Thomas Petermann
Constanze Scherz
Arnold Sauter

Dezember 2003

Biometrie und Ausweisdokumente

Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung

Zweiter Sachstandsbericht

TAB Arbeitsbericht Nr. 93

TAB
Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät das Parlament und seine Ausschüsse in Fragen des gesellschaftlich-technischen Wandels. Das TAB ist eine organisatorische Einheit des Instituts für Technikfolgenabschätzung und Systemanalyse (ITAS) des Forschungszentrums Karlsruhe in der Helmholtz-Gemeinschaft und arbeitet seit 1990 auf der Grundlage eines Vertrages zwischen dem Forschungszentrum und dem Deutschen Bundestag.

Inhalt

Zusammenfassung 3

I. Einleitung 15

II. Aktuelle politische Rahmenbedingungen 19

1. Europäische Union 19
2. USA 25
3. International Civil Aviation Organization (ICAO) 30
4. International Maritime Organization (IMO) 31
5. G8 32
6. Deutschland 32

III. Biometrie bei Ausweisdokumenten – eine Momentaufnahme internationaler Aktivitäten 39

1. Biometrisch unterstützte Grenzkontrollanwendungen 41
2. Nationale Ausweisdokumente mit Biometrie 49

IV. Leistungsfähigkeit und Eignung von Biometrien bei Ausweisdokumenten und Grenzkontrollen 55

1. Allgemeine Beschreibung und Einschätzung biometrischer Verfahren 55
2. Detailanalyse der technologischen Leistungsfähigkeit 61
   - 2.1 Erfassbarkeit 61
   - 2.2 Erkennungsgenauigkeit und Fehlerwahrscheinlichkeit 64
   - 2.3 Bedienungsaufwand und Verständlichkeit bei Enrollment und Verifikation 72
   - 2.4 Ein vorläufiges Fazit 75
3. Integration in etablierte Prozesse der Beantragung und Produktion von Ausweisdokumenten für Bundesbürger 77

4. Kosten – ein Exkurs 81

V. Überlegungen zur rechtlichen Ausgestaltung eines zukünftigen Einsatzes von biometrischen Systemen 91

1. Biometrie in Ausweisdokumenten für Bundesbürger 92
   1.1 Regelungen und Ziele 92
   1.2 Vorgaben für die Umsetzung der mit dem Terrorismusbekämpfungsgesetz geschaffenen Regelungen 94
2. Biometrie in Ausweisdokumenten für Ausländer 106
   2.1 Regelungen und Ziele 106
   2.2 Vorgaben für die Umsetzung 107
3. Fazit 114

VI. Ausblick 117

Literatur 121

1. In Auftrag gegebene Gutachten 121
2. Weitere Literatur 121
3. Ausgewählte http-Adressen 126

Anhang 127

1. Kostenmodelle für verschiedene Alternativen 127
   1.1 Handlungsalternativen und Bewertungsdimensionen 127
   1.2 Kostenmodell 129
   1.3 Evaluierung der Handlungsalternativen in den einzelnen Dimensionen 134
   1.4 Vergleichende Bewertung der Handlungsalternativen und Fazit 150
2. Tabellenverzeichnis 156
3. Abbildungsverzeichnis 157
4. Abkürzungsverzeichnis 158

Glossar 161

Zusammenfassung

Hintergrund und Ziel des Berichtes

Der weltweite *Durchbruch der Biometrie als Sicherheitstechnologie* in Form ihrer Nutzung bei der Ausrüstung von Ausweisdokumenten und entsprechenden biometriegestützten Kontrollen an Grenzübergängen scheint unmittelbar bevor zu stehen. Rund um den Globus schaffen Staaten und Staatengruppen hierfür die politischen und rechtlichen Voraussetzungen.

Die Frage, welche biometrischen Systeme und die Nutzung welcher Merkmale geeignet bzw. vorzugswürdig sind, ist mittlerweile nicht mehr so offen wie noch vor kurzem. Erkennungssysteme, die Finger, Gesicht oder Iris (bzw. eine Kombination dieser Merkmale) nutzen, haben ihre Eignung für Verifikationsanwendungen bei Ausweisdokumenten grundsätzlich unter Beweis gestellt – auch wenn ihre Performanz und Leistungsfähigkeit je nach Kontext und Systemanforderung teilweise noch verbesserungswürdig sind. Es bleibt aber ein erhebliches Entscheidungsdilemma: Mit der biometrischen Ausrüstung von nationalen Ausweisdokumenten und ihrer weltweiten Nutzung bei Grenzkontrollen ist eine Aufgabe mit so erheblichen Dimensionen zu lösen, dass bisherige Erfahrungen – z.B. mit Pilotprojekten bei Grenzkontrollen – hierzu allenfalls indirekt Erkenntnisse liefern. Angesichts der zu bewältigenden Volumina des internationalen Reiseverkehrs und von Migrationsbewegungen sowie der Komplexität der erforderlichen technischen, administrativen und rechtlichen Umsetzung auf nationaler Ebene – und erst recht in globalem Maßstab – ist die augenblickliche Wissens- und Erfahrungsbasis noch nicht stabil. Zugleich aber ist Handlungsbedarf offensichtlich.

Vor diesem Hintergrund ist es ein *Ziel dieses TAB-Berichtes* zu biometrischen Identifikationssystemen, *den augenblicklichen Stand der Diskussion* darzustellen. Dieser Bericht ist allerdings nicht das Resultat einer umfassenden Technikfolgen-Abschätzung, da die Bestandsaufnahme thematisch eingegrenzt war und insbesondere keine Folgenanalysen durchgeführt wurden. Auftragsgemäß resümiert er den Stand der wissenschaftlichen und politischen Diskussion zur Leistungsfähigkeit und Eignung dieser Technologien und entsprechender Systemlösungen bei bestimmten Ausweisdokumenten und Grenzkontrollanwendungen, formuliert Anforderungen an eine rechtsverträgliche Ausgestaltung und spricht weiteren Informations-, Diskussions- und Handlungsbedarf an. Damit

soll der Sachstandsbericht *eine Hilfestellung für die Arbeit der Fachausschüsse* des Deutschen Bundestages sein.

Politische Aktivitäten und Weichenstellungen, internationale Entwicklungen

In vielen Staaten sind mit Tests, Pilotprojekten und Machbarkeitsstudien, aber zunehmend auch mit Gesetzen und Verordnungen erste Grundlagen für eine biometrische Ausstattung von Ausweisdokumenten und biometrische Grenzkontrollen gelegt worden (Kap. II). Zahlreiche Staaten haben bereits eine *Entscheidung für nationale Ausweisdokumente* mit Biometrie getroffen bzw. erste Schritte unternommen (Kap. III). Die *USA* haben seit längerem den Weg in Richtung eines biometrisch gestützten Systems der Ein- und Ausreisekontrolle eingeschlagen. Auf *EU*-Ebene sind ebenfalls politische und rechtliche Weichenstellungen erfolgt, die die Voraussetzungen für eine abgestimmte biometrische Nutzung bzw. Ausrüstung von Ausweisdokumenten, Visa und Aufenthaltstiteln für Drittstaatenbürger eröffnen. In *Deutschland* sind hierzu das Pass- und Personalausweisgesetz und das Ausländergesetz geändert worden: Eine Einbringung zusätzlicher biometrischer Merkmale (Gesicht oder Finger oder Hand) in Ausweisdokumente für Bundesbürger und Ausländer kann jetzt vorgenommen werden. Es bedarf aber weiterer Konkretion der Modalitäten und Einzelheiten durch den Gesetz- und Verordnungsgeber.

Mit den *G8-Staaten* hat sich ein weiterer Akteur zu Wort gemeldet. Diese wollen – unter gemeinsamer US-amerikanisch/französischer Leitung – eine hochrangige Arbeitsgruppe ins Leben rufen, um erste politische Entscheidungen in die Wege zu leiten. Zur Vorbereitung ist an breit angelegte Testprogramme gedacht. Die G8-Staaten unterstützen ausdrücklich die International Civil Aviation Organization (*ICAO*) und deren Bemühungen zur Standardisierung biometrischer Verfahren.

Die ICAO – eine Sonderorganisation der Vereinten Nationen – hat nach längerer Vorarbeit die Empfehlung ausgesprochen, in internationale Reisedokumente das Gesichtsbild als erstes – für die Mitgliedsstaaten verbindliches – Merkmal aufzunehmen. Für Staaten, die mithilfe der Biometrie Datenbankabgleiche vornehmen wollen, wird optional Fingerabdruck und/oder Iris genannt.

Technische Leistungsfähigkeit und Eignung

Der Bericht fasst den Stand der Diskussion zur technischen Leistungsfähigkeit und Eignung der Handgeometrie-, Fingerabdruck- sowie Gesichts- und Iriserkennung für die Nutzung bei Ausweisdokumenten und bei Grenzkontrollen mit dem Ziel der Verifikation zusammen. Dazu wird nach einer kurzen allgemeinen Charakterisierung der Stärken und Schwächen der einzelnen biometrischen Verfahren (Kap. IV.1) deren *spezifisches Leistungsprofil für die Ausweisanwendung* näher beschrieben (Kap. IV.2).

Bei der Prüfung entlang verschiedener Kriterien stellt sich die Situation wie folgt dar:

– Im Falle einer biometrischen Ausrüstung der Ausweisdokumente muss sichergestellt sein, dass das vorgesehene Merkmal möglichst *keine oder nur eine sehr geringe Zahl von Bürgern von der Anwendung ausschließt*. Fingerabdruck-Verfahren werden dieser Anforderung nur bedingt gerecht. Vorliegende Tests und Erfahrungen zeigen, dass hier bei etwa 2 % der Gesamtbevölkerung Probleme bei der biometrischen Erfassung (enrollment) auftreten. Die Enrollment-Ausfallraten von Hand- und Iriserkennungs-Verfahren sind zwar geringer als die des Fingerabdrucks, bei bestimmten Nutzergruppen bleiben aber Probleme aufgrund ihres Alters oder ihrer Ethnie. Die Nutzerausfallrate für die Gesichtserkennung ist marginal.
– Die Handgeometrieerkennung erweist sich im Hinblick auf die Anforderung der *Unterscheidbarkeit* – besonders bei umfangreichen Anwendungen – als weniger geeignet. Die Unterscheidbarkeit bei Iris, Finger und Gesicht ist aufgrund der hohen Anzahl an eindeutigen Informationen grundsätzlich besser gewährleistet. Seriöse Qualitätstests belegen die hohe Einzigartigkeit der Merkmale Finger und Gesicht auch bei großen Datenbeständen. Für die Iris liegen hierzu Belege aus Großanwendungen bislang nicht vor.
– Für biometrische Anwendungen ist es wichtig, dass das Merkmal sich nicht in kurzen Zeitabständen verändert. Unter dem Gesichtspunkt der *Stabilität* ist der Einsatz von Fingerabdruck-Verfahren aufgrund bestimmter Einschränkungen kritisch zu beurteilen. Nachteilig bei der Handgeometrieerkennung ist die späte Stabilisierung des Merkmals erst im Alter von 20 Jahren. Die Stabilität des Gesichtes ist für die Ausweisanwendung ausreichend, da Veränderungen dieses Merkmals innerhalb größerer Zeitabstände erfolgen, so dass mit vertretbarem Aufwand „Neuregistrierungen“ vorge-

nommen werden könnten. Die Iris dürfte in Bezug auf das Kriterium der Stabilität am unproblematischsten sein.

– Bisher durchgeführte Studien deuten auf eine hohe *Erkennungsleistung* von Iriserkennungs-Verfahren hin, die es aber noch in Großanwendungen zu überprüfen gilt. Die Handgeometrieerkennung erzielt zwar in Kleinszenarien gute Erkennungsraten, die Problematik der nicht eindeutig unterscheidbaren Identität von Handgeometriemustern in größeren Anwendungen müsste allerdings erst in umfangreichen Teststudien widerlegt werden. Fingerabdruck- und Gesichtserkennungs-Verfahren haben in aktuellen und unabhängigen Studien ihre Erkennungsleistung auch bei umfangreichen Datenmengen unter Beweis gestellt. Die augenblicklich erreichbare Leistung der beiden Verfahren *bei Verifikationsanwendungen* ist dabei ungefähr gleich einzustufen.

  Sowohl Fingerabdruck- als auch Gesichtserkennungs-Verfahren sind heute so weit ausgereift und leistungsstark, dass ihr Einsatz im Vergleich zur bisherigen Situation eine Effektivierung der Grenzkontrollen im Verifikationsmodus verspricht. Die Frage, ob die hier erwartbare Erkennungsleistung eine hinreichende Sicherheit gewährleisten wird und ob die erhofften Verbesserungen bei der Grenzkontrolle den hierzu erforderlichen Aufwand rechtfertigen, muss politisch entschieden und begründet werden. Dabei sollte offen diskutiert werden, dass es – trotz eindrucksvoll geringer Fehlerraten – in der Praxis eines Masseneinsatzes nur zu einem relativen Sicherheitszugewinn kommen kann, da Falschidentifikationen in einem gewissen Umfang weiter erfolgen werden.

– Für die Ausweisanwendung sind *Verfahren mit niedrigem Bedienungsaufwand* und hoher Verständlichkeit *günstig*. Vorteile bieten hier Gesichtserkennungs-Verfahren als kontaktloses Verfahren ohne großen Positionierungsaufwand. Fingerabdruck-Verfahren sind zwar bequem nutzbar, erfordern aber eine, wenn auch kurze, Einlernzeit. Auch bei der Handgeometrieerkennung treten Bedienungsfehler eher selten auf. Die Iriserkennung ist im Hinblick auf den Bedienungsaufwand im Vergleich weniger günstig einzuschätzen, da sie genaue Verhaltensvorschriften und eine gewisse Einlernzeit erfordert.

  Der bei allen Verfahren erforderliche Aufwand beim Enrollment und bei der Kontrolle dürfte grundsätzlich den bisher üblichen Zeitrahmen der Ausweisbeantragungs- und Kontrollprozesse nicht entscheidend verändern. Für eine umfassende Einschätzung müssen aber weitere Aspekte wie die Systemumgebung sowie bauliche, infrastrukturelle und organisatorische Aspekte mit herangezogen werden. Ob beispielsweise im Falle der Ausweiskon-

trolle an Flughäfen mehr Zeit erforderlich wäre oder ob biometrische Verfahren längerfristig zu Zeiteinsparungen führen könnten, hängt von den konkreten Systembedingungen und Leistungsanforderungen vor Ort ab.

Es zeigen sich bei jeder Technologie sowohl gewisse Stärken als auch Schwächen. So erweist sich die *Gesichtserkennung* bei zwei Kriterien als führend (Enrollment-Ausfallrate, Bedienungsaufwand/Verständlichkeit), sie ist aber bei der Erkennungsleistung schwächer zu bewerten. Die *Iriserkennung* ist bei der Erkennungsleistung führend. Sie weist allerdings schwächere Werte beim Bedienungsaufwand auf. Die *Handgeometrieerkennung* weist insgesamt durchschnittliche Leistungen, allerdings eine hohe Falschakzeptanzrate auf. Die *Fingerabdruckerkennung* ist bei keinem Kriterium den anderen Verfahren überlegen, weist aber im Durchschnitt gute Werte auf, sieht man von einer nicht zufrieden stellenden Enrollment-Ausfallrate ab. Die Unterschiede, die sich bei den einzelnen Kriterien ergeben, sind allerdings nicht sehr gravierend.

Insgesamt ist deshalb der Schluss zu ziehen, dass *drei Verfahren* – Gesichts-, Iris- und Fingerabdruckerkennung – über *eine in etwa vergleichbare technische Leistungsfähigkeit* verfügen. Die Handgeometrie fällt demgegenüber etwas ab. Zur Entscheidung für oder gegen eine Technologie müssten weitere Kriterien und Fragestellungen in die Abwägung mit einbezogen werden.

Auswirkungen auf bestehende Verfahren der Datenerhebung und Produktion

Eine Umsetzung des Ziels der biometrischen Modernisierung von Ausweisen und Ausweiskontrollen könnte erhebliche Konsequenzen nach sich ziehen – beispielsweise eine komplette Erhebung der biometrischen Daten der Bundesbürger. Spielt man gedanklich die Folgen verschiedener Optionen für den Teilbereich der Erhebungs- und Produktionsverfahren bei Pass und Personalausweisen durch, zeigen sich die folgenden Konsequenzen (Kap. IV.3):

Datenerhebung

Unter dem Aspekt des Organisationsaufwandes betrachtet, wäre die praktikabelste Option, *mit dem bisherigen Ausweiskonzept* und im Rahmen der bestehenden und vertrauten Erhebungs- und Produktionsverfahren *Lichtbilder ausreichender Qualität auf dem Ausweisdokument* für die automatische Analyse *zu nutzen*. Ein Template könnte dezentral oder zentral generiert werden.

Für *Fingerabdruck-, Handgeometrie- und Iriserkennungs-Verfahren* müsste eine komplette Erhebung der biometrischen Daten der deutschen Bevölkerung erfolgen. Bei einer dezentralen Erfassung wäre es erforderlich, alle Meldestellen und Bürgerbüros mit biometrischen Systemen auszurüsten und das Personal zu schulen. Bei einer zentralen Erfassung müsste für die Generierung des Templates auf der Basis eines Fingerabdruckes dieser abgerollt auf einem Träger zur Verfügung gestellt werden. Zur Sicherstellung ausreichender Qualität wäre geschultes Personal erforderlich. Für die Iriserkennung und die Handgeometrieerkennung ist grundsätzlich eine dezentrale Erfassung in den Meldestellen erforderlich, da die Ursprungsmerkmale sich nicht als Rohdaten ablegen und versenden lassen.

Während für die Erhebung von Fingerabdrücken und für die Gesichtserkennung umfangreiche Erfahrungen aus Großanwendungen vorliegen, fehlen Erfahrungswerte mit der großflächigen Datenerfassung und -pflege bei der Erhebung von Irismuster und Handgeometrie. Probleme einer bevölkerungsweiten Irismuster- oder Handgeometrieerhebung müssten deshalb sorgfältig antizipiert werden.

Datenspeicherung auf dem Dokument

Die Konsequenzen einer Einführung und Nutzung von Biometrie für das etablierte Dokumentenkonzept lassen sich wie folgt umreißen: Ohne weitgehende Folgen bliebe die *Ablage* des Merkmals Gesicht *in optischer Form* durch Abdruck eines Fotos auf dem Ausweisdokument, da dieses Verfahren heute schon fester Bestandteil der Ausweisproduktion ist. Könnte eine biometrische Analyse des Gesichtes vom Foto erfolgen, müsste kein biometrisches Template gespeichert werden. Dazu wäre die Sicherstellung eines ausreichenden Standards (z.B. gemäß ICAO) notwendig. Die Fotoablage des Fingerabdruckes erfordert eine Änderung des Ausweisdokumentes, da das Foto zusätzlich zum „Gesichtsfoto“ abgelegt werden müsste. Dies ist aber auf dem bisherigen Ausweisdokument nicht vorgesehen.

Bei der Integration eines biometrischen Templates in das Ausweisdokument mittels eines *Barcodes* ist zu beachten, dass der Barcode ausschließlich während der zentralen Produktion aufgebracht werden kann. Die Barcode-Speicherung im Ausweisdokument ist derzeit nicht vorgesehen.

Bei der Integration eines *Chips* in das Ausweisdokument muss mit einem erheblich höheren Aufwand gerechnet werden, u.a. aufgrund der fehlenden Infrastruktur von Lesegeräten. Kontaktlose Chips ließen sich in das bisherige

Dokument integrieren, nicht aber kontaktbehaftete Chips. Vorteilhaft ist, dass die Chips erst bei der Dokumentenausgabe beschrieben werden können. Verlässliche Aussagen über Manipulationssicherheit und Haltbarkeit können wegen fehlender Großanwendungen und Tests noch nicht gemacht werden. Die Speicherung in Chipform ist zwar aufgrund der erforderlichen Produktionsumstellung das aufwendigste Verfahren, sie bietet aber ein größeres Anwendungspotenzial.

Kosten

Bislang ist die Kostenfrage allenfalls in Ansätzen diskutiert. Man kann aber bereits jetzt sagen, dass die verschiedenen Identifikationstechnologien Hard- und Softwarekosten in vergleichbarem Umfang mit sich bringen. Ferner ist festzuhalten, dass die Biometriekomponenten im Gesamtsystem nicht der entscheidende Kostenfaktor sind. Um für die Beantwortung der Frage nach den gesamten (einmaligen und laufenden) Kosten über alle Systemebenen hinweg einen ersten Einstieg zu bieten, werden in einem Exkurs für verschiedene Einsatzvarianten Kostenmodelle erörtert (Kap. IV.4).

- *Biometrische Nutzung der bestehenden Dokumente* (Option 1)
  Hierbei werden die auf den Personaldokumenten aufgedruckten Passbilder mit den Gesichtsinformationen der Person für eine biometrische Auswertung herangezogen. Der heutige Beantragungsprozess mit Abgabe eines Passbildes bliebe erhalten. Die notwendigen Anpassungen ergäben sich im Wesentlichen auf der Ausstellungsebene, wo die Qualität der Passbilder normalisiert und standardisiert werden muss.
- *Technische Aufwertung der bestehenden Dokumente mit biometrischen Daten* (Option 2)
  Die Daten werden in *Speichertechnik* in das Ausweisdokument eingebracht. Als Speicher kommen Barcodes oder digitale Speicherelemente in Frage. Alternativ bieten sich die zentrale Erfassung und Verarbeitung der biometrischen Merkmale (2a) und die dezentrale Erfassung und Verarbeitung der biometrischen Merkmale in den einzelnen Meldestellen an (2b).
- *Das bestehende Dokumentenkonzept wird durch ein vollständig neues Konzept abgelöst* (Option 3)
  Bei dieser Alternative wird das Dokument (z.B. Smartcards) durch ein elektronisches Speicherelement aufgewertet. Hierdurch ergäben sich Kombinationsmöglichkeiten für den Flächeneinsatz der elektronischen Unterschrift sowie u.U. Impulse für den elektronischen Rechts- und Geschäftsverkehr.

Eine grobe Abschätzung einmaliger und laufender jährlicher Kosten zeigt folgendes Bild:

Option 1 erfordert 22 Mio. Euro einmaliger und 4,5 Mio. Euro laufender Kosten. Bei Option 2 beziffern sich die einmaligen Kosten auf 614 Mio. Euro und 322 Mio. Euro bei der dezentralen Neuerfassung (Variante 2b) bzw. 179 Mio. Euro und 55 Mio. Euro bei der zentralen Prozessgestaltung (Alternative 2a). Option 3 als die technologisch anspruchsvollste Variante erfordert einmalige Investitionen in Höhe von 669 Mio. Euro sowie 610 Mio. Euro an laufenden jährlichen Kosten.

Der durchgeführte Kostenvergleich zeigt ferner, dass in Optionen, bei denen dezentrale Merkmalsneuerfassung und Templategenerierung – und damit eine Neuausstattung mit Hardware – erforderlich sind, die Kosten um ein Mehrfaches höher ausfallen, als bei den Alternativen, wo die Mehrkosten auf der Ebene der Produktion der Ausweise entstehen.

Trotz seiner Bedeutung liefert auch das Kostenkriterium per se keine ausreichende Grundlage für eine Entscheidung. Vielmehr müssten weitere Aspekte im Sinne einer Kosten-Nutzen-Analyse mit einbezogen werden. Eine vorläufige Abwägung führt zu folgenden Überlegungen:

Unterstellt man, dass bei allen Alternativen der Sicherheitszugewinn in etwa gleich einzuschätzen ist, sprechen für einen Einstieg in Option 1 – und damit die Technologie der Gesichtserkennung – die geringen Kosten, die Beibehaltung bestehender Prozesse sowie eine vermutlich größere Akzeptanz bei der Bevölkerung. Dazu käme, dass diese Option einen Übergang zu anderen grundsätzlich offen ließe. Dagegen spricht ein gewisser Konservativismus des Ansatzes, der zunächst keinerlei innovationsfördernde Impulse gibt oder einen Zusatznutzen erschließt.

Option 2 bringt grundsätzlich einen höheren Kostenaufwand mit sich und wirft die Frage auf, wie sich die Akzeptanz eines flächendeckenden Enrollments von Bundesbürgern gestaltet. Andererseits wäre durch die Beibehaltung der Dokumentenfamilie eine gewisse Kontinuität gewahrt, und es wäre ein höheres technologisches Niveau erreichbar.

Option 3 verknüpft die Dimension der Sicherheit mit einer innovationspolitischen Perspektive. Zwar fallen hier die meisten Kosten an, es würde aber vermutlich mit der Einführung einer modernen Karte ein innovativer Weg beschritten, der auch wirtschaftliche Impulse vermittelt. So würde für Bundesbürger (mittelfristig auch für hier lebende ausländische Bürger) ein Dokument bereitgestellt, das nicht nur die konventionelle Authentifikation erlaubt, sondern auch

als Eckpfeiler einer elektronischen Unterschrift für den elektronischen Geschäftsverkehr einsetzbar wäre.

Rechtsgrundlagen

Das im Januar 2002 in Kraft getretene Gesetz zur Bekämpfung des internationalen Terrorismus („Terrorismusbekämpfungsgesetz“) enthält als ein wichtiges Element die Regelung der Aufnahme biometrischer Merkmale in Pässe und Personalausweise von Deutschen sowie in Ausweisdokumente für Ausländer. Das Gesetz sieht vor, dass neben dem Lichtbild und der Unterschrift weitere Merkmale in den Pass und Personalausweis – auch in verschlüsselter Form – aufgenommen werden dürfen. Gleichzeitig wird durch neue Vorschriften die Aufnahme derartiger biometrischer Merkmale auch in die Identifikationspapiere von Ausländern und Asylbewerbern ermöglicht. Die Arten der biometrischen Merkmale, ihre Einzelheiten, die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung sollten durch ein noch zu erlassendes Ausführungsgesetz bzw. eine Rechtsverordnung gesondert geregelt werden. Damit beabsichtigt der Gesetzgeber, die Möglichkeiten zur computergestützten Identifizierung von Personen auf der Grundlage der Ausweisdokumente zu verbessern, u.a. um zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen. Zur augenblicklichen gesetzlichen Grundlage ist folgendes anzumerken (Kap. V):

– Hinsichtlich der Ausweispapiere für Bundesbürger hat der Gesetzgeber geregelt, dass die biometrischen Merkmale nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung ausgelesen und verwendet werden dürfen, so dass dem aus dem Grundrecht auf informationelle Selbstbestimmung hergeleiteten *Zweckbindungsgrundsatz ausreichend Rechnung getragen* ist. Anders ist der Bereich der „Ausländerausweise“ zu beurteilen. Hier ist die Aufnahme biometrischer Merkmale geregelt, *es fehlt aber vollständig eine ausreichend bestimmte Zwecksetzung*. § 5 Abs. 7 AuslG enthält eine pauschale Verarbeitungsbefugnis für alle Stellen im Rahmen ihrer gesetzlichen Aufgaben. Dies ist mit den verfassungsrechtlichen Vorgaben zur Zweckbindung und dem Bestimmtheitsgebot nicht in Einklang zu bringen.
– Der Gesetzgeber hat eine Beschränkung der in Betracht kommenden biometrischen Merkmale auf solche von „Fingern oder Händen oder Gesicht“ vorgenommen. Damit sind nicht nur andere, sondern ist auch die Kombination mehrerer Merkmale ausgeschlossen. *Diese Einschränkung* ist nach heutigem

technischem Kenntnisstand *problematisch*, da hierdurch u.U. die Leistungsfähigkeit biometrischer Systeme nicht auszuschöpfen ist.

– Hinsichtlich der Auswahl der einzelnen in Betracht kommenden biometrischen Merkmale ist zu berücksichtigen, dass bei der Anwendung biometrischer Verfahren sensible, persönlichkeitsbezogene Zusatzinformationen anfallen können. Deshalb ist es notwendig, die mit der Aufnahme der biometrischen Merkmale verbundenen Risiken zu begrenzen. In Betracht kommt hierfür vor allem ein *Verzicht auf die Speicherung von Rohdaten*.
– Die vom Gesetzgeber – ohne nähere Vorgaben – geschaffene Befugnis, die Merkmale und Angaben auch in verschlüsselter Form in das jeweilige Dokument zu integrieren, macht eine genaue *Regelung* der Frage erforderlich, *in welcher Weise eine Verschlüsselung vorzunehmen* ist bzw. die biometrischen Daten mit einer elektronischen Signatur zu signieren sind. Angesichts der hierfür erforderlichen Sicherheitsumgebung erscheint *eine zentrale Erstellung der Dokumente vorzugswürdig*.
– Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger zurzeit gesetzlich ausgeschlossen. Eine Speicherung auf dem Ausweisdokument genügte, um den gesetzlichen Zweck zu erreichen. Die Einrichtung zentraler Referenzdateien für Ausländer ist gesetzlich nicht ausgeschlossen. Eine *zentrale Datenspeicherung* bei öffentlichen Stellen und ohne strenge Zweckbindung ist jedoch aus Gründen der Ungleichbehandlung im Sinne des Art. 3 GG und des Prinzips der Verhältnismäßigkeit *problematisch*. Eine dezentrale Speicherung der Daten in einem Register würde z.B. die Verwendung zu strafrechtlichen Ermittlungszwecken oder zur „Rasterfahndung“ ermöglichen. Die Speicherung biometrischer Merkmale in einem Datenbestand, der nicht der alleinigen Verfügungsgewalt des Betroffenen unterliegt, *birgt die Gefahr einer Zweckentfremdung* und ist datenschutzrechtlich problematisch.

  Für die Speicherung der biometrischen Merkmale von Ausländern wäre im Lichte des Grundrechts auf informationelle Selbstbestimmung eine Speicherung außerhalb des Ausweisdokumentes bei einer dezentralen oder zentralen Ausländerbehörde aber vertretbar, wobei eine ausschließliche Bindung an Zwecke der Datensicherung gesetzlich vorgesehen werden müsste.

Weiterer Bedarf an Information, Diskussion und Entscheidung

Auf *Gesetzes- und Verordnungsebene* sind wichtige Aspekte der Umsetzung der bislang getroffenen gesetzlichen Regelungen zu klären. Die Vorentscheidungen

des Gesetzgebers werden dabei wahrscheinlich neu zu diskutieren sein. Hier ist z.B. der Umstand zu nennen, dass für die Regelung der Aufenthaltstitel für Ausländer eine präzise Zwecksetzung für die Nutzung biometrischer Daten bislang nicht erfolgt ist. Eine wohl definierte Zweckbindung würde aber datenschutzrechtliche Bedenken weitgehend ausräumen und die durch den Gesetz- und Verordnungsgeber verfolgten Ziele transparent machen.

Zu klären wäre weiter, ob die vorgenommene Beschränkung der in Betracht kommenden biometrischen Merkmale auf solche von „Fingern oder Händen oder Gesicht“ zukünftig noch Bestand haben sollte oder ob nicht auch die Kombination mehrerer Merkmale bzw. Systeme rechtlich eröffnet werden soll. Damit könnte u.U. die Leistungsfähigkeit biometrischer Systeme besser ausgeschöpft werden.

Angesichts der Schutzwürdigkeit biometrischer Daten als personenbezogene Daten ist es notwendig, die mit ihrer Aufnahme möglicherweise verbundenen problematischen Folgen zu begrenzen. Dementsprechend sollte vor allem auf die Speicherung von Rohdaten verzichtet und dem Prinzip der Datensparsamkeit Geltung verschaffen werden.

Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger zurzeit gesetzlich ausgeschlossen, die Einrichtung zentraler Referenzdateien für Ausländer aber nicht. Eine solche zentrale Datenspeicherung wäre jedoch aus Sicht des Datenschutzes problematisch. Dies gilt grundsätzlich auch für die Speicherung in dezentralen Registern. Geklärt werden sollte, in welchem Verhältnis AFIS (Automated Fingerprint Identification System), das auch einer Identifizierung von Ausländern dient, und der Einsatz von Biometrie auf „Ausländerausweisen“ mit dem gleichen Zweck stehen.

Politischer Diskussions- und Handlungsbedarf ergibt sich auch daraus, dass umfassende *Implementierungsschritte* auf allen Ebenen zu *planen* und in ihren *Konsequenzen* zu *durchdenken* sind – von der Ausstellungs- bis zur Kontrollebene. Weitere Abstimmungsprozesse auf EU-Ebene und letztlich weltweit sind erforderlich, will man mehr Sicherheit erreichen und zugleich weder den globalen Reiseverkehr unangemessen beeinträchtigen noch Belange des Datenschutzes verletzen. Von Bedeutung dürfte auch die Präsenz deutscher Vertreter in den Gremien der International Civil Aviation Organization und der EU sein, um dort eigene Beiträge einzubringen und nationale Interessen zu vertreten.

Die politischen, finanziellen und organisatorischen Konsequenzen einer Einführung und Nutzung biometrischer Identifikationssysteme auf allen Ebenen, sind erst in Ansätzen durchdacht. Hier wären umfassende *Folgenanalysen* an-

gebracht, die Fingerzeige für eine politische und datenschutzrechtliche Gestaltung der bereits jetzt eingetretenen Entwicklungsdynamik liefern.

Ein so umfangreiches und komplexes Vorhaben wie die biometrische Vermessung aller Bundesbürger sowie von Millionen von ausländischen Bürgern, die nach Europa einreisen oder Asyl suchen, legt es nahe, die Frage nach der Akzeptanz zu stellen. Zu den Bemühungen um technische Praktikabilität sollten deshalb solche um *gesellschaftliche Akzeptabilität* treten. Zahlreiche Fragen, zu denen bislang nur wenig eindeutige Antworten zu finden waren, müssten in einem transparenten „öffentlichen Diskurs" angesprochen werden. Mehr Klarheit und größere Differenziertheit hätte vor allem die Erörterung der Frage verdient, welche Beiträge zu welchen Zielen mit welchen biometrischen Dokumenten erbracht werden können und sollen.

Im Lichte dieser Diskussion wären des Weiteren die Eignung technischer Lösungen und die Vertretbarkeit unterschiedlicher Kostenvolumina vergleichend zu diskutieren. Dabei käme es insbesondere darauf an, klar zu machen, dass Biometrie nur einen begrenzten Zielbeitrag zu mehr Sicherheit leisten kann. Biometrie ist ein technischer Ansatz von Prävention und Kontrolle und somit nur ein – wenngleich wesentliches – Element einer übergreifenden Strategie.

Ferner sollte das Spannungsfeld zwischen dem Ziel Sicherheit einerseits sowie den Zielen Schutz der Privatsphäre und Begrenzung des Missbrauchspotenzials andererseits offen diskutiert und durch technische und rechtliche Maßnahmen reduziert werden.

Letztlich wäre die Meinungsbildung und Entscheidungsfindung auch um Fragen und Ziele der Innovationspolitik anzureichern: Gemeinsam mit Entwicklern und Anbietern sollten Strategien entwickelt werden, die auf einen technologischen Sprung vom bisherigen Dokumentenkonzept zu einer Smartcard-basierten Lösung zielen. Für deutsche Unternehmen, die im internationalen Wettbewerb grundsätzlich gut positioniert sind, eröffnet ein solches technisch-gesellschaftliches Innovationsprojekt die Perspektive, mit eigenen Produkten und Dienstleistungen Wettbewerbsvorteile zu erzielen.

Ein transparenter öffentlicher Diskurs könnte geeignet sein, ein Bewusstsein für die Bedeutung der Dynamik der gesellschaftlich-technischen Entwicklung zu schaffen, die mit der zukünftig intensiven Nutzung der Biometrie verbunden sein dürfte.

I. Einleitung

Die weltweit diskutierte und teilweise bereits implementierte Option einer biometrischen Ausrüstung von Ausweisdokumenten und entsprechender biometriegestützter Kontrollen an Grenzübergängen kann primär als eine *Reaktion* auf die *veränderte Sicherheitslage seit dem 11. September 2001* gesehen werden. In vielen Staaten sind mit Gesetzen und Verordnungen, aber auch mit Tests, Pilotprojekten und Machbarkeitsstudien erste Grundlagen gelegt worden. Die USA haben mit mehreren Gesetzen sowie im Zuge der sukzessiven Intensivierung der Grenzkontrollen seit längerem den Weg in Richtung eines biometrisch gestützten Systems der Einreisekontrolle beschritten. Die Staatengruppe der G8 hat eigene Aktivitäten entwickelt und unterstützt insbesondere die Bemühungen der International Civil Aviation Organization (ICAO) bei ihren Bemühungen um eine weltweite Standardisierung bei internationalen Reisedokumenten. Auf EU-Ebene sind ebenfalls politische und rechtliche Weichenstellungen erfolgt, die die Voraussetzungen für eine harmonisierte biometrische Nutzung bzw. Ausrüstung von Ausweisdokumenten, Visa und Aufenthaltstitel für Drittstaatenbürger schaffen sollen.

In Deutschland sind hierzu das Pass- und Personalausweisgesetz und das Ausländergesetz geändert worden: Eine Einbringung zusätzlicher biometrischer Merkmale (Gesicht oder Finger oder Hand) in Ausweisdokumente für Bundesbürger und Ausländer kann jetzt vorgenommen werden. Es besteht aber *weiterer Bedarf an Information, Diskussion und Entscheidung*: Auf Gesetzes- und Verordnungsebene sind wichtige Aspekte der Umsetzung der bislang erfolgten gesetzlichen Regelung zu klären. Die politischen, finanziellen und organisatorischen Konsequenzen sowie mögliche Konflikte, z.B. zwischen den Zielen, mehr Sicherheit zu erreichen und die Privatsphäre zu schützen, sind erst in Ansätzen durchdacht.

Ein zentrales Dilemma, mit denen sich Entscheidungsträger konfrontiert sehen, ist der Umstand, dass mittlerweile zwar sehr viel bessere Informationen über die durchaus fortgeschrittene Leistungsfähigkeit biometrischer Systeme vorliegen. Mit der biometrischen Modernisierung von nationalen Ausweisdokumenten für den Reiseverkehr und der Anwendung bei Grenzkontrollen ist aber eine Aufgabe mit so erheblichen Dimensionen zu lösen, dass bisherige Erfahrungen mit Pilotprojekten bei Grenzkontrollen hierzu allenfalls indirekt Erkenntnisse liefern.

Diese schwierige Ausgangslage lässt sich am Beispiel der USA verdeutlichen: Dort reisen jährlich 500 Mio. Menschen ein, darunter sind 350 Mio. Ausländer. In allen Konsulaten der USA wurden 2002 8,4 Mio. Visaanträge gestellt. Die Einreise erfolgt an ca. 400 Grenzübergängen (IBG 2003, S. 2). Diese Volumina und die Komplexität der administrativen und technischen Dimensionen erhöhen sich nochmals, wenn man sich vergegenwärtigt, dass eigentlich nur ein globales Konzept zum Management internationaler Reiseströme und Migrationsbewegungen geeignet ist, die Potenziale der Biometrie bei Effizienz, Komfort und Sicherheit auszuschöpfen. Schließlich dürfte auch die Kostenfrage nicht trivial sein.

Seit Vorlage des ersten Sachstandsberichtes des TAB (TAB-Arbeitsbericht Nr. 76; Drucksache 14/10005 vom 10. Oktober 2002) zielten die Aktivitäten des TAB auftragsgemäß darauf, die technische Entwicklung sowie die politische und rechtswissenschaftliche Diskussion auf dem Felde der biometrischen Identifikationssysteme zu verfolgen. Ergänzend wurde der Versuch unternommen, weltweite Aktivitäten bei mit biometrischen Merkmalen ausgestatteten Personalausweisen, Pässen und Visa zu identifizieren, um hier einen Überblick zu gewinnen.

Entsprechend ist es das *Ziel des zweiten Sachstandsberichtes des TAB* zu biometrischen Identifikationssystemen, eine Einschätzung der Leistungsfähigkeit und Eignung dieser Technologien und entsprechender Systemlösungen bei Ausweisdokumenten und Grenzkontrollanwendungen zu geben sowie Anforderungen an eine rechtsverträgliche und datenschutzfreundliche Umsetzung zu definieren. Der Bericht ist dementsprechend nicht das Resultat einer umfassenden Technikfolgen-Abschätzung. Vielmehr dokumentiert er eine thematisch eingegrenzte, aktuelle Bestandsaufnahme der wissenschaftlichen und politischen Diskussionen. Damit soll ein Beitrag zur Verbesserung der Informations- und Diskussionsgrundlagen für die Arbeit der Fachausschüsse des Deutschen Bundestages geliefert werden.

Zu diesem Zweck *ist der Bericht folgendermaßen aufgebaut*: Das folgende Kapitel II zeichnet ein Bild des Standes der weltweiten politischen Aktivitäten, die das Ziel verfolgen, mithilfe biometrischer Verfahren Ausweis- und Reisedokumente fälschungs- und missbrauchssicherer zu machen und mehr Sicherheit bei Grenzkontrollen zu erreichen. Kapitel III illustriert diese Tendenz durch eine aktuelle Momentaufnahme von Pilotprojekten und bereits heute implementierten Grenzkontrollanwendungen sowie von Planungen und Umsetzungen von Programmen zur biometrischen Nutzung und Ausrüstung von Ausweisdokumenten insbesondere für den internationalen Reiseverkehr. In Kapitel IV wird der aktuelle Stand der Diskussion zur Leistungsfähigkeit und Eignung biome-

trischer Technologien zusammengefasst. Kapitel V dient einer kritischen Darstellung und Diskussion der mit dem Terrorismusbekämpfungsgesetz geschaffenen Grundlagen für die zukünftige biometrische Nutzung von Ausweisdokumenten für Bundesbürger und Ausländer sowie des weiteren Bedarfs an Klärung ihrer Zwecke und Modalitäten. Kapitel VI spricht den weiteren Diskussions- und Handlungsbedarf an.

Wesentliche Inhalte dieses Berichtes basieren auf folgenden, im Rahmen des Monitorings vergebenen Gutachten: Die Firmen Booz Allen Hamilton GmbH, Bundesdruckerei GmbH und ZN Vision Technologies AG haben mit ihren Analysen umfassend zum Kapitel IV beigetragen. Die Steinbeis GmbH & Co. KG für Technologietransfer – Steinbeis-Transferzentrum Biometrie und Identifikationslösungen führte im Rahmen ihres Gutachtens u.a. eine internationale Recherche durch, die die Basis für Kapitel III legte. Ergänzend wurde ein Gutachten der Firma B&L Management Consulting GmbH herangezogen, das besonders für die Abfassung des Kapitel IV hilfreich war. Die rechtlichen Aspekte biometrischer Identifikationssysteme, denen das Kapitel V gewidmet ist, sind in einem Rechtsgutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein erschlossen worden. Allen Gutachterinnen und Gutachtern möchten wir für ihre Arbeit und ihre Bereitschaft zu einem kontinuierlichen Meinungsaustausch mit der Projektbearbeiterin und den Projektbearbeitern danken. Sie haben mit ihren Beiträgen den Bericht in dieser Form möglich gemacht. Für die Auswahl und Fokussierung sowie die letztliche Integration der jeweiligen Gutachten in den Bericht des TAB zeichnet das Projektteam verantwortlich.

TAB

II. Aktuelle politische Rahmenbedingungen

Auf nationaler, europäischer und US-amerikanischer Ebene wurden in den letzten Jahren verschiedene Schritte unternommen, das Pass- und Personalausweiswesen, die Asylverfahren sowie die Einreisebestimmungen sicherer zu machen und zu harmonisieren. Die Möglichkeiten zur Nutzung biometrischer Verfahren sind hierbei vielfach geschaffen und ihre Umsetzung ist angegangen worden. Neben der Erarbeitung und Umsetzung von Gesetzen und Verordnungen fördert die Politik verschiedene Forschungsvorhaben und Praxistests, um die Verwendung biometrischer Merkmale in Reisedokumenten zu prüfen und weiter auszuschöpfen.

Im Folgenden wird ein Überblick über die Entwicklungen auf der internationalen und nationalen politischen Ebene gegeben, deren Dynamik gerade in letzter Zeit erheblich zugenommen hat.

1. Europäische Union

In der Folge der Anschläge vom 11. September 2001 ist insbesondere durch die Europäische Kommission eine Reihe von Initiativen ergriffen worden. Diese zielen darauf, EU-weit *eine abgestimmte, kohärente Strategie* für eine verbesserte Sicherheit bei Asylverfahren, den Visa und den Aufenthaltstiteln für Drittstaatenangehörige sowie bei den Pässen von EU-Bürgern zu entwickeln und umzusetzen.

EURODAC

Asylbewerber und illegale Zuwanderer in die Mitgliedsstaaten der EU werden seit Januar 2003 europaweit mit dem automatisierten Fingerabdruckidentifizierungs-System *AFIS* erfasst. Ihre Fingerabdrücke werden in dem länderübergreifenden System *EURODAC* gespeichert und verglichen. Dadurch sollen Mehrfachanträge eines Asylbewerbers in verschiedenen Ländern der EU ausgeschlossen sowie unerlaubt in das Unionsgebiet eingereiste Personen erkannt werden. Wird festgestellt, dass ein Bewerber bereits in einem Land einen Antrag gestellt hat, wird er dorthin zurückgeschickt. Rechtliche Grundlage von EURODAC ist das Dubliner Übereinkommen, das seit September 1997 den

asylrechtlichen Teil des Schengener Durchführungsübereinkommens ersetzt. Danach soll nur noch ein Mitgliedsstaat für die Prüfung eines Asylantrages zuständig sein, und zwar grundsätzlich der Staat, der die Einreise des jeweiligen Bewerbers zu verantworten hat. Nach In-Kraft-Treten der EURODAC-Verordnung (VO EG/407/2002) ist seit dem 15. Januar 2003 jeder EU-Mitgliedsstaat verpflichtet, die Fingerabdrücke jedes mindestens 14 Jahre alten Asylbewerbers und Ausländers, der in Verbindung mit dem unerlaubten Überschreiten einer Dubliner-Außengrenze aufgegriffen und nicht zurückgewiesen wurde, aufzunehmen und unverzüglich an EURODAC zu übermitteln.[1]

Durch die Einführung von EURODAC ist auch bei AFIS mit Änderungen zu rechnen: Erste Feldversuche mit der so genannten Live-Scan-Technologie haben im Polizeibereich stattgefunden. Fingerabdrücke sollen in Zukunft digital, also nicht mehr mit Druckerschwärze, aufgenommen und gespeichert werden. Das so genannte METAMORPHO-Verfahren (Auswertung und Vergleich der Handflächen, in Ergänzung der bisherigen zehn Fingerkuppen) wird dabei die Anbindung von Live-Scan-Stationen an das weiterhin u.a. vom BKA genutzte AFIS ermöglichen (Bundesbeauftragter für den Datenschutz 2003).

Visa und Aufenthaltstitel für Drittstaatenangehörige

Von Relevanz für die zukünftige Entwicklung des Einsatzes von Biometrie in Ausweisdokumenten und bei Grenzkontrollen sind – neben den EURODAC-Verordnungen – auch die *Verordnungen zur einheitlichen Visagestaltung*, insbesondere VO EG/1683/95, Art. 1, 6, geändert durch VO EG/334/2002 vom 23. Februar 2002. Diese sehen bislang die Integration eines „gemäß Hochsicherheitsnormen hergestellten Lichtbildes“ in Visadokumenten vor. Bindend für die nationalen Gesetz- und Verordnungsgeber sind vor allem die Maßstäbe der Fälschungssicherheit, die Aufnahme weiterer biometrischer Merkmale ist hier nicht ins Auge gefasst.

Ferner sieht das Schengen-Akquis, insbesondere das Schengener Durchführungsübereinkommen (SDÜ), *gemeinsame Regelungen für die sichtvermerksfähigen Reisedokumente* sowie Form, Inhalt und Gültigkeitsdauer der Sichtvermerke insbesondere für kurzfristige Aufenthalte vor (Art. 17 Abs. 3 SDÜ). Entsprechende Entscheidungen werden durch einen Exekutivausschuss getrof-

1 Bis 2004 soll das System ca. zwei Mio. Antragsteller verwalten, etwa 500.000 Datenvergleiche pro Sekunde ermöglichen und mit einer Genauigkeit von 99,9 % arbeiten (Computerwoche 2003, S. 33).

fen. Insoweit dürfte der deutsche Gesetz- und Verordnungsgeber an die Vorgaben des Ausschusses gebunden sein. Sichtvermerke für längere Aufenthalte (länger als drei Monate) werden gemäß Art. 18 SDÜ nach Maßgabe des nationalen Rechts erstellt. Auch hier sind keine verbindlichen Mindeststandards hinsichtlich der Aufnahme biometrischer Merkmale vorgesehen.

Gleiches ergibt sich auch aus der *Verordnung* EG/1030/2002 *zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige* vom 13. Juni 2002, die in jedem Mitgliedsstaat unmittelbare Geltung hat. Die Verordnung verlangt als biometrisches Mindestmerkmal die Einbringung eines Lichtbildes. Die Aufnahme weiterer biometrischer Merkmale ist nicht vorgesehen. Allerdings weist Erwägung 6 der genannten Verordnung darauf hin, dass die Mitgliedsstaaten und die Kommission in regelmäßigen Abständen diese Option prüfen.

Mit der Vorlage eines Vorschlags vom 24. September 2003 zur Änderung der o.g. Verordnung EG/1683/95 des Rates über eine einheitliche Visagestaltung sowie zur Änderung der Verordnung EG/1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige *hat die Europäische Kommission die Entwicklung weiter vorangetrieben*.

In der Begründung wird auf die Bemühungen zur Verbesserung der Dokumentensicherheit auf europäischer Ebene infolge der Anschläge vom 11. September 2001 Bezug genommen (Europäische Kommission 2003b). Übergreifendes Ziel sei, Personen aufzuspüren, die mit gefälschten amtlichen Dokumenten in die EU einreisen wollen.

Die Mitgliedsstaaten – so die Kommission weiter – hätten zuletzt auf der informellen Tagung ihrer Justiz- und Innenminister am 28. und 29. März 2003 in Veria darauf hingewiesen, dass sie eine Erhöhung der Sicherheitsstandards und eine Vereinheitlichung von Visa und Reisedokumenten allgemein begrüßten und biometrische Identifikatoren in Visa und Aufenthaltstiteln für Drittstaatler befürworteten. Der Europäische Rat schließlich habe am 19./20. Juni 2003 in Thessaloniki bekräftigt, dass „in der EU ein kohärenter Ansatz in Bezug auf biometrische Identifikatoren oder biometrische Daten verfolgt werden muss, der in harmonisierte Lösungen für Dokumente für Staatsangehörige von Drittländern, Pässe von EU-Bürgern und Informationssysteme (VIS und SIS II) mündet“. Der Rat habe die Kommission aufgefordert, „entsprechende Vorschläge auszuarbeiten und mit dem Bereich Visa zu beginnen“ (Europäische Kommission 2003b, S. 3).

Das Gesicht ist nach den Vorschlägen der Kommission das wichtigste biometrische Merkmal, um Interoperabilität zu gewährleisten. Es soll den Mitglieds-

staaten überlassen bleiben, ob sie an der Grenze nur eine Kontrolle mittels der auf einem Bildschirm projizierten digitalen Fotografie oder – als anspruchsvollere Lösung – mittels einer biometrischen Gesichtserkennung durchführen wollen. Die Wahl der Technologie soll im Ermessen der Mitgliedsstaaten liegen, vorausgesetzt die von der ICAO entwickelten *Qualitätsnormen für digitale Lichtbilder* werden erfüllt. Als ein zweites biometrisches Merkmal soll der Abdruck zweier Finger aufgenommen werden, da der Fingerabdruck sich am besten für den Abgleich mit Datenbanken eigne. Die Aufnahme dieses zweiten Identifikators soll für die Mitgliedsstaaten verpflichtend sein, vor allem deshalb, weil für eine ausreichende Übereinstimmungsquote mindestens zwei biometrische Identifikatoren erforderlich seien. Die biometrischen Daten sollen in einem Speicherelement mit ausreichender Kapazität gespeichert werden. Der *Zeitplan* sieht zunächst ein Lichtbild als biometrisches Merkmal bis 03. Juni bzw. 14. August 2005 vor. Danach soll die digitale Aufnahme und Speicherung des Lichtbildes innerhalb von zwei Jahren und der Fingerbilder innerhalb von drei Jahren nach der Annahme entsprechender Spezifikationen erfolgen (Europäische Kommission 2003b).

Schengen-Informationssystem, Visa-Informationssystem

In engem zeitlichen Zusammenhang mit der Einigung des Rates der Europäischen Union auf die Integration des biometrischen Merkmals Gesicht in Form eines Lichtbildes in Visa hatte der EU-Ministerrat beschlossen, den 1990 installierten Zentralcomputer der Schengen-Staaten zu ersetzen und ihn u.a. um die Funktionen von *SIS* (Schengen-Informationssystem) zu erweitern. Dieses Informationssystem ist für 18 Staaten ausgelegt (15 Mitgliedsstaaten, Island, Norwegen und ggf. ein weiteres Mitglied). Allerdings ist die Technologie von SIS der ersten Generation inzwischen überholt, neue Entwicklungsoptionen wurden geprüft, und neue Funktionen sind vorgesehen: Neben dem reinen Informationssystem soll ein Ermittlungssystem eingerichtet werden; dazu müssen neue Datenkategorien festgelegt werden. Schwerpunkte müssten die „Prävention und Erkennung von Bedrohungen der öffentlichen Ordnung und Sicherheit und weniger die Ermittlung im Bereich der organisierten Kriminalität“ sein, so die Europäische Kommission (Tätigkeitsbereiche der Europäischen Union, Justiz und Inneres, Informationssystem Schengen II; http://europa.eu.int/scadplus/leg/de/s22000.htm).

Zu den Vorschlägen für eine Erweiterung des Schengen-Informationssystems (*SIS II*) gehört auch, zusätzliche Identifikationsdaten zu erheben. Da die Regelung über die Integration des Lichtbildes in EU-Visa bereits am 03. Juni 2002 in Kraft getreten ist, könnte beispielsweise das Lichtbild und damit die biometrische Gesichtsinformation im SIS allen Mitgliedsstaaten zur Nutzung an Grenzkontrollposten zur Verfügung gestellt werden (Booz Allen Hamilton et al. 2003, S. 40).

In den am 13. Juni 2002 angenommenen Leitlinien misst der Europäische Rat dem Visa-Informationssystem (*VIS*) als einem System zum Austausch von Visadaten zwischen den europäischen Mitgliedsstaaten hohe Bedeutung zu. Das System solle u.a. „folgende Ziele verwirklichen: Bekämpfung des Visabetrugs, Verhütung des sog. Visa Shopping und Verbesserung der konsularischen Zusammenarbeit“ (Europäisches Parlament 2003, S. 4). Um diesen Zielen gerecht werden zu können, wird VIS ein sog. „Central Visa Information System“ (C-VIS) und in jedem Mitgliedsstaat ein „National Visa Information System“ (N-VIS) umfassen. In einer von der Europäischen Kommission erstellten *VIS-Durchführbarkeitsstudie* wird der Fingerabdruck aller zehn Finger eines Antragstellers befürwortet, da nur dieses Verfahren nachweislich ein hohes Maß an Erkennungssicherheit liefere.[2] Das Dokument soll zwei Fingerabdrücke enthalten.

Die Kommission verfolgt mit ihren Vorschlägen zwei Ziele: Erstens soll die Frist zur Umsetzung der Lichtbild-Bestimmung von 2007 auf 2005 vorverlegt werden und zweitens sollen die Mitgliedsstaaten verpflichtet werden, auf eine harmonisierte Art und Weise biometrische Identifikatoren in Visa und Aufenthaltstitel für Drittstaatenangehörige zu integrieren und Interoperabilität zu gewährleisten. Maßnahmen, die die Dokumente der EU-Bürger betreffen, sollen noch in diesem Jahr folgen.

Aktuelle Studien und Forschungsprojekte

Initiiert durch die Europäische Kommission, gründete sich 2002 das *BIOVISION Consortium*, ein Zusammenschluss verschiedener Organisationen aus Großbritannien, Irland, Italien, Deutschland, Dänemark und den Niederlanden. Dieses

2 Ziel dieser Studie war es, die praktische Durchführbarkeit eines Systems für den Austausch von visumspezifischen Daten zwischen den Mitgliedsstaaten einschließlich der dafür erforderlichen Finanz- und Humanressourcen zu prüfen. Abzuschätzen war der Umfang der zu speichernden Daten und der Zeitpunkt, zu dem die erforderlichen Daten in das VIS aufgenommen werden können.

Konsortium legte der Europäischen Kommission am 28. August 2003 eine Roadmap vor, die die zukünftige Entwicklung der biometrischen Schlüsseltechnologien aufzeigt, insbesondere die innerhalb der Europäischen Union (Biovision 2003). Die Roadmap versucht, Bedingungen zu benennen, die biometrischen Anwendungen in europäischen Schlüsselmärkten förderlich sein könnten; der Fokus wird also auf wirtschaftliche Anwendungen und weniger auf Anwendungen im Bereich des Pass- und Ausweiswesens gelegt.

Am 21. Juli 2003 wurde in der Nachfolge von BIOVISION das *European Biometric Forum (EBF)* etabliert. Dem EBF gehören Experten und Vertreter aus Wirtschaft und Gesellschaft an, die den Markt für biometrische Anwendungen in und aus Europa einschätzen sollen. Damit wird der Versuch unternommen, Entwicklern und Anbietern biometrischer Anwendungen ein Forum zu bieten sowie den europaweiten Austausch von technologischem Wissen und von Erfahrungen aus biometrischen Anwendungen zu fördern (http://www.eu-biometricforum.com).

Im Zusammenhang mit dem Erlass von Leitlinien zur Einrichtung eines gemeinsamen *Visa-Informationssystems* (VIS) durch den Europäischen Rat im Juni 2002 wurde die Europäische Kommission aufgefordert, eine *Durchführbarkeitsstudie* auf der Grundlage dieser Leitlinien zu erstellen. Die vorgelegte Studie enthält eine Analyse der technischen und finanziellen Aspekte von VIS. Im Ergebnis wird die Bedeutung biometrischer Merkmale für die Effizienz des Systems ausdrücklich hervorgehoben. Fingerabdrücke und Gesicht werden als biometrische Identifikatoren empfohlen: Mit der Fingerabdrucktechnik wäre die notwendige Genauigkeit gewährleistet, um Personen identifizieren zu können, und die Fingerabdruck-Datenbanken könnten auch dann noch genutzt werden, wenn neue biometrische Techniken eingeführt würden. Durch die Verwendung eines zweiten biometrischen Identifikators (Gesicht) könnte die Identifikationsgenauigkeit noch weiter verbessert werden (Europäische Kommission 2003a, S. 4). Die geschätzten Investitionskosten lägen zwischen 130 Mio. und 200 Mio. Euro, die Einrichtung von VIS könnte bis zu zwölf Jahre in Anspruch nehmen.

Im Bereich der *Forschung zu biometrischen Basistechnologien* finanziert die EU derzeit das Projekt VIPBOB (VIrtual Pin Based On Biometrics; Laufzeit: 01.03.2002–29.02.2004). Es widmet sich dem Einsatz von Biometrie als PIN, der Verknüpfung von Biometrien und kryptografischer Authentisierung sowie der Kompatibilität mit bereits bestehenden Infrastrukturen. In den vergangenen Jahren hatte die EU in diesem Forschungsbereich weitere Projekte initiiert und finanziert: z.B. SABRINA mit dem Ziel, sichere Authentifizierungsmöglichkeiten durch eine Ultraschallabtastung der Haut zu entwickeln (Laufzeit:

01.01.2001–31.12.2002), FINGERCARD, in dessen Verlauf die Integration von Fingerbildsensoren in Smartcards untersucht wurde (Laufzeit: 01.01.2001–30.06.2002), sowie das Projekt TUBA (Time-Reserved Mirroring of acoustic waves for biometric authentication; Laufzeit: 01.09.2002–30.04.2003).

Die EU unterstützt außerdem *Forschungsprojekte*, die sich mit konkreten *biometrischen Anwendungen* befassen: Derzeit läuft z.B. das Projekt S-TRAVEL, in dessen Rahmen Standardlösungen für den sicheren Grenzübertritt entwickelt werden sollen (Laufzeit: 01.11.2002–30.04.2004). Zuvor wurden die Projekte PAIDFAIR (Laufzeit: 01.06.2001–30.11.2002), E-POLL (Laufzeit: 01.09.2000–31.11.2002) und U-FACE (Laufzeit: 02.04.2000–01.10.2002) abgeschlossen.

2. USA

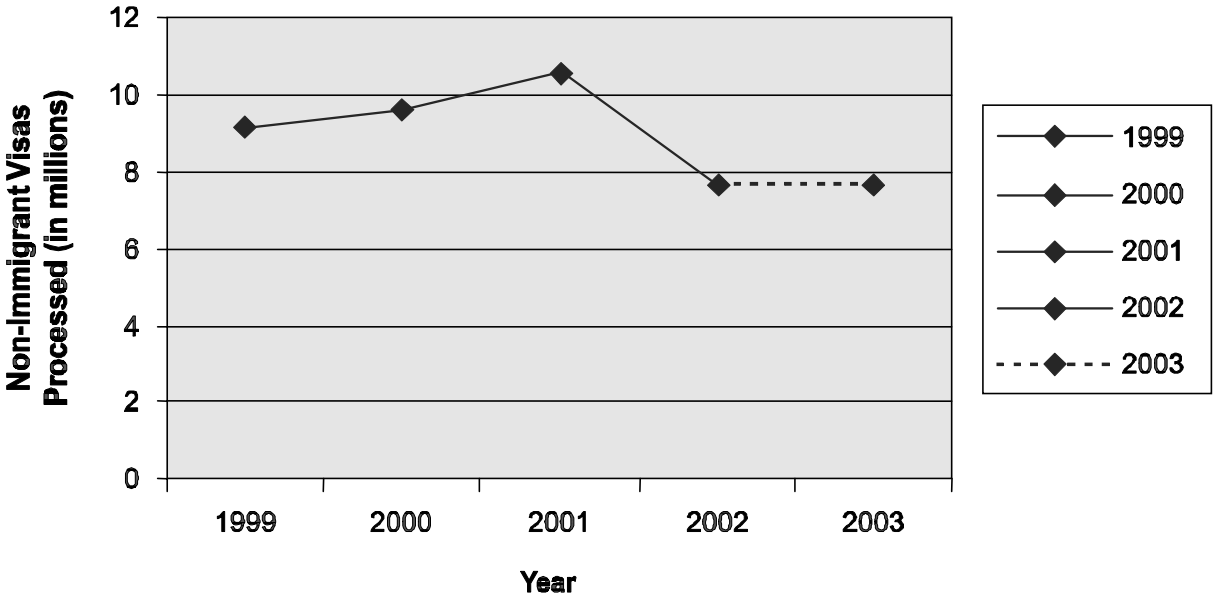
Bereits seit 1993 gibt es in den USA Programme und Projekte für automatisierte Grenzkontrollanwendungen, die biometrische Identifikationssysteme verwenden: So werden zum Beispiel im Rahmen des INS Passenger Accelerated Service System (*INSPASS*) – ein vom „Immigration and Naturalization Service“ (INS) eingerichtetes System für die biometrisch unterstützte Grenzkontrolle – Vielflieger verifiziert (vgl. Kap. III.2).[3]

Im Rahmen des „Border Crossing Card And Border Biometrics Program“ enthalten alle *Border Crossing Cards* (BCC) – die von mexikanischen Staatsbürgern für einen kurzen Aufenthalt in den USA genutzt werden – seit 1998 mindestens ein biometrisches Merkmal. Diese BCC ist laminiert, trägt verschiedene Sicherheitsmerkmale und hat eine zehnjährige Gültigkeit. Die Border Crossing Cards, die an mexikanische Staatsbürger und dauerhaft in Mexiko lebende Bürger anderer Nationalität ausgegeben werden, sind sog. „*laser visas*“. Sie wurden neben den Funktionen der BCC um die eines Visums speziell für Besucher erweitert (http://travel.state.gov/bcc.html). Die bei den Ausstellungsbehörden gespeicherten biometrischen Merkmale der Antragsteller werden elektronisch an den INS übermittelt. Seit dem Jahr 2001 wird zusätzlich zum Fingerabdruck Gesichtserkennung eingesetzt, um Doppelanträge bei den Visa aus-

3 INSPASS ist ein Handgeometrieerkennungs-System, das erstmals im Mai 1993 am JFK-Flughafen in New York pilotiert wurde und derzeit an sieben US-amerikanischen (Los Angeles, Miami, Newark, New York (JFK), San Francicso, Washington-Dullus) und zwei kanadischen Flughäfen (Vancouver, Toronto) im Einsatz ist.

stellenden Behörden zu verhindern. Die Zahl der beantragten Visa insgesamt ging seitdem deutlich zurück (Abb. 1).

Abb. 1: Visabeantragungen in den USA von 1999 bis 2003



Quelle: U.S. Department of State 2002, S. 37

Von Januar bis Juli 2002 lief die Pilotphase des sog. „*National Security Entry-Exit Registration System*“ (NSEERS). Seit 01. Oktober 2002 ist NSEERS an 238 Stellen im operativen Einsatz, u.a. um Einreisende in die USA aus bestimmten Staaten auf kriminelle und terroristische Aktivitäten zu überprüfen. Dazu werden Fotografien und Fingerabdrücke der einreisenden Personen gegen Datenbanken (AFIS-Datenbank und IDENT-Datenbank) abgeglichen. Das NSEER-System integriert mehrere Elemente und Maßnahmen, wie z.B. das Automated Biometric Identification System. NSEERS soll zukünftig in einem umfassenden Entry-Exit-System aufgehen.

Gesetzgebung und Umsetzung legislativer Vorgaben

Seit dem 11. September 2001 wurden drei Gesetze verabschiedet, die den Ein- und Ausreiseablauf von Ausländern in die USA betreffen. Auf der Grundlage des „Aviation and Transportation Security Act“ können Gepäckstücke von Flugreisenden elektronisch überprüft und Informationen zu den Gepäckstücken schneller übermittelt werden. Relevant für das Pass- und Personalausweiswesen

in den USA sind der *US Patriot Act* und der *Enhanced Border Security and Visa Entry Reform Act of 2002*.

Patriot Act

Dieses Gesetz beinhaltet u.a. die zeitnahe und stufenweise Implementierung von sicheren Grenzkontrollsystemen. Vorgesehen ist u.a., ab dem 26. Oktober 2004 nur noch fälschungssichere und maschinenlesbare Visa und Reisedokumente für international Reisende mit biometrischen Merkmalen auszustellen sowie schrittweise Lesegeräte zur Verifikation dieser Dokumente an allen Grenzkontrollpunkten der USA zu installieren. Der angestrebte Stichtag für ein voll funktionsfähiges Entry-Exit-System ist Januar 2006.

Enhanced Border Security and Visa Entry Reform Act

Dieses Gesetz vom Mai 2002 verlangt von allen Staaten, ab dem 26. Oktober 2004 fälschungssichere Reisedokumente mit biometrischen Merkmalen für die Einreise in die USA auszustellen. Diese Regelung gilt auch für Staaten, die am so genannten *Visa Waiver Program* teilnehmen. Die zuständigen Stellen in den USA sind bis spätestens zum gleichen Zeitpunkt verpflichtet, nur noch maschinenlesbare, fälschungssichere und mit biometrischen Merkmalen gemäß ICAO-Standard versehene Visa und andere Reisedokumente auszugeben. An allen Einreiseorten müssen bis 26. Oktober 2004 entsprechende Systeme installiert sein.

Im Zuge der Verschärfung der Einreisebestimmungen in die USA werden damit auch ausländische Regierungen angehalten, neue Ausweisbestimmungen zu verabschieden. Nachdem die kanadische Regierung den US-amerikanischen Vorstellungen im Rahmen eines gemeinsamen *Smart Border Action Plan* bereits nachgekommen ist, sind die anderen am „Visa Waiver Program“ beteiligten Staaten vor die gleiche Entscheidung für (oder gegen) biometrische Ausweisdokumente gestellt.

U.S. VISIT

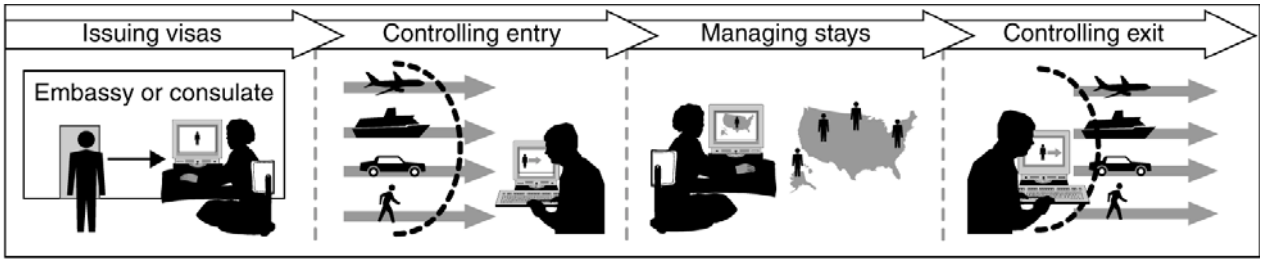
In der Konsequenz der legislativen Vorgaben ist vom *U.S. Department of Homeland Security* (DHS) ein umfassendes Konzept zur Überwachung von Ein- und Ausreise sowie des Aufenthalts entwickelt worden – das *U.S.-„Visitor and Immigrant Status Indication Technology System“* (U.S. VISIT). In dessen Rahmen soll ein umfassendes Entry-Exit-System – zunächst an den Seegrenzen und den

Lufthäfen – implementiert werden, wobei die biographischen Daten und biometrischen Merkmale der Besucher und Einreisenden an den Grenzkontrollpunkten aufgenommen werden (Booz Allen Hamilton et al. 2003, S. 42). Nach Veröffentlichungen des DHS sollen bei U.S. VISIT biometrische Merkmale der Finger und des Gesichtes zum Einsatz kommen. Geplant ist ferner, bereits in den Konsulaten, die die Visa ausstellen, zunächst Fingerbild und Foto abzunehmen. Später könnten weitere Merkmale (wie Iris) und Verfahren einbezogen werden. Die erhobenen Daten wären dann bei der tatsächlichen Einreise in die USA an den Grenzübergängen abrufbar.

Der Zeitplan von U.S. VISIT sieht vor, dass ab dem 01. Januar 2004 von den meisten Besuchern (ausgenommen sind z.B. Reisende unter dem Visa Waiver Program), die an Flughäfen oder Seehäfen in die USA einreisen, ein digitales Foto gemacht und zwei Fingerabdrücke eingelesen werden. Diese Daten werden dann mit Listen abgeglichen, auf denen Personen registriert sind, denen eine Einreise in die USA zu verweigern ist. Gleichzeitig werden der Ausreisetag und die Aufenthaltsadresse festgehalten, damit Personen, die zwar legal einreisen, sich durch die Verzögerung ihrer Ausreise dann aber illegal in den USA aufhalten, rechtzeitig ausgewiesen werden können (Abb. 2).

Abb. 2: Kontrollsystem für die Ein- und Ausreise in die USA

Simplified Diagram of the Border Security Process



Quelle: GAO 2003b, S. 6

Für US-Bürger entfallen die genannten Prozeduren, sie werden also nicht biometrisch erfasst. Das Department of State soll aber „zukünftig“ maschinenlesbare Reisepässe für US-Bürger ausgeben, die biometrische Merkmale des Gesichtes enthalten.

Aktuelle Projekte und Tests

Etwa seit dem Jahr 2000 sind mit Unterstützung bzw. unter der Federführung von Ministerien, Behörden und weiteren Einrichtungen verstärkt Tests zur Überprüfung der Leistungsfähigkeit biometrischer Systeme durchgeführt worden (vgl. Kap. IV). Die folgende Tabelle gibt einen Überblick über ausgewählte, in den USA durchgeführte unabhängige Biometrietests.

Tab. 1: Biometrietests in den USA seit 2000

Name	*ausführende Behörde/Institut*	*abgeschlossen im Jahr*	*Merkmal*
Biometric Product Testing	National Physical Laboratory	2000	Gesicht, Iris, Finger, Hand, Vene, Sprache
Facial Recognition Vendor Test (FRVT 2000)	DoD, National Institute of Justice, NIST	2000	Gesicht
Fingerprint Verification Competition 2000	University of Bologna, Michigan State University, San Jose State University	2000	Finger
Facial Recognition Technology	Department of State, Bureau of Consular Affairs	2001	Gesicht
Personnel Identification Pilot Study	Army Research Laboratory	2001	Gesicht, Iris
Fingerprint Identification Device	Federal Aviation Administration (FAA) und Safe Skies	2001	Finger
Hand Geometry Identification Device	FAA und Safe Skies	2001	Hand
Facial Recognition Device	FAA und Safe Skies	2002	Gesicht
Iris Recognition Device	FAA und Safe Skies	2002	Iris
Fingerprint Verification Competition 2002	University of Bologna, Michigan State University, San Jose State University	2002	Finger
Face Recognition Vendor Test (FRVT 2002)	15 Organisationen, u.a. DoD, NIST und National Institute of Justice	2003	Gesicht

Quelle: Eigene Darstellung, nach GAO 2002, S. 60 f.

Mit den Ergebnissen dieser und anderer Tests liegen der US-Regierung, aber auch anderen Staaten, mittlerweile recht aussagekräftige und relativ neutrale Daten über die Technologien vor, die bei einem flächendeckenden Masseneinsatz in Frage kommen könnten.

3. International Civil Aviation Organization (ICAO)

Die International Civil Aviation Organization (ICAO), 1947 als UN-Sonderorganisation gegründet, hat 188 Mitgliedsstaaten und koordiniert seit 1997 in enger Kooperation mit der International Organization for Standardization (ISO) die Implementierung maschinenlesbarer Reisedokumente, die mit biometrischen Merkmalen ausgestattet werden sollen. Die Richtlinien und Empfehlungen dieser Behörde spielen eine bedeutende Rolle bei der Festlegung internationaler Standards. Zwar hat die ICAO selbst keine Hoheitsbefugnisse; ihre Richtlinien gelten daher auch nicht unmittelbar in den Mitgliedsstaaten. Sie müssen vielmehr von den jeweiligen Vertragsstaaten in entsprechende nationale Rechtsvorschriften transformiert werden.

Die Bundesrepublik hat sich verpflichtet, Reisedokumente nach den Standards der ICAO auszugeben. In einer Entschließung des Rates der EU (2000/C310/01, Anhang II), die keine unmittelbar rechtsbindende Wirkung hat, wurde übereinstimmend festgelegt, Reisepässe mit maschinenlesbaren Lesezonen gemäß ICAO-Dokument 9303 Teil 1 und 2 auszustatten. Eine rechtlich bindende Verpflichtung zur Umsetzung des ICAO-Standards ist im Rahmen der Entschließung der EU zur Sicherung von Pässen und Reisedokumenten nur mittelbar gegeben.

Im Mai 2003 stellte die Behörde einen Beschluss für die Vereinheitlichung biometrischer Informationen in Reisepässen und anderen maschinenlesbaren Reisedokumenten vor. Danach sei die *Gesichtserkennung* die zu bevorzugende Biometrie als „globally interoperable biometric for machine-assisted identity confirmation“ (ICAO 2003a). In einer vergleichenden Analyse verschiedener Biometrien schnitt die Technologie der Gesichtserkennung mit Blick auf die Vergleichsgeschwindigkeit – sowohl in Bezug auf den 1:1-Vergleich (Person – Dokument) als auch im Hinblick auf den Abgleich personenbezogener Merkmale mit Datenbanken – am besten ab; Finger- und Iriserkennung werden optional als Ergänzung empfohlen, sollten Staaten „identity confirmation“ mithilfe eines Dokuments erwägen. Schließlich wird die Speicherung von „images rather

than templates“ in einem Chip empfohlen. Die Empfehlung für die Gesichtserkennung wird in das ICAO-Dokument 9303 „Machine Readable Travel Documents“ Eingang finden.

4. International Maritime Organization (IMO)

Die International Maritime Organization (IMO) hat auf ihrer 22. Tagung (19. bis 29. November 2001) eine Entschließung mit dem Titel „Prüfung von Maßnahmen und Verfahren zur Verhütung von Terrorakten, die die Sicherheit von Passagieren und Mannschaften und die Sicherheit von Schiffen bedrohen“ angenommen. Bei der damit verbundenen Abklärung der Möglichkeiten und Chancen eines einheitlichen Ausweises für Seeleute wurde auch angeregt, biometrische Identifikationsmerkmale (nach den Vorgaben der ICAO) zu prüfen und ggf. zu übernehmen.

Auf einer internationalen Arbeitskonferenz im Juni 2003 entstand der Bericht VII (1) „Zur Verbesserung der Sicherheit der Personalausweise für Seeleute“. Darin werden insbesondere Änderungen des Internationalen Übereinkommens zum Schutz des menschlichen Lebens auf See (SOLAS) von 1974 in Betracht gezogen (u.a. automatische Schiffsidentifikations-Systeme und Sicherheitsmaßnahmen bei den Informationen über Schiff, Ladung, Mannschaft und Passagiere). Der Bericht hält fest, dass das grundlegende Kriterium für die Ausgabe eines Passes die Nationalität und nicht der Beruf sei. Ein Personalausweis für Seeleute solle deshalb den nationalen Reisepass auch nicht ersetzen, sondern ergänzen (http://www.ilo.org/public/german/standards/relm/ilc/ilc91/pdf/rep-vii-2a.pdf).

Eine Konvention der Internationalen Arbeitsorganisation (ILO) vom 05. Juni 2003 sieht ebenfalls vor, biometrische Merkmale in Ausweise für Seeleute zu übernehmen. Die Dokumente sollen mit einem Fingerabdruck versehen werden; dadurch wäre weltweit die Identität von 1,2 Mio. Seeleuten an Bord des Schiffes, in Häfen und auch an Flughäfen eindeutig festzustellen. Dafür sollen die Mitgliedsstaaten der ILO eine gemeinsame Datenbank aufbauen (http://www.ilo.org/public/english/bureau/inf/pr/2003/25.htm).

5. G8

Die Justiz- und Innenminister der G8-Staaten haben auf ihrem Treffen am 05. Mai 2003 in Paris die Maßnahmen zur Bekämpfung des internationalen Terrorismus präzisiert. Dazu zählt auch ein verstärkter Einsatz biometrischer Technologien. Er solle neue Möglichkeiten beim Kampf gegen den internationalen Terrorismus und gegen Fälschungsdelikte eröffnen.

Betont wird, dass die Vorhaben der einzelnen Staaten stärker als bisher aufeinander abgestimmt und dass international gültige Standards angestrebt würden: „In this spirit, the G8 contributed to the International Civil Aviation Organisation's (ICAO) work in the form of a Declaration (G8 Roma and Lyon Groups Statement for ICAO on Biometric Applications for International Travel). The declaration identifies three guiding principles in establishing the standards: universality of standards to ensure perfect technical interoperability, urgency in implementing these technologies and technical reliability." (http://www.g8.fr/evian/extras/389.pdf: Final official statement – Presidents' Summary)

Die G8-Staaten wollen ferner – unter gemeinsamer US-amerikanisch/französischer Leitung – eine hochrangige Arbeitsgruppe ins Leben rufen, die erste politische Entscheidungen in die Wege leiten soll. Zu diesem Zweck sollen breit angelegte Testprogramme vorbereitet werden, mit deren Hilfe Entscheidungen in Bezug auf biometrische Daten und definierte Ziele besser fundiert werden können.

6. Deutschland

Im Zuge der intensiven Diskussionen um Maßnahmen zur Verbesserung der Sicherheitslage nach dem 11. September 2001 wurde auch in Deutschland der Einsatz biometrischer Verfahren erörtert. Mit dem „Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz)" vom 09. Januar 2002 ist der Gesetzgeber entsprechend tätig geworden (vgl. Kap. V). Bei Ausweisdokumenten für Bundesbürger und Ausländer wird die Möglichkeit computerunterstützter Identifizierung von Personen durch biometrische Daten in Ausweisdokumenten eröffnet. Mithilfe der Biometrie soll deren Fälschung erschwert bzw. unterbunden und es soll verhindert werden, „dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen können". Entsprechend werden zweifelsfreie Feststellung der Echtheit von Dokumenten und

der Identität von Personen erwartet (Bundestag 2001, S. 47). Hierzu nimmt das Gesetz Änderungen des Passgesetzes (PassG) und des Gesetzes über Personalausweise (PAuswG) dergestalt vor, dass – neben Lichtbild und Unterschrift – *weitere biometrische Merkmale* in Pass und Personalausweis auch in verschlüsselter Form aufgenommen werden dürfen. Alternativ können dies nunmehr auch die Merkmale von Fingern oder Händen oder Gesicht sein.

Ein zukünftiges „besonderes Bundesgesetz" soll diese Vorgaben konkretisieren: Zu regeln sind die „Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form […] sowie die Art der Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung" (§ 4 Abs. 4 PassG neu, § 1 Abs. 5 PAuswG neu).

Im *Ausländergesetz* (AuslG) wird die Nutzung biometrischer Merkmale in der oben genannten Art und Weise ebenfalls als Option eröffnet. Vor allem die Aufenthaltsgenehmigung, aber auch der Ausweisersatz, die Bescheinigung über die Duldung und die „Bescheinigung über die Wirkung [...] [der] Antragsstellung (Fiktionsbescheinigung)" können künftig biometrische Merkmale von Fingern oder Händen oder Gesicht enthalten (§ 5 Abs. 4, § 39 Abs. 1, § 56a, § 69 Abs. 2 AuslG neu). Damit sollen Fälschung und Missbrauch von Dokumenten effektiv verhindert und insgesamt die „Möglichkeiten der Identitätssicherung" erweitert und verbessert werden. Die konkrete Ausgestaltung der so eröffneten Möglichkeiten liegt beim Bundesministerium des Innern und erfolgt durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf (§ 5 Abs. 6, § 39 Abs. 1, § 56a, § 69 Abs. 2 AuslG neu).

Aktuelle Tests und Projekte in Deutschland

Schon in den Jahren 1999 und 2000 hatte das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam mit dem Bundeskriminalamt (BKA) eine „Vergleichende Untersuchung biometrischer Identifikationssysteme – *BioIS*" durchführen lassen, die erste ihrer Art in Deutschland. Das Fraunhofer-Institut für Graphische Datenverarbeitung (IGD) in Darmstadt war für die technische Untersuchung – ein Praxisvergleich verschiedener Systeme – zuständig, das Modul Technikfolgen-Abschätzung wurde vom Wissenschaftlichen Institut für Kommunikationsdienste GmbH (WIK), Bad Honnef, bearbeitet. Ein Ziel dieser und anderer Aktivitäten war es, national und international abgestimmte Evaluierungs-, Normierungs- und Zertifizierungskriterien zu erarbeiten, die für den Einsatz, für die Anwendung und zur Bewertung biometrischer Verfahren, z.B. im Rahmen der gesetzeskonformen Digitalen Signatur, notwendig sind (http://

www.bsi.de). Als Fortsetzung dieser Studie ist *BioKrit* anzusehen, eine Untersuchung, die von Februar 2001 bis Februar 2002 vom TÜV IT und der Firma secunet Security Networks AG im Auftrag des BSI durchgeführt wurde. Folgende Aspekte wurden im Rahmen von BioKrit untersucht:

– Der in BioIS entwickelte Entwurf „Technischer Evaluationskriterien für biometrische Systeme“ sollte mit zwei biometrischen Systemen auf seine Brauchbarkeit für die Evaluation biometrischer Systeme näher betrachtet werden. Der Entwurf der technischen Evaluationskriterien sollte im Anschluss aufgrund der gemachten Erfahrungen überarbeitet werden.
– Auf Basis des britischen Schutzprofils „Biometric Device Protection Profile“ (http://www.cesg.gov.uk/biometrics/) sollten für mindestens eines der biometrischen Systeme konkrete Sicherheitsvorgaben erstellt werden. Diese Sicherheitsvorgaben bildeten die Grundlage für eine formale Evaluierung und Zertifizierung auf Basis der Common Criteria.
– Es sollte geprüft werden, ob sich die technischen Evaluationskriterien eignen, die in den Sicherheitsvorgaben formulierten Sicherheitsfunktionalitäten technisch zu überprüfen. Bei einer möglichen Nutzbarkeit der technischen Evaluationskriterien könnten diese die Basis für eine international anerkannte Methodologie bilden (BSI 2001).

Gegenwärtig untersucht das BSI in Zusammenarbeit mit dem BKA biometrische Identifikationsmöglichkeiten im Zusammenhang mit Ausweisdokumenten. In der ersten Phase des Projektes *BioP I* wurden ausschließlich Gesichtserkennungs-Systeme auf ihre Leistungsfähigkeit bei einer Verifikation mit Personaldokumenten getestet. Dies erfolgte in einer kontrollierten Testumgebung beim BKA in Wiesbaden. Im weiteren Verlauf des Projektes in der zweiten Phase BioP II werden darüber hinaus weitere biometrische Identifikationssysteme in einer kontrollierten Testumgebung am Frankfurter Flughafen evaluiert. Hierbei handelt es sich um einen vergleichenden Systemtest der Verfahren Gesichts-, Fingerabdruck- und Iriserkennung mit einer großen Nutzergruppe. Sowohl in BioP I als auch II werden die Empfehlungen der ICAO berücksichtigt. Mit der Durchführung beider Projektphasen wurde die Firma secunet Security Networks AG beauftragt. Mit den so gewonnenen Erkenntnissen sollen Aussagen über die grundsätzliche Leistungsfähigkeit und Eignung der unterschiedlichen biometrischen Verfahren für einen Einsatz im Zusammenhang mit Ausweisdokumenten getroffen und Kriterien entwickelt werden, nach denen biometrische Systeme in Ausweisdokumenten eingesetzt werden könnten.

Im Rahmen des Projektes *BioFinger* wird die Leistungsfähigkeit von Fingerabdruckerkennungs-Systemen im Hinblick auf die Verifikation untersucht. Initiiert wurde dieses Projekt vom BSI, durchgeführt wird es vom Fraunhofer-Institut für Graphische Datenverarbeitung (IGD). Aufgrund der Anforderungen an ein Personaldokument, möglichst lange (mind. zehn Jahre) einsetzbar zu sein, wird in diesem Forschungsprojekt besonderes Augenmerk auf die mögliche Beeinflussung der Abbildung von Fingerabdrücken (Alter, optische Auflösungen, „gerollte“ und „aufgelegte“ Abdrücke) gelegt. Dieser Aspekt ist auch im Hinblick auf die Kompatibilitätsanforderungen beim Einsatz unterschiedlicher Sensoren von Bedeutung (B&L 2003, S. 10).

Mit der Durchführung des Projektes *BioFace* wurde ebenfalls das Fraunhofer-Institut für Graphische Datenverarbeitung (IGD) beauftragt. In einer ersten Phase (*BioFace I*) wurden die biometrischen Merkmale von 200.000 Gesichtern gespeichert und nach verschiedenen Merkmalen klassifiziert. In der zweiten Projektphase (*BioFace II*) wurden Leistung und Effizienz der Erkennungsalgorithmen und -systeme mit großen Datenmengen untersucht. Im Juni 2003 hat das BSI den Abschlussbericht „BioFace I&II“ vorgelegt (http://www.bsi.bund.de/fachthem/BioFace/BioFaceIIBericht.pdf). Besonders die Ergebnisse aus BioFace II zeigen, dass Ursachen für Veränderungen im Verhalten und in der Erkennungsleistung biometrischer Gesichtserkennungs-Systeme noch genauer analysiert werden müssen. So scheint das verwendete Bildmaterial (Gesichtsbilder von Europäern) großen Einfluss auf die Testergebnisse zu haben. Da sich in den vorausgegangenen Projektphasen außerdem gezeigt hatte, dass die Bildqualität einen deutlichen Einfluss auf die Erkennungsleistung von Gesichtserkennungs-Systemen hat, dient die aktuelle Projektphase *BioFace III* der näheren Betrachtung des Einflusses so genannter störender Faktoren wie Mimik der Person, fotografische Bedingungen und Aufnahmeperspektive.

Im Auftrag des BMWA und des BMI führen das IGD, Verbund Mikroelektronik (Projektkoordination), das Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration (Technik), das Institut für Informatik und Gesellschaft (IIG) (Wirtschaft) und die Projektgruppe „Verfassungsverträgliche Technikgestaltung“ an der Universität Kassel (provet) (Recht) seit Januar 2003 eine *Machbarkeitsstudie „Digitaler Personalausweis“* durch. Die Studie beschäftigt sich neben rechtlichen und technischen auch mit wirtschaftlichen Fragen. Zum einen soll durch die Integration der Funktionalitäten der elektronischen Signatur, der Verschlüsselung und Authentifizierung der elektronische Rechtsverkehr gefördert werden. Auch soll zumindest ein biometrisches Merkmal integriert werden

können, um die Fälschungs- und Identifikationssicherheit von Ausweisen zu verbessern. Der Abschluss der Studie ist für Dezember 2003 vorgesehen.

TeleTrusT Deutschland e.V./Arbeitsgruppe 6

In der TeleTrusT-Arbeitsgruppe 6 „Biometrische Identifikationsverfahren“ sind die meisten der deutschen Hersteller biometrischer Lösungen sowie Anwender, Behörden und wissenschaftliche Einrichtungen vertreten. Die Arbeitsgruppe hat den Auftrag, „den Einsatz geeigneter biometrischer Identifikationsverfahren zu fördern, die auf körpereigenen biometrischen Merkmalen eines Benutzers basieren, um die erforderlichen Sicherheitsverfahren der Informationstechnik, z.B. das PIN-Verfahren, zu ergänzen bzw. abzulösen. Dazu gehört ganz wesentlich die Information einer breiten Öffentlichkeit über biometrische Verfahren, unterschiedliche Methoden, mögliche Anwendungsgebiete und damit eine Förderung der Akzeptanz für den Umgang mit biometrischen Identifikationsverfahren im alltäglichen beruflichen und privaten Gebrauch“ (http://www.teletrust.de/glossar.asp?Id=60700&Sprache=D_&HomePG=0).

Das von der Arbeitsgruppe 6 initiierte Projekt *BioTrusT* wurde am 31. März 2002 beendet. In diesem Projekt vom BMWA wurde in einem Zeitraum von drei Jahren eine Vielzahl biometrischer Identifikationsverfahren getestet. Dabei standen sozioökonomische, rechtliche und technische Perspektiven gleichberechtigt nebeneinander: Es ging um die Analyse der Akzeptanz durch die Nutzer bzw. Verwender und Betreiber biometrischer Identifikationsverfahren, um daten- und verbraucherschutzrechtliche Aspekte sowie die Prüfung der Zuverlässigkeit und Alltagstauglichkeit der untersuchten Systeme.

Im August 1998 hatte die Arbeitsgruppe 6 bereits einen sog. *Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren* „als Hilfsmittel für die sachbezogene Arbeitsebene potenzieller Anwender oder Betreiber“ vorgelegt. Das Papier bietet in komprimierter Form eine allgemeine Einführung in Prinzip und Varianten der Biometrie, beschreibt ausgewählte technische Merkmale, umreißt grundsätzliche juristische Aspekte und listet mögliche Fragen aus Betreiber- und Nutzersicht auf. Im Anhang findet sich eine Checkliste zu den behandelten Kriterien, anhand derer mögliche Anwender die Verfahren vergleichen und für die jeweilige Applikation ein geeignetes auswählen können (TeleTrusT 1998). Im Juli 2002 ist die überarbeitete Fassung dieses Kriterienkataloges erschienen.

Die AG 6 des TeleTrusT e.V. war darüber hinaus im Zeitraum von 2002 bis 2003 am Roadmap-Projekt BIOVISION beteiligt. Gefördert von der EU-Kom-

mission, hatte es die Untersuchung des gegenwärtigen Forschungs- und Entwicklungsstandes biometrischer Verfahren mit Blick auf zukünftig notwendige Forschungsvorhaben auf EU-Ebene zum Ziel. Die Arbeitsgruppe 6 betreute insbesondere das rechtliche und sozialwissenschaftliche Arbeitsfeld (vgl. http://www.eubiometricsforum.com).

Seit Ende 2002 versucht ein Teil der Arbeitsgruppe 6, der Arbeitskreis „*Rechtsfragen der Biometrie*“, Einsatz- und Handlungsempfehlungen aus juristischer Sicht mit technischem Sachverstand zu entwickeln. Neben Fragen des Datenschutzes (Muster-Einwilligungserklärung, Privacy Best Practices on Biometrics) beschäftigt sich der Arbeitskreis mit Fragen des Persönlichkeitsschutzes von Arbeitnehmern am Arbeitsplatz (Muster-Betriebsvereinbarung, Arbeitnehmerdatenschutz). Am 31. März 2003 fand die erste Sitzung statt, in der Vertreter des BSI, der Firmen Siemens, T-Systems und Softpro, der Bundesbeauftragte für den Datenschutz und der hessische Datenschutzbeauftragte sowie weitere Mitglieder aus AG 6 und AG 1 (Juristische Aspekte einer vertrauenswürdigen elektronischen Kommunikation) zusammenarbeiten. Weiterhin erfolgt hier eine Kooperation mit dem Deutschen Forum für Kriminalprävention und dem dort eingerichteten Arbeitskreis Biometrie. Die Arbeitsergebnisse werden in den fortlaufend zu aktualisierenden Kriterienkatalog einfließen (http://www.teletrust.de/dokumente/ag6_akrub-zielarbeitsprogr.pdf).

TAB

III. Biometrie bei Ausweisdokumenten – eine Momentaufnahme internationaler Aktivitäten

Weltweit werden bei der Herstellung, Ausgabe und Nutzung von ID-Dokumenten zunehmend hohe Sicherheitsstandards angelegt und moderne Verfahren und Technologien genutzt. Staaten in aller Welt unternehmen *Anstrengungen*, ihr *Melde-, Pass- und Personalausweiswesen zu modernisieren*, Ausweise missbrauchssicherer sowie die *Grenzkontrollen effektiver* zu machen. Immer häufiger wird dabei auf biometrische Technologien zurückgegriffen. Besonders im arabischen und asiatischen Raum gibt es zahlreiche Staaten, die eine Entscheidung für die *Neugestaltung ihres nationalen Ausweises unter Nutzung biometrischer Merkmale* getroffen bzw. bereits erste Schritte unternommen haben. Neben dieser Kategorie nationaler ID-Dokumente sind weitere Varianten von Ausweisdokumenten mit Biometrie zu nennen, deren Nutzung im öffentlichen Bereich erfolgt (siehe Textkasten).

ID-Dokumente mit Biometrie in hoheitlichen und öffentlichen Kontexten

Traveller Cards vereinfachen den Grenzübertritt, da durch sie die Grenzkontrolle beschleunigt abgewickelt werden kann. Solche „Grenzkarten“ sind zumeist kostenpflichtig, und ihre Gültigkeit wird häufig auf ein bis zwei Jahre begrenzt. Sie werden an Personen ausgegeben, die die mit der Karte verbundenen Serviceleistungen in Anspruch nehmen möchten – beispielsweise für Vielflieger ein vereinfachtes Check-in. Häufig ist die sog. Grenzkarte Teil eines lokal begrenzten Programms, z.B. das Kundenbindungsprogramm „Privium“ des Flughafens Schiphol in Amsterdam. Solche Karten sind zwar kein hoheitliches Ausweisdokument – sie werden aber oft in Zusammenarbeit mit Behörden ausgegeben und bei Grenzkontrollen genutzt.

Die *Wahlkarte* dient der Identifizierung der zur Wahl Berechtigten. Sie ist v.a. dann sinnvoll, wenn die Wahlregister unvollständig sind. Wahlkarten sind in afrikanischen und lateinamerikanischen Ländern teilweise im Einsatz und auf den Philippinen geplant (STZ 2003, S. 97).

Der *Führerschein* dient – neben der amtlichen Bestätigung der Fahrerlaubnis – u.a. in den USA, in Großbritannien und Irland als Ausweisdokument.

In der EU ist eine Führerschein-Karte vorgesehen, die Frage der Biometrie ist aber noch offen (STZ 2003, S. 95).

Das Spektrum der *Sozialversicherungsausweise* reicht von Krankenversicherungskarten über Arbeitslosenversicherungs- bis hin zu Rentenversicherungskarten. In einigen US-Staaten (z.B. in Kalifornien, Conneticut, Illinois, Massachusetts, New Jersey) ist die Arbeitslosenversicherungskarte mit Biometrie im Einsatz. Sie wird dort – neben der Berechtigungsüberprüfung – für die Auszahlung des Arbeitslosengeldes an Geldautomaten genutzt.

Die *Asylkarte* – in den Niederlanden und in Großbritannien bereits im Einsatz – enthält die persönlichen Daten und Biometrie der Antragsteller. Die Karte soll den Asylsuchenden authentifizieren, um Mehrfachanträge zu verhindern. Die Asylkarte ermöglicht ferner die Authentifizierung bei der Auszahlung von Unterstützungsleistungen (STZ 2003, S. 96 f.).

Um zumindest einen ungefähren Einblick in den aktuellen Stand der Diffusion von ID-Dokumenten mit Biometrie zu gewinnen, hat das Steinbeis-Transferzentrum (STZ 2003) im Auftrag des TAB eine internationale Recherche durchgeführt, die 107 Projekte und Aktivitäten im öffentlichen Bereich aus 55 Ländern identifizierte. In 70 dieser Aktivitäten wurde bei den entsprechenden Dokumenten Biometrie verwendet. Damit lag zunächst eine interessante Momentaufnahme des Diffusionsprozesses biometrischer Technologien über alle Anwendungsfelder hinweg vor. Für die Zwecke dieses Sachstandsberichtes wurde eine weitere Auswahl getroffen: Die folgenden Ausführungen beziehen sich auf insgesamt *48 aktuelle Fallbeispiele*. Aufgrund der Schnelligkeit der Entwicklung und der in Teilen unsicheren Informationsbasis erhebt die Übersicht keinen Anspruch auf Vollständigkeit. Sie stellt lediglich eine eher unscharfe Momentaufnahme entlang der folgenden Kategorien dar:

- *Grenzkontrollanwendungen*
  - Pilotprojekte und Tests, die zeitlich begrenzt und mit einer ausgewählten Benutzergruppe durchgeführt werden bzw. wurden
  - Systeme, die im ständigen Einsatz (teilweise aus Piloten hervorgegangen), aber ebenfalls lokal und hinsichtlich der Nutzergruppe limitiert sind
- *nationale Ausweisdokumente*
  - die in fortgeschrittener Planung oder in der Implementierungsphase sind oder deren Implementierung erfolgt ist

Von den 48 Fallbeispielen liegen zu 33 relativ verlässliche Detailinformationen (wie Laufzeit des Pilotprojektes, Implementierungsstatus, Anzahl der ausgegebenen ID-Dokumente) vor.[4]

1. Biometrisch unterstützte Grenzkontrollanwendungen

Grenzübertritte an Flug- und Seehäfen sowie an Landübergängen erfolgen in der Regel unter Kontrolle der Reisedokumente: Pass oder Personalausweis und ggf. ein Visum werden vorgelegt und die Echtheit des Dokumentes überprüft. Durch visuellen Vergleich des Fotos mit dem Gesicht des Reisenden wird überprüft, ob der Reisende berechtigter Inhaber des Ausweisdokumentes ist. Außerdem können bei Vorliegen entsprechender Voraussetzungen die auf dem Dokument gespeicherten Daten mit einem Fahndungsregister oder einer Liste „unerwünschter" Personen abgeglichen werden. Diese Form der Grenzkontrolle wird bislang nur in seltenen Fällen und begrenztem Umfang biometrisch unterstützt.

Zeitlich begrenzte Pilotprojekte und Tests bei ausgewählten Benutzergruppen

In einigen Pilotprojekten und Tests wurde in jüngster Zeit versucht, die Vorteile biometrischer Anwendungen bei der Grenzkontrolle (Beschleunigung des Grenzübertritts, erhöhte Sicherheit durch Biometrie unterstützte Verifikation des Einreisenden) auszuloten: In Australien werden beispielsweise im Projekt „Smart Gate" verschiedene Gesichtserkennungs-Systeme an Flughäfen getestet, am Flughafen Nürnberg wurde von Juli 2002 bis März 2003 ein Pilotprojekt durchgeführt, um gefälschte Pässe besser identifizieren zu können, am Flughafen Tokyo wurde bis März 2003 eine durch Gesichts- und Iriserkennung unterstützte Grenzkontrollanwendung für Vielflieger getestet. Die folgende Tabelle

4 Diese im Folgenden kurz beschriebenen biometrischen Anwendungen wurden im Wesentlichen vom Steinbeis-Transferzentrum (STZ 2003) recherchiert und durch das TAB-Projekt-Team aktualisiert und ergänzt.

gibt einen Überblick über neun aktuelle Pilotprojekte seit dem Jahr 2002, bei denen Grenzkontrollanwendungen mit Biometrie getestet wurden oder werden.

Tab. 2: Grenzkontrollanwendungen: Pilotprojekte und Tests (seit 2002)

Land	*Biometrie*	*Einsatzort*	*Laufzeit*
Australien	Gesicht	Flughäfen	seit November 2002
Deutschland	Gesicht	Flughafen Nürnberg	Juli 2002 bis März 2003
Deutschland	Iris	Flughafen Frankfurt	geplanter Beginn: Herbst 2003; Laufzeit: sechs Monate
Deutschland	Gesicht	deutsch-tschechischer Grenzübergang Waidhaus/Rozvadov	Beginn: Januar 2003, mittlerweile abgeschlossen
Großbritannien	Iris	Flughafen Heathrow	Pilottest mit ca. 2.000 Karten von Februar bis Dezember 2002
Japan	Gesicht, Iris	Narita Airport, Tokyo	seit Januar 2003
Malaysia	Iris	Grenze nach Singapur; Checkpoints Woodlands und Tuas	Testphase im 2. Quartal 2002 abgeschlossen
Saudi-Arabien	Iris	Flughafen „King Abdulaziz International Airport“ in Jidda	Beginn des Pilotprojektes im 1. Quartal 2002
Schweiz	Gesicht	Flughafen Zürich	Januar bis März 2003

Quellen: Booz Allen Hamilton et al. 2003; STZ 2003; eigene Recherchen

Es zeigt sich, dass in den hier identifizierten Projekten zu Grenzkontrollanwendungen ausschließlich Gesichtserkennungs- und Iriserkennungs-Systeme getestet wurden. Die meisten Tests fanden an Flughäfen statt. Deren bauliche und infrastrukturelle Gegebenheiten weisen im Vergleich zu Grenzübergängen zu Land und zur See bestimmte Vorzüge auf.

Lokal begrenzte biometrische Systeme im ständigen Einsatz

Zahlreiche biometrische Systeme für den Grenzübertritt sind mittlerweile implementiert und im Einsatz. Die Bandbreite solcher Anwendungen reicht von Passkontrollen an Flughäfen über Grenzkarten, die beispielsweise Pendlern den täglichen Grenzübertritt erleichtern sollen, bis hin zu kompletten Grenzkontrollsystemen wie im Fall der Vereinigten Arabischen Emirate. Bei allen hier aufgeführten Beispielen sind die Nutzergruppen begrenzt (Vielflieger, Pendler, ausgewählte Nutzergruppen). Im Folgenden werden insgesamt zehn Fallbeispiele – geordnet nach der genutzten Technologie – in Kürze beschrieben:

Fingerabdruck-Systeme

Der *Flughafen Hong Kong* bietet eine Grenzkarte an, welche die Grenzkontrolle beschleunigen soll und damit einen Komfortgewinn für Vielflieger verspricht. Die sog. „Frequent Traveller Card“ speichert die biometrischen Merkmale des Fingers auf einem Chip (STZ 2003).

SENTRI (Secure Electronic Network For Travelers Rapid Inspection) ist eine Grenzkontrollanwendung, in deren Rahmen aus Mexiko kurzzeitig in die USA Einreisende über ihren Fingerabdruck identifiziert werden. Laut U.S. Department of Justice (Februar 2003) nehmen 42.000 Pendler am SENTRI-Programm teil.

Im Rahmen des *NSEERS*-Programms (National Security Entry-Exit Registration System) werden Personen über 16 Jahren aus bestimmten Staaten (u.a. Afghanistan, Algerien, Bahrain, Iran, Lybien, Oman, Syrien, Jemen), die in die USA einreisen, fotografiert und unter Eid über die Dauer ihres geplanten Aufenthalts befragt. Die Einreisenden müssen sich über ihren Fingerabdruck identifizieren. Die Fingerabdrücke werden mit Datenbanken abgeglichen, um sicherzustellen, dass es sich bei der einreisenden Person nicht um eine handelt, die krimineller oder terroristischer Aktivitäten verdächtigt wird.

Iriserkennungs-Systeme

Am *Flughafen Amsterdam* (Schiphol) gibt es – nach einer Pilotphase – seit Oktober 2002 das Programm „Privium“ für Vielflieger aus der EU, in dessen Rahmen auch eine „Traveller Card“ angeboten wird. Mittels Iriserkennung (Speicherung der Irismerkmale auf einem Chip) wird eine beschleunigte Grenzkontrolle gewährleistet (Abb. 3).

Abb. 3: Privium-Kontrollraum am Flughafen Schiphol

Quelle: http://www.schiphol.nl/privium.html

Seit Anfang 2003 ist in den *Vereinigten Arabischen Emiraten* ein Iriserkennungs-System dauerhaft implementiert. Es soll dafür sorgen, dass einmal des Landes verwiesene Personen auch mit neuen, gefälschten Papieren nicht wieder einreisen können (Rönneberg 2003). Dem Einsatz dieses flächendeckenden Grenzkontrollsystems war eine Versuchsphase vorausgegangen, in der nach Behördenangaben bereits mehrere Dutzend Personen erkannt werden konnten, die mit gefälschten Papieren einzureisen versuchten. Iris-Scan-Terminals wurden an sechs Flughäfen, an allen Land- und See-Grenzübergängen sowie in zahlreichen Abschiebegefängnissen installiert (http://www.heise.de/newsticker/data/pmz-07.04.03-000/).

Im Rahmen des „CANPASS-Air Programs“ bietet *Kanada* ausgewählten Vielfliegern mit US-amerikanischer oder kanadischer Staatsbürgerschaft eine schnellere und komfortablere Einreise an. Mittels Iriserkennung wird die Identität der zuvor im Rahmen des Programms registrierten Personen überprüft; aufwendige Sicherheitskontrollen können auf diese Weise umgangen werden (Abb. 4). Das CANPASS-Air Program soll zu einem späteren Zeitpunkt für Reisende aus visafreien Staaten und Staaten, die dem Nordamerikanischen Freihandelsabkommen angehören, geöffnet werden. Der Pearson Airport in Toronto bietet seit Januar, der Vancouver International Airport seit Mitte 2003 dieses Programm an. Zu einem späteren Zeitpunkt wollen weitere sechs kanadische

Flughäfen (Calgary, Edmonton, Halifax, Montreal, Ottawa, Winnipeg) das entsprechende System implementieren (http://www.ccra-adrc.gc.ca/newsroom/factsheets/2002/sep/canpass-e.pdf; http://www.ccra-adrc.gc.ca/newsroom/releases/2002/sep/iris-e.pdf).

Abb. 4: CANPASS-Schalter

Quelle: http://www.cic.gc.ca/english/pub/border2000/border2000.html

Handgeometrie-Systeme

Seit 1998 sind am *Flughafen „Ben Gurion International Airport“* in Tel Aviv 21 Handscanner aufgestellt; über 100.000 Passagiere wurden registriert. Jeden Monat nutzen bis zu 50.000 Reisende ihre Grenzkarte, auf der die handgeometrischen Merkmale elektronisch speichert sind und die dem Nutzer ein vereinfachtes Check-in ermöglicht (Abb. 5). Das Angebot richtete sich ursprünglich nur an Vielflieger; es wurde mittlerweile für alle israelischen Staatsbürger geöffnet (GAO 2002, S. 164).

Abb. 5: Handscanner am Flughafen Ben Gurion

Quelle: http://www.msnbc.com/news/729756.asp?pne=msn

In Israel soll ein System implementiert werden, das den Grenzübertritt für etwa 120.000 ausländische Arbeiter, die täglich die *Grenze von palästinensischem Gebiet nach Israel überqueren*, automatisieren und beschleunigen soll. Die Überprüfung erfolgt mittels kontaktloser Smartcards mit Mikroprozessor, auf die ein hoch aufgelöstes Lichtbild sowie die biometrischen Daten der Hand aufgebracht sind. Im Rahmen des sog. „Basel-Projektes“ soll dieses Grenzkontrollsystem zuerst am Grenzkontrollpunkt Erez zwischen dem Gaza-Streifen und Israel implementiert werden (Booz Allen Hamilton et al. 2003, S. 178; http://www.portfoliopr.com/clients/OTI/PressReleases/OTI08_20_03.html).

In den *USA* ist das Vielflieger-Programm *INSPASS* (Immigration and Naturalization Service’s Passenger Accelerated Service System) im Einsatz, das an sieben Flughäfen des Landes (und an zwei kanadischen Flughäfen) eine (teil-) automatisierte Grenzkontrolle ermöglicht. Seit 1995 fanden über 300.000 Check-in-Vorgänge über die INSPASS-Kioske statt. Dabei wird ein Live-Scan der Hand genommen, und die Merkmale werden mit den zuvor in einer Datenbank hinterlegten Merkmalen abgeglichen. Das Programm kann von US-Bürgern, Bürgern aus Kanada und von den Bermudas sowie von Bürgern der Staaten genutzt werden, die am Visa Waiver Program teilnehmen und mindestens drei Mal im Jahr in die USA einreisen (GAO 2002, S. 163).

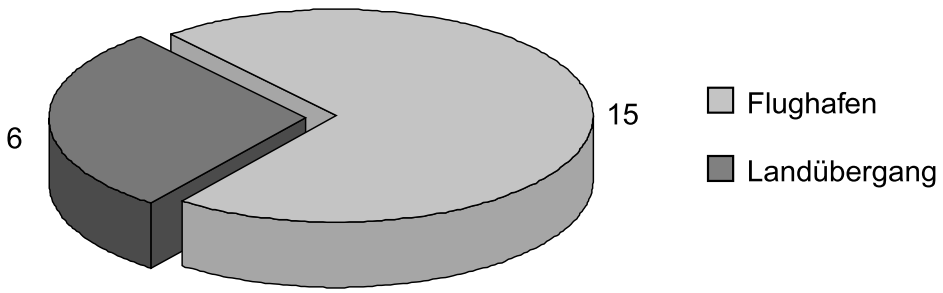
Gesichtserkennungs-Systeme

Am *Flughafen Keflavik* auf Island wurde im Juni 2001 das Gesichtserkennungs-System „FaceIt“ implementiert: Mit teilweise versteckten Kameras werden die Gesichter von Reisenden, die sich auf dem Flughafengelände aufhalten, fotografiert und mit Datenbankbildern verglichen. Dazu wird das aufgenommene Bild an einen Zentralraum weitergeleitet und dort von einem Computer mit Gesichtern gesuchter Personen verglichen. Stellt der Computer eine gewisse Ähnlichkeit der Gesichtsmerkmale fest, vergleicht ein Polizist die Bilder; im Verdachtsfall erfolgt eine Personenüberprüfung (Lucius 2002).

Zusammenfassende Einordnung

Betrachtet man die Verteilung der Grenzkontrollanwendungen hinsichtlich des Kontrollortes, finden sich die meisten ausschließlich an Flughäfen (13 von insgesamt 19). Vier Anwendungen gibt es ausschließlich an Grenzübergängen zu Lande oder wurden an solchen getestet (Waidhaus/Rozvodov, Malaysia/Singapur, SENTRI, Israel). Zwei der genannten Grenzkontrollanwendungen (NSEERS, Vereinigte Arabische Emirate) finden sich sowohl an Flughäfen als auch an Grenzübergängen zu Lande (Abb. 6).

Abb. 6: Kontrollorte biometrischer Grenzkontrollanwendungen

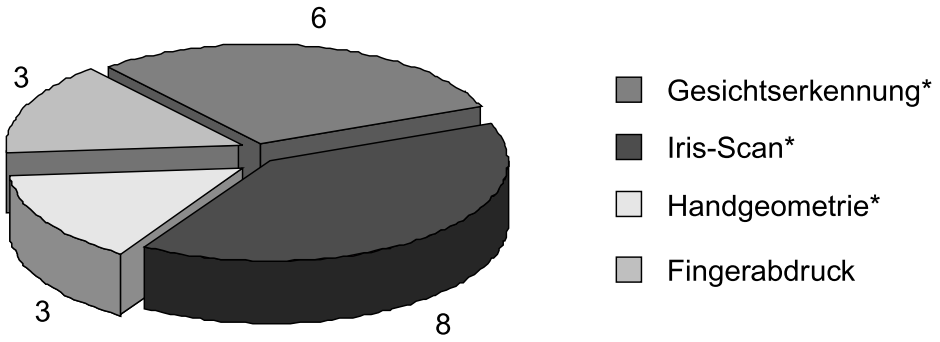


* Doppelnennung in zwei Fällen.

Quelle: Eigene Darstellung

Bezüglich der Nutzung des biometrischen Merkmals ergibt sich folgendes Bild: In acht Fällen wird die Iris, in sechs Fällen das Gesicht als biometrisches Merkmal verwendet; in drei Fällen die Hand und in drei Fällen der Fingerabdruck (Abb. 7).

Abb. 7: Verwendete Biometrien bei Grenzkontrollanwendungen (Pilot und implementiert)

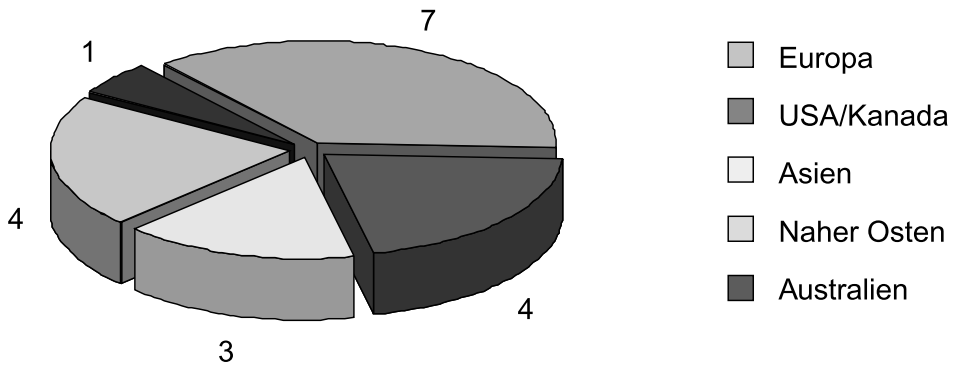


* In einem Fall (Israel) wird sowohl die Handgeometrie- als auch die Gesichtserkennung verwendet. In einem anderen Fall (Japan) wurden sowohl die Gesichts- als auch die Irismerkmale aufgenommen.

Quelle: Eigene Darstellung

Die regionale Verteilung stellt sich so dar: Die meisten Grenzkontrollsysteme wurden oder werden in Europa (Nürnberg, Waidhaus/Rozvodov, Frankfurt, Zürich, Heathrow, Keflavik, Amsterdam) getestet oder sind dort implementiert, gefolgt von USA/Kanada (NSEERS, CANPASS, INSPASS, SENTRI), dem Nahen Osten (Saudi-Arabien, Vereinigte Arabische Emirate, Ben Gurion Tel Aviv, Israel) und Asien (Tokyo, Malaysia/Singapur, Hong Kong) (Abb. 8).

Abb. 8: Biometrische Grenzkontrollanwendungen nach Regionen



Quelle: Eigene Darstellung

2. Nationale Ausweisdokumente mit Biometrie

Zahlreiche Länder haben die Einführung nationaler Ausweisdokumente für den internationalen Reiseverkehr mit Biometrie beschlossen, einige haben Absichtserklärungen abgegeben, die eine solche flächendeckende Einführung nahe legen und einige haben mit der Implementierung bereits begonnen. Die Einführung eines nationalen Personalausweises wird häufig durch Handlungsbedarf bei der Modernisierung der staatlichen Verwaltung und mit den Erfordernissen an eine erhöhte Sicherheit begründet. Ein wesentlicher Bestandteil eines neuen nationalen ID-Systems ist deshalb auch oft der Neuaufbau des Einwohnermelderegisters (STZ 2003, S. 129).

Die Recherchen haben Hinweise auf insgesamt 30 Länder ergeben. Aufgrund der unzureichenden und sich ständig wandelnden Informationslage kann im Folgenden auch hier nur ein grober Überblick gegeben werden. Zunächst werden die Vorhaben in 16 Ländern kurz beschrieben. Danach werden 14 Länder lediglich tabellarisch (und ohne nähere Beschreibung) erfasst, da hier nähere und sichere Informationen (bis Redaktionsschluss) nicht zu erhalten waren.

Europa

Bosnien-Herzegowina gibt seit 2002 Personalausweise aus, auf denen die biometrischen Fingermerkmale des Ausweisinhabers in drucktechnischer Form (2D-Barcode) abgelegt sind. Nach einer ersten Ausgabephase (bis Februar 2003) startete im März 2003 eine zweite Phase, das erweiterte Rollout. Derzeit sind ca. 2,5 Mio. ID-Karten ausgegeben, sie entsprechen internationalen Standards und können deshalb als Reisedokument verwendet werden (STZ 2003).

Großbritannien plant die Umsetzung eines Programms zur Einführung neuer ID-Dokumente in zwei Phasen. Wesentliche Elemente sind u.a. die Einführung von ID-Karten ab August 2007 zusammen mit einem sukzessiven Rollout biometrischer Pässe (und evtl. Führerscheinen). Innerhalb von fünf Jahren sollen 80 % der (erwachsenen) Bevölkerung dann einbezogen sein. Die Biometrie ist noch offen, für Pässe ist an kontaktlose Chips gedacht, die Merkmale des Gesichtes und ein weiteres biometrisches Merkmal speichern. Ferner soll ein National Identity Register neu aufgebaut werden. Es wird die biometrischen Daten enthalten, die bei der Ausgabe der ID-Karten erhoben werden (UK Secretary of State for the Home Department 2003).

In *Italien* wurde 1998 ein Gesetz zur Einführung der sog. „Carta d'Identita Elettronica" (CIE) verabschiedet. Seit 2004 wird die CIE an italienische Staatsbürger zunächst ohne Biometrie ausgegeben. Bis 2010 sollen die biometrischen Merkmale des Fingers oder der Iris in die Ausweise integriert werden. Die CIE soll den Bürgern zusätzlich als qualifizierte digitale Signatur dienen (http:// www.cartaidentita.it; http://www.anci.it).

In den *Niederlanden* ist geplant, in Rathäusern, Konsulaten und Botschaften frühestens ab 2004 das sog. „Dutch Travel Document" mit Biometrie auszugeben (Montelbaan 2003, S. 8). Alle Bürger sollen diesen nationalen Personalausweis erhalten, um multiple Identitäten bei der Beantragung aufdecken und den Passinhaber eindeutig verifizieren zu können. Nach einer umfangreichen Evaluierung verschiedener biometrischer Technologien wurde die Gesichtserkennung als das zu favorisierende Verfahren ermittelt, u.a. wegen der Verfügbarkeit bereits vorliegender Passbilder (STZ 2003).

Afrika

In *Ägypten* werden seit Januar 2001 42 Mio. Bürger mit ID-Ausweiskarten ausgestattet, die mit fortgeschrittenen Sicherheitsmerkmalen, u.a. dem biometrischen Fingerabdruck, versehen sind. Hierzu wurde eine vollständig neue Infrastruktur aufgebaut: von der landesweiten Datenerfassung der Bürger über die ID-Karten-Produktion bis zur Verifikation der Karten mittels Leseendgeräten (http://www.gdm.de).

Botswana hat seit Juli 1998 ca. 800.000 Personalausweise für den internationalen Reiseverkehr ausgestellt, die den Fingerabdruck des Daumens, auf einem Chip speichern. Dieser biometrische Personalausweis soll flächendeckend an alle Bürger Botswanas ausgegeben werden (http://www.face.co.za).

Seit Februar 2003 können die Bürger *Nigerias* einen neuen Personalausweis beantragen, der ihren Fingerabdruck in drucktechnischer Form (2D-Barcode) enthält. Bisher wurden landesweit 60.000 Enrollment-Center eröffnet, um alle 60 Mio. Einwohner zu erfassen. Die Bürger sind nicht verpflichtet, diesen biometrischen Personalausweis zu beantragen, allerdings können sie nur über diesen Verwaltungsleistungen in Anspruch nehmen (STZ 2003).

Mittlerer und Naher Osten

Der *Jemen* plant, in den nächsten fünf bis acht Jahren ca. 5 Mio. nationale ID-Dokumente für den internationalen Grenzübertritt auszugeben. Auf diesen ID-

Karten wird der codierte Fingerabdruck des Ausweisinhabers gespeichert sein. Neben einer verbesserten Kontrolle, welcher Bürger in welcher Höhe öffentliche Zuwendungen erhält, erhofft man sich auch eine kostengünstigere Ausweisproduktion als bei herkömmlichen Karten (STZ 2003, http://www.word-sun.com/ds30.html).

Im März 2003 haben die *Vereinigten Arabischen Emirate* den Aufbau eines nationalen biometrisch unterstützten ID-Systems in die Wege geleitet. Die verwendete biometrische Technologie wird das „Automated Fingerprint Identification System" (AFIS) sein. Insgesamt sollen mehrere Millionen ID-Karten ausgegeben werden, die den Bürgern der Vereinigten Arabischen Emirate v.a. einen vereinfachten Zugang zu Behördendienstleistungen ermöglichen sollen (http://www.sagem.com/en/communiques-en/cp-1sem2003-en.htm#mar-18). Neben E-Government-Funktionen sollen zu einem späteren Zeitpunkt weitere wie Führerschein und Krankenkarte hinzukommen (http://www.gemplus.com/companyinfo/press/2003/governmentiduae30042003.html).

Asien

Brunei produziert seit August 2000 Ausweise mit Chips, die den Fingerabdruck speichern. Zurzeit sind ca. 350.000 ID-Karten dieser Art im Markt. Das Ziel ist auch hier, alle Einwohner mit diesem Ausweis auszustatten, der für die Ein- und Ausreise nach und von Brunei gültig wäre (STZ 2003).

Hong Kong plant, bis 2007 alle Bewohner mit einer biometrischen ID-Karte auszustatten, die als Generalausweis (u.a. Sozialausweis, Führerschein) verwendet werden soll. Diese ID-Karte ist Teil des sog. SMARTICS (Smart Identity Card System) und wird die Fingerabdrücke der Daumen beinhalten. Der Nutzen für die Bürger wird in den fälschungssicheren und multifunktionalen Anwendungsmöglichkeiten gesehen (Booz Allen Hamilton et al. 2003, S. 168; http://www.legco.gov.hk/yr01-02/english/bc/bc56/papers/bc561011cb2-2872-1e.pdf).

Macao gibt seit Dezember 2001 Karten mit Chips aus, die den biometrischen Fingerabdruck speichern. Diese ID-Karten sollen als Personalausweis und internationales Reisedokument die Grenzkontrollen beschleunigen (Citizen Card). Das nationale ID-Dokument (Zusatzfunktionen: Führerschein, Studentenausweis, Krankenversicherungskarte, E-Commerce-Funktionen) soll innerhalb von vier Jahren kostenpflichtig an alle Bürger Macaos ausgegeben sein (ca. 470.000 Karten) (STZ 2003; http://www.siemens.com: Pressemitteilung vom 16. Mai 2003).

Malaysia hat sich bei seiner „MyKad“ ebenfalls für den auf einem Chip gespeicherten Fingerabdruck als biometrisches Merkmal entschieden. Nach einem Pilottest von 1996 bis 2001 mit 5 Mio. Karten waren Ende 2002 2 Mio. Karten ausgegeben. Geplant sind insgesamt 22 Mio. Karten. Sie gelten als internationales Reisedokument und sind mit weiteren Funktionen versehen (u.a. Führerschein, E-Cash-Funktion, Krankenversicherungskarte).

Südamerika

Guatemala hat im Juli 1999 die Produktion von ID-Karten, die den Fingerabdruck in drucktechnischer Form als 2D-Barcode speichern, in Auftrag gegeben. Diese als Personal- und Reisedokument verwendbaren Karten werden in Guatemala selbst und in sechs Konsulaten in den USA (Los Angeles, San Francisco, Chicago, New York, Houston und Miami) ausgegeben. Es wird erwartet, dass bis 2004 über eine Million Guatemalteken einen solchen biometrischen Pass beantragt haben. Als Vorteil wird herausgestellt, dass in den US-Konsulaten unverzüglich ein neuer Pass ausgestellt werden kann, wenn der Inhaber seinen in den USA verliert: Die bei der ersten Beantragung des Passes gespeicherten Fingermerkmale werden mit einer Datenbank abgeglichen, die Identität des Passinhabers wird festgestellt, und ein neuer Pass kann ausgestellt werden (STZ 2003; http://www.printrakinternational.com/1999/pr071499.html).

Die Bewohner des Bundesstaates Rio de Janeiro (*Brasilien*) erhalten seit November 2000 nur noch Personalausweise mit den biometrischen Merkmalen des Fingerabdruckes (2D-Barcode). Das verwendete Fingerabdruck-System soll bei 4.000 Ausweisantragstellern täglich 20 bis 40 Betrugsfälle finden (STZ 2003).

Australien

Australien gibt seit Dezember 2001 nur noch Personalausweise aus, die die biometrischen Gesichtsinformationen des Ausweisinhabers enthalten. Nach einer umfangreichen technologischen und operativen Evaluierung verschiedener biometrischer Technologien wurde das Gesicht als die zu favorisierende Biometrie ermittelt, u.a. auch deshalb, weil die bereits verwendeten Passbilder genutzt werden können. Ziel dieses Konzeptes, dessen Entwicklung eng an das Grenzkontrollprojekt „Smart Gate“ gebunden ist, ist es auch, Mehrfachanträge aufzudecken (Booz Allen Hamilton et al. 2003, S. 165).

Zusammenfassende Einordnung

Mit den bereits erwähnten Vorbehalten bezüglich der Informationslage zeigt die *regionale Verteilung keine eindeutigen Schwerpunkte*. Eine nähere Betrachtung fördert zu Tage, dass Aktivitäten in Europa in einem weniger fortgeschrittenen Stadium sind als Aktivitäten in anderen Regionen der Welt: Dort sind in vielen Ländern Aufträge an Systemlieferanten und andere Anbieter vergeben bzw. ist die Implementierung bereits angelaufen und zum Teil recht weit vorangeschritten.

Von den insgesamt 16 hier genannten Staaten, die landesweite Ausweisdokumente mit Biometrie beschlossen oder eingeführt haben, haben sich *zwölf für den Fingerabdruck und zwei für das Gesicht als biometrisches Merkmal entschieden*. Anders als bei den in Kapitel III.1 genannten Grenzkontrollanwendungen, wo nur in drei Fällen der Fingerabdruck als Merkmal genutzt wird, scheinen diese Staaten bei ihren Ausweisdokumenten mit Biometrie dem Fingerabdruck die Priorität zu geben. Im Falle Großbritanniens und Italiens ist die Biometrie noch offen.

Die Gutachter des Steinbeis-Transferzentrums (STZ) konnten weitere Staaten identifizieren, die die Einführung von biometrischen Ausweisdokumenten, die zum Grenzübertritt berechtigen, planen. Nähere Informationen zum Stand der Implementierung oder zum Vorhaben selbst konnten nicht gefunden werden. Dennoch sollen diese Beispiele in Tabelle 3 der Vollständigkeit wegen zumindest genannt werden.

Tab. 3: Weitere nationale ID-Dokumente

Staat	*Biometrie*	*Status/Laufzeit*	*weitere Informationen*
Argentinien	Fingerabdruck	1998: Beauftragung eines Firmenkonsortiums, weiterer Verlauf unklar	Im Rahmen eines umfassenden nationalen ID-Systems soll u.a. das „Documento Nacional de Identidad“ auf seine Echtheit überprüft werden können.
Bulgarien	Fingerabdruck	keine Angaben	Ausgabebehörde: Ministerium der Finanzen
China	Merkmal noch offen	im Test	Ausgabebehörde: Ministerium für öffentliche Sicherheit
Elfenbeinküste	Fingerabdruck	ca. 9 Mio. Ausweise wurden bereits ausgegeben.	keine Angaben
Kambodscha	Fingerabdruck	ca. 8 Mio. Ausweise wurden bereits ausgegeben.	keine Angaben
Kolumbien	Fingerabdruck	ca. 4 Mio. Ausweise wurden bereits ausgegeben.	keine Angaben
Kosovo	Fingerabdruck	ca. 1 Mio. Ausweise wurden bereits ausgegeben.	Ausgabebehörde: United Nations Mission in Kosovo (UNMIK)
Libanon	Fingerabdruck	keine Angaben	keine Angaben
Mauretanien	Fingerabdruck	keine Angaben	keine Angaben
Nigeria	Fingerabdruck	Das Projekt ist seit 2002 bekannt.	Mithilfe einer Border Crossing Card werden ausländische Arbeiter und Händler an nigerianischen Grenzübergängen identifiziert.
Oman	Fingerabdruck	Die ersten Ausweise sollen Ende 2003 ausgegeben werden.	Neben der Funktion als Reisedokument soll die Karte Behörden-Dienstleistungen ermöglichen und beschleunigen. Nutzer sind neben den Bürgern auch ausländische Personen, die sich länger als 14 Tage im Oman aufhalten.
Philippinen	Fingerabdruck	Pilotprojekt	keine Angaben
Südafrika	Fingerabdruck	keine Angaben	Ausgabebehörde: Department of Home Affairs
Thailand	Fingerabdruck	keine Angaben	Ausgabebehörde: Ministry of Information

Quellen: STZ 2003; eigene Recherchen (Stand: Dezember 2003)

IV. Leistungsfähigkeit und Eignung von Biometrien bei Ausweisdokumenten und Grenzkontrollen

Es wird im Folgenden versucht, die technische Leistungsfähigkeit und Eignung der Handgeometrie-, Fingerabdruck- sowie Gesichts- und Iriserkennung für die Nutzung bei Ausweisdokumenten und bei Grenzkontrollen *mit dem Ziel der Verifikation* einzuschätzen. Anforderungen wie Abgleich mit Datenbanken oder Fahndungslisten werden nicht thematisiert.

Dazu wird nach einer kurzen allgemeinen Charakterisierung der Stärken und Schwächen der einzelnen biometrischen Verfahren (Kap. IV.1) deren *spezifisches Leistungsprofil* entlang ausgewählter Kriterien (Nutzerausfallrate, Erkennungsleistung, Bedienungsaufwand und Verständlichkeit) näher beschrieben (Kap. IV.2). In einem nächsten Schritt wird die Frage diskutiert, wie sich die einzelnen *Verfahren in die etablierten Prozesse der Ausweisbeantragung und -erstellung integrieren* lassen (Kap. IV.3). Schließlich werden in einem Exkurs vier Kostenmodelle präsentiert. Diese stellen *grobe Abschätzungen einmaliger und laufender Kosten* dar, wie sie aus unterschiedlichen Einsatzszenarien für die biometrische Nutzung bzw. Aufwertung von Pässen und Personalausweisen resultieren könnten (Kap. IV.4).

Dieses Kapitel basiert im Wesentlichen auf Teilen eines gemeinsam von der Booz Allen Hamilton GmbH, der Bundesdruckerei GmbH und der ZN Vision Technologies AG für das TAB erarbeiteten Gutachtens.

1. Allgemeine Beschreibung und Einschätzung biometrischer Verfahren

Handgeometrie

Zur Erfassung der physiologischen Merkmale der Hand dienen ca. 90 geometrische Parameter wie Fingerlänge, Breite der Hand und der Finger oder die Fingerkrümmung. Dazu werden die Umrisse der Hand von der Seite und von der Oberfläche mit einer Kamera aufgenommen (Abb. 9). Die vom Handleser ermittelten geometrischen Merkmale werden dann mit den gespeicherten Referenz-

merkmalen verglichen, bei hinreichender Übereinstimmung wird die Personenidentität akzeptiert, andernfalls abgelehnt. Die meisten Handgeometrieapplikationen dienen der Verifikation, also dem 1:1-Vergleich.

Abb. 9: Erfassen der Handgeometrie

Quelle: http://www.cardweb.com/graphic/abi/handscan.gif

Insgesamt handelt es sich bei der Handgeometrieerkennung um *ein etabliertes, relativ robustes Verfahren*, das aber seit einigen Jahren *kaum Fortentwicklungen* erfahren hat (GAO 2002, S. 161). Vorteilhaft ist der geringe erforderliche Speicherplatz (je nach System 10–96 Bytes). Nachteilig ist, dass das verwendete biometrische Merkmal aufgrund der Beschränkung auf eine relativ begrenzte Anzahl geometrischer Informationen nicht über die Unterscheidbarkeit verfügt, die andere biometrische Verfahren bieten.

Fingerabdruck

Der Fingerabdruck, also der Abdruck der Fingerbeere auf einem Objekt, zeigt die charakteristischen Täler und Erhebungen des Hautleistenreliefs. Die Papillarlinien können schleifen-, wirbel- und bogenförmig angeordnet sein. Sie sind im Grundsatz individuell einzigartig und verändern sich lebenslang nicht.

Derzeit werden verschiedene Methoden zur *Erfassung des Fingerabdruckes* verwendet, dazu gehören zum Beispiel optische Lesegeräte. Hierbei wird der Finger auf eine durchsichtige, beleuchtete Hartplastik- oder Glasoberfläche gelegt und der Fingerabdruck mit einer darunter befindlichen Kamera aufgenommen. Zum Zweiten kommen so genannte „kapazitive" Fingerabdruckleser zum Einsatz. Kapazitive Leser sind Mikrochips, die über eine sensible Oberfläche aus bis zu 100.000 leitenden Platten verfügen. Nach Auflage des Fingers auf die leitende Oberfläche wird der Fingerabdruck mittels elektrischer Messungen eingelesen, und ein digitales Abbild des Hautleistenreliefs wird direkt erzeugt. Eine dritte Technologie ist die Verwendung von Ultraschall. Hierbei tastet der Sensor mit Ultraschall den Finger ab und liest ein Echosignal ein (Breitenstein 2002, S. 36 ff.).

Jeder Fingerabdruck kann aufgrund von Unfällen, durch Abnutzung bei manueller Arbeit oder durch Krankheit kurz- oder langfristig verändert werden. Ferner sind Finger oft durch Schweiß, Talg oder Schmutz verunreinigt, daher weist das erzeugte Bild zum Teil starke Störungen auf. Deshalb werden häufig zusätzliche Verfahren zur Verbesserung der Bildqualität eingesetzt, die allerdings den Erkennungsvorgang verlangsamen (Breitenstein 2002, S. 37). Die meisten Fingerabdruck-Verfahren nehmen zudem beim Enrollment die Abdrücke mehrerer Finger auf, um darauf gegebenenfalls bei zu großen Störungen der Aufnahme zurückgreifen zu können.

Zur *Analyse der Fingerabdrücke* stehen generell zwei Verfahren zur Verfügung. Das geläufigste Verfahren, das so genannte mikroskopische Verfahren, extrahiert und speichert die auf dem Finger befindlichen End- oder Verzweigungspunkte von Hautleisten aus dem aufgenommenen Fingerbild („Minuzienanalyse"), meist sind davon 40–80 auf dem Finger zu finden (Breitenstein, 2002, S. 38). Die Minuzien werden aus dem Bild extrahiert und mit ihren Positionen auf dem Fingerabdruck versehen, so dass sich das „Minuzienmuster" ergibt. Bei der Verifikation werden die extrahierten Minuzien mit denen des Referenzabdrucks verglichen. Die Fingerabdrücke werden als identisch angesehen, wenn eine hohe Anzahl identischer Charakteristika erkannt wird. Bei makroskopischen Verfahren wird das Muster des Fingerabdruckes (Schleifen, Bögen, Wirbel) für einen Vergleich herangezogen („pattern matching"). Durch den Mustervergleich kann eine höhere Erkennungsleistung als bei den minuzienbasierten Verfahren realisiert werden, der Rechen- und Systemaufwand ist jedoch entsprechend höher.

Abb. 10: Lesegerät für Fingerabdrücke

Quelle: http://www.br-online.de/wissen-bildung/thema/biometrie/finger.shtml

Die Hauptanwendungsgebiete für die mittlerweile sehr ausgereiften Fingerabdruck-Verfahren sind derzeit – neben der Kriminalistik – bei Convenience-Applikationen wie Zugangsberechtigung zum PC oder Auto-Wegfahrsperre zu finden (Breitenstein 2002, S. 41).

Gesichtserkennung

Das Gesicht wird als biometrisches Merkmal durch Knochen, Muskulatur und Behaarung charakterisiert und unterscheidet sich zwischen den Geschlechtern und Bevölkerungsgruppen signifikant in seiner Ausprägung (Breitenstein 2002, S. 41).

Die Erfassung erfolgt mittels einer Kamera in zwei aufeinander folgenden Schritten: Der Gesichtsfindung („face detection“) und der Gesichtserkennung im engeren Sinne („face recognition“). Bei der Gesichtsfindung, der Separierung des Gesichtes vom Hintergrund, werden zahlreiche Verfahren angewendet. So wird beispielsweise das Gesicht durch die Registrierung kleinster Gesichtsbewegungen oder durch die Bestimmung von gesichtsähnlichen Formen im

Bild erkannt. Aufbauend auf der Information, dass ein Gesicht vorliegt, werden anschließend die Gesichtsposition und -größe normiert. Im zweiten Schritt, der Gesichtserkennung, muss – da nie zwei gleiche Bilder eines Gesichtes entstehen – die Variabilität in Pose, Ausdruck sowie alters- oder umweltbedingte Veränderungen berücksichtigt werden.

Die gängigen Systeme erfassen üblicherweise verschiedene geometrische oder strukturelle Merkmale. Beispielsweise werden beim System der Gesichtsmetrik individuelle Gesichtskennzeichen wie Auge, Nase, Mund zueinander ins Verhältnis gesetzt. Das System „Eigenface“ projiziert verschiedene Aufnahmen eines kompletten Gesichtes übereinander, um das Live-Merkmal möglichst genau nachzubilden. Beim so genannten Graph-Matching-Verfahren werden einzelne Gesichtssegmente direkt verglichen, wobei das Bild durch Gitterkoordinaten bis zur größtmöglichen Übereinstimmung verformt wird. Unabhängig von den gewählten Methoden wird nach hinreichender Übereinstimmung des Live-Bildes mit dem Referenzdatensatz auf Identität geschlossen (Breitenstein 2002, S. 44).

Abb. 11: Vermessung eines Gesichtes

Quelle: http://www.bundesdruckerei.de/pics/4_presse/fotoarchiv/border_downloads/23_bord.jpg

Die Gesichtserkennung ist eine *etablierte, relativ fortgeschrittene Technologie*, die hauptsächlich im Bereich der Zutrittskontrolle eingesetzt wird. Eine Verbesserung der Erkennungsleistung solcher Systeme wurde besonders in den letzten fünf Jahren aufgrund von deutlichen Fortschritten bei der Algorithmen-Entwicklung erreicht (NIST 2002a, S. 20). Insbesondere konnte der Einfluss von typischen Fehlerquellen, wie etwa Beleuchtung, Pose, Gesichtsausdruck oder auch Alterung erheblich reduziert werden. Unkontrollierte Lichtverhältnisse sind aber nach wie vor ein gewisses Problem.

Die Gesichtserkennung wird überwiegend im Verifikationsverfahren in zahlreichen Nutzungskontexten angewendet.

Iriserkennung

Bei der Iriserkennung wird zunächst ein hoch aufgelöstes Bild der Regenbogenhaut erfasst. Mithilfe eines kontrastverstärkenden Filters werden die Abgrenzungen der Iris bestimmt.

Abb. 12: Scannen einer Iris

Quelle: http://www.br-online.de/wissen-bildung/thema/biometrie/finger.shtml

In einem weiteren Schritt wird der Bereich zwischen dem inneren Rand (an der Pupille) und dem äußeren Rand (an der Lederhaut) segmentiert (Busch/Daum 2002, S. 157). Für die Merkmalsberechnung werden acht Zonen um die Pupille

herangezogen. Da die Iris der Muskel ist, der den Lichteinfall im Auge reguliert, besteht die technische Herausforderung darin, das Zusammenziehen und Erweitern der Pupille rechnerisch zu kompensieren. Das biometrische Template setzt sich zumeist aus einer Merkmalsmenge von 173 Informationen zusammen (GAO 2002, S. 47). Zur Identitätsprüfung wird das Template mit einem Referenztemplate verglichen. Liegt eine hinreichende Übereinstimmung vor, wird auf Identität geschlossen.

Bei der Iriserkennung wird allgemein die *hohe Einzigartigkeit des zu identifizierenden Merkmals* betont. Die Technologie wird bislang vor allem für Zugangskontrollen eingesetzt (GAO 2002, S. 202).

2. Detailanalyse der technologischen Leistungsfähigkeit

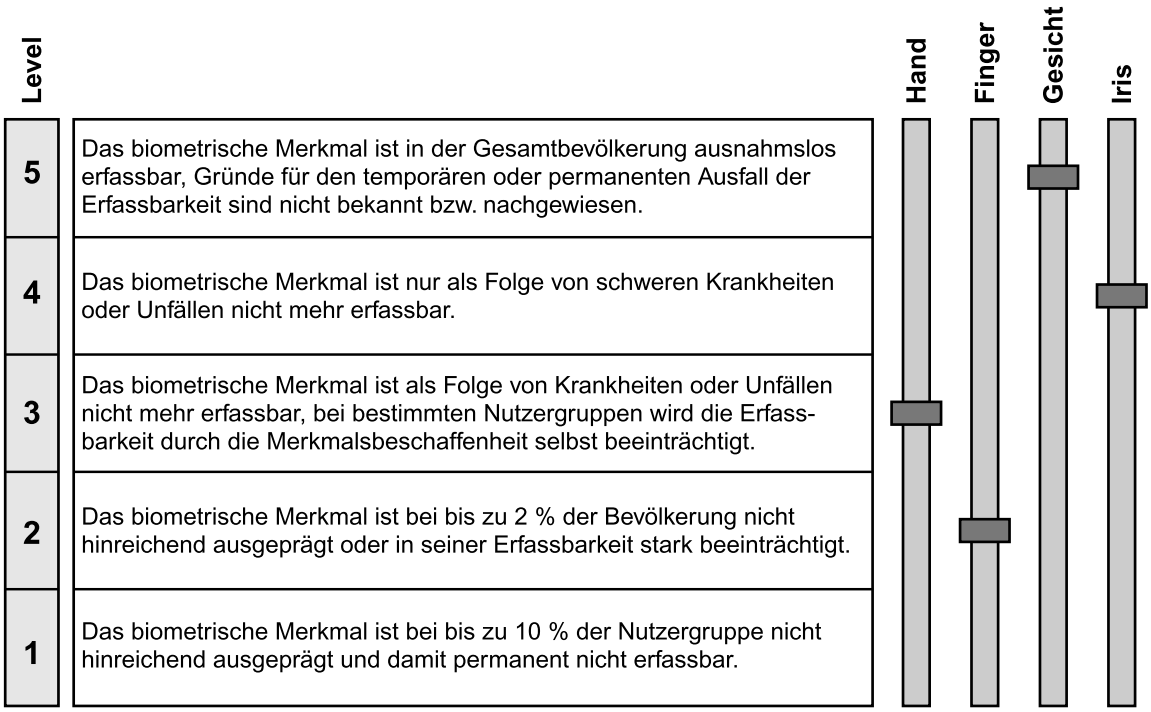
Die technologische Leistungsfähigkeit biometrischer Systeme ist in besonderem Maße vom jeweiligen Anwendungsgebiet abhängig. Im Folgenden werden solche Kriterien an die hier zu diskutierenden Systeme angelegt, die über ihre Leistungsfähigkeit bei Ausweisdokumenten bzw. bei der Kontrolle im Verifikationsmodus Auskunft geben können.

2.1 Erfassbarkeit

„Erfassung“ bedeutet die Aufnahme von biometrischen und alphanumerischen Personendaten als Referenzdatensatz einer Person in ein Rechnersystem, sowohl bei der Registrierung als auch bei der Erfassung am Kontrollort. Die Daten können direkt von der Person abgenommen oder über Formblätter in das System aufgenommen werden. Die Live-Erfassung bietet den Vorteil, dass die gewonnenen Daten sofort auf ihre Qualität überprüft werden können (STZ 2003, S. 16).

Für die Ausweisanwendung sollte die Merkmalsbeschaffenheit möglichst wenig Personen ausschließen. Ein bestimmter Umfang ständig nicht erfassbarer Personen in der Bevölkerung wäre ein Ausfallkriterium für biometrische Applikationen, wohingegen temporäre Nichterfassbarkeit das Enrollment zu einem späteren Zeitpunkt offen lässt. Die hier diskutierten Ausfallgründe liegen ausschließlich auf direkt merkmalsgebundener Ebene.

Abb. 13: Vergleichende Bewertung von Erfassbarkeit und Enrollment-Ausfallrate



Quelle: Booz Allen Hamilton et al. 2003, S. 66

Die Erfassbarkeit der *Handgeometrie* kann aufgrund von verletzten Fingern oder Knochenbrüchen temporär nicht möglich sein. Ein permanenter Ausfall der Erfassbarkeit kann bei überdurchschnittlich großen bzw. kleinen Handflächen auftreten, da Standardhandleser mit „durchschnittlichen" Handgrößen arbeiten. Kinder können daher erfahrungsgemäß erst ab einem Alter von acht Jahren durch Handgeometrie-Verfahren erfasst werden. Auch für Fälle schwerer Arthritis ist die Erfassung nicht möglich, da die vorgeschriebene Positionierung nicht erfolgen kann (Booz Allen Hamilton et al. 2003, S. 64).

Die Erfassbarkeit von *Fingerabdrücken* ist temporär durch Verletzungen der Fingerkuppen oder Fingerbrüche und durch Verschmutzungen der Fingerkuppen eingeschränkt. Ein permanenter Ausfall des Fingerabdruckmusters kann durch Verbrennungen oder Vernarbungen der Fingerkuppen erfolgen. Auch intensive manuelle Arbeit oder die Arbeit mit toxischen Mitteln kann das Fingermuster zerstören. Es müssten deshalb Ersatzfinger aufgenommen werden oder Ausweichmöglichkeiten auf andere Merkmale vorgesehen werden, was einen zusätzlichen finanziellen, administrativen und technischen Aufwand erfordert.

Die Erfassbarkeit des *Gesichtes* kann temporär, z.B. durch das Tragen von Verbänden nach schweren Gesichtsoperationen, ausfallen. Permanente Ausfälle, z.B. durch Krankheiten, die eine erhebliche Deformierung des Gesichtes zur Folge haben, dürften äußerst selten sein. Selbst bei lokal begrenzten Verletzungen bleibt das Gesicht als Gesamtmerkmal erfassbar (Booz Allen Hamilton et al. 2003, S. 65). Über den Einfluss von Gesichtsveränderungen durch plastische Chirurgie liegen keine aussagekräftigen Erkenntnisse vor.

Die Erfassbarkeit des *Irismusters* kann temporär durch eine Ausdehnung der Iris infolge der Einnahme bestimmter Medikamente (Atropin) beeinträchtigt werden. Permanente Ausfälle der Erfassbarkeit treten aufgrund von Augenerkrankungen z.B. Augenlinsentrübung oder Glaukome (Grüner Star) auf. Des Weiteren behindern Schlupflider oder schmale Augenlider, die die Iris teilweise bedecken, die Erfassung. Nach Busch/Daum (2002, S. 157) soll dies das Enrollment bei asiatischen Bevölkerungsgruppen erschweren.

Fazit

Im Falle einer biometrischen Ausrüstung der Ausweisdokumente muss sichergestellt sein, dass das Merkmal möglichst keine oder nur eine sehr geringe Zahl von Bürgern von der Anwendung ausschließt. Fingerabdruck-Verfahren werden dieser Anforderung nur bedingt gerecht. Das US-amerikanische Standardisierungsinstitut NIST folgert aus seinen Tests und den Erfahrungen anderer Einrichtungen und Behörden, dass bei etwa 2 % der Gesamtbevölkerung Probleme beim Enrollment auftreten (NIST 2002a, S. 21). Die International Biometric Group (IBG) weist darauf hin, dass bis zu 2 % der Bevölkerung keine ausreichend geeigneten Fingerabdrücke – bei bestimmten Sensoren – besitzen (IBG 2003, S. 8). Die Enrollment-Ausfallraten von Hand- und Iriserkennungs-Verfahren sind zwar geringer als die des Fingerabdrucks, bei bestimmten Nutzergruppen bleiben aber Probleme aufgrund ihres Alters oder ihrer Ethnie. Die Ausfallraten dieser Merkmale sind zum heutigen Zeitpunkt nur qualitativ einzuschätzen. Die Nutzerausfallrate für die Gesichtserkennung ist marginal (Booz Allen Hamilton et al. 2003, S. 65).

2.2 Erkennungsgenauigkeit und Fehlerwahrscheinlichkeit

Unterscheidbarkeit und Stabilität der biometrischen Merkmale und vor allem der berechneten Templates sind die wesentlichen Einflussgrößen für die Fehlerwahrscheinlichkeit des jeweiligen biometrischen Verfahrens: Die Unterscheidbarkeit beeinflusst die Falschakzeptanzrate, und die Stabilität beeinflusst die Falschrückweisungsrate.

2.2.1 Unterscheidbarkeit und Falschakzeptanzrate

Je höher die Anzahl eindeutiger biometrischer „Details“ pro biometrischem Merkmal, desto eindeutiger die Unterscheidbarkeit und desto geringer die Falschakzeptanzrate. Dabei ist nicht nur die Menge der Informationen bedeutend, sondern auch ihre statistische Unabhängigkeit und damit geringe Redundanz. Eine zu geringe Informationsmenge im Merkmal verringert im Allgemeinen die Trennungsleistung zwischen den Merkmalen und erhöht so die Falschakzeptanzrate (Booz Allen Hamilton et al. 2003, S. 67). Die folgende Tabelle gibt eine Übersicht über die Anzahl der für die biometrische Erkennung benutzten distinktiven Informationen der einzelnen Merkmale.

Tab. 4: Übersicht der distinktiven, für die biometrische Analyse benutzten Informationen

Merkmal	*Informationen*
Hand	etwa 90 geometrische Parameter
Finger	40–80 unabhängige Minuzien oder bis zu ca. 900–1.200 globale Muster
Gesicht	je nach Methode von ca. 512 für die Eigenface-Methode bis ca. 2.000 unabhängige Merkmale bei Graph-Matching-Verfahren
Iris	ca. 170 unabhängige Strukturmerkmale

Quellen: Booz Allen Hamilton et al. 2003, S. 67; Breitenstein 2002; GAO 2002; NIST 2002a

2.2.2 Stabilität und Falschrückweisungsrate

Der maßgebliche Grund für Falschrückweisungen sind Unterschiede zwischen dem Referenzdatensatz und dem Live-Merkmal, die bei der Verifikation entstehen können. Daher müssen die ausgewerteten Merkmale und die daraus ge-

nerierten Templates eine ausreichende Stabilität besitzen. Diese definiert sich durch die Resistenz des Merkmalsmusters gegenüber Veränderungen durch Wachstum, Krankheit oder Verschleiß. Daneben können merkmalsunabhängige Störquellen bei der Aufnahme die Qualität der Informationen beeinträchtigen. Diese können aber durch ein ausgereiftes Erkennungsverfahren und einen hochwertigen Sensor sowie durch Anwenderschulungen gut kompensiert werden (Booz Allen Hamilton et al. 2003, S. 70).

Das *Handgeometriemuster* des Menschen weist zunächst eine geringe zeitliche Stabilität auf. Insbesondere Wachstum führt zu starken Veränderungen des Handmusters. Ab einem Alter von etwa 13 oder 14 Jahren stabilisiert sich das Handmuster (GAO 2002, S. 159), erst ab einem Alter von etwa 20 Jahren erfolgen keine bedeutenden Veränderungen mehr. Die Hände verändern sich allerdings bei auftretender Arthritis (Booz Allen Hamilton et al. 2003, S. 61). Schwellungen, wie sie nach langen Flügen auftreten, können die Falschrückweisungsrate beeinflussen (B&L 2003, S. 12). Eine externe Störquelle sind die nicht exakte Auflage der Handfläche auf die Sensoroberfläche oder das Tragen von Ringen bei der Merkmalsaufnahme (GAO 2002, S. 160).

Das *Fingermuster* hat eine eingeschränkte Stabilität, da Veränderungen des Fingermusters unter anderem durch Abnutzungen, Verletzungen und Verschmutzungen, insbesondere bei manuell arbeitenden Menschen auftreten (Breitenstein 2002, S. 40). Zusätzliche Störfaktoren sind nicht exakt auf der Sensoroberfläche aufliegende Fingerkuppen oder verschmutzte oder zerkratzte Sensoroberflächen (GAO 2002, S. 158).

Das *Gesichtsmuster* besitzt insgesamt eine mittlere Stabilität. Es erfährt durch Wachstum bis zu einem Alter von 12–14 Jahren Veränderungen, danach weist es eine hohe Stabilität auf. Störquellen sind unkontrollierte Lichtverhältnisse, die zu einem Informationsverlust bei der Bildaufnahme führen. Posenvarianzen können bei einer Drehung des Kopfes bis zu 20° verarbeitet werden. Haarwuchs, Brillen oder Schminke sind Störungen, die bei qualitativ hochwertigen Verfahren gut kompensiert werden können (Booz Allen Hamilton et al. 2003, S. 69).

Das *Irismuster* besitzt eine hohe zeitliche Stabilität. Es erreicht im Laufe des ersten Lebensjahres seine endgültige Ausprägung. Allerdings können im Alter Krankheiten wie Glaukome zu Veränderungen des Irismusters führen (GAO 2002, S. 197). Störquellen für die eindeutige Erkennung sind unkontrollierte Lichtverhältnisse, darüber hinaus Posenvarianzen, teilweise Verdeckungen durch Wimpern/Augenlider oder Reflexionen der feuchten Augenoberfläche (Busch/Daum 2002, S. 157).

Fazit

Die Handgeometrieerkennung erweist sich im Hinblick auf die Anforderung der Unterscheidbarkeit als kritisch, da sie mit einer begrenzten Zahl geometrischer Informationen arbeitet. Besonders bei umfangreichen Anwendungen ist das Risiko identischer Handgeometrieformen nicht auszuschließen. Das General Accounting Office hat aufgrund dieser mangelnden Unterscheidbarkeit die Handgeometrieerkennung für Grenzkontrollen skeptisch beurteilt (GAO 2002, S. 4 f.).

Die Unterscheidbarkeit bei Iris, Finger und Gesicht ist aufgrund der hohen Anzahl an eindeutigen Informationen grundsätzlich besser gewährleistet. Die in den USA durch das Standardisierungsinstitut NIST durchgeführten Qualitätstests haben die hohe Einzigartigkeit der Merkmale Finger und Gesicht auch bei großen Datenbeständen (620.000 Fingerabdrücke, 120.000 Gesichtsbilder) bestätigt. Die Einzigartigkeit („accuracy“) der Iris wird ähnlich hoch wie die des Fingers eingeschätzt (NIST 2002a, S. 7) – Belege aus Großanwendungen liegen bislang aber nicht vor.

Für biometrische Anwendungen ist es wichtig, dass das Merkmal sich nicht in kurzen Zeitabständen verändert. Unter dem Gesichtspunkt der Stabilität ist der Einsatz von Fingerabdruck-Verfahren aufgrund bestimmter Einschränkungen kritisch zu beurteilen. Nachteilig bei der Handgeometrieerkennung ist ihre späte Stabilisierung erst im Alter von 20 Jahren, da ein deutscher Bürger ab dem Alter von 16 Jahren zum Personalausweisbesitz verpflichtet ist. Die Stabilität des Gesichtes ist für die Ausweisanwendung ausreichend, da Veränderungen dieses Merkmals innerhalb größerer Zeitabstände erfolgen, so dass mit vertretbarem Aufwand „Neuregistrierungen“ vorgenommen werden könnten. Die Iris dürfte in Bezug auf das Kriterium der Stabilität am unproblematischsten sein.

2.2.3 Fehlerraten – ausgewählte Testergebnisse

Die umfangreichsten Studien und Tests liegen für Fingerabdruck- und Gesichtserkennungs-Verfahren vor (Tab. 5 u. 6). Das US-amerikanische Standardisierungsinstitut NIST beispielsweise hat die Erkennungsleistung der Gesichterkennung und der Fingerabdruckerkennung auf der Basis von bis zu 120.000 Gesichtsbildern und 620.000 Fingerabdrücken in Originaldatenbeständen getestet (NIST 2002a, S. 5). Die Erkennungsleistung von Iris- und insbesondere Handerkennungs-Verfahren ist bislang noch nicht großflächig getestet worden, die vorliegenden Tests begrenzten Umfangs (Tab. 7 u. 8) sind für die Ausweisan-

wendung nur bedingt aussagekräftig.[5] Auch ist darauf hinzuweisen, dass die Angaben ausschließlich für Verifikationsanwendungen gelten. Für andere Szenarien, wie Abgleich mit Fahndungslisten oder Datenbanken, fallen die Fehlerraten teilweise deutlich anders aus. Schließlich muss für die Gesichtserkennungs-Systeme angemerkt werden, dass die Tests zwar unter kontrollierten Lichtbedingungen günstige Werte erbringen, dass aber Anwendungen außerhalb geschlossener Gebäude doch drastische Qualitätseinbußen nach sich ziehen (NIST 2002a).

Die in den Tabellen aufgeführten Verifikationstests und ihre Ergebnisse für die einzelnen Verfahren sind nur begrenzt vergleichbar, u.a. wegen z.T. großer Unterschiede in den Testszenarien, in den Testumfängen und in den Tests angelegten Schwierigkeitsgraden. Anzumerken ist auch, dass insbesondere bei den Tests mit über 100.000 Datensätzen die jeweiligen biometrischen Merkmale größtenteils in digitalisierter Form (Porträtfotos, Fingerabdruckbilder) genutzt wurden, um Mehrfach-Testdurchläufe unter wechselnden Bedingungen organisatorisch überhaupt durchführen zu können.

Letztlich darf bei einer vergleichenden Bewertung der durchgeführten Tests im Bereich der Fingerabdruck- und der Gesichtserkennung nicht übersehen werden, dass gescannte Bilder – mit teilweise schlechter Bildqualität – verwendet wurden. Dies ist beim Vergleich mit den Testergebnissen für die Iriserkennung zu berücksichtigen, da diese Testverfahren mit den durch das Testsystem selbst enrollten Bildern durchgeführt wurden. Somit waren dort die Randbedingungen in Bezug auf Hintergrund und Lichtverhältnisse günstig sowie das Bildmaterial von standardisierter und guter Qualität.

5 Grundsätzlich wären Tests in der Größenordnung von mehreren Millionen erforderlich: „Eine statistische Signifikanz von Modellen wäre bei einer FAR-Angabe von 10^{-6} mit 30 Mio. Versuchen und nicht mehr als 30 Fehlversuchen erreicht.“ (Bromba 2003, S. 17)

Tab. 5: Fehlerratenangaben für Fingerabdruck-Verfahren in neueren Tests

Test	*Umfang*	*FAR*	*FRR*	*Datenherkunft*
Test „Information Technology Laboratory“ des NIST im Rahmen der staatlichen Evaluierung biometrischer Verfahren für den Einsatz bei Grenzkontrollen (NIST Accuracy Certification Study 2002)	Auswahl von 6.000 Fingerabdrücken operationeller Qualität aus Datenbank mit 620.000 Personen	1 %	10 %	Auswahl aus der INS INDEX (Immigration and Naturalization Service) Datenbank, die insgesamt 3 Mio. Fingerabdruckbilder von 620.000 Personen operationeller Qualität beinhaltet.
Test „Information Technology Laboratory“ des NIST im Rahmen der staatlichen Evaluierung biometrischer Verfahren für den Einsatz in Grenzkontrollen (NIST SD 29 Verification Tests 2002)	insgesamt 6.048 Fingerabdruckbilder mittlerer Qualität (216 Personen à zwei Datensätze mit je zehn gerollten und vier flachen Fingerabdrücken)	1 %	5,3 %	Spezial-Datenbank des NIST
2. Internationaler Wettbewerb für Fingerabdruck-Algorithmen in Verifikationsanwendungen; Organisatoren: Biometric Systems Lab, U.S. National Biometric Test Center, Pattern Recognition and Image Processing Laboratory of Michigan State University. 31 Teilnehmer (Fingerprint Verification Competition 2002)	insgesamt 880 Fingerabdruckbilder mittlerer Qualität von 110 Fingern	1 %	Teilnehmermittelwert: 9 %	eine künstliche, drei Original-Datenbanken

Quellen: FVC 2002; NIST 2002a u. b, nach Booz Allen Hamilton et al. 2003, S. 74

Tab. 6: Fehlerratenangaben für Gesichtserkennungs-Verfahren in neueren Tests

Test	*Umfang*	*FAR*	*FRR*	*Datenherkunft*
Test „Information Technology Laboratory“ des NIST im Rahmen der staatlichen Evaluierung biometrischer Verfahren für den Einsatz in Grenzkontrollen (NIST Accuracy Certification Study 2002)	3.000 aus 620.000 Bildern operationeller Qualität	1 %	10 %	Auswahl aus der INS (Immigration and Naturalization Service)-FACE-Datenbank mit je zwei Porträtbildern
2. internationaler Leistungstest, getragen durch NIST, DoD Counterdrug Technology Development Program Office und 17 weitere Institutionen (Face Recognition Vendor Test [FRVT 2002])	121.000 Bilder operationeller Qualität von ca. 37.000 Personen	1 %	Mittelwert der drei Test-sieger: 11 %	Bildauswahl aus der U.S. Department of State Visa-Datenbank mit 6,3 Mio. Bildern von Visaantragstellern aus Konsulaten in Mexiko
operationeller Test (Zutrittskontroll-Szenario) durchgeführt durch die US Navy, getragen durch das „US DoD Counterdrug Technology Development Program Office“ (Face recognition at a Chokepoint, Scenario Evaluation 2002)	drei Datenbanken: 100/400/1.575 Bilder operationeller Qualität	0,4 % bei Stufe 1, 0,5 % bei Stufe 2	2,9 % bei Stufe 1, 5,2 % bei Stufe 2	Bilder operationeller Qualität aus Mitarbeiterausweisen von NAVSEA-Angestellten, Lieferanten und Freiwilligen; Test in zwei Schwierigkeitsstufen: Stufe 1: Brille bei Enrollment u. Verifikation, Stufe 2: Enrollment mit, Verifikation ohne Brille und umgekehrt

Quellen: Bone/Blackburn 2002; FRVT 2002; NIST 2002a u. b, nach Booz Allen Hamilton et al. 2003, S. 75

Tab. 7: Fehlerratenangaben für Handgeometrie-Verfahren in neueren Tests

Test	*Umfang*	*FAR*	*FRR*	*Anmerkung*
Test der „Aviation Security Biometrics Working Group“ (ASBWG) der „Federal Aviation Administration“ in Kooperation mit der „Safe Skies Alliance“ (FAA Hand Geometry Testing 2001)	39 Personen	0–2 %	1–5 %	operationeller Test: Zutrittskontrolle von Flughafenangestellten
Test des „Centre for Mathematics and Scientific Computing National Physical Laboratory“ (GB) (NPL National Physical Laboratory Biometric Product Testing 2000)	200 Personen	1 %	1,4 %	Verifikationstests mit Freiwilligen in einem simulierten Büroumfeld

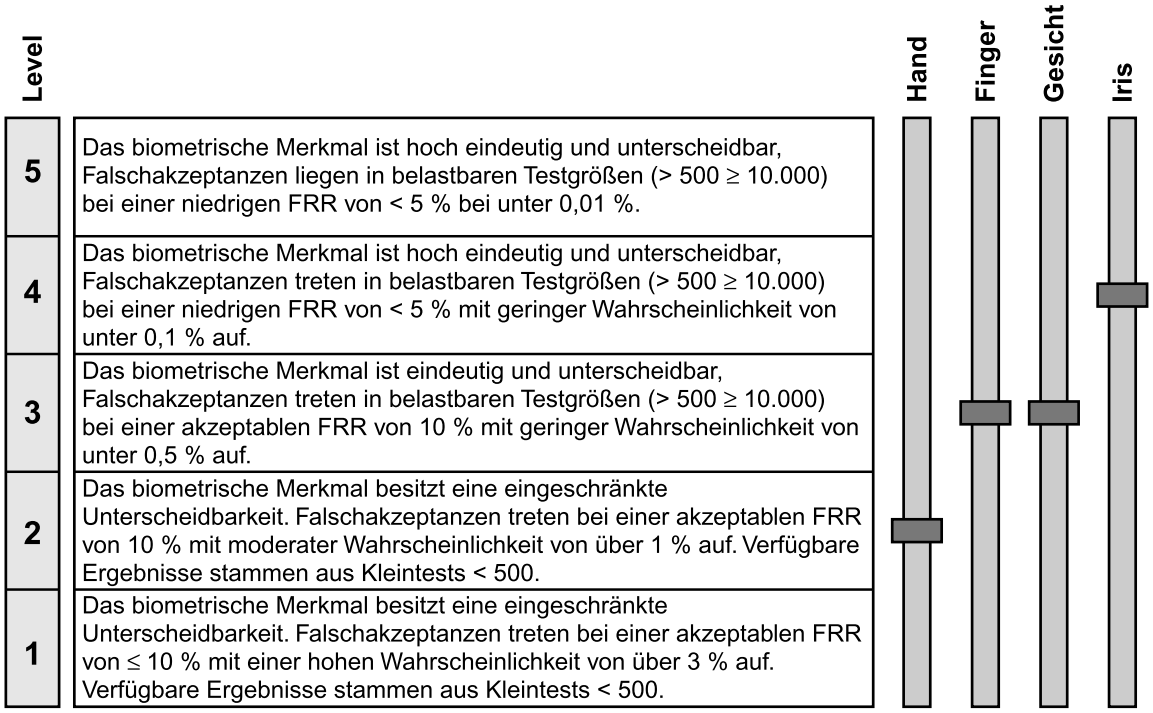
Quellen: FAA 2001; GAO 2002, S. 161 f.; NPL 2001; nach Booz Allen Hamilton et al. 2003, S. 76

Tab. 8: Fehlerratenangaben für Iriserkennungs-Verfahren in neueren Tests

Test	*Umfang*	*FAR*	*FRR*	*Anmerkung*
Test durchgeführt durch das U.S. Army Research Laboratory (U.S. Army Research Laboratory 2001)	258 Personen	< 1 %	6 %	Verifikationstests mit Freiwilligen in einem simulierten, operationellen Umfeld
Pilotprojekt: Verifikationsanwendung im Rahmen eines automatisierten Passagier-Check-in (Privium Programm Flughafen Schiphol/Niederlande)	ca. 2.000 Personen	< 0,001 %	< 1 %	Vielflieger-Programm des Flughafenbetreibers Schiphol Group mit Reisenden aus 18 europäischen Ländern; Projektbeginn: Oktober 2001
Test des „Centre for Mathematics and Scientific Computing National Physical Laboratory”(GB) (NPL National Physical Laboratory Biometric Product Testing 2000)	200 Personen	0 %	1,9 %	Verifikationstests mit Freiwilligen in einem simulierten Büroumfeld

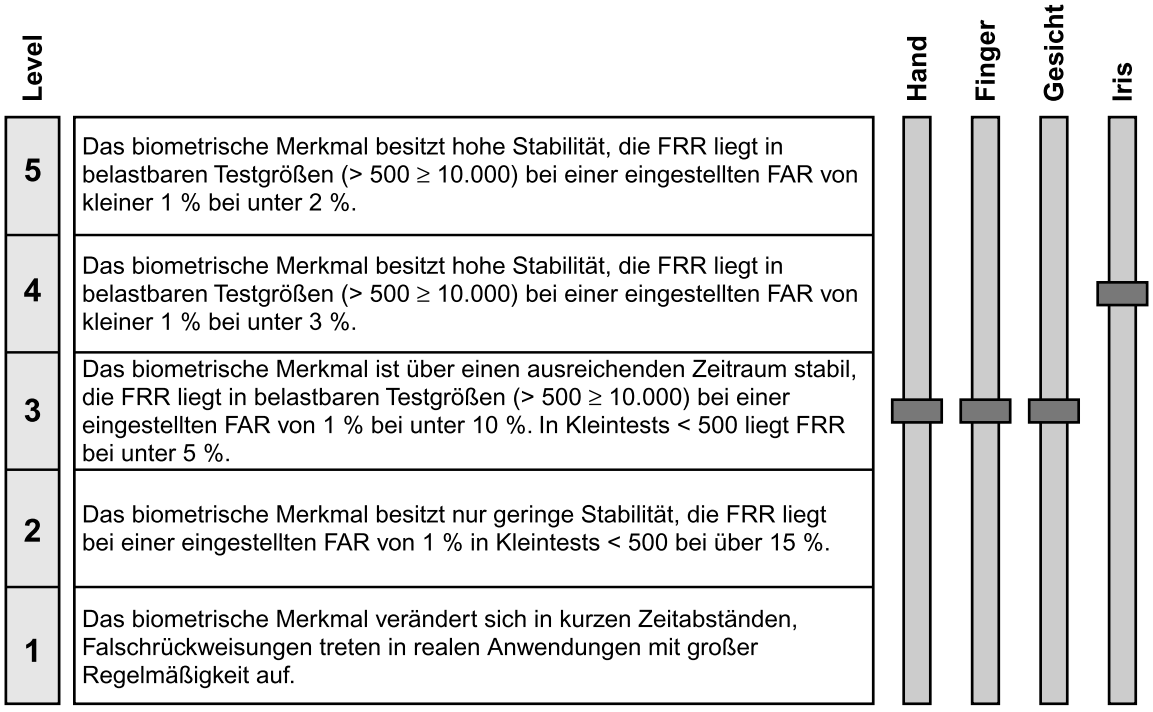
Quellen: GAO 2002, S. 201; National Defense Magazine 2001; NPL 2001, nach Booz Allen Hamilton et al. 2003, S. 76

Abb. 14: Vergleichende Bewertung der Falschakzeptanzrate (FAR)



Quelle: Booz Allen Hamilton et al. 2003, S. 79

Abb. 15: Vergleichende Bewertung der Falschrückweisungsrate (FRR)



Quelle: Booz Allen Hamilton et al. 2003, S. 79

Fazit

Bisher durchgeführte Studien deuten auf eine hohe Erkennungsleistung von Iriserkennungs-Verfahren hin, die es aber noch in Großanwendungen zu überprüfen gilt. Die Handgeometrieerkennung erzielt zwar in Kleinszenarien gute Erkennungsraten, das Problem der nicht eindeutig unterscheidbaren Identität von Handgeometriemustern in größeren Anwendungen müsste allerdings erst in umfangreichen Teststudien widerlegt werden. Fingerabdruck- und Gesichtserkennungs-Verfahren haben in aktuellen und unabhängigen Studien zur Leistungsmessung bei umfangreichen Datenmengen ihre hohe Erkennungsleistung unter Beweis gestellt. Die Leistung der beiden Verfahren bei Verifikationsanwendungen ist dabei ungefähr gleich einzustufen (GAO 2002, S. 20).

Die erhobenen Werte für die Erkennungsleistung spiegeln den heutigen Stand der Technik wider. Bei Fingerabdruck- und Gesichtserkennungs-Verfahren als Verfahren, die eine aufwendige Mustererkennung durchführen, ist davon auszugehen, dass sie sich weiter verbessern (Booz Allen Hamilton et al. 2003, S. 78). Sowohl Fingerabdruck- als auch Gesichtserkennungs-Verfahren sind heute bereits so weit ausgereift und leistungsstark (s. Abb. 14 u. 15), dass ihr Einsatz im Verifikationsmodus im Vergleich zu bisherigen Grenzkontrollen eine Effektivierung der Kontrollen verspricht. Für Identifikationsaufgaben wird das Fingerabdruck-Verfahren vom GAO (2002, S. 1) als leistungsstärker eingeschätzt.

Die Frage, ob die erwartbare Erkennungsleistung bei der Verifikation eine hinreichende Sicherheit gewährleistet wird und ob die erhofften Verbesserungen bei der Grenzkontrolle den hierzu erforderlichen Aufwand rechtfertigen, muss politisch entschieden und begründet werden. Dabei sollte offen diskutiert werden, dass – trotz eindrucksvoller geringer Fehlerraten – in der Praxis eines Masseneinsatzes immer noch eine relativ große Zahl von Personen falsch erkannt wird.

2.3 Bedienungsaufwand und Verständlichkeit bei Enrollment und Verifikation

Die Prozessgeschwindigkeit biometrischer Verfahren wird von der Dauer des Enrollments und der Verifikation bestimmt. Der hierfür erforderliche Zeitaufwand ist wesentlich abhängig vom Positionierungsaufwand für die Merkmalserfassung und der Verständlichkeit des Vorgangs für den Nutzer. Hierbei ist der *Kooperationsgrad des Anwenders* eine wesentliche Einflussgröße für die

Bedeutung der Eignung biometrischer Verfahren. In der Literatur wird häufig darauf hingewiesen, dass intuitiv handhabbare Verfahren besser akzeptiert werden als solche, die spezifische Verhaltensschritte vorschreiben oder vom Nutzer eine ungewohnte Haltung erfordern.

Die Bedienung von *Handgeometrie-Systemen* schreibt eine exakte Positionierung der Hand auf dem Lesegerät mittels Stäbchen vor. Dies verhindert Positionierungsfehler und fördert die Verständlichkeit. Die direkte Auflage der Hand auf der Sensoroberfläche stößt bei einem Teil der Nutzer auf hygienische Vorbehalte (GAO 2002, S. 160).

Bei den *Fingerabdruck-Systemen* muss der Finger exakt auf einem Sensor positioniert und der Auflagedruck kontrolliert werden. Dies führt bei einem Teil der Benutzer zu Problemen, die aber nach kurzer Einlernzeit behebbar sind. Für die meisten Fingerabdruck-Systeme werden wegen etwaiger Beeinträchtigungen des Fingermusters mehrere Finger eingelesen, was den Bedienungsaufwand erhöht. Fingerabdruck-Verfahren als kontaktbehaftete Lösung stoßen zum Teil auf hygienische Bedenken (Breitenstein 2002, S. 40).

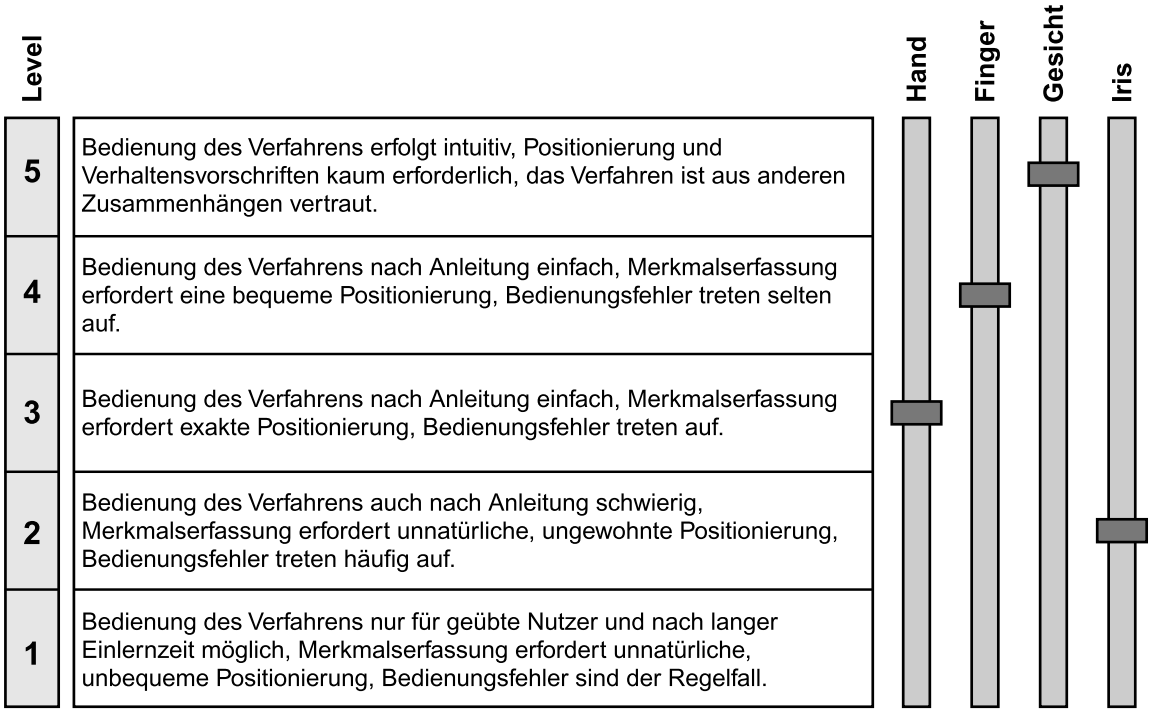
Die *Gesichtsaufnahme* erfordert keinen Kontakt, ist bis zu einer Distanz von 1,5 m möglich und verlangt vom Nutzer nur relativ geringen Positionierungsaufwand. Die Einlernzeiten sind gering, und Verhaltensvorschriften sind nur in geringem Maße erforderlich. Gewisse Akzeptanzprobleme können sich ergeben, da manche Nutzer Bedenken äußern, ohne ihr Einverständnis erfasst zu werden (GAO 2002, S. 174).

Die *Iriserkennung* erfordert eine exakte Positionierung der Augen vor der Kameralinse, die Distanz zur Kamera liegt bei Zugangskontrollen zwischen 7,5 und 25 cm (GAO 2002, S. 194). Zur Einnahme der optimalen Position sind genaue Verhaltensvorschriften zu befolgen. Der Positionierungsaufwand ist dementsprechend hoch. Zur Benutzerführung sind einige Systeme mit Sprachausgaben ausgestattet. Bewegliche Weitwinkel-Kameras, zur Steigerung der Nutzerfreundlichkeit, sind mittlerweile verfügbar, allerdings liegen hiermit noch keine verwertbaren Erfahrungen vor.

Für eine Gesamtbeurteilung in organisatorischer und zeitlicher Hinsicht muss als zusätzliche Größe und weiterer Zeitaufwand die Systemumgebung, z.B. die Integration des Systems in eine Durchgangskabine oder Schleuse, berücksichtigt und damit weiterer Zeitaufwand veranschlagt werden.

Im Vergleich zu dem eben diskutierten Zeitrahmen fällt die eigentliche Rechenzeit (nach korrekter Erfassung des Merkmals) weniger ins Gewicht, soll aber dennoch angesprochen werden.

Abb. 16: Vergleichende Bewertung von Bedienungsaufwand/Verständlichkeit



Quelle: Booz Allen Hamilton et al. 2003, S. 85

Für alle hier diskutierten Verfahren beträgt der Zeitaufwand für das Enrollment im engeren Sinn – beginnend mit der konkreten Positionierung vor dem Sensor und endend mit der Ablage des generierten Templates – normalerweise zwischen drei und zehn Sekunden. Die Rechenzeit zur Erzeugung des biometrischen Templates umfasst nur Sekundenbruchteile.

Für die Verifikationsgeschwindigkeit ist der Merkmalserfassungsvorgang die wesentliche Größe. Wie beim Enrollment umfasst die Zeit für die Verifikation die Erfassung und Umrechnung des Live-Merkmals in ein biometrisches Template, den Vergleich zwischen diesen und dem Referenztemplate und die Aussage, dass eine Person erkannt oder abgelehnt ist. Nach bislang vorliegenden Erfahrungen ist für die Verifikationszeit – ebenfalls wie beim Enrollment beginnend mit der korrekten Positionierung des Merkmals – ebenfalls eine Zeitspanne von drei bis zehn Sekunden zu veranschlagen (Booz Allen Hamilton et al. 2003, S. 80).

Fazit

Für die Ausweisanwendung sind *Verfahren mit niedrigem Bedienungsaufwand* und hoher Verständlichkeit *günstig* (s. Abb. 16). Vorteile bieten hier Gesichtserkennungs-Verfahren als kontaktlose Verfahren ohne großen Positionierungsaufwand. Fingerabdruck-Verfahren sind zwar bequem nutzbar. Allerdings können Probleme mit der Verschmutzung des Sensors auftreten. Auch ist zur Vermeidung von Bedienungsfehlern eine kurze Einlernzeit erforderlich. Auch bei der Handgeometrieerkennung treten Bedienungsfehler eher selten auf. Die Iriserkennung ist im Hinblick auf den Bedienungsaufwand im Vergleich weniger günstig einzuschätzen, da sie genaue Verhaltensvorschriften und eine gewisse Einlernzeit erfordert (Booz Allen Hamilton et al. 2003, S. 85).

Zusammenfassend lässt sich feststellen, dass alle vier Verfahren grundsätzlich den bisher üblichen Zeitrahmen der Ausweisbeantragungs- und Kontrollprozesse nicht entscheidend verändern. Für eine umfassende Einschätzung müssen aber weitere Aspekte wie die Systemumgebung sowie bauliche, infrastrukturelle und organisatorische Aspekte mit herangezogen werden. Ob beispielsweise bei der Personenkontrolle an Flughäfen biometrische Verfahren längerfristig zu Zeiteinsparungen führen könnten, hängt von den konkreten Systembedingungen und Leistungsanforderungen vor Ort ab. Das GAO schließt eine Verlängerung der Kontrollzeiten nicht aus, wenn keine entsprechenden Maßnahmen (z.B. beim Personal) ergriffen werden (GAO 2002, S. 126).

2.4 Ein vorläufiges Fazit

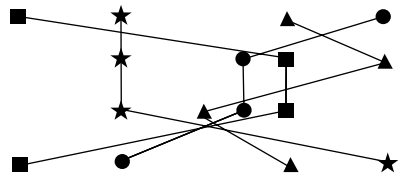
Der bisher durchgeführte technische Leistungsvergleich ergibt zunächst – bei einer gleichen Gewichtung aller Kriterien – ein Ranking der vier Verfahren, das in Tabelle 9 zusammengefasst wird.

Die *Gesichtserkennung* erweist sich bei zwei Kriterien als führend (Enrollment-Ausfallrate, Bedienungsaufwand/Verständlichkeit), sie liegt aber bei der Erkennungsleistung nur auf Level 3. Die *Iriserkennung* ist bei der Erkennungsleistung (FAR und FRR) führend. Sie weist allerdings schwächere Werte beim Bedienungsaufwand auf. Die *Handgeometrieerkennung* weist insgesamt durchschnittliche Leistungen, allerdings eine hohe Falschakzeptanzrate auf. Die *Fingerabdruckerkennung* ist bei keinem Kriterium den anderen Verfahren überlegen, weist aber im Durchschnitt gute Werte auf, sieht man davon ab, dass sich

die geringe Stabilität des Merkmals bei der Bewertung der Enrollment-Ausfallrate negativ niederschlägt.

Tab. 9: Zusammenfassung des technischen Vergleichs

Evaluationskriterien	*L5*	*L4*	*L3*	*L2*	*L1*
Enrollment-Ausfallrate (Nutzerausfallrate)					
Erkennungsleistung: FAR					
Erkennungsleistung: FRR					
Bedienungsaufwand/Verständlichkeit					



■ Gesichtserkennung ★ Iriserkennung ▲ Handgeometrieerkennung ● Fingerabdruckerkennung

Quelle: nach Booz Allen Hamilton et al. 2003, S. 101

Insgesamt ist der Schluss zu ziehen, dass drei Verfahren – Gesichts-, Iris- und Fingerabdruckerkennung – über eine in etwa vergleichbare Leistungsfähigkeit verfügen. Die Handgeometrie fällt demgegenüber etwas ab.

Für eine breitere Fundierung des Auswahl- und Entscheidungsprozesses müssten weitere Überlegungen angestellt und insbesondere Aspekte, die die internationale Zusammenarbeit, die globale Interoperabilität, die Leistungs- und Funktionsanforderungen aus politischer Sicht (high-level-goals), die gesellschaftliche Akzeptanz sowie die Datenschutzfreundlichkeit betreffen, in die Erwägungen mit einbezogen werden.

Auch ergäbe sich aus nationaler Sicht die Notwendigkeit, den Aufwand und die Kosten einer Einführung biometrisch aufgewerteter Ausweisdokumente vergleichend abzuschätzen. Als Einstieg sollen die beiden folgenden Abschnitte dienen. Zunächst werden Überlegungen zur Integration solcher neuartigen Dokumente in die bestehenden Verfahren der Beantragung und Produktion und danach erste modellhafte Erörterungen der möglichen Kosten zur Diskussion gestellt.

3. Integration in etablierte Prozesse der Beantragung und Produktion von Ausweisdokumenten für Bundesbürger

Eine biometrische Ausrüstung von nationalen Ausweisdokumenten könnte eine biometrische Datenerhebung der gesamten Bevölkerung mit dem entsprechenden technischen (und finanziellen) Aufwand der Datenerhebung und -ablage erforderlich machen. Im Folgenden werden erste, vorläufige Überlegungen angestellt, wie sich die einzelnen Verfahren in den etablierten Prozess der Ausweisbeantragung und die vorhandene technische Infrastruktur in den Meldebehörden sowie in die Produktion integrieren lassen.

Datenerhebung

Der Einsatz automatischer *Gesichtserkennungs-Verfahren unter Nutzung vorliegender Lichtbilder hinreichender Qualität* erfordert voraussichtlich den geringsten Aufwand der Datenerhebung. Unter der – nicht unumstrittenen – Prämisse der Eignung vorliegender Lichtbilder könnten Templategenerierung und biometrischer Datenvergleich auf dieser Basis bewerkstelligt werden, ohne dass ein zusätzliches Enrollment erforderlich wäre. Der bisherige, sichere Ablauf der Ausweisbeantragung könnte beibehalten werden, Risiken des Aufwandes einer neuen Datenerhebung entfielen. Das biometrische Template kann sowohl dezentral in den Meldebehörden als auch zentral, z.B. in der Produktionsstätte, aus den Rohdaten im Lichtbild erstellt werden. Empfehlenswert wäre aber eine Bildqualitätsüberprüfung in den Meldestellen durch einen Vergleich zwischen Lichtbild und Live-Bild der Person. Zukünftig würden sich die Prozeduren an den von der ICAO vorgegebenen Standards für die Integration von Lichtbildern in internationale Reisedokumente orientieren.

Für *Fingerabdruck-, Handgeometrie- und Iriserkennungs-Verfahren* müsste eine komplette Erhebung der biometrischen Daten der deutschen Bevölkerung erfolgen. Bei einer dezentralen Erfassung wäre es erforderlich, alle Meldestellen und Bürgerbüros, in denen der Antragsprozess durchgeführt wird, mit biometrischen Systemen auszurüsten. Aus Gründen der Qualitätssicherung müsste das Personal geschult und der Erfassungsprozess sehr sorgfältig durchgeführt werden. Räumliche und bauliche Veränderungen wären eine eventuelle weitere Konsequenz.

Bei einer zentralen Erfassung müsste für die Templategenerierung auf der Basis eines Fingerabdruckes dieser abgerollt auf einem Träger zur Verfügung gestellt werden. Hierzu wäre eine Qualitätsüberprüfung und entsprechend geschultes Personal erforderlich. Für die Iriserkennung und die Handgeometrieerkennung ist grundsätzlich eine dezentrale Erfassung in den Meldestellen durchzuführen, da die Ursprungsmerkmale sich nicht als Rohdaten ablegen und versenden lassen. Dies erhöht den organisatorischen und finanziellen Aufwand (Booz Allen Hamilton et al. 2003, S. 92 f.).

Während für die Erhebung von Fingerabdrücken und für die Gesichtserkennung umfangreiche Erfahrungen aus Großanwendungen vorliegen, fehlen Erfahrungswerte mit der großflächigen Datenerfassung und -pflege bei der Erhebung von Irismuster und Handgeometrie. Probleme, Kosten oder Risiken einer bevölkerungsweiten Irismuster- oder Handgeometrieerhebung müssten deshalb sorgfältig antizipiert werden (NIST 2002a, S. 5).

Datenspeicherung im Ausweisdokument

Als Speichertechnologie kommt zum einen die Ablage des „Ursprungsmerkmals“ *in optischer Form* (z.B. Fotos) in Frage. Zum Zweiten ist eine Templatespeicherung *in drucktechnischer Form* durch 1D/2D-Barcodes oder Hologramme sowie – drittens – eine Speicherung *in elektronischer Form* durch kontaktlose Chips, kontaktbehaftete Chips oder Dual Interface Chips möglich.

Es ist zu fragen, wie sich das jeweilige Speicherverfahren in das etablierte Dokumentenkonzept integrieren lässt. Es lassen sich hierzu folgende Einschätzungen formulieren (Booz Allen Hamilton et al. 2003, S. 94 ff.):

– Das kostengünstigste Speicherverfahren ist die Ablage des Merkmals Gesicht in optischer Form durch Abdruck eines Fotos auf dem Ausweisdokument, da dieses Verfahren heute schon fester Bestandteil der Ausweisproduktion ist. Könnte eine biometrische Analyse des Gesichtes vom Foto erfolgen, müsste kein biometrisches Template gespeichert werden. Die Übernahme der ICAO-Empfehlungen würde einen hinreichenden Bildstandard sicherstellen. Die Fotoablage des Fingerabdruckes erforderte eine Änderung des Ausweisdokumentes, da das Foto des jeweiligen Merkmals zusätzlich zum „Gesichtsfoto“ abgelegt werden müsste. Dies ist aber auf dem bisherigen Ausweisdokument nicht vorgesehen.
– Für die Integration eines biometrischen Templates in das Ausweisdokument mittels eines Barcodes muss das Template bei der Herstellung des Doku-

mentes bereits vorliegen, da der Barcode ausschließlich während der zentralen Produktion aufgebracht werden kann. Die Barcode-Speicherung im Ausweisdokument ist derzeit allerdings nicht vorgesehen. Nachteilig sind die relativ begrenzte Speicherkapazität (von ca. 500–1.000 Byte) sowie die fehlende Infrastruktur.

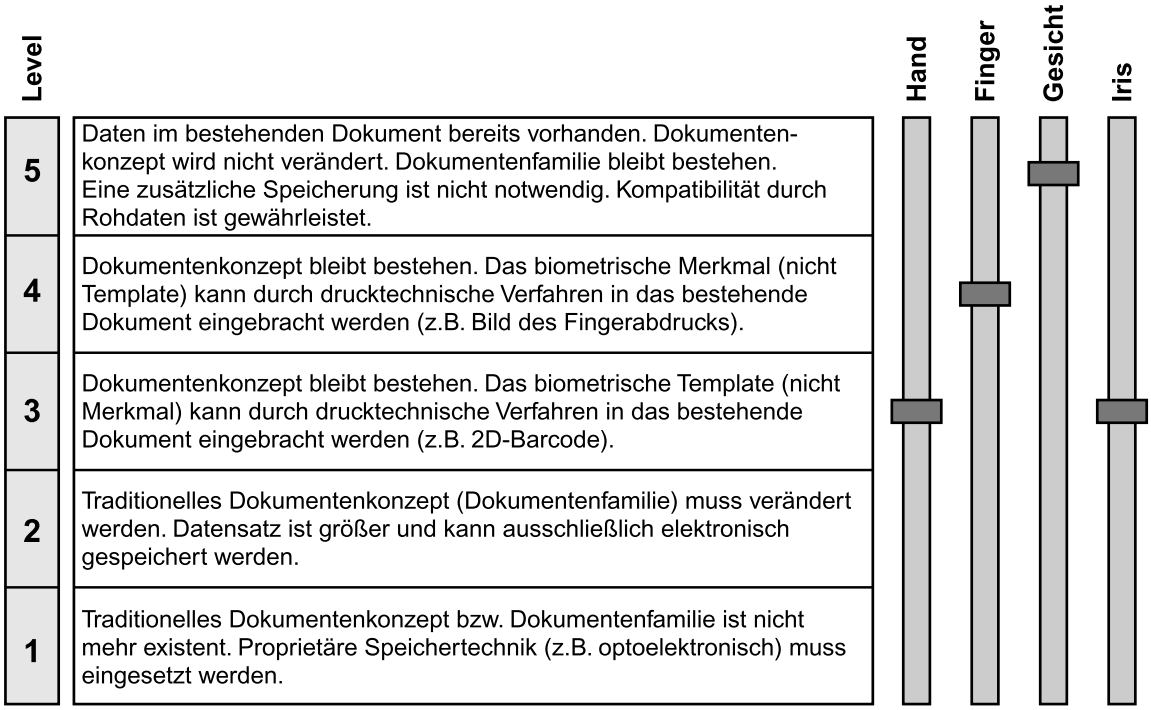
– Das Verfahren der Chipspeicherung[6] ist einmal möglich mit kontaktlosen Chips. Solche „Transponder" sind relativ dünn und könnten in das bisherige Ausweisdokument integriert werden, doch bieten sie bisher nur ein maximales Speichervolumen von 4 KB. Es sind allerdings bereits höhere Speichervolumen im Gespräch bzw. vorgesehen (ICAO, USA) und wohl demnächst auch technisch realisierbar. Eine weitere Möglichkeit sind kontaktbehaftete Chips. Sie erfordern einen Träger und sind nicht in das existierende Ausweisdokument integrierbar. Bei der Integration eines Chips in das Ausweisdokument muss mit einem erheblich höheren Aufwand an Material und Produktionskosten[7] gerechnet werden, u.a. aufgrund der fehlenden Infrastruktur von Lesegeräten. Vorteilhaft hingegen ist, dass die Chips flexibel beschreibbar sind und damit die Möglichkeit gegeben ist, diese erst bei der Dokumentenausgabe zu beschreiben. Verlässliche Aussagen über Manipulationssicherheit und Haltbarkeit können wegen fehlender Großanwendungen und Tests noch nicht gemacht werden.
– Weitere Fragen, wie die nach dem Verhältnis der Lebensdauer der Chips und der Gültigkeitsdauer der Ausweisdokumente, sind noch zu klären (vgl. Kap. V). Weiterhin könnten sich Probleme durch die kurzen Innovationszyklen der Halbleiterindustrie ergeben, da Module, die heute dem Stand der Technik entsprechen, bereits in kurzer Zeit veraltet sind und durch leistungsfähigere Module mit anderen, unter Umständen inkompatiblen Merkmalen ersetzt werden. Dies hieße u.U., dass die eingeführten Module nicht mehr verfügbar sind (Booz Allen Hamilton et al. 2003, S. 95).

---

6 Grundsätzlich ist zwischen kontaktlosen („Transponder") und kontaktbehafteten abfragbaren Chips zu unterscheiden. Transponder sind mit einer Antenne versehen und werden durch ein elektrisches Feld mit der notwendigen Energie versorgt. Nach diesem Prinzip wird die Information in den Transponder eingebracht bzw. ausgelesen.

7 Booz Allen Hamilton et al. (2003, S. 97) schätzen – jeweils abhängig von Verfahren mit dem Ort der Templateerzeugung – den einmaligen Aufwand im Fall kontaktloser Chips für neue Produktionsanlagen sowie die Anpassung der IT-Umgebung auf bis zu 14 Mio. Euro, den einmaligen Aufwand für Produktentwicklung und Testmaterial auf ca. 8 Mio. Euro. Bei kontaktbehafteten Chips wird mit bis zu 50 Mio. Euro bzw. etwa 10 Mio. Euro für die Produktionskosten gerechnet.

Abb. 17: Vergleichende Bewertung der Integrierbarkeit



Quelle: Booz Allen Hamilton et al. 2003, S. 98

Fazit

Unter dem Aspekt des Organisations- und Kostenaufwandes betrachtet (Abb. 17), wäre die günstigste Möglichkeit zur biometrischen Ausrüstung der Ausweisdokumente die Option, mit dem bisherigen Ausweiskonzept und den bestehenden und vertrauten Erhebungs- und Produktionsverfahren Lichtbilder ausreichender Qualität auf dem Ausweisdokument für die automatische Analyse zu nutzen. Entsprechend den ICAO-Vorschriften wäre es zukünftig wohl erforderlich, Lichtbilder hinreichender Qualität in den Meldestellen selbst zu erzeugen.

Im Falle der Speicherung auf dem Dokument müssten für Iris, Hand und Finger zum einen Templates der gesamten Bevölkerung neu generiert werden und zum anderen die bisherige Datensammlung und das Datenablagesystem, das Produktionssystem und die Produktionstechnik reorganisiert und angepasst werden. Die Speicherung in Chipform ist zwar aufgrund der erforderlichen Produktionsumstellung das kostenintensivste Verfahren (Kap. IV.4), es bietet aber das größte Anwendungsspektrum (Booz Allen Hamilton et al. 2003, S. 98).

4. Kosten – ein Exkurs

Für eine Gesamteinschätzung der Leistungsfähigkeit und Eignung biometrischer Systeme sind die kurz- und mittelfristig entstehenden Kosten von großer Bedeutung. Deshalb werden im Folgenden Kostenmodelle für drei Optionen zur Nutzung biometrischer Verfahren von Ausweisdokumenten für Bundesbürger hinsichtlich der damit verbundenen, insbesondere finanziellen Aufwendungen zur Diskussion gestellt.

Die von der Booz Allen Hamilton GmbH, der Bundesdruckerei GmbH und der ZN Vision Technologies AG erarbeiteten Kostenabschätzungen sind aus der Sicht des TAB durchaus plausible Schätzungen und eine erste brauchbare Näherung an das Thema. Da die Frage „Wie viel Geld für welche Sicherheit" bis heute allenfalls am Rande behandelt wurde, sind die folgenden Ausführungen als Grundlage für eine intensivere Diskussion sowie weitere detaillierte Untersuchungen gedacht.

Im Folgenden werden die wesentlichen Ergebnisse des o.g. Gutachtens zu drei Handlungsalternativen[8] stark gekürzt wiedergegeben – die vollständigen Ausführungen sind im Anhang dokumentiert.

Die Optionen

Es wurden drei alternative Optionen zugrunde gelegt.

- *Biometrische Nutzung der bestehenden Dokumente* (Option 1)
  Hierbei werden die auf den Personaldokumenten aufgedruckten Passbilder mit den Gesichtsinformationen der Person für eine biometrische Auswertung herangezogen. Der heutige Beantragungsprozess mit Abgabe eines Passbildes bliebe erhalten. Die notwendigen Anpassungen ergäben sich im Wesentlichen auf der Ausstellungsebene, wo die Qualität der von den Bürgerinnen und Bürgern gelieferten Passbilder normalisiert und standardisiert werden muss.

8 Im Gutachten wird auch die Alternative entwickelt und diskutiert, zunächst einmal abzuwarten. Da diese Option angesichts der in Kapitel II und III beschriebenen Weichenstellungen und Vorentscheidungen nicht mehr realitätstüchtig sein dürfte, wird auf sie an dieser Stelle verzichtet.

- *Technische Aufwertung der bestehenden Dokumente mit biometrischen Daten* (Option 2)
  Die Daten werden in *Speichertechnik* in das Ausweisdokument eingebracht. Als Speicher kommen Barcodes oder digitale Speicherelemente in Frage. Alternativ bieten sich die zentrale Erfassung und Verarbeitung der biometrischen Merkmale (2a) und die dezentrale Erfassung und Verarbeitung der biometrischen Merkmale in den einzelnen Meldestellen an (2b).
- *Das bestehende Dokumentenkonzept wird durch ein vollständig neues Konzept abgelöst* (Option 3)
  Bei dieser Alternative wird das Dokument (z.B. Smartcards) durch ein elektronisches Speicherelement aufgewertet. Hierdurch ergäben sich Kombinationsmöglichkeiten für den Flächeneinsatz der elektronischen Unterschrift sowie u.U. Impulse für den elektronischen Rechts- und Geschäftsverkehr.

Annahmen für alle Optionen

- Für die 6.500 Meldestellen zur Beantragung von Personalausweisen und Reisepässen wird – im Bundesdurchschnitt – von jeweils einem Arbeitsplatz pro 7.500 Einwohner ausgegangen. Es wird nicht zwischen den unterschiedlichen Größen der Ämter unterschieden, sondern es werden grundsätzlich Mittelwerte angenommen.
- Laufende Kosten für die Wartung von Hardware und Software werden pauschal mit 20 % der Anschaffungskosten p.a. angesetzt. Dabei wird nicht zwischen den verschiedenen möglichen Technologien unterschieden. Für Schulungskosten wird ein (mittlerer) Tagessatz von 400 Euro angesetzt.
- Für die Grenzkontrollen an deutschen Flughäfen werden nur die Großflughäfen Frankfurt am Main, München, Düsseldorf, Hamburg, Hannover, Berlin/Tegel und Berlin/Schönefeld betrachtet, über die zusammen 80 % des Fluggastaufkommens im Extra-EU-Verkehr abgewickelt werden. Die Anzahl der Kontrollstationen wird hier mit 200 angesetzt.
- Bei der Ausrüstung von Grenzübergängen an Landgrenzen wird von 18 Übergängen zu Polen und zur Tschechischen Republik mit je drei Erkennungsgeräten ausgegangen. Für Seehäfen mit intensiverem internationalem Personenverkehr wird von 200 Kontrollpunkten an Landgrenzen und Seehäfen ausgegangen.
- Für die unter Alternativen „2b“ und „3“ diskutierten Handlungsalternativen, die eine Erfassung der biometrischen Daten in den Meldestellen beinhalten, wird für die fortlaufende Administration und für die Betreuung der Hard- und

Software der Endgeräte im Durchschnitt ein zusätzlicher Personalaufwand von ca. 0,5 FTE („Full Time Equivalent“) pro Meldestelle angenommen.

- Unter der Annahme, dass die gängige Praxis der dezentralen Aufbewahrung der Ausweisdaten beibehalten wird, müssen zukünftig auch die jeweiligen biometrischen Referenzdaten in den Meldestellen abgelegt werden. Die für die Referenzdatenspeicherung notwendige IT-Infrastruktur existiert aber i.d.R. noch nicht. Demnach wird angenommen, dass die bestehenden Melderegister erweitert werden müssen.
- In allen diskutierten Handlungsalternativen wird davon ausgegangen, dass kein zentrales IT-System und insbesondere keine zentrale Datenbank für biometrische Daten angelegt werden.
- Für alle Handlungsalternativen wird davon ausgegangen, dass zunächst Pilotprojekte durchgeführt werden.

Die folgenden Kostenabschätzungen beinhalten jeweils *nur die Mehrkosten im Vergleich zu den heutigen Ausweissystemen*. Dabei wird zwischen einmaligen und laufenden Kosten – jeweils auf vier Ebenen – unterschieden (Tab. 10).

Die Kostenmodelle sind vor dem Hintergrund zahlreicher Unsicherheiten zu betrachten. Unter anderem lassen sich aktuelle Endgerätekosten nur bedingt auf eine mögliche Anwendung bei Ausweissystemen übertragen. Die Zahl der notwendigen Meldestellen und die konkreten Anforderungen an die Systeme sind noch nicht festgelegt. Die Auswirkungen der technologischen Weiterentwicklung auf Stückkosten und Größenordnungen von Skaleneffekten sind unklar.

Die wesentlichen Kostenkomponenten der Alternativen basieren auf Mittelwerten, die sich aus Bandbreitenabschätzungen für die einzelnen Kosten ergeben. Verglichen mit den genannten Unsicherheiten, die für die jeweiligen Kostenkomponenten Unterschiede von mehr als 50 % bedeuten können, sind die Unterschiede in den Kosten für den Einsatz der verschiedenen biometrischen Verfahren in erster Näherung zu vernachlässigen (GAO 2002).

Tab. 10: Übersicht Kostenkomponenten

Bereich	*einmalige Kosten*	*laufende Kosten*
Ausstellungsebene	• Einrichtung Erfassungssystem (HW/SW) • Schulung • Einrichtung Qualitätssicherungssystem (HW/SW) • Erweiterung Melderegister • Erweiterung Datentransfer • Marketing, Kommunikation • dezentrales Projektmanagement	• Personalkosten Erfassung (zusätzlicher Personalbedarf) • Wartung Erfassungssysteme (HW/SW) • Systempflege Qualitätssicherung • erweiterte Systempflege Melderegister
Produktionsebene	• Modifikation Produktionstechnik Ausweise • Produktentwicklung • Testmaterial • Projektmanagement	• laufende Dokumentenproduktion (Personalausweise, Reisepässe, Visa) • ggf. Speichertechnologie
Kontrollebene	• Einrichtung Personalkontrollsysteme an Grenzkontrollpunkten (HW/SW) • Schulung • dezentrales Projektmanagement	• Wartung Kontrollsysteme • Personalkosten Personenkontrolle • fortlaufende Schulung
zentrale Koordinierung	• Programm-Management • Auftragsvergabe und Lieferantenmanagement • Vorbereitung/Durchführung Pilotprojekt(e) • QS-Management • Projektsteuerung	• fortlaufendes Programm-Management

Kostenschätzungen im Einzelnen

In *Option 1* wird das in Form des Passfotos bereits vorhandene biometrische Merkmal „Gesicht“ vom Ausweis gelesen und gegen das Live-Bild der Person abgeglichen. Es sind auch Überprüfungen gegen Datenbankbilder (z.B. bildbasierte Fahndungslisten oder Visaantragsteller-Datenbank) machbar, zum heuti-

gen Zeitpunkt jedoch rechtlich ausgeschlossen. Als biometrische Verfahren in dieser Handlungsalternative kommt nur die Gesichtserkennung in Betracht.

Der Zielerreichungsbeitrag bestünde vor allem in einer qualitativ verbesserten Personenkontrolle bei Grenzübergängen, da die bislang rein manuelle Verifikation der Identität nachhaltig unterstützt wird. Offen ist, ob mit nennenswerten Einsparungen beim Personal an den Grenzkontrollen gerechnet werden kann.

Anders als bei den weiteren Optionen ist keine Veränderung des Ausweises erforderlich, aber die Implementierung von Endgeräten und entsprechenden Betriebskonzepten, die u.a. eine Optimierung der Lichtbildqualität und eine Überarbeitung ausgewählter Prozesse beinhaltet.

Die rechtlichen Rahmenbedingungen für diese Handlungsalternative sind heute bereits gegeben. Sowohl national als auch international ist das Gesicht in Form des Passfotos festgelegter Standard für Ausweisdokumente. Die Einführung der Technologie kann stufenweise erfolgen, da die manuelle Verifikation der Identität auf Basis der Passfotos weiterhin möglich ist. Die wesentlichen Kostenkomponenten dieser Option sind in Tabelle 11 aufgeführt.

Tab. 11: Option 1: Biometrische Nutzung bestehender Dokumente – Kostenübersicht

	einmalige Kosten (gesamt) in Mio. Euro	*laufende Kosten (gesamt) in Mio. Euro*
Ausstellung	5,2	0,6
Produktion	0,0	0,0
Kontrolle	9,8	3,9
Koordinierung	6,2	0,0
Kosten insgesamt	*21,2*	*4,5*

Für die einmalige Einrichtung des Systems resultieren die Kosten von etwa 21,2 Mio. Euro im Wesentlichen aus den Hardware- und Software-Kosten für Endgeräte an den Grenzübergängen und der Schulung des Personals. Die Kosten für Geräte im Außeneinsatz, die z.B. gegen Witterung und Diebstahl geschützt werden müssen, werden inklusive einmaliger Installation und eventueller Baumaßnahmen mit 20.000 Euro pro Kontrollpunkt abgeschätzt, innerhalb von Gebäuden werden jeweils 15.000 Euro pro Kontrollpunkt angesetzt. Für die Durchführung von Pilotversuchen für die biometrischen Systeme werden in

einem ersten Schritt pro Anbieter 100.000 Euro und für einen detaillierteren zweiten Schritt 300.000 Euro angenommen.

Die laufenden Kosten für die Nutzung der heutigen Ausweise mithilfe automatischer Gesichtserkennung ergeben sich vor allem aus der fortlaufenden Schulung des Personals an den Landesgrenzen.

Option 2 bedeutet technisch gesehen die Einbindung von zusätzlichen biometrischen Daten in Personalausweise und Reisepässe, wobei die wesentlichen äußeren Merkmale und die Erscheinungsform der Dokumente gleich bleiben. Die bisherigen Herstellungsprozesse für die Dokumente müssen zwar geändert, aber nicht grundlegend neu konzipiert werden. Mit dieser Option kann ein Beitrag zur Erreichung des Zieles erbracht werden, die Qualität der Personenkontrollen – insbesondere bei Grenzübertritten – durch die automatische Überprüfung biometrischer Merkmale zu steigern. Die Ausrüstung der bestehenden Ausweisgeneration mit zusätzlichen biometrischen Daten könnte über optisch lesbare Speichermedien wie 2D-Barcodes oder Hologramme erfolgen. Für den Personalausweis in seiner heutigen Form ist darüber hinaus die Einführung von (dünnen) kontaktlosen Chips (Transponder), die von Leseterminals gelesen werden können, technisch machbar.

Prinzipiell sind alle vier der hier näher betrachteten biometrischen Verfahren mit dieser Option realisierbar. Die rechtlichen Grundlagen sind noch zu schaffen.

Die Tabellen 12 und 13 fassen die wesentlichen Kostenkomponenten zusammen. Dabei wird in der Variante 2b davon ausgegangen, dass die Erfassung und Verarbeitung der biometrischen Merkmale („Templategenerierung“) der Bürger in den Meldestellen erfolgt. Prinzipiell sind für die Verfahren Fingerabdruck- und Gesichtserkennung auch eine Beibehaltung des bisherigen Beantragungsprozesses und die Verlagerung der Templategenerierung an eine zentrale Stelle, z.B. die Produktionsstätte, möglich. Dabei würden die dezentral aufgenommenen Bilder der Fingerabdrücke oder der Gesichter als „Rohdaten“ konventionell oder elektronisch zu einer zentralen Stelle übertragen, die die Erzeugung der Templates übernimmt (Variante 2a).

Die einmaligen und laufenden *Kosten* für das Erfassungssystem, die Qualitätssicherung und die Erweiterung der Melderegister *hängen* in hohem Maße *davon ab*, ob die biometrischen Templates *dezentral in den Meldestellen* oder an *zentraler Stelle* erzeugt werden. Bei einer dezentralen Erfassung in der Ausstellungsebene ist von zusätzlichen Kosten für Hardware und Software von ca. 400 Mio. Euro – im Vergleich zur zentralen Variante – auszugehen. Hauptsächlich diese Kosten für die Ausstellungsebene führen zu einmaligen Kosten von ca. 614 Mio. Euro – im Vergleich zu ca. 179 Mio. Euro bei zentraler Produktion.

Tab. 12: Option 2a: Aufwertung bestehender Ausweisdokumente mit biometrischen Daten in Speichertechnik (zentral) – Kostenübersicht

	einmalige Kosten (gesamt) in Mio. Euro	*laufende Kosten (gesamt) in Mio. Euro*
Ausstellung	95,4	0,6
Produktion	25,0	48,3
Kontrolle	33,4	6,2
Koordinierung	24,8	0,0
Kosten insgesamt	*178,6*	*55,1*

Tab. 13: Option 2b: Aufwertung bestehender Ausweisdokumente mit biometrischen Daten in Speichertechnik (dezentral) – Kostenübersicht

	einmalige Kosten (gesamt) in Mio. Euro	*laufende Kosten (gesamt) in Mio. Euro*
Ausstellung	530,5	277
Produktion	25,0	48,3
Kontrolle	33,4	6,2
Koordinierung	24,8	0,0
Kosten insgesamt	*613,7*	*331,5*

Bei den laufenden Kosten spielen die Betriebs- und Wartungskosten für die Hardware und Software in den Meldestellen und für das Qualitätssicherungssystem die größte Rolle. Insgesamt ergeben sich Kosten von ca. 331 Mio. Euro für Option 2b. Für die zusätzlichen Kosten in der Produktion der Ausweise, die sich aus der Einbindung zusätzlicher biometrischer Daten und eines elektronischen kontaktlosen Transponders ergeben, wird von zwei bis drei Euro pro Dokument ausgegangen. Die Veränderung der Produktionsprozesse zur Ausrüstung der Ausweisdokumente ist relativ kurzfristig innerhalb von zwei bis drei Jahren zu realisieren.

Option 3 „Einführung einer neuen Ausweisgeneration“: Mit dieser Handlungsalternative soll die Entwicklung und Einführung einer neuen Ausweisge-

neration, d.h. eines Chip-basierten digitalen Dokumentes (z.B. in Kreditkartenformat) – zumindest in Ansätzen zur Diskussion gestellt werden.

Im Fokus dieser Option steht neben einer möglichen Erhöhung der öffentlichen Sicherheit durch verbesserte, teilautomatisierte Verifikationsverfahren via Biometrie auch das *Ziel, Anstöße zu technischen Innovationen* in Deutschland zu geben.

Die Kosten für eine mögliche Einführung können zum jetzigen Zeitpunkt nur grob abgeschätzt werden, da sie in erheblichem Umfang von den genauen technischen und organisatorischen Anforderungen an das Gesamtsystem abhängen.

Die Kostenabschätzung in Tabelle 14 zeigt, dass sich die einmaligen Kosten für die Einführung einer neuen Ausweisgeneration von ca. 669 Mio. Euro zu wesentlichen Teilen aus der Hardware und Software für die Erfassungs- und Qualitätssicherungssysteme sowie für das Melderegister ergeben. Um den Nutzen der „neuen Karte“ für den Bürger transparent zu machen und entsprechende Aufmerksamkeit zu erzeugen, ist von einem erheblichen Aufwand für Marketing und Kommunikation auszugehen.

Tab. 14: Option 3: Neues Dokumentenkonzept mit Speicherelementen – Kostenübersicht

	einmalige Kosten (gesamt) in Mio. Euro	*laufende Kosten (gesamt) in Mio. Euro*
Ausstellung	530,5	277
Produktion	80,0	331,8
Kontrolle	33,4	1,4
Koordinierung	24,8	0,0
Kosten insgesamt	*668,7*	*610,2*

In der Produktion müssen neue Verfahren implementiert und entsprechende einmalige Investitionen getätigt werden. Hier ist – in einer ersten Schätzung – von einer finanziellen Größenordnung von etwa bis zu 80 Mio. Euro auszugehen. Für eine mögliche Implementierung wird der Finanzbedarf für die Pilotphase mit 6,4 Mio. Euro abgeschätzt. Die laufenden Kosten summieren sich zu einem zusätzlichen Finanzbedarf gegenüber dem heute bestehenden System von ca. 610 Mio. Euro p.a.

Fazit

Der durchgeführte Kostenvergleich zeigt, dass ein *entscheidender Kostenfaktor die Hardware-Ausstattung der Meldestellen* ist. Anders formuliert, sind in Optionen, bei denen dezentrale Merkmalsneuerfassung und Templategenerierung erforderlich sind (Option 2b und 3), die Kosten um ein Mehrfaches höher, als bei den Alternativen, wo die (laufenden) Mehrkosten auf der Ebene der Produktion der Ausweise anfallen (Option 2a). Im Vergleich zur dezentralen Option ist die Alternative „Neues Ausweisdokument" nicht unverhältnismäßig viel kostenintensiver (ist allerdings diesbezüglich erheblich unsicherer abzuschätzen).

Wie schon bei der Diskussion des Kriteriums der technischen Eignung kann auch das Kostenkriterium per se keine ausreichende Grundlage für eine Entscheidung liefern. Vielmehr müssten weitere Aspekte im Sinne einer Kosten-Nutzen-Analyse mit einbezogen werden. Eine erste – unvollständige – Abwägung führt zu folgenden Überlegungen:

Unterstellt man, dass bei allen Alternativen der Sicherheitsgewinn in etwa gleich einzuschätzen ist, sprechen für einen Einstieg in *Option 1* die geringen Kosten, die Beibehaltung bestehender Prozesse sowie eine vermutlich größere Akzeptanz bei der Bevölkerung. Dazu käme, dass diese Option einen Übergang zu anderen Optionen grundsätzlich offen ließe. Dagegen spricht ein gewisser Konservativismus des Ansatzes, der zunächst keinerlei innovationsfördernde Impulse gibt oder weitere Zusatznutzen erschließt – diesen aber auch nicht verbaut.

Option 2 bringt grundsätzlich einen höheren Kostenaufwand mit sich und wirft die Frage auf, wie sich die Akzeptanz eines flächendeckenden Enrollments von Bundesbürgern gestaltet. Andererseits wäre durch die Beibehaltung der Dokumentenfamilie eine gewisse Kontinuität gewahrt, und es wäre ein höheres technologisches Niveau erreichbar.

Option 3 verknüpft die Dimension der Sicherheit mit einer innovationspolitischen Perspektive. Zwar fallen hier die meisten Kosten an, es würde aber vermutlich mit der Einführung einer modernen Karte ein innovativer Weg beschritten, der auch wirtschaftliche Impulse vermittelt. So würde für Bundesbürger (mittelfristig auch für hier lebende ausländische Bürger) ein Dokument bereitgestellt, das diesen nicht nur die konventionelle Authentifikation erlaubt, sondern auch als Eckpfeiler einer elektronischen Unterschrift für den elektronischen Geschäftsverkehr einsetzbar wäre.

TAB

V. Überlegungen zur rechtlichen Ausgestaltung eines zukünftigen Einsatzes von biometrischen Systemen

Mit dem Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz, TBG) vom 09. Januar 2002 wurden insgesamt Vorschriften in 21 Gesetzen und Rechtsverordnungen geändert bzw. neu geschaffen. Nach der Begründung zum Gesetzentwurf der Bundesregierung war Ziel des Gesetzes die Schaffung der notwendigen gesetzlichen Voraussetzungen für eine Verbesserung des behördlichen Informationsaustausches, für die Verhinderung der Einreise terroristischer Straftäter nach Deutschland und die notwendigen identitätssichernden Maßnahmen (Bundesrat 2001, S. 82).

Ein wichtiges Element des Gesetzes ist die Regelung der Aufnahme biometrischer Merkmale in Pässe und Personalausweise sowie in Ausweisdokumente für Ausländer. Durch die Regelungen, die die Aufnahme biometrischer Merkmale in *Identifikationspapiere von Bundesbürgern* vorsehen, sollen im Pass- und Personalausweisrecht die Möglichkeiten zur „computergestützten Identifizierung von Personen“ auf der Grundlage der Ausweisdokumente verbessert werden, u.a. um zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen. Dazu ist vorgesehen, dass neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale in Pass und Personalausweis – auch in verschlüsselter Form – aufgenommen werden dürfen. Gleichzeitig wird durch neue Vorschriften im AuslG und AsylVfG die Aufnahme biometrischer Merkmale auch in die *Identifikationspapiere von Ausländern und Asylbewerbern* ermöglicht.

Die Arten der biometrischen Merkmale, ihre Einzelheiten, die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung sollen durch ein noch zu erlassendes Ausführungsgesetz hinsichtlich Pass und Personalausweis bzw. eine Rechtsverordnung bezüglich der ausländerrechtlichen Regelungen gesondert geregelt werden.

Ziel der Ausführungen in diesem Kapitel ist es, die *Vorgaben und Weichenstellungen des TBG darzustellen und zu diskutieren* sowie *Anforderungen an* eine *zukünftige Ausgestaltung der Rechtsgrundlagen* für die dort genannten Ausweisdokumente für Bundesbürger und Ausländer[9] *zu benennen*.

---

9 Insofern sind Visa für Angehörige von Drittstaaten nur indirekt einbezogen (s. hierzu Kap. II.1).

Die nachfolgenden Ausführungen basieren im Wesentlichen auf einem Gutachten des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD-SH), das im Zusammenhang mit der Erstellung dieses Sachstandsberichtes in Auftrag gegeben wurde.

1. Biometrie in Ausweisdokumenten für Bundesbürger

Im Folgenden werden die vom Gesetzgeber vorgesehenen Regelungen für die Aufnahme biometrischer Merkmale dargestellt (Kap. V.1.2) sowie die darin enthaltenen inhaltlichen Vorgaben hinsichtlich ihrer Geeignetheit, Erforderlichkeit und Angemessenheit im Blick auf Anforderungen an die Ausgestaltung einer zukünftigen gesetzlichen Grundlage kritisch diskutiert (Kap. V.1.2).

1.1 Regelungen und Ziele

Artikel 7 Terrorismusbekämpfungsgesetz (Änderung des Passgesetzes)

Durch Art. 7 des Terrorismusbekämpfungsgesetzes wurden u.a. § 4 PassG zwei neue Absätze hinzugefügt. § 4 Abs. 3 PassG lautet nunmehr: „Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. Auch die in Abs. 1 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden.“[10]

Der ebenfalls neu gefasste § 4 Abs. 4 PassG lautet: „Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen sowie Angaben in verschlüsselter Form nach Abs. 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.“

10 Bei den Angaben in Abs. 1 Satz 2 handelt es sich um Familienname und ggf. Geburtsname (Nr. 1), Vornamen (Nr. 2), Doktorgrad (Nr. 3), Ordensname/Künstlername (Nr. 4), Tag und Ort der Geburt (Nr. 5), Geschlecht (Nr. 6), Größe (Nr. 7), Farbe der Augen (Nr. 8), Wohnort (Nr. 9), Staatsangehörigkeit (Nr. 10).

Nach der Begründung zum Gesetzentwurf soll auf dieser Basis zukünftig zweifelsfrei *überprüft* werden können, *ob die Identität der betreffenden Person mit den im Dokument abgespeicherten Originaldaten übereinstimmt* (Bundesrat 2001, S. 84). Es wird weiter ausgeführt, die Zuverlässigkeit der Identifizierung einer Person allein durch den visuellen Abgleich zwischen Lichtbild und Person sei von der subjektiven Wahrnehmungsfähigkeit abhängig und werde auch durch zahlreiche andere Faktoren, wie z.B. die Qualität des Lichtbildes, den natürlichen Alterungsprozess oder die Veränderung von Haar- und Barttracht beeinträchtigt. Die Aufnahme weiterer biometrischer Merkmale sei daher Voraussetzung für eine Verbesserung der Identifizierungsmöglichkeiten einer Person anhand des vorgelegten Ausweisdokumentes (Bundesrat 2001, S. 110).

Um datenschutzrechtlichen Belangen gerecht zu werden, hat der Gesetzgeber eine weitere Vorschrift in § 16 Abs. 6 PassG aufgenommen, die regelt, dass die im Pass enthaltenen verschlüsselten Angaben nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen und verwendet werden dürfen.

Artikel 8 Terrorismusbekämpfungsgesetz (Änderung des Gesetzes über Personalausweise)

Inhaltlich entsprechen die in § 1 Abs. 4 und 5 PAuswG neu aufgenommenen Regelungen § 4 Abs. 3 und 4 PassG. In der Gesetzesbegründung wird hierzu ausgeführt, der beabsichtigte umfassende Schutz vor Identitätsmanipulationen mit Reisedokumenten werde nur erreicht, wenn nicht nur der Pass, sondern auch der Personalausweis, der von vielen europäischen Staaten als Reisedokument anerkannt werde, die gleiche Absicherung habe wie der Pass (Bundesrat 2001, S. 112). Der Inhalt der Gesetzesbegründung entspricht dem der Begründung zu den geänderten Vorschriften im PassG.

Eine dem oben erwähnten § 16 Abs. 6 gleich lautende Regelung über die Verwendungszwecke verschlüsselter Merkmale und der Auskunftsrechte der Betroffenen enthält § 3 Abs. 5 PAuswG.

1.2 Vorgaben für die Umsetzung der mit dem Terrorismusbekämpfungsgesetz geschaffenen Regelungen

1.2.1 Ausgestaltung durch ein zukünftiges Bundesgesetz

Die Ermächtigungsgrundlagen im PassG und PAuswG erlauben zwar die Aufnahme bestimmter biometrischer Merkmale, überlassen die nähere Ausgestaltung jedoch einem Bundesgesetz.

Mit dieser Festlegung auf das Erfordernis einer gesetzlichen Grundlage wird dem Umstand Rechnung getragen, dass Eingriffe in das Grundrecht auf informationelle Selbstbestimmung nach der Rechtsprechung des Bundesverfassungsgerichts einer (verfassungsgemäßen) gesetzlichen Grundlage bedürfen, „aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“ (zit. n. ULD-SH 2003, S. 47). Weiterhin entspricht dies der Verpflichtung des Gesetzgebers, in grundlegenden normativen Bereichen alle wesentlichen Entscheidungen selbst zu treffen, soweit diese einer staatlichen Regelung zugänglich sind.

Da im *TBG* bestimmte Voraussetzungen geschaffen und Vorentscheidungen getroffen wurden, soll die Frage aufgeworfen werden, ob diese Vorgaben *für den Gesetz- und Verordnungsgeber der Ausführungsbestimmungen bindend* sind, was z.B. hinsichtlich der Aufzählung der für die biometrischen Merkmale in Betracht kommenden Körperbereiche in den erlassenen Vorschriften von besonderer Relevanz ist. Grundsätzlich gilt hinsichtlich des Verhältnisses von Gesetzen die sog. Lex-posterior-Regelung, d.h. aufgrund der Gleichrangigkeit formeller Gesetze geht das später erlassene Gesetz dem älteren Gesetz vor. Das für den Bereich des Pass- und Personalausweiswesens erforderliche Ausführungsgesetz als Parlamentsgesetz könnte somit auch über den bisherigen Regelungsinhalt der Vorschriften des Pass- und PAuswG hinausgehen. Diese Möglichkeiten sind aber nicht Gegenstand der folgenden Darstellung. Vielmehr werden die mit dem TBG geschaffenen Vorschriften anhand der gegenwärtigen Vorgaben des Gesetzgebers beurteilt und der im Lichte dieser Vorgaben zu erkennende Handlungsbedarf angesprochen.

1.2.2 Nennung biometrischer Merkmale bestimmter Körperbereiche

§ 4 Abs. 3 Satz 1 PassG bzw. § 1 Abs. 4 Satz 1 PAuswG geben die Körperbereiche vor, auf die sich die biometrischen Merkmale beziehen können. So sollen „biometrische Merkmale von Fingern oder Händen oder Gesicht“ zulässig sein. Der Gesetzgeber hat nicht geregelt, um welche Merkmale es sich im Einzelnen handeln soll.[11] Vielmehr sind die Arten der biometrischen Merkmale und ihre Einzelheiten nach § 4 Abs. 4 Satz 1 PassG und § 1 Abs. 5 Satz 1 PAuswG durch ein weiteres Bundesgesetz zu regeln.

Ausschluss bestimmter Merkmale?

Die *Nennung* von Fingern, Händen und Gesicht *ist abschließend*. Biometrische Verfahren, die sich auf andere Körpermerkmale beziehen, scheiden demnach aus. Die in Betracht kommenden Körperbereiche werden ferner präzise aufgeführt. Angesichts dessen liegt der Schluss nahe, dass z.B. die Iriserkennung oder die Erkennung anhand des Retinamusters vom Körperbereich „Gesicht“ wohl nicht umfasst werden. Vielmehr ist es plausibel anzunehmen, dass der Gesetzgeber nicht lediglich die Bezeichnung „Gesicht“ in das Gesetz aufgenommen hätte, wenn er auch Iris oder Retina als biometrischen Merkmale hätte zulassen wollen (ULD-SH 2003, S. 50).

Ausschluss einer Kombinationslösung?

Es stellt sich auch die Frage, ob die Auswahl des Gesetzgebers die genannten Merkmale alternativ oder kumulativ zulässt. Aus dem Wortlaut des Gesetzes ergibt sich eine Antwort nicht zwingend. Allerdings lässt sich der Gesetzesbegründung entnehmen, dass *die drei genannten Körperbereiche* nach dem Willen des Gesetzgebers *alternativ zu verstehen* sind (Bundesrat 2001, S. 110). Teilt man diese Lesart, wäre eine kombinierte Anwendung verschiedener biometrischer Systeme nicht zugelassen. Dies wirft die Frage auf, ob die gesetzgeberische Beschränkung auf einzelne biometrische Merkmale überhaupt geeignet ist, den mit der Regelung erstrebten Zweck zu erreichen. Das Gebot der Geeignetheit verlangt gemäß der bundesverfassungsgerichtlichen Rechtsprechung den Einsatz solcher Mittel, mit denen der gewünschte Erfolg am ehesten gefördert werden kann.

---

11 Nolte (2002, S. 576) charakterisiert dieses Vorgehen als „gesetzgebungstechnisch merkwürdig“.

In diesem Zusammenhang ist auf den aktuellen Kenntnisstand zu den Fehlerraten fortgeschrittener Systeme hinzuweisen (s. Kap. IV.2). Die beispielsweise durch das NIST dokumentierten Testergebnisse weisen für die Gesichtserkennung eine Erkennungsrate von 90 % auf, die FAR lag bei 1 %. Auch bei den eingesetzten Fingerabdruck-Scannern lag bei einer gleichen FAR eine Erkennungsquote von über 90 % vor. In der Praxis hieße dies – wie eine Hochrechnung des Wertes von 1 % auf die Gesamtzahl der Visa zeigt – dass trotz biometrischer Kontrolle jährlich rund 150.000 Personen über diese Methode nicht korrekt identifiziert würden. Der Direktor des NIST wies darauf hin, dass selbst eine Kombination aus Gesichtserkennung und Fingerabdruckerkennung – wie sie das NIST (2002a) empfiehlt – nicht zu einer völlig sicheren Kontrolle führen könne (abrufbar unter: http://www.nist.gov/public_affairs/releases/n03-01.htm).

Nach dem aktuellen Informationsstand ist ein Verzicht auf eine Kombination mehrerer Merkmale unter dem Gesichtspunkt der Zuverlässigkeit biometrischer Systeme zumindest problematisch. Eine gesetzgeberische Entscheidung, biometrische Merkmale der genannten Körperbereiche lediglich alternativ zuzulassen, dürfte das Problem der Erkennungssicherheit nur suboptimal lösen.[12] Da selbst eine Kombination zweier Verfahren zu nicht zu vernachlässigenden Raten falscher Identifikation führt, ist es *zweifelhaft*, ob bei einer Beschränkung auf ein einziges biometrisches Merkmal bzw. System *eine akzeptable Falschzurückweisungs- bzw. Falscherkennungsrate erreicht werden kann* (ULD-SH 2003, S. 51).

Folgen der Auswahl bestimmter Merkmale für die Gültigkeitsdauer von Pass und Personalausweis

Bei Erlass des Bundesgesetzes sollte ein besonderes Augenmerk auf die mit der Auswahl bestimmter biometrischer Merkmale verbundenen Folgen gerichtet werden. So stellt sich bei der Aufnahme biometrischer Merkmale z.B. ein Problem im Hinblick auf die Gültigkeitsdauer von Pässen und Ausweisen, die gemäß § 5 Abs. 1 PassG zehn Jahre beträgt. Bei Personen, die das 26. Lebensjahr noch nicht vollendet haben, ist die Gültigkeitsdauer fünf Jahre. Gleiches gilt für Personalausweisinhaber, die das 26. Lebensjahr noch nicht vollendet haben (§ 2 Abs. 1 Satz 2 PAuswG). Die kürzere Gültigkeitsdauer trägt dem Umstand Rechnung, dass die körperliche Entwicklung dieser Personen in diesem Alter noch nicht abgeschlossen ist, so dass das Bild im Reisepass bereits nach wenigen

12 Multimodale Verfahren brächten andererseits Datenschutzprobleme mit sich, was bislang noch nicht hinreichend diskutiert worden ist.

Jahren eine zuverlässige Identifizierung des Passinhabers nicht mehr gewährleistet. Bei der Aufnahme biometrischer Merkmale ergibt sich ein ähnliches Problem, das sich jedoch nicht auf eine bestimmte Altersgruppe beschränken lässt. Vielmehr können biometrische Merkmale Änderungen unterworfen sein, die u.U. dazu führen, dass eine Verifikation aufgrund dieses Merkmals lediglich in einem begrenzten Zeitraum möglich ist (s. Kap. IV.1 u. IV.2).

Bei der Auswahl eines biometrischen Merkmals ist deshalb darauf zu achten, dass eine Verifikation über den gesamten Gültigkeitszeitraum des entsprechenden Dokumentes sichergestellt werden kann (ULD-SH 2003, S. 52).

Eindringtiefe, Missbrauchsmöglichkeiten, Zumutbarkeit

Bei Eingriffen in das Recht auf informationelle Selbstbestimmung liegt u.a. eine größere Eingriffstiefe vor, wenn durch die Art der verarbeiteten Daten eine Zweckänderung erleichtert wird oder eine vergleichsweise größere Missbrauchsgefahr besteht. Dies führt zur Frage, ob der Gesetzgeber mit der Begrenzung auf die genannten Körperbereiche aus datenschutzrechtlicher Sicht vorzuziehende Merkmale ausgeschlossen hat.

Allgemein lässt sich sagen, dass ein biometrisches Merkmal aus datenschutzrechtlicher Sicht vor allem dann geeignet ist, wenn es dem Gebot der Direkterhebung entspricht sowie möglichst wenig überschießende Informationen preisgibt.

- Der im Datenschutzrecht geltende Grundsatz der sog. *Direkterhebung* verlangt, dass personenbezogene Daten grundsätzlich bei der betroffenen Person selbst zu erheben sind und zwar mit ihrer Kenntnis und gegebenenfalls Mitwirkung (§ 4 Abs. 2 Satz 1 BDSG). Die Erfordernisse der Kenntnis und Mitwirkung des Betroffenen ergeben sich unmittelbar aus dem Recht auf informationelle Selbstbestimmung. Danach soll der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen (ULD-SH 2003, S. 64). An dieser Mitwirkung fehlt es dann, wenn Daten heimlich bei der betroffenen Person erhoben werden. Biometrische Verfahren, die für den Masseneinsatz geeignet sein sollen, müssen so gewählt und eingesetzt werden, dass die Daten gerade nicht unbemerkt erfasst werden (können), sondern vielmehr der Betroffene Kenntnis von der Anwendung hat. Es sind dementsprechend aus datenschutzrechtlicher Sicht biometrische Verfahren vorzuziehen, die eine aktive Mitwirkung des Betroffenen erfordern und deshalb eine verdeckte Erfassung biometrischer

Merkmale nicht oder allenfalls unter erschwerten Bedingungen zulassen. Hierfür kommen Verfahren in Betracht, die einen Körperkontakt oder eine bestimmte „Aufnahmeposition“ erfordern, wie z.B. Fingerabdruck-Verfahren, Handgeometrie-, Handvenenmuster-, Iris- und Retinaerkennung oder verhaltensbasierte Merkmale wie die Unterschriftsdynamik (ULD-SH 2001, S. 10). Die Gesichtserkennung ist bei dieser grundsätzlichen Betrachtungsweise zwar weniger „datenschutzfreundlich“. Gleichwohl könnten bei einer Verwendung im Zusammenhang mit Ausweisdokumenten die konkreten Bedingungen ihres Einsatzes beim Enrollment bzw. bei der Erfassung vor Ort zum Zwecke der Verifikation als kooperatives Verfahren gestaltet werden. Dadurch wäre das theoretische Missbrauchspotenzial in der Praxis weitgehend reduziert.

Die gesetzlich vorgesehenen Merkmale Finger und Hände zeichnen sich dadurch aus, dass sie vom Besitzer unwillentlich hinterlassen werden, die Merkmale des Gesichtes können gegen dessen Willen erhoben werden (und missbräuchlich genutzt werden können). Dies ist bei anderen biometrischen Merkmalen, wie z.B. der Retina oder der Iris, nicht der Fall. Gerade diese Merkmale hat der Gesetzgeber nicht explizit einbezogen.

Bei einer grundsätzlichen Betrachtungsweise sprechen also datenschutzrechtliche Kriterien und Ziele in gewissem Umfang gegen die gewählten Merkmale (und die Iris wäre in dieser Hinsicht vorzuziehen). Gleichwohl müssten aber in einer Gesamtabwägung weitere Aspekte, wie technische Funktionalität und Leistungsfähigkeit sowie weitere Schutzziele, wie Erhöhung des Sicherheitsniveaus, Schutz von Leben und Gesundheit oder Vermeidung von Missbrauch mit einbezogen werden. Diese erweiterte Abwägung könnte u.U. auch gegen datenschutzfreundliche Merkmale sprechen bzw. andere Merkmale dennoch als geeignet erscheinen lassen.

- Weiter ist unter dem Gesichtspunkt der *Verhältnismäßigkeit* zu beachten, dass biometrische Rohdaten bestimmte besonders schützenswerte Informationen über den Merkmalsträger aufzeigen können. Neben Rückschlüssen auf Geschlecht, Alter und ethnische Herkunft, die anhand des Gesichtes und der Sprache zu ziehen sind, lassen Aufnahmen des Augenhintergrundes u.U. Hinweise auf Krankheiten wie Arteriosklerose, Diabetes und Bluthochdruck zu. Bei der Verwendung von Fingerabdrücken scheint es statistische Korrelationen von Fingerabdruckmustern und Krankheiten, wie chronische Magen-Darm-Beschwerden, Leukämie und Brustkrebs zu geben (Probst 2002, S. 118 f.). Da nicht auszuschließen ist, dass mit derartigen, wissenschaftlich nicht unbedingt gesicherten Erkenntnissen Diskriminierungen

verbunden sein können, ist aus datenschutzrechtlicher Sicht sicherzustellen, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben (Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2002). Die Erfassung biometrischer Merkmale, die solche überschießenden Informationen über den Betroffenen preisgeben, würde ansonsten den Einzelnen in unverhältnismäßiger Weise in seinem Grundrecht auf informationelle Selbstbestimmung beeinträchtigen.

Es bedarf daher einer Abwägung zwischen dem berechtigten staatlichen Interesse an einer zweifelsfreien Identifizierung bzw. Verifizierung anhand biometrischer Merkmale und dem schutzwürdigen Interesse des Betroffenen an größtmöglicher Gewährleistung seines Grundrechts auf informationelle Selbstbestimmung (vgl. z.B. Albrecht 2003). Als angemessene und datenschutzgerechte Möglichkeit, hier zu einem Ausgleich zu kommen, bietet sich der *Verzicht auf die Speicherung entsprechender Rohdaten* an.

- Bei einem Masseneinsatz biometrischer Systeme sind grundsätzlich *strenge Anforderungen* an die Leistungsfähigkeit des gewählten Systems zu stellen. Zur Erreichung des vom Gesetzgeber verfolgten Zweckes der zweifelsfreien Überprüfung der Identität der das Dokument vorlegenden Person mit dem berechtigten Inhaber des Dokumentes bedarf es nicht nur eines Systems, mit dessen Hilfe die Zahl der Personen, die die Grenzkontrollen mit falscher Identität passieren können, möglichst gering zu halten. Auch die in aller Regel nicht vollständig zu vermeidenden fälschlichen Zurückweisungen berechtigter Personen müssen sich in einem für die Betroffenen zumutbaren Rahmen bewegen. (Die entsprechende Leistungsfähigkeit der Systeme ist in Kapitel IV erörtert worden.)

  In diesem Zusammenhang ist gefordert worden, dass eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten vor der Ausgabe der Ausweise und Pässe bereits durch die örtlichen Pass- und Personalausweisbehörden ausgeschlossen werden muss. Zu diesem Zweck bedarf es flankierender technischer und organisatorischer Maßnahmen, wie z.B. eine vor der Aushändigung des Dokumentes erfolgende Prüfung mithilfe eines Referenz-Kontrollsystems (Konferenz der Datenschutzbeauftragten 2002, S. 3). Unter Umständen sind daher solche Systeme vorzuziehen, die zusätzlich eine sog. Interne Qualitätskontrolle der aufgenommen biometrischen Daten zur sofortigen Überprüfung ihrer Tauglichkeit für den späteren Erkennungszweck vornehmen.

1.2.3 Einbringung von Merkmalen und Angaben in verschlüsselter Form

Gemäß § 4 Abs. 3 Satz 2 und 3 PassG sowie § 1 Abs. 4 Satz 2 und 3 PAuswG dürfen das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass oder Personalausweis eingebracht werden.

- Eine Verschlüsselung könnte einmal dadurch erreicht werden, dass die auf dem Pass oder Personalausweis enthaltenen Daten über den Inhaber des Dokumentes mittels des gewählten Verfahrens so unkenntlich gemacht werden, dass sie lediglich von Berechtigten, die im Besitz des Schlüssels sind, wieder gelesen werden könnten. Um einen solchen *Schutz vor unbefugter Kenntnisnahme* zu erreichen, bedarf es eines *Verschlüsselungsverfahrens*, das wissenschaftlich anerkannt ist und nach dem Stand der Technik als sicher gilt.
- Eine Verschlüsselung im Sinne von Unkenntlichmachung ist zwar auch geeignet, um biometrische Daten *vor einer Verfälschung durch Unbefugte zu schützen*. Eine vorteilhaftere Option sind jedoch Public-Key-Signatur-Verfahren. Diese ermöglichen einen Authentizitäts- und Integritätsnachweis, indem der Aussteller die biometrischen Daten um eine *elektronische Signatur* ergänzt, die nur er erzeugen kann. Die Prüfung der Signatur geschieht beim Lesen mit einem zweiten (Prüf)Schlüssel. Von Vorteil ist, dass mit dem Prüfschlüssel nur die Prüfung der Signatur, nicht aber deren Erstellung möglich ist. Daher kann der Prüfschlüssel öffentlich bekannt gemacht werden, ohne die Sicherheit des Verfahrens zu gefährden. Ähnlich wie bei der Verschlüsselung hängt die Sicherheit des Signaturverfahrens von der Länge der verwendeten Signaturschlüssel ab. Verschlüsselungs- und Signaturverfahren sind kombinierbar und können gleichzeitig Authentizität, Integrität und Vertraulichkeit der biometrischen Daten sicherstellen (ULD-SH 2003, S. 55).

  Auch an dieser Stelle stellt sich das bereits erörterte Problem des Gültigkeitszeitraums der Pässe und Personalausweise. Legt man den Gültigkeitszeitraum für Pässe und Personalausweise von derzeit fünf bis zehn Jahren zugrunde, so sind aus datenschutzrechtlicher Sicht Verschlüsselungs- bzw. Signaturverfahren zu fordern, die mindestens für diesen Gültigkeitszeitraum als sicher gelten müssen (Konferenz der Datenschutzbeauftragten 2002, S. 3). Da gemäß § 14 Abs. 3 der Signaturverordnung (SigV) qualifizierte Zertifikate höchstens fünf Jahre gelten dürfen, *sind entsprechende Regelungen* vom Gesetz- bzw. Verordnungsgeber *noch zu schaffen*, dabei wäre ein über die

Gültigkeitsdauer hinausreichender Schutz durch Verschlüsselungsverfahren wünschenswert (ULD-SH 2003, S. 56).

Für die Bürger stellt sich ohne weitere Maßnahmen die Situation gleich dar: Auf ihren Ausweisen finden sich „unverständliche" Daten, für deren Verständnis sie auf die Mithilfe der Behörde (etwa in Form einer Auskunftsverpflichtung nach § 16 Abs. 6 PassG bzw. § 3 Abs. 5 PAuswG) oder auf technische Mittel angewiesen sind. Ob diese Daten signiert, verschlüsselt (im kryptographischen Sinn) oder lediglich codiert (mit einem öffentlich bekannten Code) vorliegen, kann der Betroffene im Einzelfall nicht erkennen.

Der Gesetzgeber hat mit der Formulierung „dürfen auch in mit Sicherheitsverfahren verschlüsselter Form [...] eingebracht werden" eine Kann-Bestimmung geschaffen. Würde er die Verschlüsselung der Daten vorsehen, so muss geregelt werden, welche Stelle die Verschlüsselung/Signatur vornehmen soll. In Betracht kommen die jeweiligen örtlichen Pass- und Personalausweisbehörden oder aber die Bundesdruckerei oder eine andere öffentliche oder private zentrale Stelle.

In diesem Zusammenhang bedarf es des Weiteren der Regelung von Sicherheitsvorkehrungen, die verhindern, dass der Entschlüsselungs- bzw. Signaturerstellungsschlüssel Unbefugten bekannt wird. Dies ist insbesondere zu beachten, wenn Verschlüsselungsverfahren zum Einsatz kommen, deren Ver- und Entschlüsselungsschlüssel gleich ist (sog. „symmetrische Verfahren"): Da jedes Prüf- bzw. Lesegerät für biometrische Ausweise diesen Schlüssel enthalten muss, besteht die Gefahr, dass durch den Diebstahl eines Gerätes der Schlüssel kompromittiert wird und der unrechtmäßige Besitzer in die Lage versetzt wird, selbst Verschlüsselungen vorzunehmen (ULD-SH 2003, S. 56).

1.2.4 Verwendungszweck

§ 16 Abs. 6 PassG und § 3 Abs. 5 PAuswG enthalten Vorgaben dahingehend, dass die im Pass oder Personalausweis gespeicherten Angaben *nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung*[13] *des Pass- oder Personalausweisinhabers* ausgelesen werden dürfen. Insoweit legt der Gesetzgeber im Rahmen dieser Vorschriften bereits fest, für welche Zwecke die Daten verwendet werden dürfen. Eine darüber hinausgehende Verarbeitung und Nutzung der Daten ist nicht eröffnet: Eine Verwendung zur direkten Identifi-

13 Garstka (2002, S. 525) nimmt an, dass der Gesetzgeber den Begriff „Identitätsprüfung" fälschlich gewählt hat und damit die Authentizitätsprüfung (Verifikation) gemeint hat.

zierung, z.B. durch die automatische Erkennung gesuchter Personen im Rahmen einer Videoüberwachung, wird durch die Vorschriften ebenso ausgeschlossen (Garstka 2002, S. 525) wie Identifikationsanwendungen in Form von Abgleichen mit Datenbanken.

Die Verwendung von Personalausweis und Pass im nichtöffentlichen Bereich ist in § 4 PAuswG bzw. § 18 PassG eingeschränkt. Die Dokumente dürfen danach auch hier als Ausweis- und Legitimationspapier benutzt werden. Die Seriennummer darf aber nicht zum Abruf von Dateien oder zu deren Zusammenführung verwendet werden. Auch ein automatisierter Abruf oder eine automatisierte Speicherung des Dokuments ist ausdrücklich verboten. Dies schließt eine entsprechende Nutzung und dadurch auch faktisch die Weiterverarbeitung der biometrischen Daten durch Private mit aus (ULD-SH 2003, S. 76).

Die Frage, ob der in der Vorschrift genannte Verwendungszweck der Überprüfung der Echtheit des Dokumentes bzw. der Identitätsprüfung den Anforderungen genügt, die nach dem strengen Zweckbindungsgrundsatz zu stellen sind, dürfte im Hinblick auf Pässe und Personalausweise von Bundesbürgern wohl zu bejahen sein.

1.2.5 Verbot der Einrichtung einer bundesweiten Datei für Bundesbürger

PassG und PAuswG regeln, dass eine bundesweite Datei, in der die biometrischen Merkmale gespeichert werden, nicht eingerichtet wird (§ 4 Abs. 4 Satz 2 PassG, § 1 Abs. 5 Satz 2 PAuswG).[14] Mit der Aufnahme eines Verbotes zur Einrichtung einer bundesweiten Datei hat der Gesetzgeber einer zentralen Speicherung (und Auswertung) der biometrischen Daten eine Absage erteilt.

1.2.6 Speicherung und sonstige Verarbeitung biometrischer Merkmale

Der Gesetzgeber hat hinsichtlich der Aufnahme biometrischer Merkmale in Pässe und Personalausweise die Regelung der „Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung“ einem weiteren Bundesgesetz überlassen. Es ist wohl davon auszugehen, dass der Gesetzgeber mit der Formulierung in § 4

14 Diese Regelung war in dem Gesetzentwurf zunächst nicht enthalten. Vielmehr wurde sie erst aufgrund des Änderungsantrages der Fraktionen SPD und Bündnis 90/DIE GRÜNEN vom 11. Dezember 2001 eingefügt. Dort heißt es zur Begründung: „Die Einrichtung einer bundesweiten Datei ist nicht vorgesehen. Dies gilt in gleicher Weise für eine länderübergreifende Vernetzung der lokalen Register.“ (http://www.cilip.de/terror/aenderung11122001.pdf)

Abs. 4 Satz 1 PassG bzw. § 1 Abs. 4 Satz 1 PAuswG die technischen Modalitäten der Speicherung, Verarbeitung und Nutzung gemeint hat. Welche Anforderungen an die Regelung dieser Modalitäten zu stellen sind, wird im Folgenden in zwei Konstellationen erörtert:

Speicherung im Pass oder Personalausweis

Es ist denkbar, die biometrischen Merkmale ausschließlich im Pass oder Personalausweis zu speichern. Da anhand der biometrischen Merkmale festgestellt werden soll, ob derjenige, der das Dokument vorlegt, auch tatsächlich der berechtigte Inhaber des Dokumentes ist, wäre zur Erfüllung dieses Zweckes eine Speicherung außerhalb des jeweiligen Dokumentes nicht erforderlich. Damit hätten die Betroffenen – im Sinne der Realisierung der informationellen Selbstbestimmung – die alleinige Verfügungsgewalt über ihre biometrischen Daten.

Dezentrale Speicherung in Registern

Eine weitere Möglichkeit bestünde darin, die biometrischen Merkmale – zusätzlich zur Speicherung im Pass bzw. Personalausweis selbst – in dezentralen (elektronischen) Registern zu speichern. Gegenwärtig werden die in Pässen und Personalausweisen gespeicherten Daten über die Person des Pass- bzw. Personalausweisinhabers im Pass- bzw. Personalausweisregister gespeichert. § 16 Abs. 2 PassG bzw. § 3 Abs. 2 PAuswG regeln derzeit ausdrücklich, dass die Beantragung, Ausstellung und Ausgabe von Pässen bzw. Personalausweisen nicht zum Anlass genommen werden darf, die dazu erforderlichen Angaben bei anderen Stellen als bei den zuständigen Pass- bzw. Personalausweisbehörden zu speichern.

Die Bundesdruckerei, die die Pässe und Personalausweise personengebunden herstellt und die zu diesem Zwecke von den Pass- und Personalausweisbehörden die für die personengebundene Herstellung erforderlichen Daten einschließlich des Lichtbildes erhält, darf lediglich eine zentrale Speicherung der Seriennummern (s.o.) der Pässe zum Nachweis des Verbleibs der Pässe vornehmen (§ 16 Abs. 3 Satz 1 PassG, § 3 Abs. 3 Satz 1 PAuswG). Die Speicherung der übrigen im Pass oder Personalausweis enthaltenen Angaben ist unzulässig, soweit sie nicht ausschließlich und vorübergehend der Herstellung des Passes

bzw. Personalausweises dient. Die Angaben sind anschließend zu löschen (§ 16 Abs. 3 Satz 2 PassG, § 3 Abs. 3 Satz 2 PAuswG).[15]

Da gegenwärtig die Speicherung biometrischer Merkmale nicht von den im Pass- und Personalausweisregister zu speichernden Angaben umfasst wird, bedarf es noch einer Regelung in dem zu erlassenden Ausführungsgesetz.

Beurteilung

Die genannten Möglichkeiten der Speicherung biometrischer Daten auf den Ausweisen selbst, in einem dezentralen Datenbestand oder einem zentralen Datenbestand sind aus datenschutzrechtlicher Sicht unter dem Gesichtspunkt der Verhältnismäßigkeit unterschiedlich zu bewerten.

Der in der Begründung zum Terrorismusbekämpfungsgesetz angeführte *Zweck*, die „Möglichkeiten zur computergestützten Identifizierung von Personen auf der Grundlage der Ausweisdokumente" zu verbessern sowie zu verhindern, dass „Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen", *kann durch eine Speicherung allein auf dem Ausweis erreicht werden*.[16]

Fraglich ist deshalb, ob die Speicherung der Daten außerhalb der Ausweise unter dem Gesichtspunkt der Zweckbindung sowie der Datenvermeidung und Datensparsamkeit überhaupt als verhältnismäßig angesehen werden kann. Es ist zu bedenken, dass eine Speicherung in dezentralen Registern die Möglichkeit eröffnete, die Daten zu Ermittlungs- und Fahndungszwecken sowie zur Vorbeugung der Gefahr an die Polizei und andere Strafverfolgungsbehörden zu übermitteln. Eine derartige Nutzung verstieße gegen den Verhältnismäßigkeitsgrundsatz. Schließlich stünde eine Speicherung der biometrischen Daten in dezentralen Registern – ohne spezifische gesetzliche Regelung – nicht mit dem Recht

15 In diesem Zusammenhang ist zu erwähnen, dass auch die Zusammenfassung von Melde-, Personalausweis- und Passregistern unzulässig wäre. Auch wenn diese einzelnen Register organisatorisch bei den Einwohnermeldeämtern ein Register darstellen, so muss die funktionelle Trennung – gemäß den Vorgaben des Bundesverfassungsgerichts – strikt gewährleistet sein.

16 Der Zweck der Verhinderung von „Doppelidentitäten" durch Abgleich biometrischer Daten einer Person mit denjenigen anderer Personen im Sinne einer Identifikation würde dahingegen eine Speicherung personenbezogener Daten in Referenzdateien voraussetzen. Dies hat der Gesetzgeber angesichts der Gefahren für das Recht auf informationelle Selbstbestimmung abgelehnt. Es wäre damit zu rechnen, dass nicht nur Strafverfolgungsbehörden, sondern auch Unbefugte durch unbefugten Zugriff auf die Datenbanken (Hacking) in den Besitz der Daten gelangen. Aus datenschutzrechtlicher Sicht ist eine zentrale Datei, die die Referenzdaten aller Bundesbürger umfasst, auch aus Verhältnismäßigkeitsgründen als unzulässig anzusehen (Entschließung der Konferenz der Datenschutzbeauftragten 2002).

auf informationelle Selbstbestimmung in Einklang, weil sie eine zweckfremde Nutzung der Daten ohne Einwilligungsmöglichkeit der Betroffenen zuließe.

Weiterhin käme eine Speicherung der biometrischen Daten durch die Ausstellungsbehörde „für die Akten“ in Betracht. Der einzige Zweck der Speicherung bestünde darin, im Einzelfall die Ordnungsmäßigkeit des Verwaltungshandelns überprüfen zu können, indem (manuell) Einblick in die aufbewahrten Unterlagen genommen würde. Zu unterscheiden wäre hier, ob die biometrischen Rohdaten, die Templates oder beide gespeichert werden. Im Hinblick auf das Gebot der Datensparsamkeit ist eine Speicherung allein der Templates zu bevorzugen.

Im Falle einer elektronischen Speicherung auf den Ausweisen würde dieser Datenbestand der biometrischen Merkmale vermutlich auch elektronisch gespeichert werden. In diesem Fall wäre zu gewährleisten, dass der Datenbestand von den übrigen Datenbeständen abgeschottet ist und im Hinblick auf die enge Zweckbindung einer wirksamen Zugriffsregelung unterliegt.

Allerdings ist zu bedenken, dass die entsprechenden biometrischen Merkmale in jedem Falle in einem Datenbestand gespeichert würden, der nicht der Verfügungsgewalt des Betroffenen unterläge. Im Hinblick auf das informationelle Selbstbestimmungsrecht ist es deshalb vorzuziehen, die biometrischen Merkmale des Pass- oder Personalausweisinhabers lediglich auf dem Dokument und damit im Verfügungsbereich des Betroffenen selbst zu speichern (ULD-SH 2001, S. 11).

1.2.7 Rechte der Betroffenen

Rechte der Betroffenen und insbesondere das Recht auf Auskunft über ihre Daten sind zentraler Bestandteil des Datenschutzrechts. Den von der Datenverarbeitung Betroffenen muss eine größtmögliche Information über die ihn betreffende staatliche Datenverarbeitung geboten werden. Im Hinblick auf dieses Transparenzgebot ist zwar fraglich, ob die Zulassung der Verschlüsselung der Daten des Betroffenen auf dem Pass oder Personalausweis diesem Gebot nicht entgegensteht, da der Betroffene im Falle der Verschlüsselung gerade nicht sehen kann, welche Daten über ihn gespeichert sind. Da der Gesetzgeber den Betroffenen in § 16 Abs. 6 PassG und § 3 Abs. 5 PAuswG jedoch ausdrücklich ein Auskunftsrecht (und damit Kontroll-, Abwehr- und Gestaltungsrechte) eingeräumt hat, ist dem Transparenzgebot Genüge getan.

2. Biometrie in Ausweisdokumenten für Ausländer

Analog zu den Ausführungen über Ausweisdokumente für Bundesbürger werden nachfolgend zunächst die Regelungen für Ausweisdokumente für Ausländer vorgestellt und danach die mit dem TBG erfolgten Vorgaben im Blick auf u.U. gegebenen Handlungsbedarf diskutiert (Kap. V.2.2). Aufgrund dieser Fokussierung werden die EU-Visa im Folgenden nicht betrachtet (s. hierzu Kap. II.1).

2.1 Regelungen und Ziele

Während das Ausländer- und Asylverfahrensrecht bislang keine Vorschriften darüber enthielt, in welcher Form Aufenthaltstitel auszugestalten sind, wurden nunmehr mit dem TBG Regelungen geschaffen, die konkrete Vorgaben enthalten: In die für Ausländer auszustellenden Dokumente können – wie in die Identifikationspapiere für Bundesbürger – ebenfalls biometrische Merkmale aufgenommen werden.

Artikel 11 Terrorismusbekämpfungsgesetz (Änderung des Ausländergesetzes)

In § 5 AuslG werden die Formen, in denen eine *Aufenthaltsgenehmigung* durch die Ausländerbehörde erteilt werden kann, geregelt. Hierbei handelt es sich um die Aufenthaltserlaubnis (§§ 15 u. 17), die Aufenthaltsberechtigung (§ 27), die Aufenthaltsbewilligung (§§ 28 u. 29) und die Aufenthaltsbefugnis (§ 30). Die Arten der Aufenthaltsgenehmigung unterscheiden sich nach Dauer und/oder Zweck des jeweiligen Aufenthalts.

Während das AuslG bisher die Gestaltung von Aufenthaltstiteln nicht regelte, wird nunmehr durch die Ergänzung des § 5 AuslG ein einheitliches Vordruckmuster für die Aufenthaltsgenehmigung vorgesehen, mit dem eine Vielzahl identifizierender Merkmale aufgenommen wird. Die Aufenthaltsgenehmigung kann wie bisher als Klebeetikett in den Pass oder das Passersatzpapier des Ausländers eingeklebt (§ 5 Abs. 2 AuslG) oder aber als eigenständiges Dokument ausgestellt werden (§ 5 Abs. 3 AuslG). In beiden Fällen kann die Aufenthaltsgenehmigung gemäß § 5 Abs. 4 AuslG neben dem Lichtbild und der eigenhändigen Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers enthalten. Diese Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in die Aufenthaltsgenehmigung eingebracht

werden. In ihrem Inhalt entspricht die Vorschrift insoweit § 4 Abs. 3 PassG bzw. § 1 Abs. 4 PAuswG.

Die Aufnahme biometrischer Merkmale ist auch für die unterschiedlichen, nach einheitlichem Muster gestalteten *„Ausländerausweise“* vorgesehen. Hierbei handelt es sich um den Ausweisersatz (§ 39 Abs. 1 AuslG), die Duldungsbescheinigung (§ 56a AuslG) sowie die Fiktionsbescheinigung (§ 69 Abs. 2 AuslG).

Neben der Aufnahme biometrischer Merkmale in die genannten Dokumente sieht § 5 Abs. 2 AuslG vor, dass die Aufenthaltsgenehmigung eine *Zone für das automatische Lesen* enthält. Diese enthält zahlreiche identifizierende Merkmale, u.a. Familienname, Geburtsdatum, Geschlecht, Staatsangehörigkeit, die alle öffentlichen Stellen „zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen“ können (§ 5 Abs. 7 AuslG). Die Vorschrift des § 5 Abs. 5 und 7 AuslG wird auch für den Ausweisersatz, die Duldungsbescheinigung und die Fiktionsbescheinigung, die ebenfalls eine Zone für das automatische Lesen enthalten können, entsprechend anwendbar erklärt.

Nach der Gesetzesbegründung ist das *Speichern der Daten erforderlich, um maschinelle Datenabgleiche durchführen zu können* (Bundesrat 2001, S. 127).

Artikel 12 Terrorismusbekämpfungsgesetz (Änderung des Asylverfahrensgesetzes)

Da § 63 Abs. 2 AsylVfG auf die Geltung des § 56a AuslG verweist, können biometrische Merkmale auch in die Bescheinigung über die Aufenthaltsgestattung von Asylbewerbern aufgenommen werden. Die Vordruckmuster und Ausstellungsmodalitäten sind vom Bundesministerium des Innern durch Rechtsverordnung zu bestimmen.

2.2 Vorgaben für die Umsetzung

2.2.1 Ausgestaltung durch eine Rechtsverordnung

Im Unterschied zu den Identifikationspapieren für deutsche Bundesbürger bedarf es als Voraussetzung zur Einbringung von biometrischen Merkmalen in Aufenthaltstitel und Ausweise für Ausländer nicht eines Ausführungsgesetzes, sondern lediglich einer Rechtsverordnung. Gemäß § 5 Abs. 6 AuslG handelt es sich um eine Rechtsverordnung des Bundesministeriums des Innern, die der Zustimmung des Bundesrates bedarf.

- Nach Art. 80 GG müssen Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz bestimmt werden (Art. 80 Abs. 1 Satz 2 GG). Im Hinblick auf die Anforderungen des Art. 80 Abs. 1 Satz 2 GG ist es zunächst *fraglich, ob die Zwecke im AuslG und im AsylVfG ausreichend bestimmt sind*, da eine inhaltliche Konkretisierung völlig fehlt.
- Ferner *ist der Verzicht auf eine gesetzliche Grundlage problematisch*, da hier Eingriffe in das Recht auf informationelle Selbstbestimmung in Rede stehen. Auch wenn solche Einschränkungen nicht in jedem Fall der Grundlage eines formellen Gesetzes bedürfen, müsste dennoch ein sachlicher Grund dargetan werden, der eine unterschiedliche Behandlung von Bundesbürgern und Ausländern rechtfertigt. In der Gesetzesbegründung wird kein Grund für die unterschiedliche Behandlung von Bundesbürgern und Ausländern angeführt. Angesichts der gleich lautenden Vorschriften zur Aufnahme biometrischer Merkmale im Pass- bzw. PAuswG und dem AuslG bzw. AsylVfG ist es mit dem Gleichheitsgrundsatz nicht zu vereinbaren, für Bundesbürger ein formelles Gesetz vorzusehen und für Ausländer eine Rechtsverordnung für ausreichend zu erachten (ULD-SH 2003, S. 42).
- Schließlich gilt auch hier die Verpflichtung, dass der Gesetzgeber in grundlegenden normativen Bereichen alle wesentlichen Entscheidungen selbst treffen muss. § 5 Abs. 6 AuslG überlässt die Regelung sämtlicher Modalitäten, wie z.B. die Wahl der biometrischen Merkmale, die Aufnahme und die Abspeicherung im Rahmen des Erstellungsvorgangs oder das Führen von Referenzdateien sowie die Nutzung dieser Daten der zu erlassenden Rechtsverordnung. Da mit der Aufnahme der biometrischen Merkmale sowie ihrer weiteren Speicherung, Verarbeitung und Nutzung in das auch für Ausländer geltende Recht auf informationelle Selbstbestimmung eingegriffen wird, ist es *mit dem vom Bundesverfassungsgericht* in seiner Rechtsprechung aufgestellten Grundsatz, nach dem alle wesentlichen Entscheidungen vom Parlament selbst zu regeln sind, nicht vereinbar, die Ausgestaltung der Modalitäten der Aufnahme biometrischer Merkmale ohne nähere Präzisierung und Eingrenzung einer Rechtsverordnung zu überlassen (ULD-SH 2003, S. 48).

2.2.2 Nennung biometrischer Merkmale bestimmter Körperbereiche

Hier kann im Wesentlichen auf die vorstehenden Ausführungen verwiesen werden (Kap. V.1.2.2). Da die entsprechenden Vorschriften im AuslG und im AsylVfG inhaltlich gleich lautend sind, ergibt sich keine grundsätzlich abweichende Beurteilung.

Gleichwohl eröffnet sich eine weiter gehende Problematik. Während das PassG und das PAuswG eine Beschränkung des Auslesens der Daten auf die Überprüfung der Echtheit des Dokumentes und die Identitätsprüfung des Inhabers vorsehen (Kap. V.1.2.4), fehlt eine derartige Regelung im AuslG. Dadurch ist die Nutzung für polizeiliche Zwecke über die generellen gesetzlichen Übermittlungsbefugnisse der Ausländerbehörden und die Erhebungsbefugnisse durch Polizeibehörden eröffnet (Kap. V.2.2.4) – z.B. eine Verwendung dieser Daten für polizeiliche Spurenabgleiche, z.B. mit an Gläsern hinterlassenen Fingerabdrücken. Die Praxis der Videoüberwachung im öffentlichen Raum ermöglicht auch die Vornahme von Musterabgleichen mit anderweitig erfassten Videobildern (Weichert 2002, S. 425).[17]

Angesichts dieser Möglichkeiten wäre aus Gründen der Verhältnismäßigkeit und zur *Verhinderung einer zweckwidrigen Nutzung* besonders darauf zu achten, dass ein Merkmal verwendet wird, das keine personenbezogenen Zusatzinformationen enthält. Wie bereits oben dargestellt, kann dieses durch den *Verzicht auf die Speicherung von Rohdaten* erreicht werden.

Hinsichtlich der Problematik der Geeignetheit der biometrischen Merkmale zur Verifikation über den erforderlichen Gültigkeitszeitraum des Passes oder Personalausweises für Bundesbürger lässt sich für „Ausländerausweise“ eine Parallele ziehen. So existieren zwar Aufenthaltsgenehmigungen für lediglich einen kurzen Gültigkeitszeitraum (z.B. Aufenthaltsbewilligung gemäß § 28 AuslG, die in der Regel längstens für zwei Jahre erteilt wird). Andere Aufenthaltsgenehmigungen gelten jedoch auch unbefristet (z.B. Aufenthaltsberechtigung gemäß § 27 AuslG). Unter im AuslG näher geregelten Voraussetzungen kann die jeweilige Aufenthaltsgenehmigung verlängert werden.

Es ist daher erforderlich, bei Schaffung der Rechtsverordnung die Geeignetheit der biometrischen Merkmale zur dauerhaften Verifikation oder Identifika-

17 In der Erprobung beim BKA befinden sich Verfahren, die Gesichtsaufnahmen aus Videoüberwachungskameras biometrisch auswerten sollen. Denkbar ist der Einsatz sog. „Watchlists“, die – Fahndungslisten vergleichbar – Aufnahmen von gesuchten oder zu überprüfenden Personen enthalten.

tion des Merkmalsinhabers sorgfältig zu prüfen und gegebenenfalls die *Gültigkeitsdauer* von „Ausländerausweisen“ *anzupassen*.

2.2.3 Verschlüsselung

Das zuvor erörterte Problem des Gültigkeitszeitraums der Ausweisdokumente stellt sich auch im Blick auf die Verschlüsselung. Kryptografische Algorithmen können nur innerhalb eines bestimmten Zeitraums als sicher gelten. Dieser Tatsache hat der Gesetzgeber z.B. im Signaturgesetz Rechnung getragen, indem er die Gültigkeitsdauer von Zertifikaten beschränkt hat. Dieselbe Vorsicht sollte der Gesetzgeber auch beim Einsatz kryptografischer Verfahren zur Verschlüsselung und/oder Signatur biometrischer Daten in Ausweisen walten lassen. Wenn nur von einer begrenzten Dauer des sicheren kryptografischen Schutzes biometrischer Daten (sei es durch Verschlüsselung oder durch Signaturen) auszugehen ist, wäre die Gültigkeitsdauer der Ausweise an diese Schutzdauer anzupassen.

2.2.4 Art der Speicherung und sonstigen Verarbeitung und Nutzung von Daten – Verwendungszweck

Neben dem Lichtbild und der eigenhändigen Unterschrift kann die Aufenthaltsgenehmigung weitere biometrische Merkmale von Fingern oder Händen oder Gesicht, die auch in mit Sicherheitsverfahren verschlüsselter Form in die Aufenthaltsgenehmigung eingebracht werden können, enthalten (§ 5 Abs. 4 AuslG). In welcher Weise die Aufnahme dieser Merkmale erfolgen soll, bleibt der noch zu erlassenen Rechtsverordnung überlassen. Die Aufnahme der Merkmale in die *Zone für das automatische Lesen* ist in § 5 Abs. 5 abschließend beschrieben.

Die in § 5 Abs. 7 AuslG enthaltene Befugnis aller öffentlichen Stellen zur Speicherung, Übermittlung und Nutzung der in der Zone für das automatische Lesen enthaltenen Daten beschränkt sich insoweit auf die in § 5 Abs. 5 AuslG genannten Angaben. *Biometrische Merkmale werden von dieser Befugnis nicht erfasst.*

Es erscheinen Bedenken gerechtfertigt, dass die Nutzung biometrischer Daten in Ausländerausweisen weder geregelt ist noch in den Verordnungsermächtigungen (§ 5 Abs. 6 AuslG, § 39 Abs. 1 AuslG, § 56a AuslG, § 69 Abs. 2 AuslG) als regelungsbedürftig angesehen wird. Würden zukünftig in den entsprechenden

Verordnungen lediglich die Ausstellungsmodalitäten für die biometrischen Daten geregelt, so blieben Nutzungs- und Übermittlungsbefugnisse ungeregelt.

Unklar ist, in welcher Weise nach dem Willen des Gesetzgebers die biometrischen Daten auf die Ausweise aufgebracht werden sollen, wenn diese nicht in der Zone für das automatische Lesen enthalten sein dürfen. Da biometrische Daten ausschließlich automatisch ausgelesen werden können, erscheint es konsequent, für diese eine „weitere Zone für das automatische Lesen" aufzunehmen, was ergänzender Regelungen bedarf.

Anders als bei den für die Bundesbürger geltenden Vorschriften wurde in das AuslG keine Begrenzung der Zwecke der Datenverarbeitung und -nutzung aufgenommen. Stattdessen enthält § 5 Abs. 7 AuslG eine pauschale Befugnis zur Verarbeitung sämtlicher automatisch lesbarer Daten für sämtliche öffentlichen Stellen, die die Daten zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen können. Nach der Gesetzesbegründung ist die Speicherung der Daten „erforderlich, um maschinelle Datenabgleiche durchführen zu können" (Bundesrat 2001, S. 127).

Zwar sieht die *Vorschrift* eine Beschränkung auf die Erforderlichkeit „zur Erfüllung ihrer gesetzlichen Aufgaben" vor, dieser *fehlt es jedoch an der verfassungsrechtlich gebotenen Bestimmtheit*. Da auch keine Beschränkung der Zwecke im polizeilichen Bereich (Gefahrenabwehr, Strafverfolgung) erfolgt, die Vorschrift für alle öffentlichen Stellen gilt und der Betroffene nicht erkennen kann, für welche Zwecke seine Daten verarbeitet und genutzt werden sollen, ergibt sich eine immer noch zu weitgehende Verarbeitungsbefugnis. Weiter ist – wie bei AFIS, wo bzgl. einer großen Gruppe der Ausländerbevölkerung (Asylsuchende und Bürgerkriegsflüchtlinge gem. § 41a AuslG, § 16 AsylVfG) eine polizeiliche Nutzung von Fingerabdruckdaten zugelassen wird (§ 78 Abs. 3 AuslG, § 16 Abs. 5 AsylVfG) – durch § 5 Abs. 7 AuslG eine polizeiliche *Nutzung von Daten bei unverdächtigen Personen* zugelassen.

Die Regelung in § 5 Abs. 7 AuslG enthält schließlich *systemwidrig* im Ausländerrecht eine Befugnisnorm für sämtliche öffentliche Stellen und steht im inhaltlichen Widerspruch zu bereichsspezifischen Regelungen (z.B. § 3 AZRG, der keine Ermächtigung zur zentralen Speicherung enthält).

Eine *Verwendungsregelung für private Stellen* ist, da die „Ausländerausweise" voraussichtlich auch im privaten Bereich genutzt werden dürften, im Interesse der Gleichbehandlung und dem Schutz vor Datenmissbrauch durch Private *erforderlich*.

2.2.5 Kein Verbot einer zentralen Speicherung

Anders als bei den für Bundesbürger geltenden Regelungen, ist im AuslG oder AsylVfG eine Pflicht zur dezentralen Speicherung von biometrischen Daten nicht statuiert. Es ist daher nicht gesetzlich ausdrücklich ausgeschlossen, zentrale Referenzdateien für die biometrischen Merkmale von Ausländern und Asylbewerbern, z.B. beim Bundesverwaltungsamt, einem künftigen Bundesamt für Migration und Flüchtlinge, der Bundesdruckerei oder auch dezentrale Referenzdateien bei den die Dokumente ausstellenden Ausländerbehörden, einzurichten.[18] Da in jedem Fall in den Unterlagen der jeweils zuständigen Ausländerbehörden ein Verweis auf die Ausweiserstellung vorgenommen werden müsste, wären diese Daten über das Ausländerzentralregister (AZR) zentral erschlossen (DVD 2001).

Gemäß § 3 Nr. 1 AZRG ist im AZR die meldende Stelle und deren Geschäftszeichen zu speichern. Die Vorschrift enthält dagegen *keine Ermächtigung zur Speicherung biometrischer Daten*.

Durch eine zentrale Speicherung von derartigen Ausländerdaten würde eine *zweckändernde Nutzung* dieser Daten erheblich erleichtert. Für die Durchführung von Datenabgleichen genügte das Vorliegen eines entsprechenden biometrischen Referenzmusters für eine Zuordnung der biometrischen Datensätze. Eine Nutzung der biometrischen Ausländerdaten für andere Zwecke ist nach der derzeitigen Rechtslage nicht eingeschränkt, sondern für öffentliche Stellen ausdrücklich auf jeden gesetzmäßigen Zweck und jede Form der Datenverarbeitung ausgeweitet (§ 5 Abs. 7 AuslG). Eine Nutzung durch Private ist ebenfalls nicht ausdrücklich ausgeschlossen. Durch die erleichterte Abgleichsmöglichkeit und das Fehlen von spezifischen Zweckbindungsregelungen würde bei einer zentralen Speicherung von biometrischen Merkmalen von Ausländern *eine nicht gerechtfertigte Ungleichbehandlung* gegenüber deutschen Staatsangehörigen erfolgen.[19]

Eine Ungleichbehandlung wäre allenfalls sachlich begründbar, wenn mit dem Ausländerzentralregister ausländer- und asylrechtliche Zwecke verfolgt werden,

---

18 Einer zentralen Speicherung der biometrischen Ausweisdaten beim Bundeskriminalamt (BKA) steht entgegen, dass eine solche Datenverarbeitung nicht zu den Aufgaben dieser Behörde gehört.

19 Das Grundgesetz enthält zwar eine Privilegierung von Deutschen in Bezug auf bestimmte Grundrechte (Art. 8 Abs. 1, 9 Abs. 1, 11 Abs. 1, 12 Abs. 1, 16 Abs. 1 u. 2 Satz 1 GG), jedoch gilt dieses nicht für das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Hierbei handelt es sich um ein sog. Jedermann-Grundrecht, das in gleicher Weise für Nicht-Deutsche gilt (ULD-SH 2003).

die z.B. am aufenthaltsrechtlichen Status eines Ausländers anknüpfen, oder wenn vom Aufenthaltsrecht des Ausländers Entscheidungen anderer öffentlicher Stellen abhängen (z.B. Erwerbstätigkeit, Arbeitsaufnahme, Sozialleistungen). Zu den aufenthaltsrechtlichen Zwecken gehören aber gerade nicht die Zwecke der Gefahrenabwehr und Strafverfolgung. Mit der Vorschrift des § 5 Abs. 7 AuslG, die erlaubt, dass „öffentliche Stellen die in der Zone für das automatische Lesen enthaltenen Daten zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen“ können, wird also über die ausschließlich aufenthaltsrechtlichen Zwecke hinausgegangen. Diese weite Zweckänderung kann eine Ungleichbehandlung von Deutschen und Ausländern jedoch nicht rechtfertigen (ULD-SH 2003, S. 60).

Eine zentrale Speicherung biometrischer Daten von Ausländern in allen öffentlichen Stellen stellte aus den gleichen Gründen eine sachlich nicht gerechtfertigte Ungleichbehandlung dar, da die biometrischen Merkmale gerade nicht für aufenthaltsrechtliche Maßnahmen erforderlich sind. Hierfür reichen vielmehr die bereits im AZR gespeicherten Daten aus.

Im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung wäre eine Speicherung der biometrischen Merkmale außerhalb des Ausweisdokumentes allenfalls bei einer dezentralen oder zentralen Ausländerbehörde vorstellbar, wobei jedoch eine ausschließliche Bindung an die Zwecke der Datensicherung gesetzlich vorgesehen werden müsste (vgl. § 14 Abs. 4 BDSG).

2.2.6 Rechte der Betroffenen

Abweichend von der Rechtslage für Bundesbürger wurde Ausländern ein gesetzlicher Auskunftsanspruch über den Inhalt der verschlüsselten Merkmale und Angaben nicht eingeräumt. Dies ist deshalb kritisch zu beurteilen, da auch Ausländern ein verfassungsrechtlich begründeter und über das allgemeine Datenschutzrecht normativ zugesicherter Auskunftsanspruch zusteht (§ 19 BDSG). Gesetzmäßige Gründe zum Ausschluss des Auskunftsanspruchs können bzgl. der auf den Ausweisdokumenten gespeicherten verschlüsselten Daten nicht zum Tragen kommen (§ 19 Abs. 4 BDSG). Die Auskunftserteilung bedingt nicht eine Offenlegung des (geheimen) Schlüssels an den Betroffenen. Auch sonstige Gründe, z.B. solche der öffentlichen Sicherheit, begründen keine Notwendigkeit der Geheimhaltung (ULD-SH 2003, S. 77).

3. Fazit

Im Datenschutzrecht gilt ein aus dem Grundrecht auf informationelle Selbstbestimmung hergeleiteter strenger Zweckbindungsgrundsatz. Hinsichtlich der Bundesbürger hat der Gesetzgeber geregelt, dass die biometrischen Merkmale nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung ausgelesen und verwendet werden dürfen. Hiermit ist dem Zweckbindungsgrundsatz ausreichend Rechnung getragen. Anders ist der Bereich der „Ausländerausweise" zu beurteilen. Die pauschale Verarbeitungsbefugnis in § 5 Abs. 7 AuslG und das Fehlen einer Regelung der Verwendungszwecke biometrischer Daten – bzw. schon eines Hinweises auf Regelungsbedürftigkeit – sind mit den verfassungsrechtlichen Vorgaben zur Zweckbindung und mit dem Bestimmtheitsgebot nicht in Einklang zu bringen.

Der Gesetzgeber hat ausdrücklich als in Betracht kommende biometrische Merkmale solche von „Fingern oder Händen oder Gesicht" genannt. Hieraus ließe sich plausibel folgern, dass nicht nur andere, sondern auch die Kombination mehrerer Merkmale ausgeschlossen sind. Folgt man dem, wäre hierdurch nach heutigem technischem Kenntnisstand u.U. die Leistungsfähigkeit biometrischer Systeme nicht auszuschöpfen.

Hinsichtlich der Auswahl der einzelnen in Betracht kommenden biometrischen Merkmale ist zu berücksichtigen, dass bei der Anwendung biometrischer Verfahren besonders schützenswerte Zusatzinformationen anfallen können. Unter dem Gesichtpunkt der Verhältnismäßigkeit ist es notwendig, die mit der Aufnahme der biometrischen Merkmale verbundenen Nebenwirkungen zu begrenzen. In Betracht kommt vor allem ein Verzicht auf die Speicherung von Rohdaten.

Die vom Gesetzgeber – ohne nähere Vorgaben – geschaffene Befugnis, die Merkmale und Angaben auch in verschlüsselter Form in das jeweilige Dokument zu integrieren, macht eine genaue Regelung der Frage erforderlich, in welcher Weise eine Verschlüsselung vorzunehmen ist bzw. die biometrischen Daten mit einer elektronischen Signatur zu signieren sind. Außerdem ist zu bestimmen, welche Stelle(n) die Verschlüsselung vornehmen bzw. die Signatur erzeugen soll(en). Angesichts der hierfür erforderlichen Sicherheitsumgebung erscheint eine zentrale Erstellung der Dokumente vorzugswürdig.

Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger zurzeit gesetzlich ausgeschlossen. Eine Speicherung auf dem Ausweisdokument würde genügen, um den gesetzlichen Zweck zu erreichen. Die Einrichtung zen-

traler Referenzdateien für Ausländer ist nicht gesetzlich ausgeschlossen. Eine solche zentrale Datenspeicherung wäre jedoch aus Gründen der Ungleichbehandlung im Sinne des Art. 3 GG und des Prinzips der Verhältnismäßigkeit problematisch. Auch eine dezentrale Speicherung der Daten in einem Register würde die Verwendung zu strafrechtlichen Ermittlungszwecken oder zur „Rasterfahndung“ ermöglichen. Da die Speicherung biometrischer Merkmale in einem Datenbestand, der nicht der alleinigen Verfügungsgewalt des Betroffenen unterliegt, die Gefahr einer (unzulässigen) Zweckentfremdung birgt, ist auch die Speicherung in dezentralen Registern rechtlich problematisch. Ungeklärt ist bisher, in welchem Verhältnis AFIS, das auch dem Zweck der Identifizierung von Ausländern dient, und der Einsatz von Biometrie auf „Ausländerausweisen“ mit genau demselben Zweck stehen.

Für die Speicherung der biometrischen Merkmale von Ausländern wäre im Lichte des Grundrechts auf informationelle Selbstbestimmung eine Speicherung außerhalb des Ausweisdokumentes bei einer dezentralen oder zentralen Ausländerbehörde vertretbar.

Die vorstehenden Überlegungen verweisen auf einen sehr differenzierten Handlungsbedarf für den Gesetz- und Verordnungsgeber. Dieser ist wesentlicher Bestandteil eines insgesamt sich ergebenden Informations-, Diskussions- und Handlungsbedarf, der im folgenden Kapitel VI angesprochen wird.

TAB

VI. Ausblick

Der Entwicklungspfad biometrischer Identifikationssysteme bei Ausweisanwendungen ist zunehmend schmaler geworden: Die Zahl politischer und technischer Optionen für unterschiedliche Einsatzszenarien hat sich ebenso reduziert wie der nationale Gestaltungsspielraum. Gleichwohl besteht weiterer Bedarf an Information, Diskussion und Entscheidung: Auf der politischen Agenda stehen die gesetzgeberische Ausgestaltung der bislang im TBG grundsätzlich eröffneten Einsatzmöglichkeiten sowie Planungs- und Abstimmungsaktivitäten auf nationaler und internationaler Ebene. Schließlich wäre die Aufgabe in Angriff zu nehmen, einen öffentlichen Diskurs anzustoßen und aktiv mitzugestalten, der auch über die interessierten Kreise und die Gruppen der Experten hinausgeht.

Auf *Gesetzes- und Verordnungsebene* sind wichtige Aspekte der Umsetzung der bislang getroffenen gesetzlichen Regelungen zu klären. Die Vorentscheidungen des Gesetzgebers werden dabei wahrscheinlich neu zu diskutieren sein. Hier ist vor allem der Umstand zu nennen, dass für die Regelung der Aufenthaltstitel für Ausländer eine präzise Zwecksetzung für die Nutzung biometrischer Daten bislang nicht erfolgt ist. Eine wohl definierte Zweckbindung würde aber datenschutzrechtliche Bedenken ausräumen und die durch den Gesetz- und Verordnungsgeber verfolgten Ziele transparent machen.

Zu klären wäre weiter, ob die vorgenommene Beschränkung der in Betracht kommenden biometrischen Merkmale auf solche von „Fingern oder Händen oder Gesicht“ zukünftig noch Bestand haben sollte oder ob nicht auch die Kombination mehrerer Merkmale bzw. Systeme rechtlich eröffnet werden soll. Damit könnte u.U. die Leistungsfähigkeit biometrischer Systeme besser ausgeschöpft werden.

Angesichts der Schutzwürdigkeit biometrischer Daten als personenbezogene Daten ist es notwendig, die mit ihrer Aufnahme möglicherweise verbundenen problematischen Folgen zu begrenzen. Dementsprechend sollte vor allem auf die Speicherung von Rohdaten verzichtet und dem Prinzip der Datensparsamkeit Geltung verschafft werden. Es ist weiter genau zu regeln, in welcher Weise die Verschlüsselung der Daten vorzunehmen ist bzw. wie die biometrischen Daten mit einer elektronischen Signatur zu signieren sind.

Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger zurzeit gesetzlich ausgeschlossen. Eine Speicherung auf dem Ausweisdokument würde genügen, um den vorgesehenen gesetzlichen Zweck zu erreichen.

Es ist aber nicht ausgeschlossen, dass bei einer Diskussion um eine Zweckänderung oder -erweiterung auch ein zentrales Register wieder zu erörtern ist.

Die Einrichtung zentraler Referenzdateien für Ausländer ist gesetzlich nicht ausgeschlossen. Eine solche zentrale Datenspeicherung wäre jedoch aus Sicht des Datenschutzes äußerst problematisch. Dies gilt grundsätzlich auch für die Speicherung in dezentralen Registern, da die Speicherung biometrischer Merkmale in einem Datenbestand, der nicht der alleinigen Verfügungsgewalt des Betroffenen unterliegt, die Gefahr einer Zweckentfremdung mit sich bringt. Geklärt werden sollte, in welchem Verhältnis AFIS, das auch einer Identifizierung von Ausländern dient, und der Einsatz von Biometrie auf „Ausländerausweisen“ mit dem gleichen Zweck stehen.

Für die Speicherung der biometrischen Merkmale von Ausländern wäre im Lichte des Grundrechts auf informationelle Selbstbestimmung eine Speicherung außerhalb des Ausweisdokumentes bei einer dezentralen oder zentralen Ausländerbehörde vertretbar.

Politischer Diskussions- und Handlungsbedarf ergibt sich auch daraus, dass umfassende *Implementierungsschritte* auf allen Ebenen zu *planen* und in ihren *Konsequenzen* zu *durchdenken* sind – von der Ausstellungs- bis zur Kontrollebene. Da eine sicherheitspolitische Insellösung kaum Sinn macht und in weiten Teilen auch rechtlich nicht möglich ist, sind weitere Abstimmungsprozesse auf EU-Ebene und letztlich weltweit erforderlich, will man mehr Sicherheit erreichen und zugleich weder den globalen Reiseverkehr unangemessen beeinträchtigen noch Belange des Datenschutzes und das Recht auf informationelle Selbstbestimmung verletzen. Von Bedeutung dürfte auch die Präsenz deutscher Vertreter in den Gremien der ICAO und der EU sein, um dort eigene Beiträge einzubringen und nationale Interessen zu vertreten.

Die politischen, finanziellen und organisatorischen Konsequenzen einer Einführung und Nutzung biometrischer Identifikationssysteme auf allen Ebenen sowie mögliche Konflikte, z.B. zwischen den Zielen Sicherheit und Schutz der Privatsphäre, sind erst in Ansätzen durchdacht. Hier wären umfassende *Folgenanalysen* angebracht, die Fingerzeige für eine politische und datenschutzrechtliche Gestaltung der bereits jetzt eingetretenen Entwicklungsdynamik liefern.

Der *politische Diskurs*, verstanden als eine offene Kommunikation mit der allgemeinen Öffentlichkeit und Repräsentanten gesellschaftlicher Gruppen, ist bislang kaum entwickelt. Politische, rechtliche und technisch-organisatorische Vorentscheidungen fallen, ohne dass Ziele und Instrumente sowie Nutzen und Kosten der zukünftigen Nutzung von Biometrie im öffentlichen Bereich durch aktive politische Kommunikation umfassend vermittelt werden.

Ein so umfangreiches und komplexes Vorhaben wie die biometrische Vermessung aller Bundesbürger sowie von Millionen von ausländischen Bürgern, die nach Europa einreisen oder Asyl suchen, legt es aber nahe, auch die Frage der Akzeptanz anzugehen. Zu den Bemühungen um technische Praktikabilität sollten deshalb solche um gesellschaftliche Akzeptabilität treten. Zahlreiche Fragen, zu denen im bisherigen politischen Diskurs nur wenig eindeutige Antworten zu finden waren, müssten hier angesprochen werden. Dazu zählen vor allem die Ebene politischer Ziele und Teilziele: Die bisherige Zielführung der Biometrie bei Ausweisdokumenten für Bundesbürger ist durch den Gesetzgeber zwar definiert: Es soll die Einreise solcher Personen erschwert werden, die sich mit gefälschten oder Papieren anderer Personen legitimieren wollen. Im Rahmen dieser Zielsetzung kann aber kein essenzieller Beitrag zur Terrorismusbekämpfung geleistet werden – wie dies hin und wieder anklingt. Mehr Klarheit und größere Differenziertheit hätte deshalb die Erörterung der Frage verdient, welche Beiträge zu welchen Zielen mit welchen biometrischen Dokumenten erbracht werden können und sollen.

Auch die Zielsetzung einer biometrischen Ausrüstung und Nutzung von Aufenthaltstiteln und Ausweisdokumenten für Ausländer ist noch zu unklar. Allgemeine Hinweise auf die Bekämpfung des Terrorismus oder Missbräuche von Visa und Aufenthaltstiteln sollten differenzierter vermittelt werden. Es müsste aber auch klar ausgesprochen werden, welche Vorstellung und Konzepte der Nutzung biometrischer Technologien zugrunde liegen und warum es legitim sein könnte, begrenzte Eingriffe in Rechte von Betroffenen vorzunehmen.

Im Lichte dieser Diskussion wäre des Weiteren – unter Bezugnahme auf gewünschte Ziele – die Eignung technischer Lösungen und die Vertretbarkeit unterschiedlicher Kostenvolumina vergleichend zu diskutieren: Welcher Beitrag zu welcher Sicherheit ist erwünscht, und wie viel ist er uns wert?

Dabei käme es insbesondere darauf an, offen die Grenzen aller Lösungsmodelle zu diskutieren, also insbesondere klar zu machen, dass Biometrie nur einen begrenzten Zielbeitrag zu mehr Sicherheit leisten kann. Biometrie ist ein technischer Ansatz von Prävention und Kontrolle und somit nur ein – wenngleich wesentliches – Element einer übergreifenden Strategie.

Ferner sollte auch das Spannungsfeld zwischen dem Ziel Sicherheit einerseits sowie den Zielen Schutz der Privatsphäre und Begrenzung des Missbrauchspotenzials andererseits verdeutlicht werden. Konflikte zwischen verschiedenen Zielen und Möglichkeiten, diese durch technische und rechtliche Maßnahmen zu reduzieren, sollten offen diskutiert werden.

Letztlich wäre die Meinungsbildung und Entscheidungsfindung auch um Fragen und Ziele der Innovationspolitik anzureichern: Gemeinsam mit Entwicklern und Anbietern könnten Strategien entwickelt werden, die auf einen technologischen Sprung vom bisherigen Dokumentenkonzept zu einer Smartcard-basierten Lösung zielen. Hierzu ist ein Blick auf internationale Entwicklungen hilfreich, der zeigt, wie mit einem solchen Konzept mehrere Funktionen zugleich realisierbar wären – wie z.B. die konventionelle Authentifikation und die Nutzung bei Rechtsgeschäften im Internet.

So sind Smartcard-basierte Ausweisdokumente im außereuropäischen Ausland bereits in einigen Ländern umgesetzt worden. Doch auch in Europa gehen Länder mit der Einführung einer so genannten eID-Karte den Weg hin zu elektronischen, Chipkarten-basierten Lösungen. Beispielsweise sind Finnland, Italien, Belgien, Estland und die Schweiz hier bereits aktiv geworden. Hieraus entsteht für Deutschland Handlungsbedarf verbunden mit der Möglichkeit, von der Vorreiterrolle anderer europäischer Länder zu profitieren. Für deutsche Unternehmen, die im internationalen Wettbewerb grundsätzlich gut positioniert sind, könnte ein solches technisch-gesellschaftliches Innovationsprojekt die Perspektive eröffnen, mit eigenen Produkten und Dienstleistungen Wettbewerbsvorteile zu erzielen (B&L 2003).

Als Beispiel für eine Möglichkeit, einen „öffentlichen Diskurs“ zu den genannten Themenaspekten zu gestalten, soll das Verfahren der „öffentlichen Konsultation“ (consultation exercice) genannt werden, das in Großbritannien zur dort geplanten „National IDCard“ über einen Zeitraum von etwa sieben Monaten durchgeführt wurde. Dabei wurden – auf der Basis eines „consultation papers“ der Regierung – Interessenvertreter (stakeholders) um Ihre Meinung und konstruktive Lösungsvorschläge gebeten. Mittels Befragungen und Fokusgruppen wurden die Meinungen und Einstellungen der Bevölkerung erhoben. Das Gesamtergebnis wurde publiziert und zur Diskussion gestellt, um eine bessere Basis für politische Entscheidungen zu haben.

Ein Verfahren wie dieses könnte auch hierzulande geeignet sein, den allgemeinen Informationsstand zu verbessern und ein Bewusstsein für die Bedeutung der Dynamik der gesellschaftlich-technischen Entwicklung zu schaffen, die mit der zukünftig intensiven Nutzung der Biometrie verbunden sein dürfte.

Literatur

1. In Auftrag gegebene Gutachten

B&L (B&L Management Consulting GmbH) (2003): Leistungsfähigkeit biometrischer Identifikationssysteme zur Ausrüstung von Ausweispapieren. Frankfurt/Düsseldorf

STZ (Steinbeis GmbH & Co. KG für Technologietransfer – Steinbeis-Transferzentrum Biometrie und Identifikationslösungen) (2003): Leistungsfähigkeit biometrischer Identifikationssysteme im öffentlichen Bereich: Ausweisdokumente, E-Government. München

ULD-SH (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) (2003): Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen. Kiel

BOOZ ALLEN HAMILTON GMBH, BUNDESDRUCKEREI GMBH, ZN VISION TECHNOLOGIES AG (2003): Leistungsfähigkeit biometrischer Identifikationssysteme zur Ausrüstung von Ausweispapieren. Bochum

2. Weitere Literatur

ALBRECHT, A. (2003): Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz. Baden-Baden

BEHRENS, M., ROTH, R. (2002): BioTrusT: Untersuchung der Akzeptanz und Nutzung biometrischer Identifikations-Verfahren. In: Nolde/Leger 2002, S. 399–419

BIOVISION (2003): Roadmap to Successful Deployment from the User and System Integrator Perspective. Final Report

BONE, M., BLACKBURN D. (Hg.) (2002): Face Recognition at a Chokepoint. Scenario Evaluation Results, DoD Counterdrug Technology Development Program Office, o.O.

BREITENSTEIN, M. (2002): Überblick über biometrische Verfahren. In: Nolde/Leger 2002, S. 35–82

BROMBA, M. (2003): Bioidentifikation. Fragen und Antworten (http://www.bromba.com/faq/biofaqd.htm; zuletzt abgerufen am 27.11.2003)

BSI (Bundesamt für Sicherheit und Informationstechnik) (2001): Newsletter 02.2001 vom 18.06.2001, Bonn

BSI (Bundesamt für Sicherheit und Informationstechnik) (2003): BioFace. Vergleichende Untersuchung von Gesichtserkennungssystemen. Öffentlicher Abschlussbericht BioFace I&II, Bonn

BUNDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ (2003): 19. Tätigkeitsbericht 2001–2002 (http://www.bfd.bund.de/information/tb19/index.html; zuletzt abgerufen am 01.12.2003)

BUNDESRAT (2001): Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz). Drucksache 920/01, Berlin

BUSCH, C., DAUM, H. (2002): Frei von Zweifel? Biometrische Erkennung: Grundlagen, Verfahren, Sicherheit. In: Computermagazin c't Heft 5, S. 156–161

COMPUTERWOCHE (2003): Biometrie scannt Asylbewerber. In: Computerwoche Nr. 4

DHS (U.S. Department of Homeland Security) (2003): First 100 Days of Homeland Security. DHS Announces New ‚US VISIT System' for Travelers as the Department Marks Its First 100 Days. Pressemitteilung vom 29.04.2003 (http://www.whitehouse.gov/news/releases/2003/04/print/20030429-7.html; zuletzt abgerufen am 27.11.2003)

DVD (Deutsche Vereinigung für Datenschutz) (2001): Stellungnahme zu den Ausländer datenschutzrechtlich besonders betreffenden Regelungen des Gesetzentwurfes der Bundesregierung bzw. der Bundestagsfraktionen von SPD und Bündnis 90/DIE GRÜNEN zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 15.11.2001 (http://www.cilip.de/terror/dvd-stell.pdf; zuletzt abgerufen am 27.11.2003)

ENTSCHLIEßUNG DER 63. KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER (2002): Biometrische Merkmale in Personalausweisen und Pässen. 07.03./08.03.2002 (http://www.datenschutz-berlin.de/doc/de/konf/63/bio.htm; zuletzt abgerufen am 20.10.2003)

EUROPÄISCHE KOMMISSION (2003a): Entwicklung einer gemeinsamen Politik in den Bereichen Illegale Einwanderung, Schleuserkriminalität und Menschenhandel, Außengrenzen und Rückführung illegal aufhältiger Personen. KOM(2003)323 endgültig vom 03.06.2003

EUROPÄISCHE KOMMISSION (2003b): Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung (EG) Nr. 1683/95 des Rates über eine einheitliche Visagestaltung. Vorschlag für eine Verordnung des Rates zur Änderung der Verordnung (EG) Nr. 1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige. KOM(2003)558 endgültig vom 24.09.2003

EUROPÄISCHES PARLAMENT (2003): Arbeitsdokument über das Schengener Informationssystem II: künftige Entwicklungen. Ausschuss für Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten, Berichterstatter: Carlos Coelho, PE 329.884

FAA (Federal Aviation Administration) (2001): Fact Sheet. Aviation Security Initiatives Post September 11, November 2001 (http://www1.faa.gov/index.cfm/apa; zuletzt abgerufen am 10.12.2003)

FVC (Fingerprint Verification Competition) (2002): durchgeführt durch Biometric Systems Lab (University of Bologna), U.S. National Biometric Test Center (San Jose State University), Pattern Recognition and Image Processing Laboratory (Michigan State University), BioLab – University of Bologna (2001–2002)

G8 (2003): Final official statement – Presidents' Summary. Evian (http://www.g8.fr/evian/extras/389.pdf; zuletzt abgerufen am 27.11.2003)

GAO (United States General Accounting Office) (2002): Technology Assessment. Using Biometrics for Border Security

GAO (United States General Accounting Office) (2003a): Border Security. Challenges in Implementing Border Technology

GAO (United States General Accounting Office) (2003b): Information Technology. Homeland Security needs to improve entry exit system expenditure planning. Report to Congressional Committees

GARSTKA, H. (2002): Terrorismusbekämpfung und Datenschutz. Zwei Themen im Konflikt. In: Neue Justiz, Heft 10, S. 524–525

HUBER, B. (2002): Die Änderung des Ausländer- und Asylrechts durch das Terrorismusbekämpfungsgesetz. In: NVwZ 2002, Heft 7, S. 787–794

IBG (International Biometric Group) (2003): White House OSTP Biometric Report Brief. A Visa Issuance/Border Crossing Case Study

ICAO (International Civil Aviation Organization) (2003a): Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for Travelling Public. News Release PIO 09/2003 vom 28.05.2003

ICAO (International Civil Aviation Organization) (2003b): Biometrics Development of Machine Readable Travel Documents. Technical Report, Version 1.9 (http://www.icao.int/mrtd/download/technical.cfm; zuletzt abgerufen am 01.12.2003)

INNENAUSSCHUSS (2001): Bericht des Innenausschusses (4. Ausschuss) 1. zu dem Gesetzentwurf der Bundesregierung – Drucksachen 14/7727, 14/7754 – Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), 2. Gesetzentwurf der Fraktionen SPD und Bündnis 90/DIE GRÜNEN – Drucksache 14/7386 (neu) – Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), 3. Antrag der Abgeordneten Wolfgang Bosbach, Volker Rühe, Eckart von Klaeden, weiterer Abgeordneter und der Fraktion der CDU/CSU – Drucksache 14/7065 (neu) – Sicherheit 21 – Was zur Bekämpfung des internationalen Terrorismus jetzt zu tun ist. Deutscher Bundestag, Drucksache 14/7864, Berlin

INTERNATIONALES ARBEITSAMT (2003): Verbesserung der Sicherheit der Personalausweise für Seeleute. Bericht VII (2A) der Internationalen Arbeitskonferenz. 91. Tagung, Genf (http://www.ilo.org/public/german/standards/relm/ilc/ilc91/pdf/rep-vii-2a.pdf; zuletzt abgerufen am 09.12.2003)

KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER (2002): Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen (Positionspapier – AK-Technik) (http://www.datenschutz.mvnet.de/beschlue/63biomet.html; zuletzt abgerufen am 01.12.2003)

LUCIUS, R.v. (2002): Das Profil der Massen. Am Flughafen Reykjavik ist die biometrische Gesichtserkennung schon im Einsatz. In: Frankfurter Allgemeine Zeitung vom 01.08.2002, S. 7

MONTELBAAN INTERNET&ICT (2003): Market Consultation on Use of Biometrics for Dutch Travel Documents. Version 1.0 vom 07.01.2003

NATIONAL DEFENSE MAGAZINE (2001): Pentagon Endorses Biometrics To Enhance Computer Security (http://www.nationaldefensemagazine.org; zuletzt abgerufen am 10.12.2003)

NIST (National Institute for Standards and Security) (2002a): Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability. (ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf; zuletzt abgerufen am 27.11.2003)

NIST (National Institute for Standards and Security) (2002b): Conference Presentations: Patriot Act – Enhanced Border Security Act. (http://www.itl.nist.gov/iad/894.03/fing/pact2002.pdf; zuletzt abgerufen am 27.11.2003)

NOLDE, V., LEGER, L. (Hg.) (2002): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln

NOLTE, M. (2002): Die Anti-Terror-Pakete im Lichte des Verfassungsrechts. In: Deutsches Verwaltungsblatt 117, S. 573–578

NPL (National Physical Laboratory) (2001): Biometric Product Testing. Final Report, Teddington (http://www.otg.ca/news/npl.pdf; zuletzt abgerufen am 27.11.2003)

PROBST, TH. (2002): Biometrie aus datenschutzrechtlicher Sicht, In: Nolde/Leger 2002, S. 115–128

RÖNNEBERG, A. (2003): Der biometrische Reisepass. In: Die Welt vom 19.09.2003

TAB (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag) (2002): Biometrische Identifikationssysteme – Sachstandsbericht (Autoren: Petermann, Th., Sauter, A.). Arbeitsbericht Nr. 76, Berlin

TELETRUST (TeleTrusT Deutschland e.V.) (1998): Kriterienkatalog – Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Arbeitsgruppe 6: Biometrische Identifikationsverfahren, Stand 28.08.1998 (http://www.teletrust.de; zuletzt abgerufen am 10.10.2003)

THE WHITE HOUSE (2003): Securing America's Borders Fact Sheet: Border Security. (http://www.whitehouse.gov/homeland/01.html; zuletzt abgerufen am 27.11.2003)

U.S. DEPARTMENT OF JUSTICE (2003): INS Extends Enrollment Period for SENTRI. Pressemitteilung vom 28.02.2003 (http://www.immigration.com/newsletter1/senins.html; zuletzt abgerufen am 10.12.2003)

U.S. DEPARTMENT OF STATE (2000): Program Performance Report. Fiscal Year 2001, Washington

U.S. DEPARTMENT OF STATE (2002): Program Performance Report. Fiscal Year 2003, Washington

UK SECRETARY OF STATE FOR THE HOME DEPARTMENT (2003): Identity Cards. The Next Steps. (http://www.homeoffice.gov.uk/docs2/identity_cards_next-steps_031111.pdf; zuletzt abgerufen am 01.12.2003)

ULD-SH (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) (2001): Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen. Gutachten für den Deutschen Bundestag, vorgelegt dem Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), Kiel

WEICHERT, TH. (1999): Automatisches Fingerabdruck-Identifizierungssystem – AFIS. In: Datenschutz und Datensicherheit 23, S. 167

WEICHERT, TH. (2002): Datenschutz für Ausländer … nach dem 11. September 2001. In: Datenschutz und Datensicherheit 26, S. 423–428

3. Ausgewählte http-Adressen

http://csrc.nist.gov/cc/
http://dip.bundestag.de/btd/14/073/1407386.pdf
http://europa.eu.int
http://travel.state.gov/bcc.html
http://wg8.de/
http://www.bfd.bund.de
http://www.biometricgroup.com
http://www.biotrust.de/
http://www.bmi.bund.de
http://www.bsi.de
http://www.cesg.gov.uk
http://www.datenschutz.de
http://www.datenschutzzentrum.de
http://www.dhs.gov
http://www.eubiometricforum.com
http://www.face.co.za
http://www.frvt2002.org
http://www.g7.utoronto.ca/
http://www.gao.gov
http://www.homeoffice.gov.uk
http://www.ibgweb.com
http://www.icao.int
http://www.igd.fhg.de
http://www.ilo.org
http://www.legco.gov.hk
http://www.nist.gov
http://www.portfoliopr.com
http://www.senate.gov/
http://www.teletrust.de
http://www.vzbv.de/go/
http://www.whitehouse.gov/homeland/index.html
http://www.wordsun.com

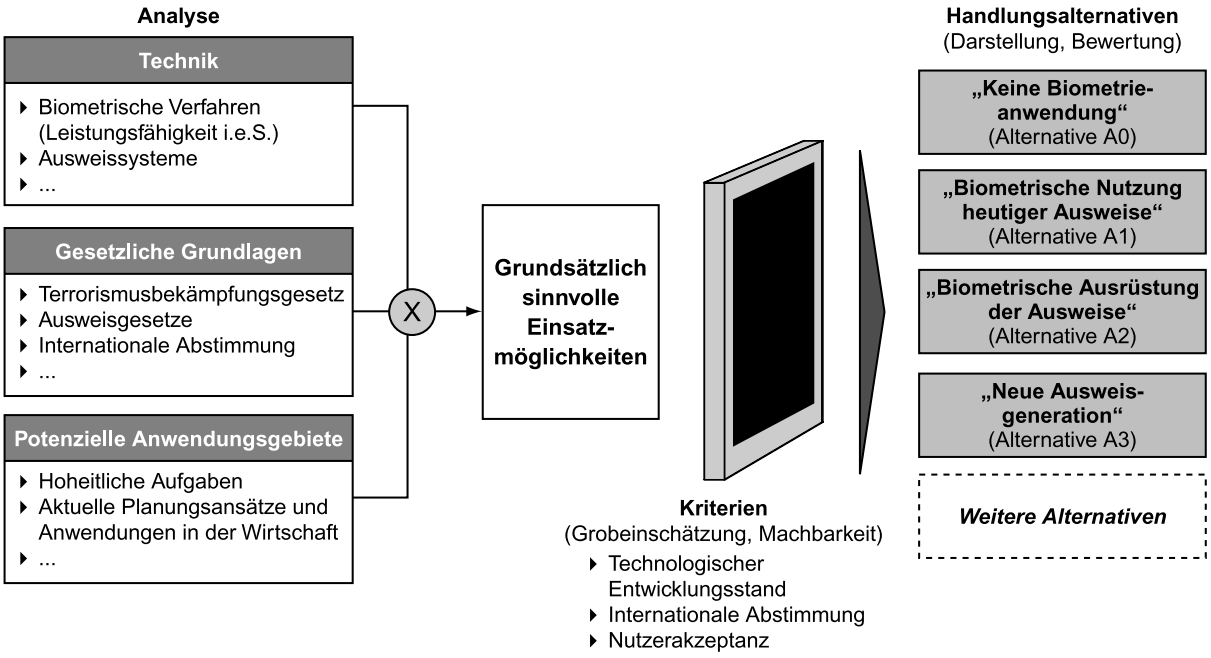
Anhang

1. Kostenmodelle für verschiedene Alternativen (Auszug aus: Booz Allen Hamilton et al. 2003, S. 126–154, geringfügig gekürzt)

1.1 Handlungsalternativen und Bewertungsdimensionen

Vor der in den vorhergehenden Kapiteln beschriebenen Ausgangslage sollen im Folgenden Handlungsalternativen abgeleitet und bewertet werden. Der Detailgrad der Darstellung und Bewertung der Handlungsalternativen orientiert sich an dem Mehrwert, den dieses Gutachten zum jetzigen Zeitpunkt zu der Diskussion um die mögliche Einführung von biometrischen Merkmalen in Ausweispapiere beitragen kann. In diesem Sinne werden neben einer „Basisalternative“ drei grundsätzlich unterschiedliche Möglichkeiten zur Aufnahme von biometrischen Merkmalen in die Ausweisdokumente analysiert. Eine Detaillierung der einzelnen Prozesse, die mit den einzelnen Handlungsalternativen verbunden werden könnten, ist hingegen nicht Gegenstand der folgenden Ausführungen.

Abb. 18: Ableitung von Handlungsalternativen



Quelle: Booz Allen Hamilton et al. 2003

Aus den rechtlichen Grundlagen, der technischen Analyse und den in dieser Studie betrachteten potenziellen Anwendungsgebieten unterscheiden wir die folgenden Handlungsalternativen:

- „Abwarten und Beobachten: Keine Biometrieanwendung“ (Alternative A0)
- „Biometrische Nutzung heutiger Ausweise“ (Alternative A1)
- „Biometrische Ausrüstung der Ausweise“ (Alternative A2)
- „Neue Ausweisgeneration“ (Alternative A3)

Handlungsalternative A2 wird dabei in Folge in zwei Varianten diskutiert:

- Variante A2a „Biometrische Ausrüstung durch Neuerfassung der biometrischen Merkmale in den Meldebehörden“: Neben den Veränderungen in der Ausweisproduktion wird der Beantragungsprozess in den Meldebehörden um den Prozess der Merkmalserfassung und -verarbeitung („Templategenerierung“) erweitert. Es erfolgt also eine dezentrale Merkmalserfassung und Templategenerierung.
- Variante A2b „Biometrische Ausrüstung unter Nutzung bestehender Prozesse“: Der Beantragungsprozess bleibt unverändert, die biometrischen Merkmale werden lokal als Rohdaten (z.B. Foto) in den Meldestellen bzw. Bürgerbüros gesammelt und zur Weiterverarbeitung an die zentrale Produktionsstätte weitergeleitet. Die Veränderungen beschränken sich also auf die Ausweisproduktion, die Templategenerierung erfolgt an zentraler Stelle in der Produktionsstätte.

Die vier Handlungsalternativen werden entlang mehrerer Dimensionen analysiert und bewertet, die aus unserer Sicht die zentralen Kriterien beinhalten, nach denen eine mögliche Entscheidungsfindung stattfinden sollte:

- Zielsetzung
- Technischer Ansatz
- Potenzieller Nutzen
- Rechtliche Rahmenbedingungen
- Kosten und Risiken
- Implementierung

Neben der zentralen Bedeutung der Zielsetzung werden die Unterschiede hinsichtlich der technischen Realisierung dargestellt. Wesentlicher Faktor ist – aus Praktikabilitätsgründen – die äußere Form des Ausweises und die damit verbundenen technischen Möglichkeiten und Limitationen. Der mögliche Nutzen, der sich aus den Handlungsalternativen ergeben kann, umfasst u.a. den Beitrag der neuen Technologie zur öffentlichen Sicherheit und Effizienzsteigerungen in

ausgewählten Anwendungsgebieten. Eine differenzierte Bewertung des Beitrags zur Sicherheit ist dabei prinzipiell schwierig. Dieses Gutachten versucht daher, primär die Unterschiede zwischen den Handlungsalternativen darzustellen – im Gegensatz zu einer abschließenden absoluten Bewertung des „Sicherheitsgewinns“. Die rechtlichen Rahmenbedingungen wurden bereits diskutiert; die für die jeweiligen Handlungsalternativen relevanten Punkte werden in den folgenden Abschnitten zusammengefasst und kommentiert. Soweit es die zu diesem Zeitpunkt noch nicht abgeschlossene Definition der Anforderungen an die möglichen Systeme erlaubt, werden über ein einheitliches Kostenmodell erste – sehr grobe und vorläufige – Abschätzungen mit Bandbreiten für den Finanzbedarf der einzelnen Handlungsalternativen aufgezeigt. Abschließend wird zu jeder der Handlungsalternativen ein Ausblick auf die mögliche Implementierung gegeben, wie z.B. die Notwendigkeit, Pilotprojekte durchzuführen.

1.2 Kostenmodell

Um einen konsistenten Vergleich der Kosten für die einzelnen Handlungsalternativen zu ermöglichen, werden im Folgenden die Kosten getrennt nach

- Ausstellungsebene,
- Produktionsebene und
- Kontrollebene

betrachtet. Die folgenden Kostenabschätzungen beinhalten jeweils nur die Mehrkosten im Vergleich zu den heute existierenden Ausweissystemen. Wenn also z.B. von Kosten für Dokumente mit biometrischen Merkmalen gesprochen wird, dann sind grundsätzlich die Mehrkosten gegenüber den heutigen Ausweisen gemeint. Dabei wird prinzipiell zwischen einmaligen und laufenden Kosten unterschieden, um ein möglichst umfassendes Bild der gesamten Kosten zu zeichnen. Einmalige Kosten entstehen im Zusammenhang mit der Planung, dem Design und der Einführung eines biometrischen Systems, während laufende Kosten aus dem kontinuierlichen Betrieb und der regelmäßigen Wartung und Instandsetzung des Systems folgen. Grundsätzlich werden in diesem Kostenmodell nicht die möglichen Zuständigkeiten seitens der öffentlichen Hand diskutiert, die mögliche Verteilung der Aufwände ist auch nicht Gegenstand der Analyse. In diesem Sinne werden auch keine weiteren Annahmen über eine mögliche Beteiligung der Industrie in der Form von Investments, z.B. für Pilotprojekte, gemacht.

Annahmen (handlungsalternativenübergreifend)

- Für die dezentralen Meldestellen zur Beantragung von Personalausweisen und Reisepässen wird – im Bundesdurchschnitt – von jeweils einem Arbeitsplatz pro 7.500 Einwohner ausgegangen. Bei der Abschätzung der Kosten, die sich im Zusammenhang mit der Einführung biometrischer Systeme ergeben, wird hinsichtlich der Meldestellen (ca. 6.500 bundesweit) nicht zwischen den unterschiedlichen Größen der Ämter unterschieden, sondern es werden grundsätzlich Mittelwerte angenommen.
- Laufende Kosten für die Wartung von Hardware und Software werden pauschal mit 20 % der Anschaffungskosten p.a. angesetzt. Dabei wird – als erste Näherung – nicht zwischen den verschiedenen möglichen Technologien und eventuell unterschiedlichem Wartungsaufwand unterschieden. Dieser Ansatz berücksichtigt, dass die Wartungskosten für ein System, das z.T. auf neuen Technologien aufbaut, erfahrungsgemäß höher liegen als z.B. bei Standard-IT-Lösungen.
- Für Schulungskosten im Rahmen des Enrollments oder der Personenkontrolle, z.B. für die Nutzung von neuen Geräten oder die Umstellung von Arbeitsabläufen, wird ein (mittlerer) Tagessatz von 400 Euro angesetzt.
- Für die Grenzkontrollen an deutschen Flughäfen werden im Folgenden nur die Großflughäfen Frankfurt am Main, München, Düsseldorf, Hamburg, Hannover, Berlin/Tegel und Berlin/Schönefeld betrachtet, über die zusammen 87 % des Fluggastaufkommens im Extra-EU-Verkehr abgewickelt werden (Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften). Die Anzahl der Stationen, an denen an diesen Flughäfen internationale Fluggäste mittels biometrischer Systeme kontrolliert werden, hängt von der – eventuell noch abzuändernden – Gestaltung der Räumlichkeiten vor Ort ab und wird hier mit 200 abgeschätzt.
- Bei der Ausrüstung von Grenzübergängen an Landgrenzen wird von 18 Übergängen zu Polen und zur Tschechischen Republik ausgegangen. Im Schnitt wird jeder Übergang mit ca. drei Erkennungsgeräten ausgestattet werden, um z.B. PKW- und LKW-Kontrollen effizient abwickeln zu können. Neben den Landgrenzen wird auch der Einsatz von biometrischen Erkennungssystemen an deutschen Seehäfen angenommen. Insbesondere für Seehäfen mit intensiverem internationalem Personenverkehr müssten jeweils mehrere Kontrollpunkte eingerichtet werden. Insgesamt wird für die Abschätzung der Mengengerüste und Kosten der einzelnen Handlungsalternativen von 200 Kontrollpunkten an Landgrenzen und Seehäfen ausgegangen.

- Für die unter Alternativen „A2a“ und „A3“ diskutierten Handlungsalternativen, die eine Erfassung der biometrischen Daten in den Meldestellen beinhalten, wird angenommen, dass zur fortlaufenden Administration und zur Betreuung der Hard- und Software der Endgeräte im Durchschnitt mit einem zusätzlichen Personalaufwand von ca. 0,5 FTE („Full Time Equivalent“) pro Meldestelle zu rechnen ist.
- Identifikationssysteme, die auf Basis von biometrischen Merkmalen, z.B. bei Fahndungstätigkeiten, eingesetzt werden könnten, werden nicht betrachtet und damit verbundene Kosten bleiben im Folgenden unberücksichtigt.
- Kosten für eine mögliche Public-Key-Infrastruktur, die ggf. im Zuge der Einführung von biometrischen Merkmalen in Ausweissystemen aufgebaut wird, werden nicht betrachtet, da dieser Aufwand nicht direkt dem biometrischen System zugeordnet werden kann.
- Der zusätzliche Bedarf an Arbeitsfläche beim Enrollment und der Platzbedarf der biometrischen Systeme bei Grenzkontrollen werden hier nicht explizit berücksichtigt, sondern fließen indirekt über die angesetzten jährlichen Betriebs- und Wartungskosten in die Rechnung ein. In Abhängigkeit von spezifischen Lösungsvorschlägen, z.B. für die Grenzkontrolle an Landgrenzen, sollte dieser Punkt in eine spätere, detailliertere Kostenkalkulation mit einbezogen werden.
- Anträge inklusive der Passfotos werden zurzeit dezentral in den Meldestellen verwaltet und verwahrt, um so nach Aushändigung des fertigen Ausweisdokumentes den Ausgabeprozess amtlich nachweisen zu können. Unter der Annahme, dass diese gängige Praxis der dezentralen Aufbewahrung der Ausweisdaten beibehalten wird, müssten zukünftig auch die jeweiligen biometrischen Referenzdaten in den Meldestellen abgelegt werden. Die für die Referenzdatenspeicherung notwendige IT-Infrastruktur existiert aber i.d.R. noch nicht. Demnach wird angenommen, dass die bestehenden Melderegister erweitert werden müssen.
- In allen diskutierten Handlungsalternativen wird davon ausgegangen, dass kein zentrales IT-System und insbesondere keine zentrale Datenbank für biometrische Daten angelegt werden.
- Botschaften, die ebenfalls Dokumente ausstellen und damit auch die für die Erfassung der biometrischen Daten notwendigen Systeme benötigen, werden nicht gesondert betrachtet.
- Für alle Handlungsalternativen (bis auf Alternative A0) wird davon ausgegangen, dass – nicht zuletzt aufgrund des erheblichen technologischen Risikos – zunächst Pilotprojekte durchgeführt werden, die u.a. zur Auswahl

der Lieferanten dienen. Es wird dabei jeweils ein zweistufiges Verfahren angenommen, in dem in einem ersten Schritt die vier biometrischen Verfahren (Fingerabdruck-, Handgeometrie-, Gesichts- bzw. Iriserkennung) mit drei Anbietern oder Bietergemeinschaften getestet werden. In einem zweiten Schritt werden zwei ausgewählte Verfahren mit jeweils zwei Anbietern in einem intensiveren, abschließenden Verfahren getestet.

Kosten für Hard- und Software sind aus marktüblichen Stückpreisen, z.B. für Scanner, Kameras, Sensoren etc. abgeleitet. Neben marktüblichen Kostendaten für „Standard"-Hard- und Software im Bereich Biometrie ist in die Kostenkalkulation Expertenwissen hinsichtlich der zu erwartenden Kosten für die hier diskutierten speziellen Handlungsalternativen eingeflossen. Einerseits ergeben sich Mehrkosten aus Anpassungen der heutigen Geräte für den Einsatz in hoheitlichen Aufgaben. Andererseits sind aufgrund der beachtlichen Größe der möglichen Systeme Skaleneffekte („Volumendiscounts") in Form von geringeren Kosten zu erwarten. Während z.B. für Fingerabdruck-Systeme heute bereits relativ große Stückzahlen von Endgeräten produziert werden und sich dies auch in entsprechenden Preisstrukturen niederschlägt, gibt es zum jetzigen Zeitpunkt deutlich weniger Geräte, die auf der Hand-, Iris- oder Gesichtserkennung basieren. Eine genaue Quantifizierung und die Abschätzung der entsprechenden Unsicherheiten (Lernkurveneffekte, Skalenökonomien) in den Kostenschätzungen gehen jedoch über den Rahmen dieser Studie hinaus.

Die folgende Kostenanalyse und die weitere Detaillierung sind vor dem Hintergrund einer Reihe von Unsicherheiten in der Analyse zu betrachten.

- Heutige Endgerätekosten lassen sich nur bedingt auf eine mögliche Anwendung in Ausweissystemen übertragen. Konkrete Anforderungen an die Systeme sind noch nicht festgelegt und die Auswirkung der technologischen Weiterentwicklung auf Stückkosten und Größenordnungen von Skaleneffekten sind noch nicht vollständig absehbar.
- Die Prozesse der Erfassung der biometrischen Daten (Ausstellungsebene) und insbesondere die Zahl der Meldestellen, in denen die neuen Ausweispapiere beantragt werden können, sind noch nicht definiert. Damit ergeben sich wesentliche Unsicherheiten in den Abschätzungen für den dezentralen Personal- und Schulungsbedarf.
- Der nötige Aufwand für die Erweiterung der Melderegister kann zum jetzigen Zeitpunkt nur grob abgeschätzt werden.
- Der genaue Umfang des Einsatzes von mobilen biometrischen Verifikationssystemen, z.B. im Polizeieinsatz, ist noch offen.

Tab. 15: Übersicht Kostenkomponenten

Bereich	*einmalige Kosten*	*laufende Kosten*
Ausstellungsebene	• Einrichtung Erfassungssystem (HW/SW) • Schulung • Einrichtung Qualitätssicherungssystem (HW/SW) • Erweiterung Melderegister • Erweiterung Datentransfer, DIGANT* • Marketing, Kommunikation • dezentrales Projektmanagement	• Personalkosten Erfassung (zusätzlicher Personalbedarf) • Wartung Erfassungssysteme (HW/SW) • Systempflege Qualitätssicherung • erweiterte Systempflege Melderegister
Produktionsebene	• Modifikation Produktionstechnik Ausweise • Produktentwicklung • Testmaterial	• laufende Dokumentenproduktion (Personalausweise, Reisepässe, Visa) • ggf. Speichertechnologien
Kontrollebene	• Einrichtung Personenkontrollsysteme an Grenzkontrollpunkten (HW, SW) • Schulung • dezentrales Projektmanagement	• Wartung Kontrollsysteme • Personalkosten Personenkontrolle • fortlaufende Schulung
zentrale Koordinierung	• Programm-Management • Auftragsvergabe und Lieferantenmanagement • Vorbereitung/Durchführung Pilotprojekt(e) • QS-Management • Projektsteuerung	• fortlaufendes Programm-Management

* Die Bundesdruckerei bietet seit dem Jahr 2000 das Modul DIGANT für kommunale Einwohnerverfahren an. Mit DIGANT wird eine vereinfachte elektronische Abwicklung des Antragsverfahrens für Pässe und Ausweise ermöglicht. An einem DIGANT-Arbeitsplatz können das Passbild und die Unterschrift mit einem Scanner bei der Antragsstellung digital erfasst werden. Die digitalen Antragsdatensätze werden durch das Einwohnerverfahren automatisch zu einer Bestellung zusammengefasst. An einem Bestellarbeitsplatz, der mit dem D-SAFE-Modul der Bundesdruckerei ausgestattet ist, wird ein elektronisches Bestellformular digital signiert. Die Bestelldaten werden mit starken kryptographischen Verfahren verschlüsselt und über Datenleitungen direkt zur Bundesdruckerei übertragen.

- Die Strategie für einen möglichen Rollout und die entsprechenden Kommunikations- und Marketinginstrumente ist noch unklar.

Für jede der folgenden Handlungsalternativen werden entsprechende Überlegungen hinsichtlich der Unsicherheit in den Abschätzungen der Kosten angestellt. Die folgenden Tabellen fassen die wesentlichen Kostenkomponenten je Alternative zusammen und basieren auf Mittelwerten, die sich aus Bandbreitenabschätzungen für die einzelnen Kosten ergeben. Vor dem Hintergrund der hier genannten Unsicherheiten, die für die jeweiligen Kostenkomponenten Unterschiede von mehr als 50 % bedeuten können, sind die Unterschiede in den Kosten für den Einsatz der verschiedenen biometrischen Verfahren in erster Näherung zu vernachlässigen. Laut einer Studie des United States General Accounting Office (GAO 2002a) beträgt z.B. der Unterschied in den Hardwarekosten für Fingerabdruck-, Iris- und Gesichtserkennungs-Systeme bei Einführung von biometrischen Merkmalen in US-Pässen lediglich ±12 %. Entsprechend steht in dieser Studie bei dem Kostenmodell und der Diskussion der ökonomischen Konsequenzen der einzelnen Handlungsalternativen nicht die Unterscheidung einzelner biometrischer Verfahren im Vordergrund.

1.3 Evaluierung der Handlungsalternativen in den einzelnen Dimensionen

1.3.1 Handlungsalternative „A0“: Abwarten und Beobachten: Keine biometrische Massenanwendung

Neben den folgenden drei Alternativen, die in unterschiedlichen Formen eine konkrete Realisierung biometrischer Ausweise bzw. von Pilotprojekten umfassen, soll zunächst als Alternative „Abwarten und Beobachten“, d.h. kein Einsatz biometrischer Verfahren, betrachtet werden. Der Grundgedanke dieser Alternative ist es, angesichts der Unsicherheiten hinsichtlich der Machbarkeit von biometrischen Massenanwendungen zunächst weitere nationale und internationale Entwicklungen zu beobachten. Dabei sollte laufend zwischen den möglichen Vor- und Nachteilen für Deutschland in der Rolle eines „Nachzüglers“ abgewogen werden.

Prinzipiell ermöglicht diese Handlungsalternative die Minimierung des Risikos von Fehlinvestitionen, z.B. in nicht ausgereifte Technologien und Konzepte. Die zu erwartende Akzeptanz der möglichen Systeme in der Bevölkerung

kann im Laufe der Zeit aus Pilotprojekten ebenfalls besser eingeschätzt werden. Demgegenüber sollte berücksichtigt werden, dass sich hieraus für den Standort Deutschland Nachteile ergeben können, wenn andere Länder oder Regionen in einem so schnell wachsenden Markt wie der Biometrie einen deutlichen Vorsprung erreichen. Beispiele für ähnliche Entwicklungen, in denen staatliche Programme den Aufstieg und Erfolg von Technologien und Branchen vorangetrieben haben, sind z.B. die Internet-Initiativen der USA. Zudem ist zu berücksichtigen, dass Deutschland in der möglichen Rolle eines „Nachzüglers" Standards, die in anderen Ländern und Regionen in der Zwischenzeit gesetzt werden, zumindest zum Teil in eigene Pläne integrieren müsste. Dies kann, z.B. aus datenschutzrechtlicher und kommerzieller Sicht, einen Nachteil für Deutschland darstellen, wenn entsprechende Standards übernommen oder aber unter hohem Kostenaufwand erweitert werden müssten.

Ein externer „Handlungsdruck" könnte sich z.B. durch die Einführung von verbindlichen Standards in den USA ergeben, wenn die visumfreie Einreise für Ausländer – wie bereits diskutiert – nur noch für ausgewählte Länder gelten würde, in deren Ausweisdokumenten standardisierte biometrische Informationen enthalten sind.

Während in dieser ersten Handlungsalternative seitens der öffentlichen Hand keine biometrische Massenanwendung initiiert wird, sind weitere ausgewählte Biometriepilotprojekte und Anwendungen mit geschlossenen Benutzergruppen durchaus denkbar und sinnvoll. Diese sollten z.B. auch Vorhaben beinhalten, die die internationale Zusammenarbeit an konkreten Beispielen vorantreiben. Aus diesen einzelnen Pilotprojekten ist zunächst kein wahrnehmbarer Nutzen für die Gesamtbevölkerung zu erwarten. Es ist jedoch durchaus möglich und sinnvoll, den konkreten Nutzen (z.B. Sicherheits- und Effizienzsteigerungen) in den Pilotprojekten herauszuarbeiten und transparent darzustellen. Daneben ist es vorstellbar, dass mit einer entsprechenden begleitenden Kommunikation die Akzeptanz in der Bevölkerung hinsichtlich der Notwendigkeit und Nutzung von biometrischen Systemen gesteigert wird.

Insgesamt ist – im Vergleich zu den anderen Handlungsalternativen – von einem sehr geringen Finanzbedarf seitens der öffentlichen Hand auszugehen, der im Wesentlichen aus den bestehenden Fördermitteln und -einrichtungen gedeckt werden kann.

1.3.2 Handlungsalternative „A1“: Biometrische Nutzung heutiger Ausweise

Zielsetzung dieser Handlungsalternative ist der Rollout zur flächendeckenden Implementierung von Biometrie in Ausweisanwendungen in Deutschland (nach einem Pilotprojekt). Der technische Ansatz geht dabei davon aus, dass das bereits vorhandene biometrische Merkmal „Gesicht“ in Form des Passfotos vom Ausweis gelesen und gegen das Live-Bild der Person abgeglichen werden kann, ohne dass eine zusätzliche Ausrüstung des Ausweises mit biometrischen Daten erforderlich ist. Neben der automatisierten Verifikation sind auch Überprüfungen gegen Datenbankbilder (z.B. bildbasierte Fahndungslisten oder Visaantragsteller-Datenbank) denkbar. Eine bundesweite Datenbank schließt der Gesetzgeber zum heutigen Zeitpunkt jedoch aus. Als biometrisches Verfahren in dieser Handlungsalternative kommt nur die Gesichtserkennung in Betracht, da für Fingerabdruck-, Iris- oder Handgeometrieerkennung zusätzliche Informationen in die Dokumente aufgenommen werden müssten. Als einzige der Handlungsalternativen, die aktiv die Biometrie vorantreiben, erfordert Alternative A1 keine Veränderung der Ausweise, sondern „nur“ die Implementierung von Endgeräten und entsprechenden Betriebskonzepten, die u.a. eine Optimierung der Lichtbildqualität und eine Überarbeitung ausgewählter Prozesse beinhaltet. Der potenzielle Nutzen, der sich aus der biometrischen Nutzung der heutigen Ausweise ergibt, stellt sich im Wesentlichen in Form einer qualitativ verbesserten Personenkontrolle bei Grenzübergängen dar. Durch einen automatisierten Abgleich des Gesichtes der reisenden Person mit dem Lichtbild im Ausweis kann die bislang rein manuelle Verifikation der Identität erheblich unterstützt werden. Ein vollständiger Ersatz für manuelle Kontrollen, d.h. eine vollständige Automatisierung, wird die Biometrie aus heutiger Sicht wahrscheinlich nicht liefern. Pilotversuche müssen zeigen, inwieweit mit nennenswerten Einsparungen beim Personal an den Grenzkontrollen gerechnet werden kann.

Die rechtlichen Rahmenbedingungen für diese Handlungsalternative sind heute bereits gegeben. Sowohl national als auch international ist das Gesicht in Form des Passfotos festgelegter Standard für Ausweisdokumente. Die Einführung der Technologie kann stufenweise erfolgen, da die manuelle Verifikation der Identität auf Basis der Passfotos weiterhin möglich ist.

Die wesentlichen Kostenkomponenten für die einmalige Einrichtung und den fortlaufenden Betrieb des Systems sind in den folgenden Tabellen 16 und 17 dargestellt.

Tab. 16: Abschätzung der einmaligen Kosten – Handlungsalternative A1 (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem			5.200.000		5.200.000
Qualitätssicherung					0
Melderegister					0
Marketing, Kommunikation				53.333	53.333
Projektmanagement, dezentral					0
Ausstellungsebene	**0**	**0**	**5.200.000**	**53.333**	**5.253.333**
Produktion Ausweisdokumente					0
Speichermedien, Chiptechnologien					0
Produktionsebene, Dokumentensystem	**0**	**0**	**0**	**0**	**0**
Personenkontrolle Flughafen	4.000.000		1.600.000		5.600.000
Personenkontrolle an deutschen Landgrenzen	3.000.000		1.200.000		4.200.000
sonstige Personenkontrollen; mobiler Einsatz					0
Kontrollebene	**7.000.000**	**0**	**2.800.000**	**0**	**9.800.000**
Projektmanagement, Koordinierung		472.500		2.000.000	2.472.500
Beratung, Konzeption, Fachkonzepte				600.000	600.000
Ausschreibung				800.000	800.000
Pilotprojekte, 4 Verfahren à 3 Hersteller, Phase 1				1.200.000	1.200.000
Pilotprojekte, 2 Verfahren à 2 Hersteller, Phase 2				1.200.000	1.200.000
zentrale Koordinierung	**0**	**472.500**	**0**	**5.800.000**	**6.272.500**
einmalige Kosten, Einführung	**7.000.000**	**472.500**	**8.000.000**	**5.853.333**	**21.325.833**

Tab. 17: Abschätzung der laufenden Kosten – Handlungsalternative A1 (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem					0
Qualitätssicherung		630.000			630.000
Melderegister					0
Marketing, Kommunikation					0
Projektmanagement, dezentral					0
Ausstellungsebene	**0**	**630.000**	**0**	**0**	**630.000**
Produktion Ausweisdokumente PA					0
Produktion Ausweisdokumente RP					0
Produktion Ausweisdokumente Visa					0
Speichermedien PA					0
Speichermedien RP					0
Produktionsebene, Dokumentensystem	**0**	**0**	**0**	**0**	**0**
Personenkontrolle Flughafen	800.000		1.000.000		1.800.000
Personenkontrolle an deutschen Grenzen	600.000		1.000.000		1.600.000
sonstige Personenkontrollen; mobiler Einsatz			500.000		500.000
Kontrollebene	**1.400.000**	**0**	**2.500.000**	**0**	**3.900.000**
laufende Kosten p.a., Betrieb	**1.400.000**	**630.000**	**2.500.000**	**0**	**4.530.000**

Für die einmalige Einrichtung des Systems resultieren die Kosten von 21,3 Mio. Euro im Wesentlichen aus den Kosten für Endgeräte an den Grenzübergängen, der Schulung des Personals für diese Geräte sowie für die Pilotierung und zentrale Koordinierung des Projektes. Dabei wird angenommen, dass neben den sieben Großflughäfen zusätzlich 200 Landgrenzen und Seehäfen mit biometrischen Erkennungsgeräten, d.h. für diese Handlungsalternative mit Gesichtserkennungsgeräten, ausgestattet werden. Die Kosten für Geräte im Außeneinsatz, die z.B. gegen Witterung und Diebstahl geschützt werden müssen, werden in-

klusive einmaliger Installation und eventueller Baumaßnahmen mit 20.000 Euro pro Kontrollpunkt abgeschätzt. Für Kontrollpunkte innerhalb von Gebäuden ist entsprechend von einem geringeren Aufwand auszugehen, und es werden jeweils 15.000 Euro pro Kontrollpunkt angesetzt.

Sowohl an den Flughäfen als auch an den Landgrenzen und Seehäfen muss das Grenzpersonal im Umgang mit den neuen Systemen geschult und entsprechende Änderungen bzw. Ergänzungen in Schulungsunterlagen und Richtlinien vorgenommen werden. Dabei ist bei der höheren Anzahl der Grenzkontrollen an Flughäfen im Vergleich zu Seehäfen und entsprechender Unterschiede im Personalbedarf von unterschiedlichen Kosten pro Kontrollpunkt und damit von unterschiedlichen Gesamtkosten auszugehen. Für die Durchführung von Pilotversuchen für die biometrischen Systeme werden in einem ersten Schritt pro Anbieter 100.000 Euro und für einen detaillierteren zweiten Schritt 300.000 Euro angenommen.

Die laufenden Kosten für die Nutzung der heutigen Ausweise mithilfe automatischer Gesichtserkennung ergeben sich zum größten Teil aus der fortlaufenden Schulung des Personals an den Landesgrenzen, aber auch aus der Schulung von Beamten und Angestellten, z.B. für Fahndungstätigkeiten.

Aus finanzieller Sicht ergeben sich wesentliche Unsicherheiten für die hier dargestellte grobe Kostenabschätzung, u.a. aufgrund der folgenden Punkte:

- Die Kosten für Hard- und Software lassen sich aus den heute vorliegenden Herstellerangaben nur schwer auf eine mögliche Massenanwendung projizieren.
- Der genaue Aufwand für Schulungen hängt von dem Einführungskonzept und insbesondere dem angestrebten Zeitrahmen ab.
- Der Aufwand für „Marketing“ und Kommunikation ist zurzeit nur schwer abzuschätzen und wird nicht zuletzt durch mögliche Akzeptanzprobleme bei Angestellten oder Reisenden bestimmt.

Für diese Handlungsalternative A1 ergeben sich aus Kostensicht die größten Unsicherheiten aus dem Umfang und der Qualität der Ausstattung der Kontrollstellen mit Biometrieendgeräten. So ergeben sich z.B. bei der Annahme von Unsicherheiten in den Kosten für Hard- und Software sowie der Anzahl der Kontrollstellen von 10 % ca. 2,2 Mio. Euro an einmaligen und ca. 0,3 Mio. Euro an laufenden Kosten.

Mit der heute zur Verfügung stehenden Technologie kann diese Handlungsalternative „A1“ im Prinzip unmittelbar realisiert werden. Eine zweistufige Pilotierung der Anwendung wäre mit begrenztem Kostenaufwand von etwa

2,4 Mio. Euro durchführbar und würde mögliche Risiken der Einführung weiter reduzieren. Im Vergleich zu den folgenden Alternativen spielt für die biometrische Nutzung heutiger Ausweise die Umweltbetrachtung oder Szenarioanalyse aufgrund der relativ sicheren Entscheidungsgrundlagen eine untergeordnete Rolle. Der Nutzen ist insgesamt kurz- bis mittelfristig realisierbar.

1.3.3 Handlungsalternative „A2“: Biometrische Ausrüstung der heutigen Ausweise

Mit der „Ausrüstung“ der heutigen Ausweise wird in diesem Gutachten die Einbindung von zusätzlichen biometrischen Daten in Personalausweise, Reisepässe bzw. Visa verstanden, ohne dabei die wesentlichen äußeren Merkmale und die Erscheinungsform der Dokumente zu ändern. Das bedeutet, dass die bestehenden Herstellungsprozesse für die Dokumente geändert, aber nicht grundlegend neu konzipiert werden müssten. Die „Dokumentenfamilie“ bliebe bestehen. Mit dieser Handlungsalternative ist das Ziel verbunden, die Qualität der Personenkontrollen – insbesondere bei Grenzübertritten – durch die automatische Überprüfung biometrischer Merkmale (Fingerabdruck, Handgeometrie, Gesicht, Irismuster) zu steigern, ohne sich dabei dem zusätzlichen Aufwand der Einführung einer vollständig neuen Dokumentengeneration auszusetzen. Die Ausrüstung der bestehenden Ausweisgeneration mit zusätzlichen biometrischen Daten könnte über optisch lesbare Speichermedien wie 2D-Barcodes oder Hologramme erfolgen. Für den Personalausweis in seiner heutigen Form ist darüber hinaus die Einführung von (dünnen) kontaktlosen Chips (Transponder), die von Leseterminals gelesen werden können, technisch machbar. Entsprechend der Zielsetzung dieser Handlungsalternative sollte die Veränderung der Ausstellungs- und Produktionsprozesse für die Ausrüstung der Ausweise so gering wie möglich ausfallen, d.h. bei der Ausarbeitung des Feinkonzeptes sollte weitestgehend auf Verwendung bestehender Prozesse und Technologien zurückgegriffen werden. Prinzipiell sind alle vier der hier näher betrachteten biometrischen Verfahren mit dieser Handlungsalternative A2 realisierbar. Die rechtlichen Rahmenbedingungen sind durch das Terrorismusbekämpfungsgesetz gegeben, wobei zu beachten ist, dass die Iris nicht explizit im Wortlaut des Gesetzes verankert ist und hier eventueller rechtlicher Handlungsbedarf geklärt werden müsste.

Im Gegensatz zu Handlungsalternative A1, d.h. der biometrischen Analyse der heutigen Ausweise, sind mit der Ausrüstung der Dokumente und der Erfassung der zusätzlichen Merkmale zusätzliche Kosten – sowohl einmalige wie

laufende – verbunden. Die Tabellen 18–21 fassen unter den oben diskutierten Annahmen die wesentlichen Kostenkomponenten zusammen. Dabei wird in der Variante A2a dieser Handlungsalternative davon ausgegangen, dass die Erfassung und Verarbeitung der biometrischen Merkmale („Templategenerierung“) der Bürger dezentral, d.h. in den Meldestellen erfolgt. Prinzipiell sind für die Verfahren Fingerabdruck- und Gesichtserkennung auch eine Beibehaltung des bisherigen Beantragungsprozesses und die Verlagerung der Templategenerierung an eine zentrale Stelle, z.B. die Produktionsstätte, möglich. Dabei würden die dezentral aufgenommenen Bilder der Fingerabdrücke oder der Gesichter als „Rohdaten“ auf konventionellen oder elektronischen Wegen zu einer zentralen Stelle übertragen, die die Erzeugung der Templates übernimmt. Die Kostenkonsequenzen daraus werden in einer Variante A2b dargestellt.

Die einmaligen und laufenden Kosten für das Erfassungssystem, die Qualitätssicherung und die Erweiterung der Melderegister hängen in hohem Maße davon ab, ob die biometrischen Templates dezentral in den Meldestellen (A2a) oder an zentraler Stelle (A2b) erzeugt werden. Bei einer dezentralen Erfassung in der Ausstellungsebene ist von zusätzlichen Hardware- und Softwarekosten von ca. 400 Mio. Euro auszugehen, die im Falle einer Erzeugung der Templates an zentraler Stelle nicht anfallen würden.

Die einmaligen Kosten von ca. 614 Mio. Euro für Alternative A2a setzen sich hauptsächlich aus den Kosten für Hardware und Software für die Ausstellungsebene zusammen, d.h. für Endgeräte, das Qualitätssicherungssystem und die Erweiterung der Melderegister. Bei den Kosten für Endgeräte wird in dieser Kalkulation nicht explizit zwischen den einzelnen biometrischen Verfahren unterschieden, da aus heutiger Sicht die Preisunterschiede zwischen den Verfahren (bei Annahme einer ähnlichen oder der gleichen Qualität) deutlich geringer sind als die finanziellen Unsicherheiten, die sich insgesamt in dem Kostenmodell ergeben, insbesondere im Hinblick auf das Mengengerüst für die Ausstellungs- oder Kontrollebene und die Frage nach dem Umfang der Erweiterung des Melderegisters.

Tab. 18: Abschätzung der einmaligen Kosten – Handlungsalternative A2a (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem	106.666.667		10.400.000		117.066.667
Qualitätssicherung	65.000.000				65.000.000
Melderegister	227.500.000				227.500.000
Marketing, Kommunikation				80.000.000	80.000.000
Projektmanagement, dezentral		40.950.000			40.950.000
Ausstellungsebene	**399.166.667**	**40.950.000**	**10.400.000**	**80.000.000**	**530.516.667**
Produktion Ausweisdokumente	10.000.000				10.000.000
Speichermedien, Chiptechnologien	15.000.000				15.000.000
Produktionsebene, Dokumentensystem	**25.000.000**	**0**	**0**	**0**	**25.000.000**
Personenkontrolle Flughafen	3.000.000		1.600.000		4.600.000
Personenkontrolle an deutschen Landgrenzen	4.000.000		800.000		4.800.000
sonstige Personenkontrollen; mobiler Einsatz	24.000.000				24.000.000
Kontrollebene	**31.000.000**	**0**	**2.400.000**	**0**	**33.400.000**
Projektmanagement, Koordinierung		2.835.000		12.000.000	14.835.000
Beratung, Konzeption, Fachkonzepte, …				2.000.000	2.000.000
Ausschreibung				1.600.000	1.600.000
Pilotprojekte, 4 Verfahren à 3 Hersteller, Phase 1				2.400.000	2.400.000
Pilotprojekte, 2 Verfahren à 2 Hersteller, Phase 2				4.000.000	4.000.000
zentrale Koordinierung	**0**	**2.835.000**	**0**	**22.000.000**	**24.835.000**
einmalige Kosten, Einführung	**455.166.667**	**43.785.000**	**12.800.000**	**102.000.000**	**613.751.667**

Tab. 19: Abschätzung der einmaligen Kosten – Handlungsalternative A2b (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem			5.200.000		5.200.000
Qualitätssicherung					0
Melderegister					0
Marketing, Kommunikation				80.000.000	80.000.000
Projektmanagement, dezentral		10.237.500			10.237.500
Ausstellungsebene	**0**	**10.237.500**	**5.200.000**	**80.000.000**	**95.437.500**
Produktion Ausweisdokumente	10.000.000				10.000.000
Speichermedien, Chiptechnologien	15.000.000				15.000.000
Produktionsebene, Dokumentensystem	**25.000.000**	**0**	**0**	**0**	**25.000.000**
Personenkontrolle Flughafen	3.000.000		1.600.000		4.600.000
Personenkontrolle an deutschen Landgrenzen	4.000.000		800.000		4.800.000
sonstige Personenkontrollen; mobiler Einsatz	24.000.000				24.000.000
Kontrollebene	**31.000.000**	**0**	**2.400.000**	**0**	**33.400.000**
Projektmanagement, Koordinierung		2.835.000		12.000.000	14.835.000
Beratung, Konzeption, Fachkonzepte, …				2.000.000	2.000.000
Ausschreibung				1.600.000	1.600.000
Pilotprojekte, 4 Verfahren à 3 Hersteller, Phase 1				2.400.000	2.400.000
Pilotprojekte, 2 Verfahren à 2 Hersteller, Phase 2				4.000.000	4.000.000
zentrale Koordinierung	**0**	**2.835.000**	**0**	**22.000.000**	**24.835.000**
einmalige Kosten, Einführung	**56.000.000**	**13.072.500**	**7.600.000**	**102.000.000**	**178.672.500**

Tab. 20: Abschätzung der laufenden Kosten – Handlungsalternative A2a (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem	21.333.333	204.750.000			226.083.333
Qualitätssicherung	16.250.000	630.000			16.880.000
Melderegister	34.125.000				34.125.000
Marketing, Kommunikation					0
Projektmanagement, dezentral					0
Ausstellungsebene	**71.708.333**	**205.380.000**	**0**	**0**	**277.088.333**
Produktion Ausweisdokumente PA	18.000.000			315.000	18.315.000
Produktion Ausweisdokumente RP	9.000.000				9.000.000
Produktion Ausweisdokumente Visa	5.000.000				5.000.000
Speichermedien PA	9.000.000				9.000.000
Speichermedien RP	4.500.000				4.500.000
Speichermedien Visa	2.500.000				2.500.000
Produktionsebene, Dokumentensystem	**48.000.000**	**0**	**0**	**315.000**	**48.315.000**
Personenkontrolle Flughafen	600.000				600.000
Personenkontrolle an deutschen Grenzen	800.000				800.000
sonstige Personenkontrollen; mobiler Einsatz	4.800.000				4.800.000
Kontrollebene	**6.200.000**	**0**	**0**	**0**	**6.200.000**
laufende Kosten p.a., Betrieb	**125.908.333**	**205.380.000**	**0**	**315.000**	**331.603.333**

Von den einzelnen Komponenten der laufenden Kosten spielen unter den gegebenen Annahmen die Betriebs- und Wartungskosten für die Hardware und Software in den Meldestellen und für das Qualitätssicherungssystem die größte Rolle. Insgesamt ergeben sich Kosten von ca. 331 Mio. Euro p.a. für Alternative A2a. Für die zusätzlichen Kosten in der Produktion der Ausweise, die sich aus der Einbindung zusätzlicher biometrischer Daten ergeben, wird von zwei bis

drei Euro pro Dokument ausgegangen. Dabei wird im Sinne einer aus finanzieller Sicht konservativen Betrachtung bereits von der teureren Variante der Einbindung eines elektronischen kontaktlosen Transponders ausgegangen.

Tab. 21: Abschätzung der laufenden Kosten – Handlungsalternative A2b (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem					0
Qualitätssicherung		630.000			630.000
Melderegister					0
Marketing, Kommunikation					0
Projektmanagement, dezentral					0
Ausstellungsebene	**0**	**630.000**	**0**	**0**	**630.000**
Produktion Ausweisdokumente PA	18.000.000			315.000	18.315.000
Produktion Ausweisdokumente RP	9.000.000				9.000.000
Produktion Ausweisdokumente Visa	5.000.000				5.000.000
Speichermedien PA	9.000.000				9.000.000
Speichermedien RP	4.500.000				4.500.000
Speichermedien Visa	2.500.000				2.500.000
Produktionsebene, Dokumentensystem	**48.000.000**	**0**	**0**	**315.000**	**48.315.000**
Personenkontrolle Flughafen	600.000				600.000
Personenkontrolle an deutschen Grenzen	800.000				800.000
sonstige Personenkontrollen; mobiler Einsatz	4.800.000				4.800.000
Kontrollebene	**6.200.000**	**0**	**0**	**0**	**6.200.000**
laufende Kosten p.a., Betrieb	**54.200.000**	**630.000**	**0**	**315.000**	**55.145.000**

Unsicherheiten in den Kostenabschätzungen resultieren vor allem aus der noch nicht abschließend geklärten Anzahl der Meldestellen, an denen die Bürgerin-

nen und Bürger einen neuen (biometrischen) Ausweis beantragen können sowie den Kosten für Endgeräte. So ergeben sich z.B. aus einer Variation der Anzahl der Meldestellen von 10 % bereits Unterschiede von ca. 45 Mio. Euro in den einmaligen Kosten. Einen vergleichbar hohen Einfluss haben die Hardware-Stückkosten innerhalb des Kostenmodells: Auch hier ergeben Schwankungen von z.B. 10 % Kostenunterschiede von mehr als 40 Mio. Euro.

Aus technischer Sicht ist die Veränderung der Produktionsprozesse zur Ausrüstung der Ausweisdokumente relativ kurzfristig, d.h. in einem Entscheidungs- und Projekthorizont von zwei bis drei Jahren zu realisieren. Dabei ist in dieser Zeit – wie in der obigen Kostenbetrachtung – bereits ein zweistufiges Auswahlverfahren hinsichtlich der Anbieter und der Durchführung von Pilotprojekten enthalten.

1.3.4 Handlungsalternative „A3“: Einführung einer neuen Ausweisgeneration

Mit dieser Handlungsalternative soll die Entwicklung und Einführung einer neuen Ausweisgeneration, d.h. eines Chip-basierten digitalen Dokumentes – zumindest in Ansätzen und soweit es die biometrischen Verfahren betrifft – diskutiert werden.

Mit einer solchen Einführung wäre die Zielsetzung verbunden, für die Bundesbürger ein Dokument bereitzustellen, das ihnen nicht nur die konventionelle Authentifikation erlaubt, sondern auch als Eckpfeiler einer elektronischen Unterschrift für den elektronischen Geschäftsverkehr einsetzbar wäre. Es ist an dieser Stelle zu bemerken, dass mit der Einführung einer neuen Generation von digitalen Personalausweisen bzw. Reisepässen zunächst nur deutsche Staatsbürger in den Besitz eben dieser Ausweise kämen. Es ist sinnvoll und wünschenswert, auch den in Deutschland lebenden ausländischen Bürgern den Zugang zu einer entsprechenden digitalen Karte zu ermöglichen, die z.B. für die elektronische Unterschrift eingesetzt werden kann. Hiermit verbundene Aufwände bzw. Verrechnungsmodelle sind in dem vorliegenden Gutachten und insbesondere in der Kostenanalyse nicht berücksichtigt. Im Fokus dieser Handlungsalternative steht also neben einer möglichen Erhöhung der öffentlichen Sicherheit durch verbesserte, teilautomatisierte Verifikationsverfahren via Biometrie auch der Anstoß von technischen Innovationen in Deutschland und die Erhöhung der Attraktivität des Landes als Wirtschaftsstandort. Dabei kommen zu den Überlegungen, die bereits im Rahmen der vorhergehenden Handlungs-

alternativen diskutiert wurden, weitere Kostenargumente und organisatorische wie rechtliche Herausforderungen hinzu.

Der Beitrag, der durch diese Handlungsalternative A3 zur Erhöhung der öffentlichen Sicherheit geleistet wird, unterscheidet sich dabei nicht von der vorhergehenden Alternative A1 und A2, d.h. der biometrischen Nutzung oder der biometrischen Ausrüstung der bestehenden Ausweisgeneration. Die biometrischen Daten werden elektronisch verschlüsselt auf dem im Dokument integrierten Chip gespeichert und zu Verifikationszwecken mit den Live-Merkmalen an der Person verglichen. Der heutige Stand der Chipkarten-Technologie bietet in Kombination mit den in diesem Gutachten diskutierten Verfahren prinzipiell die Voraussetzungen zu einer erfolgreichen Umsetzung.

Die Kosten für eine mögliche Einführung können zum jetzigen Zeitpunkt und im Rahmen dieser Studie nur grob abgeschätzt werden und hängen in erheblichem Umfang von den genauen technischen und organisatorischen Anforderungen an das Gesamtsystem ab. Analog zu den Erläuterungen der Handlungsalternative A2 wird auf die möglichen Kostenunterschiede zwischen den einzelnen biometrischen Verfahren nicht detailliert eingegangen.

Die Kostenabschätzung in Tabelle 22 zeigt, dass sich die einmaligen Kosten für die Einführung einer neuen Ausweisgeneration von ca. 669 Mio. Euro zu wesentlichen Teilen aus der Hardware und Software für die Erfassungs- und Qualitätssicherungssysteme sowie für das Melderegister ergeben. Um den Nutzen der „neuen Karte“ für den Bürger transparent zu machen und entsprechende Aufmerksamkeit – auch mit Hinblick auf privatwirtschaftliche Anwendungen – zu erzeugen, ist von einem erheblichen Aufwand für Marketing und Kommunikation auszugehen.

Seitens der Produktion der Ausweise müssen neue Verfahren implementiert und entsprechende einmalige Investitionen in Herstellungsverfahren getätigt werden. Hier ist – in einer ersten sehr groben und vorläufigen Schätzung – von einer finanziellen Größenordnung von ca. 60–80 Mio. Euro auszugehen. Für eine mögliche Implementierung wird, wie bei den vorhergehenden Handlungsalternativen, eine zweistufige Pilotphase angenommen, wobei der Finanzbedarf aufgrund der höheren Komplexität der Lösung mit 6,4 Mio. Euro etwas höher abgeschätzt wurde.

Die laufenden Kosten, die sich aus der Einführung einer neuen Ausweisgeneration ergeben, sind in Tabelle 23 zusammengefasst. Insgesamt ergibt sich ein zusätzlicher Finanzbedarf gegenüber dem heute bestehenden System von ca. 610 Mio. Euro p.a.

Tab. 22: Abschätzung der einmaligen Kosten – Handlungsalternative A3 (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem	106.666.667		10.400.000		117.066.667
Qualitätssicherung	65.000.000				65.000.000
Melderegister	227.500.000				227.500.000
Marketing, Kommunikation				80.000.000	80.000.000
Projektmanagement, dezentral		40.950.000			40.950.000
Ausstellungsebene	**399.166.667**	**40.950.000**	**10.400.000**	**80.000.000**	**530.516.667**
Produktion Ausweisdokumente	60.000.000				60.000.000
Speichermedien, Chiptechnologien	20.000.000				20.000.000
Produktionsebene, Dokumentensystem	**80.000.000**	**0**	**0**	**0**	**80.000.000**
Personenkontrolle Flughafen	3.000.000		1.600.000		4.600.000
Personenkontrolle an deutschen Landgrenzen	4.000.000		800.000		4.800.000
sonstige Personenkontrollen; mobiler Einsatz	24.000.000				24.000.000
Kontrollebene	**31.000.000**	**0**	**2.400.000**	**0**	**33.400.000**
Projektmanagement, Koordinierung		2.835.000		12.000.000	14.835.000
Beratung, Konzeption, Fachkonzepte				2.000.000	2.000.000
Ausschreibung				1.600.000	1.600.000
Pilotprojekte, 4 Verfahren à 3 Hersteller, Phase 1				2.400.000	2.400.000
Pilotprojekte, 2 Verfahren à 2 Hersteller, Phase 2				4.000.000	4.000.000
zentrale Koordinierung	**0**	**2.835.000**	**0**	**22.000.000**	**24.835.000**
einmalige Kosten, Einführung	**510.166.667**	**43.785.000**	**12.800.000**	**102.000.000**	**668.751.667**

Tab. 23: Abschätzung der laufenden Kosten – Handlungsalternative A3 (in Euro)

	Hardware, Software	*Personal*	*Schulung*	*Sonstige*	*gesamt*
Erfassungssystem	21.333.333	204.750.000			226.083.333
Qualitätssicherung	16.250.000	630.000			16.880.000
Melderegister	34.125.000				34.125.000
Marketing, Kommunikation					0
Projektmanagement, dezentral					0
Ausstellungsebene	**71.708.333**	**205.380.000**	**0**	**0**	**277.088.333**
Produktion Ausweisdokumente PA	180.000.000			315.000	180.315.000
Produktion Ausweisdokumente RP	90.000.000				90.000.000
Produktion Ausweisdokumente Visa	5.000.000				5.000.000
Speichermedien PA	45.000.000				45.000.000
Speichermedien RP	9.000.000				9.000.000
Speichermedien Visa	2.500.000				2.500.000
Produktionsebene, Dokumentensystem	**331.500.000**	**0**	**0**	**315.000**	**331.815.000**
Personenkontrolle Flughafen	600.000				600.000
Personenkontrolle an deutschen Grenzen	800.000				800.000
sonstige Personenkontrollen; mobiler Einsatz					0
Kontrollebene	**1.400.000**	**0**	**0**	**0**	**1.400.000**
laufende Kosten p.a., Betrieb	**404.608.333**	**205.380.000**	**0**	**315.000**	**610.303.333**

Ähnlich wie bei der Handlungsalternative A2 ergeben sich zum jetzigen Zeitpunkt auch für die Einführung einer neuen Ausweisgeneration wesentliche Unsicherheiten hinsichtlich des zu erwartenden Kostenrahmens. Die wichtigsten Einflussfaktoren innerhalb des hier betrachteten Rahmens sind die Kosten für Hard- und Software sowie die Anzahl der Meldestellen, die mit biometrischen Erfassungsgeräten ausgestattet werden sollen. So machen auch hier z.B. Unter-

schiede von 10 % in den Kosten und der Anzahl der Meldestellen bereits Unterschiede von jeweils mehr als 40 Mio. Euro aus. Im Vergleich hierzu hat der Umfang der Ausrüstung der Kontrollstellen (z.B. Flughäfen, Landesgrenzen) mit Endgeräten einen deutlich geringeren Einfluss auf die Gesamtkosten.

1.4 Vergleichende Bewertung der Handlungsalternativen und Fazit

Zahlreiche Pilotprojekte, aber auch konkrete Einsätze im nicht hoheitlichen Bereich belegen, dass durch den Einsatz biometrischer Verfahren eine Erhöhung der Sicherheit und Effizienzsteigerungen erreicht werden können. Welche der vier in diesem Gutachten näher beleuchteten Technologien für den Einsatz in Ausweisdokumenten am besten geeignet ist, muss unter Berücksichtigung der gewünschten und erzielbaren Nutzen und Effekte eingehend analysiert werden. Die Bewertungsgrundlage für die zu berücksichtigenden Faktoren ist mit diesem Gutachten geschaffen worden. Denkbar ist neben dem Einsatz eines biometrischen Verfahrens auch eine Kombination aus mehreren Technologien, z.B. von Gesichts- und Fingerabdruckerkennung. Bezüglich der Verwendung in Ausweispapieren ist allerdings festzuhalten, dass als einzige Technologie die Gesichtserkennung auf die Verwendung eines bereits in den Dokumenten enthaltenen biometrischen Merkmals – nämlich das Gesicht in Form des Passfotos – abzielt und damit im Hinblick auf die Implementierung attraktive Vorteile genutzt werden können.

Während die technologische Leistungsfähigkeit der Verfahren im Großen und Ganzen belegt ist, ist die Nutzerakzeptanz heute bei großflächigen Anwendungen nur bedingt abschätzbar. Es ist beispielsweise nicht klar, wie die große Mehrheit der Bürger reagiert, wenn bei jedem Grenzübertritt ein Fingerabdruck oder ein Foto der Person abgenommen wird bzw. erheblicher Kooperationsaufwand zur Erfassung, z.B. des Irismusters, erforderlich ist. Die Akzeptanz des breiten Einsatzes biometrischer Verfahren kann durch Marktforschungs- bzw. reine Pilotprojekte mit einigen hundert Teilnehmern nur bedingt eingeschätzt werden. Hier besteht für den Staat – sofern er sich mit dem Gedanken eines großflächigen Einsatzes trägt – ein Restrisiko.

Datenschutzrechtlich ist der Einsatz von biometrischen Merkmalen zumindest in Deutschland im Rahmen des Terrorismusbekämpfungsgesetzes dann abgedeckt, wenn eine biometrische Verifikationsanwendung („1:1-Vergleich“) mit dezentraler Datenhaltung auf dem Ausweismedium erfolgt und somit keine

Abgleiche mit einer zentral gehaltenen Datenbank vorgenommen werden. Solange der Nutzer „im Besitz“ seiner Daten bleibt und die Verwendung der Daten für ihn transparent ist, ist gegen den Einsatz biometrischer Merkmale aus (datenschutz-)rechtlicher Sicht nichts einzuwenden. Berücksichtigt man – wie dies der Bundesdatenschutzbeauftragte fordert – das Prinzip der sparsamen Datenerfassung, so sollte eine optimale Nutzung der heute schon bestehenden Merkmale Vorrang vor einer Erfassung zusätzlicher biometrischer Merkmale haben.

Das Gutachten skizziert grob vier Handlungsalternativen (mit einer weiteren Aufgliederung der Handlungsalternative 2), die dem deutschen Staat beim Einsatz biometrischer Verfahren im Ausweiswesen zur Verfügung stehen. Ausgangspunkt ist dabei die Handlungsalternative „Kein Einsatz biometrischer Verfahren“, die eine rein passive, abwartende Haltung des Staates charakterisiert. Kosten und Nutzen der anderen Handlungsalternativen müssen jeweils gegenüber dieser Alternative A0 („Abwarten und Beobachten: Keine Biometrieanwendung“) gemessen werden.

Die vier Handlungsalternativen unterscheiden sich erheblich in ihrer Investitionsintensität. Tabelle 24 fasst die wesentlichen Eckdaten der Kostenabschätzung zusammen. Es wird dabei zwischen einmaligen Investitionen und laufenden Aufwendungen unterschieden. Die Werte sind jeweils mit Bandbreiten von +/- 50 % zu verstehen.

Tab. 24: Zusammenfassung Kostenabschätzung je Handlungsalternative

Alternative	*einmalige Kosten*	*laufende Kosten (p.a.)*
Alternative A1: „Biometrische Nutzung heutiger Ausweise“	22 Mio. Euro	4,5 Mio. Euro
Alternative A2: „Ausrüstung der Ausweise“		
Variante 2a „Neuerfassung in Meldebehörden“	614 Mio. Euro	332 Mio. Euro
Variante 2b „Nutzung bestehender Prozesse“	179 Mio. Euro	55 Mio. Euro
Alternative A3: „Neue Ausweisgeneration“*	669 Mio. Euro	610 Mio. Euro
Alternative A0 „Abwarten und Beobachten: Keine Biometrieanwendung“	0	0

* In der Alternative 3 wird nur die dezentrale Erfassung betrachtet.

Auffällig sind die große Spanne zwischen den einzelnen Optionen (Faktor bis zu 30) und der erhebliche Unterschied zwischen den Varianten a und b der Handlungsalternative A2. Hier wird deutlich, dass ein wesentlicher Kostentreiber mit der Hardware-Ausstattung der Meldestellen gegeben ist. Diese entfällt dann, wenn die bestehenden Ausweisdokumente entweder unverändert gelassen werden (A1) oder zwar biometrisch ergänzt bzw. ausgerüstet werden, sich die Veränderungen aber auf den Prozess der Ausweisproduktion beschränken (Handlungsalternative A2b) und keine Merkmalsneuerfassung und Templategenerierung in den Meldebehörden erfolgt. Hingegen führt die Einführung eines völlig neuen Ausweistyps (z.B. auf Basis einer Smartcard; Alternative A3) im Vergleich zu einer vollständig dezentral organisierten Ausrüstung der bestehenden Ausweisdokumente durch Merkmalserfassung und Templategenerierung in den Meldestellen (Handlungsalternative A2a) nur zu geringen Unterschieden in der finanziellen Belastung. Einschränkend muss allerdings erwähnt werden, dass bei dieser Alternative A3 die Kostenbandbreite, bedingt durch die nicht voraussehbaren Implikationen, weit größer ist als bei den anderen Alternativen. Im Falle einer Entscheidung zwischen den beiden Handlungsalternativen A2a und A3 erwarten wir, dass finanzielle Argumente deutlich hinter Nutzenaspekten und politischen Zielsetzungen zurücktreten werden.

Die mit den Handlungsalternativen A2 und A3 verbundenen erheblichen Investitionen könnten zwar technologisch stärker abgesichert werden, indem man die bereits laufenden Feldversuche auswertet und sie zur Entscheidung für den Einsatz einer bestimmten Technologie heranzieht. Diese bisherigen, primär technisch orientierten Untersuchungen werden jedoch kaum Schlussfolgerungen auf Nutzerakzeptanz und potenzielle Implikationen eines Masseneinsatzes zulassen. Anders ausgedrückt, könnte sich bei der Entscheidung für die Alternative A2 oder A3 der Staat in einer Situation befinden, in der zwar mit erheblichem Investitionsaufwand grundsätzlich taugliche Technologien zum Einsatz kommen, diese jedoch bei der konkreten Implementierung auf Schwierigkeiten oder aber generell bei der Bevölkerung auf dermaßen geringe Akzeptanz stoßen, dass sie im Extremfall wieder aufgegeben werden müssten.

Hier bietet sich Alternative A1, d.h. die biometrische Nutzung der heutigen Ausweise bzw. der heutigen Passfotos, an. Zum einen kommt für diese Alternative die vermutlich hinsichtlich der Nutzerakzeptanz bzw. der Kooperation der Bevölkerung verträglichste Technologie, die Gesichtserkennung, zum Einsatz, zum anderen wären wesentlich geringere Investitionen im Extremfall eines Scheiterns abzuschreiben. Wir empfehlen damit dem Bundestag bzw. dem Büro für Technikfolgen-Abschätzung, die Nutzung der Biometrie in den heutigen

Ausweisdokumenten in jedem Fall als ersten Schritt in Erwägung zu ziehen, um das Thema „Einsatz der Biometrie im Ausweiswesen“ vom Niveau rein technisch orientierter Pilotprojekte und strategischer Untersuchungen auf die konkrete Massenanwendung zu heben. Nur dadurch lassen sich unserer Einschätzung nach die eventuellen Risiken, die mit einem flächendeckenden Einsatz verbunden sind, mit vertretbarem finanziellen Aufwand bestimmen. Die Erkenntnisse und Erfahrungen aus einem solchen Masseneinsatz sind im Übrigen auch dann – zumindest eingeschränkt – verwertbar, wenn letztlich die zunächst zum Einsatz gelangende Gesichtserkennungs-Technologie aus technischen Gründen oder einem eventuellen internationalen Abstimmungserfordernis heraus abgelöst oder mit anderen Verfahren kombiniert wird. Da das Foto stets Teil eines Ausweisdokumentes sein wird, macht es in Anbetracht der niedrigen Kosten in jedem Fall Sinn, dieses Merkmal auch voll zu nutzen. Sollte sich im Zuge der Implementierung der Handlungsalternative A1 herausstellen, dass das Verfahren den Anforderungen nicht voll gerecht wird, so ist zunächst zu untersuchen, ob dies in der eventuell mangelhaften Qualität der eingesetzten Passfotos begründet ist. Ist dies der Fall, kann ein Übergang zu Handlungsalternative A2b vorgenommen werden, wodurch sich die Qualität der eingesetzten Passfotos deutlich verbessern und sich dementsprechend die Leistung der Variante der biometrischen Analyse des Passfotos bedeutend steigern ließe.

Die Ausrüstung bestehender Ausweise bzw. die Einführung einer neuen Ausweisgeneration (Handlungsalternativen A2 und A3) könnte somit nach erfolgreichem Einsatz der biometrischen Nutzung heutiger Ausweise durchaus zu einem späteren Zeitpunkt wieder aufgegriffen werden. Wir denken, dass derzeit noch keine Empfehlung für eine dieser beiden Alternativen ausgesprochen werden kann, da

- ein erhebliches finanzielles Risiko besteht;
- unklar ist, wie sich die Nutzerakzeptanz gegenüber den neuen Daten im Ausweis gestaltet;
- darüber hinaus denkbar ist, mehrere biometrische Merkmale kombiniert zu nutzen (z.B. Gesicht und Fingerabdruck);
- keinerlei prozessuale Erfahrungen mit dem Masseneinsatz gegeben sind.

Auch die Frage, ob nach Klärung dieser offenen Punkte eher Alternative A2a („Neuerfassung in den Meldebehörden“) oder A3 („neue Ausweisgeneration“) gewählt wird, ist heute ebenfalls nur bedingt einschätzbar. Die Alternativen unterscheiden sich im finanziellen Aufwand nur unerheblich. Hier gilt es, die Vorteile eines Beibehaltens der Dokumentenfamilie (politisch leichter durch-

setzbar, Kontinuität) gegenüber eventuellen Zusatznutzenpotenzialen (z.B. Einsatz für E-Commerce etc.) abzuwägen.

Ein generelles Abwarten beim Einsatz der Biometrie ist aus Sicht der Autoren dieses Gutachtens abzulehnen, da sich durch einen großflächigen Einsatz der Biometrie in Deutschland erhebliche Nutzenpotenziale in fünf Bereichen ergeben können:

- Zum einen erfolgt bei jeder Handlungsalternative eine Erhöhung der Sicherheit. Zwar weisen die in Deutschland eingesetzten Ausweise eine hohe Fälschungssicherheit auf, jedoch kann die Identitätsüberprüfung insbesondere bei Grenzkontrollen durch ein technisch unterstütztes biometrisches Verfahren verbessert werden. Hierbei sind nicht nur die tatsächliche Erhöhung der Sicherheit, sondern auch das subjektiv empfundene Sicherheitsgefühl als wünschenswert zu erwähnen.
- Erste Einschätzungen gehen heute davon aus, dass auch die Prozesseffizienz bei Grenzübertritten gesteigert werden kann. Da der technisch unterstützte Vergleich des Lichtbildes im Ausweis mit der betreffenden Person sehr viel schneller durchgeführt werden kann als durch den Grenzbeamten, könnten nicht nur die Prozesszykluszeiten an den Grenzübergängen erheblich beschleunigt, sondern vermutlich auch Personalressourcen effizienter eingesetzt werden.
- Langfristig – bei Einsatz einer neuen Ausweisgeneration – können sich auch neue Impulse für den Einsatz der elektronischen Unterschrift ergeben. Dadurch würde auch der E-Commerce belebt und Betrugsfälle im Internet könnten wirkungsvoll bekämpft werden.
- Die Vorteile eines „first movers“ hinsichtlich der internationalen Verankerung von Datenschutzrichtlinien sind zu beachten. Falls Deutschland eine abwartende Haltung bei der Einführung biometrischer Merkmale im Ausweis annehmen sollte, ist davon auszugehen, dass die in Deutschland traditionell stärkeren Datenschutzbestrebungen durch internationale Initiativen ausgehöhlt werden.
- Auch die deutsche Volkswirtschaft profitiert potenziell. Deutsche Unternehmen sind im Biometriemarkt mit signifikantem Marktvolumen und prognostizierten zweistelligen Wachstumsraten grundsätzlich gut positioniert. Eine erste Gegenüberstellung zeigt auf der Anwendungsseite die heutige große Dominanz des nordamerikanischen Kontinents. Europäische und insbesondere deutsche Unternehmen sind derzeit gezwungen, mit ihren Produkten im Ausland zu reüssieren, da vergleichbare Großanwendungen in

Deutschland fehlen. Dieser implizite Wettbewerbsnachteil könnte durch ein entsprechendes Großprojekt in Deutschland kompensiert werden. Die oftmals bemängelte fehlende Innovationskraft Deutschlands in ausgewählten Industrien könnte durch ein staatliches Votum pro Biometrie zumindest im Hinblick auf eine ausgewählte Innovationstechnologie bereinigt werden.

Die Gutachter empfehlen daher Handlungsalternative A1.

2. Tabellenverzeichnis

Tab. 1: Biometrietests in den USA seit 2000 29
Tab. 2: Grenzkontrollanwendungen: Pilotprojekte und Tests (seit 2002) 42
Tab. 3: Weitere nationale ID-Dokumente 54
Tab. 4: Übersicht der distinktiven, für die biometrische Analyse benutzten Informationen 64
Tab. 5: Fehlerratenangaben für Fingerabdruck-Verfahren in neueren Tests 68
Tab. 6: Fehlerratenangaben für Gesichtserkennungs-Verfahren in neueren Tests 69
Tab. 7: Fehlerratenangaben für Handgeometrie-Verfahren in neueren Tests 70
Tab. 8: Fehlerratenangaben für Iriserkennungs-Verfahren in neueren Tests 70
Tab. 9: Zusammenfassung des technischen Vergleichs 76
Tab. 10: Übersicht Kostenkomponenten 84
Tab. 11: Option 1: Biometrische Nutzung bestehender Dokumente – Kostenübersicht 85
Tab. 12: Option 2a: Aufwertung bestehender Ausweisdokumente mit biometrischen Daten in Speichertechnik (zentral) – Kostenübersicht 87
Tab. 13: Option 2b: Aufwertung bestehender Ausweisdokumente mit biometrischen Daten in Speichertechnik (dezentral) – Kostenübersicht 87
Tab. 14: Option 3: Neues Dokumentenkonzept mit Speicherelementen – Kostenübersicht 88
Tab. 15: Übersicht Kostenkomponenten 133
Tab. 16: Abschätzung der einmaligen Kosten – Handlungsalternative A1 137
Tab. 17: Abschätzung der laufenden Kosten – Handlungsalternative A1 138
Tab. 18: Abschätzung der einmaligen Kosten – Handlungsalternative A2a 142
Tab. 19: Abschätzung der einmaligen Kosten – Handlungsalternative A2b 143
Tab. 20: Abschätzung der laufenden Kosten – Handlungsalternative A2a 144
Tab. 21: Abschätzung der laufenden Kosten – Handlungsalternative A2b 145
Tab. 22: Abschätzung der einmaligen Kosten – Handlungsalternative A3 148
Tab. 23: Abschätzung der laufenden Kosten – Handlungsalternative A3 149
Tab. 24: Zusammenfassung Kostenabschätzung je Handlungsalternative 151

3. Abbildungsverzeichnis

Abb. 1: Visabeantragungen in den USA von 1999 bis 2003 26
Abb. 2: Kontrollsystem für die Ein- und Ausreise in die USA..... 28
Abb. 3: Privium-Kontrollraum am Flughafen Schiphol 44
Abb. 4: CANPASS-Schalter 45
Abb. 5: Handscanner am Flughafen Ben Gurion 46
Abb. 6: Kontrollorte biometrischer Grenzkontrollanwendungen..... 47
Abb. 7: Verwendete Biometrien bei Grenzkontrollanwendungen (Pilot und implementiert) 48
Abb. 8: Biometrische Grenzkontrollanwendungen nach Regionen..... 48
Abb. 9: Erfassen der Handgeometrie..... 56
Abb. 10: Lesegerät für Fingerabdrücke 58
Abb. 11: Vermessung eines Gesichtes..... 59
Abb. 12: Scannen einer Iris 60
Abb. 13: Vergleichende Bewertung von Erfassbarkeit und Enrollment-Ausfallrate..... 62
Abb. 14: Vergleichende Bewertung der Falschakzeptanzrate (FAR)..... 71
Abb. 15: Vergleichende Bewertung der Falschrückweisungsrate (FRR) 71
Abb. 16: Vergleichende Bewertung von Bedienungsaufwand/Verständlichkeit..... 74
Abb. 17: Vergleichende Bewertung der Integrierbarkeit.....80
Abb. 18: Ableitung von Handlungsalternativen 127

4. Abkürzungsverzeichnis

AFIS	Automated Fingerprint Identification System
ASBWG	Aviation Security Biometrics Working Group
AsylVfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
B&L	B&L Management Consulting GmbH
BCC	Border Crossing Card
BDSG	Bundesdatenschutzgesetz
BKA	Bundeskriminalamt
BMI	Bundesministerium des Inneren
BMWA	Bundesministerium für Wirtschaft und Arbeit
BSI	Bundesamt für Sicherheit in der Informationstechnik
C-VIS	Central Visa Information System
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DVD	Deutsche Vereinigung für Datenschutz
EBF	European Biometric Forum
FAA	Federal Aviation Administration
FAR	False Acceptance Rate
FRR	False Rejection Rate
FRVT 2000	Facial Recognition Vendor Test 2000
FRVT 2002	Face Recognition Vendor Test 2002
FVC	Fingerprint Verification Competition
GAO	U.S. General Accounting Office
IBG	International Biometric Group
ICAO	International Civil Aviation Organization
IGD	Fraunhofer-Institut für graphische Datenverarbeitung
IIG	Institut für Informatik und Gesellschaft
ILO	International Labour Organization

IMO	International Maritime Organization
INS	Immigration and Naturalization Service
INSPASS	INS Passenger Accelerated Service System
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NPL	National Physical Laboratory
NSEERS	National Security Entry Exit Registration System
N-VIS	National Visa Information System
PassG	Passgesetz
PAuswG	Personalausweisgesetz
SDÜ	Schengener Durchführungsübereinkommen
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
SigV	Signaturverordnung
SIS	Schengen-Informationssystem
SMARTICS	Smart Identity Card System
SOLAS	International Convention for the Safety of Life at Sea
STZ	Steinbeis GmbH & Co. KG für Technologietransfer – Steinbeis-Transferzentrum Biometrie und Identifikationslösungen
TAB	Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
TBG	Terrorismusbekämpfungsgesetz
U.S. VISIT	United States Visitor and Immigrant Status Indicator Technology
ULD-SH	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UNMIK	United Nations Mission in Kosovo
VIS	Visa-Informationssystem
WIK	Wissenschaftliches Institut für Kommunikationsdienste GmbH

TAB

Glossar

Algorithmus – Rechenfunktion bzw. Rechenvorschrift.
Application Program Interface (API) – Programmierschnittstelle bei Anwendungen
Authentisierung/Authentifikation – Systematische Methode zur Überprüfung der Identität einer Person. Sie gibt Aufschluss über die Identität einer Person, sagt jedoch nichts über deren Zugriffsrechte aus. Einfache Authentisierungs-Methoden basieren auf Nutzername und Passwort; sicherer sind einmal verwendbare Passwörter; am sichersten sind multimodale biometrische Verfahren.
Barcode (Strichcode) – spezieller Identifizierungscode, in Form von vertikalen Balken unterschiedlicher Breite. Der Barcode stellt binäre Informationen dar, die sich mit einem optischen Scanner lesen lassen.
Biometric Application Program Interface (BioAPI) – durch ein Industriekonsortium standardisierte Anwendungsprogrammier-Schnittstelle für die Integration biometrischer Systeme in Anwendungen.
Biometrischer Sensor – Hardware-Komponente eines biometrischen Systems, die zunächst die biometrischen Messdaten liefert (z.B. Fingerabdruck-Sensoren).
Elektronische Signatur – ist eine digitale Lösung für eine rechtsverbindliche Unterschrift auf elektronischem Wege. Die so genannte „qualifizierte elektronische Signatur“ ermöglicht, im elektronischen Rechts- und Geschäftsverkehr den Urheber und die Integrität von Daten zuverlässig festzustellen. Als eine Art Siegel zu digitalen Daten ist eine „qualifizierte elektronische Signatur“ im Sinne des Signaturgesetzes eine solche, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit erzeugt wird (§ 2 Nr. 3). Sie wird mit einem privaten kryptographischen Schlüssel erzeugt. Mit Hilfe des dazugehörigen öffentlichen Schlüssels kann die Signatur jederzeit überprüft und damit der Signaturschlüssel-Inhaber und die Unverfälschtheit der Daten überprüft werden.
Enrollment – umfasst das erstmalige Erfassen und (Ver-)Messen des biometrischen Merkmals der zukünftigen Nutzer, die Umwandlung der Rohdaten in einen Referenzdatensatz und die Speicherung desselben, des sog. Templates (s.u.). So wird z.B. der Mittelwert aus drei hintereinander erfolgten Messungen desselben Fingerabdrucks gebildet und danach auf einer Smartcard (Match-On-Card-Verfahren, s.u.) oder in einer Template-Datenbank abgelegt.
EER (Equal Error Rate) – FAR und FRR (s.u.) können nicht theoretisch berechnet, sondern müssen empirisch ermittelt werden. FAR und FRR beeinflussen sich dergestalt, dass eine Absenkung der falschen Akzeptanz die falsche Zurückweisung erhöht und umgekehrt. Bei Gleichgewicht der Werte spricht man von EER.
FAR (False Acceptance Rate) – Rate falscher Akzeptanz; gibt die Wahrscheinlichkeit dafür an, dass ein fremdes Individuum bei der Präsentation seiner Verifikationsdaten fälschlicherweise als der rechtmäßige Eigentümer der Referenzdaten verifiziert wird. Die FAR ist abhängig von der gewählten Toleranzgrenze, innerhalb der die Verifikations- und Referenzdaten im Falle einer erfolgreichen Authentisierung übereinstimmen müssen: Je kleiner die Toleranzgrenze, desto kleiner die FAR, und umso größer wird dafür die FRR (s.u.).

FRR (False Rejection Rate) – Rate falscher Zurückweisung; gibt die Wahrscheinlichkeit dafür an, dass der rechtmäßige Besitzer der biometrischen Referenzdaten beim Präsentieren seiner Verifikationsdaten fälschlicherweise zurückgewiesen wird. Die FRR ist abhängig von der Toleranzgrenze, innerhalb der die Verifikations- und Referenzdaten für eine erfolgreiche Authentisierung übereinstimmen müssen: Je größer die Toleranzgrenze, umso kleiner wird die FRR, und umso größer wird dafür die FAR.
Graph-Matching-Verfahren – Verfahren zum direkten Vergleich einzelner Gesichtselemente: Das Gesicht wird von einer hochauflösenden Kamera erfasst; das so entstandene Gesichtsbild durch Gitterkoordinaten bis zur größtmöglichen Übereinstimmung mit dem Referenzbild verformt. Bei hinreichender Übereinstimmung des Live-Bildes mit dem Referenzdatensatz wird auf Identität geschlossen.
Identifikation – Feststellung der Identität eines Individuums. Bei biometrischer Identifikation liefert das Individuum zunächst seine biometrischen Messdaten, aus denen die Verifikationsdaten gebildet werden. Es wird dann eine Datenbasis von Referenzdaten von N Individuen nach solchen Referenzdaten durchsucht, die mit den präsentierten Verifikationsdaten eine vorher festgelegte Übereinstimmung zeigen. Man nennt diesen Prozess daher auch „1:n-Vergleich".
Lebenderkennung – auch „live check" oder „liveness test" genannt. Hierbei handelt es sich um eine Methode, um sicherzustellen, dass tatsächlich auch eine lebende Person authentifiziert wird. Zu diesem Zwecke sucht das System z.B. nach Bewegungen innerhalb des Gesichts, um auszuschließen, dass dem System eine Attrappe oder Maske vorgehalten wird.
Match-On-Card-Verfahren – Verfahren, bei dem der Vergleich von aktuell erhobener biometrischer Information mit einer Referenzinformation auf einer Smartcard stattfindet, wobei die Referenzinformation sich immer im geschützten Sicherheitsbereich der Karte befindet und nicht ausgelesen werden kann.
Merkmals-Extraktions-Algorithmus – Bei einem biometrischen Vergleichsverfahren werden die vom biometrischen Sensor aufgenommenen Messdaten nicht komplett abgespeichert bzw. verglichen; es müssen charakteristische Merkmale extrahiert werden Die Extraktion der abzuspeichernden Referenzdaten bzw. der mit ihnen zu vergleichenden Verifikationsdaten aus aufgenommenen Messdaten erfolgt mit einem geeigneten Merkmals-Extraktions-Algorithmus.
Minutien – charakteristische Punkte eines Fingerabdruck-Bildes wie Verzweigungs- und Endpunkte von Linien. Die mathematischen Informationen zur Codierung der Minutien werden mit einem entsprechenden Merkmals-Extraktions-Algorithmus aus den Daten eines Fingerabdruck-Bildes extrahiert und als Verifikations- und Referenzdaten zur Fingerabdruck-Erkennung verwendet: Ein Individuum wird als Besitzer der entsprechenden Referenzdaten erkannt, wenn sie in einer vorher festgelegten Anzahl von Minutien mit den Verifikationsdaten übereinstimmen.
Public Key Infrastructure (PKI) – Kombination von Software und Services, um die Vertraulichkeit, Integrität und Verbindlichkeit von Anwendungen, wie etwa E-Commerce oder E-Banking, sicherzustellen. Mit der PKI-Software werden Transaktionen verschlüsselt und digital signiert sowie digitale Zertifikate erstellt und verwaltet. Grundgedanke des Verfahrens ist, dass jeder Kommunikationsteilnehmer mit zwei individuellen Schlüsseln ausgestattet wird (vgl. digitale Signatur). Der eine Schlüssel, der private key (Entschlüsselungsschlüssel), muss absolut vertraulich gehalten und entsprechend, z.B.

durch biometrische Verfahren, gesichert werden. Der andere Schlüssel, der public key (Signaturerstellungsschlüssel), soll hingegen denen offen stehen, die mit dem Besitzer des Schlüsselpaares in Kommunikation stehen. Um dies zu ermöglichen, sind Infrastrukturen zu schaffen, die Möglichkeiten des Austausches von Schlüsseln und Zertifikaten zwischen den handelnden Personen ermöglichen – und zwar innerhalb der einzelnen Organisationen, zwischen Organisationen sowie auf nationaler und internationaler Ebene. Die hierzu notwendige komplexe Infrastruktur wird als PKI bezeichnet, wobei man vor allem organisationsinterne PKIs und öffentliche PKIs unterscheidet.

Referenzdaten – die mit dem Merkmals-Extraktions-Algorithmus gebildeten, abzuspeichernden Daten zur biometrischen Charakterisierung eines Individuums (vgl. Template).

Smartcard – Karte in der genormten Größe einer Kreditkarte, enthält einen elektronischen Chip. Dieser ist durch eine Reihe von Sicherheitsmerkmalen geschützt und kann Daten speichern sowie verarbeiten. Smartcards sind in der Lage, ihre Besitzer durch interne Prüfung eines Passwortes/PIN oder eines biometrischen Templates zu erkennen. Die Smartcard wird auch als Speichermedium für persönliche Daten genutzt.

Template – Referenzdatensatz, der den Vergleichswert darstellt, mit dem bei allen darauf folgenden biometrischen Überprüfungen die neuen Messdaten übereinstimmen müssen, um den Nutzer identifizieren zu können. Da die Messungen eines biometrischen Merkmals nie identische Ergebnisse ergeben, reicht ein festgelegter Grad an Ähnlichkeit mit dem Template, um einen Nutzer erfolgreich zu identifizieren. Es ist nicht möglich, aus einem Template das zugehörige vollständige Messergebnis eines biometrischen Merkmals zurückzurechnen.

Toleranzgrenze – Biometrische Messdaten sowie die daraus mit Hilfe des Merkmals-Extraktions-Algorithmus gebildeten Verifikationsdaten sind auch für dasselbe Individuum niemals gleich, sondern immer statistischen Schwankungen unterworfen. Deshalb kann man bei biometrischer Identifikation oder Verifikation niemals exakte Übereinstimmung von Verifikationsdaten und Referenzdaten verlangen, sondern nur eine Übereinstimmung innerhalb einer gewissen Toleranzgrenze.

Transponder – dünner, kontaktloser Chip, der mit einer Antenne versehen ist und durch ein elektrisches Feld mit notwendiger Energie versorgt wird. Derzeit reicht das Speichervolumen bis maximal 4 MB.

Verifikation – Bei der Verifikation wird geprüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt. Ihre aktuell erhobenen biometrischen Daten werden nur mit ihren Referenzdaten verglichen (1:1-Vergleich).

TAB

TAB

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag

Neue Schönhauser Str. 10 · 10178 Berlin
Telefon: 0 30 / 28 49 10
Telefax: 0 30 / 28 49 11 19
e-mail: buero@tab.fzk.de
Internet: www.tab.fzk.de