AIRPORT-SECURITY –

Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen

Ein Diskussionsbeitrag

Impressum

Stiftung DFK – Deutsches Forum für Kriminalprävention
Direktor: Norbert Seitz
Dahlmannstr. 5-7

53113 Bonn

DFK-Arbeitskreis Kriminalprävention und Biometrie

erarbeitet von:

ZVEI-Arbeitsgruppe Biometrietechnik
und
DFK-Arbeitsgruppe Biometrie und Recht

Redaktion: Jürgen Junghanns (BHE), Ulrich Krienen (ZVEI), Norbert Küster (ZVEI/DFK)

Bildnachweise:
Abdruck mit freundlicher Genehmigung von
Interflex (Abb.1, 2; 4); Viisage Technology (Abb. 3); IR Europe (RSI) (Abb.5); byometric (Abb.7)

Zusammenfassung

Sicherheit auf Flughäfen – ein Anliegen der Bundesregierung

Die Stiftung DFK – Deutsches Forum für Kriminalprävention greift mit dem hier vorgelegten Konzept „Airport-Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen“ ein Anliegen der Bundesregierung auf. Lutz Diwell, Staatssekretär im Bundesministerium des Innern, hat es in seiner Rede zum 5. Internationalen Airportforum am 11. September 2003 in Frankfurt so formuliert:

> „*Es ist mir ein Anliegen, daß zur Erhöhung der Sicherheit die uns zur Verfügung stehenden und geeigneten technologischen Entwicklungen genutzt werden. Mit der Biometrie ist in den letzten Jahren eine neue Schlüsseltechnologie entstanden, die hierbei erhebliche Sicherheitsgewinne ermöglichen kann. Biometrische Merkmale – seien es Fingerabdrücke, Lichtbilder oder Iris-Fotos – können die Identifikation einreisender Personen verbessern. Daneben sind sie ein geeignetes Hilfsmittel zur eindeutigen Zuordnung von Dokumenten zu ihren Inhabern. Mit Hilfe der Biometrie können und werden wir eine neue Sicherheitsinfrastruktur aufbauen.*“

DFK-Konzept: Ergänzung zu Maßnahmen im hoheitlichen Bereich

Parallel zu dem von Staatssekretär Diwell angesprochenen Bereich hoheitlicher Kontrollen sollen mit diesem Konzept die neuen technischen Möglichkeiten der Biometrie zur Erhöhung der Sicherheit im nicht hoheitlichen Bereich eines Flughafens gezeigt werden. Zugleich geht es darum, aktuelle Diskussionen und Vorschläge zu strukturieren.

Sicherheit ist ein Ziel aller Infrastruktureinrichtungen, da sie Grundvoraussetzung für deren wirtschaftlichen Erfolg ist. Passagiere, also Kunden, die sich nicht sicher fühlen, meiden Flugreisen so weit wie möglich oder wählen Flughäfen, die den gewünschten Sicherheitsstandard bei optimalem Komfort bieten.

Begrenzung steigender Aufwendungen der Unternehmen

Fluggesellschaften und Flughafenbetreiber sehen sich mit organisatorisch und finanziell überbordenden Aufwendungen durch neue staatliche Sicherheitsanforderungen konfrontiert. Diese führen sowohl zu höheren direkten Kosten pro Flug als auch zu deutlich verlängerten Abfertigungszeiten.

Daher müssen neue sicherheitstechnische Maßnahmen in die vorhandenen Abläufe integriert werden. Sie dürfen keine vermeidbare zusätzliche Belastung beinhalten, und mit den verwendeten Techniken sollte sich zusätzlicher Nutzen sowohl für Kunden als auch Betreiber einstellen.

Die in diesem Konzept vorgeschlagenen Maßnahmen gehen von den Auflagen aus, die von allen Betreibern von Verkehrsflughäfen in Europa auf-

EU-Verordnung zur Flughafensicherheit als Ausgangspunkt

grund der **Verordnung (EG) Nr. 2320/2002** des Europäischen Parlaments und Rates vom 16.12.2002 zur Festlegung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt umgesetzt und in die Arbeitsabläufe des Flughafenbetriebs integriert werden müssen. Die volle Wirksamkeit der in der EU-Verordnung vorgesehenen Maßnahmen war bis zum 19. Januar 2004 herzustellen. Ergänzend wird Bezug genommen auf das geplante Luftsicherheitsgesetz (LuftSiGE), dessen Entwurf vom Bundeskabinett am 7.11.2003 in das parlamentarische Verfahren eingebracht wurde (Artikel 1 des „Gesetzes zur Neuregelung von Luftsicherheitsaufgaben"; liegt inzwischen mit Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung als Bundestagsdrucksache 15/2361 vom 14.1.2004 vor; die 1. Lesung des Gesetzentwurfs im Deutschen Bundestag fand am 30.01.2004 statt.).

Kernpunkte des DFK-Konzeptes: Flughafenausweis und Flugpaß

Kernpunkte des DFK-Konzeptes sind die Einführung eines standardisierten **„Flughafenausweises" für Mitarbeiter und berufsbedingte Dauerbesucher** von Flughafenbetreibern, Fluggesellschaften und sonstigen im Sicherheitsbereich tätigen Unternehmen. Außerdem wird die Einführung eines **„Flugpasses" für Passagiere der gewerblichen Luftfahrt** auf freiwilliger Basis vorgeschlagen. Beide Ausweise tragen biometrische Merkmale ihrer berechtigten Inhaber . Damit kann an entsprechend ausgerüsteten Kontrollpunkten überprüft werden, ob der aktuelle Ausweisbenutzer der rechtmäßige Ausweisinhaber ist. Die Kontrollstellen befinden sich für Mitarbeiter dezentral über das gesamte Flughafengelände verteilt, für Passagiere an jedem Übergang vom Check-In zum Gate, insbesondere aber an allen Übergängen vom öffentlich zugänglichen zum nicht öffentlich zugänglichen Bereich, also etwa zu Sicherheitsbereichen wie der sogenannten Luftzone eines Flughafens.

Flughafenausweis für Mitarbeiter mit biometrischen Daten

Der mit biometrischen Daten aufgeladene Ausweis ist ein technisch weiter entwickelter „Flughafenausweis", wie er für alle Mitarbeiter, insbesondere jene, die im Sicherheitsbereich eines Flughafens tätig sind, durch die genannte EU-Verordnung nun vorgeschrieben ist. Fach- und Dauerbesucher sollen ihn unter den gleichen Voraussetzungen erhalten. Der Ausweis wird entsprechend den Vorgaben der EU-Verordnung nur nach vorheriger amtlicher Zuverlässigkeitskontrolle vom Flughafenbetreiber ausgegeben. Mit ihm können sich Berechtigte im für sie freigegebenen Teil der Sicherheitszone eines Flughafens ohne autorisierte Begleitung bewegen.

Smart Cards mit RFID-Chip

Auf Grund ihrer inzwischen fortgeschrittenen technischen Reife werden **„prozessorgestützte Smart Cards mit RFID („Radio Frequency Identification")-Technik"** vorgeschlagen. Das sind Ausweiskarten, die berührungslos mit einem entsprechenden Leser arbeiten. Aufgrund der international stark gestiegenen Anforderungen und Nachfrage hat die Entwicklung der Hard- und Software solcher Smart Cards mit integriertem RFID-Speicherchip in jüngster Zeit starke Fortschritte gemacht. Ihre Speicherkapazität liegt derzeit bei 32kB. Außer Daten für verschiedene biometrische

Verifikationsverfahren lassen sich Zugriffsberechtigungen und Sicherheitsapplikationen ebenso speichern wie Daten über Zutrittsberechtigungen zu Sicherheitsbereichen oder das ausgebende Unternehmen.

Ziel: Verifikation des Kartennutzers

Biometrische Erkennungsmethoden und deren Integration in bestehende Sicherheitseinrichtungen dienen **der „Verifikation" des Kartennutzers**. „Verifikation" bedeutet in diesem Zusammenhang die Überprüfung, ob beim aktuellen Vorgang der Kartennutzer mit dem für diese Karte hinterlegten und/oder mit den auf der Karte selbst gespeicherten Kenndaten des Berechtigten identisch ist.

Kostendämpfung durch Teilautomatisierung

Diese Sicherheitseinrichtungen wiederum haben eine definierte Schnittstelle zu den prozeßorientierten Systemen am jeweiligen Kontrollpunkt.

Vorteil: dezentrale, automatische Verifikation

Die vorgeschlagenen Maßnahmen sollen eine Teilautomatisierung bei den sicherheitsrelevanten Prozeduren ermöglichen, die zu mehr Effizienz trotz höherer Sicherheitsstandards führen. Für Flughafenbetreiber und Fluggesellschaften soll auf diese Weise ein wirtschaftlicher Betrieb möglich bleiben. Mitarbeiter und zum Teil auch Fluggäste sollen von Prozeduren befreit werden können, die häufig als sehr lästig empfunden werden, jedoch zur Erhöhung der Sicherheit nichts Wesentliches beitragen.

Flugpaß mit biometrischen Daten für Passagiere zur Verhinderung des Bordkartentauschs

Der entscheidende Vorteil eines solchen Ausweises für Mitarbeiter und Dauerbesucher liegt in der Möglichkeit einer dezentralen, automatischen Verifikation des Nutzers. Gleichzeitig erscheint denkbar, für derart ausgestattete, verifizierte Ausweisnutzer auf die sonst durch die EU-Verordnung vorgeschriebene lückenlose physische Kontrolle der Person und der Überprüfung der von ihr mitgeführten Gegenstände zu verzichten, da die Person schon amtlich auf ihre Vertrauenswürdigkeit überprüft wurde. Diese Kontrollen könnten für solche überprüften und für vertrauenswürdig befundenen Personen auf die in der Verordnung vorgesehenen „fortlaufenden, angemessenen Stichprobendurchsuchungen" beschränkt werden.
Allerdings erlaubt die gegenwärtige Regelung der EU-Verordnung seit Ablauf der Übergangsperiode am 19.01.2004 einen solchen (partiellen) Verzicht auf physische Personenkontrollen nicht. Insofern enthält das DFK-Konzept zugleich einen Vorschlag, bei der anstehenden Revision der EU-Verordnung den Mitgliedstaaten eine flexiblere Handhabung der konkreten Sicherheitsmaßnahmen zu erlauben, wenn sie durch Nutzung neuartiger Techniken das bisherige Sicherheitsniveau übertreffen können.

Der in diesem Konzept außerdem vorgeschlagene neuartige „Flugpaß" für Passagiere arbeitet auf gleicher Basis, hat allerdings einen gegenüber dem Mitarbeiterausweis stark eingeschränkten und abweichenden Einsatzbereich. Zwei Aspekte sprechen für den Flugpaß: Zur Erhöhung der Flughafensicherheit und unter kriminalpräventiven Gesichtspunkten muß zukünftig gewährleistet sein, daß die in einem Flugzeug beförderten Personen iden-

tisch sind mit denen, die eingecheckt wurden. Dies ist heute – nach Angaben von Fluggesellschaften – nicht gewährleistet und auch tatsächlich relativ häufig nicht der Fall, weil nach dem Check-In die Bordkarten getauscht oder einer anderen Person ausgehändigt werden können, die dann das Flugzeug betritt. Dies schafft immer wieder erhebliche Sicherheitsprobleme Mit einem Flugpaß, auf dem die biometrischen Daten des eingecheckten Fluggastes gespeichert sind, kann dies vermieden werden.

Unterschiedliche Einsatzarten des Flugpasses

Ein solcher Flugpaß kann unter Sicherheitsgesichtspunkten auf unterschiedliche Weise genutzt werden: Einerseits (ausschließlich) als Boardingkarte, andererseits aber, auf Grundlage vertraglicher Vereinbarungen zwischen einem Fluggast und einer oder mehreren Fluggesellschaften und/oder einem und mehreren Flughafenbetreibern, als Dauerausweis zur Erleichterung des Check-Ins, des Boardings im Selbstabfertigungsverfahren, als Zutrittsausweis für Lounges und schließlich noch zur verstärkten Kundenbindung.

DFK-Konzept verfolgt gesamtheitlichen Ansatz zur Verbesserung der Flughafensicherheit

Der Grundansatz dieses Konzeptes zielt darauf ab, die wesentlichen Bereiche des gesamten Flughafenbetriebes im Zusammenhang und die Arbeitsabläufe prozeßorientiert unter Sicherheitsgesichtspunkten zu betrachten und unter vorrangig kriminalpräventiven Gesichtspunkten Vorschläge zur Erhöhung der Sicherheit des Flughafen- und Flugbetriebes durch Nutzung neuartiger technischer Möglichkeiten zu unterbreiten. Daher betrachtet dieses Konzept außer den Mitarbeitern auch andere Personengruppen, die nicht öffentlich zugängliche Bereiche eines Flughafens regelmäßig besuchen müssen, nämlich Fachbesucher verschiedener Kategorien, aber auch das allgemeine Publikum, das die öffentlich zugänglichen Ankunfts- und Abflughallen in großer Zahl benutzt.

Besucherverwaltungssystem für nicht öffentlich zugängliche Bereiche

Videoüberwachung für Ankunfts- und Abflughallen

Datenschutz verlangt genaue Prüfung im Einzelfall

Für alle Besucher nicht öffentlich zugänglicher Flughafenbereiche wird die konsequente Nutzung von Besucherverwaltungssystemen vorgeschlagen, die – für gelegentliche Besucher – mit Ausweisen ohne biometrische Daten der Besucher auskommen. Lediglich für Dauer- und Fachbesucher, die über längere Zeit und regelmäßig wiederkehrend den Sicherheitsbereich betreten müssen, sollen, wie für Mitarbeiter, Flughafenausweise mit biometrischen Daten des Berechtigten ausgegeben werden.

Für die Ankunfts- und Abflughallen werden Videoüberwachungsmaßnahmen vorgeschlagen, die mit biometrischen Gesichtserkennungssystemen ausgerüstet sind, die unter definierten Randbedingungen nur das Bild einer mit Hausverbot belegten und/oder gesuchten Person anzeigen, wenn diese einen der Kontrollpunkte passiert.

In dem Konzept werden – für die verschiedenen Anwendungszwecke getrennt – auch die rechtlichen, insbesondere datenschutzrechtlichen Rahmenbedingungen betrachtet und Hinweise für notwendige Klärungen gegeben. Die Prüfung der rechtlichen Rahmenbedingungen muß kursorisch

bleiben und sich notwendigerweise mit Hinweisen begnügen, weil eine konkrete rechtliche Prüfung detaillierte Festlegungen der organisatorischen Abläufe und der technischen Verfahren voraussetzen würde. Das kann und soll hier nicht geleistet werden. Die Anwendung technischer Maßnahmen zur Personenkontrolle ist politisch und rechtlich umstritten. Insbesondere von Seiten der Datenschutzbehörden des Bundes und der Länder werden immer wieder Bedenken geltend gemacht. Sie müssen in der konkreten Anwendung berücksichtigt und – bezogen auf den Einzelfall – genau geprüft werden.

DFK-Konzept: Fachdiskussion fördern

Die Stiftung DFK – Deutsches Forum für Kriminalprävention beabsichtigt mit der Vorlage dieses Konzeptvorschlages, die gegenwärtig geführten vielfältigen Diskussionen um die Nutzung technischer Verfahren zur Verbesserung der Sicherheit auf Flughäfen und des Flugbetriebs zu strukturieren. So soll die weitere Diskussion auf der Fachebene und unter Fachleuten vorangebracht werden.

Einladung an alle Interessierten zu weiteren Beiträgen

Dieses Konzept dient des weiteren der Vorbereitung einer Veranstaltung des DFK zum Thema. Dazu ist es unabweisbar notwendig, Vorschläge zur Nutzung biometrischer Verfahren in technischer und organisatorischer Hinsicht zu konkretisieren.

Dies bedeutet aber nicht, daß die Stiftung DFK – Deutsches Forum für Kriminalprävention die hier zur Diskussion gestellten technischen und organisatorischen Maßnahmen für den besten oder gar einzig gangbaren Weg hält. Der Vorstand der Stiftung DFK – Deutsches Forum für Kriminalprävention und der DFK-Arbeitskreis Kriminalprävention und Biometrie, der die Erarbeitung dieses Konzeptvorschlages verantwortet, sind für weitere Anregungen und jeden Diskussionsbeitrag zum Thema dankbar.

Inhaltsverzeichnis

D. Sicherung öffentlich zugänglicher Bereiche des Flughafens

1. Ausgangslage
2. Rechtliche Rahmenbedingungen
3. Einsatz von Videoüberwachung zur Personenerkennung/ Personensuche

E. Grundlageninformationen:
Methoden der biometrischen Erkennung

1. Allgemeines zu kooperativen Verfahren
2. Gesichtserkennung (kooperativ)
3. Handgeometrie-Erkennung
4. Fingerabdruck-Erkennung
5. Iris-Erkennung

F. Anhang:
Normung und Standardisierung biometrischer Verfahren

Einleitung

Sicherheit ist nie absolut und statisch

Sicherheit ist nichts, was in einem absoluten, endgültigen Sinne beschreibbar oder gar erreichbar wäre. Sicherheit ist vielmehr immer im Zusammenhang mit der tatsächlichen oder zu erwartenden Gefahrenlage zu definieren und anzustreben. In komplexen organisatorisch-technischen Prozessen und Abläufen wie denen auf Flughäfen müssen präventive Maßnahmen zur effektiven Verhinderung bzw. Beherrschung zu erwartender Gefahrenlagen integriert sein. Alle Maßnahmen müssen für sich und in ihrer Gesamtheit den Beteiligten darüber hinaus subjektiv ein Sicherheitsgefühl vermitteln.

Sicherheit im Flughafenbereich betrifft viele Gruppen

Der Wunsch nach Sicherheit steht bei den meisten Menschen an vorderster Stelle, besonders, wenn sie auf Reisen und damit nicht in ihrer gewohnten Umgebung sind. Die Erfüllung dieses Wunsches gehört teils zum Kundendienst bzw. zur Attraktivität der Betreiber von Reise- und Tourismuseinrichtungen, teils fällt sie aber auch unter die hoheitlichen Aufgaben staatlicher Behörden.

Bedrohungsabwehr nicht nur Staatsinteresse

Die Sicherheit im Flughafenbereich betrifft nicht nur Fluggäste, sondern zahlreiche andere Personen, etwa Mitarbeiter des Flughafenbetreibers und diverser Fremdfirmen, das fliegende Personal und sonstige Mitarbeiter der Fluggesellschaften, darüber hinaus auch verschiedenste Arten von Besuchern. Angesichts dieser Vielzahl von Personen, die den Flughafenbereich aus den verschiedensten Gründen und in unterschiedlichster Weise nutzen sowie der Ausdehnung und Komplexität des Flughafengeländes und der Gebäude – jedenfalls an stärker frequentierten Flughäfen – sind die Anforderungen an die Sicherheitssysteme enorm. In den letzten Jahren sind die Flughafenbetreiber wie auch die Fluggesellschaften immer größeren Herausforderungen ausgesetzt, die aus kriminellen Handlungen resultieren – namentlich illegale Immigration, Handel mit Rauschgift, Schmuggel, Diebstahl und Terrorismus.

DFK-Konzept für nicht hoheitlichen Bereich

Angesichts der Komplexität der Bedrohung kann es nicht nur im Interesse des Staates sein, mit seinen eigenen hoheitlichen Strukturen die Sicherheit auf Flughäfen für alle Beteiligten zu erhöhen. Vielmehr verfolgen auch Flughafenbetreiber und Fluggesellschaften dieses Ziel. Gleichzeitig müssen sie aber darauf achten, daß Sicherheitsmaßnahmen nicht ihre Kernaufgabe verdrängen, als Unternehmen Gewinne zu erwirtschaften. Flughafenbetreiber und Fluggesellschaften müssen daher stärker als der Staat darauf bedacht sein, ein hohes Sicherheitsniveau möglichst effizient und ohne unzumutbare Beeinträchtigung des Reisekomforts der Passagiere zu erreichen. Langfristig sind technische Maßnahmen dem Einsatz von Personal unter Kostengesichtspunkten vorzuziehen.

In diesem Vorschlag sollen ohne Präjudiz und ohne irgendeine Präferenz in strukturierter Form Möglichkeiten aufgezeigt werden, wie Flughafenbetreiber und Fluggesellschaften im nicht hoheitlichen Bereich, für den sie rechtlich vorrangig verantwortlich sind, das Ziel hoher Sicherheit kostengünstig

und unter Wahrung hoher Flexibilität durch neuartige technische Maßnahmen erreichen können.

Hoheitliche Aufgaben, die auf Flughäfen ebenfalls anfallen, wie zum Beispiel Ein- und Ausreisekontrolle („Bordercontrol“; Identitätsprüfung) sind nicht Gegenstand dieses Konzeptes. Eine Koordination der Kontrollen, die nach diesem Konzept im nicht-hoheitlichen Bereich einerseits, im hoheitlichen Bereich andererseits anfallen, wird hier ebenfalls nicht erörtert, weil sie in jedem Fall einer gesetzlichen Grundlage bedürfte.

Nutzung biometrischer Daten in amtlichen Ausweisen für Kontrollen im privatrechtlichen Bereich umstritten

Dies gilt auch für die Nutzung biometrischer Daten, die künftig in amtlichen Ausweisen wie Personalausweisen und Reisepässen gespeichert werden, durch private Organisationen wie Flughafenbetreiber und Fluggesellschaften, sowie umgekehrt für eine etwaige Nutzung biometrischer Daten in Ausweisen privater Organisationen („Flugausweis“ und „Flugpaß“) durch den Staat für hoheitliche Zwecke, zum Beispiel für Personenkontrolle oder Strafverfolgung. Da es zumindest für den zweiten Fall gesetzlicher Regelungen bedürfte, die bisher fehlen und für derartige Fallgestaltungen hier auch nicht gefordert werden sollen, bleiben bewußt viele technisch denkbare Anwendungen außer Betracht. Von Seiten des Bundesbeauftragten für den Datenschutz wurden aber auch für den ersten Fall Bedenken gegen eine solche private Nutzung von in amtlichen Ausweisen enthaltenen biometrischen Daten des Inhabers vorgetragen, weil die vorgeschlagenen technischen Verfahren zu einer, wenn auch kurzzeitigen Speicherung der biometrischen Daten des Inhabers außerhalb des Ausweises führen.

Private Sammlungen biometrischer Daten vermeidbar

Allerdings kann und soll an dieser Stelle nicht unerwähnt bleiben, daß im Rahmen des DFK-internen Arbeitsprozesses zur Erstellung dieses Konzeptes auch auf erhebliche datenschutzrechtliche Vorteile verwiesen wurde, die eine Nutzung von in amtlichen Ausweisen künftig enthaltenen biometrischen Daten des berechtigten Inhabers für die „Verifikation“ im Rahmen privater Kontrollsysteme mit sich brächte, würde der deutsche Gesetzgeber dies – wie die entsprechende Nutzung bisheriger Lichtbildausweise auch – erlauben. Es wären insbesondere zusätzliche private Sammlungen biometrischer Daten in vielen Fällen überflüssig, die bei einem parallelen Betrieb hoheitlicher und privater biometrischer Ausweissysteme – wovon das hier vorgelegte Konzept ausgeht – unvermeidbar sind. Zuverlässige Verifikationsverfahren könnten dann etwa im Passagierbetrieb auch außerhalb des Vielfliegerbereichs leichter und daher mit einem für den gesamten Flugbetrieb potentiell größeren Sicherheitsgewinn durchgeführt werden. Beim Check-In könnte der Fluggast bereits verifiziert oder auch identifiziert werden, statt – wie auch in diesem Konzept vorgeschlagen – dem beim Check-In vorgelegten Ausweis, soweit er überhaupt vorgelegt wird, ohne weiteres zu glauben und so sicherzustellen, daß die eingecheckte Person später auch das (richtige) Flugzeug besteigt.

Weitere rechtliche Klärung notwendig

Eine entsprechende Freigabe der technischen Nutzung der künftig amtlich bei der Ausstellung von Reisepässen und Bundespersonalausweisen erhobenen biometrischen Daten auch für private Zwecke durch den Gesetzge-

ber und die Behörden sollte daher regierungsseitig überlegt werden. Den DFK-Gremien schien eine weitere rechtliche Klärung notwendig, ob und inwieweit die Nutzung von Systemen zur Erkennung biometrischer Daten in amtlichen Ausweisen für Sicherheitskontrollen im privaten Bereich einerseits durch den Staat erlaubt werden könnte oder müßte, andererseits überhaupt eingeschränkt werden dürfte, steht doch einer solchen Nutzung der herkömmlichen amtlichen Ausweispapiere schon derzeit tatsächlich nichts entgegen, geschieht es doch allenthalben jedenfalls in der eingeschränkten Form einer manuellen Kontrolle und zur „Verifikation“ in Form eines visuellen Vergleichs des Ausweisfotos mit dem Gesicht des Benutzers. Bislang sind dagegen keine Bedenken laut geworden. Allerdings werden die Ausweisdaten etwa bei Einlaßkontrollen im privaten Bereich bislang auch nicht automatisch gespeichert. Insofern sind gewisse Unterschiede der technischen Verfahren erkennbar.

Für das hier vorgelegte Konzept werden von der künftigen Notwendigkeit getrennter Systeme ausgegangen und insofern das Ergebnis einer noch durchzuführenden, genaueren rechtlichen Untersuchung dieses Aspektes ebenso wie eine etwa notwendige politische Entscheidung des Gesetzgebers und der Bundesregierung zu dieser Frage bewußt nicht antizipiert.

Beispiele für biometrische Anwendungen

Der Arbeitskreis Kriminalprävention und Biometrie der Stiftung DFK – Deutsches Forum für Kriminalprävention will mit dem hier vorgelegten Konzept beispielhaft die Einsatzmöglichkeiten neuartiger Techniken im Rahmen kriminalpräventiver Zielsetzungen zeigen. Der Einsatzort „Flughafen“ wurde unter verschiedenen Gesichtspunkten ausgewählt: Zum einen wegen des aktuellen Handlungsbedarfs, zum anderen wegen des – bei aller Komplexität eines einzelnen Flughafenbetriebs – gleichwohl begrenzten Anwendungsfeldes.

DFK-Konzept ohne technische Details

Der DFK-Arbeitskreis Kriminalprävention und Biometrie verfolgt mit diesem Konzept einen systematischen und ganzheitlichen Ansatz. Es werden bewußt alle Bereiche eines Flughafenbetriebs betrachtet. Es sollen nicht lediglich Vorschläge unterbreitet werden, die – aus welchen Gründen auch immer – aktuell auf möglichst wenig Widerspruch stoßen und sich deshalb am leichtesten kurzfristig durchsetzen ließen. Ob überhaupt einige und ggf. welche der hier zur Diskussion gestellten Anwendungen in welcher Reihenfolge umgesetzt werden – die Entscheidung darüber ist nicht Sache der Stiftung DFK – Deutsches Forum für Kriminalprävention. Das DFK versteht sich zu diesem Thema lediglich als Ideengeber und Anreger.

Das DFK betrachtet es daher auch nicht als seine Aufgabe, technische Detailkonzepte für bestimmte Anwendungen auszuarbeiten und insbesondere auch nicht, alle rechtlichen oder auch nur datenschutzrechtlichen Rahmenbedingungen bestimmter technischer Einsatzvarianten zu klären. Derlei muß jeweils im unmittelbaren Zusammenhang mit einer konkreten Einsatzplanung geklärt werden. Die in diesem Konzept enthaltenen Hinweise zu den rechtlichen Rahmenbedingungen, vor allem zum Datenschutz, sind daher nur allgemeiner und grundsätzlicher Natur. Sie sollen

verdeutlichen, daß die rechtlichen Rahmenbedingungen in bestimmten Einsatzgebieten unterschiedlich sind und nicht davon ausgegangen werden kann, daß alle rechtlichen Einsatzfragen bereits geklärt wären.

Formale Grundlagen und Begriffe

Die nachfolgende Ausarbeitung bezieht sich ausdrücklich auf die Flughafensicherheitsverordnung der Europäischen Union (Verordnung (EG) Nr. 2320/2002 des Europäischen Parlamentes und des Rates vom 16.12.02 zur Festlegung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt, Amtsblatt EG Nr. L-355 vom 30.12.2002 S. 1 ff.). Diese EU-Verordnung gilt mit unmittelbarer Wirkung jedermann gegenüber in der gesamten Europäischen Union, ohne dass es eines nationalen Umsetzungsgesetzes bedürfte (Art. 249 EGV).

Die in diesem Konzept des DFK-Arbeitskreises Kriminalität und Biometrie benutzten Begriffe werden in dem Sinne verwendet, wie sie der Anhang der vorgenannten Verordnung festlegt. Danach sind z.B.:

- die „Luftseite“ die Bewegungsflächen eines Flughafens, angrenzendes Gelände und angrenzende Gebäude bzw. Teile davon,
- die „Landseite“ der Bereich eines Flughafens, bei dem es sich nicht um die Luftseite handelt und der alle öffentlich zugänglichen Bereiche umfaßt,
- ein „gewerblicher Flug“ ein Flug oder eine Flugverkehrsleistung im Linien- oder Bedarfsdienst der/die von der Öffentlichkeit oder privaten Gruppen gegen Entgelt genutzt werden kann,
- der „Sicherheitsbereich“ die Luftseite eines Flughafens, deren Zugang kontrolliert wird, um die Sicherheit der Zivilluftfahrt zu gewährleisten. Zu den Sicherheitsbereichen zählen u.a. alle Abflugbereiche zwischen den Sicherheitskontrollpunkten und dem Luftfahrzeug, Gepäckabfertigungsbereiche, Fracht-Lagerhallen, Postzentren und Einrichtungen der Reinigungs- und Bordverpflegungsdienste auf der Luftseite,
- das „Abfertigungsgebäude“ das Hauptgebäude oder die Gruppe von Gebäuden für die Abfertigung der Fluggäste und der Fracht im gewerblichen Luftverkehr und das Besteigen der Luftfahrzeuge.

Für etwaige weitere Begriffe wird auf die Begriffsbestimmungen unter Ziffer 1. im Anhang der vorgenannten Verordnung verwiesen.

Ergänzend wird Bezug genommen auf das geplante Luftsicherheitsgesetz (LuftSiGE), dessen Entwurf vom Bundeskabinett am 7.11.2003 in das parlamentarische Verfahren eingebracht wurde (Artikel 1 des „Gesetzes zur Neuregelung von Luftsicherheitsaufgaben“; liegt inzwischen mit Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung als Bundestagsdrucksache 15/2361 vom 14.1.2004 vor; die 1. Lesung des Gesetzentwurfs im Deutschen Bundestag fand am 30.01.2004 statt).

„ICAO“ ist die „International Civil Aviation Organisation“, eine Staatenorganisation mit derzeit 185 Mitgliedern und Sitz in Montreal, gegründet 1944 durch das Abkommen von Montreal. Näheres findet sich im Internet unter www.icao.int .

A. „Flughafenausweis“ mit biometrischen Merkmalen für Mitarbeiter

1. Ausgangslage und Rahmenbedingungen

1.1 Ist-Zustand

Hochkomplexe Strukturen erfordern genaue Differenzierung

Flughäfen bestehen nicht nur aus Terminals sowie Start- und Landebahnen, selbst wenn dies Fluggästen oftmals so erscheinen mag. Flughäfen verfügen ebenso über Büro- und Verwaltungstrakte, Schulungs- und Aufenthaltsräume, Wartungshallen, Sicherheitszonen und den Tower, um nur einige Bereiche zu nennen. Nicht alle dieser Bereiche sind für Besucher absolut gesperrt. Zulieferer bringen Waren, Geschäftspartner haben Termine auf dem Flughafengelände, Besuchergruppen werden herumgeführt. Wie lassen sich hier die Sicherheit verbessern und insbesondere Straftaten, nicht nur, aber in erster Linie mit potentieller Gefährdung des Flugverkehrs im weitesten Sinne verhindern?

Relevante Personengruppen

Die Komplexität der Verhältnisse am Flughafen erfordert eine Differenzierung, vorzugsweise zunächst durch eine Einteilung der Personenkreise am Flughafen. Es lassen sich folgende Personengruppen unterscheiden:

A) Mitarbeiter des Flughafenbetreibers (Festangestellte, Leihkräfte)
B) vertraglich an den Flughafenbetreiber gebundene Fremdunternehmer und deren Mitarbeiter, z.B. Bodenpersonal (Ground Services), Reiseveranstalter (Ticketverkauf), Ladenpersonal, Gastronomiekräfte
C) Mitarbeiter der Fluggesellschaften (Flug- und Servicepersonal)
D) Zulieferer
E) Behörden, z.B. Bundesgrenzschutz, Polizei, Zoll, Flugsicherung
F) Fluggäste, Passagiere
G) Besucher

Gegenwärtig unzureichende Verifikation

Gegenwärtig konzentrieren sich viele Sicherheitsmaßnahmen auf die Kontrolle der Passagiere. Doch was ist mit den Tausenden Beschäftigten? Zwar müssen alle Beschäftigten bei ihrer Einstellung oder ersten Beschäftigung am Flughafen ein polizeiliches Führungszeugnis vorlegen. Wer aber einmal einen entsprechenden Ausweis besitzt, hat unbegrenzt Zutritt zum Vorfeld – Mechaniker, Reinigungskräfte, Caterer. Genau genommen werden diese Zutrittsrechte auch bisher schon personenbezogen vergeben. Da der Ausweis am Ort der Prüfung den Karteninhaber „repräsentiert“, ist der augenblickliche Benutzer des Ausweises im Besitz der Zutrittsrechte, gleichgültig, ob er der legale Inhaber ist oder den Ausweis nur gefunden, geliehen, gefälscht oder gestohlen hat. Diese Sicherheitslücke gerade im sensiblen Bereich eines Flughafens muß geschlossen werden, indem verläßlich überprüft wird, ob der aktuelle Ausweisnutzer tatsächlich mit der Person übereinstimmt, für die er ausgestellt wurde.

Effektive Zutrittskontrolle für sensible Betriebsbereiche notwendig

Es wird davon ausgegangen, daß sich die Infrastruktur-, Technik- und Verwaltungsbereiche im „Nichtöffentlichen Bereich“ befinden. Auch wenn es sich hierbei nicht im Sinne der Begriffsbestimmungen der EU-Verordnung – notwendigerweise – um den „Sicherheitsbereich“ eines Flughafens, nämlich die „Luftseite“, handelt, sind dies doch in der Regel Bereiche, die im Sinne der EU-Verordnung als „sensibel“ für die Betriebssicherheit des Flughafens, seiner Benutzer und die Sicherheit des Flugverkehrs insgesamt einzustufen sind. Schon jetzt ist es daher weithin üblich, den Zutritt zu diesem „sensiblen“ Flughafenbereich einer Zutrittskontrolle zu unterwerfen.

ITK-Strukturen besonders sensibel

Sicherheitstechnisch kommt dem zentralen Informations- und Kommunikationstechnikbereich aufgrund der vollständigen IT-Durchdringung und Vernetzung des Flughafenbetriebes und des Luftverkehrs eine große Bedeutung zu. Die Besonderheit dieses Bereiches ist, daß zwar die Technikzentralen (Rechenzentrum, Serverparks) in der Regel im nicht öffentlich zugänglichen Bereich eines Flughafens angesiedelt sind, aber prinzipiell über die in allen öffentlichen und nichtöffentlichen Bereichen stehenden Terminals vielfältige Zugriffe zumindest auf die Daten-Infrastruktur möglich sind.

Schutz vor unbefugtem Zugang zu ITK-Netzen

Somit muß der Zugang zu diesen Netzen unabhängig von der Lokation gleichwertig geschützt werden. Dies betrifft insbesondere die Authentifizierung der Bediener der PCs. Berücksichtigt werden muß zudem die Tatsache, daß nicht nur Festangestellte des Flughafenbetriebs, der Fluggesellschaften oder dort angesiedelten Unternehmen beschäftigt sind, sondern auch externe Dienstleister und Aushilfskräfte bzw. Mitarbeiter von Zeitarbeitsunternehmen, die häufig wechseln und oft nur einmal kurzzeitig auf dem Flughafen tätig werden. Der Faktor der unterschiedlich ausgeprägten Mitarbeiterfluktuation darf nicht zu Blockade oder Schwächung der einzuführenden Sicherheitsmaßnahmen führen.

EU-Verordnung stellt neue Anforderungen

EU-Vorgaben zur Flughafenplanung

1.2 Anforderungen der EU

Die EU-Verordnung über die Sicherheit in der Zivilluftfahrt stellt an die Sicherheitsmaßnahmen auf Flughäfen neue, deutlich höhere Anforderungen. Vor allem werden öffentlich zugängliche Bereiche von anderen Bereichen, insbesondere Sicherheitsbereichen, strikt getrennt. Allgemein gilt der luftseitige Bereich eines Flughafens als Sicherheitsbereich. Doch können darüber hinaus von den Flughafenbetreibern weitere Zonen des Geländes als „Sicherheitsbereich“ ausgewiesen werden. Dies wird in der Regel überall dort notwendig sein, wo betriebsnotwendige technische Infrastrukturen geschützt werden müssen.

Die EU-Verordnung schreibt vor, daß Flughäfen so zu planen und auszulegen sind, daß „Sicherheitskontrollen für Fluggäste, Gepäck, Fracht ... der Luftfahrtunternehmen“, „Sicherung und Kontrolle des Zugangs zur Luftseite, zu Sicherheitsbereichen und zu anderen sicherheitskritischen Bereichen und Einrichtungen des Flughafens“ und der „effiziente Einsatz von Sicherheitsausrüstungen“ gewährleistet sind. Land- und die luftseitige Bereiche

sind voneinander abzugrenzen. Auf jedem Flughafen sind darüber hinaus Sicherheitsbereiche auszuweisen.

Der „Zugang“ zu Sicherheitsbereichen (Begriff der EU-VO) bzw. „sicherheitsempfindlichen Bereichen“, namentlich allen „sensiblen Teilen der sicherheitsempfindlichen Bereiche“ (beides lt. Terminologie des § 8 Abs.1 Nrn. 4 und 5 RegE LuftSiG) und Einrichtungen des Flughafens und zu „anderen luftseitigen Bereichen“ (Terminologie der EU-VO) ist jederzeit zu kontrollieren, „um den Zutritt Unbefugter zu verhindern“. Neben dieser reinen Zutrittskontrolle ist – seit Ablauf der Übergangsfrist am 19. Januar 2004 zwingend und ausnahmslos - eine physische Personenkontrolle vorzusehen, um sicherzustellen, daß „kein verbotener Gegenstand in einen Sicherheitsbereich oder an Bord eines Luftfahrzeuges gelangen kann“.

Pflicht zur lückenlosen Personenkontrolle bei Übertritt in einen Sicherheitsbereich

Das gesamte am Flughafen beschäftigte oder häufig am Flughafen verkehrende Personal einschließlich der Beschäftigten des Flughafenbetreibers und der Luftfahrtunternehmen sowie anderer Unternehmen und Stellen ist mit „Flughafenausweisen“ auszustatten. Diese enthalten wenigstens den Namen und ein Lichtbild des Inhabers und haben begrenzte Gültigkeitsdauer. Es können weitergehende Maßnahmen vom Flughafenbetreiber getroffen oder von den Behörden angeordnet werden. Der Flughafenausweis ist während der Dienstzeit jederzeit sichtbar zu tragen.

Amtliche Zuverlässigkeitsprüfung vorgeschaltet

Personal, das Zutritt zu Sicherheitsbereichen haben muß, ist – im Vorfeld der Erteilung eines Flughafenausweises – einer Zuverlässigkeitsprüfung durch die Sicherheitsbehörden zu unterziehen. Diese ist regelmäßig in relativ kurzen Abständen zu wiederholen. Weitere Einzelheiten dieser Zuverlässigkeitsprüfung sind zum Teil in der EU-Verordnung, ausführlicher in § 7 RegE LuftSiG festgelegt oder in einer noch vom Bundesminister des Innern mit Zustimmung des Bundesrates aufgrund von § 18 Abs.1 RegE LuftSiG zu schaffenden Rechtsverordnung später zu regeln.

Vertragsverhältnis als Grundlage

Bei jedem Übertritt von der Land- zur Luftseite, beim Zutritt zu Sicherheitsbereichen oder sicherheitskritischen Einrichtungen ist der Flughafenausweis zu kontrollieren. Dabei ist – wie zuvor dargestellt – gemäß ausdrücklicher Anordnung die Ausweisprüfung so vorzunehmen, daß der Zutritt Unbefugter wirksam und jederzeit verhindert wird.

1.3 Datenschutzrechtliche Situation beim „Flughafenausweis“ für Mitarbeiter

Die Luftseite sowie sonstige Sicherheitsbereiche und sicherheitskritischen Einrichtungen unterliegen generell einer Zutrittsbeschränkung zugunsten der Mitarbeiter des Flughafenbetreibers selbst, der Mitarbeiter von Drittfirmen, die wiederum in einem Vertragsverhältnis zum Flughafenbetreiber stehen, derjenigen von Luftfahrtunternehmen und sonstigen Fremdfirmen in deren Auftrag. In allen Fällen liegt Tätigkeiten einer solchen Person in ei-

nem sicherheitsrelevanten Flughafenbereich ein Arbeits- oder sonstiges Vertragsverhältnis zugrunde.

Im Rahmen eines solchen Vertragsverhältnisses sind in Ausführung der EU-Verordnung der Flughafenbetreiber sowie die Fluggesellschaften gezwungen – wenn bisher noch nicht geschehen –, in die Arbeitsverträge mit ihren Mitarbeitern eine Erklärung des Mitarbeiters aufzunehmen, daß dieser die notwendigen Sicherheitskontrollen beachtet und die nach der EU-Verordnung notwendigen und etwa darüber hinaus gehenden technischen Kontrollen akzeptiert. Art und Umfang können und müssen im Arbeitsvertrag genau festgelegt werden.

a. Zustimmung des Betriebsrates; Notwendigkeit einer Betriebsvereinbarung

Einführung biometrischer Zutrittskontrollen mitbestimmungspflichtig

Für die Einführung von biometrischen Sicherheitssystemen und Zugangskontrollen auf Basis solcher Systeme ist im übrigen die Zustimmung des Betriebsrates notwendig, da es sich um mitbestimmungspflichtige Systeme gemäß § 87 Abs.1 Nr.6 BetrVG handelt. Dies gilt jedenfalls, solange solche biometrischen Systeme vom Unternehmen auf freiwilliger Basis und nicht, wie jetzt lediglich die „Flughafenausweise“ als bloße Lichtbildausweise, in bestimmten Betriebsbereichen unmittelbar durch Gesetz oder auf gesetzlicher Grundlage hoheitlich vorgeschrieben werden. Die Zustimmung des Betriebsrates gemäß § 87 Abs.1 Nr.6 BetrVG ist nur innerhalb desjenigen Unternehmens erforderlich und möglich, dessen eigene Mitarbeiter einen entsprechenden biometrisch aufgeladenen Ausweis zur Verwendung im Rahmen von Überwachungsmaßnahmen im eigenen Unternehmen, nicht notwendig auf dem eigenen Betriebsgelände, aber im Rahmen der eigenen Unternehmensorganisation erhalten sollen.

Bei Mitarbeitern von Fremdfirmen, die ebenfalls in ein biometrisch aufgeladenes Ausweis- und Verifikationssystem eines Flughafenbetreibers einbezogen werden, bedarf es der Zustimmung des Betriebsrates des Flughafenbetreibers nicht; jedenfalls wäre dessen Betriebsrat insoweit nicht zuständig. Statt dessen obliegt es gemäß einem in diesen Tagen verkündeten Urteil des Bundesarbeitsgerichts (Urt.v.27.1.2004 – Az.: 1 AZR 7/03) in einem solchen Fall der Betriebsleitung des Zulieferers, mit der Geschäftsleitung des Betriebs, in den er seine Mitarbeiter zur Auftragsausführung schickt, Auftragsbedingungen auszuhandeln, die seinen eigenen innerbetrieblichen Vereinbarungen mit dem Betriebsrat seines Unternehmens in bezug auf die Anwendung technischer Kontrollsysteme generell und biometrischer Zutrittskontrollsysteme im besonderen entsprechen. Soweit solche Vereinbarungen mit dem Betriebsrat fehlen, sind sie zunächst auszuhandeln. Die Zustimmung des Betriebsrates muß zur Not mit den im BetrVG vorgesehenen Verfahren erstritten werden. Die Zustimmung ist nicht verzichtbar.

Über die im einzelnen noch nicht publizierten Urteilsgründe hat das BAG bisher u.a. verlauten lassen:

BAG-Urteil zur Mitbestimmung bei biometrischen Zutrittskontrollen im Kundenbetrieb

> *„Der Betriebsrat hat mitzubestimmen, wenn ein Arbeitgeber seine Arbeitnehmer anweist, sich in einem Kundenbetrieb der dort eingerichteten biometrischen Zugangskontrolle zu unterziehen. Die Anweisung betrifft das betriebliche Verhalten der entsandten Kundendienstmitarbeiter und ist daher nach § 87 Abs. 1 Nr. 1 BetrVG mitbestimmungspflichtig. Außerdem handelt es sich um die nach § 87 Abs.1 Nr. 6 BetrVG mitbestimmungspflichtige Anwendung einer technischen Überwachungseinrichtung.*
>
> *Dem Mitbestimmungsrecht des Betriebsrats steht nicht entgegen, daß das Zugangskontrollsystem im Kundenbetrieb eingerichtet ist. Zwar hat der Arbeitgeber auf die dortigen Verhältnisse keinen unmittelbaren Einfluß. Er gibt aber den entsandten Arbeitnehmern die mitbestimmungspflichtigen Anweisungen. Daher ist zwischen ihm und dem Betriebsrat zu vereinbaren, ob und in welcher Weise die Arbeitnehmer der Zugangskontrolle in einem fremden Betrieb unterworfen werden. Der Arbeitgeber muß bei der Vertragsgestaltung mit dem Kunden dafür sorgen, daß die mit dem Betriebsrat getroffenen Vereinbarungen umgesetzt werden. Individualrechtliche Rechtspositionen der betroffenen Arbeitnehmer bleiben hiervon unberührt.“*

Zustimmung des Betriebsrates unabdingbar

Damit ist den datenschutzrechtlich notwendigen Anforderungen Genüge getan, denn die Zustimmung des Betriebsrates gilt datenschutzrechtlich als Zustimmung auch mit Wirkung für und gegen jeden einzelnen Mitarbeiter, weil eine dahin gehende Betriebsvereinbarung, die überdies Bestandteil der Arbeitsverträge wird, als ausreichende Rechtsgrundlage gem. § 4 Abs.1 2.Alt. und § 4a BDSG gilt.

EU-Verordnung ändert Betriebsverfassungs-Recht nicht

Die Mitbestimmung des Betriebsrates insoweit könnte, wenn ein solcher besteht, vom Arbeitgeber auch nicht durch Klauseln im individuellen Arbeitsvertrag ersetzt oder unterlaufen werden, auch wenn der jeweilige Mitarbeiter aus ihnen genau erfährt, welche Kontrollen durchgeführt und welche Techniken angewendet werden (können) und er sich individuell ausdrücklich damit einverstanden erklärt, sich derartigen Prozeduren im eigenen wie ggf. auch im Kundenbetrieb zu unterziehen.

Auch der Umstand, daß die Zutrittskontrollen zu Sicherheitsbereichen auf Flughäfen durch die EU-Flughafensicherheitsverordnung hoheitlich vorgeschrieben sind, ändert nichts an der Notwendigkeit, daß auch beim Zulieferbetrieb dessen Betriebsrat zustimmen muß, bevor die Geschäftsleitung des Zulieferbetriebes ihre Mitarbeiter zur Erledigung eines hereingenommenen Auftrags in einen Sicherheitsbereich eines Flughafens schicken kann. Denn einerseits sind jedenfalls biometrische Zutrittskontrollen bisher

nicht in der EU-Verordnung vorgeschrieben, andererseits gibt es auch Einsatzfelder außerhalb von Sicherheitsbereichen eines Flughafens, für deren Zutritt technische Kontrollen nicht erforderlich sind, und zum dritten kann stets nur im Einzelfall geprüft werden, ob es zur Ausführung des hereingenommenen Auftrags wirklich unumgänglich notwendig ist, den Sicherheitsbereich eines Flughafens zu betreten und die Mitarbeiter den dafür notwendigen Zutrittskontrollen zu unterwerfen.

Notwendigkeit von Zutrittskontrollen bei Vertragsverhandlung klären

Soweit einzelne Mitarbeiter von Zulieferfirmen eines Flughafenbetreibers, die Firmen als solche oder deren Betriebsrat derlei nicht akzeptieren, der Flughafenbetreiber darauf aber nicht verzichten darf, müßten sich die Zulieferfirmen nach anderen Auftraggebern, der Flughafenbetreiber nach anderen Auftragnehmern umsehen. Für Flughafenbetreiber wie für alle anderen im nicht öffentlich zugänglichen Bereich eines Flughafens ansässigen Unternehmen dürfte es allerdings angeraten sein, bei Vertragsverhandlungen mit Zuliefer- und sonstigen Drittfirmen die Frage einer etwa notwendigen und noch einzuholenden Zustimmung des Betriebsrates der Drittfirma zum Gegenstand der Verhandlungen und gegebenenfalls auch einer ausdrücklichen Zusicherung der Drittfirma zu machen, um unliebsame Überraschungen zu vermeiden.

Detaillierte und präzise Regelungen treffen

Diese Verträge müssen im Hinblick auf Umfang der Erhebung und Nutzung der Daten sowie anzuwendende biometrische Verfahren ausdrückliche, klare und detaillierte Regelungen enthalten, die dann Gegenstand einer etwaigen Zustimmung des Betriebsrates des Zulieferbetriebes gegenüber dessen Unternehmensleitung sein können. Ob und wenn ja, welche biometrischen Daten im einzelnen durch wen erfaßt und wo, wie lange und durch wen verarbeitet und gespeichert werden dürfen, ist auch von Gegenstand und Dauer des Vertrages abhängig. Kurzfristige Lieferverträge oder langfristig angelegte Dienstleistungsverträge bedürfen dabei unterschiedlicher Behandlung. Im Zweifelsfall sind jeweils unterschiedliche organisatorische Abläufe in Erwägung zu ziehen, um eine langfristige Speicherung biometrischer Daten zu vermeiden.

Datenspeichersysteme besonders begründen

b. Besondere Begründung für Datenspeicherung außerhalb des Ausweises

Sowohl gegenüber den für die Aufsicht zuständigen Landesdatenschutzbeauftragten wie gegenüber dem Betriebsrat bei Verhandlungen über eine Betriebsvereinbarung zu begründen ist ferner die Notwendigkeit einer etwaigen Speicherung biometrischer Ausweisdaten in einer Referenzdatenbank eines Hintergrundsystems ebenso wie eine etwaige zentrale Datenspeicherung, jeweils unter Darstellung des dadurch erreichbaren Sicherheitsgewinns oder anderer legitimer, gegenüber den grundrechtlich geschützten Interessen des Betroffenen höherwertiger Belange.

Dies gilt schon bisher für jede zentrale Speicherung personenbezogener Daten. Demgegenüber ändert sich nichts dadurch, daß ein bisher schon

vorhandener bzw. vorgeschriebener maschinenlesbarer Lichtbildausweis, für dessen Daten eine (zentrale) Referenzdatenbank existiert, zusätzlich mit biometrischen Merkmalen aufgeladen wird. Ohne technische und datenschutzrechtliche Feinheiten zu bemühen, wird hier davon ausgegangen, daß es sich bei biometrischen stets um personenbezogene Daten handelt, die dem Datenschutzrecht unterliegen.

Erforderlichkeit zentraler Speicherung genau prüfen

Entsprechend den datenschutzrechtlichen Geboten der Erforderlichkeit und Datensparsamkeit muss stets im Einzelfall entschieden werden, ob die zentrale Speicherung von Daten, insbesondere biometrischen Daten, sowie die Erfassung und Speicherung von Bewegungsdaten zur Erreichung des verfolgten Zweckes wirklich nötig sind und einen entscheidenden Vorteil bringen gegenüber anderen, vorzugsweise dezentralen oder gänzlich andersartigen, auf organisatorischen Maßnahmen beruhenden Sicherheitslösungen. Wegen der mit der Zentralisierung der Datenspeicherung verbundenen höheren Eingriffsintensität in die grundrechtlich geschützte Freiheitssphäre des Bürgers ist die Frage, ob Daten zentral gespeichert werden oder nicht, stets auch eine Rechtsfrage, die einer Abwägung und Wertung divergierender Interessen auf der Grundrechtsebene bedarf. Bloße Zweckmäßigkeitserwägungen genügen zur Rechtfertigung einer zentralen Datenspeicherung daher nicht.

c. Speicherung biometrischer Daten für mehrere Verfahren auf einem Ausweis

Erforderlichkeit kumulativer Speicherung biometrischer Daten besonders begründen

Gleiches gilt für die kumulative Speicherung biometrischer Daten des Berechtigten für mehrere biometrische Verifikationsverfahren einerseits sowie die gleichzeitige und kumulative Nutzung mehrerer biometrischer Verifikationsverfahren für das Passieren einer bestimmten Kontrollstelle andererseits. Für Piloten kann die Ausgabe eines einzigen Ausweises mit allen Daten für die unterschiedlichen Verfahren statt mehrerer Ausweise, auf denen die biometrischen Daten nur für jeweils ein einziges Verfahren aufgebracht sind, zweckmäßig sein. Piloten müssen sich auf unterschiedlichen Flughäfen am ehesten verschiedenen biometrischen Verifikationsverfahren unterwerfen. Ganz anders beurteilt sich die Situation für den nur stationär auf einem einzigen Flughafen Beschäftigten.

Mehrere Ausweise für je ein Verfahren oder ein Ausweis für mehrere Verfahren?

Die Ausgabe mehrerer Ausweise mit unterschiedlichen biometrischen Daten statt der Ausgabe eines Ausweises, auf dem die Daten für alle Verfahren gleichzeitig gespeichert sind, muss weder einen Sicherheitsgewinn noch einen besseren Schutz personenbezogener Daten bringen, würde aber nicht verhindern, dass solche Daten überhaupt zunächst erfasst werden, damit sie der Arbeitgeber, also zum Beispiel die Fluggesellschaft, in einen Ausweis aufnehmen kann. Für Erfassung und Verarbeitung mehrerer biometrischer Daten für die kumulative Anwendung verschiedener Verfahren im Inland an demselben Platz durch denselben Betreiber gelten datenschutzrechtlich andere Maßstäbe, weil die reine Zweckmäßigkeit zur Legitimation kumulativer biometrischer

Datenerfassung und –verarbeitung nach gegenwärtiger Rechtslage nicht genügt.

Insofern muss entsprechend den datenschutzrechtlichen Geboten der Erforderlichkeit und Datensparsamkeit jeweils situationsangemessen beurteilt werden, welche Vorgehensweise rechtlich gesichert beschritten werden kann und soll.

2. Biometrische Merkmale im Flughafenausweis für Mitarbeiter

Vorgeschriebene Flughafenausweise auch mit biometrischen Daten ausstatten

Es wird vorgeschlagen, die nach der EU-Verordnung an Mitarbeiter der Flughafenbetreiber, der Fluggesellschaften, sonstiger im Flughafen ansässiger Unternehmen sowie die der Zuliefer- und sonstigen Drittfirmen und auch „Dauer-Besucher“ auszugebenden „Flughafenausweise“ künftig nicht nur, wie in der EU-Verordnung zwingend vorgeschrieben, mit Namen und Lichtbild des Inhabers sowie der Gültigkeitsdauer zu versehen, sondern darüber hinaus auch biometrische Daten des Berechtigten aufzunehmen.

DFK-Konzept: neutral gegenüber einzelnen biometrischen Verfahren

Es soll hier ausdrücklich offen bleiben, für welches Verfahren bzw. welche Art biometrischer Daten in den Ausweis aufgenommen werden sollen – auch, ob nur ein oder mehrere biometrische Merkmale genutzt werden. Die Entscheidung darüber wird im Einzelfall von der jeweils aktuell verfügbaren Technik, die sich im übrigen in rasanter Fortentwicklung befindet, abhängen, aber auch und vor allem den konkreten Einsatzszenarien. Unter abstrakten technischen Gesichtspunkten ist die Aufnahme mehrerer unterschiedlicher biometrischer Daten in einen Ausweis denkbar. Um diese generell oder in bestimmten Einzelfällen selektiv oder kumulativ einzusetzen, wird in einer dezidierten Einzelfallbetrachtung nicht zuletzt der rechtliche Rahmen jeweils genau auszuloten sein.

Mit der hier vorgelegten Darstellung der technischen Möglichkeiten ist keine Vorentscheidung für deren tatsächlichen Einsatz, ebenso wenig ein Präjudiz im Sinne einer generellen rechtlichen Zulässigkeit getroffen.

2.1 Ziel, Nutzen und Zwecksetzung

Ziel ist Verhinderung von Ausweismißbrauch

Ziel der Ergänzung der bisherigen Lichtbildausweise durch biometrische Daten ist die Verhinderung von Mißbrauch des Ausweises. Solcher Mißbrauch ist mit den bisherigen Ausweisen vielfältig möglich, da Sichtkontrollen durch das Sicherheitspersonal beim Passieren einer Kontrollstelle unter Vorlage eines Lichtbildausweises lediglich kursorisch erfolgen. Dies mag genügen, wenn bei geringer Frequenz über längere Zeit in der Regel dieselben Personen die Kontrollstellen passieren. Bisweilen ist die Feststellung, ob die Person, die einen Lichtbildausweis vorzeigt, identisch ist mit der Person, die auf dem Ausweis abgebildet ist, durch einen Menschen nur außerordentlich schwer zu treffen. Verifikationsmöglichkeiten durch das

Sicherheitspersonal stoßen hier wegen der beschränkten menschlichen Wiedererkennungsfähigkeit an Grenzen.

Effektive Verifikation durch manuelle Sichtkontrolle nicht möglich

Dies schränkt die Effektivität der Kontrollen an den Übergängen vom öffentlichen zum nichtöffentlichen bzw. Sicherheitsbereich eines Flughafens deutlich ein. Da die EU-Verordnung aber bei den Kontrollen an diesen Übergangsstellen – im Rahmen des wirtschaftlich Vernünftigen – höchstmögliche Wirksamkeit verlangt, bietet sich die Nutzung biometrischer Verifikationsverfahren an.

Es kann dabei im Rahmen dieser Ausarbeitung grundsätzlich offen bleiben, welches biometrische Verfahren, das nachfolgend in Teil D dargestellt ist, zur Verifikation Anwendung findet. Keinesfalls erscheint es notwendig, nur ein einziges oder ein allgemein im voraus generell bestimmtes Verfahren für alle Sicherheitskontrollen am Übergang zum nicht-öffentlichen Bereich anzuwenden oder aus der Vorgegebenheit des Lichtbildes im Ausweis eine Präferenz für das Verfahren biometrischer Gesichtserkennung abzuleiten. Vielmehr erlaubt die EU-Verordnung für einzelne Teile von Sicherheitsbereichen verschiedene, auch unterschiedlich intensive Sicherheitskontrollen.

Im Rahmen des Verhältnismäßigkeitsgrundsatzes, der sowohl das rechtliche wie das wirtschaftliche Denken prägt, liegt auf der Hand, daß hochwirksame Verfahren wie - möglicherweise - die kumulative Anwendung mehrerer biometrischer Verifikationsverfahren vorzugsweise für besonders sensible Teile des Sicherheitsbereiches eingesetzt werden, also zum Beispiel zentrale Einrichtungen der Sicherheits-, Informations- und Kommunikationstechnik. Zu diesen Bereichen müssen stets nur sehr wenige Mitarbeiter Zutritt haben, so daß sich einerseits der höhere technische Aufwand, andererseits der höhere Zeitbedarf für die Durchführung der Kontrolle rechtfertigt, ohne gleichzeitig die Arbeitsabläufe zu beeinträchtigen.

Ein biometrisches Merkmal meist ausreichend für effektive Verifikation

Andererseits wird für den Regelfall die Nutzung eines einzigen biometrischen Merkmals zusätzlich zu den bisher schon üblichen ausreichen, um das angestrebte, gegenüber dem bisherigen Zustand deutlich verbesserte Sicherheitsniveau mittels ausreichender Verifikation der Ausweisbenutzer zu erreichen. Insofern wird auch die Nutzung eines einzigen Merkmals schon aus praktischen, organisatorischen und finanziellen Gründen häufig ausreichen und insofern ein „effizienter Einsatz“ gegeben sein. Der „effiziente Einsatz“ von Sicherheitsausrüstungen ist im übrigen in der EU-Verordnung als „grundlegende Anforderung“ für die Auslegung von Flughäfen ausdrücklich erwähnt. „Übermäßiges“ und daher Ineffizientes ist auch EU-rechtlich ausdrücklich zu vermeiden.

Nutzbarkeit integrierter RFID-Chips technisch nicht einschränken

Wenn es an einem Flughafen für die dort in Sicherheitsbereichen tätigen Mitarbeiter in der Regel genügt, die Flughafenausweise nur mit einem biometrischen Merkmal aufzuladen, so folgt daraus nicht, daß der RFID-Chip technisch so gestaltet sein müßte, daß er nur dieses Merkmal verarbeiten können darf, für die Nutzung durch Aufladen weiterer biometrischer Merkmale für andere Verfahren also technisch gesperrt sein müßte. Gerade für

das fliegende Personal der Fluggesellschaften könnte die Situation eintreten, daß sie an verschiedenen Flughäfen mittels unterschiedlicher biometrischer Verfahren verifiziert werden, weil künftig die unterschiedlichen Flughäfen, zumal in unterschiedlichen Staaten nicht alle dasselbe biometrische Verfahren nutzen werden.

ICAO ohne Beschränkung auf ein bestimmtes biometrisches Verfahren

Anzustreben ist insoweit eine – auf ICAO-Basis – international für alle Flughafenbetreiber und Fluggesellschaften vereinheitlichte Praxis. Aber gerade in den dortigen Beratungen über entsprechende Richtlinien werden angesichts eines industriepolitisch bedingten Mangels entsprechender Einigungsmöglichkeiten für verschiedene biometrische Verfahren ausgerüstete Ausweise befürwortet, die mit allen biometrischen Daten seines berechtigten Inhabers aufgeladen werden (können), die für die in den verschiedenen Staaten vorgesehenen Verfahren nötig sind, auch wenn jeweils an einem Flughafen nur ein bestimmtes Verfahren und also ein kleiner Teil der geladenen Daten genutzt werden.

Flughafenbetreiber und Fluggesellschaften müssen aber noch weitere Aspekte beachten. Sie sind nämlich durch die EU-Verordnung gehalten, einerseits die Flughafenausweise an allen Kontrollpunkten zur Luftseite und zu Sicherheitsbereichen zu kontrollieren. Sie sind aber außerdem gehalten, den Zugang zur Luftseite und zu Sicherheitsbereichen, insbesondere über Räume von Pächtern auf dem Flughafen, Wartungshangars, Frachteinrichtungen und andere Service- und Betriebsgebäude „auf das unabdingbare Mindestmaß zu beschränken“.

Beschränkung der Zahl der Übergänge zur Luftseite bei Personenkontrollen

Daraus würde etwa für den praktischen Betrieb auf einem größeren Flughafen folgen, daß das Betriebspersonal den Wechsel von der Land- auf die Luftseite innerhalb des Flughafengebäudes nur noch an wenigen Punkten vornehmen können dürfte, weil die Zahl der Übergangsstellen radikal reduziert werden müßte. Eine Reduktion wäre für jeden Flughafenbetreiber aber auch aus wirtschaftlichen Gründen unvermeidbar, solange an jedem Übergang zum Sicherheitsbereich Personal zur Kontrolle eingesetzt werden muß. Kontrollpersonal ist teuer, auch deshalb, weil für einen reibungslosen ganzjährigen Betrieb rund um die Uhr je Position vier bis fünf Personen für notwendig sind und angestellt werden müßten, sollen gesetzlich vorgeschriebene Ruhezeiten, Urlaub, Wochenenden und Feiertage sowie durchschnittliche Krankheitszeiten berücksichtigt werden.

Reduktion der Übergangsstellen sprengt Arbeitszeitbudgets für Personal der Fluggesellschaften

Nach dem eindeutigen Wortlaut der EU-Verordnung muß auch das fliegende Personal (Crew) auf dem Weg von der Flugdatenausgabe („Briefing“) bis zum Flugzeug ebenfalls diese Sicherheitskontrollen passieren. Wenn diese Kontrollen nur an wenigen Punkten in weitem Abstand über das gesamte Flughafengelände verteilt sind, ergeben sich gegenüber dem jetzigen Zustand bei Umsetzung der EU-Verordnung für das fliegende Personal der Fluggesellschaften plötzlich enorm weite Wege und erheblicher Zeitverlust. Dieser ist deshalb für die Fluggesellschaften relevant, weil solche Wegzeiten jedenfalls nach deutschem Arbeits- und Luftfahrtrecht als Arbeitszeit der Piloten zu rechnen sind. Die Fluggesellschaften haben wie-

derholt die nachvollziehbare Befürchtung geäußert, daß sie mit den bisher für ihr fliegendes Personal vorgesehenen Zeitbudgets nicht mehr auskämen, wenn für dieses Personal nur noch an wenigen Stellen der Übertritt vom öffentlichen zum nicht-öffentlichen Bereich möglich wäre, statt wie bisher am jeweiligen Abflug- bzw. Ankunftsgate.

Lösungsvorschlag: dezentrale Verifikation anhand biometrischer Ausweisdaten

Es wird daher vorgeschlagen, das bisherige System der weiträumig dezentralen Übergänge vom öffentlichen zum Sicherheitsbereich, auch zur Luftseite beizubehalten und zur Aufrechterhaltung des von der EU-Verordnung vorgeschriebenen höheren Sicherheitsstandards die Personengruppen A) bis E) [vgl. Nr. 1.1.] mit Flughafenausweisen auszustatten, die zusätzlich zu den bisher üblichen Angaben (Lichtbild, Name, Unterschrift, Verfalldatum bzw. Gültigkeitsdauer und Berechtigungsmerkmalen) mit biometrischen Daten aufgeladen sind, um die jederzeitige sichere, aber vor allem automatische bzw. maschinelle Verifikation seines Benutzers gegenüber dem tatsächlich Berechtigten an möglichst vielen Kontrollstellen vornehmen zu können.

Zutrittsrechte präzise definierbar und programmierbar

Technisch denkbar erscheint auch, die mit biometrischen Daten des Berechtigten aufgeladenen Flughafenausweise, die dadurch jederzeit individualisiert sind, technisch so auszustatten, daß sie dem fliegenden Personal den Zutritt nur zu demjenigen Abfluggate gestatten, von dem sie abfliegen, so daß für das fliegende Personal die Wege von den Aufenthalts- und Briefingräumen im Abfertigungsgebäude bis zu „ihrem“ Flugzeug und zurück kurz bleiben.

EU-Verordnung: mehr Flexibilität bei den Kontrollen notwendig

Auch erscheint denkbar und angemessen, im Falle einer solchen sicheren Verifikation des Ausweisnutzers die sonst in der EU-Verordnung zwingend vorgeschriebenen Durchsuchungen der Person einschließlich der von ihr mitgeführten Gegenstände auf Stichprobendurchsuchungen zu beschränken. Eine solche Abweichung in besonderen Fällen gestattete die EU-Verordnung den Mitgliedstaaten ausdrücklich nur für die Übergangszeit bis zum 18.01.2004; die seinerzeit gültige Regelung sollte in ähnlicher Form wieder eingeführt werden. Eine Änderung des Anhangs der EU-Verordnung sollte den Regierungen der Mitgliedstaaten insoweit Flexibilität einräumen, die die gegenwärtige Verordnung nicht ermöglicht. Eine solche Änderung erscheint angesichts eines reellen Sicherheitsgewinns durch Aufbringung biometrischer Daten in die Flughafenausweise sowohl sicherheitstechnisch denkbar wie politisch vertretbar.

Zuverlässigkeitsprüfung sollte Vorrang haben, insbesondere für fliegendes Personal

Dies scheint zumindest für das fliegende Personal aus mehreren Gründen gerechtfertigt, weil gerade dieses als Inhaber von Flughafenausweisen mit Zutrittsberechtigung zu Sicherheitsbereichen und zur Luftseite zwingend einer regelmäßigen, in relativ kurzen Abständen zu wiederholenden Zuverlässigkeitsprüfung unterzogen werden muß, die von amtlichen Stellen auf gesetzlicher Grundlage durchgeführt wird. Derart als „zuverlässig“ eingestuftem Personal muß letztlich ebenso viel Vertrauen entgegengebracht werden, daß es die eingeräumten operativen Möglichkeiten nicht mißbraucht und die für die Berufsausübung mitgeführten Gegenstände

nicht zur Gefährdung der Luftfahrt einsetzt, wie beamtetem Personal staatlicher Sicherheitsbehörden. Das fliegende Personal hätte doch leicht die Möglichkeit, auf der Luftseite und im Flugzeug vorhandenes Material – speziell das ihnen anvertraute Fluggerät selbst durch Herbeiführen eines Absturzes – zu mißbrauchen, ohne irgendein Teil oder Gerät erst noch auf die Luftseite und in das Flugzeug schmuggeln zu müssen.

EU-Verordnung: mehrstufiges Kontrollsystem

Dem DFK ist bewußt, daß das im Anhang unter Ziffer 2. der EU-Verordnung vorgesehene System von Sicherheitsmaßnahmen mehrstufig in dem Sinne angelegt ist, daß die Flughafenmitarbeiter, insbesondere auch das fliegende Personal der Fluggesellschaften, zunächst anhand der mitgeführten Ausweise identifiziert bzw. verifiziert wird und schon durch diese Ausweiskontrolle alle nicht befugten Personen am Zutritt zum Sicherheitsbereich gehindert werden, so daß infolgedessen die als zweite Sicherheitsstufe angeordnete physische Durchsuchung des Personals einschließlich aller von ihm mitgeführten Gegenstände nur an den Berechtigten, die zuvor die Ausweiskontrolle passiert haben, vorgenommen wird.

EU-Verordnung: Unausgewogenheit zwischen Verifikation und Durchsuchung

Eine gewisse Unausgewogenheit im Hinblick auf das damit zu erreichende Sicherheitsniveau ist aber zwischen beiden Prüfstufen kaum zu übersehen, legt man bisherige Verfahren zugrunde. Nach dem bisherigen Standard, den die EU-Verordnung auch nur vorsieht, findet die Identitäts- bzw. Verifikationskontrolle anhand von Lichtbildausweisen mittels menschlicher, also manueller Kontrolle statt. Menschen nehmen den notwendigen Bildvergleich (Gesicht des Benutzers gegen Abbild im Ausweis) vor. Ein solcher Vergleich „Gesicht zu Bild“ ist auch für geübte Personen außerordentlich schwierig. Das sichere Erkennen von Identität und Differenzen in Relation zu einem Ausweislichtbild ist für einen Menschen häufig nicht möglich. Die Gründe liegen teils beim Kontrolleur, teils beim Kontrollierten und wirken häufig kumulativ. Die Erkennungsraten bei Ausweismißbrauch und ähnlichen Delikten werden von einigen Kritikern auf Null geschätzt; auch Wohlmeinende kommen über wenige Prozentpunkte kaum hinaus.

Dies bedeutet für das in der EU-Verordnung vorgesehene Konzept zur Erhöhung der Flughafensicherheit durch konsequente Kontrolle der Mitarbeiter des Flughafenbetreibers, der Fluggesellschaften und sonstiger auf dem Gelände ansässiger Unternehmen, daß eine lückenlose physische Kontrolle der Personen und der von ihnen mitgeführten Gegenstände beim Passieren der Land-/Luft-Grenze zwar ein hohes Maß an Sicherheit bewirken kann, so daß keine verbotenen Gegenstände mitgeführt werden. Doch ob die Person, die kontrolliert wird, mit dem Berechtigten identisch ist, für den nach vorheriger amtlicher Zuverlässigkeitskontrolle ein Berechtigungsausweis ausgestellt wurde, kann mit der bisher vorgesehenen Ausgabe bloßer Lichtbildausweise und deren Kontrolle nicht in gleichem Maße gewährleistet werden.

In der Konsequenz bedeutet dies, daß leichter ein Unbefugter mit nicht verbotenen Gegenständen in den Sicherheitsbereich gelangen kann als ein

Berechtigter mit verbotenen Gegenständen. Im Ergebnis bleibt eine erhebliche Unsicherheit trotz umfangreicher Maßnahmen bestehen.

DFK-Konzept zielt auf Beseitigung bestehender Sicherheitslücken bei der Ausweiskontrolle

Der hier unterbreitete Vorschlag zielt darauf ab, diese Unsicherheiten bei der Verifikation der Personen, die Zutritt zum Sicherheitsbereich unter Vorlage eines Ausweises begehren, zu beseitigen. Dies entspricht der Überzeugung, daß ein höheres Sicherheitsniveau zuerst dadurch erreicht werden kann, daß nur auf Zuverlässigkeit amtlich überprüfte Personen tatsächlich auch Zutritt zum Sicherheitsbereich erhalten. Kann dies durch geeignete technische und organisatorische Maßnahmen gewährleistet werden, kann im Gegenzug eine gewisse Beschränkung bei der physischen Kontrolle dieser Personen und der von ihnen mitgeführten Gegenstände beim Zutritt zum Sicherheitsbereich hingenommen werden, ohne daß eine nennenswerte Verringerung des Sicherheitsniveaus im Ergebnis zu verzeichnen wäre. Denn zahlreiche, objektiv zu Sabotageakten des Flugbetriebs geeignete Materialien sind stets auch auf der Luftseite bzw. in der Sicherheitszone eines Flughafens verfügbar.

Amtliche Zuverlässigkeitskontrolle nicht entwerten

Soll die amtliche Zuverlässigkeitskontrolle der diesem Begriff innewohnenden und der mit der Maßnahme nach der EU-Verordnung und dem (geplanten) LuftSiGE verfolgten Zielsetzung gerecht werden, muß das Ergebnis ein Grundvertrauen in die derart geprüften und mit Zutrittsberechtigung ausgestatteten Personen sein, daß sie die ihnen sich objektiv bietenden Möglichkeiten nicht mißbrauchen. Ließe sich ein solches Ergebnis nicht vertreten, geriete auch die Überprüfung als solche unter Legitimationszweifel und wäre verfassungsrechtlich angreifbar, denn nach ständiger Rechtsprechung des Bundesverfassungsgerichts ist der Gesetzgeber generell, nicht nur bei freiheitseinschränkenden Maßnahmen verpflichtet, nur objektiv zur Erreichung des Gesetzgebungsziels geeignete Maßnahmen vorzuschreiben bzw. zu ergreifen. Insofern steht dem Gesetzgeber nicht jede Maßnahme zu wählen frei, auch wenn das Gesetzgebungsziel als solches jeweils verfassungsrechtlich legitim ist.

Vertrauen in überprüfte Personen sollte Vorrang haben

Dieses notwendige Grundvertrauen in die geprüften Personen, die bekannt sind und nach ihrer Überprüfung unter Vertrag genommen wurden, sollte angesichts des Umstandes, daß eine unüberschaubare Vielzahl von potentiell zu gefährlichen Eingriffen in den Luftverkehr geeigneten Gegenständen auf der Luftseite, ja sogar in jedem Flugzeug stets vorhanden sind und sein müssen, ein deutlich höheres Gewicht bei der künftigen Sicherheitsstruktur erhalten als die physische Kontrolle solcher Personen. Sie kann sich auf Stichproben mittels mobiler Kontrolleinheiten beschränken, wenn eben durch geeignete technische Maßnahmen sichergestellt wird, daß tatsächlich nur überprüfte und als zuverlässig eingestufte, deshalb mit einer Zutrittsberechtigung ausgestattete Personen auch im Einzelfall Zutritt erhalten.

Der Erpressung berechtigter mittels Technik vorbeugen

Dagegen kann auch letztlich nicht mit Erfolg die Notwendigkeit physischer Kontrollen der Mitarbeiter einschließlich der des fliegenden Personals damit begründet werden, daß nur auf diese Weise verhindert werden könne, daß

Mitarbeiter erpreßt oder sonst dazu mißbraucht würden, nach dem Anhang der EU-Verordnung bzw. § 11 LuftSiGE verbotene Gegenstände in den Sicherheitsbereich einzuschleusen. Denn solche Bedenken könnte mindestens ebenso gegen das seitens des Flughafenbetreibers und der Behörden eingesetzte Sicherheitspersonal vorgebracht werden. Weshalb also sollte zwischen gleichermaßen sicherheitsüberprüftem Personal nur aufgrund ihrer unterschiedlichen Einsatzbereiche ein Unterschied gemacht werden, weil die einen zur Überprüfung der anderen eingesetzt werden?

Automatische, maschinelle Verifikationsprüfungen anhand biometrisch aufgeladener Ausweise und darauf basierende, rein technische Zutrittsschleusen stellen kein höheres Sicherheitsrisiko gegenüber der Zutrittskontrolle mittels Sicherheitspersonal dar, weil etwa ein Berechtigter von einem Unberechtigten mittels vorgehaltener Waffe oder durch Erpressung dazu gezwungen werden könnte, ihn gleichzeitig mit seinem eigenen Sicherheits-Check durch die automatische, maschinelle Kontrolle zu schleusen. Ein solches Szenario könnte durch Vereinzelungsschleusen, die zusätzlich mit Alarm- und Überfallmeldern sowie Videoüberwachungseinrichtungen ausgestattet sind, verhindert werden, ohne daß es zusätzlichen Kontrollpersonals an jedem Übergangspunkt bedürfte. Schließlich dürfen ohnehin nur solche biometrischen Systeme eingesetzt werden, die nach anerkannten Maßstäben hinreichend sicher sind.

Risiko verlagert sich

Allerdings muß deutlich im Bewußtsein bleiben, daß bei dieser Verschiebung der Gewichtung der beiden Kontrollstufen (Ausweiskontrolle zum einen, physische Kontrolle auf Mitführen verbotener Gegenstände zum anderen) die Einhaltung der Sicherheitskette bei Erstellung und Ausgabe der Mitarbeiterausweise von entscheidender Bedeutung ist und dabei wiederum die Verläßlichkeit der amtlichen Zuverlässigkeitskontrolle. Dessen genaue Ausgestaltung in § 7 LuftSiGE ist gegenwärtig noch in der politischen Diskussion.

2.2 Technische Ausgestaltung und Verfahren

Flughafenausweis für Mitarbeiter als persönliche Datenbank

Für die Personengruppen A bis E [vgl. oben Nr. 1.1] – ggf. unter Ausschluß der staatlichen Sicherheitskräfte –, die dafür ihre Dienstausweise benutzen, wird ein multifunktionaler Mitarbeiterausweis eingesetzt. Dieser ist öffentlich zu tragen und kann schon durch äußerliche Merkmale die Sicherheitsstufe des Inhabers anzeigen.

Der neue **„Flughafenausweis“** enthält die personenbezogenen einschließlich der biometrischen Daten des Beschäftigen. Er stellt also die persönliche „Datenbank“ der berechtigten Person für Gültigkeitsbereich und -dauer des Ausweises dar.

Der **Flughafenausweis der Mitarbeiter** entspricht einer genormten Ausweiskarte und ist eine berührungslos arbeitende passive Karte (RFID-SmartCard ohne Batterie) mit kontaktlosem und, falls für Zusatzanwendun-

gen nötig, mit zusätzlichem kontaktbehaftetem Chip. Die Karte verfügt über einen großen Datenspeicher.

Abb. 1: Beispiel Flughafenausweis für Mitarbeiter

Die Vorderseite enthält:

- Lichtbild des Ausweisinhabers
- Personaldaten wie z.B. Name
- Ausweiskennung
- Logo / Name des Aus- bzw. Arbeitgebers

Die Rückseite enthält:

- rechtliche Vertragssituation
- Magnetstreifen, frei ggf. für ausgeber-/arbeitgeberspezifische Informationen

Die Speicher enthalten:

- Personendaten
- Biometriedaten
- Ausweiskennung
- Administrationsdaten
- Gültigkeitsdauer

Der Ausweis wird an speziellen Ausgabeschaltern am Flughafen – idR vom Flughafenbetreiber selbst bzw. in seiner unmittelbaren Verantwortung - ausgestellt.

Ausrüstung der Ausgabestellen für die biometrischen Flughafenausweise

Als Ausrüstung ist erforderlich:

- PC mit passender Ausweiserstellungs-Software
- Erfassungseinheit für biometrische Daten
- Lichtbildkamera
- Kartendrucker
- Validierungsleser zum Gültigmachen der Karte
- Biometrisches Erkennungsgerät

Ausweisdatenerfassung zentral; Verarbeitung zentral oder lokal

Die Daten der Beschäftigten eines Unternehmens werden nach den Richtlinien des Flughafenbetreibers unter Berücksichtigung eigener Vorgaben oder aufgrund der EU-Flugsicherheitsverordnung vom Flughafenbetreiber zentral bearbeitet und zum Zweck der beschriebenen Prüfung der Berechtigung vom Zutrittskontrollsystem (ZKS) übernommen, je nach gewählter technischer Variante durch Rückfrage des Zutrittkontrollgeräts am Übergangspunkt beim Zentralspeicher oder durch rein lokale Verifikation. Beide Möglichkeiten werden hier bewußt offen gehalten, auch wenn aus datenschutzrechtlicher Sicht eine dezentrale Verifikationsprüfung am jeweiligen Übergangspunkt bevorzugt wird.

Mehrere biometrische Verfahren vorsehen

Für höchste Sicherheitsansprüche, zum Beispiel die Zutrittsgewährung zu Rechenzentren und Server- oder Sicherheitszentralen oder ähnlich „sensiblen Teilen der sicherheitsempfindlichen Bereiche“ (vgl. § 8 Abs.1 Nr.5 LuftSiGE), können beim Beschäftigtenausweis zusätzliche Informationen wie gestaffelte Berechtigungen und auch Daten für mehrere biometrische Verfahren eingesetzt werden, die parallel bzw. kumulativ angewendet werden.

Bewegungsdaten erfaßbar

Bewegungsdaten von Erkennungs- und Zutrittsvorgängen werden, soweit unabweisbar erforderlich, nur gemäß der getroffenen Betriebsvereinbarung oder gar nicht erfaßt. Sofern sie befugt erfaßt werden, können sie später in dem nach Gesetz und Vertrag erlaubten Umfang ausgewertet werden.

Für die Personengruppen A) bis E) [vgl. oben Nr. 1.1] können, wenn nötig jeweils differenziert, Übergänge mit automatischer Zutrittskontrollprüfung mittels des biometrisch aufgeladenen „Flughafenausweises“ an beliebigen Türen, Schleusen, Toren und Schranken erfolgen. Zusätzlich kann der biometrisch aufgeladene Flughafenausweis zur Verifikation des fliegenden Personals beim Briefing vor dem Abflug genutzt werden.

Unterschiedliche technische Verfahren bei Ausweisprüfung

Mit einem Zutrittskontrollsystem (ZKS) werden an diesen Punkten die einer Person zugewiesenen Zutrittsberechtigungen geprüft. Dazu können unterschiedliche Ausweis- und Ausweislesetechniken in Verbindung mit biometrischen Funktionen – für Fall-back-Zwecke, wenn das Biometrie-System am Checkpoint versagt, ggf. zusätzlicher PIN-Code – und weitere Sicherheitsmodule eingesetzt werden. Bei Übereinstimmung der gemessenen Parameter mit den gespeicherten Werten und der Zutrittsberechtigung der

Person nach Ort und Zeit gibt das Zutrittskontrollsystem (ZKS) den Zutritt frei.

ITK-Infrastruktur besonders schützenswert

Sicherheitstechnisch kommt den Einrichtungen der Informations- und Kommunikationstechnik aufgrund der vollständigen IT- und TK-Durchdringung und Vernetzung des Flughafenbetriebes und des Luftverkehrs insgesamt eine sehr große Bedeutung zu. Mißbrauch dieser Systeme kann für die gesamte Luftsicherheit nicht nur des einen Flughafens, sondern weit darüber hinaus beträchtliche negative Konsequenzen haben. Die Besonderheit dieser Einrichtungen besteht darin, daß sie zugleich in öffentlich und nicht öffentlich zugänglichen Bereichen der Flughäfen angesiedelt sind, weil etwa an jedem Abfertigungsschalter in den öffentlich zugänglichen Bereichen der Abflughallen eine Vielzahl von PC, Telefonen und ähnlichen Einrichtungen für jeden, der sich dort aufhält, de facto physisch zugänglich ist.

ITK-Schutz durch Authentifizierung der Nutzer

Ein wirksamer Schutz dieser technischen Infrastrukturen muß daher über wirksame Maßnahmen zur Authentifizierung der berechtigten Benutzer der Einrichtungen, insbesondere der PCs gewährleistet werden. Dabei muß auch berücksichtigt werden, daß nicht nur fest angestellte Mitarbeiter des Flughafenbetreibers, der Fluggesellschaften sowie auf dem Flughafengelände angesiedelter Unternehmen mit Aufgaben betraut sind, die die Benutzung dieser Geräte erforderlich machen. Vielmehr werden, etwa für die Abfertigung von Passagieren auch Aushilfskräfte sowie Mitarbeiter von Zeitarbeitsunternehmen und sonstige Kräfte eingesetzt. Es besteht also eine hohe Mitarbeiterfluktuation. Dadurch darf aber weder das Sicherheitsniveau gesenkt werden noch dürfen – bei Einhaltung des Sicherheitsniveaus – Blockaden oder Schwächen der einzuführenden Sicherheitsmaßnahmen auftreten.

Insofern ist in Betracht zu ziehen, ob für die Bediener solcher technischen Einrichtungen, insbesondere der PCs anstelle der oder zusätzlich zu den im Abschnitt E näher beschriebenen biometrischen Erkennungsverfahren, ein anderes, dort nicht beschriebenes System eingesetzt werden soll oder muß. Ein solches System könnte z.B. die Sprechererkennung sein.

Zur Technik der RFID-Speicherchips

Technische Unterschiede bei RFID-Chips

Die hier zur Verwendung vorgeschlagenen RFID-Speicherchips unterscheiden sich von denjenigen, die unter gleichem Namen als Ersatz für die sog. Strich- oder Bar-Codes in Warenetiketten propagiert, produziert und auch teilweise bereits eingesetzt werden. Bei RFID-Chips in Warenetiketten handelt es sich um relativ einfache Chips ohne Betriebssystem, die von beliebigen Lesestationen jederzeit ausgelesen werden können. Gleichzeitig kann in solchen Fällen bei diesen Waren-Etiketten aus technischen Gründen stets nur der gesamte gespeicherte Datensatz ausgelesen werden. Neben solchen einfachen Chips sind, ebenfalls für die Warendistribution,

RFID-Chips am Markt erhältlich, die bereits wesentlich mehr als lediglich einen Strich-Code-Ersatz bieten; sie verfügen z.T. bereits über ein rudimentäres Betriebssystem, das die Strukturierung des gespeicherten Datensatzes in mehrere, getrennt nutzbare Teil-Datensätze erlaubt. Die Speicherkapazität solcher heute bereits weit verbreiteten RFID-Chips beginnt bei 128 Bits; Chips mit 1,2kB, 2,4kB und 3,6kB Speichervolumen sind ebenfalls erhältlich.

Neuartige RFID-Chips mit Sicherheitsstruktur und Betriebssystem

Über diese RFID-Technik gehen die hier zur technischen Grundlage der Vorschläge ausgesuchten RFID-Chips wesentlich hinaus. Um etwa die für ein Gesichtserkennungsverfahren notwendigen Daten speichern zu können, sind mindestens 8kB Speicherplatz erforderlich, für die für andere biometrische Erkennungsverfahren benötigten Daten jeweils mindestens weitere 6-8kB. Insofern werden für die reinen Biometriedaten für angenommene 3 biometrische Verfahren mindestens 24kB benötigt. Hinzu kommen die notwendigen Speicherkapazitäten für ein Betriebssystem zur differenzierten Nutzung, für Zugriffssicherungen usw., ferner für sonstige Betriebsdaten des Arbeitgebers, Zutrittsberechtigungen (örtliche und zeitliche Freigaben bzw. Sperren) etc. Insofern werden für die hier besprochenen RFID-Anwendungen Chips mit einer Speicherkapazität von mindestens 32kB vorausgesetzt.

Minimum 32kB, besser 64kB

Solche 32kB-RFID-Chips werden derzeit bereits vereinzelt am Markt angeboten und werden sowohl von den US-Behörden als auch von ICAO für den Einsatz in amtlichen Dokumenten bereits gefordert. Bis zum Jahresende 2004 haben einige Hersteller die Großserienreife solcher 32kB-RFID-Chips zugesagt. Die Entwicklungslabors haben auch bereits 64kB und 72kB-RFID-Chips vorgestellt, bisher jedoch nur als Labor-Modelle.

Speichergrößen von mindestens 32kB sind erforderlich, wenn man nicht die biometrischen Templates, sondern komprimierte Abbilder der biologischen Eigenschaften abspeichern will. Bei örtlich begrenztem Einsatz und der Verwendung festgelegter Algorithmen für die biometrische Erkennung wird das Template selbst gespeichert, das in der Regel viel weniger Speicherplatz benötigt.

Unbefugtes Auslesen der Daten muß verhindert werden

Das unbefugte Auslesen der auf solchen Chips gespeicherten Daten kann und muß durch geeignete Sicherheitsmaßnahmen auf dem Chip einerseits und am Lesegerät andererseits verhindert werden. Zwar würde ein unbefugtes Auslesen und Speichern der biometrischen Daten des Ausweisinhabers dem Täter noch nicht weiterhelfen, weil seine eigenen biometrischen Daten, nicht mit den entwendeten Daten übereinstimmen. Er könnte solche Daten mithin nicht in gleicher Weise unmittelbar zu betrügerischen Zwecken bzw. zum Erschleichen eines Zutritts nutzen, wie das mit einem herkömmlichen Ausweis an einer normalen, ausweisgestützten manuellen Zugangskontrolle häufig möglich ist.

Gleichwohl muß dem – unbemerkten – Zugriff Unbefugter auf biometrische Daten anderer Personen frühzeitig und systematisch begegnet werden, nicht zuletzt aus datenschutzrechtlichen Gründen. Dazu bietet sich zunächst an, im Betriebssystem des RFID-Chips unterschiedliche Zugriffsrechte auf die jeweiligen biometrischen Datensätze, die für verschiedene Verfahren gegebenenfalls gespeichert sind, vorzusehen. Darüber hinaus muß eine mit der jeweils eingesetzten Lesesystemtechnik abgestimmte Authentifizierungsroutine vorgesehen sein, mit deren Hilfe der Chip zweifelsfrei erkennen kann, ob sich eine berechtigte Lesestation bei ihm meldet und welche Daten sie auslesen darf.

Sicherheitsroutinen in die Lesestationen einbauen

Weil der RFID-Chip definitionsgemäß keine immanent eigene Energie besitzt, muß ihm jede für ein Auslesen notwendige Energie von außen über das vom Lesegerät aufgebaute elektromagnetische Feld zugeführt werden. Aus dieser technischen Rahmenbedingung ergibt sich zugleich, daß die wesentlichen Sicherheitsroutinen an den Lesestationen ansetzen müssen. Sie müssen softwaretechnisch in Bezug auf Authentifizierung und Sicherheitskontrollen ausgerüstet sein. Sie müssen gleichzeitig gegen unbefugte Entwendung besonders gesichert sein, etwa durch eine Alarmgebung an die Sicherheitszentrale, wenn sie außer Betrieb gesetzt oder gar unbefugt abmontiert werden. Für einen solchen Fall wird z.B. eine Selbstzerstörungsroutine vorgesehen sein müssen, die automatisch alle gespeicherten Abfrage-/Leseprogramme sowie sonstige Datensätze löscht oder auf andere Weise das Gerät betriebsunfähig, jedenfalls für Unbefugte unbrauchbar macht.

2.3 Vorteile des Flughafenausweises mit biometrischen Daten

Folgende erkennbaren Vorteile des Einsatzes eines Flughafenausweises mit biometrischen für auf dem Flughafen in Sicherheitsbereichen bzw. nicht öffentlich zugänglichen Bereichen tätige Beschäftigte des Flughafenbetreibers selbst, der Fluggesellschaften wie auch aller sonstigen Unternehmen sollen hier noch einmal ohne Anspruch auf Vollständigkeit zusammengefaßt dargestellt werden.

Hauptvorteil: wirksame Verifikation

Zunächst liegt der Hauptvorteil darin, daß mit Hilfe der biometrischen Daten eine zuverlässigere Verifikation der Ausweisbenutzer im Verhältnis zu den tatsächlich ausgegebenen Berechtigungen erreicht werden kann und gleichzeitig eine höhere Effizienz der Kontrollen. Das gelingt dadurch, daß sie einerseits eine Reduzierung des Personals bei der Ausweiskontrolle erlauben, vor allem aber eine dezentrale Kontrolle und dadurch die bisher üblichen Abläufe vor allem beim Personaleinsatz der Fluggesellschaften eingehalten werden können. Gerade für das fliegende Personal werden arbeitszeitverschlingende Umwege zum eigentlichen Arbeitsplatz im Flugzeug vermieden. Dadurch wird bei den Fluggesellschaften eine sonst womöglich notwendige deutliche Aufstockung des Personals einschließlich

der damit verbundenen Kostenbelastung vermieden, die als solche im Sinne der Zielsetzung der EU-Flugsicherheitsverordnung keinen Sicherheitsgewinn brächte.

Verzicht auf physische Kontrollen bei biometrischer Verifikation

Zudem könnte auf physische Kontrollen von Personen, die mit derartigen Flughafenausweisen mit biometrischen Daten der Berechtigten ausgestattet sind, verzichtet werden. Auch von ihnen mitgeführtes Gepäck und sonstiges Material müßte an den Übergangsstellen zum Sicherheitsbereich nicht mehr kontrolliert werden, weil die Inhaber eines solchen Ausweises zusätzlich generell einer amtlichen Zuverlässigkeitskontrolle, die regelmäßig wiederholt wird, unterzogen würden. Auch dadurch können wiederum Zeitverzögerungen für das zu kontrollierende Personal, etwa der Fluggesellschaften, aber auch der Personaleinsatz zur physischen Kontrolle von Personen und mitgeführten Gegenständen an den Übergangspunkten reduziert werden. Dadurch kann die zusätzliche Personalkostenbelastung für den Flughafenbetreiber, der diese Kontrollen nach der Verordnung vorsehen muß, in Grenzen gehalten werden.

Insgesamt wird gerade im eigentlichen Flugbetrieb die Sicherheit dadurch erhöht, daß die Crew-Mitglieder im Flughafen, am Gate, am Flugzeugeingang, an der Cockpittür - und womöglich später auch noch im Cockpit, obwohl dies von der EU-Verordnung nicht berührt wird – ebenso wie das Bodenpersonal sicher verifiziert werden können.

Höhere Sicherheit durch zuverlässige Verifikation

Darüber hinaus kann ein solcher Flughafenausweis mit biometrischen Daten der Mitarbeiter, weitgehende Reibungslosigkeit der technischen Einsatzfähigkeit der biometrischen Systeme vorausgesetzt, im täglichen Betrieb schon allein deshalb eine wesentlich höhere Sicherheit gegenüber dem jetzigen System der manuellen Sichtprüfung reiner Lichtbildausweise erreichen, weil ein solches technisches System einerseits nicht unter Ermüdungserscheinungen leidet, andererseits auch andere, physiologisch bedingte Erkennungsschwierigkeiten des Menschen vermeidet. Es wäre eine lückenlose Verifikation aller Personen rund um die Uhr möglich, die den Sicherheitsbereich eines Flughafens betreten (wollen).

Dezentrales Übergangssystem zu Sicherheitsbereichen

Ferner läßt sich – wie schon erwähnt – mit Hilfe eines solchen Ausweissystems ein dezentralisierter Übertritt vom öffentlichen zum nicht öffentlichen Bereich wesentlich leichter organisieren, so daß nicht sämtliche bisher üblichen Abläufe am Flughafen völlig verändert werden müßten. Für den Flughafenbetreiber bedeutet dies eine erhebliche Ersparnis an Personalkosten für Kontrollpersonal, für die Fluggesellschaften – allein wegen des Zeitverlustes am Boden – die Vermeidung von Neueinstellungen.

Derzeit noch kein „matchig-on-card“

Die unterschiedlichen Möglichkeiten, 32kB-RFID-Chips einzusetzen, bringen jeweils Vor- und Nachteile. Das von Datenschützern bevorzugte „matching-on-card“, bei dem die biometrischen Daten ausschließlich auf der Karte abgelegt sind und auch der biometrische Abgleich dort stattfindet, läßt sich nach dem gegenwärtigen Stand der Technik noch nicht praktikabel bewerkstelligen, weil diese Karten keine eigene Energie verwenden,

sondern auf die Energiezufuhr im Rahmen ihrer Kommunikation mit einem Lesegerät für die Herstellung ihrer Funktionsfähigkeit angewiesen sind.

Vorteil: RFID-Technik wird international eingesetzt

Der Vorteil der RFID-Chips liegt darin, daß solche für die biometrischen Sicherheitsanwendungen in amtlichen Ausweisen und Reisedokumenten als Standard künftig international verlangt und auch von der Bundesregierung eingesetzt werden. Der Einsatz einer einheitlichen Ausweistechnik für Reisedokumente einerseits, Flugpässe und Mitarbeiterausweise andererseits, ermöglicht die Installation einheitlicher Prüftechnik-Hardware, die für unterschiedliche Prüf- und Einsatzzwecke lediglich unterschiedlich programmiert wird, wobei die Programmierung wiederum zentral erfolgen kann. Für den Flughafenbetreiber ist die RFID-Technik daher kostengünstig und rationell.

Probleme beim „matching-on-card“ und die Folgen

Im Hinblick auf die Speicherung und Abfrage biometrischer Daten gibt es zumindest in Bezug auf Mitarbeiter – und Dauerbesucher – zwei unterschiedliche Ansätze. Seitens der Datenschützer wird bisher ein Speichern der Daten allein auf der Karte bevorzugt. Eine solche Vorgehensweise bedingt, weil gleichzeitig ein matching-on-card auf der Karte – wie dargestellt – jedenfalls nach derzeitigem Stand der Technik nicht möglich ist, daß bei der Kontrolle die biometrischen Daten zumindest vorübergehend in das Lesegerät übertragen und dort zwischengespeichert werden, solange die Verifikation andauert. Die biometrischen Daten sind also zum einen dauerhaft dezentral vorhanden. Zum anderen werden sie, wenn auch nur kurzzeitig, in diversen Lesestationen verwendet. Insoweit erhöht sich, trotz aller denkbaren und notwendigen Sicherungsmaßnahmen, das Risiko unbefugter Nutzung der Daten. Dies kann, auch wenn die Mißbrauchsmöglichkeiten zunächst nicht auf der Hand liegen, gleichwohl einen Sicherheitsnachteil darstellen.

Alternativen zur Speicherung biometrischer Daten „on chip“

Dieser ließe sich vermeiden, wenn die biometrischen Daten überhaupt nicht mehr direkt als Klardaten auf der Karte gespeichert würden, sondern auf der Karte selbst nur eine (verschlüsselte) eineindeutige Zertifikats-ID vorhanden wäre, die an berechtigten Stationen ausgelesen würde und die, in Verbindung mit den biometrischen Daten, die am Kontrollpunkt vom Nutzer unmittelbar überprüft werden, von der Prüfstation gegen die in einer Referenzdatenbank in einem Hintergrundsystem abgeglichen würden.

Leichtere Ersatzbeschaffung eines verlorenen Ausweises bei Datenhinterlegung

Eine solche Vorgehensweise würde im Übrigen nicht nur die Sicherheit erhöhen, sondern ebenso den Aufwand bei einer Wiederbeschaffung des Ausweises im Verlustfall deutlich mindern. Eine strikt dezentrale Vorgehensweise ohne Hinterlegung der biometrischen Daten in einem Referenzsystem würde zwangsläufig zur Folge haben, daß ein Flughafenmitarbeiter das gesamte Prozedere der Ausweisausstellung wie bei der Erstausstellung erneut durchlaufen müßte, einschließlich der Einholung eines amtlichen Zuverlässigkeitszeugnisses. Denn derjenige, der in Verbindung mit einer Verlustanzeige die Neuausstellung eines Flughafenausweises begehrt, müßte erst auf seine Berechtigung, überhaupt einen Ausweis beantragen zu dürfen, verifiziert werden. Bei Hinterlegung biometrischer Erken-

nungsmerkmale in einem Referenzsystem könnte die Übereinstimmung des Antragstellers mit dem Berechtigten leicht, zeitsparend und kostengünstig verifiziert werden.

Geringeres Diebstahlrisiko bei Verwendung einer Karten-ID

Würde lediglich die oben vorgeschlagene ID auf der Karte gespeichert, wäre es völlig sinnlos, sich die Mühe zu machen, solche Zahlenfolgen – mögen sie ihrerseits verschlüsselt sein oder nicht – unbefugt auszulesen. Sie besitzen für sich allein keinerlei Aussagekraft noch irgendeinen Wert. Insbesondere stellen solche Zertifikatsdaten keinerlei personenbezogenes Datum im Sinne des Datenschutzes dar. Auch die Gefahr, daß Lesestationen illegal abmontiert und mißbraucht werden, sinkt deutlich, was wiederum den Vorbeugungsaufwand gegen solchen Mißbrauch der Lesestationen stark verringern helfen würde.

Insgesamt kann mit Hilfe eines solchen Flughafenausweises, der mit biometrischen Daten des jeweiligen berechtigten Ausweisinhabers aufgeladen und automatisch verarbeitbar ist, dem Anliegen der Regierungen, insbesondere auch den Vorgaben der EU-Luftsicherheitsverordnung wesentlich leichter und umfassender Rechnung getragen werden als mit bisher üblichen Sicherheitssystemen und der lediglich manuellen Sichtprüfung reiner Lichtbildausweise.

Weiterer technischer Anwendungsnutzen inner- und außerhalb des Flughafens denkbar

Unter rein technischen Gesichtspunkten sind weitere Vorteile eines solchen biometrisch aufgeladenen Flughafenausweises denkbar, die hier nicht näher untersucht, sondern nur erwähnt werden sollen. Insoweit unterbleibt daher auch eine ausführliche Darstellung der rechtlichen, namentlich datenschutzrechtlichen Rahmenbedingungen.

Als solche weiteren Funktionen bzw. Applikationen könnten auf einem biometrisch aufgeladenen Mitarbeiterausweis realisiert werden:

- Zeit- und Betriebsdatenerfassung
- Personaleinsatzplanung
- Kantinenabrechnung mittels interner Geldbörse oder Kontoabzug
- Interne Geldbörse für Automaten und Mitarbeitereinkauf
- Berechtigung der Nutzung von Fahrzeugen und Betriebseinrichtungen
- Einsatz im ÖPNV

B. „Flughafenausweis“ mit biometrischen Merkmalen für Fach- und Dauerbesucher

1. Ist-Situation bei Besuchern

Sehr heterogene Personengruppe

Die Personengruppe der Besucher ist in sich sehr heterogen, so daß eine Differenzierung wichtig ist. Die meisten Besucher bringen oder holen Fluggäste ab. Sie kommen also nicht nur relativ selten, sondern halten sich auch nur in öffentlich zugänglichen Bereichen der Ankunfts- oder Abflughallen auf. In diesen öffentlich zugänglichen Bereichen findet eine Verifizierung oder andere Art der Überprüfung der Besucher nicht statt.

Unterschiedliche Motive und Ziele

Daneben haben aber sowohl der Flughafenbetreiber wie auch die auf dem Flughafengelände ansässigen Unternehmen und Betriebe – Fluggesellschaften, Dienstleister aller Art, Verkaufsbetriebe (Läden, Gaststätten etc.) – Besucher, die dort aus beruflichen Gründen zu tun haben, zum Beispiel Vertreter (Ein- und Verkäufer) für geschäftliche Verhandlungen. Diese Gruppe läßt sich wiederum differenzieren in Einmal-Besucher und Mehrfach-Besucher, also solche, die regelmäßig wiederkehren.

Außerdem gibt es eine kleine Gruppe von „special guests“, die etwa auf Einladung der Geschäftsleitung des Flughafenbetreibers oder einer Fluggesellschaft dem Flughafen einen Besuch abstatten.

Bei den letztgenannten Gruppen finden bereits jetzt Überprüfungen jedenfalls dann statt, wenn sie unbegleitet Sicherheitsbereiche betreten.

2. Anforderungen der EU

EU-Verordnung: Kontrollzwang für alle Besucher von Sicherheitsbereichen

Unter das Überprüfungsgebot nach der EU-Luftsicherheitsverordnung beim Übertritt vom öffentlich zugänglichen zum nicht öffentlich zugänglichen Bereich, insbesondere zu Sicherheitsbereichen wie der so genannten „Luftseite“, fallen alle Personen, also auch Besucher wie etwa Firmenvertreter zwecks Einkaufs-, Verkaufs- oder sonstigen geschäftlichen Verhandlungen. Diese werden hier unter dem Begriff des „Fachbesuchers“ zusammengefaßt.

Da es sich nicht um Flugpassagiere handelt, müßten für alle Fachbesucher, soweit sie den nicht öffentlich zugänglichen Flughafenbereich betreten wollen oder müssen, ebenfalls Flughafenausweise ausgegeben werden.

3. Datenschutzrechtliche Situation

Gesonderte Handhabung gegenüber Mitarbeiterausweisen

Aus datenschutzrechtlichen Gründen sollte ein solcher Ausweis für Besucher, gleich welcher Art, gegenüber den Flughafenausweisen für Mitarbeiter gesondert gehandhabt werden. Es läßt sich nämlich nicht auf bereits vorhandene oder ohnehin aus anderen Gründen notwendigerweise – schriftlich – abzuschließende Anstellungs-, Arbeits-, Werk- oder Dienstverträge zurückgreifen, in denen die datenschutzrechtlich notwendigen Einzelheiten hinsichtlich Erhebung, Speicherung und Handhabung sowie Art und Umfang der Daten vereinbart werden können.

Differenzierende Lösungen

Auch verlangt die Heterogenität der „Besucher" nach einer differenzierenden Lösung, um insoweit dem Verhältnismäßigkeitsprinzip zu genügen, das sowohl eine Kategorie des Marketings wie auch eine rechtliche, speziell auch datenschutzrechtliche Kategorie darstellt.

4. „Besucher-Ausweise", mit und ohne biometrischen Daten

„Abholer" und „Bringer" bleiben unkontrolliert

Bei Besuchern, die lediglich Fluggäste abholen oder bringen, ist ein spezieller Besucherausweis weder aus Sicherheitsgründen nötig noch angesichts der Masse solcher Personen an Flughäfen überhaupt denkbar. Besucher des Flughafens werden also nicht in das hier vorgestellte Sicherheitskonzept einbezogen, solange sie sich nur im öffentlich zugänglichen Bereich etwa der Ankunfts- und Abflughallen oder auf den Besucherterrassen aufhalten. Betreten sie allerdings Sicherheitsbereiche, gelten für sie analog die gleichen Sicherheitsmaßnahmen wie für die anderen Berechtigten in diesen Arealen.

Kontrolle oder Begleitung

Besucher nicht-öffentlicher Bereiche werden schon bisher im Prinzip den gleichen Sicherheitsmaßnahmen unterworfen wie berechtigte Beschäftigte. Sofern dies nicht überall möglich ist, sollten sich Besucher nur in Begleitung berechtigter Mitarbeiter bewegen dürfen.

Besuchergruppen mit Führung

Daneben gibt es vielfach Besuchergruppen – also Personen – die eigentlich nicht Fachbesucher sind, die aber gleichwohl zumindest auch Teile des nicht öffentlich zugänglichen Bereichs betreten. Solche Besuchergruppen sind allerdings stets vorangemeldet und werden von befugtem Fachpersonal (Guides) des betreuenden Unternehmens (Flughafenbetreiber, Fluggesellschaft etc.) geführt und bis zum Verlassen des Sicherheitsbereichs beaufsichtigt.

Besucherverwaltungssysteme nutzen

Empfang und Betreuung von Einzelpersonen lassen sich noch relativ leicht bewältigen. Komplizierter wird es bei Gruppen. Kein Unternehmen kann es sich leisten, die Daten erst bei der Ankunft aufzunehmen und dabei die Zugangsberechtigungen zuzuteilen. Die Aufnahme per Bleistift und Papier ist längst obsolet, zumal handgeschriebene Besucherscheine oftmals unleserlich sind. Hilfreicher und daher heute häufig schon benutzt sind Besu-

cherverwaltungssysteme. Mit diesen lassen sich Besucher schnell und problemlos entsprechend der Vorgaben des Werkschutzes aufnehmen.

Vorteile von Besucherverwaltungssystemen

Besucherverwaltungssysteme haben einen entscheidenden Vorteil: Regelmäßig gepflegt, sind sie für den Werkschutz von hohem Wert. So wird bei jedem Besucher geprüft, ob für ihn oder sein Unternehmen Zutrittsbeschränkungen oder sogar -verbote bestehen. Schnittstellen zu Zugangskontrollsystemen ermöglichen anstelle eines Besucherscheins, Ausweiskarten auszugeben. Diese vordefinierten Ausweiskarten mit bereits zugewiesenen Zutrittsberechtigungen enthalten neben den Besucherdaten alle Zutrittsbeschränkungen und können über ein Kartenlesegerät das unbefugte Eindringen verhindern. So werden aus herkömmlichen Besucherscheinen Ausweise. Schranken oder Türen beispielsweise öffnen sich dann nur, wenn die Besucherkarte eingelesen und für korrekt befunden wurde. Unbefugten bleibt der Zutritt verwehrt. Einmal-Ausweise werden beim Verlassen des Flughafengeländes durch einen Leser eingezogen.

Einmal-Ausweise ohne Biometriedaten für Besucher

Solche Einmal-Ausweise für gelegentliche Besucher, auch im Rahmen von Gruppen, entsprechen herkömmlichen Ausweisen. Deren Aufladung mit biometrischen Daten des jeweils Berechtigten wäre zwar technisch denkbar. Dies ist jedoch einerseits deshalb nicht notwendig, weil solche Besucher die Sicherheitsbereiche stets mit autorisierter Begleitung betreten. Andererseits wäre darüber hinaus auch der Zeit- und Kostenaufwand zur Erstellung biometrischer Ausweise im Verhältnis zur denkbaren Ersparnis gleich Null oder sogar negativ. Generell lassen sich Gesprächspartner, Guides, Führungsrouten und Aufenthaltsbereiche problemlos in ein Besucherverwaltungssystem eingeben. So weiß der Werkschutz stets, wo sich ein Besucher oder eine Besuchergruppe gerade befindet, beziehungsweise wer das Gelände noch nicht verlassen hat.

Bei „Fachbesuchern“, die also den Flughafen und ein dort ansässiges Unternehmen zu geschäftlichen Zwecken aufsuchen, ist zwar generell denkbar, daß sich diese alle der Prozedur zur Ausstellung eines mit ihren biometrischen Daten aufgeladenen Lichtbildausweises unterziehen. Denn sie suchen den Flughafen freiwillig auf, so daß man ihnen in einem Antrag auf Ausstellung eines Berechtigungsausweises zum Betreten des nicht öffentlich zugänglichen Bereichs auch eine Einverständniserklärung mit dem Erheben, Speichern und Verarbeiten biometrischer Daten abverlangen könnte, wenn Zweck und Umfang dieser Maßnahmen und die weitere Nutzung klar geregelt wären. Allerdings wird bei Einmal-Besuchern der damit verbundene Aufwand den Sicherheits-Mehrwert nicht rechtfertigen.

Besucher abholen und begleiten

Insoweit ist dem Besuchten zuzumuten, seinen Besucher entweder im öffentlich zugänglichen Bereich zu empfangen oder an einem bestimmten Übergang vom öffentlichen zum nicht-öffentlichen Bereich abzuholen und den Besucher während dessen gesamten Aufenthalt im Sicherheitsbereich ständig zu begleiten. In solchen Fällen würde weiterhin – wie bisher schon üblich – ein einfacher Besucherausweis ohne biometrische Daten genügen.

Datenschutzanforderungen sind zu wahren

Die Erfassung einiger weniger Daten eines solchen Einmal-Besuchers ist in diesem Umfang auch im Verhältnis zum verfolgten Zweck als angemessen zu betrachten. Eine – vorübergehende, in der Regel kurzzeitige – Speicherung solcher Besucherdaten ist datenschutzrechtlich im Rahmen des vom Flughafenbetreiber zuvor klar definierten und schriftlich niedergelegten Sicherungszwecks unbedenklich, ebenso deren Abgleich mit etwa im Besuchermanagementsystem hinterlegten Daten über Personen, denen teilweise oder generell der Zutritt aus unterschiedlichen Gründen zu verwehren ist.

Andere Ausgangslage bei Dauerbesuchern

Dem gegenüber wird bei Mehrfach- oder Dauer-Besuchern sowohl vom Besucher wie auch von Seiten des Besuchten der Wunsch aufkommen, den Besucher nicht jedesmal am Übergangspunkt abholen und dann während des gesamten Aufenthaltes im Sicherheitsbereich begleiten zu müssen. In solchen Fällen sollte vom Flughafenbetreiber mit Zustimmung eines auf dem Gelände ansässigen Unternehmens ein „Flughafenausweis für Dauerbesucher“ ausgegeben werden können.

Ausweisantrag als Vertragsgrundlage für Datenerfassung

Dann würde zwischen dem Antragsteller und dem Flughafenbetreiber ein Vertragsverhältnis begründet, im Rahmen dessen wiederum dem antragstellenden Besucher genau erläutert werden sollte, welche Daten zu welchem Zweck wo gespeichert, verarbeitet oder an Dritte weiterübermittelt werden. In einem solchen Rahmen und auf einer solchen vertraglichen Grundlage wären wiederum aus datenschutzrechtlicher Sicht auch Erhebung und Speicherung biometrischer Daten des Besuchers in dem für Mitarbeiter zuvor beschriebenen Rahmen und Umfang unbedenklich.

Überprüfung für Dauerbesucher wie für Mitarbeiter

Denn wenn ein solcher Mehrfach-Besucher unbegleitet Sicherheitsbereiche passieren können soll, wird er sich denselben Überprüfungen unterziehen müssen, die für einen auf dem Gelände ständig Beschäftigten notwendig sind. Dies gilt insbesondere für die in der EU-Luftsicherheitsverordnung für Mitarbeiter zwingend vorgeschriebene amtliche Zuverlässigkeitsprüfung durch die Sicherheitsbehörden. Die Beantragung eines solchen Ausweises mit den dafür erforderlichen Prozeduren ist schon bisher in Deutschland nicht gänzlich unbekannt. Dasselbe Verfahren wird etwa bei der Beantragung von Dauer-Zutrittsberechtigungen zu militärischen Geheimbereichen, aber auch für Lobby-Ausweise des Deutschen Bundestages seit vielen Jahren praktiziert.

„Dauer-Besucherausweise“ datenschutzrechtlich unbedenklich

Da die Beantragung freiwillig ist und ein Besuch solcher Bereiche stets auch auf andere, wenngleich zeitraubendere Art möglich bleibt, weil der Besucher jedesmal auf seinen Abholer warten und dieser ihn begleiten muß, scheinen gegen ein etwaiges Zusatzerfordernis nach Erfassung und Speicherung biometrischer Daten des Antragstellers auf dem für ihn ausgestellten „Dauer-Besucherausweis“ datenschutzrechtlich unter dem Gesichtspunkt der Zumutbarkeit und Verhältnismäßigkeit keine Bedenken zu bestehen.

5. Technische Ausgestaltung und Verfahren

Technik und Vorgehensweise wie beim Mitarbeiterausweis

Im Hinblick auf Ausgestaltung und Verfahren der Ausgabe eines biometrischen Flughafenausweises für Fach- und Dauerbesucher gelten die Ausführungen im Teil A. Nr. 2.2 und hinsichtlich der Vorteile die Ausführungen unter Teil A. Nr. 2.3 sinngemäß.

Gleiches gilt für die rechtlichen, insbesondere datenschutzrechtlichen Rahmenbedingungen für solche speziellen Besucherausweise, weil sie nicht an jeden Besucher, sondern nur an eine beschränkte Gruppe ausgegeben werden, die sich in einer speziellen Situation befindet. Besuchergruppen und sonstige Einmalbesucher erhalten, wie dargestellt, nach diesem Konzept auch künftig nur einen der auch bisher üblichen Besucherausweise ohne biometrische Daten, weil und solange sie sich in Begleitung autorisierter Personen in Sicherheitsbereichen aufhalten.

Die große Zahl der Begleitpersonen oder Abholer von Flugpassagieren, die sich in den öffentlich zugänglichen Bereichen der Ankunfts- und Abflughallen aufhalten sowie Besucher von Aussichtsterrassen und ähnlichen, allgemein zugänglichen Räumen werden ohnehin keiner allgemeinen Ausweisvergabe oder Ausweiskontrolle unterzogen.

C. „Flugpaß“ mit biometrischen Merkmalen für Passagiere der gewerblichen Luftfahrt

1. Ausgangslage und Rahmenbedingungen; künftige Anforderungen

EU-Verordnung: Zutritt zur „Luftseite“ und zum Flugzeug ist zu kontrollieren

Nach der EU-Verordnung gehören Warte- und Boardingbereiche für abfliegende Fluggäste (Passagiere) in den Abfertigungsbereichen der Flughäfen zur „Luftseite“, jedenfalls zum Sicherheitsbereich, da von dort der unmittelbare Zutritt zum Flugzeug eröffnet ist. Deshalb kann die EU-Verordnung dahin interpretiert werden, daß auch insoweit die allgemeine Vorgabe gilt, den Zutritt zu Sicherheitsbereichen und anderen luftseitigen Bereichen jederzeit so zu kontrollieren, daß der Zutritt Unbefugter verhindert, mit anderen Worten geprüft wird, ob derjenige, der ein Flugticket bzw. eine Bordkarte vorzeigt, mit dem identisch ist, der er nach der Bordkarte sein müßte (Verifikation). Dies wird bisher, wenn überhaupt, durch Vorzeigen des Personalausweises neben der Bordkarte beim Passieren der Zutrittskontrolle zum Abflugbereich kontrolliert.

Bordkartentausch unterbinden

Andererseits haben auch die Fluggesellschaften selbst schon seit längerem großes Interesse daran, den immer wieder vorkommenden Tausch von Bordkarten zu unterbinden, um sicherzustellen, daß sich wirklich diejenigen Personen im Flugzeug befinden, deren Namen auf der Passagierliste stehen. Davon können die Fluggesellschaften aufgrund bisheriger Erfahrungen derzeit nicht ausgehen.

1.2 Rechtliche Situation

Beförderungsvertrag als Grundlage für Datenerfassung und –verarbeitung

Datenschutzrechtlich ist von einem Beförderungsvertrag auszugehen, in dem die Fluggesellschaft mit dem Passagier vertraglich vereinbaren kann und ggf. muß, welchen Kontrollen er sich unterziehen muß bzw. welche Dokumente er zu seiner Legitimation und zur Verifikation seiner Berechtigung am Abfertigungsschalter bis hin zum Flugzeug und im Flugzeug akzeptieren muß, wenn er befördert werden will. Schon jetzt sehen die Buchungsbedingungen zahlreicher Fluggesellschaften die Vorlage eines Personalausweises oder sonstigen amtlichen Dokumentes beim Check-In vor, insbesondere dort, wo nicht vorab ein Flugticket ausgestellt und übersandt wird.

Nutzung biometrischer Daten ebenfalls denkbar

Wird die bisher weithin, aber auch jetzt schon nicht mehr ausnahmslos übliche Bordkarte aus Papier mit rückseitig aufgebrachtem Magnetstreifen durch eine andersartige Belegform ersetzt, die der Fluggast am Check-In-Schalter erhält und die ihm das Passieren aller Kontrollen bis zum Einsteigen in das Flugzeug ermöglicht, dann eingezogen oder ungültig wird, wäre die Erfassung selbst biometrischer Daten des Fluggastes prinzipiell nicht nur technisch, sonder auch rechtlich denkbar. Aus dem Beförderungsvertrag kann das Flugunternehmen durchaus das legitime Recht ableiten, daß sie nur denjenigen auch befördern muß, mit dem bzw. für den ein Vertrag

geschlossen wurde und den sie beim Check-In für die Mitnahme akzeptiert hat. Der heimliche Tausch von Bordkarten nach dem Check-In beinhaltet aus juristischer Sicht eine einseitige Vertragsänderung von Seiten des Kunden/Passagiers. Das muß eine Fluggesellschaft genauso wenig akzeptieren wie irgendein Partner eines beliebigen anderen Vertrages.

Bordkartentausch als einseitige Vertragsänderung

Erst recht wäre es unter kriminalpräventiven Gesichtspunkten und aus der Perspektive des Datenschutzes rechtlich vertretbar, zur Erhöhung der Sicherheit im Flugverkehr biometrisch aufgeladene Bordkarten zu dem ausdrücklichen Zweck auszugeben, die (unbefugte) Weitergabe von Bordkarten nach dem Check-In auszuschließen und auf diese Weise eine Übereinstimmung zwischen den Personen auf der Check-In- bzw. Boarding-Liste und den beförderten Passagieren sicherzustellen. Die biometrischen Daten sollten aus datenschutzrechtlicher Sicht bereits nach Abschluss des Boardings, müßten aber spätestens nach erfolgter Landung des Flugzeugs am Zielflughafen gelöscht werden. Dies gilt jedenfalls, soweit es nicht zur Klärung von Rückfragen wegen der etwaigen Beförderung eines am Zielflughafen illegal Einreisenden oder anderen relevanten Vorkommnissen erforderlich sein sollte, im Einzelfall die biometrischen und sonstigen Daten eines Passagiers länger, jedoch auch dann nur für zuvor festgelegte Zeiträume zu speichern.

Kriminalpräventiv wäre Verhinderung des Bordkartentauschs wünschenswert

Läge das Aufladen biometrischer Daten auf einen Boarding-Ausweis insoweit noch im legitimen Interesse der Fluggesellschaft und wäre damit datenschutzrechtlich vertretbar, so erscheint eine darüber hinausgehende, allgemeine Einführung eines biometrisch aufgeladenen, speziellen Flugausweises, der von Passagieren generell benutzt werden muß und ohne den sie praktisch nicht mehr fliegen könnten, weil etwa ohne ihn bzw. die auf ihm gespeicherten biometrischen Daten schon die Buchung einer Flugreise und/oder auch das Einchecken zu einem gebuchten Flug nicht mehr möglich wäre, unter den gegebenen rechtlichen Rahmenbedingungen in Deutschland – derzeit – nicht zulässig. Denkbar sind aus datenschutzrechtlichen Gründen in überschaubarer Zeit realisierbare, biometrisch aufgeladene Ausweise für Flugpassagiere entweder nur für besondere Personengruppen auf der Grundlage entsprechender vertraglicher Vereinbarungen vorzugsweise mit Fluggesellschaften, möglicherweise aber auch Flughafenbetreibern oder – auf der Grundlage des Beförderungsvertrages – im eng begrenzten Bereich des Boardings und der Passage im Rahmen dieses einen Fluges.

Weitergehende, verpflichtende Nutzung biometrisch aufgeladener Flugpässe derzeit nicht zulässig

Für einen „Flugpaß“, der grundsätzlich von der Buchung über Check-In, Boarding, aber auch zum Beispiel für die Gepäck-Zuordnung am Zielflughafen einsetzbar wäre, zumal wenn Flughafenbetreibern oder Fluggesellschaften seine Nutzung von den Passagieren zwingend verlangen wollten, wären über die Schaffung entsprechender Rechtsgrundlagen in Deutschland bzw. der Europäischen Union hinaus auch noch weltweit einheitliche technische Einsatzbedingungen, etwa im Rahmen von ICAO abzustimmen. Ehe derlei aus dem Bereich technischer Visionen in Realitätsnähe rückt, erscheint es realistischer anzunehmen, daß die ebenfalls schwierigen Ab-

Rechtsgrundlagen für allgemeinen „Flugpaß“ fehlen derzeit

stimmungsgespräche über die Standardisierung biometrischer Verfahren für amtliche Reisedokumente trotz aller Differenzen zwischen den Regierungen kurzfristig zur Festlegung auf praktikable Verfahren und Parameter voranschreiten, so daß die entsprechenden Reisedokumente dann genutzt werden könnten. Insoweit wäre dann nur die Freigabe zur privaten Nutzung der Ausweisdaten, Verfahren und Parameter durch den nationalen Gesetzgeber erforderlich. Insoweit wird auch auf das in der Einleitung dazu Gesagte verwiesen.

Weltweite Abstimmung nötig

Ein Flugpaß wiederum, der auf vertraglicher Basis als individueller Dauerausweis an Vielflieger oder einen anderen Personenkreis durch eine oder mehrere Fluggesellschaften und/oder Flughafenbetreiber ausgegeben wird, könnte allerdings schneller für ähnliche Zwecke genutzt werden, weil er auf Vertragsbasis ausgegeben würde. Außerdem haben es Fluggesellschaften und Flughafenbetreiber selbst in der Hand, die technischen Einsatzbedingungen zu schaffen und überregional zu harmonisieren. Schon die Benutzung dieser Karte etwa zur Erleichterung des Boarding bedarf einer Absprache zwischen der einen Fluggesellschaft und einer Vielzahl von Flughafenbetreibern im Inland, in Europa und außerhalb Europas, soll sie dem berechtigten Inhaber wirklich von Nutzen sein.

Einheitliche Technik wünschenswert

Aus Sicht der Flughafenbetreiber müßte die verwendete biometrische Technik in den von verschiedenen Fluggesellschaften ausgegebenen Ausweisen identisch sein. Andernfalls müßte der Flughafenbetreiber eine Vielzahl von Systemen bereit stellen, was einen nicht unerheblichen Mehraufwand mit sich brächte.

2. Der „Flugpaß“ mit biometrischen Merkmalen

DFK-Vorschlag: Flugpaß mit biometrischen Daten für Vielflieger

Vorgeschlagen wird die Einführung eines neuartigen „Flugpasses“ für Passagiere, deren biometrische Daten auf den Ausweis aufgebracht sind. Die Ausgabe erfolgt auf freiwilliger Basis und aufgrund vertraglicher Vereinbarung, etwa im Rahmen von Vielfliegerprogrammen oder anderer Special-Services der Fluggesellschaften.

2.1 Ziel, Nutzen und Zwecksetzung

Zunehmende Kontrollen für Vielflieger lästig

Aufgrund der sich ständig verschärfenden Kontrollen gerade für Flugpassagiere haben die Kontrollen einen hohen Lästigkeitswert. Außerdem kosten sie viel Zeit. Beides stört insbesondere Vielflieger. Die Fluggesellschaften müssen daher darauf bedacht sein, die Schwelle des noch Zumutbaren nicht zu überschreiten, gleichwohl aber das erforderliche Sicherheitsniveau zu halten.

Flugpaß zur effektiven Verifikation

Beides zu kombinieren, könnte dadurch gelingen, daß ein neuer Flugpaß ausgegeben wird, der nicht notwendigerweise ein Lichtbildausweis sein muß, der aber auf einem integrierten Chip biometrische Daten gespeichert

hat, die jederzeit durch dazu Befugte verifizieren lassen, ob der Inhaber, der ihn an einem Kontrollpunkt vorzeigt, auch tatsächlich derjenige ist, dem das Luftfahrtunternehmen bzw. der Flughafenbetreiber aufgrund eines Vertrages bestimmte Vergünstigungen zuerkannt hat.

Zusätzliche Anwendungen

Der neue Flugpaß kann zudem Datenträger für die Vielfliegerprogramme der Fluggesellschaften und weitere kundenorientierte Applikationen sein; damit erschließen sich zusätzliche Anwendungen und eine Verbesserung des Kosten/ Nutzenverhältnisses.

Bewegungsdaten alsbald löschen

Bewegungsdaten beim Einsatz des Flugpasses werden spätestens nach Beendigung des Fluges gelöscht. Mit seiner Zustimmung zu den Zusatzprogrammen von Luftfahrtgesellschaften und/oder Flughafenbetreibern stimmt der Passagier auch heute schon der zweckgebundenen Nutzung dieser Daten für das jeweilige Programm zu. Diese Zustimmung könnte auf die zweckgebundene Verwendung der biometrischen Daten erstreckt werden.

Etwaige „Identitätsprüfung“ nicht Teil dieses Konzeptes

Verifikation statt Identifikation

In beiden Varianten wird im Übrigen nicht die „Identität“ des Passagiers geprüft. Ob die Fluggesellschaften die Identität des gebuchten Passagiers anhand eines von der Person, die unter einem von ihr am Check-In-Schalter angegebenen und auf der Buchungsliste tatsächlich erscheinenden Namens begehrt, für einen bestimmten Flug eingecheckt zu werden, zuvor die Vorlage eines amtlichen Ausweises verlangen, wie dies derzeit schon zum Teil geschieht, oder nicht, insbesondere ob sie dies künftig generell verlangen sollten, etwa zur weiteren Erhöhung der Sicherheit im Flugverkehr oder nicht, ist nicht Teil des hier vorgestellten Konzeptes und soll daher hier nicht betrachtet werden. Daher bleibt auch die Frage unerörtert, ob die Fluggesellschaften im Falle einer Überprüfung der Identität des Einzucheckenden anhand eines amtlichen Ausweises die womöglich dort eingebetteten biometrischen Daten zur Verifikation rechtlich benutzen dürfen und sie technisch benutzen können.

2.2 Technische Ausgestaltung und Verfahren

Biometrische Daten nur auf dem Flugpaß

Der neue Flugpaß enthält die personenbezogenen einschließlich der biometrischen Daten des Passagiers. Er stellt also eine persönliche „Datenbank“ dar. Die biometrischen Daten bleiben im Besitz des Passagiers, ausschließlich gespeichert im Flugpaß. Es muß jedenfalls für Boarding-Zwecke keine zentrale Speicherung erfolgen.

Papierflugticket für Biometrie nicht nutzbar

Das Papierflugticket mit Magnetstreifen ist als Datenträger für die Sicherheitsfunktionen, insbesondere Daten der Biometrie, teils aus technischen, vor allem aber aus organisatorischen Gründen nicht einsetzbar. Es kann entweder die bei bestimmten Verfahrensweisen anfallenden Datenmengen

nicht speichern, ist nicht sicher genug oder eine sichere Aufbringung biometrischer Daten erscheint angesichts der Vielzahl der Ausgabestellen für Papierflugtickets nicht ohne weiteres organisierbar.

Flugpaß für Flugdaten nicht nutzbar

Die Flugdaten können vor allem aus Handhabungsgründen auf dem neuen Flugpaß nicht dargestellt werden. Als Hauptgrund steht dem die weltweite Standardisierung des heutigen Systems mit sich häufig ändernden Flugdaten – gerade beim Umsteigen auf einen anderen Flug – entgegen. Voraussetzung für den Einsatz als universelles elektronisches Ticket ist also die Standardisierung in den internationalen Gremien mit dem entsprechenden Zeitaufwand. Das vorgeschlagene Verfahren erlaubt im Gegenzug auch das Beibehalten der eingeführten und bewährten Buchungs- und Reservierungssysteme.

Beide Dokumente notwendig

Das Papierflugticket und der neue Flugpaß werden, solange nicht auch volle Flugdaten auf der neuartigen Speicherchipkarte untergebracht werden können, also gemeinsam benötigt. Dies hat einen großen Vorteil gegenüber der Speicherung aller Daten nur auf einer einzigen Karte:

Ein Verlust oder ein Diebstahl des Papierflugtickets führt nicht zu einem Problem, da das Papierflugticket eine Referenz zum neuen biometrischen Flugpaß erhält und nur mit diesem zusammen gültig ist.

Technische Daten wie bei Mitarbeiterausweis

Im Übrigen entsprechen die technischen Daten prinzipiell denen des oben im Teil A vorgeschlagenen Flughafenausweises mit integrierten biometrischen Daten für Mitarbeiter. Auch der Flugpaß entspricht einer genormten Ausweiskarte und ist eine berührungslos arbeitende passive Karte (RFID-Smart Card ohne Batterie) mit kontaktlosem und, sofern für Zusatzanwendungen nötig, mit zusätzlichem kontaktbehafteten Chip. Die Karte verfügt über einen großen Datenspeicher.

Nutzung für reine Boardingzwecke unrentabel

Bei einer Nutzung des biometrisch aufgeladenen Ausweises für reine Boarding-Zwecke würde die Karte beim Betreten des Flugzeugs gelöscht und eingezogen. Dann würde es genügen, auf der Karte einige wenige der nachfolgend benannten Daten zu speichern, in erster Linie den Namen des Fluggastes, seine Flugdaten und eben seine biometrischen Daten. Da das Verfahren schnell gehen müßte und die Akzeptanz zusätzliche und gar umständliche bzw. zeitraubende Sicherheitsmaßnahmen bei den Passagieren vermutlich gering ist, könnte nur ein einfaches biometrisches Verfahren in Betracht kommen.

Bei einer Benutzung der Karte als „Flugpaß“ für Vielflieger aufgrund jeweils spezieller vertraglicher Vereinbarungen mit den Fluggesellschaften müßten zum Beispiel folgende Daten erfaßt bzw. angezeigt werden:

Abb. 2: Beispiel für den neuen Flugpass für Vielflieger

Die Vorderseite enthält:

- Lichtbild des Ausweisinhabers
- Personaldaten wie z.B. Name
- Ausweiskennung
- Logo / Name der Fluggesellschaft bzw. des Ausgebers

Die Rückseite enthält:

- rechtliche Vertragssituation
- Magnetstreifen, frei ggf. für carrierspezifische Informationen

Die Speicher enthalten:

- Personendaten
- Biometriedaten
- Ausweiskennung
- Administrationsdaten
- Gültigkeitsdauer

Organisatorische Sicherungen

Der Ausweis wird durch die Fluggesellschaften ausgestellt und in einem gesicherten Verfahren, wie jetzt schon bei ähnlichen Ausweisen, an den Berechtigten übersandt. Er kann technisch und sollte auch aus Sicherheitsgründen zeitlich befristet und darüber hinaus bei Verlust oder anderen wichtigen Gründen jederzeit gesperrt werden können.

2.3 Vorteile von Flugpässen mit biometrischen Merkmalen

Kriminalpräventiver Vorteil: sichere Verifikation des Passagiers

Unter kriminalpräventiven Gesichtspunkten wäre ein Vorteil von Flugpässen mit biometrischen Merkmalen, auch soweit sie nur zu Boarding-Zwecken benutzt würden, daß sie eine sichere Verifikation der tatsächlich beförderten Passagiere ermöglichen. So kann sichergestellt werden, dass diejenigen, die für einen bestimmten Flug eingecheckt sind und deren Namen insofern erfaßt werden, tatsächlich auch diejenigen sind, die befördert werden. Dies bringt bei einem Zwischenfall schon deshalb Vorteile, weil leichter als bisher festgestellt werden kann, wie viele und welche Personen von einem Ereignis mit einem Flugzeug betroffen sind. Darüber hinaus hat die Verifizierung der mitfliegenden Passagiere gegenüber der Check-In-Liste auch einen konkreten kriminalpräventiven Vorteil, weil die Verschleie-

rung der Identität eines potentiellen Straftäters erschwert wird, zumal dann, wenn beim Check-In die Vorlage eines amtlichen Ausweises zur Identitätsprüfung allgemein üblich wird.

Zusatznutzen

Im Übrigen wäre einiger Zusatznutzen denkbar, nämlich:

- vereinfachtes Handling bei Abflug, Ankunft und Stop over
- Selbst-Check-in mindestens für Passagiere ohne Gepäck
- schnellere Abfertigung bei Check-in und am Gate
- Kundenbindung bei zusätzlicher Nutzung als Traveller-Card

Weitere Applikationen

Weitere Funktionen könnten als zusätzliche Applikationen auf dem Flugpaß realisiert werden, die einerseits dem Karteninhaber einen besseren Service bieten und andererseits dem Anbieter eine rationellere Abwicklung ermöglichen. Die Dateistruktur moderner Chipkarten-Ausweise bietet sich für solche Aufgaben mit spezifischen Bereichen für die einzelnen Anwendungen direkt an.

Beispiele von Funktionen unter Einsatz des Flugpasses:

- Bonuskartenaktionen für Restaurants, Geschäfte, Services, Mietwagen etc.
- Kombinierter Flugschein, Bahnfahrkarte, Mietwagenzugang auf einer Chipkarte
- Bargeldloses Zahlen als Teil eines Membership-Programms

Ferner kann wegen der grundsätzlichen technischen Ähnlichkeit und Handhabung von Flughafenausweis einerseits und Flugpaß andererseits zumindest für bestimmte Mitarbeiter von Fluggesellschaften die Möglichkeit geschaffen werden, daß diese beim Boarding als Passagier keinen weiteren Ausweis benötigen. Hier kann vielmehr der Flughafenausweis als Bordkarte eingesetzt werden, der dann allerdings beim Besteigen des Flugzeugs natürlich nicht ungültig und eingezogen wird wie bei normalen Passagieren.

2.5 Grenzen des Einsatzes von Flugpässen mit biometrischen Daten

Standards und überregionale Abstimmung nötig

Ein Flugpaß, der von Passagieren generell auf mehreren Flughäfen, insbesondere auch außerhalb Deutschlands oder auch Europas, also weltweit benutzt werden könnte, könnte erst eingeführt werden, wenn entsprechende Absprachen zur Vereinheitlichung der Systeme auf nationale Ebene

mindestens zwischen den verschiedenen Flughafenbetreibern und Fluggesellschaften, bei einer Verwendung auch außerhalb Deutschlands innerhalb von Europa durch zusätzliche zwischenstaatliche Vereinbarungen und auf weltweiter Ebene durch entsprechende einheitliche ICAO-Richtlinien unter gleichzeitiger Vereinheitlichung der technischen Standards geregelt würden. Solche vereinheitlichten Standards sind derzeit zwar im Gespräch, aber noch nicht absehbar. Insoweit bleibt die weitere Entwicklung abzuwarten.

D. Sicherung öffentlich zugänglicher Bereiche des Flughafens

1. Ausgangslage und Rahmenbedingungen

Ankunft- und Abflughallen als kriminogene Orte

Die öffentlich zugänglichen Bereiche eines Flughafens, also seine Ankunfts- und Abflughallen, sind aufgrund ihrer Unübersichtlichkeit und der Vielzahl von Tatgelegenheiten ein Ort vielfältiger krimineller Handlungen. Häufige Delikte sind Diebstähle von Ausweisen, Wertgegenständen und Gepäck.

Daneben beklagen zumindest einige Flughafenbetreiber in Deutschland immer wieder Fälle von Sachbeschädigung und Vandalismus bis hin zu potentiell gemeingefährlichen Straftaten wie Legen von Bränden in Papierkörben, Abstellen als Gepäck getarnter Bomben und ähnliche Delikte.

Hausverbote durchsetzen

Schließlich haben zumindest die größeren Flughafenbetreiber immer wieder auch mit Personen zu tun, die Fluggäste und/oder Besucher belästigen oder die weitläufigen, öffentlich zugänglichen Bereiche der Flughafenhallen im Bereich von Ankunft und Abflug für unerwünschte Zwecke nutzen. Solche Personen fallen in der Regel über längere Zeit hinweg immer wieder auf und werden regelmäßig der Räumlichkeiten und des Flughafengeländes verwiesen, erhalten also Hausverbot von Seiten des Flughafenbetreibers als Inhaber des Hausrechtes.

2. Rechtliche Bewertungen und Rahmenbedingungen

Video-Überwachung als Ausgangspunkt

Der zuvor unter Nr. 1 beschriebene Bereich des Flughafengeländes liegt außerhalb des unmittelbaren Regelungsbereichs der EU-Flughafensicherheitsverordnung und des geplanten deutschen Luftsicherheitsgesetzes.

Um die Sicherheit in diesem öffentlich zugänglichen Bereich zu erhöhen, sind verschiedene technische Maßnahmen denkbar, die künftig miteinander kombiniert werden könnten. Technischer Ausgangspunkt und heute schon bisweilen anzutreffen ist die Videoüberwachung solcher Bereiche, mit und ohne Aufzeichnung der Bilddaten.

§ 6b BDSG beachten

Eine solche Videoüberwachung kann der Grundeigentümer und Inhaber des Hausrechts einrichten, bei den hier diskutierten „öffentlich zugänglichen Räumen“ allerdings nur unter Beachtung mindestens der in § 6b BDSG definierten Voraussetzungen und Rahmenbedingungen. Zudem müssen Überwachung und Aufzeichnung durch den Flughafenbetreiber oder einen von ihm beauftragten Dritten ausschließlich auf privatrechtlicher Basis erfolgen.

Gut sichtbare Hinweise

Auf die Videoüberwachung, je nach landesrechtlicher Situation ergänzend auch auf die Speicherung von durch Videoüberwachung aufgenommenen Bilder einschließlich der speichernden Stelle, ist ausreichend sichtbar durch Beschilderung hinzuweisen. Die insoweit notwendige Beschilderung ist

künftig durch Verwendung eines genormten Hinweiszeichens für Videoüberwachung möglich, das derzeit erarbeitet wird.

3. Einsatz der Videoüberwachung zur Personenerkennung / Personensuche

Videoüberwachung mit Biometrie aufrüsten

Im Rahmen einer allgemeinen Überwachung öffentlich zugänglicher Bereiche des Flughafens kann unter rein technischer Sicht die Biometrie auch zur Personenerkennung und Personensuche (Personenidentifikation) benutzt werden. Dazu können die meist schon vorhandenen CCTV-Überwachungskameras und –systeme herangezogen, wenn sie mit geeigneter Gesichtserkennungssoftware aufgerüstet werden.

Dabei werden nicht-kooperative Verfahren der biometrischen Erkennung eingesetzt. Der Beobachtete muß also selbst keinen Beitrag zu seiner Identifikation leisten. Solche auf der Gesichtserkennung basierende Systeme machen Vorschläge zur Identität der betroffenen Person, wobei die Meldung erst erfolgt, wenn ein vorher eingestellter Ähnlichkeitsgrad erreicht wird.

Abgleich zu gespeicherten Bilddaten

In aller Regel enthält das System eine relativ kleine Liste von gesuchten oder nicht erwünschten Personen, deren Erscheinen gemeldet wird. Speicherung und Alarmierung können unterschiedlich organisiert werden. Die Alarmierung kann automatisch erfolgen, wenn das System eine Person detektiert, die einen bestimmten, zuvor eingestellten Grad an identischen Merkmalen mit einer Person hat, deren Merkmale hinterlegt sind. Die Speicherung kann dann – zunächst vorübergehend für kurze Zeit – durch Alarmierung automatisch erfolgen. Eine Speicherung zur weiteren Bearbeitung des Vorgangs kann dann nach Überprüfung der detektierten Person vom Leitstellenpersonal veranlaßt werden. Es ist aber auch möglich, das Verfahren so zu organisieren, daß eine Speicherung und Alarmierung grundsätzlich erst nach entsprechender Bestätigung durch das Leitstellenpersonal erfolgt.

Verifikation durch das System, Identifikation anschließend manuell

Je nach Betrachtungsweise wird nicht die beobachtete bzw. vom System erfaßte, sich im öffentlichen Bereich aufhaltende natürliche Person identifiziert, sondern mittels biometrischer Verfahren eine sich dort bewegende Person im Verhältnis zu einem gespeicherten Bild auf Übereinstimmung mit diesem verifiziert. Ob die Person, die durch das System erfaßt wird, tatsächlich identisch ist mit der Person, deren Daten im System hinterlegt sind, aus welchen Gründen auch immer, muß sodann vom Sicherheitspersonal durch manuelle Überprüfung festgestellt werden. Erst diese Feststellung beinhaltet dann die eigentliche Identifizierung.

Einsatzorte: Rolltreppen, Türen

Ein effizienter Einsatz solcher Systeme erfolgt in Bereichen, die auf „natürliche“ Weise die Besucher zum vereinzelten Passieren zwingen - also Rolltreppen, Türen etc.

Abb. 3: Automatische Gesichtserkennung

Die meisten der im öffentlich zugänglichen Flughafenbereich (Ankunfts- und Abflughalle) installierten CCTV-Kameras bieten einer zentralen Leitstelle die Möglichkeit, den Bereich von Ferne ständig einzusehen oder bei Auftreten bestimmter Ereignisse das Kamerabild automatisch in die Leitwarte zu schalten bzw., sofern das Signal dort ständig vorliegt, das Bild sichtbar zu machen.

Je nach festgelegtem Sicherheitsprotokoll für die Benutzung der CCTV-Anlage sind für die verschiedenen Funktionen wie Schwenken, Zoomen, Speichern und Zugriff auf gespeicherte Bilder Autorisierungshierarchien einzuführen. Solche gehören heute zum Standard im Rahmen des sogenannten organisatorischen Datenschutzes bei der Videoüberwachung.

Bei einer „hinterlegten“ Personensuche (Gesichtsvergleich) ist eine Freigabe von autorisierter Stelle, deren Kriterien in Abstimmung mit dem Datenschutz zu erarbeiten sind, erforderlich.

Das Verfahren der Gesichtserkennung ist als benutzerfreundlich einzustufen, da die beobachtete, ggf. zu erkennende Person weder Auge noch Hand aktiv benutzen muß. Es ist allerdings bei dieser Einsatzart auch in sehr verdeckter Form möglich. Die zu überwachende Person weiß und

merkt von dieser Überwachung nichts, wenn kein Hinweis auf diese mit der Gesichtserkennung gekoppelte Videoüberwachung erfolgt. Auf die mit einer derartigen Überwachungsmaßnahme verbundenen datenschutzrechtlichen Erfordernisse wurde oben bereits hingewiesen.

sichtbare Hinweise erforderlich; § 6b BDSG beachten

Um die Vorteile der Gesichtserkennung zu nutzen, erfolgt in einer Leitstelle eine entsprechende Nachbearbeitung im Sinne des bereits erwähnten manuellen Abgleichs.

E. Grundlageninformationen - Methoden der biometrischen Erkennung

1. Allgemeines zu kooperativen Verfahren

In diesem Abschnitt werden nur so genannte „kooperative“ biometrische Erkennungsverfahren beschrieben.

„Kooperativ“ bedeutet in diesem Zusammenhang nicht, daß der Benutzer das biometrische System freudig und mit kaum verhaltener Begeisterung nutzt. Er muß aber mit ihm kooperieren, indem er seinen PIN-Code oder seinen Ausweis präsentiert und/oder sich vor dem Erfassungsgerät „in Positur stellt“.

Als sogenannte „statische“ oder „physiologische“ biometrische Methoden stehen zur Zeit zur Verfügung:

- Fingerabdruck-Erkennung
- Gesichtserkennung
- Handgeometrie-Erkennung
- Iris-Erkennung

Die dynamischen oder verhaltensbedingten Verfahren wie zum Beispiel Unterschrifts- oder Sprechererkennung bleiben in diesem Dokument im weiteren unerörtert, da sie in dem hier interessierenden Kontext vermutlich nur in Sonderfällen einzusetzen wären.

Alle genannten Verfahren können zur „Verifikation der behaupteten Identität“ benutzt werden, um sicherzustellen, daß die Person, die das Verfahren durchläuft, diejenige ist, die sie nach dem vorgelegten Referenzdatum (Pin-Code, Ausweis etc.) vorgibt zu sein [sog. „1:1-Vergleich“]. In diesem Sinne findet keine Identifizierung dahingehend statt, ob der Inhaber des Ausweises unter diesem Namen tatsächlich existiert und in den amtlichen Registern (Einwohnermeldeverzeichnis, Standesamtsregister) als existente Person registriert ist. Eine solche echte „Identifikation“ [1:n-Vergleich] ist ohne Rückgriff auf amtliche Register nicht möglich und daher staatlichen Stellen auf Grundlage einer besonderen gesetzlichen Erlaubnis vorbehalten. Solche Verfahren finden zwar im Rahmen der allgemeinen Flughafensicherheit auch statt, doch ausschließlich im hoheitlichen Bereich, etwa bei der Einreise- und Ausreisekontrolle (Grenzübertritt). Diese hoheitlichen Kontrollen sind nicht Gegenstand dieser Ausarbeitung. Ihr Verfahren bleibt daher auch hier im Rahmen dieses Abschnittes unbetrachtet.

Die einzelnen biometrischen Verfahren werden nachfolgend kurz vorgestellt. Dabei wird davon ausgegangen, daß alle Verfahren in marktverfügbaren Systemen unterschiedlicher Hersteller aufgrund einer wenigstens teilweise bereits langjährigen Nutzung in verschiedenen Anwendungen alltagstauglich sind.

2. Gesichtserkennung (kooperativ)

Die Gesichtserkennung ist berührungslos. Daher stellt sie ein komfortables und wenig aufdringliches Verfahren der biometrischen Erkennung dar

Es kann davon ausgegangen werden, daß eine für die konkrete Anwendung erforderliche, hinreichende Erkennungssicherheit für die hier aufgeführten Anwendungen bei der Verifikation 1:1 nach gegenwärtigem Stand der Technik bei entsprechender Kalibrierung des eingesetzten Systems zu erreichen ist.

Die Berliner Flughafengesellschaft hat im Jahre 2003 eine entsprechende Einrichtung zur Kontrolle der Mitarbeiter beim Zutritt zum Sicherheitsbereich installiert.

Abb. 4:
System für kooperative Gesichtserkennung

Für die Gesichtserkennung werden verschiedene Verfahren angewendet. Die in Deutschland am häufigsten eingesetzten Verfahren arbeiten mit über 1.000 individuellen Gesichtsmerkmalen, die mathematisch verarbeitet und zu einem resultierenden „Gesichtsvektor“ zusammengesetzt werden. Dieser Vektor zeigt hohe individuelle Ausprägung, die die Verifikation des Probanden gegenüber der behaupteten Identität dieser Person laut Referenzdokument zulassen.

3. Handgeometrie

Die biometrische Prüfung der Handgeometrie ist ein seit langem im Einsatz befindliches Verfahren zur Verifikation einer behaupteten Identität. Sie wird also in der Regel zusammen mit Ausweis oder PIN angewendet.

Für die Erfassung und Speicherung des Templates ist die Größe des Templates mit nur neun Bytes als vorteilhaft anzusehen.

In der Praxis werden auf Handgeometrie basierende Systeme unter anderem bereits auf vielen nordamerikanischen Flughäfen und bei INSPASS, dem US-Frequent-Traveller-Verfahren, eingesetzt.

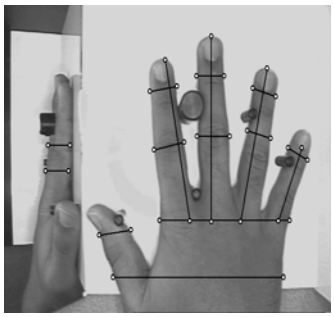

Abb. 5: Handgeometrie

Die Konturen der Hand, welche beim Menschen unterschiedlich sind, werden durch ein Spiegelsystem von einer Kamera erfasst und ausgewertet. Dabei wird die Kontur der Hand an über 90 Messpunkten über Länge, Breite, Krümmung registriert und die relativen Positionen von Fixpunkten zueinander analysiert. Die Prüfung erfolgt sehr schnell.

4. Fingerabdruck-Erkennung

Fingerabdruck-Erkennung ist das älteste biometrische Verfahren. Es wird seit langem in der Kriminalistik angewendet, wenngleich bis vor einiger Zeit ohne automatisierte Verfahren. Die Verläufe der Papillaren (Hautleisten) der Fingerkuppen und insbesondere ihre Endungen und Verzweigungen haben einen hohen Unterscheidungsgrad, so daß eine individuelle Erkennung, insbesondere eine 1:1-Verifikation, erfolgreich durchgeführt werden kann.

Abb. 6 Fingerabdruck-Erkennung

Die Minutien der Finger (Verzweigungen und Endungen der Papillaren) sind eindeutig, unveränderlich und nicht veränderbar; sie werden bei der Geburt vorgegeben. Erkennungsschwierigkeiten kann es bei Kindern unter 6 Jahren und älteren Menschen sowie bei temporären Veränderungen der Fingerkuppen, z.B. infolge von Verletzungen geben.

Neben der Erkennung der Minutien gibt es noch die Erkennung der Papillarmuster und den direkten Bildvergleich des Fingerabdrucks sowie weitere spezielle Techniken.

5. Iris-Erkennung

Wie beim Fingerabdruck zeigt auch die Iris individuelle Ausprägungen ihrer Muster. Dies Muster werden zur Erkennung herangezogen. Dabei wird die Farbe der Iris nicht berücksichtigt. Das Irismuster bildet sich pränatal in den letzten Wochen vor der Geburt zufallsbedingt aus, ist also nicht genetisch bedingt. Wie auch bei Fingerabdrücken ist das Muster der menschlichen Augeniris einzigartig und unveränderlich.

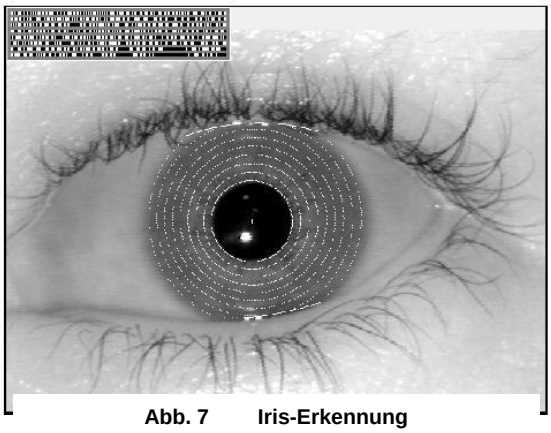

Abb. 7 Iris-Erkennung

Für die Codierung der Struktur der Netzhaut werden vielfach orientierungssensitive, zweidimensionale Filter-Algorithmen benutzt. Die entstehenden biometrischen Daten beruhen auf einer Merkmalsmenge von 266 Informationen. Die Iris-Erkennung zeichnet sich durch ihr hohes Maß an Individualität des zu identifizierenden Merkmals aus.

F. Anhang

Normung und Standardisierung biometrischer Verfahren

1. Normungsbedarf

Bei geschlossenen Anwendungen, die von einem bestimmten Hersteller bedient werden, besteht prinzipiell kein Normungsbedarf. Bei offenen Anwendungen und Systemen, bei denen Systemkomponenten unterschiedlicher Hersteller sowie ein nicht im vorhinein begrenzter Personenkreis betroffen ist, sowie aus Gründen der Investitionssicherheit Interoperabilität zwischen den Systemen gefordert ist, besteht dagegen hoher Normierungsbedarf.

Verschiedene Arten von generischen internationalen Standards hierarchischer Natur werden zur Unterstützung der Identifikation und Verifikation benötigt. Die nachfolgende Grafik illustriert diese Abhängigkeiten:

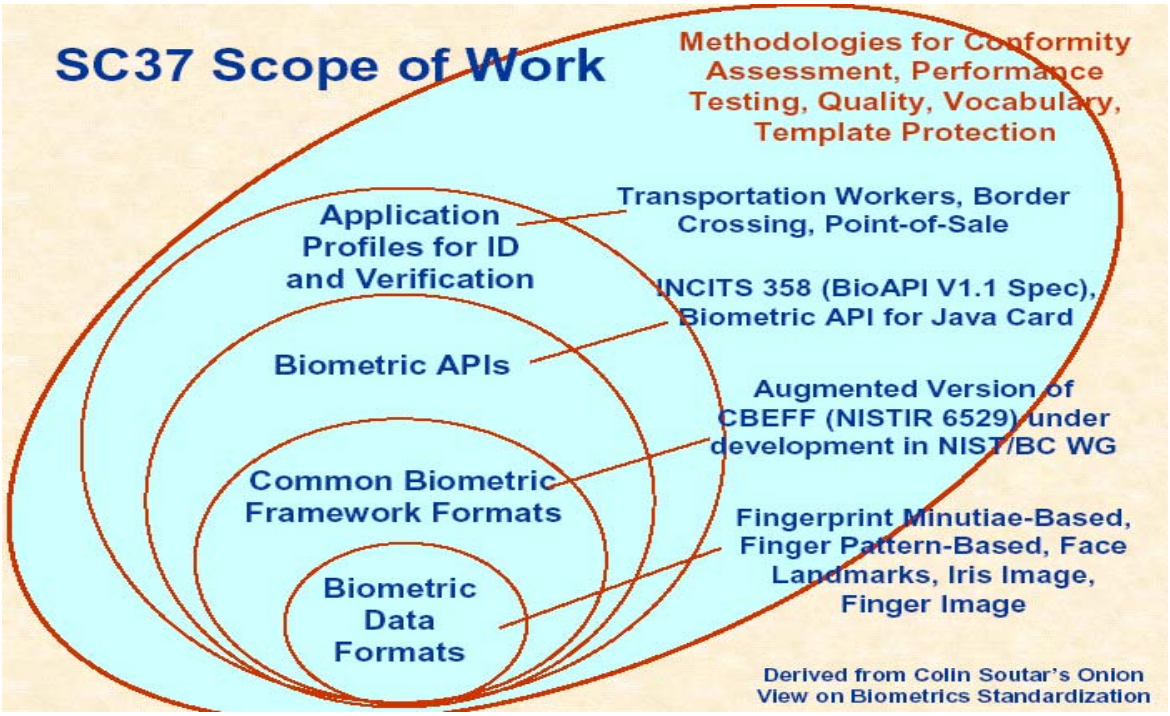

Abb. 8

2. Bisherige Standards

In den letzten Jahren wurden mehrere biometrische Standards erarbeitet und international harmonisiert. Dies wurde durch verschiedene Konsortien erarbeitet :

- BioAPI Consortium
- Biometric Consortium
- NIST/Biometric Consortium Biometric Working Group
- International Biometric Industry Association (IBIA)
- Biometric Foundation
- UK Biometrics Working Group der CESG
- Teletrust e.V., AG 6 Biometrische Identifikationsverfahren

Die bisher erarbeiteten Standards bzw. empfohlene Verfahrensweisen umfassen u.a.:

- ISO/IEC 7816-11 — für den Einsatz biometrischer Verfahren mit dem Einsatz von SmartCards
- NISTIR6529 CBEFF — Common Biometric Exchange File Format
- BioAPI — Festlegung biometrischer Schnittstellen
- BEM — Empfehlung zur Evaluierung biometrischer Systeme für die Common Criteria
- BPTR — Best Practice in Testing and Reporting Performance of Biometric Devices
- Kriterienkatalog des Teletrust e.V. AG 6

Weitere relevante Standardisierungsbestrebungen sind in der folgenden Tabelle aufgeführt:

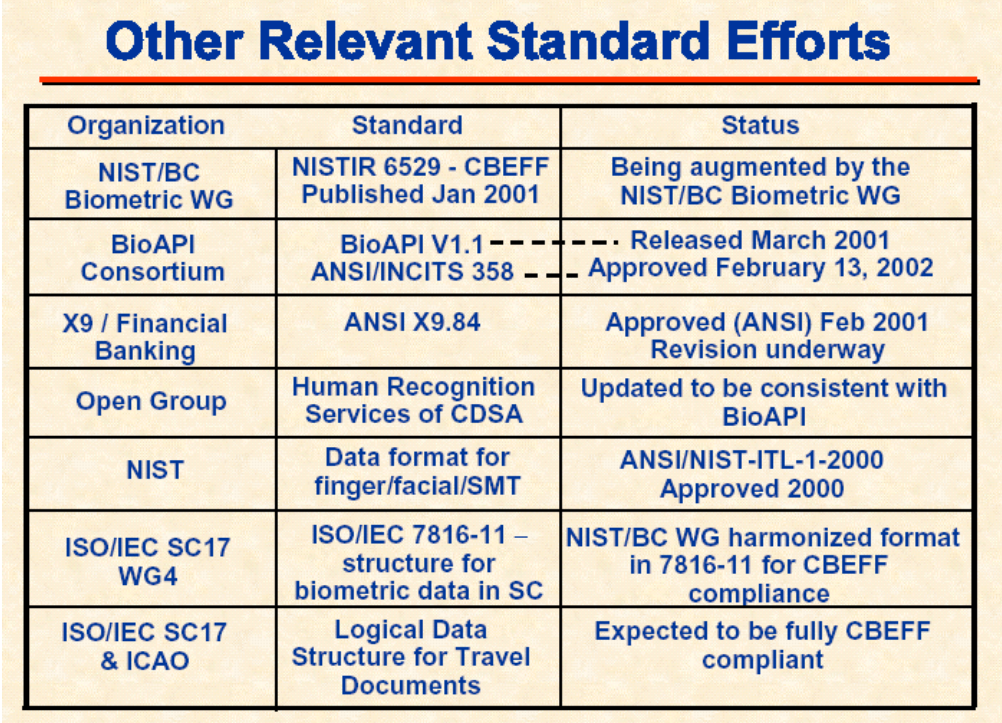

Abb. 9

Aufgrund der Ereignisse vom 11. September 2001 wurden in den USA u.a. folgende Gesetzte erlassen:

- Public Law 107-71 – “Aviation and Transportation Security”
- Public Law 107-56 – “The USA Patriot Act”
- Public Law 107-173 – “Border Security Act”

Das Ziel dieser Gesetze ist neben dem grundsätzlich beabsichtigten verstärkten Einsatz biometrischer Verfahren zur Terrorismus- und Kriminalitätsbekämpfung, die durch die bisherigen Konsortien erarbeiteten Standards zu international anerkannten Standards zu führen.

3. SC37

Aufgrund dieser Gesetze wurde der dringende internationale Standardisierungsbedarf erkannt: Insbesondere die Homeland Security betreibt ihre Aktivitäten mit einer internationalen Blickrichtung. Im Juni 2002 wurde das neue Steering Committee SC37 für Biometrik gegründet. Gleichzeitig wurde die Abgrenzung zu den bestehenden Gruppen SC17 (Cards and personal identification und SC27 (IT-Security Techniques) getroffen. Mittlerweile hat die SC37 zweimal getagt.

Das DIN (Deutsche Institut für Normung) als nationales deutsches Normungsgremium erstellt keine nationalen Normen für Biometrie mehr, sondern erarbeitet im Internationalen Kontext Normen innerhalb der ISO (International Standards Organisation), zu der mittlerweile 125 Mit-

gliedsländer gehören. Das DIN bildet seine Mitarbeit über sog. nationale Spiegelgremien ab. Das nationale Spiegelgremium der SC37 ist die NI37, die am 20.3.2003 gegründet wurde und auf der letzten SC 37Tagung vertreten war.

Das SC37 hat 6 Special Groups etabliert:

1. **Harmonized Biometric Vocabulary and Definitions** zur Vereinheitlichung der verwendeten Termini.

2. **Biometric Technical** Interfaces zur Standardisierung der Schnittstellen und Interaktionen zwischen biometrischen Komponenten und Sub-Systemen. Außerdem werden hier Sicherheitsmechanismen zum Schutz von gespeicherten Daten und Datentransfers, wie auch Referenzmodelle für die Architektur für Multi-Vendor-Systeme und deren Anwendungen bearbeitet.

3. **Biometric Data Interchange Formats** zur Normierung bezüglich Inhalt und Bedeutung biometrischer Daten für spezifische biometrische Verfahren.

4. **Profiles for Biometric Applications** für die Normierung von Anwendungsprofilen.

5. **Biometric Testing and Reporting** normiert die Testverfahren und das Reporting dieser Tests für die jeweiligen biometrischen Methoden. Die Sicherheitstechnische Bewertung dieser Ergebnisse verbleibt bei der SC27.

6. **Cross-Jurisdictional and Social Aspects** zur Bewertung der nominierten Verfahren bezüglich der rechtlichen und sozialen Aspekte. Dies kann Verfahrensanweisungen für den Einsatz von technischen Maßnahmen zur Erhöhung des Datenschutzes und der Benutzerfreundlichkeit beinhalten.

An folgenden Themen wird zur Zeit im SC37 und dessen Special Groups sowie den nationalen Spiegelgremien gearbeitet:

- Anwendungsprofil Verifikation und Identifikation von Mitarbeitern im Transportwesen
- Anwendungsprofil Personenidentifikation für den Grenzübergang
- Anwendungsprofil biometrische Verifikation im POS System (Point of Sale)
- Datenaustauschformat für Fingermuster
- Datenaustauschformat für Fingerminutien
- Datenaustauschformat für Gesichtserkennung
- Datenaustauschformat für Fingerbild
- Datenaustauschformat für Iris-Erkennung
- Datenaustauschformat für Sprach-Erkennung/ Verifizierung
- Harmonisierung des Vokabulars

4. ICAO

Die International Civil Aviation Organization (ICAO) ist eine heute unter das Dach der Vereinten Nationen eingegliederte Staatenorganisation zur Sicherung der internationalen Zusammenarbeit und zur Schaffung von Regulierungen, Standards und Prozeduren in der Zivilen Luftfahrt In der ICAO sind die Regierungen der Mitgliedsländer vertreten. Die Zusammenarbeit zwischen ISO und ICAO begann in den 90-er Jahren. Die ICAO übergibt ihren Normierungsvorschlag als Associated Body dem SC37 zur Normierung.

Gesichtserkennung ist die von der ICAO und ISO privilegierte Technologie zur Bekämpfung von Terrorismus. ICAO hat Ende Mai 2003 bekanntgegeben, daß bevorzugt die Merkmale des Gesichts in Reisedokumente aufgenommen und zur Erkennung herangezogen werden sollen. Von den Regierungen hat die der USA die Empfehlung bereits in entsprechende Gesetze und Richtlinien umgesetzt; innerhalb der EU ist die Positionierung der Regierungen der Mitgliedstaaten zu dieser Frage noch nicht abgeschlossen. Die EU-Kommission ihrerseits hat aber bereits empfohlen, ICAO zu folgen. Bezüglich der Sicherheit an Flughäfen und im Luftverkehr ist den Empfehlungen der ICAO besondere Beachtung zu schenken.