Einführung, Nutzen und Gefahren durch Funkchips

Michael Ring, Peter Ungvári

1 Einleitung

Der Austausch von Informationen gehört für jeden Menschen zum Alltag. Ob ein Bestellschein ausgefüllt wird oder auf einem Flughafen der Pass eines Menschen kontrolliert, es werden dabei immer Informationen über Menschen, Waren oder Prozesse ausgetauscht.

Mit der zunehmenden Globalisierung und dem damit verbundenen internationalen Personen- und Güterverkehr wird es erforderlich, Informationen, insbesondere auch über Menschen, über Landesgrenzen hinweg, zugänglich und austauschbar zu machen.

Die Lösung dieser Problematik erfordert dabei den Einsatz moderner und leistungsfähiger Technologien. Es muss einerseits der Zugang zu den Datensätzen als solches ermöglicht werden. Dies wird in vielen Fällen über das bereits bestehende Internet realisiert. Andererseits muss die Zuordnung des Menschen oder auch eines Transportgutes zu dem entsprechenden Datensatz erfolgen, was speziell im Bereich Datenschutz und Datensicherheit eine Vielzahl von Konsequenzen nach sich zieht. Die Zuordnung der Daten muss somit fälschungssicher und trotzdem für den Menschen zumutbar realisiert werden.

RFID ist ein Mittel, um die Identifikation von Menschen und Gütern zu ermöglichen, welches die Eigenschaft besitzt kontaktlos zu arbeiten. Es ist somit möglich, ohne eine feste Verbindung zum Informationssystem Daten und Identifikationsschlüssel zu übertragen.

Mit dieser Ausarbeitung sollen die Möglichkeiten und die Funktionsweise von RFID und insbesondere auch die Gefahren und Missbrauchspotentiale betrachtet werden. Es sollen dabei vor allem die für den Umgang mit personenbezogenen Daten relevanten Aspekte der RFID-Technologie untersucht und die Grundlagen der Erfassung und Auswertung biometrischer Daten erörtert werden.

Aufgrund aktueller, politischer Entwicklungen wird dabei der Schwerpunkt auf die Einführung des neuen, digitalen Reisepasses gelegt, welcher im November 2005 eingeführt werden soll. Es wird dabei auf die Umsetzung der technischen Problemstellungen, die Art der gespeicherten Daten und die Probleme beim internationalen Austausch dieser Daten, speziell im Bereich des Flugverkehrs eingegangen.

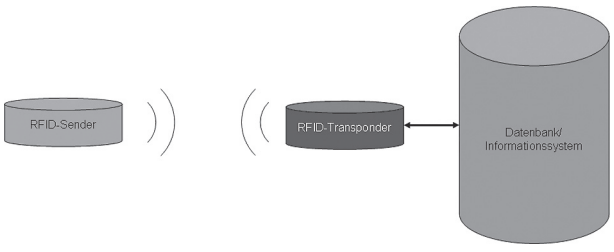

Abb. 1: RFID-Komponenten

Da mit Einführung einer neuen Technologie durch alle Bevölkerungsschichten hindurch auch gesellschaftliche Probleme und Folgen entstehen können, wird abschließend die Akzeptanz der Technologie als solches und des digitalen Reisepasses in Form einer Umfrage untersucht und ausgewertet.

2 Grundlagen

2.1 Grundlagen RFID

RFID steht für „Radio Frequency Identification“ und ermöglicht, wie bereits der Name beschreibt, die Identifikation auf Basis von Funksignalen. Die Umsetzung einer RFID-Infrastruktur erfordert im Wesentlichen drei Arten von Komponenten:

- RFID-Sender
- RFID-Transponder
- Datenbank bzw. Informationssystem.

Der RFID-Sender ist dabei eine Sende- und Empfangsstation, welche in der Lage ist mit RFID-Transpondern in der näheren Umgebung zu kommunizieren und Informationen über die identifizierten Transponder mittels eines Netzwerkes an ein Informationssystem, welches über eine Datenbank verfügt, weiterzuleiten. Das Informationssystem ist dabei üblicherweise in Form einer Client-/ Server-Architektur realisiert.

Die RFID-Transponder bestehen aus wenigen Schaltkreisen, welche ausschließlich auf bestimmte Funk-Frequenzen reagieren. Passive RFID-Transponder benötigen keine eigene Stromversorgung, wie z. B. eine Batterie, wodurch sie über eine sehr hohe Lebensdauer verfügen. Die Distanz zum Auslesen des Transponders ist von den eingesetzten RFID-Sendern und deren Montage abhängig und liegt dabei zwischen wenigen Zentimetern und maximal zwei Metern.

Auf dem RFID-Transponder kann dabei nur eine begrenzte Anzahl von Informationen gespeichert werden, wodurch zwei gängige Verfahren zur Speicherung von Daten möglich sind:

- Speicherung aller Informationen auf dem Transponder
- Speicherung eines Identifikationsschlüssels auf dem Transponder

Die Möglichkeit alle Informationen auf dem Transponder zu speichern ist ausschließlich in solchen Fälle sinnvoll, wo es nur eine beschränkte Menge an Informationen gibt bzw. der Zugang zu einer Datenbank, aufgrund der Art der Anwendung, nicht uneingeschränkt möglich ist.

Die Möglichkeit ausschließlich einen Identifikationsschlüssel auf dem Transponder zu speichern bietet sich vor allen Dingen dann an, wenn die Menge der Informationen den Speicherplatz des Transponders übersteigt und darüber hinaus der Zugang zu einer Datenbank, in welcher die entsprechenden Informationen abgelegt sind, dauerhaft möglich ist.

Beide Lösungen bieten dabei verschiedene Vor- und Nachteile, welche je nach dem zu lösenden Problem sorgfältig gegeneinander abgewägt werden müssen.

Es sind darüber hinaus auch Mischformen beider Anwendungsmöglichkeiten realisierbar, bei welchen eine Auswahl von relevanten Daten direkt auf dem Transponder gespeichert ist und zusätzlich weitere Informationen mittels eines gespeicherten Schlüssels aus einer Datenbank geladen werden können.
Die Möglichkeiten die RFID-Technologie anzugreifen lassen sich im Wesentlichen in zwei Bereiche unterteilen. Einerseits besteht die Gefahr, dass der RFID-Transponder durch Unberechtigte ausgelesen und die enthaltenen Daten gespeichert werden. Andererseits können Gefahren auch dadurch entstehen, dass der Zugang zum Informationssystem bzw. dessen Datenbank, mittels welcher die Verknüpfung von Identifikationsschlüsseln und Daten möglich ist, nicht ausreichend reglementiert oder geschützt ist. Es ist so unter Anderem möglich die Kommunikation zwischen Sendern und Transpondern mitzuhören und die übermittelten Daten zu speichern. Um diese sehr einfach zu realisierenden Angriffe zu unterbinden und so das Mitlesen sensibler Daten zu erschweren kommen bei personenbezogenen Anwendungen häufig moderne Verschlüsselungsverfahren zum Einsatz.

2.2 Anwendungsgebiete

RFID kommt in verschiedenen Anwendungsgebieten zum Einsatz. Ziel ist dabei immer die Identifikation, die Ortung sowie das sog. „Tracing“, also die Verfolgung eines Objektes oder einer Person. Der Hauptnutzen der Technologie entstand dabei im Bereich der Logistik und des Transportwesens. Mittels RFID ist es möglich z. B. einen Güter-Container mit einer eindeutigen Kennung zu versehen, und diesen an den einzelnen Punkten des Transportweges zu identifizieren und in einer Datenbank zu registrieren. Für den Transportunternehmer sowie dessen Kunden ist es somit möglich, jederzeit den aktuellen Standort des Containers bis auf die genaue Position innerhalb eines Containerlagers zu bestimmen.

Die erzeugten Daten dienen neben dem Abfragen des aktuellen Standortes des Containers auch zur Analyse des Transportweges und im größeren Umfang auch von Transportflüssen und ganzen Logistikketten. Logistikunternehmen erhalten somit wertvolle Informationen, welche unmittelbar in die zeitliche und finanzielle Optimierung von Prozessen einfließen können.

Auch in anderen Anwendungsgebieten hat sich RFID etabliert. Bereits heute basieren viele der eingesetzten Mechanismen zur Diebstahlerkennung auf Basis der RFID-Technologie. Es kann z. B. mittels RFID festgestellt werden, dass ein Produkt, welches nicht bezahlt wurde, aus dem Geschäft entfernt wird. In Zukunft kann dieser Mechanismus z. B. auch für das Bezahlen von Waren genutzt werden. Wenn der Kunde und die Ware bekannt und beim Geschäft registriert sind, könnte das Bezahlen eines Produktes einfach durch das Verlassen des Geschäftes realisiert werden, da der entsprechende Produktwert unmittelbar vom Konto des identifizierten Kunden abgebucht werden kann. Große Handelsketten wie z. B. die METRO oder Tengelmann forschen auf diesem Anwendungsgebiet.

Die am Beispiel von Waren oder Containern dargestellten Anwendungen lassen sich dabei auch sehr leicht auf den Menschen übertragen. Es wäre somit möglich z. B. die Reiseroute eines Menschen ähnlich der Route eines Containers zu verfolgen, da z. B. an jedem besuchten Flughafen ein Datensatz mit Zeit, Ort und ggf. sogar dem Reiseziel der betreffenden Person erzeugt und zentral gespeichert werden kann und ggf. ein automatischer Alarm ausgelöst wird, wenn eine Person z. B. nicht zur Aus- oder Einreise berechtigt ist.

Die Problematik liegt dabei neben der Identifikation des gespeicherten Schlüssels und der Ermittlung der zum Schlüssel passenden Informationen auch darin, die Zugehörigkeit vom Identifikationsschlüssel und der betreffenden Person einwandfrei feststellen zu können. Es werden für personenbezogene Anwendungen somit Daten benötigt, welche anhand der individuellen Merkmale einer Person eine eindeutige Identifikation ermöglichen. Daten mit diesen Eigenschaften werden als biometrische Daten bezeichnet.

3 Der digitale Reisepass

Am 1. November des Jahres 2005 wird der neue digitale Reispass in Deutschland eingeführt. Dieser soll mit 59 € rund doppelt soviel wie der „klassische“ Reisepass kosten. Anhand gespeicherter biometrischer Daten soll zum einen die Verbindung zwischen der Person und deren Reispass verstärkt werden und zum anderen soll auf diesem Wege die Fälschungssicherheit erhöht werden. Als Kerntechnologie kommt dabei RFID zur Datenspeicherung und Kommunikation zum Einsatz. Im Folgenden wird erläutert was biometrische Daten sind, wie diese erhoben werden und welche Probleme mit der Entwicklung und Einführung des neuen digitalen Reispass entstanden sind bzw. noch entstehen können.

Mit der Einführung des neuen Reisepasses im Jahr 2005 wird dabei ausschließlich das Gesichtsbild als Identifikationsmerkmal verwendet. Erst im Jahr 2007 soll neben dem Gesichtsbild auch der Fingerabdruck als Pflichtmerkmal ergänzt werden.

3.1 Biometrische Daten

Noch vor wenigen Jahren schien die Biometrie ein Wesen der Zukunft zu sein. Menschen wurden höchsten in Science-Fiction-Romanen mit dieser Materie und deren Anwendungsgebieten konfrontiert. Doch was damals noch futuristisch schien, ist heute bereits Realität und wird ab dem 1. November diesen Jahres mit der Einführung des neuen digitalen Reisepasses für Jedermann zum Alltag.

Auch wenn es so scheint als sei die Biometrie eine Wissenschaft des 20. Jahrhundertes, muss gesagt werden, dass die Ursprünge dieser scheinbar neuen Wissenschaft bis in das Jahr 1500 v. Chr. zurückreichen. In dieser Zeit zeichneten bereits die Babylonier ihre Handelsverträge mit dem eigenen Fingerabdruck ab. In China und Japan wurden Fingerabdrücke bereits zwischen 600 und 900 n. Chr., ebenfalls als Stempel und Siegel, eingeführt. Darüber hinaus wurde in China erstmals den Fingerabdruck als Beweismaterial in Strafprozessen eingesetzt. Leonardo Da

Vinci setzte sich als erster im 15. Jahrhundert wissenschaftlich mit der Vermessung menschlicher Körperteile auseinander. Seine Ergebnisse sind bis heute eine wesentliche Grundlage für Forschungen auf dem Gebiet der Biometrie. Einen weiteren Meilenstein setzte Marcello Malphigi, ein bedeutender Wissenschaftler an der Universität von Bologna. Dieser erforschte im 17. Jahrhundert die Poren der menschlichen Haut und stieß als erster auf das sog. Papillarlinienmuster auf den menschlichen Fingerkuppen (vgl. Abb. 2). Darauf aufbauend formulierte der englische Wissenschaftler Francis Galton im 19. Jahrhundert Aussagen über die Individualität des Fingerabdrucks. Trotz der langen Geschichte steht die Biometrie heute noch am Anfang ihrer Entwicklung.

Abb. 2: Papillarlinienmuster

In der heutigen Zeit wird die Biometrie wie folgt definiert: „Biometrie ist die Technik der Erkennung von Personen anhand persönlicher Charakteristika, z. B. Gesicht und Fingerabdruck." [5]. Die am bekanntesten und geläufigsten biometrischen Daten sind

– der „klassische " Fingerabdruck und
– der genetische Fingerabdruck.

Der genetische Fingerabdruck wird heute erfolgreich in der Verbrechensbekämpfung und -aufklärung angewandt. Trotz großer und zahlreicher Erfolge in der Verbrechensaufklärung ist diese Methode heute noch umstritten und deren Einsatz nach wie vor sehr kostenintensiv. Der genetische Fingerabdruck wird als biometrisches Merkmal in dieser Ausarbeitung deshalb nicht weiter betrachtet.

Das wohl am bekannteste und älteste biometrische Merkmal ist der Fingerabdruck. Dieser wird ebenfalls unter anderem in der Verbrechensaufklärung, zur Überführung von Straftätern angewandt. Die Bestimmung bzw. Ermittlung des Fingerabdrucks erfolgt nach einem alten Verfahren, welches auch schon Francic Galton für seine Forschungen angewandt hat. Im Gegensatz zur damaligen Zeit erfolgt die Erfassung heute automatisiert mit Hilfe von Scannern und Computern. Dabei werden aus dem Fingerabdruck mittels einer Software eindeutige Merkmale extrahiert. Dies sind zum einen Verzweigungen und zum anderen das Ende, welche die Papillarlinien beschreiben. Diese Merkmale bezeichnete Galton als Minutien (lateinisch: Kleinigkeit). Die heutigen automatisierten Verfahren nutzen zu 80 % die Minutien zur Erfassung des Fingerabdrucks. Die restlichen 20 % nutzen unter anderem die Lage und Richtung der Hauptlinien.

Obwohl nahezu alle Systeme identische Verfahren anwenden, existieren heute eine Vielzahl an Techniken zur Erkennung der Merkmale. Man unterscheidet hier zwischen kontaktfreien und kontaktbehafteten Systemen. Die kontaktfreien Sensoren haben den Vorteil, wie die Bezeichnung schon andeutet, dass der Finger nicht auf den Sensor gelegt werden muss. Dies hat den Vorteil, dass der Sensor wesentlich langsamer verdreckt und somit auch hygienische Aspekte gewährleistet sind.

Bei der kontaktfreien Methode werden heute hoch auflösende Kameras und Ultraschall-Sensoren verwendet. Diese sind jedoch sehr teuer, so dass heute vor allem kontaktbehaftete Sensoren Anwendung finden. Diese sind darüber hinaus billiger und kompakter als kontaktfreie Sensoren und eignen sich somit besser für Massenanwendungen. Dabei werden heute sowohl Silizium- als auch Druck-Sensoren angewandt. Wie die vier erwähnten Technologien den Fingerabdruck im Einzelnen scannen, kann Tabelle 1 entnommen werden.

hoch auflösende Kameras	Eine Ausnahme bezüglich der Größe ist die CCD-Kamera. Dieses System funktioniert relativ einfach. Ein Prisma wird von einer Seite bestrahlt und von einer anderen Seite zeichnet eine Kamera die Reflexion der Lichtstahlen auf, die entstehen wenn auf der dritten Seite ein Finger aufgelegt wird.
Ultraschall-Sensoren	Eine weitere Möglichkeit ist die Abtastung des Rillenprofils mittels Ultraschall. Ultraschallwellen tasten den Finger nach Höhen und Tiefen ab und können somit den Fingerabdruck rekonstruieren.
Silizium-Sensor	Ein Siliziumkern misst die elektrische Aufladung zwischen den Papilliarlinien und erstellt so ein 8-bit Graustufenbild.
Druck-Sensoren	Auf der Chipoberfläche befinden sich winzige Widerstandssensoren. Wenn ein Finger auf den Drucksensor gelegt wird, ändert sich der Widerstand an den Stellen, an denen die Papilliarlinien auf dem Sensor aufliegen. Diese Sensoren sind nur wenige Millimeter dick und eignen sich dadurch für den Massenmarkt.

Tab. 1: Technologien zur digitalen Erfassung des Fingerabdrucks

Ein weiteres biometrisches Merkmal ist das menschliche Gesicht. Im Gegensatz zur Fingerabdruckerkennung ist die Gesichtserkennung eine sehr junge Wissenschaft und kaum älter als 10 Jahre. Das US-amerikanische Verteidigungsministerium („DoD" – Department of Defense) legte in den 90iger Jahren mit dem „Face Recognition Program" (FERET) die ersten Grundlagen und testete bereits erste automatisierte Systeme. Nach der Jahrtausendwende erfolgte eine Neuauflage und Erweiterung der Tests unter dem Namen „Facial Recognition Vendor Test". In Deutschland beschäftigt sich seit dem Jahre 2002 das „Bundesamt für Sicherheit in der Informationstechnik" (BSI) mit der Untersuchung von Algorithmen zur Gesichtserkennung.

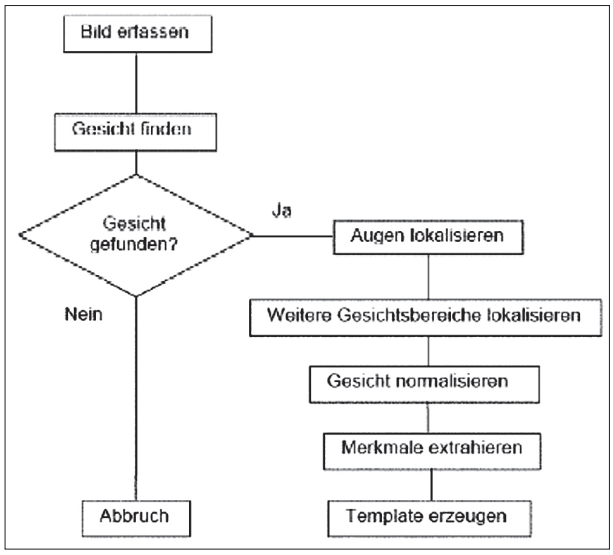

Abb. 3: Vorgehensweise bei der Template-Erzeugung

Man unterteilt den Prozess der Gesichtserkennung dabei in drei wesentliche Arbeitsschritte:
– Template erzeugen,
– Referenzdatensatz erzeugen und
– Gesichtsbilder vergleichen.

Um den Vergleich zweier Gesichtsbilder schneller und einfacher zu gestalten werden zunächst die Merkmale des Gesichts erfasst und in einem Merkmalsdatensatz, dem sog. Template gespeichert (vgl. Abb. 3). Es werden in erster Linie solche Merkmale erfasst, welche sich nur schwer durch Mimik verändern lassen, zum Beispiel die obere Kante der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes.

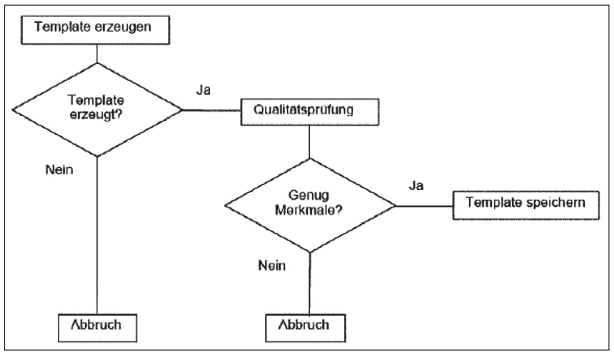

Abb. 4: Vorgehensweise bei der Referenzdaten-Erzeugung

Im nächsten Arbeitsschritt werden Referenzdaten erzeugt (vgl. Abb. 4). Diese werden dann zur Identifikation von Personen angewandt. Die Referenzdatenbank entsteht durch das Einspeichern von Gesichtsbildern. Dabei werden die bereits erfassten Merkmale der Templates mit den neuen Bildern verglichen und ggf. um weitere Merkmale ergänzt bzw. verfeinert. Um veränderte Kopfhaltungen oder auch Mundöffnungen berücksichtigen zu können, werden zur Erstellung des Referenz-Templates auch mehrere Gesichtsbilder aus zum Beispiel Videosequenzen genutzt. Die Referenzdaten-Erzeugung verfeinert die zuvor erzeugten Templates.

Im letzten Schritt, dem Vergleich der Gesichtsbilder, werden die gespeicherten Bilder bzw. Gesichtsmerkmale mit Hilfe komplexer mathematischer Algorithmen kombiniert und verglichen. Im Ergebnis erhält man den Grad der Ähnlichkeit mit dem gespeicherten Template bzw. Referenzdatensatzes.

offen	Dieses Merkmal kann ohne weitere Hilfsmittel beobachtet werden. (z. B. Gesicht)
leicht verdeckt	Ein Nebenstehender kann dieses Merkmal beobachten (z. B. Fingerabdruck)
verdeckt	Dieses Merkmal kann nur mit Hilfe eines bestimmten Detektors erfasst werden. (z. B. Retina-Muster)
diskret/ schwer verdeckt	Das Merkmal ist nicht direkt beobachtbar, sondern das Ergebnis, welches eine (geheime) Funktion aus dem Personenverhalten analysiert. Das Abhören von Messdaten bringt keine auswertbare Information.

Tab. 2: Verfahren zum Vergleich von Gesichtsmerkmalen

Im Bereich der Gesichtserkennung werden heute neben dem beschriebenen Prinzip auch noch weitere Verfahren angewandt:

Neben den erwähnten biometrischen Merkmalen/Verfahren existieren auch weitere, wie
– Iriserkennung,
– Stimmerkennung und
– Handgeometrie.

Weiterführend werden nur die ausführlich beschriebenen Merkmale Fingerbadruck und Gesicht betrachtet, da diese als neues Merkmal digital im neuen Reisepass gespeichert werden. Die Entscheidung seitens der Europäischen Union für das Gesicht als primäres Identifikationsmerkmal beruht auf eine Empfehlung der UN-Zivilluftfahrt-Organisation (International Civil Aviation Organization – ICAO). Der Fingerabdruck wurde als eine Art „Ersatzmerkmal" zusätzlich mit aufgenommen, da dieser sich durch eine hohe Praxistauglichkeit auszeichnet. Des Weiteren soll der Fingerabdruck die Flexibilität bei den Kontrollen erhöhen. An Stellen, an denen die Gesichtserkennung aufgrund schlechter Beleuchtungsverhältnisse oder bei einem eventuellen Massenandrang nicht möglich ist, soll dennoch eine Identifikation möglich sein.

3.2 Anwendungsgebiete Biometrie

Wie bereits festgestellt wurde, werden biometrische Merkmale ab November dieses Jahres digital auf RFID-Funkchips im neuen Reisepass gespeichert. Das tatsächliche Anwendungsgebiet der Biometrie ist allerdings wesentlich größer. Zum einen findet diese Wissenschaft Anwendung, um wichtige Dokumente (zum Beispiel den Reispass) fälschungssicherer zu gestalten. Zum anderen werden biometrische Daten hauptsächlich dort angewandt, wo die Identität eines Menschen eine eminent wichtige Rolle spielt und verlässlich und schnell ermittelt werden muss. Heutige Anwendungen sind
– Sicherung von Computern und Daten (Samsung führte als erster Notebook-Hersteller die User-Authentifizierung über einen Fingerabdruck ein.)
– Zugangskontrollen (Das Militär setzte mit als erstes die Personenidentifikation anhand biometrischer Merkmale zur Zugangskontrolle an Hochsicherheitsgebäuden ein.)
– Auszahlung von Sozialgeldern (Das erste Land, welches biometrische Daten, den Fingerabdruck, zur Überprüfung der rechtmäßigen Auszahlung von Sozialgeldern einführte, war Südafrika. Ausschlaggebend hierbei war der hohe Anteil an Analphabeten in der Bevölkerung. Ähnliche Systeme bzw. Verfahren befinden sich in Kolumbien und Spanien in der Einführung und nutzen ebenso den Fingerabdruck.)
– Arbeitszeiterfassung (Eine Supermarktkette mit 450 Supermärkten erfasst die Arbeitszeiten des Personals anhand der Identifikation über den Fingerabdruck. Der anfängliche Widerstand des Personals konnte aufgrund einer Datenschutzüberprüfung überbrückt werden.)

Das wohl bekannteste und aktuellste Anwendungsbeispiel für biometrische Merkmale ist, wie bereits mehrfach erwähnt, der neue digitale Reispass. Mittels der neuen Daten sollen Personen besser, schneller und vor allen Dingen sicherer Identifiziert werden können. Des Weiteren wird so eine Verbesserung der Fälschungssicherheit erzielt. Für die Identifizierung existieren zwei Systeme:

– AFIS (Automatisches Fingerabdruck Identifizierungssystem)
– AFAS (Automatisches Fingerabdruck Authentifizierungssystem)

Beim AFIS wird der Fingerabdruck gescannt und anhand einer Datenbank identifiziert. Dabei wird der Fingerabdruck mit allen in der Datenbank gespeicherten Abdrücken verglichen. Das Ergebnis ist eine Liste mit allen möglichen Treffern, welche sortiert nach der Trefferwahrscheinlichkeit ausgegeben wird.

AFAS wird zur Identifizierung über den Fingerabdruck beim neuen Reispass angewandt. Zusätzlich zum gescannten Fingerabdruck fordert das System eine Identität an. Diese Identität bzw. deren Identifikationsschlüssel liefert der Reispass bzw. dessen RFID-Chip. Das System vergleicht dann den zur ermittelten Identität gespeicherten Fingerabdruck in der Datenbank mit dem gescannten Abdruck.

3.3 Gefahrenpotentiale

Alle vorgestellten Verfahren ähneln sich dadurch, dass die biometrischen Merkmale in Merkmalsvektoren abgespeichert werden. Beim digitalen Reisepass kommt dabei der Merkmalsvektor des Referenzmusters, der von Benutzern bei der Registrierung bzw. den Ämtern erstellt wird (Enrollment-Prozess) zum Einsatz. Dieser wird in einer Datenbank und dem Reisepass abgespeichert und dient dem Vergleich mit Testmustern. Testmuster werden bei jeder Authentifizierung der Person erstellt. Aus verfahrensabhängigen Gründen kommt es meist aber zu kleinen Ungenauigkeiten bei der Erstellung, so dass die Merkmalsvektoren trotz identischer Quelle, dem Inhaber des Reisepasses, nicht vollständig identisch sind. Deshalb wird beim Vergleich des Referenzmusters mit dem Testmuster der genaue Unterschied mit Hilfe von Abstandsmetriken (z. B. Hamming-Distanz oder Euklidische Distanz) ermittelt. Wird ein vordefinierter Schwellwert nicht überschritten, so gelten die Muster als identisch. Die Festsetzung des Schwellwertes beeinflusst die „false accept rate“[1] und die „false reject rate“[2]. Man kann dabei sagen, dass je höher der Schwellwert gewählt wurde, das System umso sicherer ist.

Angriffe auf RFID-Systeme und Gegenmaßnahmen

Angriff	Kosten	Gegenmaßnahmen	Kosten
Abhören der Kommunikation zwischen Tag und Lesegerät	hoch	Verlagerung ins Backend,Abschirmung, Verschlüsselung	mittel
Unauthorisiertes Auslesen der Daten	mittel bis hoch	Detektoren, Authentifizierung	mittel
Unauthorisiertes Verändern der Daten	mittel bis hoch	Read-only-Tags, Detektoren, Authentifizierung	gering bis mittel
Cloning und Emulation	mittel	Erkennung von Duplikaten, Authentifizierung	mittel
Ablösen des Tags vom Trägerobjekt	gering	Mechanische Verbindung, Alarmfunktion (aktive Tags), Zusatzmerkmale	gering bis mittel
Mechanische oder chemische Zerstörung	gering	Mechanische Verbindung	gering bis mittel
Zerstörung durch Fremdeinwirkung	mittel	selbst heilende Sicherung (nur begrenzt wirksam)	in Serie gering
Zerstörung durch Missbrauch eines Kill-Befehls	mittel	Authentifizierung	mittel
Entladen der Batterie (nur aktive Tags)	mittel	Schlafmodus	in Serie gering
Blocker-Tag	gering	Verbot in AGB (nur begrenzt wirksam)	gering
Störsender	mittel bis hoch	Messungen, Frequenzsprungverfahren	mittel bis hoch
Feldauslöschung	gering (jedoch schwierig)	keine	-
Feldverstimmung	sehr gering	aktive Frequenznachführung	mittel bis hoch
Abschirmung	sehr gering	verbesserte Lesestation (nur begrenzt wirksam)	mittel

Abb. 5: Angriffe auf RFID [7]

Biometrische Daten lassen sich somit durch direkte Täuschung des Systems adaptieren. Täuschung heißt, dass ein echtes biometrisches Merkmal durch ein Imitat ersetzt wird. Der Fingerabdruck kann so zum Beispiel durch künstliche Finger aus Wachs oder Silikon nachempfunden werden. Auch einer eventuellen Lebendprüfung kann mittels eines nachempfundenen Pulsierens widerstanden werden. Auch ein Gesicht ließe sich mit Wachs und Silikon adaptieren. Die Iris, auch wenn sie als Merkmal beim digitalen Reisepass nicht zum Einsatz kommt, könnte in diesem Szenario anhand einer Kontaktlinse nachempfunden werden. Generell kann eine Fälschung von biometrischen Merkmalen nur mit sehr hohem und kostenintensivem Aufwand betrieben werden.

Ein weiteres Angriffsszenario ist der so genannte Akquisitionsangriff. Hier wird versucht biometrische Daten anderer Personen zu erlangen. Mit welchem Erfolg ein solcher Angriff durchgeführt werden kann, ist abhängig vom biometrischen Merkmal selbst. So kann ein Fingerabdruck vergleichsweise Einfach erfasst werden, da dieser von Jedermann unfreiwillig an jedem berührten Gegenstand hinterlassen wird. Dieser ist somit passiv erfassbar. Eine Einstufung aller biometrischen Merkmale kann Tab. 3 entnommen werden.

Elastische Graphen	Es werden markante Stellen (sog. Knoten) im Gesicht gesucht und untereinander verbunden. Das entstehende Gitter wird mit dem Gitter eines normierten Referenzbildes verglichen, dabei wird versucht mit Drehung, Streckung und Stauchung die Bilder aufeinander abzubilden. Die verbleibenden Unterschiede ergeben das Maß für die Ähnlichkeit.
Geometrische Merkmale	Dieses Verfahren ähnelt dem der elastischen Graphen. Dabei bilden die relativen Positionen zueinander einen Vektor. Der Abstand zwischen diesem Vektor zu dem des Referenzbildes ergibt die Ähnlichkeit der Bilder.
Eigenfaces	Grundlage für dieses Verfahren ist eine Sammlung von Basisbildern des Gesichts. Diese werden so kombiniert, dass sie mit dem zu vergleichenden Bild so ähnlich wie möglich sind.

Tab. 3: biometrische Merkmale – Einstufung [1]

Biometrische Daten lassen sich nicht nur über einen Aquisitionsangriff erfassen und daraufhin digitalisieren, sondern unter Umständen auch direkt vom RFID-Chip ausspähen. Dies ist zum einen davon abhängig, ob die Chips die Daten von sich aus, ohne Überprüfung bzw. Authentifizierung des Anfragers preisgeben, und zum anderen ist das Ausspähen von Daten davon abhängig, ob biometrische Daten direkt auf dem Chip gespeichert werden, oder ob lediglich eine ID gespeichert ist, welche einen Datensatz in einer zentralen Datenbank referenziert. Beim digitalen Reisepass werden beide Varianten miteinander kombiniert eingesetzt. Im letzteren Fall wäre das Angriffsziel nicht der Chip selbst, sondern die Datenbank. Eine weitere Alternative im Ausspähen von biometrischen Daten ist das Mithören der Kommunikation zwischen Sender und Transponder. Hier können Angreifer den Datenaustausch mithören, wenn dieser nicht verschlüsselt erfolgt. Hier ist die Sicherheit zusätzlich von der kryptographischen Qualität der Verschlüsselung abhängig.

Grundsätzlich ist das Ausspähen von biometrischen Daten, sowohl beim direkten Datenabruf vom Chip, als auch beim Abhören der Kommunikation, abhängig von der Signalreichweite möglich. Je größer die maximale,

zum Auslesen benötigte Rechweite ist, desto unauffälliger und unbemerkt lassen sich biometrische Daten unbefugt erfassen.

Eine weitere Missbrauchsgefahr stellt die Zweckentfremdung der Daten dar. Mit Zeckentfremdung ist gemeint, dass die Daten über die Authentifizierung des „Merkmalinhabers" hinaus für einen Zweck genutzt werden, für den diese nicht erhoben wurden. Eine Möglichkeit besteht in der Verfolgungsmöglichkeit einer Person von einem entfernten zentralen Punkt aus.

Des Weiteren besteht die Gefahr, dass Daten unzulässigerweise an Dritte weitergegeben werden. Im Allgemeinen kann man sagen, dass auf die Einhaltung der datenschutzrechtlichen Bestimmungen besonders geachtet und dies überprüft werden muss.

3.4 Gegenmaßnahmen

Um Angriffe abzuwehren, welche direkt das Auslesen der Daten des RFID-Transponders zum Ziel haben, wird beim neuen digitalen Reispass ein zweistufiges Sicherheitssystem verwendet.

Mit der ersten Stufe, dem sog. „Basic Access Control", werden zunächst der Name, das Geburtsdatum, das Geschlecht sowie das Gesichtsbild des Passinhabers geschützt. Die Daten werden dabei mittels eines geheimen Schlüssels kodiert, welcher laut BSI eine Stärke von 56 Bit besitzt und somit mit gängigen DES-Schlüsseln vergleichbar ist. Der Schlüssel wird dabei mittels eines Algorithmus aus den Daten des maschinenlesbaren Teils des Reispasses erzeugt. Die Errechnung des Schlüssels erfordert somit einen direkten, optischen Zugang zum geschützten Dokument, also dem Reisepass.

Die zweite Stufe, „Extended Access Control" genannt, wird erst nach der Einführung des Fingerabdrucks als zusätzliches Merkmal verwendet. Es handelt sich dabei um einen Public-Key-Authentisierungsmechanismus sowie einer Public/Private-Key-Infrastruktur (PKI), welche es dem RFID-Chip des Reisepasses ermöglicht, die Zugriffsrechte des Lesegerätes anhand eines Zertifikates zu verifizieren. Es obliegt dabei dem Land, welches den Pass herausgegeben hat, festzulegen, welche Zertifikate benötigt werden um auf bestimmte Daten zuzugreifen. Es ist somit auch möglich ausländischen Lesegeräten nur einen beschränkten Zugriff auf die Daten zu gewähren.

Auch bei der zweiten Sicherheitsstufe soll das Auslesen der Daten aus einem geschlossenen Reispass generell unterbunden werden.

3.5 Politische und Gesellschaftliche Probleme

Die zentrale und internationale Organisation für die Verbesserung der Sicherheit von Reisedokumenten ist die ICAO (International Civil Aviation Organization). Aufgabe der ICAO ist es, Spezifikationen und Standards für Reisedokumente für eine weltweite Interoperabilität zu schaffen.

Eines der bedeutendsten Programme der ICAO ist das MRTD (Machine Readable Travel Documents). Bis 2001 beschäftigte man sich im MRTD der MRZ (Machine Readable Zone) auf Reisedokumenten. Nach den Anschlägen vom 11. September 2001 in New York wurden in den USA neue Sicherheitsgesetze verabschiedet. Ein Beschluss mit großen Auswirkungen sah die Einführung von biometrischen Merkmalen als Sicherheitsstandard von Reisedokumenten vor. Aufgrund dessen verabschiedete die ICAO im Mai 2004 den Standard bzw. die Spezifikation für die interoperable Nutzung von biometrischen Daten und deren Speicherung in der MRZ. Die wichtigsten Punkte sahen das Gesicht als zwingendes biometrische Merkmal in Reisedokumenten für alle Länder vor. Als Speicher- und Kommunikationstechnologie wurde RFID empfohlen. Ebenso wurde eine einheitliche Datenstruktur verabschiedet. Alles darüber hinausgehende, zum Beispiel die zusätzliche Speicherung des Fingerabdrucks als biometrisches Merkmal, ist optional und obliegt den nationalen Interessen des jeweiligen Landes.

Auf Basis dieser Spezifikationen verabschiedete die Europäische Union am 13. Dezember 2004 die Einführung von digitalen Reisepässen. Dieser Beschluss sah, gemäß den standardisierten Forderungen der ICAO vor, das Gesicht als biometrisches Merkmal in der ersten Stufe und RFID- als Datenhaltungs- und Kommunikationstechnologie vor. In der zweiten Stufe soll zusätzlich der Fingerabdruck als biometrisches Merkmal gespeichert werden.

Mit den internationalen Vorgaben ergaben sich die heutigen Probleme und Kritiken. Nach dem Beschluss der Einführung des Reisepasses schlugen Datenschützer in Deutschland Alarm. Man kritisierte RFID als eine zu unsichere Technologie, da unter anderem die Kommunikation nicht sicher genug gegen unbefugtes Abhören sei. Die USA erschlugen diese Kritik mit dem Argument, dass die Signalstärke lediglich ein Abhören in einem Umkreis von 10 cm zuließe. Aufgrund dieser kleinen Reichweite wurden keine datenschutzrechtlichen Maßnahmen für notwendig befunden. Nach Messungen des „National Institute of Standards and Technology" (NIST), welche die Kritiken bestätigten, und zunehmenden öffentlichem Druck, wurde das Problem jedoch anerkannt und die Verschärfung der Sicherheits- sowie Verschlüsselungsmaßnahmen vorangetrieben.

Ein zentrales Problem dabei sind internationale Differenzen in der Anwendung des Datenschutzes. Da Datenschutz-sichernde Mechanismen gemäß ICAO optional sind, entstehen Konflikte zwangsläufig dann, wenn ein Land entsprechende Funktionen implementiert, ein anderes dagegen nicht. Innerhalb Europas sollte es hier jedoch keine Probleme geben, da man sich europaweit über die notwendigen Sicherheitsaspekte und -problematiken verständigt hat. Eine langfristige, politische Lösung dieser Konflikte im internationalen Bereich steht dabei noch aus, wobei insbesondere die USA sowie der mittlere und nahe Osten im Zentrum der Diskussionen stehen.

Datenschutzrechtliche Aspekte spiegeln sich auch in gesellschaftlichen Problemen bzw. Ängsten wieder. Gemäß einer, von einer Computerzeitschrift im Jahr 2001, durchgeführten Umfrage (3676 Teilnehmer), haben über die Hälfte aller Befragten Angst vor einem unbefugten Zugriff auf die Daten und Missbrauch. Damit verbunden lehnten bereits damals 11.9 % eine Identifizierung über biometrische Daten generell ab. Mit der zunehmenden Thematisierung der mit dem neuen digitalen Reisepass verbundenen Problematiken, speziell im Bereich des Datenschutzes, ist die gesellschaftliche Skepsis dabei eher

gestiegen als gesunken. Nicht zuletzt spielt dabei auch die Politik der USA, welche sich die weltweite Bekämpfung des Terrorismus zum Ziel gesetzt hat und dabei immer wieder mit ihren, für europäische Verhältnisse, zweifelhaften Methoden in den Medien steht, eine nicht zu unterschätzende Rolle.

4 Umfrage zum Thema RFID

4.1 Voraussetzungen

Da RFID und der neue digitale Reisepass Themen sind, welche alle Altersgruppen betreffen, wurde versucht, mit der vorliegenden Umfrage auch möglichst alle Altersgruppen abzudecken. Dabei wurden 58 Personen im Alter zwischen 16 und 76 Jahren beider Geschlechter befragt.

Die Verteilung der Altersgruppen stellt sich dabei wie folgt dar:

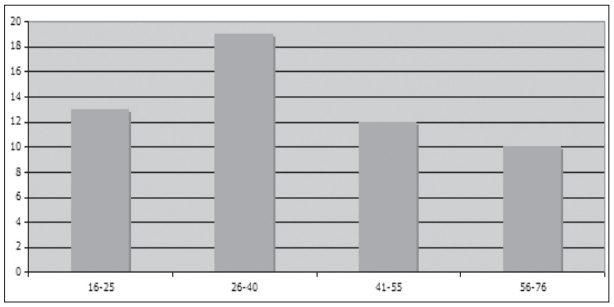

Abb. 6: Altersgruppenverteilung der Umfrage

Die Umfrage wurde dabei am frühen Nachmittag in einem gut besuchten Einkaufszentrum durchgeführt. Es wurde darüber hinaus keine Vorauswahl von Umfrageteilnehmern durchgeführt, so dass davon ausgegangen werden kann, dass Menschen verschiedener Gesinnungen und verschiedener gesellschaftlicher Schichten befragt wurden.

Es wurden jedem Teilnehmer 10 Fragen gestellt, welche im Wesentlichen in drei Bereiche unterteilt werden können:

- Basiswissen zur RFID-Technologie sowie allgemein zum Datenschutz (Fragen 1, 6, 7)
- Kenntnisse über den neuen digitalen Reisepass und dessen Anwendung (Fragen 2, 3, 4, 5)
- Meinungsfragen den digitalen Reisepass betreffend (Fragen 8, 9, 10)

Es ist allgemein anzumerken, dass die Fragen rein subjektiv beantwortet wurden. Auch wenn Teilnehmer angegeben haben, z. B. über die RFID-Technologie informiert zu sein, kann dies nicht objektiv bewertet werden.

Jeder Teilnehmer hatte dabei die Möglichkeit auf jede Frage mit den Zahlen von 1-5 zu Antworten, wobei 1 für „trifft zu“ und 5 für „trifft nicht zu“ steht.

4.2 Auswertung

Zur Interpretation der gesammelten Umfrageergebnisse werden die drei genannten Bereiche der Umfrage im Folgenden einzeln ausgewertet. Zur Interpretation der Ergebnisse werden zum Teil auch Informationen, welche aus Gesprächen mit den Teilnehmern während der Umfrage stammen, herangezogen.

4.2.1 Basiswissen zur RFID-Technologie sowie allgemein zum Datenschutz

Es wurde im Rahmen der Umfrage deutlich, dass sowohl der Begriff RFID, als auch die Kenntnis über diese Technologie (Frage 1) den wenigsten Umfrageteilnehmern bekannt waren, was aufgrund des durchschnittlichen Wertes von 3,8 deutlich wurde. Im Gegensatz dazu waren die meisten Teilnehmer der Meinung, ausreichend über die Thematik Datenschutz informiert zu sein (Frage 6/Durchschnittswert 2,2). Über die Vor- und Nachteile der RFID-Technologie im Bezug auf den Datenschutz waren die Einschätzungen des eigenen Kenntnisstandes relativ Ausgewogen (Frage 7/ Durchschnittswert 2,7). Dies war nach den Aussagen vieler Teilnehmer auch dadurch bedingt, dass das Thema wenige Tage zuvor erneut durch die Medien gegangen war und als Folge dessen, dass Otto Schilly die endgültige Einführung des digitalen Reisepasses zum 1. November 2005 bekannt gegeben hatte.

Zusammenfassend ist zu sagen, dass die Kenntnisse über die Themen RFID, Datenschutz, sowie die damit in Zusammenhang stehenden Vor- und Nachteile sich relativ ausgewogen darstellen. Dies wird anhand des Durchschnittswertes dieses Fragenkomplexes von rund 2,87 deutlich. Aufgrund der Medienpräsenz des Themas im Zeitraum der Umfrage sollte jedoch davon ausgegangen werden, dass der Wert deutlich höher hätte ausfallen müssen.

4.2.2 Kenntnisse über den neuen digitalen Reisepass und dessen Anwendung

Dieser Fragenkomplex zielte speziell darauf ab, den subjektiven Wissensstand über das Thema des digitalen Reisepasses und im Speziellen auch biometrischer Daten zu ermitteln. Die meisten Teilnehmer der Umfrage wussten worum es sich generell beim neuen digitalen Reisepass handelt (Frage 2/Durchschnittswert 2,2). Auch die Tatsache, warum der Reisepass eingeführt werden soll war im Wesentlichen bekannt (Frage 3/Durchschnittswert 2,6). Der Begriff der biometrischen Daten war mehr als der Hälfte der befragten Personen bekannt (Frage 4/Durchschnittswert 2,2). Welche biometrischen Daten gespeichert werden sollen, wussten nur etwas weniger Teilnehmer (Frage 6/Durchschnittswert 3). Auch wenn bei der direkten Nachfrage aufgefallen ist, dass nur ein geringer Anteil der befragten Teilnehmer wirklich beide Merkmale (Gesichtsbild, Fingerabdruck) benennen konnten. Der tatsächliche Wert ist somit wahrscheinlich um einiges schlechter.

Der Durchschnittswert dieses Fragenkomplexes liegt mit 2,5 über dem erwarteten Durchschnitt, obwohl wie bereits erwähnt beim direkten Nachfragen selten korrekte Antworten kamen und der Wert somit, auch in Anbetracht der Medienpräsenz des Themas, höher hätte ausfallen müssen.

4.2.3 Meinungsfragen den digitalen Reisepass betreffend

Der letzte Fragenkomplex zielte darauf ab, die Meinungen zu einzelnen Themen und weniger Wissen abzufragen. Zunächst wurde erfragt, ob der jeweilige Teilnehmer den Behörden und Ämtern im Umgang mit seinen Daten vertraut. Das Ergebnis ist mit einem Durchschnittswert von

3,7 (Frage 8) äußerst negativ ausgefallen. Die Aufklärung über das Thema digitaler Reisepass seitens der Regierung hielten die Wenigsten für ausreichend (Frage 9), was an einem vernichtenden Durchschnittswert von 4,5 deutlich wurde. Im Gespräch mit den Teilnehmern wurde klar, dass das Thema zwar in den Medien präsent war, jedoch politische und technische Begründungen und Erklärungen gänzlich vermisst wurden. Viele Teilnehmer waren dabei erstaunlicherweise der Meinung, dass die mangelhafte Informationspolitik seitens der Regierung durchaus gewollt und somit vorsätzlich war.

Abschließend wurde die Frage gestellt, ob der jeweilige Teilnehmer für oder gegen die Einführung des neuen digitalen Reisepass ist, was mit einem Durchschnittswert von 3,1 (Frage 10) zu einem ausgewogenen Ergebnis führte. Viele Teilnehmer merkten an, dass nicht zuletzt der erhöhte Preis des neuen Reisepasses gegen dessen Einführung spricht.

Dieser sehr wichtige Themenkomplex zeigte deutlich, wie viel Aufklärungs- und Überzeugungsarbeit seitens der Regierung und der Ämter noch zu leisten ist, um ein positives und weniger skeptisches Meinungsbild dem neuen Reisepass gegenüber zu erreichen.

4.3 Externe Umfragen

Im Rahmen einer Internet-Recherche wurden weitere Meinungsumfragen zum Thema des neuen Reisepasses gefunden. Dabei ist insbesondere auf eine Umfrage der Website www.neuer-reisepass.de hinzuweisen, deren Fragen bereits von über 17.000 Teilnehmern beantwortet wurden. Das Ergebnis fällt dabei deutlich negativer aus, als bei der im Rahmen dieser Ausarbeitung durchgeführten Umfrage. Rund 2/3 der Teilnehmer halten die Einführung des digitalen Reispasses für unnötig und stehen der Gesamtproblematik eher negativ gegenüber. Auch diese Umfrage kommt mit 72,1 Prozent zu dem deutlichen Ergebnis, dass die Aufklärung seitens der Regierung ungenügend ist.

5 Zusammenfassung und Schlussfolgerungen

Die Thematik des digitalen Reisepasses hat sich als sehr komplex dargestellt. Neben einer Vielzahl technischer Problemstellungen, welche zwar schon thematisiert, trotzdem jedoch noch nicht endgültig gelöst sind, sind auch politische und gesellschaftliche Aspekte durch die Thematik betroffen. Durch alle involvierten Themengebiete hindurch wird vor allem ein zwingender Bedarf deutlich, der Bedarf an Kommunikation.

Es ist dabei neben der Bildung eines internationalen Konsens, zum einheitlichen Umgang mit Identitätsdokumenten und dem Aufbau der damit verbundenen Infrastruktur zum weltweiten und sicheren Datenaustausch, vor allem die Aufklärung der eigenen Bevölkerung erforderlich.

Der digitale Reisepass ist ein Schritt in Richtung mehr Sicherheit im internationalen Personenverkehr. Man muss jedoch auch die richtigen Akzente im Bezug auf den internationalen Datenschutz setzen, einer Thematik, welcher mit dem Fortschreiten der Globalisierung und des weltweiten Informationsaustausches ein nicht zu unterschätzender Stellenwert zukommt.

Zusammenfassend ist zu sagen, dass Entwicklungen, welche jeden einzelnen Menschen betreffen, und dazu zählt der neue Reisepass unumstritten, grundsätzlich ein hohes Maß an Kommunikation erfordern und eben diese Kommunikation, zu der auch nicht zuletzt die Aufklärung gehört, ein absolutes Killerkriterium für den Erfolg einer Idee ist, die letztendlich doch nur zu Einem beitragen soll, unser aller Sicherheit.

Anmerkungen

1 Referenzmuster und Testmuster stammen von unterschiedlichen Personen stammen. Dennoch erkennt das System sie als von ein und derselben Person stammend an. Ist diese Fehlerrate zu hoch, muss der Schwellwert heruntergesetzt werden.

2 Das System erkennt nicht die gleiche Person, obwohl Referenzmuster und Testmuster von der gleichen Person stammen.

Literatur

[1] TeleTrust e. V. Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik (http://www.teletrust.de)

[2] Analyse biometrischer Verfahren (http://www.biometrieinfo.de)

[3] BSI – Bundesamt für Sicherheit in der Informationsindustrie (http://www.bsi.de)

[4] ePass: die neuen biometrischen Ausweise (http://www.neuer-reisepass.de)

[5] Bundesministerium des Innern (http://www.bmi.bund.de)

[6] c't Magazin für Computertechnik (Ausgaben 21.02.2005/ 13.06.2005)

[7] Zeitschrift Comuterwoche (http://www.computerwoche.de)

Autoren

B. IC Sc. Michael Ring
Technische Fachhochschule Wildau
Fachbereich Ingenieurwesen/Wirtschaftingenieurwesen
Master-Studiengang Telematik, Seminargruppe TM/04
mring@igw.tfh-wildau.de

B. IC Sc. Peter Ungvári
Technische Fachhochschule Wildau
Fachbereich Ingenieurwesen/Wirtschaftingenieurwesen
Master-Studiengang Telematik, Seminargruppe TM/04
pungvari@igw.tfh-wildau.de