Öffentliche Anhörung im Innenausschuss des Deutschen Bundestages

Aufnahme biometrischer Merkmale in den Reisepass Änderung des PassG

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)192 D

Stellungnahme des BKA

Inhalt

1 Einleitung 2
1.1 Sicherheitspolitische und polizeiliche Zielsetzung 2
1.2 Stand der Umsetzung und weitere Schritte auf EU-Ebene 3
1.3 Status der Ausweisdokumente in Deutschland 4
2 Stellungnahme zum Gesetzentwurf der Bundesregierung zur Änderung des PassG 5
2.1 Erfassung, Speicherung und Nutzung von biometrischen Daten des Passes 5
2.2 Datenabgleich beim BKA für Drittstaatsangehörige 6
2.3 Online-Abruf von Lichtbilddaten 6
3 Stellungnahme zum Antrag der Fraktion der FDP [BT 16/854]: Sicherheitslücken bei biometrischen Pässen beseitigen 7
4 Stellungnahme zum Antrag der Fraktion der FDP [BT 16/3046]: Keine Einführung des elektronischen Personalausweises 8
5 Stellungnahme zum Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN [BT 16/4159]: Datenschutz und Bürgerrecht bei der Einführung biometrischer Ausweise wahren 11
6 Stellungnahme zum TA-Bericht „Biometrie und Ausweisdokumente“ [BT 15/4000] 11

1 Einleitung

1.1 Sicherheitspolitische und polizeiliche Zielsetzung

Die Terroranschläge des 11. September 2001 und die späteren Ereignisse in Europa führten international, auf EU-Ebene und im nationalen Rahmen zu einer Vielzahl politischer Entscheidungen und Maßnahmen zur Forcierung der Terrorismusbekämpfung, bei der die Sicherheit im Reiseverkehr, insbesondere die Verbesserung der Luftsicherheit, von wesentlicher Bedeutung ist. Die Weiterentwicklung der Dokumentensicherheit und die Einführung biometrischer Identitätsprüfungsverfahren stellen hierbei wichtige Bausteine dar.[1] So hat der Deutsche Bundestag bereits im Terrorismusbekämpfungsgesetz vom 9. Januar 2002 erstmalig die Möglichkeit der Einführung und elektronischen Speicherung biometrischer Merkmale in Personaldokumenten beschlossen.[2]

Neben der Bekämpfung der Fälschungskriminalität ist es angesichts des Problems der missbräuchlichen Benutzung echter Identitätsdokumente durch Unberechtigte die Zielsetzung der Einführung biometrischer Verfahren, die bisherigen auf Sichtkontrolle gestützten Mechanismen der Einreise-, Aufenthalts- und Identitätskontrolle durch Einsatz automatisierter messtechnischer Verfahren zu erweitern und zu objektivieren:

- Erfassung biometrisch messbarer Individualitätsmerkmale zur Charakterisierung einer Person und deren Verknüpfung mit der herkömmlich (z.B. in Form personenbezogener Daten im Ausweispapier) dokumentierten Identität,
- Abspeicherung der Daten in informationstechnisch erweiterten, fälschungssicheren Reisedokumenten in international interoperablem Format,
- maschinell gestützte Korrelation der im aktuellen Kontrollprozess erhobenen biometrischen Merkmale mit der dokumentierten Identität zur Verifikation der Zugehörigkeit von Reisedokument und dessen Benutzer.

Die Kombination dieser Sicherheitsfunktionen führt zu einer modularen Erweiterung des bisherigen Kontrollablaufs durch maschinell gestützte Echtheits- und Identitätsprüfungsschritte und damit zu einer durch technische Präventionsmaßnahmen weiterentwickelten Sicherheitskonzeption auf höchstmöglichem Niveau.

---

[1] Resolution des Sicherheitsrats der Vereinten Nationen 1373 vom 28. September 2001, Nr. 2g, Aktionsplan der Europäischen Union zur Terrorismusbekämpfung vom 21. September 2001, Erklärung des Europäischen Rates zum Kampf gegen den Terrorismus vom 25. März 2004, Nr. 6, USA PATRIOT Act of 2001 (Public Law 107-56) and Enhanced Border Security and Visa Entry Reform Act of 2002 (H.R. 3525), Terrorismusbekämpfungsgesetz vom 9. Januar 2002

[2] Bislang schon in den Dokumenten enthaltene Lichtbilder und Unterschriften sind auch biometrische Merkmale.

1.2 Stand der Umsetzung und weitere Schritte auf EU-Ebene

Auf dem EU-Gipfel von Thessaloniki 2003[3] konkretisierte der Europäische Rat die bisherigen Zielsetzungen im Sinne eines kohärenten Ansatzes bezogen auf

- die Integration biometrischer Daten in die Pässe der EU-Bürger,
- die Integration biometrischer Daten in die Dokumente von Drittstaatsangehörigen, z.B. in Form von biometrischen Aufenthaltstitelkarten,
- sowie die Einbeziehung der Biometrie im Visaverfahren und bei der Entwicklung der EU-Datenbanksysteme VIS (Visa-Informationssystem) und SIS II.

Mit der Ratsverordnung vom 13. Dezember 2004[4] wird die Rechtsgrundlage geschaffen für

- die Einbringung der biometrischen Merkmale Gesichtsbild und Fingerabdrücke in die von den EU-Mitgliedstaaten ausgegebenen Pässe,
- die Festlegung gemeinsamer Standards für die Integration eines RF(Radiofrequenz)-Chips als Datenspeicher,
- die Anwendung gemeinsamer Mindeststandards zur Fälschungssicherheit und
- die Einführung gemeinsamer informationstechnischer Sicherheitsfunktionen und Zugriffsschutzmechanismen gegen Missbrauch und Manipulation der Daten im Chip (Sicherstellung der Integrität, Authentizität und Vertraulichkeit für die biometrischen Daten).

Die Mitgliedstaaten waren verpflichtet, bis 28. August 2006 Pässe mit RF-Chip und gespeichertem Gesichtsbild einzuführen, spätestens ab 28. Juni 2009 ist die Aufnahme von Fingerabdrücken vorgeschrieben.

Die Entscheidung auf europäischer Ebene für das Gesichtsbild beruhte auf der Empfehlung der International Civil Aviation Organization (ICAO).[5] Für Fingerabdrücke als zweites Merkmal sprach die hohe Praxistauglichkeit der hierzu entwickelten Abnahme- und Erkennungssysteme. Die Festlegung der EU auf zwei biometrische Merkmale war erforderlich, um hohe Verifikationssicherheit und Flexibilität bei der Kontrolle zu ermöglichen. In Abhängigkeit von der Kontrollinfrastruktur stehen beide Biometrieverfahren zur Verfügung. An Stellen, an denen die Gesichtserkennung nicht praktikabel ist (z.B. bei schlechten Beleuchtungsverhältnissen), soll eine Verifikation durch Fingerabdrücke möglich sein. Als weltweit fest-

[3] Europäischer Rat von Thessaloniki, 19. und 20. Juni 2003, Schlussfolgerungen des Vorsitzes, Abschnitt II, Nr. 11: Entwicklung einer gemeinsamen Politik in Bezug auf die illegale Einwanderung

[4] Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. L 385 vom 29.12.2004, S. 1-6

[5] ICAO-Dokument 9303, Part 1 „Machine Readable Passports“, 6th Edition, 2006

gelegter Biometriestandard ist die Gesichtserkennung als Basiskontrollverfahren zu etablieren.

1.3 Status der Ausweisdokumente in Deutschland

Der bisherige deutsche Pass nach EU-Modell (wie auch der Personalausweis) hat aufgrund der Anwendung von Spitzentechnologien der Sicherungstechnik in zentraler Produktion und Personalisierung bereits ein weltweit führendes Sicherheitsniveau erreicht.
Maßgeblich hierfür sind insbesondere die materialmäßige und drucktechnische Ausstattung mit technologisch aufwendigen Sicherheitsmerkmalen, die Integration der Personaldaten in einen hochgradig gegen Abänderungsmanipulationen geschützten Passkartenaufbau und die bisher einmalige Hologrammtechnologie mit dem individuell eingebrachten holographischen Lichtbild.

Dieses sicherungstechnische Dokumentenkonzept bildet die Grundlage, das Passsystem durch Einführung biometrischer Verfahren so zu erweitern, dass sowohl die Dokumentenkontrolle wie auch die Personenkontrolle mit den verfügbaren Möglichkeiten der technischen Prävention verbessert werden können.
Mit der ab 1. November 2005 in Deutschland begonnenen Ausgabe der (nach Maßgabe der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 erstellten) Pässe sowie der Diplomaten- und Dienstpässe als elektronische Pässe (ePässe) mit RF-Chip und biometriegeeignetem Gesichtsbild wurde die erste Stufe der vorgesehenen Maßnahmen verwirklicht. Inzwischen sind ca. 3 Millionen ePässe erfolgreich produziert worden, Funktionsfähigkeit und Konformität mit EU-Anforderungen und ICAO-Standards wurden in internationalen Interoperabilitätstests nachgewiesen.

Für die polizeiliche Anwendung elektronischer Pässe und biometrischer Verfahren im Kontrollprozess haben die zuständigen Gremien der Ständigen Konferenz der Innenminister und -senatoren der Länder mit der Planung begonnen und in entsprechenden Beschlüssen zustimmend votiert.

2 Stellungnahme zum Gesetzentwurf der Bundesregierung zur Änderung des PassG

2.1 Erfassung, Speicherung und Nutzung von biometrischen Daten des Passes

Mit dem als Entwurf vorgelegten Gesetz zur Änderung des Passgesetzes werden die Voraussetzungen dafür geschaffen, dass Deutschland ab November 2007 in Umsetzung der EG-Verordnung 2252/2004 elektronische Reisepässe ausstellen kann, in deren Chips neben dem Lichtbild auch Fingerabdrücke gespeichert werden. Kern des Entwurfs sind die Schaffung einer Rechtsgrundlage für die Erhebung der Fingerabdrücke durch die Passbehörden sowie die Regelung der Befugnisse der den Pass und dessen Inhaber kontrollierenden Stellen. Parallelregelungen finden sich im Freizügigkeitsgesetz / EU, im Aufenthaltsgesetz und Asylverfahrensgesetz. Diese Bestimmungen werden aus polizeilicher Sicht befürwortet.

Dies betrifft insbesondere folgende Regelungen:

- Schaffung einer Rechtsgrundlage zur Erhebung der Fingerabdrücke durch die Passbehörden (§ 4 Absatz 3 und § 6 Absatz 2), die Einzelheiten der Erfassung der biometrischen Merkmale, einschließlich der Altersregelungen (§ 4 Absatz 4 bis 6) und die Sollbestimmung zum persönlichen Erscheinen des Passbewerbers (§ 6 Absatz 1)[6]

- Schaffung einer Rechtsgrundlage zur Erhebung und zum Auslesen der biometrischen Daten sowie deren Vergleich bei Deutschen (§ 16a PassG), Unionsbürgern und ihren Familienangehörigen (§ 8 Absatz 2 Freizügigkeitsgesetz) sowie von Drittstaatsangehörigen (§ 16 Absatz 1a Asylverfahrensgesetz, § 49 Absatz 1 Aufenthaltsgesetz) im Rahmen von Kontrollen

- Schaffung einer Befugnis zur AZR-Abfrage und zur Durchführung des Konsultationsverfahrens (u.a. mit dem BKA) vor der Ausstellung amtlicher Pässe an Nichtdeutsche (§ 6 Absatz 2b PassG) im Zusammenhang mit der Öffnungsklausel für die Ausstellung amtlicher Pässe an nicht-deutsche Staatsangehörige (§ 1 Absatz 4 Satz 2 PassG)

    - Wegfall des Kindereintrags in den Reisepass der Eltern (§ 4 Absatz 5 Satz 3 PassG alt)

[6] Auszug aus der Gesetzesbegründung: „Die Soll-Vorschrift ermöglicht in Ausnahmefällen auch die Datenerfassung durch eine andere mit hoheitlichen Befugnissen ausgestattete Stelle, z.B. durch für Auslandsvertretungen tätige Honorarkonsuln."

- Wünschenswert wäre auch bei Empfang eines neuen Passes eine verpflichtende Rückgabe des alten Dokuments an die Passbehörde, um Missbrauchsfällen vorzubeugen.

2.2 Datenabgleich beim BKA für Drittstaatsangehörige

Die im Gesetzentwurf enthaltenen Regelungen zur Änderung des Asylverfahrensgesetzes und des Aufenthaltsgesetzes dienen einer Präzisierung von Gegenstand und Zweck der Amtshilfe des BKA bei der Feststellung der Identität von Drittstaatsangehörigen in asyl- und ausländerrechtlichen Verfahren. Damit verbunden ist die

- Schaffung einer Rechtsgrundlage für den Abgleich der Lichtbilder und Fingerabdrücke mit den Datenbeständen des BKA bei Drittstaatsangehörigen (§ 16 Absatz 3 und 4 Asylverfahrensgesetz, § 89 Absatz 1 Aufenthaltsgesetz) in Amtshilfe sowie Ergänzung der bestehenden Regelung zur Übermittlung der Fingerabdrücke bei erkennungsdienstlichen Maßnahmen bei Asylbewerbern um die Befugnis auch zur Übermittlung der Lichtbilder.

2.3 Online-Abruf von Lichtbilddaten

Über die Änderungen hinaus, die unmittelbar auf das Erfordernis der Aufnahme biometrischer Merkmale in Pässe zurückzuführen sind, enthält der Entwurf weitere Änderungen, u.a.

- die Zulassung des automatisierten Abrufs von Lichtbildern aus den Pass- und Personalausweisregistern durch Polizei- und Ordnungsbehörden bei Straßenverkehrsordnungswidrigkeiten (§ 22a PassG und § 2c PersAuswG)

Hierdurch werden unter eng umgrenzten Voraussetzungen bereits bestehende Verwaltungsabläufe durch moderne Informationstechniken vereinfacht. Eine Erweiterung der Möglichkeit zum automatisierten Abruf von Lichtbilddaten durch Polizeibehörden in bestimmten Eilfällen auf den Zweck der Verfolgung von Straftaten[7] ist sinnvoll. Liegen z.B. Hinweise auf bestimmte Personen vor, die einer Straftat verdächtig sind, können die Lichtbilddaten bei der zuständigen Pass-/Personalausweisbehörde schneller erhoben werden, als dies z.B. bei unmittelbarer Abholung oder Übersendung per Post, Fax oder ggf. E-Mail möglich ist - sofern

[7] s. Stellungnahme des Bundesrates zum Gesetzentwurf vom 16. Februar 2007 (BR-Drs. 16/07), Nr. 7b, Erweiterung der Zulassung des automatisierten (Online-)Abrufs auf alle in den Pass- und Ausweisregistern gespeicherten personenbezogenen Daten und auf den Zweck der Verfolgung von Straftaten

die jeweiligen Behörden zu dem betreffenden Zeitpunkt überhaupt für eine Abholung oder Übersendung erreichbar sind.
Tatverdächtige können somit i.d.R. schneller identifiziert und letztlich unbeteiligte Personen durch die Ermittlungen schneller entlastet werden.

Allerdings sind auch Fallkonstellationen im Sinne der Gefahrenabwehr denkbar, in denen eine solche Abrufmöglichkeit bei der Verhütung von Straftaten erforderlich sein kann.

3 Stellungnahme zum Antrag der Fraktion der FDP [BT 16/854]: Sicherheitslücken bei biometrischen Pässen beseitigen

Die wesentlichen durch die FDP vorgetragenen Argumente sind unzutreffend. Die im Antrag enthaltenen Aussagen sind wie folgt zu kommentieren:

1. Das aktive Auslesen eines kontaktlosen Chips (z.B. aus der Hosentasche) durch ein unberechtigtes Lesegerät könne in einer Entfernung von bis zu 10 m erfolgen:

   Nach Untersuchungen des BSI und weiteren Studien externer Institutionen ist das **aktive Auslesen** eines im ePass verwendeten Chips nur unter optimalen Bedingungen **bis zu maximal 20 cm** möglich. Um die Pässe auslesen zu können, muss ein Lesegerät daher bis auf eine geringe Entfernung an den ePass herankommen, Pass und Lesegerät sich mehrere Sekunden in Ruhe befinden und die Passnummer, das Geburtsdatum des Inhabers und das Ablaufdatum des Reisepasses bekannt sein bzw. in einem aufwändigen Verfahren „geraten“ werden (d.h. Überwindung des Zugriffsschutzes Basic Access Control).

   Selbst wenn ein solcher Spionage-Versuch gelänge, stellt sich die Frage, welchen Informationsgewinn der „Angreifer“ hätte? Bekannt waren ihm vorab bereits Passnummer, Geburtsdatum und Ablaufdatum. Neu ermittelt wurden nur Name und Vorname, Geschlecht, Staatsangehörigkeit sowie das Passfoto. Vor- und Nachname, Geschlecht und Staatsangehörigkeit wird der „Angreifer“ aber vorher gewusst haben. Schließlich hatte er bereits Passnummer, Geburtsdatum und Ablaufdatum des Passes herausgefunden. Bleibt als möglicher Ertrag das Passfoto. Aber auch das Aussehen seiner Zielperson muss dem „Angreifer“ vorher bekannt gewesen sein – wie sonst hätte er das Lesegerät bei der richtigen Person auf den erforderlichen Abstand zum ePass (ca. 20 cm)

heranbringen können? Das digitale Passfoto aus dem Chip wäre zudem bei Vorliegen krimineller Energie weitaus einfacher und unauffälliger zu bekommen: Mit einer leistungsfähigen Digitalkamera müsste sich ein Datenspion nicht auf 25 cm der Zielperson nähern.

2. Das passive Mitlesen einer Kommunikation (zwischen Chip und einem berechtigten Lesegerät z.B. bei der Grenzkontrolle), um die Daten nicht vor Ort, sondern nachträglich zu entschlüsseln, könne in einer Entfernung von bis zu 30 m erfolgen:

   Ein fehlerfreies passives Mitlesen ist nach Untersuchungen des BSI nur unter optimalen Bedingungen und in einer Entfernung von weniger als 2,70 m möglich.

3. Die Verschlüsselungsstärke betrüge maximal 56 Bit:

   Als **Verschlüsselungsverfahren** wird im ePass ein Standardverfahren mit einem Kommunikationsschlüssel von 112 Bit eingesetzt.

4 Stellungnahme zum Antrag der Fraktion der FDP [BT 16/3046]: Keine Einführung des elektronischen Personalausweises

Die EU-Mitgliedstaaten und auch der Deutsche Bundestag (siehe Terrorismusbekämpfungsgesetz vom 9. Januar 2002) haben sich darauf verständigt, biometrische Merkmale in Personaldokumenten einzuführen. Die von den Mitgliedsstaaten ausgestellten Pässe, Visa und Aufenthaltstitel werden dabei nach Maßgabe des Rechts der EG erstellt, während bei den von den Nationalstaaten ausgegebenen Personalausweisen das jeweilige nationalen Recht maßgebend ist.[8] In all diesen Bereichen soll die Fälschungssicherheit der Dokumente erhöht sowie Missbrauch ausgeschlossen werden.
Bestimmend für das Sicherheitskonzept eines elektronischen Personalausweises ist dabei seine Funktion im Kontrollprozess:

[8] Die Entschließung der im Rat vereinigten Vertreter der Mitgliedstaaten der EU vom 4./5.12.2006 über Mindestsicherheitsnormen für die als Reisedokument gültigen Personalausweise sieht, ausgehend vom Haager Programm des JI-Rates vom 13. Juli 2005, jedoch die gleichen Maßnahmen wie für Pässe vor.

- Der Personalausweis hat weiterhin eine Funktion als Passersatz, d.h. als Reisedokument innerhalb der Europäischen Union und des Schengenraums einschließlich der Anerkennung als Einreisedokument zur Einreise über die EU-Außengrenze. Daher muss der künftige elektronische Personalausweis wie der elektronische Pass mit einem kontaktlosen RF-Chip ausgestattet sein, in dem in äquivalenter Weise wie beim Pass biometrische Daten gespeichert sind. Die Speicherung biometrischer Merkmale im ePA analog zum ePass ist unverzichtbar für ein lückenloses nationales und EU-weites Sicherheitskonzept.
- Wie bisher hat der Personalausweis in Deutschland und im grenzkontrollfreien europäischen Binnenraum die Funktion eines Identitätsdokuments für behördliche Identitätsprüfungen ebenso wie zum Identitätsnachweis im privaten und geschäftlichen Alltag.
- Zusätzlich zur Speicherung biometrischer Daten soll mit dem elektronischen Personalausweis dem Ausweisinhaber eine elektronische Authentisierungsfunktion und auf Wunsch darüber hinaus eine digitale Signaturfunktion zur Verfügung gestellt werden.

Für den Schutz der gespeicherten personenbezogenen Daten auf dem Chip des ePA kommen abgestufte Sicherheitsmechanismen zum Einsatz:

- Weniger sensitive, weitgehend öffentlich verfügbare personenbezogenene Daten (z.B. Name, Geburtsdatum, Lichtbild) werden mit dem Verfahren **Basic Access Control** (BAC) geschützt.

  Mit Basic Access Control (BAC) wird ein Auslesen der auch auf dem Dokument sichtbaren Daten, wie Foto, Name, Geburtsdatum nur dann ermöglicht, wenn ein Zugriff auf die Daten der maschinenlesbare Zone (MRZ) des Passes/Personalausweises gegeben ist. Im Kontrollprozess wird dies durch optisches Auslesen der maschinenlesbaren Zone auf der Personaldatenseite des Dokuments realisiert, d.h. nach Übergabe des Dokuments durch den Inhaber an einen Kontrollbeamten.
  Um die Pässe/Personalausweise unberechtigt auslesen zu können, muss ein Lesegerät bis auf eine geringe Entfernung an das jeweilige Dokument herankommen, Dokument und unberechtigtes Lesegerät sich mehrere Sekunden in Ruhe befinden und die Dokumentennummer, das Geburtsdatum des Inhabers und das Ablaufdatum des Dokuments bekannt sein bzw. in einer aufwändigen rechentechnischen Simulation ermittelt werden. Der Informationsgewinn ist gering und steht in keinem Verhältnis zu dem dafür erforderlichen Aufwand. Ein Auslesen „aus der Hosentasche“ ist praktisch unmöglich.

- Sensitive personenbezogene Daten (insbesondere Fingerabdrücke) werden mit dem Verfahren **Extended Access Control** (EAC) geschützt.

  Mit Implementierung der Fingerabdrücke, als zweites biometrisches Merkmal, kommen beim ePass zusätzliche Schutzmechanismen in Form von Extended Access Control (EAC) beim Auslesen zum Tragen. Der Einsatz der EAC ermöglicht die Vergabe selektiver Zugriffsrechte, so dass nur autorisierte Lesegeräte auf die Fingerabdruckdaten zugreifen können. Durch Nutzung einer Public Key Infrastruktur (PKI) wird eine stark gesicherte Verbindung zur Datenübertragung zwischen einem (berechtigtem) Lesegerät und dem RF-Chip aufgebaut, so dass ein Entschlüsseln von unberechtigt mitgelesenen Daten unmöglich ist. Das Sicherheitsniveau der verwendeten Verschlüsselung wird national (BSI) und international (u.a. US-NIST) als sicher angesehen.
  EAC wird auch beim elektronischen Personalausweis eingesetzt werden.

Zu den Ausführungen im Antrag zum Entwicklungsstand biometrischer Systeme ist zu sagen:

Ziel der Biometriestudie **BIOP II**, die bereits zwischen November 2003 und 2004 von BSI und BKA durchgeführt wurde, war eine auf Grund wissenschaftlicher Kriterien angelegte Erprobung von drei biometrischen Verfahren (Gesichts-, Fingerabdruck- und Iriserkennung) vor dem Hintergrund der bevorstehenden Anwendung biometrischer Merkmale in Reisedokumenten.

Die in BioP II erreichten Erkennungsleistungen lassen unter optimierten Voraussetzungen durchaus die Eignung biometrischer Systeme für einen Praxiseinsatz erkennen. Durch die Teilnehmer des Projektes wurden die im Test befindlichen Geräte sowohl vom Design als auch der Benutzerfreundlichkeit her als verbesserungswürdig angesehen, jedoch stand den Herstellern der prototypischen Systeme nur ein stark begrenzter Zeitraum für Konstruktion und Fertigung zur Verfügung. Die Testteilnehmer bedienten die biometrischen Systeme mit sehr unterschiedlichen Häufigkeiten, was sich in der schlechteren Erkennungsleistung für ungeübte Personen (höhere Falschrückweisungsrate) widerspiegelt. Für den Echteinsatz biometrischer Verfahren im hoheitlichen Bereich ist die Bedienung der Systeme mit Unterstützung geschulter Personen (Grenzkontrollbeamte) gegenüber „Selbstbedienungsanwendungen“ vorzuziehen.

5 Stellungnahme zum Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN [BT 16/4159]: Datenschutz und Bürgerrecht bei der Einführung biometrischer Ausweise wahren

Hinsichtlich der vorgebrachten Sicherheitsbedenken sowie zum geplanten Einsatz von biometrischen Merkmalen in Personalausweisen wird auf die ausführliche Darstellung zu den Anträgen der FDP-Fraktion (siehe Stellungnahme zur BT-Drucksache 16/854, Kapitel 3, und BT-Drucksache 16/3046, Kapitel 4) verwiesen.

Was die Einführung von Lichtbild-Referenzdateien und deren Online-Abruf angeht, ist Folgendes anzumerken:

- Hintergrund der Forderung des Antrags ist der im Regierungsentwurf zum Passgesetz vorgesehene automatisierte (Online-)Abruf von Lichtbildern aus den dezentralen Pass- und Ausweisregistern. Dieser dient ausschließlich der Vereinfachung der bereits heute unter bestimmten Voraussetzungen zulässigen Übermittlung von Lichtbildern an „andere Behörden“ auf deren Ersuchen. Es handelt sich damit im Wesentlichen um eine Verfahrenserleichterung für die beteiligten Stellen.
  Allerdings sind auch Fallkonstellationen denkbar, in denen eine solche Abrufmöglichkeit bei der Verhütung und Verfolgung von Straftaten erforderlich sein kann.

- Eine Schaffung von vernetzten Lichtbilddateien ist mit der Regelung im Gesetzentwurf weder verbunden noch beabsichtigt.

Der Forderung, biometrische Merkmale in den Pässen ausschließlich zur Verifikation (1:1-Abgleich) der Identität einzusetzen, wird hinsichtlich deutscher Pässe mit einer entsprechenden Verwendungsbeschränkung in § 16a PassG-Entwurf Rechnung getragen.

6 Stellungnahme zum TA-Bericht „Biometrie und Ausweisdokumente“ [BT 15/4000]

Der erstmalig im Dezember 2003 komplett vorgelegte Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung „Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung“ ist aus hiesiger Sicht eine umfassende, fachlich weitgehend korrekte aber nicht mehr vollständig aktuelle Darstellung

des sehr komplexen Themengebietes „Biometrie und Ausweisdokumente“ und stellt nach wie vor einen wertvollen Diskussionsbeitrag dar.

Bei der Gegenüberstellung denkbarer technischer und administrativer Anwendungsoptionen der verschiedenen Biometrieverfahren mit abgestuftem Aufwand auf der Ausstellungs-, Dokumenten- und Kontrollebene

- Handlungsalternative 1: biometrische Nutzung der bestehenden Dokumente
- Handlungsalternative 2: technische Aufwertung der bestehenden Dokumente mit biometrischen Daten
- Handlungsalternative 3: Ablösung des bestehenden durch ein neues Dokumentenkonzept

kommt der TA-Bericht zu den gleichen Schlußfolgerungen wie BKA, BSI und BGS in ihren damaligen Einschätzungen des Themas. Der TA-Bericht liefert jedoch erstmalig eine quantitative Abschätzung der zu erwartenden Kosten in Abhängigkeit von der gewählten Biometrievariante.

Die inzwischen auf Grund nationaler und internationaler Vorgaben (insbesondere EU sowie ICAO) realisierte Lösung der Integration eines kontaktlosen Datenträgers (RF-Chip) in den Pass und die dezentrale Aufnahme der biometrischen Merkmale in den lokalen Passbehörden (ab 01.11.2005 Lichtbild, ab 01.11.2007 Lichtbild und Fingerabdrücke) entspricht der in der TA-Studie dargestellten Handlungsalternative 2.

Im Kapitel „Ausblick“ fordern die TAB-Autoren die Präsenz deutscher Vertreter in den Gremien der ICAO und EU, um „eigene Beiträge einzubringen und nationale Interessen zu vertreten“. BKA und BSI sind seit Jahren bei ICAO, der EU sowie der Normungsorganisation ISO aktiv und gestalten insbesondere die technischen Spezifikationen für „Biometrie in Ausweisdokumenten“ maßgeblich mit. So ist es insbesondere dem deutschen Engagement in diesen Gremien zu verdanken, dass die datenschutzrechtlich relevante Gefahr des unbemerkten Auslesens der RF-Chips der Pässe durch den Zugriffsschutzmechanismus „Basic Access Control“ wirksam unterbunden wird und dieser Schutzmechanismus für EU-Pässe verbindlich vorgeschrieben ist, ebenso wie EAC für den Schutz der Fingerabdrücke.