www.din.de/go/verbraucherrat

DIN Verbraucherrat

Studie

Biometrische Erkennungssysteme – Nutzen und Hemmnisse im Verbraucheralltag

Impressum

Herausgeber:

DIN-Verbraucherrat
DIN e.V.

Saatwinkler Damm 42/43
13627 Berlin

E-Mail: verbraucherrat@din.de
Web: http://www.din.de/go/verbraucherrat

Gefördert durch:

Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Autor:

Dr. Olaf Henniger

Abteilung Smart Living & Biometric Technologies
Fraunhofer-Institut für Graphische Datenverarbeitung IGD
Fraunhoferstraße 5
64283 Darmstadt

Berlin, Dezember 2020

FORSCHUNGSBERICHT

Biometrische Erkennungssysteme – Nutzen und Hemmnisse im Verbraucheralltag

Dr. Olaf Henniger

Abteilung Smart Living & Biometric Technologies
Fraunhofer-Institut für Graphische Datenverarbeitung IGD
Fraunhoferstraße 5
64283 Darmstadt

Versionsnummer	1.1
Status	Final
Erstellungsdatum	8. Januar 2021
Auftraggeber	DIN e.V. DIN-Verbraucherrat Saatwinkler Damm 42/43 13627 Berlin

Kurzfassung

Biometrische Systeme dienen der automatisierten Erkennung natürlicher Personen anhand ihres Verhaltens und ihrer biologischen Charakteristika. Ausgehend von einer strukturierten Übersicht von aktuell von Verbrauchern genutzten und mit großer Wahrscheinlichkeit in den nächsten fünf Jahren zur Nutzung angebotenen biometrischen Erkennungssystemen wurde eine Online-Befragung zur Ermittlung der Verbrauchersicht auf biometrische Erkennungssysteme durchgeführt. Die Befragungsergebnisse sind bezogen auf alle Verbraucher in Deutschland nicht repräsentativ, decken jedoch einen Großteil der biometrischen Erkennungssysteme ab, die in Deutschland im Einsatz sind. Personen mit hoher Affinität zur Technikinteraktion sind überrepräsentiert.

67 % der Befragten benutzen biometrische Erkennungssysteme. Das Entsperren von mobilen Endgeräten ist die »Killer-Applikation«, die der Biometrie, insbesondere der Fingerabdruck- und der Gesichtserkennung, im Verbraucheralltag zum Durchbruch verhilft. Der Anteil der Befragten, die über ein Endgerät mit integrierten biometrischen Erkennungssystemen verfügen, liegt bei 80 %, wovon 71 % auch ein biometrisches Verfahren gewohnheitsmäßig zum Entsperren des Geräts nutzen (53 % Fingerabdruckerkennung, 17 % Gesichtserkennung und 1 % Iriserkennung). Die am weitesten verbreiteten biometrischen Anwendungen nutzen die biometrischen Sensoren in mobilen Endgeräten (Entsperren von Endgeräten, Freischalten von Endgeräten zur kryptographischen Authentisierung im Internet, Online-Banking, mobiles Bezahlen). »Nischenanwendungen« sind Sprechererkennung zur Anruferauthentisierung und zur Zugangskontrolle zu digitalen Sprachassistenten und Venenmustererkennung zur Zugangskontrolle zu Räumen und Gebäuden. Andere verwendbare biometrische Charakteristika, wie handschriftliche Unterschriften, sind noch nicht im Verbraucheralltag angekommen. Zur Bargeldabhebung an Geldautomaten und zur Arbeitszeiterfassung setzen die Befragten biometrische Verfahren gar nicht ein.

Eine Mehrheit der Befragten sieht biometrische Erkennungssysteme als benutzerfreundlich und sicher an, kennt aber auch die Risiken biometrischer Erkennungssysteme. In der Altersgruppe über 60 Jahre ist die tatsächliche Nutzung, aber auch die Bereitschaft zur zukünftigen Nutzung biometrischer Erkennungssysteme weniger verbreitet als im Durchschnitt aller Befragten. Das kann an höheren Sicherheitsanforderungen in dieser Altersgruppe liegen. Unter Berücksichtigung der Leitwerte des DIN-Verbraucherrats wurden aus den Befragungsergebnissen Handlungsempfehlungen für die Verbraucherkommunikation abgeleitet: Alle potenziellen Benutzer sollten über Benutzerfreundlichkeit und Sicherheit biometrischer Erkennungssysteme informiert werden, um Informations- und Erfahrungsdefizite abzubauen. Verbraucher in der Altersgruppe über 60 Jahre sollten besonders auf den Nutzen biometrischer Erkennungssysteme und die vorhandenen

Sicherheitsmaßnahmen hingewiesen werden, wohingegen Verbraucher in der Altersgruppe bis 30 Jahre besonders über Risiken biometrischer Erkennungssysteme unterrichtet werden sollten.

Des Weiteren wurden Empfehlungen zum Verbraucherschutz bei der freiwilligen Nutzung biometrischer Erkennungssysteme abgeleitet, Defizite in der Normung biometrischer Technologien hinsichtlich der Erwartungen des Verbraucherschutzes identifiziert und Handlungsempfehlungen zur Überwindung dieser Defizite abgeleitet: Es wird empfohlen, für die Normung geeignete Biometric-Template-Protection-Verfahren auszuwählen und zu normen. Bei der Normung biometrischer Algorithmen, die auf maschinellem Lernen beruhen, wird empfohlen, möglichst erklärbare Verfahren auszuwählen, um Leistungsunterschiede zwischen demographischen Gruppen vermeiden zu können.

Abstract

Biometric systems are used for the automated recognition of natural persons based on their biological and behavioural characteristics. Based on a structured overview of biometric recognition systems currently used by consumers and most likely to be offered for use in the next five years, an online survey was conducted to determine the consumers' view of biometric recognition systems. The results of the survey are not representative of all consumers in Germany, but cover a large part of the biometric recognition systems in use in Germany. People with a high affinity for technology interaction are overrepresented.

67% of the respondents use biometric recognition systems. The unlocking of mobile devices is the »killer application« that helps biometrics, in particular fingerprint and face recognition, to achieve a breakthrough in everyday life of consumers. The percentage of respondents who hold a device with integrated biometric recognition systems is 80%, 71% of whom also use a biometric method to unlock the device (53% fingerprint recognition, 17% face recognition, and 1% iris recognition). The most widespread biometric applications (unlocking a device, authorizing a device for cryptographic authentication on the Internet, online banking, and mobile payment) use the biometric sensors integrated into mobile devices. »Niche applications« are speaker recognition for caller authentication and for access control to digital speech assistants and vein pattern recognition for access control to rooms and buildings. Other usable biometric characteristics, such as handwritten signatures, have not yet arrived in everyday consumer life. The respondents do not use biometric methods at all for cash withdrawals at cash machines and for recording time and attendance.

A majority of respondents consider biometric recognition systems as user-friendly and secure, but are also aware of the risks of biometric recognition systems. The actual use of biometric recognition systems, but also the willingness to use them in the future, is less widespread in the age group over 60 years than in the average of all respondents. This may be due to higher security requirements in that age group. Taking into account the guiding values of the Consumer Council, recommendations for consumer communication actions were derived from the survey results: All potential users should be informed about usability and security of biometric recognition systems in order to reduce information and experience deficits. Consumers in the age group over 60 years should be informed especially about the benefits of bio-metric recognition systems and available security measures, whereas consumers in the age group up to 30 years should be informed especially about the risks of biometric recognition systems.

Furthermore, recommendations for consumer protection in voluntary biometric applications were derived, deficits in the standardization of biometric technologies with regard to the expectations of consumer protection were identified, and recommendations for action to overcome these deficits were derived: It is recommended to select and standardize suitable biometric template protection methods. When standardizing biometric algorithms based on machine learning, it is recommended to select methods that are as explainable as possible in order to be able to avoid performance variations across demographic groups.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

FIDO	Fast Identity Online
FNIR	Falschnegatividentifizierungsrate
FPIR	Falschpositividentifizierungsrate
ICAO	International Civil Aviation Organization
iTAN	Indexed Transaction Authentication Number
LED	Light-Emitting Diode
MRTD	Machine-Readable Travel Document
NFC	Near-Field Communication
PC	Personal Computer
PIN	Personal Identification Number
PP	Protection Profile
PSD	Payment Services Directive
RTP	Registered Traveller Programme
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
USB	Universal Serial Bus
VIS	Visa Information System

1 Einführung

1.1 Hintergrund

Biometrische Systeme dienen der automatisierten Erkennung natürlicher Personen anhand ihres Verhaltens und ihrer biologischen Charakteristika [1]. Verwendbare Charakteristika sind z.B. die Gesichtsgeometrie, Fingerlinienmuster, Irismuster, Venenmuster in Hand oder Finger, die Stimme oder handschriftliche Unterschriften.

Biometrische Verfahren wurden zunächst vorrangig in hoheitlichen Anwendungen genutzt, halten jedoch zunehmend Einzug in kommerzielle Alltagsanwendungen (z.B. Smartphone- bzw. PC-Login, Zugangskontrolle zu privaten oder betrieblichen Räumen oder Gebäuden, Authentisierung im Zahlungsverkehr). Biometrische Verfahren werden dabei entweder als ein Faktor einer Zweifaktorauthentisierung oder als einziger Authentisierungsfaktor genutzt.

Bei richtiger Auswahl und Gestaltung der Verfahren kann Biometrie eine hohe Sicherheit der jeweiligen Anwendung und im Vergleich zu besitz- oder wissensbasierten Authentisierungsverfahren mehr Bequemlichkeit für die Benutzer bieten. Auf Grund der langfristigen Personengebundenheit biometrischer Daten birgt der Einsatz biometrischer Verfahren neben Chancen auch Risiken. Nach der Europäischen Datenschutzgrundverordnung [2] handelt es sich bei biometrischen Daten um besonders schützenswerte personenbezogene Daten. Ihre Verarbeitung ist im Wesentlichen nur mit ausdrücklicher Einwilligung der betroffenen Person oder auf gesetzlich geregelter Grundlage erlaubt.

Wenn sich Verbraucher (d.h. natürliche Personen, die Waren oder Dienstleistungen zur privaten Bedürfnisbefriedigung nutzen) frei für oder gegen die Nutzung der Biometrie entscheiden können, hängt die Entscheidung von der Akzeptanz biometrischer Erkennungssysteme ab. Verbraucher-akzeptanz ist gesellschaftlich geprägt und Schwankungen unterworfen. Aktuelle Studien vermitteln sehr unterschiedliche Bilder zur Verbraucherakzeptanz biometrischer Erkennungssysteme [3], [4], [5].

1.2 Ziele der Studie

Diese Studie hat zum Ziel, die aktuelle Verbrauchersicht auf biometrische Erkennungssysteme zu ermitteln und allgemeine bzw. für Deutschland spezifische Faktoren, die diese Sichtweise be-einflussen, herauszufinden. Daraus werden Handlungsempfehlungen für die Verbraucher-kommunikation und für die Normung abgeleitet.

Es wurde bewusst der Ansatz gewählt, die subjektive Sicht der Verbraucher abzufragen, statt den Handlungsempfehlungen eine Technikanalyse zugrunde zu legen. Eine verbrauchergerechte und sichere Gestaltung der Technik ist unverzichtbar, die Verbraucher müssen jedoch auch ausreichend informiert sein und die Technologie akzeptieren.

1.3 Organisation der Studie

Der Rest dieses Dokuments ist wie folgt gegliedert: Kapitel 2 gibt eine strukturierte Übersicht über biometrische Erkennungssysteme, die aktuell von Verbrauchern genutzt werden oder mit großer Wahrscheinlichkeit in den nächsten fünf Jahren Verbrauchern zur Nutzung angeboten werden. Kapitel 3 stellt die Ergebnisse einer Online-Befragung zur Ermittlung der Verbrauchersicht auf solche biometrische Systeme vor. Kapitel 4 gibt eine Übersicht über bestehende Normen und Standards mit Bezug zur Biometrie. Kapitel 5 gibt Handlungsempfehlungen für die Verbraucherkommunikation und für die weitere Normung biometrischer Technologien, um die Erwartungen des Verbraucherschutzes zu erfüllen.

2 Übersicht über biometrische Erkennungssysteme

2.1 Einführung

Vor einiger Zeit hatte der BITKOM e.V. eine Übersicht über Biometrie-Referenzbeispiele zusammengestellt [6], die jedoch einer Aktualisierung bedarf. Mittlerweile ist eine Vielzahl biometrischer Erkennungssysteme im praktischen Einsatz, die sich an verschiedene Kundengruppen richten.

Die biometrischen Erkennungssysteme können auf verschiedene Weise klassifiziert werden:

- in biometrische Verifikations- und Identifikationssysteme:
  - Unter biometrischer Verifikation versteht man den Vergleich einer biometrischen Probe mit einer biometrischen Referenz, um die Behauptung zu prüfen, dass sie von der gleichen Person stammen. Zur Eingabe der behaupteten Identität werden z.B. Benutzernamen, Identifikationsnummern, personengebundene Chipkarten oder Sicherheitstoken eingesetzt.
  - Unter biometrischer Identifikation versteht man den Vergleich der biometrischen Merkmale einer natürlichen Person mit *n* biometrischen Referenzen, um gegebenenfalls herauszufinden, welche der *n* registrierten Referenzen von dieser Person stammt.
- in biometrische Erkennungssysteme mit kooperativen und unkooperativen Datensubjekten:
  - Kooperative Datensubjekte verwenden das biometrische Erkennungssystem bewusst mit dem Ziel, vom System erkannt zu werden.
  - Die biometrischen Charakteristika unkooperativer Datensubjekte können von biometrischen Erkennungssystemen in einer Weise erfasst werden, bei der die betroffene Person nicht kooperieren muss. Typische Einsatzszenarien sind Fahndungen oder die Identifikation in Referenzdatenbanken.
- nach ihrem Einsatzzweck (siehe Abschnitt 2.2) oder
- nach der Systemarchitektur (siehe Abschnitt 2.3).

Dieses Dokument konzentriert sich auf freiwillige Anwendungen mit kooperativen Datensubjekten. Die Informationen über Anbieter und Produkte basieren auf veröffentlichten Angaben und beanspruchen keine Vollständigkeit. Zu beachten ist, dass Produktinformationen auf Grund stetiger technischer Weiterentwicklung relativ schnell veralten.

2.2 Klassifizierung nach Einsatzzweck

2.2.1 Überblick

Nach dem Zweck ihres Einsatzes können biometrische Erkennungssysteme wie folgt eingeteilt werden:

- hoheitliche Anwendungen (siehe Abschnitt 2.2.2),
- Zugangskontrolle zu gesicherten Bereichen und IT-Systemen (siehe Abschnitt 2.2.3),
- Finanzanwendungen (siehe Abschnitt 2.2.4),
- Arbeitszeiterfassung (siehe Abschnitt 2.2.5),
- Komfortanwendungen (siehe Abschnitt 2.2.6),
- Gesichtersuchmaschinen (siehe Abschnitt 2.2.7).

2.2.2 Einsatz in hoheitlichen Anwendungen

2.2.2.1 Automatisierte Grenzkontrolle

Seit 2005 stellen Staaten elektronische Reisepässe aus, die einen Smartcard-Chip enthalten, auf dem biometrische Daten sicher gespeichert sind. Die gespeicherten biometrischen Daten sind ein Gesichtsbild und in einigen Staaten (u.a. den EU-Staaten) zwei Fingerbilder des Halters. Die EU-Verordnung 2252/2004 [7] legt fest, welche Sicherheitsmerkmale in europäischen Reisepässen enthalten sein müssen. Sie basiert auf den standardisierten Bausteinen der Internationalen Zivil-luftfahrt-Organisation (ICAO) [8], die das Mandat hat, Spezifikationen für maschinenlesbare Reise-dokumente (MRTD) zu entwickeln.

Immer mehr Staaten nutzen die elektronischen Reisepässe zur automatisierten Grenzkontrolle. Dabei werden die in Ausweispapieren gespeicherten biometrischen Daten mit aktuell aufge-nommenen biometrischen Daten des Reisenden verglichen, um festzustellen, ob dieser der recht-mäßige Ausweisinhaber ist.

An manchen Grenzkontrollpunkten haben Vielreisende aus Drittstaaten die Möglichkeit, sich freiwillig vorab biometrisch registrieren und überprüfen zu lassen, um Wartezeiten zu verkürzen und die Grenze schneller überqueren zu können (Registered Traveller Programme, RTP).

In der Europäischen Union wird ein Entry-Exit-System für die elektronische Erfassung des Zeitpunkts und Orts der Ein- und Ausreise von Drittstaatsangehörigen mit und ohne Visum eingeführt, um u.a. die Einhaltung der zulässigen Aufenthaltsdauer zu überwachen. Neben Daten zum verwendeten

Reisedokument werden dabei auch Fingerabdrücke und Gesichtsbilder der Reisenden gespeichert und verglichen.

2.2.2.2 Identifikation von Personen

Die in Polizeidatenbanken gespeicherten biometrischen Daten von Personen, die von polizeilichen Ermittlungen betroffen waren oder sind, stehen Polizeidienststellen zur Recherche anhand von Finger- oder DNA-Spuren, Täterfotos oder Videosequenzen zur Verfügung.

Vielen Menschen in armen Ländern fehlen Ausweisdokumente. Dies schränkt ihre Möglichkeiten für wirtschaftliche, soziale und politische Teilhabe erheblich ein. Um diese Lücke zu schließen, sind biometrische Datenbanken und Erkennungssysteme eine mögliche Lösung [9], [10]. Angesichts der Verfügbarkeit von Passfotos hoher Qualität in den elektronischen Reisepässen können auch hoch entwickelte Staaten versucht sein, Bürgerdatenbanken aufzubauen, die neben alphanumerischen biographischen Daten auch biometrische Daten enthalten. Als Begründung können die Verhinderung von Identitätsdiebstahl durch Suche nach Duplikaten oder die Verbesserung der Strafverfolgungsfunktionen dienen. In Europa rufen solche Pläne jedoch Bedenken hinsichtlich des Datenschutzes hervor, da die möglichen Vorteile den Eingriff in die Privatsphäre der Menschen nicht überwiegen [11].

Es gibt Überlegungen, an sicherheitsrelevanten Orten zusätzlich zu Überwachungskameras, die alle Passanten erfassen, Software zur Gesichtserkennung einzusetzen, um zur Suche ausgeschriebene Personen erkennen zu können [12]. Dem stehen Bedenken hinsichtlich des Datenschutzes der unbeteiligten Passanten entgegen [13]. Am Bahnhof Berlin Südkreuz lief ein Feldversuch mit automatischer Gesichtserkennung, der die Unzulänglichkeiten solcher Systeme im Falle unkooperativer Datensubjekte in unkontrollierter Umgebung gezeigt hat: Bei Recherche gegen eine Fahndungsliste von ca. 200 Personen erreichten die besten Gesichtsidentifikationssysteme bei guten Lichtverhältnissen eine Falschnegatividentifikationsrate (FNIR) von ca. 20 % bei einer Falschpositividentifikationsrate (FPIR) von ca. 0,1 %, also einem falschen Alarm pro Kamera und Stunde bei einem angenommenen Personenaufkommen von 1000 Personen pro Stunde [14]. Je länger die Fahndungsliste, desto höher wird die FPIR.

2.2.2.3 Suche nach Duplikaten

Das europäische Visa-Informationssystem (VIS) ist ein System zum Austausch von Daten über Kurzzeit-Visa zwischen den Staaten des Schengener Abkommens. Von Personen, die ein Visum beantragen, werden zehn Fingerabdrücke und ein digitales Foto zusammen mit den im

Visumantragsformular angegebenen alphanumerischen Daten in einer sicheren zentralen Datenbank gespeichert. Die gespeicherten Fingerabdrücke werden miteinander verglichen, um Dopplungen bei Visa-Antragstellern zu entdecken. An den Außengrenzen des Schengen-Raums werden die Fingerabdrücke des Visuminhabers mit denen in der Datenbank verglichen, um festzustellen, ob dieser der rechtmäßige Inhaber ist.

Die EU-Datenbank mit Fingerabdrücken von Asylbewerbern EURODAC (European Dactyloscopy) soll verhindern, dass Personen in mehreren EU-Mitgliedstaaten Asyl beantragen können. Die in der EURODAC-Datenbank gespeicherten Fingerabdrücke werden miteinander verglichen, um Dopplungen zu entdecken.

2.2.3 Zugangskontrolle

2.2.3.1 Zugangskontrolle zu mobilen Endgeräten

Seit Einführung eines in die Home-Taste integrierten Fingerabdrucksensors im iPhone 5s (Apple Touch ID) im Jahr 2013 kommen mehr und mehr Smartphones mit Fingerabdruckerkennung, 2D- oder 3D-Gesichtserkennung oder auch Iriserkennung auf den Markt [15]. Es gibt zahlreiche Technologie- und Endgeräteanbieter. Gebräuchliche Smartphones können verschiedene biometrische Zugangskontrollsysteme bieten:

- Fingerabdruckerkennung: Der Fingerabdrucksensor kann in die Home-Taste (z.B. Apple-Geräte mit Home-Taste [16], [17]), den seitlichen Ein-/Ausschalter (Sony Xperia Z5 [18]), die Rückseite des Smartphones (z.B. Samsung Galaxy S8 [19]) oder in bzw. hinter das Display (zuerst im Vivo X20 Plus UD [20]) integriert sein.
- 2D-Gesichtserkennung: Diese wird über die Frontkamera realisiert (z.B. Samsung Galaxy S8 [19]).
- 3D-Gesichtserkennung: Ein Punktprojektor projiziert ein Raster von unsichtbaren Infrarotpunkten auf das Gesicht des Benutzers, um aus der Verformung des Rasters Tiefeninformationen zu gewinnen. Das entstehende Muster und das Gesichtsbild werden von einer Infrarotkamera aufgenommen, um den Benutzer zu authentisieren (ab iPhone X [21]).
- Iriserkennung: In die Vorderseite des Smartphones kann ein Irisscanner bestehend aus Infrarot-LED und Infrarotkamera integriert sein (z.B. Samsung Galaxy S8 [19]).

Es werden zwei Sicherheitsstufen für die biometrischen Systeme unterschieden: 2D-Gesichtserkennung gilt als weniger sicher als 3D-Gesichtserkennung, Fingerabdruckerkennung und Iriserkennung und darf Anwendungen mit hohen Sicherheitsanforderungen nicht entsperren.

Die biometrischen Systeme innerhalb des Smartphones lassen sich wie folgt einsetzen:

- Entsperrung: Das Smartphone kann durch jedes der biometrischen Systeme, durch das Zeichnen von Mustern auf dem Touchscreen sowie die Eingabe von PIN oder Passwort entsperrt werden.
- Freischalten des Smartphones zur kryptographischen Authentisierung im Internet.
- Autorisierung von Bezahlprozessen: Bei Zahlungen über Near Field Communication (NFC) kann ein biometrisches Verfahren genutzt werden, um die Transaktion freizugeben.
- Zugriff auf geschützte Ressourcen: Innerhalb des Speichers gibt es speziell gesicherte Ordner (z.B. Passwortspeicher), die bei jedem Zugriff eine zusätzliche Authentisierung erfordern, die auch durch biometrische Verfahren erledigt werden kann.

Zum Schutz der biometrischen Referenzdaten und zur Ausführung der biometrischen Vergleichsoperationen wird speziell gesicherte Hardware innerhalb des Smartphones (Trusted Execution Environment, TEE [22]) genutzt, z.B. Apple Secure Enclave [23] und die Knox-Sicherheitsplattform von Samsung [24].

Kontinuierliche Authentisierung kann Authentisierungsprozesse komfortabler gestalten. Hat sich eine Person einmal authentisiert, entscheidet das System, wie lange der Zugriff erlaubt ist. Viele Systeme erfordern z.B. eine Passworteingabe bei der Installation neuer Software. Bei kontinuierlicher Authentisierung wird über Sensoren überprüft, ob die authentisierte Person noch anwesend ist, und gegebenenfalls nicht bei jedem Zugriff eine neue Authentisierung gefordert. Dies ist z.B. in der Apple Watch umgesetzt: Nach PIN-Eingabe wird über den eingebauten Pulssensor geprüft, ob ein Herzschlag vorhanden ist, und erst bei dessen Fehlen (wenn die Uhr nicht mehr am Handgelenk ist) wird das System gesperrt [25].

2.2.3.2 Freischalten eines Endgeräts zur kryptographischen (Client/Server-) Authentisierung

Anstatt sich im Internet mit Benutzername / Passwort zu authentisieren, können sich Benutzer sicher und bequem mit Hilfe kryptgraphischer Protokolle und eines Endgeräts unter ihrer Kontrolle authentisieren. Die Grundlage bilden z.B. die Spezifikationen der FIDO- (Fast Identity Online) Allianz [26].

Bei der Registrierung zu einem Dienst wird auf dem Gerät des Benutzers ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel generiert. Der öffentliche Schlüssel wird mit einem Attestierungsschlüssel, der vom Hersteller bei der Produktion fest auf alle Geräte des gleichen Modells geschrieben wird, signiert an den Server gesendet und der private Schlüssel wird sicher auf dem Gerät (im sog. FIDO-Authenticator) gespeichert. Der Zugriff auf den privaten Schlüssel wird durch biometrische Verfahren (z.B. Fingerabdruck- oder Iriserkennung) oder andere Verfahren gesichert. Für die Authentisierung sendet der Server eine Anfrage mit einer Zufallszahl

(Challenge) an das Gerät des Benutzers. Der FIDO-Authenticator signiert die Zufallszahl sowie weitere Daten mit dem privaten Schlüssel und beantwortet mit dem Ergebnis die Anfrage. Der Server kann mittels des hinterlegten öffentlichen Schlüssels die Authentizität des Benutzers überprüfen.

Hardware- und Software-Produkte, deren Konformität zu den FIDO-Spezifikationen nachgewiesen wurde, können ein FIDO-Zertifikat als Gütesiegel erhalten.

2.2.3.3 Mehrfaktorauthentisierung im Internet

Verhaltensbiometrische Lösungen analysieren z.B. die Art und Weise, wie der Benutzer auf der Tastatur oder der Bildschirmtastatur tippt. Dies kann verwendet werden, um die Sicherheit von Passwörtern für den Zugang zu Web- und Cloud-Anwendungen zu erhöhen [27].

2.2.3.4 Zugangskontrolle zu stationären Endgeräten

Biometrische Verfahren können zum Log-in auf Betriebssystemebene auf stationären Endgeräten verwendet werden. Mit Windows 10 wurde Windows Hello eingeführt, das die biometrische Verifikation auf Windows-Geräten ermöglicht. Der biometrische Sensor muss von Microsoft zertifiziert sein. Die biometrischen Referenzdaten werden kryptographisch gesichert auf dem stationären Endgerät gespeichert. Auch hardwaregestützte Schutzmaßnahmen über ein TPM (Trusted Platform Module) werden unterstützt.

Die Benutzer können sich von einem stationären Endgerät aus, auf dem sie sich lokal mit Windows Hello biometrisch authentisieren, einem Active-Directory-Konto gegenüber kryptographisch authentisieren [28].

2.2.3.5 Freischalten von Smartcards und anderen Sicherheitstoken

Die Verbraucher tragen eine Vielzahl von Smartcards (Chipkarten mit Mikroprozessorchip) bei sich, z.B. Debit- und Kreditkarten von Direkt- und Filialbanken, Gesundheitskarten, Dienstausweise und Mitgliedskarten. Zum Freischalten sicherheitsrelevanter Funktionen müssen zumeist PINs eingegeben werden. Biometrischer On-Card-Vergleich kann eine benutzerfreundliche Alternative zur PIN-Eingabe bieten. Auch »Biometric Systems-on-Card«, bei denen auch der biometrische Sensor und die Signalverarbeitung in die Smartcard eingebettet sind, sind technisch realisierbar [29].

Sicherheitstoken mit Schnittstellen wie NFC oder USB können zur kryptographischen Authentisierung von Benutzern an Computersystemen verwendet werden. Yubikey Bio mit integrierter Fingerabdruckerkennung soll die Vorteile eines Sicherheitstokens mit dem Komfort der biometrischen Anmeldung vereinen und unterstützt die FIDO2-Spezifikationen [30]. Die biometrischen Referenzdaten werden in einem Secure Element gespeichert, wo sie vor physischen Angriffen geschützt sind.

2.2.3.6 Entsperren anderer Geräte

Zum Beispiel können USB-Speichersticks zum Schutz vertraulicher Daten mit einem integrierten Fingerabdruckerkennungssystem ausgestattet sein. Erst wenn einer der berechtigten Finger verifiziert ist, wird der Speicher geöffnet. Der kryptographische Schlüssel ist für jedes Gerät verschieden und wird bei der Registrierung auf Basis des Fingerabdrucks generiert. Die Ver- und Entschlüsselung selbst erfolgt ohne weiteres Zutun des Benutzers beim Schreiben und Lesen der Daten.

2.2.3.7 Zugangskontrolle zur IT-Service-Hotline

Zur Anruferauthentisierung z.B. in der Anwendung »Passwortrücksetzung« in der IT-Service-Hotline werden Sprecherverifikationssysteme verschiedener Hersteller eingesetzt. Der Zweck ist die schnelle und sichere Wiederherstellung der Arbeitsfähigkeit, falls ein Passwort zurückzusetzen ist.

2.2.3.8 Zugangskontrolle zu gesicherten Bereichen

Biometrische Verfahren können zur Kontrolle des physischen Zutritts zu Räumen oder Gebäuden verwendet werden. Neben Verifikationssystemen befinden sich auch Identifikationssysteme (die ohne zusätzliche Chipkarten oder Sicherheitstoken auskommen) im Einsatz. Die zunehmende Leistungsfähigkeit von biometrischen Erkennungssystemen ermöglicht auch Systeme mit zahlreichen Teilnehmern. Auch für den privaten Bereich gibt es Zugangskontrollsysteme z.B. für Haustüren [31]. Der Fingerabdruck ersetzt den Schlüssel und öffnet nach erfolgreicher Identifikation die Tür.

Biometrische Verfahren können auch verwendet werden, um Dauerkarten für Freizeiteinrichtungen an eine bestimmte Person zu binden. Zum Beispiel setzt der Zoo Hannover zu diesem Zweck Gesichtserkennung ein. Beim ersten Besuch wird ein digitales Foto direkt an den Drehkreuzen aufgenommen und gespeichert. Bei jedem weiteren Besuch wird an den Drehkreuzen auf die gleiche Weise ein digitales Foto aufgenommen und durch einen Vergleich die Identität verifiziert.

In Überwachungsszenarien werden Gesichtsbilder aufgenommen und mit gespeicherten Gesichtsbildern aus einer Sperrliste (z.B. von Personen, die sich freiwillig vom Zugang zu einem Spielcasino ausgeschlossen haben oder mit einem Hausverbot belegt sind) verglichen [32].

2.2.4 Finanzanwendungen

2.2.4.1 Online- und Voice-Banking

Seit Inkrafttreten der überarbeiteten europäischen Zahlungsdiensterichtlinie (Payment Services Directive 2, PSD2), die Mehrfaktorauthentisierung verlangt [33], haben die lange im Online-Banking gebräuchlichen iTAN-Listen ausgedient. In Online-Banking-Apps (z.B. BestSign-App der Postbank [34]) wird der Benutzer entweder wissensbasiert oder biometrisch auf dem Smartphone authentisiert, das kryptographisch gegenüber dem Bank-Server authentisiert wird. Zur Freigabe einer Transaktion erhält der Benutzer eine Benachrichtigung ans Smartphone und kann diese wissensbasiert oder biometrisch bestätigen.

Beim »Voice Banking« muss man einen digitalen Sprachassistenten auf sein Smartphone installieren und mit dem Bankkonto verbinden. Mit Hilfe von Sprachbefehlen können Überweisungen vorbereitet werden. Um eine per Spracherkennung vorbereitete Überweisung auszuführen, muss der Kunde sicherheitshalber noch in die Online-Banking-App gehen und die Transaktion wie bisher freigeben [35].

2.2.4.2 Bargeldabhebung am Geldautomaten

Zum Beispiel in Japan wird Biometrie als zusätzliches Sicherheitsverfahren an Geldautomaten eingesetzt. Beim Geldabheben wird der Fingerabdruck oder das Venenmuster der Handfläche oder Finger aufgenommen und geprüft. In Deutschland gab es Feldversuche, jedoch keine Praxiseinführung [36].

2.2.4.3 Bargeldloses Bezahlen

Google Pay ist ein elektronisches Zahlungssystem des Herstellers Google zum Bezahlen mit mobilen Endgeräten. Bei Google Pay müssen die Daten der unterstützten Kredit- oder Debitkarte [37] sicher auf dem mobilen Endgerät gespeichert werden. Diese Daten werden bei einer Transaktion nicht an den Händler übertragen. In Ladengeschäften kann mittels »Tap and Pay« über bestehende NFC-Terminals bezahlt werden, wenn die hinterlegte Karte akzeptiert wird. Innerhalb von Apps, die die Google Payment API integriert haben (z.B. Groupon und Uber), kann über die Schaltfläche »Pay with

Google« bezahlt werden. Google Pay unterstützt die Benutzerauthentisierung mittels Fingerabdruckerkennung [38].

Apple Pay ist ein elektronisches Zahlungssystem des Herstellers Apple zum Bezahlen mit mobilen Endgeräten von Apple. Es arbeitet mittels NFC in Kombination mit der App Wallet. Das System kann auch genutzt werden, um Zahlungen in dafür vorgesehenen Apps oder im Safari-Browser durchzuführen [39]. Die Nutzer geben die Transaktionen über 3D-Gesichtserkennung oder Fingerabdruckerkennung frei.

Sparkassen und Volksbanken haben eigene Apps für das bargeldlose Bezahlen unter Verwendung von mobilen Endgeräten auf den Markt gebracht [40].

In der Edeka-Regionalgesellschaft Südwest wurde das digiPROOF-Bezahlsystem zum Bezahlen per Fingerabdruck installiert. Die zur Zahlungsabwicklung benötigten Daten werden mit dem Fingerabdruck-Template verbunden und davon getrennt sicher abgespeichert. Bei der Zahlung wird eine spezielle Taste gedrückt (Zahlart »digiPROOF«), der Fingerabdrucksensor leuchtet auf und der Kunde legt den registrierten Finger darauf. Das aufgenommene Template wird mit den in der Datenbank hinterlegten Templates verglichen (1-zu-*n*-Vergleich). Wird ein passendes Template erkannt, werden die zur Zahlungsabwicklung notwendigen Daten an die Kasse zurückgegeben [41].

2.2.4.4 VideoIdent-Verfahren

Das VideoIdent-Verfahren dient der Online-Verifikation über einen Video-Chat. Insbesondere von Online-Banken wird es angeboten, um die persönlichen Daten ihrer Kunden z.B. bei einer online beantragten Kontoeröffnung bestätigen zu lassen und das Postident-Verfahren zu ersetzen. Die Verbraucher benötigen ein gültiges Ausweisdokument (Reisepass oder Personalausweis), eine Webcam am bzw. im Computer, Laptop, Tablet oder Smartphone, einen Webbrowser und eine leistungsfähige Internetverbindung. Ein automatischer Vergleich des präsentierten Gesichts mit dem Gesicht im Ausweis findet bisher nicht statt.

2.2.5 Arbeitszeiterfassung

Biometrische Verfahren können zur Arbeitszeiterfassung verwendet werden. Arbeitszeiterfassungssysteme laufen oft im Identifikationsmodus. Neben dem Erfordernis der individuellen Einwilligung ist bei biometrischer Arbeitszeiterfassung die Mitbestimmungspflicht durch Arbeitnehmervertretungen zu beachten [42].

2.2.6 Komfortanwendungen

2.2.6.1 Fahrzeugtechnik

Biometrische Komfortanwendungen sind Anwendungen, die den Benutzer anhand seines Verhaltens und seiner biologischen Charakteristika erkennen, um individuelle Einstellungen vorzunehmen, die jedoch keine hohen Sicherheitsanforderungen zu erfüllen brauchen.

Der Gentex Biometric Mirror ist ein Prototyp für biometrische Anwendungen im Fahrzeugbereich [43]. Ein Irisscanner, Infrarotbeleuchtung und ein Steuergerät sind in den Rückspiegel eines Fahrzeugs integriert. Das Enrolment erfolgt lokal im Fahrzeug und die biometrischen Daten werden im Steuergerät verglichen. Neben der Zugangskontrolle (Wegfahrsperre wird nur deaktiviert, wenn der Fahrer in der Liste der erlaubten Personen ist) ist die Identifikation des Fahrers für folgende Zwecke vorgesehen:

- Personalisierung: Hat die Person ein Profil hinterlegt, können Spiegel, Sitze, Lenkrad, Musikrichtung und wichtige Navigationsziele eingestellt werden.
- Car-Sharing: Wenn das Fahrzeug im Rahmen von Car-Sharing-Anwendungen genutzt werden soll, können die biometrischen Probedaten mit einer zentralen Datenbank verglichen und Bezahlvorgänge (z.B. Maut, Parkgebühren) automatisiert werden. Allerdings ist hierfür eine zentrale Enrolment-Datenbank notwendig.
- Verknüpfung zu HomeLink: Das Fahrzeug kann mit Hausautomatisierungslösungen verknüpft werden, z.B. zur Öffnung von Garagen oder Steuerung von Lichtern.

Continental hat ein ähnliches prototypisches System vorgestellt [44] mit zwei biometrischen Sensoren innerhalb des Fahrzeugs: einem Fingerabdrucksensor im Cockpit und einer Kamera für die Gesichtserkennung im Rückspiegel.

Der Einsatz biometrischer Erkennungssysteme im Fahrzeugbereich über Komfortanwendungen hinaus kann Gefahr für die körperliche Unversehrtheit des Fahrzeugnutzers oder die Gefahr der Entführung zum Erzwingen des biometrischen Zugangs mit sich bringen. Um ein Fingerabdruckerkennungssystem zum Deaktivieren der Wegfahrsperre eines gestohlenen Oberklassewagens zu überwinden, wurde schon einmal der benötigte Finger abgeschnitten [45]. Solche Angriffe unterstreichen die Notwendigkeit einer effektiven Erkennung biometrischer Präsentationsangriffe (Lebenderkennung) und die Notwendigkeit einer Risikobewertung beim Einsatz biometrischer Systeme.

2.2.6.2 Digitale Sprachassistenten

Digitale Sprachassistenten-Software wie Alexa von Amazon, Siri von Apple, Google Assistant von Google, Cortana von Microsoft und Bixby von Samsung kann gesprochene Sprache erkennen und verstehen und sprachgesteuert Fragen beantworten, Dialoge führen und Assistenzdienste erbringen. Sie ist vor allem in Smartphones, aber auch in stationäre Endgeräte, Smart TVs oder Smart Speakers (Echo von Amazon, Google Home oder Apple HomePod) integriert. Die Systeme sind so konzipiert, dass sie im Bereitschaftsmodus die Sprache zunächst geräteintern verarbeiten und auf einen Aufwachbefehl wie »Alexa«, »Hey, Siri«, »OK, Google« bzw. »Hey, Cortana« warten. Nachdem ein Aufwachbefehl erkannt wurde, senden die digitalen Sprachassistenten Sprachdaten zur Verarbeitung in die Cloud, auch von Personen, die nicht wissen, dass mitgehört wird [46]. Google hat schon Spracherkennungssoftware entwickelt, die nur noch ein halbes Gigabyte Massenspeicher belegt und lokal auch ohne Netzwerkverbindung läuft [47].

Um der unbefugten Benutzung vorzubeugen und personalisierte Dienste zu ermöglichen, bieten die neuesten Versionen einiger digitaler Sprachassistenten die Möglichkeit zur Stimm- bzw. Sprecher-erkennung.

2.2.6.3 Smart Home

Biometrische Verfahren können in Zukunft im Falle mehrerer Benutzer zur Personalisierung des Verhaltens von Hausautomatisierungssystemen verwendet werden. Abgesehen von biometrischen Türschlössern und Smart-Home-Steuerungen mit Sprach- und Sprechererkennung [48] befindet sich die Biometrie im Bereich Smart Home noch in einem frühen Stadium.

2.2.7 Gesichtersuchmaschinen

Für Facebook-Nutzer ist eine Funktion zur Erkennung von Personen verfügbar, aber standardmäßig ausgeschaltet. Mit dieser Funktion ist es möglich, auf einem hochgeladenen Foto markierte Personen auf allen Facebook-Bildern zu erkennen.

Der Cloud-Computing-Anbieter Amazon Web Services (AWS) bietet einen Bilderkennungsdienst an, der in hochgeladenen Fotos u.a. Gesichter suchen und vergleichen kann (Amazon Rekognition Image).

Technologisch wäre eine biometrische Suche auch für Google kein Problem. Das Hindernis sind vor allem die Gesetze und Verordnungen zum Datenschutz.

ClearView AI bietet Strafverfolgungsbehörden an, Fotos von Unbekannten zur Identifizierung mit online veröffentlichten Bildern zu vergleichen [49]. PimEyes ist eine kostenlose Suchmaschine für (eigene) Gesichtsbilder [50]. Alle, von denen es Fotos im Internet gibt, könnten schon Teil der Datenbanken sein.

2.3 Klassifizierung nach der Systemarchitektur

Biometrische Referenzdaten können an verschiedenen Orten gespeichert und mit Probedaten verglichen werden: auf einem tragbaren Sicherheitstoken wie einer Smartcard, in einem abgeschotteten Biometriemodul, das mit einem Client verbunden oder in diesen eingebettet sein kann (z.B. Trusted Execution Environment), lokal auf einem Client (stationäres oder mobiles Endgerät in einem Netz) oder räumlich entfernt in einem Server. Wo die Speicherung und der Vergleich der biometrischen Daten stattfinden, beeinflusst das Angriffsrisiko und die Handhabbarkeit des biometrischen Erkennungssystems. Die gängigsten Systemarchitekturen biometrischer Erkennungssysteme sind [51]:

- Store on Token, Compare on Token: Die biometrischen Referenzdaten werden auf einem tragbaren Sicherheitstoken gespeichert. Die Probedaten werden im Token mit den Referenzdaten verglichen, um den Zugriff auf sicherheitsrelevante Funktionen oder Daten im Token freizuschalten.
- Store on Token, Compare on Device: Die biometrischen Referenzdaten werden auf einem tragbaren Sicherheitstoken gespeichert und zum Vergleich mit den Probedaten an ein abgeschottetes Biometriemodul gesendet.
- Store on Token, Compare on Server: Die biometrischen Referenzdaten werden auf einem tragbaren Sicherheitstoken gespeichert. Sowohl die Referenzdaten als auch die Probedaten werden zum Vergleich an einen Server gesendet.
- Store on Device, Compare on Device: Die biometrischen Referenzdaten werden in einem abgeschotteten Biometriemodul gespeichert und mit den Probedaten verglichen.
- Store on Client, Compare on Client: Die biometrischen Referenzdaten werden auf einem mit einem Netzwerk verbundenen Client gespeichert und mit den Probedaten verglichen.
- Store on Server, Compare on Server: Die biometrischen Referenzdaten werden auf einem Server gespeichert. Die Probedaten werden zum Vergleich an den Server gesendet. Diese Systemarchitektur wird z.B. bei der Anruferauthentisierung und der Prüfung des Tippverhaltens bei der Passworteingabe im Internet eingesetzt.

3 Online-Befragung zur Ermittlung der Verbrauchersicht auf biometrische Erkennungssysteme

3.1 Überblick

Um die Verbrauchersicht auf aktuell genutzte und in naher Zukunft angebotene biometrische Erkennungssysteme zu ermitteln und daraus Handlungsempfehlungen für die Normung und die Verbraucherkommunikation abzuleiten, wurde eine Online-Befragung durchgeführt. Der Online-Fragebogen (siehe Anhang A) umfasste Fragen

- zu soziodemographischen Angaben,
- zur aktuellen Nutzung biometrischer Erkennungssysteme,
- zu ihrer empfundenen Benutzerfreundlichkeit und Sicherheit sowie
- zur Bereitschaft zur zukünftigen Nutzung biometrischer Systeme.

Zur Erstellung des Fragebogens und zur Durchführung und Auswertung der Befragung wurde das Online-Umfrage-Tool Umbuzoo [52] genutzt, das schon für andere Befragungen des DIN-Verbraucherrats datenschutzrechtlich geprüft und genutzt wurde. Antworten wurden im September und Oktober 2020 gesammelt.

3.2 Teilnehmer

Die beabsichtigte Grundgesamtheit ist die Menge aller Verbraucher in Deutschland. Bei Online-Befragungen kann jedoch keine Repräsentativität bezogen auf alle Verbraucher, sondern nur Repräsentativität bezogen auf spezielle Gruppen von Internetnutzern erreicht werden [53]. Um sich einer Zufallsstichprobe anzunähern, wurden Methoden zur aktiven und passiven Auswahl der Teilnehmer angewandt:

- Aktive Auswahl: Die Mitglieder verschiedener beruflicher E-Mail-Verteiler und Mailinglisten mit und ohne Bezug zur Biometrie wurden zur Teilnahme an der Befragung eingeladen. Die Empfänger wurden gebeten, die Einladung weiter zu verteilen.
- Passive Auswahl: Einladungstexte und Links zur Befragungsseite wurden auf die Webseiten des Fraunhofer IGD und des DIN-Verbraucherrats gestellt und in den sozialen Netzwerken LinkedIn, Facebook und Twitter geteilt. Außerdem wurde das Online-Panel PollPool [54] zur Gewinnung von Teilnehmern genutzt.

Insgesamt wurde der Online-Fragebogen 210-mal ausgefüllt. Da es sich um eine Zufallsstichprobe handelt, kann für jede der im Weiteren empirisch ermittelten relativen Häufigkeiten ein Vertrauensbereich angegeben werden, innerhalb dessen ihr wahrer Wert mit einer bestimmten Wahrscheinlichkeit liegt. Bei einer Stichprobengröße von 210 Antworten beträgt die Größe des Vertrauensbereichs, der mit 95%iger Sicherheit den wahren Wert einer empirisch ermittelten relativen Häufigkeit von 5 % bzw. 95 % enthält, ±3 % und die Größe des 95%-Vertrauensbereichs einer empirisch ermittelten relativen Häufigkeit von 50 % ±7 % [55].

90 der Befragten (43 %) waren Frauen und 120 (57 %) Männer (0 % divers). Abbildung 1 zeigt die Altersstruktur der Befragten. Abbildung 2 zeigt die Häufigkeit der höchsten Bildungsabschlüsse der Befragten.

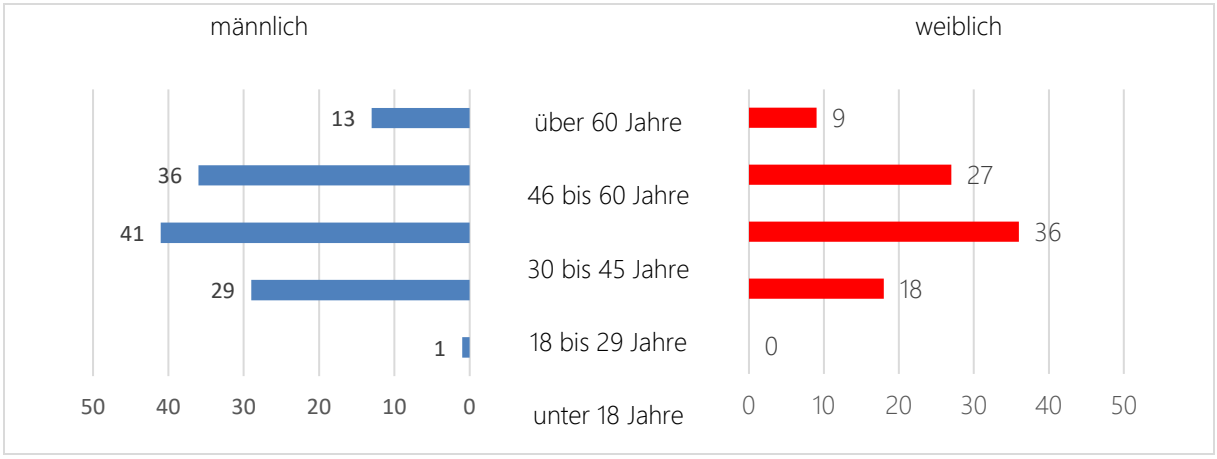

Abbildung 1 Anzahl der Befragten pro Altersgruppe und Geschlecht

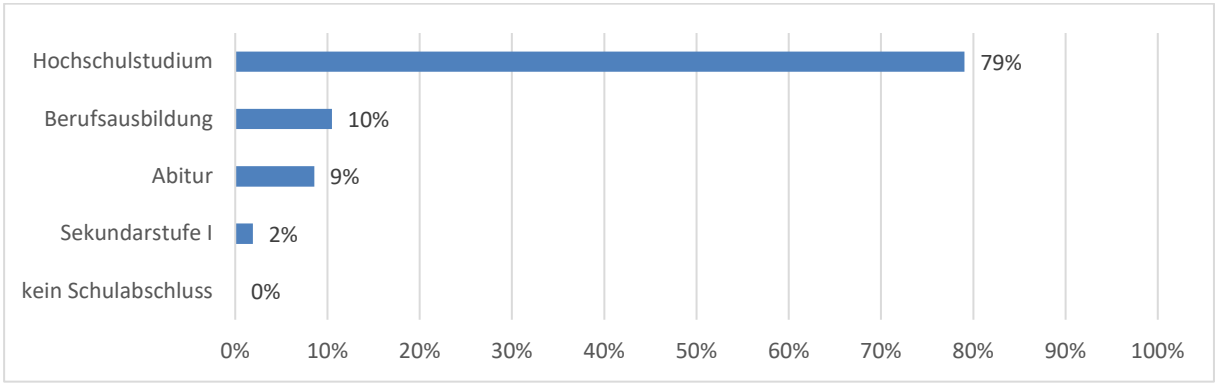

Abbildung 2 Höchster Bildungsabschluss der Befragten

79 % der Befragten gaben an, über einen Hochschulabschluss zu verfügen, während bundesweit (Stand 2018) nur 22 % der Bevölkerung im Alter von 25 bis unter 65 Jahren über einen Hochschulabschluss verfügen [56]. Die Abweichung der Verteilung der soziodemographischen Angaben der Befragten von der Verteilung in der Grundgesamtheit zeigt, dass Repräsentativität bezogen auf alle

Verbraucher in Deutschland nicht erreicht wurde. Da die Befragung online stattfand, ist anzunehmen, dass Personen mit hoher Affinität zur Technikinteraktion überrepräsentiert sind. Dank der Verwendung beruflicher E-Mail-Verteiler mit Bezug zur Biometrie ist anzunehmen, dass die Befragten einen Großteil der biometrischen Erkennungssysteme, die in Deutschland im Einsatz sind, abdecken.

3.3 Bisherige Nutzung biometrischer Erkennungssysteme

3.3.1 Überblick

140 der Befragten (67 %) benutzen von Zeit zu Zeit biometrische Erkennungssysteme. 70 der Befragten (33 %) benutzen keine biometrischen Erkennungssysteme. Abbildung 3 zeigt, wie die Nutzung biometrischer Erkennungssysteme in den Altersgruppen verbreitet ist. In der Altersgruppen über 60 Jahre ist die Nutzung biometrischer Erkennungssysteme signifikant weniger verbreitet als im Durchschnitt.

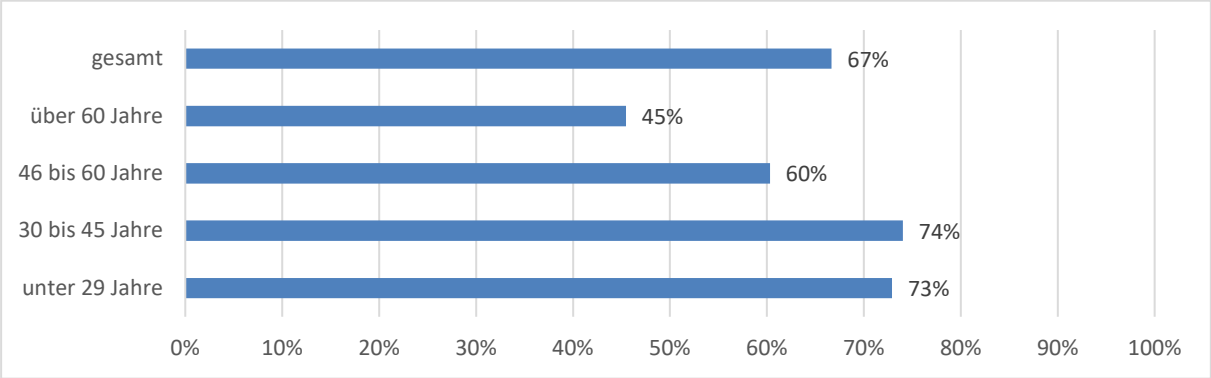

Abbildung 3 Nutzung biometrischer Erkennungssysteme nach Altersgruppen

Abbildung 4 zeigt, welche biometrischen Verfahren von wie viel Prozent der Biometrienutzer genutzt werden. Unter den Biometrienutzern setzt die große Mehrheit (94 %) Fingerabdruck-erkennung ein. 50 % der Biometrienutzer nutzen Gesichtserkennung. Immerhin 14 % der Biometrie-nutzer nutzen Sprechererkennung. Iris- und Venenmustererkennung werden von wenigen genutzt. Nur drei der Befragten gaben an, Unterschriftserkennung zu nutzen, und zwar ausschließlich zum bargeldlosen Bezahlen. Höchstwahrscheinlich handelt es sich um Zahlung per Lastschriftverfahren mit elektronischer Speicherung der Unterschrift, jedoch ohne automatische Unterschriftserkennung. Darum wurden diese Angaben von der Auswertung ausgeschlossen. Keiner der Befragten gab andere biometrische Verfahren an. Die Summe ist größer als 100 %, da Mehrfachnennungen möglich waren. 54 % der Biometrienutzer gaben an, mehr als ein biometrisches Verfahren zu nutzen.

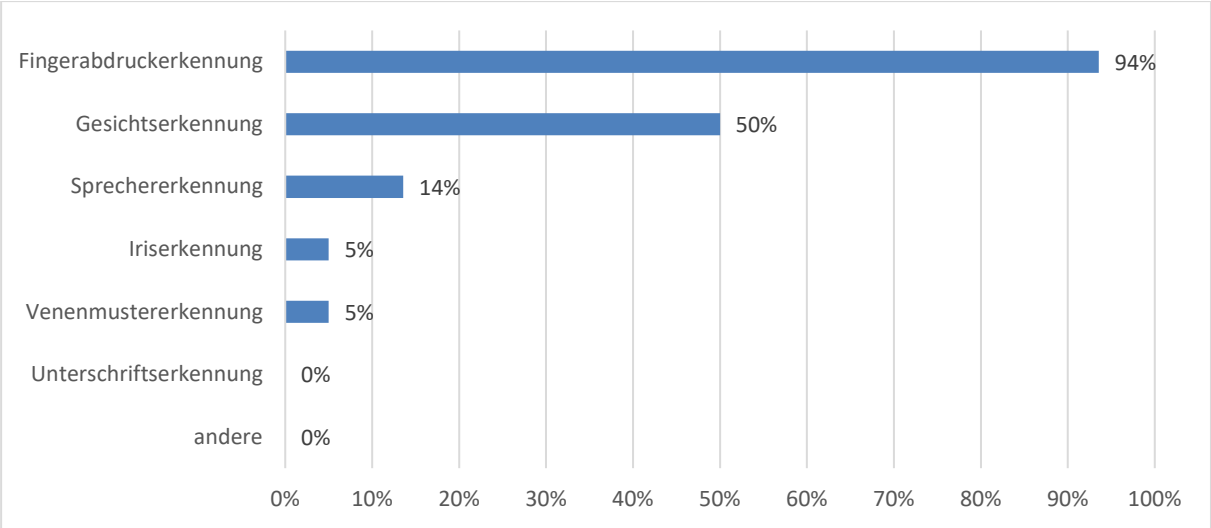

Abbildung 4 Benutzte biometrische Verfahren

Die folgenden Abschnitte zeigen, bei welchen Vorgängen die gebräuchlichen biometrischen Verfahren genutzt werden und welche Erfahrungen die Benutzer mit Falschrückweisungen, Falschakzeptanzen und biometrischen Präsentationsangriffen gesammelt haben. Am weitesten verbreitet sind biometrische Anwendungen, die die in biometriefähige Endgeräte integrierten Sensoren nutzen (Entsperren von Endgeräten, Freischalten von Endgeräten zur kryptographischen Authentisierung im Internet, Online-Banking, mobiles Bezahlen). Zur Bargeldabhebung an Geldautomaten und zur Arbeitszeiterfassung setzen die Befragten biometrische Verfahren gar nicht ein.

3.3.2 Fingerabdruckerkennung

Abbildung 5 zeigt, bei welchen Vorgängen von wie viel Prozent der Biometrienutzer Fingerabdruck-erkennung genutzt wird. Mehrfachnennungen waren möglich. Keiner der Befragten gab neben den vorgegebenen Klassen andere Vorgänge an. Der Vorgang »Anmelden bei der BARMER-App« wurde unter »Freischalten des Smartphones zur Authentisierung« gezählt.

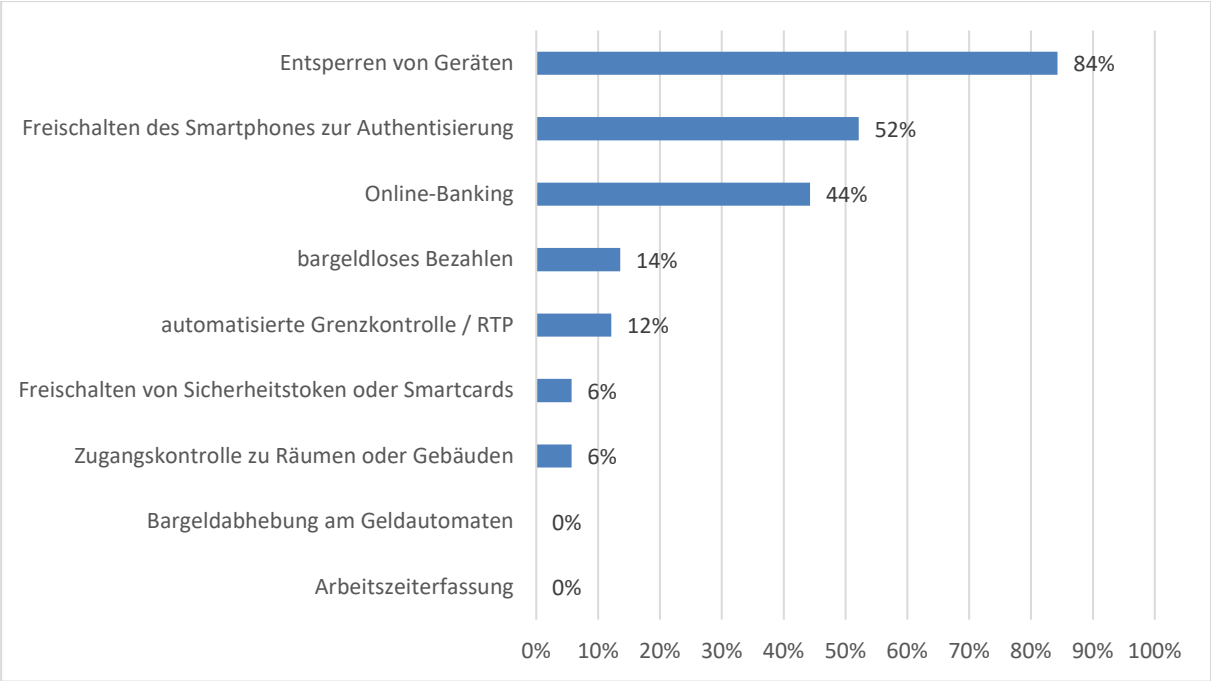

Abbildung 5 Vorgänge, bei denen Fingerabdruckerkennung benutzt wird

Abbildung 6 zeigt, welcher Anteil der Benutzer jeweils angab, bei der Fingerabdruckerkennung »sehr selten«, »selten«, »gelegentlich« bzw. »häufig« von fälschlichen Rückweisungen betroffen zu sein und auf Ausweichlösungen zurückgreifen zu müssen. Die Mehrheit der Benutzer gab an, sehr selten oder selten von fälschlichen Rückweisungen betroffen zu sein.

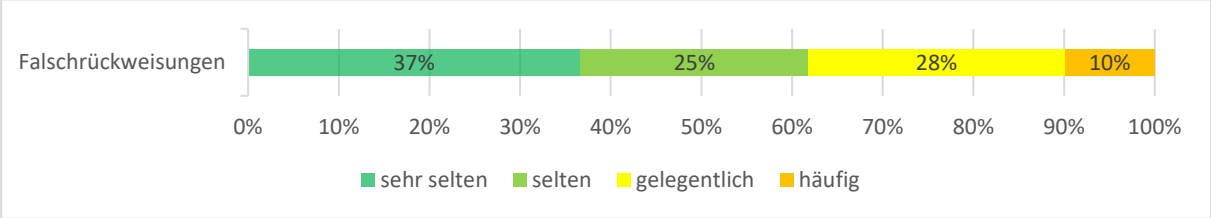

Abbildung 6 Gefühlte Häufigkeit falscher Rückweisungen bei der Fingerabdruckerkennung

3 % der Benutzer von Fingerabdruckerkennung gaben an, schon einmal von der Verwechslung ihrer Fingerabdrücke mit denen anderer Personen betroffen gewesen zu sein. 2 % der Benutzer gaben an, bei der Fingerabdruckerkennung schon einmal von einer täuschend echten Imitation ihrer biometrischen Merkmale betroffen gewesen zu sein. Fingerabdruckerkennungssysteme, die nicht ausreichend widerstandsfähig gegen sog. Präsentationsangriffe sind, können mit Attrappen z.B. aus Silikon, die den Fingerabdruck der betroffenen Person imitieren, bezwungen werden [57].

3.3.3 Gesichtserkennung

Abbildung 7 zeigt, bei welchen Vorgängen von wie viel Prozent der Biometrienutzer Gesichtserkennung genutzt wird. Mehrfachnennungen waren möglich. Neben den vorgegebenen Klassen von Vorgängen gab jeweils einer der Befragten an, auch zur Personenerkennung in einer Fotosammlung und zum Entsperren von Internet-Accounts automatische Gesichtserkennung einzusetzen.

Die am weitesten verbreitete Anwendung von Gesichtserkennung nach dem Entsperren von Endgeräten ist die automatisierte Grenzkontrolle.

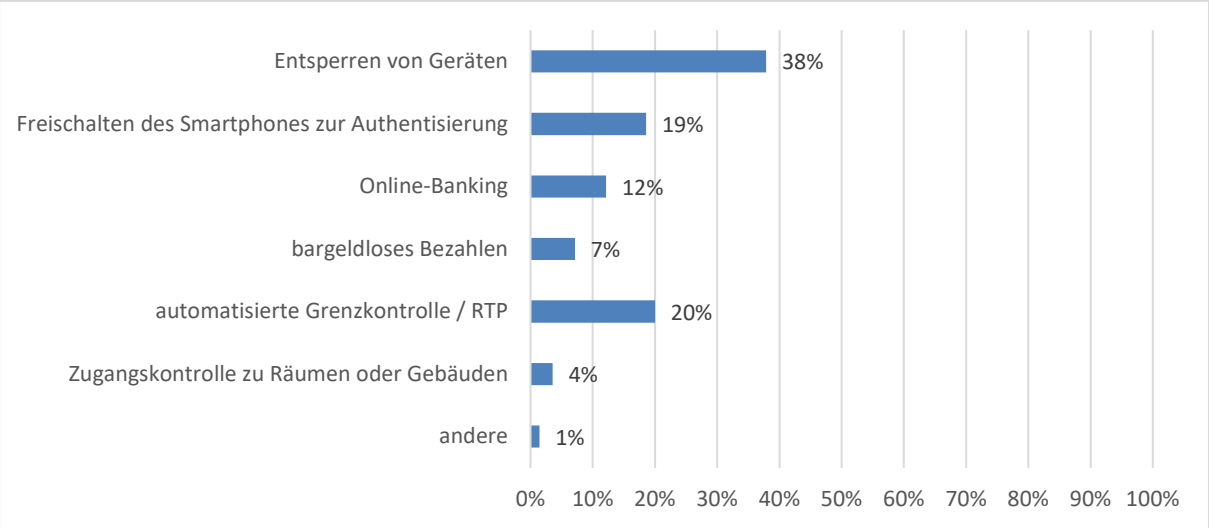

Abbildung 7 Vorgänge, bei denen Gesichtserkennung benutzt wird

Abbildung 8 zeigt, welcher Anteil der Benutzer jeweils angab, bei der Gesichtserkennung »sehr selten«, »selten«, »gelegentlich« bzw. »häufig« von fälschlichen Rückweisungen betroffen zu sein und auf Ausweichlösungen zurückgreifen zu müssen. Ähnlich wie bei der Fingerabdruckerkennung gab die Mehrheit der Benutzer an, sehr selten oder selten von fälschlichen Rückweisungen betroffen zu sein.

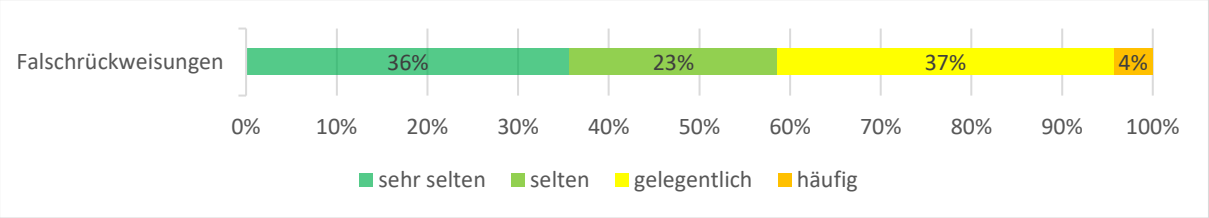

Abbildung 8 Gefühlte Häufigkeit falscher Rückweisungen bei der Gesichtserkennung

10 % der Benutzer von Gesichtserkennung gaben an, schon einmal von der Verwechslung ihres Gesichts mit dem anderer Personen betroffen gewesen zu sein. 4 % der Benutzer gaben an, bei der Gesichtserkennung schon einmal von einer täuschend echten Imitation ihrer biometrischen Merkmale betroffen gewesen zu sein. Gesichtserkennungssysteme, die nicht ausreichend widerstandsfähig gegen Präsentationsangriffe sind, können z.B. durch ausgedruckte Fotos oder auf einem Bildschirm abgespielte Aufnahmen der betroffenen Person, die vor die Kamera gehalten werden, oder durch Silikonmasken bezwungen werden [58].

3.3.4 Sprechererkennung

Abbildung 9 zeigt, bei welchen Vorgängen von wie viel Prozent der Biometrienutzer Sprechererkennung genutzt wird. Jeweils einer der Befragten gab an, zur »Textübersetzung« und zur »Spracheingabe für E-Mail-Nachrichten, WhatsApp« automatische Sprechererkennung einzusetzen. Höchstwahrscheinlich ist in beiden Fällen keine Sprechererkennung, sondern Spracherkennung zur automatischen Transkription des gesprochenen Worts in geschriebenen Text gemeint. Darum wurden diese Angaben von der Auswertung ausgeschlossen. »Passwort-Reset« wurde unter »Hotline-Anrufe« gezählt. »Google Assistant« wurde unter »Zugangskontrolle zu digitalen Sprachassistenten« gezählt.

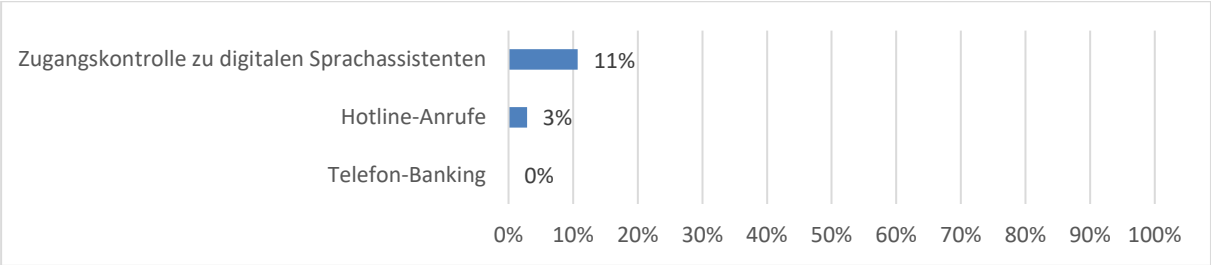

Abbildung 9 Vorgänge, bei denen Sprechererkennung benutzt wird

Abbildung 10 zeigt, wie oft die Benutzer bei der Sprechererkennung von fälschlichen Rückweisungen betroffen sind und auf Ausweichlösungen zurückgreifen müssen. Bei der Sprechererkennung waren die Benutzer häufiger von fälschlichen Rückweisungen betroffen als bei der Fingerabdruck- und Gesichtserkennung.

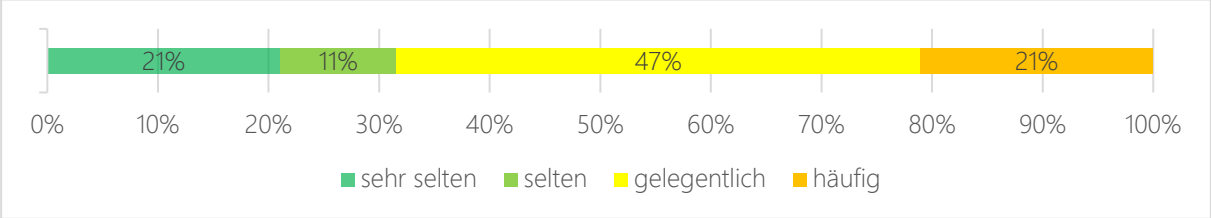

Abbildung 10 Gefühlte Häufigkeit falscher Rückweisungen bei der Sprechererkennung

37 % der Benutzer gaben an, schon einmal von einer Verwechslung ihrer Stimme mit der anderer Personen betroffen gewesen zu sein. 11 % der Benutzer gaben an, bei der Sprechererkennung schon einmal von einer täuschend echten Imitation ihrer biometrischen Merkmale betroffen gewesen zu sein.

3.3.5 Iriserkennung

Abbildung 11 zeigt, bei welchen Vorgängen von wie viel Prozent der Biometrienutzer Iriserkennung genutzt wird. Keiner der Befragten gab neben den vorgegebenen Klassen andere Vorgänge an.

Alle Benutzer von Iriserkennung gaben an, sehr selten oder höchstens selten von fälschlichen Rückweisungen betroffen zu sein und auf Ausweichlösungen zurückgreifen zu müssen. Keiner der Benutzer gab an, schon einmal von der Verwechslung seiner Iris mit der anderer Personen oder von einer täuschend echten Imitation seiner Iris (z.B. auf einer Kontaktlinse) betroffen gewesen zu sein.

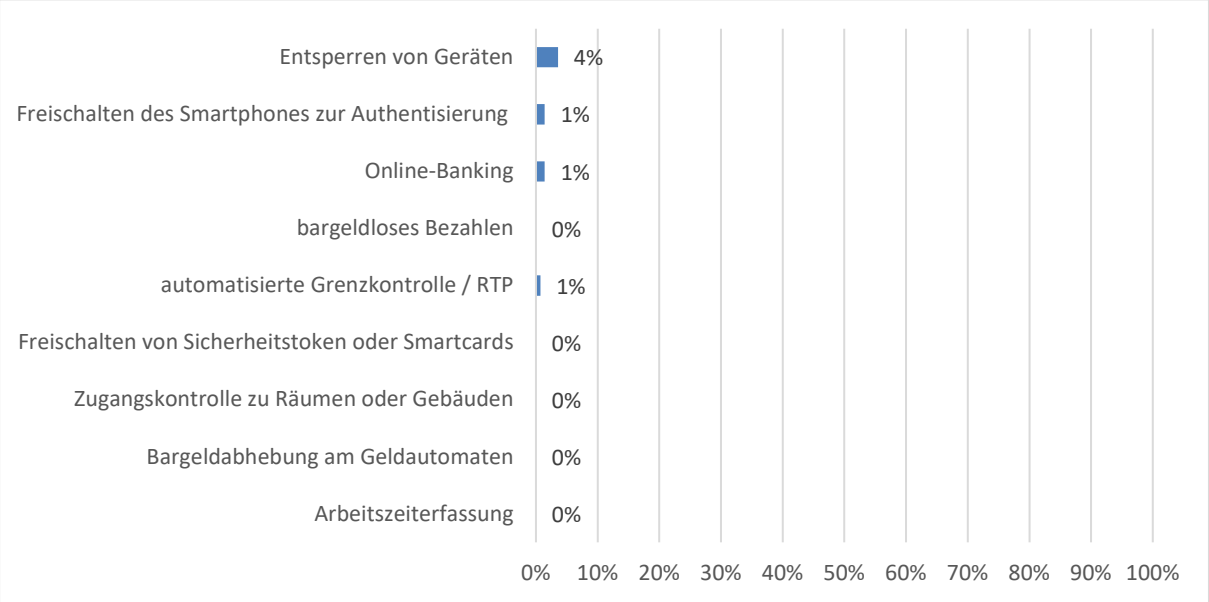

Abbildung 11 Vorgänge, bei denen Iriserkennung benutzt wird

3.3.6 Venenmustererkennung

Alle Benutzer von Venenmustererkennung gaben an, dieses Verfahren ausschließlich zur Zugangskontrolle zu Räumen oder Gebäuden einzusetzen. Sechs der sieben Benutzer von Venenmustererkennung gaben an, sehr selten oder selten von fälschlichen Rückweisungen betroffen zu sein und auf Ausweichlösungen zurückgreifen zu müssen. Keiner der Benutzer gab an, schon einmal von der

Verwechslung seines Venenmusters mit dem anderer Personen oder von einer täuschend echten Imitation seines Venenmusters betroffen gewesen zu sein.

3.3.7 Verfügbarkeit von Endgeräten mit integrierten biometrischen Sensoren

80 % der Befragten verfügen über mindestens ein biometriefähiges Endgerät. 16 % der Befragten verfügen über kein biometriefähiges Endgerät. 4 % der Befragten wussten nicht, ob sie über ein biometriefähiges Endgerät verfügen.

Abbildung 12 zeigt, wie die Befragten mit biometriefähigem Endgerät dieses im Normalfall entsperren. 71 % der Befragten mit biometriefähigem Endgerät nutzen im Normalfall ein biometrisches Verfahren zum Entsperren dieses Endgeräts (53 % nutzen Fingerabdruckerkennung, 17 % Gesichtserkennung, 1 % Iriserkennung). 28 % der Befragten mit biometriefähigem Endgerät nutzen im Normalfall ein wissensbasiertes Verfahren zum Entsperren dieses Endgeräts (23 % tippen eine PIN oder ein Passwort ein und 5 % nutzen Gestenerkennung auf dem Touchscreen). Neben den vorgegebenen Verfahren gab ein Befragter an, sein biometriefähiges Endgerät im Normalfall durch »Bluetooth-Nähe zur Smartwatch« zu entsperren. Nur einer der Befragten gab an, dass sein Endgerät gar nicht gesperrt wird. Vor der Einführung biometrischer Sensoren in Smartphones gaben 86 % der Teilnehmer einer Umfrage an, dass ihre Smartphones aus Gründen der Bequemlichkeit nicht gesperrt werden (höchstens Tastensperre mit einheitlicher Freigabekombination zum Schutz vor versehentlichem Gebrauch) [59].

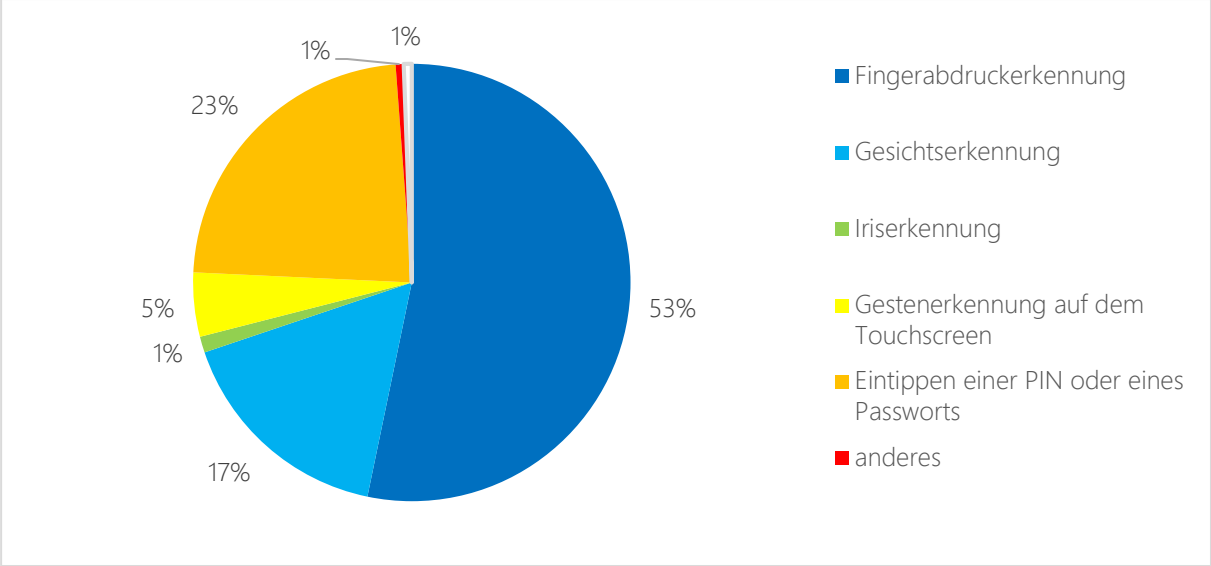

Abbildung 12 Zum Entsperren biometriefähiger Endgeräte eingesetzte Verfahren

Abbildung 13 zeigt, wie die Verfügbarkeit von biometriefähigen Endgeräten in den Altersgruppen verbreitet ist. In der Altersgruppe über 60 Jahre sind biometriefähige Endgeräte signifikant weniger verbreitet als im Durchschnitt.

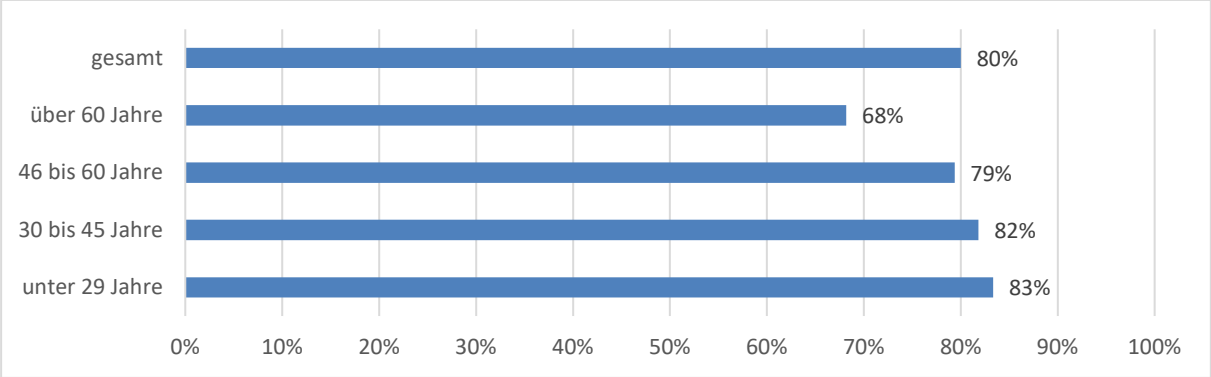

Abbildung 13 Verfügbarkeit von biometriefähigen Endgeräten nach Altersgruppen

Abbildung 14 zeigt, wie die Nutzung biometrischer Verfahren zum Entsperren biometriefähiger Endgeräte in den Altersgruppen verbreitet ist. In der Altersgruppen über 60 Jahre sind biometriefähige Endgeräte nicht nur signifikant weniger verbreitet als im Durchschnitt, sondern werden, selbst wenn vorhanden, auch signifikant seltener als im Durchschnitt biometrisch entsperrt.

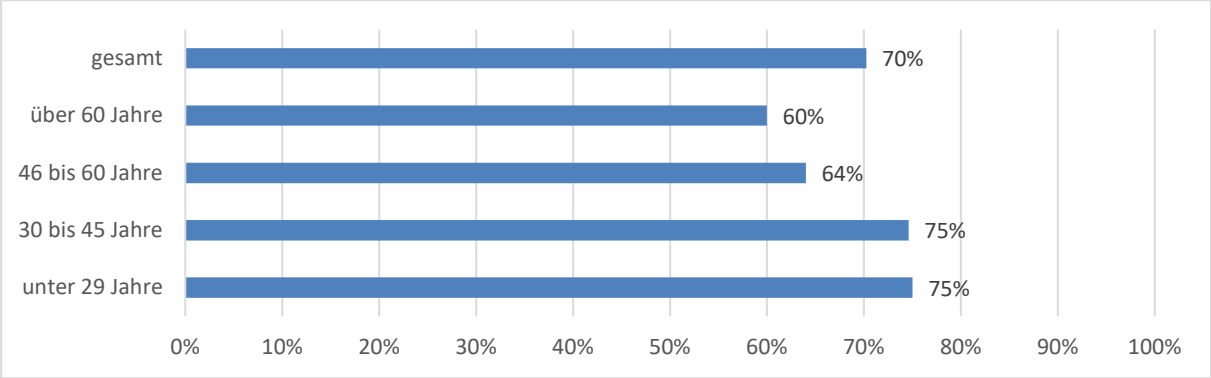

Abbildung 14 Nutzung biometrischer Verfahren zum Entsperren biometriefähiger Endgeräte nach Altersgruppen

Abbildung 15 zeigt, aus welchen Gründen wie viel Prozent der Befragten mit biometriefähigem Endgerät die biometrische Funktion zum Entsperren ihres Endgeräts benutzen. Der Hauptgrund ist, dass die Befragten die Biometrie als bequemer als PIN oder Passwort empfinden. Mehrfachnennungen waren möglich. Neben den vorgegebenen Gründen gab ein Befragter »Biometrie kann ich nicht vergessen« als Grund an.

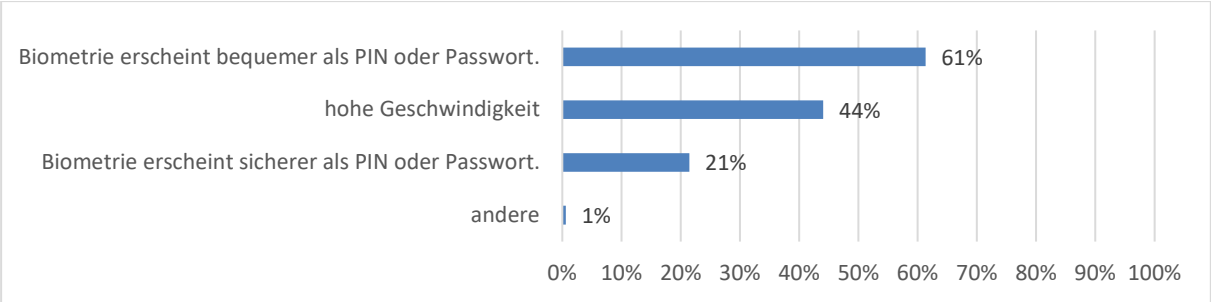

Abbildung 15 Gründe, die biometrische Funktion zum Entsperren zu benutzen

Abbildung 16 zeigt, aus welchen Gründen wie viel Prozent der Befragten mit biometriefähigem Endgerät dieses nicht biometrisch entsperren. Die Hauptgründe sind die Erfahrung, dass Biometrie nicht zuverlässig funktioniert, und Sorge vor Missbrauch der biometrischen Daten. Mehrfachnennungen waren möglich. Jeweils ein Befragter gab als Grund an

- »Angst, das Gerät nicht nutzen zu können, falls Gerät die Biometrie nicht erkennt« und
- »Vertraute Person soll mein Handy entsperren können«.

»Mein Handy sagt mir immer „Ihr Finger muss trocken sein "« wurde unter »Biometrie funktioniert nicht zuverlässig« gezählt. »Keine Datenbank ist hackersicher« wurde unter »Sorge vor Missbrauch meiner biometrischen Daten« gezählt. »Passwörter kann man ändern, Biometrie nicht« wurde unter »Sorge vor unbefugter Überwindung der biometrischen Funktion« gezählt. »PIN ist einfacher« und »zu faul, biometrisches System zu aktivieren« wurden unter »Aktivierung der Biometrie ist zu kompliziert« gezählt.

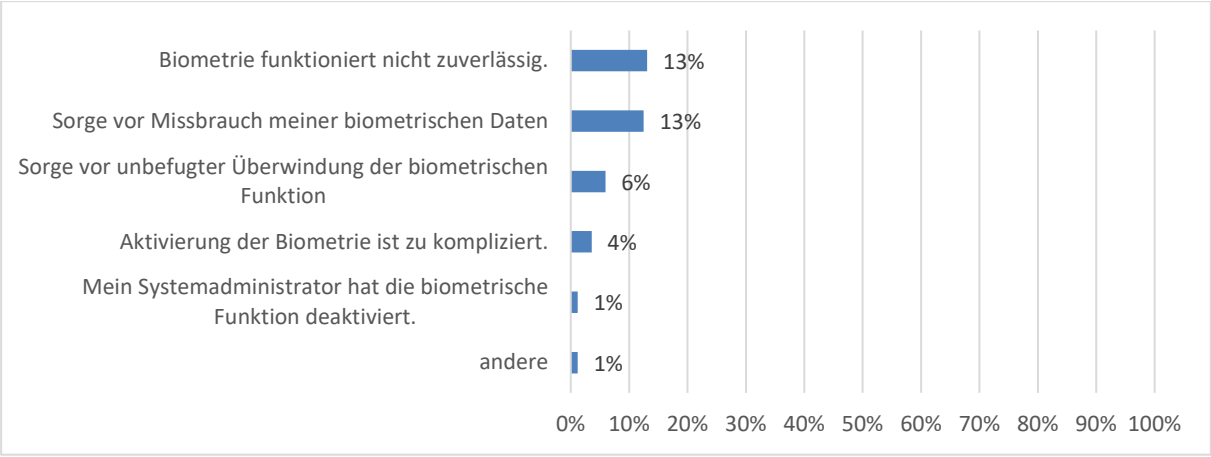

Abbildung 16 Gründe, nicht die biometrische Funktion zum Entsperren zu benutzen

3.3.8 Teilen von Fotos, die zur persönlichen Identifizierung geeignet sind

Abbildung 17 zeigt, welcher Anteil der Befragten angab, schon einmal Fotos, die ihre Identifizierung ermöglichen würden, im Internet geteilt zu haben. Nur von 30 % der Befragten enthält das Internet keine Fotos, die zur persönlichen Identifizierung geeignet sind.

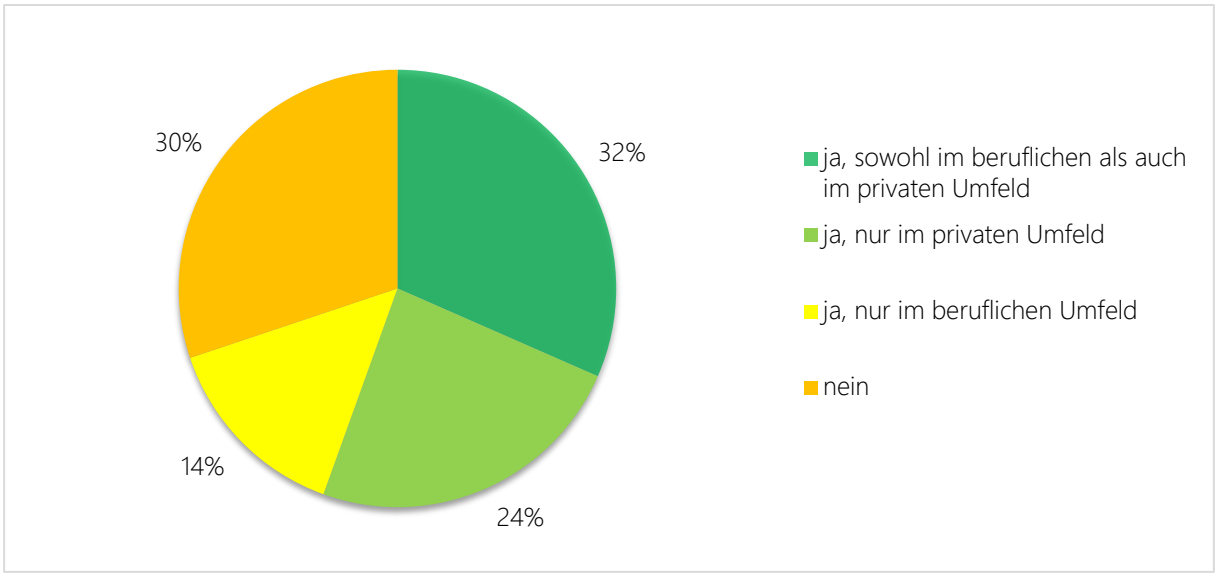

Abbildung 17 Teilen von Fotos, die zur persönlichen Identifizierung geeignet sind

3.3.9 Benutzung digitaler Sprachassistenten

Abbildung 18 zeigt, welcher Anteil der Befragten angab, einen digitalen Sprachassistenten zu benutzen. Obwohl digitale Sprachassistenten-Software in zahlreiche Smartphones integriert ist, benutzen nur 29 % der Befragten einen digitalen Sprachassistenten.

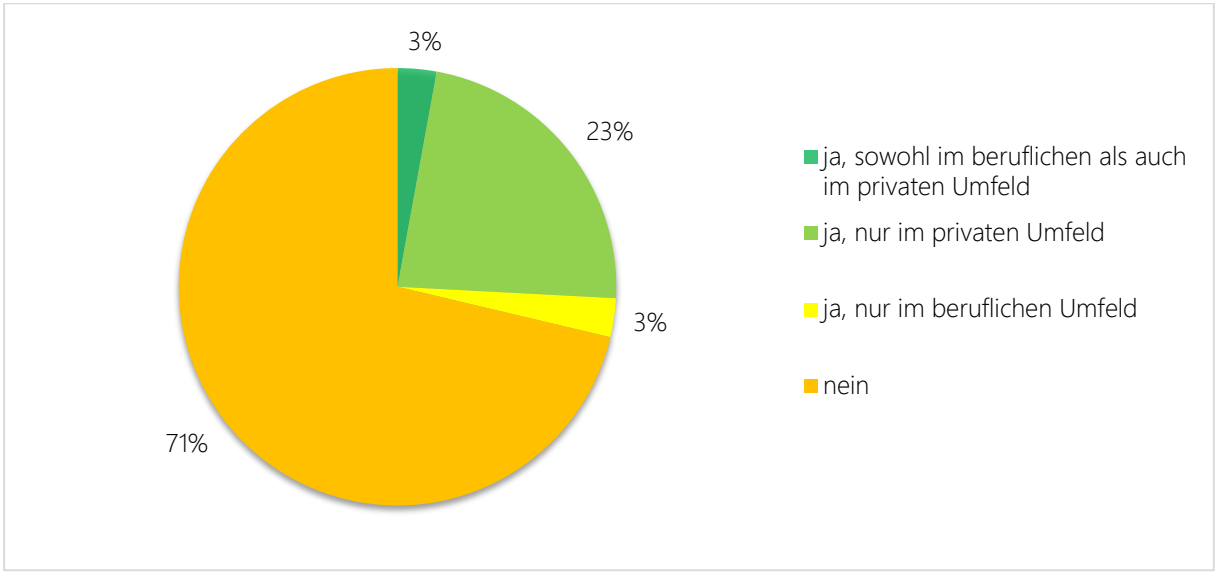

Abbildung 18 Benutzung digitaler Sprachassistenten

3.4 Wahrnehmung biometrischer Erkennungssysteme

3.4.1 Benutzerfreundlichkeit

Alle Befragten, nicht nur die, die Biometrie bisher schon nutzen, wurden nach ihrer Wahrnehmung der Benutzerfreundlichkeit und Sicherheit biometrischer Erkennungssysteme und, zum Vergleich, anderer Authentisierungsfaktoren gefragt. Abbildung 19 zeigt, welcher Anteil der Befragten jeweils angab, die angegebenen Authentisierungsfaktoren als »sehr benutzerfreundlich«, »eher benutzerfreundlich«, »wenig benutzerfreundlich« bzw. »gar nicht benutzerfreundlich« zu empfinden. Die Authentisierungsfaktoren sind nach der Häufigkeit der gefühlten Benutzerfreundlichkeit geordnet. An der Spitze steht die Fingerabdruckerkennung, vor der weit verbreiteten wissensbasierten Authentisierung mit PIN oder Passwort und der besitzbasierten Authentisierung mittels Smartphone oder Chipkarte. Fingerabdruckerkennung wird von 85 % der Befragten als sehr oder eher benutzerfreundlich empfunden. Bei den anderen biometrischen Authentisierungsfaktoren haben viele Befragte die Antwortmöglichkeit »ich weiß nicht« ausgewählt. Hier besteht ein Informations- und Erfahrungsdefizit.

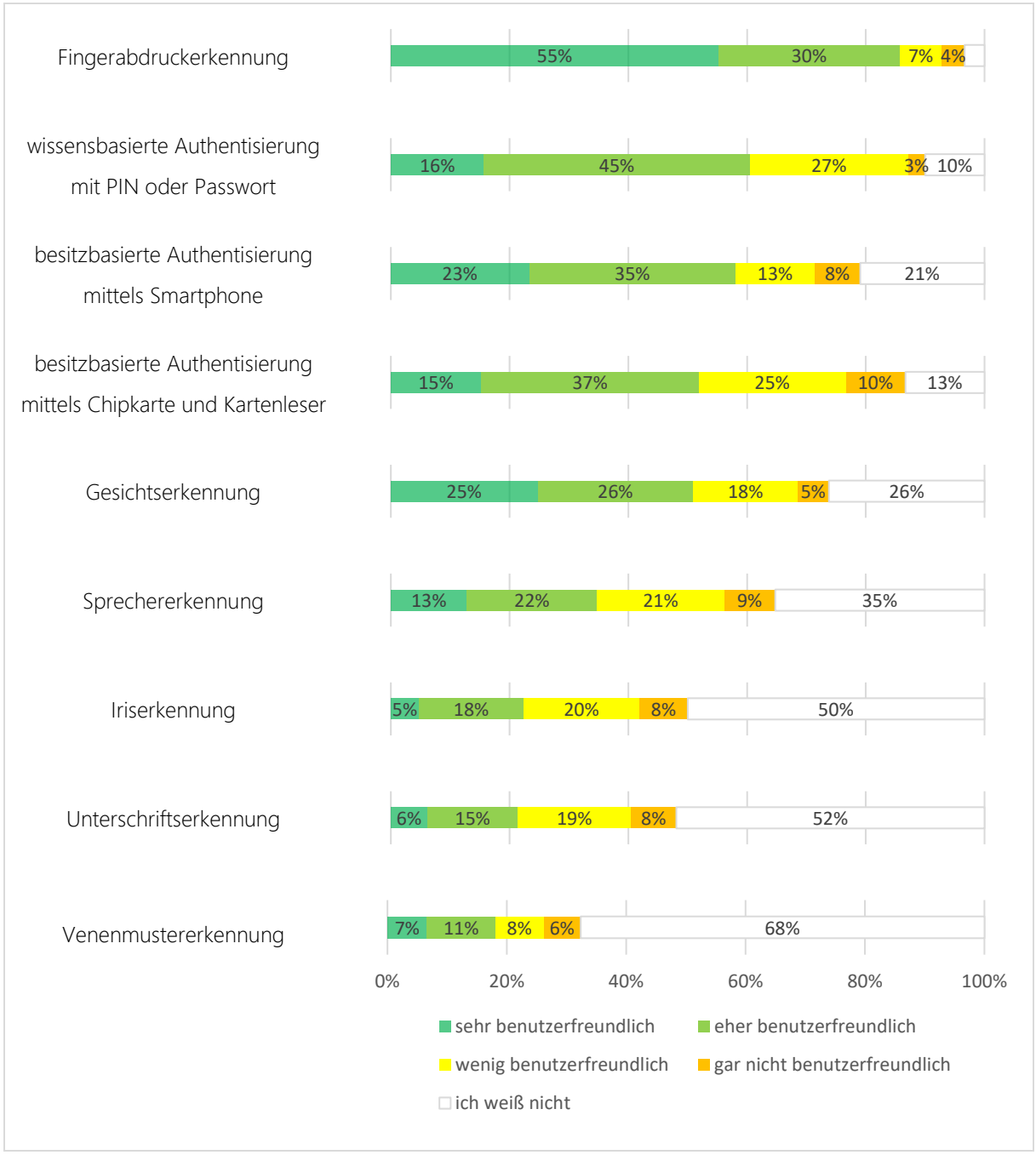

Abbildung 19 Gefühlte Benutzerfreundlichkeit von Authentisierungsfaktoren

3.4.2 Sicherheit

Abbildung 20 zeigt, welcher Anteil der Befragten jeweils angab, die angegebenen Risiken als »hoch«, »signifikant«, bzw. »gering« einzuschätzen. Die Risiken sind nach der Häufigkeit der gefühlten Bedrohung geordnet. An der Spitze steht die zweckentfremdende Nutzung biometrischer Daten, vor dem Erzwingen der biometrischen Authentisierung und der Sorge, von einer täuschend echten Imitation der biometrischen Charakteristika betroffen zu sein. Das Risiko, von einem

biometrischen Doppelgänger betroffen zu sein, wird von der Mehrheit der Befragten als gering angesehen. Es besteht also weithin Vertrauen, dass biometrische Erkennungssysteme ihren Zweck, verschiedene Personen zu unterscheiden, erfüllen können.

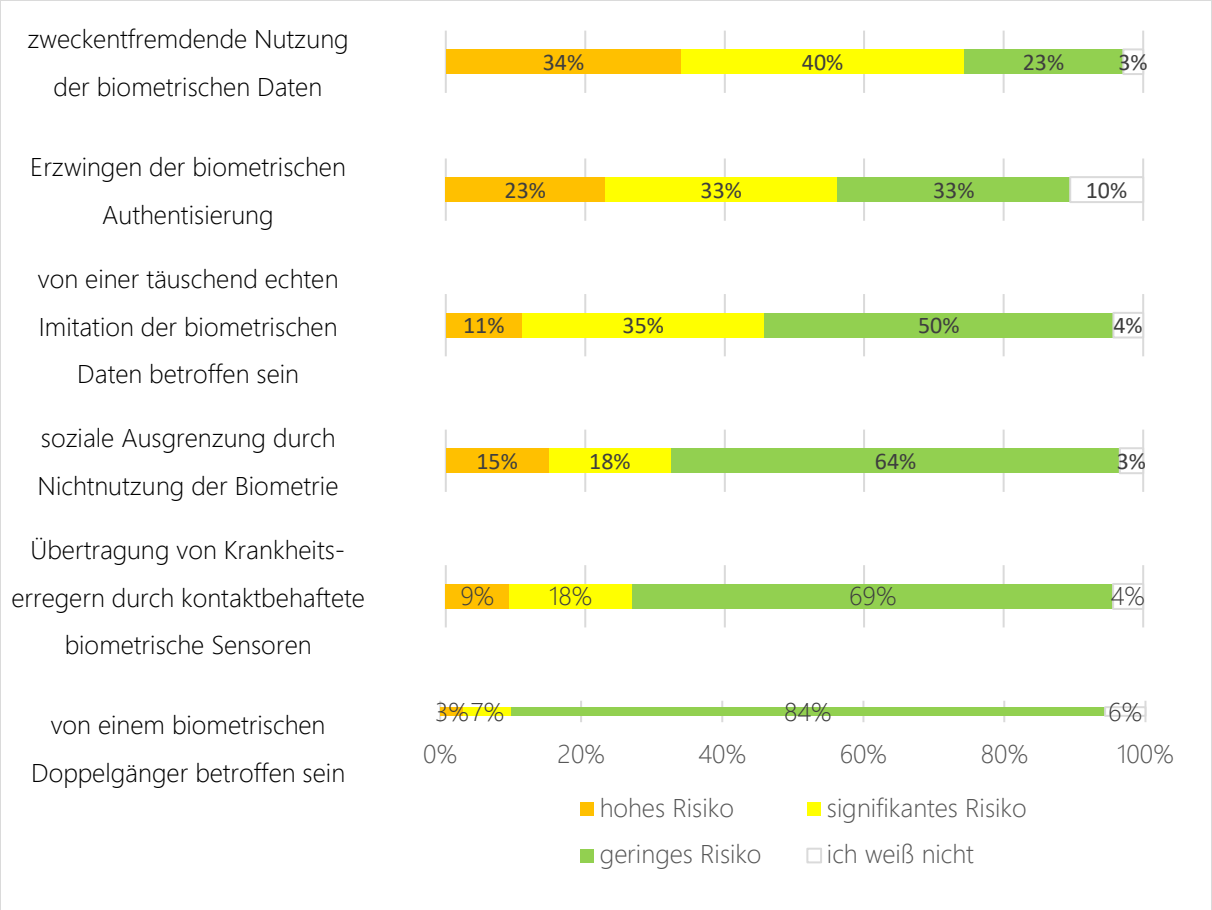

Abbildung 20 Einschätzung von Risiken

Abbildung 21 zeigt, bei welchen Formen der zweckentfremdenden Nutzung biometrischer Daten von wie viel Prozent der Befragten das Risiko besonders hoch eingeschätzt wird. Mehrfachnennungen waren möglich. Das Risiko des Diebstahls und Missbrauchs biometrischer Daten durch Kriminelle wurde am häufigsten als besonders hoch eingeschätzt. Jeweils ein Befragter gab als besonders hohes Risiko an

- »geführte Datenbanken z.B. Google-Gesichtserkennung bei privaten Fotos«,
- »Verlust der Privatsphäre durch lückenlose Überwachung (Kamera)«,
- »Racial Profiling«,
- »Biometrische Daten werden garantiert verkauft werden, egal was die Gesetzgebung vorschreibt«.

»Bei Leak der Biometriedaten in kriminelle / unbefugte Hände ist die eigene Biometrie auch für offizielle Vorgänge (etwa einen Personalausweis) verbrannt« wurde unter »Diebstahl und Missbrauch biometrischer Daten durch Kriminelle« gezählt.

Abbildung 22 zeigt, welcher Anteil der Befragten jeweils angab, die angegebenen Authentisierungsfaktoren als »sehr sicher«, »eher sicher«, »wenig sicher« bzw. »gar nicht sicher« zu empfinden. Die Authentisierungsfaktoren sind nach der Häufigkeit der gefühlten Sicherheit geordnet. Die Fingerabdruckerkennung wird nicht nur am häufigsten als sehr oder eher benutzerfreundlich eingeschätzt (siehe Abbildung 19), sondern auch am häufigsten als sehr oder eher sicher. Bei der Venenmustererkennung fällt wieder ein großes Informations- und Erfahrungsdefizit auf.

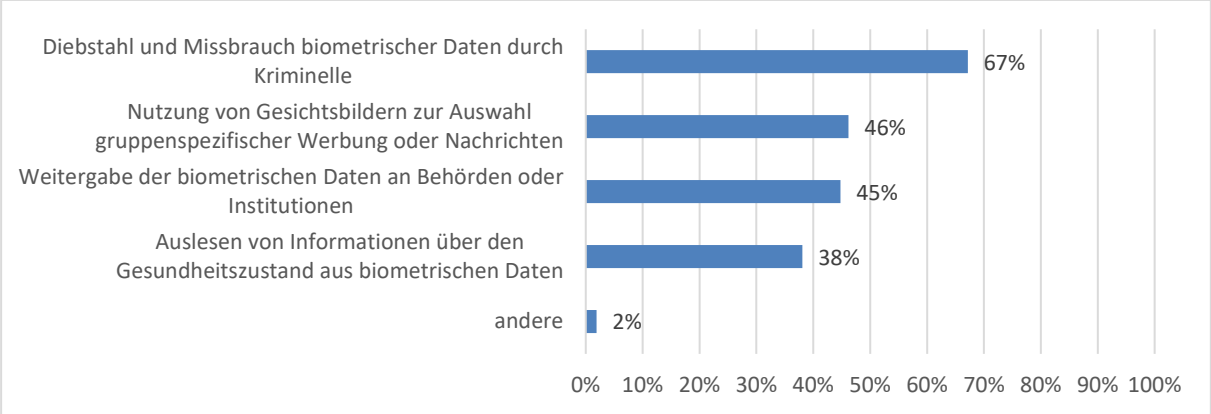

Abbildung 21 Formen der zweckentfremdenden Nutzung mit besonders hohem Risiko

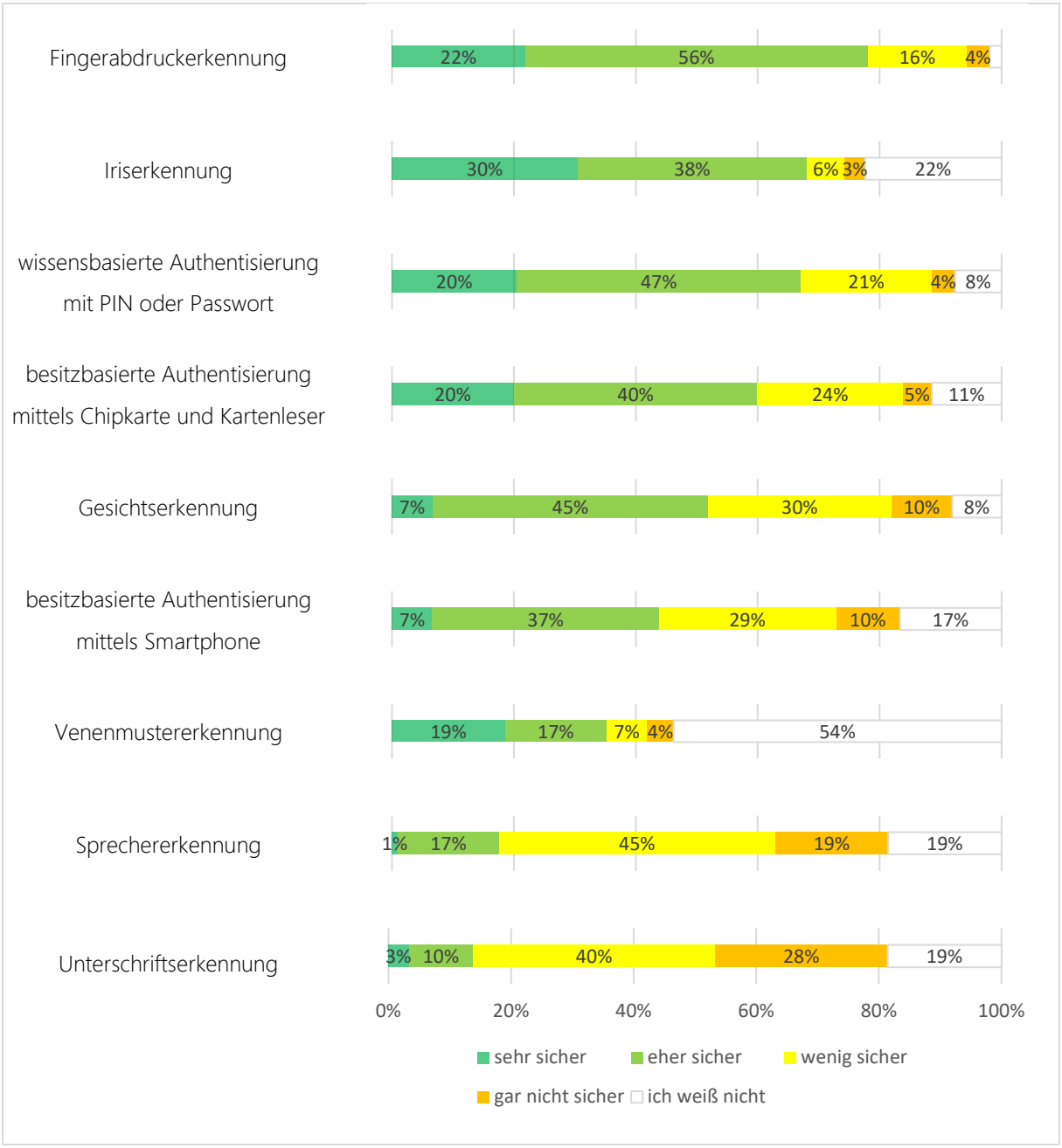

Abbildung 22 Gefühlte Sicherheit von Authentisierungsfaktoren

Abbildung 23 zeigt, welcher Anteil der Befragten jeweils angab, die Erfassung ihrer biometrischen Daten an den angegebenen Orten als »sehr sicher«, »eher sicher«, »wenig sicher« bzw. »gar nicht sicher« zu empfinden. Die Erfassung biometrischer Daten an einem Gerät unter der eigenen Kontrolle wird deutlich häufiger als sehr oder eher sicher eingeschätzt als die Erfassung an einem öffentlichen Dienstleistungssystem (z.B. Geldautomat).

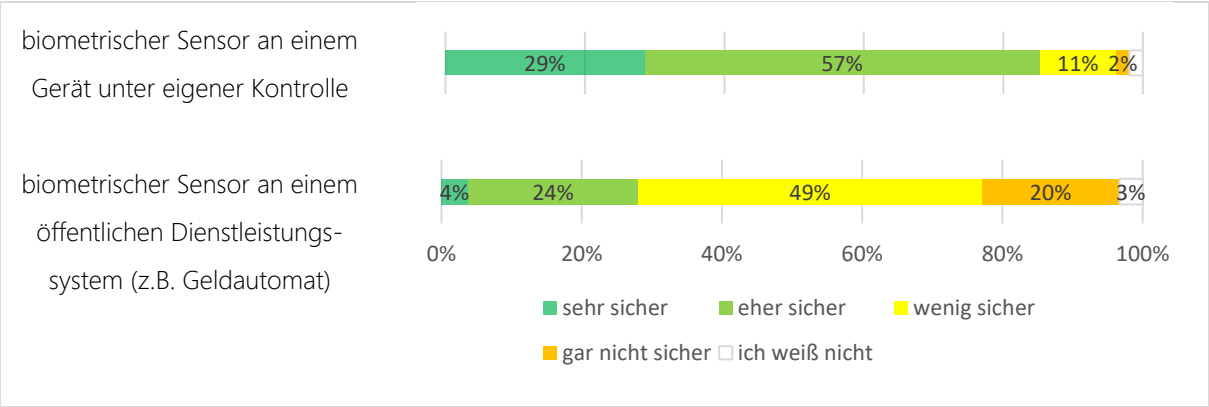

Abbildung 23 Gefühlte Sicherheit von Erfassungsorten biometrischer Daten

Abbildung 24 zeigt, welcher Anteil der Befragten jeweils angab, die Speicherung und Verarbeitung ihrer biometrischen Daten an den angegebenen Orten als »sehr sicher«, »eher sicher«, »wenig sicher« bzw. »gar nicht sicher« zu empfinden. Die Speicherung und Verarbeitung biometrischer Daten auf Hardware-Sicherheitstoken, Smartcards oder Geräten unter der eigenen Kontrolle wird deutlich häufiger als sehr oder eher sicher eingeschätzt als die Speicherung und Verarbeitung auf staatlichen oder privatwirtschaftlichen Servern in der Cloud.

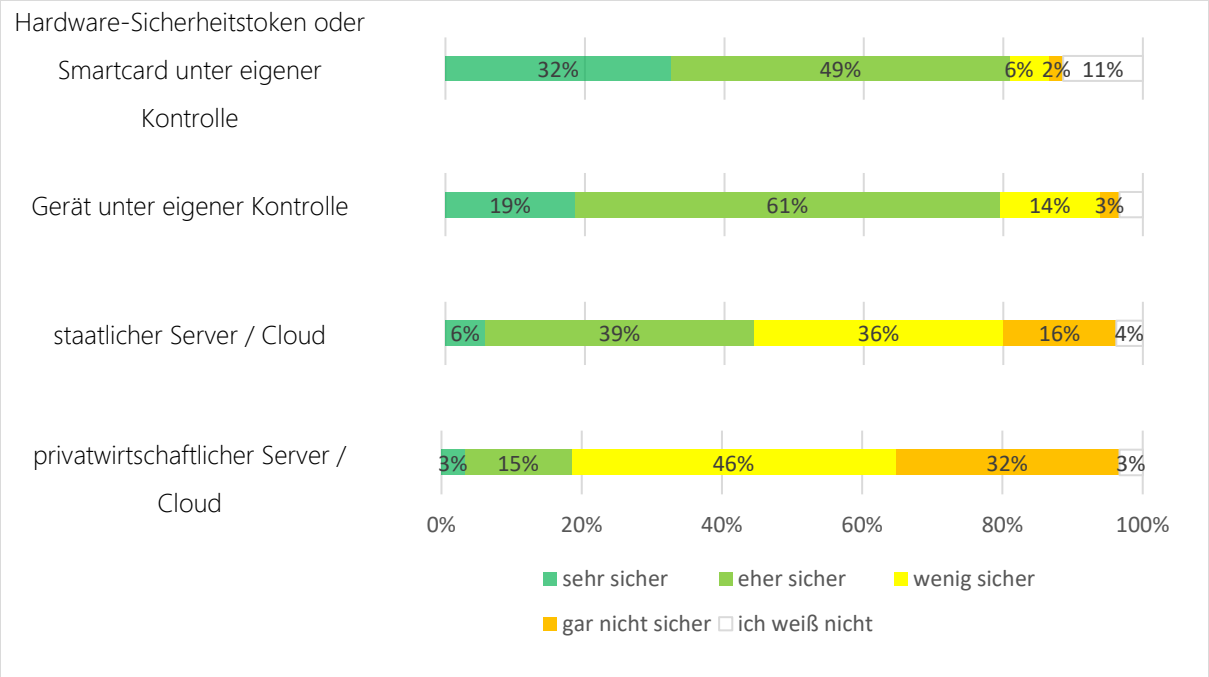

Abbildung 24 Gefühlte Sicherheit von Speicher- und Verarbeitungsorten biometrischer Daten

3.5 Bereitschaft zur zukünftigen Nutzung biometrischer Erkennungssysteme

3.5.1 Überblick

Abbildung 25 zeigt, welcher Anteil der Befragten bereit wären, für die angegebenen Vorgänge biometrische Verfahren zu benutzen, sofern sich diese als ausreichend benutzerfreundlich und sicher erweisen. Die Vorgänge sind nach der Häufigkeit der Benutzerakzeptanz geordnet. An der Spitze steht das Entsperren von Endgeräten. 83 % der Befragten wären bereit, dafür biometrische Verfahren einzusetzen. Am geringsten ist die Bereitschaft, biometrische Verfahren an Geldautomaten zur Bargeldabhebung einzusetzen.

Abbildung 25 Bereitschaft zur zukünftigen Nutzung biometrischer Erkennungssysteme

Abbildung 26 zeigt, wie häufig die Bereitschaft zum biometrischen Entsperren von Endgeräten in den Altersgruppen vorliegt. Mit zunehmendem Alter nimmt die Bereitschaft zum biometrischen Entsperren von Endgeräten signifikant ab.

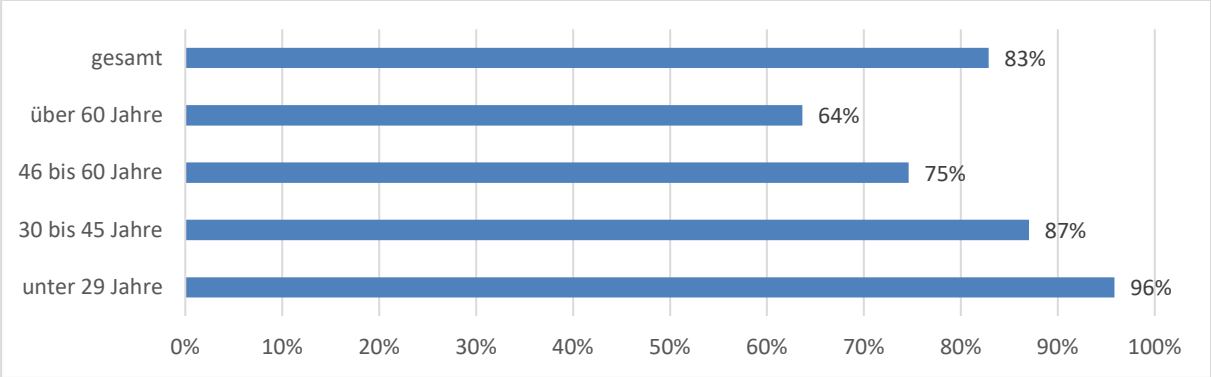

Abbildung 26 Bereitschaft zum biometrischen Entsperren von Endgeräten nach Altersgruppen

3.5.2 Entsperren und Freischalten persönlicher Endgeräte

Abbildung 28 zeigt, welche biometrischen Verfahren wie viel Prozent der Befragten bereit wären, zum Entsperren persönlicher Endgeräte oder zum Freischalten der Endgeräte für die Authentisierung im Internet zu benutzen. Mehrfachnennungen waren möglich. Am häufigsten wurde die Fingerabdruckerkennung gewählt. Sie findet Akzeptanz bei 80 % der Befragten. Neben den vorgegebenen Verfahren gab jeweils einer der Befragten an, bereit zu sein, auf persönlichen Endgeräten »Cardio-Biometrics oder Retina« und eine »Kombination aus mehreren Verfahren« einzusetzen.

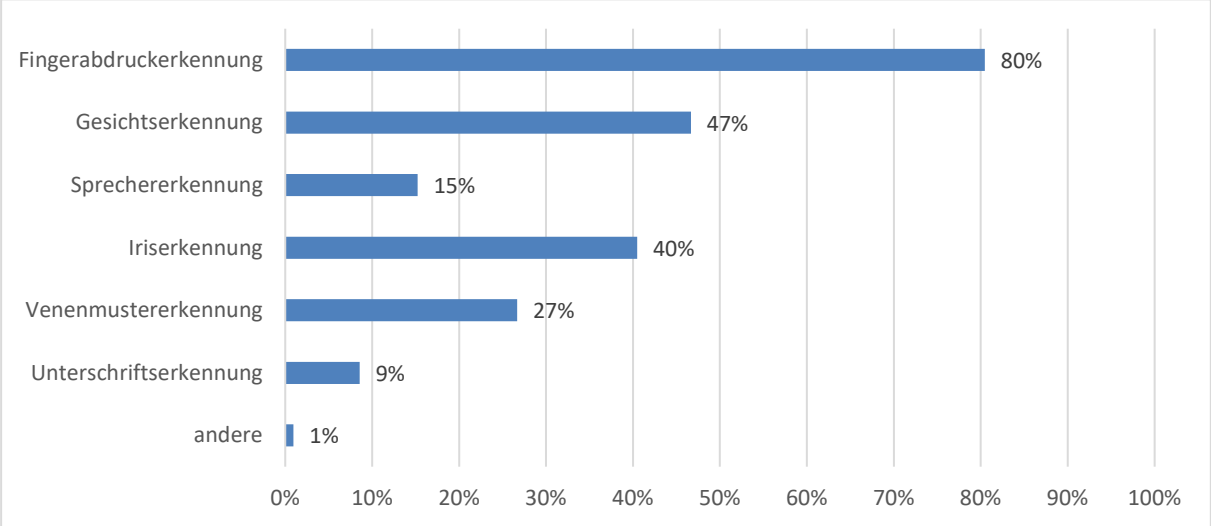

Abbildung 27 Bereitschaft zur Nutzung biometrischer Verfahren auf Endgeräten

3.5.3 Zugangskontrolle zu Räumen oder Gebäuden

Abbildung 28 zeigt, welche biometrischen Verfahren wie viel Prozent der Befragten bereit wären, bei der Zugangskontrolle zu Räumen oder Gebäuden zu benutzen. Mehrfachnennungen waren möglich. Neben den vorgegebenen Verfahren gab einer der Befragten an, bereit zu sein, bei der Zugangskontrolle zu Räumen oder Gebäuden eine »Kombination aus mehreren Verfahren« einzusetzen.

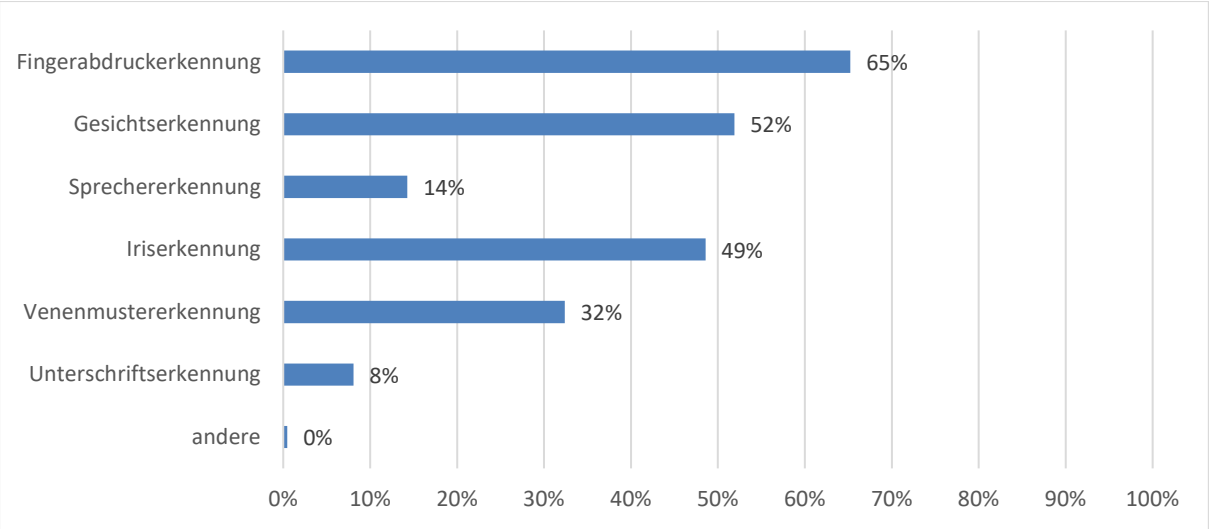

Abbildung 28 Bereitschaft zur Nutzung biometrischer Verfahren bei der Zugangskontrolle zu Räumen oder Gebäuden

3.5.4 Arbeitszeiterfassung

Abbildung 29 zeigt, welche biometrischen Verfahren wie viel Prozent der Befragten bereit wären, bei der Arbeitszeiterfassung zu benutzen. Mehrfachnennungen waren möglich. Neben den vorgegebenen Verfahren gab einer der Befragten an, bereit zu sein, bei der Arbeitszeiterfassung eine »Kombination aus mehreren Verfahren« einzusetzen.

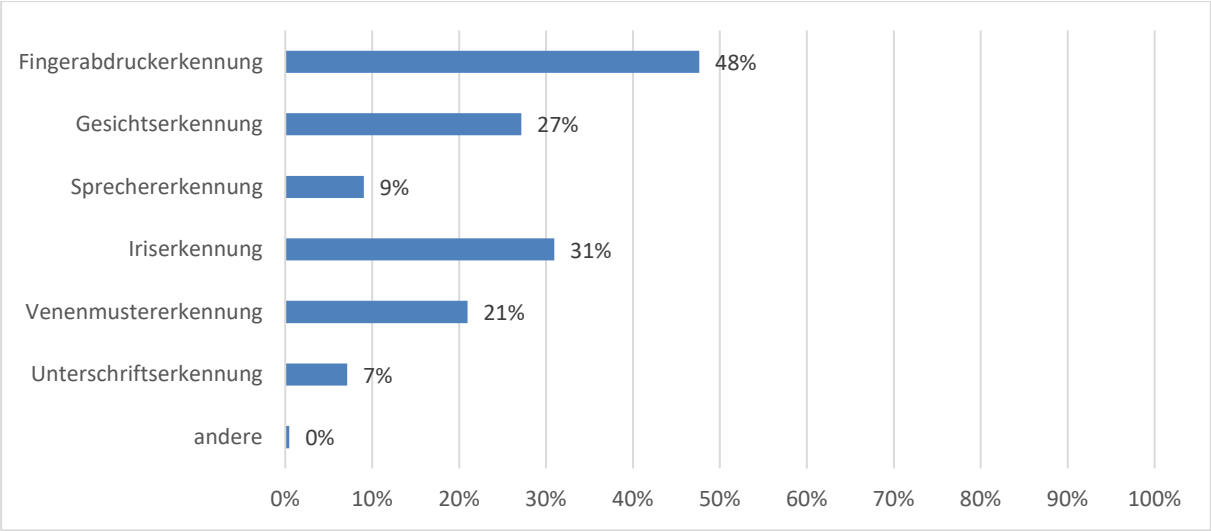

Abbildung 29 Bereitschaft zur Nutzung biometrischer Verfahren zur Arbeitszeiterfassung

3.5.5 Freischalten von Sicherheitstoken oder Smartcards

Abbildung 30 zeigt, welche biometrischen Verfahren wie viel Prozent der Befragten bereit wären, zum Freischalten von Sicherheitstoken oder Smartcards zu benutzen. Mehrfachnennungen waren möglich. Neben den vorgegebenen Verfahren gab jeweils einer der Befragten an, bereit zu sein, »Cardio-Biometrics oder Retina« und eine »Kombination aus mehreren Verfahren« einzusetzen.

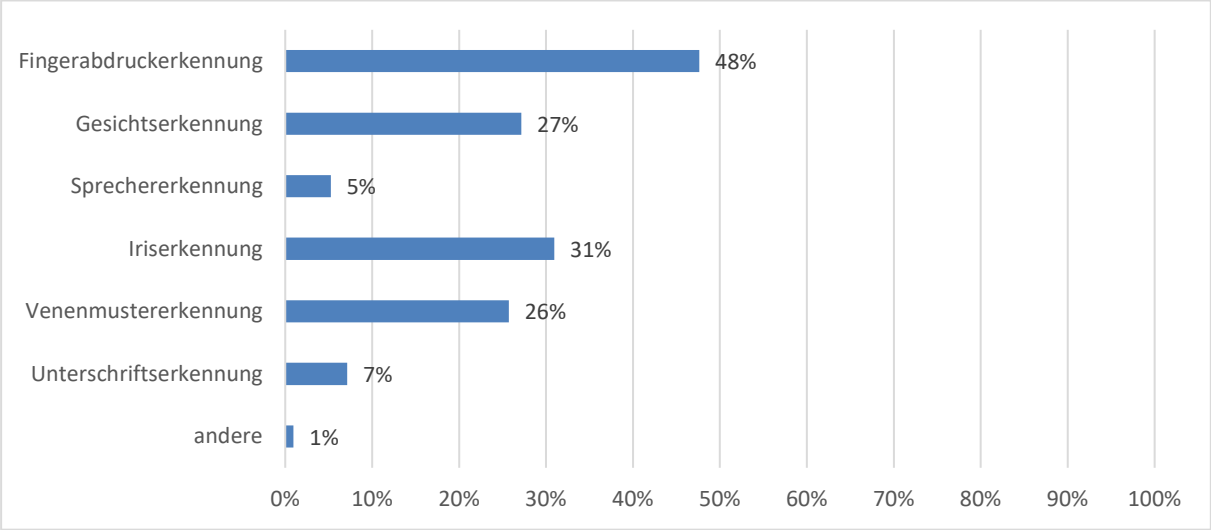

Abbildung 30 Bereitschaft zur Nutzung biometrischer Verfahren zum Freischalten von Sicherheitstoken oder Smartcards

3.5.6 Online-Banking

Abbildung 31 zeigt, welche biometrischen Verfahren wie viel Prozent der Befragten bereit wären, beim Online-Banking zu benutzen. Mehrfachnennungen waren möglich. Neben den vorgegebenen biometrischen Verfahren gab jeweils einer der Befragten an, bereit zu sein, beim Online-Banking »Cardio-Biometrics« bzw. eine »Kombination aus Fingerabdruck und wissensbasierter PIN« einzusetzen.

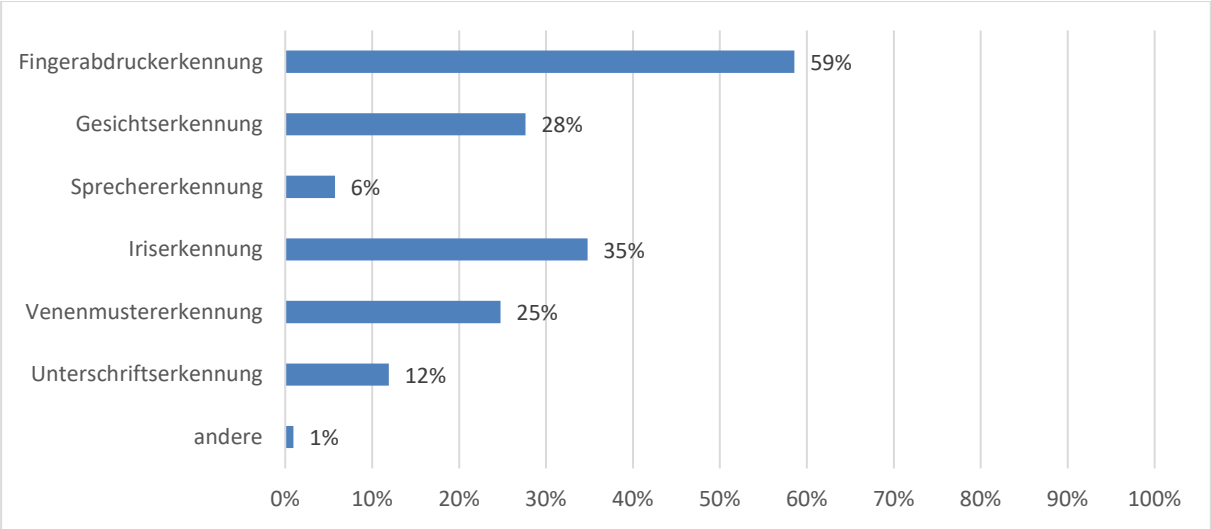

Abbildung 31 Bereitschaft zur Nutzung biometrischer Verfahren beim Online-Banking

3.5.7 Bargeldloses Bezahlen und Bargeldabhebung am Geldautomaten

Abbildung 32 zeigt, welche biometrischen Verfahren wie viel Prozent der Befragten bereit wären, beim bargeldlosen Bezahlen oder bei der Bargeldabhebung am Geldautomaten zu benutzen. Mehrfachnennungen waren möglich. Einer der Befragten wies darauf hin, nur beim bargeldlosen Bezahlen, nicht jedoch am Geldautomaten bereit zu sein, Fingerabdruckerkennung zu benutzen.

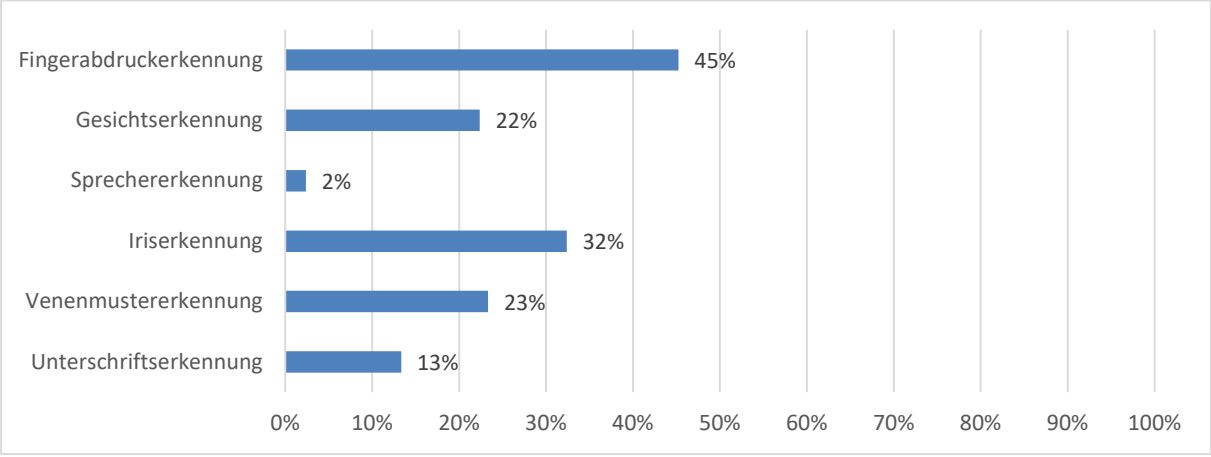

Abbildung 32 Bereitschaft zur Nutzung biometrischer Verfahren am Geldautomaten oder beim bargeldlosen Bezahlen

3.5.8 Verarbeitung des Gesichtsbilds

Abbildung 33 zeigt, welcher Anteil der Befragten in die Verarbeitung ihres Gesichtsbilds zu den angegebenen Zwecken einwilligen würde. Die große Mehrheit der Befragten lehnt die Verarbeitung von Gesichtsbildern zwecks Auswahl gruppenspezifischer Werbung oder Nachrichten (z.B. angepasst an Alter und Geschlecht), zwecks Gesichtserkennung im Internet und zwecks Wiedererkennung von Stammkunden ab.

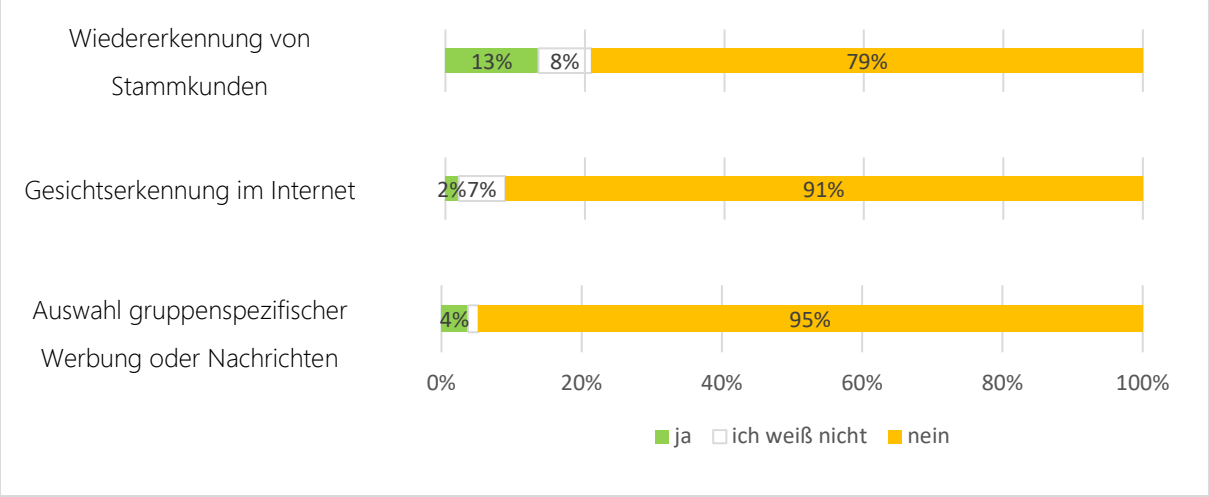

Abbildung 33 Bereitschaft zur Einwilligung in die Verarbeitung des Gesichtsbilds

3.6 Anmerkungen und Anregungen der Befragten

27 Befragte hinterließen Anmerkungen und Anregungen. Die Anmerkungen und Anregungen können den folgenden Kategorien zugeordnet werden:

- Zustimmung zu biometrischen Erkennungssystemen
  - »Biometrische Erkennungssysteme sind ein absolutes Muss, gerade in Verbindung mit Digitalisierung und den neuen Arbeitswelten, wie z.B. Home Office oder dem Sichern von Daten, die für Unternehmen überlebenswichtig sind.«
- Verbesserungsvorschläge
  - »Bestimmt in Kombination mit bestehenden Erkennungssystemen (4-Augen-Prinzip) sehr sicher«

- »Jedes System kann geknackt werden. Die PIN im Kopf + biometrische Daten halte ich für eine gute Kombi. Sich in sensiblen Bereichen allein auf biometrische Daten zu beziehen, ermöglicht Undenkbares – gefährlich in sämtlichen Gesellschaftssystemen von unterschiedlichen Kräften. Schaut mal Sciencefiction und Krimis. Die Ideen sind technisch möglich: Finger abtrennen… Traurig, dass Deutschland die Software für Gesichtserkennung im öffentlichen Raum an China geliefert hat. So zumindest Nachrichten, die ich gehört habe. Davon unberührt: Forschung sollte weitergehen.«
- »Lokale Geräte, die die biometrischen Daten nie herausgeben (zum Beispiel Abgleich mit einer Smartcard, die ich selbst initialisieren kann): gut. Lokale Geräte, die extern initialisiert werden (z.B. Personalausweis): schlecht. Remote Geräte, die biometrische Daten verarbeiten: schlecht.«
- »Bei aller Technik-Skepsis ist die Sicherheit keine absolute Frage, sondern immer in Relation zu anderen, auch wissensbasierten Verfahren, die dann ggf. "Social Hacking"-anfällig sind, zu sehen. Daher glaube ich, dass die Biometrie ein praktischer Sicherheitsgewinn ist. Der Einsatz wird nur unnötig durch Inkompatibilitäten auf technischer Seite erschwert und Verunsicherung bleibt durch die Gesetzgebung unbeachtet (->Beweislast).«
- »Bei den sicherheitsrelevanteren Authentifizierungen sollten die biometrischen Verfahren immer mit einer 2-Faktor-Authentifizierung erfolgen (Biometrie-Biometrie oder Biometrie-Haben/Wissen). Dazu empfehle ich zentrale Speicherungen so weit wie möglich zu vermeiden und biometrische Templates sollten immer verschlüsselt sein.«
- »Man sollte nicht vergessen, dass es auch Leute ohne Smartphone gibt.«
- »Benutzerfreundlich, aber unsicher. Daher sollte der Anwendungsfall entsprechend sein.«
- »Biometrische Erkennungssysteme sind zwar durchaus innovativ und praktisch, bergen jedoch auch Risiken, die viele nicht bereit sind einzugehen. Letztendlich sollte es eine freiwillige Alternative bleiben und nicht als einzige Variante eingeführt werden«
- »Standardisierung ist extrem wichtig; das Thema Überwindungssicherheit wird noch nicht ausreichend berücksichtigt.«
- »Letztlich spielt die Sicherheit meiner erfassten Daten die entscheidende Rolle. D.h., Daten dürfen nicht rückverfolgbar sein (Bewegungsmuster etc.)«
- »Ich benutze Gesichtserkennung hauptsächlich mit Smartphone, und da gibt es Unstimmigkeiten. Das Handy bleibt entsperrt, wenn ich es einstecke, und fängt dann an zu telefonieren, schaltet das Licht ein, fotografiert in der Tasche rum … Das Verfahren steckt imho noch in den Kinderschuhen.«
- »Darf nicht obligatorisch sein. Generell kann es immer Diebstahl von biometrischen Daten geben. Ähnlich wie quasi alle Passwörter irgendwann gestohlen werden, wird das auch bei

biometrischen Daten auf Servern sein. Anders als Passwörter kann man diese aber nicht ändern. Wer darauf sein Sicherheitssystem begründet, sollte sich der Verantwortung bewusst sein, dass jederzeit Unbefugte darauf zugreifen können und dass Biometrie keine Belegkraft hat (nur weil ein Fingerabdruck erkannt wurde, steht nicht fest, dass es sich um die korrekte Person handelt), sondern einfach als zusätzliche Hürde zu verstehen ist.«

- Ablehnung biometrischer Erkennungssysteme
  - »Bei der Gesichtserkennung wird man zum gläsernen Menschen. Die Daten können überall gespeichert werden und man hat keinerlei Kontrolle darüber. Man ist leichter zu identifizieren, da selbst in beruflichen Netzwerken das eigene Bild hochgeladen wird. Bei der Google-Gesichtserkennung ist es sogar schon möglich, Verwandte zu identifizieren.«
  - »In was für einer Gesellschaft wollen wir leben? Welche Datenspuren beengen ein Leben in Freiheit vor Verfolgung, Diskriminierung und Commerzzwängen?«
  - »Es ist völliger Wahnsinn, nicht änderbare biologische Kennzeichen als Passwörter in einem grundsätzlich unsicherbaren System wie dem Internet zu verwenden. Diese ganze Idee ist bescheuert und zeugt vor allem von Kurzzeitdenken gieriger US-Firmen, überwachungsgeiler gieriger chinesischer Faschisten, und Universitätsstudenten die genau ein Semester weit in die Zukunft schauen. Aber die kosmetische Chirurgie wird es freuen, zumal die dann erforderlichen Gesichtsstrukturveränderungen richtig aufwändig und daher teuer werden. Da heißt, ein Hack irgendeines mangelhaft aufgebauten Webshops, wo man biometrisch bezahlt hat, heißt nicht, dass man sich ein neues Passwort überlegen muss, sondern dass man ein neues Gesicht braucht. Oder eine neue Handfläche. Oder neue Augen. Definitives Zukunftspotential!«
  - »Vier Fragen und Forderungen sind mindestens zu stellen / zu erfüllen: 1. Die Systeme müssen 100% sicher sein – Gesichtserkennung kann zur Zeit nicht 100% sicher sein. 2. Rechtfertigt der technische Aufwand den Einsatz, wo doch ein sicheres Password alle Anforderungen erfüllt und nur das Gedächtnis des Nutzers strapaziert. 3. Bei flächendeckendem Einsatz ist die Überwachung des Individuums (Gesichtserkennung) vollkommen. Die Atombombe sollte es auch nicht geben. Die Ausrede Terrorismus zählt nicht. 4. Wozu noch mehr störanfällige Technik – Software hat immer Fehler!!!! Ich könnte sehr viele Störfälle – auch kurz zurückliegende aufzählen.«
  - »Sind gefährlich, aber in der Zukunft werden wir keine andere Wahl haben. Leider.«
  - »Kritische Sicht, da 1. wesentlich größere Kontrollmöglichkeiten 2. wesentlich größere Auswertungsmöglichkeiten 3. schleichender Verlust der Fähigkeit, abstrakte Zahlen-/Buchstabenkombinationen zu generieren bzw. sich zu merken 4. Verlust von Unabhängigkeit«

- »Ich bin gegen den digitalen Faschismus und möchte, dass allen Menschen Möglichkeiten der Partizipation geboten werden, egal, über welche technischen Mittel sie verfügen.«
- »Ich finde die Vorstellung gruselig, dass an allen möglichen Stellen und von allen möglichen Institutionen / Unternehmen eine Vielzahl meiner biometrischen Daten gesammelt und ausgewertet wird. Diese Daten gehen m.E. keinen etwas an. In welcher Art man biometrische Daten heute auswerten kann, weiß ich nicht. Die Auswertungsmöglichkeiten ändern sich in Zukunft ganz sicher in Richtung mehr, spezifischer, schneller… Um so weniger kann ich mir vorstellen, was wer wozu alles mit den Daten machen kann. Daher würde ich so weit wie möglich auf biometrische Erkennungssysteme verzichten.«
- »George Orwells düstere Zukunftsvisionen werden durch biometrische Erkennungssysteme noch übertroffen, siehe Chinas verabscheuungswürdiges Sozialkreditsystem.«
- »Meiner Sicht nach haben alle biometrischen Erkennungsverfahren ein großes Problem. Sobald sie einmal geklaut wurden, sei es durch einen Fingerabdruck auf einer Glasscheibe oder ein IR-Foto der Iris mit einem Zoom-Objektiv, sind diese "Features" verbrannt! Das Schlimme daran ist, man kann sie nicht ändern!! Was wiederum bedeutet, biometrische Features, die irgendwie fälschbar sind, sind stets ungeeignet.«

- Anmerkungen zur Befragung:

  - »Interessante Umfrage. Regt zum Nachdenken an!«
  - »Wieso fragen Sie nicht nach Verhaltensbiometrie? Tippverhalten, bzw. am Smartphone auch Gerätehaltung, Wischverhalten, Druck, …? Außerdem eine Anmerkung zur Umfrage: Ich glaube, dass Sie mit der gewählten Sprache den Normal-Verbraucher oft nicht erreichen. Viel zu technische Ausdrücke. "Wissensbasierte Authentisierung"? "Mobiles oder stationäres Endgerät mit integrierten Sensoren"? Unterschied zwischen "Entsperren von Geräten" und "Freischalten des Smartphones zur Authentisierung im Internet"? Ich weiß (oder ahne), was Sie meinen, weil ich beruflich damit zu tun habe, aber meine Eltern (Studierte) oder meine Tochter (Gymnasium Oberstufe) ver-stehen das trotz überdurchschnittlich hoher Bildung nicht.«
  - »Diese Umfrage zeigt (auf Macintosh, Firefox) die Auswahlen nicht immer an. Bei Popups gibt es auch mal Pixelsalat.«
  - »Die Kombination macht es aus. Es ist nicht „entweder oder " sondern „und ". Daher empfand ich die Antwortmöglichkeiten etwas starr.«
  - »Es wäre hilfreich gewesen, wenn am Anfang die verschiedenen Prozesse mit dem jeweiligen aktuellen Entwicklungsstand und Sicherheitsstand vorgestellt worden wären. So konnte ich mich leider nur auf die beiden Prozesse beziehen, die ich kenne (Fingerabdruck und

Gesichtserkennung). Generell finde ich vieles davon praktisch und bin gespannt auf weitere Entwicklungen in dem Bereich.«

4 Stand der Normung biometrischer Technologien

4.1 Einführung

Normen sind erforderlich, wenn Komponenten verschiedener Hersteller interagieren sollen. Wenn alle Komponenten eines biometrischen Systems aus einer Hand stammen, kann Interoperabilität zwischen den Komponenten auch ohne Normung erreicht werden. Normen sorgen jedoch nicht nur für Interoperabilität, sie spezifizieren auch weitergehende Anforderungen z.B. zur Betriebssicherheit von Produkten, zu Datenschutz und Datensicherheit sowie zur Mensch-Maschine-Schnittstelle.

Die folgenden Abschnitte geben einen Überblick über relevante internationale und europäische Normungsgremien und ihre Projekte mit Bezug zur Biometrie aber auch über relevante Industriestandards.

4.2 ISO/IEC JTC 1/SC 17 – Cards and Security Devices for Personal Identification

Der Aufgabenbereich von ISO/IEC JTC 1/SC 17 ist die Normung im Bereich der Karten und Geräte für die persönliche Identifizierung. Die folgenden von ISO/IEC JTC 1/SC 17 entwickelten internationalen Normen und Technischen Berichte (Technical Reports, TRs) mit Bezug zur Biometrie sind in Kraft bzw. befinden sich derzeit in der Überarbeitung:

- ISO/IEC 7816-11:2017, Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods [60]
- ISO/IEC 11694-6:2014, Identification cards – Optical memory cards – Linear recording method – Part 6: Use of biometrics on an optical memory card
- ISO/IEC 17839, Information technology – Biometric System-on-Card
  - ISO/IEC 17839-1:2014, ~ – Part 1: Core requirements [61]
  - ISO/IEC 17839-2:2015, ~ – Part 2: Physical characteristics [62]
  - ISO/IEC 17839-3:2016, ~ – Part 3: Logical information interchange mechanism [63]
- ISO/IEC 18584:2015, Information technology – Identification cards – Conformance test requirements for on-card biometric comparison applications
- ISO/IEC 24787:2018, Information technology – Identification cards – On-card biometric comparison [64]
- ISO/IEC TR 30117:2014, Information technology – Guide to on-card biometric comparison standards and applications

Darüber hinaus entwickelte ISO/IEC JTC 1/SC 17/WG 3 den ICAO TR »Portrait Quality«. Die für das Aufnehmen von Passbildern relevanten Abschnitte daraus wurden von ISO/IEC JTC 1/SC 37 in ISO/IEC 39794-5:2019 aufgenommen.

4.3 ISO/IEC JTC 1/SC 27 – Information Security, Cybersecurity and Privacy Protection

Der Aufgabenbereich von ISO/IEC JTC 1/SC 27 ist die Entwicklung von Normen für Datensicherheit und Datenschutz und für sichere Informations- und Kommunikationstechnologien. Die folgenden von ISO/IEC JTC 1/SC 27 entwickelten internationalen Normen und Technischen Berichte mit Bezug zur Biometrie sind in Kraft bzw. werden derzeit entwickelt:

- ISO/IEC 17922:2017, Information technology – Security techniques – Telebiometric authentication framework using biometric hardware security module
- ISO/IEC 19792:2009, Information technology – Security techniques – Security evaluation of biometrics
- ISO/IEC 19989, Information security – Criteria and methodology for security evaluation of biometric systems
  - ISO/IEC 19989-1:2020, ~ – Part 1: Framework
  - ISO/IEC 19989-2:2020, ~ – Part 2: Biometric recognition performance
  - ISO/IEC 19989-3:2020, ~ – Part 3: Presentation attack detection
- ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection [65]
- ISO/IEC 24761:2019, Information technology – Security techniques – Authentication context for biometrics
- ISO/IEC 27553, Information technology – Security techniques – Security requirements for authentication using biometrics on mobile devices

4.4 ISO/IEC JTC 1/SC 37 – Biometrics

Der Aufgabenbereich von ISO/IEC JTC 1/SC 37 ist die Normung generischer biometrischer Technologien für die Erkennung von Menschen. Außerhalb des Aufgabenbereichs von ISO/IEC JTC 1/SC 37 sind die Arbeiten in ISO/IEC JTC 1/SC 17 zur Anwendung biometrischer Technologien auf Karten und Geräte für die persönlichen Identifizierung sowie die Arbeiten in ISO/IEC JTC 1/SC 27 zu

Sicherheitsaspekten und Sicherheitsbewertung biometrischer Erkennungssysteme. Die folgenden von ISO/IEC JTC 1/SC 37 entwickelten internationalen Normen und Technischen Berichte zu den Themengebieten

- harmonisiertes biometrisches Vokabular,
- biometrische technische Schnittstellen,
- biometrische Datenaustauschformate,
- technische Implementierung biometrischer Systeme,
- biometrische Tests und Testberichte sowie
- rechtliche und gesellschaftliche Aspekte der Biometrie

sind in Kraft bzw. werden derzeit entwickelt:

- ISO/IEC 2382-37:2017, Information technology – Vocabulary – Part 37: Biometrics
- ISO/IEC 5152, Biometric performance estimation methodologies using statistical model
- ISO/IEC 19784, Information technology – Biometric application programming interface
  - ISO/IEC 19784-1:2018, ~ – Part 1: BioAPI specification
  - ISO/IEC 19784-2:2007, ~ – Part 2: Biometric archive function provider interface
  - ISO/IEC 19784-4:2011, ~ – Part 4: Biometric sensor function provider interface
- ISO/IEC 19785, Information technology – Common Biometric Exchange Formats Framework
  - ISO/IEC 19785-1:2020, ~ – Part 1: Data element specification
  - ISO/IEC 19785-2:2006, ~ – Part 2: Procedures for the operation of the Biometric Registration Authority
  - ISO/IEC 19785-3:2020, ~ – Part 3: Patron format specifications
  - ISO/IEC 19785-4:2010, ~ – Part 4: Security block format specifications
- ISO/IEC 19794, Information technology – Biometric data interchange formats[1]
  - ISO/IEC 19794-1:2006, ~ – Part 1: Framework. First edition
  - ISO/IEC 19794-1:2011, ~ – Part 1: Framework. Second edition

[1] Für die Teile 1, 2, 4, 5, 6, 7, 8 und 9 von ISO/IEC 19794 werden ausnahmsweise die ersten Auflagen auch nach der Veröffentlichung der zweiten Auflagen im Normenkatalog beibehalten, da die in diesen ersten Auflagen definierten biometrischen Datenaustauschformate im Einsatz sind (z.B. in elektronischen Reisepässen) und nicht alle diese Formate in den zweiten Ausgaben beibehalten wurden.

- ISO/IEC 19794-2:2005, ~ – Part 2: Finger minutiae data. First edition
- ISO/IEC 19794-2:2011, ~ – Part 2: Finger minutiae data. Second edition
- ISO/IEC 19794-3:2006, ~ – Part 3: Finger pattern spectral data
- ISO/IEC 19794-4:2005, ~ – Part 4: Finger image data. First edition
- ISO/IEC 19794-4:2011, ~ – Part 4: Finger image data. Second edition
- ISO/IEC 19794-5:2005, ~ – Part 5: Face image data. First edition
- ISO/IEC 19794-5:2011, ~ – Part 5: Face image data. Second edition
- ISO/IEC 19794-6:2005, ~ – Part 6: Iris image data. First edition
- ISO/IEC 19794-6:2011, ~ – Part 6: Iris image data. Second edition
- ISO/IEC 19794-7:2007, ~ – Part 7: Signature/sign time series data. First edition
- ISO/IEC 19794-7:2014, ~ – Part 7: Signature/sign time series data. Second edition
- ISO/IEC 19794-8:2006, ~ – Part 8: Finger pattern skeletal data. First edition
- ISO/IEC 19794-8:2011, ~ – Part 8: Finger pattern skeletal data. Second edition
- ISO/IEC 19794-9:2007, ~ – Part 9: Vascular image data. First edition
- ISO/IEC 19794-9:2011, ~ – Part 9: Vascular image data. Second edition
- ISO/IEC 19794-10:2007, ~ – Part 10: Hand geometry silhouette data
- ISO/IEC 19794-11:2013, ~ – Part 11: Signature/sign processed dynamic data
- ISO/IEC 19794-13:2018, ~ – Part 13: Voice data
- ISO/IEC 19794-14:2013, ~ – Part 14: DNA data
- ISO/IEC 19794-15:2017, ~ – Part 15: Palm crease image data

- ISO/IEC 19795, Information technology – Biometric performance testing and reporting
  - ISO/IEC 19795-1:2006, ~ – Part 1: Principles and framework
  - ISO/IEC 19795-2:2007, ~ – Part 2: Testing methodologies for technology and scenario evaluation
  - ISO/IEC TR 19795-3:2007, ~ – Part 3: Modality-specific testing
  - ISO/IEC 19795-4:2008, ~ – Part 4: Interoperability performance testing
  - ISO/IEC 19795-5:2011, ~ – Part 5: Access control scenario and grading scheme
  - ISO/IEC 19795-6:2012, ~ – Part 6: Testing methodologies for operational evaluation
  - ISO/IEC 19795-7:2011, ~ – Part 7: Testing of on-card biometric comparison algorithms
  - ISO/IEC 19795-9:2019, ~ – Part 9: Testing of on-card biometric comparison algorithms
  - ISO/IEC 19795-10, ~ – Part 10: Quantifying biometric system performance variation across demographic groups

- ISO/IEC 20027:2018, Information technology – Best practices for slap tenprint fingerprint captures

- ISO/IEC TR 20322, Information technology – Cross jurisdictional and societal aspects of implementation of biometric technologies – Biometrics and elderly
- ISO/IEC TR 21419, Information technology – Cross jurisdictional and societal aspects of implementation of biometric technologies – Use of biometrics for identity management in healthcare
- ISO/IEC TR 21421, Information technology – Cross jurisdictional and societal aspects of implementation of biometric technologies – Biometrics and identity management for major incident response
- ISO/IEC 21472, Information technology – Scenario evaluation methodology for user interaction influence in biometric system performance
- ISO/IEC TR 22116, Information technology – A study of the differential impact of demographic factors in biometric recognition system performance
- ISO/IEC TS 22604, Biometric recognition of subjects in motion in access related systems
- ISO/IEC 24358, Face-aware capture subsystem specifications
- ISO/IEC 24708:2008, Information technology – Biometrics – BioAPI Interworking Protocol
- ISO/IEC 24709, Information technology – Conformance testing for the biometric application programming interface (BioAPI)
  - ISO/IEC 24709-1:2017, ~ – Part 1: Methods and procedures
  - ISO/IEC 24709-2:2007, ~ – Part 2: Test assertions for biometric service providers
  - ISO/IEC 24709-3:2011, ~ – Part 3: Test assertions for BioAPI frameworks
- ISO/IEC 24713, Information technology – Biometric profiles for interoperability and data interchange
  - ISO/IEC 24713-1:2008, ~ – Part 1: Overview of biometric systems and biometric profiles
  - ISO/IEC 24713-2:2008, ~ – Part 2: Physical access control for employees at airports
  - ISO/IEC 24713-3:2009, ~ – Part 3: Biometrics-based verification and identification of seafarers
- ISO/IEC 24714, Information technology – Jurisdictional and societal considerations for biometric applications
- ISO/IEC TR 24722:2015, Information technology – Biometrics – Multimodal and other multibiometric fusion
- ISO/IEC TR 24741:2018, Information technology – Biometrics – Overview and application
- ISO/IEC 24779, Information technology – Cross-jurisdictional and societal aspects of implementation of biometric technologies – Pictograms, icons and symbols for use with biometric systems

- ISO/IEC 24779-1:2016, ~ – Part 1: General principles
- ISO/IEC 24779-4:2017, ~ – Part 4: Fingerprint applications
- ISO/IEC 24779-5:2020, ~ – Part 5: Face applications
- ISO/IEC 24779-9:2015, ~ – Part 9: Vascular applications

- ISO/IEC 29109, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794

  - ISO/IEC 29109-1:2009, ~ – Part 1: Generalized conformance testing methodology
  - ISO/IEC 29109-2:2010, ~ – Part 2: Finger minutiae data
  - ISO/IEC 29109-4:2010, ~ – Part 4: Finger image data
  - ISO/IEC 29109-5:2019, ~ – Part 5: Face image data
  - ISO/IEC 29109-6:2011, ~ – Part 6: Iris image data
  - ISO/IEC 29109-7:2011, ~ – Part 7: Signature/sign time series data
  - ISO/IEC 29109-8:2011, ~ – Part 8: Finger pattern skeletal data
  - ISO/IEC 29109-9:2011, ~ – Part 9: Vascular image data
  - ISO/IEC 29109-10:2010, ~ – Part 10: Hand geometry silhouette data

- ISO/IEC 29120-1:2015, Information technology – Machine readable test data for biometric testing and reporting – Part 1: Test reports
- ISO/IEC 29141:2009, Information technology – Biometrics – Tenprint capture using biometric application programming interface (BioAPI)
- ISO/IEC TR 29144:2014, Information technology – Biometrics – The use of biometric technology in commercial Identity Management applications and processes
- ISO/IEC TR 29156:2015, Information technology – Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
- ISO/IEC 29159-1:2010, Information technology – Biometric calibration, augmentation and fusion data – Part 1: Fusion information format
- ISO/IEC 29164:2011, Information technology – Biometrics – Embedded BioAPI
- ISO/IEC TR 29189:2015, Information technology – Biometrics – Evaluation of examiner assisted biometric applications
- ISO/IEC TR 29194:2015, Information Technology – Biometrics – Guide on designing accessible and inclusive biometric systems
- ISO/IEC TR 29195:2015, Traveller processes for biometric recognition in automated border
- ISO/IEC TR 29196:2018, Information technology – Guidance for biometric enrolment

- ISO/IEC 29197:2015, Information technology – Evaluation methodology for environmental influence in biometric system performance
- ISO/IEC TR 29198:2013, Information technology – Biometrics – Characterization and measurement of difficulty for fingerprint databases for technology evaluation
- ISO/IEC 29794, Information technology – Biometric sample quality
    - ISO/IEC 29794-1:2016, ~ – Part 1: Framework
    - ISO/IEC 29794-4:2017, ~ – Part 4: Finger image data
    - ISO/IEC TR 29794-5:2010, ~ – Part 5: Face image data
    - ISO/IEC 29794-6:2015, ~ – Part 6: Iris image data
- ISO/IEC 30106, Information technology – Object oriented BioAPI
    - ISO/IEC 30106-1:2016, ~ – Part 1: Architecture
    - ISO/IEC 30106-2:2016, ~ – Part 2: Java implementation
    - ISO/IEC 30106-3:2016, ~ – Part 3: C# implementation
    - ISO/IEC 30106-4:2019, ~ – Part 4: C++ implementation
- ISO/IEC 30107, Information technology – Biometric presentation attack detection
    - ISO/IEC 30107-1:2016, ~ – Part 1: Framework
    - ISO/IEC 30107-2:2017, ~ – Part 2: Data formats
    - ISO/IEC 30107-3:2017, ~ – Part 3: Testing and reporting
    - ISO/IEC 30107-4:2020, ~ – Part 4: Profile for testing of mobile devices
- ISO/IEC 30108, Information technology – Biometric Identity Assurance Services
    - ISO/IEC 30108-1:2015, ~ – Part 1: BIAS services
    - ISO/IEC 30108-2, ~ – Part 2: REST-based implementation
- ISO/IEC TR 30110:2015, Information technology – Cross jurisdictional and societal aspects of implementation of biometric technologies – Biometrics and children
- ISO/IEC TR 30125:2016, Information technology – Biometrics used with mobile devices
- ISO/IEC 30136:2018, Information technology – Performance testing of template protection schemes [66]
- ISO/IEC 30137, Information technology – Use of biometrics in video surveillance systems
    - ISO/IEC 30137-1:2019, ~ – Part 1: Design and specification
    - ISO/IEC 30137-4, ~ – Part 4: Ground truth and video annotation procedure

- ISO/IEC 39794, Information technology – Extensible biometric data interchange formats
  - ISO/IEC 39794-1:2019, ~ – Part 1: Framework
  - ISO/IEC 39794-2, ~ – Part 2: Finger minutiae data
  - ISO/IEC 39794-4:2019, ~ – Part 4: Finger image data
  - ISO/IEC 39794-5:2019, ~ – Part 5: Face image data
  - ISO/IEC 39794-6, ~ – Part 6: Iris image data
  - ISO/IEC 39794-9, ~ – Part 9: Vascular image data
  - ISO/IEC 39794-16, ~ – Part 16: Full body image data
  - ISO/IEC 39794-17, ~ – Part 17: Gait image sequence data

4.5 ISO/TC 68/SC 2 – Financial Services, Security

ISO/TC 68/SC 2 entwickelt Normen für die IT-Sicherheit im Bereich Bankwesen, Wertpapiere und andere Finanzdienstleistungen. Die folgende von ISO/TC 68/SC 2 entwickelte internationale Norm mit Bezug zur Biometrie wird derzeit überarbeitet:

- ISO 19092:2008, Financial services – Biometrics – Security framework

4.6 CEN/TC 224 – Personal Identification and Related Personal Devices with Secure Element

Auf europäischer Ebene ist das technische Komitee CEN/TC 224 relevant für biometrische Erkennungssysteme. Der Aufgabenbereich von CEN/TC 224 umfasst die Normung von Verfahren und Sicherheitstoken zur persönlichen Identifizierung in einem sektorübergreifenden Umfeld. Die folgenden von CEN/TC 224 entwickelten europäischen Normen (EN), Technischen Berichte (TR) und Technischen Spezifikationen (TS) mit Bezug zur Biometrie sind in Kraft oder befinden sich in der Entwicklung:

- CEN/TS 16428:2012, Biometrics interoperability profiles – Best Practices for slap tenprint captures
- CEN/TS 16634:2014, Personal identification – Recommendations for using biometrics in European Automated Border Control
- CEN/TS 16920:2016, Environmental influence testing methodology for operational deployments of European ABC systems
- CEN/TS 16921:2016, Personal identification – Borders and law enforcement application profiles for mobile biometric identification systems

- EN 17054:2019, Biometrics multilingual vocabulary based upon the English version of ISO/IEC 2382-37:2012
- CEN/TS 17261:2018, Biometric authentication for critical infrastructure access control – Requirements and evaluation
- CEN/TS 17262:2018, Personal identification – Robustness against biometric presentation attacks – Application to European Automated Border Control
- FprCEN/TS 17631, Personal identification – Biometric group access control
- Personal identification – Usage of biometrics in breeder documents
- Personal identification – European enrolment guide for biometric ID documents
- Overview on biometric enrolment and verification across Europe

4.7 FIDO-Allianz

Die FIDO-Allianz wurde von IT-Unternehmen gegründet, um offene Industriestandards für die Authentisierung im Internet zu schaffen. Die FIDO-Allianz hat die folgenden Spezifikationen, alle mit Bezug zur Biometrie, entwickelt:

- Universal Second Factor (U2F oder CTAP1) [67] (spezifiziert Hard- und Software für die Zweifaktorauthentisierung),
- Universal Authentication Framework (UAF) [68] (spezifiziert das dazugehörige Netzwerkprotokoll zur passwortlosen Authentisierung),
- Client-to-Authenticator Protocols (CTAP) [69] (ergänzt die Web-Authentication- (WebAuthn) Spezifikation des W3C [70]. Beide Spezifikationen zusammen werden als FIDO2 bezeichnet).

4.8 GlobalPlatform

GlobalPlatform ist eine Organisation, die Industriestandards für sichere Chiptechnologie erstellt. Von GlobalPlatform stammen die folgenden biometriebezogenen Spezifikationen für Trusted Execution Environments (TEE):

- TEE System Architecture [22],
- TEE TUI Extension: Biometrics API [71],
- TEE Biometric System PP-Module [72].

5 Handlungsempfehlungen

5.1 Verbraucherkommunikation

Durch die Integration biometrischer Erkennungssysteme in mehr und mehr Smartphones haben schon viele Verbraucher biometrische Verfahren, insbesondere die Fingerabdruck- und Gesichtserkennung, kennen- und schätzen gelernt. Es gibt jedoch Unterschiede zwischen den Altersgruppen und biometrischen Modalitäten. Unter Berücksichtigung der Ziele, von denen sich der DIN-Verbraucherrat leiten lässt [73], nämlich

- Sicherheit und gesundheitliche Unversehrtheit der Verbraucher,
- Datenschutz und Datensicherheit sowie Schutz der Persönlichkeitsrechte,
- Verhindern ökonomischer Nachteile für Verbraucher,
- Gebrauchstauglichkeit und Qualität von Produkten und Dienstleistungen,
- Nachhaltigkeit (gleichwertige Berücksichtigung ökonomischer, ökologischer und sozialer Aspekte),
- Herstellung von Transparenz und Vergleichbarkeit auf Märkten,
- Schutz vor Täuschung und
- Wahrung der Interessen besonders schutzbedürftiger gesellschaftlicher Gruppen,

lassen sich aus den Befragungsergebnissen die folgenden Handlungsempfehlungen für die Verbraucherkommunikation ableiten:

1. Allen potenziellen Benutzer biometrischer Erkennungssysteme sollten die Empfehlungen zum Verbraucherschutz beim freiwilligen Einsatz biometrischer Systeme (Abschnitt 5.2) beachten.

2. In der Altersgruppe über 60 Jahre ist die tatsächliche Nutzung biometrischer Erkennungssysteme, aber auch die Bereitschaft zu ihrer zukünftigen Nutzung (d.h. die Verbraucherakzeptanz) weniger verbreitet als im Durchschnitt. Verbraucher in dieser Altersgruppe sollten besonders auf den Nutzen biometrischer Erkennungssysteme und die vorhandenen Sicherheitsmaßnahmen hingewiesen werden.

3. In der Altersgruppe bis 30 Jahre ist die Bereitschaft zur Nutzung biometrischer Erkennungssysteme deutlich weiter verbreitet als im Durchschnitt. Verbraucher in dieser Altersgruppe sollten besonders auf Risiken biometrischer Erkennungssysteme hingewiesen werden, um Schäden vorzubeugen.

4. Einige Verbraucher nutzen Venenmustererkennungssysteme für die Zugangskontrolle zu Räumen oder Gebäuden zu ihrer Zufriedenheit, siehe Abschnitt 3.3.6. Bei der Mehrheit der Verbraucher besteht jedoch ein Informations- und Erfahrungsdefizit bezüglich Venenmustererkennung, siehe Abbildung 19 und Abbildung 22. Potenzielle Benutzer sollten über Benutzerfreundlichkeit und Sicherheit der Venenmustererkennung informiert werden.

5.2 Verbraucherschutz bei der freiwilligen Nutzung biometrischer Systeme

Jeder Typ biometrischer Systeme erfordert eine eigene Analyse der potenziellen Schwachstellen und Risiken. Dennoch lassen sich die folgenden allgemeinen Empfehlungen zum Verbraucherschutz beim freiwilligen Einsatz biometrischer Verfahren geben:

1. Eingedenk der in der Online-Befragung geäußerten Bedenken und Risikoeinschätzungen ist den Verbrauchern zu empfehlen, bevorzugt solche biometrischen Erkennungssysteme einzusetzen, bei denen die biometrischen Daten auf einem Gerät oder Sicherheitstoken unter ihrer Kontrolle erfasst und in einem Trusted Execution Environment verarbeitet werden und vor unbefugtem Auslesen geschützt sind. Dazu gehören insbesondere

   - in Smartphones integrierte Fingerabdruck-, Gesichts- und Iriserkennungssysteme (Store on Device, Compare on Device),
   - Biometric Systems on Card bzw. Token mit eingebettetem Fingerabdrucksensor (Store on Token, Compare on Token).

   Diese Systemarchitekturen minimieren die Gefahren der zweckentfremdenden Nutzung der biometrischen Daten sowie der Übertragung von Krankheitserregern an der Oberfläche öffentlicher kontaktbehafteter biometrischer Sensoren.

   Typische Einsatzgebiete sind das Freischalten des persönlichen Smartphones bzw. Sicherheitstokens für die Client/Server-Authentisierung, die Offline-Autorisierung von Bezahlprozessen und der Zugriff auf geschützte Ressourcen innerhalb des Smartphones bzw. Sicherheitstokens.

   Im Falle besonders hoher Sicherheitsanforderungen ist es auf Grund der Gefahr der erzwungenen oder unwillentlichen biometrischen Authentisierung (z.B. durch Auflegen des Fingers auf den Sensor [74]) nicht zu empfehlen, Biometrie zum Entsperren des Smartphones einzusetzen, trotz der gefühlten Benutzerfreundlichkeit. Aus dem gleichen Grund ist es im Falle besonders hoher Sicherheitsanforderungen ebenfalls nicht zu empfehlen, Biometrie als einzigen

Authentisierungsfaktor auf dem Sicherheitstoken einzusetzen. In diesem Falle sollte ein stärkerer Authentisierungsfaktor eingesetzt werden, damit nicht alle geschützten Funktionen durch erzwungene oder unwillentliche biometrische Authentisierung zugänglich werden.

2. Wenn sich die Erfassung, Verarbeitung und Speicherung biometrischer Daten außerhalb eines persönlichen Smartphones bzw. Sicherheitstokens nicht vermeiden lässt (z.B. Store on Server, Compare on Server), dann ist den Verbrauchern zu empfehlen, nur solche biometrischen Erkennungssysteme zu benutzen, in denen die biometrischen Daten vor unbefugtem Auslesen und Veränderung geschützt sind. Die biometrischen Daten können elektronisch signiert und verschlüsselt übertragen und gespeichert werden oder durch »Biometric Template Protection«-Techniken geschützt werden, die biometrische Vergleiche auch ohne Rücktransformation der geschützten Templates in Klartext ermöglichen. Dies vermindert die Gefahr des Diebstahls und der zweckentfremdenden Nutzung der biometrischen Daten.

   Typische Einsatzgebiete, bei denen sich die Verarbeitung und Speicherung biometrischer Daten außerhalb des Verfügungsbereichs des Betroffenen nicht vermeiden lässt, sind die Sprechererkennung zur Anruferauthentisierung, die schlüssellose Zugangskontrolle zu gesicherten Bereichen, die Erkennung des Tippverhaltens bei der Mehrfaktorauthentisierung im Internet und biometrische Zahlungssysteme ohne Smartcard und Smartphone.

3. Unabhängig von der Systemarchitektur ist den Verbrauchern zu empfehlen, nur solche biometrischen Erkennungssysteme zu verwenden, die widerstandsfähig sind gegen Präsentationsangriffe (d.h. Präsentationen nachgemachter oder natürlicher biometrischer Charakteristika am biometrischen Aufnahmegerät in einer Weise, die die beabsichtigte Funktionsweise des biometrischen Systems beeinträchtigen kann), zumindest gegen naheliegende einfache Präsentationsangriffe. Dies vermindert sowohl die Gefahr des Missbrauchs biometrischer Daten zur täuschend echten Imitation biometrischer Charakteristika als auch die Gefahr für die körperliche Unversehrtheit des Verbrauchers [45].

4. Generell ist zu empfehlen, nur solche biometrischen Erkennungssysteme einzusetzen, für die die Einhaltung der relevanten Anforderungen, insbesondere an Sicherheit, Datenschutz und Benutzbarkeit, durch unabhängige Evaluierungslabors geprüft und bestätigt wurde.

5. Zusätzlich zu biometrischen Authentisierungsfaktoren müssen immer gleichermaßen benutzerfreundliche und sichere Rückfalllösungen vorhanden sein, da die Verwendung der Biometrie freiwillig ist (außer bei hoheitlichen Anwendungen). Dies vermindert die Gefahr der sozialen Ausgrenzung bei Nichtnutzung der Biometrie.

5.3 Normung biometrischer Technologien

Viele der Anforderungen an die Normung biometrischer Verfahren [75] wurden schon umgesetzt, siehe Kapitel 4. Für die weitere Normung lassen sich die folgenden Handlungsempfehlungen geben:

1. Hinsichtlich der Erwartungen des Verbraucherschutzes bestehen noch Lücken in der Normung von Technologien zur Verbesserung des Privatsphärenschutzes (Privacy-Enhancing Technologies). Zu diesen Technologien gehören

   - Smartcards oder andere Sicherheitstoken zum Speichern biometrischer Referenzdaten unter der Kontrolle der betroffenen Person (ISO/IEC 7816-11 [60]) oder zum biometrischen On-Card-Vergleich (ISO/IEC 24787 [64]),
   - biometrische Systems-on-Card (ISO/IEC 17839 [61], [62], [63]),
   - vertrauenswürdige Ausführungsumgebungen auf mobilen Endgeräten (TEE [22]) und
   - Biometric-Template-Protection-Techniken zum Schutz biometrischer Daten (ISO/IEC 24745 [65]).

   ISO/IEC 24745 [65] enthält Leitlinien zum Schutz der Vertraulichkeit und Integrität biometrischer Daten bei ihrer Speicherung und Übertragung, normiert jedoch kein bestimmtes Biometric-Template-Protection-Verfahren. Mit ISO/IEC 30136 [66] liegt eine Norm vor, die die Evaluierung von Sicherheit, Datenschutz und Benutzbarkeit von Biometric-Template-Protection-Verfahren unterstützt. Es wird empfohlen, auf der Grundlage von ISO/IEC 30136 geeignete Biometric-Template-Protection-Verfahren für die Normung auszuwählen und zu normen. Solange es keine ausgereiften, genormten Biometric-Template-Protection-Verfahren gibt, werden trotz der Datenschutzvorteile solcher Verfahren in Enrolment-Datenbanken weiterhin zumeist biometrische Rohdaten gespeichert und mit herkömmlichen kryptographischen Verfahren geschützt. Dies dient dem Schutz der für das biometrische Enrolment getätigten Investitionen: Bei einem Wechsel des Biometric-Template-Protection-Verfahrens ginge die bisherige Enrolment-Datenbank verloren.

2. Der Einsatz neuer Verfahren des maschinellen Lernens hat in den vergangenen Jahren zu einer deutlichen Steigerung der Leistungsfähigkeit biometrischer Erkennungssysteme geführt. In demographischen Gruppen, die nicht ausreichend in den Trainingsdaten repräsentiert waren (z.B. anderes Geschlecht oder Hautfarbe), kann es jedoch gehäuft zu Erkennungsfehlern kommen. Für die Akzeptanz des maschinellen Lernens spielen Erklärbarkeit und Nachvollziehbarkeit eine wichtige Rolle: Faktoren, die zu einer automatisierten Entscheidung führen, sollen auch von Menschen verstanden werden können. Um die Diskriminierung

demographischer Gruppen vermeiden zu können, ist zu empfehlen, bei der Normung biometrischer Algorithmen (z.B. für die Qualitätsbewertung von Gesichtsbildern) möglichst erklärbare Verfahren auszuwählen (siehe auch [76]).

Anhang A
Inhalt des Online-Fragebogens

A.1 Startseite

Willkommen zur Online-Umfrage »Biometrische Erkennungssysteme – Nutzen und Hemmnisse im Verbraucheralltag«!

Biometrische Erkennungssysteme (also Systeme, die der automatisierten Erkennung von Personen anhand ihres Verhaltens und ihrer biologischen Charakteristika dienen) halten zunehmend Einzug in den Alltag. Das Fraunhofer-Institut für Graphische Datenverarbeitung IGD führt diese Befragung im Auftrag des DIN-Verbraucherrates durch, um die Verbrauchersicht auf aktuell genutzte und in naher Zukunft angebotene biometrische Systeme zu ermitteln.

Die Beantwortung der Fragen dauert ca. 15 Minuten. Alle Eingaben sind anonym. Bei Rückfragen kontaktieren Sie bitte Kristina Unverricht (DIN-Verbraucherrat) oder Olaf Henniger (Fraunhofer IGD).

A.2 Soziodemographische Angaben

A.2.1 Alter

unter 18 Jahre | 18 bis 29 Jahre | 30 bis 45 Jahre | 46 bis 60 Jahre | über 60 Jahre

A.2.2 Geschlecht

männlich | weiblich | divers

A.2.3 Höchster Bildungsabschluss

Hochschulstudium | Berufsausbildung | Abitur | Sekundarstufe I | kein Schulabschluss

A.3 Aktuelle Nutzung

A.3.1 Benutzen Sie von Zeit zu Zeit biometrische Erkennungssysteme?

ja | nein

A.3.2 Falls Sie biometrische Erkennungssysteme benutzen, welche biometrischen Verfahren benutzen Sie? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprechererkennung | Unterschriftserkennung | andere, und zwar …

A.3.3 Falls Sie Fingerabdruckerkennung benutzen, bei welchen Vorgängen benutzen Sie Fingerabdruckerkennung? (Mehrfachnennungen möglich)

Online-Banking | Bargeldabhebung am Geldautomaten | bargeldloses Bezahlen | Zugangskontrolle zu Räumen oder Gebäuden | Entsperren von Geräten | Freischalten des Smartphones zur Authentisierung im Internet | Freischalten von Sicherheitstoken oder Smartcards | Arbeitszeiterfassung | automatisierte Grenzkontrolle / Registered Traveller Programme | andere, und zwar …

A.3.4 Falls Sie Fingerabdruckerkennung benutzen, wie oft sind Sie bei der Fingerabdruckerkennung von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.5 Falls Sie Fingerabdruckerkennung benutzen, waren Sie bei der Fingerabdruckerkennung schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.6 Falls Sie Gesichtserkennung benutzen, bei welchen Vorgängen benutzen Sie Gesichtserkennung? (Mehrfachnennungen möglich)

Online-Banking | bargeldloses Bezahlen | Zugangskontrolle zu Räumen oder Gebäuden | Entsperren von Geräten | Freischalten des Smartphones zur Authentisierung im Internet | automatisierte Grenzkontrolle / Registered Traveller Programme | andere, und zwar …

A.3.7 Falls Sie Gesichtserkennung benutzen, wie oft sind Sie bei der Gesichtserkennung von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.8 Falls Sie Gesichtserkennung benutzen, waren Sie bei der Gesichtserkennung schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.9 Falls Sie Iriserkennung benutzen, bei welchen Vorgängen benutzen Sie Iris-erkennung? (Mehrfachnennungen möglich)

Online-Banking | Bargeldabhebung am Geldautomaten | bargeldloses Bezahlen | Zugangskontrolle zu Räumen oder Gebäuden | Entsperren von Geräten | Freischalten des Smartphones zur Authentisierung im Internet | Freischalten von Sicherheitstoken oder Smartcards | Arbeitszeiterfassung | automatisierte Grenzkontrolle / Registered Traveller Programme | andere, und zwar …

A.3.10 Falls Sie Iriserkennung benutzen, wie oft sind Sie bei der Iriserkennung von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.11 Falls Sie Iriserkennung benutzen, waren Sie bei der Iriserkennung schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.12 Falls Sie Venenmustererkennung benutzen, bei welchen Vorgängen benutzen Sie Venenmustererkennung? (Mehrfachnennungen möglich)

Online-Banking | Bargeldabhebung am Geldautomaten | bargeldloses Bezahlen | Zugangskontrolle zu Räumen oder Gebäuden | Entsperren von Geräten | Arbeitszeiterfassung | automatisierte Grenzkontrolle / Registered Traveller Programme | andere, und zwar …

A.3.13 Falls Sie Venenmustererkennung benutzen, wie oft sind Sie bei der Venenmustererkennung von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.14 Falls Sie Venenmustererkennung benutzen, waren Sie bei der Venenmustererkennung schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.15 Falls Sie Sprechererkennung benutzen, bei welchen Vorgängen benutzen Sie Sprechererkennung? (Mehrfachnennungen möglich)

Telefon-Banking | Hotline-Anrufe | Zugangskontrolle zum digitalen Sprachassistenten | andere, und zwar …

A.3.16 Falls Sie Sprechererkennung benutzen, wie oft sind Sie bei der Sprechererkennung von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.17 Falls Sie Sprechererkennung benutzen, waren Sie bei der Sprechererkennung schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.18 Falls Sie Unterschriftserkennung benutzen, bei welchen Vorgängen benutzen Sie Unterschriftserkennung? (Mehrfachnennungen möglich)

Online-Banking | bargeldloses Bezahlen | andere, und zwar …

A.3.19 Falls Sie Unterschriftserkennung benutzen, wie oft sind Sie bei der Unterschrifts-erkennung von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.20 Falls Sie Unterschriftserkennung benutzen, waren Sie bei der Unterschrifts-erkennung schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.21 Falls Sie ein anderes biometrisches Verfahren benutzen, bei welchen Vorgängen benutzen Sie das andere biometrische Verfahren? (Mehrfachnennungen möglich)

Online-Banking | bargeldloses Bezahlen | Zugangskontrolle zu Räumen oder Gebäuden | Entsperren von Geräten | Freischalten des Smartphones zur Authentisierung im Internet | Freischalten von Sicherheitstoken oder Smartcards | Arbeitszeiterfassung | automatisierte Grenzkontrolle / Registered Traveller Programme | andere, und zwar …

A.3.22 Falls Sie ein anderes biometrisches Verfahren benutzen, wie oft sind Sie bei dem anderen biometrischen Verfahren von fälschlichen Rückweisungen betroffen und müssen auf Ausweichlösungen zurückgreifen?

häufig | gelegentlich | selten | sehr selten

A.3.23 Falls Sie ein anderes biometrisches Verfahren benutzen, waren Sie bei dem anderen biometrischen Verfahren schon einmal von den folgenden Vorfällen betroffen?

	ja	nein
Verwechslung Ihrer biometrischen Merkmale		
täuschend echte Imitation Ihrer biometrischen Merkmale		

A.3.24 Verfügen Sie über ein mobiles oder stationäres Endgerät mit integrierten Sensoren zum biometrischen Entsperren?

ja | nein | ich weiß nicht

A.3.25 Falls Sie über ein mobiles oder stationäres Endgerät mit integrierten Sensoren zum biometrischen Entsperren verfügen, wie entsperren Sie Ihr biometriefähiges Endgerät im Normalfall?

Eintippen einer PIN oder eines Passworts | Gestenerkennung auf dem Touchscreen | Fingerabdruck-erkennung | Gesichtserkennung | Iriserkennung | anders, und zwar … | Mein Endgerät wird gar nicht gesperrt.

A.3.26 Falls Sie Ihr biometriefähiges Endgerät biometrisch entsperren, aus welchen Gründen benutzen Sie die biometrische Funktion zum Entsperren Ihres Endgeräts? (Mehrfachnennungen möglich)

Biometrie erscheint mir bequemer als PIN oder Passwort. | Biometrie erscheint mir sicherer als PIN oder Passwort. | hohe Geschwindigkeit | andere, und zwar …

A.3.27 Falls Sie Ihr biometriefähiges Endgerät nicht biometrisch entsperren, aus welchen Gründen benutzen Sie die biometrische Funktion zum Entsperren Ihres Endgeräts normalerweise nicht? (Mehrfachnennungen möglich)

Aktivierung der Biometrie ist zu kompliziert. | Biometrie funktioniert nicht zuverlässig. | Sorge vor Missbrauch meiner biometrischen Daten | Sorge vor unbefugter Überwindung der biometrischen Funktion | Mein Systemadministrator hat die biometrische Funktion deaktiviert. | andere, und zwar …

A.3.28 Haben Sie schon einmal Fotos, die Ihre Identifizierung ermöglichen würden, im Internet geteilt?

ja, sowohl im beruflichen als auch im privaten Umfeld | ja, nur im beruflichen Umfeld | ja, nur im privaten Umfeld | nein

A.3.29 Benutzen Sie einen digitalen Sprachassistenten?

ja, sowohl im beruflichen als auch im privaten Umfeld | ja, nur im beruflichen Umfeld | ja, nur im privaten Umfeld | nein

A.4 Wahrnehmung biometrischer Erkennungssysteme

A.4.1 Wie benutzerfreundlich empfinden Sie die folgenden Authentisierungsfaktoren?

	sehr benutzer-freundlich	eher benutzer-freundlich	wenig benutzer-freundlich	gar nicht benutzer-freundlich	ich weiß nicht
Fingerabdruckerkennung					
Gesichtserkennung					
Iriserkennung					
Venenmustererkennung					
Sprechererkennung					
Unterschriftserkennung					
wissensbasierte Authentisie-rung mit PIN oder Passwort					
besitzbasierte Authentisierung mittels Smartphone					
besitzbasierte Authentisierung mittels Chipkarte und Kartenleser					

A.4.2 Wie schätzen Sie die folgenden Risiken ein?

	hohes Risiko	signifikantes Risiko	geringes Risiko	ich weiß nicht
von einem biometrischen Doppelgänger betroffen sein				
von einer täuschend echten Imitation der biometrischen Daten betroffen sein				
Erzwingen der biometrischen Authentisierung				
Zweckentfremdung der biometrischen Daten				
soziale Ausgrenzung durch Nichtnutzung der Biometrie				
Übertragung von Krankheits-erregern durch kontaktbehaftete biometrische Sensoren				

A.4.3 Falls Sie das Risiko der Zweckentfremdung der biometrischen Daten als hoch oder signifikant einschätzen, welche Risiken sind Ihrer Meinung nach besonders hoch? (Mehrfachnennungen möglich)

Weitergabe der biometrischen Daten an Behörden oder Institutionen | Diebstahl und Missbrauch biometrischer Daten durch Kriminelle | Auslesen von Informationen über den Gesundheitszustand aus biometrischen Daten | Nutzung von Gesichtsbildern zur Auswahl gruppenspezifischer Werbung oder Nachrichten | anderes, und zwar …

A.4.4 Wie sicher empfinden Sie die folgenden Verfahren zur Benutzerauthentisierung?

	sehr sicher	eher sicher	wenig sicher	gar nicht sicher	ich weiß nicht
Fingerabdruckerkennung					
Gesichtserkennung					
Iriserkennung					
Venenmustererkennung					
Sprechererkennung					
Unterschriftserkennung					
wissensbasierte Authentisierung mit PIN oder Passwort					
besitzbasierte Authentisierung mittels Smartphone					
besitzbasierte Authentisierung mittels Chipkarte und Kartenleser					

A.4.5 Wie sicher empfinden Sie die Erfassung Ihrer biometrischen Daten an den folgenden Orten?

	sehr sicher	eher sicher	wenig sicher	gar nicht sicher	ich weiß nicht
biometrischer Sensor an einem öffentlichen Dienstleistungssystem					
biometrischer Sensor an einem Gerät unter Ihrer Kontrolle					

A.4.6 Wie sicher empfinden Sie die Speicherung und Verarbeitung Ihrer biometrischen Daten an den folgenden Orten?

	sehr sicher	eher sicher	wenig sicher	gar nicht sicher	ich weiß nicht
staatlicher Server / Cloud					
privatwirtschaftlicher Server / Cloud					
Gerät unter Ihrer Kontrolle					
Hardware-Sicherheitstoken oder Smartcard unter Ihrer Kontrolle					

A.5 Zukünftige Nutzung

A.5.1 Wären Sie bei den folgenden Vorgängen bereit, biometrische Erkennungssysteme zu benutzen, sofern sich diese als ausreichend benutzerfreundlich und sicher erweisen?

	ja	nein	ich weiß nicht
Online-Banking			
Bargeldabhebung am Geldautomaten			
bargeldloses Bezahlen			
Zugangskontrolle zu Räumen oder Gebäuden			
Entsperren von Endgeräten			
Freischalten des Smartphones zur Authentisierung im Internet			
Freischalten von Sicherheitstoken oder Smartcards			
Arbeitszeiterfassung			
automatisierte Grenzkontrolle / Registered Traveller Programme			

A.5.2 Falls Online-Banking, welche biometrischen Verfahren wären Sie bereit, beim Online-Banking zu benutzen? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprecher-erkennung | Unterschriftserkennung | andere, und zwar …

A.5.3 Falls Bargeldabhebung am Geldautomaten oder bargeldloses Bezahlen, welche biometrischen Verfahren wären Sie bereit, bei der Bargeldabhebung am Geld-automaten oder beim bargeldlosen Bezahlen zu benutzen? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprecher-erkennung | Unterschriftserkennung | andere, und zwar …

A.5.4 Falls Zugangskontrolle zu Räumen oder Gebäuden, welche biometrischen Verfahren wären Sie bereit, bei der Zugangskontrolle zu Räumen oder Gebäuden zu benutzen? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprechererkennung | Unterschriftserkennung | andere, und zwar …

A.5.5 Falls Entsperren von Endgeräten oder Freischalten des Smartphones zur Authentisierung im Internet, welche biometrischen Verfahren wären Sie bereit, auf Ihren Endgeräten zu benutzen? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprechererkennung | Unterschriftserkennung | andere, und zwar …

A.5.6 Falls Freischalten von Sicherheitstoken oder Smartcards, welche biometrischen Verfahren wären Sie bereit, beim Freischalten von Sicherheitstoken oder Smartcards zu benutzen? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprechererkennung | Unterschriftserkennung | andere, und zwar …

A.5.7 Falls Arbeitszeiterfassung, welche biometrischen Verfahren wären Sie bereit, bei der Arbeitszeiterfassung zu benutzen? (Mehrfachnennungen möglich)

Fingerabdruckerkennung | Gesichtserkennung | Iriserkennung | Venenmustererkennung | Sprechererkennung | Unterschriftserkennung | andere, und zwar …

A.5.8 Würden Sie in die Verarbeitung Ihres Gesichtsbilds zu den folgenden Zwecken einwilligen?

	ja	nein	ich weiß nicht
Wiedererkennung von Stammkunden			
Auswahl gruppenspezifischer Werbung oder Nachrichten			
Gesichtserkennung im Internet			

A.6 Anmerkungen und Anregungen – Möchten Sie uns noch etwas über Ihre Sicht auf biometrische Erkennungssysteme mitteilen?

Freier Text

A.7 Ende der Befragung

Vielen Dank!

Bei eventuellen Rückfragen kontaktieren Sie bitte Kristina Unverricht (DIN-Verbraucherrat) oder Olaf Henniger (Fraunhofer IGD).

Literaturverzeichnis

[1] CEN/TC 224/WG 18, *Europäische Norm EN 17054 – Mehrsprachiges biometrisches Vokabular, basierend auf der englischen Fassung der ISO/IEC 2382-37:2012,* 2019.

[2] *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung),* 2016.

[3] IBM Security, „Future of Identity Study – Consumer perspectives on authentication: Moving beyond the password, " 2018.

[4] pwc, „Biometrische Authentifizierungsverfahren – Bevölkerungsbefragung, " 2018.

[5] Paysafe/Agentur Loudhouse, „Lost in Transaction: The end of risk? Will biometrics replace passwords for online payment authentication in 2019?, " 2019.

[6] BITKOM, „Biometrie – Referenzprojekte, " 2009.

[7] *Verordnung (EG) Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten,* 2004.

[8] ICAO, *Doc 9303 – Machine readable travel documents.*

[9] A. Gelb und J. Clark, „Identification for Development: The Biometrics Revolution, " 2013.

[10] Unique Identification Authority of India, „Features of Aadhar, " 2017. [Online]. Available: https://uidai.gov.in/your-aadhaar/about-aadhaar/feature-of-aadhaar.html. [Zugriff am 8. Oktober 2020].

[11] European Union Agency for Fundamental Rights, „Fundamental rights implications of storing biometric data in identity documents and residence cards, " 2018.

[12] M. Stempfle, „Gesichtserkennung: Kameras ja, Software nein, " Tagesschau, 24 Januar 2020. [Online]. Available: https://www.tagesschau.de/inland/gesichtserkennung-bundespolizei-101.html. [Zugriff am 27 November 2020].

[13] European Commission, „White Paper on Artificial Intelligence – A European approach to excellence and trust, " 2020.

[14] Bundespolizeipräsidium, „Teilprojekt 1 "Biometrische Gesichtserkennung" im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das BMI, das

Bundespolizeipräsidium, das BKA und die DB AG am Bahnhof Berlin Südkreuz – Abschlussbericht, " 2018.

[15] J. Lee, „ABI Research forecasts 95% of smartphones to feature fingerprint sensors by 2022, " Biometric Update, 3. May 2017. [Online]. Available: http://www.biometricupdate.com/201705/abi-research-forecasts-95-of-smartphones-to-feature-fingerprint-sensors-by-2022. [Zugriff am 16. September 2020].

[16] Apple, „About Touch ID advanced security technology – Apple Support, " 11. September 2017. [Online]. Available: https://support.apple.com/en-us/HT204587. [Zugriff am 24. September 2020].

[17] Apple, „Touch ID auf dem Mac verwenden – Apple Support, " 8. August 2020. [Online]. Available: https://support.apple.com/de-de/HT207054. [Zugriff am 24. September 2020].

[18] M. Frontzeck-Hornke, „Fingerabdruckscanner von Sony im ersten Test, " teltarif.de, 3. September 2015. [Online]. Available: https://www.teltarif.de/sony-xperia-z5-compact-finger-abdruck-scanner-test. [Zugriff am 8. November 2020].

[19] Samsung Electronics Co., Ltd., „Samsung Galaxy S8 and S8+ – Official Samsung Galaxy Site, " [Online]. Available: https://www.samsung.com/global/galaxy/galaxy-s8/. [Zugriff am 16. September 2020].

[20] A. Low, „Vivo X20 Plus UD: First phone with in-screen fingerprint scanner, " CNET, 24. Januar 2018. [Online]. Available: https://www.cnet.com/reviews/vivo-x20-plus-ud-preview/. [Zugriff am 8. November 2020].

[21] Apple, „About Face ID advanced technology – Apple Support, " 26. Februar 2020. [Online]. Available: https://support.apple.com/en-us/HT208108. [Zugriff am 5. November 2020].

[22] Global Platform, „TEE System Architecture Version 1.2, " 2018.

[23] Apple Support, „Secure Enclave – Übersicht, " [Online]. Available: https://support.apple.com/de-de/guide/security/sec59b0b31ff/web. [Zugriff am 24. November 2020].

[24] Samsung, „Samsung Knox – Sichere mobile Plattform und Lösungen, " [Online]. Available: https://www.samsungknox.com/de. [Zugriff am 24. November 2020].

[25] Tyrone, „Apple Watch Wrist Detection Facts, " iPhoneTricks.org, 23 Juni 2015. [Online]. Available: https://www.iphonetricks.org/apple-watch-wrist-detection-facts/. [Zugriff am 16. September 2020].

[26] FIDO Alliance, „FIDO Alliance – Open Authentication Standards More Secure than Passwords, " [Online]. Available: https://fidoalliance.org/. [Zugriff am 16. September 2020].

[27] A. Perala, „TypingDNA Brings Behavioral Biometrics Solution to ForgeRock Identity Platform," FindBiometrics, 18. August 2020. [Online]. Available: https://findbiometrics.com/typingdna-brings-behavioral-biometrics-solution-forgerock-identity-platform/. [Zugriff am 25. November 2020].

[28] O. von Westernhagen, „Anmeldung ohne Passwort: "Windows Hello" wird zum FIDO2-Authenticator," Heise online, 10. Mai 2019. [Online]. Available: https://www.heise.de/security/meldung/Anmeldung-ohne-Passwort-Windows-Hello-wird-zum-FIDO2-Authenticator-4418470.html. [Zugriff am 25. November 2020].

[29] Thales Gemalto, „White Paper: Biometrics for Financial Institutions and the new Gemalto Biometric Sensor Payment card," 2017.

[30] P. Schmitz, „Der Yubikey wird biometrisch," Security Insider, 4. Dezember 2019. [Online]. Available: https://www.security-insider.de/der-yubikey-wird-biometrisch-a-888159/. [Zugriff am 12. Oktober 2020].

[31] ekey, „Einzel-Zutrittslösungen," [Online]. Available: https://www.ekey.net/de/ekey_home/. [Zugriff am 16. September 2020].

[32] „Aus Face-Check wird Play Safe plus technische Neuerungen," Automaten-Markt, 26. September 2018. [Online]. Available: https://www.automatenmarkt.de/nachrichten/artikel/aus-face-check-wird-play-safe-plus-technische-neuerungen/. [Zugriff am 24. November 2020].

[33] Europäisches Parlament und Rat der Europäischen Union, „Richtlinie (EU) 2015/2366 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG," 2015.

[34] Postbank, „Postbank BestSign App," [Online]. Available: https://www.postbank.de/privatkunden/bestsign-app.html. [Zugriff am 16. Oktober 2020].

[35] „Voice Banking: Was ist das?," Mobilebanking.de, [Online]. Available: https://www.mobilebanking.de/magazin/voice-banking-definition.html. [Zugriff am 16. Oktober 2020].

[36] M. Schröder, „Geldautomaten: Hand auflegen statt PIN eingeben," Der Tagesspiegel, 21 Februar 2010. [Online]. Available: https://www.tagesspiegel.de/wirtschaft/geldautomaten-hand-auflegen-statt-pin-eingeben/1687730.html. [Zugriff am 19 Oktober 2020].

[37] D. Pöhler, „Wie Zahlungen mit dem Handy funktionieren – und wer es anbietet," Süddeutsche Zeitung, 25. Oktober 2018. [Online]. Available:

https://www.sueddeutsche.de/wirtschaft/mobiles-zahlen-1.4183096. [Zugriff am 16. September 2020].

[38] M. Singh, „Google Play Gets Fingerprint Payment Authentication for Android 6.0 Marshmallow," NDTV Gadgets 360, 23. October 2015. [Online]. Available: https://gadgets.ndtv.com/apps/news/google-play-gets-fingerprint-payment-authentication-for-android-60-marshmallow-756275. [Zugriff am 16. September 2020].

[39] „So funktioniert Apple Pay in Deutschland," internetworld.de, 11. Dezember 2019. [Online]. Available: https://www.internetworld.de/sonstiges/apple/so-funktioniert-apple-pay-in-deutschland-2403744.html. [Zugriff am 16. Oktober 2020].

[40] E. Atzler, „Handelsblatt," Das ist die Antwort der Sparkassen auf Google Pay, 27. Juni 2018. [Online]. Available: https://www.handelsblatt.com/finanzen/banken-versicherungen/mobiles-bezahlen-das-ist-die-antwort-der-sparkassen-auf-google-pay/22742270.html. [Zugriff am 16. September 2020].

[41] it-Werke, „Biometric Payment: digiPROOF," [Online]. Available: https://www.it-werke.com/digiproof/. [Zugriff am 16. Oktober 2020].

[42] TeleTrusT-Arbeitsgruppe "Biometrie", „Positionspapier: Regelung des Biometrie-Einsatzes in der Arbeitswelt," 2012.

[43] Gentex Corp., „Gentex Introduces Biometric Authentication System for Automotive Use," GlobalNewswire, 5. January 2017. [Online]. Available: https://www.globenewswire.com/news-release/2017/01/05/903770/0/en/Gentex-Introduces-Biometric-Authentication-System-for-Automotive-Use.html. [Zugriff am 16. September 2020].

[44] Continental, „Continental Introduces Biometrics to Vehicles at CES 2017," PR Newswire, 15 December 2016. [Online]. Available: https://www.prnewswire.com/news-releases/continental-introduces-biometrics-to-vehicles-at-ces-2017-300379341.html. [Zugriff am 16. September 2020].

[45] J. Kent, „Malaysia car thieves steal finger," BBC news, 31. März 2005. [Online]. Available: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm. [Zugriff am 25. November 2020].

[46] Wissenschaftliche Dienste – Deutscher Bundestag, „Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware "Alexa" durch Amazon," 2019.

[47] M. Bronstein, „Bringing you the next-generation Google Assistant," Google, 7. Mai 2019. [Online]. Available: https://www.blog.google/products/assistant/next-generation-google-assistant-io/. [Zugriff am 10. November 2020].

[48] S. Salazar, „Google Home Mini has arrived—here' s what you can do with it, " The Keyword, 19. Oktober 2017. [Online]. Available: https://www.blog.google/products/home/google-home-mini-has-arrivedheres-what-you-can-do-it/. [Zugriff am 27. November 2020].

[49] K. Hill, „The Secretive Company That Might End Privacy as We Know It, " The New York Times, 18. Januar 2020. [Online]. Available: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. [Zugriff am 27. November 2020].

[50] D. Laufer und S. Meineck, „Eine polnische Firma schafft gerade unsere Anonymität ab, " netzpolitik.org, 10. Juli 2020. [Online]. Available: https://netzpolitik.org/2020/gesichter-suchmaschine-pimeyes-schafft-anonymitaet-ab/. [Zugriff am 16. September 2020].

[51] International Committee for Information Technology Standards, „INCITS M1/07-0185rev: Study Report on Biometrics in E-Authentication, " 2007.

[52] Dooler UG, „Umbuzoo-Homepage, " [Online]. Available: https://www.umbuzoo.de/. [Zugriff am 1. Oktober 2020].

[53] Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V., Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e.V., Berufsverband Deutscher Markt- und Sozialforscher e.V. und Deutsche Gesellschaft für Online-Forschung e.V., „Standards zur Qualitätssicherung für Online-Befragungen, " 2001.

[54] Abel & Burkart GbR, „Pollpool-Homepage, " [Online]. Available: https://www.poll-pool.com/. [Zugriff am 1. Oktober 2020].

[55] M. Eid, M. Gollwitzer und M. Schmitt, Statistik und Forschungsmethoden, Beltz Verlag, 2017.

[56] Autorengruppe Bildungsberichterstattung , „Bildung in Deutschland 2020 – Ein indikatorengestützter Bericht mit einer Analyse zu Bildung in einer digitalisierten Welt, " 2020.

[57] J. Krißler und C. Rütten, „Feine Linien – Wie leicht sich Fingerabdrucksensoren austricksen lassen, " *c't,* p. 102–103, Heft 12 2007.

[58] S. Marcel, M. Nixon, J. Fierrez und N. Evans, Handbook of Biometric Anti-Spoofing, Springer, 2019.

[59] F. Breitinger und C. Nickel, „User Survey on Phone Security and Usage, " in *BioSIG*, 2010.

[60] ISO/IEC 7816-11, „Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods, " 2017.

[61] ISO/IEC 17839-1, „Information technology – Biometric System-on-Card – Part 1: Core requirements, " 2014.

[62] ISO/IEC 17839-2, „Information technology – Biometric System-on-Card – Part 2: Physical characteristics," 2015.

[63] ISO/IEC 17839-3, „Information technology – Biometric System-on-Card – Part 3: Logical information interchange mechanism," 2016.

[64] ISO/IEC 24787, „Information technology – Identification cards – On-card biometric comparison," 2018.

[65] ISO/IEC 24745, „Information technology – Security techniques – Biometric information protection," 2011.

[66] ISO/IEC 30136, „Information technology – Performance testing of biometric template protection schemes," 2018.

[67] FIDO Alliance, „Universal 2nd Factor (U2F) Overview," 2017.

[68] FIDO Alliance, „FIDO UAF Architectural Overview," 2017.

[69] FIDO Alliance, „Client to Authenticator Protocol (CTAP)," 30. Januar 2019. [Online]. Available: https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html. [Zugriff am 27. November 2020].

[70] W3C, „Web Authentication: An API for accessing Public Key Credentials Level 1," 4. März 2019. [Online]. Available: https://www.w3.org/TR/webauthn/. [Zugriff am 27. November 2020].

[71] Global Platform, „TEE TUI Extension: Biometrics API Version 1.0," 2018.

[72] Global Platform, „TEE Biometric System PP-Module Version 1.0," 2020.

[73] DIN-Verbraucherrat, „Leitsätze für die Verbrauchervertretung in der Normung," 2016.

[74] A. Zilber, „Arkansas girl used her mom's fingerprints to unlock iPhone and buy 13 Pokemon gifts on Amazon," Daily Mail Online, 27. Dezember 2016. [Online]. Available: https://www.dailymail.co.uk/news/article-4069090/Mommy-shopping-Six-year-old-Arkansas-girl-used-sleeping-mom-s-fingerprints-unlock-iPhone-buy-13-Pokemon-gifts-Amazon-total-250.html. [Zugriff am 27. November 2020].

[75] Projektteam BioNorm, „Standardisierung zur Anwendung biometrischer Verfahren für die Personenidentifikation – Anforderungen, Bestandsaufnahme, Vorschläge," 2003.

[76] W. Wahlster und C. Winterhalter, „Deutsche Normungsroadmap Künstliche Intelligenz," DIN; DKE, 2020.

Änderungsverlauf

Version	Erstellungsdatum	Änderungen
1.0	3. Dezember 2020	zum Review freigegeben
1.1	11. Dezember 2020	Kommentare des DIN-Verbraucherrats eingearbeitet