HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Frau
Janka Patzschke

Systematische Übersichtsarbeit für zukünftige Forschungsgegenstände von forensischen Auswertungen digitaler Zutrittskontrollsysteme

Mittweida, November 2023

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Systematische Übersichtsarbeit für zukünftige Forschungsgegenstände von forensischen Auswertungen digitaler Zutrittskontrollsysteme

Autorin:
Janka Patzschke

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w2-B

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
M.Sc. Felix Fischer

Einreichung:
Mittweida, 15.11.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Systematic review for future research subjects of forensic analysis of digital access control systems

Author:
Janka Patzschke

Course of Study:
General and Digital Forensic Science

Seminar Group:
FO20w2-B

First Examiner:
Prof. Dr. rer. nat. Dirk Labudde

Second Examiner:
M.Sc. Felix Fischer

Submission:
Mittweida, 15.11.2023

Defense/Evaluation:
Mittweida, 2023

Bibliografische Beschreibung

Patzschke, Janka:
Systematische Übersichtsarbeit für zukünftige Forschungsgegenstände von forensischen Auswertungen digitaler Zutrittskontrollsysteme. – 2023. – 52 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023.

Referat

Das Ziel der vorliegenden Arbeit ist es eine Übersicht über aktuell relevante und am Markt vertretene Zutrittskontrollsysteme zu erstellen. Dazu wird zuerst die grundlegende Theorie hinter den einzelnen Zutrittskontrollsystemen vorgestellt. Im Anschluss werden die vorgestellten Zutrittskontrollsysteme durch selbst ausgewählte Kriterien nach Sicherheit und Komfort bewertet. Dabei stellte sich der Handvenenscan in dem Bereich Sicherheit durch das sehr niedrige Verlust-, Weitergabe- und Nachahmungsrisiko und im Bereich Komfort durch die kontaktlose Verwendung, dem geringen Aufwand, der niedrigen Schmutzempfindlichkeit und dem niedrigen Schmutzempfinden als hervorragend heraus. Anschließend wird ein Flussdiagramm als Entscheidungshilfe vorgestellt. Dieses hat den Zweck das geeignete Zutrittskontrollsystem für die private Nutzung oder der Nutzung im Unternehmen zu finden. Dabei werden aktuell auf dem Markt befindliche Produkte vorgestellt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Auto-ID ..... Automatische Identifikation und Datenerfassung

CCD ..... charge-coupled device (*dt. ladungsgekoppeltes Bauteil*)

EEPROM ..... Electrically Erasable Programmable Read-Only Memory (*dt. elektronisch löschbarer programmierbarer Nur-Lese-Speicher*)

FRAM ..... Ferroelectric Random Access Memory (*dt. Ferroelektrischer Direktzugriffsspeicher*)

HF ..... High-Frequency (*dt. Hochfrequenz*)

IEC ..... International Electrotechnical Commission (*dt. Internationale Elektrotechnische Kommission*)

ISO ..... International Organization for Standardization (*dt. Internationale Organisation für Normung*)

LF ..... Low-Frequency (*dt. Niedrigfrequenz*)

MIFARE ..... Mikron fare collection (*dt. Mikron Fahrgeld-System*)

MITM ..... Man-in-the-Middle

NFC ..... Near Field Communication (*dt. Nahfeldkommunikation*)

PIN ..... Persönliche Identifikationsnummer

RFID ..... Radio Frequency Identificaion (*dt. Funkerkennung*)

ROM ..... Read-Only Memory (*dt. Festwertspeicher*)

UHF ..... Ultra-High Frequency (*dt. Ultra-Hochfrequenz*)

1 Einleitung

Das Bedürfnis nach Sicherheit und Schutz ist sowohl für Privatpersonen als auch Unternehmen maßgebend bei der Entscheidung über eine Zutrittskontrolle [1, 2]. Heutzutage wird es immer wichtiger zusätzliche Maßnahmen zu ergreifen, um private oder geschäftliche Räume sowie das Eigentum zu schützen [1]. Wichtig ist dieser Schutz im Unternehmensumfeld für die Sicherung von vertraulichen Informationen sowie von wertvollen Geschäftseinrichtungen [2]. Im privaten Umfeld ist das persönliche Wohlbefinden wesentlich von einem gesicherten Zutritt anhängig [1].

Einen solchen Schutz lässt sich mithilfe der Zutrittskontrolle erreichen [3]. Dabei kann sichergestellt werden, dass nur befugte Personen physischen Zutritt zu einem schützenswerten Bereich haben [3]. Dieser schützenswerte Bereich kann im privatem Umfeld das Zuhause oder im Unternehmensumfeld Gebäude, Räume oder Freigelände sein [1, 3]. Die Zutrittskontrolle kann manuell durch Wachpersonal oder digital durch Maschinen erfolgen [3]. Die digitale Zutrittskontrolle erfolgt heutzutage immer häufiger mit Codekombinationen, Schlüsselkarten oder biometrischen Merkmalen [4]. Doch die Anfänge der Zutrittskontrolle waren viel einfacher. Die erste Form der Zutrittskontrolle wurde bei Ausgrabungen im alten Irak in den Ruinen der antiken assyrischen Stadt Ninive in Form eines hölzernen Stabes und eines Riegels gefunden [4]. Dieses antike sogenannte *ägyptische Schloss* datiert die erste Zutrittskontrolle auf vor circa 6.000 Jahre [4]. Im alten Rom wurden Holzschlösser abgeschafft und auf Metallschlösser umgestellt [4]. Circa 870 bis 900 vor Christus entstanden durch das Hinzufügen von Hindernissen, Schutzvorrischtungen und Vorsprüngen das erste *gesicherte Schloss* [4]. Das Prinzip, dass ein Schlüssel exakt auf diese Hindernisse und Vorsprünge angepasst war, ist heutzutage noch bekannt [4]. Im Laufe der Zeit änderte sich diese Technik nicht wesentlich, bis im Jahre 1778 das erste *Zylinderschloss* patentiert wurde [4]. Dieses fügte dem gekerbten Schlüssel noch einen doppeltwirkenden Hebelmechanismus hinzu [4]. Trotz dieser Sicherheitsmaßnahmen war das Schloss weiterhin für geübte Einbrecher überwindbar [4]. Das erste zuverlässige, aufbruchssichere Schloss wurde erst 1784 auf den Markt gebracht [4]. Die Schlossart, die heutzutage am häufigsten verwendet wird, entstand 1861 durch den amerikanischen Erfinder Linus Yale Jr. [4]. Die Geschichte der Zutrittskontrolle ist allerdings nicht abgeschlossen und befindet sich in einer ständigen Weiterentwicklung. Es werden immer sicherere und flexibelere Lösungen der Zutrittskontrolle zu Räumlichkeiten und schützenswerten Bereichen gesucht [5]. Der Zweck, Eigentum und Orte gesondert zu schützen, blieb jedoch der Gleiche [4].

Die Zutrittskontrolle beschäftigt sich bei der Erfüllung dieser Aufgabe mit einer entscheidenden Frage: „Wer ist wann und wo zutrittsberechtigt?“ [6]. Die Frage *Wer* definiert dabei den berechtigten Personenkreis oder die berechtigte Person, die Zutritt zu einem schützenswerten Bereich erhält [5]. Im Unternehmensumfeld können dies zum Beispiel Personal, Reinigungskräfte oder Besucher sein [5]. Privat könnten dies die Anwohner und Besucher sein. Für eine moderne Zutrittskontrolle ist es immer wichtiger, dass der Zutritt für einzelne Personen oder Personengruppen zeitlich flexible angepasst werden kann [5]. Durch das Einstellen von persönlichen Berechtigungen kann der Zutritt fein auf bestimmte Bereiche und bestimmte Zeiten angepasst werden [5]. Zusätzlich erhält man eine genaue Aufzeichnung

darüber, *wann* eine Person kommt und geht [7]. Die letzte grundsätzliche Frage ist das *Wo*. Durch die Zutrittskontrolle kann genau auf eine Person oder Personengruppe zugeschnitten werden, für welchen Bereich, Raum oder Abteilung der Zutritt genehmigt wird [5]. Somit kann einer Person der Zutritt zu einem Bereich erlaubt und zu einem anderen Bereich verboten werden [5]. Dies bietet eine hohe Flexibilität und Sicherheit für sensible Bereiche [5].

1.1 Motivation

Die Bedeutung einer zuverlässigen Zutrittskontrolle wird immer deutlicher. Der Schutz vor einem unbefugten Zutritt, dem Diebstahl von sensiblen Informationen oder Eigentum war schon lange ein Teil der Menschheitsgeschichte und wird auch weiterhin eine entscheidende Rolle einnehmen [1]. Aus diesem Grund soll diese Arbeit dazu dienen eine Übersicht für die auf dem Markt befindlichen Arten der digitale Zutrittskontrolle zu erstellen. Dabei soll eine Auseinandersetzung mit der Sicherheit und dem Komfort der einzelnen Methoden erfolgen.

1.2 Abgrenzung

In dem seit Mai 2018 bestehenden Paragraph § 64 des Bundesdatenschutzgesetz *Anforderungen an die Sicherheit der Datenverarbeitung* wird zwischen der Zugangskontrolle, der Verwehrung des unbefugten Zuganges zu Datenverarbeitungsanlagen und der Zugriffskontrolle, der Gewährleistung, dass zugangsberechtigte Personen ausschließlich auf die der Berechtigung umfassenden Daten Zugriff haben, unterschieden. Zuvor gab es zusätzlich eine Abgrenzung zwischen der Zutritts- und der Zugangskontrolle.

In der alten Fassung des Bundesdatenschutzgesetz vor Mai 2018 werden in Anlage zu § 9 Satz 1 die Zutrittskontrollen als Systeme definiert, deren Aufgabe es ist „Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren “[8]. Damit sind Zutrittskontrollsysteme dazu da, den physischen Zutritt zu einem Gebäude oder Areal, in dem sich Datenverarbeitungsanlagen befinden, für Unbefugte zu verhindern. Maßnahmen des Schutzes sind unter anderem Berechtigungsausweise oder Türkontroll- und Einlasssysteme [9]. Die Aufgaben von Zugangskontrollsysteme wurde hingegen definiert als „zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können“[8]. Durch geeignete Schutzmaßnahmen wird die Nutzung der Datenverarbeitungssysteme durch Unbefugte verhindert. Diese Schutzmaßnahmen sind zum Beispiel das Einrichten einer Kombination aus Nutzername und Passwort, das Prüfen von Netzwerkadressen oder die Installation von Virenscannern, Malwareschutz und Spamfilter [9]. Laut Anlage zu § 9 Satz 1 der alten Fassung, haben Zugriffskontrollsysteme die Aufgabe „zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“[8]. Das bedeutet, dass sichergestellt wird, dass Personen, die sowohl Zutritt, als auch Zugang zu den Datenverarbeitungssystemen haben, ausschließlich die Daten nutzen können, für die sie die erforderlichen Berechtigungen besitzen [9]. Methoden der Zugriffskontrolle sind unter

anderem die Einführung von Lese-, Schreib- und Ausführungsberechtigungen [9]. Eine Kombination aus Zutritts-, Zugangs- und Zugriffskontrollsystemen führt zu einem umfassenden Schutz der zu verarbeitenden Daten [9].

Für eine klare Abgrenzung des Zutritts *zu* und der Nutzung *von* Datenverarbeitungssystemen, werden in der folgenden Arbeit die Definitionen aus der alten Fassung des Bundesdatenschutzgesetzes nach Anlage zu § 9 Satz 1 verwendet. Im Verlauf der Arbeit wird nicht weiter auf Zugangs- oder Zugriffskontrollsysteme eingegangen.

Die Arbeit beschäftigt sich ausschließlich mit digitalen Zutrittskontrollsystemen. Manuelle Kontrollsysteme wie Wachpersonal oder mechanische Schließsysteme wie Schranken, Zäune oder Drehkreuze werden nicht betrachtet.

1.3 Zielstellung

Im Verlauf der Arbeit soll eine Übersicht der existierenden Zutrittskontrollsysteme für zukünftige forensische Forschung erarbeitet werden. Es gibt eine Vielzahl von unterschiedlichen Systemen und Produkten. Diese Übersicht soll nur einen groben Überblick über derzeit produzierte Zutrittskontrollsysteme und ein besseres Verständnis ihrer Funktionsweise geben. Gleichzeitig sollen die Zutrittskontrollsysteme in dieser Übersicht vorgestellt und nach ihrer Sicherheit und dem Anwendungskomfort gruppiert werden. Dabei erfolgt eine kritische Auseinandersetzung mit den Vor- und Nachteile im Bereich Sicherheit und Komfort. Dazu wird eine Bewertungsmatrix für die Sicherheit und den Komfort erstellt. Weiterhin soll ermittelt werden, ob es das beste Zutrittskontrollsystem gibt oder ob diese Bewertung von dem Verwendungszweck abhängig ist.

1.4 Aufbau dieser Arbeit

Die vorliegende Arbeit beginnt mit einem Kapitel *theoretischen Grundlagen*, die für das Verständnis der nachfolgenden Themengebiete essentiell sind. Dafür wird zu Beginn erklärt, was ein Auto-ID-System ist und welche in dieser Arbeit vorgestellt werden. Danach wird der Unterschied zwischen zugewiesenen und originären Merkmalen erläutert, die jeweiligen Auto-ID-Systeme entsprechend zugeordnet und die Theorie hinter jedem Auto-ID-System näher beschrieben. Diese Informationen haben für die weiteren Abschnitte der Arbeit eine große Relevanz.

Nachdem alle relevanten Grundlagen erläutert sind, werden die vorgestellten Auto-ID-Systeme auf Grundlage der vorangegangenen Theorie im Kapitel *Bewertung der Auto-ID-Systeme* nach Sicherheit und Komfort bewertet. Dabei wird die Sicherheit nach dem Verlust-, Weitergabe- und Nachahmungsrisiko sowie nach der Veränderbarkeit und möglichen Schutzmechanismen bewertet. Die Bewertung des Komforts erfolgt nach den Kriterien, ob ein Gegenstand zur Identitätskontrolle benötigt wird und wie hoch der Aufwand, die Schmutzempfindlichkeit und das subjektive Schmutzempfinden des Benutzers ist. Daraufhin erfolgt eine Auseinandersetzung mit den Ergebnissen anhand einer Sicherheits-Komfort-Matrix. Zum Abschluss des Themenkomplexes wird die Multi-Faktor-Authentifizierung vorgestellt.

Im anschließendem Kapitel *Marktübersicht* wird ein Flussdiagramm als Entscheidungshilfe bei der Suche nach einem geeigneten Auto-ID-System vorgestellt. Anhand dessen werden 20 Zutrittskontrollsysteme näher betrachtet.

Zum Abschluss werden im Kapitel *Fazit* alle Erkenntnisse zusammengefasst, Probleme der Arbeit erläutert sowie ein Ausblick zu weiteren Auto-ID-Systemen gegeben, die für zukünftige Forschung relevant sein könnte.

2 Theoretische Grundlagen

Im folgenden Abschnitt werden Grundlagen erläutert, die für das weitere Verständnis der Arbeit erforderlich sind. Dafür wird erklärt, was Auto-ID-Systeme sind und wie man sie gruppieren kann. Anschließend werden die ausgesuchten Systeme innerhalb ihrer Gruppeneinteilung betrachtet. Alle Ergebnisse werden in Tabelle A.1 zusammengefasst.

2.1 Automatische Identifikations- und Datenerfassungssysteme

Auto-ID-Systeme werden als Systeme zur automatischen Identifizierung und Datenerfassung, deren Zweck es ist, durch technologische Unterstützung Daten zu identifizieren, erheben, erfassen und übertragen, definiert [10]. Als elektronische Zutrittskontrollsysteme verwendet, verhindern sie den unbefugten Zutritt zu schützenswerten Anlagen. Um dies zuverlässig und sicher umsetzen zu können, muss nachgewiesen werden, dass eine Person, die einen Bereich betreten möchte, tatsächlich die Person ist die sie behauptet zu sein. Dafür können einer Person Merkmale zugewiesen werden oder ihre originären Merkmale verwendet werden [11].

Umsetzbar als elektronische Zutrittskontrollsysteme ist die Eingabe eines Persönliche Identifikationsnummer (PIN)/Passwortes, Magnetstreifenkarten, kontaktbehafteten Chipkarten, kontaktlosen Chipkarten mittels RFID oder Near Field Communication (*dt. Nahfeldkommunikation*) (NFC) sowie verschiedene Methoden der biometrischen Zutrittskontrolle [12]. In Abbildung 2.1 ist eine Übersicht einer Auswahl an Auto-ID-Systeme, die als Zutrittskontrollsysteme verwendet werden können, dargestellt. Ersichtlich in der Abbildung 2.1 wird die Gruppierung der Auto-ID-Systeme. Nach der Unterscheidung in originäre und zugewiesene Merkmale, können die originären Merkmale beziehungsweise die biometrischen Systeme in dynamische und statische Verfahren eingeteilt werden. Die zugewiesenen Merkmale unterscheiden sich in der Anwendungsform. Eine Gruppe kann nur kontaktbehaftet angewendet werden und die andere kann kontaktlos verwendet werden. In der folgenden Arbeit werden nur die Auto-ID-Systeme behandelt, die in den grau hinterlegten Feldern mit einer durchgezogenen Umrandung sind. Die Auto-ID-Systeme in den grau hinterlegten Feldern mit einer gestrichelten Umrandung werden nicht näher betrachtet und dienen nur einer größeren Übersicht.

2.2 Zugewiesene Merkmale

Als zugewiesene Merkmale zählen Gegenstände und Informationen, die eine Person als Identifikationsmedium gegenüber eines Zutrittskontrollsystemes wissen oder besitzen kann [11]. Dies können zugewiesene Benutzernamen und Passwörter, aber auch physische Gegenstände wie Identifikationskarten sein [11]. Die Anwendung der zugewiesenen Merkmale kann entweder durch direkten Kontakt mit einem Lesegerät oder kontaktlos erfolgen. Der Nachteil von zugewiesenen Merkmalen ist, dass es zum Verlust, der Weitergabe sowie der Nachahmung jener physischer Gegenstände oder dem Vergessen der zugewiesenen Merkmale kommen kann [11].

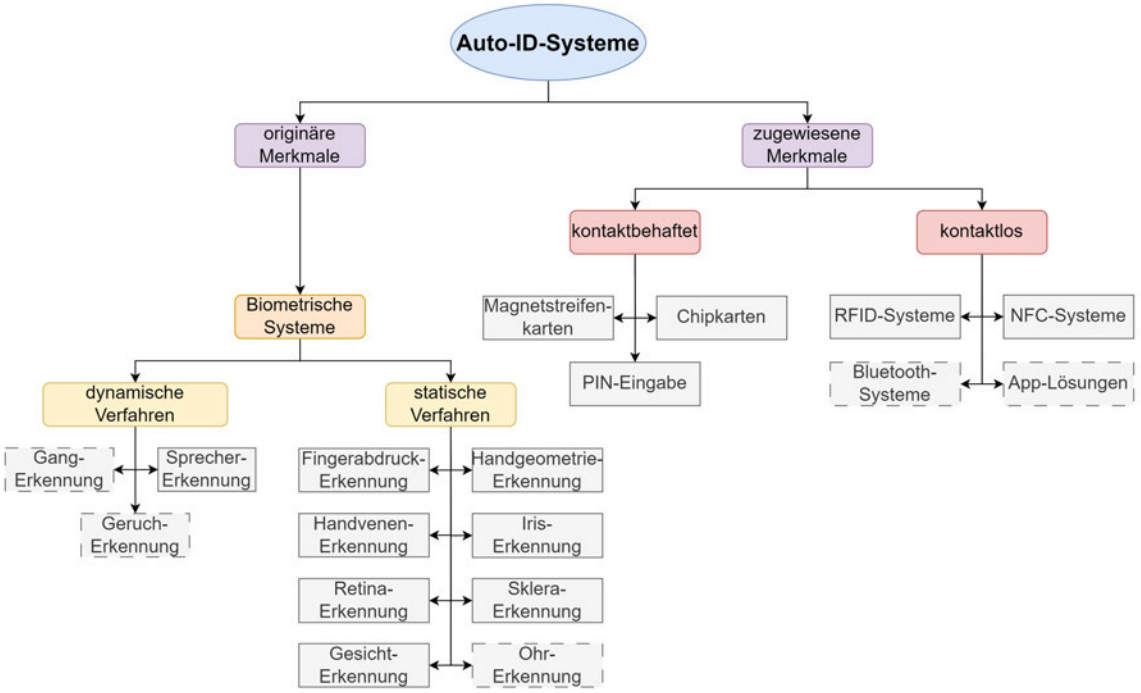

Abbildung 2.1: Übersicht der automatischen Identifikations- und Datenerfassungssysteme zur elektronischen Zutrittskontrolle, sowie Gruppierung und Vorstellung der in der Arbeit behandelten Systeme

2.2.1 Kontaktbehaftete Zutrittskontrolle

Bei der kontaktbehafteten Zutrittskontrolle wird das gewählte Identifikationsmedium im direkten Kontakt mit einem Terminal genutzt [12]. Darunter zählen die Eingabe einer PIN sowie das Durchziehen oder Anhalten einer Karte mit Magnetstreifen oder eines Chipmoduls [12]. Kontaktbehaftete Zugriffskontrollsysteme sind in der Anschaffung häufig kostengünstig [13, 14], jedoch gelten sie aufgrund ihrer Anfälligkeit für Fälschungen als unsicher [12].

2.2.1.1 PIN/Passwort

Die Zutrittskontrolle mit einer neben dem zu kontrollierenden Eingang angebrachten Tastatur ist eine einfache und kostengünstige Art der Identitätsüberprüfung [13]. Der einzugebende Code kann entweder auf eine Tür oder eine Person bezogen sein [13].

Bei türbezogenen Codes kennt eine Gruppe von Menschen die geheime Ziffernfolge für den Zutritt zu schützenswerten Gebieten [13]. Die Eingabe des Geheimcodes öffnet für alle Personen, die den Code kennen, diese Tür. Die eingegebenen Ziffern werden im System zusammengesetzt und auf Übereinstimmungen mit dem im System hinterlegten Zutrittscodes geprüft [13]. Bei der ein- oder mehrmaligen falschen Eingabe des Geheimcodes kann die Tastatur gesperrt und ein Alarm ausgelöst werden [13]. Nachteile an türbezogenen Codes ist der leichtfertige Umgang einer großen Gruppe zutrittsberechtigter Personen mit Geheimhaltung des Passwortes gegenüber unbefugten Personen sowie die fehlende Möglichkeit der Identifizierung einzelner Personen, die zu einer bestimmten Zeit Zutritt hatten [13].

Die persönliche Identifizierung einzelner Personen ist durch die PIN möglich. Bei personenbezogenen PIN-Codes erhält jede befugte Person ihren eigenen geheimen Code zum Zutritt in schützenswerte Gebiete [13]. Die Tastatur kann sowohl erkennen, ob der eingegebene Code im System gespeichert und zutrittsberechtigt ist, aber auch zu wem diese PIN gehört [13]. Bei Verwendung wird sowohl die Person, als auch die Begehungszeit gespeichert [13]. Da die PIN personenbezogen ist, kann bei unbefugter Verwendung durch eine andere Person davon ausgegangen werden, dass die berechtigte Person leichtfertig mit der Geheimhaltung umgegangen ist [13]. Jedoch ist die persönliche Hürde der unbefugten Weitergabe aufgrund der guten Rückverfolgungsmöglichkeit geringer als bei türbezogenen Codes, die schon einer großen Gruppe bekannt sind [13].

2.2.1.2 Magnetstreifenkarten

Die Nutzung von Magnetstreifenkarten ist vor allem in der Gebäudekontrolle bei Parkhäusern und Hotels verbreitet [15] und bietet eine weitere kostengünstige Möglichkeit der Zutrittskontrolle [14]. Dabei werden auf einem Magnetstreifen Informationen elektromagnetisch gespeichert [16]. Das Auslesen der Daten erfolgt mit einem Durchzugsleser [15]. Das Magnetband, das bis zu 1024 Bit Daten speichern kann, besteht dabei aus drei Spuren, bei dem zwei Spuren für den Lesevorgang spezifiziert sind und die dritte Spur zum Lesen und Schreiben von Daten genutzt werden kann [15]. Die Daten auf dem Magnetband lassen sich einfach überschreiben [14]. Nachteilig ist, dass es durch andere magnetische Felder zu einer Entmagnetisierung und somit zu einem Löschen oder Beschädigen der gespeicherten Daten kommen kann [16]. Zusätzlich können die Daten auch beliebig kopiert, gelesen und leicht verändert oder gelöscht werden [17]

2.2.1.3 Kontaktbehaftete Chipkarten

Kontaktbehaftete Chipkarten sind genormte Kunststoffkarten, in denen ein Mikrochip, der eine Datenübertragung durch direkten Kontakt zwischen Leser und Karte ermöglicht [18], eingebaut ist [19]. Dabei sind die Abmessungen und physikalischen Eigenschaften der Karte durch die International Organization for Standardization (*dt. Internationale Organisation für Normung*) (ISO) und International Electrotechnical Commission (*dt. Internationale Elektrotechnische Kommission*) (IEC) nach dem Standard ISO/IEC 7810 sowie die Maße, Position und physikalischen Eigenschaften des Mikrochips nach dem Standard ISO/IEC 7816-2 genormt [19]. Die genormte Dicke von 0,76 Millimetern bietet abzüglich der Kunststoffhülle wenig Platz für das Chipmodul [19], wodurch es schlecht vor Abnutzung, Verschmutzung und Korrosion geschützt ist [18].

Chipkarten können in Speicherkarten und Prozessorkarten unterscheiden werden (siehe Abbildung 2.2) [19]. Der Speicher von Speicherkarten kann nur gelesen und beschrieben werden [15]. Speicherkarten können dabei ohne oder mit Sicherheitslogik ausgestattet sein. Speicherkarten mit Sicherheitslogik haben einen gesicherten Speicherzugriff, wodurch Funktionen wie das Lesen oder Schreiben auf dem Speicher durch bestimmte Schutzmechanismen nur durch Eingabe der PIN ermöglicht wird [19]. Damit können die sich darauf befindlichen Daten nur vom Eigentümer verwendet werden [18]. Typisch für Karten ohne Sicherheitslogik sind Karten mit Electrically Erasable Programmable Read-Only Memory (*dt. elektronisch*

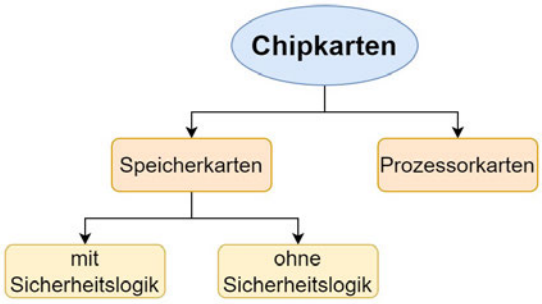

Abbildung 2.2: Übersicht der Chipkarten-Typen mit Unterteilung in Speicher- und Prozessorkarten

löschbarer programmierbarer Nur-Lese-Speicher) (EEPROM) [19]. Bei EEPROM-Speicherkarten kann somit frei auch den Speicher zugegriffen und uneingeschränkt beschrieben, gelesen und gelöscht werden [19]. Im Unterschied zu Speicherkarten ist bei Prozessorkarten für die Verschlüsselung noch zwischen Speicher und Ausgabe ein Prozessor geschaltet [18]. Dieser Mikroprozessor ermöglicht eine Rechnerstruktur mit Betriebssystem, Arbeitsspeicher und Rechenwerk [15]. Im Speicher ist ein Read-Only Memory (*dt. Festwertspeicher*) (ROM) sowie ein EEPROM enthalten [18]. Der Zugriff auf das EEPROM ist nur über das Betriebssystem möglich [18].

2.2.2 Kontaktlose Zutrittskontrolle

Im Gegensatz zu kontaktbehafteten Zutrittskontrollsystemen, erfordern kontaktlose Zutrittskontrollsysteme keinen direkten Kontakt mit einem Lesegerät [19]. Dabei reicht der Empfang zwischen Transponder und Lesegerät von wenigen Zentimetern bis hin zu mehreren Metern [19]. Aufgrund des fehlenden direkten Kontakts und somit geringere Abnutzung und Verschmutzung ist die Wartung der kontaktlosen Lesegeräte niedriger [18]. RFID- und NFC-Transponder-Chips dienen der kontaktlosen Datenübertragung und werden in verschiedenen Medien verbaut, wodurch sie nach vorheriger Registrierung im System die Identifikation einer Person ermöglichen [12].

2.2.2.1 Radio Frequency Identificaion

Ein RFID-Zutrittskontrollsystem basiert auf der Funkerkennung mittels Radiowellen, die zwischen Transponder und Lesegerät kommunizieren [20]. Dies findet kontaktlos und nur auf Abruf statt [20]. Die Lesegeräte der meisten modernen RFID-Systeme sind in der Lage mehrere Transponder auseinanderzuhalten und mit ihnen einzeln zu kommunizieren [21]. Dieser Vorgang wird als Antikollision bezeichnet [21]. Auch ein Mehrfachzugriff bei dem mehrere Transponder gleichzeitig auf dasselbe Lesegerät zugreifen, kann möglich sein [21]. Das Lesegerät ist häufig stationär, an eine Stromversorgung angeschlossen und meist durch einen Computer mit einem Netzwerk verbunden [20]. Die Stromversorgung des Transponders hingegen kann aktiv durch eine Batterie übernommen werden oder passiv durch die Stromversorgung mittels Induktion, indem sie dem magnetischen oder elektromagnetischen Feld Energie entzieht [21]. Sowohl der Transponder als auch das Lesegerät besitzen eine Antenne, die Senden und Empfangen kann, als auch einen Chip zum Verarbeiten der kodierten Radiosignale, die bei passiven Systemen zur Stromversorgung dienen können [20, 21]. Abhängig von

der gewünschten Reichweite sind die Antennen auf den Low-Frequency (*dt. Niedrigfrequenz*) (LF), High-Frequency (*dt. Hochfrequenz*) (HF) oder Ultra-High Frequency (*dt. Ultra-Hochfrequenz*) (UHF)-Bereich ausgelegt [21]. Die Antennen der drei Frequenzbereiche basieren auf unterschiedlichen Funktionsweisen [21]. Der LF-Bereich basiert auf dem Nahfeld, der HF-Bereich auf magnetischer Kopplung und der UHF-Bereich auf Fernfeld [21]. Dabei sind für RFID-Systeme die Frequenzen 120-135 kHz, 13,56 MHz sowie 868 MHz, 915 MHz, 2,45 GHz und 5,5 GHz relevant [20]. Die am häufigsten verwendete Frequenz für RFID-Systeme ist 13,56 MHz [22]. Standardisiert ist die Verwendung mittels ISO 18000, mit den Untergruppen ISO 18000-2 für LF, ISO 18000-3 für HF und ISO 18000-6 für UHF [22]. Damit die verwendeten Frequenzen der RFID-Systeme nicht mit Radiosendern oder anderen Funkanlagen interferieren, müssen sie nicht nur ihren technischen Erfordernissen entsprechen, sondern auch den staatlichen Regelungen der Frequenzbereiche und Sendeleistungen [21].

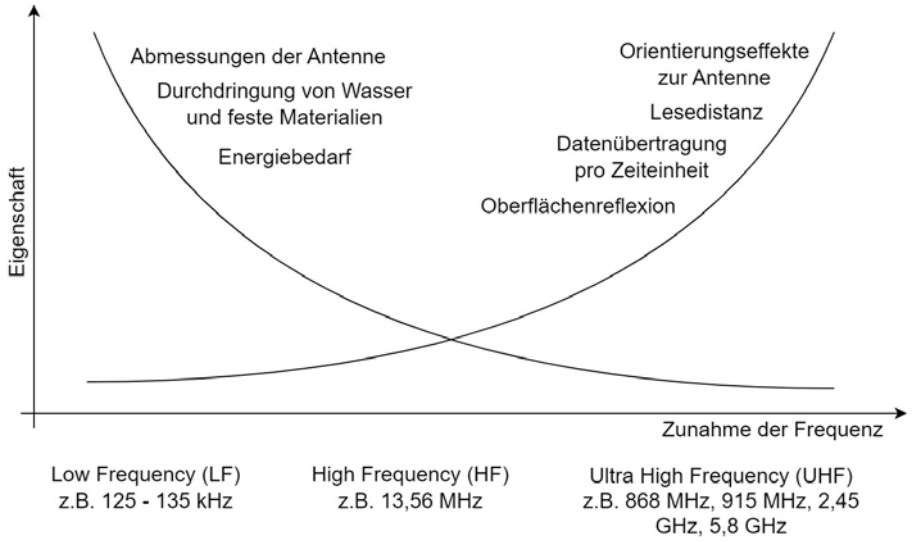

Abbildung 2.3: Frequenzbereiche und relevante Eigenschaften für RFID nach C. Kern [21]

Allerdings eignet sich nicht jede Frequenz für die Verwendung als RFID-Zutrittskontrollsystem [21]. Abbildung 2.3 zeigt wichtige Eigenschaften die abhängig von den verschiedenen Frequenzen sind [21]. Darunter zählen Eigenschaften wie die Durchdringung von Wasser und festen Materialien, der Energiebedarf, die Oberflächenreflexion, die Datenübertragung pro Zeiteinheit, die Lesedistanz und die Orientierungseffekte zur Antenne. Die Durchdringung von Wasser und festen Materialien nimmt mit zunehmender Frequenz ab, da Dämpfungseffekte auftreten [21]. Diese treten in leichter Form im LF-Bereich, aber in stärkerer Form in im UHF-Bereich auf [21]. Da der Mensch zum Großteil aus Wasser besteht, ist der UHF-Bereich für die Zutrittskontrolle nicht geeignet [21]. Im HF-Bereich sind erst eindeutige Signaldämpfungen festzustellen, wenn der Transponder zwischen die Handflächen gelegt wird [21]. Weiterhin sinkt der Energiebedarf bei den höheren Frequenzen [21]. Für die Zutrittskontrolle ebenfalls wichtig ist, dass je nach verwendeten Material im UHF-Bereich ein großer Energieverlust auftritt, sodass keine sichere Lesung garantiert werden kann [21]. Für eine höhere Frequenz spricht jedoch, dass die Datenübertragungsrate steigt, da mehr Schwingungen pro Zeiteinheit als bei tiefen Frequenzen erfolgen [21]. Höhere Frequenzen können auch eine höhere Lesedistanz erreichen [21]. LF und HF reichen im Vergleich zu UHF nur circa 50 Zen-

timeter, UHF hingegen bis zu zwei Meter weit [21]. Die Lesedistanz ist aber auch zusätzlich abhängig von der Ausrichtung zur Leseantenne [21]. Dieser Effekt fällt bei tiefen Frequenzen weniger stark aus [21].

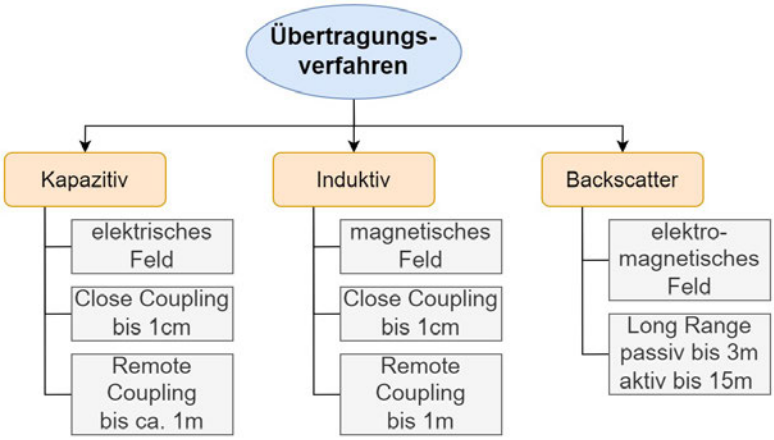

Abbildung 2.4: Übertragungsverfahren der Stromversorgung nach C. Kern [21]

Die Übertragung von Daten zwischen dem Transponder und dem Lesegerät kann kapazitiv, induktiv oder mit dem Backscatter-Verfahren erfolgen [21]. Abbildung 2.4 stellt die drei Übertragungsverfahren dar, zeigt auf welcher Basis sie funktionieren und wie weit ihre Reichweite ist. Die kapazitive Übertragung nutzt das elektrische Feld, welches zwischen zwei parallel angeordneten Platten eines Plattenkondensators entsteht [21]. Die Dekodierung des Transpondersignals findet anhand des sich ändernden elektrischen Feldes statt [21]. Die kapazitive Übertragung arbeitet sowohl mittels Kurzkopplung als auch Fernkopplung [21]. Dabei reicht die Kurzkopplung bis zu einem Zentimeter und findet häufig Anwendung in Hochsicherheitsbereichen [23]. Bei der Fernkopplung kann eine Reichweite von bis zu einem Meter erreicht werden [23]. RFID-Systeme, die auf Induktion basieren, ermöglichen mit der aufgenommenen Energie sowohl den Betrieb ihres Chips, als auch das abzugebende Signal [21]. Die Energie wird aus dem magnetischen Feld gezogen [21]. Auch die induktive Übertragung funktioniert mittels Kurz- als auch Fernkopplung [21]. Das Backscatter-Verfahren wird von RFID-Systemen genutzt, die mehr als ein Meter reichen müssen [21]. Bei diesen Langstreckenkopplungssystemen wird in Europa im Bereich von 868 MHz gearbeitet [21]. Dabei werden vom Lesegerät elektromagnetische Wellen ausgesendet und am Lesegerät nicht zurückgesendet, sondern reflektiert [21]. Bei passiver Energieversorgung des Transponders können bis zu drei Meter erreicht werden, bei aktiver Energieversorgung bis zu 15 Meter [21].

Der enthaltene Speicher im RFID-System dient dazu Daten zu übermitteln und abzuspeichern [21]. Der Speicher kann entweder bereits vom Hersteller programmiert werden oder vom Nutzer [21]. Wobei er einmal oder mehrfach programmiert werden kann [21]. Ähnlich wie bei Speicherkarten, kann die Speicherung mit EEPROM oder auch mit EEPROM (Ferroelectric Random Access Memory (*dt. Ferroelektrischer Direktzugriffsspeicher*) (FRAM)) erfolgen [21]. EEPROM (FRAM) hat eine geringere Leistungsaufnahme sowie eine höhere Schreibgeschwindigkeit [21].

Nachteilig ist, dass RFID-Systeme einige Schwachpunkte haben. Die Daten können ausgelesen, manipuliert oder gelöscht werden [24]. Die Manipulation kann durch Spoofing und Replay-Attacken, Man-in-the-Middle (MITM)-Attacken oder durch das Einschleusen von Malware erfolgen [24]. Später wird die ausgelesene Kommunikation genutzt, um dem Lesegerät eine autorisierte Kommunikation vorzutäuschen [24]. Eine weitere Art des Angriffs sind MITM-Attacken, bei denen sich ein Angreifer unbemerkt zwischen die offizielle Kommunikation des Chips und des Lesegeräts schaltet, gesendete Daten abfängt, manipuliert und weiterschickt [24]. Durch das Einschleusen von Malware besteht die Möglichkeit beliebige Programmcodes auszuführen oder Datenbankeinträge zu manipulieren [24].

2.2.2.2 Near Field Communication

Die Technologie hinter NFC basiert auf der Weiterentwicklung der RFID- und der Chipkarten-Standards [17]. NFC gilt bei Distanzen bis zehn Zentimetern als Übertragungsstandard [19]. Basierend auf der Norm ISO/IEC 14443, wird der Nachrichtenaustausch zwischen Transponder und Lesegrät definiert [17]. Der Nachrichtenaustausch zwischen zwei NFC-Geräten basiert auf dem neuentwickelten Protokoll, welches in ISO/IEC 18092 beziehungsweise in ECMA-340 definiert ist [17]. Anders als bei RFID-Systemen, trennt NFC nicht zwischen Lesegerät und Transponder [17]. NFC integriert sowohl ein aktives Lesegerät als auch einen passiven Transponder [17].

Die Energie- und Datenübertragung basiert ebenfalls auf der RFID-Technologie [25]. NFC-Systeme nutzen dabei ausschließlich die bei RFID-Systemen am weitesten verbreitete Frequenz von 13,56 MHz und sind induktiv gekoppelt [25]. NFC kann Übertragungsgeschwindigkeiten bis zu 424 kbit/s erreichen [19]. Mit der durch Induktion aus dem magnetischen Feld gezogenen Energie, muss sowohl der Betrieb des Chips gewährleistet werden, als auch die Erzeugung eines ausreichend starken abzugebenden Signals [21]. Die Energieversorgung kann aktiv, passiv oder semi-passiv stattfinden [25]. Als aktiv gilt ein Transponder, wenn er eine eigene Stromversorgung besitzt und ein eigenes Hochfrequenzsignal erzeugt [25]. Passiv ist ein Transponder, wenn er seine gesamte Stromversorgung aus dem Energiefeld des Lesegeräts bezieht [25]. Ein semi-passiver Transponder wird üblicherweise durch Batterien versorgt und nutzt das Hochfrequenzfeld des Lesegeräts, da er kein eigenes Feld erzeugen kann [25]. Die Funktionsweise der Datenübertragung ist abhängig von der Energieversorgung [25]. Passive und semi-passive Systeme haben eine feste Rollenverteilung zwischen Lesegerät und Transponder [25]. Dabei wird die Übertragung über zwei Kanäle geleitet, vom Lesegerät zum Transponder, dem sogenannten Uplink, und vom Transponder zum Lesegerät, dem sogenannten Downlink [25]. Aktive Systeme hingegen haben keine feste Einteilung der Rollen. [25]. Das in dem Augenblick sendende Gerät übernimmt die Aufgabe der aktiven Lese- und Schreibeinheit [25]. Hierbei wird der Kanal für die Datenübertragung abwechselnd nur in Richtung von Lesegerät zum Transponder genutzt [25].

Nachteilig bei der kontaktlosen Datenübertragung ist, dass die Kommunikation einfach und auch aus größerer Entfernung abgehört werden kann [19]. Auch kann ein Angreifer die Datenübertragung mit einem Störsender blockieren oder anstelle des eigentlichen Kommunikationspartners auf Befehle antworten [19]. Ebenfalls sind NFC-Systeme anfällig für MITM-Attacken. Hierbei schaltet sich ein Angreifer zwischen die beiden kommunizierenden NFC-

Geräte und lässt alle Kommunikation über sich laufen und dient als Vermittler [19]. Doch diese Attacken lassen sich nur umsetzen, wenn beide NFC-Geräte komplett vom HF-Feld abgeschirmt sind [19].

Anwendung finden NFC-Systeme unter anderem bei der Zutrittskontrolle zu Gebäuden, Privat- oder Geschäftsräumen, aber auch Garagen und Hotels [26]. Als Schlüssel können hier kontaktlose Chipkarten mit NFC oder auch NFC-Mobiltelefone verwendet werden [26]. Der Vorteil eines NFC-Mobiltelefons liegt darin, dass mehrere Schlüssel integriert werden können [26]. Standardmäßig basieren viele NFC-Mobiltelefone auf Mikron fare collection (*dt. Mikron Fahrgeld-System*) (MIFARE) [26], einem System, welches ursprünglich als elektronisches Bezahlsystem des Personennahverkehrs entwickelt wurde [27]. Es ist kompatibel zum Standard ISO/IEC 14443 Typ A und ist das weltweit häufigste kontaktlose Chipkartensystem [27].

2.3 Originäre Merkmale

Originäre Merkmale sind im Gegensatz zu den zugewiesenen Merkmalen untrennbar mit einer bestimmten Person verbunden [28], da sie auf physischen Merkmalen der Person beruhen [29]. Der Vorteil der originären Merkmale liegt darin, dass es zu keiner Weitergabe oder dem Vergessen kommen kann [11]. Grundsätzlich besteht die Verwendung eines biometrischen Verfahrens aus zwei Schritten: dem Enrollment und dem Matching [30]. Das Enrollment ist das Anlegen eines Referenzmusters durch die erstmalige Registrierung der originären Merkmale [30]. Beim Matching wird das gespeicherte Referenzmuster abgerufen und mit der Person verglichen, die Zutritt erbittet [30]. Biometrische Verfahren identifizieren oder verifizieren eine Person auf Basis dieser individuellen, personenbezogenen und -gebundenen Merkmale [30, 31]. Bei der Identifikation werden die originären Daten mehrerer Personen in einem beliebig großen Referenzdatensatz gespeichert und abgerufen wenn der Vergleich mit einer zu identifizierenden Person erforderlich ist [31, 32]. Der 1:n-Vergleich der originären Daten mit dem Datensatz erfordert einen hohen zeitlichen und rechnerischen Aufwand [31, 32]. Bei der Verifikation hingegen wird in einem 1:1-Vergleich überprüft, ob die, für eine gewisse Person, gespeicherten Daten mit der im Moment zu verifizierenden Person übereinstimmen [31, 32]. Die Verifikation bietet somit eine hörere Sicherheit und einen geringeren zeitlichen Aufwand als die Identifikation [32]. Die originären Merkmale müssen die folgenden vier Eigenschaften erfüllen, um zur Zutrittskontrolle verwenden werden zu können:

- „Universalität (bei jedem Menschen vorhanden),
- Einzigartigkeit (bei jedem Menschen verschieden),
- Beständigkeit (ohne Veränderung über die Zeit),
- Erfassbarkeit (durch ein technisches System quantitativ messbar)“[32].

Die Verwendung originärer Merkmale bietet eine hohe Sicherheit, erfordert aber auch bei der Überprüfung einen höheren Zeitaufwand [11].

2.3.1 Statische Verfahren

Statische Verfahren bauen auf physiologischen Merkmalen einer Person auf, die sich nur über lange Zeiträume hinweg ändern können [29]. Zur Überprüfung des Zutritts können statische Verfahren wie die Fingerabdruck-, Handgeometrie-, Venenmuster-, Gesichts- und Iriserkennung verwendet werden [29]. Ein weiteres statisches Verfahren wäre die Verwendung des Ohres als Zutrittskontrollsystem. Das Ohr erfüllt die Anforderungen der Universalität, variiert jedoch im Bezug auf die Einzigartigkeit und Beständigkeit und wird somit nicht näher betrachtet [31].

2.3.1.1 Fingerabdruckerkennung

Bei der Fingerabdruckerkennung werden die individuellen Erhöhungen, die sogenannten Papillarlinien, mittels Sensoren erfasst [28, 31]. Aufgrund der individuellen Muster, wie Bögen, Schleifen oder Wirbel und weiteren Besonderheiten [31], gleicht kein Fingerabdruck einem anderen [29]. Fingerabdrücke besitzen eine Einzigartigkeit von 1:1.000.000 [30]. Die Fingerabdrücke eines Menschen bilden sich bereits vollständig im vierten Embryonalmonat aus und bleiben das ganze Leben gleich [31].

Das Abtasten des Fingers zum Anlegen des Referenzmusters erfolgt dreidimensional mit Weiß- oder Farblicht [29]. Durch die Verwendung von Farblicht können nicht nur Betrugsversuche mittels Fotografien erkannt werden, sondern es erfolgt auch im Gegensatz zur Verwendung von Weißlicht eine Überprüfung, ob die Person lebt [29]. Diese Lebendfingerspektronomie basiert auf der Auswertung eines Spektrogramms des roten Blutfarbstoff [29]. Die von den Sensoren erfassten Erhebungen der Haut werden zur Digitalisierung in elektrische Signale umgewandelt [28]. Damit werden auch Datenschutzprobleme umgangen, die bei der Abspeicherung des aufgenommenen Fingerabdrucks entstehen [29]. Für die Erstellung eines zum Vergleichen geeignetem Basisrasters des Fingerabdrucks wird das aufgezeichnete dreidimensionale Bild der charakteristischen Linien und Vertiefungen nach dem Digitalisieren reduziert [29]. Das anschließende Matching des erfassten Fingerabdrucks erfolgt durch einen Abgleich mit den zuvor abgespeicherten Informationen [28].

Trotz der Beständigkeit des Fingerabdrucks eines Menschen bis zum Tod [19], kann der Scan des Fingerabdrucks nicht für jede Person als zuverlässiges Zutrittskontrollsystem genutzt werden [32]. Durch die zu feinen Strukturen der Finger von Kindern oder älteren Personen kann keine einwandfreie Erkennung durch den Scanner garantiert werden [32]. Ebenso wird das Ergebnis eines Scans durch Hautverletzungen und -verschmutzungen beeinträchtigt [32], vor allem wenn der Scan und Abgleich nur mittels weniger Finger erfolgt [33]. Neben der Schmutzempfindlichkeit des Verfahrens ist bei der Wahl des Zutrittskontrollsystems auch die subjektive Wahrnehmung des Schmutzempfindes relevant [33]. So haben kontaktbasierte Fingerabdruckscanner deutliche Akzeptanzprobleme [33]. Einige Scanner arbeiten mittels einer Führungsschiene an einer Lösung dieses Problems, indem der Finger den eigentlichen Scanner nicht mehr berühren muss, sondern sich in einem bestimmten Abstand zur Kamera befindet [30]. Fingerabdruckscanner bieten so auch den Vorteil, dass die Einnahme dieser Position des Fingers zur Kamera deutlich weniger Aufwand ist, als bei anderen biometrischen Verfahren, bei denen der gesamte Körper aufwendig positioniert werden muss [33].

2.3.1.2 Handgeometrieerkennung

Die Handgeometrieerkennung als Zutrittskontrollsystem basiert auf dem Fakt, dass keine Hand einer Anderen gleicht [29]. Die Einzigartigkeit der Handgeometrie liegt bei 1:1.000 [30]. Sie unterscheiden sich durch ihre Proportionen, Maße und Winkel der Finger [29]. Die verwendeten charakteristischen Handproportionen sind in Abbildung 2.5 dargestellt [29].

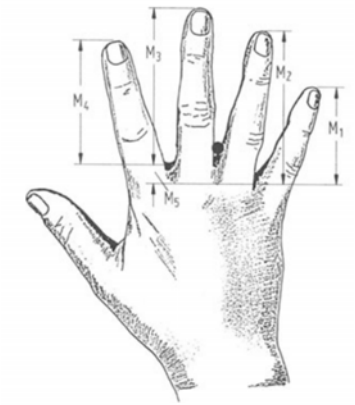

Abbildung 2.5: Charakteristische Merkmale der Handproportionen [29]

Optische Verfahren werden zur Vermessung der ausschlaggebenden geometrischen Merkmale genutzt [30]. Die Vermessung der Handgeometrie findet dreidimensional statt [29]. Im Vergleich zu einer zweidimensionalen wird bei einer dreidimensionalen Vermessung auch die Fingerstärke berücksichtigt, wodurch die Überlistung mittels Fotografien verhindert wird [29]. Nach der Vermessung und Ersterfassung der Handgeometrie werden die Daten digitalisiert und im System abgespeichert [29]. Bei einer erneuten Erfassung der Hand wird für das Matching auf die gespeicherten Daten zurückgegriffen und ein Vergleich der relevanten geometrischen Merkmale und Längen durchgeführt [29]. Der Vorteil der Handgeometrieerkennung liegt darin, dass Details der Handoberfläche, wie zum Beispiel Fingerabdrücke oder -nägel aber auch Linien, Narben und Schmutz den Scan nicht beeinflussen [30]. Ein weiterer Vorteil ist, dass das Verfahren keine aufwendige Einnahme einer Ganzkörper-Position erfordert [33]. Abbildung 2.6 zeigt die Position, die die Hand zur Vermessung einnehmen muss.

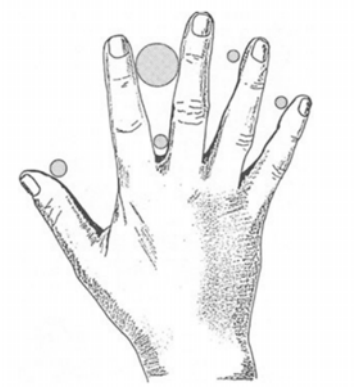

Abbildung 2.6: Anlagepunkte einer dreidimensionalen Handdatenidentifizierung zur Vermessung der Fingerlängen, Fingerstärken und Fingergeometrie [29]

2.3.1.3 Handvenenerkennung

Ein Handvenen-Scanner arbeitet basierend auf der Absorptionseigenschaft von Hämoglobin, dem roten Blutfarbstoff [30]. Die angewendete Technologie verwendet Nahinfrarotlicht [32]. Das Infrarotlicht wird vom Hämoglobin des „zum Herzen[s] zurückfließende[n], sauerstoffreduzierte[n] Blut[es]“ [32] absorbiert und stark vom restlichen Gewebe reflektiert [30]. Durch die Verwendung von Nahinfrarotlicht wird anhand der Messung von Blutfluss und Puls überprüft, dass die zu überprüfende Person lebt [34]. Das unterschiedlich absorbierte oder reflektierte Licht wird vom Scanner aufgenommen, wodurch sich die Handvenen als dunkle Muster abbilden [30]. Die Handvenen-Muster sind ein Leben lang unveränderlich und von Person zu Person unterschiedlich [32]. Abbildung 2.7 verdeutlicht diesen Ablauf der Handvenenerkennung. Das daraus entstehende Handvenen-Muster wird als Referenz für den späteren Vergleich zum Zweck der Zutrittskontrolle in einer Datenbank hinterlegt [35].

Abbildung 2.7: Ablauf eines Handvenen-Scans mit originalem Bild der Hand (Links), dem Scan durch Nahinfrarotlicht mit dunklen Mustern des Handvenen-Netzes (Mitte) und dem daraus berechneten Handvenen-Musters (Rechts) [35]

Bei der Handvenenerkennung wird in handelsüblichen Modellen die reflektierte Bildgebung verwendet [34]. Dabei befinden sich die Lichtquelle sowie der Sensor auf der gleichen Seite [34], wodurch eine kontaktlose Datenaufnahme der Hand möglich ist [32, 34]. Die kontaktlose Aufnahme bedarf keiner aufwendigen Einnahme einer Position [33]. Dadurch, dass bei der Handvenenerkennung kein sichtbares Licht verwendet wird, muss keine Rücksicht auf die Sonneneinstrahlung genommen werden [33]. Ausnahmen dabei bilden extreme Lichtverhältnisse sowie Temperatureinflüsse [32]. Es wird davon ausgegangen, dass die Handvenenerkennung gegenüber Eigenschaften der Haut und Hautschäden unempfindlich ist, da tiefer gelegene Strukturen betrachtet werden [34]. Empirisch gibt es dafür aber keine Belege [34].

2.3.1.4 Fingervenenerkennung

Die Fingervenenerkennung arbeitet genau wie die Handvenenerkennung basierend auf der Absorption von Nahinfrarotlicht durch den roten Blutfarbstoff Hämoglobin [34]. Die Funktionsweise, der Ablauf und einige Besonderheiten und Vorteile entsprechen den Beschreibungen der Handvenenerkennung aus Kapitel 2.3.1.3. Doch anders als bei der Handvenenerkennung findet die Fingervenenerkennung aufgrund der in marktüblichen Systemen verwendeten transilluminierenden Bildgebung kontaktbehaftet statt [34]. Bei der transilluminierenden Bildgebung befindet sich der Finger zwischen dem Sensor und der Lichtquelle [34]. Das von

der Lichtquelle ausgestrahlte Nahinfrarotlicht muss das menschliche Gewebe des Fingers durchdringen, bevor es im Sensor aufzeichnet werden kann [34]. Die benötigten Systeme sind aufgrund des beschriebenen Aufbaus größer und benötigen auch mehr Energie [34]. Ein Beispiel eines aufgezeichnete Bild der dunkel abgebildeten Fingervenen ist in Abbildung 2.8 zu sehen.

Abbildung 2.8: Fingervenen als dunkles Muster nach Scan durch Nahinfrarotlicht [36]

Der Fingervenen-Scan benötigt eine genauere Positionierung des Fingers, um die wenigen im Finger vorhandenen Bezugspunkte der Venen zu erkennen [36]. Dadurch ist die Fingervenenerkennung weniger sicher und benutzerunfreundlicher als die Handvenenerkennung [36].

2.3.1.5 Gesichtserkennung

Bei der Gesichtserkennung wird das Gesicht einer Person von charge-coupled device (*dt. ladungsgekoppeltes Bauteil*) (CCD)-Kameras, Digitalkameras oder Webcams gescannt und anhand mathematischer Verfahren in Vektoren transformiert [37]. Die Berechnung der Merkmalsvektoren kann mit verschiedenen Methoden erfolgen, beispielsweise durch die Erstellung eines sogenannten Graphen [37]. Dafür wird ein elastisches Gitternetz erstellt, welches über das Gesicht gelegt wird [37]. Dabei werden ausgehend von den spezifischen lokalen Informationen des Knotenpunktes innerhalb des Graphen jeweils ein Vektor berechnet [37]. Zusammengenommen bilden diese berechneten Vektoren den Merkmalsvektor eines Gesichts [37]. Die Gesichtsähnlichkeit zweier Gesichter wird nicht anhand der aufgenommenen Bilder bestimmt, sondern durch den Vergleich ihres Ähnlichkeitsmaßes [37]. So müssen die Merkmalsvektoren alle relevanten Informationen über ein Gesicht enthalten [37]. Die signifikante Reduktion der Gesichtsdaten auf einen Merkmalsvektor ermöglicht zwar die biometrische Gesichtserkennung, birgt aber durch die Reduktion der Eindeutigkeit auch Risiken, wie den daraus resultierenden möglichen Informationsverlust [37]. Die Herausforderung der Gesichtserkennung besteht darin, „die Merkmale genügend zu komprimieren, um Robustheit gegenüber Veränderungen des Merkmals zu erreichen und zugleich die Kompression so niedrig zu halten, dass das Merkmal beziehungsweise dessen Vektor immer noch eindeutig ist“ [37]. Es muss also ein Mittelweg zwischen Kompression und Datenreduktion gefunden werden [37].

Die Gesichtserkennung kann mittels zwei- oder dreidimensionaler Verfahren erfolgen [28]. Bei der zweidimensionalen Methode wird das Bild eines Gesichts in rechteckige Segmente unterteilt [28]. Die anschließende Analyse der Unterschiede zwischen zwei Gesichtern erfolgt von einem Segment zum anderen und benötigt für eine aussagekräftige Zuverlässigkeit nur etwa zehn Prozent der Segmente [28]. Bei der Methode mit einem dreidimensionalen Verfahren wird zusätzlich noch die räumliche Komponente betrachtet [28]. Für das Anlegen einer

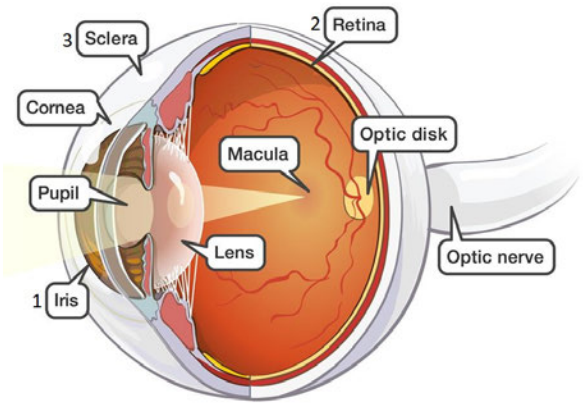

Abbildung 2.9: Äußere und Innere Ansicht des Auges mit 1-Iris, 2-Retina und 3-Sklera [39]

Referenz im Enrollment-Schritt erfolgt die Aufnahme einer zutrittsberechtigten Person durch nur wenige exemplarische Frontalaufnahmen [37]. Diese dürfen nicht unscharf, über- oder unterbelichtet sein [28]. Außerdem wird eine vollständige Abbildung des Gesichts benötigt [28]. Variationen im Gesichts können mit einem größeren Spektrum an Bildern abgedeckt werden [37]. Nach dem Enrollment wird der Merkmalsvektor wie beschrieben berechnet und gespeichert [37]. Das Erfassen des Gesichts ist sowohl stark vom richtigen Abstand der Kamera als auch von den Lichtverhältnissen der Umgebung abhängig [32]. Nachteilig ist, dass der richtige Abstand zur Kamera sowohl beim Enrollment als auch bei der späteren Zutrittskontrolle eine Einnahme einer aufwendigen Ganzkörperposition bedarf [33]. Ebenso kann der Vergleich durch getragene Schminke [32], Brillen [38], Bärte [38] oder auch Krankheiten erschwert oder gar verhindert werden [32].

2.3.1.6 Iriserkennung

Die Iris, auch Regenbogenhaut genannt, ist die kreisrunde pigmentierte Schicht des Auges, in deren Mitte sich die Pupille befindet (siehe Abbildung 2.9) [31]. Mit über 200 Einzelmerkmalen [31] bilden diese sehr feinen Unterschiede der Iris [28] ein einzigartiges Muster [31] und gehören dadurch zu den sichersten und zuverlässigsten biometrischen Zutrittskontrollsystemen [28]. Die Einzigartigkeit der Iris liegt bei 1:6.000.000 [30]. Die Aufnahme und Abtastung der Struktur erfolgt im Infrarotbereich [30, 31]. Das aufgenommene Muster der signifikantesten Punkte wird anschließend zum späteren Vergleich in einen zweidimensionalen Barcode umgewandelt [28]. Ohne die Veränderung durch Krankheiten oder andere invasive Eingriffe bleibt die Iris ein Leben lang gleich [28, 31]. Problematisch ist aber, dass statistisch etwa 2 von 100.000 Menschen mit Aniridie geboren werden, also keine Iris besitzen [32]. Auch bei blinden Personen lässt sich die Iriserkennung nicht einwandfrei anwenden [32]

2.3.1.7 Retinaerkennung

Die Retina, die Netzhaut des Auges, ist die innerste, lichtempfindliche Schicht (siehe Abbildung 2.9) [34]. Das Aderngeflecht, welches die Netzhaut durchzieht ist bei jedem Menschen individuell [34]. Die Einzigartigkeit liegt bei 1:1.000.000 [30]. Die Aufnahme erfolgt durch die

Beleuchtung des Augenhintergrundes [34]. Ein Verfahren, welches bisher nur im Hochsicherheitsbereich Anwendung findet und sehr hohe Kosten ausweist [34]. Eine praktische und kommerzielle Anwendung gibt es bisher nicht [34].

2.3.1.8 Skleraerkennung

Die Sklera ist der weiße Teil des Auges, welches mit feingliedrigen, detaillierten Adern durchzogen ist (siehe Abbildung 2.9) [34]. Für eine Aufnahme werden hochauflösende Bilddaten benötigt [34]. Die beiden Augenecken sollten dabei „durch zwei nicht-frontale Augenbilder abgebildet werden, in denen die Blickrichtung unterschiedlich ist“ [34]. Da die Extraktion der Adermuster sehr herausfordernd ist, gibt es bislang wenige Spezialisten, die diese feingliedrige Beschaffenheit mit einer akzeptablen Erkennungsgenauigkeit extrahieren können [34]. Deshalb gibt es gegenwärtig keine praktische Anwendung in kommerziellen Systemen [34]. Das Start-Up *EyeVerify* nahm es sich zum Ziel die Skleraerkennung in mobilen Online-Banking-Systemen verwenden zu können, verschwand aber nach dem Aufkauf durch die Alibaba-Group vom Markt [34].

2.3.2 Dynamische Verfahren

Dynamische Verfahren charakterisiert, dass die Zutrittskontrolle auf Messungen einer bestimmten Handlung basieren. Diese Handlung kann sich über einen längeren Zeitraum aber auch aufgrund von psychischen und physischen Schwankungen kurzfristig ändern [29]. Zur Überprüfung des Zutritts können auf verhaltenstypische Merkmale beruhende, dynamische Verfahren wie die Sprechererkennung verwendet werden [29]. Weitere verhaltensbezogene Merkmale sind der Geruch und der Gang eines Menschen. Auch sie erfüllen das Kriterium der Universalität, variieren aber in der Einzigartigkeit und der Konstanz [31], wodurch sie nicht näher betrachtet werden.

2.3.2.1 Sprechererkennung

Die Sprechererkennung beruht auf dem einzigartigen und persönlichen Sprachbild [29]. Es setzt sich bei jeder Person aus einer Mischung von anatomischen Merkmalen [29], soziokulturelle Einflüssen, Aussprachgewohnheiten und der dialektalen Färbung [37] aber auch aus bevorzugt verwendeten Redewendungen sowie sprechertypischen Wörtern und Satzstellungen [29] zusammen. Unterschieden wird beim Sprechen in die dynamischen und statischen Eigenschaften [37]. Die statischen Eigenschaften werden durch die anatomischen Merkmale einer Person bestimmt, aus denen sich wiederum eine Grundfrequenz des Sprachsignal bildet [29]. Dieses ist abhängig von der Abmessung und Spannung der Stimmbänder sowie dem subglottalen Luftdruck [29]. Der subglottale Luftdruck ensteht durch die Atemluft und bildet sich unter den Stimmlippen [40]. Erst wenn dieser groß genug ist, lassen sich die Stimmlippen auseinander drücken, die Stimmlippen schwingen und bilden Töne [40]. Anhand einer Kontrolle des beim Sprechen entstehenden Schalldrucks, kann eine Überlistung mittels Tonaufnahme ausgeschlossen werden [29]. Die dynamischen Eigenschaften werden vollständig durch das charakteristische Sprachverhalten einer Person bestimmt [29]. Darunter fallen

die Sprachmelodie, die Lautübergänge sowie die Sprechgeschwindigkeit [29]. Diese dynamischen Eigenschaften sind nur teilweise veränderbar [29]. Speziell Dialektmerkmale, die im Kindesalter erlernt wurden, können sich im Erwachsenenalter nicht vollständig unterdrücken lassen [29].

Die Art und der Umfang der Aufzeichnung eines Referenzmusters im Enrollment ist abhängig von dem geplanten Konzept der Sprechererkennung [37]. Unterschieden wird in die textabhängige, die vokabularabhängige, die ziffernbasierte und die textunanhängige Sprechererkennung [37]. Bei der textabhängigen Sprechererkennung wird der exakt gleiche Text sowohl zum Enrollment als auch zur Erkennung verwendet und damit nur die Aussprache dieses Textes aufgezeichnet [37]. Die vokabelabhängigen Sprechererkennung benötigt das Anlegen eines großen Vokabulars, damit aus mehreren Wörtern des Vokabulars verschiedene oder möglicherweise auch zufällige Testsätze gebildet werden können [37]. Die ziffernbasierte Sprechererkennung ist eine deutlich zeitsparendere Art der vokabelabhängigen Sprechererkennung, bei der das Vokabular ausschließlich aus den Zahlen zwischen Null und Neun besteht [37]. Die Länge der daraus zufällig gebildeten Ziffernkette kann beliebig bestimmt werden [37]. Die textunanhängige Sprechererkennung basiert weder auf einem vordefinierten Text oder dem Anlegen eines Vokabulars, sondern auf der Erstellung eines vollständigen Stimmprofils [37]. Das Enrollment müsste das gesamte Lautinventar einer Sprache vollständig abdecken, wodurch der Zeitaufwand für die meisten Anwendungen untragbar wäre [37]. Wichtig beim Enrollment ist auch, dass die Tonaufnahme in denselben akustischen Umgebungsbedingungen wie der Vergleich stattfindet [29] und auch Einflüsse durch Charakteristika des verwendeten Mikrofones berücksichtigt werden [37].

Eine Herausforderung der Analyse des charakteristischen Sprachbildes ist, dass Sprache nicht reproduzierbar ist [29]. Es sei nicht möglich dasselbe Wort exakt gleich auszusprechen [29]. Dadurch muss zum Vergleich ein mittlerer Merkmalsvektor aus mehrfach aufgenommenen Sprachproben erstellt werden [29]. Der dazu entwickelte Algorithmus „bestehen im wesentlichen aus einer Markov-Kette mit zustandsabhängigen Linearkombinationen von Gaußschen Verteilungsdichten“ [37]. Das bedeutet, dass das System auf einer sogenannten Markov-Kette basiert, die den zukünftigen Zustand nur anhand des aktuellen Zustand vorhersagt [41]. Diese Zustandsübergänge basieren auf gegebenen Wahrscheinlichkeiten [41]. In diesem Fall arbeitet das Modell mit der Gaußschen beziehungsweise Normalverteilung. Das Ziel ist es, in diesem Fall die Wahrscheinlichkeit zu bestimmen, dass von einer gewissen Person ein übereinstimmendes Sprachsignal erzeugt wurde [37]. Für einen funktionierenden Abgleich müssen Toleranzen zum Referenzmuster festgelegt werden [30].

Der Abgleich der Sprechererkennung bietet eine hohe Flexibilität aus der ein hoher Bedienkomfort und ein hohes Sicherheitsniveau entsteht [37]. Auch die durch Stimmungsschwankungen veränderte Sprechgeschwindigkeit und Grundfrequenz kann verhältnismäßig gut kontrolliert werden [29]. Problematisch hingegen können Veränderungen der statischen, anatomischen Eigenschaften aufgrund von Krankheiten wie zum Beispiel einer Erkältung werden [29]. Diese Veränderungen können am ehesten von Systemen, die auf dynamischen Eigenschaften basieren, bewältigt werden [29]. Gänzlich versagen alle Systeme, wenn die zu überprüfende Person stottert [29].

3 Bewertung der Auto-ID-Systeme

Im Folgenden werden die in Kapitel 2 vorgestellten Auto-ID-Systeme tabellarisch strukturiert und anhand von selbst gewählten Kriterien nach ihrer Sicherheit und dem Anwendungskomfort eingestuft. Die daraus resultierenden Ranglisten wurde genutzt, um das Verhältnis zwischen Sicherheit und Komfort graphisch darzustellen. Die Sklera- und Retina-Erkennung wird im Folgenden nicht näher betrachtet, da es aktuell keine praktischen und kommerziellen Systeme gibt [34].

3.1 Vergleich der Sicherheit

Tabelle 3.1 soll dafür dienen die Sicherheit der Auto-ID-Systeme nach den Kriterien Risiko des Verlustes, Risiko der Weitergabe, Risiko der Nachahmung und Wahrscheinlichkeit einer Veränderung des benutzten Auto-ID-Systems zu bewerten [11, 31]. Die Auto-ID-Systeme sind dafür in auf Wissen, Besitz oder Inhärenz basierend unterteilt.

Die benutzen Kriterien dienen dazu Auto-ID-Systeme miteinander zu vergleichen, unabhängig. ob sie auf Wissen, Besitz oder Inhärenz basieren. In der Bewertung vorteilhaft für ein Auto-ID-System ist es, wenn bekannte Schwachstellen durch Schutzmechanismen ausgebessert werden. Als Grundlage der Einschätzung dienen die zusammengetragenen Eigenschaften der Auto-ID-Systeme sowie die erwähnten Vor- und Nachteile aus Kapitel 2 und in Tabelle A.1. Die Bewertung erfolgt durch die Einschätzung, ob die Wahrscheinlichkeit des Eintretens eines Sicherheitsrisiko sehr niedrig, niedrig, mittel, hoch oder sehr hoch ist. Zur Erstellung der Rangfolge wird die Einschätzung in einen Zahlenwert übersetzt und für jedes Auto-ID-System zusammengerechnet. Eine sehr niedrige Wahrscheinlichkeit gibt einen Punkt, eine niedrige Wahrscheinlichkeit zwei Punkte, eine mittlere Wahrscheinlichkeit drei Punkte, eine hohe Wahrscheinlichkeit vier Punkte und eine sehr hohe Wahrscheinlichkeit fünf Punkte. Zusätzlich gibt es noch einen Punkt, wenn kein Schutzmechanismus vorhanden ist, der das Auto-ID-System vor einem Sicherheitsrisiko schützt. Das bestmögliche Ergebnis kann demzufolge entstehen, wenn alle Wahrscheinlichkeiten der Sicherheitsrisiken sehr niedrig sind und zusätzlich Schutzmechanismen vorliegen. Das schlechtestmögliche Ergebnis entsteht, wenn alle Wahrscheinlichkeiten der Sicherheitsrisiken sehr hoch sind und keine Schutzmechanismen vorliegen.

PIN/Passwort Die Eingabe eines Codes über eine Tastatur benötigt ausschließlich das Wissen des richtigen Passwortes. Das Verlustrisiko ist daher nur im Sinne des Vergessens des Passwortes möglich [11]. Dies stellt ein mittleres Risiko da. Das Weitergaberisiko des geheimen Passwortes ist hoch, besonders dann, wenn eine große Gruppe an Personen das selbe Passwort verwenden [13]. Sehr hoch ist das Risiko, dass das Passwort ausgespäht und nachgeahmt werden kann [13]. Die Tastaturfelder sind gegebenenfalls einsehbar, sodass das Passwort leicht in Erfahrung zu bringen ist, indem der das Passwort eingebenden Person unauffällig über die Schultern geschaut wird [13]. Ein neues Passwort einzustellen ist leicht, sodass das Risiko, dass sich das gewählt Passwort ändert, hoch ist. Obwohl es einige

Tabelle 3.1: Sicherheitsvergleich der Auto-ID-Systeme; Legende: Sehr Niedrig = 1, Niedrig = 2, Mittel = 3, Hoch = 4, Sehr Hoch = 5

Auto-ID-Systeme	Verlust	Weitergabe	Nachahmung	Veränderbarkeit	Schutzmechanismen	Platzierung
PIN / Passwort	Mittel	Hoch	Sehr Hoch	Hoch	Sichtschutz, Ziffernverwürfelung [13]	7. Platz
Magnetstreifenkarten	Hoch	Hoch	Hoch	Sehr Hoch		8. Platz
kontaktbehaftete Chipkarte	Hoch	Hoch	Mittel	Hoch	Sicherheitslogik	6. Platz
RFID-Chips	Hoch	Hoch	Hoch	Hoch	Verschlüsselung der Daten	7. Platz
NFC-Chips	Hoch	Hoch	Hoch	Mittel		7. Platz
Fingerabdruck	Niedrig	Mittel	Niedrig	Niedrig	Prüfung auf Puls	3. Platz
Handgeometrie	Sehr Niedrig	Mittel	Niedrig	Sehr Niedrig	Dreidimensionale Aufnahmen	2. Platz
Handvene	Sehr Niedrig	Sehr Niedrig	Sehr Niedrig	Sehr Niedrig	Prüfung auf Puls	1. Platz
Fingervene	Sehr Niedrig	Sehr Niedrig	Sehr Niedrig	Sehr Niedrig	Prüfung auf Puls	1. Platz
Gesicht	Sehr Niedrig	Mittel	Mittel	Mittel	Lebenderkennung	4. Platz
Iris	Niedrig	Sehr Niedrig	Sehr Niedrig	Niedrig		2. Platz
Sprecher	Niedrig	Mittel	Mittel	Mittel	Schalldruckmessung	5. Platz

Schutzmechanismen wie die Verwendung von einem Sichtschutz oder einem Tastenfeld mit Ziffernverwürfelung gibt [13], erreicht die Passworteingabe über ein Tastenfeld im Vergleich der ausgewählten Auto-ID-Systeme den siebten Platz.

Magnetstreifenkarten Für auf Besitz basierende Auto-ID-Systeme ist das Verlustrisiko deutlich höher als bei auf Wissen oder Inhärenz basierende Auto-ID-Systeme [11]. So ist das Verlustrisiko einer Magnetstreifenkarte, die als Ausweis täglich mit sich geführt werden muss, hoch [11]. Auch das Risiko der Weitergabe dieser Magnetstreifenkarte ist hoch, da keine Überprüfung stattfindet, wer die Karte verwendet, sondern nur auf wen sie zugelassen ist [11]. Ebenfalls ist das Nachahmungsrisiko bei Magnetstreifenkarten hoch [11], da sie keine Schutzmechanismen gegen unbefugtes Kopieren besitzen [17]. Dieser fehlende Schutzmechanismus führt auch dazu, dass Magnetstreifenkarten leicht verändert oder überschrieben werden können [14, 17]. Zusätzlich sind sie nicht gegen äußere Einflüsse geschützt [16] Somit

ist die Veränderungswahrscheinlichkeit der Magnetstreifenkarte sehr hoch. Die Magnetstreifenkarten erreichen in diesem Vergleich den letzten Platz und sind anhand der betrachteten Kriterien das unsicherste Auto-ID-System.

kontaktbehaftete Chipkarten Da kontaktbehaftete Chipkarten auch auf dem Besitz eines Identifikationsmedium basieren, ist auch hier das Verlustrisiko sowie das Risiko der Weitergabe hoch [11]. Wie hoch das Nachahmungsrisiko ist, hängt davon ab, ob es sich um eine Prozessorkarte oder eine Speicherkarte mit oder ohne Sicherheitslogik handelt. Auf den Speicher von Speicherkarten ohne Sicherheitslogik kann uneingeschränkt zugegriffen werden [19], wodurch das Nachahmungsrisiko hoch ist. Speicherkarten mit Sicherheitslogik sowie Prozessorkarten haben einen gesicherten Zugriff [18, 19], wodurch das Nachahmungsrisiko niedrig ist. Somit kann für kontaktbehaftete Chipkarten im Allgemeinen ein mittleres Nachahmungsrisiko angenommen werden. Eine ähnliche Einordnung kann man für die Veränderungswahrscheinlichkeit einer kontaktbehafteten Chipkarte vornehmen. Speicherkarten ohne Sicherheitslogik können uneingeschrängt beschrieben oder gelöscht werden [19]. Die Wahrscheinlichkeit, dass sich das Identifikationsmedium ändert, ist somit hoch. Speicherkarten mit Sicherheitslogik und Prozessorkarten hingegen sind gesondert gesichert und können nur aufwendig verändert werden [18, 19]. Die Veränderungswahrscheinlichkeit ist somit niedrig. Hinzu kommt jedoch, dass Chipkarten schlecht gegen Abnutzung durch den direkten Kontakt oder Korrosion des Chip geschützt sind [18]. Zusammen betrachtet, ist die Wahrscheinlichkeit, dass sich kontaktbehaftete Chipkarten im Laufe der Zeit ändern, hoch. Kontaktbehaftete Chipkarten können in dem Vergleich der ausgewählten Auto-ID-Systeme auf den sechsten Platz eingeordnet werden.

Radio Frequency Identification RFID-Chips können in verschiedenen Objekten eingebaut werden. Die Identifikation beruht auf dem Besitz des gewählten Objektes. Wie bei anderen auf Besitz basierenden Auto-ID-Systemen, ist das Verlust- und Weitergaberisiko des Identifikationsmediums hoch [11]. RFID-Chips verwenden ein simples Schaltungssystem, bei dem die Informationen übertragen werden, wenn ein Lesegerät diese abruft [42]. Durch die ungeprüfte Abfrage kann anhand der übermittelten Informationen eine Karte nachgeahmt werden [42]. Das Nachahmungsrisiko ist somit hoch. Die Veränderung der Daten des RFID-Systems ist durch verschiedenste Angriffsarten möglich [24]. Sie können manipuliert oder gelöscht werden [24]. Somit ist das Veränderungsrisiko hoch. Die Daten können durch eine einfache Verschlüsselung geschützt werden [24]. RFID-Systeme erreichen in dem Vergleich der ausgewählten Auto-ID-Systeme den siebten Platz.

Near Field Communication Systeme, die auf NFC basieren, benötigen ebenfalls ein physische Identifikationsmedium. Ihnen liegt der Besitz dieses Mediums zugrunde. Somit ist das Verlust- und Weitergaberisiko hoch [11]. Die Daten der NFC-Systeme können durch die kontaktlose Übertragung leicht ausgelesen werden [19]. Das Risiko, dass die ausgelesenen Daten zur Nachahmung von NFC-Systemen genutzt werden, ist hoch. Die mittels MITM-Angriffe ausgelesenen Daten können auch manipuliert werden. Jedoch unterliegt die Erfolgsrate eines solchen Angriffs einigen Bedingungen [19]. Dass sich das Identifikationsmedium verändert, birgt ein mittleres Risiko. NFC-Systeme erreichen somit ebenfalls den siebter Platz.

Das Risiko ein Auto-ID-System zu verlieren oder weiterzugeben, welches auf der Inhärenz eines Identifikationsmedium basiert, ist allgemein gering [11]. Die originären Merkmale werden so ausgewählt, dass sie auch über eine sehr lange Zeit beständig bleiben [32]. Ein originäres Merkmal kann sich jedoch aufgrund von Krankheiten oder Verletzungen ändern [32].

Fingerabdrücke Die physische Verfassung des Fingerabdrucks ist für einen Scan von großer Bedeutung [43]. Erkrankungen oder Verletzungen können die Unversehrtheit des Fingerabdrucks dauerhaft beschädigen [43]. Die Außenschicht der Haut ist die Epidermis und die darunter befindliche Schicht die Dermis [43]. Während Verletzungen der obersten Epidermisschicht den Fingerabdruck nicht verändern, wird die Struktur des Fingerabdrucks durch eine Verletzung der Dermis und dem Entstehen einer Narbe dauerhaft verändert [32, 43]. Aufgrund dessen bietet das Aufnehmen sämtlicher Fingerabdrücke im Enrollment klare Vorteile gegenüber dem Aufnehmen von nur ein bis zwei [33]. Das Risiko alle Fingerabdrücke als originäres Merkmal vollständig zu verlieren, ist aufgrund der hohen Anzahl alternativer Finger niedrig [44]. Das Weitergaberisiko von Fingerabdrücken ist moderat. Durch die Kooperation einer Person lassen sich höherwertige Fälschungen anfertigen [45]. Kooperativen Fälschungen, „bei denen der zu fälschend[e] Finger während der Fälschungserstellung verfügbar ist“ [45], bieten mehr Informationen und sind deutlich schwerer zu erkennen [45]. Ein Negativ des Fingerabdrucks kann durch das Hineindrücken des Fingers in eine weiche Masse angefertigt werden [45]. Anschließend kann die Erstellung eines Positiv mittels beliebigen Materials erfolgen, welches in das Negativ gegeben wird und dort aushärtet [45]. Da Fingerabdrücke an der Oberfläche liegende originäre Merkmale sind [11], werden sie bei jeder Berührung von Objekten zudem unfreiwillig zurück gelassen [45]. Aus diesen hinterlassenen Fingerabdrücke kann mit geringen Kosten eine Fälschung angefertigt werden [45]. Der Chaos Computer Club veröffentlichte 2006 eine einfache Anleitung zur Anfertigung einer Attrappe [45]. Dafür musste der Fingerabdruck zuerst sichtbar gemacht, digitalisiert und nachbearbeitet werden [45]. Anschließend wird er auf eine Folie gedruckt, um die Fingerstruktur nachzubilden [45]. Zuletzt muss eine Holzleim-Glycerin-Mischung aufgetragen und die gehärtete Attrappe in Fingergröße zugeschnitten werden [45]. Der Erfolg dieser Fälschungen ist jedoch stark abhängig von der Qualität der hinterlassenen Fingerabdrücke [45], weshalb das Nachahmungsrisiko niedrig ist. Die Veränderungswahrscheinlichkeit von Fingerabdrücken ist niedrig. Beeinflusst werden können sie nur durch Verletzungen [32]. Auch wenn sie das Merkmal an sich nicht ändert, kann es dazu kommen, dass die Fingerabdrücke von sehr jungen oder sehr alten Menschen nicht einwandfrei für einen Scan verwendet werden können [32]. Durch die Verwendung von Farblicht kann eine Überprüfung auf Puls stattfinden und somit garantiert werden, dass es sich bei dem zu überprüfenden Finger um den einer lebenden Person handelt [29]. Fingerabdrücke können als ein sicheres Identifikationsmedium verwendet werden und erreichen in diesem Vergleich den dritten Platz.

Handgeometrie Bei der Verwendung der Handgeometrie als Identifikationsmedium ist das Verlustrisiko sehr niedrig, da die Handgeometrie nicht durch Narben oder kleinere Verletzungen beeinflusst wird [11, 30]. Es ist denkbar, dass von der Handgeometrie ebenfalls, wie bei den Fingerabdrücken beschrieben, kooperative Fälschungen angefertigt werden können. Allerdings benötigt die biometrische Verwendung der Handgeometrie eine präzise Fingerpositionierung mittels der in Abbildung 2.6 abgebildeten Distanzpflöcke [46]. Deshalb ist das Weitergaberisiko der Handgeometriedaten moderat einzuschätzen. Niedrig ist hingegen das Nachahmungsrisiko. Obwohl die Handgeometrie ein oberflächliches originäres Merkmal ist,

ist die Anfertigung einer Fälschung ohne Kooperation der betroffenen Person aufgrund der benötigten präzisen Positionierung sehr schwer [29, 46]. Sehr gering ist die Wahrscheinlichkeit, dass sich die Handgeometrie verändert, da sie sich aus anatomischen Eigenschaften [11] wie den Proportionen, den Maßen und Fingerwinkeln zusammensetzt [29]. Sicherer wird die Verwendung der Handgeometrie, wenn nicht nur eine zweidimensionale sondern eine dreidimensionale Überprüfung stattfindet [29]. So kann eine Überlistung mit Fotokopien verhindert werden [29]. Handgeometrie als Auto-ID-System kann auf den zweiten Platz eingeordnet werden.

Hand- und Fingervenen Hand- und Fingervenen sind die einzigen originären Merkmale der ausgewählten Auto-ID-Systeme, die sich unter der Haut befindet und somit nicht frei zugänglich sind [32, 47]. Venenmuster sind aufgrund dieser Verborgenheit externen Einflüssen gegenüber unempfindlich und bilden somit ein unveränderliches originäres Merkmal [47]. Dem Sicherheitsforscher und Hacker Jan Krissler alias Starbug gelang es jedoch unter Laborbedingungen das Handvenenmuster mittels einer modifizierten Spiegelreflexkamera aus der Ferne zu fotografieren, mit dem extrahierten Handvenenmusters eine Wachsattrappe anzufertigen und den Handvenenscanner des Herstellers Fujitsu und den Fingervenenscanner des Herstellers Hitachi zu überwinden [48]. Nichts desto trotz ist es unter realen Bedingungen [48] „fast unmöglich Adernstrukturen ohne Benutzerzustimmung oder aus der Distanz aufzunehmen, und andererseits [ist es] sehr schwierig, Artefakte herzustellen die für Angriffe verwendet werden können“ [34]. Die aufgenommenen Bilder des Venenmusters weisen allgemein eine geringe Qualität auf [34]. Aus diesen Gründen ist das Weitergabe- und Nachahmungsrisiko der Hand- und Fingervenenmuster sehr niedrig. Zudem wird angenommen, dass die abgebildeten Venenmuster unempfindlich gegenüber oberflächlichen Verletzungen sind [34, 38], da tiefer gelegene Strukturen betrachtet werden [34]. Eine Veränderung der Venenmuster in der Hand oder im Finger ist somit sehr unwahrscheinlich. Die zum Scannen verwendete Nahinfrarotstrahlung dient auch der Feststellung auf Lebendigkeit [34]. Sowohl die Handvenen-, als auch die Fingervenen-Erkennung schneidet in diesem Vergleich in allen Kategorien am besten am und bilden somit gemeinsam den ersten Platz.

Gesicht Ein aussagekräftiger Vergleich zweier Gesichter benötigt nur etwa zehn Prozent der zuvor im Gesicht eingeteilten Segmente [28]. Krankheiten beeinträchtigen den Vergleich möglicherweise [32], führen allerdings nicht zu einem kompletten Verlust des Identifikationsmedium. Das Risiko ist dementsprechend sehr niedrig. Das Gesicht ist ein sehr öffentlich zugängliches Körperteil [32, 45]. Video- oder Bildaufnahmen der biometrischen Daten lassen sich sowohl bewusst als auch unbewusst anfertigen [45]. Die aus diesen Aufnahmen gewonnenen Daten lassen sich zur Anfertigung einer Gesichtsmaske nutzen [32, 45]. Das Weitergabe- und Nachahmungsrisiko ist somit als moderat einzuschätzen. Ebenfalls moderat ist die Veränderungswahrscheinlichkeit. Nicht nur schwere Krankheiten können das Gesicht beeinflussen und zu Beeinträchtigungen des Scans führen [32]. Es ist auch möglich, dass die Funktionsweise durch das Verwenden von Schminke, das Tragen einer Brille oder eines Bartes eingeschränkt wird [32, 38]. Sicherer wird die Gesichtserkennung durch die Lebenderkennung [45]. Anhand mehrerer hintereinander aufgenommener Bilder können menschliche Verhaltensweisen wie Kopfbewegungen oder Zwinkern analysiert und somit eine Attrappe enttarnt werden [45]. Die Erkennung durch den Gesichtsvergleich erreicht den vierten Platz.

Iris Die Iris kann ebenfalls als Auto-ID-System verwendet werden. Als auf Inhärenz basierendes Auto-ID-System ist das Verlustrisiko niedrig [11]. Jedoch kann die Funktionsfähigkeit des Scans durch Krankheiten beeinträchtigt werden [32]. Da auch die Iris öffentlich zugängliche biometrische Daten beinhaltet, können diese sowohl bewusst, aber auch unbewusst ohne Kenntnis der betroffenen Person erfasst werden [45]. Aus den aufgenommenen Bildern oder Videos lassen sich theoretisch Attrappen wie ausgedruckte Bilder, Glasaugen oder Kontaktlinsen herstellen [45]. Jedoch gilt die Anfertigung einer Iris-Attrappe aufgrund der hohen Anzahl an Einzelmerkmalen als sehr schwierig [28, 31]. Eine erfolgreiche Weitergabe und Nachahmung der Iris ist deshalb eine sehr große Herausforderung [45] und stellt ein sehr niedriges Risiko da. Die Wahrscheinlichkeit, dass die Iris sich im Laufe des Lebens ändert, ist niedrig. Beeinflusst werden kann die Iris jedoch durch invasive Eingriffe [31] oder verschiedene Krankheiten wie eine Irisverfärbung oder Blindheit [32]. Die Iriserkennung gilt als eines der sichersten Auto-ID-Systeme [28] und erreicht in diesem Vergleich den zweiten Platz.

Sprecher Die Sprechererkennung ist ein dynamisches Verfahren [29]. Anders als bei den zuvor erwähnten, auf Inhärenz basierenden Auto-ID-Systemen, können kurzfristige Schwankungen der Merkmale auftreten [29]. Das Risiko eines vollständigen Verlustes des originären Merkmals ist niedrig [11]. Anhand von Audioaufnahmen lassen sich Sprechererkennungssysteme täuschen [29]. Das Risiko, dass das eine Aufzeichnung der Sprachprobe weitergegeben wird, ist moderat [29]. Ebenfalls moderat ist das Risiko, dass die Sprachprobe nachgeahmt wird. Dies ist durch das Aufzeichnen oder Nachahmen der Stimme möglich [29]. Das Nachahmen einer anderen Stimme ist schwierig, da ein persönliches Sprachbild nicht nur aus soziokulturellen Einflüssen und Sprachgewohnheiten besteht [37], sondern auch durch anatomische Merkmale geprägt wird [29]. Anhand von Aufzeichnungen einer Stimmprobe lassen sich manipulierte Stimmen erstellen [49]. Diese Audioaufnahmen benötigen eine möglichst hohe und konstante Qualität [49]. Zur Erstellung können mittels Trainingsdaten trainierte Text-to-Speech- oder Voice Conversion-Verfahren verwendet werden [49]. Bei Text-to-Speech (*dt. Text-zu-Sprache*) Verfahren wird ein eingegebener Text in ein sprecherspezifisches Audiosignal umgewandelt [49]. Bei Voice-Conversion (*dt. Stimmenumwandlung*) Verfahren stellt ein Benutzer ein Audiosignal bereit, welches nachträglich so manipuliert wird, dass es der gewollten Sprechercharakteristik entspricht [49]. Durch die Überprüfung des bei Sprechen entstehenden Schalldrucks kann jedoch die Fälschung mittels Aufzeichnungen ausgeschlossen werden [29]. Das einzigartige Sprachprofil einer Person besteht aus den statischen anatomischen Eigenschaften und den dynamischen Eigenschaften wie der Sprachmelodie oder Sprechgeschwindigkeit [29]. Stimmungsschankungen können die dynamischen Eigenschaften kurzfristig stark beeinflussen [29]. Ebenso problematisch sind Erkältungskrankheiten [29]. Erkältungen wirken sich auf die anatomischen Eigenschaften aus [29]. Aufgrund dessen besteht eine mittlere Wahrscheinlichkeit, dass sich das Sprachprofil, wenn auch nur kurzfristig, ändert [29]. Verglichen mit den anderen originären Merkmalen, ist die Sprechererkennung das unsicherste Merkmal. Sie erreicht im allgemeinen Vergleich jedoch den fünften Platz.

Ergebnisse Der Vergleich der vorgestellten Auto-ID-Systeme ergab unter den gewählten Kriterien folgende Platzierung im Bezug auf die Sicherheit:

1. Platz: Hand- und Fingervenen-Erkennung
2. Platz: Handgeometrie- und Iris-Erkennung
3. Platz: Fingerabdruck-Erkennung
4. Platz: Gesichtserkennung
5. Platz: Sprechererkennung
6. Platz: kontaktbehaftete Chipkarten
7. Platz: RFID- und NFC-Chips sowie PIN/Passwort
8. Platz: Magnetstreifenkarten

Anhand der Tabelle 3.1 wird deutlich, dass originäre Merkmale, die auf Inhärenz basieren, sich in der Frage der Sicherheit besser eignen als die zugewiesenen Merkmale, die auf Wissen und Besitz basieren.

3.2 Vergleich des Komforts

Tabelle 3.2 vergleicht den Anwendungskomfort der Auto-ID-Systeme und bewertet diesen danach, ob ein Gegenstand zur Identifizierung benötigt wird, sowie nach den Kriterien Aufwand, Schmutzempfindlichkeit des Auto-ID-Systems und subjektives Schmutzempfindes des Benutzers [11, 32, 33]. Die Auto-ID-Systeme sind dafür in auf Wissen, Besitz oder Inhärenz basierend unterteilt.

Die benutzen Kriterien dienen dazu Auto-ID-Systeme miteinander zu vergleichen, unabhängig ob sie auf Wissen, Besitz oder Inhärenz basieren. In der Bewertung für ein Auto-ID-System ist es vorteilhaft, wenn kein Gegenstand zur Identifikation benötigt wird, da dieser verloren oder vergessen werden kann [11]. Als Grundlage der Einschätzung dienen die zusammengetragenen Eigenschaften der Auto-ID-Systeme sowie die erwähnten Vor- und Nachteile aus Kapitel 2 und in Tabelle A.1. Die Bewertung erfolgt durch die Einschätzung, ob ein Komfortkriterium sehr niedrig, niedrig, mittel, hoch oder sehr hoch ist. Zur Erstellung der Rangfolge wird die Einschätzung in einen Zahlenwert übersetzt und für jedes Auto-ID-System zusammengerechnet. Sehr Niedrig gibt einen Punkt, Niedrig zwei Punkte, Mittel drei Punkte, Hoch vier Punkte und sehr Hoch fünf Punkte. Zusätzlich gibt es einen Punkt, wenn kein Gegenstand benötigt wird. Das bestmögliche Ergebnis kann demzufolge entstehen, wenn alle Komfortkriterien sehr niedrig sind und zusätzlich kein Gegenstand benötigt wird. Das schlechtestmögliche Ergebnis entsteht, wenn alle Komfortkriterien sehr hoch sind und ein Gegenstand benötigt wird.

PIN/Passwort Die PIN/Passwort-Eingabe an einer Tastatur benötigt nur das Wissen über das richtige Passwort und keinen Gegenstand zur Identifizierung [13]. Diese Möglichkeit der Zutrittskontrolle gilt als die Einfachste, da „lediglich die Kenntnis einer Zahlenkombination und die richtige Eingabe derselben voraussetzt [wird], um eine Türe [...] zu öffnen“ [13]. Der Aufwand ist dementsprechend sehr niedrig. Die Schmutzempfindlichkeit solcher Tastaturen ist meist niedrig. Dies kann daran liegen, dass es sich bei den verwendeten Tastaturen um geschlossene Systeme mit einem Gehäuse handelt. Dieses Gehäuse kann das Eindringen von

Tabelle 3.2: Komfortvergleich der Auto-ID-Systeme; Legende: Sehr Niedrig = 1, Niedrig = 2, Mittel = 3, Hoch = 4, Sehr Hoch = 5

Auto-ID-System	Gegenstand benötigt	Aufwand	Schmutzempfindlichkeit	subjektives Schmutzempfinden	Platzierung
PIN / Passwort	Nein	Sehr Niedrig	Niedrig	Hoch	2. Platz
Magnetstreifenkarten	Ja	Niedrig	Hoch	Mittel	5. Platz
kontaktbehaftete Chipkarte	Ja	Niedrig	Sehr Hoch	Mittel	6. Platz
RFID-Chips	Ja	Sehr Niedrig	Niedrig	Niedrig	1. Platz
NFC-Chips	Ja	Niedrig	Niedrig	Niedrig	2. Platz
Fingerabdruck	Nein	Niedrig	Hoch	Hoch	5. Platz
Handgeometrie	Nein	Hoch	Sehr Niedrig	Hoch	4. Platz
Handvene	Nein	Niedrig	Niedrig	Niedrig	1. Platz
Fingervene	Nein	Hoch	Mittel	Hoch	6. Platz
Gesicht	Nein	Hoch	Niedrig	Niedrig	3. Platz
Iris	Nein	Hoch	Niedrig	Niedrig	3. Platz
Sprecher	Nein	Niedrig	Niedrig	Niedrig	1. Platz

Schmutzpartikeln minimieren und schützt so die verbaute Technologie. Durch das kompakte Design sind auch die Abstände zwischen den Tasten sehr gering oder nicht existent, sodass keine größeren Schmutzpartikel eindringen können (siehe Kapitel 4.1.1, 4.2.2, 4.1.2, 4.2.3 und 4.2.4). „Wichtiger als die Schmutzempfindlichkeit der Verfahren ist die subjektive Wahrnehmung der Probanden“ [33]. Kontaktbehaftete Auto-ID-Systeme haben dabei in der Regel größere Akzeptanzprobleme, als kontaktlose Verfahren [33]. Die Haut ist zum Schutz von einer fettartigen Substanz durchzogen, welche bei jedem Kontakt zusammen mit Schmutz und anderen Hautsekreten wie Schweiß übertragen wird [50, 51]. Häufige Interaktion begünstigt den Aufbau größerer Mengen Hautsekrete und Schmutz. Bei fehlender Reinigung können diese Ablagerungen stark sichtbar und auch spürbar werden [13]. Das subjektive Schmutzempfinden und die Wahrscheinlichkeit einer daraus resultierenden Ablehnung der Verwendung ist somit hoch. Aufgrund des sehr geringen Aufwand und der niedrigen Schmutzempfindlichkeit erreicht die Eingabe eines Passwortes den zweiten Platz.

Magnetstreifenkarte Die Verwendung der Magnetstreifenkarte als Auto-ID-System basiert auf dem Besitz der Karte. Der Aufwand in der Verwendung einer Magnetstreifenkarte ist niedrig und besteht lediglich darin, sie bei sich zu führen und anschließend sehr dicht an einem Lesegerät vorbei zu ziehen [14]. Das Einführen in das Lesegerät und der direkte Kontakt können über die Zeit zu Abrieb und Verschleiß der Karte und des Magnetstreifens führen. Magnetstreifenkarten sind aufgrund ihres dünnen Design anfällig für physische Abnutzungen und Verschmutzungen [18, 52]. Diese können die Lesbarkeit des Magnetstreifen beeinträch-

tigen. Die Schmutzempfindlichkeit ist dementsprechend hoch. Das subjektive Schmutzempfinden ist bei Magnetstreifenkarten moderat. Die Karte als persönlicher Gegenstand wird meist nicht so genau betrachtet und die Verschmutzungen nicht bewusst wahrgenommen [53]. Wie bei anderen kontaktbehafteten Verfahren hat auch die Magnetstreifenkarte größere Akzeptanzprobleme [33]. Die Verwendung von Magnetstreifenkarten erreicht im Vergleich des Komforts den fünften Platz.

kontaktbehaftete Chipkarten Der Verwendungskomfort der kontaktbehafteten Chipkarten ähnelt dem der Magnetstreifenkarten. Kontaktbehaftete Chipkarten benötigen zur Identifizierung ebenfalls den Besitz eines Objektes, welches mit geringem Aufwand mit direktem Kontakt in das Lesegerät eingeführt werden muss. Allerdings sind sie aufgrund ihrer geringen Dicke und dem daraus resultierendem geringen Platz im Inneren für das Chipmodul schlechter gegen physische Beschädigungen wie Abnutzung, Korrosion oder Verschmutzung geschützt als Magnetstreifenkarten [18, 19, 54]. Das subjektive Schmutzempfinden ist trotz sehr hoher Schmutzempfindlichkeit moderat. Wie bei Magnetstreifenkarten werden kontaktbehaftete Chipkarten meist nicht genau betrachtet [53] und erreichen im Vergleich der Auto-ID-Systeme den letzten Platz.

Radio Frequency Identification Die RFID-Technologie ermöglicht eine kontaktlose Verwendung der Chipkarte und bietet damit einen deutlich höheren Verwendungskomfort. Der Aufwand in der Verwendung einer RFID-Chipkarte ist sehr niedrig und besteht lediglich darin, sie bei sich und im vorgegebenen Abstand am Lesegerät vorbei zu führen [55]. Dennoch kann diese Karte vergessen oder verloren werden [11]. Abhängig von Übertragungsverfahren kann die Übermittlung im Abstand von einem Zentimeter bis hin zu 15 Metern erfolgen. Aufgrund der geschlossenen Bauweise, sind RFID-Chipkarten vor äußeren Einflüssen geschützt [56]. Der RFID-Chip befindet sich im Inneren des Plastikgehäuses und ist damit nahezu verschleißfrei [56]. RFID-Chipkarten haben somit eine niedrige Schmutzempfindlichkeit. Ebenso niedrig ist das subjektive Schmutzempfinden bei der Verwendung von RFID-Karten. Der kontaktlose Gebrauch verlängert durch weniger Abnutzung nicht nur die Funktionsfähigkeit der RFID-Karte, sondern verringert auch die Anhaftung von Schmutz durch den direkten Kontakt mit dem Lesegerät. Zusätzlich dazu wird wie bei den Magnetstreifenkarten erläutert, die Karte als persönlicher Gegenstand nicht so genau betrachtet [53]. Aufgrund der kontaktlosen Verwendung erreicht die RFID-Chipkarte den ersten Platz.

Near Field Communication NFC ähnelt in vielen Punkten der RFID-Technologie [17]. Der Verwendungsaufwand ist im Vergleich zu RFID etwas höher, da NFC eine kürzere Reichweite hat [19]. Dennoch ist der Aufwand niedrig, da sie ebenfalls nur mit sich und in geringer Entfernung am Lesegerät vorbei geführt werden muss [55]. Die Punkte Schmutzempfindlichkeit und subjektives Schmutzempfinden sind bei RFID und NFC gleich niedrig. NFC-Karten haben ebenfalls ein geschlossenes Design und im Inneren den NFC-Chip, wodurch dieser vor Schmutz und Abnutzung geschützt ist [56, 57]. Aufgrund des etwas höheren Aufwandes durch die kürzere Reichweite erreicht die NFC-Chipkarte den zweiten Platz.

Fingerabdruck Fingerabdruckscanner arbeiten mit einem einzigartigen biometrischen Merkmal und benötigen dementsprechend keinen Gegenstand zur Identifikation. Der Verwendungsaufwand ist niedrig, da der Scan keine aufwendige Positionierung des gesamten Körpers erfordert und nur wenige Sekunden dauert [29, 33]. Der Fingerabdruckscan benötigt den

direkten Kontakt des Fingers mit einer Auflagefläche [29]. Durch die kontaktbehaftete Verwendung ist der Scanner anfällig für Schutz- und Ölanlagerungen, die durch den natürlichen Fettfilm der Haut auf den Sensor gelangen [50, 51]. Diese Verschmutzungen beeinträchtigen die Verwendung stark [43]. Staubige oder eingefettete Finger führen dazu, dass der Fingerabdruck nicht oder nur teilweise aufgenommen werden kann, da die Papillarlinien breiter aufgenommen werden und der Fingerabdruck so ineinander verfließt [43]. Es bilden sich teilweise komplett schwarze Flächen auf dem Scan [43]. Jedoch ist nicht nur die Schmutzempfindlichkeit der Aufnahme hoch, sondern auch das subjektive Schmutzempfinden des Benutzers [33]. Bei einer häufig wiederholten Verwendung des Fingerabdruckscanners können sich durch die fettige Schutzschicht der Haut sichtbare Ablagerungen bilden [50, 51], „weshalb die Fingerabdruckverfahren in der Regel mit größeren Akzeptanzproblemen behaftet sind“ [33]. Die Verwendung von Fingerabdrücken als Auto-ID-System bietet nur einen geringen Nutzerkomfort und erreicht deshalb den fünften Platz.

Handgeometrie Die Messung der Handgeometrie basiert ebenfalls auf der Inhärenz einer biometrischen Eigenschaft und hat somit den Vorteil, dass das Identifikationsmedium fest mit dem Benutzer verbunden ist [28]. Der Benutzungsaufwand ist jedoch aufgrund der aufwendigen Handpositionierung hoch (siehe Abbildung 2.6) [46]. Der Handgeometriescanner hat eine sehr niedrige Schmutzempfindlichkeit. Anders als bei dem Fingerabdruckscanner, werden Verschmutzungen vom Handgeometriescanner nicht beachtet [30]. Somit wird die Funktionsfähigkeit des Scans nicht von Schmutz beeinträchtigt. Dennoch ist der Scan durch das Anlegen an die Distanzpflöcke kontaktbehaftet und das subjektive Schmutzempfinden hoch. Durch den Kontakt mit dem Sensor können die Öle der Haut auf dem Sensor zurück bleiben und so bei häufiger Benutzung zu größeren Öl- und Schmutzansammlungen führen [50, 51]. Die Verschmutzungen können sowohl sichtbar als auch mit der Zeit spürbar sein. Aufgrund des hohen Aufwandes und subjektiven Schmutzempfindens belegt der Handgeometriescan den vierten Platz.

Handvenen Die Verwendung eines Handvenenscanners bietet nicht nur Vorteile bei der Positionierung des Scanners im Raum, da kein sichtbares Licht verwendet wird, sondern benötigt keine aufwendige Kamerapositionierung und kann schnell genutzt werden [33, 47]. Der kontaktlose Scan bedarf nur eine grobe Positionierung der Hand über dem Sensor [32, 47]. Der Aufwand ist dementsprechend niedrig. Die Schmutzempfindlichkeit des Verfahrens ist ebenfalls niedrig. Dies liegt daran, dass durch die kontaktlose Verwendung keine Schmutzpartikel und Öle der Haut auf den Sensor übertragen werden und zusätzliche im Inneren liegendes biometrisches Merkmal betrachtet wird, welches unempfindlich gegenüber Hauteigenschaften ist [34, 50, 51]. Ein weiterer Vorteil der kontaktlosen Verwendung ist, dass das subjektive Schmutzempfinden ebenfalls niedrig ist. Da kein direkter Kontakt mit dem Sensor stattfindet, nehmen die Benutzer dieses Verfahren als hygienischer war [34, 47]. Der Handvenenscan erreicht deshalb im Komfortvergleich den ersten Platz.

Fingervenen Der Fingervenenscan basiert auf derselben Grundlage wie die des Handvenenscans [34]. Jedoch bedarf der Fingervenenscan aufgrund des feineren Venenmusters einer deutlich genaueren Positionierung des Fingers [36]. Er gilt wegen des hohen Aufwandes als benutzerunfreundlicher im Vergleich zum Handvenenscan [36]. Ebenso findet er wegen der transilluminierenden Bildgebung kontaktbehaftet statt [34]. Die kontaktbehaftete Verwendung kann, wie zuvor erwähnt, dazu führen, dass sich die Öle der Haut auf dem Sensor

absetzen und somit Verschmutzungen auftreten [50, 51]. Obwohl der Scan möglicherweise nicht durch diese Verschmutzungen beeinträchtigt wird, leidet das subjektive Schmutzempfinden unter der kontaktbehafteten Nutzung [34]. Die Verwendung des Fingervenenmusters als Auto-ID-System erreicht im Komfortvergleich aufgrund der moderaten Schmutzempfindlichkeit und des hohen Schmutzempfindens durch die kontaktbehaftete Verwendung den letzten Platz.

Gesicht Die Verwendung des Gesichtes als biometrisches Merkmal benötigt eine exakte Positionierung zum Sensor und dauert deshalb länger als andere Identifikationsverfahren [33]. Zusätzlich dazu führen die zahlreichen aufwendigen Bedingungen für eine zuverlässige Verwendung zu einem hohen Aufwand [28]. So muss das aufgenommene Bild eine Frontalaufnahme, nicht verschwommen, nicht über- oder unterbelichtet sein und das vollständige Gesicht muss abgebildet werden [28]. Allerdings können auch Bärte, Brillen oder Schminke zu Einschränkungen führen [32, 38]. Dennoch bringt die Art der Gesichtserkennung auch Vorteile. Die Gesichtserkennung ist ein kontaktloses Verfahren und deshalb kaum anfällig für Verschmutzungen. Dies führt zu einer niedrigen Schmutzempfindlichkeit und einem niedrigen Schmutzempfinden. Die Gesichtserkennung befindet sich aufgrund ihres hohen Aufwandes im Mittelfeld der Auto-ID-Systeme und erreicht den dritten Platz.

Iris Der Irisscan erfordert ebenfalls eine aufwendige Positionierung des gesamten Körpers und benötigt somit mehr Zeit für die Kontrolle [33]. Die Aufnahme der individuellen Unterschiede der Iris stellt einen hohen Aufwand dar [28]. Der Irisscan ist ein kontaktloses Verfahren und hat somit die zuvor erwähnten Vorteile im Bezug auf die Schmutzempfindlichkeit und dem subjektiven Schmutzempfinden gegenüber kontaktbehafteten Verfahren [33]. Der Irisscan erreicht den dritten Platz.

Sprecher Bei der Sprechererkennung wird das einzigartige Sprachprofil einer Person genutzt um einen personengebunden Schlüssel zu erstellen [29]. Besonders bei der Sprechererkennung ist die hohe Flexibilität, die einen hohen Bedienkomfort ermöglicht [37]. Es werden anhand des Referenzmuster Toleranzen festgelegt, wodurch die Sprechererkennung auch bei Erkältungen oder Stimmungschwankungen weiter verwendet werden kann [29, 30]. Art und Umfang des persönlichen Schlüssels sind frei wählbar und können beliebig kurz oder lang sein [29]. Der Aufwand der Sprechererkennung ist gering, da zur Identifizierung lediglich der zuvor festgelegte Text ausgesprochen werden muss [29]. Da die Sprechererkennung vollständig kontaktlos abläuft, findet keine Verschmutzung des Mikrofons sowie keine Übertragung von Schmutz zu anderen Benutzern statt. Aufgrund des geringen Aufwandes sowie der Vorteile einer kontaktlosen Verwendung erreicht die Sprechererkennung den ersten Platz im Komfortvergleich.

Ergebnisse Der Vergleich der vorgestellten Auto-ID-Systeme ergab unter den gewählten Kriterien folgende Platzierung im Bezug auf den Komfort:

1. Platz: RFID-Chips, Handvenen- und Sprechererkennung
2. Platz: PIN/Passwort und NFC-Chips
3. Platz: Gesichts- und Iriserkennung
4. Platz: Handgeometrie-Erkennung
5. Platz: Magnetstreifenkarten und Fingerabdruck-Erkennung
6. Platz: kontaktbehaftete Chipkarten

Anhand der Tabelle 3.2 wird deutlich, dass mit Ausnahme der Eingabe einer PIN oder eines Passwortes kontaktlose Verfahren einen besseren Benutzungskomfort bietet. In diesem Vergleich konnte im Sinne des Komforts kein deutlicher Unterschied zwischen Auto-ID-Systemen, die auf Besitz, Wissen oder Inhärenz basieren, festgestellt werden.

3.3 Sicherheits-Komfort-Matrix

Die folgende Graphik 3.1 zeigt das Verhältnis von Sicherheit und Komfort der vorgestellten Auto-ID-Systeme. Dazu werden die Platzierungen aus den Kapiteln 3.1 und 3.2 verwendet. In der x-Achse wird die Sicherheit dargestellt und in der y-Achse der Komfort. Zusätzlich wird das Diagramm in vier Felder aufgeteilt, die anzeigen, ob ein Auto-ID-System:

- niedrige Sicherheit und niedrigen Komfort,
- niedrige Sicherheit und hohen Komfort,
- hohe Sicherheit und niedrigen Komfort oder
- hohe Sicherheit und hohen Komfort bieten.

Niedrige Sicherheit, niedriger Komfort Sowohl die Magnetstreifenkarte als auch die kontaktbehaftete Chipkarte bieten nur eine niedrige Sicherheit und niedrigen Benuterkomfort. Die Magnetstreifenkarte als Auto-ID-System weist zahlreiche Sicherheitslücken auf, wodurch Daten leicht manipulierbar oder löschbar sind und bietet durch die kontaktbehaftete Verwendung auch nur einen geringen Nutzungskomfort. Magnetstreifenkarten belegen in der Sicherheit den achten und im Komfort den fünften Platz. Auch die kontaktbehafteten Chipkarten bieten nur eine niedrige Sicherheit und einen niedrigen Komfort. Kontaktbehaftete Chipkarten sind etwas sicherer als Magnetstreifenkarten, haben aber wegen des schlechten Schutzes vor physischen Beschädigungen einen geringeren Anwendungskomfort. Sie belegen sowohl im Sicherheitsvergleich als auch im Komfortvergleich den sechsten Platz.

Hohe Sicherheit, niedriger Komfort In dem Bereich der hohen Sicherheit und des niedrigen Komforts ist der Fingerabdruckscanner, der Handgeometriescanner als auch der Fingervenenscanner einzuordnen. Den Fingerabdruck als Auto-ID-System zu verwenden, bietet aufgrund des geringen Verlust- oder Weitergaberisikos eine hohe Sicherheit. Allerdings ist der Benutzerkomfort durch die kontaktbehaftete Verwendung gering. Fingerabdruckscanner belegen in Sachen Sicherheit den dritten Platz, während sie im Komfort auf dem fünften Platz liegen. Der Handgeometriescanner ist sicherer und benutzerfreundlicher als der Fingerabdruckscanner. Wenn es um Sicherheit und Komfort geht, befinden sich die Verwendung der Handgeometrie als Auto-ID-System auf dem zweiten Platz in Sachen Sicherheit und auf

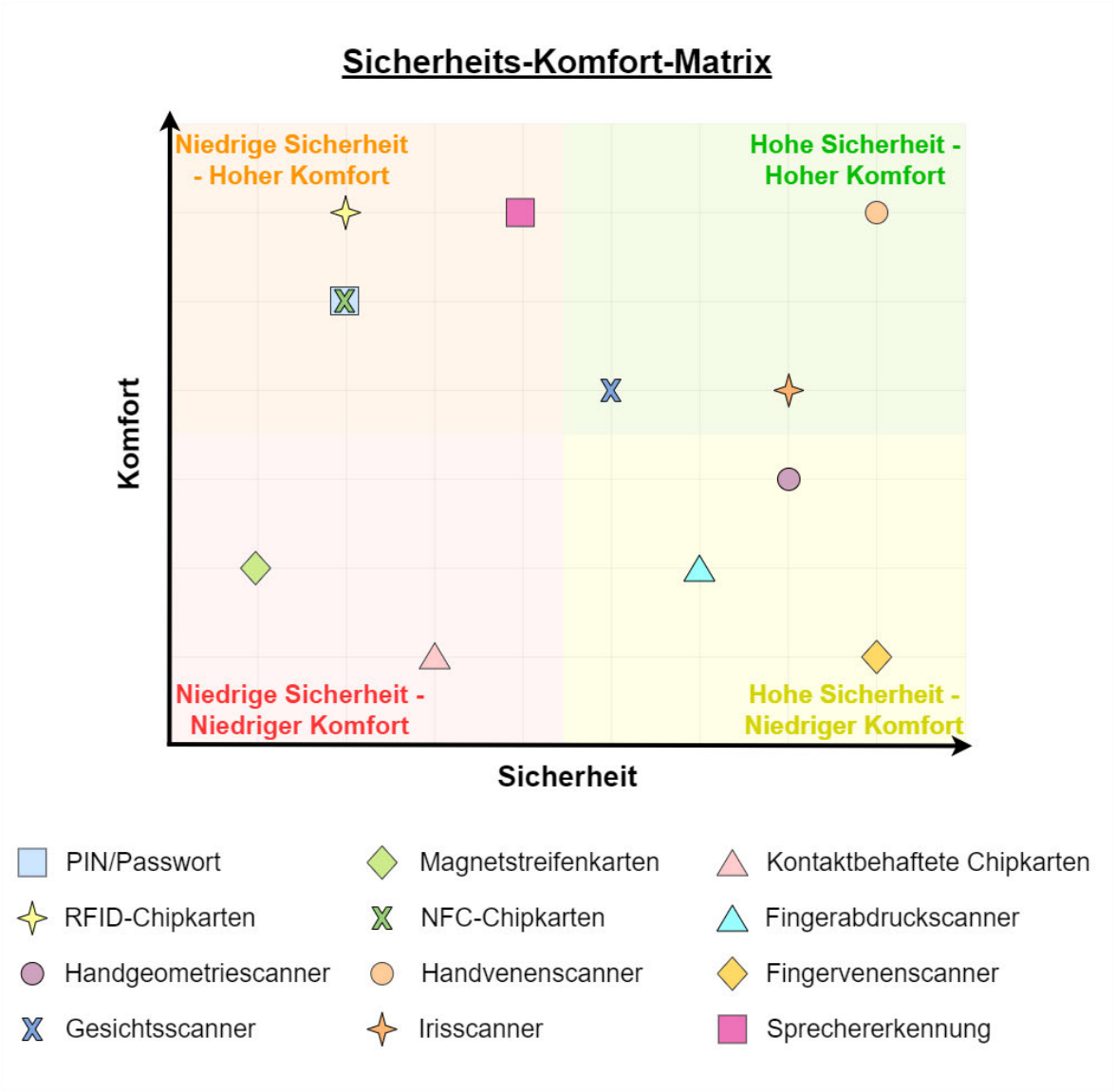

Abbildung 3.1: Verhältnis aus Sicherheit und Komfort aller vorgestellter Auto-ID-Systeme

dem vierten Platz in Bezug auf Komfort. Die hohe Sicherheit entsteht durch ein sehr niedriges Verlust- und Veränderungsrisiko der Handgeometrie. Der niedrige Komfort entsteht durch den hohen Aufwand der Handpositionierung als auch dem Unbehagen durch die kontaktbehaftete Verwendung. Die Verwendung der Fingervenen als Auto-ID-System ist eines der sichersten, jedoch aufgrund der peniblen Positionierung sowie der kontaktbehafteten Verwendung eines der benutzerunfreundlichsten Verfahren. In Bezug auf Sicherheit und Komfort nehmen Fingervenenscanner den ersten beziehungsweise den sechsten Platz ein.

Niedrige Sicherheit, hoher Komfort Als Auto-ID-System bieten die Verwendung von PIN /Passwort, NFC- als auch RFID-Chipkarten und Sprechererkennung nur eine niedrige Sicherheit, aber einen hohen Benutzungskomfort. In Punkto Sicherheit teilen sich die Verwendung von PIN /Passwort und die NFC-Chipkarten den siebten sowie in Punkto Komfort den zweiten Platz. Die geringe Sicherheit entsteht bei PIN und Passwort durch das hohe Weitergabe- und sehr hohe Nachahmungsrisiko und bei den NFC-Chipkarten durch das hohe Verlust- und Weitergaberisiko. Der hohe Komfort entsteht durch die einfache Verwendung und dem

geringen Schmutzempfinden. Die Sicherheit der RFID-Karten ist genau so gering wie die des PIN/Passwortes und der NFC-Karten. Jedoch sind RFID-Karten aufgrund der sehr einfachen Verwendung durch die hohe Funkreichweite benutzerfreundlicher. In der Sicherheit erreichen sie den siebten Platz, während sie im Komfort den ersten Platz belegen. Ebenfalls auf dem ersten Platz in Punkto Komfort liegt die Sprechererkennung. Im Bezug auf Sicherheit ist die Sprechererkennung auf dem fünften Platz einzuordnen. Ein Grund für die geringe Sicherheit ist die moderate Nachahmungswahrscheinlichkeit durch Text-to-Speech- und Voice-Conversion-Verfahren. Der hohe Komfort entsteht durch eine einfache, kontaktlose Verwendung und durch die hohe Flexibilität durch die zuverlässige Verwendung, auch bei Stimmungsschwankungen.

Hohe Sicherheit, hoher Komfort Im Bereich der hohen Sicherheit und des hohen Komforts liegen die Gesichtserkennung, der Irisscanner und der Handvenenscanner. Der Gesichts- und Irisscan liegen im Bezug auf den Komfort gemeinsam auf dem dritten Platz. Die Gesichtserkennung bietet eine moderate Sicherheit und kann auf dem vierten Platz eingeordnet werden. Der hohe Komfort entsteht durch die hygienische, kontaktlose Verwendung. Sicherer als die Gesichtserkennung ist der Irisscan. Aufgrund der vielen Einzelmerkmale der Iris lassen sich nur sehr schwer Fälschungen anfertigen, wodurch der Irisscan auf dem zweiten Platz im Sicherheitsvergleich liegt. Das sicherste und benutzerfreundlichste Auto-ID-System ist die Handvenenerkennung. In beiden Vergleichen erreicht der Handvenenscan den ersten Platz. Dies liegt an dem verborgenen biometrischen Merkmales der Venen, welches sich gar nicht oder nur sehr schwer fälschen lässt. Die kontaktlose Verwendung benötigt keine genau Positionierung der Hand und ist somit sehr benutzerfreundlich.

Anhand der Graphik 3.1 ist zu sehen, dass die Mehrheit der Auto-ID-Systeme entweder eine hohe Sicherheit oder einen hohen Komfort bieten. Die meisten Auto-ID-Systeme, die eine hohe Sicherheit haben, können nur einen niedrigen bis moderaten Komfort erreichen. Die Ausnahme bildet die Handvenenerkennung, welche sowohl eine hohe Sicherheit als auch einen hohen Komfort gewährleistet. Ebenfalls ist anhand der Graphik 3.1 zu erkennen, dass sich in den Bereichen der hohen Sicherheit ausschließlich biometrische Verfahren befinden. Das einzige biometrische Verfahren, welches nur eine geringe Sicherheit aufweist, ist die Sprechererkennung. In den Bereichen des hohen Komforts sind mit Ausnahme der PIN- und Passwort-Eingabe nur kontaktlose Verfahren einzuordnen. Kombiniert wird dies im Bereich der hohen Sicherheit und des hohen Komforts, in dem sich ausschließlich kontaktlose, biometrische Verfahren befinden.

3.4 Multi-Faktor-Authentifizierung

Die vorgestellten Systeme basieren alle auf der Ein-Faktor-Authentifizierung, bei der nur eine Art der Identifikation genutzt wird [58]. Allerdings gibt es auch Systeme, die mehrere Identifikationsarten nutzen. „Die Zwei-Faktor-Authentifizierung erfordert genau zwei Identifikationsmethoden“[58], dabei können Wissen und Besitz, Wissen und Inhärenz als auch Besitz und Inhärenz kombiniert werden. Eine weitere Möglichkeit ist die Drei-Faktor-Authentifizierung [58]. Dabei können Wissen, Besitz und Inhärenz kombiniert werden. Der entschiedene Vorteil liegt darin, dass mehrere Identifikationsmethoden gestohlen oder gefälscht werden müsste, um sich Zutritt zu verschaffen [58].

Tabelle 3.3: Kombinationsmöglichkeiten der Multi-Faktor-Authentifizierung

	Besitz	**Inhärenz**
Wissen	PIN/Passwort + Chipkarte	PIN/Passwort + biometrisches Merkmal
Besitz		Chipkarte + biometrisches Merkmal

Tabelle 3.3 zeigt die Kombinationsmöglichkeiten der Zwei-Faktor-Authentifizierung und stellt dabei jeweils ein Beispiel für jede Möglichkeit vor. Wissen und Besitz könnten kombiniert werden, indem man vor der Überprüfung einer Identifikationskarte eine PIN eingeben muss [59]. Diese Methode wird außerhalb der Zutrittskontrolle bereits bei Geldkarten verwendet [59]. Hierbei überprüft der Geldautomat nach dem Einfügen der Geldkarte erst die zugehörige PIN, bevor er weitere Interaktionen zulässt [59]. „Auch bei Zutrittskontrollanlagen ist diese Überprüfung technisch leicht durchführbar“[59] und erhöht die Sicherheit der Zutrittskontrolle [60]. Ebenso ist die Kombination aus Wissen und Inhärenz umsetzbar, indem dem biometrischen Merkmal wie zum Beispiel einem Fingerabdruck im Enrollment eine PIN zugeordnet wird [29]. Bei der eigentlichen Kontrolle muss diese PIN dann eingegeben werden, bevor das biometrische Merkmal erfasst werden kann [29]. Die letzte Möglichkeit ist die Kombination aus Besitz und Inhärenz. Dabei wird im Enrollment das Basisraster des biometrischen Merkmales auf einer Identifikationskarte gespeichert [29]. „Diese Art der zusätzlichen Überprüfung [...] macht bei elektronischen Zutrittskontrollanlagen aber nur dann einen Sinn, wenn das Referenzmuster vom System ausgelagert wird und somit auch Systemmanipulationen unterbunden werden können“[59]. Für eine Drei-Faktor-Authentifizierung ist es möglich Wissen, Besitz und Inhärenz zu kombinieren. Dabei kann ein biometrisches Merkmal auf einer Identifikationskarte gespeichert werden, bei der vor der Benutzung eine PIN eingegeben werden muss.

4 Marktübersicht

Im folgenden Kapitel erfolgt die Vorstellung verschiedener Produkte zur Zutrittskontrolle. Die vorgestellten Informationen basieren auf Herstellerangaben. Das Flussdiagramm 4.1 dient der Entscheidungshilfe, welches Auto-ID-System sich für einen privaten Benutzer oder ein Unternehmen unter gewünschten Kriterien eignen würde. Die Einordnung nach Sicherheit und Komfort entspricht den Ergebnissen aus Kapitel 3.

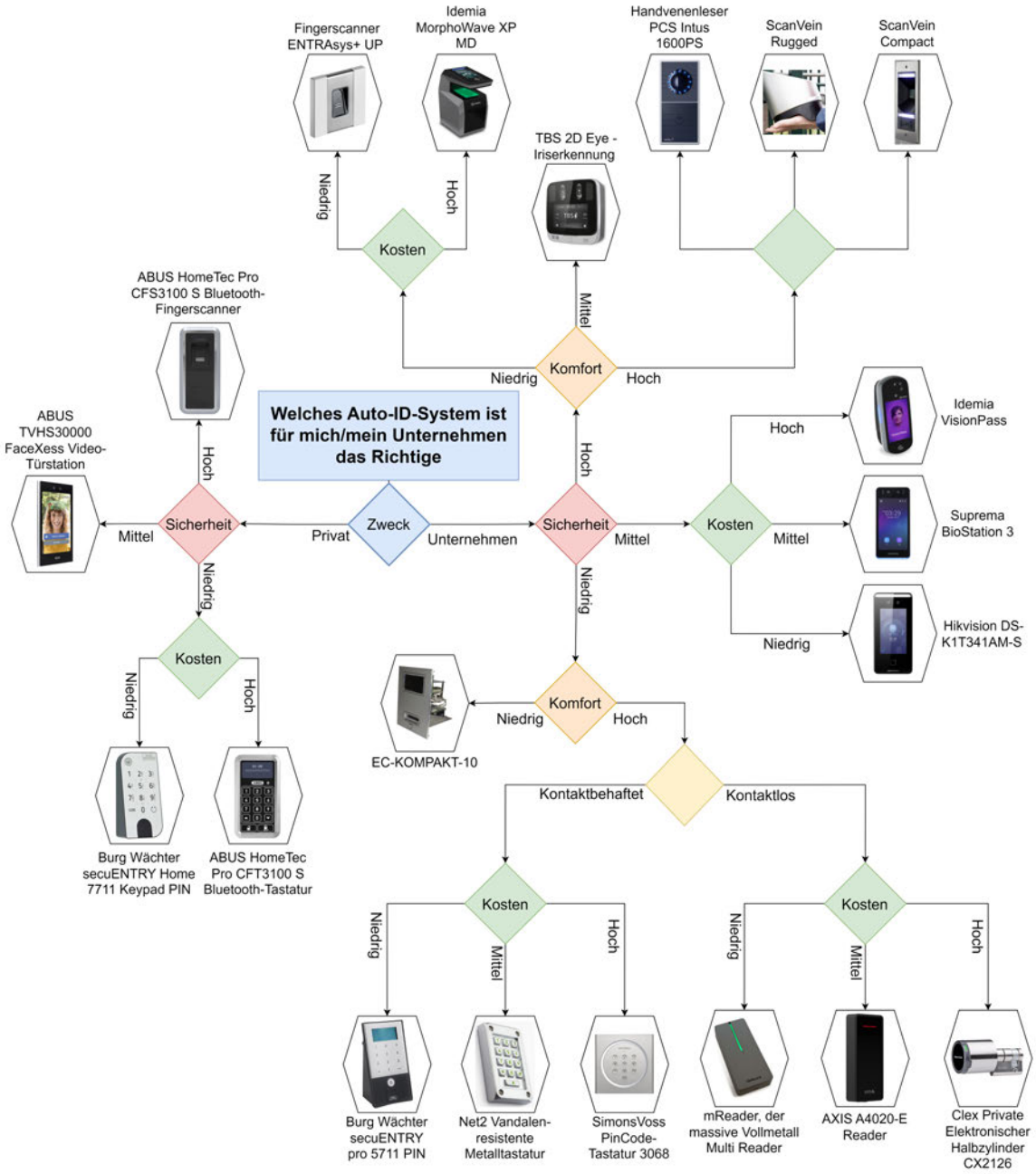

Abbildung 4.1: Flussdiagramm als Entscheidungshilfe für die Suche nach einem geeigneten Auto-ID-System mit der Unterscheidung nach privater Nutzung und der Nutzung im Unternehmen

Es werden ausgewählte Produkte vorgestellt, die in den Suchmaschinen *Google* und *Ecosia* unter den Suchbegriffen „Zutrittskontrolle“, „Zutrittssysteme“, „Zutrittskontrollsysteme“, „Produkte“, „Sachsen“, „privat“, „Home“, „kaufen“, „buy“, „Preis“, „Marktübersicht“, „Scanner“, „PIN“, „Tastatur“, „RFID“, „biometrisch“, „Venen“, „Spracherkennnung“, „Sprechererkennung“, „Magnetstreifenkarten“, „Chipkarte“, „Chipkartenlesegerät“, „Handgeometrie“, „Gesichtsleser“, „Gesichtserkennung“, „Gesicht“ und „Iris“ am 06. und 07. November 2023 zu finden waren.

4.1 private Nutzung

Die folgenden Produkte sind für die private Nutzung vorgesehen. Es werden zwei Tastaturen, ein Gesichtsscanner und ein Fingerabdrucksscanner vorgestellt.

4.1.1 Burg Wächter secuENTRY Home 7711 Keypad PIN

Abbildung 4.2: Burg Wächter secuENTRY Home 7711 Keypad PIN [61]

- Preis: 75,00 Euro
- Bedienung: per Zahlencode
- siehe Abbildung 4.2

Die secuENTRY Home 7711 Tastatur von Burg Wächter eignet sich für eine private Nutzung mit niedriger Sicherheitsanforderung und niedrigen Kosten. Das Gerät ist batteriebetrieben und ermöglicht eine Türöffnung durch die Eingabe eines Zahlencodes. Die Nutzung kann in Temperaturen von -15 bis +50 Grad Celsius und einer relativen Luftfeuchtigkeit bis 95 Prozent erfolgen. Weiterhin ist die Tastatur durch Sperrzeiten geschützt. Bei dreimaliger Falscheingabe der PIN sperrt die Tastatur für eine Minute, bei weiteren falschen Eingaben jeweils drei Minuten. [61]

4.1.2 ABUS HomeTec Pro CFT3100 S Bluetooth-Tastatur

Abbildung 4.3: ABUS HomeTec Pro CFT3100 S Bluetooth-Tastatur [62]

- Preis: 124,70 Euro
- Bedienung: per Zahlencode
- siehe Abbildung 4.3

Die HomeTec Pro CFT3100 S Bluetooth-Tastatur von ABUS ist optimal für eine private Nutzung mit niedrigen Sicherheitsbedürfnissen und einen höheren Budget. Das Gerät ist batteriebetrieben und die Türöffnung erfolgt durch die Eingabe eines Zahlencodes. Die Montage ist kabellos und dadurch einfach und flexibel. Als Gegenmaßnahme für ein ungewolltest Ausspähen des Zahlencodes kann ein Sichtschutz angebaut werden. Besonders an der Tastatur ist, dass zusätzliche zeitplanabhängige Zutrittsberechtigungen vergeben werden können. [62]

4.1.3 ABUS TVHS30000 FaceXess Video-Türstation

Abbildung 4.4: ABUS TVHS30000 FaceXess Video-Türstation [63]

- Preis: 1.111,00 Euro
- Bedienung: Gesichtserkennung
- optional mit Codeeingabe oder NFC-Karte
- siehe Abbildung 4.4

Die Gesichtserkennung mittels der TVHS30000 FaceXess Video-Türstation von ABUS ist für eine private Nutzung mit einem mittleren Sicherheitsanspruch geeignet. Das Terminal ist wasserfest und somit auch für den Außenbereich geeignet. Es wird empfohlen die Installation nicht selbst vorzunehmen und regelmäßige Wartungen durchzuführen, um eine zuverlässige

Verwendung zu garantieren. Die Gesichtserkennung erfolgt schnell, kontaktlos und auf bis zu drei Metern. Eine Gesichtserkennung ist durch die Dual-Kamera, bestehend aus einer optischen und einer Infrarot-Kamera, sowohl am Tag und in der Nacht möglich. Ebenfalls ist dadurch eine zuverlässige Kontrolle trotz Masken oder Mützen möglich. Dabei verfügt das Terminal über eine Anti-Spoofing-Technologie mit der eine Überlistung durch Fotos oder Videos verhindert werden kann. Zusätzlich kann eine zwei-Faktor-Authentifizierung mittels NFC oder PIN erfolgen. Die Benutzerdaten werden auf dem Gerät verschlüsselt gespeichert. Besucherdaten werden nicht gespeichert. Für Besucher existiert eine separate virtuelle Klingeltaste. [63, 64]

4.1.4 ABUS HomeTec Pro CFS3100 S Bluetooth-Fingerscanner

Abbildung 4.5: ABUS HomeTec Pro CFS3100 S Bluetooth-Fingerscanner [65]

- Preis: 232,85 Euro
- Bedienung: per Fingerabdruck
- siehe Abbildung 4.5

Der ABUS HomeTec Pro CFS3100 S Bluetooth-Fingerscanner ist geeignet für die private Zutrittskontrolle bei einem hohen Sicherheitsanspruch. Dabei wird die Tür mit dem Fingerabdruck geöffnet und geschlossen. Es können bis zu 28 verschiedene Finger registriert werden. Der Fingerabdruckscanner ist batteriebetrieben und kann einfach und flexibel auch in Außenbereichen montiert werden. [65]

4.2 Nutzung im Unternehmen

Die folgenden Produkte sind für die Nutzung im Unternehmen vorgesehen. Es werden ein Magnetstreifen- und Chipkartenlesegerät, drei Tastaturen, drei RFID-Leser, drei Gesichtserkenner, zwei Fingerabdruckscanner, ein Iriserkenner und drei Handvenenscanner vorgestellt.

4.2.1 EC-KOMPAKT-10

Abbildung 4.6: EC-KOMPAKT-10 von W. Arnold GmbH [66]

- Preis: unbekannt
- Bedienung: per Magnetstreifen- und Chipkarten
- siehe Abbildung 4.6

Der EC-KOMPAKT-10 von W. Arnold GmbH ist ein Zutrittskontrollsystem für Magnetstreifen- und Chipkarten. Das Haupteinsatzgebiet ist die Zutrittskontrolle mit Bankkarten, jedoch kann die Zutrittskontrolle auch unabhängig davon erfolgen. Der motorisierte Kartenleser ist für Umgebungsbedingungen von -5 bis +50 Grad Celsius und 10 bis 90 Prozent relative Luftfeuchtigkeit ausgelegt. [66]

4.2.2 Burg Wächter secuENTRY pro 5711 PIN

Abbildung 4.7: Burg Wächter secuENTRY pro 5711 PIN [67]

- Preis: 165,00 Euro
- Bedienung: per Zahlencode
- siehe Abbildung 4.7

Die Tastatur secuENTRY pro 5711 PIN von Burg Wächter eignet sich optimal für ein Unternehmen, welches einen niedrigen Sicherheitsbedarf hat, hohen Komfort und eine kontaktbehaftete Anwendung zu einem niedrigen Preis sucht. Die Montage ist flexibel, da das Gerät zusätzlich über Bluetooth verfügt und batteriebetrieben ist. Die Tastatur kann deshalb in bis zu vier Metern Entfernung zum Schließzylinder angebracht werden. Die Anbringung im Außenbereich ist durch die staub- und wasserdichte Bauweise möglich. Auf dem secuENTRY pro 5711 PIN lassen sich bis zu 2000 sechsstellige Codes speichern. Das System arbeitet mit personenbezogenen Codes für die Zutrittskontrolle. Bei dreimaliger Falscheingabe des Codes sperrt sich die Eingabe eine Minute, jede weitere falsche Eingabe erhöht die Sperrzeit auf weitere drei Minuten. [67]

Abbildung 4.8: Net2 Vandalen-resistente Metalltastatur von Paxton [68]

4.2.3 Net2 Vandalen-resistente Metalltastatur

- Preis: 188,00 Euro
- Bedienung: per Zahlencode
- siehe Abbildung 4.8

Die vandalen-resistente Metalltastatur Net2 von Paxton ist optimal für ein Unternehmen, welches einen niedrigen Sicherheitsbedarf hat, hohen Komfort und eine kontaktbehaftete Anwendung zu einem mittleren Preis sucht. Das robuste Metallgehäuse ist nicht nur vor Vandalismus geschützt, sondern auch wetterfest und frostsicher, sodass die Metalltastatur sowohl im Innen- als auch Außenbereich angewendet werden kann. Der Hintergrund der einzelnen Tasten ist beleuchtet, sodass sie sich auch für die Anwendung im Dunkeln eignet. Die Zutrittskontrolle wird computerbasiert gesteuert und ermöglicht die Verwaltung von bis zu 50.000 Nutzern. [68–70]

4.2.4 SimonsVoss PinCode-Tastatur 3068

Abbildung 4.9: SimonsVoss PinCode-Tastatur 3068 [71]

- Preis: 349,90 Euro
- Bedienung: per Zahlencode
- siehe Abbildung 4.9

Die PinCode-Tastatur 3068 von SimonsVoss ist geeignet für ein Unternehmen, welches nur eine niedrige Sicherheit abdecken muss, dafür aber einen hohen Komfort und eine kontaktbehaftete Anwendung suchen und ein hohes Budget haben. Die Tastatur ist batteriebetrieben und ermöglicht deshalb eine einfache Installation sowohl im Innen- als auch Außenbereich. Die Bedienung erfolgt durch die Eingabe einer vier- bis achtstelligen PIN. Es können bis zu drei unterschiedliche PIN vergeben werden. Die Tastatur verfügt über einen Manipulationsalarm, der nach fünfmaliger falscher Eingabe einen akustischen Ton für eine Minute abspielt. [71–73]

Abbildung 4.10: mReader, der massive Vollmetall Multi Reader [74]

4.2.5 mReader, der massive Vollmetall Multi Reader

- Preis: 79,00 Euro
- Bedienung: durch RFID
- siehe Abbildung 4.10

Der mReader ist optimal für ein Unternehmen, welches eine Zutrittskontrolle für eine niedrige Sicherheit mit hohem Komfort und einer Kontaktlosen Anwendung sucht und dabei nur ein niedriges Budget hat. Der mReader ist ein RFID-Lesegerät, welches mit den Frequenzen 125 kHz und 13,56 MHz arbeitet. Dies ermöglicht eine Lesereichweite von bis zu fünf Zentrimetern. Durch das Vollmetallgehäuse ist das RFID-Lesegerät wasserdicht und somit für den Außenbereich bei Temperaturen von -20 bis +50 Grad Celsius und einer Luftfeuchtigkeit bis 95 Prozent geeignet. [74]

4.2.6 AXIS A4020-E Reader

Abbildung 4.11: AXIS A4020-E Reader [75]

- Preis: 244,95 Euro
- Bedienung: durch RFID
- siehe Abbildung 4.11

Der AXIS A4020-E Reader ist optimal für die Nutzung im Unternehmen, welches nur ein niedrigen Sicherheitsanspruch hat, aber hohen Komfort und eine kontaktlose Anwendung sucht und das zu einem mittleren Preis. Die robuste Bauart schützt das Lesegerät und ermöglicht einen Einsatz im Innen- sowie Außenbereich. Der RFID-Leser A4020-E unterstützt die meisten Karten, die mit 13,56 MHz arbeiten. Zusätzlich besitzt der Leser eine Manipulationserfassung, welche den Besitzer über Manipulationsversuche informiert. [75, 76]

Abbildung 4.12: Clex Private Elektronischer Halbzylinder CX2126 [77]

4.2.7 Clex Private Elektronischer Halbzylinder CX2126

- Preis: ab 614,90 Euro
- Bedienung: durch RFID
- siehe Abbildung 4.12

Der elektrische Halbzylinder CX2126 von Clex kann für ein Unternehmen mit niedrigem Sicherheits- und hohem Komfortanspruch auf ein kontaktlose Verwendung genutzt werden, wenn ein hohes Budget zur Verfügung steht. Der Halbzylinder ist batteriebetrieben und lässt sich in jedes handelsübliche Schloss einbauen. Es gibt eine Version, die auch wassergeschützt und somit für den Außenbereich geeignet ist. Es kann eine Anwendung in einem Temperaturbereich von -20 bis +65 Grad Celsius stattfinden. Der elektrische Halbzylinder CX2126 von Clex arbeitet auf 868 MHz und kann bis zu 96 passive Transponder verwalten. [77]

4.2.8 HIKVISION DS-K1T341AM-S Gesichtserkennungsterminal

Abbildung 4.13: HIKVISION DS-K1T341AM-S Gesichtserkennungsterminal [78]

- Preis: 408.17 Euro
- Bedienung: per Gesichtserkennung und RFID
- siehe Abbildung 4.13

Das HIKVISION DS-K1T341AM-S Gesichtserkennungsterminal ist optimal für Unternehmen, die mittlere Sicherheitsbereiche absichern muss und dabei nur ein niedriges Budget hat. Die Gesichtserkennung findet bequem und schnell aus einer Entfernung von 0,3 bis 1,5 Metern und in unter 0,2 Sekunden statt. Das Gerät kann bis zu 1500 Gesichter und zusätzlich auch bis zu 1500 RFID-Karten speichern. Es können Karten gelesen werden, die im 13,56 MHz Bereich arbeiten. Das Gesichtserkennungsterminal kann sowohl im Innen- als auch Außenbereich verwendet werden und verträgt Temperaturen von -30 bis +60 Grad Celsius und eine Luftfeuchtigkeit von bis zu 90 Prozent. [78, 79]

Abbildung 4.14: Suprema BioStation 3 [80]

4.2.9 Suprema BioStation 3

- Preis: ab 1.875,00 Euro
- Bedienung: per Gesichtserkennung und RFID
- siehe Abbildung 4.14

Die Suprema BioStation 3 ist ein Gesichtserkennungssystem, welches optimal für die Nutzung in Unternehmen ist, welche ein mittleres Sicherheitsbedürfnis haben und ein mittleres Budget. Zusätzlich zu einem Zutrittskontrollsystem ist die BioStation 3 auch eine Türsprechanlage. Es können bis zu 100.000 Nutzer verwaltet werden. Neben der Gesichtserkennung, können auch RFID-Karten gelesen werden, die in einem Bereich von 125 kHz und 13,56 MHz arbeiten. Das Gerät kann sowohl im Innen- als auch Außenbereich verwendet werden und bleibt bei Temperaturen von -20 bis +50 Grad Celsius und einer Luftfeuchtigkeit von bis zu 95 Prozent funktionsfähig. [80, 81]

4.2.10 Idemia VisionPass

Abbildung 4.15: Idemia VisionPass [82]

- Preis: 5.207,20 Euro
- Bedienung: per Gesichtseerkennung
- siehe Abbildung 4.15

Das Gesichtserkennungsterminal VisionPass von Idemia eignet sich optimal in Unternehmen, die ein mittleren Sicherheitsbereich absichern müssen und dabei ein hohes Budget zur Verfügung haben. Das Termininal besitzt sowohl einen zwei- und dreidimensionalen als auch

einen Infrarot-Sensor, sodass bei alle Lichtverhältnissen eine Zutrittskontrolle stattfinden kann. Es ist sowohl möglich das Terminal innen als auch außen anzubringen. Das Terminal kann in Temperaturen von -10 bis +45 Grad Celsius und einer Luftfeuchtigkeit von 10 bis 80 Prozent arbeiten. Die Gesichtsidentifizierung kann in circa einer Sekunde stattfinden, sodass eine Person im Laufen nicht stoppen muss. Für eine komfortable und rollstuhlgerechte Anwendung verfügt der Sensor über einen vertikalen Erkennungswinkel von 120 bis 210 Zentimetern. Die Gesichtserkennung benötigt nur 30 Prozent des Gesichts, um eine Person identifizieren zu können, sodass problemlos auf Masken, Bärten oder Schminke reagiert werden kann. Es können 20.000 Benutzer verwaltet werden. Mit der passenden Lizenz kann dies auf 40.000 erweitert werden. Als Schutzmaßnahme verfügt der Idemia VisionPass über eine Antispoofing-Technologie, die sowohl digitale als auch ausgedruckte Fotos und dreidimensionale Masken erkennt. [82–85]

4.2.11 Fingerscanner ENTRAsys+ UP

Abbildung 4.16: Fingerscanner ENTRAsys+ UP [86]

- Preis: 220,15 Euro
- Bedienung: per Fingerabdruck
- siehe Abbildung 4.16

Der Fingerscanner ENTRAsys+ UP kann in einem Unternehmen eingesetzt werden, welches einen hohen Sicherheitsbereich schützen soll, dabei nur einen niedrigen Komfort benötigt und nur ein kleines Budget hat. Es können bis zu 50 Fingerabdrücke gespeichert werden. Der Fingerabdruckscanner kann von -25 bis +55 Grad Celsius eingesetzt werden. [86]

4.2.12 Idemia MorphoWave XP MD

- Preis: 5.870,87 Euro
- Bedienung: per Fingerabdruck sowie RFID und NFC
- siehe Abbildung 4.17

Der berührungslose Fingerabdruckscanner MorphoWave XP MD von Idemia ist optimal für ein Unternehmen, das einen hohen Sicherheitsbereich schützen muss, nur niedrige Ansprüche an den Komfort hat und ein ein hohes Budget zur Verfügung steht. Der Fingerscan funktioniert kontaktlos durch eine Winkbewegung. Dabei kann die Hand schnell und intuitiv durch den Sensor geführt werden. Das Scannen und Verifizieren der vier Fingerabdrücke dauert

Abbildung 4.17: Idemia MorphoWave XP MD [87]

nicht länger als eine Sekunden, wodurch sich der Scanner in Bereichen mit hohem Personendurchsatz eignet. Zusätzlich können bis zu 100.00 Benutzer verwaltet werden. Durch den Einsatz einer künstlichen Intelligenz können auch beschädigte, nasse, schmutzige oder trockene Fingerabdrücke gescannt werden. Neben dem Fingerabdruckscan kann die Zutrittskontrolle auch mit allen kontaktlosen Kartentechnologien wie RFID und NFC erfolgen. Der Idemia MorphoWave Finegrabdruckscanner verfügt zum Schutz vor unbefugten Zutritt sowohl über eine Fingerabdrucktäuschungserkennung sowie einer Doppelbenutzungssperre, bei der eine Person einen Raum erst wieder verlassen muss, bevor sie sich wieder anmelden kann [88]. Der Scanner ist für Betriebstemperaturen von -10 bis +55 Grad Celsius geeignet. [87, 89–91]

4.2.13 TBS 2D Eye-Iriserkennung

Abbildung 4.18: TBS 2D Eye-Iriserkennung [92]

- Preis: unbekannt
- Bedienung: per Iriserkennung
- optional: per PIN
- siehe Abbildung 4.18

Die zweidimensionale Iriserkennung 2D Eye von TBS kann in Unternehmen mit hohen Sicherheits- und mittleren Komfortansprüchen eingesetzt werden. Die Iriserkennung kann mit einer oder beiden Iriden stattfinden, dabei wird die Iris mittels einer Gesichtserkennung automatisch lokalisiert. Es können standardmäßig bis zu 10.000 Benutzer verwaltet werden. Die Verwendung ist nur im Innenbereich und bei einer Betriebstemperatur von Null bis +45 Grad Celsius sowie einer Luftfeuchtigkeit von 10 bis 90 Prozent vorgesehen. [92–94]

Abbildung 4.19: Handvenenleser PCS INTUS 1600PS [95]

4.2.14 Handvenenleser PCS INTUS 1600PS

- Preis: unbekannt
- Bedienung: per Handvenenscan
- optional: per PIN und RFID
- siehe Abbildung 4.19

Der INTUS 1600PS Handvenenscanner ist optimal geeignet für Unternehmen, die sowohl einen hohen Sicherheitsbedarf haben, als auch einen hohen Komfortanspruch. Der Scanner arbeitet mit der PalmSecure Technologie von Fujitsu und kann optional auch mit PIN oder RFID bedient werden. Der Handvenenscan erfolgt kontaktlos und in einem Abstand von drei bis acht Zentimetern. Es können bis zu 1000 Nutzer verwaltet werden. Der Betrieb des Scanner ist nur bei Temperaturen von +5 bis +40 Grad Celsius möglich und somit nur für den Innenbereich. In einem Zusatzpaket ist es jedoch möglich eine Heizung einbauen zu lassen, wodurch der Scanner für den Außenbereich und Betriebstemperaturen von -20 bis +40 Grad Celsius geeignet ist. [95, 96]

4.2.15 ScanVein Rugged

Abbildung 4.20: ScanVein Rugged [97]

- Preis: unbekannt
- Bedienung: per Handvenenscan
- siehe Abbildung 4.20

Der Handvenenscanner ScanVein Rugged ist optimal für Unternehmen, die einen hohen Sicherheits- und Komfortanspruch haben. Der Scanner ist für den Außeneinsatz konzipiert. Er ist allwetter- und salzwasserbeständig und wurde in Betriebstemperaturen von -25 bis +85 Grad Celsius erfolgreich getestet. [97]

4.2.16 ScanVein Compact

Abbildung 4.21: ScanVein Compact [98]

- Preis: unbekannt
- Bedienung: per Handvenenscan
- optional: per RFID
- siehe Abbildung 4.21

Der Handvenenscanner ScanVein Compact ist optimal in Unternehmen, die einen hohen Sicherheitsbereich schützen müssen und dabei hohen Komfort suchen. Der Scanner arbeitet mit der PalmSecure Technologie von Fujitsu. Er kann im geschützten Außenbereich bei Temperaturen von -25 bis +85 Grad Celsius und einer Luftfeuchtigkeit von bis zu 100 Prozent eingesetzt werden. Zum Schutz verfügt er über eine Sabotage-Detektion. [98]

5 Fazit

In dieser Arbeit wurden unterschiedliche Auto-ID-Systeme vorgestellt, näher betrachtet und anschließend nach Sicherheit und Benutzungskomfort sortiert. Es wurden die PIN/Passwort-Eingabe, die Magnetstreifen- und kontaktbehafteten Chipkarten, RFID- und NFC-Systeme, Fingerabdruck-, Handgeometrie-, Handvenen-, Fingervenen-, Gesichts-, Iris-, Retina-, Sklera- und Sprechererkennung betrachtet. Anschließend wurde die Sicherheit der Systeme anhand ihres Verlust-, Weitergabe- und Nachahmungsrisiko sowie anhand ihrer Veränderbarkeit als auch existierenden Schutzmechanismen bewertet. Die Bewertung des Anwendungskomforts erfolgte durch die Tatsache, ob ein Gegenstand benötigt wird und wie hoch der Aufwand, die Schmutzempfindlichkeit und das subjektive Schmutzempfinden ist. Diese Bewertungen ermöglichten es, eine Rangfolge der Auto-ID-Systeme zu bilden. Die Hand- und Fingervenenerkennung belegen in Punkto Sicherheit den ersten Platz. Auf dem zweiten Platz liegen die Handgeometrie- und Iriserkennung. Der dritte Platz wird von der Fingerabdruckerkennung, der vierte Platz von der Gesichtserkennung und der fünfte Platz von der Sprechererkennung belegt. Auf dem sechsten Platz liegen die kontaktbehafteten Chipkarten. Den siebten Platz teilen sich die RFID- und NFC-Chips sowie die PIN/Passwort-Eingabe. Den achten und somit letzten Platz im Vergleich der Sicherheit belegen die Magnetstreifenkarten. Im Vergleich des Komforts belegen die RFID-Chips sowie die Handvenen- und Sprechererkennung den ersten Platz. Den zweiten Platz teilen sich die PIN/Passwort-Eingabe und die NFC-Chips. Anschließend folgen auf dem dritten Platz die Gesichts- und Iriserkennung, auf dem vierten Platz die Handgeometrieerkennung und auf dem fünften Platz die Magnetstreifenkarten und die Fingerabdruckserkennung. Den sechsten und letzten Platz belegen die kontaktbehafteten Chipkarten. Anhand dieser Rangfolgen wurde ein Vergleich zum Verhältnis aus Sicherheit und Komfort erstellt.

Dabei wurde deutlich, dass der Handvenenscan in allen Bereichen führend ist und für viele Anwendungen ein optimales Zutrittskontrollsystem darstellt. Dies liegt am sehr niedrige Verlust-, Weitergabe- und Nachahmungsrisiko sowie an der kontaktlosen Verwendung, dem geringen Aufwand, der niedrigen Schmutzempfindlichkeit und dem niedrigen Schmutzempfinden. Magnetstreifen- und kontaktbehaftete Chipkarten stellten sich hingegen in allen Bereichen aufgrund der niedrigen Sicherheit und des niedrigen Komforts als mangelhaft heraus. Bei den anderen vorgestellten Auto-ID-Systeme zeichnetet sich grob ab, dass Komfort und Sicherheit umgekehrt proportional zu einander sind. Steigt der Komfort, sinkt die Sicherheit und steigt die Sicherheit, sinkt der Komfort. Weiterhin zeigte sich, dass überwiegend die biometrische Zutrittskontrollsysteme eine höhere Sicherheit aufweisen. Im Bereich eines Benutzerkomforts sind es mehrheitlich kontaktlose Verfahren, die eine hohe Bewertung erzielten. Viele Nachteile beim Abwägen zwischen Sicherheit und Komfort könnten durch eine Multi-Faktor-Authentifizierung ausgeglichen werden.

Bei der Beurteilung der Auto-ID-Systeme und dem Erstellen einer Übersicht ausgewählter Auto-ID-Systeme kam es zu diversen Herausforderungen. Eine dieser bestand in der Beurteilung der Systeme im Bereich Komfort. Dafür wurde auf bekannten Suchmaschinen wie Google, Google Scolar und Ecosia als auch auf Informationsdiensten wie SpringerLink nach ausführlichen Studien oder Auseinandersetzungen zu diesem Thema gesucht. Während der

Recherche konnten jedoch keine Studien gefunden werden. In allen allgemeinen Quellen zu den Zutrittskontrollsystemen konnte nur festgestellt werden, dass kontaktbehaftete Verfahren gegenüber kontaktlosen Verfahren aufgrund der hygienischen Bedenken Nachteile haben. Die durchgeführte Bewertung des Komforts ist aufgrund der geringen Quellenlage lediglich subjektiv und anhand logischer Rückschlüsse zum Hygieneverhalten entstanden. Eine weitere Herausforderung gab es bei der Erstellung einer Marktübersicht. Die Abbildung der aktuell auf dem Markt verkauften Systeme war nur begrenzt realisierbar. Dies lag unter anderem an der Tatsache, dass einige Informationen nicht frei zugänglich waren. Einige Unternehmen und Vertriebe stellen die Informationen zu ihren Produkten und Preisen nur über gesonderte Anfragen von Unternehmen an ein Verkaufsteam zur Verfügung. Diese Anfragen bedurften Informationen wie Firmennamen oder Anzahl der Mitarbeiter. Als Privatperson war diese Kontaktaufnahme dadurch nicht möglich. Einige Vertriebsseiten boten einen eingeschränkten Einblick für Privatpersonen. Für die vollständigen Informationen und Preise benötigte man jedoch lizenzierte Handelsaccounts. Ebenfalls herausfordernd war, dass viele Auto-ID-Systeme theoretisch für die Zutrittskontrolle geeignet sind, aber in der Realität keine oder kaum kommerzielle Anwendung finden. Dies kann unterschiedliche Gründe haben. Ein Grund bei der Skleraerkennung war die Übernahme des Start-Up und Entwicklers *EyeVerify* durch die *Alibaba-Group* [34]. Im Anschluss verschwand die neu erforschte Technik vom Markt.

In dieser Bachelorarbeit konnte eine umfassende Übersicht zum Thema Zutrittskontrollsysteme gegeben werden, wobei der Schwerpunkt auf einer allgemeinen Betrachtung zum Einstieg in das Thema lag. Aufgrund des begrenzten Umfangs dieser Arbeit konnten einige spezifische Auto-ID-Systeme nicht näher behandelt werden. Während den Recherchen zu den originären Merkmalen konnten weitere biometrische Merkmale gefunden werden, die sich in der Theorie aufgrund ihrer Verbreitung für die Zutrittskontrolle eignen würden. Darunter fallen die Ohr-, Geruchs- oder Gangerkennung. Jedoch variiert die Einzigartigkeit und Konstanz dieser Merkmale. Zukünftige Forschungen könnten sich auf diesen originären Merkmalen und ihrer Eignung als Zutrittskontrollsystem konzentrieren. Weiterhin wurden die zahlreichen App- und Bluetooth-Lösungen aufgrund des begrenzten Umfanges nicht näher betrachtet werden. Diese könnten in zukünftigen Forschungen spezifische untersucht werden. Die vorliegende Arbeit legt somit den Grundstein für weiterführende Forschungen.

Anhang A: Tabelle Übersicht

Tabelle A.1: Übersicht aller Auto-ID-Systeme aus Kapitel 2 eingeteilt in die Art ihrer Authentifizierung mit Beschreibung der grundlegenden Technik sowie ihren Vor- und Nachteilen

Auto-ID-Systeme	**Art der Authentifizierung**	**Technik**	**Vor- und Nachteile**
PIN / Passwort	Wissen	Eingabe eines tür- oder personenbezogenen Codes ins Tastaturfeld [13]	Vorteile: – sehr einfach [13] – sehr kostengünstig [13] Nachteile: – leicht überwindbar [13] – einfache Weitergabe des Codes [13] – nur unzureichende Schutzmechanismen (wie Sichtschutz, Ziffernzerwürflung oder Sperrung bei Falscheingabe) [13]
Magnetstreifenkarten	Besitz	elektromagnetische Speicherung von Informationen auf einem Magnetstreifen [16]	Vorteile: – kostengünstig [14] Nachteile: – Beschädigung oder Löschen der Daten durch Entmagnetisierung [16] – Beliebiges Kopieren, Lesen, Verändern oder Löschen der Daten [17]

kontakt-behaftete Chipkarten	Besitz	Datenüber-tragung durch direkten Kontakt zwischen Lese-gerät und Karte mit eingebautem Mikrochip; Un-terscheidung in Speicher- und Prozessorkarten [18, 19]	<u>Vorteile:</u> – kostengünstig [14] – gesicherter Speicherzugriff bei Speicherkarten mit Si-cherheitslogik durch PIN [19] – Verschlüsselung der Daten auf Prozessorkarten durch zwischen Speicher und Aus-gabe geschalteten Prozessor [19] <u>Nachteile:</u> – schlecht vor Abnutzung, Ver-schmutzung und Korrosion ge-schützt [18] – ungesicherter Speicher-zugriff bei Speicherkarten ohne Sicherheitslogik [19]
RFID	Besitz	Kontaktlose Da-tenübertragung durch Funker-kennung von Radiowellen [20]; Nutzung von Niedrig-, Hoch- oder Ultra-Hoch-Frequenzen [21]; 13,56 MHz weltweit am häu-figsten genutzte Frequenz [22]	<u>Vorteile:</u> – schnelle Datenübertragung [21] – kontaktlose Übertragung mit Reichweiten von 1 cm bis 15 m [21] – Antikollision und möglicher Mehrfachzugriff [21] <u>Nachteile:</u> – Frequenznutzung unterliegt staatlichen Regelungen [21] – Eigenschaften und Reichwei-te stark abhängig von der ge-wählten Frequenz [21] – Daten können einfach ausge-lesen, manipuliert oder ge-löscht werden [24]

NFC	Besitz	kontaktlose Datenübertragung basierend auf RFID- und Chipkarten-Standard; keine Trennung zwischen Lesegerät und Transponder [17]	Vorteile: – kontaktlose Datenübertragung mit einer Reichweite bis zu 10 cm [19] – NFC-Systeme können je Notwendigkeit sowohl Lesegerät als auch Transponder sein [25] – Integration mehrerer Schlüssel [26] Nachteile: – kontaktlose Datenübertragung kann einfach und aus großer Entfernung abgehört werden [19] – Datenübertragung kann durch Störsender geblockt werden [19]
Fingerabdruck	Inhärenz	dreidimensionales Abtasten der individuellen Erhöhungen des Fingers [28]; Erstellung eines Referenzmusters durch Umwandlung der Erhebungen in digitale Signale [28]	Vorteile: – Universell vorhanden (Ausnahme Krankheit) [31] – Einzigartigkeit der Fingerabdrücke 1:1.000.000 [30] – ein Leben lang gleich (Ausnahme Krankheit und Verletzungen) [31] – Lebendfingerspektronomie durch Farblicht [29] Nachteile: – Probleme bei Kindern und älteren Menschen [32] – Abdruck durch Verschmutzung und Verletzungen beeinträchtigt [32] – kontaktbehaftetes Verfahren [30]

Handgeometrie	Inhärenz	dreidimensionale, optische Vermessung der ausschlaggebenden geometrischen Handproportionen [29, 30]; Erstellung eines digitalen Referenzmusters [29]	Vorteile: – Universell vorhanden [29] – Einzigartigkeit der Handgeometrie 1:1.000 [30] – Nicht beeinflussbar durch Fingerabdrücke, Narben oder Schmutz [30] – dreidimensionale Messung verhindert Betrug durch Fotografien [29] Nachteile: – kontaktbehaftet [29]
Handvene	Inhärenz	Sichtbarmachung des Handvenenmusters aufgrund von Absorption der verwendeten Nahinfrarotlicht durch das Hämoglobin im Blut [30, 32]; reflektierte Bildgebung [34]; Umwandlung des Musters in ein digitales Referenzmuster [35]	Vorteile: – Universell vorhanden [32] – Einzigartig [32] – ein Leben lang gleich [32] – Prüfung auf Blutfluss und Puls durch Nahinfrarotlicht [34] – kontaktlos [32, 34]

Fingervene	Inhärenz	Sichtbarmachung des Fingervenenmusters aufgrund von Absorption der verwendeten Nahinfrarotlicht durch das Hämoglobin im Blut [30, 32]; transilluminierende Bildgebung [34]; Umwandlung des Musters in ein digitales Referenzmuster [35]	<u>Vorteile:</u> – Universell vorhanden [32] – Einzigartig [32] – ein Leben lang gleich [32] – Prüfung auf Blutfluss und Puls durch Nahinfrarotlicht [34] <u>Nachteile:</u> – kontaktbehaftet [34] – höherer Energieverbrauch [34] – wenige Bezugspunkte der Venen [36] – benötigt exakte Positionierung des Fingers [36]
Gesicht	Inhärenz	zwei- oder dreidimensionaler Scan des Gesichts und Berechnung der Gesichtsähnlichkeit durch spezifische, lokale Knotenpunkte [28, 37]	<u>Vorteile:</u> – Universell vorhanden – kontaktlos [37] – benötigt nur wenige Referenzbilder [37] <u>Nachteile:</u> – benötigte Reduktion der Gesichtsdaten kann zum Merkmals- und Informationsverlust führen [37] – hohe Ansprüche an die Qualität der Referenzbilder [28] – benötigt aufwendige Positionseinnahme des gesamten Körpers [33] – beeinflussbar durch Schminke, Bärte, Brillen oder Krankheiten [32, 38]

Iris	Inhärenz	Scan der Iris mittels Infrarotlicht und Umwandlung des aufgenommenen Musters in zweidimensionalen Barcode [28, 30, 31]	Vorteile: – Universell vorhanden (Ausnahme Krankheit) [32] – Einzigartigkeit der Iris 1:6.000.000 [30] – ein Leben lang gleich (Ausnahme Krankheit und Verletzungen) [28, 31] – kontaktlos Nachteile: – Funktion bei blinden Personen beeinträchtigt [32]
Retina	Inhärenz	Beleuchtung des Augenhintergrundes und Aufnahme des Adergeflechts [34]	Vorteile: – Universell vorhanden – Einzigartigkeit der Retina 1:1.000.000 [30] Nachteile: – sehr hohe Kosten [34] – bisher keine kommerzielle Anwendung [34]
Sklera	Inhärenz	Aufnahme hochauflösender Bilddaten des Adermusters [34]	Vorteile: – Universell vorhanden – Einzigartig Nachteile: – Extraktion der Venenmuster nur durch wenige Spezialisten [34]

Sprecher-erkennung	Inhärenz	Aufnahme des charakteristischen Sprachbild durch textabhängige, vokabelabhängige, ziffernbasierte oder textunabhängige Sprachproben [37]	Vorteile: – Universell vorhanden – Einzigartig – Überprüfung des Schalldrucks verhindert die Verwendung von Tonaufnahmen [29] – hohe Flexibilität, Bedienkomfort und Sicherheit [37] Nachteile: – Beeinträchtigung durch Krankheiten [29] – Vollkommenes Versagen bei Stottern [29]

Literaturverzeichnis

[1] H. Frater. „Alles rund um das Thema Sicherheit für das eigene Zuhause“. (), Adresse: https://www.wissen.de/alles-rund-um-das-thema-sicherheit-fuer-das-eigene-zuhause (besucht am 14. 11. 2023).

[2] Securitas. „Zutrittskontrolle: Kontrollierter Zugang zu Ihren Objekten“. (), Adresse: https://www.securitas.de/services/sicherheitstechnik/zutrittskontrolle/ (besucht am 14. 11. 2023).

[3] D.-I. S. Luber und P. Schmitz. „Was ist Zutrittskontrolle?“ (9. Feb. 2022), Adresse: https://www.security-insider.de/was-ist-zutrittskontrolle-a-1094283/ (besucht am 14. 11. 2023).

[4] B. Dimri. „Sicherheit: Die lange Geschichte von Schloss und Schlüssel“. (17. Juni 2021), Adresse: https://www.ancient-origins.de/nachrichten-geschichte-alte-traditionen/schloesser-und-schluessel-007120 (besucht am 11. 11. 2023).

[5] A. S. AG. „Warum Sie auf eine elektronische Zutrittskontrolle umsteigen sollten“. (), Adresse: https://azs.de/zutrittskontrolle-wiki/vorteile-elektronische-zutrittskontrolle/ (besucht am 11. 11. 2023).

[6] S. T. GmbH. „Zutrittskontrolle“. (2023), Adresse: https://www.simons-voss.com/de/lexikon/zutrittskontrolle.html#zutrittskontrolle-digital (besucht am 28. 08. 2023).

[7] dormakaba. „Ein umfassender Leitfaden zur elektronischen Zutrittskontrolle: 19 Vorteile, die für einen Wechsel sprechen“. (17. Dez. 2019), Adresse: https://blog.dormakaba.com/de/ein-umfassender-leitfaden-zur-elektronischen-zutrittskontrolle-19-vorteile-die-fuer-einen-wechsel-sprechen/ (besucht am 11. 11. 2023).

[8] Bundesdatenschutzgesetz. „Anlage (zu § 9 Satz 1)“. (), Adresse: https://datenbank.nwb.de/Dokument/304191 anl1/ (besucht am 14. 11. 2023).

[9] D.-I. S. Luber und P. Schmitz. „Was ist Zugangskontrolle?“ (29. Dez. 2017), Adresse: https://www.security-insider.de/was-ist-zugangskontrolle-a-673084/ (besucht am 14. 08. 2023).

[10] M. Helmus, A. Meins-Becker, L. Laußat und A. Kelm, „Auto-ID-Systeme neben RFID“, in *RFID in der Baulogistik: Forschungsbericht zum Projekt „Integriertes Wertschöpfungsmodell mit RFID in der Bau- und Immobilienwirtschaft“*. Wiesbaden: Vieweg+Teubner, 2009, S. 199, ISBN: 978-3-8348-9319-2. DOI: 10.1007/978-3-8348-9319-2 6. Adresse: https://doi.org/10.1007/978-3-8348-9319-2 6.

[11] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 103, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6 2. Adresse: https://doi.org/10.1007/978-3-642-95683-6 2.

[12] M. Hartung. „Software zur Zutrittskontrolle - Wissenswertes und Vergleich der verschiedenen Anbieter-Lösungen“. (2023), Adresse: https://www.datafox-partner.de/softwareanbieter-uebersicht-vergleich/zutrittskontrolle-software/ (besucht am 23. 08. 2023).

[13] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 191–195, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6 2. Adresse: https://doi.org/10.1007/978-3-642-95683-6 2.

[14] C. Kern, „Einordnung verschiedener Auto-ID-Systeme“, in *Anwendung von RFID-Systemen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 19, ISBN: 978-3-540-44478-7. DOI: 10.1007/978-3-540-44478-7 3. Adresse: https://doi.org/10.1007/978-3-540-44478-7 3.

[15] M. Helmus, A. Meins-Becker, L. Laußat und A. Kelm, „Auto-ID-Systeme neben RFID“, in *RFID in der Baulogistik: Forschungsbericht zum Projekt „Integriertes Wertschöpfungsmodell mit RFID in der Bau- und Immobilienwirtschaft“*. Wiesbaden: Vieweg+Teubner, 2009, S. 210–219, ISBN: 978-3-8348-9319-2. DOI: 10.1007/978-3-8348-9319-2 6. Adresse: https://doi.org/10.1007/978-3-8348-9319-2 6.

[16] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 133–138, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6 2. Adresse: https://doi.org/10.1007/978-3-642-95683-6 2.

[17] J. Langer und M. Roland, „Einführung“, in *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 1–11, ISBN: 978-3-642-05497-6. DOI: 10.1007/978-3-642-05497-6 1. Adresse: https://doi.org/10.1007/978-3-642-05497-6 1.

[18] C. Kern, „Einordnung verschiedener Auto-ID-Systeme“, in *Anwendung von RFID-Systemen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 28–30, ISBN: 978-3-540-44478-7. DOI: 10.1007/978-3-540-44478-7 3. Adresse: https://doi.org/10.1007/978-3-540-44478-7 3.

[19] J. Langer und M. Roland, „Smartcard Technologie“, in *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 33–43, ISBN: 978-3-642-05497-6. DOI: 10.1007/978-3-642-05497-6 3. Adresse: https://doi.org/10.1007/978-3-642-05497-6 3.

[20] C. Kern, „Einordnung verschiedener Auto-ID-Systeme“, in *Anwendung von RFID-Systemen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 33–94, ISBN: 978-3-540-44478-7. DOI: 10.1007/978-3-540-44478-7 3. Adresse: https://doi.org/10.1007/978-3-540-44478-7 3.

[21] C. Kern, „Technik“, in *Anwendung von RFID-Systemen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 37–94, ISBN: 978-3-540-44478-7. DOI: 10.1007/978-3-540-44478-7 4. Adresse: https://doi.org/10.1007/978-3-540-44478-7 4.

[22] C. Kern, „Standardisierung“, in *Anwendung von RFID-Systemen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 169–181, ISBN: 978-3-540-44478-7. DOI: 10.1007/978-3-540-44478-7 6. Adresse: https://doi.org/10.1007/978-3-540-44478-7 6.

[23] T. Weber. „RFID Reichweite“. (2023), Adresse: https://www.rfid-grundlagen.de/reichweite.html (besucht am 07. 09. 2023).

[24] T. Weber. „RFID-Sicherheit und Angriffsmethoden“. (2023), Adresse: https://www.rfid-basis.de/rfid-sicherheit.html (besucht am 19. 10. 2023).

[25] J. Langer und M. Roland, „Technische Grundlagen“, in *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 12–32, ISBN: 978-3-642-05497-6. DOI: 10.1007/978-3-642-05497-6 2. Adresse: https://doi.org/10.1007/978-3-642-05497-6 2.

[26] J. Langer und M. Roland, „Anwendungen der NFC-Technologie“, in *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 205–241, ISBN: 978-3-642-05497-6. DOI: 10.1007/978-3-642-05497-6 9. Adresse: https://doi.org/10.1007/978-3-642-05497-6 9.

[27] J. Langer und M. Roland, „NFC-Technologie“, in *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 87–108, ISBN: 978-3-642-05497-6. DOI: 10.1007/978-3-642-05497-6 5. Adresse: https://doi.org/10.1007/978-3-642-05497-6 5.

[28] C. Kern, „Einordnung verschiedener Auto-ID-Systeme“, in *Anwendung von RFID-Systemen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 20–27, ISBN: 978-3-540-44478-7. DOI: 10.1007/978-3-540-44478-7 3. Adresse: https://doi.org/10.1007/978-3-540-44478-7 3.

[29] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 162–191, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6 2. Adresse: https://doi.org/10.1007/978-3-642-95683-6 2.

[30] M. Helmus, A. Meins-Becker, L. Laußat und A. Kelm, „Auto-ID-Systeme neben RFID“, in *RFID in der Baulogistik: Forschungsbericht zum Projekt „Integriertes Wertschöpfungsmodell mit RFID in der Bau- und Immobilienwirtschaft“*. Wiesbaden: Vieweg+Teubner, 2009, S. 200–205, ISBN: 978-3-8348-9319-2. DOI: 10.1007/978-3-8348-9319-2 6. Adresse: https://doi.org/10.1007/978-3-8348-9319-2 6.

[31] D. Labudde, „Biometrie und die Analyse digitalisierter Spuren“, in *Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt*, D. Labudde und M. Spranger, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, S. 25–58, ISBN: 978-3-662-53801-2. DOI: 10.1007/978-3-662-53801-2 2. Adresse: https://doi.org/10.1007/978-3-662-53801-2 2.

[32] T. Bengs und W. Grudzien, „Biometrie in der Kreditwirtschaft - Warum Biometrie nicht allein Tresore sichern sollte“, *Datenschutz und Datensicherheit - DuD*, 2007.

[33] U. Weigmann, K. Deimer, C. Leininger, L. Turba und S. Jurran, „Biometrie am BBI — Chancen und Randbedingungen“, *Datenschutz und Datensicherheit - DuD*, 2011.

[34] A. Uhl, „Venen Biometrie - Stand der Technik“, *Datenschutz und Datensicherheit - DuD*, 2020.

[35] I. S. America. „Palm vein recognition“. (), Adresse: https://identytech.com/palm-vein-recognition/ (besucht am 25. 09. 2023).

[36] RECOGTECH. „Wie funktioniert Venenmustererkennung?“ (), Adresse: https://www.recogtech.com/de/wissenbasis/venenmustererkennungwa (besucht am 26. 09. 2023).

[37] M. Dose und H. Reininger, „Biometrie“, in *Sicherheit und Rechtsverbindlichkeit mobiler Agenten*, R. Gitter, V. Lotz, U. Pinsdorf und A. Roßnagel, Hrsg. Wiesbaden: Vieweg+Teubner, 2007, S. 119–127, ISBN: 978-3-8350-9120-7. DOI: 10.1007/978-3-8350-9120-7_9. Adresse: https://doi.org/10.1007/978-3-8350-9120-7_9.

[38] N. N.V. „Welche biometrische Zutrittskontrolle ist am besten für Sie geeignet?“ (), Adresse: https://www.nedapsecurity.com/de/insight/welche-biometrische-zutrittskontroll-loesung-ist-am-besten-fuer-sie-geeignet/ (besucht am 21. 10. 2023).

[39] the Hospital for Sick Children. „Eye anatomy and function“. (20. Sep. 2019), Adresse: https://www.aboutkidshealth.ca/article?contentid=1941&language=English# (besucht am 27. 09. 2023).

[40] P. D. med. Christian Offergeld. „Physiologische Funktionen“. (), Adresse: http://hno-lernprogramm.uniklinik-freiburg.de/3D-Vorlesung/47/ (besucht am 02. 10. 2023).

[41] S. Dörn, „Markov-Modelle“, in *Programmieren für Ingenieure und Naturwissenschaftler: Intelligente Algorithmen und digitale Technologien*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, S. 219–290, ISBN: 978-3-662-54304-7. DOI: 10.1007/978-3-662-54304-7_6. Adresse: https://doi.org/10.1007/978-3-662-54304-7_6.

[42] L. Shenzhen Wenxinran Intelligent Technology Co. „Ist es möglich, RFID-Karten zu klonen? Ein umfassender RFID-Sicherheitsleitfaden“. (27. März 2021), Adresse: https://www.rfidfuture.com/de/clone-rfid-cards.html#Why-RFID-Cards-Are-Cloned-So-Easily (besucht am 19. 10. 2023).

[43] M. Drahanský, O. Kanich, R. Pernický und Š. Barotová, „Verarbeitung von beschädigten Fingerabdrücken in der polizeilichen Praxis“, *Datenschutz und Datensicherheit - DuD*, 2017.

[44] B. für Sicherheit in der Informationstechnik. „Biometrie in elektronischen Ausweisdokumenten - Erfassung der Fingerabdrücke“. (), Adresse: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Elektronische-Ausweisdokumente/Biometrie/Fingerabdruecke/fingerabdruecke.html (besucht am 25. 10. 2023).

[45] C. Kalla und P. Schuch, „Sicherheit in der Fingerabdruck-Identifikation“, *Datenschutz und Datensicherheit - DuD*, 2013.

[46] M. Drahanský, R. Dvořák und J. Váňa, „Personenerkennung mittels 3D Handgeometrie“, *Datenschutz und Datensicherheit - DuD*, 2011.

[47] N. Krebs. „PalmSecureTM - Ihre Hand ist Ihre Lösung“. (10. Apr. 2019), Adresse: https://stahlgmbh.de/images/Meldungen/2019-04-10_BusinessBreakfast_sicherer_IT_Arbeitsplatz/slides_palmsecure.pdf (besucht am 25. 10. 2023).

[48] P. Beuth. „Hacker tricksen Venenscanner mit Wachs aus“. (27. Dez. 2018), Adresse: https://www.spiegel.de/netzwelt/gadgets/biometrie-hack-venen-scanner-fallen-auf-wachshaende-herein-a-1243583.html (besucht am 25. 10. 2023).

[49] B. für Sicherheit in der Informationstechnik. „Deepfakes - Gefahren und Gegenmaßnahmen“. (), Adresse: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html#doc1009562bodyText6 (besucht am 30. 10. 2023).

[50] E. Rudolf-Müller. „Haut“. (21. Feb. 2022), Adresse: https://www.netdoktor.de/anatomie/haut/ (besucht am 01. 11. 2023).

[51] BDVA. „Latente Fingerspuren“. (), Adresse: https://www.bvda.com/de/latente-fingerspuren# (besucht am 01. 11. 2023).

[52] Electricity-Magnetism. „Wie funktioniert eine magnetische Karte?“ (), Adresse: https://www.electricity-magnetism.org/de/wie-funktioniert-eine-magnetische-karte/ (besucht am 01. 11. 2023).

[53] M. Nerad. „Kreditkarte & EC-Karte richtig putzen & desinfizieren: Das ist wichtig!“ (), Adresse: https://www.kreditkartenportal.de/magazin/kreditkarte-ec-karte-richtig-putzen-desinfizieren-das-ist-wichtig.html (besucht am 01. 11. 2023).

[54] Electricity-Magnetism. „Wie funktionieren Magnetstreifenkarten?“ (), Adresse: https://www.electricity-magnetism.org/de/wie-funktionieren-magnetstreifenkarten/ (besucht am 01. 11. 2023).

[55] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 143–148, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6_2. Adresse: https://doi.org/10.1007/978-3-642-95683-6_2.

[56] S. S. GmbH. „RFID-Karten“. (), Adresse: https://www.allaboutcards.de/de/plastikkarten/rfid-medien/rfid-karten (besucht am 01. 11. 2023).

[57] V. P. und Handels GmbH. „Chipkarten Aufbau“. (), Adresse: https://www.variuscard.com/plastikkarten/chipkarten/chipkarten-aufbau/ (besucht am 03. 11. 2023).

[58] DRACOON. „Multi-Faktor-Authentifizierung: So schützen Sie Ihre digitale Identität mit MFA“. (21. Sep. 2023), Adresse: https://blog.dracoon.com/de/multi-faktor-authentifizierung-mfa (besucht am 05. 11. 2023).

[59] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 109, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6_2. Adresse: https://doi.org/10.1007/978-3-642-95683-6_2.

[60] G. Walz und D. Kruse, „Zutrittskontrolle“, in *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*, G. Walz, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992, S. 204–206, ISBN: 978-3-642-95683-6. DOI: 10.1007/978-3-642-95683-6_2. Adresse: https://doi.org/10.1007/978-3-642-95683-6_2.

[61] E. Security. „Burg Wächter secuENTRY Home 7711 Keypad PIN“. (), Adresse: https://www.expert-security.de/burg-waechter-secuentry-home-7711-keypad-pin.html# (besucht am 09. 11. 2023).

[62] E. Security. „ABUS HomeTec Pro CFT3100 S Bluetooth-Tastatur“. (), Adresse: https://www.expert-security.de/abus-hometec-pro-cft3100-s-bluetooth-tastatur.html (besucht am 09. 11. 2023).

[63] E. Security. „ABUS TVHS30000 FaceXess Video-Türstation“. (), Adresse: https://www.expert-security.de/abus-tvhs30000-facexess-video-tuerstation.html?refid=googleshopping&msclkid=9bea5c841ec616f3193d39cfabcd2fa7&utm_source=bing&utm_medium=cpc&utm_campaign=(DE%3AWhoop!)%20MarkenRSL&utm_term=4581046492599510&utm_content=(DE%3AWhoop!)%20Abus (besucht am 09. 11. 2023).

[64] ABUS. „FaceXess Video-Türstation“. (), Adresse: https://mobil.abus.com/de/Privat/Tuersicherheit/Tuersprechsysteme/Kabelgebundene-Tuersprechsysteme/FaceXess-Video-Tuerstation (besucht am 09. 11. 2023).

[65] E. Security. „ABUS HomeTec Pro CFS3100 S Bluetooth-Fingerscanner“. (), Adresse: https://www.expert-security.de/abus-hometec-pro-cfs3100-s-bluetooth-fingerscanner.html (besucht am 09. 11. 2023).

[66] W. A. GmbH. „EC-KOMPAKT“. (), Adresse: https://cardcontrol.de/schranken-und-zubehoer/zufahrtssysteme-zutrittssysteme/magnet-chip/#ec-kompakt (besucht am 09. 11. 2023).

[67] E. Security. „Burg Wächter secuENTRY pro 5711 PIN“. (), Adresse: https://www.expert-security.de/burg-waechter-secuentry-pro-5711-pin.html# (besucht am 09. 11. 2023).

[68] mess-elektronik-groß GmbH. „Net2 Vandalen-resistente Metalltastatur“. (), Adresse: https://www.megzeit.de/shop/metalltastatur-vandalen-resistente-pin-code-tastatur-fuer-zutrittskontrolle/ (besucht am 09. 11. 2023).

[69] mess-elektronik-groß GmbH. „Net2 Zutrittskontrolle - Leistungsmerkmale“. (), Adresse: https://www.megzeit.de/wp-content/uploads/2020/09/Net2_Leistungsmerkmale.pdf.

[70] P. Access. „Vandalen-resistente Metalltastatur“. (), Adresse: https://www.paxton-access.com/de/vandalen-resistente-metalltastatur/ (besucht am 09. 11. 2023).

[71] E. Security. „SimonsVoss PinCode-Tastatur 3068“. (), Adresse: https://www.expert-security.de/simonsvoss-pincode-tastatur-3068.html (besucht am 09. 11. 2023).

[72] ModiTech. „SimonsVoss - PinCode-Tastatur 3068 - TRA.PINCODE“. (), Adresse: https://shop.moditech.de/digitale-Schliessanlagen/SimonsVoss-PinCode-Tastatur-3068 (besucht am 09. 11. 2023).

[73] Sicher24. „Simons Voss - PIN-Code Tastatur 3068“. (), Adresse: https://www.sicher24.de/digitale-schliesszylinder/simons-voss-pin-code-tastatur-3068-mit-4-bis-8-stelligem-code-n.html (besucht am 09. 11. 2023).

[74] I-Keys. „mReader, der massive Vollmetall Multi Reader“. (), Adresse: https://www.i-keys.de/de/zutrittskontrollsysteme/wandleser-fuer-controller/em4102-uni/mreader-der-massive-vollmetall-multi-reader.html (besucht am 09. 11. 2023).

[75] AXIS. „AXIS A4020-E Reader“. (), Adresse: https://www.axis.com/de-at/products/axis-a4020-e (besucht am 09. 11. 2023).

[76] E. Security. „AXIS A4020-E RFID Leseeinheit ohne Tastatur IP65“. (), Adresse: https://www.expert-security.de/axis-a4020-e-rfid-leseeinheit-ohne-tastatur-ip65.html (besucht am 09. 11. 2023).

[77] W. Sicherheit. „Clex Private Elektronischer Halbzylinder CX2126“. (), Adresse: https://www.wagner-sicherheit.de/sicherheitstechnik/clex-private-elektronischer-halbzylinder-cx2126.html (besucht am 09. 11. 2023).

[78] HikVision. „DS-K1T341AM-S“. (), Adresse: https://www.hikvision.com/de/products/Access-Control-Products/Face-Recognition-Terminals/Value-Series/ds-k1t341am-s/ (besucht am 09. 11. 2023).

[79] G. Protect. „HIKVISION DS-K1T341AM-S Gesichtserkennungsterminal“. (), Adresse: https://www.germanprotect.com/hikvision-ds-k1t341am-s-gesichtserkennungsterminal.html (besucht am 09. 11. 2023).

[80] ZutrittsShop. „Suprema BioStation 3 Zutrittskontrolle + VOIP Sprechanlage (Gesichtserkennung, RFID, QR-Code)“. (), Adresse: https://www.zutrittsshop.de/de/codeschloesser/suprema-biostation-3-zutrittskontrolle-voip-sprechanlage.html?gad=1&gclid=CjwKCAiA3aeqBhBzEiwAxFiOBvyc QNBsoNhuYhlftZZ0oaibjDt6ziEY WbFzSnUrJVHRWrRRPi2HhoCVMMQAvD BwE&gclsrc=aw.ds (besucht am 09. 11. 2023).

[81] esay secure. „BioStation 3“. (), Adresse: https://www.easysecure.com/de/hardware/suprema-biostation-3 (besucht am 09. 11. 2023).

[82] D. Biometrieladen. „Vision Pass“. (), Adresse: https://www.biometrieladen.de/visionpass/ (besucht am 09. 11. 2023).

[83] Idemia. „VisionPass“. (), Adresse: https://www.idemia.com/wp-content/uploads/2021/02/visionpass-idemia-brochure-202111.pdf (besucht am 09. 11. 2023).

[84] G. Protect. „Idemia VisionPass MDPI Gesichtserkennungsterminal“. (), Adresse: https://www.germanprotect.com/idemia-visionpass-mdpi-gesichtserkennungsterminal.html (besucht am 09. 11. 2023).

[85] Bosch. „Gesichtsleser, MDPI“. (), Adresse: https://commerce.boschsecurity.com/de/de/Facial-recognition-reader-MDPI/p/F.01U.391.137/ (besucht am 09. 11. 2023).

[86] Sommer. „Fingerscanner ENTRAsys+ UP Fingerprint-Scanner“. (), Adresse: https://shop.sommer.eu/de/fingerscanner-entrasys-up-fingerprint-scanner-s11186-00001 (besucht am 09. 11. 2023).

[87] G. Protect. „Idemia MorphoWave XP MD Berührungsloser Fingerabdruck Scanner, Katenleser, Mifare“. (), Adresse: https://www.germanprotect.com/idemia-morphowave-xp-md-beruhrungsloser-fingerabdruck-scanner-katenleser-mifare.html (besucht am 09. 11. 2023).

[88] A. Electronic. „Schutzmaßnahmen in der Zutrittskontrolle“. (), Adresse: https://www.ata.de/sicherheitstechnik/zutrittskontrollanlagen/schutzmassnahmen.html (besucht am 10. 11. 2023).

[89] Bosch. „Berührungsl. 3D-Fingerabdr.leser, MDPI“. (), Adresse: https://commerce.boschsecurity.com/de/de/Contactless-3D-fingerprint-reader-MDPI/p/F.01U.391.138/ (besucht am 09. 11. 2023).

[90] Idemia. „Contactless fingerprint“. (), Adresse: https://www.idemia.com/contactless-fingerprint (besucht am 09. 11. 2023).

[91] G. Sicherheit. „Idemia-Lösungen für Zutrittskontrolle und Zeiterfassung“. (), Adresse: https://www.git-sicherheit.de/news/idemia-loesungen-fuer-zutrittskontrolle-und-zeiterfassung (besucht am 09. 11. 2023).

[92] Honeywell. „2D-Iriserkennung“. (), Adresse: https://buildings.honeywell.com/de/de/products/by-category/access-control/readers-and-keypads/biometric-readers/iris-recognition-2d#overview (besucht am 09. 11. 2023).

[93] T. Biometrics. „Iris Erkennung 2D Eye“. (), Adresse: https://tbs-biometrics.asia/de/2d-eye/ (besucht am 09. 11. 2023).

[94] Honeywell. „TBS Finger Scanner, 2D EYE Iris Scanner“. (), Adresse: https://buildings.honeywell.com/gb/en/products/by-category/access-control/readers-and-keypads/biometric-readers/tbs-finger-scanner-2d-eye-iris-scanner (besucht am 10. 11. 2023).

[95] Interflex. „Handvenenleser INTUS 1600PS“. (), Adresse: https://interflex.com/de-de/produkt/hardware/terminals-zutrittskontrolle/biometrische-terminals/handvenenleser-pcs-intus-1600ps/ (besucht am 10. 11. 2023).

[96] EPS. „Handvenenscanner als Zutrittssystem für IT und Serverraum“. (), Adresse: https://www.eps-dc.com/de/produkt/handvenenerkennung-als-zutrittssystem-fur-it/ (besucht am 09. 11. 2023).

[97] iCognize. „ScanVein Rugged“. (), Adresse: https://icognize.de/scanvein-rugged/ (besucht am 09. 11. 2023).

[98] iCognize. „ScanVein Compact“. (), Adresse: https://icognize.de/scanvein-compact/ (besucht am 09. 11. 2023).

Eidesstattliche Erklärung

Hiermit versichere ich – Janka Patzschke – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 15. November 2023 — Janka Patzschke

Ort, Datum