Biometrie

Referenzprojekte

BITKOM

Impressum

Herausgeber: BITKOM
Bundesverband Informationswitschaft,
Telekommunikation und neue Medien e. V.

Albrechtstraße 10 A
10117 Berlin
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Lutz Neugebauer
Tel.: 030.27576-242
l.neugebauer@bitkom.org

Redaktion: Lutz Neugebauer, Leila Ambrosio (BITKOM)
In Zusammenarbeit mit: Dr. Sandra Schulz (Giesecke & Devrient GmbH),
Michael von Foerster (Bosch Sicherheitssysteme GmbH), Gregor Költzsch (Bundesdruckerei GmbH)
und Rudolf Gurland (T-Systems Enterprise Services GmbH)

Gestaltung / Layout: Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)

Bildernachweise
S.3, 6, 7, 22: Bosch Sicherheitssysteme GmbH
S.8, 16, 29: Bundesdruckerei GmbH
S.9: ekey biometric systems Deutschland GmbH
S.10, 11: it-werke e. K.
S.12, 21: TST Biometrics GmbH
S.13: Deutscher Sparkassen Verlag GmbH
S.14: iSM - Institut für System- Management GmbH
S.15: Interflex Datensysteme GmbH & Co. KG
S.18,19: VOICE.TRUST AG
S.20: Siemens IT Solutions and Services
S.23, 24: L-1 Identity Solutions AG
S.25: NEC Deutschland GmbH
S.26, 27: DERMALOG Identification Systems GmbH
S.28: secunet Security Networks AG
S.30: Fraunhofer-Institut für Sichere Informationstechnologie
S.31: T-Systems Enterprise Services GmbH
S.32: BITKOM e. V.

Biometrie

Referenzprojekte

BITKOM

Inhaltsverzeichnis

Einleitung

Die deutsche Biometriewirtschaft entwickelt Lösungen auf international höchstem technischem Niveau. Der Einsatz von Biometrie ermöglicht damit bequeme, nutzerfreundliche und sichere Lösungsansätze für verschiedene komplexe Aufgabenstellungen.

Der hohen technischen Leistungsfähigkeit und Produktqualität stehen nicht unbeträchtliche Widerstände und Barrieren bei der Einführung entgegen. Die „Biometrie-Broschüre“ soll über die Technologie aufklären sowie anhand von Referenzbeispielen aus dem täglichen Leben die Einsatzfähigkeit von Biometrie darstellen. Hierbei wird besondere Aufmerksamkeit auf die Vorteile für den Nutzer gelegt, da Biometrie immer eine personenbezogene Anwendung darstellt.

Quelle: Bosch Sicherheitssysteme

Potentiell interessierte Unternehmen sowie Anwendergruppen erhalten durch die Broschüre einen Überblick über vorhandene Projekte bzw. Referenzen und erhalten damit einen Eindruck von der vielfältigen Einsatzmöglichkeit von Biometrie zur Erleichterung des täglichen Lebens im privaten Umfeld, im Arbeitsumfeld oder im öffentlichen Umfeld.

Einführung in das Thema Biometrie

Biometrie ist abgeleitet aus dem Griechischen: “bios” (Leben) und “metron” (messen). Unter Biometrie versteht man automatisierte Methoden zur Erkennung von Menschen anhand von physiologischer Charakteristika oder Verhalten.

Allgemein findet die biometrische Erkennung in fünf Stufen statt:

Enrolment

- Erstmalige Erfassung und Speicherung der biometrischen Merkmale
- Qualitätssicherung
- ggf. Merkmalextraktion

Verifikation/ Identifikation

- Erneute Aufnahme der biometrischen Merkmale bei der späteren Anwendung
- Vergleich der Daten mit mindestens einem existierendem Datensatz

Beispiele für biometrische Merkmale

Physiologisch: Angeboren, Einzigartig, Unveränderbar, Nicht transferierbar

- Fingerabdruck
- Gesicht
- Iris
- Handgeometrie
- Fingergeometrie
- Retina
- Venen
- Ohrform
- Geruch

Verhalten: Erlernt und trainiert, Veränderbar

- Stimme
- Unterschrift
- Tastenanschlag
- Gang
- Gestik
- Gesichtsmimik

Einsatzfelder biometrischer Verfahren in allen Bereichen des täglichen Lebens

Die Verwendung von biometrischen Verfahren erhält zunehmend Einzug in die verschiedenen Bereiche des täglichen Lebens. Wurden Begriffe wie Daktyloskopie und erkennungsdienstliche Behandlung in der Vergangenheit mit dem hoheitlichen Einsatz von Biometrie verbunden, so steht heute ein leistungsfähiges Instrument für Rollen und Identitätsmanagement im öffentlichen, privaten und beruflichen Umfeld zur Verfügung. Die unterschiedlichen Anwendungsfelder von biometrischen Verfahren in den jeweiligen Lebensbereichen unterliegen zum einen verschieden rechtlichen und regulatorischen Bedingungen, zum anderen haben sie in ihrer Ausprägung die Spannweite von Komfortmerkmal bis Hochsicherheitsanwendung. In der folgenden Darstellung und den zugeordneten Referenzen werden die wesentlichen Aspekte des Einsatzes von biometrischen Verfahren in den verschiedenen Lebensbereichen skizziert.

Einsatz im privaten und persönlichen Umfeld

Im privaten Lebensbereich sichert Biometrie heute die Verfügung über die eigenen Daten, verbunden mit einem hohen Komfort in der Anwendung. Der Paradigmenwechsel vom Haben und Wissen (Karte und Pin) zum Sein (Biometrie) kann im persönlichen Umfeld nachhaltige Erleichterungen schaffen und zugleich eine hohe Sicherheit im Umgang und mit der Verfügung über personenbezogene Daten sichern.

Für den Nutzer von Biometrie im privaten Umfeld stehen

- Bequemlichkeit
- Einfache Handhabung
- Wahlfreiheit des Verfahrens (Bezahlen mit dem Fingerabdruck oder z.B. bar)
- Entscheidungsfreiheit zur Verwendung seiner Daten

im Vordergrund.

Akzeptanz und Usability der Anwendung stehen auch in den beteiligten Unternehmen noch deutlich vor Kostenargumenten. Für Unternehmen, die ihren Kunden ein biometrie-gestütztes Verfahren im Rahmen ihres geschäftlichen Verhältnisses anbieten, stehen

- Akzeptanz des Endnutzers
- Erhöhung des Umsatzes
- Schutz der Daten des Kunden
- Kostenersparnis bei Endkundenprozessen

im Vordergrund.

Der rechtliche Rahmen wird durch die Einhaltung von gesetzlichen Vorgaben (z.B. BDSG) als Minimalbedingung gesetzt, allerdings wird dies zumeist durch die freiwillige Teilnahme an einer geschlossenen Benutzergruppe aushandelbar.

Für das private Umfeld gilt zukünftig die Devise:
Biometrie – die Freiheit gönne ich mir.

Einsatz im geschäftlichen Umfeld sowie in Unternehmen und Organisationen

Das berufliche und geschäftliche Umfeld ist geprägt von Rollen und Identitäten, die im Unternehmen oder Organisationen verwaltet werden und in der Regel mit einzelnen Kennungen und Berechtigungen verbunden sind. Durch die Verwendung eines einzelnen, einzigartigen biometrischen Schlüssels lassen sich auch hier deutliche Vereinfachungen schaffen.

Die Anforderungen aus dem geschäftlichen Umfeld an die Technologie und die entsprechenden Systeme lassen sich wie folgt darstellen.

Die Technologie:

- ist leistungsfähig und hat notwendigen Reifegrad
- für Nutzer und die Arbeitnehmer- und Interessensvertretungen akzeptabel
- unterstützt Unternehmensprozesse
- bewirkt Kostenersparnis
- ist skalierbar
- schafft Sicherheit

Der rechtliche Rahmen wird durch das jeweilige Innenverhältnis von Unternehmen zu Mitarbeiter oder Organisation zu Mitglied bestimmt. Die Einhaltung von gesetzlichen Vorgaben wird durch die verpflichtende Teilnahme an einer geschlossenen Benutzergruppe nicht beeinträchtigt. Neben den Komfortmerkmalen, die in der Nutzung in Unternehmen und Organisationen für den Einzelnen, analog zum Privaten Umfeld, entstehen, sind hier Aspekte der Prozessoptimierung, Governance und Sicherheit in Sinne eine Sicherung eines reibungslosen Geschäftsbetriebes stärker im Fokus.

Einsatz im hoheitlichen Anwendungsfeld und im öffentlichen Umfeld

Im hoheitlichen Bereich ist ein traditionelles Einsatzfeld die kriminaltechnische Erfassung oder erkennungsdienstliche Behandlung. Mit modernen AFIS-Systemen steht hier bereits ein starkes biometrisches Instrument für die Behörden mit Sicherheitsaufgaben zur Verfügung, das dabei hilft, Bürger und staatliche Integrität gegen Einflüsse von Außen zu schützen.

Durch die veränderte Sicherheitslage, neue Anforderungen im Luftverkehr sowie in Hinblick auf die Sicherung der EU-Außengrenzen gibt es weitere Anwendungsfelder für Biometrie im öffentlichen Umfeld. Die Biometrie dient, den Bürger in seinen Rechten zu schützen und ein Instrument bereitzustellen, das Bürger- Behördenkontakte, aber auch Kontakte zwischen Bürgern und anderen Unternehmen erleichtert.

Die Verwendung von Biometrie zur Authentisierung hilft dabei Bürgerdienste unabhängig von Ort und Zeit online anzubieten und rechtsicher auszuführen. Bei Großveranstaltungen, bei Wahlen oder zur Besucherkontrolle in Einrichtungen mit hohem Schutzbedarf lassen sich biometrische Verfahren anwenden.

Im Focus stehen dabei aus hoheitlicher Sicht:

- Hohe Sicherheit
- Internationale Interoperabilität
- Verwendbarkeit bei großen Benutzergruppen

Die gesetzlichen Anforderungen in diesem regulierten Umfeld sehen den Einsatz biometrischer Verfahren unter Wahrung der Persönlichkeitsrechte vor.

Entwicklungsprojekte

Über die bestehenden Verfahren und Anwendungen hinaus werden Neu- und Weiterentwicklungen vorangetrieben, die Verfahrenssicherheit und Usability im Focus haben. Die Ergebnisse dieser Projekte werden wesentlich dazu beitragen, weitere Anwendungsfelder zu erschließen und den täglichen Umgang mit Biometrie als Zugangsschlüssel zu erleichtern.

Die als Entwicklungsprojekte beschriebenen Lösungen verwenden Systeme und Methoden, die den Charakter von Vorprodukten haben oder noch nicht umfangreich erprobt und eingesetzt werden.

1 Privates Umfeld

1.1 Zoo Hannover: Dauerkartenkontrolle

Projektbeschreibung

Der „Erlebnis-Zoo Hannover“ stand vor der Herausforderung den großen Besucherandrang bei Dauerkartenbesuchern und die damit verbundene Kontrolle von insgesamt über 70.000 Jahreskarten zu bewältigen. Ob die Besucher mal mit Brille oder Bart erscheinen, wird durch das Erkennungsverfahren unerheblich: der Missbrauch von nicht übertragbaren Dauerkarten wird verhindert und dem Besitzer der Dauerkarte ein komfortabler und schneller Zugang zum Zoo Hannover ermöglicht.

Umsetzung

An den Eingängen sind Kartenleser und digitale Kameras installiert. In weniger als einer Sekunde wird das Live-Gesicht mit den gespeicherten Gesichtsdaten verglichen, die Eintrittsberechtigung festgestellt und der Zugang freigegeben. Das Gesichtserkennungssystem musste an die vorhandenen Systeme angeschlossen werden. Sowohl das Kassensystem, das Kartensystem als auch die Vereinzelungsanlage mussten über Schnittstellen angesteuert werden.

Besonderheit

Die Zutrittskontrolle „Erlebniszoo Hannover“ weißt nach, dass Gesichtserkennungssysteme auch im realen Außeneinsatz und mit großen Datenbanken tadellos funktionieren.

Technische Details	
Laufzeit:	Seit 2002
Merkmal:	Gesichtserkennung
Nutzer:	> 130.000
Transaktionen:	Bis zu 6000 pro Tag
Datenträger:	Barcode auf Karte
Sensoren:	6

Kontakt

BOSCH Sicherheitssysteme GmbH, Michael von Foerster
michael.vonfoerster@de.bosch.com

Ähnliche Projekte

Zutrittskontrolle im Dierenpark Emmen, Niederlande (Gesicht)

Technische Details	
Laufzeit:	Seit Mai 2006
Merkmal:	Gesicht
Nutzer:	200.000 Nutzer
Transaktionen:	Bis zu 700 Enrolments / bis zu 3.000 Verifizierungen an Spitzentagen
Datenträger:	200.000, 2D Barcode Dauerkarten
Sensoren:	14 Sensoren

Kontakt

L-1 Identity Solutions AG, Katrin Booms, kbooms@l1id.com

1.2 Anonyme Zutrittskontrolle für Spielcasinos

Projektbeschreibung

Nach einem Urteil des BGH (AZ III ZR 65/05) aus dem Jahr 2005 müssen Spielbanken ihrer Überwachungspflicht auch bei Automatenspielern nachzukommen (Bestätigung am 22. November 2007 - III ZR 9/07). Der BGH bejaht damit auch für Automatenspielsäle eine allgemeine Kontrollpflicht, die den Zutritt von antragsgemäß gesperrten Spielern verhindern soll. Bosch Sicherheitssysteme hat für die Spielbank Bad Homburg ein anonym arbeitendes Gesichtserkennungssystem installiert und nunmehr an die neue Rechtssprechung angepasst. Es erkennt zuverlässig Personen, deren Gesichtsbilder aufgrund einer freiwilligen Selbstsperre gespeichert sind. Das Aufsichtspersonal ist damit in der Lage, den entsprechenden Personen das Spielen im Automatensaal der Spielbank automatisch zu untersagen. Personen, die sich bei der Spielbank haben registrieren lassen, nutzen nunmehr den automatischen, biometrischen Zutritt mittels Gesichtserkennung.

Umsetzung

Registrierte Gäste benutzen zum Zutritt Ihre Casino-Karte. Aufgrund der Kartennummer wird mittels Verifikation verglichen, ob der Gast auch tatsächlich der berechtigte Karteninhaber ist. Ist das der Fall, öffnet sich eine Schleuse und der Gast kann ohne weitere Kontrollen den Automatensaal betreten. Will sich der Gast sperren lassen, kann die Karte für weitere Zutritte gesperrt werden.

Besonderheit

Das Aufsichtspersonal ist damit in der Lage, das Spielen von entsprechenden Personen im Automatensaal der Spielbank ohne eine für den Spieler lästige Ausweiskontrolle zu verhindern. Im Automatensaal des Casinos in Bad Homburg hat Bosch bereits im Sommer 2005 ein Gesichtserkennungssystem zum Schutz der Spieler mit auffälligem Spielverhalten installiert. Das System wurde jetzt der aktuellen Rechtsprechung angepasst.

Technische Details	
Laufzeit:	Seit 2005
Merkmal:	Gesichtserkennung
Nutzer:	Jeder Besucher der Spielbank
Transaktionen:	> 300 pro Tag
Datenträger:	Lokale Datenbank
Sensoren:	Digitalkameras

Kontakt

BOSCH Sicherheitssysteme GmbH - Michael von Foerster
michael.vonfoerster@de.bosch.com

Ähnliche Projekte

Zutrittskontrolle in weiteren 9 Spielbanken in Baden-Württemberg, Sachsen sowie Hamburg

Technische Details	
Laufzeit:	Seit Dezember 2006 im Dauerbetrieb
Merkmal:	Gesichtserkennung
Nutzer:	Jeder Besucher
Transaktionen:	Vertraulich
Datenträger:	Lokale Datenbank
Sensoren:	Mehrere digitale Hochleistungs-Videokameras

Kontakt

Cross Match Technologies GmbH, Roberto Wolfer
roberto.wolfer@crossmatch.com

1.3 Fußball-Weltmeisterschaft 2006: Adidas-Arena

Projektbeschreibung

Während der Fußball-Weltmeisterschaft 2006 führte die Bundesdruckerei gemeinsam mit Philips und T-Systems am Mitarbeitereingang der „adidas World of Football" vor dem Reichstag erfolgreich eine biometrische Zutrittskontrolle mit EAC auf Basis des Fingerabdrucks durch. Die Bundesdruckerei lieferte das Gesamtsystem, Philips stellte die hochsichere SmartMX-Chiptechnologie für die kontaktlosen biometrischen Mitarbeiterausweise zur Verfügung, und T-Systems implementierte das EAC-Verfahren auf Basis des eigenen Chipkartenbetriebssystems TCOS.

Umsetzung

Im Rahmen der Zutrittskontrolle wurde für den Schutz der Fingerabdruckdaten der adidas-Mitarbeiter und akkreditierter Besucher die Extended Access Control (EAC) eingesetzt. Diese Zutrittskontrolle der neuesten Generation sorgt verlässlich dafür, dass nur autorisierte Personen Einlass erhalten.

Besonderheit

Weltweit kam zum ersten Mal eine Zutrittskontrolle mit Chipkarten zum Einsatz, die den Standards der zweiten Generation der ICAO entspricht und EAC umsetzt. Diese Extended Access Control wird notwendig, da die Karten Fingerabdruckbilder enthalten, die besonders stark gegen unrechtmäßigen Zugriff geschützt werden sollen. Mit diesem System wird ein neues Maß für den Schutz der persönlichen Daten erreicht: Diese bleiben unter ausschließlicher Kontrolle des Anwenders und sind auch bei Verlust des Ausweises sicher gegen Diebstahl geschützt.

Technische Details	
Laufzeit:	Seit Mitte 2005 produktiv
Merkmal:	Finger
Nutzer:	2000 Nutzer
Transaktionen:	Ca. 20.000 Verifikationen
Datenträger:	2.000 Token
Sensoren:	9

Kontakt
Bundesdruckerei GmbH, Gregor Költzsch,
gregor.koeltzsch@bdr.de

1.4 Zutrittskontrolle zur Bibliothek des Heilwig Gymnasiums

Projektbeschreibung

Seit Mitte Februar 2007 müssen die Oberstufenschüler des Heilwig Gymnasiums in Hamburg-Alsterdorf nicht mehr auf einen Lehrer warten, der Ihnen die Tür der Bibliothek, in der es auch acht Computerarbeitsplätze gibt, aufsperrt. Sie ziehen stattdessen lediglich ihren Finger über einen biometrischen Sensor. Die Schulleitung suchte nach einer Lösung diese Räume abzusichern und gleichzeitig den berechtigten Schülern einen unkomplizierten Zutritt zu gewähren.

Umsetzung

In Betrieb sind drei ekey® TOCAnet M Terminals mit Edelstahlabdeckung. Das Zutrittssystem basiert auf einer Server- und Terminalarchitektur, welche für größere Unternehmen und Behörden entwickelt wurde. Die Schüler werden im Sekretariat eingelernt und können anschließend mit dem Fingerscan die Türe öffnen. Durch das System lassen sich innerhalb einer Organisation weltweit unterschiedliche Zutrittsbereiche einfach verwalteten. Die Nachvollziehbarkeit der Transaktionen ist über ein Logfile gewährleistet. Das System besteht aus einem Fingerscanner, einer Steuereinheit sowie der dazugehörigen Software.

Besonderheit

Die Schüler bekommen weder einen Schlüssel, noch eine Zutrittskarte oder einen Code. Die biometrischen Daten werden als Template zentral auf dem Server vorgehalten. Für die Schüler wird zudem eine bestimmte Uhrzeit definiert, in der Sie die Bibliothek betreten dürfen. Für die Schulleitung war es hierbei besonders von Vorteil, bestimmten Schülern auch außerhalb der regulären Unterrichtszeiten den Zutritt zur Bibliothek ermöglichen zu können. Im Moment sind rund 300 Schüler in diesem System erfasst. In Planung ist die Erfassung sämtlicher

Schüler. Weiterhin soll das System auch in anderen Bereichen, wie beispielsweise den Computerräumen, eingesetzt werden.

Technische Details	
Laufzeit:	Seit Februar 2007
Merkmal:	Finger, thermische Zeilensensoren
Nutzer:	300
Transaktionen:	450 Identifikationen/Tag
Datenträger:	Keine Datenträger notwendig
Sensoren:	3

Kontakt

ekey biometric systems Deutschland GmbH
Dr. Konrad Baier, Konrad.Baier@ekey.net

Ähnliche Projekte

Absicherung einer Schule in Puerto Rico

Technische Details	
Laufzeit:	Seit Frühjahr 2007
Merkmal:	Fingerabdruck, berührungslos optisch und kapazitiv (PC Log In), Verifikation
Nutzer:	1.400 Schüler täglich mind. 2x
Sensoren:	8 Sensoren im Zutrittsbereich

Kontakt

TST Biometrics GmbH
Martin Ditscherlein, md@tst-bioemtrics.com

1.5 EDEKA – Märkte mit biometrischem Zahlsystem

Projektbeschreibung

Die EDEKA Regionalgesellschaft Südwest verfolgt das Ziel, in Ihren Märkten innovative Zahlsysteme einzusetzen. IT – Werke pilotierte den ersten Markt Ende 2005 in Rühlsheim mit dem Produkt digiPROOF. Nach erfolgreichen Tests erfolgte ab Mitte 2006 die Ausrollung in die Fläche der Regionalgesellschaft mit bis zu 5 Märkten pro Woche.

Seit Ende 2006 erfolgt die Ausstattung von EDEKA Märkten in weiteren Regionalgesellschaften.

Umsetzung

Die Teilnehmer erklären sich schriftlich mit der Erfassung Ihrer kundenbezogenen Daten einverstanden, die zur Zahlungsabwicklung benötigt werden. Diese Informationen werden mit dem von der Fingerkuppe gewonnenen Template verbunden und in einer separaten Datenbank abgespeichert.

Bei einer Zahlung schließt die Kassiererin den Kassenvorgang mit einem separaten Tastendruck (Zahlart digiPROOF) ab. Der Scanner leuchtet auf und der Kunde legt den registrierten Finger darauf. Dieses Template wird mit den in der Datenbank hinterlegten Templates (1:n) abgeglichen. Wird ein Template als richtig erkannt, werden die notwendigen Daten zur Zahlungsabwicklung an die Kasse zurückgegeben, die Kasse schließt den Kassenvorgang ab und übergibt den Zahlungsdatensatz an das Folgesystem ab. Das System kann in allen Handels- und Marktumgebungen eingesetzt werden.

Besonderheit

Damit das System in die Kassenumgebung integriert werden kann, muss mit dem Lieferanten der Kassensoftware eine Schnittstelle programmiert werden.

Technische Details	
Laufzeit:	Ende 2005 – Ende offen
Merkmal:	Finger
Nutzer:	150.000
Transaktionen:	Identifikation über 2.500.000 p. A.
Datenträger:	Datenbank
Sensoren:	700

Ähnliche Projekte

Bezahlfunktion für Schüler an Schulen der Stadt Offenburg (Finger)

Technische Details	
Laufzeit:	Oktober 2006 – Ende offen
Merkmal:	Finger
Nutzer:	2000
Transaktionen:	Identifikation 1500/Tag
Datenträger:	Datenbank
Sensoren:	11

Kontakt für beide Projekte
it-werke e. K. , Stefan Sewöster / sewoester@it-werke.de
Rolf Biben / biben@it-werke.de

1.6 Virtuelle Kundenkarte iCARD im „Zebra – Club“ des Gewandhauses Gruber, Erding

Projektbeschreibung

Das Gewandhaus Gruber in Erding betreibt an 4 Standorten 10 Mode-, Sport- oder Schuhgeschäfte. Gruber beabsichtigte ein Kundenbindungsprogramm einzuführen, das sich generell von den bisher am Markt platzierten Kartenlösungen unterscheidet. Auf die Ausgabe einer realen Kundenkarte wurde verzichtet.

Umsetzung

Die Teilnehmer des „Zebra Clubs“ erklären sich schriftlich mit der Erfassung von kundenbezogenen Daten einverstanden, die zur Zahlung und zur Kundenbindung relevant sind. Diese Daten werden mit dem von der Fingerkuppe gewonnenen Template in einer separaten Datenbank verknüpft und abgespeichert. Für eine spätere Kundenanalyse, werden alle Daten des Kassenbons abgespeichert. Der Abschluss des Einkaufs wird durch das Erfassen der Fingerkuppe vom Käufer bestätigt. Auf dem Kassenbon kann der Kunde den aktuellen Stand der Zebrapunkte erkennen. Daten für die Kundenbindung werden in entsprechende Dateien abgelegt. Soll der Kassenbon durch eine Zahlung mit dem digiPROOF – System ausgeglichen werden, übergibt iCARD die zur Abwicklung notwendigen Daten wie Bankverbindung an die Kasse zurück. Die Kasse schließt den Kassenvorgang ab und übergibt den Zahlungsdatensatz an das Folgesystem ab. Mittels separat aufgestellter Kiosk – Terminals kann der Kunde sich durch das Auflegen der Fingerkuppe auf einen Scanner jederzeit darüber informieren, welchen Umsatz, welche Artikel, wie viel Zebra – Punkte und welche Prämien er bisher erworben hat. Aktuelle Angebote sind ebenfalls darüber zu erfragen. iCARD ist eine virtuelle biometrische Kundenkarte, die alle Eigenschaften und Funktionen einer physikalischen Treuekarte hat. Mit der iCARD steht dem Handel ein Instrument für Kundenbindung und Customer Relationship Management zur Verfügung. iCARD hat im Gegensatz zur realen Treuekarte den Vorteil, dass sie an den jeweiligen aktuellen Bedürfnissen angepasst werden kann, ohne dass auf Kundenseite Veränderungen notwendig sind. Deutliche Kostenvorteile, erleichterte Akzeptanz und eine schnelle Anpassung an veränderte Rahmenbedingungen sind die Folge. iCARD in Verbindung mit der Zahlart digiPROOF beschleunigt darüber hinaus den Zahlprozess an der Kasse um das 5fache gegenüber den herkömmlichen Zahlungsarten BAR oder Kreditkarte.

Besonderheit

Damit iCARD in die bestehende Kassenumgebung integriert werden konnte, musste mit dem Hersteller der Kassensoftware und des Warenwirtschaftsprogramms eine Schnittstelle programmiert werden. Alle 10 Standorte sind per VPN verbunden mit einem zentralen Server, der alle digi X Daten speichert. Alle Transaktionen finden online statt

Technische Details	
Laufzeit:	4. Quartal 2006 – Ende offen
Merkmal:	Finger
Nutzer:	5500
Transaktionen:	Identifikation 800.000 per anno
Datenträger:	Null, da virtuelle Lösung
Sensoren:	25

Kontakt

it-werke e. K., Stefan Sewöster / sewoester@it-werke.de
Rolf Biben / biben@it-werke.de

1.7 Zutrittskontrolle in einem Privathaus

Projektbeschreibung

Im privaten Anwesen eines deutschen Unternehmers sollten sämtliche Eingänge von außen sowie wichtige Türen im Haus durch biometrische Zutrittskontrolle abgesichert werden. TST Biometrics GmbH, München lieferte hierzu die benötigten berührungslosen Fingerabdrucksensoren BiRD, die Zutrittskontrolle wurde mit der Softwarelösung einer Partnerfirma realisiert.

Ziel der Umstellung auf Zugang mittels Fingerabdruck war es vor allem, eine Gefährdung des Anwesens durch verlorene Schlüssel oder Karten zu vermeiden, einen hohen Komfort für die Bewohner zu erreichen und höhere Sicherheit bei Wechsel des Hauspersonals zu bekommen.

Umsetzung

Alle mit Fingerabdrucksensor gesicherten Türen wurden mit Motorschlössern ausgestattet, die durch Türcontroller angesteuert werden. Die Fingerabdrucksensoren wurden in geeigneten witterungsgeschützten Gehäusen integriert und über Ethernetkabel mit dem zentralen Server verbunden. Die Zutrittskontrollsoftware erkennt, wenn ein Finger aufgelegt wird und löst die Aufnahme des Fingerbildes aus. Nach Vergleich des Fingerbildes mit den in der Datenbank gespeicherten Fingerdaten wird bei Erkennen einer berechtigten Person die Tür geöffnet. Für alle biometrisch gesicherten Türen können in der Software individuelle Zugangsberechtigungen festgelegt werden.

Besonderheit

Die Anwendung von biometrischer Zugangskontrolle in einem Privathaus nutzt den Vorteil der berührungslosen Fingerabdrucktechnologie von TST Biometrics. Diese Technologie eignet sich besonders dazu, bei Anwendung im Außenbereich kalte, feuchte oder verschmutzte Finger zu erfassen und zu erkennen. Ebenso werden die Finger aller Familienmitglieder insbesondere von Kindern oder älteren Personen problemlos erkannt. Neben der Zugangssicherung von außen wurden im Haus spezielle Bereiche ebenfalls biometrisch gesichert, u. a. der Pool-Raum um zu vermeiden, dass kleine Kinder unbeaufsichtigt in den Pool gehen können. Über Fingerabdruck kann bei dem System außerdem die Alarmanlage aktiviert und deaktiviert werden.

Technische Details	
Laufzeit:	Seit März 2007
Merkmal:	Fingerabdruck, berührungslos, Identifikation
Nutzer:	Ca. 25 Nutzer
Sensoren:	9 Sensoren im Innen- und Außenbereich

Kontakt:
TST Biometrics GmbH
Martin Ditscherlein
md@tst-bioemtrics.com

2 Einsatz in Unternehmen und Organisationen

2.1 Zugangssicherung des Deutscher Sparkassenverlags

Projektbeschreibung

Im Rahmen des Aufbaus des Zertifizierungsdiensteanbieters Deutscher Sparkassenverlag gemäß Signaturgesetz wurde als Zugangssicherung zu den Sicherheitsräumen ein Fingerprint-Verfahren eingeführt.

Umsetzung

Jeder Mitarbeiter besitzt einen Mitarbeiterausweis (Chipkarte mit Funkeigenschaft), welcher ihn zum Zutritt berechtigt. Bei den Sicherheitsräumen wird zusätzlich durch ein Fingerprint-Verfahren sichergestellt, dass es sich auch um den Karteninhaber handelt. Zum Austritt muss ebenfalls gebucht werden, so dass hier durch eine Bilanzierung und damit wiederum die Schaltung der Alarmsysteme möglich ist.

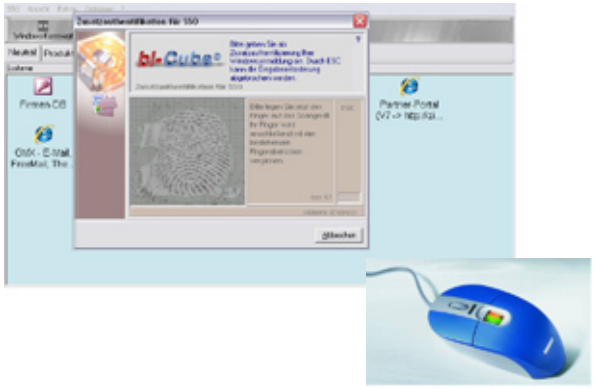
Besonderheit

Das eingesetzte Verfahren musste einer Umsetzungsprüfung gemäß Signaturgesetz durch eine Prüf- und Bestätigungsstelle stand halten.

Technische Details	
Laufzeit:	Seit Mitte 2005 produktiv
Merkmal:	Fingerprint
Nutzer:	Zur Zeit ca. 180 Personen, Tendenz steigend
Transaktionen:	Ca. 230 bis 250 Identifikationen / Tag
Datenträger:	Chipkarten
Sensoren:	Zur Zeit 17 Stück

Kontakt
Deutscher Sparkassen Verlag GmbH
Dr. Matthias Georg Stehle, matthias.stehle@dsv-gruppe.de

2.2 Single Sign On-Lösung mit Biometrie bei der Allianz Versicherung in Spanien



Projektbeschreibung

Die Allianz Seguros Spanien, die spanische Tochter der Allianz Versicherungen, hat gemeinsam mit dem Institut für System-Management (iSM) aus Deutschland und der Sopra Group Spanien, analysiert, welche biometrische SSO-Lösungen die vielfältigen Anforderungen der Allianz Seguros erfüllen.

Die Anforderungen lagen schwerpunktmäßig sowohl in der Integration der Biometrie und der bereits vorhandenen Passwortmanagementlösung als auch in der Integration der ebenfalls existierenden Portallösung. Dabei übernahm die Sopra Group als IT-Dienstleister der Allianz Seguros die Aufgabe, die verschiedenen Lösungen zu eruieren. Nach einer umfangreichen Marktrecherche wurde den Anforderungen der Allianz entsprechend, bi-Cube® SSO Lösung des Instituts für System-Management implementiert.

Umsetzung

Die Zielstellungen der Allianz Spanien waren im Wesentlichen die Verbesserung des Komforts für den Mitarbeiter und die Erhöhung der Sicherheit durch die Einführung einer biometrischen SSO-Lösung, die den Einsatz von Passwörtern generell überflüssig macht. Der Benutzer nutzt nun seinen Fingerabdruck zur Anmeldung am Betriebssystem und ebenfalls zur Anmeldung an alle integrierten Systeme.

Besonderheit

In der bisherigen IT-Landschaft musste sich jeder Mitarbeiter mindestens sechs Passworte zu verschiedenen Applikationen (u.a. SAP, Lotus Notes, 3270 Emulation) merken. Diese unterschiedlichen Applikationen waren aufgrund der Verschiedenheit der Systeme in keinem Fall im Rahmen einer Portallösung zu integrieren. Dementsprechend war der Einsatz einer qualifizierten SSO-Lösung hier zwingend notwendig, da nur mit einem entsprechenden technologischen Ansatz die verschiedenen Applikationen integriert werden konnten. Die Einführung des Fingerabdrucks zur Verifikation des Users und der Wegfall der Passwörter wurden durch die Allianz Mitarbeiter als deutliche Erhöhung des Komforts bewertet.

Technische Details	
Laufzeit:	01.11.2005 bis 01.11.2006
Merkmal:	Fingerabdruck
Nutzer:	1.500
Transaktionen:	15.000 – 20.000/Tag
Datenträger:	Fingerabdruck wird verschlüsselt (Triple DES) zentral und dezentral abgespeichert
Sensoren:	1.500

Kontakt

iSM - Institut für System- Management GmbH
Ronny Grudzinski, ronny.grudzinski@secu-sys.de

2.3 Zutrittsregelung und Zeiterfassung in einer Privatbank mit Identifikation per Iris- und 3D-Gesichtserkennung

Projektbeschreibung

Für die Schweizer Privatbank Pictet & Cie Banquiers wurde ein Zutrittskontroll- und Zeiterfassungssystem umgesetzt. Hierbei trat die Interflex AG, Schweiz, Ingersoll Rand Security Technologies als Generalunternehmer auf, während Partnerunternehmen die Gesichts- und Iriserkennungssysteme installierten. Durch die Kombination der Biometriemerkmale ist gewährleistet, dass nur berechtigte Personen nach der Überprüfung Zutritt zu sämtlichen Eingängen im Bankgebäude und in allen Übergängen zwischen den Sicherungsbereichen innerhalb des Gebäudes haben. Die endgültige Entscheidung, das Projekt in dieser Form durchzuführen, fiel nach monatelangen in situ-Tests mit der Iris- und der 3D-Gesichtserkennung mit ca. 400 Mitarbeitern. Die Tests ergaben nicht nur eine nahezu vollständige Fehlerfreiheit, sondern auch eine hohe Akzeptanz durch die Beschäftigten.

Umsetzung

Die biometrische Erkennung der Teilnehmer erfolgt ausschließlich durch Identifikation (keine Ausweise, keine Schlüssel, keine anderen ID-Mittel). Alle Komponenten integrierte Interflex in ein ganzheitliches Sicherheitssystem auf Basis seiner Software-Lösung IF-6020-Security. Die 3-D-Gesichtserkennung im Eingangsbereiche (Zutrittskontrolle und Zeiterfassung) der Bank lieferte A4Vision (jetzt Bioscrypt). Die byometric systems AG stellte die Iriserkennung für innere Hochsicherheitsbereiche wie etwa Tresorräume und Rechenzentren bereit.

Besonderheit

Die Größe der Anlage geht sowohl bei der Anzahl der ständigen Nutzer, der Anzahl der täglichen Buchungen und der Anzahl der installierten Sensoren weit über die bislang benutzten Anlagen hinaus.

Technische Details	
Laufzeit:	Projektbeginn im Frühjahr 2005. Schrittweise Installation und Inbetriebnahme bis Febr. 2007. Regelbetrieb seit März 2007
Merkmal:	Iriserkennung und 3D-Gesichtserkennung, nur per Identifikation
Nutzer:	Ca. 2500 Teilnehmer
Transaktionen:	mind. 12.000 Buchungen/Tag
Datenträger:	Keine
Sensoren:	Bisher ca. 90 3D-Gesichtserkennungskameras und ca. 70 Iriserkennungskameras

Kontakt
Interflex Datensysteme GmbH & Co. KG
Marcus Geigle, marcus_geigle@eu.irco.com
byometric systems AG
Werner Uhlenhoff, sales@byometric.com

2.4 Zutrittskontrolle Olympische Winterspiele Turin

Projektbeschreibung

Während der Olympischen Winterspiele in Turin 2006 stattete die Bundesdruckerei GmbH das „Deutsche Haus“ mit einem biometrischen Akkreditierungssystem aus. Damit sollte sichergestellt werden, dass nur Berechtigte das „Deutsche Haus“ betreten dürfen.

Vorteil für den Nutzer war, dass die Überprüfung der Identität sicherer, schneller und bequemer erfolgen konnte, als bei einer herkömmlichen Ausweiskontrolle. Der Nutzer konnte zudem den Prozess selbst steuern und alleine durchführen.

Umsetzung

Wer das Deutsche Haus betreten wollte, musste sich als erstes akkreditieren und erhielt eine biometrische ID-Karte. Das Foto und die persönlichen Daten wurden auf die Karte aufgedruckt. Außerdem mussten die Besucher Fingerabdrücke abgeben, die in einer Datenbank für die Dauer der Winterspiele gespeichert wurden.

Vor dem Betreten des Deutschen Hauses ließ der Besucher an einer Verifikationsstation am Eingang des Hauses seine Karte auslesen und gab einen Live-Fingerabdruck ab. Die Live-Daten wurden mit den gespeicherten Daten verglichen. Stimmten diese überein, wurde der Zutritt gewährt.

Besonderheit

Die Besucher des Hauses mussten auch ihre Karte auslesen lassen, wenn sie das Haus wieder verlassen. Dadurch konnte jederzeit bestimmt werden, wie viele und welche Personen sich im Deutschen Haus befinden. In einer Notfallsituation wäre das eine wichtige Information gewesen.

Besondere Herausforderungen des Projekts waren vor allem die widrigen Wetterbedingungen. Trotz Kälte, Schnee und Höhe arbeiteten die Verifikationsstationen jedoch einwandfrei.

Technische Details	
Laufzeit:	10.02.2006 bis 26.02.2006
Merkmal:	Finger
Nutzer:	5.000
Transaktionen:	80.000 Verifikationen
Datenträger:	5.000 Token
Sensoren:	8

Kontakt
Bundesdruckerei GmbH, Gregor Költzsch,
gregor.koeltzsch@bdr.de

2.5 Biometrie im Fußballstadion (Niederlande)

Projektbeschreibung

Der königliche holländische Fußballverband KNVB und die professionellen Fußballvereine ermitteln technische Möglichkeiten zur Verbesserung der Sicherheit im Umfeld von Fußballstadien. Zusammen mit drei Vereinen hat die KNVB ein Pilot-Projekt gestartet, um durch technische Maßnahmen Personen, denen Stadionverbot erteilt wurde, vom Betreten des Fußballstadions abzuhalten. Als biometrisches Merkmal wurde der Fingerabdruck verwendet.

Umsetzung

Das System wird gezielt bei Auffälligkeiten eingesetzt, so dass eine vollständige Bearbeitung aller Fußballzuschauer nicht erforderlich ist. Der Pilot zeigte die Machbarkeit des Konzepts basierend auf einer zentralen Fingerabdruck-Datenbank. Unter Beobachtung wurde von jedem Teilnehmer des Pilotversuchs ein Fingerabdruck genommen und mit allen gespeicherten Fingerabdrücken verglichen. Für den Fall, dass die Erfassung des Fingerabdrucks nicht erfolgreich war, gab es ein zweites Verfahren. Im Falle eines Treffers wurde der Besucher um den Abdruck eines anderen Fingers gebeten, um sicher zu stellen, dass es sich nicht um eine zufällige Übereinstimmung handelte. Idealerweise wird angestrebt, allmählich den Grad der Beobachtung zu reduzieren, je weiter das Projekt voranschreitet.

Um die Blacklist-basierte Funktionsweise abzubilden, wurde die Datenbank durch freiwillige Vertreter und Fans der Vereine gefüllt. Diese wurden mit allen zehn Fingern erfasst. Diese Fingerabdrücke wurden einer Datenbank von 15.000 anonymen Fingerabdrücken hinzugefügt, die die Gesamtzahl von Personen mit Stadionverbot in holländischen Stadien repräsentieren.

Besonderheiten

Die Geschwindigkeit der Aufnahme ist ein zentrales Kriterium: Der gesamte Prozess der Aufnahme, Musterextraktion und Vergleich gegen eine Datenbasis von 15.000 Fingerabdrücken bis zur Darstellung des Ergebnisses auf dem Bildschirm soll nicht länger als 3 Sekunden dauern, mit normaler Kooperation des Besuchers und unter Außenbedingungen. Der Grund ist, dass die Überprüfung den normalen Prozess des Zugangs zu den Stadien nicht verzögern darf.

Eine sehr hohe Genauigkeit ist erforderlich damit eine Person mit Stadionverbot mit hoher Wahrscheinlichkeit erkannt wird. Dadurch besteht für diese Personen ein sehr hohes prozentuales Risiko ermittelt zu werden, so dass sie möglichst schon davon abgehalten werden, überhaupt zum Stadion zu kommen.

Technische Details	
Laufzeit:	Erste Phase März 2007 bis Saisonende (Juni). Projekt wird fortgesetzt.
Merkmal:	Finger
Nutzer:	> 500 Nutzer
Transaktionen:	> 500 1:N Transaktionen im Stadion in zwei Stunden
Datenträger:	Datenbank
Sensoren:	Fingerabdruckscanner / 2 Sensoren pro Stadion

Kontakt
NEC Deutschland GmbH Identification Solutions Division
szielinski@hpce.nec.com

2.6 Stimmbiometrie im Sprachportal der Volksfürsorge Versicherungsgruppe

Projektbeschreibung

Seit Januar 2007 setzt die Volksfürsorge Versicherungsgruppe das von VOICE.TRUST entwickelte stimmbiometrische Verfahren zur Stimmverifikation in ihrem Sprachportal für Außendienstmitarbeiter ein.

Das Sprachportal von Volksfürsorge Versicherungen ermöglicht den Außendienstmitarbeitern den telefonischen Zugriff auf Adressdaten, die Abfrage von Versicherungssummen, Leistungsumfang der Policen, Zahlungsterminen und vieles mehr. Dadurch können sie sich jederzeit, auch von unterwegs, auf ihre Gespräche vorbereiten und ihren Kunden eine optimale Betreuung bieten.

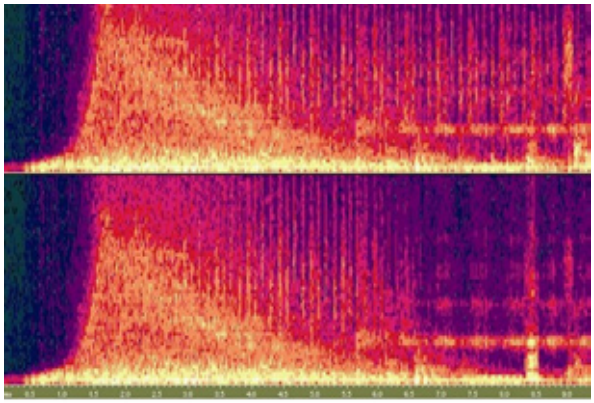
Umsetzung

Bevor der Anrufer „Zutritt“ zu dem Sprachportal erhält, muss er zunächst anhand seiner Stimme eindeutig als berechtigter Nutzer erkannt werden. Er wiederholt dazu vom System vorgegebene Begriffe, die er bei der Erstanmeldung, dem so genannten „Enrolment“, nachgesprochen hat und aus denen dabei ein Stimmprofil gebildet wurde. Zur Authentifizierung des Anrufers werden die Stimmprofile aus dem jeweiligen Anruf mit denen des Enrolments verglichen und auf dieser Basis entschieden, ob ein Anrufer zugelassen oder abgewiesen wird. Das Sprachportal wird von der D+S solutions GmbH umgesetzt und betrieben.

Besonderheit

Die Volksfürsorge Versicherungsgruppe hatte hohe Anforderungen an die Sicherheit der Authentifizierungslösung. Da die Fehlerrate für falsch erteilte Zutrittsberechtigungen bei Null liegt, genießen die Kundendaten nun höchste Sicherheit.

Hinzu kommt, dass die Automatisierung dieses Prozesses das Call-Center der Volksfürsorge Versicherungen entlastet. Da der gesamte Prozess über Sprache abgewickelt wird und der Anwender keine zusätzliche Hardware außer einem Telefon benötigt, werden außerdem Kosten gespart.



Technische Details	
Laufzeit:	Seit Januar 2007
Merkmal:	Stimme
Nutzer:	Mehr als 10.000
Transaktionen:	Mehr als 1,1 Million automatisierte Anrufe / Jahr

Kontakt

VOICE.TRUST AG, Lutz Middelkamp,
lutz.middelkamp@voicetrust.de

2.7 Stimmbiometrie für automatisiertes Passwort Reset

Projektbeschreibung

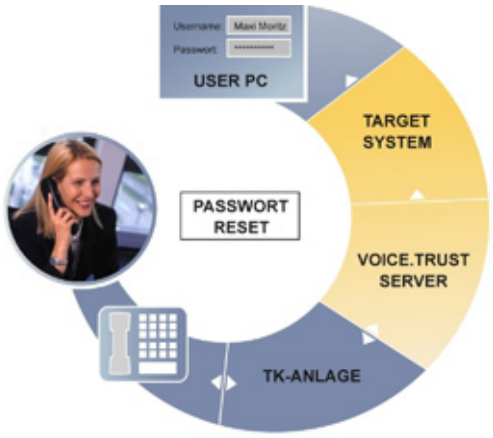
Im Rahmen eines hausinternen Verbesserungsvorschlags wurde die Volkswagen Financial Services AG 2004 auf den VOICE.TRUST Passwort Reset Service aufmerksam. Bisher bekam der Nutzer ein neues Passwort nur über eine Authentifizierung des Empfangs mittels des Werks- oder des Personal-Ausweises. Das kostete den Nutzer durchschnittlich 15 Minuten Arbeitszeit und das Unternehmen ca. 15 EUR Bearbeitungskosten.

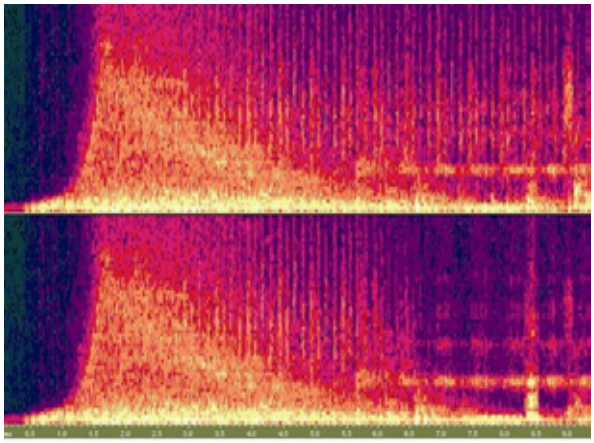
Umsetzung

In einer dreimonatigen Testphase versuchte die Volkswagen Financial Services AG das System mit Abhör-, Replay- und Zwillingsangriffen zu überlisten, ohne Erfolg. Volkswagen Financial Services AG legt besonderen Wert auf die Passwortsicherheit und entschied sich für das etwas sicherere aber auch aufwendigere Super User Rollout-Verfahren. 8 Werkstudenten brauchten 6 Wochen, um die in Frage kommenden 2.850 Nutzer persönlich anzumelden.

Besonderheit

Der Server des Systems ermöglicht über 4 Sprachkanäle Passwort Resets in Windows ADS und in über 100 SAP Systemen. Über die dreimonatige Rollout-Periode lizenzierte Volkswagen Financial Services AG weitere 4 Sprachkanäle. Ende 2007 wird Volkswagen Financial Services AG auf die Version 5 migrieren, die einen Mehrsprachen- und Mehrmandantenbetrieb auf einer Plattform erlaubt. Heute bearbeitet das System 95% der monatlich 700 Passwort Reset Anfragen für die angeschlossenen Zielsysteme. Die Investitionskosten hatten sich bereits nach 18 Monaten amortisiert.





Technische Details	
Laufzeit:	Seit August 2004
Merkmal:	Stimme
Nutzer:	Mehr als 4.100
Transaktionen:	700 Passwort Resets /Monat

Kontakt
VOICE.TRUST AG, Lutz Middelkamp
lutz.middelkamp@voicetrust.de

2.8 Absicherung PCs und Anwendungen in HNO Klinik Tübingen

Projektbeschreibung

Fingerprintauthentifizierung in der HNO-Klinik Tübingen

Umsetzung

Sicherer Zugang zu allen klinikinternen Programmen und PC-Arbeitsstationen

Besonderheit

- Eindeutige Identifizierung und Authentifizierung der Mitarbeiter der HNO Tübingen
- Einfache und praktische Handhabung
- Erleichterung des Zugangs zu den klinikinternen Programmen und PC-Arbeitsstationen
- Verringerte Kosten durch geringerem Administrationsaufwand
- Höherer Komfort für die Mitarbeiter durch Ersatz aller Passwortabfragen durch elektronische Fingerbildabgabe
- Entfall des Sicherheitsrisikos Passwort

Technische Details	
Laufzeit:	
Merkmal:	Fingerprint Authentifizierung am Server durch Siemens ID Center
Nutzer:	150
Transaktionen:	5 - 7 pro Tag und User
Datenträger:	Keine, weil biometrische Identifikation ohne Datenträger durchgeführt wird
Sensoren:	150

Kontakt

Siemens IT Solutions and Services - Biometrics Center
Siemens AG Österreich, PSE, biometrics.at@siemens.com

Ähnliche Projekte

Fingerprintauthentifizierung im Niedersächsischen Justizministerium (Finger)

Technische Details	
Laufzeit:	
Merkmal:	Fingerprint Authentifizierung am Server durch Siemens ID Center
Nutzer:	200
Transaktionen:	5 - 7 pro Tag und User
Datenträger:	Keine, weil biometrische Identifikation ohne Datenträger durchgeführt wird
Sensoren:	200

Kontakt

Siemens IT Solutions and Services - Biometrics Center
Siemens AG Österreich, PSE, biometrics.at@siemens.com

2.9 Zutrittssystem für Hochverfügbarkeits-Rechenzentrum

Projektbeschreibung

Für ein großes Hochverfügbarkeits-Rechenzentrum in NRW wurde der Zugang zum sensiblen Zentralbereich durch eine Vereinzelungsschleuse in Kombination mit biometrischer Identifikation gesichert. Besondere Voraussetzungen waren für diese Anwendung eine sehr geringe FRR bei ausgeschlossener FAR.

Nach mehreren Versuchen mit anderen biometrischen Verfahren entschied sich der Betreiber des Rechenzentrums für den Einsatz berührungsloser Fingerabdruckscanner von TST Biometrics, um eine bestmögliche Erkennungsleistung und Zuverlässigkeit bei gleichzeitig höchster Akzeptanz durch die Mitarbeiter zu erreichen.

Umsetzung

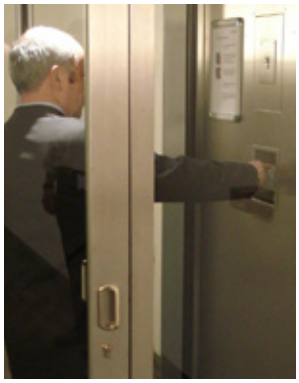
Das bisherige kartenbasierte Zutrittssystem wurde für den Zentralbereich um die biometrische Fingerabdruckerkennung erweitert. Der Außenzugang zum Gebäude des Rechenzentrums erfolgt nach wie vor mit einer RFID-Karte. Der Zutritt zum Zentralbereich mit den sensiblen Server- und Datenspeichersystemen wurde durch eine Vereinzelungsschleuse gesichert. In der Schleuse befindet sich ein berührungsloser Fingerabdrucksensor. Die Außentür zur Schleuse wird mittels RFID-Karte geöffnet. Befindet sich der Mitarbeiter in der Schleuse, muss er den Finger am Sensor auflegen. Stimmt der eingelesene Fingerabdruck mit einem in der Datenbank gespeicherten Abdruck überein, öffnet sich die Innentür der Schleuse und gibt den Zugang zum Zentralbereich frei. Andernfalls öffnet sich die Außentür erneut und die Person muss die Schleuse nach außen verlassen.

Besonderheit

Aufgrund der hohen Anforderungen an die Zuverlässigkeit des Zutrittssystems wurde besonderer Wert auf ein sorgfältiges Enrolment der Mitarbeiter gelegt. In der Praxis erwies sich dies als besonders vorteilhaft, da Erkennungsraten über 99% erreicht werden.

Technische Details	
Laufzeit:	seit Mai 2007
Merkmal:	Fingerabdruck, berührungslos, Identifikation
Nutzer:	ca. 200 Personen
Transaktionen:	> 1000 Identifikationen pro Tag
Datenträger:	k. A.
Sensoren:	k. A.

Kontakt:
TST Biometrics GmbH, Martin Ditscherlein,
md@tst-biometrics.com



3 Einsatz im öffentlichen Umfeld

3.1 Automatisierte, biometriegestützte Grenzkontrolle (ABG) am Flughafen

Projektbeschreibung

Das Bundesministerium des Innern hat 2004 auf dem Flughafen Frankfurt/Main die Einrichtung einer automatisierten und biometriegestützten Grenzkontrolle veranlasst. Die Bosch Sicherheitssysteme GmbH hat in rund vier Monaten Bauzeit am Flughafen Frankfurt, Terminal A, das ABG-System (automatisierte biometriegestützte Grenzkontrolle) eingerichtet. Interessierten Personen, deren Ein- und Ausreise grenzpolizeilich unproblematisch ist, wird im Non-Schengen-Flugverkehr das Passieren der Grenzen ohne manuelle Grenzkontrolle gestattet. Bislang haben sich mehr als 20.000 Teilnehmer - davon mehr als 1.600 Bürger aus anderen EU-Staaten - auf freiwilliger Basis in Frankfurt für das Verfahren ABG registrieren lassen.

Umsetzung

Teilnehmen kann, wer seine personenbezogenen Daten aus dem Reisepass und die biometrischen Merkmale seiner Augeniris von der Bundespolizei registrieren lässt.

Diese Daten werden bei nachfolgenden Grenzübertritten zum Nachweis der Teilnahmeberechtigung und zur biometrischen Authentifizierung benötigt. Das ABG-Verfahren stützt sich auf die maschinenlesbare Zone des Reisepasses und gliedert sich in Enrolment (Registrierung) und Autocontrol (automatisierter Kontrollvorgang beim Grenzübertritt).

Besonderheit

Die teilnehmenden Reisenden durchlaufen die etwa zehn Sekunden dauernde Iriskontrolle, und schon haben sie die Grenze passiert, ohne weitere Überprüfungen durch Grenzbeamte. Das zeitweise bis zu einer halben Stunde dauernde Anstellen an der Passkontrolle entfällt – ein großer Vorteil besonders für Vielreisende. Die mit einer sprachgestützten Benutzerführung arbeitende Grenzkontrolle erfüllt alle von der Bundespolizei gestellten Anforderungen und unterschreitet die vorgegebenen Zurückweisungsquoten.

Technische Details	
Laufzeit:	Seit 2004
Merkmal:	Iriserkennungsverfahren
Nutzer:	22.500
Transaktionen:	Darf nicht genannt werden
Datenträger:	lokale Datenbank der Bundespolizei
Sensoren:	Kameras OKI (Modell M)

Kontakt

BOSCH Sicherheitssysteme GmbH

Michael von Foerster, michael.vonfoerster@de.bosch.com

Ähnliche Projekte

Ähnliche Projekte sind weltweit realisiert: in Europa beispielsweise an den Flughäfen Heathrow (GB), Schiphol (NL), Charles de Gaulle (F)

3.2 Identitätsüberprüfung Ausweis & Reisepass Pakistan

Projektbeschreibung

Pakistan nutzt seit 2004 eine der größten Gesichtserkennungsdatenbanken weltweit zur Bekämpfung von Identitätsbetrug mit gefälschten Dokumenten. Das Land hat im Rahmen des nationalen Personalausweis- und Reisepassprogramms eine Bilddatenbank aufgebaut, die derzeit ca. 50 Millionen Einträge umfasst. Bei jedem Antrag für neue Ausweise bzw. Reisepässe wird die Identität des Antragstellers überprüft und damit die Ausstellung von Dokumenten an falsche Personen bzw. die Mehrfachausstellung an dieselbe Person verhindert.

Umsetzung

Bei Projektbeginn wurde das zunächst vorhandene Bildmaterial von ca. 34 Millionen Bildern erfasst, in einer Lichtbilddatenbank zentral abgelegt und abschnittsweise auf Mehrfacheinträge überprüft, um die Datenbank zu bereinigen. Seitdem wird von jedem neuen Antragsteller ein Bild aufgenommen und per 1:1 Verifikation mit dem für diese Person gespeicherten Referenzbild verglichen (sofern er/sie bereits zuvor ein Ausweisdokument beantragt hatte und damit bereits erfasst ist), um die Identität des Antragstellers zu bestätigen.

Besonderheit

Zusätzlich wird der gesamte Datenbestand täglich nach Dubletten durchsucht, um sicherzustellen, dass Mehrfachanträge einer Person unter verschiedenen Namen entdeckt werden. Auf diese Weise werden täglich bis zu 21.000 Fotos neuer Antragsteller bearbeitet und mit der gesamten Bilddatenbank verglichen. Dabei verzeichnen die Behörden bis zu 250 Betrugsversuche pro Tag und verhindern die weitere Bearbeitung betrügerischer Anträge und die Ausstellung mehrerer Dokumente an eine Person.

Im Juli 2005 teilte NADRA den Inhabern mehrerer Ausweisdokumente in einer landesweit veröffentlichten Meldung in Pakistans wichtigsten Zeitungen mit, dass ihre Mehrfacheinträge entdeckt wurden und sie strafrechtlich verfolgt würden, wenn sie ihre fälschlicherweise erhaltenen Ausweise nicht zurückgeben.

Technische Details	
Laufzeit:	Seit 2004
Merkmal:	Gesicht
Nutzer:	50 Millionen Einträge in der Datenbank
Transaktionen:	Vergleich von bis zu 21.000 Bildern pro Tag mit der kompletten Bilddatenbank
Datenträger:	k. A.
Sensoren:	k. A.

Kontakt

L-1 Identity Solutions AG, Katrin Booms, kbooms@l1id.com

3.3 Identitätsüberprüfung Polizeibehörde, Pinellas County, Florida, USA

Projektbeschreibung

Die Polizeibehörde in Pinellas County, Florida, USA setzt seit 2000 Gesichtserkennung zur Identifizierung von Straftätern, in der polizeilichen Fahnung und in der Strafverfolgung ein.

Umsetzung

Der Schwerpunkt des Projektes lag zunächst darauf, die Bilder von Häftlingen bei der Einweisung in die Justizvollzugsanstalt von Pinellas County aufzunehmen und unter Verwendung dieser Bilder eine Gesichtserkennungsdatenbank als Grundlage für weitere Anwendungen aufzubauen. Das bei der Einweisung aufgenommene Bild wird zum einen in der Akte der jeweiligen Person gespeichert und zum anderen für einen Datenbankabgleich verwendet. Sofern die Person schon einmal erkennungsdienstlich behandelt wurde und somit im Datenbankbestand der Polizei vorhanden ist, haben die Beamten direkten Zugriff auf die gespeicherten Daten. Vor der Entlassung wird wiederum eine Verifikation per Gesichtserkennung durchgeführt, um die Identität der Person eindeutig sicherzustellen. Auch die Beamten außerhalb der Justizvollzugsanstalt haben Zugriff auf die zentrale Gesichtserkennungsdatenbank, um beispielsweise in der Fahndung Bilder von Verdächtigen mit der Datenbank abzugleichen. Des Weiteren ermöglicht ein mobiles System in den 50 Streifenwagen der Beamten die direkte Identitätsüberprüfung einer verdächtigen Person, die z.B. kein Ausweisdokument mit sich führt, vor Ort. Darüber hinaus setzt die Polizeibehörde in Pinellas County biometrische Videoüberwachungssysteme am Flughafen, im Gerichtsgebäude und im Besucherzentrum der Justizvollzugsanstalt ein.

Besonderheit

Durch die Vernetzung der Gesichtserkennungstechnologie und der Lichtbilddatenbank hat sich die Gesichtserkennung in Pinellas County als effizientes Mittel für die Personenidentifikation erwiesen und ist zwischenzeitlich zu einer robusten Komplettlösung geworden, welche die Vorteile der Gesichtserkennung in verschiedenen Anwendungen umfassend nutzt.

Technische Details	
Laufzeit:	Seit 2000
Merkmal:	Gesicht
Nutzer:	k. A
Transaktionen:	4.000 Identitätsprüfungen pro Tag
Datenträger:	k. A.
Sensoren:	k. A.

Kontakt

L-1 Identity Solutions AG, Katrin Booms, kbooms@l1id.com

3.4 Visa Information System BioDev II

Projektbeschreibung

BioDev II wird als Nachfolgeprojekt des von Frankreich und Belgien durchgeführten BioDev I Projekts zur Vorbereitung des zukünftigen europäischen VIS (Visa Information System) durchgeführt. Teilnehmer sind ein Konsortium von acht Europäischen Staaten - Österreich, Belgien, Frankreich, Deutschland, Luxemburg, Portugal, Spanien und Großbritannien.

Vorgesehen ist eine Erfassung der biometrischen Merkmale (zehn Finger und Gesichtsbild) von Visa-Antragstellern im Ausland und nachfolgend eine 1:1- und 1:N-Überprüfung bei der Ankunft an den Außengrenzen des Schengen-Raumes.

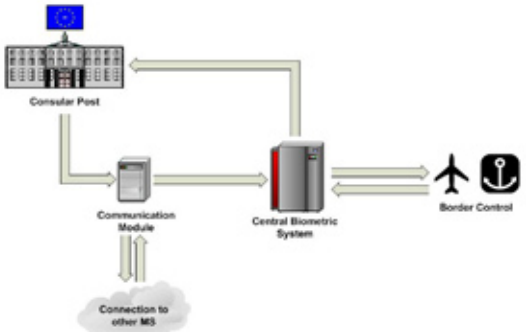
Umsetzung

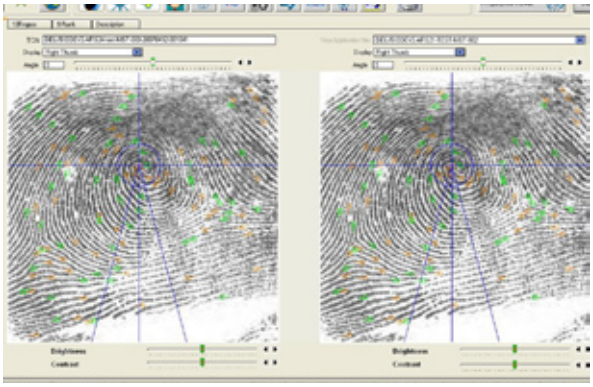
NEC hat ein kombiniertes Back-end AFIS Systems für Deutschland und Belgien geliefert. Das AFIS-System speichert die biometrischen Daten aller VISA-Anfragen der Front-end-Installationen der beiden Staaten und anderer Mitgliedsstaaten. Späten kann dann eine Verifikation und Identifikation aller Besucher mittels biometrischer VISA an den Grenzen der beiden Staaten durchgeführt werden.

Besonderheit

Die Pilotinstallation hat für eine verstärkte Zusammenarbeit zwischen den Botschaften der teilnehmenden Staaten gesorgt. Zur Zeit wird geprüft, ob sich Möglichkeiten der Einsparung durch gemeinsame Ressourcennutzung in europäischen Botschaften ergeben können.

Weitere Zielsetzungen des Projektes ist die Sammlung von Erfahrungen in der biometrischen Erfassung und Überprüfung, Erforschung von organisatorischen Konsequenzen in Botschaften und Grenzstellen, die Prüfung einer internationalen Interoperabilität von Ausrüstung, Software und Prozessen insbesondere auch im Hinblick auf ergonomische Eigenschaften und die Sicherstellung der Einhaltung internationaler Standards des europäischen Visa Informations Systems (V.I.S.).





Technische Details	
Laufzeit:	April 2007 bis April 2008 (möglicherweise länger)
Merkmal:	Finger
Nutzer:	20.000 über die Projektlaufzeit erwartet
Transaktionen:	Bis 200 pro Tag
Datenträger:	Zentrale Datenbank
Sensoren:	Fingerabdruckscanner / anfänglich 22 Sensoren

Kontakt

NEC Deutschland GmbH, Identification Solutions Division, szielinski@hpce.nec.com

3.5 Mexiko AFIS für die Steuerbehörde

Projektbeschreibung

Die Mexikanische Steuerbehörde hat den Unternehmen die Möglichkeit eingeräumt viele Transaktionen elektronisch abzuwickeln, mittels Vergabe einer Elektronischen Signatur an eine Physische Person die für die Juristische Person, das Unternehmen, zeichnet. Das System zur Erfassung der Daten inklusive eines AFIS (Automated Fingerprint Identification System) wurde im Jahr 2003 international ausgeschrieben. DERMALOG mit 2 Partnerfirmen in Mexiko gewann im Dezember 2003 die Ausschreibung bei der auch ein Benchmark während des Auswahlverfahrens durchgeführt wurde. Alle Unternehmer des Staates Mexiko, die eine Elektronische Signatur beantragen, werden biometrisch erfasst. Erst nachdem das DERMALOG AFIS festgestellt hat, dass der Antragsteller in der AFIS Datenbank einmalig vorhanden ist, wird die Elektronische Signatur an ihm vergeben. Der Unternehmer kann z.B. damit die Steuererklärungen des Unternehmens elektronisch abgeben. Ferner gab es in Mexiko häufig Fälle, dass ein Unternehmer nach einem Konkurs unter anderem Namen eine neue Firma eröffnete, ohne die alten Steuerschulden zu begleichen. Das DERMALOG AFIS wird auch dazu genutzt, auf Basis der Fingerabdrücke die richtige Identität dieser Unternehmer festzustellen.

Umsetzung

Es wurden landesweit 147 Erfassungsstellen ausgestatten mit Fingerabdruck Live Scanner, Digital Kameras, Unterschrift Pads, Computer und Flachbettscanner. Es werden 10 flache Fingerabdrücke, 1 Photo und 1 Unterschrift digital aufgenommen, sowie die Alphanumerischen Daten und auch Unternehmens bezogene Daten. Die 147 Erfassungsstellen sind Online mit der AFIS Zentrale verbunden. Die Implementierung erfolgte in knapp 6 Monaten, das System konnte termingerecht Live gehen.

Besonderheit

Das System muss in wenigen Minuten das Resultat liefern, insgesamt soll der Erfassungsprozess nicht länger als 15 Minuten dauern.

Technische Details	
Laufzeit:	Seit Juli 2004 bis heute
Merkmal:	Finger
Nutzer:	Steuerbehörde in Mexiko
Transaktionen:	Ca. 4.000 am Tag
Datenträger:	Keine
Sensoren:	Insgesamt 147 Live Scanner und Flachbettscanner

Kontakt
DERMALOG Identification Systems GmbH
Oliver von Treuenfels, treuenfels@dermalog.de

3.6 ID Card Projekt mit AFIS in Rio de Janeiro

Projektbeschreibung

Ende der 90 Jahre entschied die Regierung des Bundesstaates Rio de Janeiro in Brasilien den Prozess zur Vergabe von Personalausweise zu modernisieren. Dabei sollten die Fingerabdrücke, die bei jedem Personalausweisantrag aufgenommen werden, über ein AFIS (Automated Fingerprint Identification System) überprüft werden. Aus dem Vorhaben resultierte eine Internationale Ausschreibung, die DERMALOG innerhalb eines Konsortiums mit 2 anderen Partnern im Jahr 1998 gewonnen hat. Inzwischen, 9 Jahre später, sind ca. 6 Millionen Personen in der AFIS Datenbank mit ihren 10 Fingern erfasst. Täglich kommen ca. 5.000 Personen hinzu. Das System vergleicht somit täglich 50.000 neue Fingerabdrücke gegen 60 Millionen Fingerabdrücke der AFIS Datenbank und liefert die Ergebnisse innerhalb von 8 Stunden. Jährlich werden im Schnitt ca. 15.000 falsche Identitäten mit dem System verhindert.

Umsetzung

Es werden 10 gerollte Fingerabdrücke aufgenommen, Photo und Unterschrift, sowie die Alphanumerischen Informationen. Die Daten kommen von insgesamt 430 Erfassungsstellen, teilweise in digitaler Form, überwiegend aber in Papierform. In der Zentrale werden alle Daten ausgewertet und erst nachdem vom AFIS keine Duplikate festgestellt wurden, werden die ID-Karten personalisiert. Die biometrischen Merkmale werden auch in Form eines 2D-Barcode für künftige 1:1 Verifikationen auf der ID-Karte festgehalten.

Besonderheit

Es handelt sich um das größte AFIS in Lateinamerika und um eine der größten AFIS-Installationen in der Welt. An das System sind mehrere Behörden angeschlossen, außer den Antragstellen für den Personalausweis sind auch Polizeistationen, Notare, Justizbehörden zwecks Verifikationen, angeschlossen. Demnächst kommen auch noch Schulbehörden und Universitäten hinzu.

Technische Details	
Laufzeit:	Seit März 1999 bis heute
Merkmal:	Finger
Nutzer:	Diverse Behörden des Bundesstaates Rio de Janeiro
Transaktionen:	Ca. 5.000 Identifikationen am Tag und ca. 1.000 Verifikationen am Tag
Datenträger:	Ca. 6 Millionen Personalausweise mit 2D Barcode
Sensoren:	Insgesamt 430 Live Scanner und Flachbettscanner

Kontakt
DERMALOG Identification Systems GmbH,
Oliver von Treuenfels, treuenfels@dermalog.de

3.7 Multibiometrie in deutschen Auslandsvertretungen

Projektbeschreibung

Im Rahmen dieses Projekts wurde in 2007 für das deutsche Auswärtige Amt eine multibiometrische Lösung entwickelt, die die Verarbeitung biometrischer Daten von Fingern, Gesicht und der handgeschriebenen Unterschrift zur Beantragung von Reisedokumenten (Reisepässe) weltweit bei den rund 220 deutschen Auslandsvertretungen (Botschaften, Generalkonsulate, Konsulate, ständige Vertretungen u .w.) ermöglicht.

Seit dem 01.11.2007 ist somit die Beantragung elektronischer Reisedokumente basierend auf einer einheitlichen biometrischen Plattform möglich und anpassbar hinsichtlich zukünftiger Anforderungen an biometrische Systeme und Komponenten.

Umsetzung

Die Umsetzung der Lösung erfolgte in eine geeignete Gesamtarchitektur mit folgenden Systemkomponenten:

- Einheitliche biometrische Plattform (secunet biomiddle)
- 4-Finger-Scanner (ePass und Visa)
- Erfassung der Gesichtsbilder und Unterschriften per Scan
- Qualitätsprüfung der biometrisch erfassten Daten von Fingern und Gesicht
- Kodierung der Finger- und Gesichtsdaten erfolgt nach TRPDÜ
- Umsetzung über BioAPI 2.0 für alle eingesetzten Geräte und sonstige Komponenten (SW+HW)

Besonderheit

Insbesondere die Forderung des Auftragnehmers nach einer einheitlichen biometrischen Plattform für zukünftige (biometrische) Erweiterungen und die weltweite Einführung der biometrischen Systeme stellten eine besondere Herausforderung dar. Eine wesentliche Erweiterung, die der Auftraggeber fordert, ist die Anwendbarkeit für Visa-Beantragungen, welche bereits in einem EU-Pilotprojekt „BIODEV II“ zum Einsatz kommt.

Technische Details	
Laufzeit:	2007 (Dauer des Entwicklungs- und Einführungsprojekts) seit 01.11.2007 produktiv
Merkmal:	Finger, Gesicht
Nutzer:	Alle deutschen Staatsbürger, die bei einer deutschen Auslandsvertretung einen Reisepass beantragen.
Transaktionen:	Insgesamt ca. 200.000 Antragsteller pro Jahr weltweit.
Datenträger:	Elektronische Reisepässe
Sensoren:	600-1000 Fingerabdrucksensoren

Kontakt
secunet Security Networks AG
Marco Breitenstein
biometrics@secunet.com

4 Entwicklungsprojekte

4.1 3D Face

Projektbeschreibung

Inhalt des von der EU geförderten Projekts 3D Face ist die Entwicklung und der Test von Soft- und Hardwarekomponenten für die dreidimensionale Gesichtserkennung. Dazu hat sich ein Konsortium von 12 europäischen Partnern zusammengeschlossen.

Die Nutzung von dreidimensionalen Erkennungssystemen verspricht erhebliche Leistungssteigerungen für die Zugangs- und Grenzkontrolle. Durch die Kombination von exakten Informationen zum Profil sowie zu Gesichtsfarbe und -struktur können 3D-Erkennungssysteme Positionsänderungen besser verarbeiten. Auch der Unterschied zwischen realer Person und Fotografie ist für das System sofort ersichtlich. Zusammen mit der klassischen zweidimensionalen Gesichtserkennung ist das Verfahren daher sicherer und robuster als die zweidimensionale Gesichtserkennung allein.

Umsetzung

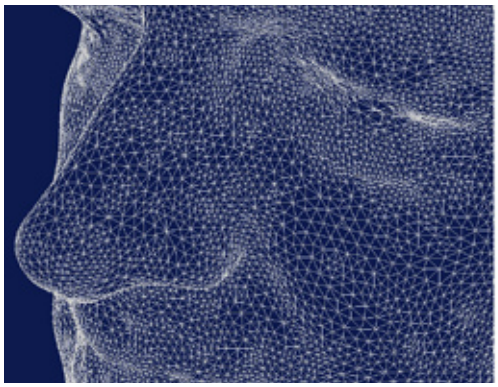
Die Bundesdruckerei GmbH ist Projektpartner und für den Test der Komponenten unter realen Bedingungen verantwortlich. Die im Projekt entwickelten Soft- und Hardwarekomponenten wird die Bundesdruckerei in ein Gesamtsystem integrieren und anschließend das System zur 3D Gesichtserkennung an den Flughäfen Berlin Schönefeld und Salzburg installieren.

Die biometrischen Referenzmerkmale werden auf einer kontaktlosen Chipkarte gespeichert und für den Vergleich mit dem Live-Merkmal mit dem VISOTEC Dokumentenprüfgerät der Bundesdruckerei ausgelesen.

Besonderheit

Im Rahmen des Projekts wurde eine End-User Group eingerichtet. Die Teilnahme an dieser ist Interessierten jederzeit möglich. Weitere Details dazu finden sich unter: www.3DFace.org

3D Face
Biometric Research



Technische Details	
Laufzeit:	01.04.2006 – 31.03.2009
Merkmal:	Gesicht
Mengengerüst:	noch offen
Weblink:	www.3DFace.org
Projekt-finanzierung	DG Information Society and Media ICT for Trust and Security Unit www.cordis.europa.eu/ist/trust-security/index.html
Call:	FP6-2004/IST/4

Kontakt

Bundesdruckerei GmbH, Björn Brecht, brecht@bdr.de

4.2 Zurechenbarkeit von Aktionen in virtuellen Welten

Projektbeschreibung

Ziel dieses vom Bundesministerium für Forschung und Bildung geförderten Projektes unter Beteiligung von Fraunhofer SIT, Fraunhofer IIS, Fraunhofer IPK, Fraunhofer IGD und Giesecke & Devrient war es, durch Nutzbarmachung biometrischer Verfahren für die Benutzerauthentisierung auf Signaturkarten die Zurechenbarkeit elektronischer Signaturen zu Personen zu verbessern und durch eine vertrauenswürdige, vor Manipulationen geschützte Signierumgebung sicherzustellen, dass beim elektronischen Signieren gilt „what you see is what you sign“.

Umsetzung

Der Prototyp eines Trusted Signature Terminals (TST) bedient sich existierender PC-Komponenten als Benutzerschnittstelle: Bildschirm, Tastatur und Maus des PCs werden direkt an das TST angeschlossen. Außerhalb des Signiermodus verbindet das TST sie mit dem PC, im Signiermodus übernimmt das TST jedoch die alleinige Kontrolle über diese Komponenten, um Manipulation über den PC auszuschließen.

Besonderheit

Eine Signaturkarte wurde um Fingerabdruck-On-Card-Matching-Software erweitert und so angepasst, dass in der Antwort auf Signaturerzeugungskommandos angezeigt wird, ob das biometrische oder das wissensbasierte Verfahren zur Benutzerauthentisierung eingesetzt wurde. Um Replay-Angriffe zu verhindern, sind die biometrischen Daten an der Kartenschnittstelle kryptographisch geschützt. Ein erster Prototyp eines On-Card-Matching-Verfahrens für handgeschriebene Unterschriften wurde erfolgreich auf Java-Karten implementiert. Für weitere Informationen siehe http://zavir.sit.fraunhofer.de/.

Technische Details	
Laufzeit:	April 2001 – Dezember 2003
Merkmal:	Finger, Unterschrift

Kontakt
Fraunhofer-Institut für Sichere Informationstechnologie
Dr.-Ing. Olaf Henniger, olaf.henniger@sit.fraunhofer.de

4.3 Verisoft Teilprojekt 4 Biometrisches Identifikationssystem

Projektbeschreibung

Ziel des Projekts Verisoft „Beweisen als Ingenieurwissenschaft“ war die Sicherheitsevaluierung von Systemen mit Formalen Methoden durchgehend von der Hardware bis zur Hochsprache. Teilprojekt 4 umfasste eine Chipkartenbasierte Identifikationssystem mit biometrischer Verifikation.

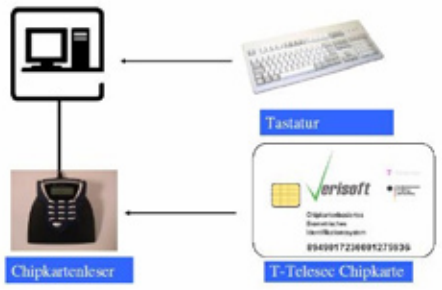
Verisoft ist ein vom BMFB gefördertes Forschungsgroßprojekt an dem unter der Leitung der Uni Saarbrücken zahlreiche Universitäten, Forschungsinstitute und Industriepartner teilnehmen (Näheres www.tetetrust.de).

Umsetzung

Es wurde ein Sicherheitsprotokoll zur Identifikation mit Biometrie und Chipkarten erstellt und formal verifiziert. Danach wurden verschiedene Implementierungen erstellt, die gegen die Spezifikation mit formalen Methoden geprüft wurden. Dabei mussten um eine durchgehende Verifikation zu erreichen, verifizierbare Implementierungen erstellt werden, die auf einen formal verifizierten Prozessor und unter einem formal verifizierten Betriebssystem funktionieren.

Besonderheit

Biometrische Verfahren haben bekanntlich immer einen Restfehler und sind daher nicht direkt mit formalen Methoden verifizierbar. Durch Kombination mit anderen Authentifikationsmitteln konnte aber ein Protokoll konstruiert und verifiziert werden, das diese Schwächen weitgehend ausgleicht und alle Sicherheitsziele erreicht. Zu diesem Ergebnis gab es mehrere Veröffentlichungen (u. a. 25. International Conference on Computer Safety, Reliability and Security, GI Sicherheit 2006).



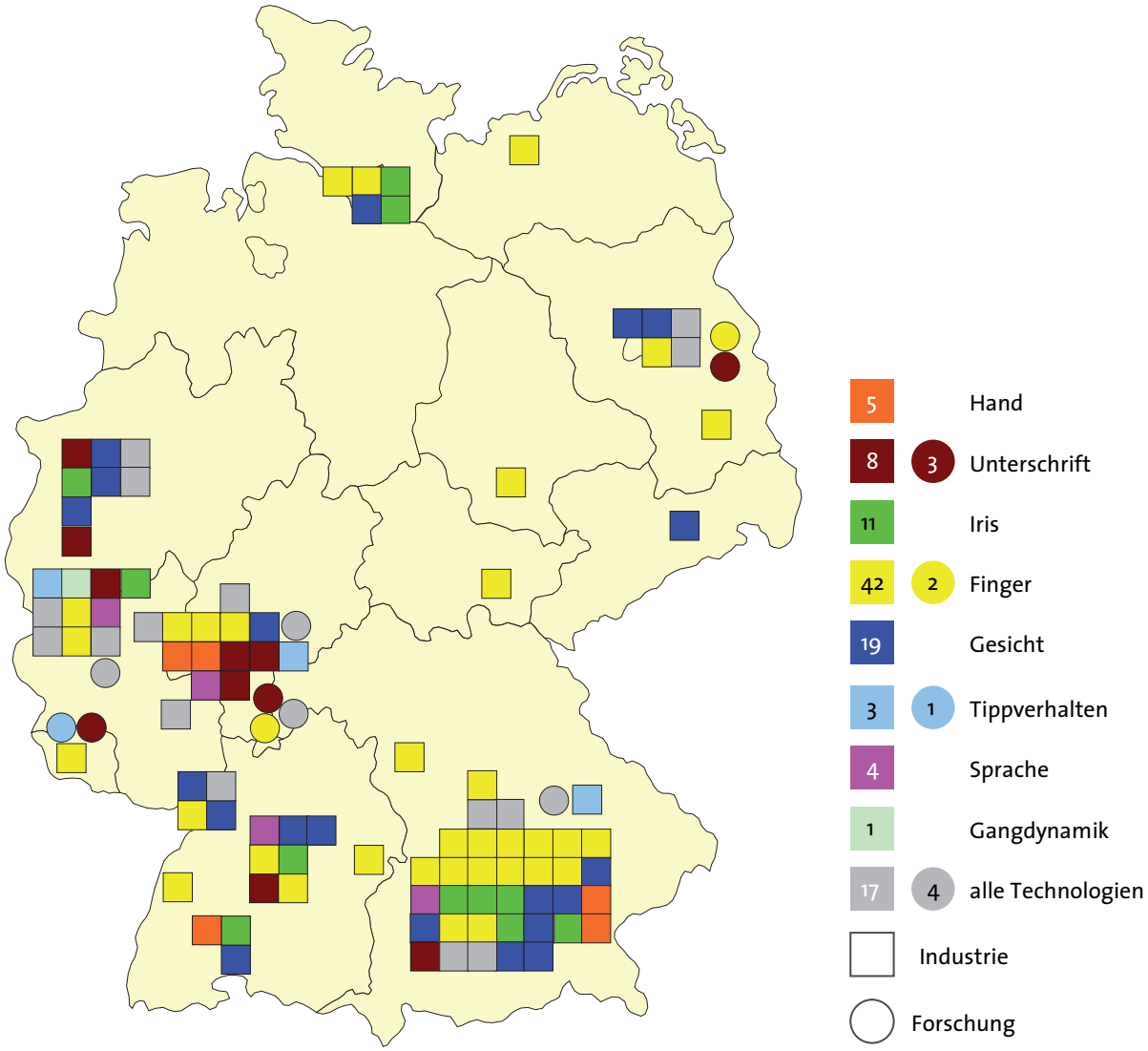
Technische Details	
Laufzeit:	Teilprojekt 4 von 01.07.03 bis 01.07.07
Merkmal:	Tippdynamik
Nutzer:	Ca. 30
Transaktionen:	Nicht erfasst
Datenträger:	40 Chipkarten
Sensoren:	Ca. 30

Kontakt

T-Systems Enterprise Services GmbH; SI, SL Security
Dr. Gunter Laßmann, Gunter.Lassmann@t-systems.com

Anhang

Landkarte Biometrie: Überblick über das Anbieter- und Leistungsspektrum



Download der aktuellen „Landkarte Biometrie“ im Internet unter: http://www.bitkom.org/files/documents/Flyer_Landkarte_Biometrie_-_V6.0_de.pdf

Deutsche Forschung im Bereich Biometrie

- Fraunhofer-Institut für Biomedizinische Technik IBMT
  Bertram Bresser / bresserb@ibmt.fhg.de / www.ibmt.fhg.de
- Fraunhofer-Institut für Grafische Datenverarbeitung IGD
  Alexander Nouak / Alexander.nouak@igd.fraunhofer.de / www.igd.fraunhofer.de/igd-a8/
- Fraunhofer Institut für Sichere Informationstechnologie SIT
  Olaf Henniger / Olaf.henniger@sit.fraunhofer.de / www.sit.fraunhofer.de
- Fraunhofer Institut für Produktionsanlagen und Konstruktionstechnik IPK
  Jochen Verhasselt / Jochen.verhasselt@ipk.fhg.de / www.ipk.fhg.de
- Institut für biometrische Identifikationssysteme
  Michael Behrens / mail@biometrics-institute.com / www.biometrics-insitute.com
- Psychologisches Institut der Universität zu Köln
  Gary Bente / bente@uni-koeln.de / www.uni-koeln.de/phil-fak/psych/diff/index.html
- Büro für Technikfolgenabschätzung beim Deutschen Bundestag
  Thomas Petermann / buero@tab.fzk.de / www.tab.fzk.de
- Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel
  Gerrit Hornung / gerrit.hornung@uni-kassel.de / www.uni-kassel.de/fb7/oeff_recht/

Weiterführende Links

- Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren:
  www.teletrust.de
- European Biometric Forum
  http://www.eubiometricforum.com/index.php?option=content&task=view&id=29&Itemid=46
- Biometrics Working Group
  http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=4
- International Biometric Group
  http://www.biometricgroup.com/reports/public/basic_reports.html
- International Civil Aviation Organization
  http://www.icao.int/index.html
- International Organization for Standardization
  http://www.iso.ch/iso/en/aboutiso/introduction/index.html#two
- BioAPI Consortium
  http://www.bioapi.org/index.asp
- Biometric Consortium
  Background of the US Government‘s Biometric Consortium
  http://www.biometrics.org/REPORTS/CTST96/
- National Biometric Security Project
  http://www.nationalbiometric.org
- International Biometric Industry Association
  www.ibia.org

- International Association for Biometrics
  http://www.afb.org.uk/docs/members.htm
- International Biometric Foundation
  http://www.ibfoundation.com
- DIN - Deutsches Institut für Normung
  http://www2.din.de
- Bundesbeauftragter für den Datenschutz
  http://www.bundesdatenschutz.de/

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.100 Unternehmen, davon 850 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org