SECURITY SOLUTIONS BIOMETRICS

BACKGROUNDER

Biometrische Sicherheitslösungen von NEC

Inhalt

BACKGROUNDER

Biometrie – was ist das?

Der Begriff „Biometrie“ hat seinen Ursprung im Griechischen und setzt sich zusammen aus den Worten „bios“ (Leben) und „metron“ (Maß). Biometrie bezeichnet somit die Lehre von der Vermessung körpereigener Eigenschaften. In Bezug auf die Informationstechnologie umfasst der Begriff die automatisierte Methode zur Identifizierung oder Überprüfung eines Individuums basierend auf physischen oder verhaltenstypischen Merkmalen und Kriterien. Biometrische Merkmale lassen sich unterteilen in aktive, verhaltenstypische Merkmale und Eigenschaften, wie z.B. Sprache, Bewegungsmuster, Anschlagdynamik auf Tastaturen oder Unterschriftendynamik. Passive, physiologische Merkmale umfassen u.a. Fingerabdruck, Gesichtserkennung, Iris- oder Retinamuster, Handgeometrie, Ohrform und Venenstruktur. Während aktive Merkmale sich ändern können, bleiben passive Merkmale ein Leben lang nahezu konstant. Auch die menschliche DNA, der so genannte genetische Fingerabdruck oder das Blutbild zählen zu den biometrischen Merkmalen, eignen sich aber nicht unmittelbar zu Kontrollzwecken, da sie einen Eingriff in den Körper des Betroffenen bedingen. Der Einsatz von DNA-Analysen erregt immer wieder Aufsehen – vor allem wenn sie zur Lösung spektakulärer Mordfälle herangezogen wird. Dann wird der Ruf nach einer Ausweitung der bestehenden Regelungen zur DNA-Analyse lauter, Politiker fordern eine Gen-Datenbank für alle, da eine DNA-Analyse schließlich nichts anderes sei als ein Fingerabdruck. Doch ist das notwendig? Wie weit reichen die bestehenden Regelungen? Wann ist eine DNA-Analyse möglich? Eine Diskussion, die noch eine ganze Zeit lang geführt werden wird.

Warum Biometrie ?

PINs (Persönliche Identifikationsnummern) und Passwörter zur Identifikation sind in der alltäglichen Anwendung als Identifikationsmerkmal bis heute weitestgehend akzeptiert und verbreitet. So sichern viele Unternehmen ihre Netzwerke, Wissens- und Datenressourcen nach wie vor mit diesen vermeintlich sicheren, konventionellen Zugangslösungen. Dabei ist jedoch zu bedenken, dass hier nur die PIN oder das Passwort erkannt werden, jedoch nicht die Person, die diese einsetzt. Auch Privatpersonen vertrauen, mangels Alternativen, weiter auf PINs. Angesichts von zahlreichen Betrugsfällen mit rechtswidrig eingesetzten Passwörtern oder PINs bedeutet dies aber auch, dass einem möglichen Missbrauch Tür und Tor geöffnet sind, da PIN oder Passwort sehr leicht auszuspionieren und ohne Wissen des eigentlichen Inhabers verwendet werden können.

Im Gegensatz dazu sind biometrische Merkmale nicht übertragbar, können auch nicht unbeabsichtigt weitergegeben werden und stellen eine eindeutige, personengebundene Identifikations- oder Verifikationsmöglichkeit dar, die Geheimzahlen und Kennwörter zunächst ergänzen und künftig ersetzen werden. Die heutigen Möglichkeiten biometrischer Technologien und Lösungen sind äußerst vielfältig, den einst effektvoll inszenierten Einsätzen in diversen Hollywood-Filmen sind längst praxisorientierte, reale Anwendungen gefolgt, die das Stadium des Experimentellen verlassen und sich in der Praxis bewährt haben. Biometrie wird heute von vielen namhaften Experten als einzig sicheres Verfahren angesehen, welches die zweifelsfreie Identifikation oder Verifikation von Personen gewährleistet.

NEC unterteilt das Feld für biometrische Sicherheitslösungen in die Marktsegmente „Law Enforcement“, „National ID“ und „Commercial“. Entsprechend vielfältig sind die möglichen Einsatzbereiche für Biometrie. Biometrische Systeme sind auf dem besten Wege, sich verstärkt den Markt für kommerzielle Sicherheits-Anwendungen bis hin zum Privatanwender zu erschließen. Kommerzielle Lösungen reichen, im Zusammenspiel mit einer fälschungssicher verschlüsselten Smart Card, von der Zutrittskontrolle zu Gebäuden über den Zugang zu Computernetzwerken, Single-Sign-On, Bezahlfunktionen in der Betriebskantine bis hin zu kostengünstigen Applikationen im Gesundheitswesen. In der kriminalistischen Ermittlungsarbeit sind biometrische Lösungen von NEC in Form leistungsfähiger AFIS Installationen (Automated Fingerprint Identification System) seit Jahrzehnten weltweit zuverlässig im Einsatz.

Auch das Marktsegment „National ID“ gewinnt zunehmend an Fahrt. Die Bundesregierung hat inzwischen ihre Pläne zur biometrischen Ausstattung der Pässe der Bundesbürger weiter präzisiert. So könnte die Einführung der Körpermerkmale in die amtlichen Dokumente in zwei Stufen erfolgen: Die Verwendung der Gesichtserkennung auf der Grundlage des Passfotos als erstem biometrischen Merkmal in deutschen Reisepässen ist demnach weiterhin vom Herbst dieses Jahres an geplant. Digitale Fingerabdrücke sowie eine Bürgerkarte ähnliche Funktion zur Verwendung im E - Commerce auf Basis einer elektronischen Signatur könnten ab dem Jahr 2007 dazukommen. Mit beiden Maßnahmen will das Bundesinnenministerium die Fälschungssicherheit des Reisepasses auf ein bisher unbekanntes Niveau heben. Damit gewinnen auch die Themen National ID und automatisierte Grenzkontrolle eine völlig neue Dimension.

Wie funktionieren biometrische Verfahren?

Obwohl alle biometrischen Verfahren spezielle Ausprägungen und Eigenschaften haben, kann der Prozess einer Identifikation oder Verifikation allgemein wie folgt beschrieben werden. Zu Beginn des Verfahrens wird der Benutzer erstmals in das System aufgenommen. Bei diesem Vorgang, Enrolment genannt, wird ein so genanntes Referenzprofil des Benutzers erstellt, welches sich aus mehreren Messungen zusammensetzt und zusammen mit der Identität des Benutzers verknüpft und als Datensatz (Template) abgespeichert wird. Das Enrolment ist insofern von entscheidender Bedeutung, da es die Basis für eine spätere hohe Erkennungsrate bildet. Deshalb führt NEC schon beim Enrolment eines Fingerabdrucks einen entsprechenden Qualitätscheck durch, bevor das Fingerabdruckbild auf einen Chip oder in eine Datenbank gespeichert wird. Das Template enthält in stark komprimierter Form die zuvor erfassten biometrischen Daten des jeweiligen Benutzers. Während des eigentlichen Erkennungsvorganges vergleicht das gewählte biometrische Verfahren das aktuell erfasste biometrische Merkmal des Benutzers, z.B. seinen Fingerabdruck, mit dem zuvor angelegten Referenztemplate. Grundsätzlich unterscheidet man zwei Arten der Erkennung.

Bei der Verifikation wird in einem 1:1 Vergleich geprüft, ob eine Person ihre behauptete Identität besitzt. D.h., es wird geprüft, ob eine Person, die behauptet eine bestimmte zu sein,

auch den physiologischen Beweis dazu erbringen kann. In diesem Falle werden die aktuellen biometrischen Daten der Person mit ihren Referenzdaten verglichen. Da die Verifikation nur den Abgleich mit dem gespeicherten Template erfordert, ist der gesamte Vorgang sehr kurz.

Bei der Identifikation wird anhand eines 1:N Vergleiches die Identität einer Person aus der Systemdatenbank heraus festgestellt. D.h., eine zunächst unbekannte Person wird mit Hilfe der Datenbank identifiziert. Im Gegensatz zur Verifikation kann die Identifikation je nach Anzahl der gespeicherten Referenzdatensätze länger dauern. Da sich einige Merkmale im Laufe der Zeit durchaus verändern können und nicht jede Messung eines biometrischen Merkmales immer exakt den gleichen Wert ergeben wird, kommt der so genannten Toleranzschwelle eines Systems große Bedeutung zu.

Übersicht über biometrische Verfahren

Methode	Vorteile	Nachteile
Fingerabdruck-erkennung	• Hohe Sicherheit – noch nie wurden zwei Personen mit identischen Fingerabdrücken gefunden • Bewährt – wird seit über 100 Jahren von Polizeibehörden zur Aufklärung von Verbrechen eingesetzt • Hochentwickelte Technologie • Hohe Anwenderfreundlichkeit	• Anwender assoziiert u.U. kriminaltechnische Ermittlungen • Funktionsstörungen bei stark verschmutzten oder abgearbeiteten Fingerkuppen möglich • Hygienische Bedenken durch Hautkontakt mit dem Sensor
Sprach-/Stimm-erkennung	• Hohe Benutzerakzeptanz da natürliche Kommunikationsform • Stimme ist eine charakteristische, individuelle Eigenschaft • Einfache und kostengünstige technologische Anwendung	• Stimme und Sprache verändern sich mit der Zeit (z.B. infolge von Alter oder Krankheit) • Leicht manipulierbar, chirurgisch veränderbar • Computerbasierte Lösungen oftmals ungenau
Retinaerkennung	• Hohe Sicherheit – keine zwei Menschen mit identischem Netzhautmuster bekannt	• Anwenderunfreundlich • Prozedur wird oft als unangenehm empfun-

		den - Angst vor “Augenscans”
Iriserkennung	• Einzigartig – keine zwei Menschen mit identischer Irisstruktur bekannt • Hohe Genauigkeit, effizientes Verfahren • Gute Akzeptanz da kein physischer Sensor Kontakt notwendig	• relativ neue Technologie • aufwändiges Verfahren • hohe Kosten • bis 2005 patentrechtlich geschützt, dadurch Weiterentwicklung behindert
Gesichtserkennung	• Hohe Genauigkeit • effizientes Verfahren • Gute Akzeptanz, da kein physischer Sensor - Kontakt notwendig	• Gesicht verändert sich im Laufe der Zeit • Chirurgisch manipulierbar
DNA Analyse	• Einzigartigkeit des Merkmales • Selbst eineiige Zwillinge haben nicht dieselbe DNS Struktur	• Probenentnahme und Analyse zeitaufwändig und kostenintensiv • Nur sehr eingeschränkt realisierbar • Datenschutzrechtlich problematisch • Einzigartigkeit durch Möglichkeit des Klonens aufgehoben

Neben den beschriebenen biometrischen Verfahren gibt es einige weitere, durchaus interessante technologische Ansätze, wie z.B. die Unterschriftenerkennung, Keystroke, Ohrerkennung, Verfahren zur Erkennung von individuellen Bewegungsmustern, Venenstruktur etc. Alle diese Verfahren spielen zumindest zum heutigen Zeitpunkt noch keine überzeugende Rolle.

Gesetzliche Rahmenbedingungen

Der Deutsche Bundestag hat bereits am 1. Januar 2002 das „Zweite Anti-Terror-Paket“ verabschiedet, das mit einem modifizierten Pass- und Personalausweisrecht die computer - gestützte Identifizierung von Personen auf der Grundlage der Ausweisdokumente verbessern und verhindern soll, dass Personen sich mit Dokumenten ähnlich aussehender Personen ausweisen. Der Entwurf sieht im Wesentlichen vor, dass neben Lichtbild und Unterschrift mindestens ein biometrisches Merkmal in Pass und Personalausweis aufgenommen werden soll. Da herkömmliche Ausweise mit Lichtbild und Unterschrift zu leicht missbräuchlich genutzt werden können, denken derzeit viele europäische Staaten sowie die USA über die Einführung von Pässen und Personalausweisen nach, die biometrische Daten enthalten sollen.

Der Rat der Europäischen Union hat am 10. Dezember 2004 die Verordnung zur Einführung biometrischer Merkmale in Reisepässen verabschiedet. Die Ausweisdokumente müssen in Zukunft maschinenlesbare Gesichtsbilder und Fingerabdrücke enthalten. Die EU-Mitgliedsstaaten sind aufgefordert das Gesichtsbild innerhalb von 18 Monaten, die Fingerabdrücke innerhalb 36 Monate in die Ausweisdokumente der insgesamt etwa 450 Millionen EU-Bürger aufzunehmen.

Bereits im Juni 2003 hatte sich die Europäische Union darauf verständigt, biometrische Daten so schnell wie möglich in Reisedokumente aufzunehmen. Dies betraf neben Reisepässen von EU-Bürgern auch die Visa für Angehörige aus Drittstaaten. Nach vollzogener EU-Erweiterung soll ein einheitliches Visa - Informationssystem, kurz C-VIS, biometrische Daten auf Basis von Fingerabdrücken von 70 Millionen Antragsstellern aufnehmen und in einer zentralen Datenbank speichern. Die USA verlangen von den Ländern, die an dem Visa Waiver Programm teilnehmen, dass sie ein Programm zur Einführung biometrischer Pässe auf den Weg gebracht haben und dass sie bis zum Stichtag des 26. Oktober 2005 mit der Ausgabe begonnen haben. Die bisher ausgeteilten Pässe behalten ihre Gültigkeit und berechtigen auch künftig zur visumfreien Einreise. Für die Inhaber herkömmlicher und noch gültiger Pässe ändert sich durch die neuen Regelungen nichts. "Wenn der Pass vorher ausgegeben wurde und noch eine Gültigkeitsdauer von zehn Jahren hat, dann kann man mit diesem Pass weiterhin visumfrei zehn Jahre in die USA einreisen", erklärt Frank Paul, der in Generaldirektion für Immigrations-, Asyl- und Grenzangelegenheiten der EU-Kommission in Brüssel für die IT-Großsysteme zuständig ist.

Nach einhelliger Expertenmeinung macht der Einsatz biometrischer Merkmale nur dann Sinn, wenn die generierten Daten weltweit gelesen, abgeglichen oder in bereits bestehenden oder neu zu installierenden Systemen analysiert werden können. Ernsthafte Probleme mit der biometrischen Identifizierung und der Arbeitsfähigkeit der dafür benötigten großen IT-Systeme erwarten die zuständigen Regierungsstellen trotz durchaus anders lautender kritischer Stimmen nicht. Das Innenministerium verweist in diesem Zusammenhang in öffentlichen Stellungnahmen darauf, dass es "aus Gründen des Datenschutzes" in den für die Erarbeitung der technischen Spezifikationen zuständigen Gremien der Internationalen

Zivilen Luftfahrtorganisation ICAO eine "verschärfte technische Zugangskontrolle für die Chips durchgesetzt" habe. Laut den ICAO-Planungen sollen die biometrischen Merkmale auf einem Funkchip gespeichert und per Radio Frequency Identification (RFID) kontaktlos ausgelesen werden können. Der Datenschutz soll dabei durch eine "wirksame Kombination aus kryptographischer Verschlüsselung und Verwendung eines Zugangsberechtigungskontrollsystems" in Form einer Public-Key-Infrastruktur gewährleistet werden.

Biometrie aus daten- und verbraucherschutzrechtlicher Sicht

Mit dem vermehrten Einsatz biometrischer Verfahren nehmen auch die Diskussionen über mögliche datenschutz- und persönlichkeitsrechtliche Risiken zu. Dabei werden biometrische Verfahren aus datenschutzrechtlicher Sicht sehr kontrovers diskutiert. Es bleibt zunächst grundsätzlich festzuhalten, dass die Verbreitung personenbezogener Daten nur dann zulässig ist, wenn sie den geltenden rechtlichen Vorgaben entspricht oder wenn die Einwilligung der betroffenen Person vorliegt. Eine unabdingbare Voraussetzung für eine breite gesellschaftspolitische Akzeptanz biometrischer Verfahren liegt in der klar definierten Zweckbindung der durch diese Verfahren gewonnenen personenbezogenen Daten. Hier geht es nicht nur um die Frage der „funktionellen“ Akzeptanz der Technologie „Biometrie“ sondern gerade auch um deren Beherrschbarkeit.

Anders als bei der Verwendung von Passwörtern oder Geheimzahlen, erfordert die Identifizierung einer Person mittels eines biometrischen Verfahrens stets den Einsatz und die Preisgabe eines dieser Person eigenen körperlichen Merkmales. Gelingt es einerseits von entwicklungstechnischer Seite durch den Einsatz geeigneter Medien, wie z.B. Smart Cards, dass gespeicherte Daten selbst in Händen Unbefugter nicht auf ihren Ursprung zurückgeführt werden können, und regelt andererseits eine weitsichtige datenschutzrechtliche Gesetzgebung alle relevanten Einsatzbereiche, wird sich bei allen Betroffenen die Akzeptanz biometrischer Verfahren signifikant und dauerhaft erhöhen. Dies betrifft in gleichem Maße auch verbraucherschutzrechtliche Belange. So ist es durchaus im Sinne des Verbraucherschutzes, die ständig steigende Flut an Passwörtern, PINs und TANs etc. zugunsten mehr benutzerfreundlicher Systeme einzudämmen, solange diese grundsätzlich jedem Nutzer den Zugang zu diesen Systemen und Lösungen ermöglichen. So dürfen z.B. Nutzer, bei denen ein gefordertes biometrisches Merkmal nur schlecht ausgebildet oder gar nicht vorhanden ist, nicht gegenüber den anderen Nutzern benachteiligt werden.

Von entscheidender Bedeutung dürfte jedoch sein, dass die globale Diskussion, die von Biometrie-Befürwortern und deren Gegnern geführt wird um eine kontroverse aber stets sachliche Ausrichtung bemüht ist. Ein Beispiel dafür mag die Stellungnahme des Menschenrechtsbeauftragten in der Russischen Föderation, Wladimir Lukin, sein. Lukin sieht in der Einführung von Personalausweisen mit biometrischen Erkennungsmerkmalen per se keinen Verstoß gegen die Menschenrechte. „Die Einführung dieser Erkennungsmerkmale sind nicht als ein Verstoß gegen die in der Verfassung der Russischen Föderation verankerten Menschenrechte zu betrachten, auch nicht als Verletzung des Rechts auf

Unantastbarkeit des Privatlebens und des Rechts auf Überzeugungsfreiheit. Natürlich unter dem Vorbehalt, dass dies dem Gesetz entspricht", geht aus Lukins Botschaft an die Gegner der Einführung von Dokumenten mit Biometrie-Merkmalen. Lukin weiter:

„Ich bin der Ansicht, dass es sich bei der Aufnahme von biometrischen Daten (nämlich Foto einer Person, deren verbale Beschreibung, Größe, Augen- und Haarfarbe, Fingerabdruck, Iris-Struktur usw.) in die Pässe der Bürger der Russischen Föderation lediglich um die Fixierung der individuellen Merkmale des Menschen handelt, die ihm von Geburt an eigen sind", so Lukin in seiner Botschaft. Die Einführung von Personalausweisen mit biometrischen Erkennungsmerkmalen biete Lukin zufolge die Möglichkeit, effektiver gegen solche Verbrechen wie Terrorismus, Geiselnahme, Handel mit Frauen und Kindern vorzugehen. (aus: Russland Online, 11.10.2004).

Aus daten- und verbraucherschutzrechtlicher Sicht entscheidend ist es, die Nutzer biometrischer Verfahren über Chancen, Risiken und potenzielle Nachteile gleichermaßen frühzeitig aufzuklären. Die sich hieraus ergebende Transparenz wird der „neuen Technologie“ Biometrie sicher förderlich sein.

Biometrische Schlüsseltechnologie von NEC

Fingerabdruckerkennung - Law Enforcement

NEC begann in den 70er Jahren mit der Erforschung von Fingerabdruck-Identifizierungs-Technologien. 1982 setzte NEC als weltweit erstes Unternehmen diesen auf Minutienrelationen basierenden Algorithmus kommerziell ein. Seither wurden weltweit mehr als 110 solcher Installationen durchgeführt: in Spanien, Südafrika, Saudi-Arabien, Japan (sowohl bei der Staatlichen Polizei als auch bei einigen regionalen Polizeirevieren), China (u.a. in Shanghai, Guangdong, Anhui, Hongkong, Macao), weiteren Ländern Asiens (z.B. Indonesien, Taiwan, Singapur und Thailand), im Südpazifik (Australien und Neuseeland), in Nord- und Lateinamerika (über 40 Großsysteme in den USA, in Kanada und El Salvador).

Des Weiteren installierte NEC eines der weltweit größten Systeme in Kalifornien. Die AFIS-Datenbank des Justizministeriums in Sacramento, Kalifornien, verzeichnet mehr als 100 Millionen Fingerabdrücke und bildet mit 12 angeschlossenen AFIS (Automated Fingerprint Identification System) die größte inner- und zwischenstaatliche Datenbank und Netzwerkbasis.

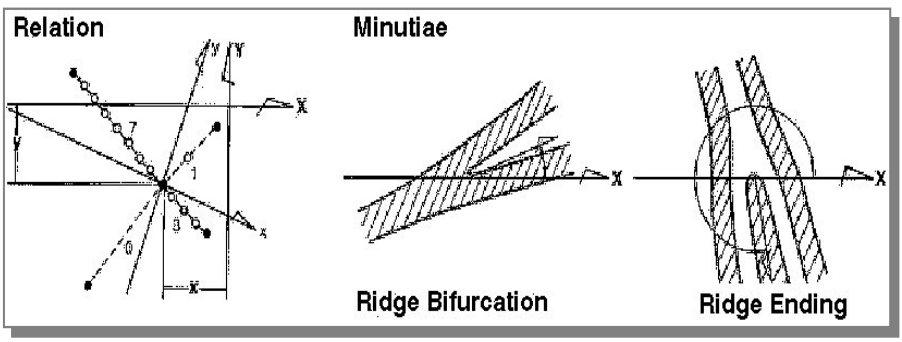
NECs automatische Fingerabdruck-Identifizierungssysteme werden heute in der gesamten Welt eingesetzt. U.a. im Gesundheitswesen, auf dem Gebiet der Zugangs- und Netzwerksicherheit sowie im Border Control und Criminal Justice Management. In verschiedenen Testreihen, wie z.B. BioP II und BioFinger werden europaweit die

BACKGROUNDER

Einsatzmöglichkeiten der NEC Fingerabdruck-Identifizierungstechnologie in Personaldokumenten und in Projekten für biometriegestützte Grenzkontrollen getestet.

Darüber hinaus vertraut eine Vielzahl von öffentlichen und privaten Organisationen bei der Bewältigung ihrer Identity-Management-Aufgaben auf die Fingerabdruck-Verifikation von NEC. Durch die Kombination von Fingerabdruck-Identifizierung mit anderen Technologien wie Smart Cards und digitalen Zertifikaten bieten NECs Identifikations-Lösungen entscheidende Vorteile wie sicheren Netzwerkzugriff, Fernzugriff auf Netzwerke, physischen Zugang, Signatur- und Verschlüsselungsdienste sowie Single-Sign-On-Fähigkeiten. Das Fingerabdruck-Identifizierungs-System von NEC erzielte bei verschiedensten unabhängigen Test immer wieder hervorragende Ergebnisse; so u.a. bei der *Fingerprint Vendor Technology Evaluation* (FpVTE) 2003.

NEC widmet sich seit über einem Vierteljahrhundert der Entwicklung einer absolut leistungsfähigen und zuverlässigen Identifikationsmethode für Fingerabdrücke. Das Ergebnis ist ein geradezu revolutionärer Vergleichsalgorithmus: die Anzahl der Rillen zwischen den Minutien dient als Grundlage für die Ermittlung eventueller Zusammenhänge zwischen den Minutien, so dass eine verlässliche Basis für den Vergleich und die Zuordnung von Fingerabdrücken gegeben ist. Da dieser Ansatz nicht von einer Referenzvorlage eines Fingerabdrucks mit entsprechend standardisierter Minutienausrichtung abhängt, bleibt das Ergebnis auch bei verwischten oder undeutlichen Fingerabdrücken unverfälscht. Genau darin besteht auch das Geheimnis der außergewöhnlichen Zuverlässigkeit des von NEC entwickelten Systems.

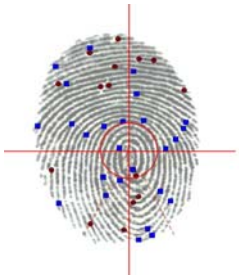


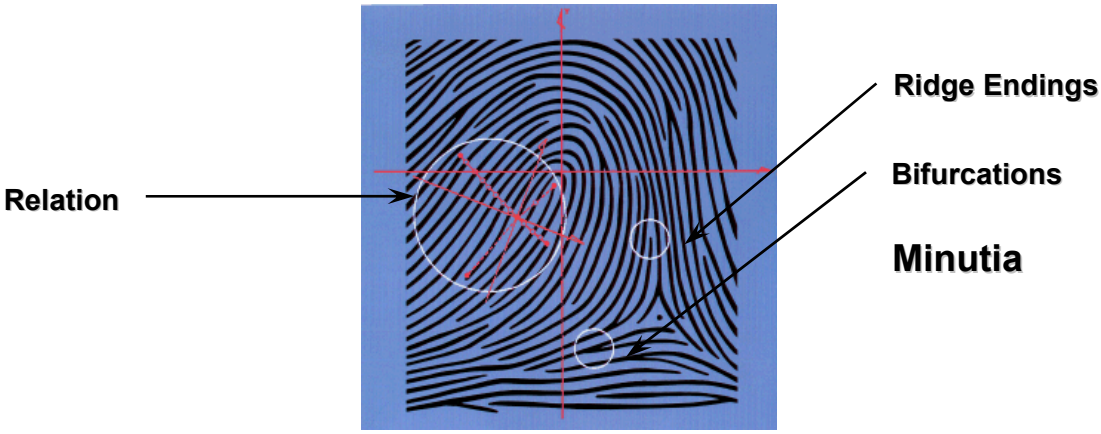
NEC bietet seinen AFIS - Kunden im Rahmen eines ganzheitlichen Lösungsansatzes die gewünschte Hardware, Software und den entsprechenden Kundenservice aus einer Hand.

BACKGROUNDER

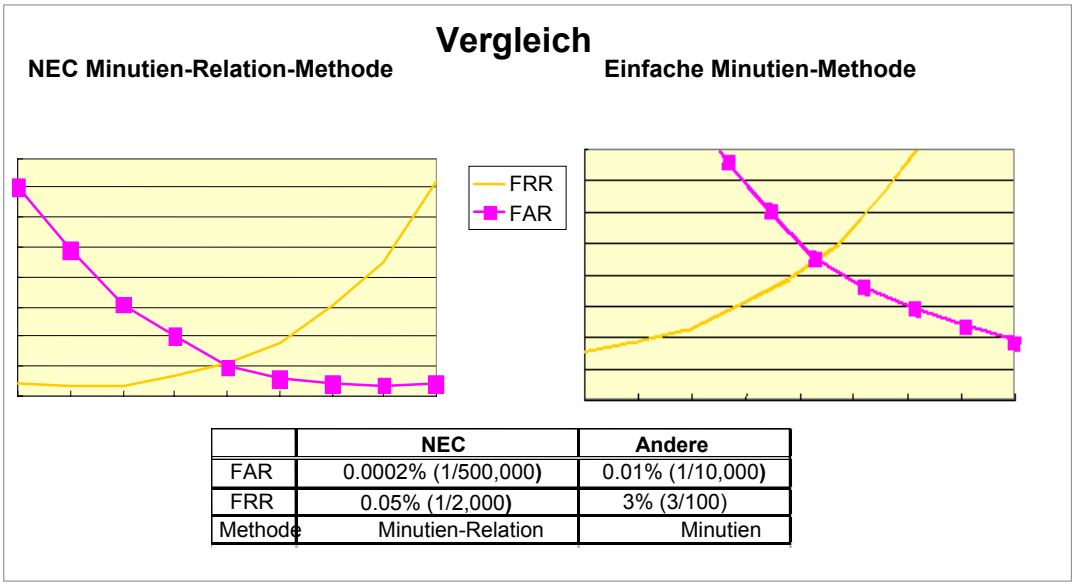
AFIS von NEC

Das von NEC entwickelte AFIS verwendet als bislang einziges System einen Bestimmungsalgorithmus, der die Rillenanzahl und die Beziehungen der einzelnen Minutien untereinander berücksichtigt. Zusätzlich werden so genannte "Zonendaten" zu Rate gezogen, die die Zahl der fälschlich ermittelten Minutien auf ein Minimum reduzieren, um so nur die klar identifizierbaren Zonen zum Vergleich zwischen Ausgangs- und Zielabdruck heranzuziehen. Dank dieser beiden Systemeigenheiten sind Betreiber eines AFIS von NEC in der Lage, hohe Erfolgsquoten zu erzielen.





Über den patentierten Identifikationsalgorithmus kann ein NEC AFIS auch undeutliche Fingerabdrücke verwerten und die Trennschärfe des Identifizierungsprozesses erhalten. Kaum ein anderer Anbieter kann mit solch erstklassigen Leistungsmerkmalen aufwarten.



	NEC	Andere
FAR	0.0002% (1/500,000)	0.01% (1/10,000)
FRR	0.05% (1/2,000)	3% (3/100)
Methode	Minutien-Relation	Minutien

AFIS gilt heutzutage weltweit als die beste Methode zur Verbrechensaufklärung, da dieses System die am Tatort hinterlassenen Fingerabdrücke schnell und zuverlässig identifiziert. Durch Einsatz der technischen Möglichkeiten von AFIS könnte die Arbeit in den Polizei- und Strafverfolgungsbehörden noch effizienter gestaltet werden.

LEXS

Da Straftäter ihre Fingerabdrücke wohl niemals absichtlich am Tatort hinterlassen, sind entsprechende Spuren häufig undeutlich, verwischt oder nur teilweise erhalten. Die Spurensicherung muss daher die originalen kriminologischen interaktiv verbessern und möglichst alle echten von verfälschten und daher nicht zu berücksichtigenden Minutien unterscheiden. Auch bei AFIS ist es unerlässlich, dass die Minutien der am Tatort aufgenommenen Spuren absolut exakt extrahiert werden, denn der Grad der Genauigkeit wirkt sich unmittelbar auf das Ergebnis der Fingerabdruck-Identifizierung (Matching) aus und ist somit von entscheidender Bedeutung.

Kriminologische Abdrücke werden in die Latent Prints Workstation für den Spezialisten und zum Laboreinsatz eingespeist und dort verarbeitet. Ein entsprechendes Abbild des Beweisstücks, beispielsweise im Original, als chemisch behandelter Abdruck, als Negativ oder als Fotografie des Abdrucks, wird direkt via angeschlossenem Flachbettscanner, Kamera oder Abdruckscanner (KS: Kompaktscanner) eingelesen. Die anschließende Optimierung der Aufnahme sowie Extraktion der Minutien erfolgt interaktiv mittels der einzigartigen NEC Software LEXS (Latent EXaminer Station). LEXS kann entweder ohne weitere Bedienereingriffe die Finger- bzw. Handabdruckbilder automatisch verarbeiten oder

aber den Bediener gezielt und interaktiv bei der Optimierung des vorliegenden Bildmaterials unterstützen. In der Tat verbindet diese Software die Fähigkeiten der Spurensicherung auf ideale Weise mit der weltbesten Technologie zur Bildbearbeitung und -optimierung.

Über das Programm kann der Anwender jeder Bilduntersuchung Vielfachachsen zuordnen, so dass tatsächlich eine allumfassende Suche durchgeführt werden kann. Falls gewünscht, kann zu jeder Achsfestlegung unabhängig ein Kernwert eingegeben werden. Systemtechnisch gibt es keine Mindestanforderungen an die Bildqualität. Keine Fingerabdrucksuche wird aufgrund mangelnder Bildqualität oder fehlenden bzw. zu umfangreichen Datenmaterials durchgeführt.

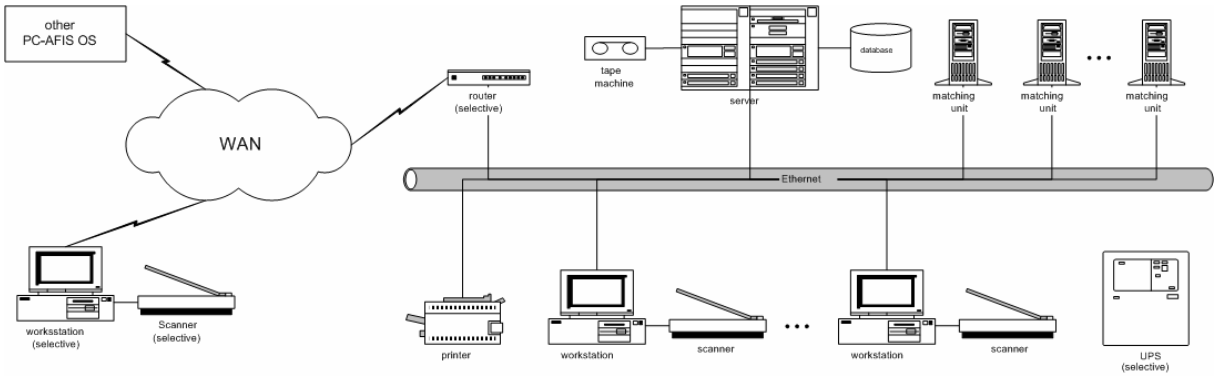
Die LEXS Software erleichtert der Spurensicherung die Verbesserung der am Tatort genommenen Abdrücke. Mittels Filtern und Bearbeitungstools stellt sie dem Anwender eine bedienerfreundliche, auf Windows NT™ ausgelegte grafische Bedieneroberfläche mit Pop-up-Menüs, Hilfe- und Bearbeitungsassistenten sowie Drag-und-Drop-Funktionen zur Verfügung.

IntronNavi™ - die PC- basierte AFIS Lösung

Seit über 30 Jahren treibt NEC als Pionier die Implementierung von AFIS voran. Heute ist NEC einer der Marktführer für AFIS-Lösungen, speziell für „latent identification“ und AFIS-Großdatenbanken. IntronNavi™ basiert auf NECs bewährter AFIS-Technologie. Diese wurde für Windows® Arbeitsplätze mit benutzerfreundlichen GUIs weiterentwickelt. IntronNavi™ ist ein vollständiges Hard- und Software-System für die Identifikation und Verifikation. Je nach Konfiguration besteht ein IntronNavi™-System aus Workstations, Matching Units (Standard PCs) und zentralem Server. Aufgrund der offenen Systemarchitektur ist IntronNavi™ skalierbar und unterstützt standardisierte Hard- und Software-Applikationen. Die IntronNavi™ Workstations setzen auf Windows® Plattformen im gängigen Office-Standard auf. Die Server basieren auf skalierbaren Microsoft NT® Konfigurationen. Eine IntronNavi™ Stand-alone Lösung bestehend aus einem PC Arbeitsplatz eignet sich typischerweise für die Bearbeitung von einigen zehntausend Fingerabdrücken und kommt ohne Datenbank-Management oder Anbindung weiterer Arbeitsplätze aus.

Die Client-Server-Systemlösung hingegen teilt die funktionalen Arbeitsabläufe zwischen Server, Matching Units und Datenbank-Management auf. Dies ermöglicht eine hohe Skalierbarkeit aller IntronNavi™ Client-Server-Lösungen. Eine Vielzahl an professionellen Bearbeitungs- und Auswertungstools sowie die Möglichkeit der Revision und Nachvollziehbarkeit von Prozessen machen IntronNavi™ zu einer hochpräzisen und kosteneffizienten Identifizierungslösung für die zeitgemäße Polizeiarbeit. IntronNavi entspricht allen internationalen Fingerabdruck-Standards inklusive ANSI/NIST, WSQ (Wavelet Scalar Quantization) und IQS (Image Quality Standard).

Beispielhafte IntronNavi™ Systemstruktur:



Fingerabdruckerkennung – Kommerzielle Lösungen

SafeSign Biometric Solution – Netzwerk-Sicherheit per Fingerabdruck

Um Personen zu erkennen und zu identifizieren, wird einerseits auf das klassische Verfahren Wissen und Besitz gesetzt: konkret auf einen PIN, ein Passwort oder einen Benutzernamen, mit dem sich das Individuum legitimiert. Parallel ist die Erkennung auch über ein Identifikationsdokument, eine Chipkarte oder ähnliche Tokens möglich, die sich im Besitz der Person befinden. Riskant ist dabei nur, dass all dies leicht verloren, vergessen, gestohlen oder dupliziert werden kann. Im Vergleich zu diesen beiden Verfahren bietet die SafeSign Biometric Solution von NEC das entscheidende Plus an Sicherheit.

Denn hier erfolgt die Identifikation eines Anwenders mittels seiner individuellen körperlichen Merkmale. Das Entscheidende – diese Merkmale können auch nicht unbeabsichtigt weitergegeben werden.

SafeSign Biometric Solution verbindet die biometrische Kompetenz von NEC mit einer modernen Smart Card - Software-Lösung von A.E.T. Jeder Anwender erhält eine fälschungssicher verschlüsselte Smart Card mit elektronischen Berechtigungszertifikaten. Diese Zertifikate sind mittels Biometrie gesichert. Anstelle des herkömmlichen PIN ist der Fingerabdruck des Anwenders auf der Smart Card enthalten. Berechtigte Personen authentifizieren sich also zunächst per Fingerabdruck. Erst dann wird mit Hilfe der SafeSign Biometric Solution das Zertifikat auf der Smart Card freigegeben - und ihr Mitarbeiter erhält Zugang zum Unternehmensnetzwerk, IT Applikationen etc. Weitere Anforderungen wie z.B. Zutritt zum Firmengebäude, Zeiterfassung, Bezahlfunktion in der Betriebskantine Online-

Shop-Bezahlung, bezahlter Helpdesk-Service oder digitale Signaturen können in die Lösung integriert werden. SafeSign Biometric Solution unterstützt alle gängigen Zertifikatstypen und kann folglich in alle PKI-Strukturen eingebunden werden – die perfekte Lösung für den multifunktionalen Mitarbeiterausweis. Eine PIN-Biometrie-basierte Lösung ist ebenfalls möglich.

Technische features:

- Basiert auf de facto Standards (PKCS, PC/SC, Active Directory, PKI etc.)
- NEC Fingerprint Bibliothek
- PKCS#11 – Bibliothek
- Token Management Utility
- PKI – Applet (auf Java Karten)
- Nahtlose Integration in Microsoft PKI®
- PKCS#15 – kompatible Kartenstruktur
- Sichere Speicherung vielfältigster digitaler X.509-Zertifikate

Gesichtserkennung

Das Gesicht spielt eine bedeutende Rolle in der menschlichen Verhaltensweise. Es ist gleichsam das Fundament unseres sozialen Umgangs. Biometrische Gesichtserkennungs-Systeme wie NeoFace™ werden auch deshalb verstärkt zum Einsatz kommen, weil sie eine berührungslose Vorgehensweise ohne direkten Kontakt oder Interaktion mit der zu identifizierenden Person ermöglichen.

Neben der Fingerabdruckserkennung konzentriert sich NEC bereits seit 15 Jahren auch auf die Entwicklung von Methoden der Gesichtserkennung. Als Ergebnis dieser Forschungsaufgaben wurde Ende 2003 das Gesichtserkennungsverfahren NeoFace™ international eingeführt. Hier flossen NECs langjährigen Erfahrungen mit großen Datenmengen und Datenbanken maßgeblich mit ein. Das Verfahren ist speziell auf Einsatzbereiche ausgelegt, in denen eine positive Gesichtserkennung besonders schnell und hochpräzise erfolgen muss. Mögliche NeoFace™ Einsatzgebiete sind z.B. Nationale ID Dokumente, Border Control Management, Zugangskontrolle zu sensiblen Zonen und Bereichen oder modernes Gefängnis-Management.

Parallel zur Fingerabdruckerkennung gewinnen biometrische Systeme für die Gesichts-erkennung zunehmend an Bedeutung. Nach Einschätzung von NEC wird sich die

Gesichtserkennung neben der Fingerabdruckerkennung zu einem der wichtigsten biometrischen Verfahren entwickeln.

NeoFace™

Hochpräzise und äußerst schnelle Datenlokalisierung

- GLVQ-basiertes Multi-Matching Gesichtserkennungs-System
- Kombinierte Merkmalsextraktion im Augen- und Gesichtsbereich
- Prüfung über Neuralnetzklassifikation
- Kurze Verarbeitungszeiten bei hoher Erkennungsrate
- Bildqualitätsunabhängige Erkennung

Hochpräzise und äußerst schnelle Verifizierung

- Adaptive Regional Blend Matching (ARBM) - Matching mit adaptiver Regionalüberblendung
- Matching auf Basis der Extraktion ähnlicher Gesichtspartien
- Identifikation und Authentifizierung über individuelle Gesichtsmerkmale
- Flexible Anpassung von NeoFace™ an Kundenanforderungen
- Integration in Videoüberwachungssysteme möglich - 1:N Identifikation
- Leichte Anbindung an ein AFIS von NEC
- Unterstützung aller gängigen Bild- und Videoformate: bmp, jpg, avi, mpeg, wmv

National ID

Die Sicherheitsanforderungen an Grenzkontrollen sind entscheidend geprägt von zwei Faktoren: der weltweit wachsenden Kriminalität verbunden mit illegalen Grenzübertritten, gefälschten Dokumenten sowie der Herausforderung, steigende Personenzahlen mit erhöhter Effizienz und sinkendem Aufwand abzufertigen. Dies funktioniert nur mit neuen Konzepten und Lösungen wie der Integration von biometrischen Merkmalen in Reisedokumente. Biometrie bedeutet Sicherheit in Bezug auf Echtheit von Reisedokumenten, tatsächlicher Übereinstimmung von Reisendem und Reisedokument und Sicherheit über die wahre Identität einer Person.

Oder das Beispiel Luftverkehr. Umfang und Intensität der Sicherheitsauflagen im Luftverkehr nehmen stark zu: Fluggast- und Gepäckkontrollen, Dokumentenkontrolle, Passenger Profiling, Identitätskontrollen und verschärfte Einreisebestimmungen in die USA. All diese Sicherheitsauflagen haben wesentliche Auswirkungen auf die Abfertigungsprozesse für Passagiere und Gepäckstücke. Einige Sicherheitsaufgaben können zumindest teilweise durch den Einsatz von Biometrie unterstützt, vereinfacht und beschleunigt werden. Wobei sicherlich den Aspekten Sicherheit und Schnelligkeit eine entscheidende Bedeutung zukommen dürfte um das anvisierte Ziel, die automatisierte Grenzkontrolle schnellstmöglich Realität werden zu lassen.

Das oben Gesagte trifft neben der Fluggastkontrolle auch auf den Einsatz von Biometrie in Bezug auf Zugangskontrollen für das Flughafenpersonal zu. Hierzu Aufschlüsse zu liefern war u.a. eine der Zielsetzungen des BioP II Projektes am Frankfurter Flughafen, an dem NEC ebenfalls teilgenommen hat. Die NEC Installation basiert auf dem von NEC entwickelten Fingerprint Algorithmus und nutzt das NEC eigene Qualitätstool für Enrolment, Erfassung und Matching der biometrischen Daten.

Biometrische Sicherheitslösungen von NEC – Praxisbeispiele

Olympische Sommerspiele Athen 2004 – Biometrisches Akkreditierungssystem für das Deutsche Haus

Die Olympischen Sommerspiele 2004 setzten neben sportlichen Höchstleistungen auch neue Maßstäbe in Sachen Sicherheit. Das Deutsche Haus, eine Einrichtung des Nationalen Olympischen Komitees für Deutschland (NOK), ist seit 1988 während der Olympischen Spiele der zentrale Treffpunkt für Sportler, Betreuer, Wirtschaftspartner, Medienvertreter und Mitarbeiter. Athleten und Besucher sollten sich im nur wenige Meter vom Olympiastadion gelegenen Deutschen Haus möglichst uneingeschränkt und entspannt bewegen können, sich dabei aber nicht nur sicher fühlen, sondern dies tatsächlich auch sein. Der Hausherr und Auftraggeber, die Deutsche Sport-Marketing GmbH (DSM), beauftragte die NEC

Deutschland GmbH und die Bundesdruckerei GmbH, mit der Bereitstellung eines biometrischen Akkreditierungssystems.

Das Akkreditierungssystem sollte entsprechend den Anforderungen des Auftraggebers im Dauerbetrieb fehlerfrei und zuverlässig zur Verfügung stehen. Während des Zeitraumes 12. bis 28. August 2004 rechnete das DSM mit insgesamt rund 4.500 Akkreditierungen. Betätigungen von Besuchern des Deutschen Hauses am Verifikationssystem mussten immer möglich sein, ohne dass eine Systemanmeldung oder der Start einer separaten Applikation erforderlich sein sollte.

Der Erfolg und die Resonanz der von NEC Deutschland GmbH und der Bundesdruckerei GmbH entwickelten biometrischen Lösung übertrafen alle Erwartungen. Während der Spiele in Athen konnten mit über 5.300 akkreditierten Besuchern weit mehr als ursprünglich erwartet von dem System profitieren. Neben einem Durchschnitt von ca. 350 akkreditierten Besuchern pro Tag, lag der Tagesrekord bei 594 erfassten Personen. Trotz erschwerter Randbedingungen wie Hitze und Staub, verschwitzten Fingerkuppen oder einer unerwartet hohen Besucherfrequenz lief das System reibungslos und zur vollen Zufriedenheit des Auftraggebers. Selbst das Enrolment des deutschen Bundesministers des Inneren, Otto Schily, das sich in der Vergangenheit bei biometrischen Systemen des Wettbewerbs oftmals als sehr schwierig erwies, gestaltete sich völlig problemlos.

Mit dem installierten Akkreditierungssystem gelang es in Athen für ein Höchstmaß an Sicherheit und Komfort zu sorgen und das im Vorfeld in das System gesetzte Vertrauen vollständig zu rechtfertigen. Der erfolgreiche Einsatz des biometrischen Systems in Athen sowie das von NEC bereits im Jahre 1998 zur Verfügung gestellte biometrische Zugangskontrollsystem für den Dopingraum bei den Olympischen Winterspielen in Nagano sind zukunftsweisende Meilensteine der Sicherheitstechnologie.

Einwanderungskontrolle

Die Einwanderungsbehörde von Singapur geht mit dem klar und deutlich formulierten Ziel an die Arbeit, "Singapur für alle Einwohner so sicher wie nur irgend möglich zu machen". Die zuständigen Behörden kontrollieren dazu alle ins Land Einreisenden aufs Genaueste und haben so einen Sicherheitsstandard geschaffen, wie er weltweit praktisch von keinem anderen Land erreicht wird. Allerdings zeigten die traditionellen zeit- und arbeitsintensiven Bearbeitungsmodalitäten bei über 600.000 zu überprüfenden Besuchern pro Monat allmählich Überlastungserscheinungen.

Mit der von NEC gemäß neuester Biometrietechnik entwickelten Lösung konnten die Besucher erstmals selbst die zur Überprüfung notwendigen Schritte vollziehen. Gleichzeitig führte dieser Ansatz zu einer allgemeinen Verbesserung der Sicherheitsstandards. Das NEC-System wurde an den drei Haupteinreisestellen eingerichtet: an den Einwandererkontrollpunkten TUA und Woodlands und am Internationalen Flughafen Changi.

Das von NEC speziell entwickelte System vereint modernste Smart Card-Technologie mit dem NEC Fingerabdruckerkennungs- und Identifikationssystem. Dank der Biometrietechnik von NEC konnte Singapur seine Überwachungsmechanismen an den stetig wachsenden Besucherstrom anpassen und gleichzeitig einen höheren Standard bezüglich Sicherheit und Effizienz erreichen.

Netzwerksicherheit

Die holländische ABN AMRO GTS Bank in Amsterdam hat bereits 1999 das TouchPass® - System von NEC mit zunächst 40 Benutzern eingeführt. Heute nutzen über 1.200 Personen diese Netzwerk-Zugangsmethode, die allein auf ihrem Fingerabdruck basiert.

Gesundheitswesen

In den Niederlanden gibt es rund 30.000 Heroinabhängige. Drogenabhängigkeit schafft gravierende soziale Probleme wie Verwahrlosung der Betroffenen oder Beschaffungskriminalität. Um diesen ständigen Teufelskreis zu durchbrechen erhalten Süchtige in Holland Substitutionsmittel wie Methadon und können so ein halbwegs normales Leben führen. Die Ausgabe des Methadons übernehmen verschiedene Institutionen wie Apotheken, Polizeidienststellen, Gemeindegesundheitszentren oder auch Gefängnisse.

Allerdings hatte das bisherige Verteilungssystem Mängel. Sie zeigten sich vor allem, wenn Teilnehmer des Substitutionsprogramms ihre Dosis von einer anderen Institution als üblicherweise erhielten, zum Beispiel weil sie verreisten oder vorübergehend in Haft waren: Dann fehlten häufig die nötigen Informationen über die korrekte Dosierung, weitere Medikamente oder andere Details. Der Grund: Die unterschiedlichen Stellen waren informationstechnisch nicht miteinander verbunden. Infolgedessen erhielten Patienten Fehldosierungen oder Substitutionsmittel sickerten auf den Schwarzmarkt durch.
1998 startete das Projekt Nationales Zentrales Verschreibungsregister (Landelijke Centrale Mideelen Registratie, LCMR). Dieses Register speichert zu jedem Teilnehmer des Methadon-Programms Stammdaten wie den Namen, die korrekte Dosierung des Substitutionsmittels und andere relevante Informationen. Es unterstützt Ärzte und Ausgabestellen bei der Dosierung und verhindert Methadonverteilung an Personen, die eigentlich keins erhalten dürften. Nach Abschluss zweier Pilotversuche wurde bis zum März 2001 das endgültige Systemdesign in einen Anforderungskatalog umgesetzt.

Nach einer ausführlichen Bewertung des Marktangebots fiel im April 2002 die Entscheidung für das Konsortium HSB/NEC: HSB Card & Cardsystems fungierte als Projektintegrator und lieferte das Kartenmanagementsystem CardCare®5, die Clientsoftware sowie die Kommunikationsmodule. NEC steuerte die spezifischen biometrischen Anwendungen, vor allem Libraries für den Software-basierenden Mustervergleich, bei. Die gesamte

Systeminstallation mit ca. 250 angeschlossenen Ausgabestellen wird demnächst abgeschlossen sein.

Ausblick

Im Rahmen der Wachstumsstrategie des Unternehmens wird NEC sein Leistungsspektrum und Lösungsportfolio kontinuierlich erweitern und weitere strategische Felder erschließen. So wird NEC Deutschland u.a. SmartCatch™, ein regel- und verhaltensbasiertes Videoüberwachungssystem im Laufe des Jahres 2005 auf dem europäischen Markt einführen.

Biometrie – ein Wachstumsmarkt

Laut einer Marktstudie von IDC aus dem Jahre 2002 wächst der Markt für biometrische Systeme im Vergleich zu anderen Segmenten im Informationstechnologiebereich überproportional stark. Systeme zur Fingerabdruckerkennung und Gesichtserkennung werden von dieser Entwicklung besonders profitieren.

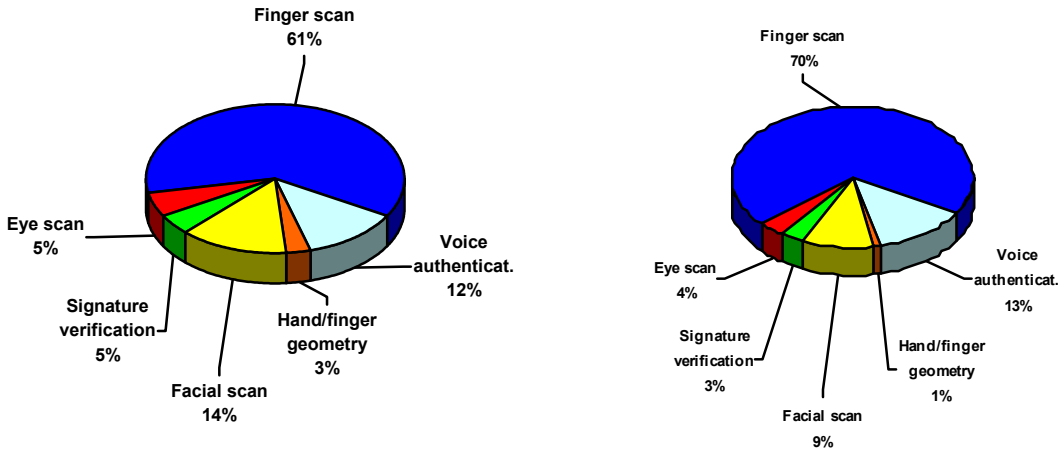


Abbildung oben: Vergleich Umsatzanteil Biometrie 2002 – 2006 (Quelle: IDC 2002)

Für Europa, den weltweit zweitgrößten Markt für Biometrie, wird der Umsatz für das Jahr 2005 auf 175,90 Millionen US-Dollar geschätzt, und bis 2006 wird er voraussichtlich auf 226,73 Millionen US-Dollar steigen. Für den Zeitraum von 2000 bis 2010 wird eine jährliche Gesamtwachstumsrate von 23,62% erwartet.

In Deutschland, dem größten europäischen Markt für Biometrie, beziffern Schätzungen den Jahresumsatz für 2005 auf 53,63 Millionen US-Dollar; bis 2010 wird mit einer weiteren Steigerung auf 187,76 Millionen US-Dollar gerechnet. Großbritannien ist derzeit der am schnellsten wachsende Markt für Biometrieapplikationen in Europa. Hier wird eine jährliche Gesamtwachstumsrate von 24,44% prognostiziert, was bis 2010 einem Jahresumsatz von 95,62 Millionen US-Dollar entspräche.

Das größte und am schnellsten wachsende Marktsegment ist die Gruppe der Nicht-AFIS-Produkte mit einer geschätzten jährlichen Wachstumsrate für die Jahre 2000 bis 2010 von 41,15%. Innerhalb dieser Produktgruppe machen Fingerabdruck-Applikationen 2004 mit geschätzten 28,22% den größten Anteil am gesamten europäischen Biometriemarkt aus. Im Betrachtungszeitraum von 2000 bis 2010 wird für die Gesichtserkennung die höchste jährliche Gesamtwachstumsrate von 46,84% erwartet.

BACKGROUNDER

Zum Unternehmen

Die NEC Corporation (NASDAQ: NIPNY, FTSE: 6701q.1) ist einer der weltweit führenden Lösungsanbieter für Informations- und Telekommunikationstechnik mit einer führenden Position bei Patentanmeldungen. NEC entwickelt für seine in einer Vielzahl von Branchen, weltweit tätigen Kunden maßgeschneiderte Lösungen in den Bereichen Computersysteme, Netzwerke und elektronische Bauelemente durch die Integration von IT- und Netzwerktechnologien sowie die Entwicklung von Halbleiter-Basistechnologien durch die NEC Electronics Corporation. NEC beschäftigt weltweit mehr als 140.000 Mitarbeiter. Der Umsatz belief sich im vergangenen Geschäftsjahr 2003/2004 auf rund 4.906 Milliarden Yen (rund 47 Milliarden US-Dollar). Mehr Informationen finden Sie unter: http://www.nec.com

Die 1987 gegründete NEC Deutschland GmbH ist eine hundertprozentige Tochter der NEC Corporation mit Sitz in Ismaning bei München. Das Produktportfolio umfasst sowohl modernste Präsentationstechnik wie Video-, LCD-, DLP(tm)-Projektoren und Plasma-Monitore, als auch optische Speichermedien wie CD-ROM, DVD-Laufwerke und Floppy-Disks. Telekommunikations-Produkte und biometrische Sicherheitslösungen runden das Spektrum ab. Zum Vertriebsgebiet gehören die Regionen Zentraleuropa mit Deutschland, Österreich und der Schweiz sowie Benelux und Ost- bzw. Südosteuropa. In allen Produktbereichen und Märkten besetzt NEC Spitzenplätze bis hin zur Marktführerschaft und ist bestens für weiteres Wachstum positioniert. NEC Deutschland beschäftigt insgesamt rund 100 Mitarbeiter in fünf Ländern. Mehr Informationen finden Sie unter: http:// www.de.nec.de.

Kontakt:
NEC Deutschland GmbH
Security Solutions Biometrics
Reichenbachstraße 1
D-85737 Ismaning
Tel.: +49 89 96 274 – 0
Fax: +49 89 96 274 – 525
www.de.nec.de

Glossar - Biometrie

	Begriff	Beschreibung
A	AFIS (Automated Fingerprint Identification System, Automatisiertes Fingerabdruck-Identifikationssystem)	Ein hochspezialisiertes Biometriesystem, das einen Fingerabdruck mit einer Datenbank von Fingerabdrücken vergleicht. AFIS werden überwiegend von der Polizei verwendet, finden jedoch auch im zivilen Bereich Anwendung. Bei der Strafverfolgung werden Fingerabdrücke am Schauplatz einer Straftat oder bei der Festnahme von Verdächtigen genommen. Siehe auch 'Fingerabdruckbild'.
	Algorithmus	Eine Folge von Anweisungen zur Lösung einer bestimmten Aufgabe durch ein (Biometrie-)System. Ein Algorithmus beinhaltet eine endliche Anzahl von Rechenschritten.
	API	Programmierschnittstelle für Anwendungen (Application Program Interface). Eine Reihe von Funktionen oder Anweisungen zur Standardisierung von Anwenderschnittstellen. Eine API ist ein vom Anwendungsentwickler verwendeter Computercode. Alle API-kompatiblen Biometriesysteme können miteinander kombiniert oder gegeneinander ausgetauscht werden. Häufig wird zwischen Low-Level- und High-Level-APIs unterschieden. Bei High-Level-APIs handelt es sich um anwendungsnahe, bei Low Level-APIs um gerätenahe Schnittstellen.
	Aufnahme in das System	Vorgang, bei dem biometrische Samples einer Person erfasst werden sowie die anschließende Aufbereitung und Speicherung der biometrischen Referenzmuster (Templates) zur Erkennung der Identität dieser Person.
	Authentifikation	Bei der Authentifikation mittels eines biometrischen Systems wird die Identität einer Person durch Identifikation oder Verifikation bestätigt. Authentifikation ist gleichbedeutend mit "Feststellung der Berechtigung".
B	Bifurkation / Verzweigung	Biometrisches Merkmal. Eine Verzweigung von mehr als einer Erhebung eines Fingerabdrucks.
	BioAPI	**Bio**metric **A**pplication **P**rogram **I**nterface ist eine standardisierte Anwenderprogrammier-Schnittstelle zur Integration biometrischer Systeme in Anwendungen.
	Biometrie	Der Begriff Biometrie stammt aus dem Griechischen und setzt sich zusammen aus den Worten 'bios' (Leben) und 'metron' (Maß). Demnach bezeichnet Biometrie die Lehre von der Vermessung körpereigener Eigenschaften. Übertragen auf die Welt der Informationstechnologie meint der Begriff die automatisierte Methode zur Identifizierung oder Überprüfung eines Individuums basierend auf physischen oder verhaltenstypischen Kriterien.
	Biometrische Merkmale	Biometrische Merkmale lassen sich unterteilen in sogenannte aktive, verhaltenstypische Merkmale und passive, physiologische Merkmale. Aktive Merkmale sind z.B. Unterschriftdynamik, Stimme, Anschlagdynamik auf Tastaturen und Bewegung. Zu den passiven Merkmalen gehören z.B. Fingerabdruck, Gesichtserkennung, Irismuster, Handgeometrie, Retinamuster und Venenstruktur.
	Biometrische Verfahren	Verfahren, die Personen anhand biometrischer Merkmale erkennen.

	Biometrisches Gerät	Der Bestandteil eines Biometriesystems, das den Sensor für die Erfassung des biometrischen Samples einer Person enthält.
D	Datenbank	Ein Speicher biometrischer Vorlagen und dazugehöriger Endbenutzerdaten. Auch wenn nur eine biometrische Vorlage oder ein Datensatz gespeichert ist, spricht man von einer Datenbank („database of one“). In der Regel enthält eine Datenbank jedoch eine größere Anzahl biometrischer Datensätze.
	Datensatz	Die Vorlage und andere Informationen über den Endbenutzer.
E	Encoding	Extraktion der Minutien innerhalb des Erfassungsvorganges.
	Ende einer Erhebung	Derjenige Punkt auf einem Fingerabdruckbild, an dem eine Erhebung endet.
	Erfassung	Vorgang, bei dem ein biometrisches Sample des Benutzers erfasst wird.
	Erhebung	Die erhöhten Muster der Fingerspitzen und Handflächen.
F	Falsche Akzeptanz-Rate (FAR)	Die Falsche Akzeptanz-Rate gibt die Wahrscheinlichkeit dafür an, dass ein fremdes Individuum bei der Präsentation seiner Verifikationsdaten fälschlicherweise als der rechtmäßige Eigentümer der Referenzdaten erkannt wird. Die Falsche Akzeptanz-Rate ist abhängig von der gewählten Toleranzgrenze, innerhalb derer die Verifikations- und Referenzdaten für eine erfolgreiche Authentifikation übereinstimmen müssen: Je kleiner die Toleranzgrenze, desto niedriger die Falsche Akzeptanz-Rate und um so höher dagegen die Falsche Rückweisungs-Rate.
	Falsche Rückweisungs-Rate (FRR)	Die Falsche Rückweisungs-Rate gibt die Wahrscheinlichkeit dafür an, dass der rechtmäßige Besitzer der biometrischen Referenzdaten fälschlicherweise zurückgewiesen wird. Die Falsche Rückweisungs-Rate ist abhängig von der Toleranzgrenze, innerhalb derer die Verifikations- und Referenzdaten für eine erfolgreiche Authentifikation übereinstimmen müssen: Je größer die Toleranzgrenze, um so niedriger wird die Falsche Rückweisungs-Rate und um so höher dagegen die Falsche Akzeptanz-Rate.
	Fingerabdruckbild	Ein körperbezogenes Biometrieverfahren, bei dem die Muster der Fingerspitzen betrachtet werden.
G	Gesichtserkennung	Ein körperbezogenes Biometrieverfahren, das auf der Analyse der Gesichtszüge beruht.
	Gleichfehlerpunkt (Equal Error Rate, EER)	Die Entscheidungsschwelle eines Systems, bei der der Anteil der falschen Rückweisungen ungefähr dem Anteil der falschen Akzeptanzen entspricht, wird als Gleichfehlerpunkt bezeichnet.
I	Identifikation	Als biometrische Identifikation bezeichnet man die Feststellung der Identität eines Individuums. Dazu gibt das Individuum zunächst seine biometrischen Meßdaten ab. Dann wird ein Pool individuenbezogener Referenzdaten auf diejenigen Referenzdaten durchsucht, die am besten zu den vorgelegten Verifikationsdaten passen. Es wird dann eine Datenbasis von Refernzdaten von „n“ Individuen nach solchen Referenzdaten durchsucht, die mit den präsentierten Verifikationsdaten die beste Übereinstimmung zeigen. Man nennt den Prozeß daher auch einen 1:N Vergleich (One-to-Many).

K	Klassifizierung	Um bei der Identifikation eines Individuums nicht zu viele Vergleiche von Fingerabdrücken durchführen zu müssen, wird ein Fingerabdruck zunächst einmal klassifiziert, d.h. die Zugehörigkeit zu einer bestimmten Klasse von Fingerabdrücken ermittelt. Auf diese Weise ist es möglich, eine Datenbasis von Fingerabdrücken in kleinere Bereiche einzuteilen und einen präsentierten Fingerabdruck dann nur mit den Referenzdaten aus dem jeweiligen Bereich zu vergleichen. Klassen von Fingerabdrücken sind z.B. "Arch" (nur einfache Bögen), "Tented Arch" (steil ansteigende und wieder steil abfallende Linien vorhanden), "Loop" (Schleife vorhanden) und "Whorl" (Windung vorhanden).
L	Latenzabdruck	Ein am Schauplatz einer Straftat aufgenommener Fingerabdruck.
	Live-Erfassung	Der Prozess der Erfassung eines biometrischen Samples mittels Interaktion zwischen einem Endbenutzer und einem Biometriesystem.
M	Match/Matching	Der Prozess, bei dem ein biometrisches Samples mit einer bereits gespeicherten Vorlage verglichen und der Grad der Übereinstimmung bestimmt wird. Die Entscheidung über eine Akzeptanz oder Rückweisung hängt davon ab, ob dieser Wert den vorgegebenen Schwellenwert übersteigt.
	Merkmals-Extraktionsalgorithmus	Bei einem biometrischen Vergleichsverfahren werden die aufgenommenen Messdaten nicht komplett abgespeichert bzw. verglichen; es müssen charakteristische Merkmale extrahiert werden. Ein geeigneter Merkmals-Extraktionsalgorithmus dient zur Extraktion der anschließend zu speichernden Referenzdaten bzw. der gemessenen Verifikationsdaten, die mit den Referenzdaten verglichen werden.
	Merkmals-Vergleichsalgorithmus	Der Merkmals-Vergleichsalgorithmus dient zum Vergleich der von einer zu verifizierenden (oder zu identifizierenden) Person präsentierten Verifikationsdaten mit vorher abgespeicherten Referenzdaten. Es wird eine Vergleichsgröße berechnet.
	Minutien	Charakteristische Punkte eines Fingerabdruckbildes (z.B.Verzweigungs- und Endpunkte von Linien).
N	Neurales Netz	Ein spezieller Algorithmus. Ein neurales Netz „lernt“ mit Hilfe künstlicher Intelligenz aus früheren Erfahrungen und lässt diese in die Berechnung einfließen, ob ein biometrisches Sample mit der Vorlage übereinstimmt.
O	One-to-Many	Synonym für Identifikation.
	One-to-One	Synonym für Verifikation.
R	Reaktionszeit	Die Zeitspanne, die ein Biometriesystem braucht um eine Entscheidung über die Identifikation oder Verifizierung eines biometrischen Samples zu treffen.
	Referenzdaten	Als Referenzdaten bezeichnet man die mit dem Merkmals-Extraktionsalgorithmus gebildeten, abzuspeichernden Daten zur Kennzeichnung eines Individuums.
S	Schwellenwert / Entscheidungsschwelle	Die Akzeptanz oder Rückweisung biometrischer Daten hängt davon ab, ob der Übereinstimmungswert über oder unter dem Schwellenwert liegt. Der Schwellenwert ist einstellbar, so dass das System je nach den Anforderungen einer Biometrieanwendung mehr oder weniger scharf eingestellt werden kann.

	Smart Card	Eine Smart Card enthält einen integrierten Chip, der ein Microcontroller mit internem Speicher oder lediglich ein Speicherchip sein kann. Die Karte wird durch direkten physischen Kontakt oder mit Hilfe einer kontaktlosen elektro-magnetischen Schnittstelle an ein Lesegerät angeschlossen. Smart Cards mit integriertem Microcontroller können beträchtliche Datenmengen speichern, eigene Funktionen (z.B. Verschlüsselung und digitale Signaturen) ausführen und intelligent mit einem Smart Card-Lesegerät interagieren.
T	Toleranzgrenze	Biometrische Meßdaten sowie die daraus mit Hilfe des Merkmals-Extraktions-algorithmus gebildeten Verifikationsdaten sind auch für dasselbe Individuum niemals gleich, sondern stets Schwankungen unterworfen. Deshalb kann man bei einer biometrischen Identifikation oder Verifikation nie eine exakte Übereinstimmung von Verifikationsdaten und Referenzdaten verlangen, sondern nur eine Übereinstimmung innerhalb einer gewissen Toleranzgrenze.
V	Verifikation	Als biometrische Verifikation bezeichnet man die Prüfung, ob ein Individuum seine vorgegebene Identität besitzt. Wie bei der biometrischen Identifikation werden zunächst die Verifikationsdaten des zu verifizierenden Individuums gebildet. Im Gegensatz zum Prozeß der Identifikation wird jedoch nur ein Vergleich mit einem einzigen Satz von Referenzdaten durchgeführt; das Individuum gilt als verifiziert, wenn Verifikations- und Referenzdaten innerhalb der beim Merkmals-Vergleichsalgorithmus festgelegten Toleranzgrenzen übereinstimmen. Man bezeichnet die biometrische Verifikation daher auch als "1:1 Vergleich".
	Verifikationsdaten	Als Verifikationsdaten bezeichnet man diejenigen Daten, die zur Identifikation oder Verifikation eines Individuums aus aktuellen biometrischen Meßdaten mit Hilfe des Merkmals-Extraktionsalgorithmus extrahiert wurden. Diese Daten werden anschließend mit Hilfe des Merkmals-Vergleichsalgorithmus mit den vorher gespeicherten Referenzdaten verglichen.
	Verschlüsselung	Vorgang, bei dem Daten in einen für Unbefugte unlesbaren Code konvertiert werden. Mit Hilfe eines Kenn- oder Passwortes werden der Code und somit auch die biometrischen Daten entschlüsselt (dekodiert).
	Vorlage / Referenzvorlage	Die biometrischen Messdaten einer registrierten Person, die das Biometrie-system mit den später erfassten biometrischen Samples vergleicht.
W	WSQ (Wavelet Transform/Scalar Quantisation)	Ein Komprimierungsalgorithmus zur Verringerung der Dateigröße der Fingerabdruckbilder.
Z	Zertifizierung	Testverfahren für ein biometrisches System um sicherzustellen, dass es bestimmte Leistungskriterien erfüllt. Systeme, die den Testkriterien entsprechen, werden als geprüft bezeichnet und von der Prüforganisation zertifiziert.