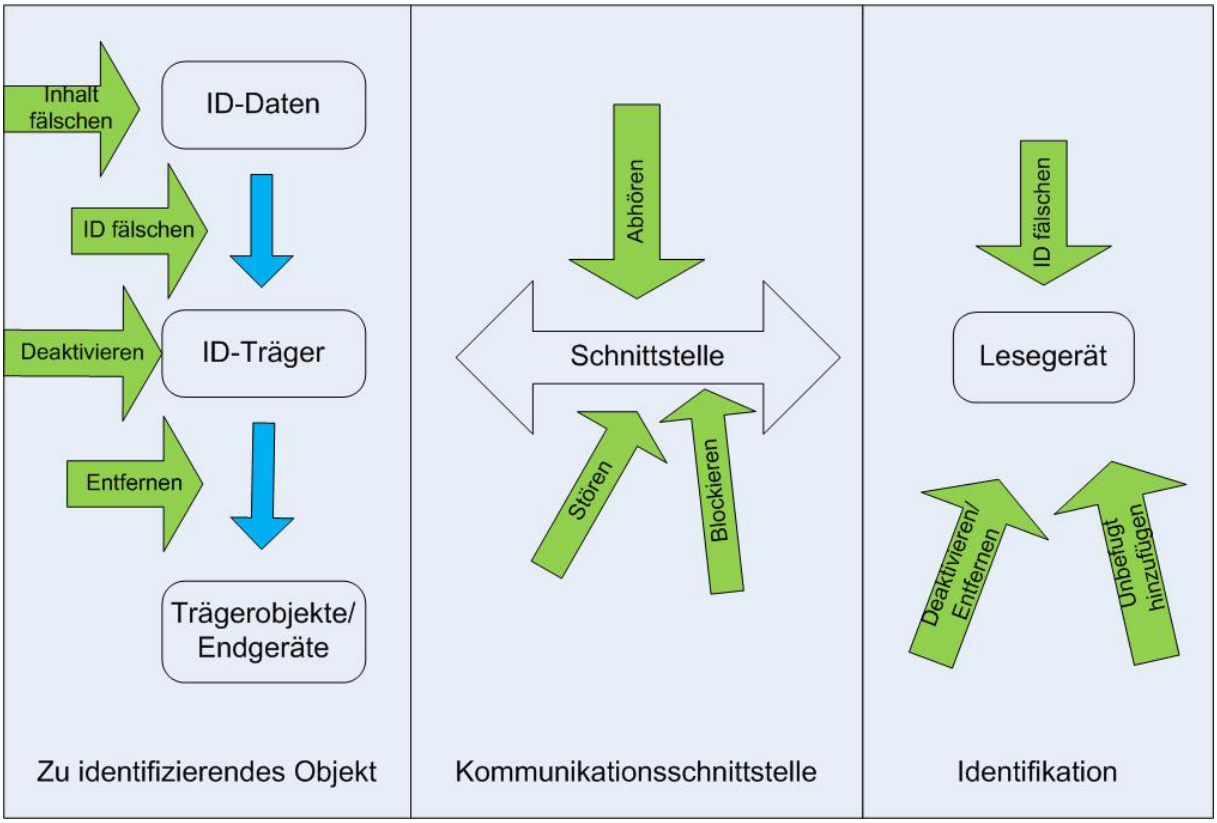

Abbildung 4.5: Angriffsmöglichkeiten auf das TPM

fehlt ihm die Möglichkeit der Identifizierung, welche durch das TPM eindeutig gegeben ist. Lediglich Angriffe gegen das Objekt mit dem TPM selbst sind nicht gesichert. Allerdings führen diese nicht zu einem Missbrauch, sondern eher zu einer Beschädigung.

4.3.5 Datenschutz

Bezüglich des Datenschutzes kann das Trusted Platform Module einerseits helfen, indem es sensible Daten des Objektes versiegelt. Durch diese Sealing-Methode können Daten gegenüber Dritten geschützt werden. Auf der anderen Seite besteht die Möglichkeit durch die Gerätzuordnung zum TPM, soweit das Gerät auch einer Person zugeordnet ist, dass über diese Personen Information und Verhaltensmuster gesammelt werden. Solange diese Funktionen aber deaktivierbar sind, ist das weniger problematisch. Wird der Einsatz jedoch erzwungen, ist ein Schutz vor solchen Datensammlungen kaum möglich. Daher ist es fragwürdig, ob die Bindung von Daten an Personen über Geräte sinnvoll ist, oder ob die Daten nicht direkt an die Personen gebunden werden sollten. Hier wäre eine Verschlüsselung durch biometrische Merkmale durchaus denkbar.

4.3.6 Chancen und Risiken in Anwendungsgebieten

Das Trusted Platform Module bietet für die Objektidentifizierung im Pervasive Computing wichtige Informationssicherheitsfunktionen wie Authentifizierung, Vertraulichkeit, Integrität und bedingte Teile von Verbindlichkeit und Anonymität. Zur Bewertung ist jedoch am wichtigsten, welche Funktionen des TPM von dem Objekt wirklich benutzt werden. Daher können Anwender (der TPM-basierenden Anwendung) und Endnutzer (mit dem TPM-Gerät) im unterschiedlichsten Maße von der Technik profitieren.
Ein Anwendungsgebiet des TPM ist z.B. das Digital Rights Management (DRM). Gerade die Musikindustrie zeigt hier viel Interesse um das Abspielen von Musik auf bestimmte Geräte zu beschränken. So könnten originale Musikstücke so verschlüsselt werden, dass sie nur von dem Gerät (z.B. MP3-Player) mit einem Endorsement Key Pair des TPM abgespielt werden können. Dies könnte zu einem wirksamen Schutz vor Raubkopien werden. Für die Nutzer schränkt dies jedoch die freie Nutzung sowohl des Gerätes als auch der Musikstücke deutlich ein. Ein ähnliches Szenario wird geboten, wenn das TPM-Verfahren bei Computern zum Einsatz kommt und für die Nutzung von lizenzierter Software benötigt wird.
Abgesehen von gewissen Nachteilen für Raubkopierer wird das TPM-Verfahren auch einige Fragen in Bezug auf die eindeutige Zuordnung bzw. Identifikation von Objekten auf. Wenn eine Zuordnungsmöglichkeit zwischen Objekten und Personen in Betrachtung genommen wird, so verringert sich die Anonymität des Nutzers bzw. wird sogar unmöglich gemacht. Diese Situation erhält man jedoch zwangsläufig in Bezug auf personennahe Authentifizierung und Anonymität. Nichts desto trotz bietet das Trusted Platform Module die gewünschten Möglichkeiten zur Schaffung von vertrauenswürdigen Plattformen. Das erhöhte Maß an Sicherheit hat jedoch, gerade im Rahmen des Pervasive Computing, einen großen Verlust an Anonymität zur Folge, was wiederum als neue Quelle für einen Missbrauch angesehen werden kann.

4.4 Szenario 2: Personenidentifikation

Nicht nur im Pervasive Computing, sondern auch im Leben muss sich jeder mit einer großen Anzahl von Schlüssel, anderen Arten der Zugangsberechtigung aber auch mit vielen Benutzeridentifikationen abgeben. Ob es nun nur eine Versicherungsnummer, eine Kontonummer, eine PIN oder ein Haustürschlüssel ist: Im Laufe der Zeit haben sich unzählige Möglichkeiten ergeben, in welchen man sich als Benutzer oder Besitzer identifizieren muss oder einfach nur eine allgemeine Zugangs- oder Fahrtenberechtigung benötigt. In Hinblick auf das Pervasive Computing wird die Anzahl im Prinzip nicht weniger. Angesichts dieser Situation wäre es denkbar alle diese Schlüssel, Nummern etc. in einem Objekt zusammenzufassen. Dieses Szenario ist in den Sicherheitsaspekten dem Szenario der Objektidentifikation ähnlich und wird nur knapp beschrieben, da der technische Teil (RFID und biometrische Merkmale) in anderen Seminararbeiten (Kapitel **??** und Kapitel 2) gründlich erläutert wird.

4.4.1 Die Universelle ID

Die Universelle ID (UID) soll als einzelnes Objekt zur Identifizierung dienen und dem Benutzer somit viel Verwaltungsaufwand ersparen, so dass man mit einem Identifikationsobjekt sowohl in der Bank sein Konto benutzen kann, eine Haus- oder Autotür öffnen kann, aber auch Fahrberechtigungen in öffentlichen Verkehrsmitteln automatisch erwerben kann. Welchen Umfang eine solche Universal ID haben soll, ist von der Anwendung abhängig. Sicher ist jedoch, dass jede UID von einer obersten Zertifizierungsstelle genehmigt und ausgestellt werden muss. Im Gegensatz zur Objektidentifizierung ist hierbei ein Benutzer eindeutig zu seiner ID zugeordnet, was ihm eine digitale Identität verschafft. Im Prinzip kann man es derzeit schon mit einem Ausweis vergleichen, wobei dieser nur einen sehr geringen Datenanteil abdeckt. Die Übertragung erfolgt dabei rein optisch, die Daten sind nicht digital, aber trotzdem für jeden Betrachter lesbar.
In die Richtung der UID gibt es bereits mehrere Pilotprojekte. In Österreich gibt es eine Bürgerkarte, welche Name und Adresse enthält, wobei neue Varianten in Planung sind, welche die Funktion der Sozialversicherungskarte für die Sozialdaten und der Bankkarte mit den Konto- und Bankdaten enthält. Außerdem sollen Studenten ihre Matrikelnummer integrieren können. Eine solche Bürgerkarte soll auch in Belgien, Finnland, Italien und der Schweiz eingeführt werden. Ähnliche Kartenanwendungen gibt es auch mit der National ID Card ind Oman, Moscow Social Card in Russland oder der National Health Insurance Card in Taiwan. Auch in Deutschland gibt es ähnliches Bestreben. Seit 2005 wird der elektronische Reisepass (ePass) eingeführt, welcher zukünftig auch mit biometrischen Daten der Person gerüstet wird. Außerdem wird ebenfalls diskutiert, ob solche Funktionen auch in einem digitalen Personalausweises enthalten sein sollten. Andere Szenarien beschreiben die Möglichkeit einer Identifikation, wobei der ID-Träger z.B. in der Kleidung angebracht wird oder direkt dem Menschen implantiert werden kann. Hierfür ist ein Gerät nötig, das eine Ad-hoc-Identifikation und Kommunikation ermöglicht. Die Technologie der UID ist folglich ein aktuelles Thema, welches von internationalem Interesse zeugt. Dementsprechend sind auch die Anforderungen an eine UID nicht gering. Gerade bei der Vereinheitlichung wird die Sicherheit immer mehr an Bedeutung gewinnen. Um diese zu Analysieren, muss jedoch vorher das Nutzerspektrum in Betracht gezogen werden. Diese sind u.a.:

- Versicherungskarten
- Kreditkarten
- EC-karten
- Firmenausweis
- Kundenkarten
- Tickets für öffentliche Veranstaltungen, Dienstleistungen und Verkehrsmittel
- Führerschein
- Sozialversicherungsdaten

- Krankenversicherungsdaten

Wichtige Unterschiede bei dem Inhalt der UID sind sowohl die Verweildauer der Daten als auch die Ausstellerinstanz. Es gibt z.B. Daten, die eine zeitliche Abhängigkeit haben, wie Tickets von öffentlichen Verkehrsmitteln. Ebenso gibt es viele verschiedene Instanzen, welche Daten auf die UID schreiben müssten.

Abbildung 4.6: Eine Universelle ID mit Ausstellerinstanzen [2]

4.4.2 Sicherheitsanforderungen an die UID

Schon hier gibt es die ersten Probleme der Sicherheit: Soll die UID von jeder Institution beschrieben werden? Wenn dies der Fall ist, so könnte aber jede Institution auf die sensiblen und persönlichen Daten zugreifen, welche für die Institution selber nicht relevant sind. Zudem besteht die Möglichkeit, wenn mehrere Instanzen auf die UID zugreifen und schreiben können, dass unbefugte Dritte auch an solche Schreibrechte gelangen. Eine Alternative besteht darin, dass die UID nur von einer Instanz beschrieben werden darf. Dies dient der Wahrung des Datenschutzes. Dafür muss ein Benutzer aber einen umständlichen Arbeitsweg in Kauf nehmen, wenn er eine UID beantragt oder etwas ändern möchte, da diese Datenänderung erst von der Ausstellerinstanz genehmigt werden muss, bevor die UID von der entsprechenden Dienststelle beschrieben wird. Auch bei den Leserechten ist es wichtig, dass die Institutionen nur auf Daten zugreifen können, welche von dem Besitzer der UID für diese Institution freigegeben wurden. So sollte ein Kaufhaus keine Auskünfte über die Versicherungen des UID-Besitzers bekommen. Allgemein sollte die Entscheidung, wer welche Daten bekommt immer von dem Besitzer kommen. Daher folgt direkt das nächste Problem: Die Identifizierung des Besitzers. Es gibt schon heute für weniger universelle Identitäten Schutzmechanismen, um den Besitzer zu identifizieren. So hat eine Bankkarte z.B. eine eindeutige Personal Identification Number (PIN) oder gewisse Benutzerkonten

arbeiten mit einer Zuordnung von Benutzernamen bzw. ID zu einem Passwort. Bei diesen Identifikationen durch Wissen wird allerdings die Identität nicht wirklich festgestellt. Ein Passwort oder eine PIN kann ohne weiteres auch weitergegeben werden. Zum anderen gibt es immer wieder Fälle, in welchen der Besitzer selber das Passwort oder die PIN vergisst. Die wissensbasierte Identifikation ist also migrierbar und bietet keine eindeutige Identifikation, sondern erschwert lediglich unbefugten Dritten den Zugriff, wobei diese die PIN bzw. das Passwort noch immer erraten könnten. Daher bieten sich für die Identifikation im Pervasive Computing die biometrischen Merkmale des Menschen an. Diese Methode verhindert zwar, dass man bewusst die Identifikation weitergibt, was bei einigen Menschen zu Umständen führen könnte, aber macht die Identifikation in den meisten Fällen sicherer und zuverlässiger. Auf die Merkmale, Technik und Sicherheitsrisiken von biometrischen Systemen wird hier nicht weiter drauf eingegangen, da dies einen anderen Teil im Rahmen des zugrunde liegenden Seminars betrifft. Letztendlich ist eine Identifikation des Besitzers gegenüber der UID unverzichtbar, unabhängig davon, welche Methode genutzt wird.

4.4.3 Sicherheit der Universellen ID

Im folgenden Teil werden die Sicherheitsrisiken (die Funktionssicherheit, die Informationssicherheit und der Datenschutz) der UID in Bezug auf die kombinierte Personenidentifikation beschrieben.

Funktonssicherheit

Im Vergleich zu der Funktionssicherheit einzelner Karten stellt die Universelle ID keinen Unterschied zu einzelnen ID Karten und Dokumenten. Der einzige Unterschied besteht darin, dass die Zerstörung oder der Verlust oder auch eine Fehlfunktion der UID für die Vielzahl an Anwendungen, welche auf die UID zugreifen, nicht mehr möglich ist, während man bei einzelnen Karten immer noch auf die anderen Karten ausweichen kann um die restlichen Funktionen zu benutzen.

Informationssicherheit

Im Vergleich zu den zu Anfang aufgelisteten Angriffsszenarien ergeben sich folgende Angriffsszenarien für die Informationssicherheit:

Inhalt fälschen: Es ist möglich, dass ein Angreifer versucht den Inhalt einer UID zu fälschen. Dies wird durch die passive Authentifizierung verhindert. Der Sicherheitsfaktor hängt hierbei von der Art und Weise ab, wie und wo die Schlüssel der DS und CSCA gespeichert wurden. Kann ein Angreifer diese erhalten, ist auch die Fälschung möglich. Die Biometrischen Daten sind durch die Extenden Access Control Methode gesichert.

ID fälschen: Ein Angreifer erlangt die ID eines Objektes und gibt sich als dieses Objekt aus. Es ist möglich, dass ein Angreifer versucht die UID zu fälschen und somit die Authenzität zu beeinflussen. Dies wird ebenfalls durch die passive Authentifizierung verhindert.

UID Kopieren: Ein Angreifer könnte versuchen die UID zu kopieren, wenn man sich in der Nähe befindet oder die UID in die Hände bekommt. Dies verhindert die aktive Authentifizierung, denn der private Schlüssel der UID ist nicht auslesbar.

Deaktivieren: Wird die UID deaktiviert, so ist es nicht mehr möglich die Leistungen zu benutzen, welche die Identifikation erfordern.

Entfernen: Dies macht keinen Sinn, da die UID nur ein Objekt ist. Ein Diebstahl vom Besitzer ist wegen der biometrischen Absicherung auch nicht möglich, solange diese nicht auch gefälscht wird.

Stören: Versucht ein Angreifer die Übertragung zu stören, so wird kein Kontakt zwischen UID und Lesegerät statt finden. Hierbei könnte eine sichre Methode, wie kontaktbehaftete UID Varianten helfen.

Abhören: Die Kommunikation zwischen ID-Träger und Lesegerät wird vom Angreifer aufgefangen und dekodiert. Während das abhören bei der RFID Technologie möglich ist, ist das dekodieren sehr viel schwieriger. Hier wird der optische Schlüssel nach der Basic Access Control Methode vorausgesetzt.

Man-in-the-Middle: Dies sollte durch die gegenseitige Identifizierung nicht möglich sein.

ID des Lesegerätes fälschen: Sollte durch die CSCA Zertifizierung nicht möglich sein.

Entfernen bzw. Deaktivieren des Lesegerätes: Wird das Lesegerät entfernt oder deaktiviert, findet keine Identifizierung statt. Hierauf hat die UID keinen Einfluss.

Lesegerät ohne Erlaubnis hinzufügen: Das auch als Skimming bezeichnete Verfahren wird durch die Basic Access Control Methode verhindert. Jedes Lesegerät braucht zum Auslesen das zertifikat der obersten Zertifizierungsinstitution.

Die UID bietet in erster Linie nur die Möglichkeit zur Authenifizierung einer Person. Viele Informationssicherheitskriterien hängen hiermit zusammen.
Die Informationssicherheit bezüglich der biometrischen Merkmale wird hier nicht behandelt, da sie den Bereich einer parallelen Seminararbeit (siehe Kapitel 3) anschneidet.

Datenschutz

Da im UID Szenario viele Daten auf dem Medium gespeichert sind, bietet dies eine vielfältige Möglichkeit persönliche Daten zu ergattern. Vom Prinzip der ICAO her ist der unberechtigte Datenklau nicht möglich, da der Zugriff auf die Daten durch das Zertifikat der obersten Zertifizierungsstelle bestimmt wird. Hier besteht lediglich die Gefahr, wenn

die UID mit einem veralteten Zertifikat des Lesegerätes arbeitet und dieses anerkennt. Ein anderer Fall ist die Erstellung von datenbezogenen Personenmustern. Die kommt z.B. durch die eindeutige Zuordnung der Person gegenüber den sonstigen Schlüsselfunktion der UID zustande. Während die Personenzuordnung bei der Bankkarte schon vorher gegeben war, ist dies für Zugtickets z.B. nicht immer von Belang. Für mehr Anonymität würde hier nur die Bereitstellung von Pseudonymen bieten. Bei dieser Anwendung muss eine eindeutige Zuordnung zwischen Person und Pseudonym entstehen. Wird diese bekannt, ist die Anonymisierung auch hinfällig. Zudem muss auch beachtet werden, dass das Erstellen von Pseudonymen ein Einschnitt in die direkte Authentifizierung sein kann und diese von ihrer Wertigkeit schmälert.

4.4.4 Aussichten für die UID

Die Universelle ID bietet hauptsächlich mehr Komfort für den Nutzer. Gerade aus diesem Grund wird sie sich durchsetzen, wenn auch langsam. Die Sicherheit hängt dabei von dem Gesamtnetzwerk, somit auch von den Zertifizierungsstellen und den Lesegeräten. Gerade in Deutschland wird der Datenschutz auch eine hemmende Funktion auf die UID haben. Hier stellt sich lediglich die Frage, in wie weit die Bevölkerung mögliche Datenangaben für Komfort heraus gibt. Ein deutlicher Nachteil wäre der Verlust der UID. Zwar sollte die Universelle ID nur vom Besitzer in Anspruch genommen werden können, aber der Verlust von sämtlichen Identifikationsmöglichkeiten wird größere Umstände mit sich bringen, als der Verlust einer einzelnen ID. Um hier für schnellen Ersatz zu sorgen, müsste die CSCA alle Daten ersatzweise gespeichert haben. Diese komplette Datensammlung stößt wiederum gegen den Datenschutz.

4.5 Szenario 3: Dezentrale Telematik

Das letzte Szenario ist das der dezentralen Telematiksysteme. Der Begriff Telematik besteht aus den Wörtern Telekommunikation und Automatik. Durch die zunehmende Integration von mikrotechnologischen und elektronischen Komponenten werden schon vorhandene Geräte „intelligenter“. Das beste Beispiel ist in diesem Fall das Automobil. Hier prüfen die Sensoren die Fahrbahnoberfläche, schalten eigenständig Licht oder Scheibenwischer ein und kontrollieren die Fahrsicherheit innerhalb gewisser physikalischer Grenzen. Auch zukünftige Ereigniserfassungen wie die Erkennung von Tieren und Menschen auf der Fahrbahn oder Abstandserkennung zwischen Autos können lokal aufgenommen werden. Bisher ist es jedoch so, dass die erfassten Daten nur für das jeweilige Objekt genutzt werden. In Verbindung mit einem Navigationssystem auf Basis von GPS oder zukünftig auch Galileo können die erfassten Daten einem Ort zugeordnet werden. Somit kann ein komplett vernetztes System aus Sensoren entstehen. Dieses Netzwerk aus Systemen zur Ortung, Sensoren und zusätzlich Telekommunikation, kann bestimmte Verfahren durch intelligente Technik erleichtern. Zum Beispiel kann bei einem Unfall automatisch Hilfe gerufen werden, bei Müdigkeit kann man sich im nächsten Motel ein Zimmer reservieren oder bei jeglichen Pannen kann die nächste Werkstatt benachrichtigt werden. Noch interessanter ist z.B. Verkehrsmeldungen wie Stau, Unfall oder auch das Wetter in Bezug auf

die Logistik, da diese Meldungen direkt vom Automobil eingebunden werden könnten. Da man gerade beim Stau auf die Sensordaten von anderen Objekten angewiesen ist muss für zuverlässige Meldungen eine Kommunikation unter den Fahrzeugen bestehen. Dies wäre durch eine einheitliche Sendestation möglich, zu welcher jedes Automobil seine Sensordaten schickt. Der Nachteil liegt hier in der Dauer, bis das Signal den Empfänger erreicht. Geschieht wenige Kilometer vor einem PKW auf der Autobahn ein Unfall und wird dieser erst dem zentralen Sendesystem gesendet und dort verarbeitet, so vergeht viel Zeit und die Meldung könnte zu spät sein. Viel besser wäre eine direkte Kommunikation an alle benachbarten Fahrzeuge, so dass diese sofort gewarnt werden und reagieren können. Diese direkte Lösung bietet das Szenario der dezentralen Telematik. Hier werden alle Sensordaten aus der Umgebung von anderen Sendeplattformen, welche de facto die Automobile wären, mit verarbeitet. Dabei handelt es sich um Ad-Hoc Kommunikation, welche je nach Reichweite eine direkte Verbindung aufbaut. Ab einer gewissen Größe sind sicherlich auch lokale Relaystationen von Interesse.
In Bezug auf die Sicherheit lassen sich im Szenario der dezentralen Telematiksysteme folgende Teilnehmer identifizieren:

- Die Autos
- Die Fahrer der Autos
- Die Infrastruktur (Verkehrszeichen, Mautsysteme, Navigation, etc.)
- Gebäude- und Anwendungsdienste, wie Raststädten, Tankstellen, Hotels, etc.

4.5.1 Sicherheit in dezentralen Telematiksystem

Da die Kommunikation wegen der Ad-Hoc Netzsituation der dezentralen Telematiksysteme nie konstant ist, sondern sich ständig ändert, muss die Sicherheit immer garantiert werden. Sobald es eine Situation gibt, welche die Technik automatisch reagieren lässt und diese für Lebewesen verantwortlich ist, darf die Technik nicht versagen. Ebenso muss die Authenzität der Verkehrsteilnehmer, insbesondere der Verkehrszeichen, gegeben sein. Schließlich wäre es mehr als nur ärgerlich, wenn das Auto nicht über eine Kreuzung fährt, weil es Signale empfängt, nach denen an dieser Kreuzung eine rote Ampel ist. Nicht zu letzt ist hier auch wieder der Datenschutz von Belang, da umfangreiche Personenprofile erstellt werden können, oder aber auch Verkehrsdelikte direkt an die Behörden übermittelt werden können. Zu diesen Herausforderungen der Sicherheit ist es ebenfalls notwendig die Vielfalt der Autoindustrie zu berücksichtigen. Denn es gibt viele Hersteller mit jeweils neue und alten Modellen.

Funktionssicherheit

Die Aufgaben der dezentralen Telematiksysteme bestehen in diesem Szenario bereits u.a. darin die Verkehrssicherheit zu erhöhen. Bereits relativ einfache Überwachungen wichtiger

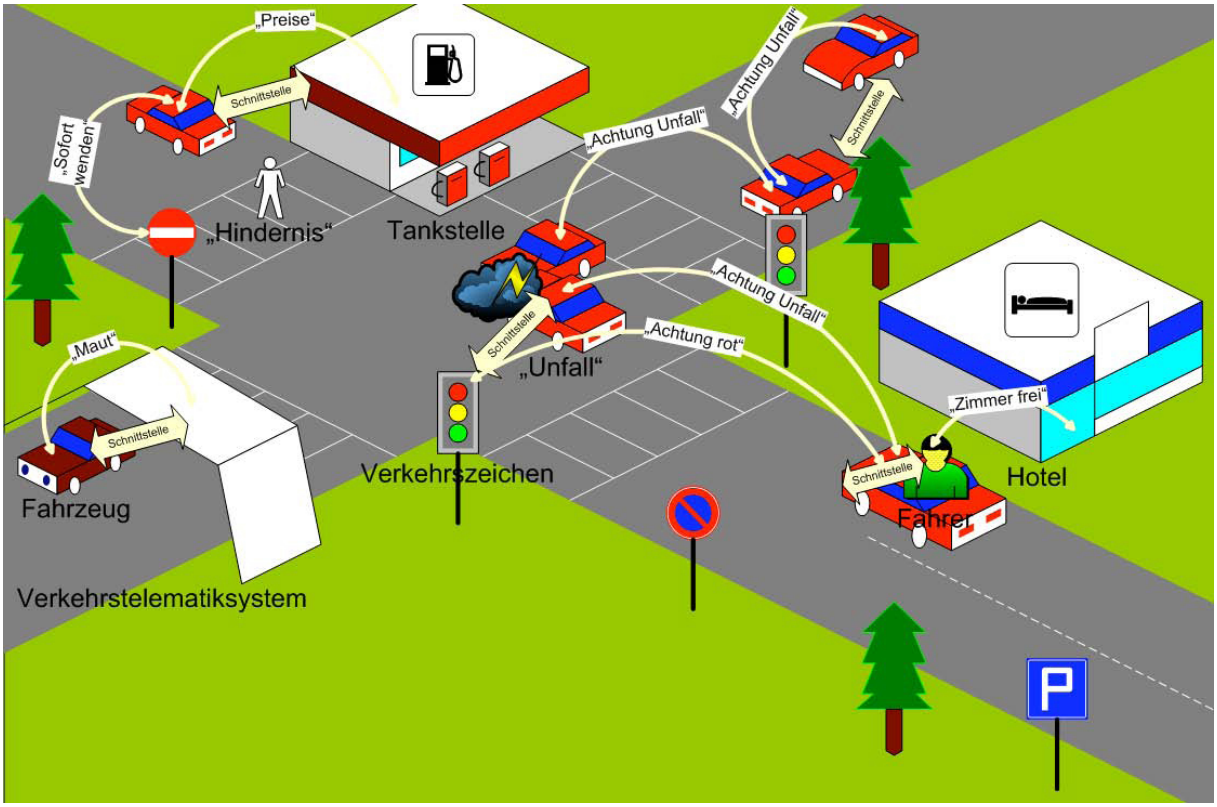

Abbildung 4.7: Anwendungsbeispiel der dezentralen Telematik [2]

Zustände, wie Fahrzeug- oder Fahrerzustand, können die Sicherheit signifikant steigern. Heutzutage dürfen Telematiksysteme den Fahrer nur indirekt unterstützten, d.h. ihn auf Fehlfunktionen etc. hinweisen, aber nicht selber eingreifen. Dies hat vor allem rechtliche Hintergründe, denn es besteht immer die Möglichkeit der Manipulation von Sensoren. In solchen Fällen könnte das Automobil zu übermäßigen Reaktionen neigen, welche folglich den Fahrer und auch andere Verkehrsteilnehmer gefährden würden. Im Szenario der dezentralen Telematiksysteme könnte eine erhöhte Sicherung der Sensoren durch einen Plausabilitätsabgleich mit Sensoren anderer Fahrzeuge getätigt werden. Somit könnte z.B. ausgeschlossen werden, dass es Glatteiswarnungen im Sommer bei 30°C gibt. Ein anderer Grund für die indirekte Unterstützung ist der Fall, dass nicht alle Fahrzeuge an dem Netzsystem teilnehmen. Sollte eine komplette Vernetzung aller Systeme im Auto bestehen, sind sicherlich auch aktivere Eingriff möglich. Kommt es zu dem Fall, dass die vernetzen Systeme des Automobils eine Internetverbindung haben, so bestünde die Möglichkeit, dass Dritte die Automobilsensoren gefährden. Daher ist es bei einer Verbindung der Sensoren und dem System des Autos mit dem Internet immer notwendig, dass der Benutzer einzelne Komponenten oder sogar das gesamte System deaktivieren kann, um sich vor möglichen Schäden zu schützen.

Informationssicherheit

Durch die verschiedenen Teilnehmer im dezentralen Telematiksystem muss man bei der Informationssicherheit mehrere Fälle unterscheiden:

- Angriff auf das Routing
- Angriff auf die Auto-Auto-kommunikation
- Angriff auf die Auto-Infrastruktur-Kommunikation
- Angriff auf die Kommunikation des Fahrers

Die meisten Angriffsszenarien zielen dabei auf das Stören oder Verfälschen der Kommunikation.
Beim **Angriff auf das Routing** wird davon ausgegangen, dass zwei Kommunikationspartner über einen Knotenpunkt Kommunizieren. Besitzt der Knotenpunkt ein falsches Protokoll, oder unterstützt andere Protokolle, als die der Teilnehmer, so tritt ein Fehler auf, das die Kommunikation nicht aufgebaut werden kann. Hier bietet sich die Möglichkeit für Angreifer diesen Punkt direkt zu manipulieren. Da der Angreifer nicht zwingend von außen auf das Netz zugreifen muss, sondern selber im Netzverkehr teilnimmt bzw. selber ein Routing-Knoten ist (was bei dezentralen Telematiksystemen immer der Fall ist, wenn die Teilnehmer auch gleichzeitig Knoten sind), bieten sich dem Angreifer mehrere Möglichkeiten:

Netzstörung: Als normaler Teilnehmer kann der Angreifer andere Teilnehmer mit Nachrichten überfluten. Zudem kann er als Routingknoten den Verkehr blocken, oder in Form einer Man-in-the-Middle Attacke die Daten manipulieren. Zudem besteht die Möglichkeit veränderte IP Pakete nach belieben durch das Netzwerk zu schicken oder das Netzwerk zu partitionieren.

Einschleusen falscher Narchrichten: Der Angreifer hat als Routingknoten prinzipiell die Möglichkeit falsche Nachrichten in das Netz zu schleusen. Dabei ist es egal, ob er in der Realität versandte Nachrichten nur gefälscht hat.

Verletzung der Privatssphäre: Durch das Mitlesen der Nachrichten ist die Privatsphäre und Anonymität nicht mehr gewährleistet.

Auto-Auto-Kommunikation Die Kommunikation von Automobil zu Automobil beinhaltet unter anderem auch die Warnung vor Hindernissen, die sich an unübersichtlichen Stellen, wie beispielsweise einer Kurve, befinden. In diesem Fall lassen sich zwei Angriffe unerscheiden:

Einspielen falscher Nachrichten: Wie beim Routing versucht der Angreifer alte Nachrichten, die er empfangen hat, erneut zu senden, neue falsche Nachrichten abzuschicken oder bestehende Nachrichten zu modifizieren. Für den ersten und den dritten Fall muss der Angreifer das kryptische System, d.h. Verschlüsselung und Zertifizierung, überwinden. Beachtet man den Zeitdruck durch den Zeitstempel, so kann man davon ausgehen, dass kein Angreifer die Rechenleistung erbringt um die Kryptografie in der kurzen Zeit zu umgehen. Im Fall der neuen falschen Nachricht muss sich der Angreifer selber authentifizieren können. Dies bedeutet, dass der Angreifer einer entsprechenden Lizenz erwerben muss, oder diese vortäuschen kann. Hier liegt die Sicherheit bei der Zertifizierungsstelle, inwiefern man ohne große Umstände an eine solche Lizenz heran kommt.

Störung des Systems: Hierbei gibt es mehrere Arten: Der Angreifer könnte die einzelnen Knoten aus dem Netz heraus attackieren, z.B. mit einem Denial of Service Angriff. Alternativ könnte er die Elektronik angreifen z.B. mit einem elektromagnetischem Puls oder anderen Störgeräten im kabellosen Verkehr. Das Netz bietet hier zahlreiche Angriffspunkte. So kann man mit entsprechenden Kenntnissen in der HF-Technik den gesamten Funkbereich stören oder Lücken des Übertragungsprotokolls IEEE 802.11p ausnutzen, um die Kommunikation zu stören, abzuhören oder zu verfälschen.

Angriffe auf die Auto-Infrastruktur-Kommunikation sind problematischer als die Angriffe auf die Auto-Auto-Kommunikation. Dies liegt im Wesentlichen daran, dass die Einrichtungen einer Infrastruktur leichter demontierbar, zerstörbar und zugänglicher sind, als Autokomponenten. Ein Beispiel hierfür wäre ein Verkehrsschild an abgelegenen Straßen. Die möglichen Angriffstypen:

Störung des Systems: Der Angreifer wird hier das schwächste Glied, die Infrastrukturkomponente, attackieren. Bei Straßenschilden können diese komplett demontiert werden. Gegen den Vandalismus wird kein Kommunikationssystem helfen. Ein ähnlich einfacher Angriff wäre die Trennung von Infrastruktur und Energie. Ebenso können auch in diesem Beispiel Störangriffe getätigt werden.

Einspielen falscher Nachrichten: Das Einspielen falscher Nachrichten ist in diesem Fall wie bei der Auto-Auto-Kommunikation. Darüber hinaus wäre es einem Angreifer möglich Verkehrsschilder zu demontieren und an anderen Orten wieder aufzustellen. Sollte es hierzu keine Sicherheitsmechanismen geben, wie eine Bindung an eine GPS Position, so ist dieser Angriff eine Leichtigkeit. Dabei muss das Schild nicht einmal in optischer Reichweite sein. Würde ein solcher Angriff mit einem Tempo 30 Geschwindigkeitsgebotsschild auf der Autobahn passieren und die Technik bei einigen Autos die Geschwindigkeit automatisch regulieren, wäre ein Unfall fast vorprogrammiert. Bei der Manipulation bei einer Tankstelle könnte ein solcher Angriff zu falschen Benzinpreisen oder sogar zum Tanken des falschen Kraftstoffes führen.

Angriffe auf die Kommunikation des Fahrers beinhalten die Kommunikation zwischen dem Fahrer und seinem Fahrzeug. Hier geht man davon aus, dass die Angreifer das Automobil als System so manipulieren, dass es bei dem Fahrer falsch ankommt, da der Kommunikationsweg selber meistens schwer zu attackieren ist und der Fahrer keine reale Netzkomponente ist. Unter diese Angriffsarten fallen somit alle Angriffe, welche die internen Anzeigen beeinträchtigen, wie die Geschwindigkeits-, oder Tankanzeige. Zudem würde jeder Angriff dazuzählen, welcher auf die Netztechnik zielt, mit der der Fahrer kommuniziert, wie Bluetooth-Freisprecheinrichtung oder Mobilfunk. Da das Auto die einzige physikalische Schnittstelle bleibt, sind die meisten Angriffe wie bei der Auto-Auto- und Auto-Infrastruktur- Kommunikation einzuordnen.

4.5.2 Datenschutz

Bisher war der Autoaufenthalt nur dem Fahrer bekannt. Im Szenario der dezentralen Telematik ist dies anders. Hier kann die Position des Autos und somit auch des Fahrers

permanent ermittelt werden. Somit lassen sich die schon bekannten Bewegungsprofile erstellen. Dies wäre sogar noch strikter als beim aktuellen Mautsystem, da dies nur auf den Autobahnen aktiv ist. Zunächst kann man keine personenbezogenen Daten von der Position eines Autos generieren. Im Fall eines Privatwagens sind Fahrzeughalter und Fahrer meistens dieselben. Je nach Vernetzungsgrad könnten auch andere Daten erfasst werden, wie die Fahrleistungen, Überschreitung der Straßenverkehrsordnung oder die gehörten Radiosender. Sollte man über dieses System auch bei Einrichtungen, z.B. einer Tankstelle, gleich bezahlen, so können auch Einkaufsgewohnheiten verfolgt werden. Da eine Vernetzung auch nach innen gehen könnte, ist es auch möglich elektronische Geräte wie PDAs, Mobiltelefone etc. zu orten. Insgesamt bietet die dezentrale Telematik ein großes Problem für den Datenschutz.

4.5.3 Fazit der dezentralen Telematik

Das Szenario der dezentralen Telematiksysteme hat gezeigt, dass es viele Angriffsmöglichkeiten gibt und die Sicherheit eine große Rolle in dieser Technologie spielt. Gerade bei dieser Technik ist es wichtig, dass die Sicherheit gleich mit integriert wird, da sich hier viele Gefahren für Leib und Leben der Personen ergeben. Letztendlich soll die dezentrale Telematik auch Leben retten, indem der Fahrer eines Fahrzeuges frühzeitig gewarnt wird.

4.6 Fazit der IT Sicherheit im Pervasive Computing

Die Sicherheitsanforderungen und auch die Szenarien haben deutlich gemacht, wie wichtig die IT Sicherheit ist, insbesondere bei einer Komplexität, wie sie das Pervasive Computing bietet. Die meisten Angriffspunkte im Pervasive Computing lassen sich auf einzelne Teilobjekte oder Teilsysteme beschränken und sind nicht unbekannt. Daher gibt es auch schon unzählige Lösungsansätze, welche sich mit den Sicherheitsfragen beschäftigen und diese bewältigen. Vielmehr besteht ein Risiko in der Vernetzung, da auch die Sicherheitsfragen teilweise systemübergreifend geklärt werden müssen.

Abbildungen

Literaturverzeichnis

[1] Claudia Eckert. *IT Sicherheit*, Oldenbourg, Wien,2006.

[2] Bundesamt für Sicherheit in der Informationstechnik. *Pervasive Computing: Entwicklung und Auswirkung*, SecuMedia Verlags-GmbH, Bonn,2006.

[3] Harald Kelter. *Pervasive Computing: Entwicklung und Auswirkung*, Bonn, 2006.

[4] Ulrich Guddat. *Automatisierte Tests von Telematiksystemen im Automobil*, Sindelfingen, 2003.

[5] Wikipedia. *Pervasive Computing*, Wikipedia, 2007.

[6] Wikipedia. *Informationelle Selbstbestimmung*, Wikipedia, 2007.

[7] Wikipedia. *Telematik*, Wikipedia, 2007.

[8] Wikipedia. *Trusted Platform Module*, Wikipedia, 2007.

Abkürzungsverzeichnis

BAC	Basic Access Control
BSI	Bundesamtes für Sicherheit in der Informationstechnik
EAC	Extended Access Control
ICAO	International Civil Aviation Organization
MRZ	Machine Readable Zone
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification