Studienarbeit

# Vergleich von Zugangssystemen für sicherheitsrelevante Bereiche

ausgeführt am Institut für Nachrichtentechnik und Informationselektronik
der Fakultät für Informatik und Elektrotechnik

der Universität Rostock

unter Anleitung von

Dr.-Ing. H.-D. Melzer

und

Dipl.-Ing. Th. Kessler

durch

cand. ing. Udo Brunswig

Matr.Nr. 098201500

Budapester Straße 32
18057 Rostock

15. April 2004

# Inhaltsverzeichnis

# Tabellenverzeichnis

# Abbildungsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| **3**DES | Triple Data Encryption Standard |
| **A**CK | Acknowledge |
| AN | Access Network |
| API | Application Interface |
| ARQ | Automatic Repeat Request |
| ATM | Asynchronous Transfer Mode |
| AuC | Authentification Center |
| AUTN | Authentication Number |
| **B**API | Biometric API |
| BC | Broadcast |
| BioAPI | Biometric API |
| BSS | Base Station Subsystem |
| BSC | Base Station Controller |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSMB | Biometric Specific Memory Block |
| BTS | Base Transceiver Station |
| **C**BEFF | Common Biometic Exchange File Format |
| CCD | Charged Coupled Device |
| CFP | Contention Free Period |
| CK | Cipher Key |
| CL | Convergence Layer |
| CLS | Clear to Send |
| CN | Core Network |
| CP | Contention Period |
| CRC | Cyclic Redundance Check |
| CSMA | Carrier Sense Multiple Access |
| CSMA/CA | CSMA mit Collision Avoidance |
| CSMA/CD | CSMA mit Collision Detection |
| **D**CS | Digital Cellular System |
| DECT | Digital Enhanced Cordless Telecommunications |
| DES | Data Encryption Standard |
| DH | Diffie-Hellman |
| DiL | Direct Link |

| | |
|---|---|
| DL | Downlink |
| DLC | Data Link Control |
| DoS | Denial of Service |
| DSSS | Direct Spread Spread Spectrum |
| **E**C | Error Control |
| EIRP | Equivalent Isotropically Radiated Power |
| ERR | Equal Error Rate |
| ESSID | Extended Service Set Identity |
| **F**AR | False Acceptance Rate |
| FHSS | Frequency Hopping Spread Spectrum |
| FRR | False Rejection Rate |
| **G**PRS | General Packet Radio Standard |
| GSM | Global System for Mobile Communications |
| **H**A-API | Human Interface API |
| HCI | Host Controller Interface |
| HE | Home Environment |
| HiperLAN | High Performance Radio Local Area Network Type 2 |
| HLR | Home Location Register |
| HMM | Hidden-Markov-Modell |
| **I**AS | Information Access Service |
| IEEE | Institute of Electric and Electronic Engineers |
| IK | Integrity Key |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protokoll |
| IrCOMM | Infrared Communication Module |
| IrDA | Infrared Data Assoziation |
| IrLAN | Infrared Local Area Network |
| IrLAP | Infrared Link Access Protokoll |
| IrLMP | Infrared Link Management Protokoll |
| IrOBEX | Infrared Object Exchange Protocol |
| ISDN | Integrated Service Digital Network |
| ISM | Industrial Scientific and Medical |
| IV | Initialisierungsvektor |
| **L**2CAP | Logical Link Control an Adaptation Protocol |

| | |
|---|---|
| LA | Location Area |
| LAI | Location Area Identifier |
| LAN | Local Area Network |
| LFSR | Linear Feedback Shift Register |
| LLC | Logical Link Control |
| LMP | Link Management Protocol |
| **M**AC | Medium Access Control |
| MAC | Message Authentication Code |
| ME | mobiles Endgerät |
| MIT | Massachusetts Institute of Technology |
| MS | Mobile Station |
| MSC | Mobile Switching Center |
| **N**FA | Number of False Acceptances |
| NFR | Number of False Rejection |
| NSS | Network and Switching Subsystem |
| OFDM | Orthogonal Frequency Division Multiplex |
| **O**FB | Output Feedback |
| OSI | Open System Interconnection |
| **P**AN | Personal Area Network |
| PC | Personal Computer |
| PCF | Point Coordination Function |
| PDA | Personal Digital Assistant |
| PFS | Perfect Forward Secrecy |
| PHY | Physical Layer |
| PIN | Personal Identify Number |
| PKI | Public Key Infrastructure |
| PLCP | Physical Layer Convergence Protokoll |
| PMD | Physical Medium Dependent |
| PUK | Pin Unlocking Key |
| **Q**oS | Quality of Service |
| **R**ADIUS | Remote Authentification Dial-In User Service |
| RAND | Zufallszahl |
| RC4 | Rivest Cipher Nr.4 |
| RegTP | Regulierungsbehörde für Telekommunikation und Post |
| RFCOMM | Radio Frequency Communication Module |

| | |
|---|---|
| RLC | Radio Link Control |
| RNC | Radio Network Controller |
| RNS | Radio Network Subsystems |
| RSA | Rivest, Shamir und Adleman Verschlüsselung |
| RTS | Ready to Send |
| **S**B | Signature Block |
| SBH | Standard Biometic Header |
| SDP | Service Discovery Protocol |
| SIM | Subscriber Identity Module |
| SIR | Serial Infrared |
| SN | Serving Network |
| SOHO | Small Office Home Office |
| SRES | Session Result |
| SSID | Service Set Identity |
| **T**CS BIN | Telephony Control Protocol Binary |
| TinyTP | Tiny Transport Protokoll |
| TMSI | Temporary Mobile Subscriber Identity |
| **U**ED | User Equipment Domain |
| UL | Uplink |
| UMTS | Universal Mobile Telecommunications System |
| USIM | User Subscriber Identity Module |
| UTRAN | Universal Terristical Radio Access Network |
| **V**FIR | Very Fast Infrared |
| VLR | Visitor Location Register |
| **X**OR | exklusiv oder |
| **W**-CDMA | Wideband Code Division Multiple Access |
| WECA | Wireless Ethernet Compatibility Alliance |
| WEP | Wired Equivalent Privacy |
| WiFi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |

# Kapitel 1

# EINLEITUNG

Der Zugang zu sicherheitsrelevanten Bereichen wie Fährhäfen, Flughäfen oder Firmengeländen wird in Bezug auf die physische Zugangskontrolle und die Zugangskontrolle in das jeweilige Datennetz heutzutage noch getrennt betrachtet.

So erhalten beispielsweise alle Mitarbeiter einer Firma einen Firmensausweis. Dieser muß am Werkstor dem Pförtner vorgelegt werden, der nach Prüfung der Echtheit des Ausweises Einlass gewährt. Für den Zugang in das Datennetz der Firma wird ein ähnlicher Ablauf vollzogen. Dem Nutzer wurde vom Administrator des Datennetzes ein Nutzerprofil mit dazugehörigem Passwort erstellt. Möchte der Nutzer Zugriff in das Datennetz haben, wählt es sich unter Eingabe des Nutzernamens und des Passwortes in das Datennetz ein. Die Verifizierung des Passwortes und damit der Nutzungsberechtigung findet durch einen Server im Netzwerk statt.

Die Verfahren zur Erlangung des Zugangs in jedes der Systeme findet nach einer sehr ähnlichen Prozedur statt. Der Einsatz von Credentials für die Authentisierung, Autorisierung und die Abrechnung ermöglicht die beiden Zugangskontrollsysteme zu einem System zusammenzufassen.

Eine Grundlage für diese Integration sind aber die vorhandenen Sicherheitsmechanismen der Kommunikationsnetze. Denn nur mit sicheren Kommunikationsnetzen kann ein Verlust der Zugangssicherheit, durch Einschleusen oder Verändern der ausgetauschten Nachrichten im Kommunikationsnetz, vermieden werden.

Die immer größer werdende Forderung nach Mobilität zieht nach sich, dass auch drahtlose Zugangssysteme, wie WLAN, GSM und UMTS in dieses Gesamtkonzept einbezogen werden. Aber grade die drahtlosen Technologien der Kommunikationsnetze stellen besonders sicherheitskritische Schwachstellen dar. Die implementierten Sicherheitsmechanismen der drahtlosen Technologien sollten mit Hilfe der geforderten Sicherheitskriterien, die zum Einsatz von Credentials nötig sind, untersucht werden.

Eine Authentisierung mit Hilfe von Credentials kann nur für die Authentisierung des genutzten Endgerätes und nicht für die Autorisierung des Nutzers erfolgen. Um die Konvergenz der Zugangskontrollsysteme zu vollziehen muss aber

eine eindeutige Nutzerauthentisierung geschehen.

Eine Möglichkeit die Authentisierung der Nutzer zu erreichen, ist die Feststellung und Speicherung (zum Vergleich mit späteren Authentisierungen) von einem oder mehreren eindeutigen nicht veränderlichen Merkmalen des Nutzers, wie zum Beispiel biometrischen Merkmalen. Die dazu nötigen Verfahren und Technologien werden in Kapitel 3 vorgestellt.

Das zweite Kapitel dieser Arbeit umfasst die Beschreibung der Identität und eine Entwicklung dieser zu einer credentialbasierten Identität. Im vierten Kapitel werden die am häufigsten genutzten drahtlosen Zugangstechnologien vorgestellt und ihre Sicherheitsmerkmale genauer erläutert und untersucht. Im fünften Kapitel findet ein Vergleich und die Bewertung der vorgestellten drahtlosen Zugangstechnologien und der biometrischen Verfahren statt.

# Kapitel 2

# CREDENTIALS

Um sich näher mit Credentials beschäftigen zu können muss im Vorfeld eine Begriffsdefinition gegeben werden.:

DEFINITION 1 (Kryptografie) Beglaubigte Teilmenge von Zugangsberechtigungen (entwickelt durch Nutzung trägerunabhängiger Daten) um die Identität einer Person oder Sache zu beglaubigen, z.B. Geburtsurkunde, Fingerabdruck oder andere biometrische Merkmale [ATSI00]

DEFINITION 2 (Sicherheit) Information, die von einer Funktionseinheit zur nächsten übertragen wird, um Unabstreitbarkeit von Zugangsrechten zu sichern [ATSI00]

Da ein Credential immer an eine Identität geknüpft ist, muss im Vorfeld geklärt werden was für Arten von Identitäten existieren. Dieses kann aber nicht vollständig geschehen, da dies den Rahmen dieser Arbeit sprengen würden. Nachfolgend werden Arten von Identitäten betrachtet, die im Kontext mit Credentials für wichtig erachtet werden.

## 2.1 Identitäten

Auf den ersten Blick kann die Identität eines Menschen oder einer Sache folgender Maßen definieren: Sie ist die Gesamtheit der Merkmale, anhand derer die Menschen sich voneinander unterscheiden. Diese Identität erlaubt auf den ersten Blick eine eineindeutige Identifikation. Werden aber eineiige Zwillinge verglichen so ist objektiv betrachtet die Anzahl der Merkmale, anhand der sie sich unterscheiden gleich null, sie sind der Definition nach identisch. Da sie aber beide gleichzeitig nebeneinander existieren, können sie nicht identisch sein.

Ein ähnliches Beispiel führt Waismann auf: "Wir sagen: "Der Mann, der jetzt ins Zimmer tritt, ist derselbe, den ich vorhin auf der Straße gesehen habe." Was ist hier mit dem Ausdruck "derselbe" gemeint? Nun, was gilt als das Kriterium dafür, dass dies wirklich derselbe Mann ist? Sind dies Merkmale wie seine Kleidung, sein Wuchs, sein Aussehen, die Farbe seiner Haare etc.? Aber all dies ist nicht

entscheidend; denn es ist gewiss denkbar, dass es zwei Menschen gäbe, die sich "aufs Haar" gleichen und die doch nicht identisch sind." [Wais02]

Das alleinige Kriterium für die Identität nach Waismann ist die Existenz in Raum und Zeit, also die kontinuierliche Existenz im Raum. Um beispielsweise die Identität eines Verbrechers mit der eines Verdächtigen festzustellen, wird die Spur des Verbrechers in die Vergangenheit zurückverfolgt. Es werden die Angaben des Verdächtigen überprüft und mit dem konstruierten Verbrechenshergang verglichen. Decken sich die Angaben von Verbrecher und Verdächtigen räumlich und zeitlich erhärtet sich die Indizienlage gegen den Verdächtigen.

Allgemein betrachtet kann daraus geschlossen werden, dass "identisch" das ist, was als identisch erklärt wird. Es ist nicht möglich alle Merkmale eines Menschen oder einer Sache zu betrachten, deshalb werden zur Identitätsbildung nur Merkmale herangezogen, die in diesem speziellen Kontext für wesentlich gehalten werden. Die schon erwähnte räumliche und zeitliche Kontinuität ist ebenfalls erforderlich.

## 2.2 Virtuelle Identitäten

Im zwischenmenschlichen Kontext sind die identitätsbildenden Merkmale unter anderem; Geschlecht, Aussehen respektive Sprache. Sich im Alltag eine andere Identität zu verschaffen, ist möglich, aber nur in einem gewissen Rahmen, da Aussehen oder Geschlecht nicht so einfach zu ändern sind.

Die Nutzer des Internet können beispielsweise in Chat-Rooms eigene virtuelle Identitäten erschaffen. Für sie besteht die Möglichkeit die eigenen Identitäts bildenden Merkmale preisgeben, wenn sie sich in den Chat-Rooms mit anderen virtuellen Identitäten unterhalten. Es können aber auch vollkommen andere Identitäts bildende Merkmale für die erschaffene virtuelle Identität gewählt werden. Den virtuellen Identitäten auch Pseudonyme oder Avatare genannt, kann nicht vertraut werden, da eine Person mehrere virtuelle Identitäten haben kann. Es ist außerdem möglich, dass mehrere Personen zu verschiedenen Zeiten dieselbe virtuelle Identität darstellen. Weiterhin ist es jederzeit möglich, eine virtuelle Identität aufzugeben.

Für Kommunikationsprozesse ist es nötig, dem Kommunikationspartner zu vertrauen. Bei virtuellen Identitäten kann dies so geschehen, dass über einen unbestimmten Zeitraum das Verhalten, im Chat z.B. die Äußerungen beobachtet werden. Haben diese Konsistenz und Kontinuität kann dem Pseudonym gewisses Vertrauen geschenkt werden. Diese Vertrauensbildung mit Konsistenz und

Kontinuität findet auch bei einem großen Internetauktionshaus Verwendung. Der Nutzer, der sich dort anmeldet, muss zwar dem Bereitsteller des Dienstes seine wahre Identität, angeben aber gegenüber den anderen Nutzern ist er eine virtuelle Identität. Da er zu Beginn keine Bewertungen besitzt, ist er für die Nutzer nicht vertrauenswürdig. Hat er eine Ware, die von jemanden anders ersteigert wurde, ordnungsgemäß verschickt, bekommt er eine positive Bewertung und wird somit vertrauenswürdiger. Wurde nichts oder nur ein Ziegelstein anstatt eines DVD-Players verschickt, erhält der Verkäufer eine negative Bewertung. Je mehr positive Bewertungen er erhält, umso vertrauenswürdiger ist er und umso mehr kann er verkaufen. Bei diesem System wird natürlich vorausgesetzt, dass sich der Verkäufer weiterhin so verhält, wie er sich in der Vergangenheit verhalten hat.

## 2.3 Einfache Digitale Identität

Eine Vertrauensbasis kann auch geschaffen werden, wenn von einer vertrauenswürdigen Person eine Empfehlung für eine andere vertrauenswürdige Person gegeben wird. Dies kann auch eine vertrauenswürdige Institution sein, die keine Nutzen davon hat, die Vertrauenswürdigkeit einer Person zu verändern. Der Person werden ein Datensatz und eine eindeutige alphanumerische Symbolfolge zugeordnet und gespeichert. Diese eineindeutige Zuordnung kann auch vom Staat vollzogen werden. So ist in den USA eine neunstellige Sozialversicherungsnummer eine solche einfache digitale Identität für jeden US-Bürger. Nur wenn ein Bürger diese Nummer besitzt, ist ein Leben in den USA möglich, nur dann kann ein Mietvertrag abgeschlossen werden, ein Konto eröffnet werden usw..

Ähnlich ist es mit der Matrikelnummer der Studenten an der Universität. Werden aber genügend Daten, z.B. an verschiedenen Aushängen die Zensuren über bestandene Prüfungen einer Matrikelnummer gesammelt kann ein Profil über den Studenten diese Matrikelnummer erstellt werden.

Das Problem dieser einfachen Identitäten ist dass, sie als Primärschlüssel genutzt werden, wenn auf Daten zugegriffen werden soll. Er ist überall gleich und somit verfolgbar. Jede einfache digitale Identität hat genau ein Pseudonym für eine Person und damit ist bei alle Institutionen bei denen dieses Pseudonym genutzt wird es für diese Person gleich.

## 2.4 Digitale Identität durch Credentials

In Anbetracht dieser Nachteile erweiterte Chaum die digitalen Identitäten mit einem System basierend aus asymmetrischer Verschlüsselung und Credentials. In diesem System ist nicht mehr nachvollziehbar, wer welche Transaktion durchgeführt hat. Die Basis dieses Systems ist, dass jeder Nutzer nicht unter nur einem Pseudonym, sondern unter mehreren Pseudonymen bekannt ist. Es ist möglich für jeden Gebrauch eine neues Pseudonym zu erstellen. Die Vertrauenswürdigkeit bleibt trotz der verschiedenen Pseudonyme erhalten. Der Nutzer kann gegenüber der Mietwagenfirma ein anderes Pseudonym verwenden als gegenüber der Bank und trotzdem die Zahlung des Betrages von der Bank zur Mietwagenfirma möglich, ohne dass es zu Zuordnungsproblemen mit dem überwiesenen Geldbetrag kommt. Der Nutzer tritt anonym auf, ist aber vertraulich.

Im Folgenden wird das Credential als ein Recht oder ein Attribut genutzt. Es kann ein Zahlungsmittel oder auch ein Zugangsrecht sein. Es wird von der Instanz X der Instanz Y zugesichert wird, dass Nutzer N diese Recht / diesen Geldbetrag besitzt.

Dieser nicht nachvollziehbare Credentialtransfer zwischen Pseudonymen kann an Beispiel von Fensterbriefumschlägen in denen ein Blatt Blaupapier liegt, erläutert werden.

Ein Nutzer N schreibt ein Pseudonym auf eine Blatt Papier steckt dieses in einen Fensterumschlag (nur das Pseudonym ist durch das Fenster zu sehen) und fügt noch ein Blatt Blaupapier hinzu. Dieses Pseudonym verwendet er immer gegenüber der Organisation X. Die Organisation X fügt nun das Credential, eine Signatur in Form eines Stempels auf den Umschlag hinzu. Das Credential (Signatur) wird nach Empfang vom Nutzer verifiziert. Er öffnet den Umschlag und entnimmt das Blatt Papier auf dem durch den Stempelabdruck auf das Blaupapier eine Signatur zu erkennen ist. Da er die Signatur der Organisation X kennt, ist das Credential dadurch verifiziert.

Möchte der Nutzer später der Organisation Y das Credential nachweisen, das er von Organisation X erhalten hat, steckt er dies in einen neuen Fensterumschlag, bei dem das Pseudonym mit dem er bei Y bekannt ist, dem Blatt hinzugefügt hat und die von Organisation X erhaltene Signatur zu lesen sind . Y kann nun das Credential verifizieren und Y ist bekannt, dass der Nutzer das Credential besitzt. Das Öffnen des Briefes ist der Organisation Y nicht möglich, somit kennt sie nicht das Pseudonym welches gegenüber Organisation X verwendet wurde.

Für dieses System ist eine Public Key Infrastructure (PKI) nötig, bei der jeder

Teilnehmer einen privaten und einen öffentlichen Schlüssel besitzt. Der Stempel im obigen Beispiel ist der private Schlüssel der Organisation. Der private Schlüssel wird dazu verwendet Nachrichten, die empfangen wurden zu entschlüsseln und zu signieren. Mit dem öffentlichen Schlüssel wird verschlüsselt und Signaturen können damit überprüft werden, deren Authentizität dann verifiziert ist. Das Verifizieren des von der Organisation X erhaltenen Umschlags in obigen Beispiel kann mittels des öffentlichen Schlüssel der Organisation X durchgeführt werden. Damit ist es dem Nutzer und der Organisation Y möglich der Echtheit des Umschlages zu vertrauen.

## 2.5 Credential-basiertes Authentifikationsprotokoll

In einigen Situationen ist es nicht möglich auf eine PKI zurückgreifen zu können. Dies ist beispielsweise dann der Fall, wenn ein mobiles Gerät sich an ein unbekanntes drahtloses Netzwerk anmelden will. Die Zertifikate und Schlüssel die die Vertrauenswürdigkeit dieses Netzes bezeugen könnten, sind dem mobilen Gerät nicht bekannt, und könnten nicht überprüft werden, da kein Zugang in ein vertrauenswürdiges Netzwerk besteht. Dennoch ist es möglich eine Authentifikation zwischen beiden Geräten herzustellen.

Die Nutzung von Credentials, die nach deren Generierung über einen sicheren Kanal zwischen dem Nutzer und dem Netz ausgetauscht werden, ist die Grundlage für die anschließende Authentifikation auf einem anderen Kanal.

Um eine sichere Authentifikation zu erhalten müssen die folgenden vier Punkte beachtet werden:

1. Prä-Authentifikation: Sichere und faire Geheimniserzeugung und Austausch der Geheimnisse über einen sicheren Kanal. Fair heißt, es darf keine Abhängigkeit zwischen den Erzeugungsalgorithmen der Partner geben.

2. Verifikation und Schlüsselerzeugung: Die Existenz des Geheimnisses auf dem jeweils anderen Gerät wird von jedem Gerät überprüft. Ist das Resultat positiv, dann werden mittels der Geheimnisse stärkere Schlüssel für die Funkstrecke erzeugt.

3. Sichere Kommunikation: Hier muss eine eventuelle kurzzeitige Verbindungsunterbrechung gehandhabt werden.

4. Aufheben der Sicherheitsassoziation: Verwerfen der Credentials und Schlüssel nach einer definierten Zeit. Diese Zeit kann von Kontextparametern abhängen,

vordefiniert oder ausgehandelt sein. Wenn ein Kommunikationspartner seinen Schlüssel nicht verwirft, ist dieser nutzlos, da der Kommunikationspartners dem Protokoll entsprechend alte Schlüssel nicht mehr akzeptiert [Chan/Kreu03].

### 2.5.1 Prä-Authentifikation

Jeder der Kommunikationspartner erzeugt jeweils ein Credential über einen Random Number Generator. Anschließend werden beide Credential über einen sicheren Kanal mittels "three way handshake" ausgetauscht. Hierbei wird dem mobilen Gerät zusätzlich eine private IP-Adresse von der Feststation zugewiesen, um es in der darauf folgenden Phase mit dieser Identität ansprechen zu können.

Der Kanal muss in dieser Phase sehr sicher sein, da ansonsten ein Identiätsdiebstahl ermöglicht werden könnte. Da aber diese Phase sehr kurz ist und keine großen Informationsmengen übertragen werden, sind einfache Verfahren mit geringer Reichweite für diese Phase geeignet. Nach Abschluss der Prä- Authentifikationsphase schalten beide Kommunikationseinheiten auf das gewünschte Kommunikationsmedium um [Chan/Kreu03].

### 2.5.2 Verifikation und Schlüsselerzeugung

In dieser Phase findet eine Einigung der beiden Partner auf einen gemeinsamen Verschlüsselungsalgorithmus, einen Message Authentification Code (MAC) - Algorithmus und eine Diffie-Hellmann-Gruppe (aus der Cipher Suite beider Geräte) statt. Folgend findet ein gegenseitiger Beweis über das Vorliegen der Credentials und die Integrität der bisher offen ausgetauschten Nachrichten statt.

In der Protokollbeschreibung stellt A die Feststation und B das mobile Gerät dar. A gibt seine Cipher Suite $CS_A$ in der Reihenfolge seiner Prioritätensetzung B bekannt. B wählt hieraus eine Teilmenge, die Cipher Suite $CS_B$ aus. Mittels der Credentials ($C_A$, $C_B$), der Noncen ($N_A$, $N_B$) und dem resultierenden Diffie-Hellmann-Schlüssel ($g^{ab}$) der beiden öffentlichen Diffie- Hellmann Werte $g^a$ und $g^b$ werden die geheimen Sitzungsschlüssel ($K_A$, $K_B$) und die geheimen MAC-Schlüssel ($M_A$, $M_B$) generiert. Die DiffieHellmann-Guppe wird nur dann ausgewählt, wenn das mobile Gerät für die sichere Kommunikationsphase (3. Phase) Schlüssel mit Perfect Forward Secrecy (PFS) benötigt, ansonsten werden alle Schlüssel ohne Diffie- Hellmann-Werte generiert. Am Ende erfolgt die gegenseitige Authentifikation zwischen der Feststation und dem mobilen Endgerät über die berechneten Werte HASH-A und HASH-B. Durch die Überprüfung der Hashwerte

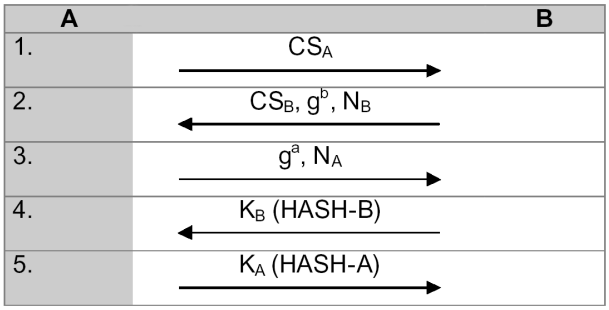


Abbildung 2.1: Ablauf der Verifikation und Schlüsselerzeugung [Chan/Kreu03]

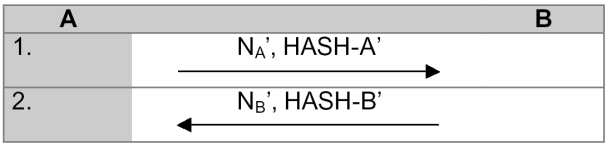


Abbildung 2.2: Verhalten bei Verbindungsunterbrechung [Chan/Kreu03]

wird die gegenseitige Authentifikation und die Integrität sowie die Authentizität der früheren Nachrichten festgestellt [Chan/Kreu03].

In die Berechnung des Hashs gehen die beschriebenen Parameter ein (‖ bezeichnet die Verkettung der Parameter):

HASH-B ($M_B$, $g^b \parallel g^a \parallel N_B \parallel N_A \parallel C_A \parallel CS_B$)

HASH-A ($M_A$, $g^a \parallel g^b \parallel N_A \parallel N_B \parallel C_B \parallel CS_A$)

Durch die Verwendung von $C_A$ und $C_B$ im Hash ist der Nachweis für die Geräteauthentifikation geliefert, $N_A$ und $N_B$ beweisen die Aktualität der Nachrichten (timeliness) [Chan/Kreu03].

### 2.5.3 Verhalten bei Verbindungsunterbrechung

Bei einem (kurzzeitigen) Ausfall einer authentifizierten Verbindung, muss die Möglichkeit bestehen, dass der legitime mobile Anwender die Verbindung wieder herstellen kann.

1. Schritt: Wenn die Verbindung abgebrochen wurde, sendet der AP eine Aufforderung an das mobile Gerät, dass dieses sich für den erneuerten Verbindungsaufbau authentifizieren soll. Der AP übermittelt hierbei die neue Nonce $N_A$ und den neuen HASH-A als Challenge: HASH-A = MAC($M_A$, $N_A \parallel C_B$).

2. Schritt: B verifiziert den HASH-A, welcher den Nachweis der Kenntnis des Credentials B enthält und überprüft die Aktualität anhand der Nonce. Anschlie-

ßend sendet B seine Response, die analog zu Schritt 1 aufgebaut ist. Die Kommunikation kann jetzt fortgesetzt werden [Chan/Kreu03].

Die bisher aufgezeigten Verfahren lassen das Überprüfen der Identität der Kommunikationsgeräte zu. Damit kann aber nicht auf die Identität des Nutzer geschlossen werden. Besonders bei mobilen Geräten besteht die Gefahr, dass diese durch Vergeßlichkeit oder Diebstahl dem Nutzer abhanden kommen und somit kann ein Missbrauch des Gerätes ist nicht ausgeschlossen.

## 2.6 Zusammenfassung

Es wurden Grundprobleme der Kommunikationstechnik aufgezeigt: Identität des Kommunikationspartners, Vertrauen in die Identität des Partners (Authenzität), die Vertaulichkeit des Kommunikationsweges, Anonymität der Kommunikation. Es wurden die Schwächen der virtuellen Identität und der einfachen digitalen Identität erkärt. Daraus wurde die Lösung dieser Probleme abgeleitet, es ist die Nutzung von Credentials zur Schaffung einer sicheren digitalen Identität. Dieses Verfahren wurde erläutert, weiterhin wurde ein Protokoll zur sicheren Authentifikation der Kommunikationspartner vorgestellt.

Die genannten Verfahren zur Authentifikation schaffen aber nur eine Vertrauensbasis zwischen den Endkommunikationsgeräten. Um beispielsweise eine Eingangstür zu einen sicherheitsrelevanten Bereich zu öffnen reicht dies nicht aus. Es muss sichergestellt werden welcher Nutzer (Mensch) diesen Bereich betreten möchte. Dies ist mit Hilfe biometrischer Verfahren möglich.

# Kapitel 3

# BIOMETRIK

Die Definition des Begriffes "Biometrik" wird in der Öffentlichkeit häufig nicht von Begriffsdefinition des Wortes "Biometrie" unterschieden, obwohl es Unterschiede gibt:

DEFINITION 1 Biometrie (nach [Dud82]):

1. Wissenschaft von der Zählung und [Körper]messung an Lebewesen; biologische Statistik
2. Zählung und [Körper]messung an Lebewesen [Dud82]

DEFINITION 2 Biometrie (nach [Lor96]) :

> Unter dem Begriff der Biometrie werden die vielfältigen Anwendungen der Mathematik, insbesondere der mathematischen Statistik, in den biologischen und ihnen verwandten Wissenschaften zusammengefasst.

Die Vermessung des menschlichen Körpers ist hier ebenfalls enthalten! [Lor96]

DEFINITION 3 Biometrik (Schnittmenge der Biometrie und Informatik) :

> Anwendungen der Biometrie in der Informatik und umgekehrt.

Häufig werden die Begriffe Biometrie und Biometrik als Kurzform für biometrische Identifikations- und Verifikationsverfahren verwendet, die wie folgt definiert sind [Brö01]:

DEFINITION 4 Biometrische Identifikation (biometric identification):

1. Erkennung einer Person anhand biometrischer Merkmale mit/ohne Einwilligung der Person
2. 1:n-Zugriff auf eine biometrische Datenbank (im Rahmen einer biometrischen Authentifikation) [Brö01]

Es wird anhand biometrischer Merkmale die Identität der zugehörigen Person ermittelt. Ein spezifischer Algorithmus generiert aus einem biometrischen Merkmal

(z.B. dem Fingerabdruckmuster) eine vergleichbare Kenngröße (”biometrische Signatur”, Template), die gespeichert wird. Bei der biometrischen Identifikation wird die zu überprüfende Signatur gegen die gesamte Datenbank aller in Frage kommenden Signaturen getestet. Gesetzt den Fall, dass sie einer der gespeicherten Signaturen hinreichend ähnlich ist, werden die zugehörigen Personendaten des Trägers der gespeicherten Identität als Antwort ausgegeben. Falls keine der gespeicherten Signaturen der untersuchten ausreichend entspricht, scheitert die Identifikation. [Biom02]

Zunehmend wichtige Einsatzfelder biometrischer Identifikationssysteme sind die Überprüfung der Handlungsberechtigung von Personen bei E-Banking- und E-Commerce-Transaktionen und im Rahmen von Zugangskontrollen zu besonders gesicherten Gebäuden, Räumen oder Gebieten (z.B. Flughafenbereiche). Die bislang vorwiegend verwendeten Passwörter oder Chipkarten in Verbindung mit Zahlencodes (PIN = Personal Identification Number), die auf ”Wissen respektive Besitz” beruhen, weisen - vor allem durch ihre ausufernde Zunahme - Schwächen bzw. Risiken auf, die mit den Wörtern Verlieren - Vergessen - Stehlen anschaulich charakterisiert werden können [Behr/Roth01]. Ob der Nutzer, der die korrekten Daten liefert, auch der rechtmäßige Inhaber derselben ist, kann von konventionellen Systemen nicht überprüft werden. Durch die individuelle Personengebundenheit und Einmaligkeit der biometrischen Merkmale soll dieses Problem gelöst werden. Biometrie soll dabei neue Qualitäts-, Komfort- und Sicherheitsdimensionen bei der Personenauthentifizierung erschließen und wird häufig als alternativlose Technologie beschrieben, ohne deren Nutzung eine wirklich umfassende Ausdehnung des elektronischen Handels für Endverbraucher nicht vorstellbar erscheint. (vgl. [Nold02])

## 3.1 Grundlagen zu biometrischen Verfahren

### 3.1.1 Prinzipielle Anforderungen an Merkmale und Verfahren

Merkmale des Menschen, ob physiologische (passive) oder verhaltensabhängige (aktive), müssten folgende vier Eigenschaften aufweisen, um ”biometrisch optimal genutzt” werden zu können: [Behr/Roth01]

- Universalität (bei jedem Menschen vorhanden),
- Einzigartigkeit (bei jedem Menschen verschieden),
- Beständigkeit (ohne Veränderungen über die Zeit) und

- Erfassbarkeit (durch ein technisches System quantitativ messbar).

Die biometrischen Verfahren bzw. Systeme wiederum müssen eine Reihe von Kriterien der Praxistauglichkeit erfüllen, u.a. [Behr/Roth01]

- technische Umsetzbarkeit (Schnelligkeit, Kompatibilität),
- Robustheit (Wartungsaufwand),
- Empfindlichkeit (Genauigkeit) und Überwindungsresistenz (Sicherheit)
- ökonomische Machbarkeit (vertretbare Kosten für Betreiber)und
- Nutzerfreundlichkeit (Zuverlässigkeit, Einfachheit/Komfort, Hygiene/Gesundheit).

Wie im Weiteren gezeigt wird, kann keines der derzeit genutzten "biometrischen Merkmale" beziehungsweise keines der verfügbaren Systeme alle genannten Kriterien vollständig erfüllen, zum Teil aus praktischen, zum Teil aus prinzipiellen Gründen. Es sind aber durchaus weltweit zahlreiche Systeme in unterschiedlichen Anwendungskontexten in Betrieb. Ökonomisch bislang am erfolgreichsten sind die Erkennung von Fingerbild, Handgeometrie, Gesicht, Stimme, Iris und Unterschrift/Handschrift [Pet/Sau02].

### 3.1.2 Grundlegende Begriffe der Biometrik

#### 3.1.2.1 Das Enrolment

Die Grundlage jedes biometrischen Verfahrens ist, unabhängig von dem genutzten Merkmal und der angewandten Technik, das Enrolment. Es umfasst das (Ver-)Messen und das Erfassen des biometrischen Merkmals der zukünftigen Nutzer, die Umwandlung der "Rohdaten" mittels eines Algorithmus in einen Referenzdatensatz und abschließend die Speicherung desselben, des Templates. Dieses stellt den Vergleichswert dar, mit dem bei allen darauf folgenden biometrischen Überprüfungen die neu ermittelten Messdaten, zumindest zu einem hohen Grad, übereinstimmen müssen, um so den Nutzer identifizieren zu können [Pet/Sau02].

Man unterscheidet zwei verschiedene Arten der biometrischen Überprüfung einer Person:

- die biometrische Verifikation, d.h. die Bestätigung der behaupteten Identität des Individuums (1:1 = die vermessene Person ist tatsächlich die, die sie zu sein behauptet), und

| erfasstes Merkmal | gemessene Charakteristik |
|---|---|
| *physiologisch (passiv)* | |
| Fingerbild (Muster der Hautleisten auf der Fingerkuppe) | Verzweigungs- und Endpunkte der Fingerlinien (Minuzien) |
| Handgeometrie | Länge, Dicke und Abstand der Finger, Profil der Hand, evtl. Venenmuster |
| Retina | Muster der Blutgefäße im Augenhintergrund |
| Iris | Muster des Gewebes um die Pupille |
| Gesicht | typische geometrische Merkmale des Gesichts (Augen, Kinn, Nase, Mund) |
| *verhaltensabhängig (aktiv)* | |
| Unterschrift (Schreibdynamik) | Schriftbild und Schriftzug, Geschwindigkeit, Druck, Beschleunigung |
| Handschrift (Schriftsemantik) | (wie z.B. Unterschrift) Syntax des Schriftbildes |
| Stimme | akustisches Spektrum (teils vorgegebene Wörter) |
| *multimodale/hybride Systeme* | |
| z.B. Gesicht-Mimik-Stimme | akustisches Spektrum und Lippenbewegung |

Tabelle 3.1: Derzeit vorrangig genutzte biometrische Merkmale des Menschen [Behr/Roth01] [Ditt01]

- die biometrische Identifikation, d.h. die Erkennung eines Individuums aus einer (definierten) Menge biometrisch registrierter Personen (1:n = die vermessene Person ist Teil der Menge {n})

#### 3.1.2.2 Verifikation

Im Fall der Verifikation werden die durch den Sensor ermittelten Messdaten mit den vorhandenen Daten der Einzelperson verglichen, die z.B. auf einer Chipkarte oder einem PDA (Personal Digital Assistant) dezentral, also im Besitz der Person, abgelegt sind oder aber zentral auf einem Server gespeichert sein können.

#### 3.1.2.3 Identifikation

Im Fall der Identifikation vergleicht das biometrische System die gemessenen Daten mit den zentral gespeicherten Daten aller zuvor Registrierten und prüft, welches Template am besten mit dem des aktuellen Nutzers übereinstimmt. Dadurch entstehen höhere Anforderungen hinsichtlich der benötigten Datenbankgröße und Identifikationszeit. Diese Art der biometrischen Erkennung wird derzeit vor allem in Hochsicherheitsbereichen mit einer geringen Anwenderanzahl oder zu polizeilichen Ermittlungszwecken eingesetzt [Pet/Sau02].

#### 3.1.2.4 Authentifizierung/Authentifikation

Als Oberbegriff gilt (biometrische Personen-)Authentifizierung/Authentifikation, der sich jedoch im deutschen Sprachraum - zumindest bislang noch - nicht durchgesetzt hat [Nold02], so dass meist allgemein von "biometrischer Personenidenfikation" gesprochen wird, auch wenn lediglich eine Verifizierung stattfindet. Begrifflich abzusetzen ist die Autorisierung (als eigentliches Ergebnis der Überprüfung der Identität des Nutzers), also die Ermächtigung bzw. Bevollmächtigung für einen Zugang oder für eine Handlung [Tele02].

#### 3.1.2.5 Einschränkungen der Einzigartigkeit, Genauigkeit und Reproduzierbarkeit

Idealerweise wäre jeder gewonnene biometrische Datensatz einzigartig für ein menschliches Individuum und diesem eindeutig zuzuordnen - ursprünglich erhobene Referenzdaten (Template) und jeweils gemessener Datensatz wären identisch. In der Praxis resultieren Einschränkungen dieser idealen Einzigartigkeit, Genau-

igkeit und Reproduzierbarkeit aus verschiedenen Gründen, welche im Folgenden aufgelistet sind:

- Jeder Messvorgang bedeutet eine starke Informationsreduktion. Aus prinzipiellen (Kapazitäts-)Gründen muss die erhobene Datenmenge begrenzt werden. Hinzu kommt die jeweilige Messgrenze (Empfindlichkeit) und Genauigkeit des Sensors bzw. des Gesamtsystems sowie das nicht zu vermeidende "Rauschen". Die zu speichernde Datenmenge des Templates sollte aus technischen Gründen (Speichergröße, Übertragungsraten) weitestgehend minimiert werden, wodurch aber die Genauigkeit reduziert wird.

- Die Genauigkeit und Einzigartigkeit des extrahierten Datensatzes ist auch davon abhängig, ob die Merkmale bei der zu erfassenden Person überhaupt und in aussreichendem Umfang vorhanden sind.

- Verhaltensabhängige Merkmale weisen aufgrund der Natur der menschlichen Motorik immer eine mehr oder weniger große Varianz auf. Doch auch physiologische Merkmale sind nur eingeschränkt zeitlich konstant. Sie können durch Alterungsprozesse, Krankheiten oder Verletzungen vorübergehend oder dauerhaft verändert werden. Leichte Veränderungen müssen daher sowohl bei "aktiven" als auch bei "passiven" Verfahren vom System toleriert werden.

- Hinzu kommen störende Umwelteinwirkungen während der Messung, z.B. unterschiedliche Lichtverhältnisse oder Temperaturveränderungen, welche die Leistungsfähigkeit von Sensoren beeinflussen können [Ditt01].

### 3.1.3 Prinzipieller Ablauf einer biometrischen Erkennung

Ein System zur biometrischen Erkennung verarbeitet die von Sensoren erfassten biometrischen Daten mit dem Ziel, mit Hilfe von vorher erfassten Referenzdaten die Identität dieser Person zu bestätigen oder zurückzuweisen. Alle biometrischen Systeme beinhalten die Prozesse Datenaufnahme, Vorverarbeitung, Merkmalsextraktion, Klassifikation und Referenzbildung. Für die Anpassung an Veränderungen des biometrischen Merkmals kann ein adaptives Verfahren eingesetzt werden. In Abbildung 3.1 und Abbildung 3.2 ist der grundsätzliche Aufbau eines biometrischen Systems dargestellt. Mit Hilfe eines Sensors werden die Eingabedaten aufgenommen. Sie werden vor oder während des Mustervergleichs vorverarbeitet

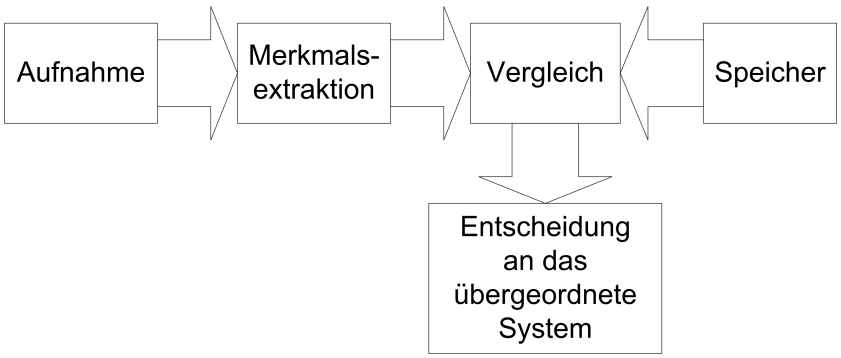


Abbildung 3.1: Ablauf eines biometrischen Verfahrens nach [Tele02]

und normalisiert. Zur Klassifikation können entweder die vorverarbeiteten Daten oder daraus extrahierte Merkmale (Templates) verwendet werden. Diese Eingangsdaten werden dabei mit den entsprechenden Referenzdaten verglichen. Zur Auswahl der Referenzdaten aus der Referenzdatenbank kann der Benutzer z. B. seine persönliche Identifikationsnummer angeben. Alternativ dazu können die Referenzdaten auch auf einem im Besitz des Nutzers befindlichen Speichermedium (z.B. Chipkarte oder PDA) gespeichert sein. Bei adaptiven Verfahren können die erhaltenen Bewertungen im Fall einer positiven Klassifikation zur Aktualisierung der Referenzdaten verwendet werden [Tele02].

### 3.1.4 Fehlerarten und -raten

Eine vollkommen theoretische Sicherheitsabschätzung, in Hinsicht auf mathematische Abschätzungen, wie man es von der Kryptographie oder der Diskussion um die PIN kennt, kann in der Biometrie nicht gemacht werden. Einer der Gründe dafür ist, dass die biometrischen Fehlerraten nur empirisch zu ermitteln sind. Empirisch ermittelte Fehlerraten können nur mit großem Testaufwand sehr klein werden.

Ist z.B. in der Kryptographie auf Grund theoretischer Überlegungen die Fehlerwahrscheinlichkeit sehr gering, trifft dies aber keinesfalls auf aus dem praktischen Versuch ermittelte oberen Schranken der Fehlerraten zu. Diese sind in der Realität um mehrere Größenordnungen größer. Die empirisch ermittelte obere Schranke einer Fehlerrate kann nie Null sein, sondern kann sich diesem Wert (bei einer sehr großen Zahl von Testpersonen) nur annähern.

Jedes biometrische System hat also immer eine unvermeidbare Restfehlerquote. Diese Fehlerquote lässt sich aber nur sehr schwer objektiv ermitteln, da sie

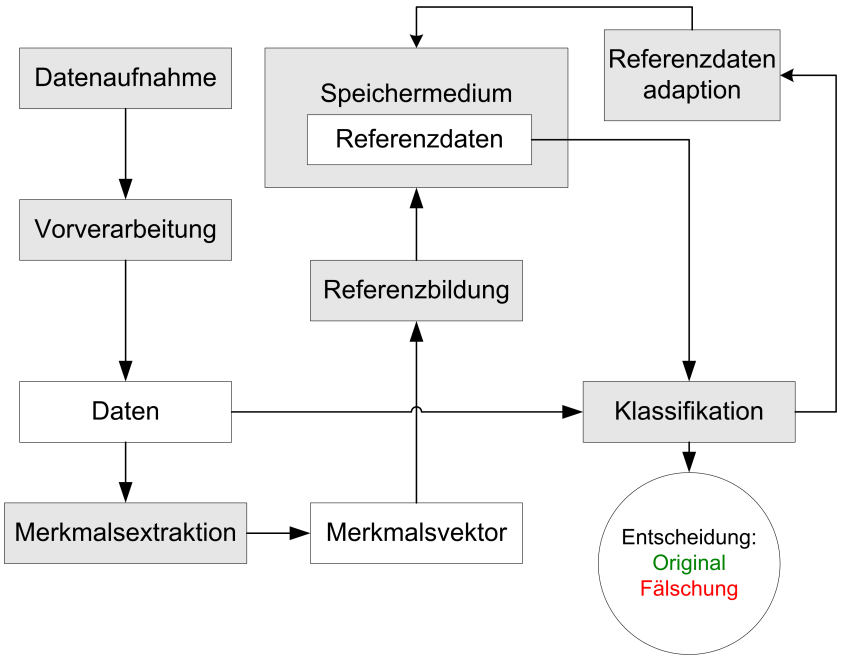


Abbildung 3.2: Ablauf einer biometrischen Verifikation nach [Tele02]

stark von der Vorauswahl der Versuchspersonen und den jeweiligen Versuchsbedingungen abhängt. Die realen Fehlerraten weichen in der Praxis nicht selten von den Angaben des Herstellers ab. Um die Fehlerraten der Hersteller beurteilen zu können, sind konkrete Angaben über Versuchsanordnung und Versuchsbedingungen notwendig. Erst die individuelle Anpassung des Systems an die Anforderungen des einzelnen Betreibers ermöglicht Aussagen über die Verwendbarkeit des Systems in der konkreten Anwendung [Tele02].

### 3.1.5 Toleranzschwelle

Da nicht bei jeder Messung eines biometrischen Merkmales genau derselbe Wert ermittelt werden kann, der beim Enrolment gespeichert wurde, muss das System eine gewisse Toleranzschwelle, bei der Entscheidung ob es sich um dieselbe Person handelt, haben. Diese Schwelle muss so gewählt werden, dass auch Personen trotz Heiserkeit, einer neuen Frisur, einem Bart, einer Schnittwunde sicher erkannt werden können. Sie darf aber nicht zu niedrig sein, so dass eine andere Person als biometrischer Zwilling Eintritt in einen Bereich erhalten kann, der durch eine biometrisches System gesichert ist.

Die Festlegung dieser Toleranzschwelle stellt sehr hohe Forderungen an ein biometrisches System. Die "False Rejection Rate" (FRR) gibt an, dass ein System

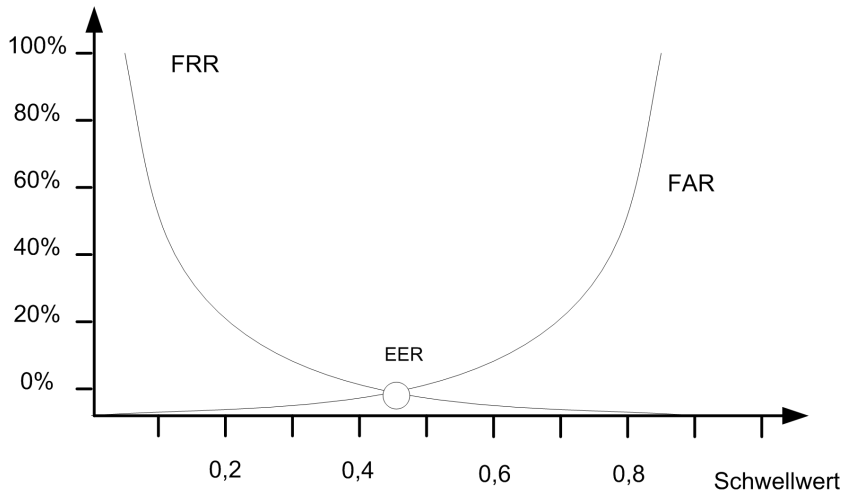


Abbildung 3.3: Verhältnis FRR und FAR [Tele02]

einem Nutzer keinen Zugang gewährt obwohl dieser zugangsberechtigt ist. Die FRR wird auch als Typ-I-Fehlerrate bezeichnet, die FAR (False Acceptance Rate) als Typ-II-Fehlerrate. Die FRR bezieht sich auf die Anzahl der fälschlich vom System zurückgewiesenen autorisierten Personen. Die FAR beinhaltet die Anzahl der nicht autorisierten Personen, die vom System akzeptiert wurden. Es gelten hierbei folgende Gesetzmäßigkeiten:

$$FRR = \frac{NFR}{NAA} * 100\% \qquad FAR = \frac{NFA}{NIA} * 100\% \tag{3.1}$$

NFR (Number of False Rejection) und NFA (Number of False Acceptances) stehen für die Anzahl der "falschen Zurückweisungen" bzw. "falschen Akzeptierungen". NAA (number of authorized identification attempts) ist die Anzahl der autorisierten Identifizierungs- oder Verifizierungsversuche. NIA (number of impostor identification attempts) ist die Anzahl der nicht autorisierten Anmeldeversuche (Hochstapler-/Betrugversuche). Weniger gebräuchlich ist die so genannte "Equal Error Rate" (ERR), auch Crossover-Rate oder Gleichfehlerrate genannt (Abb. 3.3. Sie bezieht sich auf den Schnittpunkt von FRR und FAR. Ein System beispielsweise mit einer FRR und FAR von 1% hat eine ERR von ebenfalls 1%. [Abda/Abs02]

Ein biometrisches System kann auch ein Merkmal des Menschen verwenden, dass keine 100%ige Verbreitung hat, nicht bei allen Nutzern innerhalb der Organisation des Betreibers vorhanden ist und somit nicht ausgewertet werden kann. Mit der "Failure to Enrol Rate" (FER) wird der Prozentsatz der potentiellen Nutzer

angegeben, bei denen das Enrolment nicht erfolgreich durchgeführt werden konnte. Als mögliche Ursachen sind die folgenden Aspekte zu berücksichtigen:

- Merkmal fehlt (Finger, Iris, etc..)
- Einschränkung in der Erfassung (Brille, Kontaktlinse, schwache Ausprägung des Merkmals)
- Fehlendes oder unzureichendes technisches Verständnis des Nutzers mit dem System zu interagieren (Person beherrscht den Gebrauch des Systemes auch nach mehrmaliger Einführung nicht)
- Systemprobleme z.B. Sensorqualität, Algorithmen
- Fehlende Akzeptanz des Verfahrens (z.B. aus gesundheitlichen Bedenken).

Die FER ergibt sich wie folgt:

$$FER = \frac{NNE}{NPU} * 100\% \tag{3.2}$$

wobei: NNE: die Anzahl der Personen, bei denen das Enrolment nicht durchgeführt werden konnte (number of not enroled person), NPU: die Gesamtanzahl (Population) der potentiellen Nutzer innerhalb der Organisation des Betreibers (number of potential users) [Tele02].

## 3.2 Fingerabdruckerkennung

Die Fingerabdrücke eines Menschen gelten als völlig einzigartig. Die Ausprägung der Fingerabdrücke findet im Mutterleib statt und ist u.a. von der Lage des Fötus im Mutterleib abhängig, deshalb können auch eineiige Zwillinge, die ja genetisch identisch sind, unterschieden werden. Zur Erkennung wird das gesamte Graustufenbild ("Pattern Matching") oder die sog. Minuzien ("Kleinigkeiten"; hier: endende Täler, Verzweigungen, Schweißporen der Fingeroberfläche) analysiert und Merkmale extrahiert. Anhand dieser Merkmale wird dann der Vergleich von bekanntem Datensatz und dem ermittelten Datensatz vollzogen. Die Extraktionsmethode (Minuzien) wird von der Mehrzahl der Hersteller von Fingerabdruckerkennungssystemen genutzt. In beiden Fällen werden vergleichbare Sicherheitswerte erreicht; die Verifikationszeit kann jedoch beim Pattern Matching etwas länger sein. Bei dieser Methode sind die Templates häufig um den Faktor zwei bis drei größer, z.B. typischerweise etwa 900 bis 1.200 Bytes pro Fingerbild [Behr/Roth01].

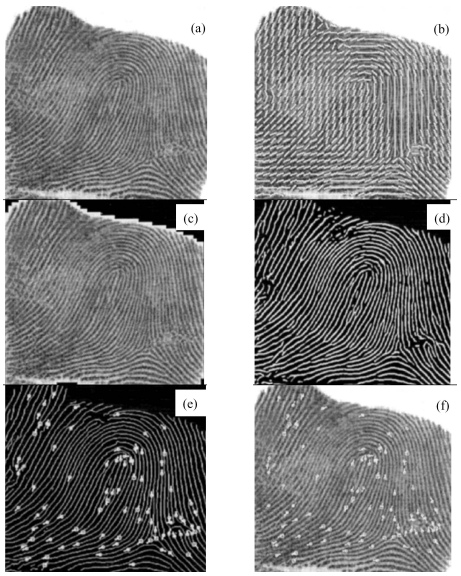


Abbildung 3.4: Gewinnung des Minuzienbildes bei der Fingerbilderkennung [Behr/Roth01]

Hingegen werden bei der kriminaltechnischen (forensischen) Verarbeitung der Fingerabdrücke die Gesamtbilder der Fingerabdrücke zu Vergleichszwecken gespeichert. Das bedeutet, dass die von den Scannern erfassten Bilder als hochwertige Schwarz-Weiß- Bilder mit z.B. 250 KByte (pro Finger!) gespeichert werden, während für die biometrische Identifikation Datensätze verwendet werden, die um den Faktor 250 bis 1.000 kleiner sind und sich auf die zur Unterscheidung benötigten Merkmale reduzieren. Daher kann bei einer biometrischen Identifikation der Fingerabdruck aus den gespeicherten Daten nicht eindeutig rekonstruiert werden, was eine Verwendung vor Gericht kaum möglich macht [Behr/Roth01].

Abbildung 3.4 demonstriert die Gewinnung der biometrischen Fingerbildinformation, des sog. Minuzienbildes. Die einzelnen Schritte sind [Behr/Roth01]:

- Gewinnung des Original-Graustufenbildes des Fingers (a)
- Berechnung des Richtungsfeldes aus dem Originalbild (b)
- Extraktion des Vordergrundanteils (c)
- Herausfilterung des Hintergrundes (d)
- Berechnung des Skelettes mit den markierten Minuzien (e)
- Überlagerung der Minuzien mit dem Original-Graustufenbild (f)

Stand der Technik für die Sensoren zur Merkmalsaufnahme sind drei Technologien: optische Sensoren, Halbleiterlösungen und Ultraschall. Sie sind im Folgenden beschrieben und detailiert erklärt.

### 3.2.1 optische Sensoren

Die Nutzung von optischen Sensoren hat sich in der Vergangenheit zwar bewährt, wird aber nicht oft genutzt. Grundlage dieses Systems ist einer Kamera, zumeist in Form eines CCD-(Charged Coupled Device) Sensors, eine Prismenoptik und eine Hartplastik- oder Glasfläche als Auflagefläche für den Finger in definiertem Kameraabstand. Anstatt von sichtbarem Licht kann auch infrarotes Licht benutzt werden. Die Auflösung des CCD-Chips ist mit bis zu 500 dpi (dot per inch) größer und damit bei einer relativ großen nutzbarer Auflagefläche deutlich besser als die unten genannte Halbleiterlösungen. Die optischen Sensoren sind unempfindlicher gegenüber Temperaturschwankungen und elektrostatischer Aufladung als Halbleiterlösungen. Probleme bereiten allerdings latente Fingerabdrücke aus der vorhergehenden Benutzung. Bei einigen Modellen besteht auch die Gefahr eines Leistungsabfalls infolge der Alterung des CCD-Chips, Ausfall der Beleuchtung oder durch Beschädigung der Oberfläche der Aufnahmefläche.

### 3.2.2 Halbleiterlösungen

Immer mehr in der Vordergrund treten die Halbleiterlösungen (kapazitative Sensoren). Seit einigen Jahren sind Sensoren verfügbar, die mittels Messung der Gleichstromkapazität zwischen der Chipoberfläche und der Fingeroberfläche digitale Graustufenbilder mit 200 bis 300 Linien - bei einer nutzbaren Fläche von ca. 10 x 15 mm bis maximal 13 x 18 mm - mit 8 bit Auflösung erzielen (Infineon, Sony, ST-Microelectronics, Veridicom). Ein System (des Herstellers Authentec) kann durch eine modifizierte Kapazitätsmessung auch die Lederhaut des Fingers unter der Oberfläche vermessen, was theoretisch deutliche Vorteile hat, da sich zum Beispiel Verletzungen weniger auswirken. Mit latenten Fingerabdrücken aus der vorhergehenden Benutzung haben allerdings auch viele der Halbleiterlösungen noch Probleme, und wie haltbar und zuverlässig sie sind, ist noch offen. Die Angaben einiger Hersteller sind viel versprechend, da sie eine um den Faktor 100 bessere Haltbarkeit als die optischen Systemen angeben. Typisch ist eine, durch die relativ kleine Aufnahmefläche bedingte, sehr große Abhängigkeit der Gesamtqualität der Erkennung von der Qualität des Enrolments. Der Benutzer muss immer die gleiche Teilfläche des Fingers wie beim Enrolment benutzen, was

eine unrealistische Disziplin des Nutzers erfordert, der oft schon Schwierigkeiten hat, sich daran zu erinnern, welchen Finger er beim Enrolment benutzt hat. Chips zur Fingerbilderfassung werden zukünftig weitaus preiswerter sein und vermutlich immer häufiger eingesetzt werden. Schon jetzt sind sie in Smartcards integriert verfügbar.

### 3.2.3 Ultraschall

Die Nutzung der Ultraschalltechnologie in Sensoren zur Fingerabdruckerkennung ist sehr zukunftsträchtig. Zurzeit haben aber nur wenige Geräte Marktreife erreicht (http://www.ultra-scan.com). Ein großer Vorteil ist, dass Schmutz oder Rückstände (latente Fingerabdrücke) keine Rolle spielen, da der akustische Widerstand der Haut (Kanten, Senken usw.) gemessen wird, und eine große Aufnahmefläche wie bei optischen Systemen möglich ist. Die Überwindung derartiger Sensoren dürfte schwieriger sein. Über die Langzeitleistungsfähigkeit ist bisher allerdings wenig bekannt.

Eine Lebenderkennung wird bisher noch nicht von allen Herstellern angeboten. Es soll verhindert werden, dass bei optischen Sensoren mit einer Fingerprofilattrappe oder einem abgeschnittenen Finger eine Authentifizierung erzielt werden kann. Ansätze für solch eine Lebenderkennung sind die Messung des Fingerpulses oder die Erfassung der Farbe der Haut, ihrer elektrischen Eigenschaften oder ihrer Reflexionseigenschaften [Behr/Roth01]. Für die Nutzer ist die Fingerbilderkennung recht einfach und bequem handhabbar. Allerdings wird vermutet, dass die Assoziation des "traditionellen" Einsatzes im Rahmen der Strafverfolgung bei Nutzern zu Vorbehalten führen kann. Hinzu kommen hygienische Bedenken bei Verwendung im öffentlichen Bereich.

## 3.3 Gesichtserkennungsmethoden

Für die Gesichtserkennung existieren verschiedene Methoden und Systeme. Die meisten analysieren diejenigen Bereiche des Gesichtes, die sich nicht aufgrund der Mimik ständig verändern. Dazu gehören die oberen Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes. Die zwei wichtigsten Verfahren sind die Eigengesichts- und die Eigenschaftsanalyse.

| | Optische Methode | Kapazitive Methode | Ultraschall-Methode |
|---|---|---|---|
| Verfahren | Finger wird auf beschichtete Oberfläche gelegt CCD-Sensor erzeugt digitales Bild des Abdrucks | misst Kapazitäten zwischen Siliziumsensor und Finger Messung wird in digitales 8-bit Graustufenbild umgewandelt | Ultraschallwellen werden ausgesendet und von der Umgebung unterschiedlich reflektiert verarbeitet Reflektion wird gemessen und zu einem Bild |
| Vorteile | am meisten erprobt vergleichsweise günstig temperaturunempfindlich | gute Qualität geringere Messoberfläche | die exakteste Methode Schmutz-, Narben- und Kratzerunempfindlich |
| Nachteile | Sensoren müssen ausreichend groß sein alte Abdrücke können Ergebnis verfälschen | eventuell zu kleine Sensorflächen | Methode befindet sich noch in der Entwicklung |

Tabelle 3.2: Vergleich der drei Methoden zur Bilderzeugung [Biom02]

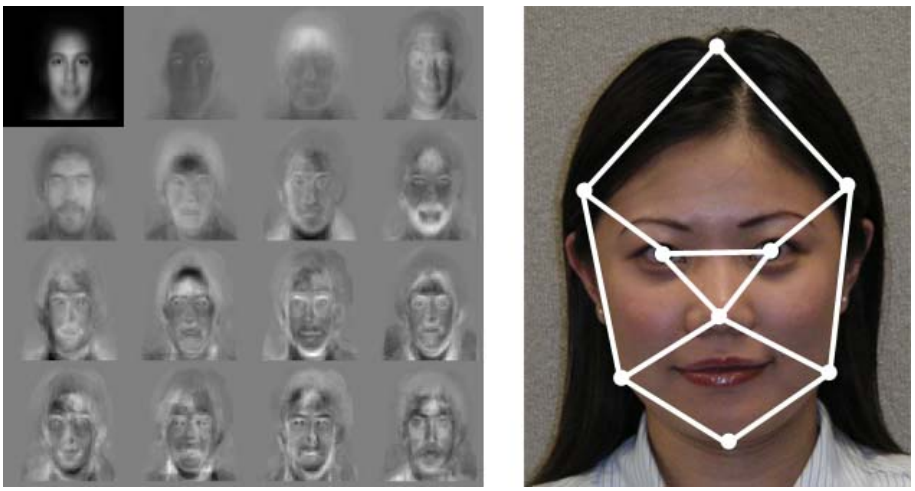

Abbildung 3.5: (a) Einzelbilder der Eigengesichtstechnik [Behr/Roth01] - (b) mit Graphen erkannte Person

### 3.3.1 Eigengesichtsanalyse

Bei der Eigengesichtsanalyse handelt es sich um ein ursprünglich vom Massachusetts Institute of Technology (MIT) entwickeltes Verfahren, das in zweidimensionalen Graustufenbildern die Erkennungsmerkmale des Gesichts abbildet (Abb. 3.5 a). Es sind jedoch 100 bis 125 Eigenbilder bei der Mehrheit der Gesichter nötig, um die jeweils typischen Eigenschaften zu erfassen. Wie bei allen Gesichtserkennungssystemen sind der Betrachtungswinkel und der Detailreichtum wichtig. Die besten Ergebnisse werden bei frontaler Bildaufnahme erzielt. Diese Gesichtserkennungstechnik wird oft in Kombination mit weiteren biometrischen Verfahren benutzt.

### 3.3.2 Eigenschaftsanalyse

Eigenschaftsanalyse (Feature analysis) ist das wohl verbreitetste System zur Gesichtserkennung. Gegenüber dem Eigengesicht-Verfahren gilt die Methode als vielseitiger, da sie Variationen der Mimik, etwa beim Sprechen oder Lächeln, akzeptiert. Die Idee dieses Verfahrens ist es über das Gesichtsbild ein flexibles Gitter zu legen, dessen Knotenpunkte Merkmalsdetektoren zugeordnet sind. Beim Vergleich zweier Gesichter können die Knoten in gewissen Grenzen verschoben werden, damit eine gewisse Übereinstimmung an den korrespondierenden Knoten ermittelten Merkmalen erreicht wird. Der Vergleich wird mit Hilfe der gewichteten Summe aus dem Unterschied der Merkmale an den Knoten und der Verzerrung des Gitters quantifiziert. (Abbildung 3.5 b) Neben diesen beiden dominierenden Systemen gibt es eine Reihe weiterer Varianten, die als Neural Network Mapping Technology oder Automatic Face Processing bezeichnet werden. Ferner gibt es erste Versuche zur Nutzung anderer Parameter, wie dreidimensionales Scannen oder das Erfassen der Wärmeverteilung im Gesicht. Natürliche und äußere Einflüsse, z.B. unterschiedliche Lichtverhältnisse oder Temperaturschwankungen, beeinflussen die Funktionalität der Gesichtserkennung. Ohne Lebenderkennung (z.B. durch Registrierung von minimalen Mund- oder Augenbewegungen) ist die Überwindung der Systeme äußerst einfach - meist genügen bereits Fotos oder Videos. Vor allem bei Kindern und Jugendlichen, aber auch in späteren Lebensphasen verändert sich das Merkmal relativ stark. [Behr/Roth01]

Die Studie BioFace in Auftrag gegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den getesteten Gesichtserkennungsystemen keine gute Noten geben können. Die Tauglichkeit der Gesichtserkennungssysteme als (unterstützende) Identifikationssysteme ist unter den erwähnten Einschränkun-

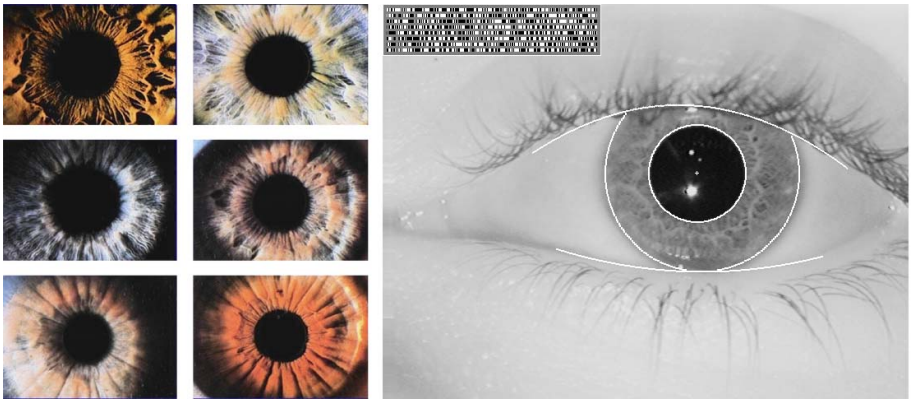

Abbildung 3.6: (a) Variationen der Iris - (b) erkannte Iris mit Iriscode

gen durch BioFace II nicht abschließend beweis- oder widerlegbar. Die Schwächen der Systeme hinsichtlich der Trennung der Matches (Vergleich zweier Bilder einer Person) von den Non-Matches (Vergleich der Bilder zweier unterschiedlicher Personen) können im Identifikationsszenario jedoch weniger kompensiert werden, als im Verifikationsszenario, so dass hier bis zur Einsatztauglichkeit noch Verbesserungen an den Algorithmen vorgenommen werden müssen [Bio01].

### 3.4 Iriserkennung

Die "Regenbogenhaut" oder Iris ist der farbige Gewebering, der die Pupille umschließt. Sie regelt wie eine Blende die Größe der Pupille und damit die Lichtstärke, die auf die Netzhaut trifft. Die charakteristischen, biometrisch nutzbaren Merkmale der Iris werden als Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen und Streifen bezeichnet. Die Farbe wird nicht berücksichtigt. Die Einzigartigkeit von Irismustern ist unbestritten. Sie gilt nicht nur für eineiige Zwillinge, sondern sogar für die zwei Augen einer Person. Veränderungen über die Zeit werden als vernachlässigbar eingestuft. Allerdings können Krankheiten des Auges, z.B. Schädigungen der Hornhaut, zu deutlichen Veränderungen führen, was eine neue Registrierung erforderlich macht [Behr/Roth01].

Zur Aufnahme der Irismuster werden Schwarz-Weiß-CCD-Kameras eingesetzt. Laser finden keine Verwendung. Eine Art der Aufnahme ist die, dass der Nutzer sich 15 - 35 cm vor der Kamera positioniert und eventuelle Positionskorrekturen - gegebenenfalls geleitet vom System - selbst vollführt. Bei der "aktiven" Aufnahme findet eine motorisch bewegte Weitwinkel-Kamera mit Hilfe von Stereoaufnahmen des Gesichtes selbstständig die Iris.

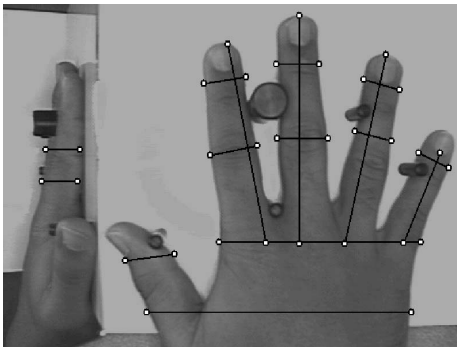

Abbildung 3.7: Handgeometrieverfahren

Das zu Grunde liegende Erkennungsprinzip beruht auf dem negativen Ergebnis eines statistischen Prüfung auf Unabhängigkeit der durch mehrfach skalierte Wellenpakete kodierten Musterphasenstruktur der Iris. Die Vielfalt der Phaseninformationen der Wellenpakete bei verschiedene Personen beträgt etwa 244 Freiheitsgrade und damit einer Informationsdichte von 3,2 $\frac{bit}{mm^2}$ der Irisfläche. Dies ermöglicht eine Echtzeitentscheidung zur Personenidentifikation mit extrem hoher Zuverlässigkeit. [Roth01]

Es wird bereits vielfach bei Zugangskontrollen im Hochsicherheitsbereich verwendet, mehrere Pilotanwendungen bei Geldautomaten und der Passkontrolle am Frankfurter Flughafen sind bekannt. Eine Lebenderkennung (z.B. durch Erfassung der Pupillenbewegung und der damit einhergehenden kontinuierlichen elastischen Verformung der Irisstruktur) kann die ohnehin hohe Überwindungssicherheit noch weiter steigern . Einem verbreiteten Einsatz stehen derzeit noch die hohen Anschaffungskosten entgegen, die allerdings bei einer Steigerung der Produktion wohl deutlich gesenkt werden könnten. Die Nutzerakzeptanz gilt als eher verhalten, da häufig die Befürchtung von Augenschäden geäußert wird. Der Grund ist die falsche aber nach wie vor verbreitete Annahme, dass ein Laser eingesetzt zur Vermessung der Iris werde [Pet/Sau02].

## 3.5 Handgeometrieverfahren

Die Erfassung der Handgeometrie ist eines der ältesten biometrischen Verfahren. Ab einem Alter von etwa 20 Jahren sind die Veränderungen an der menschlichen Hand meist nur noch gering. Bereits der Schatten einer Hand gilt als einzigartig. Für die biometrische Vermessung werden bis zu 90 Werte für Dicke, Länge, Breite und Fläche der Hand bzw. der Finger ermittelt. Theoretisch nutzbare Charakte-

ristiken der Handoberfläche, wie die Verteilung der Hautporen, werden bislang nicht herangezogen [Pet/Sau02].

Authentisierung über Handgeometrie findet heute hauptsächlich zur Arbeitszeitmessung oder als Zugangskontrolle zu Räumen oder Gebäuden Anwendung. So wird sie in etwa 50% der amerikanischen Kernkraftwerke und zur Einreisekontrolle in die USA genutzt [Mai02].

Die relevanten biometrischen Merkmale, die zu Erkennung der Nutzer benötigt werden sind u.a.: Längen und Breiten der einzelnen Finger, Dicke der Hand und der Finger und die Krümmung der einzelnen Finger in Bezug auf ihren Mittelpunkt.

Die Bedienung der Systeme ist einfach, teilweise aber unbequem (wenn z.B. für die richtige Positionierung die Hand fest an starre Anschlagstifte gedrückt werden muss, siehe Abbildung 3.7). Ein Nachteil ist sicherlich, dass der Sensor nicht berührungsfrei ist und dadurch einige Menschen das System aus Hygienegründen ablehnen. Da aufgrund der Dickenmessung dreidimensionale Aufnahmen benötigt werden, sind komplizierte Optiken erforderlich. Die Sensortechnik und mit ihr das Gesamtsystem fällt daher recht voluminös aus. Die Templategröße ist mit 10-20 Bytes klein, Angaben zur erzielbaren Genauigkeit schwanken. Eine Lebenderkennung der Hand des Nutzers zur Erhöhung der Überwindungssicherheit des biometrischen Systemes wird bislang kaum angeboten [Pet/Sau02].

Aufgrund der geringen relevanten Anzahl der biometrischen Merkmale ist die Anwendung des Handgeometrieverfahrens zur Nutzeridentifikation bei größeren Benutzergruppen nicht empfehlenswert. Der Einsatz des Verfahrens zu Nutzerverifikation ist eingeschränkt empfehlbar.

## 3.6 Sprechererkennung

Es existieren verschiedene Methoden bzw. Verfahren zur Analyse von personenbezogenen Sprachmustern. Erfasst werden unterschiedliche Parameter der Sprechcharakteristik, so die Tonhöhe, die Dynamik oder die Wellenform. Die Templategröße liegt in der Regel zwischen 1.500 - 3.000 Bytes [Behr/Roth01]. Grundsätzlich ist die Sprechererkennung, verglichen mit anderen biometrischen Verfahren, ein weniger genaues Verfahren. Sprachsysteme sind anfällig für äußere Einwirkungen, z.B. Straßengeräusche oder laute Unterhaltungen, und bei (Hals-)Erkrankungen häufig nicht einsetzbar. Hinzu kommt die prinzipiell simple Überwindbarkeit durch Stimmaufnahmen [Ditt01]. Trotz dieser Nachteile ergibt sich insbesondere im Bereich der Telekommunikation ein interessantes Anwendungsspektrum, da hier kei-

ne zusätzlichen Hardwarekosten für die Nutzer entstehen.

Nach dem Enrolment ist eine Sprecherverifikation oder Sprecheridentifikation möglich, wobei grundsätzlicher Weise gilt, dass eine Erkennung umso schwieriger wird, je mehr Muster gleichzeitig erkannt werden sollen. Daher sollte bei der Sprechererkennung überwiegend die Sprecherverifikation verwendet werden. Eine weitergehende Unterscheidung trifft man zwischen textabhängigen und textunabhängigen Sprechererkennungsverfahren: Bei den textabhängigen Systemen findet die Erkennung mittels eines bestimmten gesprochenen Textes oder Wortes (einem Schlüsselwort) statt, bei textunabhängigen wird der Sprecher anhand beliebiger Worte authentisiert. In Bezug auf Erkennungsraten (FAR/FRR) ist die Vorgabe eines Schlüsselwortes am besten geeignet. Durch eine Vorgabe des Schlüsselwortes aus einer Schlüsselwortliste lässt sich vermeiden, dass für die Erkennung ungeeignete Wörter gewählt werden. Des Weiteren sind textabhängige Systeme einfacher zu implementieren und leichter "trainierbar". Nachteilig ist, dass mit dem Wissen des Schlüsselwortes Überwindungsversuche unberechtigter Nutzer erleichtert werden.

Bei textunabhängigen Systemen sind komplexere Verfahren notwendig, die z.B. in Diktiersystemen auf PC-Basis Anwendung finden. Dazu werden so genannte Hidden-Markov-Modelle (HMM) von Wortsegmenten (Phonemen) verwendet. Text-unabhängige Sprechererkennungen haben den Nachteil, dass ihr Training langwieriger und komplexer ist und die Erkennungssicherheit auch von der Länge der Sprechzeit bei der Überprüfung abhängt [Behr/Roth01].

## 3.7 Andere Verfahren

### 3.7.1 Retina Scan

Ähnlich dem Irismuster gilt auch das Blutgefäßegeflecht in bzw. hinter der Netzhaut oder Retina, dem lichtempfindlichen Bereich im Augeninneren, als individuell einzigartig (auch bei Zwillingen). Die Anordnung der Blutgefäße der Netzhaut bleibt, wie das Irismuster, weitgehend konstant, es kann sich aber durch Krankheiten oder Verletzungen vorübergehend oder andauernd verändern. Mittels eines Infrarot-Lasers wird die Retina gescannt, wobei ca. 400 Merkmale festgehalten werden. Der Abstand des Auges zur Aufnahmeoptik muss etwa 1-2 cm betragen und es muss während des Aufnahme ruhig gehalten werden. Die Templategröße beträgt 40-96 Byte. Die Zeit für die Messung ca. 1,5 Sekunden. Wie die Iriserkennung hat der Retina-Scan als sehr empfindliches Verfahren bei der Zu-

trittssicherung zu Hochsicherheitseinrichtungen sowohl im öffentlichen als auch im privaten Bereich Verbreitung gefunden. Eine Überlistung des Systems durch Attrappen wird kaum für möglich gehalten. Nicht nur der hohe Preis, sondern auch die bislang recht hohe Rückweisungsrate (von ca. 12 % beim ersten Versuch laut Herstellerangabe) stellen ein Verbreitungshemmnis dar. Hinzu kommen Nutzervorbehalte, da eine Verursachung von Augenschäden durch den Laser befürchtet wird, auch wenn es hierfür bislang keinerlei Hinweise gibt. Konkrete Einschränkungen der Nutzbarkeit ergeben sich für Träger von Kontaktlinsen (ab einer bestimmten Dioptrienzahl), außerdem gibt es Probleme bei Astigmatismus (Hornhautverkrümmung, eine recht häufige Ursache für Fehlsichtigkeit) [Pet/Sau02].

### 3.7.2 Unterschriftenerkennung

Bei der Unterschrifts- bzw. Handschriftenerkennung ist nicht nur das optische Erscheinungsbild der Signatur (Schriftzug als "Offline-Parameter") entscheidend, sondern es werden Merkmale wie Druck, Geschwindigkeit, Beschleunigung, Auf- und Absetzpunkte sowie Stiftwinkelpositionen beim Schreiben (als "Online-Parameter") gemessen. Aufgenommen wird die Unter/Handschrift heute meistens mit einem handelsüblichen Grafiktablett oder einem PDA bzw. Touchscreen. Alternativ sind auch Spezialstifte mit Sensoren in Verwendung, welche die Parameter bei der Leistung der Unterschrift/Handschrift aufnehmen und zur Auswertung übertragen [Behr/Roth01]. Eine Erweiterung der Unterschriftanalyse liefert ein Handschriftensystem, bei welchem nicht allein die Unterschrift, sondern sog. "Semantiken" [Viel02] zur handschriftlichen Authentifizierung herangezogen werden. Dies können vordefinierte Wörter, ganze Sätze oder sogar kleine Zeichnungen (Sketches) sein. Da die Erfassung der dynamischen Parameter eine Lebenderkennung darstellt, ist die Fälschungssicherheit ziemlich hoch. Wegen der (noch) hohen Fehlerraten sind die Systeme bislang allerdings nur sehr eingeschränkt einsetzbar [Ditt01].

### 3.7.3 Messung der Tastaturanschlagdynamik

Das Verfahren der Messung des Tastaturanschlags oder Tippverhaltens ist eine relativ neue Methode und wenig verbreitet. Sie basiert auf der Idee, dass bestimmte Verhaltensweisen beim Schreiben auf einer Tastatur typisch für eine Person sind. Dabei wird beispielsweise die Anschlagdauer und der zeitliche Abstand zwischen den Tastenanschlägen gemessen. Mögliche Einsatzfelder sind Zugangskontrollen

zu Rechnernetzen bzw. Laufwerken, Dateien und Programmen, Electronic Banking, Teleworking und Fernwartung. Die Authentisierung kann dabei unaufdringlich im Hintergrund ablaufen. Problematisch bei diesem Verfahren ist, dass kurze Texte meistens nicht ausreichen, um eine gesicherte Erkennung durchzuführen und dass das Tippverhalten häufig von der verwendeten Tastatur oder der Tagesform abhängt. Gerade bei Handverletzungen kann es zu starken Abweichungen kommen. Ungeübte Schreiber haben meistens noch kein individuelles Tipp-Profil entwickelt und können daher nicht eindeutig identifiziert werden. Ganz abgesehen von den technischen Problemen, ermöglicht die Tastaturüberwachung Kontrolle und Spionage [Wett02].

## 3.8 Schnittstellen und Standards

Das enorme Wachstum auf dem Markt für Sicherheit hat besonders einen Boom für biometrischen Systeme und Applikationen zur Folge. Um Kompatibilität und Datenaustausch zwischen biometrischen Systeme und Komponenten zu gewährleisten, mussten Standards und Schnittstellen geschaffen werden. Die Spezifikation von Standards erhöht auch die Investitionssicherheit der einzelnen Hersteller, denn die Entwicklung proprietärer Standards ist teuer und niemand weiß, ob sich später dieser Standard auf dem Markt durchsetzt oder der Standard der Konkurrenz. In diesem Abschnitt wird auf den Standard BioAPI und das Austauschformat CBEFF eingegangen.

### 3.8.1 biometrisches Datenaustauschformat - CBEFF

Das Common Biometic Exchange File Format (CBEFF) spezifiziert die Struktur eines biometrischen Datensatzes, welcher für alle biometrischen Verfahren eingesetzt werden kann, um einen Datenaustausch zwischen biometrischen Komponenten oder Systemen verschiedener Hersteller zu gewährleisten. Es werden die Werte für die einzelnen Felder des Datensatzes definiert. Die eigentlichen biometrischen Daten werden nicht be- oder verarbeitet sondern in das Format eingebettet.

CBEFF beinhaltet einen Satz von verschiedene Feldern, die zum einen "required" und zum anderen "optional" sind. Dieser Datensatz kann als eine Datei behandelt werden. Die Nutzung des Datensatzes als Datenobjekt, welches eine Datenaustausch zwischen den Systemkomponenten vornimmt, ist auch möglich. Dieses Datenformat erlaubt den Applikationen, wie Datenbanken oder Verarbeitungsalgorithmen schnell wichtige Prozessinformationen über die biometrischen


Abbildung 3.8: CBEFF-Datenformat

Daten, wie z.B. welche Art der verwendeten Biometrie, Versionsnummer, Herstellername des Sensors usw..

Die grundlegenden Bestandteile des CBEFF sind in (Abb. 3.8) aufgeführt und werden im Folgenden näher erläutert:

- SBH - Standard Biometic Header - biometrischer Header, welcher Informationen über Versionsnummer, Datenfeldlänge usw. enthält
- BSMB - Biometric Specific Memory Block - biometrische Daten (Inhalt des Feldes nicht spezifiziert)
- SB  Signature Block - Signatur über SBH und BSMB (optional)

Die in Tabelle 3.3 dargestellten Datenfelder sind die Komponenten des CBEFF Datenrecords. Die angegebenen Zahlenwerte sind in hexadezimaler Schreibweise.

In CBEFF ist eine Beschreibung von biometrischen Datenelementen standardisiert. Es ist wichtig für Applikationen, die erhaltenen biometrische Daten weiterverarbeiten sollen, was für Daten sie erhalten haben und inwieweit sie diesen Daten vertrauen können. Denn beispielsweise hat der Code, der aus einem Irisbild extrahiert, wird hat eine höhere Verwechslungssicherheit als der einer Handgeometrievermessung.

### 3.8.2 biometrischer Standard BioAPI 1.1

Im Jahre 1997 finanzierte sie National Security Agency (NSA) die Entwicklung eines Human Interface API (HA-API), welche im Dezember 1997 zur Verbesserung der Sicherheit innerhalb von Regierungsbehörden veröffentlicht wurde. Im April 1998 wurde die zweite Version dieses Interfaces verabschiedet. Ein im Jahre 1998 unabhängig vom HA-API entwickelter Standard war Biometric API (BA-PI). Dieser Standard wurde vom japanischen Hersteller I/O Software entwickelt. Compaq kündigte im April 1998 die Gründung eines BioAPI Konsortiums an, das einen API-Standard für biometrische Anwendungen entwickeln sollte, um die Entstehung weiterer kleiner proprietärer APIs zu verhindern. Zunächst befasste man

| Nr. | Feldname | Required oder Optional | Bemerkungen |
|---|---|---|---|
| 1 | SBH Security Options | Required | 0x00 = nur Biometrik<br>0x10 = with Privacy (verschlüsselt)<br>0x20 = mit Integrität (signiert or MACed)<br>0x30 = mit Privacy und Integrität |
| 2 | Integrity Options | Optional | 0x01 = MACed<br>0x02 = signiert nur bei Nutzung von Integrität (z.B. SBH Optionen=0x20 or 0x30) |
| 3 | CBEFF Header Version | Optional | Version des CBEFF Headers. entweder: Major: 0x01 oder Minor: 0x00 |
| 4 | Patron Header Version | Required | Version des Headers (Patron Format Spezifikation oder Standard) |
| 5 | Biometric Type | Optional | Bezeichnung der Biometrik. |
| 6 | Record Data Type | Optional | Bezeichnung des Record Datentyps. gegenwärtig 0x02 Feld erscheint nicht wenn default genutzt wird. |
| 7 | Record Purpose | Optional | Bestimmungzweck der Daten. gegenwärtig 0x04 (nur Enrolment für Verifikation, default). Feld erscheint nicht wenn default genutzt wird. |
| 8 | Record Data Quality | Optional | Angabe über Qualität der biometrischen Daten |
| 9 | Creation Date | Optional | Erstellungszeit und -datum der Biometrischen Daten |
| 10 | Creator | Optional | ID des biometrischen Sensors |
| 11 | BSMB Format Owner | Required | Hersteller-ID welche den BSMB definiert |
| 12 | BSMB Format Type | Required | festgelgter Typ des Format Owners |
| 13 | Biometric Specific Memory Block (BSMB) | Required | definiert vom Format Owner |
| 14 | Signature | Optional | Signature of MAC; nur existent wenn SBH Wert 0x20 oder 0x30 ist. |

Tabelle 3.3: Übersicht der Optionen des Standard Biometric Header

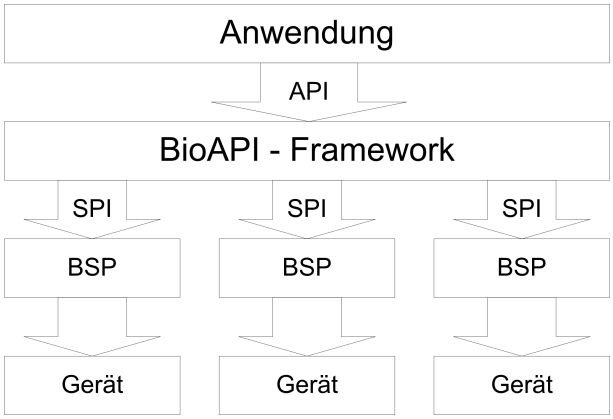


Abbildung 3.9: Einordnung des BioAPI in ein biometrisches System

sich mit der Forschung von IBM UK, ehe im März 1999, die eigene Arbeit, der HA-API und der BAPI zusammengebracht wurden und die BioAPI spezifiziert wurde. Zurzeit gehören dem BioAPI Konsortium, das im März 2001 die aktuelle Version 1.1 des BioAPI veröffentlichte, 134 Firmen bzw. Organisationen an.

Das Ziel der BioAPI-Schnittstelle ist es ein allgemeines biometrisches Authentifikationsmodell bereitzustellen. Die gewählte biometrische Technologie spielt dabei keine Rolle.

Die Grundprozeduren Enrolment, Verifikation, Identifikation und Schnittstellen zu Datenbanken, welche biometrischen Serviceprovidern (BSP) ein optimales Management der Benutzer des Systems erleichtern, sind auch in der Spezifikation von BioAPI enthalten.

BioAPI stellt aber auch Primitiven bereit, welche Anwendungen erlaubt die Erfassung der biometrischen Daten auf einem Client durchzuführen. Das anschließenden Enrolment, die Verifikation oder Identifikation kann dann zentral auf einem Server vollführt werden.

BioAPI umfasst aber keine Sicherheitsfunktionen für biometrische Anwendungen oder BSP. Er werden aber Hinweise gegeben, wie die BioAPI in Sicherheitsfunktionen eingebunden werden kann.

In der Spezifikation werden 2 Schnittstellen definiert. (Abb. 3.9) Eine API, die Applikationen höherer Abstraktionsstufen nutzen können und eine Service Provider Interface (SPI) für die verschiedene biometrischen Verfahren.

Für die API sind im Standard grundlegende Funktionen und Prozeduren implementiert, die eine Anwendung nutzen muss, um biometrische Daten zu verarbeiten. Auf Funktionalitäten, die über die grundlegenden Funktionen hinausgehen

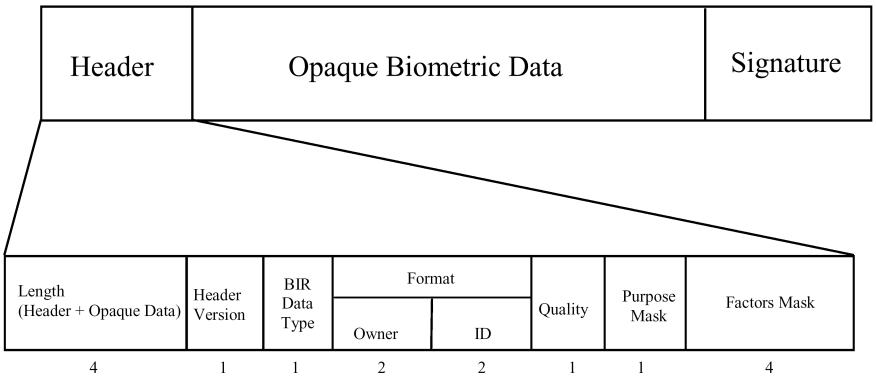


Abbildung 3.10: BioAPI IR

wurde weitgehend verzichtet.

Das Hauptziel in der Entwicklung des Standards war es für die vielen verschiedenen biometrischen Technologien und Hersteller eine Abstraktion auf hohen Niveau zu schaffen, um die Softwareentwicklung zu vereinfachen und zu beschleunigen.

Neben den Grundfunktionen ist auch ein biometrischer Datencontainer definiert. (Abb. 3.10) Der schon beschreibende CBEFF-Standard wurde komplett übernommen.

# Kapitel 4

# ZUGANGSTECHNOLOGIEN

Die Nutzung von Credentails setzt eine gewisse Basisisicherheit der zu Grunde liegenden Zugangstechnologie voraus. Diese zu berücksichtigenden Sicheheitskriterien sind:

- Vertraulichkeit
- Integrität
- Authenzität
- Zugriffskontrolle/Autorisierung
- Anonymisierung

Die Zugangtechnologien IrDA, Bluetooth, IEEE 802.11, HiperLAN/2, GSM und UMTS werden im Folgenden vorgestellt, ihrer Sicherheitsimplentationen näher erläutert und nach den Sicherheitskriterien untersucht.

## 4.1 IrDA

### 4.1.1 Einführung

Infrarotes Licht als Informationsträger wurde 1979 erstmals von der Firma Hewlett Packard eingesetzt um einen Taschenrechner mit einem Drucker zu verbinden. Viele Produkte, auch andreren Hersteller, folgten, allerdings wurden von den verschiedenen Herstellern proprietäre, zueinander nicht kompatible Protokolle zur Infrarotkommunikation eingesetzt. Die daraus folgenden Nachteile konnten 1993 mit der Gründung der Infrared Data Assoziation (IrDA) minimiert werden. Die 30 Begründer der IrDA erarbeiteten alle gängigen Standards der Infrarotkommunikation. Der erste Standard IrDA 1.0 auch SIR (Serial Infrared) genannt wurde im Jahre 1994 verabschiedet. Die maximale Datenrate von 115,2 kbit/s dieses Standards reichte nicht aus, so dass im Jahre 1995 die Erweiterung des SIR-Standards IrDA 1.1, auch FIR (Fast Infrared) (4 mbit/s) erfolgte. 1999 wurde

der Standard VFIR (Very Fast Infrared) spezifiziert mit dem eine Datenübertragung von bis zu 16 mbit/s möglich ist. Heutzutage ist das IrDA-Protokoll in alle gängigen Betriebsysteme für Desktop-PCs integriert. Auch bei Mobiltelefonen und Handheld-Rechner findet IrDA Einsatz, da es eine relativ einfache und Strom sparende Kommunikationstechnologie ist.

### 4.1.2 Eigenschaften

Die Spezifikation von IrDA enthält den Teilstandard IrDA CONTROL und IrDA DATA. Ersterer ist für die Kommunikation mit Peripheriegeräten, wie z.B. drahtlosen Mäusen, Tastaturen oder Joysticks konzipiert. Die Datenrate beträgt 75 kbit/s, bei einem maximalen Abstand vom 5 m.

IrDA DATA ist für Kommunikationsprozesse, die einen hochbitratigen Datenaustausch fordern, gedacht. Wenn allgemein von IrDA geredet wird, ist meist dieser Teilstandard gemeint. Die Eigenschaften von IrDA DATA sind im Folgenden aufgelistet:

- Datenrate maximal 16 mbit/s
- maximal Entfernung zweier Kommunikationspartner: 1 m
- Suchfunktion nach Kommunikationspartnern/-diensten in Reichweite
- automatisches Aushandeln von Übertragungsparametern
- mehrere logische Kanäle
- Broadcast möglich
- Flusskontrolle und Segmentierung
- Emulation von serieller und paralleler Schnittstelle möglich
- Protokoll zur Netzwerkanbindung verfügbar

Die Kommunikation mittels infrarotem Licht unterscheidet sich in einigen wichtigen Punkten von der Kommunikation mittels Funk, obwohl Infrarotkommunikation auch eine drahtlose Technik ist. Das infrarote Licht ist zwar wie die Funkwellen für den Menschen nicht sichtbar, unterliegt aber den Gesetzen der Strahlenoptik und kann massive Gegenstände nicht durchdringen. Das hat negative Konsequenzen für die Reichweite eines Infrarotsenders, aber auch Vorteil in

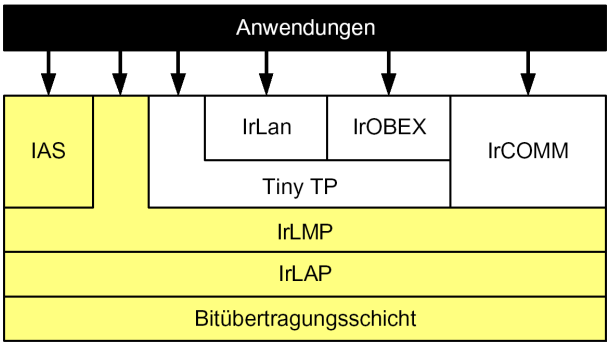


Abbildung 4.1: Der IrDA-Protokollstapel [Roth02]

Hinsicht auf Abhörsicherheit der Kommunikation. Es ist zwar möglich mit passiven Infrarotempfängern den Datenverkehr mitzuhören, aber dazu muss sich der Mithörer in unmittelbarer Sichtweite befinden. Fremdlicht (Sonnenlicht, Kunstlicht) kann die Kommunikation stören. Jedoch stellen elektromagnetische Störungen, wie sie durch elektrische Maschinen, Stromversorgungen oder Funksender entstehen keine Probleme dar. Die Infrarotkommuniktion unterliegt keinen hoheitlichen Beschränkungen durch die RegTP (Regulierungsbehörde für Telekommunikation und Post), wie es bei der Vergabe der UMTS-Frequenzen der Fall war. Dies alles macht die Art der Kommunikation für PAN (Personal Area Network) interessant. Die Kosten für optoelektrische Bauelemente für ein Mobiltelefon oder einen Handheld-Rechner belaufen sich nur auf wenige Euro, so dass dies Art der Kommunikation für den breiten Massenmarkt sehr interessant ist. [Roth02]

### 4.1.3 IrDA Protokollstapel

Einige Teilprotokolle des IrDA-Protokollstapels (Abb. 4.1) sind für eine konkrete Realisierung obligatorisch (grau), andere optional (weiß). Die obligatorischen Teile sind:

- Bitübertragungsschicht: Der entsprechende Standard (SIR,FIR,VFIR) bestimmt die Darstellung der Bits, Übertragungsgeschwindigkeit und optische Charakteristika
- IrLAP (Infrared Link Access Protokoll): Bereitstellung zuverlässiger Übertragung von Daten zwischen 2 Geräten
- IrLMP (Infrared Link Management Protokoll):Da IrLAP nur eine physische Verbindung sichert, stellt IrLMP mehrere logische Kanäle zu Verfügung

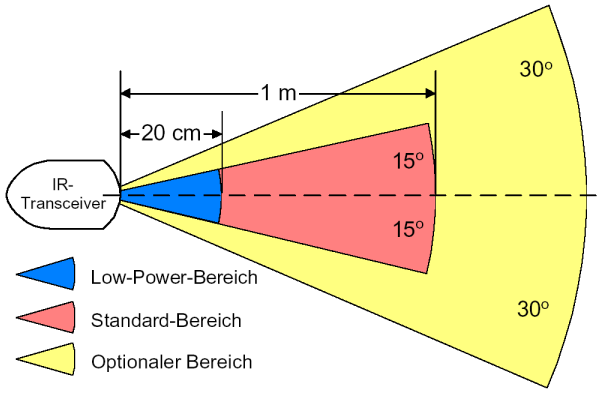


Abbildung 4.2: minimaler und optionaler Abdeckungsbereich [Roth02]

- IAS (Information Access Service): Bereitstellen einer Rechtsauskunft der Kommunikationspartner

Die Realisierung der folgenden Protokolle ist optional:

- TinyTP (Tiny Transport Protokoll): Flusskontrolle auf Basis der logischen IrLMP-Kanäle. Segmentieren/Reassemblieren der zu übertragenden größeren Datenmengen (bis zu 64 KByte)
- IrCOMM: Emulation der seriellen oder parallelen Schnittstelle
- IrOBEX (Infrared Object Exchange Protocol): Austausch komplexer Objekte z.B. Visitenkarte, formatierte Texte oder Grafiken
- IrLAN (Infrared Local Area Network) Anbindung an existierendes lokales Netzwerk

Zur Kommunikation zweier Geräte via Infrarot müssen beide Geräte in der jeweiligen Kommunikationsreichweite des Partners liegen. (Abb. 4.2) Laut IrDA muss dies mindestens der Sendekegel sein, der sich 15° um die optische Achse ergibt, maximal 30°. Dabei muss der Abstand mindesten 1 m sein. Damit mobile Geräte nicht zu viel Energie zur Kommunikation verbrauchen, gibt es eine Low-Power-Option. Hier ist die maximale Reichweite auf 20 cm begrenzt und die Datenrate auf 115,2 kbit/s beschränkt. [Roth02]

### 4.1.4 Sicherheitsmechanismen

Im IrDA-Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs spezifiziert. Es findet lediglich eine Integritätssicherung auf der

IrLAP-Protokollebene gegen Übertragungsfehler mittels CRC statt. Sicherheitsmechanismen wie Authentisierung, kryptographischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Diese müssen ggf. in höheren Ebenen implementiert werden. Im gewissem Rahmen wird die Übertragung durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und die benötigte Sichtverbindung geschützt. [BSI03]

### 4.1.5 Sicherheitsmaßnahmen

Beim Betrieb von Geräten mit IrDA-Schnittstelle ist darauf zu achten, dass diese nur im Bedarfsfall aktiviert wird: Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. So nimmt beispielsweise ein Mobiltelefon mit aktivierter IrDA-Schnittstelle SMS-Mitteilungen zum Versand an. An einen PDA oder Laptop können auch Programme über IrDA geschickt werden, die ggf. Schadfunktionen enthalten können. Außerdem belastet eine eingeschaltete IrDA-Schnittstelle die Batterie bzw. den Akku des mobilen Gerätes zusätzlich. [BSI03]

### 4.1.6 Fazit

Im IrDA-Standard wurden keine Sicherheitsmaßnahmen bezüglich Datenverschlüsselung, Authentifikation, Integritätsschutz und Anonymisierung der Kommunikation implementiert. Da die Kommunikationsreichweite laut Standard nur 1 Meter beträgt und die Ausbreitung der ausgesendeten Strahlung kontrolliert ist, kann davon ausgegangen werden, dass ein Mithören der Kommunikation nur sehr schwer möglich ist. Um dieses Risiko zu verringern sollten aber auf höherer Ebene Authentisierungsmechanismen implementiert werde.

## 4.2 Bluetooth

### 4.2.1 Einführung

Die Firma Ericsson machte im Jahre 1994 einen Entwurf für eine neue Kommunikationstechnologie. Sie sollte die Kabelverbindungen im Nahbereich, wie die z.B. zum Betrieb von Headsets an Mobiltelefonen obsolet machen. Eine Grundprämisse in der Entwicklung des Standards war es, dass nicht unbedingt eine Sichtverbindung, wie es bei Infrarotkommunikation nötig ist vorhanden sein muss. Deshalb entschied man sich für eine Kommunikation via Funk. Wie bei der Entwicklung der IrDA-Standards erkannte der Initiator der Technologie, dass ein proprietäres

Verfahren für die Verbreitung der Technologie hinderlich ist. 1998 schlossen sich die Firmen Ericsson, Nokia, IBM, Intel und Toshiba zur Bluetooth Special Interest Group (Bluetooth SIG) zusammen.

Die Kommunikation findet im ISM-Band (Industrial Scientific and Medical - Band) statt. Für diesen Frequenzbereich von 2400 - 2500 MHz müssen keine Gebühren an die RegTP abgeführt werden.

Der Standard eignet sich für viele verschiedene Einsatzszenarien:

- Das 3 in 1 Telefon: (GSM, Schnurlos- und Bluetoothtelefon) Bluetooth integriert in ein GSM-Telefon würde es ermöglichen mit einem anderen 3 in 1 Telefon via Bluetooth zu kommunizieren. Auch die Kommunikation mit einer Bluetooth-fähigen Basisstation, die Anrufe in das/vom Festnetz vermittelt wäre möglich (DECT-Ersatz). Die normale Kommunikation mittels GSM wäre die dritte Möglichkeit der Kommunikation.

- Drahtloser Zugang ins Internet: Mittels Bluetooth ist es möglich von einem Handheld-Rechner zu einem Mobiltelefon, was dann mittels GSM-Netz ins Internet routet oder zu einem PC zu kommunizieren, der an das Internet routet.

- Datensynchronisation mit einem PC: Um Daten für die Reise mitzunehmen oder zwischen Arbeitplätzen mittels Handheld-Rechner oder Laptop zu transportieren, kann zwischen den Geräten mittels Bluetooth synchronisiert werden.

- Drahtloses Headset: Drahtloses Verbinden eines Headset mit einem Telefon. (nur Audiodatenübertragung)

- Drahtlose interaktive Konferenz: Mehrere Bluetooth-fähige Geräte können, unabhängig von einer Basisstation Daten untereinander austauschen, Visitenkarten versendet, oder Termine austauschen.

### 4.2.2 Eigenschaften

Bluetooth besitzt die folgenden Eigenschaften:

- maximale Datenrate 1 mbit/s (768 kbit/s netto)

- maximale Reichweite 100m

- Automatisches Verbinden der Geräte, die in Reichweite sind

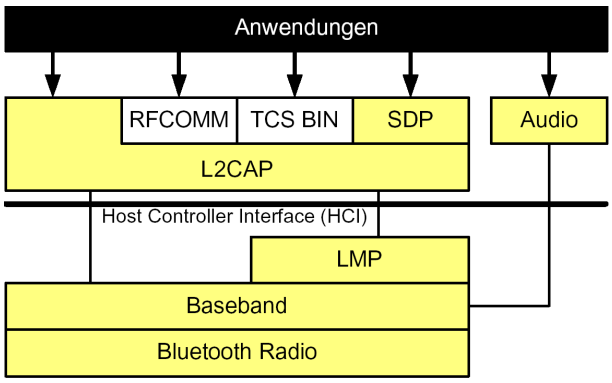


Abbildung 4.3: Bluetooth-Protokollstapel [Roth02]

- Suche nach Geräten und installierten Diensten
- mehrere zuverlässige logische Kanäle zwischen Geräten
- Broadcast zu mehreren Geräten möglich
- Bandbreitenreservierung für Audiokanäle
- QoS-Unterstützung
- Transportprotokoll mit Flusskontrolle und Segmentierung
- Emulation serieller Schnittstellen
- Dienste zur Authentifizierung und Verschlüsselung

### 4.2.3 Bluetooth-Protokollstapel

Der Bluetooth-Protokollstapel (Abb. 4.3) besteht aus folgenden Teilen:

- Bluetooth Radio und Baseband: Bereitstellen des Zugriffs der höheren Layer auf das Funkmedium.
- LMP (Link Management Protocol) Kapselung von Funktionen der Verbindungsverwaltung, QoS, Authentifikation und Verschlüsselung
- L2CAP (Logical Link Control an Adaptation Protocol) mehrere logische Kanäle und Segmentierung, QoS
- HCI (Host Controller Interface) keine Protokollschicht, sondern Kommandoschnittstelle für höhere Schichten

- SDP (Service Discovery Protocol) Dienstsuche bei Kommunikationspartnern
- RFCOMM Emulation serieller Schnittstellen
- TCS BIN (Telephony Control Protocol Binary) Funktionen zu Anrufkontrolle (für Telefone)

Die Audiodaten werden gesondert über das Baseband übertragen, sie werden nicht wie die Anwendungsdaten behandelt [Roth02].

Die Kommunikation mehrerer Bluetooth-Geräte, die sich in Reichweite befinden, kann ohne eine zentrale Administration von statten gehen. Dabei nennt man ein Netzwerk, das aus 2-8 Geräten bestehen kann, Piconet. In diesem Netz gibt es ein Gerät, den so genannten Master, der den Zugriff der Geräte auf die Funkschnittstelle regelt. Alle weiteren heißen Slave, eine Kommunikation zwischen den Slaves ist nur über den Master möglich. Es besteht auch die Möglichkeit, dass ein Slave zu verschiedene Piconets gehört, dieser Slave kann auch für das anderer Piconet den Master darstellen. Diese Netze nennt man auch Scatternet [Roth02].

Die Funkschnittstelle umfasst in der neusten Spezifikation (1.2) drei verschiedene Klassen von Geräten bezogen auf die maximale Sendeleistung und damit auf die Reichweite:

| | | | | | |
|---|---|---|---|---|---|
| Klasse 1 | : | 100,0 mW | - | 100 | m |
| Klasse 2 | : | 2,5 mW | - | 20 | m |
| Klasse 3 | : | 0,1 mW | - | 10 | m |

Zur Übertragung wird das ISM-Frequenzband um 2,4 GHz genutzt, welches in 79 Kanäle aufgeteilt wurde. In Frankreich, Spanien und Japan ist der Frequenzbereich auf nur 23 Kanäle begrenzt, ansonsten steht Bluetooth ein Bereich von 2400 bis 2483,5 MHz zu Verfügung.

Da das ISM-Band noch von vielen anderen Systemen, wie z.B. WLAN oder Babyfonen genutzt wird, ist es nicht ausgeschlossen, dass die Übertragung auf einer bestimmten Frequenz gestört wird. Deshalb wendet man bei Bluetooth-Verbindungen einen sehr schnellen Wechsel zwischen den 79 (23) Kanälen an. (Fast Frequency Hopping) Alle 625 $\mu s$ wird nach einem bestimmten Algorithmus, der Sender und Empfänger bekannt ist die Frequenz gewechselt. Die Hopping-Sequenz ist pseudozufällig, u.a. basierend auf der Geräte-ID und wiederholt sich nach ca. 23,3 Stunden [Roth02].

### 4.2.4 Verbindungsaufbau

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse, die so genannte Bluetooth Device Address. Der Verbindungsaufbau erfolgt über Inquiry und Paging.

Inquiry: Per Inquiry-Prozedur kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte im Sendebereich befinden. Nach einem Inquiry liegen alle Geräteadressen und Zeittakte der gefundenen kommunikationsbereiten Geräte vor.

Paging: Durch eine Paging-Anforderung kann nun eine Kommunikationsverbindung zu einem dieser Geräte aufgebaut werden. Das Gerät, das die Verbindung aufbaut, wird Master genannt, das andere Slave. Für den Verbindungsaufbau wird die Sprungsequenz des Slaves verwendet, die so genannte Page- Hopping-Sequence. Während des Pagings sendet der Master seine Geräteadresse und seinen Zeittakt an den Slave. Für die weitere Kommunikation wird anschließend die Sprungsequenz des Masters verwendet, die so genannte Channel-Hopping-Sequence. Neben einer Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten unterstützt Bluetooth auch Punkt-zu-Mehrpunkt- Verbindungen. Bis zu 255 Bluetooth-Geräte (im Sonderfall auch mehr) können in einem so genannten Piconet als Slaves im Park-Mode mit einem Master vernetzt sein. Zusätzlich können bis zu 7 Slaves gleichzeitig aktiv mit dem Master kommunizieren. Alle Geräte in einem Piconet folgen der gleichen Channel-Hopping-Sequence und dem Zeittakt des Masters. Prinzipiell sieht Bluetooth sogar die Möglichkeit einer Vernetzung von bis zu zehn Piconets zu einem so genannten Scatternet vor. In der Praxis kommen solche komplexen Netztopologien aber zurzeit noch selten vor [BSI03].

Die Initialisierung der Kommunikation beginnt mit der Generierung des init key. Die Funktion f berechnet aus einem geheimen PIN, der Device Adresse des Geräts ($D\_ADDR_b$) und einer Zufallszahl ($r$) berechnet und anschließend überprüft (Gleichung 4.1 und 4.2 ). Der PIN ist eine Zahl, die der jeweilige Nutzer auf einem anderem gesicherten Kanäle (z B. über Tastaturen) eingegeben wird und zwischen 8 und 128 bit lang sein muss. Wird kein PIN gewählt, wird der default PIN 0 verwendet. Die im Gerät generierte Pseudozufallszahl wird unverschlüsselt über die Luft übertragen, die Device Address ist durch vorangehende, unverschlüsselte Kommunikation bekannt.

$$\begin{array}{rcl} Alice & & Bob \\ random(r) & \longrightarrow & \end{array} \tag{4.1}$$

$$InitKey := f(PIN, D\_ADDR_b, r) \quad \longrightarrow \quad InitKey := f(PIN, D\_ADDR_b, r)$$

$$\begin{array}{rcl} Alice & & Bob \\ random(r2) & \longrightarrow & \\ a := f(D\_ADDR_b, r2, InitKey) & \longrightarrow & a' := f(D\_ADDR_b, r2, InitKey) \\ test : a = a' & & \end{array} \tag{4.2}$$

Danach wird der link key generiert, wobei die Kommunikation zu diesem Zeitpunkt durch den init key verschlüsselt ist. Der link key wird permanent gespeichert und dient zur späteren Authentisierung der Geräte und als Grundlage zur Verschlüsselung.

### 4.2.5 Authentisierung

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier- Verfahrens verwendet. Es wird grundsätzlich einseitige Authentisierung verwendet, das heißt ein Gerät (Claimant) authentisiert sich gegenüber einem anderen Gerät (Verifier). Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt. Die Authentisierung läuft wie folgt ab: Der Verifier sendet eine nach einem nicht spezifizierten Algorithmus erzeugte Pseudozufallszahl an den Claimant. Dieser beweist, dass er das gemeinsame Geheimnis (den Verbindungsschlüssel) kennt, indem er unter Benutzung des Verbindungsschlüssels aus der Pseudozufallszahl und seiner eigenen Geräteadresse eine 32 bit lange Antwort berechnet und zum Verifier zurücksendet. (Dabei berechnet er gleichzeitig aus diesen Daten einen 96 bit langen sog. Authenticated Cipher Offset, der geheim gehalten wird und bei Bedarf - als ein Teil - bei der Erzeugung eines Verschlüsselungsschlüssels verwendet wird.) Der Verifier überprüft die Antwort, indem er die gleiche Berechnung durchführt. Sind die Ergebnisse identisch, ist der Claimant authentisiert [BSI03].

### 4.2.6 Verschlüsselung

Die Verwendung der Verschlüsselung ist optional. Um die Verschlüsselung zu verwenden muss sich mindestens einer der Kommunikationspartner gegenüber dem Anderen authentisiert haben. Die Verschlüsselung kann vom Master, als auch vom Slave beantragt werden. Dabei wird die Verschlüsselung immer vom Master

gestartet, nachdem die notwendigen Parameter mit dem Slave ausgehandelt wurden. Erst nach der Einigung über die Länge des Schlüssels startet der Master die Verschlüsselung. Die geschieht durch Senden einer Zufallszahl an den Slave. Der Chiffrierschlüssel berechnet sich aus Verbindungsschlüssel, einem Cipher Offset und der Zufallszahl. Es stehen für die Verschlüsselung zwei Betriebsarten zur Verfügung: Punkt-zu-Punkt-Verschlüsselung und Punkt-zu-Mehrpunkt-Verschlüsselung. Bei Punkt-zu-Punkt-Verschlüsselung wird der Authenticated Cipher Offset des Authentisierungsprotokolls als Cipher Offset verwendet. Bei Punkt-zu-Mehrpunkt- Verschlüsselung wird dagegen die Geräteadresse des Masters als Cipher Offset genutzt. Außerdem muss der Verbindungsschlüssel durch einen Master-Schlüssel ersetzt werden, bevor die Verschlüsselung gestartet wird. Zum Verschlüsseln wird eine Stromchiffre (im Standard mit E0 bezeichnet) eingesetzt. Für jedes Datenpaket wird dabei ein neuer Initialisierungsvektor ("Spruchschlüssel") aus der Geräteadresse sowie dem Zeittakt des Masters berechnet. Verschlüsselt sind die Daten nur während des Transports per Funk. Vor der Aussendung bzw. nach Empfang liegen die Daten in den beteiligten Geräten unverschlüsselt vor; es handelt sich also nicht um Ende-zu-Ende-Verschlüsselung (d. h. Verschlüsselung der Daten von der Eingabe in Endgerät A bis zur Ausgabe/Bearbeitung in Endgerät B.) [BSI03]

### 4.2.7 Fazit

Zu den Gefährdungen, die sich bei leitungsgebundener Kommunikation ergeben kommt bei drahtloser Kommunikation noch die Gefährdung dazu, dass sich die Funkwellen in einem gewissen Rahmen unkontrolliert ausbreiten. Damit kann nicht sichergestellt werden, dass niemand die Kommunikation mithören kann.

Die einzelne Schwächen im Sicherheitskonzept von Bluetooth sind:

- Verschlüsselung ist nicht unbedingt vorgeschrieben
- unsichere Grundkonfigurationen sind nicht ausgeschlossen
- schwache PINs können erraten werden
- Geräteschlüssel als Verbindungsschlüssel ist unsicher
- schwache Integritätssicherung
- Qualität des Zufallsgenerators nicht im Standard festgelegt

In bestimmen Konfigurationen von Bluetooth ist ein Man-in-the-Middle-Angriff möglich. Dabei wird von einem Angreifer ein für die anderen beiden Kommunikationspartner transparentes Geräte in die Kommunikation geschoben. Damit kommunizieren beide Geräte über das eingeschobene Gerät. Dort kann dann eine Manipulation des Datenstroms stattfinden.

Die optionale Verschlüsselung des Datenverkehrs hat auch einige Schwächen. Trotz einer möglichen Schlüssellänge der Stromchiffre E0 von 8-128 bit wurde von [Flu/Lu01] herausgefunden, dass die Sicherheit nicht einen Schlüssel der 73 bit lang ist, übersteigt.

Der Initialisierungsvektor unter dessen Verwendung jedes übertragene Datenpaket verschlüsselt wird, ist nicht vollständig unabhängig. Er ist vom Zeittakt des Master abhängig und somit ist selbst bei Verschlüsselung ein Man-in-the-Middle-Angriff möglich. Damit ist auch die Datenintegrität nicht mehr gesichert, wenn ein Teil der abgefangenen verschlüsselten Daten im Klartext bekannt ist, währe es möglich beispielsweise IP-Header zu verändern. [BSI03]

## 4.3 Wireless LAN - IEEE 802.11

### 4.3.1 Einfühung

Die Mehrzahl der derzeit am Markt verfügbaren Funk-LAN Systeme basieren auf der 1999 vom IEEE verabschiedeten Erweiterung 802.11b des Standards 802.11. Die Hersteller-Vereinigung WiFi-Alliance (vormals WECA) dokumentiert die Kompatibilität zum Standard 802.11b durch die Vergabe des WiFi-Zertifikats. Seit November 2002 sind in Deutschland auch Frequenzen im 5 GHz-Bereich freigegeben, so dass auch Systeme der Standards 802.11a bzw. 802.11h zum Einsatz kommen werden. Aktuell ist auch IEEE 802.11g verabschiedet worden, sodass künftig mit dem Einsatz kompatibler Systeme zu rechnen ist.

Diese Standards sind heutzutage der "state of the art" mit dem größten Marktanteil für drahtlose lokale Netze. Im so genannten SOHO-Bereich (small office home), aber auch für HotSpots (öffentliche Plätze oder Gebäude mit hoher Nutzeranzahl) wird WLAN zunehmend eingesetzt.

### 4.3.2 Protokollarchitektur

Als Teilstandard der IEEE 802er Reihe wurde die bekannte Einteilung (Abb. 4.4) in Bitübertragungsschicht (Physical Layer) und Sicherungsschicht (Date Link Layer) gewählt. Die Sicherungsschicht unterteilt sich weiterhin in Media Access

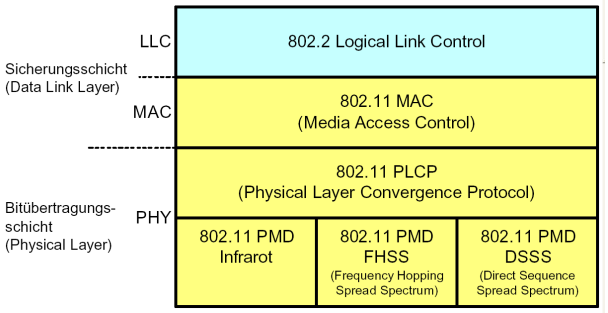


Abbildung 4.4: Die Protokollarchitektur von 802.11 [Roth02]

Control (MAC) und Logical Link Control (LLC).

Die LLC-Schicht ist mit dem Standards IEEE 802.3 definiert. Es sind in 802.11 drei Arten der Bitübertragung definiert. Eine Infrarotübertragung und 2 Funkübertragungen (FHSS und DSSS). Deshalb wurde auch der Physical Layer in 2 Teilschichten zergliedert:

- Physical Layer Convergence Protokoll (PLCP): Bereitstellung eines einheitlichen Zugriffs auf die PMD für den MAC-Layer.
- Physical Medium Dependent (PMD): konkrete Definition der Verfahren der Bitübertragung

Laut der Spezifikation von WLAN kann es in 2 verschiedenen Modi betrieben werden. Im Ad-hoc-Modus werden die Rechner ohne Basisstationen untereinander verbunden. Zwei Geräten können nur miteinander kommunizieren, wenn sie innerhalb ihrer Kommunikationsreichweite liegen. Eine Routingfunktion ist in der Spezifikation nicht vorgesehen und wird höheren Protokollschichten vorbehalten. Im Infrastrukturmodus erfolgt jede Kommunikation über eine Basisstation. Dieses Basisstation, auch Access-Point genannt, verfügt über eine Funkschnittstelle im WLAN-Standard und eine weitere kabelgebundene Schnittstelle, meist nach IEEE 802.3. Damit ist den drahtlosen Stationen eine Kommunikation in stationäre drahtgebundene Netze möglich. [Roth02]

### 4.3.3 Bitübertragungsschicht

Da IEEE 802.11a ein Standard zu drahtlosen Kommunikation ist, musste bei der Entwicklung des Standards größerer Rücksicht in Hinblick auf die Fehlersicherheit der Kommunikation gelegt werden. Die Hauptprobleme sind:

- Rauschen und Interferenzen
- Funksignale von Anderen WLAN-Stationen, die mit Übertragungen kollidieren
- Funksignale von Netzwerken, die das gleiche Frequenzband nutzen (Bluetooth)
- Störsignale von Geräten von anderen elektrischen Anlagen (Mikrowelle)

Wie auch in Abbildung 4.4 zu ersehen ist umfasste die Bitübertragung im Standard von IEEE 802.11a nicht nur die Funkübertragung, sondern auch eine Variante der Bitübertragung mittels infrarotem Licht. Diese Variante hat sich aber nicht auf dem Markt durchgesetzt und wird im Weiteren nicht weiter betrachtet.

Die Bitübertragungsschicht der Funkschnittstelle, nutzt den Frequenzbereich von 2,4 bis 2,4835 GHz, das ISM-Band. Die maximale Kommunikationsreichweite beträgt innerhalb von Gebäuden 30 m und außerhalb bis zu 300 m. Es stehen 2 Verfahren zur Funkübertragung zu Verfügung. Das FHSS (Frequency Hopping Spread Spread Spectrum) und das DSSS (Direct Sequence Spread Spectrum).

Bei FHSS wurde das zu Verfügung stehende Frequenzspektrum von 2,4 bis 2,4835 GHz in 79 Kanäle aufgeteilt. (in Frankreich, Spanien und Japan stehen nur 23 Kanäle zu Verfügung) Durch einen schnellen Wechsel der Kanäle alle 0,4 Sekunden nach einer Pseudozufallsfolge, werden schmalbandige Störungen kompensiert. Das FHSS-Verfahren hat aber eine schlechte Ausnutzung des Frequenzspektrums, deshalb wird das DSSS-Verfahren heutzutage am häufigsten eingesetzt. DSSS basiert auf Bandspreizung nach den CDMA-Verfahren und hat somit eine bessere spektrale Nutzung und eine relativ besserer Störunempfindlichkeit.

Die Datenintegrität auf Bitübertragungsebene ist nicht gewährleistet, lediglich der Header ist mittels eines 16 bit langen CRC-Feldes gesichert. [Roth02]

### 4.3.4 Sicherungsschicht

Die Sicherungsschicht besteht aus den Sublayern Logical Link Control (LLC) und Media Access Control (MAC). Der LLC-Sublayer ist in der Spezifikation IEEE 802.2 genau erläutert und wir hier nicht weiter erklärt. Die Aufgabe des MAC-Sublayers ist es den Zugriff auf das Funkmedium zu regeln. Es kommen drei Verfahren zum Einsatz.

- einfaches Carrier Sense Multiple Access mit Collision Avoidance (CSMA/CA)

- Carrier Sense Multiple Access mit Collision Avoidance mit Ready to Send und Clear to Send (CSMA/CA mit RTS/CTS
- Point Coordination Function (PCF)

**CSMA/CA** ist ein eine modifizierte Version des CSMA/CD-Zugriffverfahrens bekannt aus dem drahtgebundene Ethernet. Wie bei CSMA/CD hören alle teilnehmenden Stationen physikalisch den Verkehr auf dem Funkkanal mit. Wenn eine Station übertragen will, wartet sie bis das Medium frei ist. Danach wartet sie noch eine vorbestimmte Zeitperiode plus einer zufällig gewählten Zeitspanne, bevor sie ihren Frame übertragen will. Auch in dieser Zeitspanne (Wettbewerbsfenster) wird der Funkkanal weiter überwacht. Wenn keine andere Station innerhalb des Wettbewerbsfensters vor dem gewählten Zeitpunkt mit der Übertragung beginnt, sendet die Station ihren Frame. Hat aber eine andere Station innerhalb der Wartezeit mit der Übertragung begonnen, wird der Zeitzähler angehalten und nach der Übertragung der anderen Station weiter benutzt. Auf diese Weise gewinnen Stationen, die nicht übertragen durften, an Priorität und kommen mit einer erhöhten Wahrscheinlichkeit in den nächsten Wettbewerbsfenstern zum Zug. Eine Kollision kann nur entstehen, wenn zwei oder mehrere Stationen den gleichen Zeitslot auswählen. Diese Stationen müssen die Wettbewerbsprozedur erneut durchlaufen. [Sik02]

Bei **CSMA/CD mit RTS/CTS** wird die Kollisionsvermeidung (avoidance) noch erweitert, dass eine sendewillige Station vor dem Absetzen der Daten ein kurzes RTS-Signal (Request to Send) in die Luft schickt, das den potenziellen Empfänger über das Ziel und den Umfang der Daten informiert. Der Empfänger sendet seinerseits als Bestätigung ein CTS-Signal (Clear to Send), die alle Teilnehmer im Empfangsbereich abhören und somit darüber informiert werden, dass das Medium im Folgenden belegt sein wird. Erst dann beginnt die eigentliche Datenübertragung zwischen einem Sender und einem Empfänger, und der Abschluss der Datenübertragung sowie die Vollständigkeit der Daten wird durch ein kurzes ACK-Paket (Acknowledge) vom Empfänger bestätigt. Probleme können durch versteckte Teilnehmer (Hidden Nodes) entstehen. Dieses Kommunikationsproblem kann immer dann auftreten, wenn eine Station nicht erkennen kann, dass das Medium bereits belegt ist. Vermieden wird dieses Problem durch die abgehörten CTS- und RTS- Signale. [Sik02]

Bei **PCF** hingegen wird die Vergabe des Mediums durch einen Manager (z.B. ein Access-Point) sichergestellt. Dazu richtet der Manager eine Contention Free Period (CFP - "Streitfreie Zeit") ein, die sich zeitlich mit einer Contention Period

(CP - mehrere Stationen versuchen Zugriff auf den Kanal zu erhalten) abwechselt. Realisiert wird diese CFP, indem der Manager ein Management-Frame sendet in dessen Header ein 2Byte-Feld für alle Teilnehmer bestimmt ist. Die Teilnehmer setzen einen eigenen Timer, der anzeigt wie lange der Kanal belegt sein wird auf diesen Wert, so dass der Manager für die CFP alleinigen Zugriff auf den Kanal hat. Nun wird nacheinander jedem beim Manager gemeldete Teilnehmer (er führt sie in einer Polling Liste) die Möglichkeit gegeben, ein Frame zu versenden. Dazu sendet der Manager der Station eine Poll-Frame. Nur Stationen, die ein solches Poll-Frame erhalten haben sind berechtigt, ein Daten-Frame zu senden. [Sik02]

### 4.3.5 Sicherheitsmechanismen bei 802.11

Die Sicherheitsmechanismen aller 802.11 kompatiblen Systeme sind im Standard 802.11 definiert. Die Erweiterungen a, b, g und h des Standards bieten keine zusätzlichen Sicherheitsmechanismen, erst die Erweiterung i wird neue Sicherheitsmechanismen definieren. Die zurzeit in 802.11 definierten Mechanismen dienen ausschließlich zur Sicherung der Funkstrecke zwischen den Clients und Access-Points. Darüber hinaus lässt der Standard aber auch Freiraum für proprietäre Erweiterungen. Sämtliche Sicherheitsmechanismen des Standards 802.11, die im Folgenden dargestellt werden, sind überwindbar und bieten keinen verlässlichen Schutz für sensible Informationen. [BSI03]

#### 4.3.5.1 Netzwerkname (SSID)

Es besteht die Möglichkeit dem Lokalen Funknetzwerk einen Netzwerknamen (ESSID bzw. SSID: (Extended) Service Set Identity) zu geben. Dabei existieren es zwei Betriebsarten. Wird durch den Nutzer die Kennung "Any" angegeben, akzeptiert die Funk-LAN-Komponente beliebige SSIDs. Im anderen Fall wird der eingetragene Name überprüft und nur Teilnehmer mit der gleichen SSID können am Netzwerk teilnehmen. Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID dazu, den nächsten Access-Point zu finden. Da die SSID im Klartext über das Netz gesendet wird, kann ein Angreifer sie mit einfachen Mitteln in Erfahrung bringen. Einige Access-Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden. Das Unterdrücken der SSID auf diese Weise ist jedoch nicht standardkonform. [BSI03]

#### 4.3.5.2 MAC-Adresse

Jede Netzwerkkarte verfügt über die eindeutige Hardwareadresse die sog. MAC-Adresse (Media Access Control-Adresse). Prinzipiell ist es möglich, in einem Funk-LAN MAC-Adressen zu definieren, denen es erlaubt ist, mit einem Access-Point zu kommunizieren. Die Adresslisten müssen hierfür allerdings manuell gepflegt werden, was einen erheblichen Aufwand nach sich zieht. In vielen Einsatzszenarien ist dies nicht möglich. Das Filtern der MAC-Adressen ist nicht im Standard enthalten. Andererseits ist die Filterung von MAC-Adressen standardkonform, da die Filterung keine Auswirkungen auf die Kompatibilität der Clients hat. [BSI03]

#### 4.3.5.3 Kryptografische Sicherung

Vertraulichkeit, Integrität und Authentizität im Standard nach IEEE 802.11 sollen durch das "Wired Equivalent Privacy"-Protokoll (WEP) gesichert werden. Das WEP-Protokoll (Abb. 4.5) basiert auf der Stromchiffre RC4, mit der die Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffredaten umgewandelt werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder optional 104 bit Länge und muss den am Funk-LAN beteiligten Clients sowie dem Access-Point vorab zur Verfügung gestellt werden. Dabei wird für das gesamte Funk-LAN ein gemeinsamer Schlüssel verwendet. Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Der IV wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und über das Funk-LAN übertragen. Über WEP soll die Vertraulichkeit und Integrität der übertragenen Daten gesichert sowie die Authentisierung des Endgerätes durchgeführt werden. Die Realisierung geschieht wie folgt:

**Vertraulichkeit**: Aus dem Schlüssel und dem IV wird ein zufälliger Bitstrom generiert. Die Chiffredaten ergeben sich, indem die Klardaten bitweise mit dem Bitstrom XOR-verknüpft werden. Die Entschlüsselung der Chiffredaten beim Empfänger erfolgt widerum mit einer XOR-Verkünpfung mit dem Schlüssel.

**Integrität**: Für jedes zu übertragene Datenpaket wird eine 32-bit CRC-Checksumme berechnet. Anschließend wird das Datenpaket mit der angehängten Checksumme der WEP-Verschlüsselung unterzogen. Der Empfänger entschlüsselt das Datenpaket und überprüft die Checksumme. Bei korrekter Checksumme, wird das Datenpaket angenommen, sonst verworfen.

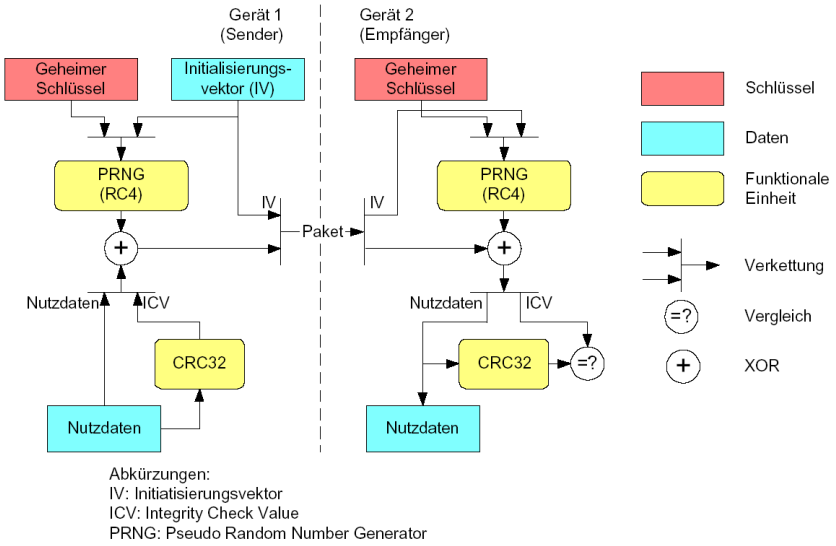


Abbildung 4.5: Prinzip der WEP-Verschlüsselung [Roth02]

**Authentisierung**: In Verbindung mit der WEP-Verschlüsselung kann zwischen zwei Authentisierungsmodi gewählt werden: "Open" (hierbei findet keine Authentisierung statt) und "Shared Key". Für die Authentisierung im "Shared Key"-Modus wird ein sog. Challenge-Response-Verfahren durchgeführt. Der Authentisierungsprozess ist nur einseitig: der Access-Point muss sich gegenüber den Clients nicht authentisieren. Zum Authentisieren wird derselbe Schlüssel verwendet wie zur Verschlüsselung der Nutzdaten. [BSI03]

### 4.3.6 Sicherheitslücken

**SSID Broadcast:** Bei einigen Access-Points besteht die Möglichkeit, die Bekanntgabe der SSID im Broadcast zu unterbinden, um das Funk-LAN vor Unbefugten zu verstecken (so genanntes "Closed System"). Dieser Schutz ist leider nur gegen einige frei verfügbare Tools wie z. B. Netstumbler wirksam. Funk-LAN-Analysatoren hingegen können die SSID auch aus anderen Management- und Steuersignalen ermitteln.

**Manipulierbare MAC-Adressen:** Diese MAC-Adressen der Funk-Clients können relativ einfach abgehört und manipuliert werden, somit sind die in den Access-Points zum Zweck des Zugriffsschutzes häufig eingebauten MAC-Adressfilter überwindbar. Die Manipulierbarkeit der MAC-Adressen hat aber auch den Vorteil, dass die Anonymität des mobilen Gerätes gewährt bleibt. Es kann nicht mehr genau bestimmt werden, ob sich das mobile Gerät schon einmal an der Basisstation

angemeldet hatte.

**Fehlendes Schlüsselmanagement:** Schlüssel müssen in einem Funk-LAN manuell eingetragen werden, in jedem Funk-LAN-Adapter (Client) und im Access-Point muss per Hand derselbe statische Schlüssel eingetragen werden. Dies erfordert physischen Zugriff auf die Komponenten. Diese Art des "Schlüsselmanagements" führt in der Praxis oft dazu, dass der geheime Schlüssel sehr selten oder überhaupt nicht gewechselt wird. Die Offenbarung eines Schlüssels, z. B. durch Verlust eines Clients oder mittels frei verfügbarer Tools, kompromittiert das gesamte Funk-LAN. Der gemeinsame geheime Schlüssel eines Funk-LAN-Clients wird, je nach Hersteller, entweder auf der Funk-LAN-Karte oder auf der Festplatte des Client- Rechners gespeichert; einige Hersteller schreiben diese Informationen sogar offen in die Registry- Datei des Windows-Betriebssystems.

### 4.3.7 Schwachstellen der Sicherheit

Das Ziel mittels WEP Vertraulichkeit, Integrität und Authentizität im Funk-LAN zu sichern, kann eindeutig als nicht erreicht eingestuft werden, denn WEP ist mittlerweile vollständig kompromittiert. Es existieren sogar frei verfügbare Tools für passive Angriffe.

**Die Schlüssellänge von 40 bit ist viel zu kurz.** Durch Probieren aller Schlüsselkombinationen (Brute-Force-Methode) ist es mit einem handelsüblichen PC innerhalb von wenigen Tagen möglich den Schlüssel zu kompromittieren. Zwar wäre diese Prozedur wieder nötig, wenn der Schlüssel verändert werden würde, aber durch das fehlende Schlüsselmanagement muss nicht davon ausgegangen werden. Wenn optional eine Schlüssellange von 104 bit gewählt wird,kann die Kommunikation als ausreichend gesichert gegen die Brute-Force- Methode angesehen werden.

**Länge von 24 bit des IV ist viel zu kurz.** Der verwendetet Stromchiffrier-Algorithmus kann nur sicher sein, wenn der generierte Bitstrom für je zwei Datenpakete unterschiedlich ist. Wird zweimal mit dem gleichen Bitstrom verschlüsselt, lassen sich sowohl die beiden Datenpakete als auch der Bitstrom rekonstruieren. Da sich der Bitstrom aus Schlüssel und IV berechnet und der Schlüssel für längere Zeit als konstant angenommen werden kann, reicht es aus, zwei verschlüsselte Datenpakete mit demselben IV abzufangen, um diese zu entziffern. Mit 24 bit sind maximal ca. 16,8 Mio. verschiedene IVs generierbar. Nach ca. 4000 Datenpaketen

ist damit die erste Wiederholung eines IVs zu erwarten. Bei regem Datenverkehr zwischen Access-Point und den per Funk-LAN angeschlossenen Rechnern ist nach einigen Stunden Aufzeichnung zu erwarten, dass jeder IV mindestens ein Mal verwendet wurde und von dort ab der Funk-LAN-Verkehr mit hoher Verlässlichkeit mitgelesen werden kann. Die Problematik des zu kurzen IVs betrifft Schlüssellängen von 40 und 104 bit gleichermaßen.

**Datenpakete können gefälscht werden.** Da eine ausreichende Sicherheit von Schlüssel und IV nicht gewährleistet ist, ist es einem Angreifer bei Besitz von Schlüssel und IV möglich den Datenstrom zu verfälschen. Sind zu einem abgehörten Chiffrat die Klardaten bekannt (IP-Adresse), kann aus dem Chiffrat der generierte Bitstrom durch die einfache XOR-Struktur berechnet werden. Wird anschließend der berechnete Bitstrom zum Chiffrieren wieder verwendet, haben diese Chiffrate zwar alle den gleichen IV - die mehrfache Verwendung eines IVs ist jedoch möglich, da der IV ausschließlich vom Sender festgelegt wird und somit der Angriff von den anderen Teilnehmern des Funk-LANs nicht bemerkt werden kann. Der Angreifer gelangt am einfachsten an einen Bitstrom, indem er eine Authentisierung mitlauscht.

**Das Authentisierungsprotokoll kann gebrochen werden.** Wird von einem Angreifer ein vollständiger Authentisierungsprozess aufgezeichnet, so ist eine Authentifikation für ihm möglich, ohne im Besitz des Schlüssels zu sein. Durch eine XOR-Verknüpfung von Challenge und Response kann er zu einer gegebenen Challenge selbst die Response berechnen werden. Da für die Authentisierung und Verschlüsselung derselbe Schlüssel verwendet wird, können mit dem errechneten Bitstrom Nachrichten gefälscht werden.

**Die Integritätssicherung mittels CRC ist wirkungslos.** Das CRC-Verfahren ist nicht geeignet die Integrität von Datenpakten sicherzustellen. Durch die Linearität ist es dem Angreifer möglich das abgefangene Paket an bestimmten Stellen zu verändern ohne die Prüfsumme zu ändern und ohne den kompletten Klartext des Paketes zu kennen. Lediglich die Kenntnis einiger Bits im Paket ist notwendig, da aber Redundanzen zwischen den einzelnen Paketen bestehen, ist dies relativ einfach zu bestimmen.

### 4.3.8 Fazit

Die geforderten Sicherheitskriterien Vertraulichkeit, Integrität, Authenzität, Zugriffskontrolle/Autorisierung und Anonymisierung sind zwar beim Entwurf der

Sicherheitsarchitektur berücksichtigt worden aber die Verfahren sind nicht ausreichend stark genug. Trotz des Versuchs die Sicherheit bei IEEE 802.11 mit der Entwicklung des WEP2-Sicherheitsverfahren mit einer Schlüssellänge von 128 bit) zu erhöhen, wurden die grundlegenden Fehler von WEP in WEP2 nicht beseitigt. Das Hauptproblem ist der zu Grunde liegende viel zu schwache RC4-Algorithmus. Es müssen also in den höheren Schichten Sicherheitsvorkehrungen in Bezug auf Verschlüsselung, Integritätsschutz und Authentisierung getroffen werden. Dies kann unter Umständen mittels Einsatz von IEEE 802.1X Authentisierung mit Hilfe eines Remote Authentification Dial-In User Service -Servers (RADIUS-Server) geschehen.

## 4.4 HiperLAN/2

HiperLAN/2 (High Performance Radio Local Area Network Type 2) wurde von der ETSI (European Telecommunications Standards Institute) als eine Konkurrenz zum amerikanischen Standard für drahtlose lokale Netzwerke (IEEE 802.11) entwickelt. Er ist Nachfolger des HiperLAN-Standards, der bei den Herstellern keinen Anklang fand. Aber auch HiperLAN/2 wartet noch auf den Durchbruch. Aussagen die die Sicherheit betreffen können deshalb nur abgeschätzt werden. Eine großer Unterschied zu IEEE 802.11 ist es, dass HiperLAN/2 quasi wie drahtloses ATM funktioniert, also zentral gesteuert, verbindungsorientiert und Quality of Service (QoS) unterstützt. Dies sind entscheidende die eventuell den Markteintritt von HiperLAN/2 erleichtern können.

### 4.4.1 Eigenschaften

- Frequenzband von 5,150-5,350 GHz oder 5,470 - 5,725 GHz
- maximal Datenrate 54 mbit/s (brutto)
- Reichweite 30 m (im Gebäude) 150 m (außerhalb)
- Ad-hoc-Modus (Direct Mode) und Infrastruktur-Modus (Centralized Mode) stehen zur Verfügung
- Unterstützung von Quality of Service (QoS)
- Stromsparmodus verfügbar

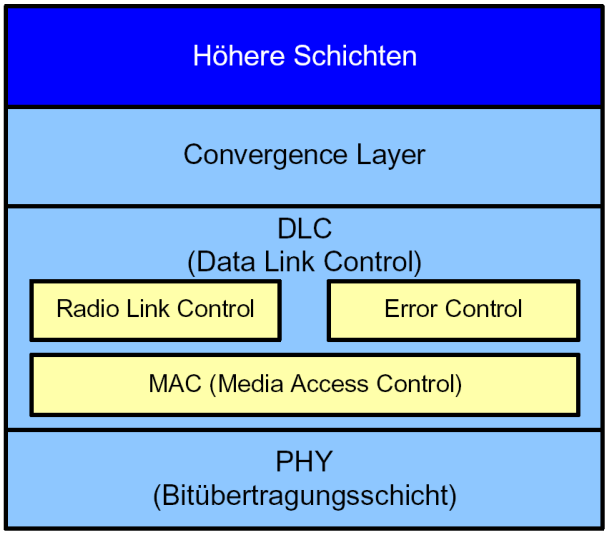


Abbildung 4.6: HiperLAN/2 Referenzmodell [Roth02]

Die emittierte Sendeleistung ist auf 200 mW (Innenräumen) und auf 1 W (EIRP) in Außenbereichen limitiert. Ein Weiterreichen der mobilen Stationen von Basisstation zu Basisstation, ein so genanntes Handover, wird auch unterstützt.

Die Bitübertragung erfolgt mit Hilfe von OFDM (Orthogonal Frequency Division Multiplex) und ist zeitschlitzgesteuert (TDMA/TDD, Time Division Multiple Access/Time Division Duplex). Es erfolgt eine feste Einteilung des physikalischen Funkkanal in Frames von 2 ms Länge. Der Frame ist wiederum in einzelne Zeitschlitze (Slots) von je 4 s Länge unterteilt. Die Slots können sowohl zum Senden als auch zum Empfangen verwendet werden. Die Zugriffssteuerung erfolgt auf jeden Fall zentral durch eine Basis-Station (auch Access-Point).

### 4.4.2 Das HiperLAN/2 Referenzmodell

Das in Abbildung 4.6 gezeigte Referenzmodell besitzt die drei Schichten Bitübertragungsschicht (PHY), Data Link Control (DLC) und den Convergence Layer. Die Aufgaben der Bitübertragungsschicht entsprechen den Aufgaben des Physical Layer von z.B. IEEE 802 oder OSI.

Es erfolgt eine weitere Untergliederung der Data Link Control - Schicht in:

- Radio Link Control (RLC): Kryptografische Verschlüsselung des Datenstromes, Handover, Power Management, Verbindungsmanagement, Broadcast, Multicast

- Error Control (EC): Bereitstellen einer zuverlässigen Datenübertragung (ARQ-Mechanismen)

- Media-Access Control (MAC) kollisionsfreier Zugriff auf das Funkmedium

Die oberste Schicht stellt der Convergence Layer dar. Die Aufgaben dieser Schicht sind das Zerlegen und Zusammensetzen der kleinen Datenpakete der unteren Layer in größere Pakete für die oberen Layer und umgekehrt. Je nach Netztopologie wird zwischen einem zellbasierten Convergence Layer (bei ATM-Netzen) und einem paketbasiertem Convergence Layer (bei z.B. Ethernet) unterschieden.

### 4.4.3 Verbindungsaufbau

Wie schon erwähnt erfolgt der Zugriff der Kommunikationspartner auf das Funkmedium zentral durch eine Basisstation (BS) geordnet. Diese Station entscheidet über die Verwendung der Slots und teilt dazu einen Frame in mehrere Phasen mit variabler Länge ein:

1. Broadcast (BC) Phase: BS sendet allgemeine Kontrolldaten und Informationen über die Verwendung der Slots für diesen Frame an alle mobilen Stationen.

2. Downlink (DL) Phase: BS sendet Kontroll- und Nutzdaten an die einzelnen mobilen Stationen.

3. Direct Link (DiL) Phase: Die mobilen Stationen tauschen Nutzdaten direkt untereinander aus.

4. Uplink (UL) Phase: Die mobilen Stationen senden Kontroll- und Nutzdaten an die BS.

5. Random Access (RA) Phase: Die mobilen Stationen senden Kontrolldaten unaufgefordert an die BS, d. h. das Senden in dieser Phase ist nicht kollisionsfrei.

Die Zuweisung einer freien MAC-Adresse von der Basisstation ist der erste Schritt, die eine mobile Station, die eine Verbindung zur einer Basisstation aufbauen möchte, durchlaufen muss. Die Anforderung der MAC-Adresse kann in der Random-Access Phase geschehen, in der das unaufgeforderte Senden von Kontrolldaten erlaubt ist. Nach dem Erhalt einer freien MAC-Adresse in der

Broadcast-Phase von der Basisstation, werden die Verbindungsparameter vereinbart. Die mobile Station gibt die von ihr unterstützen Verbindungsparameter der Basisstation bekannt. Die Basisstation überprüft die empfangenen Parameter und schlägt unter Umständen Alternativen vor. Einer Akzeptanz der mobilen Station vorausgesetzt, kann der Verbindungsaufbau entsprechend fortgesetzt werden. Bei der maximalen Ausschöpfung der bereitgestellten Sicherheitsfeatures werden dann noch die folgenden Punkte des Verbindungsaufbaus abgearbeitet:

1. Verschlüsselung: vereinbaren eines gemeinsamen Sitzungsschlüssel und Verschlüsselung der weiteren Kommunikation.

2. Authentisierung: Gegenseitige Authentisierung

3. Multicastschlüssel: Empfang des Multicast-Schlüssels durch die mobile Station

Der letzte Punkt des Verbindungsaufbaus ist der Austausch weiterer Informationen über das Netzwerk (wie z. B. den Netzwerktyp, d. h. Ethernet, UMTS, Firewire, usw.).

### 4.4.4 Sicherheitsmechanismen

Im Folgenden werden die Sicherheitsmechanismen von HiperLAN/2 genauer betrachtet. Die Aufgaben der verschiedenen Schlüssel erklärt und Verschlüsselung und Authentisierung etwas näher betrachtet.

Ableitend aus den 3 Sicherheitsstufen beim Verbindungsaufbau sind bei HiperLAN/2 drei verschiedene Schlüssel spezifiziert.

#### 4.4.4.1 Sitzungsschlüssel

Soll der Datenverkehr zwischen mobiler Station und Basisstation verschlüsselt werden, geschieht die mit den Sitzungsschlüssel, der mit Hilfe Diffie-Hellman-Schlüsselvereinbarung durchgeführt wird. Der resultierende Schlüssel ist ein DES- oder ein 3DES-Schlüssel, wobei schwache und halbschwache Schlüssel nicht erlaubt sind. Aufgrund der begrenzten Lebensdauer eines Sitzungsschlüssels initiiert die Basisstation in einstellbaren regelmäßigen Abständen einen Schlüsselwechsel.

#### 4.4.4.2 Multicastschlüssel

Die Verschlüsselung des Multicast- und Broadcast-Verkehrs für die direkten Kommunikation zwischen mobilen Stationen wird mit dem Multicastschlüssel sichergestellt. Jede Multicastgruppe besitzt einen eigenen von der Basisstation erzeugten Schlüssel. Jede mobile Station erhält ihren Multicastschlüssel auf chiffriertem Wege mit Hilfe des Sitzungsschlüssel. Der Multicastschlüssel wird erst aktiv, nachdem alle Multicastgruppenmitglieder den Empfang gegenüber der Basisstation quittiert haben. Die Aktivierung finden mittels eines Broadcastsignals statt. Wie auch der Sitzungsschlüssel ist die Lebensdauer des Multicastschlüssels begrenzt. Die Schlüsselerneuerung findet auf Initiative der Basisstation statt.

#### 4.4.4.3 Authentisierungsschlüssel

Authentisierungsschlüssel sind entweder vorverteilte symmetrische Schlüssel (mit mindestens 128 bit) oder asymmetrische Schlüsselpaare (RSA mit 512, 768 oder 1024 bit). Zur Verwaltung von Public Key Zertifikaten kann eine PKI verwendet werden. Die Nutzung eines biometrischen Verfahrens zur Generierung des Authentisierungsschlüssel wäre hier ein guter Ansatz zur Einbindung der Biometrik.

#### 4.4.4.4 Verschlüsselung

Nach der Vereinbarung des Sitzungsschlüssels beginnt sofort die Verschlüsselung der Datenübertragung zwischen Basis- und mobiler Station. Nun werden gegebenenfalls auch mehrere Multicastschlüssel durch die Basisstation verteilt. Ab jetzt ist eine direkte Kommunikation der einzelnen mobilen Station untereinander mittels Multicast/Broadcast möglich. Die einzelnen Slots werden mittels Sitzungsschlüssel oder Multicastschlüssel im DES- oder 3DES-Verfahren im OFB-Modus (Output Feedback) verschlüsselt. Der für die Verschlüsselung notwendige Initialisierungsvektor berechnet sich aus einem Startwert (Seed) und der Nummer des ersten für die Übertragung benutzten Slots im Frame. Der Seed wird für jeden neuen Frame von der Basisstation neu bestimmt. Die Generierung des Seed findet mittels eines 52-bit Pseudozufallsgenerator (LFSR) und einem zufälligen Initialisierungswert ungleich 0 statt. Der aktuelle Seed wird alle N Frames in der Broadcast Phase an die mobilen Stationen gesendet. Der Wert von N ist herstellerspezifisch. Es besteht die Möglichkeit, dass eine mobile Station den Seed selbst berechnet. Dies muss geschehen, wenn durch Übertragungsfehler kein gültiger Seed von der Basisstation empfangen wurde.

### 4.4.5 Authentisierung

wie auch bei Bluetooth wird zur gegenseitigen Authentisierung ein Challenge- Response Verfahren eingesetzt. Bei HiperLAN/2 kann aber auch ein asymmetrischer Schlüssel verwendet werden.

Als Response wird je nach Authentisierungsschlüssel (symmetrisch oder asymmetrisch) entweder ein MD5-HMAC [Bel96] oder eine RSA Signatur nach PKCS1 v1.5 [RSA93] berechnet wird. Die beiden Stationen authentisieren jeweils eine Verkettung aus der 128 bit Challenge der anderen Station, den beiden öffentlichen DH-Schlüsseln, die zur Vereinbarung des Sitzungsschlüssels verwendet wurden sowie weiteren Werten aus den Verbindungsparametern.

### 4.4.6 Sicherheitsprobleme

Wie bei allen Kommunikationstechnologien die Funk als Übertragungsmedium nutzen sind die unkontrollierbare Ausbreitung der Funkwellen und die potenziellen Bedrohung der Verfügbarkeit (DoS-Attacke) durch beabsichtigte oder unbeabsichtigte Störungen bekante Sicherheitsprobleme von HiperLAN/2. HiperLAN/2 ist zwar viel besser als IEEE 802.11 geschützt, aber nicht völlig ausreichend gegen aktive Man-in-the-Middle Angriffe gesichert.

#### 4.4.6.1 Basisangriff

Eine Man-in-the-Middle-Attacke kann nur Erfolg haben, wenn Basisstation und mobile Station nicht direkt miteinander kommunizieren können. Der Angreifer verbindet die beiden Stationen miteinander, indem er der Basisstation vortäuscht er sei eine mobile Station und umgekehrt. In dieser Konstellation ist es den Angreifer möglich, die abgefangenen Nachrichten vor dem Weiterreichen zu manipulieren. Eine Variante des Angriffs beruht auf der Verwendung verschiedener Frequenzkanäle, da HiperLAN/2 den parallelen Betrieb mehrerer Basisstationen in räumlicher Nähe zulässt.

Eine gezielte Störung des Verbindungsaufbaus eine mobilen Station mit der Basisstation durch den Angreifer, kann den Verbindungsaufbau verhindern. Da noch der Angreifer als Basisstation zur Verfügung steht verbindet sich die mobile Station nun mit dem Angreifer. Das Hindern des Verbindungsaufbaus in der Random-Access Phase kann durch provozierte Kollisionen erreicht werden. Da Kollisionen in der Random-Access Phase erlaubt sind, fällt der Angriff nicht auf.

#### 4.4.6.2 Angriff bei Verschlüsselung ohne Authentisierung

Wird von mobiler Station und Basisstation in den Verbindungsparametern Verschlüsselung, aber keine Authentisierung verabredet, bestehen für den Angreifer zwei Möglichkeiten:

1. Aushandeln eines Sitzungsschlüssel mit beiden Stationen
2. Modifikation der Verbindungsparameter während des Verbindungsaufbaus, so dass Verschlüsselung und Authentisierung abgeschaltet werden

#### 4.4.6.3 Angriff bei Verschlüsselung und Authentisierung

Ist die Verschlüsselung und Authentisierung zwingend erforderlich, da ein Kommunikationspartner nicht gewillt ist Verschlüsselung und Authentisierung abzuschalten, kann die eben beschrieben Variante nicht genutzt werden, da der vereinbarte Sitzungsschlüssel, als auch die Verbindungsparameter authentisiert werden.

Es ist aber eingeschränkt möglich, die Kommunikation zu manipulieren. Aufgrund einer fehlenden Integritätssicherung sowie den Eigenschaften der verwendeten Chiffre (Blockchiffre im OFB Modus) ist es möglich, die abgefangenen Daten gezielt zu verändern, wenn der verschlüsselte Klartext teilweise bekannt ist. So ist es beispielsweise möglich, IP-Header gezielt zu manipulieren. Diese Problematik wird ausführlich in [Bor01] behandelt.

### 4.4.7 Fazit

Durch eine konsistentere Sicherheitsarchitektur, die anerkannte Verschlüsselungsalgorithmen einsetzt und ein Schlüsselmanagement bietet HiperLAN/2 im Vergleich zum direkten Konkurrenten IEEE 802.11 eine wesentlich bessere Sicherheitsarchitektur.

Ein weiterer Vorteil von HiperLAN/2 ist die dynamische Vergabe von MAC-Adressen an die mobilen Stationen. Auf diese Weise kann das Erstellen von Bewegungsprofilen verhindert werden. Unter bestimmten Randbedingungen sind jedoch auch bei Verwendung von Verschlüsselung und Authentisierung Man-in-the-Middle Angriffe denkbar, die eine Manipulation der Kommunikation HiperLAN/2 zulässt. Um dieses zu verhindern, müssten zusätzliche Verfahren zur Integritätssicherung in HiperLAN/2 integriert werden. Da zurzeit noch keine Produkte verfügbar sind, stellt sich die Frage, ob HiperLAN/2 neben IEEE 802.11 existieren kann.

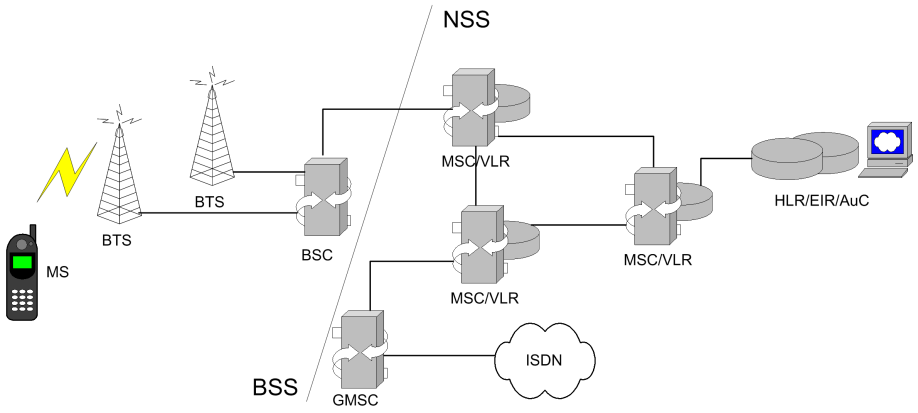


Abbildung 4.7: Die GSM-Netzstruktur

## 4.5 GSM-basierter Mobilfunk

Die Vorgänger des GSM-basierten Mobilfunks waren nationale Netze mit meist analoger Übertragungstechnik. Hohe Nutzungsentgelte und hohe Preise für Endgeräte machten den Mobilfunk für den Massenmarkt nicht attraktiv genug. Da man in jeden Land ein anderer Funkstandard herrschte waren die Netze untereinander inkompatibel. Deshalb schlossen sich 1982 die europäischen Länder zusammen um einen gemeinsamen Standard für den Mobilfunk zu schaffen.

Die Arbeitsgruppe GSM (Group Speciale Mobile) erschuf den GSM 900 / DCS 1800 - Standard. Die Nachfolgeorganisationen SMG (Special Mobile Group) und die ETSI (European Telecommunication Standards Institute) erweiterten die Spezifikation. Der Basisstandard (GSM-Phase-1) übertrug die Daten im 900-MHz-Bereich. 1991 gingen die ersten Netze nach diesem Standard in Betrieb. Die Erweiterung des Standards wurde 1994 mit Inbetriebnahme der ersten Netze im 1800-MHz-Bereich abgeschlossen.

Grundsätzlich war das GSM-Netz zur Sprachübertragung und zur schmalbandigen Datenübertragung konzipiert. Mit Hilfe neuer Dienste die auf GSM aufsetzen sind nun Übertragungsraten von bis zu 115 kbit/s (GPRS) anstatt 22,8 kbit/s möglich.

Die Datenübertragung erfolgt in GSM-basierten Netzen digital. Damit ist es möglich sehr viel mehr Teilnehmer in dem Netz zu verwalten, als es bei den alten analogen Netzen am Anfang der achtziger Jahre der Fall war. Ein Handover zwischen zwei Funkmasten ist mit GSM möglich. Eine weitere Eigenschaft ist das Roaming, es ermöglicht einem Mobilfunkteilnehmer außerhalb des eigenen Netzes; im Ausland das Netz eines anderen Mobilfunkanbieters zu nutzen.

### 4.5.1 Die Architektur von GSM-Netzen

Die Grundstruktur des GSM-Netzes besteht aus Funkzellen, die idealisierter Weise als ein Sechseck dargestellt werden. Der Mittelpunkt jeder Funkzelle ist die Base Transceiver Station (BTS). Die Sendeleistung ist für die BTS begrenzt, so dass eine Beeinträchtigung weit entfernter Zellen ausgeschlossen ist. Die direkt benachbarten Funkzellen kommunizieren mit den Mobile Station (MS - Mobiltelefon) auf einer anderen Frequenz. Durch dies Aufteilung ist eine maximale Nutzung der Frequenzen möglich.

Das GSM-Netz besteht nicht nur aus Funkzellen mit den dazugehörigen Funkmasten. All diese drahtlosen Komponenten werden auch als Base Station Subsystem (BSS) bezeichnet. (Abb. 4.7) Der drahtgebundene Teil der Vermittlung, Anbindung an das Festnetz, Administration und Kontrollfunktionen des Netzes beinhaltet wird als Network and Switching Subsystem (NSS) bezeichnet.

#### 4.5.1.1 Mobilstation

Die beiden Komponenten der Mobilstation sind das mobile Endgerät (ME) und das SIM (Subscriber Identity Module). Zusammen mit der dem SIM und dem ME ist es einem Nutzer möglich sich in das GSM-Netz einzubuchen und zu telefonieren. Auf dem SIM sind u.a. Verschlüsselungsalgorithmen A3 und A8, sowie eine eindeutige vom Mobilfunkbetreiber vergebene Teilnehmerkennung (IMSI) gespeichert. Die Algorithmen A3 und A8 dienen der Authentifizierung und der Verschlüsselung. Im ME ist neben der IMEI (International Mobile Equipment Identity) der Algorithmus A5 integriert, der auch zur Verschlüsselung dient.

#### 4.5.1.2 Base Station Subsystem

Das BSS beinhaltet mindestens eine BTS und mindestens ein Base Station Controller (BSC). In innerstädtischen Bereichen kann eine Zelle in mehre Bereiche aufgeteilt werden. Dann ist ein BSC für die Steuerung aller BTS zuständig, die ortsnah zusammenstehen. Die Anbindung an das Mobile Switching Center (MSC) findet meist via ISDN oder Richtfunk statt.

Die Kommunikation zum ME findet verschlüsselt und via Funk statt. Über einen speziellen Funkkanal findet ein ständiger Austausch von Signalisierungsinformationen zwischen ME und BTS statt.

#### 4.5.1.3 Mobile Switching Center

Das MSC übernimmt allen Signalisierungsaufgaben, wie Verbindungsaufbau und -abbau. Es ist die digitale Vermittlungsstelle des GSM-Netzes. Einem MSC sind mehrere festgelegte BSCs, die eine so genannte Location Area (LA) umfassen werden zugeteilt. Jedem MSC ist eine Datenbank namens Visitor Location Register (VLR) zugeordnet.

#### 4.5.1.4 Visitor Location Register

Im VLR werden Informationen zu den temporären Teilnehmern die sich in der LA der MSC befinden gespeichert. Dazu gehören der Location Area Identifier (LAI), der ein näher bestimmtes geographisches Gebiet bestimmt. Weiterhin erhält der Mobilfunkteilnehmer eine temporäre Teilnehmerkennung (TMSI). Diese temporäre Kennung wird aus Sicherheitsgründen zum Verbindungsaufbau anstatt der IMSI genutzt. Wird die LA verlassen wird von dem nächsten zuständigen VLR eine neue TMSI erzeugt und mit der IMSI in der Datenbank gespeichert. Die TMSI und ist nur in einer LA gültig und beim verlassen der LA werden alle gespeicherten Daten aus dem VLR gelöscht.

#### 4.5.1.5 Home Location Register / Authentification Center

Dem Home Location Register (HLR) sind alle Teilnehmerdaten, wie Anschrift, Name, IMSI bekannt und dort fest gespeichert. Auch temporäre Informationen, wie das VLR und das MSC und Daten zu Verschlüsselung und Authentifikation sind dort gespeichert. Das HLR ist meist zusammen mit dem Authentification Center untergebracht. Im AuC werden die Schlüssel für die Authentifikation und Chiffrierung erzeugt. Der geheime Teilnehmerschlüssel $K_i$ der im SIM gespeichert ist, ist nur noch dem AuC bekannt.

### 4.5.2 Die Sicherheitskonzepte des GSM-Netzes

Das Sicherheitskonzept von GSM umfasst die Zugangskontrolle in das Netz für Nutzer und ME, eine Authentifikation und eine Verschlüsselung der Kommunikation. Eine Verschlüsselung der Kommunikation ist notwendig, da sich die Funkwellen unkontrolliert ausbreiten und somit jeder sie empfangen kann. Die Identität der Nutzer ist im gewissen Sinne gewahrt, denn Informationen über die Identität sind nur im HLR und AuC gespeichert, für die MSCs werden nur temporäre Daten genutzt.

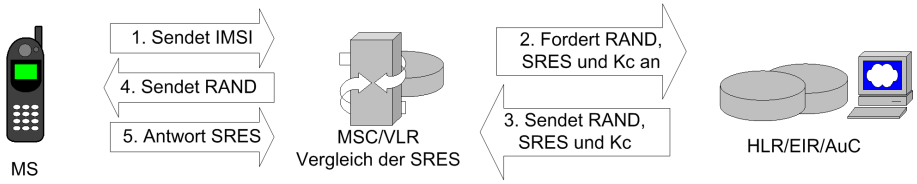


Abbildung 4.8: Die Challenge-Response-Verfahren bei Einbuchung

#### 4.5.2.1 Zugangskontrolle

Um die Gebührenabrechung für jeden Mobilfunkteilnehmer korrekt erstellen zu können, ist es nötig, dass dieser sich dem Netz identifiziert. Mit der Eingabe der PIN (Personal Identify Number) beim Anmelden des ME in das Netz identifiziert sich der Nutzer gegenüber dem Betreiber. Wird die PIN dreimal falsch eingegeben wird, kann das SIM nur durch den Pin Unlocking Key (PUK) wieder entsperrt werden. Wird diese zehnmalig falsch eingegeben ist das SIM gesperrt und damit unbrauchbar.

#### 4.5.2.2 Authentifizierung

Ist die Eingabe der PIN korrekt, versucht sich die MS in das Netz einzubuchen. Dies geschieht durch eine Verbindung mit dem BSC, welches weiter in das MSC vermittelt. Hier kann die Authentisierung des Teilnehmers erfolgen. Mit Hilfe des Algorithmus A3, der MS und AuC bekannt sind geht dies von statten. (Abb. 4.8) Das MSC fordert die MS auf die IMSI unverschlüsselt an das AuC zu übertragen. Im AuC wird mit einer 128-bit Zufallszahl (RAND) und dem geheimem Schlüssel $K_i$ durch den Algorithmus A3 das 32 bit lange Session Result (SRES) erzeugt. Parallel wird mit den Algorithmus A8 der 64 bit lange Sessionschlüssel $K_c$ generiert. Die Ergebnisse $K_C$, SRES und RAND werden an die MSC gesendet. Nur RAND wird an die MS weitergeleitet. Dort wird mittels dem Algorithmus A3 dem geheimen Schlüssel $K_i$ und RAND SRES errechnet. Durch den Algorithmus A8 ist nun auch dem ME der Sessionschlüssel $K_c$ bekannt. Die MS sendet den errechnete SRES an die MSC, wo er mit dem SRES des AuC verglichen wird. Dieses einseitige Challenge-Response-Verfahren ist ein symmetrisches Authentifizierungsverfahren und kann auch bei Location Updates oder beim Verbindungsaufbau gefordert werden. Die Algorithmen A3 und A8 sind nicht im GSM-Standard spezifiziert. Sie sind also von Netzbetreiber zu Netzbetreiber unterschiedlich implementiert.

#### 4.5.2.3 Verschlüsselung

Nach erfolgter Authentifizierung wird von dem MSC ein Signal an die MS gesendet und damit der MS signalisiert, dass ab jetzt die Kommunikation verschlüsselt wird. Der verwendete Verschlüsselungsalgorithmus heißt A5 und der Schlüssel ist der berechnete Wert $K_C$. A5 ist ein Stromchiffreverfahren. Im Gegensatz zu einem Blockchiffreverfahren ändert sich im Ergebnis nur ein Bit, wenn sich jeweils die Eingangsvektoren um ein Bit ändern. Bei Blockchiffren ist jedes Bit von Ausgang abhängig von jeden Bit des Eingangsvektoren. Damit sind Blockchiffreverfahren sicherer als Stromchiffreverfahren.

Die Verschlüsselung findet nur auf der Funkschnittstelle statt.

Es gibt verschiedene Varianten des Algorithmus' A5. Bei der Variante A5/0 findet gar keine Verschlüsselung statt. A5/2 ist die Variante, die in den nordamerikanischen GSM-Netzen eingesetzt wird. Sie ist schwächer als der europäische Algorithmus A5/1.

Man versuchte nach dem Motto "Sicherheit durch Geheimhaltung", diese Algorithmen zu schützen. Es ist aber gelungen den Algorithmus rekonstruieren.

### 4.5.3 Kritik zur Sicherheit von GSM-basierten Netzen

Die Verfahren zu Verschlüsselung und Authentifikation sind nicht veröffentlicht worden. Diese Daten wurden nur den Herstellern von Mobiltelefonen und den Mobilfunkbetreibern zugängig gemacht. Dieses Verfahren nach dem Motto 'security through obscurity' hat noch nie funktioniert, auch in diesem Falle nicht.

Wie schon erwähnt wurde der Algorithmus A5 rekonstruiert und zumindest theoretisch gebrochen. Für die Chiffreverfahren A3 und A8, die in dem SIM untergebracht sind verwendeten einige Mobilfunkbetreiber den Algorithmus COMP128. Mittels der Brute-Force-Methode war es möglich den geheimen Schlüssel $K_i$ auszulesen. Da die IMSI auch leicht zu ermitteln ist, war es möglich Kopien von SIMs zu erstellen. Da aber inzwischen die Algorithmen gewechselt wurden, ist ein Brechen der Authentisierung ist zurzeit nicht mehr möglich.

Des Weiteren ist die Schlüssellänge von $K_c$ mit 64 bit zu kurz gewählt. Ein Kompromittieren des Schlüssels ist mit der Brute-Force-Methode durchaus realistisch.

Durch den Einsatz eines Stromchiffreverfahrens ist die Integrität der über die Funkschnittstelle übertragenden Daten nicht gesichert.

Die Authentifikation ist nur einseitig, die BTS muss sich nicht gegenüber der MS authentifizieren. Ein Man-in-the-Middle-Angriff kann dies ausnutzen. Der so

genannte IMSI-Catcher gibt sich als BTS aus und die MS bucht sich über ihn ein. Der IMSI-Catcher erlaubt es dem MS die Verschlüsselung abzuschalten, nun kann das Gespräch abgehört werden. Der Betrieb eines IMSI-Catcher ist in Deutschland nur den Strafermittlungsbehörden und dem Geheimdienst vorbehalten. Die Kosten eines solchen Gerätes belaufen sich um ca. 10 - 20.000 Euro.

### 4.5.4 Fazit

Die Authentisierung und Verschlüsselung sind auf unabhängiger Hardware untergebracht. Die Verschlüsselung findet in der mobilen Station und die Authentisierung im SIM statt. Diesen Vorteil konnten die Mobilfunkbetreiber schon ausspielen. Denn als der hinter den Authentisierungsalogrithmen A3 und A8 befindliche COMP-Algorithmus gebrochen wurde, konnten die SIMs und damit die Authentisierungsalogrithmen getauscht werden. Weiterhin ist bei GSM ist die geforderte Anonymisierung des Nutzers, durch Erteilen der TMSI gut implementiert. Der Integritätsschutz ist hingegen nur mittels Stromchiffre gewährleistet, so dass eine Veränderung von Daten auf der Luftschnittstelle zumindest theoretisch möglich wäre. Der Verschlüsselungsalgorithmus A5 ist bekannt und kann theoretisch gebrochen werden. Dass die Lücke in der Authentisierung genutzt werden kann, um die Verschlüsselung auszuschalten, ist unwahrscheinlich, da der Betrieb eines IMSI-Catchers ist in Deutschland verboten und kostspielig ist.

## 4.6 UMTS

UMTS (Universal Mobile Telecommunications System) ist nach dem GSM-System und den analogen Mobilfunknetzen der Achtziger Jahre des letzten Jahrhunderts die dritte Generation des Mobilfunks. Das Ziel des GSM-Netzes war es, dem Nutzer Sprachkommunikation überall zu vertretbaren Preisen verfügbar zu machen. Dies ist auch ein Ziel des UMTS-Netzes, aber weiterhin soll die breitbandige Übertragung von Bilder, Video und Daten auch unterstützt werden. UMTS bietet eine Übertragung von 384 kbit/s bis zu 2 mbit/s, aber auch Dienstklassen mit einer geringeren Übertragungsrate von 16 Kbit/s und weniger. Auch die Mobilität wurde beim Entwurf von UMTS berücksichtigt. Bei bis zu 500 km/h sind Übertragungsraten von bis zu 144 kbit/s möglich.

Die Luftschnittstelle von UMTS ist universell, sie bietet eine Integration der verschiedensten Funksysteme an. So soll teilweise die Kommunikation von der MS nicht nur zu Funkmasten, sondern auch zu Satelliten möglich. Die Funkschnitt-

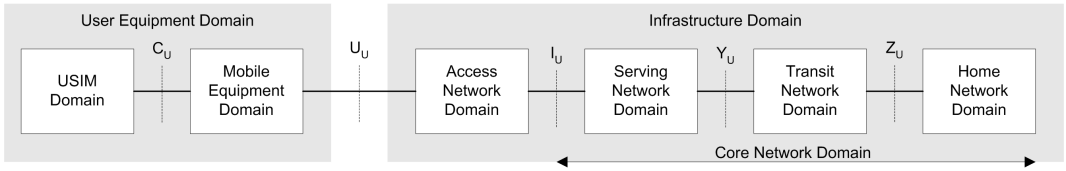


Abbildung 4.9: Die Domainstruktur vom UMTS

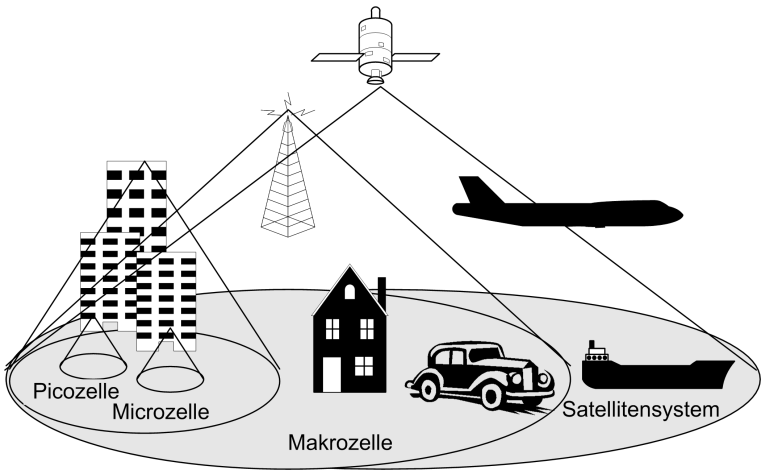


Abbildung 4.10: Die Granularität vom UMTS

stelle wird eine anderes Multiplexverfahren als GSM nutzen. Beim GSM-System wurde ein Verfahren eingesetzt, dass auf Zeit- und Frequenzmultiplex aufbaut. UMTS nutzt ein Codevielfachzugriffsverfahren W-CDMA (Wideband Code Division Multiple Access), welches eine 5 - 7fach höhere spektrale Effizienz hat und somit die knappe Ressource Frequenzspektrum besser ausnutzt.

### 4.6.1 Aufbau und Struktur von UMTS

Das UMTS-Netz kann grundsätzlich in zwei Teile (Domänen) geteilt werden. (Abb. 4.9) Zum einen die User Equipment Domain, die das Zugangsgerät (Terminal) und die USIM-Karte umfasst. Die Infrastructure Domain umfasst das Trägernetz, in welchen Verbindungsmanagement und Abrechnung stattfinden. Die Schnittstelle $U_U$ ist bei UMTS so ausgelegt, dass ein weltweites Roaming möglich ist. Deshalb wurde auch die Einbindung der satellitengestützten Kommunikation im Standard vollzogen.

Wie das GSM-Netz hat auch das UMTS-Netz eine zelluläre Struktur. (Abb. 4.10) Waren bei GSM die Dienstgüten in allen Zellen gleich, werden bei UMTS Un-

terschiede gemacht. So werden 'Hot Spots', Orte mit hoher Nutzerfrequentierung, wie Bahnhöfe oder Flughäfen von einer oder mehreren Pikozellen abgedeckt, bei denen eine maximale Übertragungsrate vom 2 mbit/s möglich ist. Aufgrund des Dopplereffektes ist bei dieser Übertragungsrate nur eine maximale Bewegungsgeschwindigkeit von 10 m/s vorgedehen. Die Mikrozelle wird Bereiche von mehreren Quadratkilometern versorgen können. Allerdings ist hier die Übertragungsrate maximal 384 kbit/s bei maximal 120 km/h. Die Makrozelle deckt etwa die die Fläche einer Großstadt ab. Der Einsatz wird aber in den ländlichen Regionen mit einer nicht so hohen Nutzerdichte geplant. Die Bandbreite wird hier maximal 144 kbit/s bei maximal 500 km/h groß sein. Die Gebiete, bei denen es sich für den Betreiber der Netzes nicht lohnt Investitionen in die terristische Infrastruktur zu tätigen werden via Satellit abgedeckt. Hier wird eine Bandbreite von 144 kbit/s garantiert.

Das eigentliche UMTS Trägernetz besteht aus dem Core Network (CN). (Abb. 4.9) Die Aufgaben des CN sind mit denen des NSS (siehe Kapitel 4.5.1) zu vergleichen. Da im UMTS-Netz auch paketvermittelter Datenverkehr verwaltet wird, sind zusätzlich zum NSS folgende Dienste nötig:

- Serving GPRS Support Node (SGSN) Der SGSN leitet bei paketvermittelnden Diensten die Verbindung zur Mobilstation weiter.

- Gateway GPRS Support Node (GGSN) Der GGSN dient als Schnittstelle zu externen Netzen (z.B. Internet).

Das Funknetz von UMTS heißt Universal Terristical Radio Access Network (UTRAN). UTRAN übernimmt innerhalb des Access Network sämtliche Funktionen und Protokolle, die zur Datenübertragung und zur Sicherheit notwendig sind. Es stellt somit die Verbindung zwischen dem Trägernetz und der Mobilstation dar. Das UTRAN ist aus mehreren Subnetzen, den so genannte Radio Network Subsystems (RNS), zusammengesetzt, denen wiederum Radio Network Controller (RNC) und Basisstationen zugeteilt sind. Der RNC ist für die eigentliche Funkübertragung zuständig.

### 4.6.2 Sicherheitsarchitektur

Abbildung 4.11 zeigt die UMTS Sicherheitsarchitektur mit HE (Home Environment), SN (Serving Network) und AN (Access Network). Die fünf Sicherheitsbereiche, die im Standard definiert sind, sind folgende:

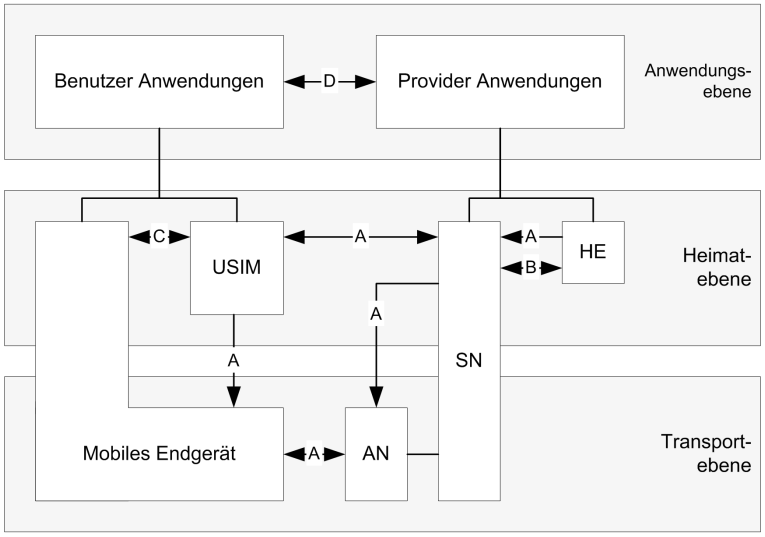


Abbildung 4.11: Die Sicherheitsarchitektur vom UMTS

- A) Netzzugangssicherheit
- B) Sicherheit im Netzwerkbereich
- C) Sicherheit im Benutzerbereich
- D) Sicherheit im Anwendungsbereich
- E) Sichtbarkeit und Konfigurierbarkeit der Sicherheitsmechanismen

#### 4.6.2.1 Netzzugangssicherheit (A)

Dieser Bereich ist für den sicheren Zugang zu den Diensten von UMTS zuständig. Die Achillesferse jedes Netzes ist die Luftschnittstelle, da sich die Funkwellen unkontrolliert ausbreiten und somit einfach abgehört werden können ist hier eine gute Sicherheitsimplementation zum Schutz der Funkschnittstelle notwendig. Im Folgendem werden die Sicherheitseigenschaften der Netzzugangssicherheit vorgestellt. :

**Vertraulichkeit der Benutzeridentität:** Jedem Benutzer wird vom Anbieter eine permanente Benutzeridentität (International Mobile Subscriber Identity IMSI) zugewiesen. Das Mitlauschen der Identität an der Luftschnittstelle und ein Rückführen der Daten auf den Benutzer muss verhindert werden. Weder der Aufenthaltsort (user location confidentiality) noch der Benutzer (user identity

confidentiality) dürfen von einem Angreifer bestimmt werden können. Die Nutzung eines Dienstes muss anonymisiert geschehen. Es darf nicht die Möglichkeit bestehen die Nutzung eines Dienst einem Nutzer zuordnen zu können. (user untraceability).

**Authentifizierung der Instanzen:** Die Authentifizierung muss vom Nutzer als auch vom Betreiber geschehen. Dadurch wird sichergestellt, das der Benutzer auch wirklich mit dem Serving Network verbunden ist, mit dem er sich verbinden möchte.

**Vertraulichkeit der Daten:** Die Einigung über den Verschlüsselungsalgorithmus (cipher algorithm agreement) zwischen dem Serving Network und der Mobilstation muss auf einem sicheren Wege geschehen können. Die Generierung eines gemeinsamer Übertragungsschlüssels, sollte nicht nur zum Beginn den Verbindungsaufbaus vollzogen werden. Bei sehr langen Verbindungszeiten, sollte dies auch nach einer bestimmen Zeiten geschehen. (cipher key agreement). Logischer Weise sollte gewährleistet werden, dass weder Daten noch Signalisierungsdaten abgehört werden können.

**Datenintegrität** Auch der Integritätsschlüssel und der Integritätsalgorithmus sollten auf sicherem Weg ausgehandelt werden können. Es muss dem Serving Network als auch der Mobilstation möglich sein, die empfangenen Daten auf Herkunft und Integrität zu überprüfen.

#### 4.6.2.2 Sicherheit im Netzwerkbereich (B)

Auch im drahtgebundenen Netzbereich ist es erforderlich, dass die Instanzen sich gegenseitig authentifizieren. Auch die Vertraulichkeit und die Integrität sowohl der Nutzdaten als auch der Signalisierungsdaten zu sichern. Die Sicherheitsarchitektur sollte auch den in Kapitel 4.6.2.1 vorgestellten Punkten genügen.

#### 4.6.2.3 Sicherheit im Benutzerbereich (C)

Die Sicherheit im Benutzerbereich betrifft die Authentisierung des Nutzers gegenüber der Mobilstation und dem User Subscriber Identity Module (USIM). Dies wird mittel eines gemeinsamen Geheimnisses erfolgen. In dem USIM ist dies Geheimnis gespeichert. Will der Nutzer des Gerät benutzen gibt er eine PIN oder ein Passwort ein, wenn dies richtig ist, kann er das Gerät und somit die Dienste nutzen. Um eine unrechtmäßige Nutzung des mobilen Gerätes mit anderen USIMs

zu vermeiden ist eine Authentisierung der USIM gegenüber dem mobilen Gerät auch im Standard vorgesehen.

#### 4.6.2.4 Sicherheit im Anwendungsbereich (D)

Um dies zu Gewährleisten muss nicht nur die Funkschnittstelle verschlüsselt werden, sondern es muss eine Ende-zu-Ende Verschlüsselung zwischen der Anwendung im Providerbereich der Benutzerumgebung stattfinden. Dafür steht den Providern eine standardisierte, virtuelle Ausführungsumgebung für mobile Geräte, welche auf Personal Java basiert zur Verfügung. Diese Umgebung ist auf jedem mobilen Gerät für UMTS implementiert. Das Hinzufügen einer Anwendung auf eine MS kann nur geschehen, wenn diese digital signiert ist. Eine digitale Signatur erhalten nur Programme die die Sicherheit nicht beeinträchtigen.

#### 4.6.2.5 Sicht- und Konfigurierbarkeit der Sicherheit (E)

Es muss dem Nutzer derzeit möglich sein den Sicherheitsstatus seiner genutzten Anwendungen zu erfahren. Er muss informiert werden, wenn eine Anwendung bestimmten Sicherheitslevel fordert oder eine Anwendung keine Verschlüsselung bietet.

Folgende Sicherheitseigenschaften werden verwendet :

**Sichtbarkeit**

- Anzeige der Netzzugangsverschlüsselung
- Anzeige der netzweiten Verschlüsselung
- Anzeige des Sicherheitslevels

**Konfigurierbarkeit**

- Freigeben/Verhindern der Benutzer-USIM-Authentikation
- Akzeptanz/Abweisung von ankommenden unverschlüsselten Verbindungen
- Aufbau oder kein Aufbau von unverschlüsselten Verbindungen
- Akzeptanz/Abweisung eines Verschlüsselungsalgorithmus

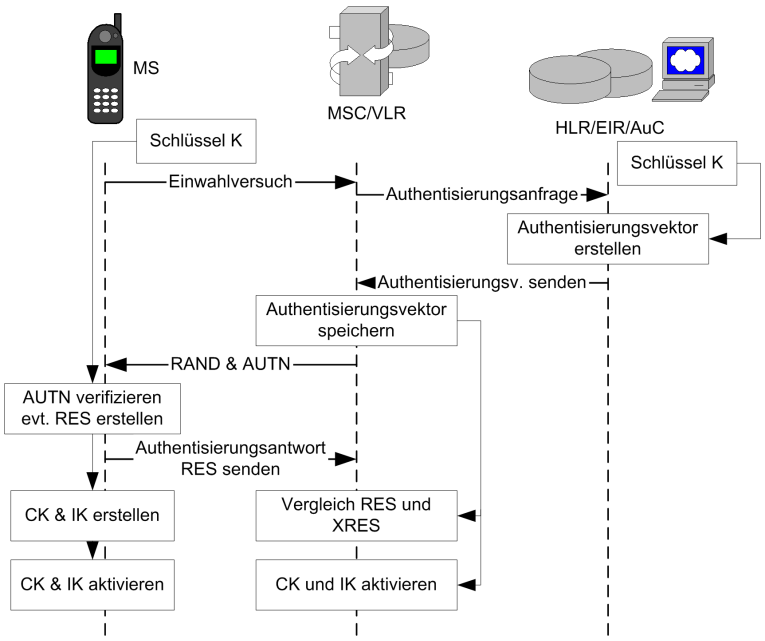


Abbildung 4.12: Authentifikation und Schlüsselzuweisung

### 4.6.3 Sicherheitsmechanismen

Die Realisierung der Sicherheitseigenschaften wird in diesem Kapitel beschrieben. Es erfolgt ein Überblick über die wichtigsten Mechanismen der Funkschnittstelle. Alle Sicherheitsmechanismen zu beschreiben würde den Rahmen dieser Arbeit sprengen.

#### 4.6.3.1 Authentifikation und Schlüsselzuweisung

Um eine Authentifikation zwischen Nutzer und Netz durchzuführen, wird auch bei UMTS auf die Methode des gemeinsamen Geheimnisses zurückgegriffen. Der geheime Schlüssel ist nur im USIM und AuC gespeichert. Um eine vollkommenem Authentifikation auszuführen wurde das Challenge-Response-Verfahren etwas verändert. Es wurde um das sequenznummerbasierte Einweg-Protokoll für Netzwerk-Authentifizierung ISO/IEC 9798-4 erweitert. Die Autorisierung des Netzes gegenüber der MS geschieht mittels des Authentisierungstokens AUTN.

Nach dem Empfang eine Authentifizierungsanforderung am VLR sendet das AuC einen Authentifizierungsvektor an das VLR (Abb. 4.12). Ein Authentifizierungsvektor besteht aus folgenden Komponenten: einer Zufallszahl RAND (128 bit), der erwarteten Antwort XRES, einem Itegritätsschlüssel IK (128 bit) und einem Authentifizierungstoken (64 bit). Jeder Authentifizierungsvektor ist nur

einmal gültig. Die Felder RAND und AUTN werden vom VLR nun an die MS gesendet. Die MS prüft mittels des gemeinsamen Geheimnisses (Schlüssel K) die AUTN, wenn sie diese akzeptiert errechnet sie die Antwort RES und sendet diese an das VLR. Gleichzeitig errechnet die MS den Verbindungsschlüssel CK und den Itegritätsschlüssel IK (jeweils bis zu 128 bit lang). Im VLR wird der von der MS empfangene RES mir den XRES des AuC verglichen. Ist dies korrekt ist die Authentifikation und Schlüsselzuweisung vollzogen und die Schlüssel werden von USIM und VLR aktiviert.

Die genaue Beschreibung des Ablaufes der Authentifikation zwischen MS und VLR, dem VLR und AuC und die Berechnung der Schlüssel, bei der 5 verschiedene Algorithmen eingesetzt werden, würde den Rahmen dieser Arbeit sprengen. Der geneigte Leser sei auf [3GPP] verwiesen.

#### 4.6.3.2 Verschlüsselung

Nach vollzogener Authentifikation und Schlüsselzuweisung wird der Nachrichtenaustausch mit dem Schlüssels CK verschlüsselt.

Die ETSI hat von den Fehlern im Standard GSM gelernt und die verwendeten Verschlüsselungsalgorithmen veröffentlicht. Damit werden die Algorithmen schon vor dem Start des UMTS-Netzes getestet und der Schaden bei Bruch der Verschlüsselung ist nicht so groß, als wenn die Algorithmen später geändert werden müssten, wenn die MS schon beim Kunden sin.

#### 4.6.3.3 Integritätsschutz

Mit Hilfe des Itegritätsschlüssels IK wird jeder Nachricht ein MAC-Feld (Message Authentication Code) angehängt. Mit Hilfe des MAC ist es dem Empfänger möglich die Integrität der Nachricht, als auch die Authentizität des Sender zu verifizieren.

#### 4.6.3.4 Identitätsschutz

Wie auch im GSM-Netz wird jeden Nutzer eine eindeutige IMSI, von Netzbetreiber zugewiesen. Während des Kommunikationsaufbaus wird für den Nutzer im VLR anhand der IMSI eine TMSI vereinbart. Diese ist so lange gültig, wie die Kommunikation anhält und er das geographische Gebiet, das dem VLR zugeordnet ist nicht verlässt. Wird das Gebiet verlassen, oder die Kommunikation beendet wird die TMSI im VLR gelöscht. Der Nutzer ist für alle Dienste nur über

die TMSI ansprechbar und alle Dienstnutzungen sind für ihn zuordbar.

### 4.6.4 Fazit

Da man eine Kompatibilität zwischen dem UMTS- und GSM-Netz erschaffen wollte, um Verfahren die sich bewährt hatten und Teile der bestehenden Infrastruktur weiter zu nutzen, wurden auch bei den Sicherheitsmaßnahmen einige Mechanismen übernommen. Die Schwachpunkte der Sicherheitstruktur von GSM wurden verbessert und es wurden wichtige Sicherheitsfeatures hinzugefügt.

Ein Schwachpunkt vom GSM war es, dass sich das Netz gegenüber dem Nutzer nicht authentifizieren muss. Dies wurde bei UMTS behoben.

Die Einbindung neuer Dienste ist nur mittels digitalen Zertifikaten möglich. Damit wird es Schadanwendungen unmöglich gemacht Daten auf der MS aus nicht autorisierten Speicherbereichen auszulesen und in diese zu schreiben.

Die Schlüssellänge zur Datenchiffrierung wurde bei UMTS auf 128 bit vergrößert. Bei GSM betrug diese Länge nur 64 bit. Des weiteren ist es bei UMTS möglich den Übertragungsschlüssels während der Kommunikation zu erneuern.

Bei UMTS wurde auch eine Intergritätssicherung der zu übertragene Daten eingeführt.

Die Verschlüsselungsalgorithmen sind veröffentlicht und wurden so entworfen, dass die Schwachstellen gebrochener Algorithmen berücksichtigt wurden.

Zurzeit ist noch keine Lücke in der Sicherheitsarchitektur oder den Verschlüsselungsalgorithmen von UMTS bekannt.

# Kapitel 5

# BEWERTUNG DER TECHNOLOGIEN

Um eine Bewertung der Technologien durchzuführen, ist es von Vorteil, wenn dies mit Hilfe bestimmter praktischer Szenarien geschehen kann. Dadurch ist eine leichtere Vergleichbarkeit mit dem späteren Einsatzgebiet der Technologie gewährleistet.

## 5.1 Klassifizierung der Einsatzszenarien

Laut BSI kann man bei der Bewertung biometrischer Technologien und drahtlosen Zugangsystemen zwischen vier verschiedenen Sicherheitsklassen mit aufsteigender Sicherheit unterscheiden.

### 5.1.1 Sicherheitsklasse 1

Die Sicherheitsklasse 1 ist die Klasse mit dem geringsten Schutzbedarf. Es handelt sich um beispielsweise einen PC für den Privatgebrauch. Auf diesem Rechner sind private Bilder und Dokumente (Briefe zu Behörden, private Briefe) gespeichert. Diese Daten haben für den Besitzer einen ideellen Wert. Ein Verlust dieser Daten würde kaum zu finanziellen Verlusten oder Imageschäden führen. Bei allen Szenarios, die der Sicherheitsklasse 1 zugeordnet sind, sind eventuelle Schadensauswirkungen begrenzt und überschaubar.

### 5.1.2 Sicherheitsklasse 2

Die Sicherheitsklasse 2 hat einen höheren Schutzbedarf. In diese Klasse fallen durch Firmen genutzte Computer. Die Server fallen nicht in diese Klasse, sondern nur die Computerarbeitsplätze. Der typische Büro-PC mit nur wenigen Nutzern ist ein exemplarisches Beispiel für die Klasse 2. Ein Datenverlust, oder die gezielte Veränderung von Daten kann zu absehbaren finanziellen Einbußen und Imageschäden führen.

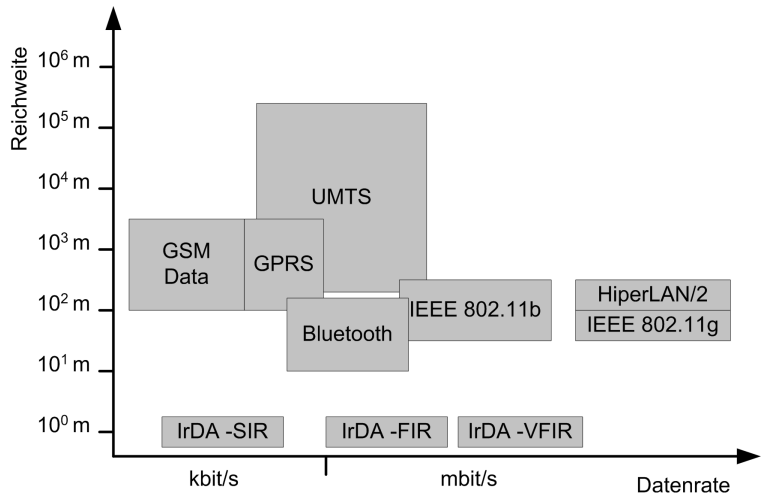


Abbildung 5.1: Überblick über drahtlose Zugangsysteme

### 5.1.3 Sicherheitsklasse 3

Der Sicherheitsklasse 3 werden Rechner mit vielen Nutzern zugeordnet. Diese Rechner sollten in gesicherten Umgebungen untergebracht sein. Die Kameraüberwachung bei Bankautomaten oder spezielle Räume für Server sind Beispiele für eine Sicherung. Ein Datenverlust, oder die gezielte Veränderung von Daten kann schon zu immensen finanziellen Verlusten und Imageschäden führen.

### 5.1.4 Sicherheitsklasse 4

Zur Sicherheitsklasse 4 zählen alle Anwendungen, bei denen ein Schadensfall ein existentiell bedrohliches, katastrophales Ausmaß erreicht. Beispiele wären Rechenzentren von Banken oder Atomkraftwerke.

## 5.2 Vergleich der Zugangstechnologien

Abbildung 5.1 zeigt eine Überblick der vorgestellten Zugangstechnologien bezüglich Reichweite und Datenübertragungsrate. Dort aufgezeigten Nutzungsfelder überschneiden sich nur bei HiperLAN/2 und IEEE 802.11g.

Der Vergleich der Sicherheit der vorgestellten Zugangstechnologien in Tabelle 5.1 stellt nicht nur die einzelne Sicherheitskriterien Vertraulichkeit, Geheimhaltung, Integrität, Authentifikation und Autorisierung dar. Auch Kriterien, wie Reichweite, Datenübertragungsrate und Marktverfügbarkeit werden betrachtet.

Die Kriterien im Einzelnen sind:

| Technologie | IrDA | Bluetooth | IEEE 802.11 | HiperLAN/2 | GSM/GPRS | UMTS |
|---|---|---|---|---|---|---|
| Reichweite (m) | 1 | 10/100 | 30/150 | 30/150 | 300/4000 | 100/weltweit |
| Datenübertragungsrate(mbit/s) | 0,115/4/16 | 1 | 11/54 | 54 | 0,115 | 2/0,144 |
| Verfügbarkeit | ja | ja | ja | nein | ja | im Aufbau |
| Verschlüsselung | ○ ○ ○ | ● ● ● | ● ○ ○ | ● ● ● | ● ● ○ | ● ● ● |
| Integrität | ○ ○ ○ | ● ○ ○ | ● ○ ○ | ● ● ● | ● ● ○ | ● ● ○ |
| Authentifikation | ○ ○ ○ | ● ● ○ | ● ○ ○ | ● ● ○ | ● ● ○ | ● ● ● |
| Zugangskontrolle, Autorisierung | ○ ○ ○ | ● ● ○ | ● ○ ○ | ● ● ○ | ● ● ○ | ● ● ○ |
| Anonymisierung | ○ ○ ○ | ○ ○ ○ | ● ○ ○ | ○ ○ ○ | ● ● ● | ● ● ● |
| Sicherheitklasse (nach BSI) | 1 | 2 | 1 | 2 | 2 | 3 |

○ ○ ○ nicht implementiert ● ○ ○ zu schwach, kompromitierbar ● ● ○ ausreichend ● ● ● sicher

Tabelle 5.1: Vergleich der Zugangsysteme

- Reichweite: Maximaler Abstand der MS und der Basisstation oder zweier MS in Meter
- Datenübertragungsrate: Maximale Brutto-Datenübertragungsrate eines Kommunikationskanals der entsprechenden Technologie.
- Verfügbarkeit: Sind Geräte auf dem Markt verfügbar, die die Technologie unterstützen.
- Verschlüsselung: Stärke der eingesetzten kryptografischen Verfahren gegen das Abhören der Kommunikation.
- Integrität: Wurden ausreichend gesicherte Verfahren eingesetzt, die eine willentliche Änderung der übertragenen Nutzdaten durch Dritte erkennen oder verhindern können.
- Authentifikation: Wie gut sind die Verfahren zur gegenseitigen Feststellung der Identität der Kommunikationspartner ?
- Zugangskontrolle, Autorisierung: Sind Verfahrensweisen implementiert, die nicht Berechtigten die Nutzung unterbindet.
- Anonymisierung: Können Bewegungsprofile erstellt werden. Sind Funktionalitäten implementiert, die es einem Teilnehmer ermöglichen anonym aufzutreten.

Die Sicherheit von IrDA erscheint auf den ersten Blick nicht sehr stark zu sein. IrDA ist aber die einzige drahtlose Zugangstechnologie, deren Sendestrahlung sich nicht unkontrolliert ausbreitet. Da auch die Reichweite relativ gering ist, sind die

Chancen für einen Angreifer relativ gering die Kommunikation zu kompromitieren.

Von den anderen Zugangstechnologien sticht UMTS mit einer sehr starken Sicherheitsarchitektur hervor. Sie baut auf die GSM-Sicherheitsarchitektur auf und verbessert diese in den entdeckten Lücken. Da der flächendeckende Einsatz von UMTS sich noch im Aufbau befindet können noch keine Ergebnisse der Sicherheitsuntersuchung in der Praxis vorgestellt werden.

Der HiperLAN/2-Standard hat eine viel bessere Sicherheitsarchitektur als sein Konkurrent IEEE 802.11. Auch die direkte Unterstützung der QoS-Faktoren von ATM und UMTS sind hier implementiert. IEEE 802.11 bietet dies nicht an. Trotz dessen ist es kritisch, ob sich für diesen Standard Produzenten finden, die HiperLAN/2 in ihren Produkten einsetzen.

Ein weiteres Problem von Bluetooth, IEEE 802.11 und HiperLAN/2 ist es, dass die Nutzung der angebotenen Sicherheitsfunktionen, wie Verschlüsselung oder Authentisierung nicht zwingend vorgeschrieben ist. Die Verwendung dieser Funktionen bleibt dem Nutzer überlassen, der schon meist mit der Konfiguration der Endgeräte überfordert ist und eine Aktivierung der Sicherheitsfunktionen dann unterlässt. Selbst wenn Verschlüsselung verwendet wird, muss beispielsweise bei Bluetooth sichergestellt werden, dass der Schlüssel (PIN) eine ausreichende Länge besitzt.

Eine Homogenisierung der Sicherheit aller Zugangssysteme kann auf Netzwerk- und Transportschicht mittels IPSec/VPN und SSH gewährleistet werden, denn die implementierten Sicherheitsfunktionen der vorgestellten Zugangsysteme können bis auf UMTS und teilweise GSM nicht die Anforderungen an eine hochsichere Kommunikation erfüllen.

## 5.3 Vergleich der biometrischen Verfahren

In Tabelle 5.2 sind die vorgestellten biometrischen Verfahren nach folgenden Kriterien verglichen:

- Einzigartigkeit des zur biometrische Identifikation genutzten Merkmals in dem Sinne, dass verschiedene Personen ausreichend unterscheidbare Merkmalsausprägungen besitzen.

- Die Konstanz eines biometrisches Merkmals sollte sich im Laufe des Lebens nicht stark ändern, um zur Wiedererkennung und damit zur Nutzung in einem biometrischen Verfahren verwendet werden zu können.
- Verfügbarkeit: Möglichst viele Personen sollten das zur biometrischen Erkennung genutzte Merkmal besitzen, dass weiterhin eine ausreichender Ausprägung zur Erfassung und Auswertung haben sollte.
- Die Akzeptanz zeigt an, wie hoch die Benutzungsbereitschaft der Nutzer ist. Der Erfassung, Speicherung der Merkmale und das verwendete biometrische Verfahren ist für einige Nutzer mehr oder weniger akzeptabel.
- Kontrollierbarkeit: Möglichkeit zur willentlichen Abgabe oder Nichtabgabe eines biometrischen Merkmals durch den Benutzer.
- Fehlerraten: Fehlerraten (FAR und FRR) im praktischen Einsatz.
- Dauer: Dauer zur erstmaligen Erfassung der biometrischen Daten (Enrolment) und für Wiedererkennung des Nutzers (Verifikation)
- Anzahl der Einzelmerkmale: Anzahl der extrahierten Einzelmerkmale, die zur Unterscheidung zwischen den Nutzern verglichen werden.
- Templategröße: Größe des Referenzmusters.
- Komfort: Gibt an wie hoch der zeitliche Aufwand und die Interaktionsanforderungen sind die an den potentiellen Nutzer gestellt werden.
- Mobilität: Mobilität der Geräte, die für die biometrische Verifikation benötigt werden.
- Sensor: Gerät zur Erfassung der Ausprägungen des biometrischen Merkmals.

Der Einsatz der verschiedenen Verfahren muss von Einsatzszenario zu Einsatzszenario neu entschieden werden. Es gibt keine optimale Lösung für alle Anwendungsfälle, wäre dies der Fall dann würde dieses Verfahren den Markt dominieren.

Die Iriserkennung ist ein Verfahren, bei dem sehr viele relevante Merkmale zum biometrischen Vergleich der Nutzer hinzugezogen werden. Die relevante Anzahl der unterscheidbaren Merkmale bei der Handgeometriemethode ist hingegen relativ gering.

| Verfahren | Finger-abdruck-erkennung | Gesichts-erkennung | Iris-erkennung | Hand-geometrie-verfahren | Sprecher-erkennung | Unter-schriften-erkennung |
|---|---|---|---|---|---|---|
| Einzigartigkeit | ●●●●○ | ●●●○○ | ●●●●● | ●●●●○ | ●●●●○ | ●●●○○ |
| Konstanz | ●●●●○ | ●●●○○ | ●●●●● | ●●●●○ | ●●○○○ | ●●○○○ |
| Verfügbarkeit | ●●●○○ | ●●●●● | ●●●○○ | ●●●○○ | ●●●●○ | ●●●○○ |
| Akzeptanz | ●●●○○ | ●●●●○ | ●●●○○ | ●●●●○ | ●●●●● | ●●●●○ |
| Kontrollierbarkeit der Abgabe | ●●●●○ | ●●○○○ | ●●●●○ | ●●●●○ | ●●●○○ | ●●●●● |
| Fehlerrate (%) | | | | | | |
| FAR | 0,01-0,001 | 0,5-2,0 | 0,01-0,1 | 0,1-5,0 | 0,1 | 1,6-20 |
| FRR | 1,0-5,0 | 1,0-3,0 | <0,1 | 0,2-5,0 | 0,01 | 2,8-25 |
| Dauer (sec) | | | | | | |
| Enrolment | <2 | 0,1-60 | <30-120 | <5 | 180 | 30 |
| Verifikation | <1 | 3-4 | 2 | 2-5 | 0,5-5 | 5-15 |
| Anzahl der Merkmale | 8-12 | k.A. | 266 | 90 | 300-2000 | bis zu 500 |
| Templategröße | 900-1.200 | <1300 | <512 | 10-20 | 1.500-3.000 | 400-1500 |
| Komfort | ●●●●○ | ●●●●● | ●●●●● | ●●●○○ | ●●●○○ | ●●●○○ |
| Mobilität | ja | ja | ja | nein | ja | ja |
| Sensor | CCD-Chip, kapazitiv, Ultraschall | SW-Kamera | SW-Kamera | SW-Kamera | Mikrofon | druckempf. Schrebpad |

Tabelle 5.2: Vergleich der Biometrischen Verfahren

Der Kostenfaktor für die Einführung eines biometrischen Verfahren spielt auch eine große Rolle und ist vom Einsatzgebiet abhängig. So ist es nicht effektiv ein relativ teures Iriserkennungssystem an jede Tür eines Hochsicherheitsbereiches zu installieren. Ein kombiniertes System bestehend aus einem Iriserkennungsystem zum Betreten des Hochsicherheitsbereiches und im Weiteren relativ günstige Fingerprintsensoren an den Türen innerhalb diese Bereiches wären eine kostengünstigerer Alternative.

# Kapitel 6

# FIRMEN

Die im Folgenden aufgelisteten Firmen haben im Bereich Biometrik respektive Zugangssysteme zumindest eines ihrer Geschäftsfelder. Ob eine dieser Firmen eine credentialbasierte Lösung entwickelt oder anbietet war nicht in Erfahrung zu bringen.

Die Firma **HID Corporation Limited** (http://www.hidcorp.com) befasst sich mit Lösungen für Smartcards, die berührungslos gelesen und beschrieben werden können. In Zusammenarbeit mit der Firma BioScrypt (www.bioscrypt.com) wurde deren Fingerabdruckerkennungssystem mit den Smartcards kombiniert. Die SmartCards nehmen die biometrischen Referenzinformationen des Nutzers auf. Damit sind die Daten in der Hand des Nutzers und damit in seiner Kontrolle. Weitere Produkte sind ein Gesichtserkennungssystem und ein Iriserkennungssystem in Kombination mit der berührungslosen SmartCard.

Die Firma **XYLO.concept GmbH** (http://www.xyloconcept.de) stellt Zugangsysteme her. Das Produkt XYLO.blue ACCESS, bietet ein Verfahren zur Türöffnung per Handy, das auf der Handy-Technologie mit Bluetooth-Schnittstelle basiert, an. Ein Fingerprintsensor für die Zugangskontrolle wir auch angeboten. Die Kommunikation der einzelnen Komponenten kann via TCP/IP stattfinden.

**Ident Technologies GmbH** (http://www.identtechnologies.de) Hauptgeschäftsgebiete sind die Entwicklung von Software für Fingerprintsensoren, Datenerfassung, Verarbeitung und Speicherung. Zusammen mir der Firma Döpke Schaltgeräte GmbH & Co. KG. wird eine Komplettlösung für die Zugangskontrolle mit Hilfe eines Fingerprintsensors angeboten. Die Kommunikationsschnittstelle bietet unter anderem Kommunikation nach den Ethernet-Standard an.

**GEZE GmbH** (http://www.geze.com) Die Kernaufgabenfelder dieser Firma sind Türsysteme und Sicherheitstechnik. Eine Komplettlösung zur Zugangskontrolle mittels Fingerprintsensor wird auch angeboten. Die Fingerprintsensoren dieser Lösung kommunizieren nur über die Steuereinheit die maximal 5 Meter

vom Sensor entfernt sein darf. Die Steuereinheit ist Stand-Alone-fähig kann aber auch via Ethernet mit einem Server kommunizieren.

**LÜTH & DÜMCHEN Automatisierungsprojekt GmbH** (http://www.horatio.de/) Softwareentwicklung für Betriebsdaten- und Personalzeiterfassung ist das Geschäftsfeld dieser Firma. Auch für die Zugangskontrolle von Betriebsräumen mittels Gesichtserkennung bietet die Firma eine Softwarelösung, die die typischen Merkmale des Gesichts erfasst, verarbeitet und entscheidet. Als Sensoren können einfache Webcams verwendet werden.

**Biometric Solutions AG** (http://www.biometric-solutions.de) Softwareentwicklung in den Gebieten Zeitdatenerfassung, Zutrittskontrolle und Videoüberwachung sind ein Standbein dieser Firma. Ein tragbares Fingerprinterfassungssystem mit RS232, USB , RJ45- Anschluss und GSM-Modul. Es kann auch als stationäres Modul verwendet werden.

**CONDAS Control- und Datensysteme GmbH** (http://www.condas.de) Identifikationssysteme, Zugangskontrolle, Videodatenüberwachung bietet CONDAS an. Ein Fingerprint-System wird angeboten, welches Verifikation oder Identifikation des Nutzer vornehmen kann. Eine Netzwerkfähigkeit im Erfassungssensor ist mittels RS-486 Bus gewährleistet.

**Kaba Benzing GmbH** (http://www.kaba-benzing.com) - Zeiterfassung, BDE und Zutrittskontrolle. Nutzung der Biometrie zur Zutrittskontrolle mittels des Biometrie-Terminals Bedanet 91 20 Fingerprint - netzwerkfähig mit dem Zutrittsmanagermodul Bedas 92 90.

**Viisage Technology AG** (http://www.viisage.com) Viisages Lösungen basieren auf Dokumenten- und Gesichtserkennungstechnologien und ermöglichen sowohl in 1:1 als auch in 1:n Situationen eine Personenidentifikation. Auch bei der Herstellung von Ausweisdokumenten bietet Viisage seinen Kunden die Möglichkeit, Daten anhand mehrerer biometrischer Merkmale auszuwerten. (Viisage hat die Firma ZN-Vision aufgekauft.)

**PCS Systemtechnik GmbH** (http://www.pcs.com) Zeiterfassung - Betriebsdatenkontrolle - Zutrittskontrolle sind die Geschäftsfelder der Firma. Das verwendete biometrische Verfahren ist die Nutzererkennung mittels des Fingerbildes. Die auf der berührungslos zu lesenden Karte gespeicherten Templates mit den

Fingerabdruck-Merkmalen werden mit den auf den Sensor aufgelegten Finger-Merkmalen verglichen. Die unterstützten Schnittstellen sind TCP/IP und RS485. Der Leser kann nur mit dem Zutrittsmanager direkt kommunizieren.

**Biometrix Int.** (http://www.biometrix.at/) Fingerabdruck- und Gesichts- Erkennungssysteme, Software und Entwicklungstools, Fingerprint-Sensoren und Fingerprint-Terminals sind die Produktfelder von Biometrix.

**Smiths Heimann Biometrics GmbH** (http://www.shb-jena.com/) entwickelt, produziert und vermarktet digitale Bildaufnahmelösungen für polizeiliche, zivile und kommerzielle Finger- und Handabdruckanwendungen weltweit. Das Produktportfolio wird durch intelligente Dokumentenleser ergänzt.

**SD Industries GmbH** (http://www.sd-industries.de) Die Firma bietet unter anderem eine Grenzübergangslösungen für eine sichere und schnelle Ein- und Ausreise zweifelsfreie Identifikation von Dokumenten und Personen an.

Des Weiteren wird eine Multibiometrie-Plattform für die einfache Adaption einzelner Erkennungsmerkmale in ein multibiometrisches Gesamtnetzwerk angeboten.

Auch Biometrische Zutrittskontroll-Systeme für die Zutrittskontrolle sensibler Bereiche und als Zugriffssicherung für IT- und IK-Anlagen mit biometrischen Erkennungssystemen sind Bestandteil der Produktpalette, sowie Match on card für singuläre und multimodale Biometrie auf Smart Cards.

**BioMet Partners Inc.** (http://www.biomet.ch/) Zugangskontrollsysteme basieren auf Fingerbilderkennung. Die Zugangssicherheit soll besser als bei normalen Fingerprint-Systemen sein, da gleichzeitig die biometrischen Daten zweier Finger erfasst und verarbeitet werden.

**DERMALOG Identification Systems GmbH** (http://www.dermalog.de) bietet Hardware und selbst entwickelte Software, sowie Datenbanken und System-Logistik für Fingerprint-Systeme an. Die für biometrische Systeme renomierte Firma hat des weiteren Grenzkontrollsysteme für maschinenlesbare Pässe und Biometrie für SmartCards und ID-Karten im Programm. Auch für Zugangsysteme bietet diese Firma Lösungen an.

**Cognitec Systems GmbH** (http://www.cognitec-systems.de) Zugangkontrolle mittels Gesichtserkennung, Gesichtserkennung in Bilddatenbanken und auf Video, Softwareentwicklungsumgebung für die von der Firma entwickelten Gesichtserkennungsalgorithmen sind die Produkte dieser Firma.

**Astro Datensysteme AG** (http://www.astro.de) bietet Zugangsysteme auf Basis von Fingerbild, Stimmerkennung, Gesichtserkennung oder einem Mix der drei Systeme. Hard- und Software, sowie Hard- / Software-Entwicklung-Kits an.

**Computer Vision und Automation GmbH** (http://www.facesnap.de/) hat sich auf Gesichtserkennung, Videoüberwachung, Personenerkennung, Herstellung von Bildausweisen und Softwarelösungen für SmartCards spezialisiert.

**VOICE.TRUST AG** (http://voicetrust.de/) VOICE.TRUST ermöglicht die sichere Authentifizierung von Usern mittels Stimme, als sinnvolle Alternative zu schwachen Passwortmechanismen oder technisch aufwendigen Authentifizierungssystemen. Das einfach zu installierende System ermöglicht es, Anwendern sicher und günstig über vorhandene Hardware (Telefon) zu authentifizieren.

# Literatur

[ATSI00] Telecom Glossary 2000,Alliance for Telecommunications Industry Solutions, American National Standards Institute, Inc. www.atsi.org

[Wais02] Waismann, F.: Über den Begriff der Identität, http://www.mauthner-gesellschaft.de/mauthner/tex/wais2.html.

[Nold02] Nolde, Veronika: Biometrische Verfahren, Deutscher Wirtschaftsdienst, Köln, 2002.

[Chan/Kreu03] Chandratilleke, S., Kreutzer, M.:Credential-basierte Ad-hoc-Authentifikation, netzwoche Netzguide E-Security 2003 (März 2003), www.vs.inf.ethz.ch/publ/se/AdHocCredential.pdf.

[Lor96] Lorenz, Rolf J.: Grundbegriffe der Biometrie, Gustav Fischer Verlag, Stuttgart/Jena/Lübeck/Ulm, 1996.

[Dud82] Drosdowski, Köster,Müller,Scholze-Stubenrecht (Hrsg.): Duden, Fremdwörterbuch, 4. Aufl., Mannheim, 1982.

[Brö01] Brömme, Arslan: Politik-gewollte Anwendungen der Biometrik: Fahndung, Ausweise, Terrorbekämpfung: Eine Diskussion unter Berücksichtigung des Datenschutzes, Vorlesungsfolien, Universität Hamburg, November 2001, http://agn-www.informatik.uni-hamburg.de/papers/pub2001.

[Biom02] Biometrik in der Gesellschaft Biometric Authentication Research Group, University of Hamburg, Januar 2002, http://agn-www.informatik.uni-hamburg.de/hct/biomtrie.pdf.

[Pet/Sau02] Petermann, Thomas, Sauter, Arnold: Biometrische Identifikationssysteme-Sachstandsbericht, Arbeitsbericht Nr.76, Büro für Technikfolgenabschätzung beim Deutschen Bundestag, 2002, http://www.tab.fzk.de/de/projekt/zusammenfassung/Ab-76.pdf.

[Behr/Roth01] Behrens, M., Roth, R.: Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt, TransMIT-Zentrum, Institut für biometrische Identifikationssysteme, Gießen, 2001.

[Ditt01] Dittmann, J., Mayerhöfer, A., Vielhauer, C.: Biometrische Systeme - FuE, Diffusionstendenzen und Anwendung. Kommentar- und Ergänzungsgutachten, im Auftrag des Deutschen Bundestages,Platanista GmbH, Darmstadt, 2001.

[Tele02] : Laßmann, G.(red.): Kriterienkatalog - Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Arbeitsgruppe 6: Biometrische Identifikationsverfahren, Stand 10.07.2002, Erfurt (http://www.teletrust.de).

[Abda/Abs02] : Abdalla S., Abschinski T.: Biometrische Authentikation: Methoden- und Verfahrensansätze unter Windows 2000 (W2K), Studienarbeit, Universität Hamburg,2002, http://agn-www.informatik.uni-hamburg.de/ papers/doc/studarb_samer_abdalla_und_timo_abschinski.pdf.

[Bio01] : BioFace - Vergleichende Untersuchung von Gesichtserkennugsystemem, BSI, Bonn , Juni 2002, http://www.bsi.bund.de/fachthem/BioFace/BioFaceIIBericht.pdf.

[Roth01] Behrens, M. Roth, R. (Hrsg.): Biometrische Identifikation, Vieweg, Braunschweig/Wiesbaden, 2001.

[Mai02] Maier, Alexander: Identifikation durch Handgeometrie Ausarbeitung am Institut für Neuroinformatik, der Universität Ulm, 2002 http://www.informatik.uni-ulm.de/ni/Lehre/WS02/HS-Biometrische-Systeme/ausarbeitungen/Handgeometrie.

[Viel02] Viehauer, C.: Handschriftliche Authentifikation für digitale Wasserzeichenverfahren, In: Sicherheit in Netzen und Medienströmen, Tagungsband des GI-Workshops "Sicherheit in Mediendaten", Berlin, S. 134-148, 2001.

[Wett02] Wettig, Steffen: Biometrie: Verfahren und ausgewählte Rechtsprobleme Präsentation im Rahmen des Seminars "Biometrie" an der Universität Jena, 2002, http://www2.informatik.uni-jena.de/ wettig/sem_biometrie_ss_2002/biometrie_uni_jena-xl-Dateien/frame.htm.

[Roth02] Roth, Jörg: Mobile Computing, Grundlagen, Technik, Konzepte, dpunkt.verlag, Heidelberg, 2002.

[BSI03] Projektgruppe "Local Wireless Communication": Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2003, http://www.bsi.bund.de/literat/doc/drahtloskom/drahtloskom.pdf.

[Flu/Lu01] Fluhrer, S. R., Lucks., S.: Analysis of the E_0 Encryption System, Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Seiten 38-48, Springer- Verlag, 2001, http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz.

[Sik02] Sikora, Axel, 802.11: Standard für drahtlose Netze, IDG Interactive, 2002, http://www.tecchannel.de/hardware/680/index.html.

[Bel96] Bellare, M., Canetti, R., Krawczyk, H.: Message Authentication using Hash Functions - The HMAC Construction. CryptoBytes, 2(1), 1996

[RSA93] RSA Laboratories. PKCS1: RSA Encryption Standard, Version 1.5, 1993

[Bor01] Borisov, N., Goldberg, I., Wagner, D.: Intercepting Mobile Communications: The Insecurity of 802.11, 7th Annual International Conference on Mobile Computing and Networking, 2001, ACM-Press 2001

[Kral03] Kralicek, S.: UMTS-Security, Universität Bochum, 2003, www.crypto.ruhr-uni-bochum.de/Seminare/ BeitraegeITS/UMTS_Security_rep.pdf.

[Rep00s] Reppekus, D.: Sicherheitskonzepte des UMTS Standards, Fernuniverstität Hagen, 2000, http://www.fernuni-hagen.de/NT/kurse/sem_2000/umts.pdf.

[3GPP] 3GPP TS 33.102: Technical Specification Group Services and System Aspects, 3G Security; Security Architecture (Release 5,), http://www.3gpp.org.

# Appendix A

# ÜBERSICHT DER HERSTELLER BIOMETRISCHER SYSTEME

In den Tabellen A bis A werden Systeme zur biometrischen Identifikation aufgelistet und nach den bekannten Randkriterien verglichen. Die Quelle die Marktübersicht der Sicherheits-Zeitschrift Protektor. (http://www.protektor.info)

| Firmenname | Remé Baltus | Bergdata Biometrics GmbH | Biometric Security | Biometric Security | Biometric Solutions AG | Biometric Solutions AG |
|---|---|---|---|---|---|---|
| Produktname | Classic Sign | DGID-3 | Face lt | Fingerscan V20 UA | MorphoTouch | FOD |
| Verfahren | Unterschrift, Tippverhalten, Gang | Fingerabdruck | Gesicht | Finger | Fingerprint | Fingerprint |
| Kurzbeschreibung | Schreib-, Tippplatte lagert auf 4 Drucksensoren | Stand-alone System für biometrische Zugangskontrolle | Software und Hardware zur Gesichtserkennung | Autonomes Terminal für Zutrittskontrolle und Zeiterfassung | Biometrischer Scanner zur Zutrittskontrolle und Zeiterfassung | Biometrischer Scanner zur Zutrittskontrolle |
| Hersteller Sensor | Rene Baltus | Atmel | Identix Inc. | Identix Inc. | Sagem | Sagem |
| Entwickler Algorithmus | M.-B. Woop | Bergdata Biometrics GmbH | Identix Inc. | Identix Inc. | Sagem | Sagem |
| Vertrieb durch (D, CH, A) | selbst | Bergdata Biometrics GmbH | Biometric Security AG, Zürich sowie Wiederverkäufer | Biometric Security AG, Zürich sowie zahlreiche Wiederverkäufer | Biometric Solutions AG | Biometric Solutions AG |
| Referenzen | 200 Testgeräte ausgeliefert | FH Giessen-Friedberg, T-Nova Berlin | nur auf Anfrage | nur auf Anfrage | SAP Roth, Commerzbank Frankfurt, Gewo Speyer | keine Angaben |
| Kosten (Endpreis): Standalone | 200,- | 995,- | | ca. 1.400,- | 1.800,- | 590,-(Identifikation), 790,- (Verifikation) |
| Vernetzte Lösung | | 950,- | | ca. 1.400,- | 2.300,- | |
| FAR % | 0 | $< 0.005$ | 0,0001 | 0,00001 | 0 | 0 |
| FRR % | 0 | $< 1$ | | 0,01 | 0 | 0 |
| FTR % | gibt es nicht | | | 0,01 | | |
| Lebenderkennung | ja | nein | ja | ja | nein | nein |
| Identifikation | ja | ja | ja | ja | ja | ja |
| Verifikation | ja | möglich | ja | ja | ja | ja |
| Dauer Enrollment (sec) | | 30 bis 180 | $< 1$ | 10 | <0 1 | <0 1 |
| Dauer Erkennung (sec) 1:1 Vergleich | 5 | rund 0,5 | | $< 1$ | | |
| 1:n Vergleich (500 Personen) | | rund 4 | $< 1$ | 5 | $< 1$ | $< 1$ |
| Max. Speichergröße (Anzahl Templates) | 1 bis 2 K | 1.000 | keine Begrenzung | 32.000 | MT 150: 1.000, MT 400:50.000 | 500 |
| Umfeldbedingungen | können variieren | können variieren | können variieren | können variieren | können variieren | können variieren |
| Betriebstemperatur (°C) | -15 bis +40 | +5 bis +45 | 0 bis +50 | 0 bis +40 | -10 bis +50 | -10 bis +50 |
| Netzwerkschnittstellen | | RS485, RS232 | Ethernet, RS485, RS232, Wählmodem | | Ethernet, RS232 | USB, RS232 |
| Anschluss von Lesern | | RS232, Wiegand in Vorbereitung | | Wiegand, ASCII, Barcode | über Konverter: Wiegand, Clock/Data, ASCII | über Konverter: Wiegand, Clock/Data, ASCII |
| Für Außenmontage geeignet | eingeschränkt | eingeschränkt | ja | eingeschränkt | ja | ja |
| Sonstiges/ Bemerkungen | Bevorzugter Einsatz: Elektronische Blaupausen mit Offline Verifikation | Relais für Türöffner integriert, SDK für Windows lieferbar (für Linux in Vorbereitung) | verschiedene Ausführungsformen | FAR/FRR sind einstellbar | IP Gehäuse lieferbar | IP Gehäuse lieferbar |

Tabelle A.1: Herstellerübersicht Biometrischen Systeme 1

| Firmenname | Bioscrypt Inc. | Bioscrypt Inc. | Bioscrypt Inc. | Cognitec Systems | CCC Corona GmbH | C-Via Computer Vision & Automation |
|---|---|---|---|---|---|---|
| Produktname | V-Pass | V-Smart | V-Station | Face VACS | FG-Print | Face Snap / Face Check |
| Verfahren | Fingerprint | Fingerprint | Fingerprint | Gesicht | Fingerprint | Gesicht |
| Kurzbeschreibung | Zugangskontrolle für Räume, interne Datenbank. | Fingerabdruckerkennung mit lokaler Speicherung der Templates keine Vernetzung aller Leser. | Zutrittskontrollterminal auf Fingerabdruckbasis. | Gesichtserkennungssystem für Zutrittskontrolle, Grenzkontrolle, Fotodatenbankanalyse Stand-Technologie. | Vernetztes Stand-Alone Zutrittskontrollsystem mit direktoptischem Fingerbildsensor ARGOS DiOS | Biometrische Zugangsüberwachung mit Hilfe von automatischer Gesichtsbildidentifikation |
| Hersteller Sensor | Authentec Inc. (AF-S2) | Authentec Inc. (AF-S2) | Authentec Inc. (AF-S2) | bei. Kamera | CCC Corona GmbH | |
| Entwickler Algorithmus | Bioscrypt Inc. | Bioscrypt Inc. | Bioscrypt Inc. | Cognitec | Identcom | Face Snap / Face Check |
| Vertrieb durch (D, CH, A) | Intraproc GmbH Wallstr. 16 40878 Ratingen Deutschland | Intraproc GmbH Wallstr. 16 40878 Ratingen Deutschland | Intraproc GmbH Wallstr. 16 40878 Ratingen Deutschland | Cognitec | Geze GmbH, Ci2T GmbH, TST Deutschland Vertriebs GmbH | SIM GmbH, NTS Deutschland GmbH, Vitronic GmbH, ces AG |
| Referenzen | u.a. Baltimore Airport, NYPD, AMEX, NATO,... | u.a. Baltimore Airport, NYPD, AMEX, NATO,... | u.a. Baltimore Airport, NYPD, AMEX, NATO,... | Infineon, Siemens, Merck, VW-Bank, Kreditbank Luxemburg | Referenzen auf Anfrage | Spielbank Hamburg, Flughafen Zürich |
| Kosten (Endpreis):Standalone | 1.125,- | 1.460,- | 1.685,- bis 2.585,- | ab 2.000,- | ab ca. 1.500,- | 15.000,- |
| Vernetzte Lösung | 1.125,- | 1.460,- | 1.685,- bis 2.585,- | ab 2.000,- | ab ca. 1.500,- | 9.500,- |
| FAR, % | < 0,2 | EER < 0,1 | <0,2 | 0,01 | vergl. Identcom | umgebungsabhängig |
| FAR, % | < 1 | | | 1,0 | vergleichbar Identcom | umgebungsabhängig |
| FTR, % | 1 | 1 | 1 | 0 | vergleichbar Identcom | 0 |
| Lebenderkennung | ja | ja | ja | ja | ja | nein |
| Identifikation | ja | nein | ja | ja | ja | ja |
| Verifikation | nein | ja | ja | ja | ja | nein |
| Dauer Enrollment (sec) | < 3 | < 3 | < 5 | 1 | ca. 1 | 0,1 |
| Dauer Erkennung (sec)1:1 Vergleich: | | <2, | < 2 | 0,5 | ca. 1 | |
| 1:n 500 Personen: | < 1 (200 Pers.) | | < 1 (200 Pers.) | 0,5 | ca. 1 | 0,3 |
| Max. Speichergröße (Anzahl Templates) | 200 | Speicherung auf Mifare | Mifare: unbegrenzt | | abhängig von Steuereinheit >5.000 | 500.000 |
| Umfeldbedingungen | können variieren | können variieren | können variieren | können variieren | können variieren | können variieren |
| Betriebstemperatur (°C) | 0 bis +50 (Sensor: -20 bis +70) | +1 bis +50 (Sensor: -20 bis +70) | +2 bis +50 (Sensor: -20 bis +70) | | -40 bis +85 | |
| Netzwerkschnittstellen | RS232, RS486 | RS232, RS486 | Ethernet, RS232, RS485 | Ethernet, RS485, RS232 | Ethernet, RS485, RS232 | Ethernet, RS232 |
| Anschluss von Lesern | Wiegand, TTL | Wiegand, TTL | Wiegand, TTL | Wiegand, Clock/Data, ASCII | Wiegand, Clock/Data, ASCII | |
| Für Außenmontage geeignet | eingeschränkt (s.u.) | eingeschränkt (s.u.) | eingeschränkt (s.u.) | eingeschränkt | ja | eingeschränkt |
| Sonstiges/ Bemerkungen | Lieferung inkl. Administrationssoftare VeriAdmin, Umschließung für Außenmontage, SDK, OEM-Modul lieferbar, Gewinner des Fingerprint Verification Contest 2002 für höchste Geschwindigkeit und höchste Genauigkeit | Lieferung inkl. Administrationssoftare VeriAdmin, Umschließung für Außenmontage, SDK, OEM-Modul lieferbar, Gewinner des Fingerprint Verification Contest 2002 für höchste Geschwindigkeit und höchste Genauigkeit | 2zeiliges LCD-Display, numerische Tastatur mit Funktionstasten, Transaction-Log für bis zu 8.192 Einträge, div. Modelle für Identifkation und Verifikation mit interner Datenbank oder Speicherung auf Mifare Karte | | | |

Tabelle A.2: Herstellerübersicht Biometrische Systeme 2

| Firmenname | Delsy Electronic Components AG | Idencom | Idencom | Identalink GmbH | Identix Inc. | Ingersoll Rand Security & Safety |
|---|---|---|---|---|---|---|
| Produktname | | BioKey 2002 | BioKey 2103 | Biopassport Enterprise Server | V20 UA | Handkey II |
| Verfahren | CMOS-Sensor DiOS | Finger | Finger | Finger, Gesicht, sonstige auf Wunsch | Fingerprint | Handgeometrie |
| Kurzbeschreibung | optischer CMOS Sensor als OEM Produkt | OEM, Fingerabdruck Erkennungsmodule | OEM, Fingerabdruck Erkennungsmodule Fingerabdruck | Plattform- und Software, uniimitierte User | Fingerscanner zur Zugangskontrolle | Maß und Form der Hand wird drei dimensional erfasst um zu verifizieren |
| Hersteller Sensor | Delsy | Atmel, Infineon & Fingerprint Car | Atmel, Infineon & Fingerprint Car | Sensorunabhängig | Identix Inc. | IR Recognition Systems |
| Entwickler Algorithmus | Standard SW einsetzbar | Idencom | Idencom | eigen | Identix Inc. | IR Recognition Systems |
| Vertrieb durch (D, CH, A) | Delsy AG, CCC Corona | Anatec, Texas Instruments | Anatec, Texas Instruments | | www.bio metronix.com | Normbau Interflex |
| Referenzen | | Kaba, Interflex, Siedle, MBB-Gelma, CM-Pappe, Miditech, Philips, TI-RFID | Kaba, Interflex, Siedle, MBB-Gelma, CM-Pappe, Miditech, Philips, TI-RFID | Synfis AG, Safeways US, Zubler AG, Eiform Inc. | Universität der Bundeswehr, Fakultät für Informatik | Flughafen San Francisco Flughafen Ben Gurion Rotterdam Harbor |
| Kosten (Endpreis): Standatone | | | | | 1.799,- | 1.595,- |
| Vernetzte Lösung | | | | 190,- | ca. 2599,- | 1.995,- |
| FAR, % | 8 | 0,00001 | 0,00001 | einstellbar | 0 bis 1:100.000 | 0 bis S |
| FRR, % | 2 | 0,02 | 0,02 | einstellbar | 1 bis 1,5 | 0 bis 2,1 |
| FTR, % | 2 | 0,01 | 0,01 | einstellbar | ca. 0,1 | 0,1 |
| Lebenderkennung | ja in Entwicklung | ja | ja | nein | nein | quasi |
| Identifikation | ja | ja | ja | ja | ja | nein |
| Verifikation | ja | ja | ja | ja | ja | ja |
| Dauer Enrollment (sec) | 0,1 | ca. 6 | ca. 6 | 60 | $< 5$ | 10 |
| Dauer Erkennung (sec)1:1 Vergleich: | 0,5 | 1,32 | 1,32 | 0,4 | ca. 1 | $< 2$ |
| 1:n Vergleich 500 Personen: | 1 | ca. 3 | ca. 3 | 2 | ca. 5 | |
| Max. Speichergröße (Anzahl Templates) | unbegrenzt | 2.500 | 2.500 | | 32.000 | 512 bis 32.512 Benutzer |
| Umfeldbedingungen | können variieren | können variieren | können variieren | können variieren | können variieren | schlecht bel. & schmutzige Umgebung |
| Betriebstemperatur (°C) | 40 bis +85 | 20 bis +85 | 20 bis +85 | 10 bis +40 | 10 bis +50 | -29 bis +49 |
| Netzwerkschnittstellen | | RS232 | RS485, RS232, UBB | Ethernet, RS485, RS232 | RS485, Wiegand, RS232; optional: Ethernet oder Modem | RS232, RS485, Ethernet |
| Anschluss von Lesern | USB | | Wiegand | beliebig | Wiegand, Proximity, Magnetstreifenkarte, SmartCard, Barcode | Wiegand, Omron, Mifare, Legic, Proxif, Interflex, Nedap |
| Für Außenmontage geeignet | ja | ja | ja | ja | nein | eingeschränkt |
| Sonstiges/ Bemerkungen | extrem robust, hochspannungs- & kratzfest | | | Identalink stellt nur Software zur Verfügung und arbeitet mit allen guten Hardwareherstellern zusammen | | Über 75.000 Geräte weltweit installiert, über 10.000.000 Benutzer |

Tabelle A.3: Herstellerübersicht Biometrische Systeme 3

| Firmenname | Ingersoll Rand Security & Safety | Ingersoll Rand Security & Safety | Kaba GmbH | OKI | Panasonic | Panasonic |
|---|---|---|---|---|---|---|
| Produktname | Handpunch 3000 | Dual Biometrics Kiosk | Kaba exos biover II | Irispass-WG | BM-ET 300 | BM-ET 500 |
| Verfahren | Handgeometrie | Handgeometrie und Gesicht | Fingerprint | Iriserkennung | Iriserkennung | Iriserkennung |
| Kurzbeschreibung | Maß und Form der Hand wird drei dimensional erfasst um zu verifizieren | Falls die Hand nicht verifiziert werden kann, schaltet das System um auf Gesicht | Thermo-Zeilensensor mit minutienbasierter Erfassung der Biometriedaten und Speicherung der Templates (2 Finger) auf dem LEGIC-Ausweis | binokulares System (erfasst und erkennt beide Augen zeitgleich), automatisch startend, autofokussierend | binokulares System (erfasst und erkennt beide Augen zeitgleich), automatisch startend, autofokussierend, integrierte Videoüberwachungslösung | binokulares System (erfasst und erkennt beide Augen zeitgleich), automatisch startend, autofokussierend, integrierte Videoüberwachungslösung |
| Hersteller Sensor | IR Recognition Systems | IR RSI & ZN | Atmel Corporation | Panasonic | Panasonic | Panasonic |
| Entwickler Algorithmus | IR Recognition Systems | IR RSI & ZN | Minutienbasiertes Verfahren | Indian Technologies | Indian Technologies | Indian Technologies |
| Vertrieb durch (D, CH, A) | Normbau Interflex | Normbau Interflex | Kaba GmbH (Dreieich) | Systems GmbH | Byometric Systems GmbH, Panasonic Deutschland GmbH, John Lay Electronics, Panasonic Austria GmbH | Byometric Systems GmbH, Panasonic Deutschland GmbH, John Lay Electronics, Panasonic Austria GmbH |
| Referenzen | MC Donalds, KLM | IATA World Conference | auf Anfrage | auf Anfrage | auf Anfrage | auf Anfrage |
| Kosten (Endpreis) Standalone | 2.295,- | | ca. 1.100,- | ab 14.500,- (zzgl. Installation) | ab 7.573,- (zzgl. Installation) | ab 14.500,- (zzgl. Installation) |
| Vernetzte Lösung | 2.795,- | 13.900,- | ca. 1.100,- | jede weitere Tür: ab 9.438,- | jede weitere Tür: ab jede 4.690,- | weitere Tür: ab 9.438,- |
| FAR % | 0 bis 5 | 0 bis 5 | 0,001 bis 1 | 0,000001 | 0,000001 | 0,000001 |
| FRR % | 0 bis 2,1 | 0 bis 2,1 | 1,9 bis 5,2 | 2 bis 3 | 2 bis 3 | 2 bis 3 |
| FTR % | 0,1 | 0,1 | | | | |
| Lebenderkennung | quasi | ja | ja | ja | nein | ja |
| Identifikation | nein | nein | nein | ja | ja | ja |
| Verifikation | ja | ja | ja | nein | ja | nein |
| Dauer Enrollment (sec) | 10 | 60 | < 10 (2 Finger) | 60 | 120 | 60 |
| Dauer Erkennung (sec)1:n 500 Personen: | | | | | | |
| 1:1 Vergleich: | < 2 | < 2 | < 2 | 8 | 5 | 8 |
| Max. Speichergröße (Anzahl Templates) | 512 bis 32.512 Benutzer | 512 bis 32.512 Benutzer | auf Ausweis gespeichert | 4.000 (2.000 User) | 10.000 (5.000 User) | 4.000 (2.000 User) |
| Umfeldbedingungen | Auch geeignet für schlecht beleuchtete und schmutzige Umgebung | Auch geeignet für schlecht beleuchtete und schmutzige Umgebung | IP54 | können variieren (Licht, Temperatur) | können variieren (Licht, Temperatur) | können variieren (Licht, Temperatur) |
| Betriebstemperatur (C) | -29 bis +49 | -29 bis +49 | -25 bis 55 | 0 bis +40 | 0 bis +40 | 0 bis +40 |
| Netzwerkschnittstellen | RS232, RS485, Ethernet | Ethernet | Ethernet, RS485 | Ethernet | Ethernet | Ethernet |
| Anschluss von Lesern | Wiegand, Omron, Mifare, Legic, Proxif, Interflex, Nedap | Wiegand, Omron, Mifare, Legic, Proxif, Interflex, Nedap | RS485 | | Wiegand | |
| Für Außenmontage geeignet | eingeschränkt | eingeschränkt | ja | nein | nein | nein |
| Sonstiges/ Bemerkungen | Über 75.000 Geräte weltweit installiert, über 10.000.000 Benutzer | Weltweit erste Dual Biometics System | | | | |

Tabelle A.4: Herstellerübersicht Biometrische Systeme 4

| Firmenname | SD Industries | SD Industries | SD Industries | Softpro | Softpro |
|---|---|---|---|---|---|
| Produktname | Iris Access | Simple | Fast | SignDoc | SignSecure |
| Verfahren | Iris | Iris | Finger, Gesicht, Iris, Unterschrift | Unterschrift | Unterschrift |
| Kurzbeschreibung | Iriserkennung für die Zutrittskontrolle | Automatischer Grenzübergang mit Dokumentenleser und Iriserkennung | Softwareapplikation für Grenzübergänge zur Identifikation von Reisedokumenten und Reisenden | Sicherung elektronischer Dokumente | Sicherung PC- und Netzwerk Log-In |
| Hersteller Sensor | LG | LG | Multibiometrie, verschiedene | Empfohlen: Interlink oder Wacom | Empfohlen: Interlink oder Wacom |
| Entwickler Algorithmus | Daughman | Daughman | | Softpro | Softpro |
| Vertrieb durch (D, CH, A) | SD Industries | SD Industries | SD Industries | Softpro, Wilhelmstrasse 34, 71034 Böblingen | Softpro, Wilhelmstrasse 34, 71034 Böblingen |
| Referenzen | Basler Versicherungen, wehrtechnische Dienstelle, T-Systems Nova | | | Mercedes-AMG | |
| Kosten (Endpreis): Standalone | 12.700,- | | auf Anfrage | auf Anfrage | auf Anfrage |
| Vernetzte Lösung | 2.700,- | | auf Anfrage | | |
| FAR % | 0,000 | | | Abh. v. Erfassungsgerät u. voreingestellten Toleranzwert | s.links |
| FRR % | 1,8 | | | s.oben | s. oben |
| FTR % | < 0,5 | | | | |
| Lebenderkennung | ja | ja | ja | bei Unterschriftenerkennungen implizit | s. links |
| Identifikation | ja | ja | ja | ja | ja |
| Verifikation | ja | ja | ja | ja | ja |
| Dauer Enrollment (sec) | < 30 | 30 | 30 | abh. v. indiv. Länge d. Unterschrift | s. links |
| Dauer Erkennung (sec) 1:n (500 Personen) | 1 | 1 | 1 | s.o. | s.o. |
| 1:1 Vergleich: | < 1 | < 1 | < 1 | s.o. | s.o. |
| Max. Speichergröße (Anzahl Templates) | | | biometrieabhängig | abh. ob Template oder Rohdaten | s.links |
| Umfeldbedingungen | können variieren | können variieren | können variieren | wie gewohnt | s.links |
| Betriebstemperatur (C) | 0 bis +40 | +10 bis +40 | -10 bis +75 | i.d.R. nahe üblicher-Raumtemperatur | s.links |
| Netzwerkschnittstellen | Ethernet, RS232, RS422 | Ethernet, RS232 | Ethernet, RS232 | auf Anfrage | auf Anfrage |
| Anschluss von Lesern | Wiegand, Clock/Data | Wiegand, CIock/Data, ASCII, Passleser | Wiegand, CIock/Data, ASCII | auf Anfrage | auf Anfrage |
| Für Außenmontage geeignet | ja | eingeschränkt | ja | bedingt | bedingt |
| Sonstiges/ Bemerkungen | | Integration von anderen biometrischen Merkmalen auf Anfrage, RFID und Smart Card verfügbar | Multibiometrie Plattform, Bio API Unterstützung, RFID Smart Card | | |

Tabelle A.5: Herstellerübersicht Biometrische Systeme 5

| | | |
|---|---|---|
| Firmenname | TST Deutschland Vertriebs GmbH | ZN Vision Technologies AG (Viisage) |
| Produktname | TST BiRD Ili | FacePass (zuvor ZN-Face) |
| Verfahren | Fingerprint | Gesicht |
| Kurz-beschreibung | Berührungsloser optischer Sensor zur Erfassung der Minutien ohne Hautkontakt. | Verifikation mittels Gesichtserkennung. Einsatzschwerpunkte sind Zutritts - und Personenkontrollen |
| Hersteller Sensor | TST | ZN Vision Technologies AG (Viisage) |
| Entwickler Algorithmus | Betrieb mit Standard- oder kundenindividuellen Algorithmen | derzeit implementiert: Sagem,Neurotechnologija, Cogent&ZN Vision Technologies AG (Viisage) |
| Vertrieb durch (D, CH, A) | TST Deutschland Vertriebs GmbH, CCC Corona GmbH, weitere Vertriebspartner auf Anfrage | weltweites Partnernetz,darunter Bosch, Siemens,G&D, Geutebrück, Novar,Oracle Surveillance, Interflex, Unisys, u.a. |
| Referenzen | Boehringer Ingelheim Pharma,CoastCom Consulting, Nordseeheilbad Esens-Bensersiel | Erlebniszoo Hannover, Flughäfen Berlin, Microsoft, RWE |
| Kosten (Endpreis):Standalone | | |
| Vernetzte Lösung | 2.500,- | |
| Leistungsfähigkeit FAR % | | abhängig von Applikation und Schwellenwert-Einstellung < 0,1 |
| FRR % | < 10 | |
| FTR % | < 3 | 0 |
| Lebend-erkennung | ja | ja |
| Identifikation | ja | nein |
| Verifikation | ja | ja |
| Dauer Enrollment (sec) | ca. 2,5 | < 0,5 |
| Dauer Erkennung (sec) 1:n 500 Personen: | ca. 2,5 | |
| 1:1 Vergleich: | ca. 2 | < 0,5 |
| Max. Speichergröße (Anzahl Templates) | serverbasierte Lösung | standardmäßig 100.000, mehr auf Anfrage |
| Umfeld-bedingungen | können variieren | können variieren |
| Betriebs-temperatur (C) | +5 bis +55 | 20 bis +40 |
| Netzwerk-schnittstellen | Ethernet | Ethernet (TCP/IP) |
| Anschluss von Lesern | kundenspezifisch auf Wunsch | Leserschnittstellen für alle marktüblichen Leser verfügbar |
| Für Außenmontage geeignet | eingeschränkt | ja |
| Sonstiges/ Bemerkungen | auch Version im Ex-Schutz- Gehäuse | sowohl als Komplettlösung (Hardware + Software) als auch als biometrische Aufbaukomponente für bereits vorhandene Zutrittskontroll- oder Zeiterfassungssysteme erhältlich. |

Tabelle A.6: Herstellerübersicht Biometrische Systeme 6

# Appendix B

# AUFGABENSTELLUNG

**Vergleich von Zugangssystemen für sicherheitsrelevante Bereiche**

Der Einsatz von Credentials für AAA Mechanismen bietet bezüglich Sicherheit und Komfort neue Möglichkeiten für die Absicherung von Kommunikationsprozessen. Die Integration von Credentials in das Sicherheitskonzept von Kommunikationsnetzen erfordert, aufbauend auf bekannte Sicherheitsmechanismen, Konzepte und Protokolle, die Entwicklung neuer, erweiterter Konzepte und Verfahren, welche die potentiellen Möglichkeiten der Credential-Technologie integrieren und auf die Weise die Sicherheit in Kommunikationsnetzen wesentlich erhöhen.

Die Entwicklung eines Netzdesigns und die daraus abzuleitenden Modelle, Schnittstellen und Spezifikationen machen eine Erweiterung der Betrachtung vom Kommunikationsnetzen unter besonderer Berücksichtigung der Eigenschaften und Möglichkeiten von Credentials in solchen Bereichen wie Performance, Sicherheit, Konfiguration, Fehlersicherheit/-toleranz sowie Überwachung und Abrechnung notwendig.

Im Rahmen der Studienarbeit sind Zugangstechnologien hinsichtlich ihrer Eignung für den Einsatz in sicherheitsrelevanten Bereichen unter Hinzuziehung von biologischen Merkmalen zu beschreiben und für bestimmte Einsatzszenarien zu vergleichen.