Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Studienarbeit

Untersuchung der Einsatzmöglichkeiten von RFIDs als Authentifizierungssystem in einer Ferienclubanlage.

vorgelegt von
Helge Rickens
am 31.03.2005

Studiengang Technische Informatik
Betreuender Prüfer: Prof. Dr. Kai von Luck

Fachbereich Elektrotechnik und Informatik
Department of Electrical Engineering and Computer Science

Helge Rickens

Untersuchung der Einsatzmöglichkeiten von RFIDs als Authentifizierungssysteme in einer Ferienclubanlage.

Studienarbeit
im Studiengang Technische Informatik

am Fachbereich Elektrotechnik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Kai von Luck

Abgegeben am 31.03.2005
Helge Rickens

Thema der Diplomarbeit
Untersuchung der Einsatzmöglichkeiten von RFIDs als
Authentifizierungssysteme in einer Ferienclubanlage.

Stichworte
Authentifizierung, RFID, Radio Frequency Identification, Strichcode, Magnetkarte, Chipkarte, Smart Card, Biometrie.

Kurzzusammenfassung
In dieser Studienarbeit werden verschiedene Systeme zur Authentifikation betrachtet. Jedes dieser Systeme wird auf seine Einsatzmöglichkeiten in einem fiktiven Szenario hin untersucht und die Ergebnisse miteinander verglichen. Auf Grundlage des Vergleiches wird die RFID-Technik als besonders geeignetes System identifiziert. Abschließend wird das RFID-System anhand des Szenarios noch einmal mit seinen Möglichkeiten zur Realisierung im Detail vorgestellt. Darüber hinaus werden generelle Möglichkeiten von heute auf dem Markt verfügbaren RFIDs aufgezeigt

Helge Rickens

Title of the paper
Analysis of the potential uses of RFID as an authentication method in a holiday club

Keywords
Authentication, RFID, radio frequency identification, bar code, magnetic card, chip card, smart card, biometry.

Abstract

In this work we consider several systems which allow for authentication. Each of these systems is analyzed in a fictitious scenario and a comparison of the results is given. Based on this comparison we find that RFID technology is especially suitable for the given task. Concluding the RFID system is presented with its potential realizations in detail. Moreover, general options of currently available RFIDs are given.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Im Alltag muss man in vielen Situationen beweisen, dass man zu einer speziellen Handlung berechtigt ist, sei es der Zutritt zu bestimmten Gebäuden oder Bereichen die Freigabe einer bargeldlosen Zahlung oder eine von vielen weiteren Handlungen. Hierfür gibt es eine ganze Reihe von Möglichkeiten, wie z.B. Schlüssel, Ausweise und viele weitere. Häufig werden auch mehrere Systeme eingesetzt, so das man ein volles Schlüsselbund benötigt und/oder ein Portmonee mit viele ID-Karten. Im Rahmen dieser Arbeit soll zumindest für eine geschlossene Umgebung ein System gesucht werden, welches alle Anforderungen einheitlich löst.

1.1 Sichere Authentifizierung

Die Aufgabe der Authentifizierung ist sicherzustellen, dass wirklich eine Berechtigung vorliegt, wobei das Verfahren für den Anwender handhabbar bleiben muss. Daher muss eine Lösung gefunden werden die ein hohes Sicherheitsniveau bietet, aber für den Anwender bequem nutzbar bleibt. Als Beispiel soll hier die EC-Karte betrachtet werden. Es ist offensichtlich sicherer, eine 12-stellige statt einer 4-stelligen Geheimzahl zu verwenden, doch da die meisten Menschen Probleme haben sich eine solche Nummer zu merken, wird die Zahl dann oft notiert und in der Nähe der Karte aufbewahrt, womit das Sicherheitsniveau letztendlich niedriger ist, als mit einer kurzen Geheimzahl.

1.2 Aufbau der Arbeit

In Kapitel 2 wird anhand eines Szenarios, welches in einem fiktiven Ferienclub angesiedelt ist, ein Überblick über verschiedene Situationen gegeben bei denen eine Authentifizierung stattfindet.
Nachdem die Anforderungen aus dem Szenario ersichtlich geworden sind, werden in Kapitel 3 die Systeme vorgestellt, die zur Lösung des Problems in Frage kommen. Zu jedem System werden die Eigenheiten des Systems aufgezeigt. Vor- und Nachteile der Systeme werden erläutert. Anschließend werden die Systeme anhand ihrer zuvor erstellten Eigenschaften direkt miteinander verglichen und bewertet, wobei sich das System mit RFID als Favorit herausstellten wird.

Das RFID-System wird in Kapitel 4 noch einmal detailliert vorgestellt und technische Lösungsansätze anhand der verschiedenen Situationen aus dem Szenario aus Kapitel 2 aufgezeigt. Weiterhin werden weitere generelle technische Möglichkeiten von RFID aufgezeigt. Anschließend werden alle Ergebnisse in Kapitel 5 kurz zusammengefasst und in Kapitel 6 ein Ausblick auf zukünftige Möglichkeiten gegeben.

2 Analyse

Für geschlossene Umgebungen sollen typische Aufgaben untersucht werden, um deren technisch nötige Vorgänge zu analysieren. Danach werden die verschiedenen Systeme vorgestellt, die für die Realisierung möglich sind und miteinander verglichen. Um eine leicht verständliche Umgebung für den Leser zu schaffen wird die Analyse anhand des Szenarios einer fiktiven Ferienclubanlage durchgeführt. Die Aktivitäten werden aus Sicht von Herrn Meier und seiner Familie betrachtet, die ihren Urlaub in dem Ferienclub verbringt. Dieses Szenario orientiert sich an dem aus der Diplomarbeit [Luep-04] von Andre Lüpke. Dazu ist auch die Studienarbeit [Maeh-04] von Lars Mählmann zu erwähnen, in der es um die sichere Datenübertragung im WLan mit mobilen Endgeräten geht und die sich zum Teil auch mit ähnlichen Problemstellungen beschäftigt.

2.1 Einführung

„Bevor Herr Meier seinen Urlaub in dem oben genannten Club antreten kann, führt er eine Buchung bei einem Reisebüro durch. Das Reisebüro übermittelt daraufhin die Daten von Herrn Meier an den Ferienclub. Der Club ist fortan über den Ankunftstag und die Aufenthaltsdauer des Gastes informiert. Er kann sich daher bereits frühzeitig auf die Ankunft von Herrn Meier vorbereiten. [Luep-04]“

2.2 Check–In

Herr Meier meldet sich nach seiner Ankunft im Hotel bei der Rezeption. Hier weist er durch eine Buchungsbestätigung und seines Ausweises nach, dass er einen Bungalow gebucht hat. Daraufhin bekommt er den Schlüssel für den Bungalow und der Rezeptionist weist ihn in die Besonderheiten der Anlage ein. Das könnten die Zeiten der Mahlzeiten sein oder das Vorgehen zur Buchung von weiteren Angeboten wie Ausflügen, Shows oder der Nutzung des Wellnessbereiches.

2.3 Zutrittskontrolle

Herr Meier und seine Familie gehen nach dem Check–In als Erstes in ihren gebuchten Bungalow. Dieser ist selbstverständlich verschlossen um Unbefugte daran zu hindern den Bungalow zu betreten. Um die Tür zu ver- und entriegeln gibt es verschiedene Möglichkeiten, vom mechanischen Schloss mit Türzylinder [ABUS-1] über das mechatronische oder elektronische Schloss bis zum Zutrittskontrollsystem [STIE-1]. Aber auch an vielen anderen Stellen ist eine Zutrittskontrolle nötig. Familie Meier hat ein all-inclusive Angebot gebucht und geht, nachdem sie ihr Gepäck ausgepackt hat, zum Essen. Um den Einlass in das all–inclusive Restaurant zu überprüfen steht ein Mitarbeiter am Eingang. Dieser überprüft ob Herr Meier und seine Familienmitglieder einen Nachweis haben, welcher dazu berechtigt das Restaurant zu betreten. Dieser Nachweis wird auch zum Authentifizieren für alle Weiteren all–inclusive Bereiche genutzt, wie den Zutritt zum ganzen oder zu Teilen des Wellnessbereiches mit Sauna, Schwimmbad und Massage, sofern dies zum gebuchten Angebot gehört. Manche Angebote können zusätzlich durch eine Limitation im Gebrauch eingeschränkt sein. Zur Vorsicht wegen eventueller gesundheitlicher Gefahren darf jeder Gast z.B. nur zweimal am Tag in die Sauna. Am nächsten Tag bucht Herr Meier für sich und seine Frau zwei Plätze für die am Abend stattfindende Galashow und erhält darauf hin zwei Tickets. Abends werden die Tickets entwertet, um eine mehrmalige Nutzung auszuschließen.
Eine Zutrittskontrolle wird nicht nur für die Gäste, sondern auch für das Personal benötigt. Dabei braucht jede Personalfunktion nur die für ihre Aufgaben benötigten Zugangsberechtigungen. Ein Koch braucht nicht in den Serviceraum für den Pool oder in die Zimmer der Gäste. Das Zimmermädchen hingegen muss in die Zimmer, um aufzuräumen aber braucht nicht in die Küche. Ein Elektriker braucht eventuell sowohl den Zutritt in die Zimmer der Gäste, in die Küche und in den Serviceraum für den Pool, um anfallende Reparaturen vorzunehmen.
Dies sind nur einige Beispiele für Zutrittskontrollen, die in einer Ferienclubanlage möglich sind. Allen ist gemein, dass man sich authentifizieren muss, um den berechtigten Zugang zu erhalten.

2.4 Payment

In dem von Herrn Meier besuchten Ferienclub mit all–inclusive Angebot kommt man nicht ohne Geld aus. Sei es, dass eine Rundreise gebucht oder dass Wellness- und Sport-Angebot erweitert oder ein Eis am Strand für die Kinder gekauft werden soll. Es gibt genügend Gelegenheiten bei denen man bezahlen muss. Manches davon kann man am Ende des Urlaubes bequem an der Rezeption begleichen, andere Dinge sind

umständlicher z.B. Bargeld für das Eis mit an den Strand zu nehmen, da man hier ständig darauf auchten muss, dass es nicht abhanden kommt. Auch andere übliche Systeme wie Kredit-, EC- und Geldkarte können zum Einsatz kommen. Weiterhin verbreiten sich eigenständige Zahlungssysteme die mit Firmen-, Vereinskarten usw. arbeiten wie z.B. [PHF-1]. Diese bieten in der Regel weitere Funktionalitäten.

2.5 Ortung / Lokalisation

Herr Meier hat für die ganze Familie einen Ausflug gebucht. Sohn Klaus ist 15 Minuten vor Beginn immer noch nicht wieder aufgetaucht. Herr Meier wendet sich hilfesuchend an die Rezeption. Diese kann nur versuchen über die Sprechanlage des Ferienclubkomplexes Klaus Meier auszurufen. Um den Aufenthaltsort heraus zu bekommen, werden Lokalisationsmechanismen benötigt. Hierfür wird entweder ein Gegenstand benötigt, der die Lokalisation ermöglicht; bei einer Peilung [EKEV-1] ist dieser Gegenstand ein Sender. Des Weiteren könnte es z.B. über Schleusen realisiert werden: beim Passieren der Schleuse wird registriert in welcher Zone sich die entsprechende Person jetzt befindet.

2.6 Diebstahlsicherung

Herr Meier kommt nicht mehr ohne sein Notebook aus und selbst im Urlaub hat er es dabei. Doch so richtig wohl ist ihm bei der ganzen Sache nicht. Ständig befürchtet er dass sein Notebook gestohlen wird. Auch der Camcorder der Familie ist gefährdet, mehr noch als das Notebook, da der Camcorder überall mit hin genommen wird. Hier gibt es meist nur die Möglichkeit die Wertgegenstände in einen Tresor oder ein Schließfach einzuschließen. Sollen weitergehende Maßnahmen getroffen werden, wird eine Ortung mit angebundenen Warnsystem benötigt.

2.7 Zeiterfassung

Herr Meier geht mit seiner Tochter zum Squash. Die erste halbe Stunde wird pauschal, anschließend wird minutengenau abgerechnet. Hierfür wird von einem Mitarbeiter registriert, wann der Court über welchen Zeitraum genutzt wird. Hierbei sind verschiedene technische Hilfsmittel einsetzbar, von einfachen Stoppuhren bis hin zu vollautomatischen Systemen.

Dem Gast kann so eine zeitlich genaue Abrechnung für die Nutzung von Anlagen und Diensten geboten werden. Diese können dann natürlich wieder mit dem Payment- und Bonussystem gekoppelt werden. Es könnte die Nutzungsdauer bestimmter Dienste oder die Aufenthaltsdauer, in bestimmten festgelegten Bereichen, erfasst werden. Anhand dieser Daten können anschließend zeitabhängige Rechnungen erstellt werden. Weiterhin kann auch die Arbeitszeiterfassung des Personals erfolgen. Die personelle Arbeitszeiterfassung kann als elektronische Stempeluhr realisiert werden.

2.8 Kundenbindung

Der Ferienclub veranstaltet eine Aktion mit dem Motto „Nur ein gesunder Gast ist ein glücklicher Gast“. Jedem Gast werden Bonuspunkte gutgeschrieben, wenn er an sportlichen Aktivitäten teilnimmt. Diese Bonuspunkte können dann später gegen Prämien eingetauscht werden. Durch das Squashspielen von Herrn Meier mit seiner Tochter hat sich auf dem Bonuspunktkonto einiges angesammelt. Herr Meier überlässt seiner Tochter die Bonuspunkte, um sie in Prämien einzutauschen. Diese entscheidet sich für einige Kosmetikartikel.
Der Urlaub der Familie Meier nähert sich dem Ende. Herrn Meier hat es so gut gefallen, dass er an der Rezeption nachfragt, wie es aussieht, ob es Ermäßigungen gibt, wenn er nächstes Jahr wieder kommen würde. Der Clubangestellte teilt ihm mit, dass er automatisch registriert sei und das es ein Bonusprogramm gibt. Wenn er das nächste Mal kommt, hat er auf alle Angebote der Clubanlage automatisch 0,25% Rabatt. Dieser würde bei häufigeren Besuchen noch weiter steigen und wenn er jetzt sofort buchen würde, gibt es noch einmal 0,05% Rabatt zusätzlich. Hier lassen sich zahllose Variationen gestalten.

3 System-Analyse

Es gibt eine Vielzahl von technischen Systemen mit denen man sich Authentifizieren kann. Hier werden diese Systeme kurz vorgestellt und hinterher sollen Vor- und Nachteile aufgezeigt werden. Alle Systeme müssen leicht digital verarbeitet werden können.

3.1 Zu analysierende Systeme

Es soll kurz vorgestellt werden, welche Systeme es gibt und in welchen Umgebungen sie ereits eingesetzt werden. Dabei werden die Systeme in drei Kategorien eingeteilt. Authentifizierung durch etwas was man hat, weiß und ist oder tut. (auch oft mit den Englischen wörtern have, know, be bezeichnet).

3.1.1 Authentifizierung durch etwas was man hat (have).

Die Authentifizierung erfolgt durch ein Objektes. Dieses Objekt enthält Daten, anhand denen eine Überprüfung erfolgt ob eine Autorisation vorliegt. Viele diese Objekte haben das Format einer Karte. Das bevorzugte Format ist das ID-1 der [ISO-7816], stark Verbreitet durch die EC- und Telefonkarte. Im Folgenden wird es Scheckkartenformat genannt.

Strichcode

Der Strichcode wird auf ein Medium aufgetragen zumeist auf eine Karte, aus Plastik oder Papier, im Scheckkartenformat. Es entspricht im Wesentlichen dem Barcode im Supermarkt, wo der Strichcode jedoch direkt auf die Verpackung der Ware gedruckt ist. Eine Übersicht über verschiedene verwendete Strichcodes gibt es in [HERD-1].

Magnetstreifenkarte

Eine Karte im Scheckkartenformat ID-1 auf der ein Magnetstreifen aufgebracht wird oft kurz Magnetkarte genannt. Auf diesem Magnetstreifen können Daten gespeichert und davon gelesen werden. Der Magnetstreifen ist nach [ISO-7811-2] in drei

Datenspuren aufgeteilt, wobei nach [ISO-7811] nur die dritte Spur zum Schreiben spezifiziert ist. Die Karten werden anhand der Eigenschaften ihres magnetisierbaren Materials unterschieden in hochkoerzitiv (High Coercitivity, HiCo) und niederkoerzitiv (Low Coercitivity, LoCo) Karten. [RAEF 99]

Chipkarten

Chipkarten gibt es in einer sehr große Anzahl an Variationen. Hierbei unterscheidet man grundsätzlich Zunächst zwischen Speicherkarten und Mikroprozessorkarten auch Smartcards genannt. Auch hier werden die Karten hauptsächlich im Scheckkarteformat verwendet.

Speicherkarten

Bei den Speicherkarten handelt es sich um Chips mit zumeist EEPORM Speicher, die zusätzlich durch Sicherheitsbaugruppen geschützt sein können.

Smartcards oder Mikroprozessorkarten

Es gibt eine Vielzahl von Smartcards. Hauptaufgabe besteht, zumeist darin Kryptografieverfahren anzuwenden. Mikroprozessorkarten enthalten eine CPU mit flüchtigem und nicht flüchtigem Speicher. Die CPU kann noch durch einen Coprozessor unterstützt werden, um Kryptografiealgorithmen schnell ausführen zu können. Diese Chipkarten werden manchmal auch als Kryptokarten oder Kryptocontrollerkarten bezeichnet [RAEF 99].

USB-Token

Ein sogenannter USB-Token ist eine Smartcard mit USB Schnittstelle in einem Kunststoffgehäuse.

Radio Frequency Identification

RFID ist ein berührungsloses Verfahren zum Lesen und Schreiben von Daten, bestehend aus dem RFID-Lesegerät, auch Scanner genannt, und dem Transponder oder Tag. Dabei wird der Transponder durch die Funksignale des Lesegerätes mit Energie versorgt. Wird nur mit der Energie der Funksignale gearbeitet spricht man von passiven Transpondern gibt es hingegen eine Batterie, zur unterstützenden Energieversorgung, wird von aktiven Transpondern gesprochen. Die Transponder gibt es in nahezu jeder Bauform, z.B. als kleine Glaskörper zum Implantieren unter die Haut (z.B. für die eindeutige Zuordnung von Haustieren zum EU-

Heimtierausweis [ALFA-1]), als Schlüsselanhänger, im Schlüssel integriert (z.B. für die Wegfahrsperre im Auto), als Papier- oder Plastiklabel zum Aufkleben oder im Scheckkartenformat.

3.1.2 Authentifizierung durch etwas was man ist oder tut (Biometrie, be)

Das Bundesamt für Sicherheit in der Informationstechnik definiert Biometrie wie folgt:
„Elektronische Verfahren zur Identitätssicherung und -überprüfung – oder kurz biometrische Systeme – erfassen einzigartige Merkmale des Menschen. Sie machen diese für Maschinen erkenn- und unterscheidbar. [...]“[BSI-4]
Hierbei unterscheidet man noch zwischen Methoden die mit physischen oder verhaltensabhängigen Merkmale arbeiten. Zu den physischen Methoden gehören unter anderem die Fingerabdruckerkennung, die Iriserkennung und die Gesichtserkennung. Tastenanschlagverhaltenserkennung, Unterschriftserkennung, und Stimmenerkennung sind verhaltensabhängige Merthode.

3.1.3 Authentifizierung durch etwas was man weiß (know)

Die Authentifizierung erfolgt aufgrund der Abfrage einer Information, die nur dem zu Authentifizierenden bekannt ist.

Passwort

Die Authentifizierung erfolgt über die Eingabe eines vorher vereinbartes Passwortes, einer Kombination von Buchstaben, Zahlen und Sonderzeichen. Die Passwortfestlegung kann hierbei unter Regeln gestellt sein, muss z.B. eine Mindestanzahl von Zeichen aufweisen.

PIN/TAN-Verfahren

PIN steht für **P**ersonal **I**dentification **N**umber und TAN für **T**rans**a**ktions **N**ummer
Das wichtigste Beispiel hierfür ist wohl das Onlinebanking. Hier wird zur Identifikation die PIN erfragt mit der man eingeschränkten Zugriff auf das System erhält. Um sicherheitsrelevante Aktionen ausführen zu dürfen, wie z.B. eine Überweisung zu tätigen, muss jede Transaktion mit einer TAN bestätig werden. Jede TAN ist nur einmal gültig, wobei man eine beliebige TAN aus einer Liste mit gültigen TANs wählen kann.

3.2 Bewertung der einzelnen Systeme

Es werden die oben vorgestellten Systeme aufgrund ihrer Eignung für den geplanten Einsatz untersucht. Dabei werden auch die Kosten berücksichtig, da ein System auch immer wirtschaftlich sein muss.

3.2.1 Authentifizierung durch etwas was man hat (have)

Sich anhand eines Gegenstandes zu Authentifizieren hat generell den Nachteil das der Gegenstand vergessen, verloren oder gestohlen werden kann. Auch muss der Gestand gegen Nachahmung gesichert[1] werden.

Strichcode

Das Strichcodesystem ist ein erprobtes System, welches schon auf dem Markt ist, mit Sichtkontakt arbeitet und sehr günstig in der Herstellung ist. Die Kosten für einen Strichcode betragen, je nach Medium, pro Stück von 0,005 € bis 0,05 €. Hinzu kommen die Kosten für die Lesegeräte, die im Bereich von 100,00 € bis 1500,00 € liegen. Die Lebensdauer der Karte ist hierbei abhängig vom Trägermaterial und von der Widerstandsfähigkeit des Aufdruckes und kann sehr hoch sein. Das Benutzen der Karte ist einfach, Sie ist lediglich unter das Lesegerät zu halten. Allerdings ist das System fehleranfällig gegen Verschmutzung. Auch das Kopieren der Karte ist nicht schwierig, da hierfür eine einfache S/W-Fotokopie des Strichcodes genügt. Was weitere Sicherheitsmaßnahmen nötig machen kann. Weiterhin ist es ein reines Lesemedium. Die Anzahl der auf dem Strichcode enthaltenden Daten ist abhängig vom verwendeten Strichcode und kann bei 2-Dimensionalen Strichcodes, bis zu ca. 4000 alphanumerische Zeichen enthalten [BMVB-1].

Magnetstreifenkarte

Auch hier handelt es sich um ein erprobtes System, welches seit längerem auf dem Markt ist, das allerdings kontaktbehaftet arbeitet. Die Kosten für eine Karte betragen ca. 0,20 € und sind damit immer noch recht günstig. Auch hier kommen die Kosten für die Lesegeräte hinzu, die zwischen 30 € und 1000 € betragen. Die Lebensdauer

[1] Zum Thema Sicherheit liefert [RAEF 99, S.450ff] ausführliche Informationen, die sich zwar auf Chipkarten bezieht aber in vielen Punkten auch auf andere Systeme übertragen lassen.

kann, bei täglichen Gebrauch, mit ein bis zwei Jahren angenommen werden, wobei der Magnetstreifen anfällig für Magnetfelder ist, die zu Datenverlust führen können. Die Handhabbarkeit des Systems hängt stark vom Lesegerät ab. Unterscheidungskriterien bei den Lesegeräten wären, ob sie den Magnetstreifen in beide Durchzugsrichtungen lesen können oder die Karte automatisch, vom einem Motor, eingezogen wird. Beides reduziert die Fehlerrate beim Einlesen der Karte. Die Magnetstreifenkarte ist ähnlich leicht zu Kopieren wie der Strichcode, nur wird hierzu spezielle Hardware benötigt. Dieses könnte man durch weitere Sicherheitsmaßnahmen absichern.
Die Anzahl der zu speichernden Daten sind nach [ISO-7811] 79 alphanumerische Zeichen auf der ersten Spur (6-Bit, nur lesend), 40 Zeichen im 4-Bit-BCD-Code[2] auf der zweiten Spur und 107 Zeichen im 4-Bit-BCD-Code auf der dritten Spur.

Chipkarten

Mit einem Pilotprojekt für Telefonkarten in Frankreich ist die weite Verbreitung der Chipkarte 1984 gestartet. Es steht damit ein erprobtes System zur Verfügung, welches die Möglichkeiten des lesenden und schreibenden Zugriffs ermöglicht. Dabei kann es Bereiche geben, auf die ausschließlich lesend zugegriffen werden kann, um die entsprechenden Daten vor Manipulation zu schützen. Die Verbindung zwischen dem Chip und dem Lesegerät wird über sechs oder acht Kontakte hergestellt. Aufgrund der mechanischen Kontaktierung verschleissen die Kontakte und stellen hier die hauptsächliche Fehlerquelle dar, die eine realistische Einsatzdauer von drei bis fünf Jahren zulässt. Die Kosten für ein Lesegerät beginnen bei ca. 30,00 € und steigen je nach Ausstattung auf einige hundert Euro an. Die Handhabbarkeit ist etwas einfacher als bei den Magnetstreifenkarten da ein Vorbeiziehen am Lesekopf entfällt. Die Sicherheit bei Chipkarten ist deutlich höher als bei Strichcode und Magnetkarten [RAEF 99].

Speicherkarten

Die einfache Speicherkarte ist vom Aufwand her genauso zu kopieren wie der Magnetstreifen und es sind die gleichen Sicherheitsmaßnahmen möglich. Darüber hinaus gibt es Chipkarten die eine PIN-Abfrage auf dem Chip ermöglichen. Die Preise für reine Speicherkarten liegen je nach Art bei ca. 0,50 € - 4,00 € bei üblichen Speichergrößen von 1 kByte bis zu 32 kByte.

[2] von engl. Binary Coded Decimal = de. dualcodierte Dezimalziffer. Hierbei werden die Dezimalziffern 0-9 durch vier Bit lange Worte dargestellt. Zum Beispiel dezimal 159 => BCD-CODE 0001 0101 1001.

Smartcards oder Mikroprozessorkarten

Der Vorteile der Smartcard gegenüber den Speicherkarten ist, dass hier starke Kryptografie-Algorithmen, z.B. 3DES[3], zum Einsatz kommen können. Zudem können Zufallszahlen generiert werden, die für Challenge-Response Verfahren [SIKT-1] benötigt werden. Dafür sind die Preise für die Karten deutlich höher und betragen bis zu 30€ pro Stück. Die gängigen Speichergrößen gehen hier momentan bis zu 64 kByte [ETHZ-1].

USB-Token

Entspricht der Smartcard, nur das hier ein USB Interface angebunden ist. Daher benötigten USB-Tokens USB-Mastergeräte, welche meistens durch PCs dargestellt werden. Die Preise für das USB-Token fangen bei ca. 30 € an

RFID

RIFD ist ein recht junges System dessen Verbreitung sich grade durchzusetzten beginnt, z.B. bei der METRO Group [METR-1]. RFID ist ein kontaktloses Verfahren. Weiterhin können die Transponder in fast jeglicher Bauform hergestellt werden. Hier ist im Wesentlichen die Antenne das begrenzende Element, von dem auch stark die erzielbare Reichweite abhängt. Die flexiblen Bauformen ermöglichen eine gute Integration in die einzusetzenden Umgebungen. Die Reichweiten für passive Transponder liegen bei 1 cm bis ca. 10 m. Die Funkstrecke birgt zusätzliche Gefahren, da zur Kommunikation kein direkter Kontakt zu den Transpondern benötigt wird [FINK 02, RAEF 99]. Bei den Transpondern gibt es, wie bei den Chipkarten auch, reine Speichermedien und Transponder mit Mikroprozessor. Weit verbreitet sind Transponder mit Speichergrößen bis zu 16 kByte. Die Preise für passive Standard-Karten liegen im Bereich von 1,00 € bis 5,00 €. Die Reichweite bei aktiven Transpondern beträgt bis zu 300 m, sie sind im Allgemeinen aber größer Aufgrund der benötigten Batterie. Die Preise für aktive Transponder sind deutlich höher als die für passive Transponder.

[3] Von engl. Triple Data Encryption Standard. Eine Weiterentwicklung vom DES [SELK 00].

3.2.2 Authentifizierung durch etwas was man ist oder tut (Biometrie, be)

Die Biometrie ist das jüngste Verfahren zur Authentifizierung. Auch wenn der Fingerabdruck als solcher schon lange zur Identifikation genutzt wird, besonders in der Kriminalistik, ist der elektronische Einsatz noch nicht sehr verbreitet. Ein Grund hierfür kann die Akzeptanz der Öffentlichkeit sein, denn gerade durch die Nutzung des Fingerabdruckes in der Kriminalistik, wird dieser häufig mit der totalen Überwachung durch den Staat in Bezug gebracht. Der große Vorteil der Biometrie ist, dass die Person der Ausweis ist und ein Verlegen oder Vergessen damit ausgeschlossen ist. Ein weiteres Kriterium ist, dass eine Weitergabe prinzipbedingt unmöglich ist. Aus rein sicherheitstechnischen Gesichtspunkten ist das ein Vorteil, kann sich aber als zusätzliches Akzeptanzproblem herausstellen, wenn man berücksichtigt das viele ihre PIN der EC-Karte an andere Personen wie z.B. Lebenspartner, Familienmitglieder oder Freunde weiter geben, obwohl die Weitergabe der PIN ausdrücklich verboten ist. Alle biometrischen Verfahren arbeiten in bestimmten Toleranzbereichen um Unterschiede z.B. Mimik, Licht oder Verschmutzung tolerieren zu können. Hier liegt auch eine der Schwierigkeiten des Systems: ist die Toleranz zu hoch, werden auch unberechtigte Personen erkannt, ist die Toleranz zu niedrig, werden die berechtigten Personen fälschlicherweise abgewiesen. Die falsche Abweisung an sich ist nicht so schlimm, da ein nochmaliger Versuch gestartet werden kann. Sollte es aber zu häufig zu Abweisungen kommen, wird das System nicht akzeptiert werden. Die Kosten für die biometrischen Systemen umfassen eine sehr weite Preisspanne, je nach Güte des Systems und gewünschten biometrischen Verfahren. Es gibt einfache Fingerprintsensoren schon ab 50 € die aber einen PC benötigen, auf dem die Auswertung läuft. Weiterhin gibt es Zutrittskontrollsystem als Türschloss die sich im Bereich von 500 € bis 1000 € bewegen. Weitere Kosten können entstehen wenn die biometrischen Referenzdaten nicht zentral sondern z.B. auf einer Chipkarte gespeichert werden sollen. Damit ist eine anonyme Authentifizierung möglich.

3.2.3 Authentifizierung durch etwas was man weiß (know)

Bei den wissen basierten Systemen ist eine Generelle Aussage nur schwer zu treffen. Diese Systeme werden häufig in Verbindung mit anderen Systemen, als zusätzliche Schutzmaßnahme eingesetzt. Ansonsten wird ein Eingabegerät für das geheime Wissen benötigt. Das kann in jeder belibiger Form vorliegen (z.B Als Tastatur am PC oder als Ziffernblock).

3.2.4 Kombinationen

Die verschieden Systeme lassen sich alle miteinander kombinieren. Als Extrem-Beispiel könnte man eine Karte herstellen, die sowohl den Strichcode, den Magnetsteifen, als auch einen Prozessor enthält. Der Prozessor kann dann über ein Dualinterface sowohl per Chip als auch per RFID betrieben werden. Bei einer Transaktion werden dann alle Kartenmerkmale gegeneinander geprüft. Weiterhin werden biometrische Daten auf dem Chip mit mehreren biometrischen Systemen verglichen und die Transaktion schließlich mit einer PIN-TAN-Kombination bestätigt.

3.3 Bewertung und Auswahl der Systeme im Vergleich

Da des Systems, wie im Szenario beschrieben, von Urlaubern genutzt werden soll, muss das System so einfach wie möglich gehalten werden. Dabei muss jedoch ein gewisses Maß an Sicherheitskriterien eingehalten werden. Folgend werden anhand dieser Kriterien die Systeme verglichen und eine Auswahl getroffen.

3.3.1 Ausschusskriterien

Da es dem Urlauber so bequem wie möglich gemacht werden soll ist ein Umgang mit Passwörtern und oder PINs soweit möglich zu vermeiden. Ist der Einsatz von PINs unvermeidbar, sollten weitere Sicherheitsmaßnahmen die Anzahl auf ein Minimum reduzieren und eine möglichst einfache Gestaltung erlauben. Dies wird erfüllt durch Passwörter / PINs, die leicht zu merken sind z.B. dadurch, dass sie kurz und frei wählbar sind. Wenn man die vorgestellten Systeme unter diesem Aspekt untersucht, fallen hier zuerst einmal die Systeme raus, die alleine darauf aufbauen, dass man etwas weiß. Bei diesen Systemen ist es so, dass man entweder das zu Wissende vorgegeben bekommt oder, im günstigeren Fall für den Gast, sich selber etwas aussuchen darf, was dann aus Sicherheitsgründen wieder Beschränkungen unterliegt, wie einer Mindestlänge, was die Merkbarkeit erschwert. Indirekt kann auch der Strichcode davon betroffen sein, denn da er sehr leicht zu kopieren ist, muss er durch weitere Sicherheitsmaßnahmen geschützt werden. Der Schutz wird durch andere Systeme realisiert, zu denen dann auch wieder die wissensbasierten Systeme gehören könnten. Bei Systemen für die die Gäste einen Gegenstand bei sich tragen müssen sollte dieser möglichst handlich und wiederstandsfähig sein. Die Bedingungen denen das Medium ausgesetzt werden könnte sind z.B. der Sand am Strand, das Salzwasser im Meer oder starke Sonnenbestrahlung. Um den

mitzuführenden Gegenstand möglichst gut vor Verlust jeglicher Art zu schützen, sollte dieser auch in jeder Lage bei sich getragen werden können. Dazu würden sich besonders Armbänder eignen, da sie für keine Aktivität abgelegt werden müssen. Scheckkarten sind nur eingeschränkt zu empfehlen da sie nicht immer bei sich getragen werden können (z.B. beim Schwimmen) und somit das Problem des Deponierens und damit des Diebstahles besteht. Es bleiben die biometrischen Verfahren, die allerdings hohe Kosten verursachen wenn sie genügend Sicherheit bieten sollen. Weiterhin gibt es in der Öffentlichkeit Akzeptanzprobleme bei den biometrischen Systemen.

3.3.2 Schlussfolgerung

Unter Berücksichtigung der oben aufgeführten Kriterien bilden sowohl RFID als auch Biometrie eine sinnvolle Auswahl. Da die biometrischen Systeme recht teuer sind und bisher wenig akzeptiert sind, sollten sie nur unterstützend eingesetzt werden. Alternativ können auch wissenbasierte Systeme zur Unterstützung eingesetzt werden. Mit unterstützendem Einsatz ist hier gemeint, dass sie entweder die Sicherheitsmaßnahmen von RFID weiter erhöhen oder das sie dort eingesetzt werden, wo RFID nicht eingesetzt werden kann, weil es selbst gestört wird oder andere Geräte beeinträchtigt. RFID eignet sich vor allem, weil es ein robustest Medium bietet das leicht bei sich getragen werden kann. Weiterhin bietet es eine hohe Sicherheit bei großer Flexibilität und moderaten Kosten. Im Folgenden wird aufgezeigt, wie ein solches System aufgebaut sein kann.

4 Möglicher Aufbau eines Beispiel-Systems

Es soll gezeigt werden, wie man die im Szenario aufgeführten Punkte mit RFID realisieren kann.

4.1 Grundlagen RFID

4.1.1 Technische Grundlagen RFID

„RFID (**Radio** F**requency** Id**entification**) **[...]** ist eine Methode, um Daten berührungslos und ohne Sichtkontakt lesen und speichern zu können.[...]
Der Begriff RFID bezeichnet dabei die komplette Infrastruktur, die es möglich macht, Informationen drahtlos aus dem RFID-Tag (auch RFID Transponder genannt) auszulesen. Dies umfasst den RFID Tag, die Sende-/Empfangseinheit, mit welcher der RFID-Tag angesprochen wird, sowie die Integration mit Servern, Diensten und sonstigen Systemen wie z. B. Kassensystemen oder Warenwirtschaftsystemen.
Die Daten werden auf so genannten RFID-Tags (engl. für "Etiketten") - oft auch Transponder - gespeichert. Die gespeicherten Daten werden über elektromagnetische Wellen gelesen. Bei niedrigen Frequenzen geschieht dies induktiv (Nahfeld), bei höheren über Funk (Fernfeld). Die Entfernung, über die ein Tag ausgelesen werden kann, schwankt aufgrund der Ausführung (aktiv/passiv), benutztem Frequenzband, Sendestärke und Umwelteinflüssen zwischen wenigen Zentimetern und max. 30 Metern.
Es gibt daneben auch chiplose RFID-Tags, welche reflektiv arbeiten. In diesen gibt es keinen gespeicherten zeitauflösenden Code, sondern ein über die Fläche verteiltes Frequenz- und Phasenbild, welches ortsauflösend als Code interpretiert wird.“
[wipe-1]

4.1.2 RFID-Tags

Die Vielzahl der RFID-Tags lassen sich im Wesentlichen durch die Bauform, die Energieversorgung, die Datenübertragung und durch die Übertragungsfrequenz unterscheiden.
Hier soll noch eine mal kurz auf die Unterscheidungskriterien eingegangen werden.

Bauformen

Transponder gibt es in nahezu jeder Bauform, passend zum jeweiligen Einsatzgebiet. Von kleinen Glasröhrchen, zum injizieren in Tier oder Mensch, als Papier- oder Folien-Label zur Kennzeichnung von Waren über das Scheckkartenformat aus Papier oder Kunststoff z.B. zur Zutrittskontrolle bis hin zur Armbanduhr. Abbildung 4-1 zeigt beispielhaft einige ausgewählte Bauformen aus dem Sortiment der Firma EHAG Electronic Hardware und TAGnology RFID Limite. Die Vielfalt der Formen ermöglicht ein breites Spektrum der Einsatzbereiche, die Abbildungen sollen dies veranschaulichen.

Abbildung 4-1 Einige RFID Transpondern der Firmen

EHAG Electronic Hardware [EHAG-1] und TAGnology RFID Limited [TAGN-1]

Die Bauform hat keinen direkten Einfluss auf die Funktion. Zum Tragen kommt hier nur die Größe der Antenne welche die Reichweite bestimmt.

Datenübertragung

Die Übertragung findet entweder im Halbduplexverfahren, bestehend aus dem Ladeintervall und dem Sendeintervall oder im Vollduplexverfahren statt, wo die Energieversorgung zeitgleich mit der Datenübertragung stattfindet. Zusätzlich wird zwischen batteriegestützten Tags (Aktiven Tags), welche eine höhere Sendereichweite ermöglichen, und Tags ohne eigene Stromversorgung (Passiven Tags) unterschieden. Für weitergehende Informationen siehe [Fink-00] und [Feld-1].
Das wichtigste Merkmal ist die Arbeitsfrequenz. Es sind Theoretisch alle Frequenzen möglich die nur durch gesetzesvorgaben eingeschrenkt werden, nachfolgend werden gängige Frequenzen mit typischen Anwendungsbereichen aufgelistet.
Die Frequenzen mit denen Transponder Heute üblicherweise arbeiten, werden mit ihren typischen Einsatzgebieten in [Tabelle 4-1] aufgezählt. Die Frequenzen die Verwendet werden dürfen werden von den jeweiligen Ländern vorgegeben, in Deutschland ist das zum Beispiel durch die [RegTP-1] geregelt und in Amerika von der [FCC-1].

125	kHz	Nutzung im Nahbereich z.B. für Zutrittskontrollsysteme
134	kHz	Hauptsächlich genutzt bei der Tieridentifikation
13,56	MHz	Ticketsysteme, Zahlungssysteme, Smart Cards, EPC (Elektronischer Produktcode) [CCG-1], Bibliothekssysteme
433	MHz	Produktidentifizierung und allgemeine industrielle Anwendungen
868	MHz	Eingesetzt in Fertigungsstraßen zur Erkennung von Teilen und Werkzeugen in der EU, Produktidentifizierung, EPC.
917	MHz	Eingesetzt in Fertigungsstraßen zur Erkennung von Teilen und Werkzeugen in den USA
2,45	GHz	Objekterkennung auf größere Entfernung wie z.B. Lkw und Wagon-Fracht.
5,8	GHz	Objekterkennung auf größere Entfernung wie z.B. Lkw und Wagon-Fracht.

Tabelle 4-1: Aufzählung von gängigen Frequenzen beim Einsatz von RFID, mit Beispielen von Einsatzgebieten.

Neben Transpondern die nur mit einer Frequenz arbeiten gibt es auch so genannte Dual-Frequenz-Transponder die dann auf zwei verschieden Frequenzen arbeiten können. So ist es zum einen möglich vorhandene Infrastruktur zu nutzen, zum anderen können verschiedene Systeme für verschiedene Aufgaben benutzt werden. Es könnte z.B. für die Zahlungssysteme die 13,56 MHz Technologie verwendet werden, die nur eine sehr geringe Reichweite von einigen cm hat, und für die Überwachung eines großen Durchganges ein RFID–Lesegerät eingesetzt werden, dass eine deutlich größere Reichweite hat. Eine weitere Möglichkeit vorhandene Infrastruktur nutzen zu können bieten die Dual-Interface-Karten. Das sind Karten bei denen der Chip einmal über das kontaktlose RFID-Interface und zum anderen über das kontaktbehaftete Interface der Chipkarte angebunden ist. Allerdings schränkt das

die Bauform des Transponders ein. Hier ist dann nur noch der Einsatz des Scheckkartenformats möglich, um die Chipkontakte normal nutzten zu können.

4.1.3 RFID-Lesegeräte

Auch bei den RFID–Lesegerät, auch Scanner genannt, gibt es eine Vielzahl an unterschiedlichen Bauweisen angepasst an ihren jeweiligen Aufgabenbereich. Abbildung 4-2 zeigt eine kleine Auswahl um einen Überblick zu verschaffen.

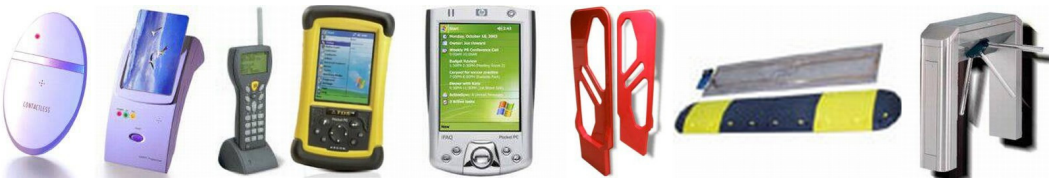

Abbildung 4-2: Verschiedene RFID-Lesegeräte der Firmen

EHAG Electronic Hardware [EHAG-1] und TAGnology RFID Limited [TAGN-1]

Allen RFID-Lesegeräten ist gemein, dass die Daten die sie erfassen, in ein weiterverarbeitenden System gegeben werden. Manche RFID-Lesegerät können zwar auch selber Daten verarbeiten, geben diese jedoch in der Regel standardmäßig ebenfalls weiter.

4.2 Einsatzbeispiele für RFID anhand des Szenarios

Um den Gästen einen schnellen Check–In zu ermöglichen, ist es von Vorteil wenn alle nötigen Vorgänge vorab erledigt werden können. Dazu ist es nötig, dass die benötigten Daten vorab an den Ferienclub gesendet werden. Dies kann auf vielerlei Wegen geschehen. Hier sind elektronische Wege vorzuziehen, da es anderenfalls durch die Portierung von einem Medium auf das andere zu Übertragungsfehlern kommen kann.

Check–In

Bei der Ankunft werden den Gästen nach einer Kontrolle der Personalien die RFID-Transponder übergeben. Diese können in der Form einer Armbanduhr (Abbildung 4-3 (links/mitte)) oder als Einweg-Armband (Abbildung 4-3 (rechts)) gestaltet sein. An der Rezeption werden die Standard-Autorisationen und die Zugangsberechtigung zum eigenen Bungalow vergeben. Es können aber auch noch weitere Autorisationen vergeben werden, sollten diese gewünscht und gegebenenfalls bezahlt werden.

Abbildung 4-3: Bsp.
Armbanduhren mit RFID-Transponder der Firma EHAG Electronic Hardware [EHAG-1] (links/mitte)
und Einweg-Armbänder mit RFID Transponder der Firma TAGnology RFID Limited [TAGN-1] (rechts)

Zutrittskontrolle

Der Bereich der Zutrittskontrolle ist vielseitig, daher werden hier ein paar typische Beispiele aufgezeigt, die in der Praxis Anwendung finden. Um die Eingangstür zum Bungalow zu öffnen, könnten RFID – Lesegeräte entweder im Türschloss (Schließzylinder) untergebracht (Abbildung 4-4 (links)) oder als externes RFID–Lesegerät in der Nähe der Tür angebracht werden (Abbildung 4-4 (rechts)). In beiden Fällen muss jetzt nur noch der Transponder in die Nähe[1] des RFID – Lesegerätes gehalten werden, um bei erfolgreicher Authentifizierung die Tür zu entriegeln.

Abbildung 4-4: Zylinderschloss-RFID–Lesegerät der Firma TAGnology RFID Limited [TAGN-1] (links)
und Unterputz-RFID-Lesegerät der Firma [VSS-1] (rechts)

Bei Anwendungen mit Einlasskontrollen, wie im Schwimmbad oder in der Sauna, kann der Zugang mittels Drehkreuz mit RFID – Lesegerät (Abbildung 4-5 (links)) geregelt werden. Auch hier wird der Transponder wieder in die Nähe des RFID – Lesegerätes gehalten und bei erfolgreicher Authentifikation, schaltet das Drehkreuz den Durchgang frei. Wenn es ausschließlich um die Erfassung geht (z.B. Zeiterfassung) können sogenannte Gate-Antennen (Abbildung 4-5 (mitte/rechts)) eingesetzt werden. Die Reichweite liegt bei einer einzelnen Antenne bei 50 cm bis 150 cm, so dass sich bei einer Nutzung von zwei Antennen eine Durchgangsbreite von bis zu ca. 250 cm realisieren lässt. Beim Durchqueren des Gates werden die

[1] Hier sind, bei 13.56 MHz Transpondern, Lesereichweiten von drei cm bis zehn cm üblich.

Transponder, auch mehrere quasi gleichzeitig[2], gelesen. Daraufhin könnte sich eine Schiebetür öffnen um den Zugang zum Casino freizugeben, der einer Altersfreigabe unterliegt.

Abbildung 4-5 Beispiel für RFID – Lesegerät von link nach rechts

Drehkreuz, Gate in zwei Varianten

Payment

Bei Bezahlvorgängen ist, wie bei allen Vorgängen bei denen Kosten entstehen, wichtig, dass der Kunde eine deutliche Willenserklärung abgibt. Einen Transponder in den Lesebereich des RFID–Lesegerätes zu halten reicht als Willenserklärung nicht aus, sodass ein weiterer Vorgang notwendig wird. Um dabei gleich auch noch eine Auslösung durch Dritte auszuschließen, könnte man hier auf das PIN-Verfahren oder ein biometrisches Verfahren wie den Fingerprint zur Willenserklärung setzen.

Abbildung 4-6: RFID–Lesegeräte mit Ziffernblock
der Firma cavitec [CAVI-1] (links) und der Firma TimeLink International [TIME-1] (rechts)

[2] Es gibt Transponder die Antikollisionsverfahren beherrschen um es zu ermöglichen mehrer Transponder im Lesebereich zu verwalten [Fink-02].

Ortung / Lokalisation

Eine Ortung anhand eines Senders vorzunehmen ist mit passiven Transpondern aufgrund der geringen Reichweite praktisch nicht möglich. Es können jedoch vorhandene Lesegeräte deren Standort bekannt ist dazu benutzt werden, Aussagen darüber zu treffen, ab sich Personen mit einer gewissen Wahrscheinlichkeit an einem bestimmten Ort aufhalten. Als Beispiel soll hier das Drehkreuz von Schwimmbad und Sauna aus dem obrigen Beispiel dienen. Zur Veranschaulichung dient Abbildung 4-7. Da jeder Gast der in die Sauna oder in das Schwimmbad möchte das Drehkreuz passieren muss kann man sagen, ob sich die gesuchte Person dort aufhält. Gibt es auch noch eine Ausgangskontrolle ist dies Aussage sicher, gibt es keine, gilt die Aussage nur mit einer gewissen Wahrscheinlichkeit. Nimmt man Abbildung 4-7 als Vorlage so können Aussagen über den Aufenthalt getroffen werden, wenn sich die Personen im Casino, Restaurant, Schwimmbad, in der Sauna oder den Bungalows aufhalten.

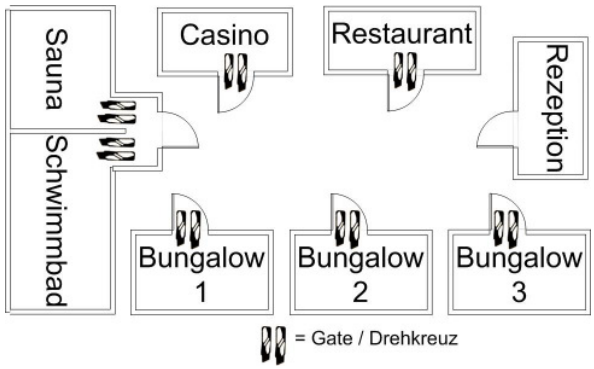

Abbildung 4-7: Beispiel des Grundrisses einer Ferienclubanlage mit Standorten der RFID-Zutrittskontrollen.

Diebstahlsicherung

Eine Diebstahlsicherung ist im gleichen Rahmen möglich, wie man sie aus Kaufhäusern kennt, in denen an den Ausgängen oder den Rolltreppen Gates stehen. In Kaufhäusern kommen 1-Bit Transponder zum Einsatz. In der Ferienclubanlage können aufgrund der komplexeren Transponder, die eine eindeutige Zuweisung ermöglichen, auch personenabhängige Transfers durch die Schleusen ermöglicht werden. Herr Meier hat seinen privaten Camcorder mit einem Transponder, den er an der Rezeption erhalten hat, markiert. Passiert der Camcorder nun ein Gate, erkennt das System den Camcorder anhand des Transponders und überprüft, ob eine autorisierte Person, in diesem Fall Herr Meier, ebenfalls das Gate passiert. Sollte dies nicht der Fall sein, wird ein Alarm ausgelöst.

Zeiterfassung

Bei der Zeiterfassung geht es in der Regel darum, dass eine zeitabhängige Kostenabrechnung erfolgen soll. Daher sollte auch hier auf eine deutliche Willenserklärung geachtet werden. Weiterhin muss bei vollautomatischen Systemen die Preisgestaltung deutlich erkennbar sein. Wenn man als Beispiel einen Squashcourt betrachtet, muss deutlich sein, ab wann Kosten entstehen und in welcher Höhe und Staffelung. Dies könnte dadurch erfolgen, dass auf einem Bildschirm an der Tür eine Miteilung steht. „Guten Tag Herr Meier sie betreten einen kostenpflichtigen Bereich. Die Kosten für die erste halbe Stunde betragen 6€, jede weiteren angefangenen 10min kosten 1,50 €. Möchten sie den Court betreten, drücken sie auf die OK Taste.“ Im Court könnte sich ein Kostenzähler befinden, an dem man die aktuellen Kosten und die gesamte Spielzeit ablesen kann. Ähnliche verfahren lassen sich für alle Anwendungsfälle finden. Wo es nicht um eine Kostenabrechnung geht, reicht eventuell ein Gate das durchschritten wird um den Timer zu starten. Ist diese Art der Erfassung nicht genau genug, wird ein zusätzlicher Mechanismus benötigt der den Timer startet, zum Beispiel eine Lichtschranke.

Kundenbindung

Bei den Kundenbindungssystemen hängt der Aufbau stark davon ab, wie die Kundenbindung aufgebaut ist. Das kann soweit gehen, dass es einem Paymentsystem (s.o.) entspricht und somit genau die gleichen Anforderungen erfüllen muss und somit denselben Aufbau hat. Bonuspunkte können für diverse Ereignisse vergeben werden. Das kann abhängig von Zahlungen sein oder von der Nutzung bestimmter Bereiche. Daher wird das System für das hier besprochene Szenario immer in die vorhandenen Systeme integriert. Es geht hier im Wesentlichen um die Erfassung der Daten, die eigentliche Auswertung erfolgt im Backendsystem.
Das Einlösen der Bonuspunkte ist abhängig davon, wie das Bonussystem gestaltet sein soll, wird wohl aber am ehesten einem Bezahlvorgang gleichen und somit auch ähnlich aufgebaut sein.

4.3 Weitere Aspekte zum Systemaufbau

Neben den RFID-Transpondern und den RFID-Lesegeräten werden für ein vollständiges System noch weitere Komponenten benötigt, auf die hier noch einmal kurz eingegangen werden soll.

4.3.1 Netzwerk

Es kommen eine ganze Reihe von Geräten zum Einsatz, die alle einen gemeinsamen Datenstamm nutzen sollen und somit miteinander verbunden sein müssen. Abbildung 4-8 stellt beispielhaft ein solches Netzwerk dar. Da eine Vielzahl von unterschiedlichen Geräten zum Einsatz kommt, kann der Aufbau sehr unterschiedlich sein. Unabhängig davon, wie das Netzwerk physikalisch aufgebaut wird, sollten folgenden Punkte beachtet werden. Die Performanz des Netzt sollte in Antwortzeit und Transferraten genügend Reserven haben, dass ein komfortables Arbeiten jederzeit möglich ist. Der Kunde wird das System nicht annehmen, wenn es ihm träge vorkommt oder ihm die Vorgänge zu lange dauern. Auch sollte drauf geachtet werden, dass Wichtige Abschnitte redundant ausgelegt werden, um größere Ausfälle zu vermeiden.

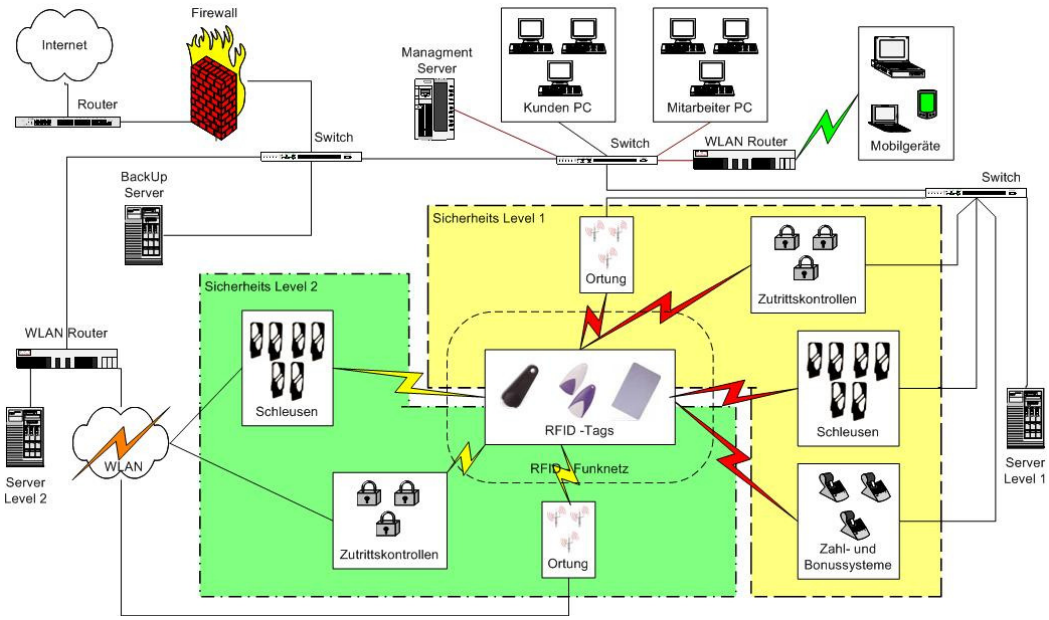

Abbildung 4-8: Schematischer Netzwerkplan

4.3.2 Backendsystem

Der Einsatz von RFID wird erst dadurch ermöglicht, dass die erfassten Daten der Transponder weiterverarbeitet werden. Hierfür werden Server benötigt, die entsprechende Dienste anbieten. Das können z.B. Datenbank-, Web-, Print-, Terminal- oder Passwort-Server sein.
Eine schnelle Bearbeitung der angeforderten Dienste ist wichtig um beim Kunden eine hohe Akzeptanz zu erreichen. Hierfür sind eine gute Architektur, zu der auch das Netzwerk gehört, und performante Hostsysteme nötig. Auch sollten hier nach Möglichkeit elementar wichtige Systeme redundant ausgelegt werden, um die Risiken eines Ausfalles zu minimieren. Um die Kosten des Systems gering zu halten sollte auch auf die Wartbarkeit des Systemes geachtet werden.

5 Resumé

Hier soll noch einmal zusammengefasst werden, was erarbeitet wurde, ein Fazit gezogen und anschließend eine Zukunftsaussicht gegeben werden.

5.1 Zusammenfassung

In dieser Studienarbeit wurden verschiedene Systeme zur Authentifikation dargestellt und untersucht. Um die Anforderungen an die Systeme anschaulich darzustellen wurden sie anhand eines Szenarios präsentiert. Jedes dieser Systeme wurde auf seine Einsatzmöglichkeiten in diesem Szenario hin untersucht und anschließend wurden die Ergebnisse der einzelnen Systeme miteinander verglichen. Auf Grundlage des Vergleiches wurde ein besonders geeignetes System ausgewählt. Die Wahl fiel auf die RFID-Technik, da sie eine vielseitige und robuste Umgebung zur Verfügung stellt, bei Kosten die eine Umsetzung auch wirtschaftlich sinnvoll machen. Abschließend wurde das RFID-System anhand des Szenarios noch einmal mit seinen Möglichkeiten zur Realisierung im Detail vorgestellt. Dafür wurden zu den einzelnen Punkten des Szenarios beispielhafte Lösungen vorgestellt. Darüber hinaus wurden generelle Möglichkeiten von heute auf dem Markt verfügbaren RFIDs aufgezeigt.

5.2 Fazit

Die Untersuchung hat gezeigt, dass mit den heute erhältlichen Mitteln eine einheitliche Authentifizierung in geschlossen Bereichen möglich ist. Die dazu verwendete Technologie der RFIDs kann drüber hinaus auch noch vielseitig für weitere Zwecke genutzt werden. Hierbei zeigen sich allerdings Bereiche in denen das System Schwächen aufweist. Dazu gehören die Ortung und Lokalisation sowie die Datensicherheit, wobei hier in erster Linie ein Akzeptanzproblem bei der Bevölkerung vorliegt. Diese Schwächen lassen sich teilweise durch den Einsatz anderer Technologien umgehen, doch die RFID-Technologie stellt aus Wirtschaftlichkeitsgründen derzeit die beste Wahl dar.

5.3 Ausblicke

Mit der Verbesserung der RFID-Technologie werden immer leistungsfähigere Transponder mit immer größeren Reichweiten möglich. Die größere Leistungsfähigkeit der Transponder ermöglicht einen besseren Schutz der Daten oder neue Anwendungsmöglichkeiten. Wenn die Reichweite ausreichend groß wird, kann auch bei passiven Transponder über Ortung über Peilung nachgedacht werden, für aktive Transpondern gibt es dafür bereits erste Ansätze. Durch die immer größer werdende Verbreitung von RFID werden die Kosten vor allem für die Transponder immer geringer, so dass die Wirtschaftlichkeit von RFID-Systemen weiter erhöht wird.

Literaturverzeichnis

[ABUS-1]	ABUS August Bremicker Söhne KG <http://www.abus.de/de/main.asp?ScreenLang=de&sid=943111598103046120120056296223101&select=0101b06&ArtikelGrID=253> (12.01.2005)
[ALFA-1]	alfavet Tierarzneimittel GmbH <http://www.alfavet.de/index.php?site=produktseite.php&tier=kennzeichnung&prod=ID-fix%B0%20Transponder&ban=ban1#sicht> (24.01.2005)
[BMVB-1]	Bundesministeriums für Verkehr, Bau- und Wohnungswesen (BMVBW) "Kleine und mittlere Speditions- und Transportunternehmen und die Nutzung neuer Kommunikationsmedien" <http://www01.iml.fhg.de/~praxishb/phb_offiziell.pdf > (19.01.2005)
[BSI-4]	Bundesamt für Sicherheit in der Informationstechnik <http://www.bsi.bund.de/literat/jahresbericht/jahresbericht_2003/44_Biometrie.htm> (18.01.2005)
[CAVI-1]	cavitec GmbH <http://www.cavitec.de/> (10.02.2005)
[CCG-1]	Centrale für Coorganisation GmbH (CCG) <http://www.epcglobal.de/> (15.02.2005)
[EHAG-1]:	EHAG Electronic Hardware AG <http://www.ehag.ch> (23.11.2004)
[EKEV-1]	Europäische Kommission, Generaldirektionen, Energie und Verkehr <http://europa.eu.int/comm/dgs/energy_transport/galileo/index_de.htm> (12.01.2005)
[ETHZ-1]	Eidgenössische Technische Hochschule Zürich <http://www.inf.ethz.ch/personal/rohs/SmartcardsUndJavacards/> (20.01.2005)
[FCC-1]	Federal Communications Commission <http://www.fcc.gov/> (15.02.2005)
[Fink-02]:	Finkzeller, K.; *rfid-Handbuch* ; 3. Aufl.Carl Hanser Verlag München Wien, 2002.
[HERD-1]	Herd Software Entwicklung – Software <http://www.herdsoft.com/ti/barvis/Strichcode_Arten.html> (21.01.2005)
[ISO-7811]	ISO 7811, Identification cards, 2001
[ISO-7816]	ISO 7816, Identification cards, 1998
[Luep-04]	Andre Lüpke; Entwurf einer Sicherheitsarchitektur für den Einsatz mobiler Endgeräte, Hochschule für Angewandte Wissenschaften Hamburg, Diplomarbeit, April 2004. <http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/diplom/luepke.pdf> (01.12.2004)
[Maeh-04]	Lars Mählmann; Sichere Übertragung im WLan mit mobilen Endgeräten (speziell unter Linux) Hochschule für Angewandte Wissenschaften Hamburg, Studienarbeit, August 2004. <http://users.informatik.haw-hamburg.de/~ubicomp/arbeiten/studien/maehlmann.pdf> (01.12.2004)

[METR-1]	METRO Group <http://www.metrogroup.de/servlet/PB/menu/1012074_l1/index.html> (27.07.2005)
[PHF-1]	Pädagogische Hochschule Freiburg PH Card <http://www.ph-freiburg.de/zentral/hochschule/phcard/index.htm> (12.01.2005)
[RAEF 99]	Rankl, W.; Effing, W.; *Handbuch der Chipkarten.;* 3. Aufl. München; Wien; Hanser, 1999
[RegTP-1]	Die Regulierungsbehörde für Telekommunikation und Post <http://www.regtp.de/reg_tele/start/in_05-05-00-00-00_m/fs.html> (15.02.2005)
[SIKT-1]	Stabsstelle IKT-Strategie des Bundes <http://www.cio.gv.at/securenetworks/vpn/Kryptologie/Kryptologie.html> (26.01.2005)
[STIE-1]	Stierlin AG Bau, Industrie, Handwerk <http://www.stierlin.ch/web/schliesssysteme/schliessanlagen.php> (12.01.2005)
[TIME-1]	TimeLink International GmbH <http://timelink.titze.de/html/de/d_products.html> (10.02.2005)
[TAGN-1]	TAGnology RFID Limited <http://www.tagnology.com/> (10.02.2005)
[VSS-1]	VSS GmbH <http://www.vesisy.de/hpvesisy.nsf/?Open> (08.02.2005)