

bio-ident

Genial einfaches biometrisches Authentisier-Verfahren mit Nullfehlerrate

Beschreibung

Zusammenfassung

Beim **bio-ident**©-Verfahren wird die Identität einer Person durch Messung ihrer Reaktion auf spontane Aufgabenstellungen festgestellt. Insbesondere wird geprüft, ob ein Proband aus einer Mehrzahl gleichartiger Begriffsassoziationen ohne Zögern die für ihn richtige auswählen kann. Im Gegensatz zu anderen Identifikationsverfahren auf Grundlage der Biometrie (Messung körperlicher oder geistiger Eigenheiten) ist 'bio-ident' vom Prinzip her fehlerfrei. Namen und Vornamen bestimmter Personen sind besonders geeignete Assoziationen für 'bio-ident', wie die drei folgenden Beispiele zeigen:

Die Abbildung zeigt den Prototyp eines tragbaren 'bio-ident'-Geräts, das mit Unterstützung der Fraunhofergesellschaft angefertigt wurde.




Der Proband hat eine Chipkarte, die seitlich in das Gerät eingeschoben wird. Im Chip sind die zum Identifizieren (auch Authentisieren genannt) verwendeten Assoziationen, die der Proband selbst ausgewählt hat, verschlüsselt gespeichert.

Nach Eingeben der Chipkarte wird auf dem Display des Geräts eine Liste von 2 x 6 Vornamen sichtbar, und darüber ein Name. Der Proband betätigt eine der zwölf seitlich vom Display neben den Vornamen angebrachten Drucktasten, um die richtige Assoziation zum dargestellten Namen auszuwählen. Danach erscheint eine neue Liste auf dem Display, auf welcher der Proband wieder durch Tastendruck die richtige Assoziation zwischen Namen und Vornamen herstellt. Dieser Vorgang wiederholt sich insgesamt mindestens fünfmal.

Wenn der Proband in der vorgegebenen Zeit (einige Sekunden) alle Assoziationen richtig gebildet hat, zeigt das Gerät die positive Authentisierung an. Wenn nicht, wird der Authentisierfehlschlag gemeldet. Das Gerät ist so programmiert, dass

es nach drei Fehlversuchen oder nach dem Überschreiten einer für die Authentisierung festgelegten maximalen Authentisierzeit gesperrt wird.

Das zweite Beispiel ist eine PC-Demonstration von 'bio-ident' mit dem Programm "SC-Authent" , das aus dem Internet heruntergeladen werden kann. Dies Programm ermöglicht unter anderem eine Beispiel-Authentisierung anhand einer Liste von 12 Vornamen, wobei nacheinander - je nach Vorgabe - zwischen 5 und 12 Namen auf dem Display erscheinen, zu denen der passende Vorname auszuwählen ist.

Das dritte Beispiel ist das **intergramm**-Verfahren zum äußerst einfachen Signieren, Verschlüsseln und Übertragen von Internet-Nachrichten , bei dem der Zugang zum Programm mit 'bio-ident' freigegeben wird.

Hintergrund

Wenn jemand am Geldautomaten Bargeld abheben will, so benötigt er zu seiner Legitimierung, auch Authentisierung genannt, außer einer Bankkarte eine meist vierstellige Geheimnummer, die PIN. Auch für Homebanking vom PC aus ist eine PIN erforderlich, in diesem Fall meistens mit fünf oder sechs Ziffern. Schließlich braucht man eine PIN, wenn man mit einer Chipkarte elektronische Texte digital signieren oder verschlüsseln will, die sicher über das Internet übertragen werden. Solche PINs und andere Codes muss man auswendig lernen und darf sie nicht aufschreiben, damit der Anspruch auf Entschädigung bei Falschbuchungen nicht verloren geht. Die meisten Menschen können sich ihre zahlreichen PINs aber nicht gut merken und notieren sie trotz aller Warnungen. Sie riskieren damit, für eventuelle Schäden haftbar gemacht zu werden.

Um dies Dilemma zu vermeiden, empfiehlt man, biometrische Kennzeichen einer Person zum Legitimieren zu verwenden. Als biometrische Merkmale bezeichnet man messbare körperliche, physiologische oder persönliche Verhaltenskennzeichen, die dazu verwendet werden können, die Identität einer Person zu verifizieren. Zu diesen Verfahren gehören der Vergleich oder die Erkennung von: Fingerbildern, Iris- und Netzhaut-Mustern, Finger- und Handgeometrien, Sprachmustern, Gesichtsformen und anderen. Die Leistungsfähigkeit dieser biometrischen Identifikationsverfahren wird von den Herstellern häufig in Fehlerraten angegeben, und zwar in ‚false acceptance rates (FAR)‘ und ‚false rejection rates (FRR)‘.

Die angegebenen Werte werden in der Praxis aus verschiedenen Gründen meistens nicht erreicht. Hierzu zählen langsame Sensor-Verschmutzung, Fehlverhalten der Probanden bei der Messung, mangelndes Vertrautsein mit dem Verfahren, Zeitdruck und weitere Einflüsse. Die Statistiken der Hersteller beruhen häufig auf der Auswertung einer unzureichenden Testzahl und auf Messungen unter kontrollierten Laborbedingungen. Sie können nur als grober Anhaltspunkt für den Vergleich verschiedener Verfahren dienen. Als Voraussage für die genaue Leistungsfähigkeit eines bestimmten Systems sind sie nicht geeignet. Deshalb überrascht es auch nicht, dass die bisher verwendeten Systeme Fehlerraten von 5 bis 15% und mehr aufweisen. Schon seit Jahren haben interessierte Beobachter einen explosionsartigen Anstieg biometrischer Anwendungen vorhergesagt, durch den die Verwendung von PINs für immer der Vergangenheit angehören würde. Die Wirklichkeit ist anders verlaufen.

Die Akzeptanz der bekannten biometrischen Authentisierverfahren beim Publikum ist bisher also gering. Außerdem liefern viele biometrische Verfahren, anders als die Legitimation mit einer PIN, niemals hundertprozentig sichere Ergebnisse, weil die biometrischen Merkmale selbst und die Messbedingungen zeitlich schwanken.

Grundlagen von 'bio-ident'

Einen besseren Weg, ohne die problematische PIN auszukommen, eröffnet das 'bio-ident' genannte Verfahren, das auf der Auswertung individueller Erfahrungen, am einfachsten in Begriffsassoziationen ausgedrückt, beruht. 'bio-ident' wurde erstmals im Dezember 1996 in der Zeitschrift "Datenschutz und Datensicherheit DuD", Ausgabe 12/96, S. 723-728 beschrieben. Im Unterschied zu den meisten anderen biometrischen Methoden und übereinstimmend mit der PIN-Authentisierung ist 'bio-ident' vom Prinzip her hundertprozentig sicher. Außerdem erfordert 'bio-ident' vom Nutzer keinen größeren manuellen Aufwand als das Eingeben einer PIN auf einer Tastatur.

Zugrunde liegt 'bio-ident' der Gedanke, individuelle Begriffsassoziationen zu rekonstruieren, die zuvor in ihre beiden Teilelemente zerlegt und dann verwürfelt wurden. Solche Assoziationen können beispielsweise aus Namen und Vornamen von Personen bestehen, mit denen derjenige, der sich authentisieren möchte (der Proband), in der Vergangenheit enge Beziehungen hatte: es kann sich dabei um frühere Mitschüler, Lehrer usw. handeln. Individuelle Begriffsassoziationen können nur vom Probanden selbst, aber von keinem andern, nach Vorlage eines ihrer Teilelemente immer wieder, quasi automatisch, aus dem Gedächtnis reproduziert werden.

Zum Rekonstruieren der Assoziationen können diese in einer ‚Multiple Choice‘-Liste dargestellt werden, zum Beispiel:

LINCOLN	
Walter	Ben
Joe	Bill
Henry	Abraham
Jennifer	David
Mary	Matthew
Tony	Caroline


Nachdem der Proband den richtigen Vornamen (Abraham) ausgewählt hat, der zum oben angezeigten Familiennamen (LINCOLN) gehört, lässt 'bio-ident' eine zweite Liste sichtbar werden mit oben einem anderen Familiennamen und darunter denselben zwölf Vornamen in neu-verwürfelter Anordnung. Der Proband hat jetzt den zu dem neuen Familiennamen gehörenden richtigen Vornamen auszuwählen, worauf eine dritte ‚Multiple Choice‘ -Liste sichtbar wird usw. Die Identifizierung ist dann beendet, wenn der Proband zu allen nacheinander gezeigten Familiennamen jeweils den richtigen Vornamen ausgewählt hat.

Im einzelnen läuft 'bio-ident' folgendermaßen ab: Zunächst gibt ein neuer Nutzer seine Assoziationen a-b in einem Initialisierungsschritt in ihrer richtigen Zuordnung in das System ein. Dabei ordnet 'bio-ident' jeweils einem der beiden Assoziations-Teilelemente a oder b, etwa jedem Vornamen, eine bestimmte Teilmenge der Ziffern eines Geheimcodes G bei (Abbildung 1-1). Dann werden die Assoziationen in ihre beiden Teilelemente a und b zerlegt, die Vornamen (a) mit ihren zugeordneten Ziffern verwürfelt und diese ungeordneten Zweiergruppen sowie die Namen (b) in ihrer ursprünglichen Reihenfolge auf eine Diskette oder Chipkarte kopiert (Abbildung 1-2).

Um sich zu authentisieren, steckt der Proband seine Diskette oder Chipkarte in das Diskettenlaufwerk bzw. das Chipkartenlesegerät seines PC, worauf auf dem Bildschirm jeweils der erste Name und eine Liste der verwürfelten Vornamen sichtbar wird (Abbildung 2-1). Der Proband klickt den zum ersten Namen gehörenden Vornamen an, worauf letzterer von der Software vorübergehend mit 1 markiert wird. Danach erscheint der zweite Name und die neu-verwürfelte Liste der Vornamen (Abbildung 2-2). Jetzt wird der zum zweiten Namen gehörige Vorname angeklickt und vorübergehend mit 2 markiert. Dann wird der dritte Name sichtbar (Abbildung 2-3) und so fort (Abbildung 2-4 und 2-5).

Wenn der Proband alle zum Authentisieren verwendeten Vornamen angeklickt hat (Abbildung 2-6), diese also jeweils mit einer Ordnungszahl markiert sind, bringt 'bio-ident' die Vornamen mit ihren Ziffern entsprechend der Reihenfolge der Ordnungszahlen in die ursprüngliche Anordnung (Abbildung 1-3) und bildet aus allen so geordneten Teilmengen aller Ziffern den Geheimcode, im Beispiel also 865 301 720 933 047 825. Er wird in einem von außerhalb des Systems nicht zugänglichen Verfahren einem Vergleichswert des Geheimcodes G gegenübergestellt, um zu entscheiden, ob die Authentisierung des Probanden erfolgreich war oder nicht.

Nach erfolgreicher Authentisierung werden die rekonstruierten Assoziationen aus Namen und Vornamen, jedoch ohne die Ziffern des Geheimcodes, verwürfelt, so dass also bei der nächsten Authentisierung die Namen in geänderter Folge erscheinen. Dann werden die Teilmengen der Ziffern des Geheimcodes erneut den Vornamen in ihrer neuen Reihenfolge zugeordnet (Abbildung 1-4). Danach verwürfelt 'bio-ident' die Vornamen mit ihren Ziffern und kopiert diese ungeordneten Zweiergruppen sowie die neu geordneten Namen auf die Diskette oder Chipkarte des Probanden. Schließlich werden im PC alle während der Authentisierung verwendeten Daten gelöscht, aus denen ein Angreifer den Geheimcode ermitteln könnte.

Die Abbildungen 1 und 2 zeigen das Prinzip von 'bio-ident' an einem Beispiel mit 6 Assoziationen. In diesem Beispiel beträgt die Sicherheit gegen zufälliges Erraten der richtigen Assoziationen nur 1:720. Baut man eine Sperre gegen wiederholte Fehlversuche ein, so wäre gleichwohl der Versuch nahezu aussichtslos, auf Anhieb den Geheimcode durch Probieren zu finden. Höhere Sicherheit erreicht man, wenn man mehr Assoziationen zum Authentisieren heranzieht. Das Äquivalent einer 4-stelligen PIN erreicht man beispielsweise schon mit 4-maligem Anklicken eines Vornamens aus einer Liste von 12 Vornamen, und die Sicherheit einer 5-stelligen PIN mit 5-maligem Anklicken eines Vornamens aus dieser Liste. Insgesamt benötigt man für einen derartigen Authentisierungsvorgang nur wenige Sekunden, wie eine Demonstration mit dem Programm "SC-Authent"  am PC zeigt

Je mehr Assoziationen man verwendet, desto größer wird die Sicherheit von 'bio-ident'. In Abbildung 3 ist die Zahl N aller möglichen Geheimcodes G (Permutationen) abhängig von der Zahl n der zum Authentisieren verwendeten Assoziationen dargestellt, und zwar ausgedrückt als die Stellenzahl der entsprechenden Binärzahl, die als Codelänge bezeichnet wird (eine binäre Einheit = 2 = 1 Bit). Zur Erinnerung: Die als Schlüssellänge bezeichnete Codelänge des für kryptologische Zwecke häufig verwendeten "Data Encryption Standard DES" beträgt 56 Bit. Allgemein werden Schlüssellängen von 128 Bit in der Kryptologie als sicher angesehen, weil ein systematisches Ausprobieren aller möglichen Schlüssel zu lange dauern oder zu teuer würde. Die Kurve A zeigt N , wenn alle vorhandenen Assoziationen n für die Authentisierung rekonstruiert werden müssen. Die Kurve B gilt für den Fall, dass nur $(n-10)$ Assoziationen für eine Authentisierung herangezogen werden, also beispielsweise 5 von insgesamt 15 vorhandenen Assoziationen. Man erkennt den Vorteil, sich mit einer Teilmenge aller vorhandenen Assoziationen zu authentisieren.

Nach Aussage der Kurve B kann man sich beispielsweise schon mit etwa zwölf Assoziationsbildungen aus einem Gesamtvorrat von 22 Assoziationen sehr sicher authentisieren (Codelänge > 50 Bit), selbst wenn man die Zahl wiederholter Fehlversuche nicht begrenzt. Ein derartiges Verfahren ohne Sperrvorrichtung lässt sich sehr einfach verwirklichen. Erwachsene mit abgeschlossener Schulbildung können nach entsprechender Anleitung ohne weiteres die genannte Anzahl personenspezifischen Assoziationen bilden.

Ausgestaltungen von 'bio-ident'

Beim 'bio-ident'-Verfahren kann der Vergleichswert des Geheimcodes G von außen her unauslesbar in einem Zentralcomputer (Server) gespeichert sein, demgegenüber der Proband sich online über eine sichere Datenkommunikation (z.B. Secure Sockets Layer SSL) durch Einlegen seiner Diskette oder Chipkarte in ein Terminal mit Bildschirm durch Assoziationsbildung authentisiert.

Der Vergleichswert kann jedoch auch, von außen her unauslesbar, auf einem lokalen Computer oder in einem speziellen Authentisiergerät registriert sein, an dessen Bildschirm bzw. Display sich der Proband direkt authentisiert.

Schließlich kann der Vergleichswert auf der Diskette oder Chipkarte selbst gespeichert sein, und zwar so, dass er mit vernünftigem Aufwand nicht entschlüsselt werden kann. Für diese Ausgestaltung von 'bio-ident' zeigt die Abbildung den Prototyp eines tragbaren Authentisiergeräts, das in der Zeitschrift „geldinstitute gi“, Heft 3, März 1999, Seiten 140-143 zuerst abgebildet wurde. Dies Gerät wurde mit Unterstützung der Fraunhofergesellschaft entwickelt. Der Proband hat eine Chipkarte, die seitlich in das Gerät eingeschoben wird. Im Chip sind die zum Identifizieren bzw. Authentisieren verwendeten Assoziationen, die der Proband bei seiner Registrierung ausgewählt hat, verschlüsselt gespeichert.



Prototyp

Nach Eingeben der Chipkarte wird auf dem Display des Geräts eine Liste von 2 x 6 Vornamen sichtbar, und darüber ein Name. Der Proband betätigt eine der zwölf seitlich vom Display neben den Vornamen angebrachten Drucktasten, um die richtige Assoziation zum dargestellten Namen auszuwählen. Danach erscheint eine neue Liste auf dem Display, auf welcher der Proband wieder durch Tastendruck die richtige Assoziation zwischen Namen und Vornamen herstellt. Dieser Vorgang wiederholt sich insgesamt mindestens fünfmal.

Wenn der Proband in der vorgegebenen Zeit (einige Sekunden) alle Assoziationen richtig gebildet hat, zeigt das Gerät die positive Authentisierung an. Wenn nicht, wird der Authentisierungsfehler gemeldet. Das Gerät ist so programmiert, dass es nach drei Fehlversuchen oder nach dem Überschreiten einer für die Authentisierung festgelegten maximalen Authentisierungszeit gesperrt wird.

Eine weitere Ausgestaltung von 'bio-ident' für den Fall, dass der Vergleichswert auf der Diskette oder Chipkarte selbst gespeichert ist, zeigt die Demonstration mit dem Programm "SC-Authent", das aus dem Internet heruntergeladen werden kann ☒. "SC-Authent" zeigt unter der Menüleiste „Authentisierung“ eine Beispiel-Authentisierung mit einer Liste von 12 Vornamen, wobei nacheinander – je nach Vorgabe - zwischen 5 und 12 Namen auf dem Display erscheinen, zu denen der passende Vorname durch Anklicken auszuwählen ist. Nachdem die entsprechende Anzahl von Assoziationen erzeugt wurden, zeigt das Programm das positive oder negative Ergebnis der Authentisierung an.

Biometrie als Mittel zur Personenüberprüfung

Eine Personenüberprüfung kann unterschiedliche Ziele haben:

1. Herauszufinden, ob eine Menschenansammlung eine ganz bestimmte Person enthält;
2. herauszufinden, wer der Überprüfte ist (Identifizierung);
3. zu entscheiden, ob der Überprüfte eine bestimmte Person ist oder nicht (Verifizierung einer Identität).

Dabei ist zu trennen zwischen drei Fällen:

- a. Der Überprüfte ist daran interessiert, seine wahre Identität zu verbergen;
- b. der Überprüfte ist daran interessiert, seine wahre Identität zu offenbaren;
- c. dem Überprüften ist das Ergebnis der Überprüfung gleichgültig.

Schließlich kommt es bei einer Personenüberprüfung noch darauf an, bis zu welchem Grad die aktive Mitwirkung des Überprüften nötig ist. Beispielsweise muss der Überprüfte bei einer biometrischen Stimmerkennung ganz bestimmte Kennworte sprechen. Je nach Zielsetzung der Überprüfung sowie Interessenlage und Mitwirkungsaufwand des Überprüften ist das geeignete Überprüfungsverfahren auszuwählen.

Zur Personenüberprüfung der Kategorie 1 gehört die Überwachung mit Videokameras in Flughäfen, Kaufhäusern oder auf öffentlichen Plätzen. Mit einer automatischen Gesichtserkennung lässt sich eine Vielzahl von Personen in Sekunden überprüfen. Die aufgenommenen Gesichter können direkt mit einer Fotodatenbank verglichen werden. Stellt das System eine hohe Übereinstimmung zwischen einer Person auf dem Videobild und einem Foto

aus der Datenbank fest, kann der oder die Betreffende sofort genauer in Augenschein genommen werden. Die Erkennungsrate von etwa 80 % eines solchen biometrischen Verfahrens reicht für Zugangskontrollen und ähnliche Aufgaben nicht aus.

Die klassische forensische Identifizierungsmethode (Kategorie 2) ist die Überprüfung von Fingerabdrücken. Diese Methode kann auch zur Identitätsverifizierung (Kategorie 3) verwendet werden. Hauptsächlich überprüft man im täglichen Leben die Personenidentität aber anhand von Personalausweisen, Reisepässen und vergleichbaren amtlichen oder nichtamtlichen Dokumenten, die in der Regel mit dem Foto des Inhabers versehen sind. Wer seine wahre Identität verbergen möchte, bedient sich gefälschter Dokumente.

Seit dem 1. November 2006: neuer biometrischer Reisepass (ePass)

Der sogenannte **ePass** wird eine Gültigkeit von 10 Jahren haben und soll einen Höchststand an Fälschungssicherheit bieten. Damit führt Deutschland als einer der ersten EU-Staaten den EU-Reisepass ein. Er kostet 59 Euro und speichert auf einem Chip das Gesichtsbild des Passinhabers. Wahrscheinlich ab 2007 wird der Reisepass auch Fingerabdrücke und einen Scan der Iris erhalten.

Die Europäische Union hat am 28.02.2005 beschlossen, elektronische Reisepässe einzuführen. Diese Reisepässe beinhalten wie bisher die personenbezogenen Daten sowie ein Lichtbild des Passbesitzers; künftig werden diese Informationen zusätzlich auch auf einem Chip gespeichert. In einer späteren Phase sollen außerdem zwei Fingerabdrücke des Passbesitzers abgespeichert werden. Das Gesichtsbild, und ab 2007 auch die Fingerabdrücke, werden im JPEG-Format auf dem Chip im Reisepass abgelegt. Die Größe eines typischen Gesichtsbildes beträgt ca. 15 Kbyte.

Für den ePass werden hochsichere Chips mit 72 kB bzw. 64 kB Speicher verwendet, die für die Passanwendung ausschließlich über eine kontaktlose Schnittstelle angesprochen werden. Der Chip und die für das Auslesen notwendige Antenne werden in die Vorderseite des Reisepasses integriert. Die auf dem Chip gespeicherten digitalen Daten sind durch verschiedene Sicherheitsmechanismen geschützt. Sie sind mit einer digitalen Signatur versehen, die die Integrität und Authentizität der Daten sicherstellt.

Der Chip kann auf einem Terminal-Gerät erst dann ausgelesen werden, wenn vorher die optischen Daten von der Datenseite des aufgeschlagenen Passes gelesen wurden. Das Terminal sendet darüber dem Chip ein kryptografisches Protokoll und übermittelt so, dass es die optischen Daten auf der Datenseite im Pass kennt. Zudem wird die Kommunikation zwischen Terminal und Pass verschlüsselt, damit ein Außenstehender nicht die Möglichkeit hat, die kontaktlose Kommunikation zwischen Pass und Terminal abzuhören. Ein aktives Auslesen des Chips ist maximal bis ca. 15 cm möglich.

Damit die Elektronik das Passbild sauber verarbeiten kann, muss es neuen Regeln entsprechen. Das Gesicht muss frontal abgebildet sein; das Halbprofil ist nicht mehr zulässig. Kopf und Frisur sollen komplett sichtbar sein, das Gesicht soll drei Viertel der Bildhöhe ausmachen. Die Person muss "mit

neutralem Gesichtsausdruck und geschlossenem Mund" in die Kamera blicken. Bei Brillenträgern sollen die Augen deutlich erkennbar sein. Ein Kopftuch aus religiösen Gründen ist zulässig, aber auch damit muss das Gesicht von der Kinnunterkante bis zur Stirn erkennbar sein.

Wenn der Chip nicht mehr funktionieren sollte, bleibt der Reisepass weiterhin ein gültiges Reisedokument. Die Kontrolle biometrischer Merkmale ist nämlich nur ein zusätzliches Instrument der Grenzkontrolle und ersetzt nicht die herkömmliche Personenkontrolle. Alle Grenzkontrollpunkte sollen bis 2008 mit Lesegeräten ausgestattet werden, die den Abgleich der biometrischen Daten ermöglichen. Die Investitionskosten hierfür werden mit 670 Mio. Euro angegeben, hinzu kommen weitere 610 Mio. Euro jährliche Betriebskosten.

Der Erfolg des ePasses bleibt abzuwarten. Anzunehmen ist, dass die Fälschung eines einmal von der Behörde ausgestellten Passes erschwert wird. Ob das auch für die Neuanfertigung von falschen Pässen zutrifft, ist nicht so sicher. Das Hauptproblem dürfte bei der Grenzkontrolle selbst liegen, wo das Gesichtsbild und später der Fingerabdruck der kontrollierten Person neu aufgenommen, digitalisiert und mit dem im Chip gespeicherten Pendant automatisch verglichen werden soll. Bei den bisher ermittelten Fehlerquoten in der biometrischen Erkennung von bis zu 15% sind starke Zweifel an der Funktionsfähigkeit der Kontrollen angebracht, vor allem, weil sich die Gesichtsgeometrie einer Person während der zehnjährigen Gültigkeit des ePasses naturbedingt ändert. Ein zweiter Schwachpunkt des ePasses ist der Chip, dessen Funktionsfähigkeit mindestens zehn Jahre zu garantieren ist.

Chipkarte als Ausweis

Eigentlich sind in der Ära des Internet die klassischen auf Papier oder ähnlichem Material gedruckten Personalausweise oder Reisepässe mit zusätzlichen Sicherheitsmerkmalen wie beim ePass überholt: Sie könnten durch die praktischeren Chipkarten ersetzt werden, in denen die personenbezogenen Daten des Inhabers und eventuelle zusätzliche Funktionen digital gespeichert sind (multifunktionale Chipkarten). Mit einem solchen digitalen Personalausweis weist man sich an einem Kartenleseterminal vor allem dadurch aus, dass man seine PIN eingibt. Einige Staaten führen derartige Personalausweise in Form von Chipkarten bereits ein. Das Arbeiten mit einer PIN ist jedoch, wie eingangs dargelegt, nicht ideal: erstens muss der Chipkarteninhaber sich auf sein unvollkommenes Gedächtnis verlassen; zweitens besteht die Gefahr, dass die PIN beim Eingeben ausgespäht wird.

Eine andere Anwendung von personalisierten Chipkarten ist die automatisierte Zugangskontrolle mit Hilfe eines am Eingang aufgestellten Kartenlesers, zum Beispiel für Besucher eines Tierparks mit einem Jahresabonnement. Anstelle der Authentisierung durch Eingabe einer PIN in eine numerische Tastatur wurden für diese Chipkarten-Anwendung verschiedene biometrische Identifizierungsverfahren ausprobiert, vor allem die Fingerabdrucktechnik. Diese Methode erscheint auf den ersten Blick recht brauchbar, hat aber den Nachteil, dass das Scannen des Fingerabdrucks häufig nicht funktioniert. In diesen Fällen muss der Besucher warten, bis ein Angestellter die Karte kontrolliert und den Eintritt freigibt. Außerdem ist es nicht jedermanns Sache, seinen Finger gegen eine möglicherweise mit Bazillen verseuchte Auflegefläche zu pressen.

Nach den ersten unbefriedigenden Ergebnissen mit dem Fingerabdruckverfahren ist man auf automatische Zugangskontrollen mit fotografischer Gesichtserkennung übergegangen, allerdings ebenfalls ohne überzeugende Ergebnisse.

bio-ident als Ausweis in der automatischen Zugangskontrolle

Wesentlich besser als mit der Biometrie im herkömmlichen Sinn können sich die Inhaber digitaler Chipkartenausweise durch 'bio-ident' ausweisen. Anstelle körperlicher Referenzwerte werden die für 'bio-ident' charakteristischen verwürfelten Vornamen mit ihren zugeordneten Ziffern und die geordneten Namen in der Chipkarte gespeichert, neben dem verschlüsselten Geheimcode G und eventuellen zusätzlichen personenbezogenen Daten des Inhabers. An jedem Kartenleseterminal kann sich der Ausweisinhaber einfach, schnell und sicher durch Bildung einiger persönlicher Assoziationen legitimieren, vgl. den Prototyp eines Authentisiergeräts mit Chipkarten.



Prototyp

Beispielsweise können Besitzer einer Zugangsberechtigungs-Chipkarte entsprechend der Anordnung des Prototyps an einem Sonderzugang mit einem kleinen Gerät kontrolliert werden, das mit einem Display und einigen Tasten versehen ist und in das der Eintretende seine Chipkarte einlegt. Er wird darauf vom Gerät aufgefordert, durch Tastendruck einige auf dem Display gezeigte Begriffspaare auszuwählen, die nur er selbst kennt. Wenn dies erfolgreich geschehen ist, öffnet sich der Zugang automatisch. Gleichzeitig nimmt eine Digitalkamera ein Bild des Eintretenden auf und registriert dieses zusammen mit seinen in dem Chip gespeicherten Ident-Daten und der Uhrzeit.

Bei Bedarf kann später durch Vergleich mit einem Referenzfoto verifiziert werden, dass der Chipkarten-Berechtigte allein und in eigener Person den Sonderzugang benutzt hat. Im Bewusstsein dieser Kontrollmöglichkeit - es ist nicht einmal nötig, dass der Vergleich mit dem Referenzfoto tatsächlich erfolgt - wird jeder Besitzer einer Zugangsberechtigungs-Chipkarte davon absehen, diese an Verwandte oder Bekannte auszuleihen oder gar zu versuchen, nach einer positiven Identifizierung zusammen mit unberechtigten Begleitern den Zugang zu passieren.

Der Aufwand für eine derartige automatische Zugangskontrolle nach dem System 'bio-ident' würde bei einigen Tausend Euro liegen.

Ausweislose Personenkontrolle mit 'bio-ident'

Ganz ohne konventionelle oder digitalisierte Personalausweise kommt man aus, wenn man bei 'bio-ident' den verschlüsselten Geheimcode G, die verwürfelten Vornamen mit ihren Ziffern und die geordneten Namen in einem von außen her unauslesbaren Zentralcomputer (Server) speichert.

Bei einem solchen idealen Verfahren zur Personenüberprüfung würde man zunächst den Namen der betreffenden Person in ein Terminal eingeben, das

über das Internet mit dem zentralen Server verbunden ist. Dann würden die verwürfelten Vornamen mit ihren Ziffern und die geordneten Namen online und verschlüsselt vom Server zum Terminal gesendet und an dessen Bildschirm vom Überprüften schrittweise durch Assoziationsbildung geordnet. Schließlich würde der hierdurch neugebildete Geheimcode G ebenfalls verschlüsselt zurück zum Server gelangen und dort mit dem Referenzwert verglichen werden. Das Ergebnis würde als positiver oder negativer Überprüfungsbescheid zum Terminal zurückgemeldet. Die zum Terminal gelangten Daten würden dort nach Gebrauch gelöscht.

Dies ausweislose Verfahren befreit den Bürger von der lästigen Pflicht, bei vielen Gelegenheiten seinen Personalausweis bei sich führen zu müssen. Die üblichen Bedenken der Datenschützer gegen eine zentrale Datenbank würden entfallen, weil dort keine heiklen biometrischen Merkmale gespeichert sind, sondern nur anonyme Begriffe und Zufallszahlen.

Die ausweislose Personenüberprüfung mit 'bio-ident' kann in der Weise ergänzt werden, dass im Zweifelsfall von der überprüften Person ein Foto mit einer Digitalkamera am Terminal aufgenommen wird, das mit einem vom zentralen Server angeforderten Referenzfoto verglichen wird.

Besondere Vorteile von 'bio-ident'

- 'bio-ident' ist einfach, für jedermann akzeptabel und erkenntungssicher wie das PIN-Verfahren.
- Memorisierung einer PIN oder eines anderen Codes nicht erforderlich; Ausspähen des Codes, zum Beispiel bei der Eingabe in die Tastatur, nicht möglich.
- Der Übergang vom PIN- auf 'bio-ident' ist bei vielen Anwendungen ohne völlige Erneuerung der Hardware gleitend möglich.
- Eine ideale ausweislose Identitätsüberprüfung ist realisierbar, weil keine personenspezifischen Referenzdaten zentral zu speichern sind.

Abbildungen 1 bis 3

Abbildung 1: Ablauf des Verfahrens

Namen, Vornamen und Ziffernteilmengen in ursprünglicher Anordnung

K O H L	H e l m u t	- 865	1
B R A N D T	W i l l y	- 301	
A D E N A U E R	K o n r a d	- 720	
S T O I B E R	E d m u n d	- 933	
K O C H	R o l a n d	- 047	
S C H R Ö D E R	G e r h a r d	- 825	

Namen in ursprünglicher Anordnung, Vornamen und Ziffernteilmengen verwürfelt

K O H L	K o n r a d	- 720	2
B R A N D T	G e r h a r d	- 825	
A D E N A U E R	H e l m u t	- 865	
S T O I B E R	R o l a n d	- 047	
K O C H	W i l l y	- 301	
S C H R Ö D E R	E d m u n d	- 933	

Namen in ursprünglicher Anordnung, Vornamen und Ziffernteilmengen neugeordnet

K O H L	H e l m u t	- 865	3
B R A N D T	W i l l y	- 301	
A D E N A U E R	K o n r a d	- 720	
S T O I B E R	E d m u n d	- 933	
K O C H	R o l a n d	- 047	
S C H R Ö D E R	G e r h a r d	- 825	

Namen und Vornamen verwürfelt, Ziffernteilmengen in ursprünglicher Anordnung

K O C H	R o l a n d	- 865	4
S T O I B E R	E d m u n d	- 301	
S C H R Ö D E R	G e r h a r d	- 720	
K O H L	H e l m u t	- 933	
B R A N D T	W i l l y	- 047	
A D E N A U E R	K o n r a d	- 825	

Abbildung 2: Anklicken der Vornamen auf dem Bildschirm

KOHL		1
Konrad	Roland	
Gerhard	Willy	
Helmut	Edmund	

BRANDT		2
Edmund	Gerhard	
Willy	Helmut	
Konrad	Roland	

ADENAUER		3
Roland	Willy	
Edmund	Konrad	
Gerhard	Helmut	

STOIBER		4
Willy	Helmut	
Edmund	Gerhard	
Roland	Konrad	

KOCH		5
Gerhard	Konrad	
Roland	Edmund	
Helmut	Willy	

SCHRÖDER		6
Roland	Willy	
Edmund	Helmut	
Konrad	Gerhard	

**Abbildung 3: Zahl N
aller möglichen Permutationen**

