Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Vor- und Zuname	geb. am	in:	Matr.-Nr.
Wolf-Rüdiger Schuckar	[redacted]	[redacted]	[redacted]

Titel:

„Technische Möglichkeiten der Personenidentifikation: Überlegungen zum Einsatz in den Bereichen Safety und Security“

Abgabedatum:
[redacted]

Betreuender Professor:	Herr Prof. Dr. Röhrs
Zweiter Prüfender:	Herr Prof. Dr. Lenschow

Fakultät Wirtschaft und Soziales
Department Wirtschaft

Studiengang:
Logistik/Technische Betriebswirtschaftslehre

I Inhaltsverzeichnis

II Tabellenverzeichnis

III Abbildungsverzeichnis

IV Erklärungen

IVa Erklärung zur Selbstständigkeit

Ich versichere, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtliche oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quelle kenntlich gemacht.

Datum	Unterschrift

IVb Einverständnis

Ich erkläre mich damit einverstanden, dass ein Exemplar meiner Bachelorthesis in die Bibliothek des Fachbereichs aufgenommen wird; Rechte Dritter werden dadurch nicht verletzt.

Datum	Unterschrift

1. Zwischen Security und Safety

1.1. Sicherheit = Security + Safety

In Industrie und Handel hat die geregelte Steuerung von Prozessen aller Art große Bedeutung. Zum einen dient sie der Kostenersparnis, da Unterbrechungen hohe Folgekosten erzeugen können. Zum anderen geht es um die Unversehrtheit der Mitarbeiter. Auch der Diebstahl von Gütern und Eigentum muss für das erfolgreiche Wirtschaften eines Unternehmens unterbunden werden. Im öffentlichen Sektor spielt die Personenidentifikation für die Verbrechensbekämpfung beziehungsweise -vereitlung eine große Rolle. Die Faktoren Fälschungssicherheit und Unverwechselbarkeit machen biometrische Systeme zudem für die Strafverfolgung immer interessanter.

Für die personalisierte Werbung stellt die Personenidentifikation ebenfalls eine Herausforderung dar. Auf diese Weise kann Werbung auf die Personen vor Ort sehr genau zugeschnitten werden.[1]

Das Deutsche fasst all diese Aspekte in einem Begriff zusammen: Sicherheit. Das Angelsächsische differenziert dieses Thema feiner in die Begriffe Security und Safety. Dabei steht Security für den Schutz vor bewussten Fremdeingriffen und Security für die Sicherheit von Prozessen.[2]

Ein wichtiger Bestandteil von Sicherheit ist es, nur ausgewählten Personen den Zugang zu bestimmten Bereichen oder Maschinen zu gestatten und diesen selektiven Zugriff sicherzustellen. Diese Arbeit setzt sich daher mit den technischen Möglichkeiten der Personenidentifikation auseinander. Die manuelle Ausweiskontrolle fällt nicht darunter, da keine technische Komponente im Spiel ist.

Gewisse Möglichkeiten der Zugangskontrolle werden daher nicht berücksichtigt, beispielsweise Laserschranken. Denn diese ermöglichen es zwar, die Anwesenheit einer Person zu registrieren, sind aber nicht in der Lage, die Zugriffsberechtigung zu kontrollieren.

---

[1] Vgl. Rathgeber, Isabel: „Werbung von gestern bis morgen: [...]“, 2004, S.73.
[2] Vgl. „Einführung in die Kryptographie“, 2003.

1.2. Zielsetzung und Aufbau

Es ist das Ziel, verschiedene Möglichkeiten der technischen Personenidentifikation darzustellen und zu bewerten.

Im zweiten Abschnitt wird zunächst eine erste Einteilung vorgenommen. Dies soll helfen das Thema zu Gliedern und zu Überschauen. Des weiteren werden hier einige grundlegende Begriffe erläutert.

Der dritte Abschnitt befasst sich mit der Vorstellung einiger Systeme die Betrachtet werden sollen. Auswahlkriterium war hier vor allem die Marktreife und -präsens.

Das vierte Kapitel stellt gewissermaßen eine Zusammenfassung der vorher gezeigten Systeme dar. Hier werden diese auch bewertet.

Im letzten Abschnitt gibt es ein Abschließendes Fazit.

2. Begriffe und Klassifizierung

2.1. Einteilung der Systeme

Grundsätzlich existieren bei den technischen Möglichkeiten der Personenidentifikation viele Überschneidungen. So kann beispielsweise ein Schlüssel Zugang zu einem Bereich gewähren, was in das Gebiet Security fällt, aber auch eine Maschine in Betrieb setzen, was dem Begriff Safety zuzuordnen wäre.

Zur einleitenden Veranschaulichung dient das folgende Schaubild:

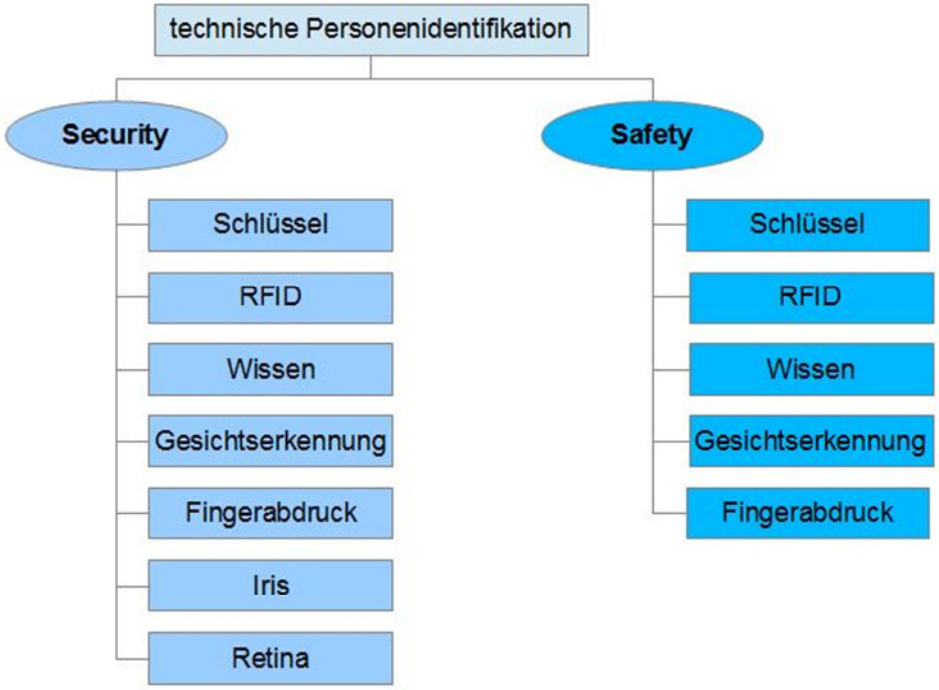

Abbildung 1: Erste Aufteilung der technischen Möglichkeiten zur Personenidentifikation.

Bereits auf den ersten Blick ist zu erkennen, dass es viele Mehrfachnennungen sowohl für Security als auch für Safety gibt. Deshalb soll zwischen „vererbbar“ und „nicht vererbbar“ unterschieden werden. Wodurch sich folgender Baum ergibt.

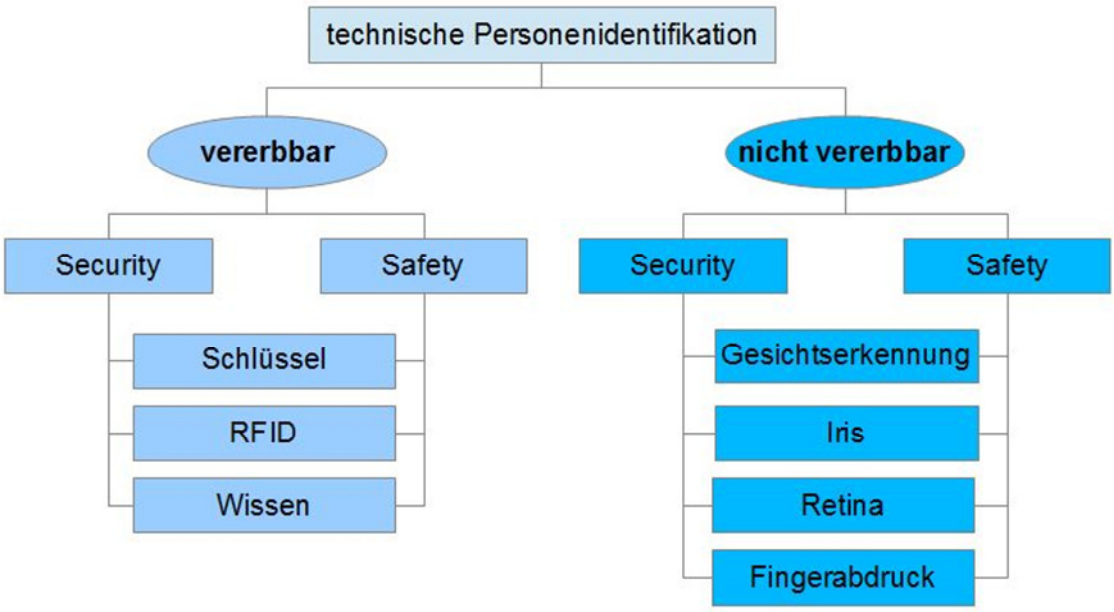

Abbildung 2: Einteilung in "vererbbar" und "nicht vererbbar".

2.2. Terminologie

Personenidentifikation ist heute ein wichtiges Mittel, um Bereiche und Güter zu schützen. Aus dem Lateinischen stammen die Wörter *identitas*[3] und *facere*[4], die mit mit „Wesenheit“ und „machen“ übersetzt werden. Aus ihnen ergibt sich die Wortschöpfung *Identifikation* – „Wesenheit machen“. Das Bertelsmann Lexikon übersetzt den Begriff *Identifizierung* mit „Gleichsetzung; die Feststellung das etwas identisch ist“[5] und was genau bezeichnet, was erreicht werden soll. Es soll sichergestellt werden, dass etwas „ein und das selbe“, also identisch[6] ist. Das bedeutet, dass nicht jedem, sondern nur ausgewählten Personen der Zugang oder die Nutzung bestimmter Einrichtungen oder Geräte gestattet wird. Das ist nicht nur in gewerblichen Bereichen von Interesse, auch im Privaten möchten wir sicher sein, dass unser Eigentum geschützt ist.

Unabhängig davon, welche Technik angewendet wird, handelt es sich doch immer

[3]Vgl. Kandler, 2008, S.48.
[4]Vgl. Müller-Lancé, 2006, S.102.
[5]Vgl. Bertelsmann Band 7, 1999, S.113.
[6]Vgl. Bertelsmann Band 7, 1999, S.113.

um eine Form von Schlüssel. Das Wort *Schlüssel* bezeichnet hier nicht den „Metallstift“ zum Öffnen oder Schließen eines Zylinderschlosses. Das Duden-Wörterbuch bietet für *Schlüssel* verschiedene Lesarten. Schlüssel kann etwa auch als Information verstanden werden, die benötigt wird, um Texte zu verstehen[7] – die bekannteste Form wäre hier die Kryptographie[8]. In dieser Arbeit wird *Schlüssel* als allgemeiner Begriff verwendet, um Gegenstände oder Informationen zu beschreiben, die benötigt werden, um Schlösser zu betätigen.

Das *Schloss* selbst ist eine Vorrichtung, die Türen, Gefäße oder Anlagen schützen soll.[9]

Security[10] und *Safety*[11] sind englische Begriffe, die nur schwer ins Deutsche übertragen werden können, da beide mit „Sicherheit“ übersetzt werden. Im Sprachgebrauch werden die Begriffe feiner differenziert. So beschreibt Safety die Sicherheit welche gefordert ist um Prozesse, Anwender und Systeme zu schützen. Security hingegen beschreibt die Absicherung gegen Fremdzugriffe bzw. Manipulationen[12].

Die von mir gewählten Begriffe *vererbbar* und *nicht vererbbar* sind folgendermaßen definiert: „Vererbbare Schlüssel“ sind Sicherungsmaßnahmen, die durch Personen weitergegeben werden können. So kann ein klassischer Schlüssel verloren, mutwillig an Dritte weitergegeben oder kopiert werden. „Nicht vererbbare Schlüssel“ treten in meist in der Form von Geräten auf, die biometrischen Merkmale einer Person erkennen und zuordnen können – obwohl auch hier Möglichkeiten bestehen, diese zu umgehen. Ansätze dazu werden bei der Einführung der Systeme gezeigt.

Die *Biometrie* oder Biometrik war ursprünglich eine mathematische Hilfswissenschaft. Sie lehrte, die Mess- und Zahlenverhältnisse der Lebewesen zu beschreiben.[13] Heute wird der Begriff meist in Verbindung mit Sicherheit verwendet. Man versteht darunter Sicherungsmaßnahmen, die darauf beruhen, dass einzigartige Körpermerkmale als Schlüssel verwendet werden.

---

[7]Vgl. duden.de - „Schlüs-sel, der“.
[8]Vgl. kleines-lexikon.de - „Kryptografie“.
[9]Vgl. fremdwort.de - „Schloss“.
[10]Vgl. dict.cc - „security“.
[11]Vgl. dict.dd - „safety“.
[12]Vgl. Albrechtsen: „Security vs safety“, 2003.
[13]Vgl. Bertelsmann Band 2, 1999, S.257.

3. Möglichkeiten der technischen Personenidentifikation

Dieses Kapitel stellt die einzelnen Möglichkeiten der Personenidentifikation dar und erläutert sie. Im ersten Abschnitt werden *nicht-biometrische*, im zweiten *biometrische* betrachtet.

Jedes Element wird zunächst erklärt und anschließend bewertet. Auch der Anwendungsbereich und die Handhabung sollen bewertet werden. Weiterhin soll eingeschätzt werden, inwiefern die unterschiedlichen Systeme in den Bereichen Security und Safety Anwendung finden können.

3.1. Nicht-biometrische Systeme/ vererbbar

Dr.-Ing. Rainer Ulrich vom Fraunhofer Institut schließt in diese Kategorie „Besitz“ und „Wissen“ ein.[14] In dieser Arbeit sollen all diese Möglichkeiten unter dem Begriff „Nicht-biometrisch“ zusammengefasst werden. Das bedeutet, dass jedes System der Personenidentifikation in diesen Abschnitt fällt, das den Schwachpunkt der Weitergabe oder Entwendung aufweist.

3.1.1. Der Schlüssel

3.1.1.1. Funktionsweise von Schlüsselsystemen

In diesem Kapitel wird nun die älteste und am weitesten verbreitete Form der Zugangskontrollen betrachtet – der Schlüssel. Es geht um den physischen Schlüssel in der Form eines Metallstiftes, der benutzt wird, um ein Schloss zu betätigen. Zu

[14]Vgl. Dr.-Ing. Ulrich, Rainer: „Biometrie in der IT-Sicherheit“, 2000.

diesem System gehören ein Zylinder und ein Schlüssel.

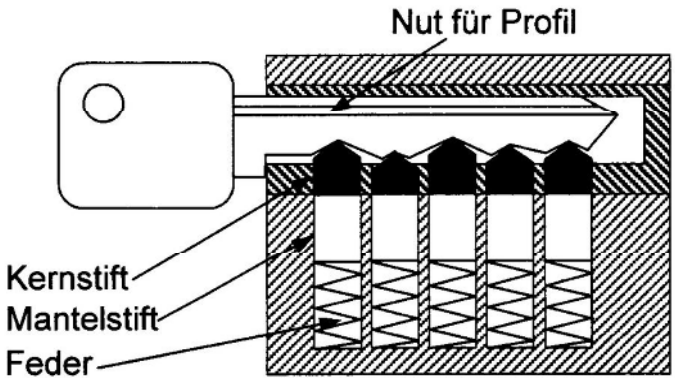

Abbildung 3: Zylinderschloss (Vgl. schule.de: „Übungsaufgaben“.).

Der Zylinder wird an der zu sichernden Tür, dem Gefäß oder System angebracht. Der Schlüssel verbleibt bei einer oder mehreren Personen, die Zugang haben sollen.

Das bekannteste Beispiel für Schlüssel im Bereich der Safety ist der Autoschlüssel. Erst dieser ermöglicht, das Fahrzeug zu betreten und zu starten. Dasselbe Prinzip wird auch für Baumaschinen oder Flurförderfahrzeuge verwendet.

Die Federn (siehe Abbildung 3) drücken die Kern- und Mantelstifte in den Schlüsselkanal, was ein Drehen des Innenzylinders verhindert. Erst durch das Einführen des passenden Schlüssels werden die Sperrstifte in die richtige Position gebracht, wodurch ein Drehen des Innenzylinders möglich wird. So kann das Schloss aufgesperrt werden.[15] Mit einer steigenden Anzahl von Stiften erhöht sich die Anzahl der möglichen Kombinationen, je nachdem, in welchen Längenabstufungen diese hergestellt werden können. Die seitlichen Rillen im Schlüssel, das sogenannte Schlüsselprofil, dient als zusätzliche Sicherungsmaßnahme, um die Passform einzigartig zu gestalten.

[15]Vgl. bauidee: „So funktioniert ein Zylinderschloss“.

Es ist möglich, mit nur einem Schlüssel den Zugang zu verschieden Bereichen zu ermöglichen.

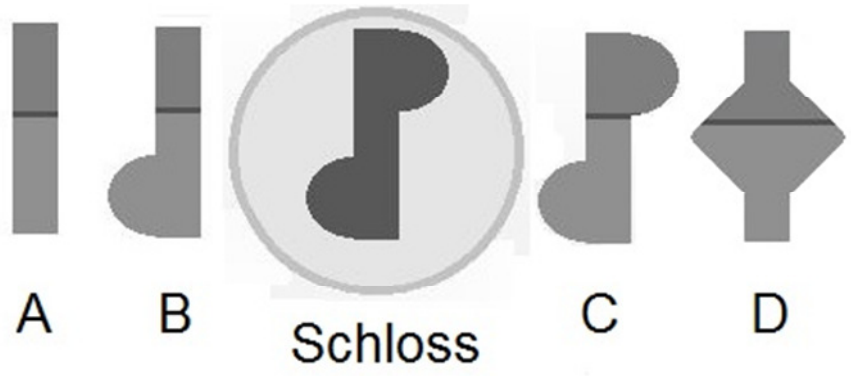

Abbildung 4: Zugangsregulierung über Schlüssel (Vgl. hasa.de: „Das Prinzip einer mechanischen Schließanlage“.)

Abbildung 4 zeigt vereinfacht, wie über die Passform von Schloss und Schlüssel Zugangs- bzw. Nutzungsrechte reguliert werden können. In diesem Beispiel können nur die Schlüssel A, B und C in das Schloss eingeführt werden. Schlüssel D passt nicht und erhält somit auch keinen Zugriff.

3.1.1.2. Bewertung des Systems Schloss-Schlüssel

Der Schlüssel als Möglichkeit der Personenidentifikation ist problematisch. Damit Schlüsselsysteme diese Aufgabe wahrnehmen können, muss die Schlüsselverwaltung vernünftig organisiert sein. Die Ausgabe und Berechtigungen der Schlüssel muss ordentlich dokumentiert werden. Sollte eine vormals zugangsberechtigte Person die Berechtigung entzogen werden, muss sichergestellt sein, dass der Schlüssel zurückgeführt wird.

Ein großer Vorteil ist die einfache Handhabung sowie die allgemeine Akzeptanz und Vertrautheit. Jeder kennt und nutzt Schlüssel von Kindesbeinen an.

Die Grundanschaffung von ist relativ kostengünstig und ein Schloss in der Regel leicht zu installieren. Auch ist es möglich, mit nur einem Schloss verschiedene Schlüssel zuzulassen und umgekehrt. Auf diese Weise können Sicherheitsbereiche

abgegrenzt werden oder Generalschlüssel umgesetzt. Nachträgliche Änderungen sowie der Verlust eines Schlüssels sind hingegen problematisch. Tritt einer dieser Fälle ein, müssen unter Umständen mehrere Schlösser ausgetauscht werden, was je nach Umfang hohe Kosten verursachen kann.

Das Hauptproblem bleibt aber die Tatsache, dass ein Schlüssel nur bedingt die Berechtigung einer Person überprüfen kann. Häufig besitzen mehrere Personen einen Schlüssel, um einen bestimmten Bereich zu betreten oder eine bestimmte Maschine zu benutzen. Dieser Personenkreis lässt sich zwar einschränken, jedoch nicht endgültig klären, wer zu welchem Zeitpunkt die Zugangsberechtigung genutzt hat. Auch das Verleihen von Schlüsseln kann zur Verletzung von Sicherheitsrichtlinien führen.

Was den physischen Kopierschutz von Schlüsseln betrifft, existieren diverse Schutzmaßnahmen. Die erste besteht darin, technische Ausprägungen so zu gestalten, dass ein Nachbau mit handelsüblichen Werkzeugen nur unter hohem wirtschaftlichen Aufwand geschehen kann. Des Weiteren sind Rohlinge von Schlüsseln nicht frei am Markt erhältlich. Gegen den Schutz vor unberechtigter Nachbestellung bietet die Firma EVVA beispielsweise eine Sicherungskarte an, die erforderlich ist, um Legitimation nachzuweisen. Weiterhin werden verschiedene technische Sicherungen in einem Schlüssel verwendet. So findet man zu Beispiel keine glatten Schlüssel, bei denen die Nut fehlt oder die Kerben, um die Stifte zu bewegen.[16]

<u>Beispielrechnung:</u>

Angenommen es handelt sich wie in Abbildung 3 um ein Zylinderschloss mit fünf Sperrstiften. Jede Stiftlänge kann zwischen 4,8mm und 8,2mm variieren, wobei eine Abstufung von 0,2 mm möglich ist.

Es ergeben sich für jeden Stift ((8,2 – 4,8) / 0,2=) 18 verschiedene mögliche Längen. Dadurch ergeben sich für die fünf Sperrstifte, die theoretisch alle gleich lang sein können, 18^5=1.889.568 mögliche Kombinationen.[17]

[16]Vgl. evva.de: „Was bedeutet Nachschlüsselsicherheit genau?“.
[17]Vgl. schule.de: „Übungsaufgaben“.

3.1.2. Radio Frequency Identification (RFID)

Das Radio Frequency Identification System ist besser bekannt unter seiner Abkürzung RFID. Bei diesem System kommuniziert ein Transponder über elektromagnetische Wellen mit einem Lesegerät.[18] Das Wort *Transponder* ist ein Neologismus, der sich aus Transmitter (Sender) und Responder (der Antwortende) zusammensetzt.[19]

Die relativ neue Technik[20] bietet vielseitige Einsatzmöglichkeiten. Neben dem Sicherheits-Bereich wird die RFID-Technik unter anderem in der Logistik eingesetzt.[21] Auch der intelligente Kühlschrank, der selbstständig erkennt, welche Lebensmittel sich in ihm befinden und automatisch Bestellungen auslösen kann, nutzt diese Technik.[22]

3.1.2.1. Die Funktion von RFID

Häufig werden RFID-Systeme in Scheckkarten eingesetzt, über die sich dann bestimmte Türen öffnen lassen – sozusagen die moderne Form des klassischen Metallschlüssels. Anders als bei diesen beruht das RFID-System nicht mehr auf mechanischem Formschluss, sondern elektronischer Datenverarbeitung.

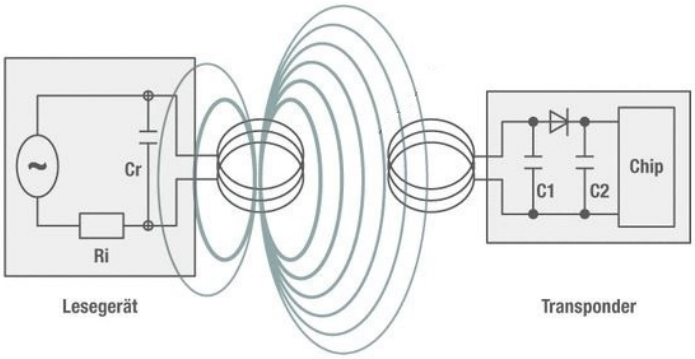

Abbildung 5: allg. RFID System (Vgl. u-tech-gmbh.de: „RFID – So funtioniert es“.)

[18]Vgl. rfid-basis.de: „Aufbau und Funktionsweise von RFID-Systemen“.
[19]Vgl. brooks-rfid.com: „RFID Techik“.
[20]Vgl. rfid-journal.de: „RFID Geschichte“.
[21]Vgl. Matheus, Klumpp: „ild Schriftenreihe Logistikforschung“, 2008.
[22]Vgl. Kern, 2006, S.1.

Die Abbildung 5 stellt ein solches RFID-System vereinfacht dar. Mit Hilfe eines Generators wird im Lesegerät ein Aufrufsignal erzeugt und an eine Antenne weitergeleitet. Diese erzeugt ein magnetisches Feld, das den umliegenden Raum durchdringt. Kommt nun ein Transponder, der ebenfalls über eine Antenne verfügt, in dieses Magnetfeld, wird in diesem eine Spannung induziert und vom Chip weiterverarbeitet. Dieser erzeugt ein Antwortsignal und sendet es an das Lesegerät zurück.[23]

Bereits in den 1960er Jahren wurden 1-Bit-Transponder als Diebstahlschutz zur Nutzung in Kaufhäusern entwickelt.[24] Für diese Anwendung reicht 1 Bit aus, um ein Ja- beziehungsweise Nein-Signal zu senden. Die Firma Fujitsu wirbt für ein RFID-System, das 8KB an Daten übertragen kann.[25] Das bedeutet, dass umfangreiche Informationen ausgelesen und abgespeichert werden können. Zur Verwendung in der Personenidentifikation besteht jedoch das Problem, das dieser Vorgang laut Fujitsu etwa vier Sekunden dauert. Dadurch würde nur eine Anwendung im Bereich der Safety in Frage kommen, wenn man längere Zeit an einer Maschine verbringt. Vorausgesetzt, die Latenzzeit könnte in den unteren Millisekundenbereich gesenkt werden, würde sich ein derartiges RFID-System auch zu Security-Zwecken eignen.

Eine spezielle Form der RFID-Technik ist die Near-Field-Communication, kurz NFC. Diese zeichnet sich dadurch aus, dass sie nur in bestimmten Frequenzbereichen arbeitet und dadurch nur in Reichweiten von zirka 15cm wirksam arbeitet.[26]

3.1.2.2. Bewertung von RFID

Der große Vorteil von RFID-Systemen gegenüber dem klassischen Schlüssel ist vor allem, dass der Benutzer keinen direkten Kontakt mit dem Lesegerät herstellen muss. Personen können im Vorbeigehen erfasst werden. Je nach Einstellung beziehungsweise Auslegung des Systems ist es möglich, Reichweiten von 0cm bis

[23]Vgl. u-tech-gmbh.de: „RFID – So funtioniert es“.
[24]Vgl. rfid-basis.de: „Aufbau und Funktionsweise von RFID-Systemen“.
[25]Vgl. Hohenauer, Florian: „Fujitsu bringt neuen Chip für Hochfrequenz-RFID-Tags [...]“, 2012.
[26]Vgl. Fakir, Simon: „Unterschied RFID und NFC – Eine kurze Erklärung“.

100m abzudecken.[27]

Hierbei ist allerdings die Handhabung entscheidend. Ab einer Reichweite von zirka 150cm benötigt der Transponder eine eigene Stromversorgung, wodurch dieser größer wird. Das Einsatzgebiet solcher Transponder wäre im Bereich der Safety beispielsweise der Bergbau. Bergarbeiter könnten mit solch einem Gerät ausgestattet werden, um im Falle eines Unglücks ihre Position leichter bestimmen zu können. Güter auf großen Industrieanlagen könnten ebenfalls kann mit Transpondern dieser Art genau verfolgt werden. In Häfen könnte auf diese Weise die Position und der Status von Containern genau überwacht und gesteuert werden.

Für die Verwendung in der Security bieten sich eher Systeme mit kurzer Reichweite an. Um Maschinen, Türen und Anlagen effektiv zu schützen, sollte die Reichweite nicht zu großzügig ausgelegt werden. Denn sonst sendet der Transponder eines Mitarbeiters, der über die entsprechende Berechtigung verfügt, eine Freigabe und eine unberechtigte Person könnte diese nutzen.

Es zeigt sich, dass hier die Wahl der Reichweite und Übertragungskapazität eine entscheidende Rolle spielt.

Ein weiterer Vorteil von RFID gegenüber Schlüsseln ist das Übertragen von Informationen. Sollten mehrere Personen berechtigten Zugang zu einem Sicherheitsrelevanten Bereich haben, besteht die Möglich nachzuverfolgen, wer wann welche Tür geöffnet beziehungsweise welche Anlage benutzt hat. Des Weiteren ist es dadurch möglich, Transponder bei Verlust zu sperren, ohne dass das gesamte System überarbeitet werden muss. Allerdings gibt es auch hier keine Garantie dafür, dass der Transponder nicht weitergegeben oder entwendet wird.

RFID-Systeme sind nicht hundertprozentig vor Manipulation sicher. Mit technischem Know-how bestehen diverse Möglichkeiten des Fremdeingriffs, von der Abschirmung bis zur Duplizierung des Transponders. In der Ausarbeitung „RFID-Manipulationsmöglichkeiten“ von Jens Leinenbach sind die Angriffsmöglichkeiten und Gegenmaßnahmen sowie deren relative Kosten tabellarisch dargestellt (Tabelle 1).

[27]Vgl. rfid-loesungen.com: „RFID Übersicht“.

Angriff	Kosten des A.	Gegenmaßnahmen	Kosten des G.
Abhören der Kommunikation von Tag und Lesegerät	hoch	Verlagerung ins Backend Abschirmung Verschlüsselung	mittel
Unautorisiertes Auslesen der Daten	mittel bis hoch	Authentifizierung [Detektoren (nicht ursachenadäquat)]	mittel
Unautorisiertes Verändern der Daten	mittel bis hoch	Read-only-Tags Authentifizierung [Detektoren (nicht ursachenadäquat)]	gering bis mittel
Cloning und Emulation	mittel	Erkennung von Duplikaten Authentifizierung	mittel
Ablösen der Tags vom Trägerobjekt	gering	mechanische Verbindung Alarmfunktion (aktive Tags) Zusatzmerkmale	gering bis mittel
Mechanische oder chemische Zerstörung	gering	mechanische Verbindung	gering bis mittel
Zerstörung durch Feldeinwirkung	mittel	selbst heilende Sicherung (nur begrenzt wirksam)	in Serie gering
Zerstörung durch Missbrauch eines Kill-Befehls	mittel	Authentifizierung	mittel
Entladen der Batterie (nur aktive Tags)	mittel	Schlafmodus	in Serie gering
Blocker-Tag	gering	Verbot in AGB (nur begrenzt wirksam)	gering
Störsender	mittel bis hoch	Messungen Frequenzsprungverfahren	mittel bis hoch
Feldauslöschung	gering (jedoch schwierig)	keine	-
Feldverstimmung	sehr gering	aktive Frequenznachführung	mittel bis hoch
Abschirmung	sehr gering	Verbesserte Lesestationen (nur begrenzt wirksam)	mittel

Tabelle 1: Vgl. Jens Leinenbach; (Vgl. Leinenbach: „RFID – Manipulationsmöglichkeiten“, S.9.)

Hier muss der Anwender entscheiden, wie hoch seine Sicherheitsansprüche sind und den damit verbundenen Kostenaufwand in Betracht ziehen. Eine Kosten-Nutzen-Analyse sollte an erster Stelle stehen.

Die Kosten für eine nachträgliche Änderung beziehungsweise Pflege des Systems halten sich in Grenzen, da lediglich Einträge in der entsprechenden Datenbank geändert werden müssen.

In der Anwendung bieten RFID-Systeme umfangreiche Möglichkeiten sowohl für Security als auch Safety – vorausgesetzt, das System wird korrekt gehandhabt. In der Security kann ein RFID-System den klassischen Schlüssel ablösen. Im Bereich der Safety ist es weiterhin möglich, während eines Prozesses bestimmte Güter zu verfolgen oder den Aufenthaltsort von Personen in gefährlichen Anlagen zu bestimmen.

3.1.3. Training und Schulung

Neben den technischen Möglichkeiten sollen die personalen Voraussetzungen behandelt werden. Denn erst über Schulungsmaßnahmen können die gewünschten Effekte erzielt werden. Bestimmte Maschinen können nicht ohne spezielle Schulungen bedient werden. Das einfachste Beispiel hierfür ist das Auto. Der Zusammenhang zwischen dem Treten der Kupplung und dem Schalten der Gänge muss einem zunächst vermittelt werden, bevor man eines benutzen kann. Dabei geht es nicht darum, dass man versteht, wozu die Kupplung dient oder was ein Getriebe ist, jedoch sollte man wissen, dass man die Kupplung irgendwann treten sollte, um je nach Geschwindigkeit in höhere oder niedrigere Gänge zu schalten und angemessen beschleunigen zu können.

In der Industrie muss oftmals geschult werden, bevor ein Benutzer bestimmte Maschinen bedienen kann. Das liegt meist an der Komplexität der Aufgaben, die ausgeführt werden sollen. Beispielsweise Bedarf es zur Nutzung von Werkzeugmaschinen einer speziellen Schulung, um diese überhaupt in vollem Umfang einsetzen zu können.[28]

3.1.3.1. Zahlenkombinationen

Auch Banken nutzen das Mittel der Personenidentifikation. Beim Geldabheben oder Einkaufen muss eine PIN eingegeben werden, um den Geldtransfer in Gang zu setzen, auch wenn das Lernen der vier Zahlen keine sonderlich umfangreiche Schulung ist. Das gleiche System wird an Tresoren oder Türschlössern mit Zahlenkombinationen verwendet. Erst wenn eine berechtigte Person die richtige Kombination eingibt, lässt sich die Tür öffnen. Bei diesen Schlössern fungiert die Zahlenkombination als Schlüssel.

[28]Vgl. kstools.com: „Schulungscenter“.

3.1.3.2. Benutzername und Passwort

Im Internet werden Benutzernamen und Passwörter verwendet, um die Berechtigung eines Nutzers zu verifizieren – eine ähnliche Vorgehensweise wie bei Zahlenkombinationen. Jedoch sind die Möglichkeiten der Verschlüsselung wesentlich größer. Hat man zum Beispiel eine vierstellige Kombination und verwendet statt Ziffern zusätzlich noch das gesamte Alphabet (A-Z, ohne Umlaute und ß), erhöht sich die Anzahl der Möglichkeiten von 10.000 auf über 1,67 Millionen. Damit ist eine Zahlen-Buchstaben-Kombination 168-mal sicherer als ein Zahlenschloss. Dieser Faktor kann durch Klein- und Großschreibung sowie Umlaute und Sonderzeichen noch weiter erhöht werden.

3.1.3.3. Bewertung von Schulungen

Bei Schulungen oder Kombinationen gibt es zwei große Probleme. Zum einen besteht wie bei allen nicht-biometrischen Systemen das Risiko der Weitergabe von Informationen, welche hier die Funktion des Schlüssels erfüllen.

Ein weit größeres Problem, gerade bei Zahlenkombinationen, ist die Bequemlichkeit menschlicher Benutzer. So werden immer wieder der Einfachheit halber Quadruple bei Viererkombinationen eingesetzt. Die App „Big Brother Camera Security“ generierte einen Sperrbildschirm, der optisch dem eines iPhones glich. Gab der Benutzer nun den Code ein, um sein Telefon zu entsperren, wurde dieser anonym an den Entwickler geschickt. Aus diesem Datenset von 204.508 gesammelten Passcodes ergab sich eine interessante Statistik.[29]

[29]Vgl. Amitay, Daniel: „Most Common iPhone Passcodes“, 2011.

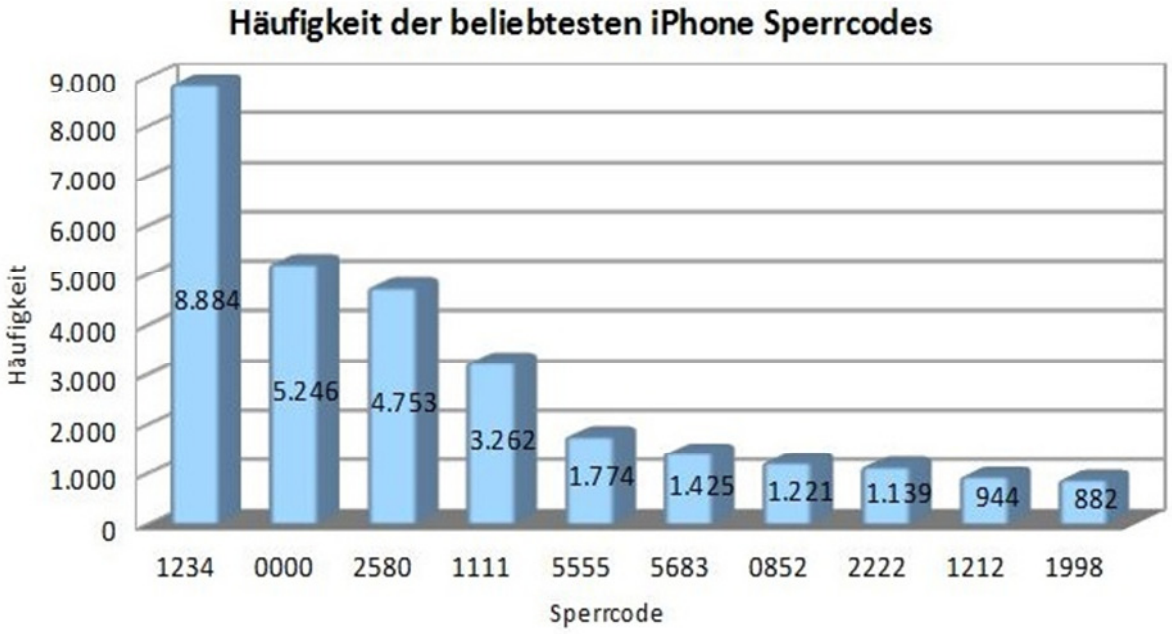

Abbildung 6: Top- Ten der häufigsten Sperrbild Codes (Vgl. Amitay, Daniel: „Most Common iPhone Passcodes“, 2011.)

Abbildung 6 zeigt die zehn beliebtesten Codes. Auf Platz eins steht die sehr leicht zu merkende Kombination *1-2-3-4.* Weiterhin sind Muster sehr beliebt. Der einzige Wert, der heraus sticht, ist die Kombination *5-6-8-3*. Doch es zeigt sich, dass diese Kombination auf der Zahlentastatur für Handys das Wort „Love“ ergibt. Nicht verwunderlich, schließlich zählt „iloveyou“ noch immer zu den beliebtesten Passwörtern im Internet.[30] Diese Top Ten der Sperrcodes beinhaltet Bereits 29.530 der gesammelten Codes. Dadurch ergibt sich für Diebe eine Wahrscheinlichkeit von 1:7, also fast 15%, durch bloßes Ausprobieren dieser Hitliste die richtige Kombination zu treffen. Kennt man den Benutzer etwas besser, erhöht man seine Chancen durch das Ausprobieren des Geburtsdatums des Benutzers, dessen Partner oder Kinder. Ebenfalls zeigte der Versuch, dass Jahreszahlen sehr beliebt sind (siehe Abbildung 7).

[30]Vgl. Imperva: „Consumer Password Worst Practices“, 2014.

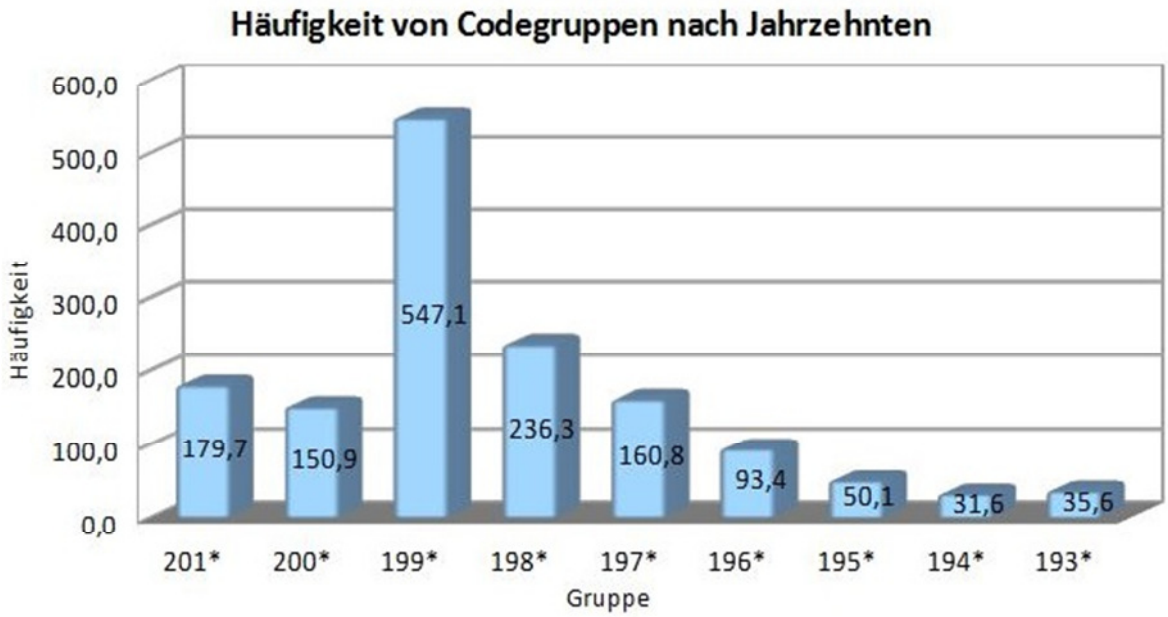

Abbildung 7: Häufigkeit der Beliebtesten Jahresgruppen (Vgl. Amitay, Daniel: „Most Common iPhone Passcodes“, 2011.)

Dieser Versuch zeigt also, dass ein Zahlenschloss keine sehr zuverlässige Methode ist, um sicherheitsrelevante Bereiche vor Fremdzugriff zu schützen.

3.1.4. Abschließend zu den vererbbaren Systemen

Das größte Problem bei diesen Mitteln ist die einfache Art der Weitergabe. „Darf ich kurz den Schlüssel haben?“ „Mach doch eben schnell selber an meinem Computer! Das Passwort lautet: *iloveyou*.“ - Sind Sätze die viel zu schnell gesagt werden.

Der klassische, mechanische Metallschlüssel hat den großen Nachteil der Reproduzierbarkeit. Wird ein Schlüssel verloren, können enorm hohe Kosten entstehen. Mitunter kann dies bedeuten das die gesamte Schließanlage überarbeitet werden muss. Benötigt man hingegen einen neuen Schlüssel bedeutet dies in der Regel einen größeren Zeitaufwand bei der Beschaffung. Das setzt auch eine gewissenhafte Buchführung des Sicherheitsbeauftragten voraus. Darüber hinaus kann dieses System lediglich Aufschluss über den Personenkreis geben, der sich Zugang verschafft hat. Zeitangaben und eine genaue Zuordnung kann dieses

System ohne weitere technische Hilfsmittel am Schloss nicht leisten.

RFID Systeme sind „schick“ und praktisch. Die Karte muss nur kurz am Schloss vorbei geführt werden und schon ist es entriegelt. Zudem entfällt ein lästiges, sperriges Schlüsselbund das man mit sich herum tragen muss. Denn eine kleine Karte kann sehr präzise auf verschiedene Schlösser programmiert werden. Sollte eine Umstellung erforderlich sein kann mit wenigen Mausklicks eine Änderung im System hinterlegt werden. Leider lassen sich RFID Systeme sehr leicht manipulieren. Schon aus reiner Böswilligkeit, kann man mit starken Magneten Transponder beschädigen.

Passwörter oder Zahlenkombinationen können schnell mal zugerufen werden oder sind zu leicht zu durchschauen. Ist der Umgang mit solchen Schlüsseln jedoch gewissenhaft, sind diese eine gute Möglichkeit für Computer, Maschinen und Türen jeglicher Art. Wahlweise können auch Muster erkannt werden, was das ganze noch „hübscher“ macht.

Bei beiden, RFID und Passwörtern ist eine flexible Gestaltung der Zugriffsberechtigungen leicht darstellbar. Genaue Zeitangaben können gemacht werden.

3.2. Biometrische Systeme/ nicht vererbbar

Die Biometrie war ursprünglich eine mathematische Hilfswissenschaft, die dazu diente, Organismen zu vermessen und zu bewerten.[31] Im Lauf der Zeit entwickelte sich aus dieser Hilfswissenschaft ein eigenständiges Gebiet, das heute hauptsächlich im Zusammenhang mit Sicherheitstechnik immer mehr an Bedeutung gewinnt.

Biometrische Systeme zeichnen sich dadurch aus, dass bestimmte einzigartige Merkmale des Menschen genutzt werden, um eine eindeutige Identifikation durchzuführen. Durch moderne Datenverarbeitung ist es möglich, solche Merkmale zu erkennen und mit einer Datenbank abzugleichen. Das setzt also voraus, dass der

[31] Vgl. Bertelsmann Band 2, 1999, S.257.

Benutzer zunächst registriert wurde[32], um solche Merkmale als als Schlüssel zu verwenden. Dadurch ergeben sich zwei grundsätzliche Prozesse: die Registrierung und die Identifikation.

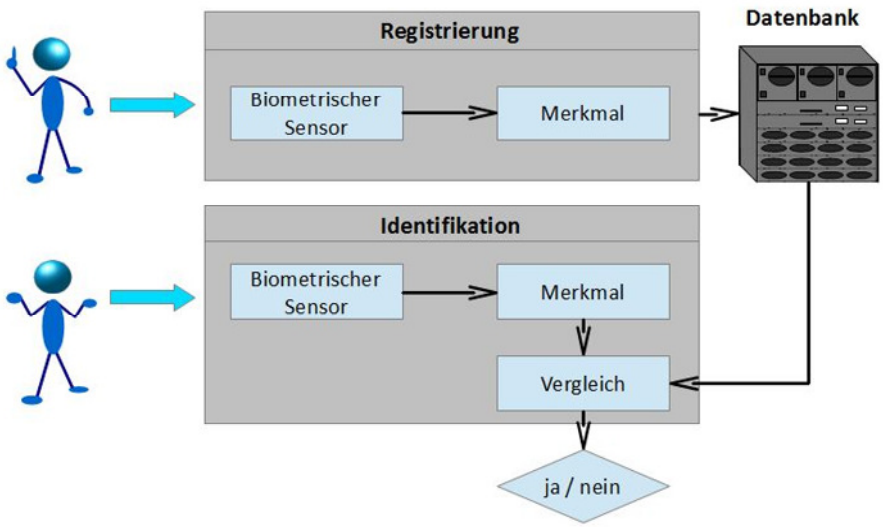

Abbildung 8: Grundsätzliche Funktion von biometrischen Systemen (Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.7.)

Das wohl bekannteste Beispiel ist der Fingerabdruck. Seit Ende des 19. Jahrhunderts wird er in der Kriminaltechnik als eindeutiges Identifikationsmerkmal eingesetzt.[33] Mittlerweile ist diese Methode sowohl im gewerblichen als auch im privaten Rahmen eine weit verbreitete Methode der Berechtigungsprüfung.

Die Identifikation bei solchen Systemen erfolgt schrittweise. Zunächst wird über einen Sensor das zu prüfende Merkmal eingelesen. Nach dieser Datenaufnahme werden die Informationen vorverarbeitet. Das bedeutet zum einen, dass die Merkmale in für den Computer verwertbare Daten umgewandelt werden müssen. Anschließend können die Daten mit gespeicherten Informationen in einer Referenzdatenbank abgeglichen und eine Entscheidung über Zugriff oder Verweigerung getroffen werden.[34]

Damit biometrische Merkmale zur Personenidentifikation genutzt werden können, müssen folgende Hauptbedingungen erfüllt sein:

· *Universalität:* Die Merkmale müssen bei jeder Person vorhanden sein.

[32]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.6.
[33]Vgl. Heindl, Robert: „System und Praxis der Daktyloskopie [...]“, 1922, S.63.
[34]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.6.

· *Einmaligkeit:* Das Merkmal muss für jede Person individuell sein.

· *Konsistenz:* Das Merkmal darf sich im Lauf der Zeit nicht wesentlich verändern.

· *Erfassbarkeit:* Das Merkmal muss quantitativ messbar sein.[35]

Hinzu kommen Nebenbedingungen, um die praktische Anwendung eines biometrischen Systems zu ermöglichen:

· *Leistungsfähigkeit:* Genauigkeit und Geschwindigkeit des Systems müssen akzeptabel sein.

· Das System selbst muss im praktischen Einsatz *akzeptiert* werden.

· *Überwindungssicherheit:* Das System muss ausreichend vor mutwilligen Manipulationen geschützt sein.[36]

Da die Merkmale zur Datenverarbeitung vereinfacht werden, um einen Abgleich durchzuführen, ist die Antwort auf den Vergleich kein klares „ja“ oder „nein“. Vielmehr gibt das System nach der Auswertung eine Wahrscheinlichkeit zurück, mit der das Merkmal mit dem in der Datenbank hinterlegten übereinstimmt. Man nutzt dafür den Schwellenwert zwischen der *Falschakzeptanzrate* FAR (False Acceptance Rate) und der *Falschrückweisungsrate* FRR (False Rejection Rate). Die FAR bezeichnet die Wahrscheinlichkeit, das unberechtigte Personen der Zugriff gewährt wird. Die FRR wiederum entspricht der Wahrscheinlichkeit, dass eine berechtigte Person nicht erkannt wird.[37]

[35]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.8.
[36]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.8.
[37]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.9.

3.2.1. Fingerabdruck Lesegeräte

3.2.1.1. Funktion von Fingerabdruck Lesegeräten

Anfangs rein in der Kriminalistik verwendet, spielen Fingerscanner eine immer größere Rolle.

Der menschliche Fingerabdruck ist für jede Person einzigartig. Die Papillarlinien, also die Muster bestehend aus Schleifen, Bögen und Wirbeln, sind so speziell, dass mit ihrer Hilfe Personen eindeutig identifiziert werden können. Weiterhin sind diese Merkmale von der Geburt bis zum Tode konstant.[38] Ein Grund, weshalb die *Daktyloskopie* seit über 100 Jahren weltweit das beliebteste Mittel für die polizeiliche Personenidentifikation ist.[39]

Heutzutage ist es natürlich nicht mehr notwendig, dass manuell „Papierdatenbanken" abgeglichen werden müssen – eine für Zugangskontrollen sehr unpraktikable Methode.

Damit der Fingerabdruck als Schlüssel genutzt werden kann, muss er zunächst von allen Personen, die das entsprechende Schloss öffnen dürfen, eingescannt und in einer Datenbank hinterlegt werden.

Um nun das das entsprechende Schloss zu öffnen beziehungsweise eine Maschine in Gang zu setzen, muss eine Scan-Vorrichtung angebracht sein. Diese liest den Fingerabdruck ein und wandelt ihn in digitale Signal um.[40] Der Rechner erkennt nun die Minutien, also Merkmale wie Wirbel, Gabelungen oder Enden.

[38]Vgl. Elster; Sieverts; Lingemann; Schneider: „Kriminalpolitik [...], Band 2", 1977, S.22.
[39]Vgl. Heindl, Robert: „System und Praxis der Daktyloskopie [...]", 1922, S.63.
[40]Vgl. Eisele: „Wie funktioniert ein Fingerabdruckscanner", 2013.

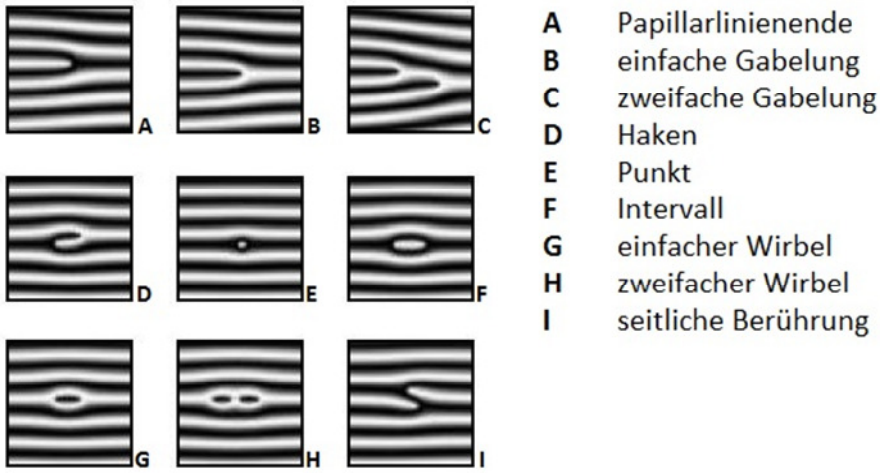

Abbildung 9: Beispiele für Minutien (Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.16.)

Da ein Computer nur verarbeiten kann, wofür er programmiert wurde, müssen die Minutien in mathematische Strukturen umgewandelt werden. Neben der Optimierung der Bildqualität werden die Positionen der Merkmale relativ zueinander in ein Koordinatensystem gesetzt[41]. Nun kann der eigentliche Vergleich beginnen.

In Deutschland gilt ein Finger als eindeutig zugeordnet, sobald zwölf Minutien übereinstimmen.[42] Der Rechner, der diese Aufgabe übernimmt, sucht nicht nur nach den Merkmalen an sich, sondern vergleicht auch ihre Position zueinander. Ist der Vergleich abgeschlossen, gibt das System „richtig“ oder „falsch“ als Antwort zurück.

3.2.1.2. Bewertung von Fingerabdruck-Systemen

Fingerabdrucklesegeräte sind eine recht sichere Methode, um Berechtigungen zu prüfen. Bei dieser Art der Personenidentifikation kommt es vor allem auf die Qualität der Technik an. 2002 erschien in der Frankfurter Allgemeinen Sonntagszeitung ein Artikel über den japanischen Mathematiker Tsutomoto Matsumoto. Dieser schaffte es mit den einfachsten Mitteln, die damals gängigen Fingerabdruckscanner zu überlisten.[43] Das besondere an seinem Vorgehen war, dass er die benötigte Gelatine

[41]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.16.
[42]Vgl. BSI: „Evaluierung biometrischer Systeme [...]“, 2004, S.17.
[43]Vgl. Schneider, Bruce: „Bärchen kommen überall hin“, 2002.

aus verflüssigten Gummibärchen gewann. Der Artikel weist auch darauf hin, dass Gelatine ähnliche physikalische Eigenschaften hat wie ein menschlicher Finger, zum Beispiel 23% Feuchtigkeit. So konnten auch Systeme von Matsumoto überlistet werden, die überprüfen, ob der Finger noch lebt.

Im Wesentlichen entwickelte er zwei Verfahren: Im ersten fertigte er einen Abdruck des Originalfingers an. Im zweiten machte er einen zurückgelassenen Fingerabdruck zunächst mit schwarzem Pulver auf einer Glasoberfläche sichtbar und fotografierte ihn ab. Nachdem dieses Foto am Computer nachbearbeitet wurde, wird es auf eine Folie gedruckt. Diese Folie dient als Maske für die Belichtung einer Leiterplatte mit einer UV-Lampe. Anschließend ätzte Matsumoto den Abdruck heraus verwendete ihn als Gussform für die Gummibärchen-Gelatine. Mit diesen „einfachen“ Methoden hatte Matsumoto selbst bei hochwertigen Geräten eine Erfolgschance von 68%.

Er liefert damit einen eindrucksvollen Beweis dafür, dass es für jedes vom Menschen geschaffene Problem eine Lösung gibt.

Prinzipiell ist eine Fingerabdruck-Kontrolle als Schlüssel sehr gut für die Betriebssicherheit geeignet, denn jeder Mensch hat einen Finger dabei. Weiterhin ist es durch die Individualität des Fingerabdrucks auch möglich, sehr feine Unterscheidungen in den Berechtigungen von verschieden Personen festzulegen. Dadurch ergibt sich gleichzeitig die Möglichkeit, Zeitpunkte des Zugriffs beziehungsweise Zugangs zu erfassen. Zudem sind Änderungen recht unkompliziert, da bei diesem System auf eine Datenbank zurückgegriffen wird. Sollten bei einzelnen Personen Berechtigungen hinzugefügt oder entfernt werden, muss diese lediglich aktualisiert werden. Ein mechanisches Umrüsten ist nicht erforderlich.

3.2.2. Augenscanner

Zunächst ein kurzer Exkurs in die Welt der Spionage: 1983 kam der James-Bond-Film "Sag niemals nie" in die Kinos. In ihm wird an einem ein Offizier der Air Force eine Hornhauttransplantation vorgenommen, um so Zugriff auf Nuklearsprengköpfen zu erhalten. Die transplantierte Hornhaut war eine Nachbildung derjenigen des

Präsidenten, welcher als einziger zugriffsberechtigt war.[44] Damals noch *science fiction,* werden der Augenscan und ähnliche Verfahren heutzutage in der Sicherheitstechnik tatsächlich angewendet.

Es gibt zwei verschiedene Ansätze, um das Auge als biometrisches Erkennungsmerkmal zu nutzen, wobei die Hornhaut zu keinem von ihnen gehört. Zum einen wird die Regenbogenhaut, zum anderen die Netzhaut abgetastet und verglichen. In diesem Abschnitt werden beide Systeme vorgestellt.

3.2.2.1. Iris - Scanner

Eine Version von Augenscannern verwendete das Bild der Iris, besser bekannt als Regenbogenhaut.

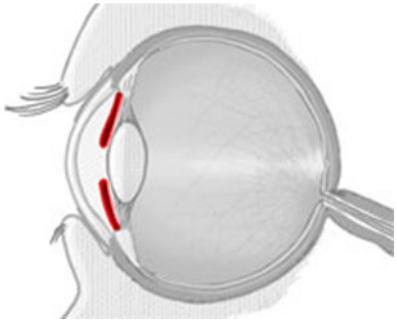

Abbildung 10: rot: die Regenbogenhaut (Iris) des Auges (Vgl. Lasikon.de: „Aufbau des menschlichen Auges“.)

1993 entwickelte John Daugman einen Algorithmus, mit dem kommerzielle Iris-Erkennungssysteme arbeiten. Dabei wird das aufgenommene Bild in einen 2kBit großes Informationspaket umgewandelt und mit Referenzmustern verglichen.[45]

[44]Vgl. IMDb.com: „James Bond - Sag niemals nie“.
[45]Vgl. Filatova; Keller: „Biometrische Identifikationsverfahren – Iriserkennung“, 2004.

3.2.2.2. Retina-Scanner

Die Netzhaut des Menschen ein einzigartiges Erkennungsmerkmal. Das entscheidende bei diesem System sind die Blutgefäße, welche die Retina durchziehen. Sie reflektieren Licht schlechter als die restlichen Nervenzellen, wodurch sie sich grafisch abbilden lassen.[46]

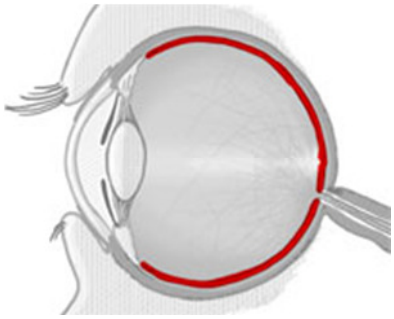

Abbildung 11: rot: die Netzhaut (Retina) im Auge (Vgl. Lasikon.de: „Aufbau des menschlichen Auges“.)

Ein Laser ist in der Lage, diese Netzhaut im Inneren des Auges durch die Linse hindurch abzutasten, um sie als Merkmal zur Identifizierung zu nutzen.[47]

3.2.2.3. Bewertung von Augenscannern

Beide relativ neuen Systeme werden von den Nutzern bisher nicht richtig akzeptiert. Zum einen mag hier der Science-Fiction-Charakter eine Rolle spielen, der bei solchen Methoden mitschwingt. Zum anderen könnte es sich um die Befürchtung handeln, dass ein Abtasten des Auges gesundheitliche Schäden mit sich bringt. Das ist nicht ganz unverständlich, bedenkt man, dass ein Laser das Innere des Auges abtasten soll. Außerdem sollte abhängig vom Anwendungsbereich überlegt werden, ob ein passives oder aktives System verwendet werden soll. Bei der passiven Erkennung muss der Nutzer die richtige Position zwischen Auge und Kamera einnehmen, um ein Abtasten zu ermöglichen. Das aktive System arbeitet etwas

[46]Vgl. Trösch, Thomas: „Der Netzhaut-Scanner für unterwegs“, 2014.
[47]Vgl. Trösch, Thomas: „Der Netzhaut-Scanner für unterwegs“, 2014.

benutzerfreundlicher, hier fokussiert die Abtasteinheit automatisch.[48]

Ein weiterer Nachteil sind die anfänglich hohen Kosten, welche die Einführung eines solchen Systems mit sich bringt.[49] Es gibt zwei Varianten von Lesegeräten: Stationäre und solche, die mit einem Netzwerk verbunden werden. Bei den Stationären muss die Datenbank manuell am Lesegerät aktualisiert werden, wohingegen die in einem Netzwerk befindlichen via Fernübertragung auf den neuesten Stand gebracht werden können. Sollte das Netzwerk allerdings ausfallen, funktioniert die gesamte Schließanlage nicht mehr. Dadurch sind die Folgekosten eine schwierige Kalkulation. Nachträgliche Änderungen wie das Aufnehmen neuer Personen oder die Abwandlung von Sicherheitskreisen sind durch einfache Datenbankänderungen möglich. Muss man nun alle stationären Lesegeräte manuell mit diesen Änderungen versorgen, kommt es auf die Anzahl der Terminals an. Über ein Netzwerk wäre dies ohne Zeitverzögerung möglich.[50]

Das größte Problem bei der Iris-Erkennung besteht noch immer darin, dass es möglich ist, solche Systeme mit Hilfe von Fotos zu manipulieren. Bereits 2002 schaffte es das Magazin *c't* in einem Test Iris-Scanner mit ausgedruckten Fotos zu überlisten.[51] Zehn Jahre später scheint dieses Problem noch nicht gelöst zu sein, wie Stefan Krempl vom Onlinemagazin *heise.de* in einem Artikel berichtet.[52]

Der Retinascanner hingegen ist schwerer zu überlisten. Jedoch werden bei diesem System immer wieder die hohen Anschaffungskosten und die Fehlerrate bei Kontaktlinsen angesprochen[53].

Der Einsatz von der Augenerkennung ist sehr vielseitig. Vom Türschloss bis zur Aktivierung von Maschinen lässt sich ein solches System etablieren. Bei Maschinen könnte man den zusätzlichen Vorteil nutzen, dass der Scanner den Bediener die gesamte Zeit über im Fokus behält, um so die Müdigkeit beziehungsweise Aufmerksamkeit zu überwachen. Ähnliche Anwendungen werden in der Automobilbranche getestet.[54]

---

[48]Vgl. Wohlfahrt, Eva: „Vor- und Nachteile der Iriserkennung“.
[49]Vgl. von Graevenitz, Gerik: „Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren“, 2006, S.167.
[50]Vgl. Wohlfahrt, Eva: „Vor- und Nachteile der Iriserkennung“.
[51]Vgl. Thalheim; Krissler; Ziegler: „Körperkontrolle [...]“, 2002.
[52]Vgl. Krempl, Stefan: „Iris-Scanner mit künstlich erzeugten Bildern ausgetrickst“, 2012.
[53]Vgl. Ottenberg, Jörg: „Retinaerkennungssysteme“.
[54]Vgl. Grünweg, Tom: „Volvo-Warnsystem: Bevor der Fahrer fahrig wird“, 2007.

3.2.3. Gesichtserkennung

Die Qualität und der Umfang der Gesichtserkennung hat in den letzten Jahren stetig zugenommen. So war es zwischenzeitlich möglich, auf Fotos, die man auf *facebook* einstellte, Freunde und Bekannte anhand von Vorschlägen zu markieren. Allerdings wurde dieses Funktion auf Drängen des Datenschutzbeauftragten der Europäischen Union in Europa entfernt.[55] Im Selbsttest überraschte die enorm hohe Trefferquote in Bezug auf die Genauigkeit der vorgeschlagenen Personen.

3.2.3.1. Funktion von Gesichtserkennung

Bei den Abtastverfahren des Gesichtes gibt es verschiedene Ansätze. Grundsätzlich wird in zwei Schritten vorgegangen. Zunächst muss das System erkennen, dass es ein Gesicht vor sich hat, um dieses danach zu bewerten.

Eine der rechenaufwändigsten Methoden ist das „Template Matching“. Das abgelesene Gesicht wird mit gespeicherten Templates, das heißt Masken, verglichen. Für diese Masken wird das Gesicht in kleine Teile zerlegt. Mund, Nase, Augen oder auch das gesamte Gesicht werden dabei mit Bildern verglichen, die sich in einer Datenbank befinden.[56]

Ein ähnliches Vorgehen benutzt die Identifizierung mit Hilfe von „geometrischen Merkmalen“. Dabei erkennt das System die einzelnen Bestandteile des Gesichtes anhand ihrer Position und Umrisse. Augen liegen nebeneinander, die Nase mittig unter den Augen und der Mund unter der Nase. Nachdem die Einzelteile des Gesichts erkannt wurden, werden diese vermessen. Die nun gewonnenen Informationen wie zum Beispiel der Abstand der Augen oder die Breite des Mundes können daraufhin mit Datenbankinformationen abgeglichen werden.[57]

Die Gesichtserkennung mit der „zwei-dimensionalen diskreten Fourier-

[55]Vgl. Gropp, Martin: „Facebook stoppt Gesichtserkennung“, 2012.
[56]Vgl. Wächter; Römer: „Gesichts-Erkennung I“, 2002.
[57]Vgl. Wächter; Römer: „Gesichts-Erkennung I“, 2002.

Transformation“ ist eine Vereinfachung der *Template Matching* Methode. Dabei wird das eingelesene Bild des zu überprüfenden Gesichts in den Frequenzbereich umgewandelt. Das Gesicht wird mathematisch zerlegt, umgewandelt und verglichen. Dadurch ergibt sich der Vorteil, dass weniger Rechenaufwand erforderlich ist.[58]

Beim „Face Bunch Graph“-Verfahren wird ein normiertes Gitter über das Gesicht gelegt. Die Knotenpunkte dieses Gitters werden auf bestimmte Merkmale wie zum Beispiel die Augen gelegt. Anschließend werden die Verbindungen zwischen diesen Knoten vermessen. Winkel und Abstand sind hier die Kerngrößen. Die so erfassten Informationen können mit Hilfe des Grundrasters normiert werden, wodurch dieses System weniger fehleranfällig für Drehungen des Kopfes ist.[59]

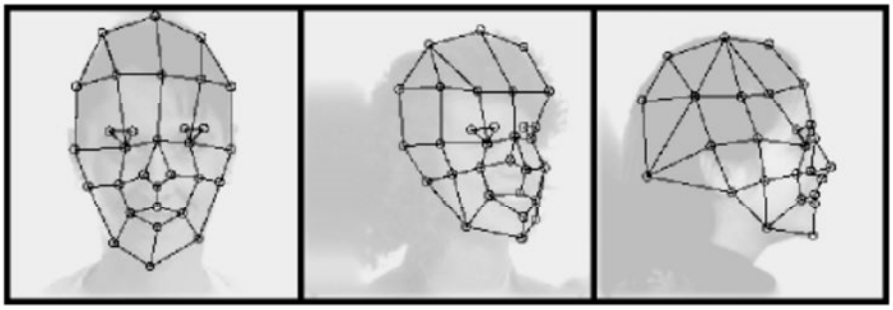

Abbildung 12: Face Bunch Graph (Vgl. Baur, Dominikus: „Automatische Gesichtserkennung: Methoden und Anwendungen”, 2006.)

Ein weiterer Ansatz zur Gesichtserkennung bildet die „Berechnung von Eigenfaces“. Bei dieser Methode wird nicht nur ein Referenzbild gespeichert, sondern gleich mehrere. Ein Computer beurteilt nun diese und beschränkt sich auf charakteristische Merkmale. Die Bilder des Probanden werden selbstständig auf markante Stellen untersucht und anschließend auf diese vereinfacht. Danach werden die Bilder wieder zu einem Ganzen zusammengefügt und als Referenzmuster abgespeichert. Diese Methode ermöglicht es, aus ungeordneten Bildern wie zum Beispiel Menschenmengen, Gesichter zu erkennen und zu identifizieren.[60]

Das sind die wesentlichen Funktionsweisen der Gesichtserkennung. Ebenfalls werden Kombinationen der verschiedenen Techniken angewendet, um höhere Genauigkeiten zu erzielen. So wird zum Beispiel die *geometrische*

[58]Vgl. Markus, Janda: „Verfahren der Gesichtserkennung mit holistischem Ansatz“.
[59]Vgl. Baur, Dominikus: „Automatische Gesichtserkennung: Methoden und Anwendungen”, 2006.
[60]Vgl. Schromm; Halder: „Gesichterkennung II – Eigenfaces“, 2002.

Gesichtserkennung meist verwendet, um die Anwesenheit eines Gesichts zu erkennen, bevor andere Mechanismen greifen.

3.2.3.2. Bewertung von Gesichtserkennung

Bei diesem System kommt es sehr stark auf die technische Ausstattung an. Neuere Systeme, die mit den neusten Algorithmen arbeiten, sind sehr zuverlässig. Das spiegelt sich allerdings entsprechend in den Anschaffungskosten wider. Spart man bei der Anschaffung, liegt die Fehlerrate unter Umständen hoch.

Zu den Hauptproblemen bei der Gesichtserkennung gehören für gewöhnlich eine heterogene Beleuchtung sowie der Aufnahmewinkel. Neuere Algorithmen versuchen verstärkt, diese Fehlerquellen zu eliminieren.[61]

Der Einsatz von Gesichtserkennung eignet sich sowohl in für Security als auch Safety. Da in den meisten Unternehmen ohnehin Kameras angebracht sind, lässt sich das System relativ einfach integrieren. In Firmen mit mehreren tausend Mitarbeitern wäre es so möglich, wesentlich schneller und genauer Betriebsfremde Personen zu erkennen beziehungsweise Alarm zu schlagen, wenn sich Mitarbeiter in einem Bereich aufhalten, für den sie nicht autorisiert sind. Bei großen Maschinenanlagen könnte auf diesem Weg ausgeschlossen werden, dass sich Personen in Gefahrenbereichen aufhalten.

Für die Strafverfolgung ist dieses System ebenfalls interessant, da es dadurch sehr einfach ist, große Menschenansammlungen zu überwachen.

Als Schlüssel für Bereiche und Anlagen ist die Gesichtserkennung ein einfacher Schlüssel – insbesondere, da dieser Schlüssel nicht vergessen werden kann.

Presseberichten zufolge stehen Googles Android und Apple vor einem großen Problem. Beide versuchten als Sperre für das Smartphone eine Gesichtserkennung zu etablieren. Jedoch lassen sich ihre Lösungsansätze mit einfachen Fotos der

[61] Vgl. Otten, Bettina: „3D Gesichtserkennung“, 2006, S.23.

berechtigten Nutzer austricksen.[62]

Allem Anschein nach ist dies ein verbreitetes Problem bei der Gesichtserkennung: Die Unterscheidung zwischen einem authentischen Gesicht und einer Aufnahme, mithin also zwischen lebend und tot. Viele Systeme können tatsächlich mit Fotos überbrückt werden.[63] Duncan Graham-Rowe hat dieses Problem in einem Artikel zusammengefasst. Es gibt zwar verschiedene Lösungsansätze, doch alle weisen Lücken auf.

Ein erster Ansatz besteht darin, die Ähnlichkeit zwischen gespeichertem und erfasstem Bild zu vergleichen. Sind sich beide Aufnahmen zu ähnlich, wird der Zugriff verweigert. Rowe schlägt in seinem Artikel vor, wie das Problem umgangen werden kann: Indem per Fotoshop bewusst einige Fehler in das Bild eingefügt werden, kann diese Schutzfunktion überbrückt werden.

Ein weiterer Ansatz besteht darin, kleinste Bewegungen zu erfassen. Sind die Bewegungen zu linear, wird das Bild abgewiesen. Laut Rowe kann auch dieser Schutz beseitigt werden – etwa, indem man das Foto leicht biegt. Das reiche in der Regel aus, um eine ausreichende Verzerrung zu erzeugen. Problematisch könnte hier die Abweisung von berechtigten Personen werden, da sie ihr Gesicht zu wenig bewegen.

Versuchsweise wurden auch Augenaufschläge als „Lebendmerkmal“ herangezogen. Jedoch stellt dies keine optimale Lösung dar. Mit einer Videoaufnahme des Gesichtes kann auch dieser Ansatz umgangen werden. Der Schwede Josef Bigun versucht, das zweidimensionale Bild in eine dreidimensionale Darstellung umzuwandeln. Dies geschieht über eine Software, die er entwickelt. Dabei sollen auch hier kleinste Bewegungen erkannt werden. Dieser Lösungsansatz soll das Foto nun endgültig erkennen. Da laut Bigun das biegen des Bildes nun nicht mehr ausreichen soll. In ersten Versuchen erreichte er mit seinem Verfahren gute Ergebnisse, eine Fehlerrate von 0,5%[64].

[62]Vgl. Arnold, Arne: „So entsperren Sie Ihr Smartphone sicher“, 2014.
[63]Vgl. Graham-Rowe, Duncan: „Biometrie: Tot oder lebendig?“, 2007.
[64]Vgl. Graham-Rowe, Duncan: „Biometrie: Tot oder lebendig?“, 2007.

3.2.4. Abschließend zu den biometrischen Verfahren

Auch biometrische Mittel der Personenidentifikation sind nicht hundertprozentig sicher. Sie bieten den großen Vorteil, dass der Schlüssel nicht so leicht weitergegeben oder vergessen werden kann. Wohin gegen gerade dies ein Manko ist, bedenkt man die noch geringe Akzeptanz solcher Systeme. Gerade passive Augenscanner erfordern einen zu starken Eingriff in die „Wohlfühlzone“ des Menschen. Auch gibt es speziell beim Retinascanner ein starkes Bedenken von Seiten des Datenschutzes, beispielsweise, da Augenscanner theoretisch Krankheiten wie Diabetes erkennen könnten.[65] Denn mit einem Augenspiegel macht ein Arzt nichts anderes – er untersucht die Netzhaut im Inneren des Auges auf eventuelle Symptome.[66] Die Diskussion hinsichtlich des Datenschutzes existiert für alle biometrischen Verfahren.

Diese Art von technischen Systemen ist sehr flexibel, was die nachträgliche Konfiguration betrifft. Es gilt jedoch zu beachten, auf welchem Weg der Abgleich stattfindet. Entweder es sind alle Datenterminals über ein Netzwerk mit einem zentralen Server verbunden oder jedes Terminal für sich ist im Besitz der benötigten Referenzdatenbank. Bei jeder dieser Möglichkeiten gibt es ein Problem: Werden die Daten zentral abgeglichen, kann es zu Problemen kommen, falls das entsprechende Netzwerk außer Funktion sein sollte. Müssen die Terminals manuell bei jeder Datenbankaktualisierung neu gespeist werden, kann dies enorme Kosten und einen erheblichen Zeitaufwand verursachen. Weiterhin würde dies zu einer Sicherheitslücke führen, da an der Konsole selbst eine Datenschnittstelle angebracht sein müsste. Ein Kompromiss zwischen beiden Systemen wäre eine Netzwerkverbindung, die beispielsweise einmal pro Stunde ein Datenupdate schickt. Ein derartiges „schlaues“ Update würde nicht die gesamte Datenbank erneuern, sondern nur neue Pakete ersetzen. Auf diese Weise wäre Terminal nicht zu lange außer Betrieb gesetzt. Des Weiteren muss sichergestellt werden, dass die Aktualisierungen der Datenbanken nur von berechtigten Benutzern vorgenommen werden.

[65]Vgl. Maier, Josephina: „Verräterischer Blick“, 2009.
[66]Vgl. Dr. med. Döring-Coen, Christine: „Untersuchung des Augenhintergrundes [...]“, 2014.

4. Auswertung der Vorgestellten Verfahren

Nach diesem kurzen Einblick in die technischen Möglichkeiten der Personenidentifikation werden die vorgestellten Systeme einander gegenübergestellt. Die getroffenen Bewertungen entstehen subjektiv anhand des zuvor erarbeiteten Wissensstandes.

Zunächst muss festgelegt werden, welche Größen von Bedeutung sind.

Die beiden ersten Faktoren stellen die Einsatzmöglichkeiten in den Bereichen Security und Safety dar. Hierbei ist die Breite der Anwendungsmöglichkeiten ausschlaggebend.

Die allgemeine Sicherheit gibt Auskunft darüber, wie tauglich das System im Normalbetrieb ist.

Ein weiteres Kriterium ist die Manipulationssicherheit von innen und außen. Die Manipulation von innen muss nicht unbedingt schadhaft gemeint sein, jedoch ist es eine Verletzung der Sicherheitsrichtlinien, wenn Informationen oder Gegenstände an andere weitergegeben werden.

Ebenfalls wird die Fehleranfälligkeit betrachtet.

Auch die Kosten sind von Interesse. Hierbei werden Anschaffung und Nachrüsten als separate Faktoren betrachtet.

Die folgende Tabelle 2 stellt diese Kerngrößen zusammenfassend dar. Zu den einzelnen Systemen sind zusätzlich positive und negative Aspekte aufgeführt, die besonders herausstachen.

	Schlüssel	RFID	Wissen	Finger-Abdruck	Iris	Retina	Gesichts-Erkennung
Security	ja	ja	ja	ja	ja	ja	ja
Safety	ja	ja	ja	ja	bedingt	bedingt	ja
allg. Sicherheit (bei richtiger Benutzung)	hoch	hoch	sehr hoch	sehr hoch	sehr hoch	sehr hoch	hoch
Manipulation							
von Innen (Angestellte)	- Weitergabe - Verlust	- Weitergabe	- Weitergabe	- bewusste Manipulation	- bewusste Manipulation	- bewusste Manipulation	- bewusste Manipulation
von Außen (Dritte)	- Schloss unbrauchbar machen + Schlüssel sind schwer nach Zu bilden	+ man benötigt Transponder für Referenzdaten - leicht störbar	+ nur durch erfragen Zugänglich - nur durch erfragen zugänglich	- Nachbildung	- kann mit einem Foto Überlistet werden	+ kaum/ schwer	- kann mit einem Foto Überlistet werden
Fehleranfälligkeit							
Falscherkennung	- kann nicht zuordnen Wer den Schlüssel benutzt	- kann nicht zuordnen Wer den Schlüssel benutzt	- kann nicht zuordnen Wer den Schlüssel benutzt	- je nach Einstellung gering	- je nach Einstellung gering	- je nach Einstellung gering	- Fehleranfällig durch Makeup, Sonnenbrillen und Frisuren
Funktionsstörung	- Schlüssel Defekt (verbogen) - Schloss verstopft	- Systemausfall (Netzwerk, Strom)	- Passwort Vergessen	- Systemausfall (Netzwerk, Strom)	- Systemausfall (Netzwerk, Strom)	- Systemausfall (Netzwerk, Strom)	- Systemausfall (Netzwerk, Strom)
Kosten							
Anschaffung	- Schlösser und Schlüssel	- Terminals und Transponder	+ gering (Computer) - Terminals für Türen	- Lesegeräte und Server	- Lesegeräte und Server	- Lesegeräte und Server	- Lesegeräte und Server
Nachrüsten	- teuer (Verlust eines General-schlüssels)	+ gering (Datenbank Änderung)	+ gering (Datenbank Änderung)	+ gering (Datenbank Änderung)	+ gering (Datenbank Änderung)	+ gering (Datenbank Änderung)	+ gering (Datenbank Änderung)

Tabelle 2: Zusammenfassung der vorgestellten Methoden

Die Informationen sind mitunter schwer überschaubar. Auch die Bewertung ist eine Herausforderung. Deswegen werden die einzelnen Kriterien bewertet. Dazu werden Noten von fünf (sehr gut) bis eins (schlecht) vergeben. Diese Reihenfolge bietet sich an, da man zum Schluss die Noten addieren kann, um einen ersten Überblick zu bekommen. Auch werden die Mittelwerte der erhaltenen Noten als weitere Bewertungshilfe angegeben. Damit ergibt sich folgende Tabelle 3.

	Schlüssel	RFID	Wissen	Finger	Iris	Retina	Gesicht
Security	5	5	5	5	5	5	4
Safety	5	5	5	5	2	2	3
allg. Sicherheit (bei richtiger Benutzung)	4	4	4	4	4	5	4
Manipulation							
von Innen (Angestellte)	1	1	1	5	5	5	4
von Außen (Dritte)	3	2	3	3	3	5	3
Fehleranfälligkeit							
Falscherkennung	2	2	2	2	2	2	2
Funktionsstörung	4	4	3	3	3	3	3
Kosten							
Anschaffung	3	3	4	2	1	1	3
Nachrüsten	1	4	4	4	4	4	4
Summe:	**28**	**30**	**31**	**33**	**29**	**32**	**30**
Mittel:	**3,11**	**3,33**	**3,44**	**3,67**	**3,22**	**3,56**	**3,33**

Tabelle 3: Bewertung der Systeme

5= sehr gut; 4= gut; 3= mittel; 2= schlecht; 1= nein/ nicht vorhanden

Man sieht schon deutlicher, wodurch sich die einzelnen Systeme auszeichnen oder nicht. Jedoch liegen die Summen und Mittelwerte so dicht beieinander, dass hier noch keine klare Aussage über das Abschneiden getroffen werden kann.

Daher werden als nächstes die Bewertungskriterien in ein Verhältnis zueinander gesetzt. Bisher wurde davon ausgegangen, dass alle betrachteten Faktoren das gleiche Gewicht haben. Dies trifft aber nicht zu, zum Beispiel sind die Anschaffungskosten nicht so entscheidend für ein System wie die Manipulationssicherheit. Die Faktoren werden deshalb betrachtet ihnen ein Rang zugeordnet. Dieser Rang dient gleichzeitig als Faktor zur Gewichtung. Deshalb ist die Wertigkeit umso höher, je großer der zugeordnete Rang ist.

	Rang
Allgemeine Sicherheit (bei richtiger Benutzung)	9
Manipulation von Außen	8
Falscherkennung	7
Funktionsstörung	6
Manipulation von Innen	5
Anwendungsmöglichkeiten Security	4
Anwendungsmöglichkeiten Safety	3
Kosten des Nachrüstens	2
Kosten der Anschaffung	1

Tabelle 4: Rangfolge der betrachteten Kriterien

Wie ergibt sich diese Sortierung? An erster Stelle steht natürlich die Allgemeine Sicherheit, da die Systeme genau dies liefern sollen. Als nächster Punkt kommt die Manipulationssicherheit von Außen, da in der Regel davon ausgegangen werden kann, dass ein Angriff auf ein Sicherheitssystem von Dritten durchgeführt wird. Falscherkennung und Funktionsstörungen nehmen hier die Plätze sieben und sechs ein. Das System muss zuverlässig arbeiten, um den Betriebsfluss nicht zu stören. Die Manipulationssicherheit von Innen folgt auf Rang fünf. Denn nur wenn auf die eigenen Mitarbeiter Verlass ist, kann ein Sicherheitssystem zuverlässig arbeiten. Die Anwendungsmöglichkeiten in den Bereichen Security und Safety liegen auf den hinteren Plätzen vier und fünf. Dass ein System keine Anwendung in einem der Bereiche findet, sagt nichts über dessen Leistungsfähigkeit aus. Security wird eine Note besser eingestuft, da der Zugang zu einigen Bereichen bereits als Maßnahme der Safety bewertet werden kann. Auf den letzten Rängen finden sich die Kosten. Diese sollten nicht im Vorderpunkt stehen, wenn man sich für ein Sicherheitssystem entscheidet. Hier werden die Anschaffungskosten auch niedriger bewertet als die Kosten für nachträgliche Änderungen. Dies liegt daran, dass die Anschaffung nur einmal getätigt werden muss und Änderungen sich im Lauf der Zeit, also über Jahre, aufsummieren können.

Die Systeme wurden innerhalb der betrachteten Kriterien benotet. Ebenfalls wurde eine Rangfolge und somit eine Wertigkeit der Faktoren bestimmt. Im nächsten Schritt sollen diese beiden Matrizen zusammengeführt werden. Dabei wird die Note der Systeme mit der Rangfolge der Bewertungskriterien multipliziert.

	Rang	Schlüssel	RFID	Wissen	Finger	Iris	Retina	Gesicht
Security	4	4 x 5 = 20	4 x 5 = 20	4 x 5 = 20	4 x 5 = 20	4 x 5 = 20	4 x 5 = 20	4 x 4 = 16
Safety	3	3 x 5 = 15	3 x 5 = 15	3 x 5 = 15	3 x 5 = 15	3 x 2 = 6	3 x 2 = 6	3 x 3 = 9
allg. Sicherheit (bei richtiger Benutzung)	9	9 x 4 = 36	9 x 4 = 36	9 x 4 = 36	9 x 4 = 36	9 x 4 = 36	9 x 5 = 45	9 x 4 = 36
Manipulation								
von Innen (Angestellte)	5	5 x 1 = 5	5 x 1 = 5	5 x 1 = 5	5 x 5 = 25	5 x 5 = 25	5 x 5 = 25	5 x 4 = 20
von Außen (Dritte)	8	8 x 3 = 24	8 x 2 = 16	8 x 3 = 24	8 x 3 = 24	8 x 3 = 24	8 x 5 = 40	8 x 3 = 24
Fehleranfälligkeit								
Falscherkennung	7	7 x 2 = 14	7 x 2 = 14	7 x 2 = 14	7 x 2 = 14	7 x 2 = 14	7 x 2 = 14	7 x 2 = 14
Funktionsstörung	6	6 x 4 = 24	6 x 4 = 24	6 x 3 = 18	6 x 3 = 18	6 x 3 = 18	6 x 3 = 18	6 x 3 = 18
Kosten								
Anschaffung	1	1 x 3 = 3	1 x 3 = 3	1 x 4 = 4	1 x 2 = 2	1 x 1 = 1	1 x 1 = 1	1 x 3 = 3
Nachrüsten	2	2 x 1 = 2	2 x 4 = 8	2 x 4 = 8	2 x 4 = 8	2 x 4 = 8	2 x 4 = 8	2 x 4 = 8
Summe:		**143**	**141**	**144**	**162**	**152**	**177**	**148**
Mittel:		**15,89**	**15,67**	**16,00**	**18,00**	**16,89**	**19,67**	**16,44**

Tabelle 5: Zusammenführung von Rangfolgen und Noten

Die neu entstandene Tabelle 5 gibt Aufschluss darüber, wie die vorgestellten Systeme in Verbindung mit den betrachteten Bewertungskriterien zueinander stehen.

ohne Gewichtung	
Finger	33
Retina	32
Wissen	31
RFID	30
Gesicht	30
Iris	29
Schlüssel	28

mit Gewichtung	
Retina	177
Finger	162
Iris	152
Gesicht	148
Wissen	144
Schlüssel	143
RFID	141

Tabelle 6: Vergleich der Bewertungen mit und ohne Gewichtung

Es fällt auf, dass sich in Folge der Gewichtung die Plätze der Bewertung verschieben. Bevor den Bewertungskriterien eine Rangfolge zugeordnet wurde, war der Fingerabdruck noch knapp in Führung, jedoch wurde dieser nach der Gewichtung vom Retinascanner deutlich abgelöst. Das RFID-System rutscht vom vierten auf den letzten Platz. Dies liegt daran, dass die Manipulation von Dritten, die sich bei diesem System recht einfach darstellt, sehr stark in die Bewertung einfließt.

Weiterhin fällt auf, dass die biometrischen Verfahren nun die Tabelle anführen. Dies

liegt am großen Nachteil, den alle nicht-biometrischen Verfahren haben. Die Tatsache, dass bei diesen Systemen der Schlüssel einfach weitergegeben werden kann, stellt eine markante Sicherheitslücke dar.

Die Nachteile bei den Augenerkennungen ist die Handhabung im Bereich Safety. Speziell der Retinascan ist jedoch das am meisten gegen Fremdzugriff gewappnete System. Der Irisscan hingegen ist technisch so unausgereift, dass noch immer Fotos in der Lage sind das System zu überlisten.

Man kann abschließend sagen, dass biometrische Systeme grundsätzlich die bessere Alternative darstellen. Bei der Anwendung dieser Verfahren muss jedoch immer eine Rücksprache mit der Arbeitnehmervertretung statt finden um den Interessen des Datenschutzes nachzukommen.

5. Die Wahl der Qual

Wohin soll man als Unternehmen tendieren, steht man vor der Wahl: biometrisch oder nicht? Das Erstellen eines Sicherheitskonzeptes sollte wohl überlegt sein. Wie stark ist das Sicherheitsbedürfnis ausgeprägt und sinnvoll?

Für den kleinen oder mittleren Bedarf sollte man von den Augenscannern absehen. Akzeptanz, Anschaffungskosten und Handhabung lassen ihn hier ausscheiden. Der Fingerabdruck und die Gesichtserkennung bieten hier eine annehmbare Alternative möchte man im kleinen Rahmen auf Biometrie setzen. Die Gesichtserkennung ist auch leicht zu etablieren. Die zumeist ohne hin vorhanden Kameras können als Lesegerät verwendet werden können. Das bedeutet, dass lediglich neue Software installiert werden muss um sie zu verwenden. Auch eignet sie sich hervorragend um größere Menschenmengen im Auge zu behalten. Von den vererbbaren Methoden bietet sich, trotz schlechtem Abschneiden, ein RFID System an. Die geringen Kosten für nachträgliche Änderungen und die enorme Flexibilität machen RFID sehr attraktiv. Einziger Nachteil ist die leichte Manipulierbarkeit und das Problem der Weitergabe. Positiv ist natürlich das breite Anwendungsspektrum von RFID. Sowohl Security als auch Safety können mit dessen Hilfe abgedeckt werden. Weiterhin ist das System

leicht Erweiterbar und Änderbar. Sollte der Arbeitscomputer nicht mit einem Fingerabdruck Lesegerät ausgestattet sein, eignen sich Passwörter für die vorübergehende Sperrung.

Sollte im Unternehmen hoher Anspruch an die Sicherheit bestehen, kommt man an einem Retinascanner nicht vorbei. Dieses System ist nur schwer zu manipulieren und bei richtiger Konfiguration sehr zuverlässig. Grundsätzlich bietet es sich bei hohen Ansprüchen an, auf biometrische Verfahren zurückzugreifen, um die Schwachstelle Mitarbeiter zu überwinden. Jedoch darf bei den biometrischen Systemen nicht in der Anschaffung gespart werden um eine hohe Zuverlässigkeit zu gewährleisten.

Für den Bereich Safety, speziell den Personenschutz eignen sich am besten RFID Systeme. Der Transponder kann neben der Schlüssel-Funktion auch zur Ortsbestimmung von Personen verwendet werden. Bis auf die Augenerkennung kommen alle hier Vorgestellten Systeme für eine Anwendung im Bereich Safety in Frage. Will man hier Biometrie als Erkennungsmerkmal anwenden, so bietet sich der Fingerabdruck als komfortabelste Lösung an.

Für die Security sollte als Mittel der Personenidentifikation ein Umdenken stattfinden. Der klassische Schlüssel, der immer noch am verbreitetsten ist, sollte nach und nach abgelöst werden. Den größten Nachteil bilden die Kosten im Falle von nachträglichen Änderungen. Kommt im schlimmsten Fall ein Generalschlüssel abhanden, führt nichts daran vorbei das alle Schlösser manuell umgearbeitet werden müssen. Will man allerdings keine biometrischen Systeme anwenden, sollte man zumindest RFID in Betracht ziehen. In diesem Fall wäre der verlorene Generalschlüssel innerhalb von Minuten zu ersetzen und der alte entwertbar.

Hat man sich für ein System entschieden muss man seinen Mitarbeitern bewusst machen das das Thema Betriebssicherheit jeden betrifft. Schlüssel dürfen nicht weitergegeben oder unachtsam liegen gelassen werden. Zumindest muss ein klarer Prozess definiert sein, unter welchen Umständen eine Weitergabe zulässig ist. Des Weiteren ist es von Vorteil wenn die Angestellten auch darauf sensibilisiert sind Spuren oder Versuche von Manipulation zu melden.

Die gezeigten Manipulationsmöglichkeiten und das Bestreben neue Optionen zur Umgehung zu finden zeigt eins. – Ein von Menschen geschaffenes Sicherheitssystem ist nur solange sicher bis eine anderer eine Lücke findet.

Egal wie gut die Sicherheit in einem Unternehmen konzipiert ist. Was die Security angeht stehen alle vor dem selben Problem. Solange der Müll nicht von den entsprechenden Mitarbeitern selbst entsorgt wird, nutzen die größten Bemühungen nichts. Reinigungskräfte müssen für jeden Bereiche eine Freigabe erhalten, in dem sie arbeiten müssen.

V Quellenverzeichnis

Albrechtsen, Eirik: „Security vs safety“, Veröffentlichung, NTNU - Trondheim, Norwegen, August 2003.

Amitay, Daniel: „Most Common iPhone Passcodes“, 13.6.2011, http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, Aufruf: 14.09.2014.

Arnold, Arne: „So entsperren Sie Ihr Smartphone sicher“ in: PC-Welt, 27.02.2014.

bauidee Redaktion: „So funktioniert ein Zylinderschloss“, http://www.selbst.de/bauen-renovieren-artikel/einbruchschutz/haussicherheit/so-funktioniert-ein-zylinderschloss-109967.html, Aufruf: 01.09.2014.

Baur, Dominikus: „Automatische Gesichtserkennung: Methoden und Anwendungen”, Veröffentlichung, Universität München, 2006.

brooks-rfid.com: „RFID Technik“, http://www.brooks-rfid.com/rfid-technik.html, Aufruf: 04.09.2014.

BSI - Bundesamt für Sicherheit in der Informationstechnik: „Evaluierung biometrischer Systeme Fingerabdrucktechnologien – BioFinger“, Öffentlicher Abschlussbericht, Bundesamt für Sicherheit in der Informationstechnik, 06.08.2004.

dict.cc: „safety“, http://www.dict.cc/?s=Safety&failed_kw=savety, Aufruf: 20.08.2014.

dict.cc: „security“, http://www.dict.cc/?s=security, Aufruf: 20.08.2014.

Die grosse Bertelsmann Lexikothek – Bertelmann Lexikon Band 2, Verlagsgruppe Bertelsmann, 1999.

Die grosse Bertelsmann Lexikothek – Bertelmann Lexikon Band 7, Verlagsgruppe Bertelsmann, 1999.

Dr. med. Döring-Coen, Christine: „Untersuchung des Augenhintergrundes (Ophthalmoskopie)“ in: netdoktor.de, 20.02.2014.

Dr.-Ing. Ulrich, Rainer: „Biometrie in der IT-Sicherheit“, 2000, http://ikt-forum.de/system/files/Biometrie%20in%20der%20IT-Sicherheit.pdf, Aufruf: 06.10.2014.

duden.de : „Schlüssel, der“, http://www.duden.de/rechtschreibung/Schluessel, Aufruf: 20.08.2014.

Eisele, Sandro: „Wie funktioniert ein Fingerabdruckscanner (Infografik)?“, 03.11.2013, http://www.digitalweek.de/technik/wie-funktioniert-ein-fingerabdruckscanner-infografik/, Aufruf: 15.09.2014.

Elster, Alexander; Sieverts, Rudolf; Lingemann, Heinrich; Schneider, Hans Joachim: „Kriminalpolitik - Rauschmittelmißbrauch, Band 2“, Walter de Gruyten, 1977.

evva.de: „Was bedeutet Nachschlüsselsicherheit genau?“, http://www.evva.de/services/faq-sicherheitstechnik/nachschluesselsicherheit/de/, Aufruf: 08.09.2014.

Fakir, Simon: „Unterschied RFID und NFC – Eine kurze Erklärung“, http://www.fakir.it/aktuelles/detail/items/unterschied-rfid-und-nfc-eine-kurze-erklaerung.html, Aufruf: 12.09.2014.

Filatova, Elena; Keller, Roman: „Biometrische Identifikationsverfahren – Iriserkennung“, Vortrag, Humboldt Universität zu Berlin – Institut für Informatik, 2004.

fremdwort.de: „Schloss“, http://www.fremdwort.de/suchen/bedeutung/Schloss, Aufruf: 20.08.2014.

Graham-Rowe, Duncan: „Biometrie: Tot oder lebendig?“ in: Technology Review, 06.08.2007.

Gropp, Martin: „Facebook stoppt Gesichtserkennung“ in: Frankfurter Allgemeine, 21.09.2012, Frankfurt.

Grünweg, Tom: „Volvo-Warnsystem: Bevor der Fahrer fahrig wird“ in: Spiegel Online Auto, 04.09.2007, Hamburg.

hasa.de: „Das Prinzip einer mechanischen Schließanlage“, http://www.hasa.de/SAMechErkl.html, Aufruf: 04.09.2014.

Heindl, Robert: „System und Praxis der Daktyloskopie und der sonstigen technischen Methoden der Kriminalpolizei“, Walter de Gruyten, 1922.

Hohenauer, Florian: „Fujitsu bringt neuen Chip für Hochfrequenz-RFID-Tags mit branchenweit führenden 9 KB FRAM auf den Markt“, 04.10.2012, http://www.fujitsu.com/emea/news/pr/fseu-de_20120904-1035-fujitsu-fram-rfid.html, Aufruf: 08.09.2014.

IMDb.com: „James Bond - Sag niemals nie“, 1983, http://www.imdb.com/title/tt0086006/plotsummary?ref_=tt_ql_6, Aufruf: 16.09.2014.

Kandler, Hans-Christoph: Rechtliche Rahmenbedingungen Biomedizinischer Forschung Am Menschen: Das Zusatzprotokoll Zum Übereinkommen Über Menschenrechte und Biomedizin Über Biomedizinische Forschung, Springer-Verlag, 2008.

Kern, Christian: „Anwendung von RFID-Systemen“, Springer Science & Business Media, 2006.

kleines-lexikon.de : „Kryptografie“, 09.12.1998, http://www.kleines-lexikon.de/w/k/kryptografie.shtml, Aufruf: 20.08.2014.

Krempl, Stefan: „Iris-Scanner mit künstlich erzeugten Bildern ausgetrickst“, 31.07.2012, http://www.heise.de/security/meldung/Iris-Scanner-mit-kuenstlich-erzeugten-Bildern-ausgetrickst-1656681.html, Aufruf: 24.09.2014.

kstools.com: „Schulungscenter“, http://www.kstools.com/de/schulungscenter.html, Aufruf: 14.09.2014.

Lasikon.de: „Aufbau des menschlichen Auges“, http://www.lasikon.de/auge/aufbau-des-auges.php, Aufruf: 24.09.2014.

Leinenbach, Jens: „RFID - Manipulationsmöglichkeiten – Datensätze sind Datenschätze“, http://www.ccc-hanau.de/documents/RFID.pdf, Aufruf: 12.09.2014.

Maier, Josephina: „Verräterischer Blick“ in: Zeit Wissen, Nr. 03/2009.

Markus, Janda: „Verfahren der Gesichtserkennung mit holistischem Ansatz“, http://www.arlbergnet.com/design/biometrics/face/fs_face05.htm, Aufruf: 04.10.2014.

Matheus, Daniel; Klumpp, Matthias: „ild Schriftenreihe Logistikforschung Band 4 - Radio Frequency Identification (RFID) in der Logistik“, Arbeitspapiere der FOM, FOM - Fachhochschule für Oekonomie & Management - Institut für Logistik- & Dienstleistungsmanagement – Schriftenreihe Logistikforschung, Februar 2008.

Müller-Lancé, Johannes: Latein für Romanisten: ein Lehr- und Arbeitsbuch, Gunter Narr Verlag, 2006.

Otten, Bettina: „3D Gesichtserkennung - Merkmalsdetektion in 3D-Scans und merkmalsbasierter Vergleich von Gesichtern“, Diplomarbeit, Universität Koblenz-Landau, März 2006.

Ottenberg, Jörg: „Retinaerkennungssysteme“, Veröffentlichung, Humboldt Universität zu Berlin – Institut für Informatik.

Prof. Dr. Sikora, Axel: „Einführung in die Kryptographie“, 25.06.2003, http://www.tecchannel.de/sicherheit/management/402017/einfuehrung_in_die_kryptographie/index2.html, Aufruf: 20.08.2014.

Rathgeber, Isabel: „Werbung von gestern bis morgen: Die Akzeptanz personalisierter Werbung“, diplom.de, 2004.

rfid-basis.de: „Aufbau und Funktionsweise von RFID-Systemen“, http://www.rfid-basis.de/funktionsweise.html, Aufruf: 04.09.2014.

rfid-basis.de: „Reichweite“, http://www.rfid-basis.de/reichweite.html, Aufruf: 08.09.2014.

rfid-journal.de: „RFID Geschichte“, http://www.rfid-journal.de/rfid-geschichte.html, Aufruf: 04.09.2014.

rfid-loesungen.com: „RFID Übersicht“, http://www.rfid-loesungen.com/RFID_Uebersicht.htm, Aufruf: 12.09.2014.

Schneider, Bruce: „Bärchen kommen überall hin“ in: Frankf. Allg. Sonntagszeitung, 19.05.2002, Nr.5, Hamburg.

Schromm, Gerhard; Halder, Martin: „Gesichterkennung II – Eigenfaces“, Veröffentlichung, 09.01.2002.

schule.de: „Übungsaufgaben“, http://marvin.sn.schule.de/~matheabi/06/ma06la.html, Aufruf: 20.08.2014.

Thalheim, Lisa; Krissler, Jan; Ziegler, Peter-Michael: „Körperkontrolle - Biometrische Zugangssicherungen auf die Probe gestellt“ in: c't Magazin, November 2002.

The Imperva Application Defense Center (ADC): „Consumer Password Worst Practices“, White Paper, Imperva, 2014.

Trösch, Thomas: „Der Netzhaut-Scanner für unterwegs“ in: Handelsblatt Online, 14.05.2014.

u-tech-gmbh.de: „RFID – So funktioniert es“, http://www.u-tech-gmbh.de/das-system/allgemeine-funktionsweise/funktionsweise-rfid.html, Aufruf: 08.09.2014.

von Graevenitz, Gerik: „Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren“, LIT Verlag Münster, 2006.

Wächter, Carsten; Römer, Stefan: „Gesichts-Erkennung I“, Veröffentlichung, Universität Ulm, 2002.

Wohlfahrt, Eva: „Vor- und Nachteile der Iriserkennung“, http://www.arlbergnet.com/design/biometrics/iris/hp_iris01.htm, Aufruf: 04.10.2014.