Biometrische Authentikation: Methoden- und Verfahrensansätze unter Windows 2000 (W2K)

- Studienarbeit-

am Arbeitsbereich AGN des FB Informatik der Universität Hamburg

30.05.2002

VERFASSER:
Samer Abdalla
Mat.Nr.: 50 19 714
Heisterbusch 6
21682 Stade

und

Timo Abschinski
Mat.Nr.: 50 02 164
Tierparkallee 26
22527 Hamburg

BETREUER:
Prof. Dr. rer.nat. (Dipl.-Phys) Klaus Brunnstein
Professor für Anwendungen der Informatik
FB Informatik, Universität Hamburg
Arbeitsbereich AGN

und

Dipl.-Inform. B. Sc. Arslan Brömme
FB Informatik, Universität Hamburg
Arbeitsbereich AGN

Alle hier nicht ausdrücklich aufgeführten Marken oder Produktnamen sind Marken oder Warenzeichen ihrer jeweiligen Inhaber.

INHALTSVERZEICHNIS

1 EINLEITUNG

In diesem Jahr übersteigt der weltweite Umsatz mit biometrischen Sicherheitsanwendungen erstmals die 500-Millionen-Euro-Grenze. Dies geht aus einer Schätzung der IBIA (Internationalen Organisation der Biometrikanbieter) hervor.
Das Wachstum geht zwar in erster Linie auf Grossaufträge der Industrie und Verwaltung zurück, jedoch kommen nun auch vermehrt Produkte für den Einsatz am heimischen oder betrieblichen PC auf den Markt. Die Palette biometrischer Zugangssicherungen für PCs reicht mittlerweile von Mäusen und Tastaturen mit integriertem Fingerabdruckscanner über Webcam-Lösungen, deren Software in der Lage ist, Gesichter registrierter Personen wieder zu erkennen, bis hin zu Scannern, die das individuelle Iris-Muster des menschlichen Auges zur Authentikation nutzen.

Diese Arbeit soll zunächst die Grundlagen erläutern und anschließend gängige biometrische Verfahren vorstellen. Im weiteren werden die Anforderungen an ein biometrisches Authentikationssystem definiert und erklärt. Zum Abschluss erfolgt ein Test einer biometrischen Software, die sich in Windows 2000 (W2K) integrieren lässt.

2 GRUNDLAGEN

2.1 Was ist Biometrik?

Biometrik = Biometrie + Informatik

Biometrik ist die Anwendung der Biometrie/Biometrik in der Informatik und umgekehrt, insbesondere bei der biometrischen Authentikation.

Lexikalisch wird die Biometrik als Lehre von der Anwendung mathematischer (statistischer) Methoden auf die Mess- und Zahlenverhältnisse der Lebewesen und ihrer Einzelteile definiert. Im engeren, auf die Computerwelt bezogenen Sinne ist dieser Begriff ein Synonym für den *Identitätsnachweis* von Personen unter Verwendung ihrer individuellen körperlichen Merkmale [1]

Die gewählten Merkmale sollten folgende Eigenschaften aufweisen:

- **Universalität** (jede Person sollte die Merkmale haben)
- **Einzigartigkeit** (Merkmale müssen so einzigartig sein, dass sie möglichst nur einer einzigen Person eindeutig zugeordnet werden können
- **Persistenz** (das Merkmal soll stabil sein, d.h. es sollte sich im Laufe der Zeit kaum verändern)
- **Merkmalsquantivität** (das Merkmal sollte quantitativ messbar sein)
- **Akzeptanz** (sollte von den Personen akzeptiert werden)
- **Performanz** (Zeitaufwand & Speichergröße)
- **Sicherheit** (sicher im Hinblick auf Hintertüren & nicht autorisierten Zugriffen)

Fachliche Definition:

Biometrie (nach [Lorenz 1996]):

Unter dem Begriff der Biometrie werden die vielfältigen Anwendungen der Mathematik, insbesondere der mathematischen Statistik, in den biologischen und ihnen verwandten Wissenschaften zusammengefasst.

→ Die Vermessung des menschlichen Körpers ist hier ebenfalls enthalten.

Biometrische Systeme lassen sich in zwei Klassen unterteilen:

2.2 Taxonomie der Biometrik

Anwendungsbezogen Technologiebezogen

Anwendungsbezogen (application type):

- Personen-Authentikation: Um Individuen zu identifizieren. Innerhalb dieser Studienarbeit ausschlaggebend
- medizinische Diagnose: Hautfarbe, Herzrhythmus und andere Eigenschaften unseres Körpers können für die medizinische Diagnose wichtig sein (TCM: „Traditional Chinese Medicine“)
- astrologische Anwendung (z.B. Handlinienlesen, etc.)
- ethische Erforschung: z.B. Bestimmung von Bevölkerungsausbreitungen über verschiedene Regionen hinweg

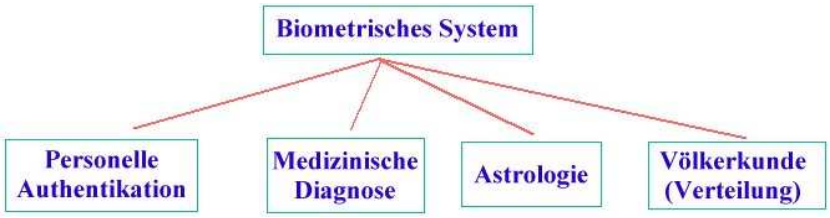


Abbildung 1 - Biometrisches System

Technologiebezogen (technology type):

Hier unterscheidet man generell in statische und dynamische Eigenschaften. Wir werden uns besonders mit der „***Personal Authentication***“ auseinandersetzen, das heißt mit der Authentikation via Kopf (Gesicht, Iris, Retina, Ohr, Zunge, ...) und Hand (Fingerabdruck, Handabdruck, ...). Die verhaltensbezogenen Eigenschaften betreffen wiederum Handschrift, Stimme, Gestik, und andere.

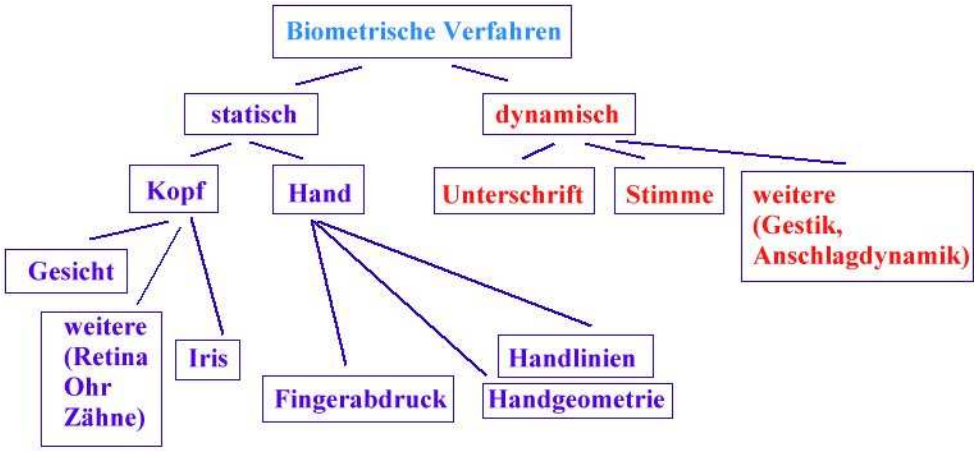


Abbildung 2 - Biometrische Verfahren

2.3 Warum Biometrik?

In der heutigen Gesellschaft nimmt die Automatisierung immer mehr zu. Die Sicherheit wird zunehmend wichtiger. Solche Fragen wie z.B.: „Ist diese Person zugangsberechtigt?“ „Ist diese Person autorisiert, eine bestimmte Transaktion durchzuführen?“ „Ist diese Person Bürger dieses Landes?“ befassen sich mit ein und dem selben Sicherheitsaspekt:
Wie identifiziert man korrekt Personen?
Biometrische Merkmale haben den grundlegenden Vorteil, dass man sie im Prinzip nicht verlieren kann. Passwörter, PIN & Co werden des Öfteren vergessen oder nicht genügend geschützt. Biometrische Verfahren sind, wenn richtig angewandt, sicherer und einfacher als konventionelle Authentikationsverfahren.

Konventionelle Verfahren:

- Wissen
- Besitz
- Zeit/Ort

Wissen:

- Passwörter: Benutzer wählen leider oft einfache Passwörter, die mit Wörterbüchern oder „Social Engineering/Hacking“ geknackt werden können
- Passwörter lassen sich leicht kopieren, abfangen oder an nicht autorisierte Personen weiterleiten
- Passwörter können leicht vergessen werden → Grund: es gibt immer mehr Bereiche in denen Passwörter eingesetzt werden. Bestimmte Passwörter werden nur sehr selten benötigt.
- Es wird häufig immer das selbe Passwort benutzt → hohes Sicherheitsrisiko!!!

Besitz:

- Schlüssel (aus Metall), Chipkarte
- Bei Verlust muss u. U. die Schließanlage ausgetauscht werden
- Schlüssel lassen sich relativ einfach vervielfältigen

Zeit/Ort:

- Benutzer kann sich z.B. nur zu einer bestimmten Zeit an einem bestimmten Ort einloggen

→ Biometrische Verfahren als „sichere“ Alternative ?!?

Merkmale eines Körperteils können auf verschiedene Weise definiert werden:

- Genotypische (werden durch Vererbung übertragen)
- Konditionierte (die Ausprägung von konditionierten Merkmalen wird durch Training bestimmt, wie es bei der Unterschrift oder dem Tastaturanschlag der Fall ist)
- Randotypische (entstehen durch zufällige Veränderungen während der embryonalen Frühphase in der Entwicklung eines Menschen)

Für die eindeutige Identifizierung einer Person sind randotypische Anteile unverzichtbar!

2.4 Erfassung neuer Daten (Enrollment):

Vor der biometrischen Autorisation lernt das System den Benutzer kennen, indem seine Merkmalsstruktur erfasst und als Referenz gespeichert wird. Diesen Vorgang bezeichnet man als Personalisierung oder Enrollment.
Nur wenn das Enrollment sorgfältig durchgeführt wird, lassen sich genügend Daten eines körpereigenen Merkmals erfassen, damit für eine spätere Erkennung, auch bei einem schlechtem aktuellen Muster, noch viele Übereinstimmungen vorhanden sind. Die gewonnenen Daten werden dabei häufig in einer zentralen Datenbank gespeichert und vereinzelt, je nach Verfahren, auch in Smartcards.

Zwei grundlegende Erkennungsverfahren:

- Verifikation
- Identifikation

2.4.1 Biometrische Identifikation (biometric identification):

a) Erkennung einer Person anhand biometrischer Merkmale, mit/ohne Einwilligung der Person
b) 1:n-Zugriff auf eine biometrische Datenbank (im Rahmen einer biometrischen Authentikation)

2.4.2 Biometrische Verifikation (biometric authentication):

a) Überprüfung der behaupteten Identität einer Person, durch Vergleich mit zu dieser Identität gespeicherten biometrischen Daten
b) 1:1-Zugriff auf eine biometrische Datenbank (im Rahmen einer biometrischen Authentikation)

2.4.5 Biometrische Authentikation (im weiteren Sinne):

Der gesamte Vorgang (Prozess), mit dem eine Person konfrontiert wird, um Zugriff auf Systemressourcen zu erhalten.

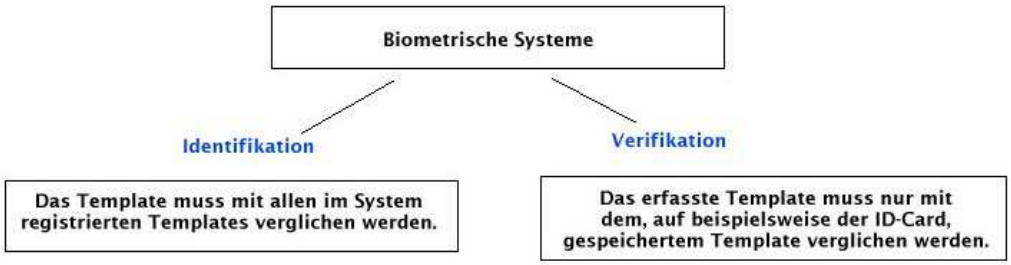


Abbildung 3 - Biometrische Systeme (Identifikation und Verifikation)

2.5 *Triviales Phasenmodell:*

1. Phase: Einlernvorgang
2. Phase: biometrische Authentikation
3. Phase: Autorisation
4. Phase: Zugriff auf Systemressourcen

2.6 Identifikation (Identification), Erkennung (Recognition) und Verifikation (Verification)

Zwischen den Begriffen Identifikation, Erkennung und Verifikation muss unterschieden werden. Ein Identifikationssystem beispielsweise beantwortet die Frage: „Wer bin ich?“. Ein Verifikationssystem wiederum beantwortet die Frage: „Bin ich die Person die ich vorgebe zu sein?“.

Ein Identifikationssystem greift in der Regel auf eine riesige Datenbank zurück, in der die biometrischen Merkmale mehrerer Personen gespeichert sind. Das System liefert das Ergebnis, ob die überprüfte Person registriert ist oder nicht. Die Ausgabe könnte also lauten: „Zugriff gewährt“ oder aber „Zugriff verweigert“.

Bei einem Verifikations-System ist es nicht notwendig Informationen in einer Datenbank gespeichert zu haben. Hier wird die Person z.B. anhand einer Passwort- oder ID-Card

überprüft, auf der zusätzlich biometrische Merkmale abgespeichert sind. Das System scannt, selektiert und analysiert nun die biometrischen Daten. Die „eingefangenen“ biometrischen Daten werden aufbereitet und mit denen auf der Passwort/ID-Card verglichen. Das System gibt anschließend ein Verifikationsergebnis aus (Zugriff gewährt/Zugriff verweigert).

2.7 Wie funktioniert nun ein biometrisches System?

Generell setzen sich alle biometrischen Systeme aus zwei Bereichen zusammen: Der „Anmeldung (Enrollment part)“ und der „Identifikation (Identification part)“.
Der „Enrollment part“ stellt sicher, dass die biometrischen Daten des Benutzers zur Verfügung gestellt und somit registriert werden, sodass diese als Kriterium bei der Identifikation genutzt werden können. Der „Identification part“ unterteilt sich in vier Stufen: capture, feature extraction, comparison und decision.

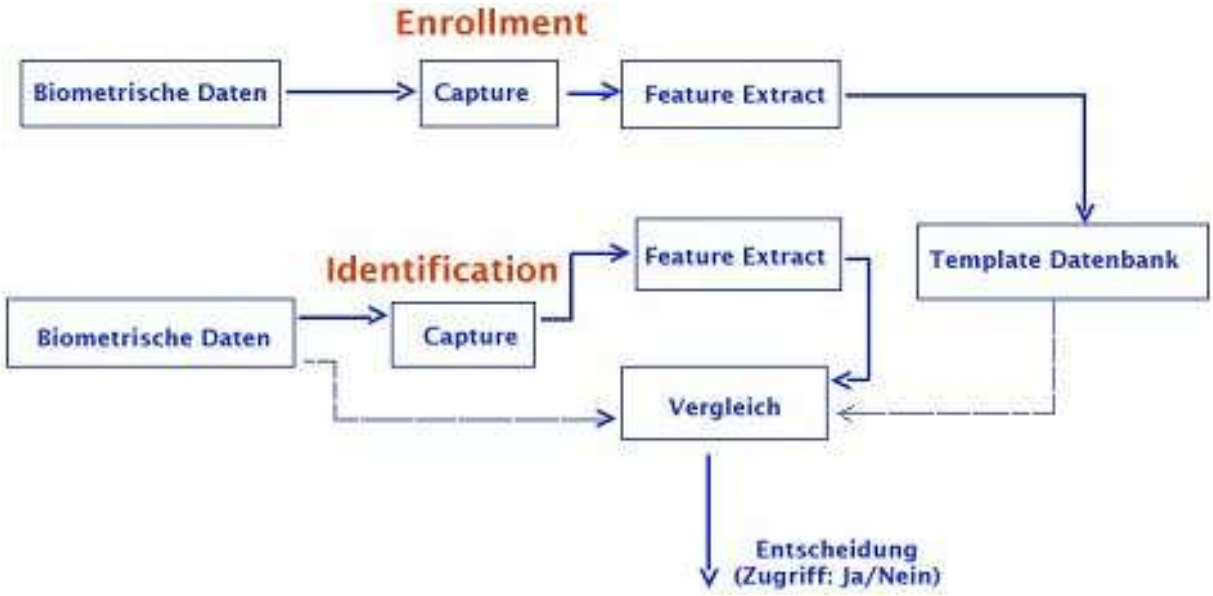


Abbildung 4 - Enrollment und Identification

2.7.1 Erfassungs-Stufe (Capture Stage)

In dieser Stufe werden physikalische oder verhaltensbezogene Eigenschaften als so genanntes ‚Sample’ erfasst. Die erfassten Daten werden in digitale Form übersetzt. In der Regel werden biometrische Daten über eine Kamera erfasst und als digitales Abbild gespeichert.

Videokameras werden beispielsweise eingesetzt um Iris und Gesicht zu scannen, wohingegen man thermale Kameras zur Gesichts- und Hand-Erkennung verwendet.
Die Fingerabdruckerkennung wird am längsten praktisch eingesetzt und ist deshalb auch weit verbreitet. Für den Retinascan benötigt man eine spezielle Kamera mit starkem präzisem Licht. Es wird also deutlich, das sich die Erfassungseinheiten (Capture-Devices) jeweils unterscheiden. Sprachbasierte Systeme benutzen beispielsweise nur einen PC-Lautsprecher mit Mikrofon und signaturbasierte Systeme benutzen ein eingebautes drucksensitives Zeichenbrett.
Das Erfassen der Daten (Capture-Stage) ist die erste Phase der automatischen Personen-Identifikation. Die Qualität des Samples, also der „eingefangen" Daten, ist hier entscheidend.

2.7.2 Selektions-Stufe (Feature Extraction Stage)

In dieser Phase werden spezifische, möglichst einzigartige Daten aus dem Sample selektiert und extrahiert. Es entsteht ein so genanntes Template. Die Templates von 2 verschiedenen Personen sollten sich immer signifikant unterscheiden. Das generierte Template aus zwei verschiedenen Samples der selben Person sollte weitgehend gleich sein.

Annährungsverfahren zur Templategenerierung:
Zunächst werden bedeutungsvolle einzigartige Features ausgemacht und überprüft; z.B. die Minutien und Poren eines Fingerabdrucks. Im nächsten Schritt werden diese Features extrahiert und in mathematischen Code umgewandelt. Die meisten dieser Annährungsverfahren nutzen viele verschiedene Bildverarbeitungsalgorithmen um die Features aus dem Sample zu extrahieren.
Wurden keine bedeutungsvollen einzigartigen Features gefunden, so muss das Sample in eine andere Dimension transformiert bzw. projiziert werden um eine verfeinerte Darstellung des Samples zu erhalten → „refined data". Nun erfolgen mehrere Testdurchläufe, um sicherzustellen, dass weitere Samples der selben Person weiterhin akzeptiert, von fremden Personen aber nicht toleriert werden. Nach diesen Testdurchläufen wird aus der „refined data" ein Template generiert.

Stimmen-, Iris-, Retina- und einige der Gesichtserkennungsverfahren nutzen diesen Ansatz mit Hilfe von Fourier- und Wavelettransformationen.

2.7.3 Vergleichs-Stufe (Comparison Stage)

In diesem Prozess wird das temporär erfasste (gescannte) Template eines Samples mit dem registrierten im System gespeichertem Template verglichen. Hierbei muss der Vergleichsalgorithmus berücksichtigen, dass sich die Samples von ein und der selben Person immer etwas unterscheiden, verursacht z.B. durch unterschiedlichen Druck des Fingers auf der Scanoberfläche oder durch einen anderen Winkel des Fingers beim Auflegen, etc. .
Man bekommt so gut wie nie von ein und der selben Person zwei mal genau das gleiche Sample. Der Algorithmus muss also so gewählt werden, dass er dies toleriert und gleichzeitig keinem Fremden Zugriff gewährt.

Wir haben bereits kennen gelernt, dass „biometrische Systeme“ sich in zwei Kategorien unterteilen lassen: Systeme zur Identifikation und Verifikation.

2.7.4 Entscheidungs-Stufe (Decision Stage)

In dieser letzten Phase entscheidet das System, ob das aus dem gescannten Sample extrahierte Template mit dem bereits registrierten Template übereinstimmt. Es wird dafür ein so genannter „matching score“ (Trefferquote) erzeugt. Um nun eine gezielte Antwort wie ‚ja’ oder ‚nein’ geben zu können, wird ein Schwellwert festgelegt. Ist der „matching score“ größer als der Schwellwert, so ist die Antwort ‚ja’, ansonsten ‚nein’.

2.8 Performanz des Systems

Wie bereits oben erwähnt, erfolgt ein Abgleich der biometrischen Daten des zu überprüfenden Samples mit dem gespeicherten Template. Durch diesen Abgleich wird ein Wert vergeben. Ist dieser Wert höher als der definierte Schwellwert, so wird der Zugang gewährt. Aufgrund dieser Technik, sind biometrische Verfahren flexibler als die Standardverfahren. Bei den konventionellen Verfahren wird ja lediglich durch die Eingabe einer PIN oder eines Passwortes der Zugriff gewährt oder verwehrt.

Betrachtet man nun die Performanz eines solchen biometrischen Systems, so gibt es zwei grundlegende Messwerte. Die so genannte „False Rejection Rate“ (FRR) und die „False Acceptance Rate“ (FAR). Die FRR wird auch als Typ-I-Fehlerrate bezeichnet, die FAR als

Typ-II-Fehlerrate. Die FRR bezieht sich auf die Anzahl der fälschlich vom System zurückgewiesenen autorisierten Personen. Die FAR beinhaltet die Anzahl der nicht-autorisierten Personen, die vom System akzeptiert wurden. Es gelten hierbei folgende Gesetzmäßigkeiten:

$$FRR = \frac{NFR}{NAA} * 100\% \qquad FAR = \frac{NFA}{NIA} * 100\%$$

NFR (number of false rejection) und NFA (number of false acceptances) stehen für die Anzahl der „falschen Zurückweisungen“ bzw. „falschen Akzeptierungen“. NAA (number of authorized identification attempts) ist die Anzahl der autorisierten Identifizierungs- oder Verifizierungsversuche. NIA (number of impostor identification attempts) ist die Anzahl der nicht autorisierten Anmeldeversuche (Hochstapler-/Betrugversuche).
Weniger gebräuchlich ist die sogenannte „Equal Error Rate“ (ERR), auch Crossover-Rate oder Gleichfehlerrate genannt. Sie bezieht sich auf den Schnittpunkt von FRR und FAR. Ein System beispielsweise mit einer FRR und FAR von 1% hat eine ERR von ebenfalls 1%.

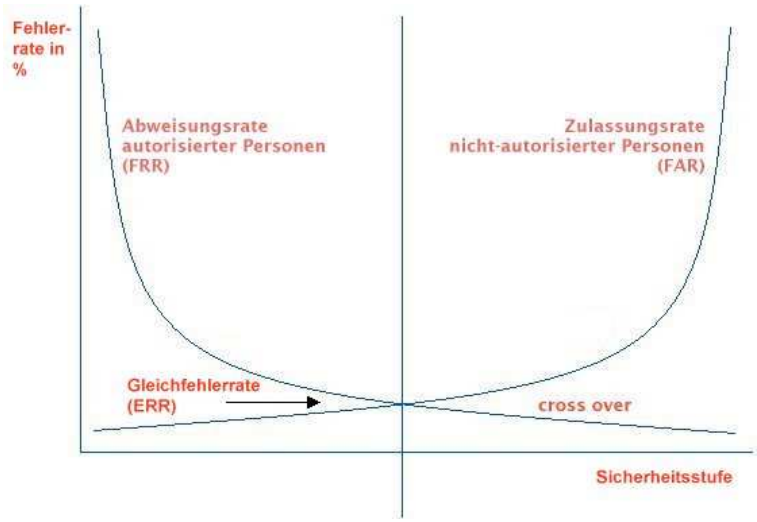


Abbildung 5 - FRR und FAR

Verringert man die FAR (False Acceptance Rate = fehlerhafte Zulassung Unberechtigter), vergrößert sich zugleich die FRR (False Rejection Rate = fehlerhafte Zurückweisung Berechtigter) und umgekehrt

Die Performanz eines biometrischen Systems, also FRR und FAR, ist abhängig von:

- den Umgebungsfaktoren (extreme Temperaturen und Feuchtigkeit beispielsweise können die Performanz eines biometrisches System beeinflussen)
- das Alter, der ethische Hintergrund und der Beruf des Benutzers
- der Religion, dem Willen, also der Akzeptanz des Benutzers (möchte ein Benutzer nicht mit dem System interagieren, so wirkt sich dies negativ auf die Performanz aus)
- der physikalische Zustand des Benutzers (ein Benutzer ohne Arme/Hände kann z.B. nicht die Signatur-Recognition nutzen)

Jeder dieser Faktoren kann die FRR und FAR beeinflussen. Es ist nun wichtig das Verhältnis zwischen FRR und FAR richtig zu gewichten. Mit ihnen lässt sich beispielsweise festlegen, ob wir eine „Ein-Versuch-Methode“ oder „Drei-Versuch-Methode“ realisieren wollen, d.h. der Benutzer hat einen oder drei Versuche sich zu identifizieren. Bei der letzteren verbessert sich natürlich auch zwangsläufig die FRR. Beide Werte können von einem Biometriker beliebig justiert werden. Eine Bank z.B. benötigt einen hohen und sicheren Zugangsschutz am Tresorraum. Unautorisierte Personen sollen hier unter keinen Umständen Zugang bekommen. Die Bank wird deshalb eine FAR unterhalb von 0,1% wählen. Mit anderen Worten soll das System also in max. einem von tausend Fällen einer nicht autorisierten Person den Zugriff gewähren. Um die Sicherheit weiter zu erhöhen kann auch eine FAR von 0,001% gewählt werden. Es muss jedoch bedacht werden, dass sich dadurch auch die FRR erhöht und sich damit als Konsequenz verschlechtert.

Es wird hieraus nun deutlich, dass die FRR und FAR Steuerungsmittel für die Performanz eines biometrischen Systems sind. Es muss jedoch auch berücksichtigt werden, dass die Anwendung selbst die Performanz eines Systems beeinflussen kann.

Um nun ein biometrisches System zuverlässig messen zu können sind weitere Performanz-Messgrößen nötig. Die so genannte „Receiver Operating Curve“ (ROC) und d’ sind die zwei geläufigsten Messgrößen. Die ROC zeigt das Verhältnis zwischen FRR und FAR in Bezug auf den Schwellwert an. Das statistische d’ dient als Trennungs-Indikator zwischen genuine-Verteilung und impostor-Verteilung. Es ist wie folgt definiert:

$$d' = \frac{\|Mimpostor - Mgenuine\|}{\sqrt{\frac{SD^2 impostor + SD^2 genuine)}{2}}}$$

wobei $M_{genuine}$, $M_{impostor}$, $SD_{genuine}$, $SD_{impostor}$ die Standardabweichung der genuine-Verteilung bzw. der impostor-Verteilung sind.

2.9 Wo können biometrische Systeme nun eingesetzt werden?

Die meisten biometrischen Applikationen sind immer noch im Teststadium und deshalb eher optional für Endanwender. Die Genauigkeit und Effektivität eines solchen Systems muss in einer Echtzeitanwendung überprüft werden. Im nächsten Kapitel werden gezielt verschiedene biometrische Anwendungen zur Personen-Authentikation betrachtet.
Prinzipiell können in jeder Situation, in der wir eine Interaktion zwischen Mensch und Maschine haben, biometrische Systeme integriert werden.

Biometrik kommt bereits in verschiedenen Bereichen zum Einsatz:

- Desktop PCs
- Netzwerke
- Bankwesen
- Telekommunikation (Netzwerke)
- Personalmonitoring (Anwesenheitskontrolle, Arbeitszeitmonitoring)
- Einwanderungskontrollen

Alle diese Anwendungsbereiche haben eines gemeinsam: Die Interaktion zwischen Mensch und Maschine!

Biometrische Anwendungen zur Personen-Authentikation lassen sich in folgende Bereiche unterteilen:

- **Polizei**: AFIS-Technologie (Automated Fingerprint Identification System)
- **Bankwesen**: Banken analysieren und prüfen seit Jahren den möglichen Einsatz von biometrischen Systemen zur Erhöhung der Sicherheit. ATM's (Bankautomaten) und Transaktionen sind potenziell gegenüber Betrügern gefährdet. Hier könnten biometrische Systeme, richtig angewandt, wesentlich mehr Sicherheit schaffen. Auch Telefon- und Internetbanking könnte so sicherer werden.
- **Computersysteme (Logical Access Control):** Biometrische Technologien haben bewiesen, das sie mehr als ‚nur' Computernetzwerke sichern können. Die Marktlage für die Biometrik-Industrie bietet momentan enormes Potential, gerade wenn man mal das Internet betrachtet (Internetbanking, persönliche Geschäftsdaten, Kreditkartennummer, medizinische Daten, und alle weiteren persönlichen Daten sind ein potentielles Angriffsziel).

Tabelle 1-1. Übersicht verschiedener biometrischer Applikationen

Biometrisches Merkmal	**Applikation**	**Mögliche Anwendung(en)**
DNA	Recognition	Forensik, Medizin, Genetik
Fingerabdruck	Recognition/Verifikation	Einwanderung, militärische Identifikation, Forensik, Zugangskontrolle
Gesicht	Verifikation/Recognition	Fahndung & Identifikation, vermisste Personen, Ausweise, Kreditkarten
Hand	Verifikation	Zugangskontrolle, Einwanderung
Unterschrift	Verifikation/Recognition	Unterschriftenverifikation,

		Identifikation anhand des Schriftbildes
Iris	Verifikation	Zugangskontrolle
Stimme	Verifikation/Recognition	Stimmenverifikation, Stimmenidentifikation, Zugangskontrolle

- **Zugangskontrolle(n):** Schulen, AKW, militärische Stützpunkte, Krankenhäuser, und Botschaften (öffentliche Einrichtungen) könnten durch biometrische Systeme sicherer werden. Gerade wenn es um eine Zugangskontrolle z.B. zu einem AKW geht, wäre eine biometrische Kontrolle weitaus sicherer als nur ein Schlüssel oder eine PIN-Abfrage alleine.

Mit biometrischen Verfahren lässt sich der Zutritt zu Gebäuden, Räumlichkeiten, sowie der Zugang zu Informationstechnologie in all ihren verfügbaren Ausprägungen - wie Computer, Anwendungen und IT-Netze realisieren und kontrollieren.

Weitere Einsatzbereiche sind mit entsprechenden Verfahren bereits Realität, wie z.B. Grenz- und Einwanderungskontrollen, Dokumentenausstellung, biometrische Wegfahrsperre für Autos, oder vorstellbar, wie „Check-In“ auf Flugplätzen, Identifizierung am Geldausgabeautomaten, oder das ausschließliche Benutzen von Waffen durch den Besitzer. Darüber hinaus können biometrische Verfahren im Zusammenhang mit der Abgabe von Willenserklärungen im elektronischen Rechtsverkehr eingesetzt werden. Wenn Dokumente mit der digitalen Signatur versehen werden, kann zur Freischaltung des privaten Schlüssels - und somit als Zugangsberechtigung zur Erzeugung der Signatur - anstatt einer PIN mit Chipkarte ein biometrisches Merkmal eingesetzt werden.

2.10 Biometrische Verfahren im Überblick:

- **Fingerabdruckerkennung**
- **Handlinienerkennung**
- **Handgeometrieanalyse**
- **Gesichtsgeometrieerkennung**
- **Irismustererkennung**
- **Gefäßstruktur der Retina**
- **Stimme → Sprachanalyse**
- DNA-Analyse
- Erkennung durch Wärmeverteilungsmuster
- Erkennung durch die Tastaturanschlagsdynamik
- Erkennung anhand der Gangart einer Person
- Erkennung anhand des Geruchsmusters einer Person
- Erkennung anhand der Ohrmuschelgeometrie

Die fettgedruckten Verfahren werden im nachfolgenden Kapitel genauer behandelt.

3 EINIGE BIOMETRISCHE AUTHENTIKATIONSVERFAHREN IM DETAIL

3.1 Iris-Erkennung (Iris-Recognition)

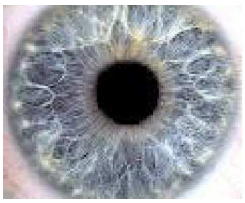


Abbildung 6 - Irismuster

3.1.2 Grundlagen:

- Iris = griech. für Regenbogenhaut
- ringförmiger Augenmuskel zwischen Hornhaut und Linse
- beim Wachstum reißt die Regenbogenhaut auf; es entstehen charakteristische und komplexe Muster aus Bändern, Furchen, Stegen und Gruften – ein fast perfekter Zufallsprozess
- reguliert durch Änderung der Pupillenweite den Lichteinfall in das Auge
- besitzt randotypische Merkmale, die während der Schwangerschaft ausgebildet werden

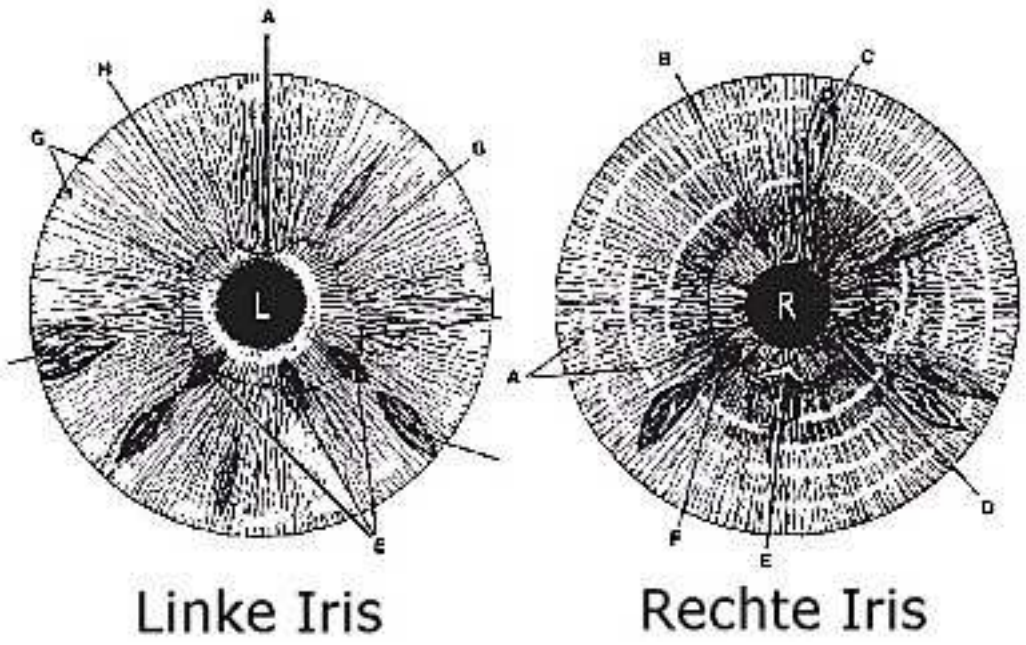


Abbildung 7 - Linke und rechte Iris

Sogar linke und rechte Iris eines Menschen sind verschieden

Enrollment:

- Aufnahme eines Bildes der Iris
  - im Infrarot-Spektrum, damit der Benutzer nicht geblendet wird
  - Kombination aus Weitwinkel- und Zoomkameras
- Selektion der Iris mit Hilfe von Wavelets und der Fourieranalyse
- Kodierung der Iris
  - Iris Code: 2048 Bit Vektor
  - komplexes Gabor-Wavelet wird mehrfach mit verschiedenen Variablenbelegungen über das Irisbild berechnet

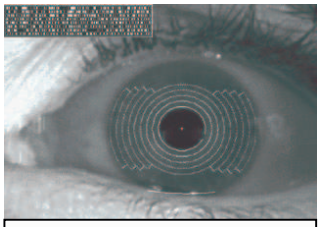


Abbildung 8 – Iriserkennung

Auswertung:

- Hamming-Distanz zwischen zwei Iris-Codes
- Vergleich von gescannter und gespeicherter Iris

3.1.3 Probleme der Iriserkennung

- Iris und Kopf bewegen sich laufend
- „kleine“ Iris auf „großem“ Kamerabild
- Augenlieder zucken über das Bild
- feuchte und gewölbte Augenoberfläche → Reflexionen
- Aussehen der Iris ist durch Krankheiten veränderbar → mögliche Gefahr!

Abbildung 9 – offenes und geschlossenes Auge

3.1.4 Anwendungen

- Typische Anwendungsgebiete
    - Bankautomaten
    - Zutrittskontrolle zu Gebäuden, Räumen (AKW)
    - Anmeldung am PC

- KnoWho-Authentication Server
    - Software von Iridian Tech.
    - arbeitet u.a. mit der Authenticam™ zusammen

- Wincor Nixdorf ProCash ATM
    - Bankautomat Pilotprojekt der Dresdner Bank in Frankfurt
    - bisher nur für Angestellte zugänglich (Stand: Sommer 2001)
    - in GB und den USA bereits seit 1999 Iris-gestütze ATM's im Einsatz

3.1.5 Produkte

LG Electronics Iris Access 3000™

Abbildung 10 - LG Electronics Iris Access 3000™

- Zugangskontrollsystem für Räume
- eingebettete Systeme an Türen sind mit einem zentralen Server verbunden

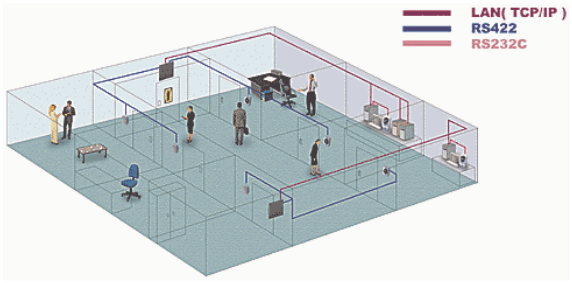


Abbildung 11 - LG Electronics: Netzverbund

Abbildung 12 – Panasonic Authenticam™

Panasonic Authenticam™ EyePicture BM-ET100US

- Zugangskontrolle für einen Windows PC via USB-Kamera und Software von Iridian
- Entfernung zur Iris während der Authentikation: 48-53 cm
- Preis: 239 $ (Stand: Februar 2002)

3.1.6 Abschließende Bewertung der Iriserkennung:

- sicher, aber kostenintensiv
- relativ kompliziert in der Benutzung (passive Systeme)
- Probleme mit der Benutzerakzeptanz

3.2 Fingerabdruck-Erkennung (Fingerprint-Recognition)

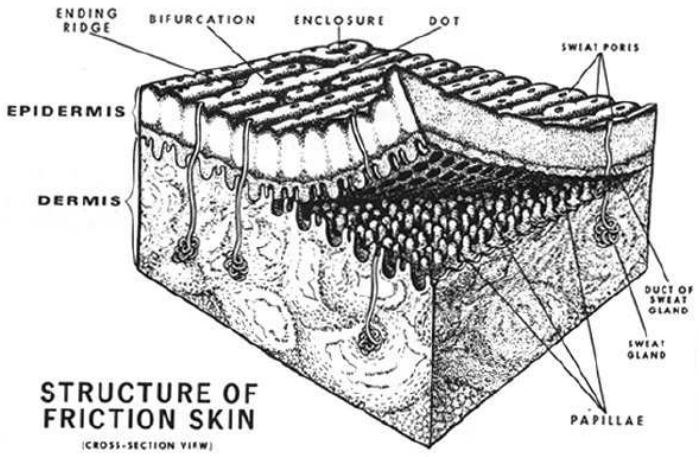


Abbildung 13 - Hautschema

3.2.1 Grundlagen

- die Ausbildung der Papillarlinien erfolgt rein zufällig innerhalb der ersten Lebenswochen
- es erfolgt laufend eine identische Reproduktion des Musters von der unterliegenden Dermis
- Fingerabdruck: Bild der erhöhten Papillarlinien
- Minutien: Linienenden und -verzweigungen als charakteristische Punkte

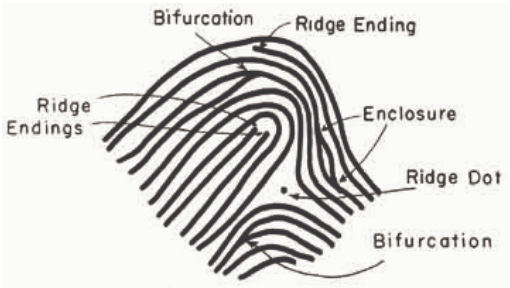


Abbildung 14 - Minutien

- Position der Minutien, Richtung und Zahl der Linien zwischen Minutien, sowie die Linienform sind charakteristisch
- zehn bis zwölf Minuten sind insgesamt (pro Abdruck) nötig, um einen menschlichen Fingerabdruck eindeutig zu identifizieren
- ältestes biometrisches Verfahren (Kriminalistik: AFIS)

3.2.2 Enrollment

- Aufnahme eines Fingerabdruckbildes mit Hilfe eines Sensors
- alle Sensoren erzeugen im Endeffekt ein Graustufenbild
- es wird mit einer Auflösung von 250 bis 625 dpi gearbeitet
- es existieren verschiedene Sensortypen: optische, kapazitive, Ultraschall, E-Feld, thermische und elektro-optische Sensoren
- Bestimmung des Orientierungsfeldes
- Vordergrund/Hintergrundtrennung
- Binarisierung (Umwandlung in Schwarz/Weiß-Bild mittels Schwellwert)
- Skelettierung (Randpixel entfernen bis dünne Linien übrigbleiben)
- eigentliche Merkmalsextraktion (Erkennung von Minutien durch Betrachtung der Pixel-Nachbarn)
- Vergleichsalgorithmen → Minutienpositionen, Radius und Struktur, Rillenzählung, Graphenvergleich, Gitterlegung
- Matching

3.2.3.1 Optische Sensoren:

Hierbei liegt der Finger flach auf der Oberfläche eines Prismas. Der aufliegende Finger wird mit einfarbigem Licht bestrahlt. Es wird eine gute Bildqualität erzielt. Die Aufnahme ist jedoch aufgrund des verwendeten Weitwinkels recht groß.

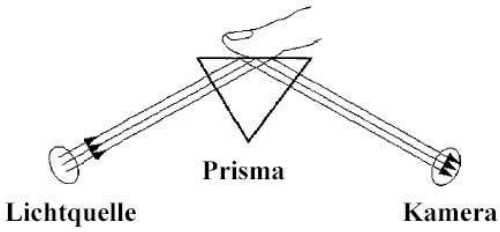


Abbildung 15 - Schema: Optischer Sensor

Abbildung 16 - morphosoric® Optiscan II

3.2.3.2 Kapazitive Sensoren:

Hier wird ein Raster von Kondensatorplatten als Sensorelement verwendet → Messung der Leitfähigkeit auf der Hautoberfläche, wobei die Kapazität an den aufliegenden Hautlinien größer ist. Kapazitive Sensoren sind recht klein und deshalb gut integrierbar. Sie sind jedoch empfindlich gegenüber elektrischer Aufladung.

Abbildung 17 - Infineon - Biometrics - FingerTIP™

3.2.3.4 Ultraschall Sensoren:

Diese Sensoren messen die durch die Kontaktstreuung verursachten Signale und berechnen das Bild der Struktur, das ihre Sensorfläche berührt. Die Kontaktfläche des Geräts, an das die zu untersuchende Struktur angelegt ist, wird von der rechten Seite von einer Ultraschallwelle erreicht. Die Wellen, die durch das angelegte Objekt kontaktgestreut werden, empfängt ein Schallwandler (T), der eine Ringbewegung ausführt, deren Achse senkrecht zu der Kontaktoberfläche (x-y) ist (der gleiche Wandler kann natürlich auch als Sender dienen; möglich ist auch die Nutzung von mehreren unbeweglichen, statt eines beweglichen Wandlers.).

Um die Struktur mit einer Genauigkeit von ca. 0,1 mm aufzulösen, ist es nötig, die Information aus etwa 256 Richtungen zu sammeln. Es wird demnach in jede dieser Richtungen ein kurzer Impuls gesendet und eine Impulsantwort empfangen (die im Falle eines Fingers ein Frequenzspektrum von ca. 4-16 MHz hat - aufgrund der gewählten Geometrie des Geräts).

- Auflösung: 1000 dpi

- unempfindlich gegenüber Einfluss von Schmutz und Feuchtigkeit → aber kälteempfindlich

Abbildung 18 - Außenansicht der Kamera der Firma Optel

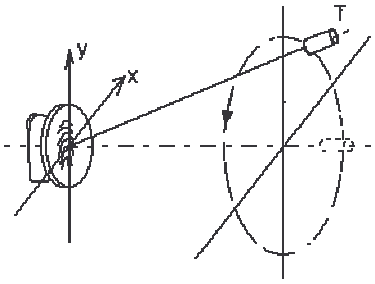


Abbildung 19 - Schema des Geräts

3.2.3.5 E-Feld Sensoren:

- ähnlich kapazitivem Sensor; Messung des elektrischen Feldes
- Erkennung der Hautunterschichten unabhängig von Schmutz, etc.

3.2.3.6 Thermische Sensoren:

- ähnlich dem kapazitivem Sensor
- Messung von Temperaturdifferenzen

3.2.3.7 Elektro-Optische Sensor-Chips:

- licht-emittierender TactileSense™ Polymer
- erzeugt zunächst optische, dann digitale Bilder
- klein und preiswert

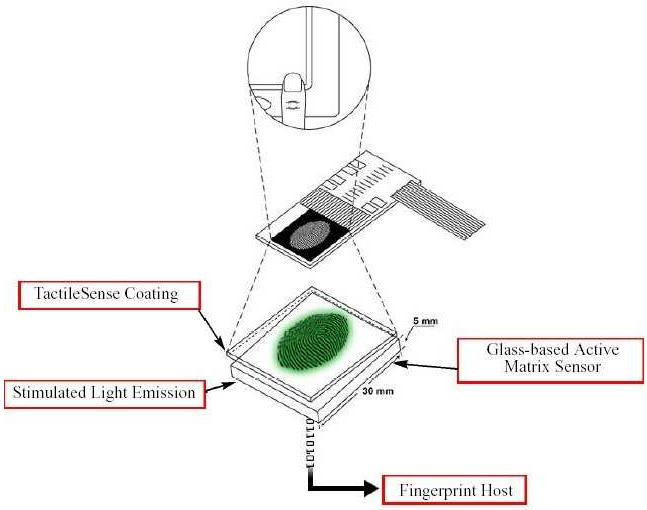


Abbildung 20 - Aufbau: Elektro-Optische Sensor-Chip

Abbildung 21 - TactileSense™ Platine

Abbildung 22 - Enrollment und Verifikation: Who Vision Software / Tactile Sense™

3.2.4 Fingerabdrucktypen:

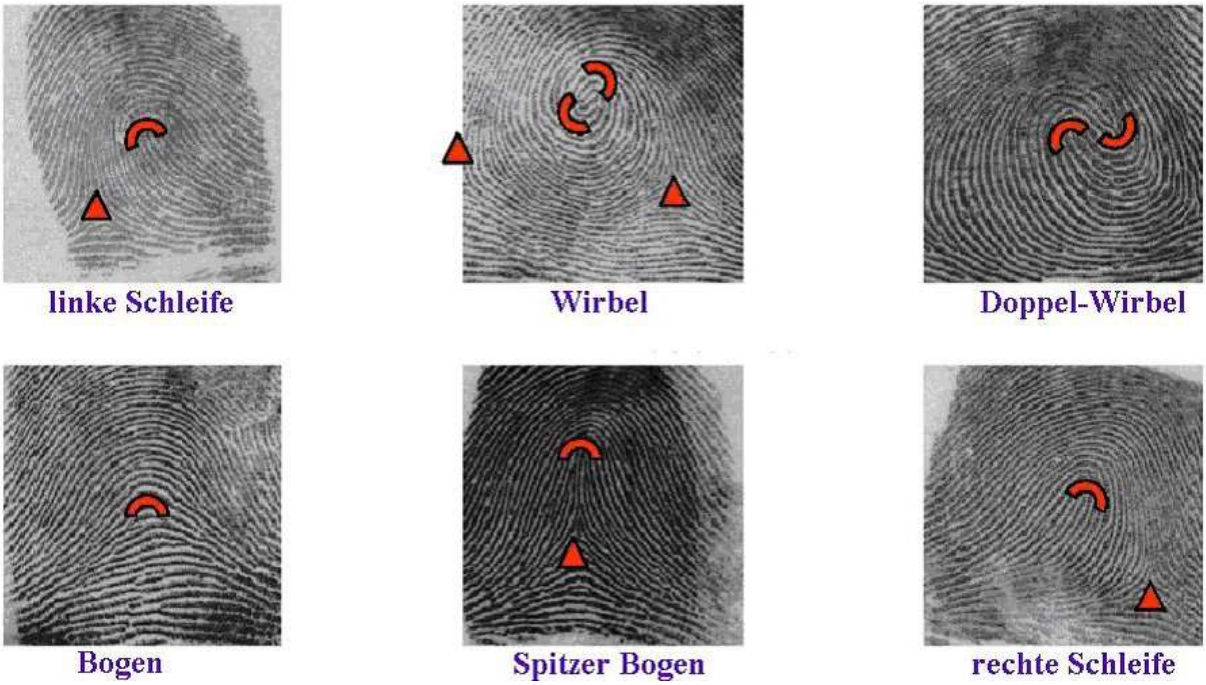


Abbildung 23 - Fingerabdrucktypen

Singuläre Punkte:

Core (◠)= maximale Krümmung zweier Linien (U-Turn)

Delta (▲) = zwei parallele Linien divergieren (Dreiecksform)

Durch zur Hilfename bestimmter Bezugspunkte ist hierüber eine Klassifizierung der Abdrücke möglich.

3.2.5 Probleme bei Bildaufnahme und Verarbeitung:

- Translation (unterschiedliche Position des Fingers auf dem Sensor)
- Rotation (unterschiedliche Orientierung des Fingers auf dem Sensor)
- unterschiedliche Skalierung (nicht-lineare Deformationen des Abdrucks → Verzerrung)

Abbildung 24 - Ausweis aus dem Jahre 1943

Zur Erinnerung: Ausweis aus jener Zeit (1943): Auch damals waren schon biometrische Merkmale im Ausweis erfasst.

3.2.6 Abschließende Betrachtung der Fingerabdruckverfahren:

- ältestes biometrisches Verfahren
- relativ geringe Kosten
- einfach zu benutzen
- Fingerabdrucksensoren sind klein und dadurch gut integrierbar

3.3 Handgeometrie (Palm/Hand-Recognition)

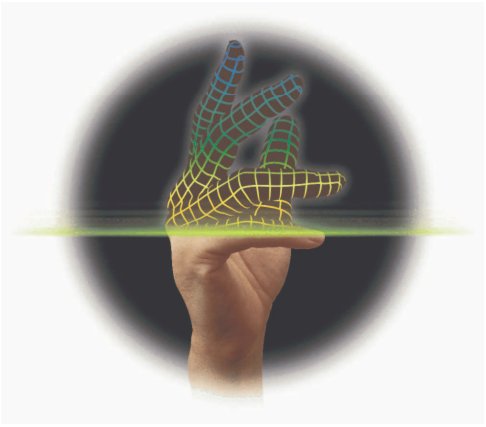


Abbildung 25 - Handgeometrie

3.3.1 Enrollment

1. Einlesen des Bildes einer Hand
    - Venen-Scan → mit IR-Kamera die Venen auf dem Handrücken scannen
    - Handflächen-Scan

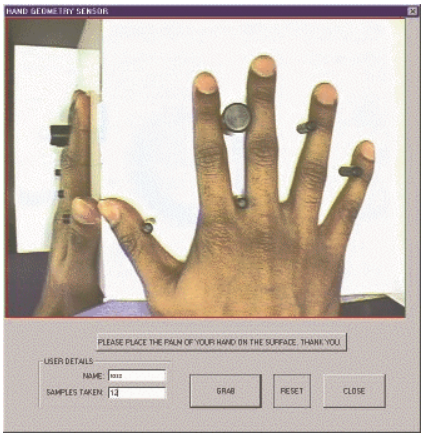


Abbildung 26 – Handflächenscan I

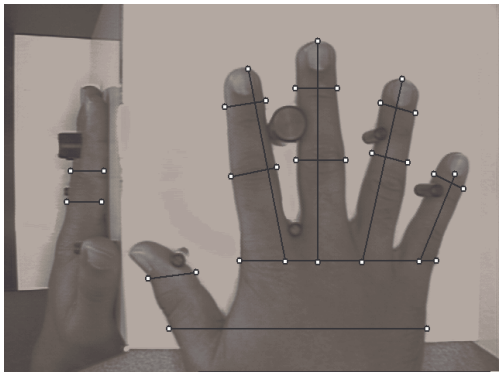


Abbildung 27 – Handflächenscan II

2. Ermittlung von Hand-Charakteristika
    - Messung der Länge, Breite und Dicke der Finger
    - über Spiegel wird die Seitenansicht der Hand berücksichtigt

3.3.2 Produkte

Abbildung 28 – Hand Punch 4000™

Abbildung 29 - San Francisco International Airport

HandPunch4000™

- Zugangskontrolle
- Verifikationszeit: weniger als eine Sekunde
- Benutzerkapazität: 530 (Aufrüstbar auf 3498)
- Templategrösse: 9 bytes

HandNet™ for Windows

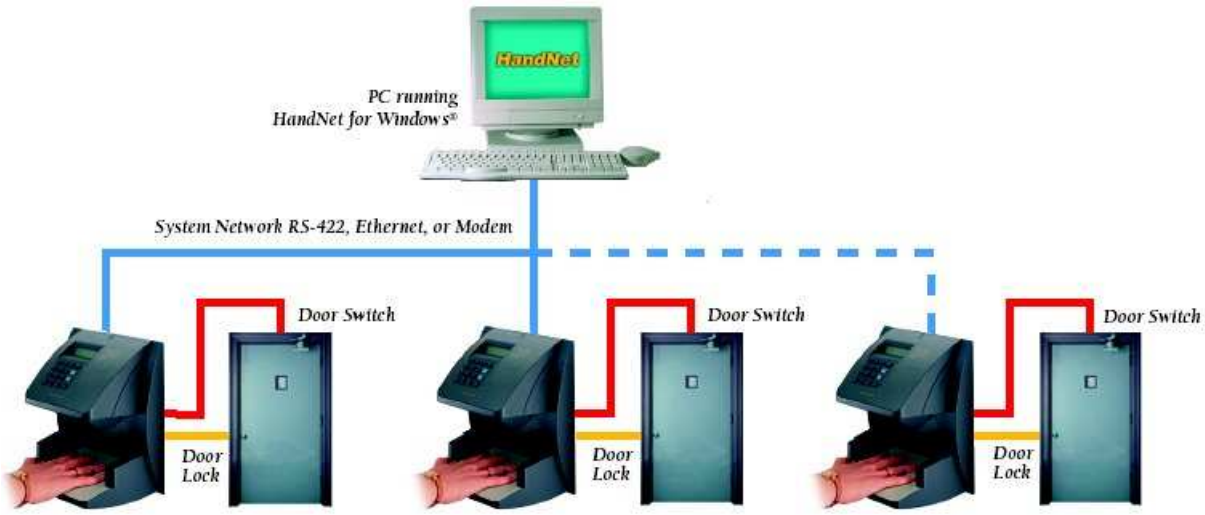


Abbildung 30 - HandNet™ for Windows - Übersicht

- Zugangskontrolle & Monitoring
- kein dedizierter PC notwendig
- max. Benutzeranzahl: 100.000

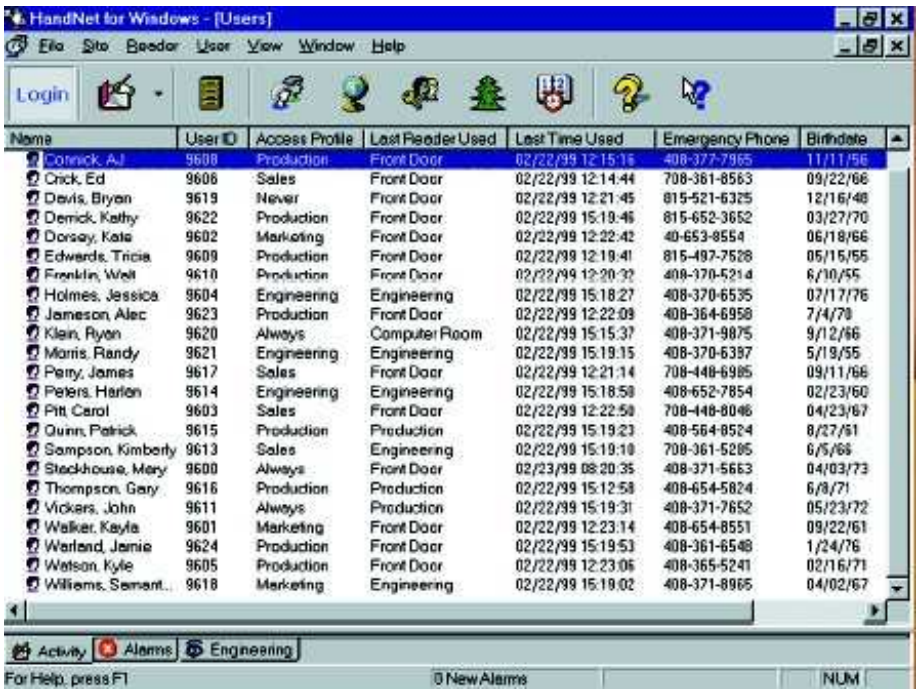


Abbildung 31 - HandNet™ for Windows - Screenshot

3.3.3 Abschließende Bewertung der Handgeometrieverfahren:

- Analyse der dreidimensionalen Beschaffenheit der Hand → Handgeometrie
- relativ große Sensoren
- mittlere Sicherheit
- Systeme sind noch relativ teuer

3.4 Gefäßstrukturen der Retina (Retina-Recognition)

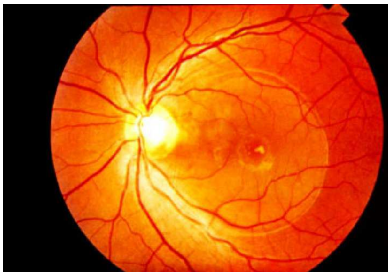


Abbildung 32 – Retina

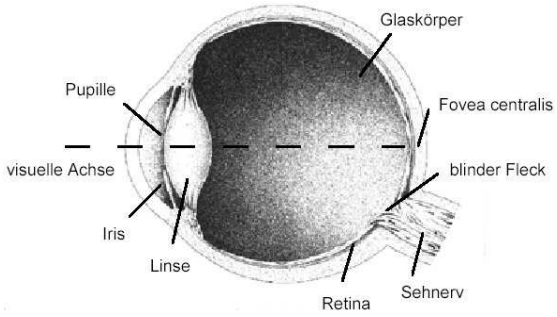


Abbildung 33 - Augenaufbau

3.4.1 Grundlagen:

- kleidet die hintere, innere Fläche des Auges aus
- enthält die Fotorezeptoren
- ca. 0.4 cm breit
- ca. 50% der Lichtquanten erreichen die Netzhaut

3.4.2 Enrollment

- Einlesen des Bildes einer Retina
- Ermittlung von Retinacharakteristika

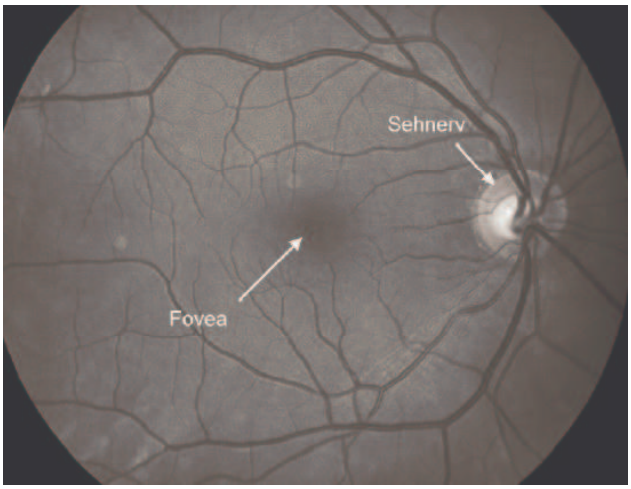


Abbildung 34 – Retina: Fovea / Sehnerv

3.4.3 Produkte

Abbildung 35 – EyeDentify™

Aus der Betriebsanleitung für den EyeDentify™

- zur Erfassung bitte “E” auf dem Keyboard drücken (Enrollment-Start)
- über das Keyboard muss nun eine fünfstellige Zahl eingegeben werden
- ebenfalls über das Keyboard wird nun ein Benutzername eingegeben
- bevor nun auf „Yes-Enroll Now“ geklickt wird, muss der Benutzer direkt in die RetinaScan-Vorrichtung gucken
- jetzt auf „Yes“ klicken
- der Benutzer muss nun seinen Kopf sehr still halten und das Auge möglichst nicht bewegen. Dieses ist der schwierigste Schritt, da viele Benutzer es nicht auf Anhieb schaffen ihr Auge bzw. den Kopf ruhig zu halten.
- ist das Sample gut genug (Rückgabewert 4-5), so kann das Enrollment abgeschlossen werden
- bitte in diesem Fall mit der „FIN“-Taste bestätigen

3.4.4 Abschließende Bewertung der Retinaverfahren:

- sehr sicher
- kostenintensiv
- (noch) kompliziert in der Benutzung
- Probleme mit der Benutzerakzeptanz

3.5 Gesichtsgeometrie-Erkennung

Abbildung 36 – Elastic Graph Matching I

Gesichtserkennungsverfahren werden, im Vergleich zu anderen biometrischen Zugangskontrollverfahren, recht gute Marktchancen eingeräumt. Vor allem wegen ihrer schon vorhandenen Integration in das Lebensumfeld der Anwender spricht einiges für diese Technik: Der Blick in eine Kamera ist für viele Menschen weitaus normaler als etwa die Vorstellung, sich mit Infrarotstrahlen in die Augen leuchten zu lassen oder einen Fingerabdruckleser zu gebrauchen, der womöglich an die erkennungsdienstliche Behandlung bei der Polizei erinnert (AFIS).

3.5.1 Verfahren/Enrollment

- Zwei Verfahren: „Elastic Graph Matching“ & „Eigenfaces“

3.5.2.1 Elastic Graph Matching:

- Erfassung besonderer Merkmale des Gesichts mit Hilfe von Graphen
- „Elastic Graph Matching“: Hierbei wird ein Gitter über das Gesicht gelegt und an den Knotenpunkten ein kleiner lokaler Umkreis betrachtet
- die Suche richtet sich insbesondere auf wichtige Punkte wie Augen- oder Mundwinkel, Nasenspitze und so weiter
- innerhalb des Vergleichsbilds gilt es, diese Gitterpunkte (innerhalb gewisser Toleranzgrenzen) aufzufinden, wobei die Relation der Punkte untereinander aufgrund der Gitterstruktur automatisch erhalten bleibt
- die ausgewählten Punkte bilden dann eine Art verbogenes elastisches Gitter

- die Übereinstimmung der Merkmale selbst, sowie der Grad der zur Wiedererkennung notwendigen Verbiegungen ergeben einen zuverlässigen Vergleichswert

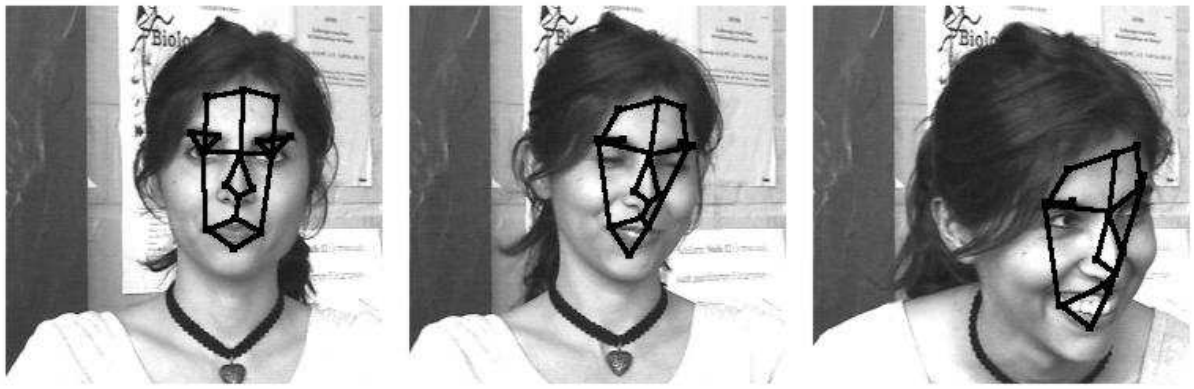


Abbildung 37 – Elastic Graph Matching II

3.5.2.2 Eigenfaces:

- Approximation eines Gesichtes durch Kombination von Basisgesichtern
- Kombination kompletter Gesichter
- die meisten Verfahren arbeiten mit einem Satz von etwa 100 Basisbildern und versuchen durch Positiv- und Negativkomposition das Abbild des gegebenen Gesichtes möglichst originalgetreu nachzubilden

Abbildung 38 - Standard Eigenfaces

3.5.3 Abschließende Bewertung der Gesichtserkennungsverfahren:

- relativ günstige Sensoren
- hohe Benutzerakzeptanz
- Erkennung relativ schwierig → höhere Fehleranfälligkeit
    - wechselnde Belichtungsverhältnisse
    - zeitweiliges Tragen einer Brille
    - starke Gewichtsabnahme führt auch zu Veränderungen im Gesicht

3.6 Sprechererkennung

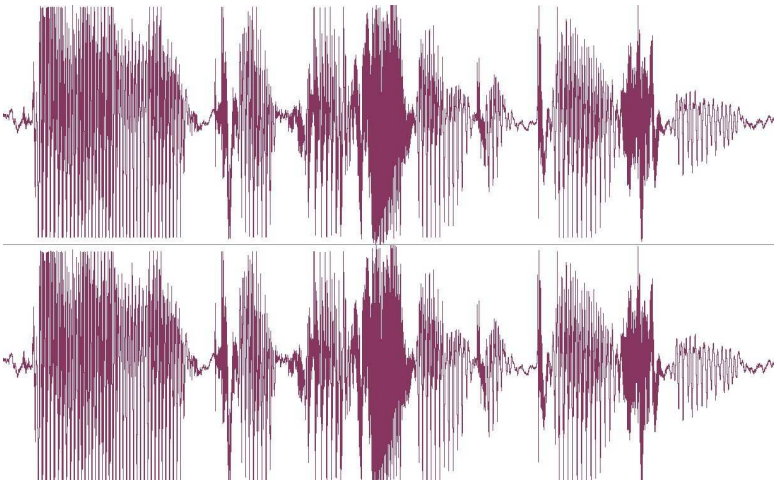


Abbildung 39 – Darstellung der Sprachsignale beim Aussprechen des Satzes: „Biometrische Authentikation“

3.6.1 Sprache wird durch zwei Vorgänge erzeugt:

- Phonotation (Sprachanregung)
  - Luftröhre, Lunge
- Artikulation (Sprachformung)
  - Kehlkopf, Mund-, Nasen-, und Rachenraum

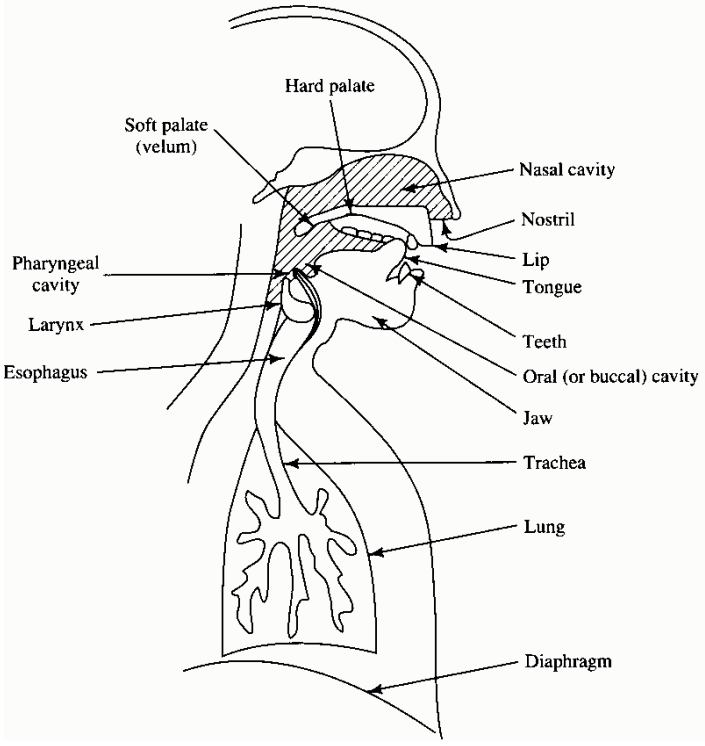


Abbildung 40 – Sprachsystem - Schema

Das kleinste Element der Sprache ist das Phonem. Spricht eine Person ein bestimmtes Phonem mehrmals hintereinander, so wird jedes Mal ein anderes akustisches Signal erzeugt. Sprachsignale sind innerhalb eines kurzen Zeitfensters konstant (etwa 5-100 ms).

Man unterscheidet Stimmverifikation, der Vergleich erfolgt mit einem abgespeicherten Referenzmuster, und Stimmidentifikation, der Vergleich erfolgt mit allen gespeicherten Referenzmustern.

3.6.2 Man unterscheidet folgende Systeme:

- Closed-Set-Systeme (nur registrierte Benutzer werden verglichen)
- Open-Set-Systeme (evtl. befinden sich nicht alle Benutzer in der DB → fehlende Benutzer können in diesem Fall registriert/enrollt werden)
- Closed-Line-Systeme (unmittelbare Aufnahme → z.B. Diktiergerät)
- Open-Line-Systeme (indirekter Zugang, z.B. via Telefon)
- Textabhängige Systeme (direkter Vergleich mit abgespeicherten Referenzdaten)
- Textunabhängige System (statistische Analyse)
- Systeme mit vorgegebenem Text (text-prompted)
- Diskrete Systeme (nach jedem Wort erfolgt eine Pause)
- Kontinuierliche Systeme (natürlicher Sprachfluss möglich)

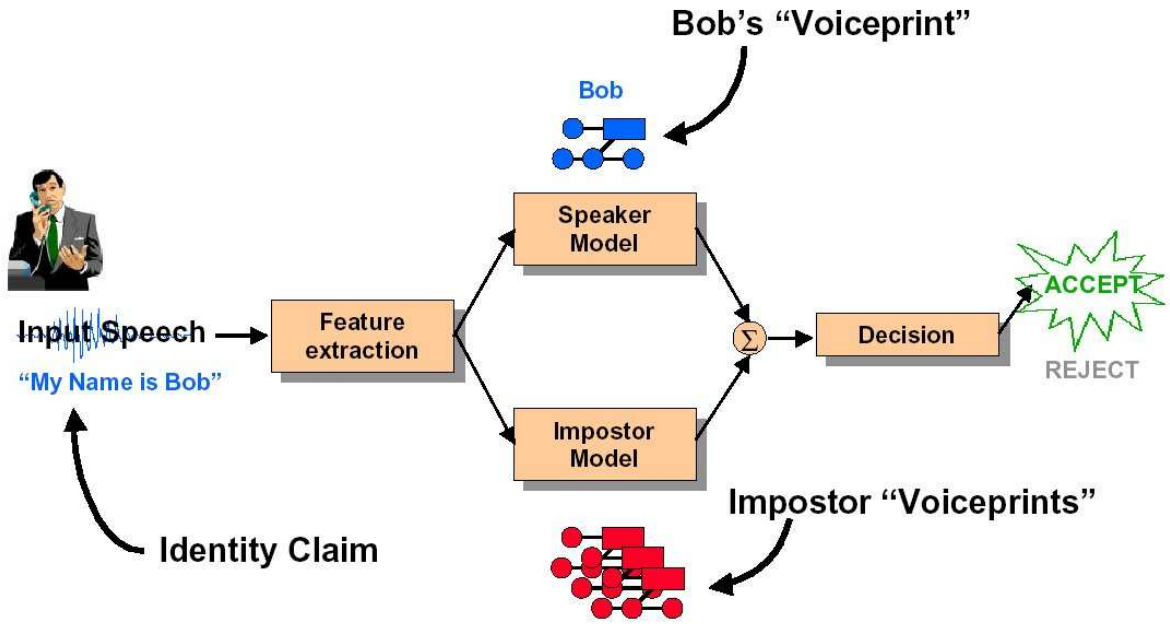


Abbildung 41 – Sprechererkennung: Schema

3.6.3 Enrollment

- Benutzer spricht einige Beispielsätze
- Merkmalsextraktion
- Generierung eines Templates

3.6.4 Verifikationsphase

- Benutzer gibt seine ID an (SmartCard, etc.)
- Benutzer spricht Satz/Schlüsselwort
- Vergleich der aktuellen Eingabe mit gespeichertem Template
- Generierung einer Trefferpunktzahl (Score)
- Score wird mit Schwellwert verglichen
- Entscheidung: Annahme/Zurückweisung

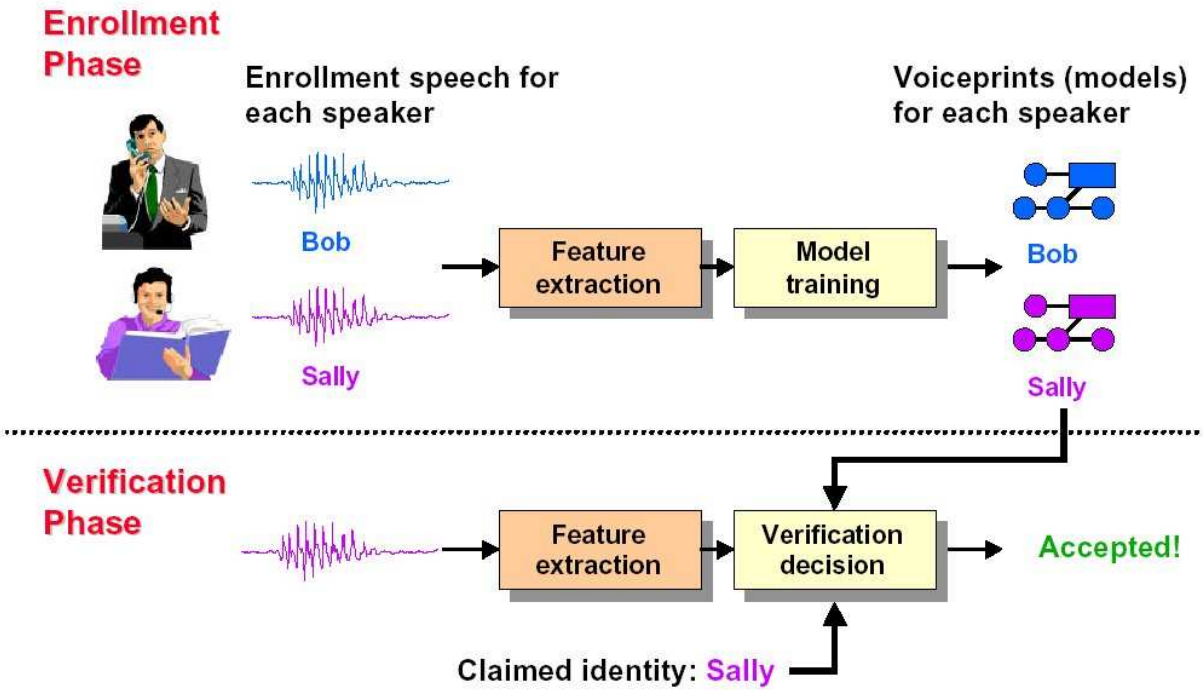


Abbildung 42 – Sprechererkennung: Enrollment und Verifikation

3.6.5 Verschiedene Verfahren möglich:

- FFT (Fast Fourier Transformation)
- HMM (Hidden Markow Model)
- Neuronale Netzwerke

3.6.6 Hidden Markow Model:

- endlicher Automat
- ein HMM pro Sprecher
- Wege stellen die Wahrscheinlichkeiten für die Folge „Zustand j nach Zustand i“ dar
- Wege mit der maximalen Wahrscheinlichkeit werden verglichen

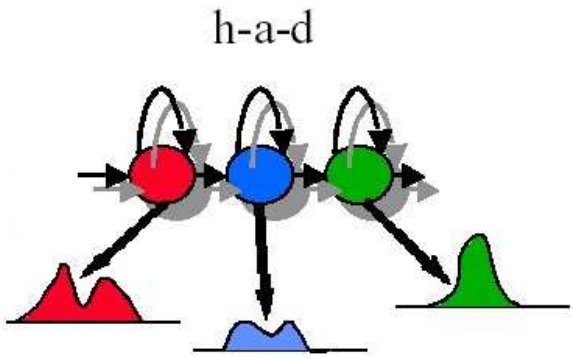


Abbildung 43 – Hidden Markow Model

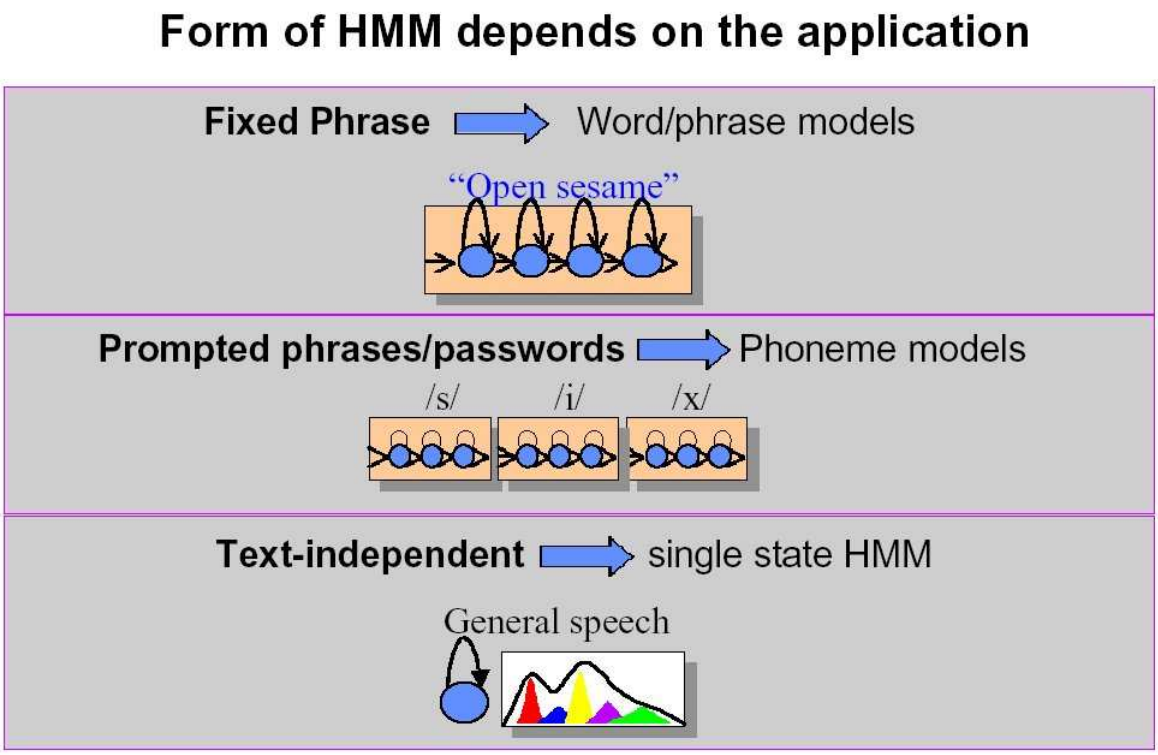


Abbildung 44 – HMM - Übersicht

3.6.7 Künstliche Neuronale Netze (KNN):

- bekannte Sprecher werden nicht durch individuelle Templates repräsentiert
- Training einer Funktion, die alle bekannten Sprecher am besten voneinander abgrenzt
- Vorteil: da es nach wie vor keinen Konsens darüber gibt, welche Merkmale eines Sprachsignals einen Sprecher am besten charakterisieren, müssen diese Merkmale nicht exakt modelliert werden
- Nachteil: bei jedem hinzugekommenen Sprecher müssen KNN neu trainiert werden
- bekannte Verfahren: „Time Delay Neuronal Networks" (TDNN), „Recurrent Networks" und „Hybride Netze"

3.6.8 Abschließende Betrachtung der Sprachanalyse:

- Erkältung oder Krankheit erhöht u. U. FRR
- Hintergrundgeräusche können das Verfahren beeinträchtigen
- unterschiedliche Geräte (im Gebäude / außerhalb des Gebäudes) → Kosten

4 ANFORDERUNGEN AN EIN BIOMETRISCHES SYSTEM

Wie bereits in den vorigen Kapiteln erwähnt, sollen hier noch einmal die generellen Anforderungen an ein biometrisches System verdeutlicht werden.

4.1 Ein biometrisches Verfahren wird durch folgende Anforderungen bestimmt:

- ***Universalität*** – jede Person verfügt über das biometrische Merkmal
- ***Einzigartigkeit*** – die Ausprägungen eines biometrischen Merkmals sind von Person zu Person unterschiedlich
- ***Permanenz*** – die biometrischen Merkmale sind dauerhaft
- ***Messbarkeit*** – die biometrischen Merkmale sind quantitativ erfassbar
- ***Performanz*** – in Bezug auf Genauigkeit, Schnelligkeit und Robustheit eines Verfahrens
- ***Akzeptanz*** – ein biometrisches Verfahren wird von den Benutzern akzeptiert
- ***Sicherheit*** – ein biometrisches System ist gegen Fälschungen sicher

4.2 Darüber hinaus sind, gerade im Zusammenhang mit der elektronischen Signatur, folgende weitere Faktoren wichtig:

- Kosten
- Benutzerfreundlichkeit
- Wartungsaufwand
- Eignung für den stationären (Büro oder öffentliches Terminal) oder mobilen Einsatz (PDA, Handy, Notebook)

Bei der Benutzerfreundlichkeit einzelner biometrischer Verfahren muss zwischen aktiven und passiven Systemen unterschieden werden.

Bei einem passiven System muss der Benutzer das biometrische Merkmal selber in eine bestimmte Aufnahmeposition fokussieren (z.B. Auge oder Gesicht). Bei einem aktiven System erfolgt eine automatische Fokussierung durch das System selbst.

4.3 Relative biometrische Brauchbarkeit

Dabei handelt es sich um ein Maß für die Bewertung eines biometrischen Verfahrens anhand folgender Faktoren:

- Universalität des biometrischen Verfahrens
- Einzigartigkeit des biometrischen Verfahrens
- Permanenz des biometrischen Verfahrens
- Messbarkeit des biometrischen Verfahrens
- Performanz des biometrischen Verfahrens
- Akzeptanz des biometrischen Verfahrens
- Sicherheit des biometrischen Verfahrens

Anhand dieser gewichteten Faktoren lässt sich ein biometrisches Verfahren bewerten und somit die so genannte relative biometrische Brauchbarkeit festlegen.

4.4 Bewertung biometrischer Verfahren* anhand der relativen biometrischen Brauchbarkeit

Biometrisches Verfahren	Universalität → besser	Einzigartigkeit → besser	Permanenz → besser	Messbarkeit → besser	Performanz → besser	Akzeptanz → besser	Sicherheit → besser
Fingerabdruck	■■■■	■■■■■■■■	■■■■■■■■	■■■■	■■■■■■■■	■■■■	■
Gesicht	■■■■■■■■	■■■■■■■■	■■■■	■■■■■■■■	■	■■■■■■■■	■■■■
Handgeometrie	■■■■	■■■■	■■■■	■■■■■■■■	■■■■	■■■■	■■■■
Iris	■■■■■■■■	■■■■■■■■	■■■■■■■■	■■■■	■■■■■■■■	■	■■■■■■■■
Retina	■■■■■■■■	■■■■■■■■	■■■■	■	■■■■■■■■	■	■■■■■■■■
Dyn. Signatur	■	■	■	■■■■■■■■	■	■■■■■■■■	■■■■
Sprecher	■■■■	■	■	■■■■	■	■■■■■■■■	■■■■
Tippverhalten	■	■	■	■■■■	■	■■■■	■■■■
Venenstruktur	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■

Tabelle: Relative biometrische Brauchbarkeit – Stand: Februar 2002

* = siehe Abbildung 2 – Kapitel 1

zum Teil aus [2]

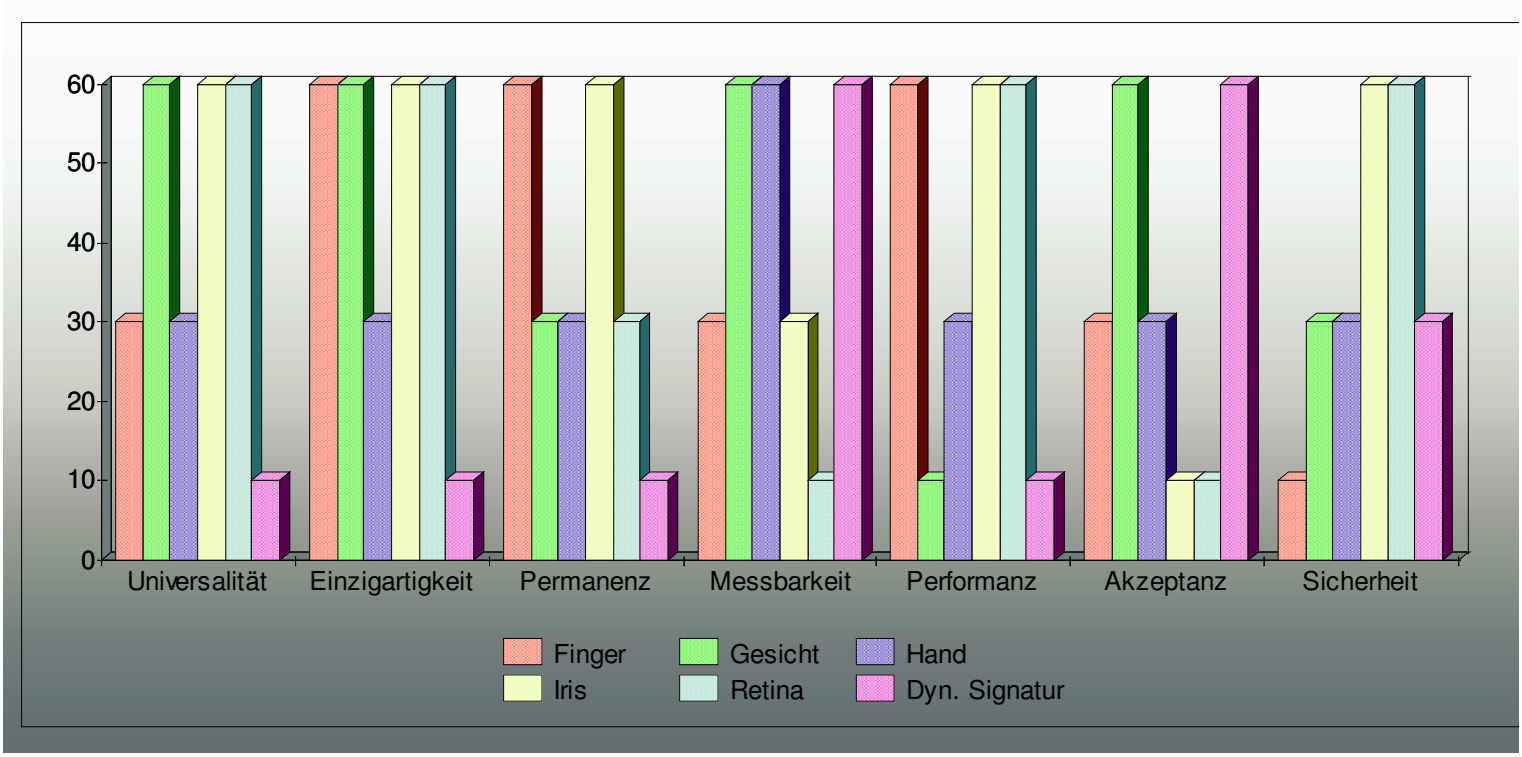


Abbildung 45 – Relative biometrische Brauchbarkeit

4.5 Bewertung der biometrischen Verfahren in bezug auf Kosten, Benutzerfreundlichkeit und Wartungsaufwand

Biometrisches Verfahren	Kosten ← besser	Benutzerfreundlichkeit → besser	Wartungsaufwand ← besser
Fingerabdruck	■	■	■■■■
Gesicht	■	■■■■■■■■ (AS) ■ (PS)	■■■■
Handgeometrie	■■■■■■■■	■	■■■■
Iris	■■■■■■■■	■■■■■■■■ (AS) ■ (PS)	■■■■
Retina	■■■■■■■■	■■■■■■■■	■■■■
Dyn. Signatur	■■■■	■	■■■■
Sprecher	■	■	■
Tippverhalten	■	■■■■	■
Venenstruktur	■■■■	■	■■■■

AS = Aktives System – PS = Passives System

Tabelle: Bewertung der biometrischen Verfahren in bezug auf Kosten, Benutzerfreundlichkeit und Wartungsaufwand - Stand: Februar 2002

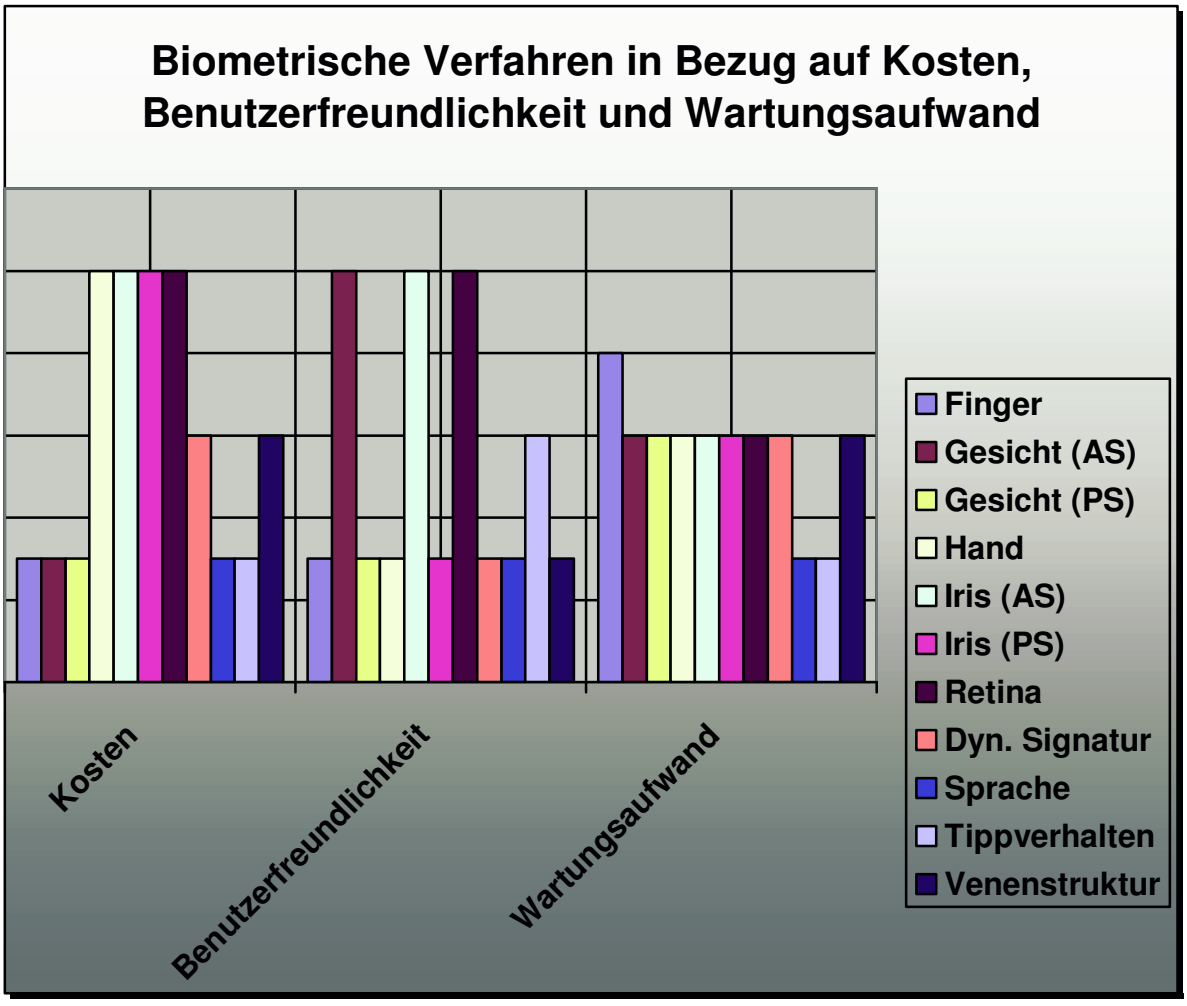


Abbildung 46 – Biometrische Verfahren in Bezug auf Kosten, Benutzerfreundlichkeit und Wartungsaufwand

5 KONZEPTE DER IMPLEMENTATION

5.1 Sicherheitsarchitektur in W2K

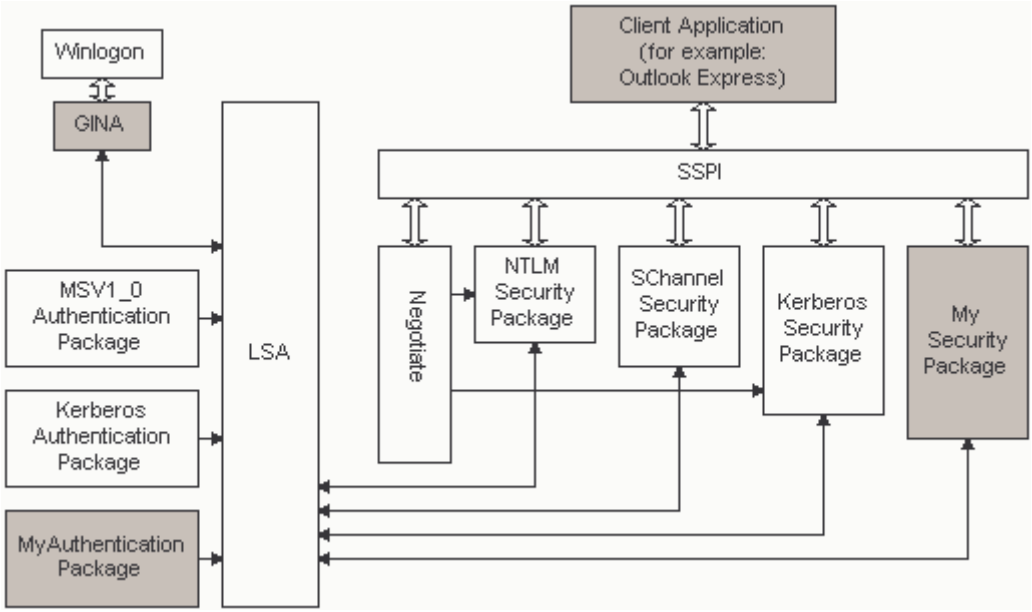


Abbildung 47 – Windows 2000: Sicherheitsarchitektur

5.1.1 WINLOGON

Winlogon ist eine Komponente von Microsoft's Windows NT/2K/XP, die eine interaktive Anmeldeunterstützung bereitstellt. Sie ruft eine austauschbare DLL zur grafischen Identifikation und Authentifizierung auf, um eine Benutzeroberfläche zur Anmeldung anzuzeigen und den Benutzer zu authentifizieren.

Das interaktive Logon-Model setzt sich aus 3 Komponenten zusammen: Der Winlogon.exe, einer dynamisch graphischen Identifizierungs- und Authentisierungsbibliothek (Graphical Identification and Authentication dynamic-link library) → „GINA.DLL" und einer beliebigen Anzahl von „network providers".

Während der Systeminitialisierung führt Winlogon folgende Schritte aus:

- erstellt die interaktive Windowsstation „winsta0“ um Tastatur, Maus und Monitor zu übernehmen. Winlogon erstellt einen „Security Descriptor“ für „winsta0“ mit nur einer ACE (Access Control Entry), die nur die Winlogon SID enthält. Dies garantiert das kein anderer Prozess ohne die Erlaubnis von Winlogon Zugriff auf die Workstation hat.

- erstellt und öffnet 3 Desktops: Anwendungsdesktop, Winlogon-Desktop und einen Screensaver-Desktop. Auf den Winlogon-Desktop hat nur sie selbst Zugriff.

- erstellt eine LPC (Local Procedure Call) Verbindung mit dem LSA-Authentification-Port von LSASS (Local Security Authentication Subsystem) um Informationen auszutauschen. Anschließend wird die Windowsumgebung initialisiert.

5.1.2 WINLOGON-ZUSTÄNDE

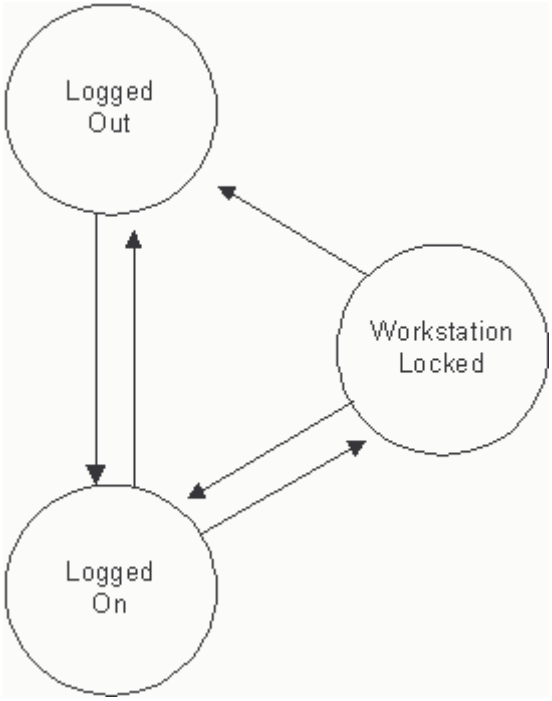


Abbildung 48 – Winlogon Zustände

5.1.2.1 Logged-Out-State

In diesem Zustand sehen Benutzer die Anmeldebox. Der Benutzer muss also erst die Authentikation durchlaufen um auf den Desktop Zugriff zu bekommen.
Meldet sich ein Benutzer erfolgreich an, so erfolgt der Aufruf eines Shell-Programms (z.B. Explorer.exe). Winlogon geht in den „Logged-On-Zustand“ über.

5.1.2.2 Logged-On-State

Wenn Winlogon sich in diesem Zustand befindet, können Benutzer mit der Shell interagieren, Applikationen starten und ausführen und somit ihre Arbeit durchführen. Aus diesem Status heraus können Benutzer entweder ihre Arbeit beenden und sich abmelden oder aber die Arbeitsstation sperren (lock). Im Falle einer Abmeldung beendet Winlogon alle Prozesse der Logon-Session und gibt die Arbeitsstation für einen anderen Benutzer frei. Entscheidet sich der Benutzer für das Sperren der Arbeitsstation, wechselt Winlogon in den „Workstation-Locked-State“ (Arbeitsstation ist nun gesperrt).

5.1.2.3 Workstation-Locked-State

In diesem Zustand wird solange ein sicherer Desktop angezeigt und ausgeführt, bis sich der Benutzer mit der selben Identifikations-/ und Authentikationsinformation anmeldet, wie der ursprüngliche Benutzer oder aber ein Administrator eine Abmeldung (Logoff) forciert.
Im Falle einer Entsicherung des Desktops, wird wieder der Applikationsdesktop angezeigt und es kann weitergearbeitet werden. Falls ein Administrator den Desktop „entsichert“, so werden alle Prozesse des zuvor angemeldeten Benutzers beendet und Winlogon wechselt in den „Logged-Out“-Zustand.

5.1.3 GINA

Graphical Identification and Authentication dynamic-link library. Eine austauschbare DLL-Komponente, welche durch die Winlogon.exe aufgerufen wird. GINA implementiert die „authentication policy“ des interaktiven Logon-Models. Über sie laufen alle Identifikations- und Authentikations-Interaktionen.

5.1.4 LSA

Local Security Authority. Ein geschütztes Untersystem des Windows NT/2K/XP Betriebssystems, das für die Benutzerauthentikation und die Erstellung von Benutzerprotokollen auf dem lokalen System zuständig ist → Local Security Policy.
Die lokale Sicherheitsautorität „LSA“ wickelt die Benutzeranmeldung und Authentifizierung auf dem lokalen Computer ab. Die LSA kann auch Benutzer an anderen Computern anmelden, wenn das Authentifizierungspaket, das die Anmeldeanforderung verarbeitet, die Durchgangsauthentikation unterstützt. LSA wird intern durch mehrere Windows NT/2K/XP-Komponenten aufgerufen, wozu u. a. Anwendungen und die gina.dll gehören.

5.1.5 SAS

Eine Schlüsselsequenz für den Logon-/Logoff-Vorgang. Die Standardsequenz ist „STRG+ALT+ENTF“.

5.1.6 SSP

Security Support Provider. Eine DLL, welche das SSPI implementiert, indem sie den Anwendungen eine oder mehrere Security-Pakete zur Verfügung stellt.

5.1.7 SSPI

Um den Programmierer unter Windows NT/2K/XP zu entlasten, besitzt es ein „Security Support Provider Interface“ (SSPI). Dieses stellt dem Nutzer einen einheitlichen Zugriff auf NT/2K/XP Sicherheitsfunktionen zur Verfügung. Damit muss sich der Nutzer nicht mehr selber um die Einhaltung von Sicherheitsanforderungen kümmern. Die Einhaltung der Sicherheit wird vom „Security Support Provider“ (SSP) übernommen. Die Anwendungen greifen über die SSPI Schnittstelle auf diesen zu.

5.1.8 Negotiate

Negotiate ist ein Sonderfall eines SSPs. Wenn eine Anwendung SSPI aufruft, kann sie einen SSP zur Abwicklung der Transaktion angeben. Falls die Anwendung jedoch keinen SSP angibt, untersucht Negotiate die Anmeldeinformationen des Benutzers und stellt fest, welcher SSP am besten zur Verarbeitung der Transaktion geeignet ist. Negotiate ermöglicht ISVs (Independent Software Vendors) die Verwendung von SSPI, um ein Verfahren zur Netzwerkanmeldung zu ermöglichen, ohne dass bekannt sein muss, welche SSPs auf dem Computer installiert sind.

5.1.9 NTLM

„NT Lan Manager“ ist ein Protokoll mit Herausforderung/Rückmeldung.
Windows NT/2K/XP verwendet NTLM, um einen sicheren Kommunikationskanal mit einem Remotecomputer aufzubauen. Zur Initiierung des Protokolls sendet ein Remoteclient ein Paket an den Server. Dieses Paket enthält eine Anforderung zum Herstellen eines sicheren Kanals. Als Antwort generiert der Server eine zufällige 64-Bit-Zahl, die er an den Client zurücksendet (→ Herausforderung). Der Client muss daraufhin eine Antwort senden, die seinen Benutzernamen enthält, und einen Nachweis, dass der Benutzer wirklich die Person ist, die er vorgibt zu sein. NTLM war bei NT4.0 (und vorherigen Versionen) der Standard für die Netzwerkauthentikation. Er wird zwar weiterhin von W2K unterstützt, ist aber nicht mehr der Standard → Kerberos.

5.1.10 SAM (Sicherheitskontenverwaltung)

Die Sicherheitskontenverwaltung („Security Account Manager“ - SAM) verwaltet die Benutzerkontendatenbank. Die Datenbank enthält Informationen für alle Benutzer und Gruppenkonten. SAM stellt außerdem die Sicherheitsbestätigung zur Verfügung, wenn die lokale Sicherheitsautorität eine Anforderung zur Benutzeranmeldung authentifiziert. Die Datenbank besteht aus Benutzern, die zu Gruppen gehören.
Die Windows NT/2K/XP-Sicherheit ermöglicht dem Administrator das Konfigurieren von Zugriffsrechten für Benutzer, durch Erstellen einer Gruppe und Erteilen von Rechten für ein Objekt oder Objekte im System für diese Gruppe. Der Zugriff auf Objekte durch einzelne

Benutzer erfolgt mittels Gruppensicherheitsbezeichner (SIDs), die im Zugriffstoken eines Benutzers enthalten sind.

5.1.11 MSV 1.0

MSV 1.0 ist ein mit Microsoft Windows NT/2K/XP installiertes Authentifizierungspaket. Es akzeptiert einen Benutzernamen und ein Hashkennwort. Es sucht die Kombination aus Benutzername und Hashkennwort in der SAM-Datenbank und zeigt an, ob die Anmeldung des Benutzers zulässig ist.

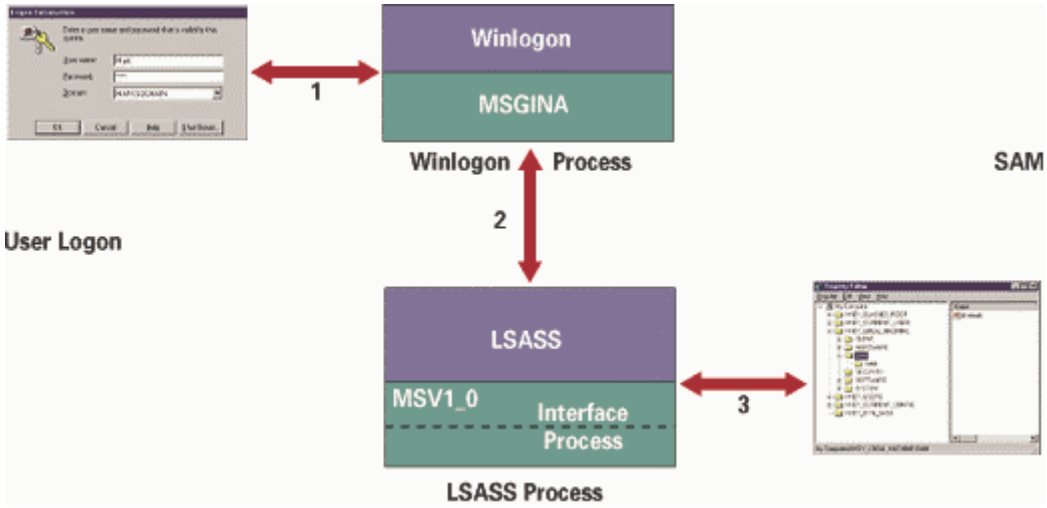


Abbildung 49 – User Logon - Schema

5.1.12 Authentifizierungspakete

Die lokale Sicherheitsautorität authentifiziert eine Anforderung zur Benutzeranmeldung, indem diese an ein Authentifizierungspaket gesendet wird. Das Authentifizierungspaket untersucht dann die Anmeldeinformationen, und authentifiziert den Benutzer oder weist ihn zurück.

Mehrere Authentifizierungspakete ermöglichen der lokalen Sicherheitsautorität die Unterstützung vieler verschiedener Arten von Anmelde- und Benutzerauthentikationsprozessen.

Zusätzlich zu den mit Windows 2000/XP (MSV 1.0 und Kerberos) installierten Authentifizierungspaketen können benutzerdefinierte Authentifizierungspakete zur Abwicklung von benutzerdefinierten Anmeldeprozeduren geschrieben werden. Wenn beispielsweise ein System unterstützt werden soll, das eine neue Art eines Anmeldeprozesses definiert, wie z. B. Netzhautabtastung oder Spracherkennung, so muss ein benutzerdefiniertes Authentifizierungspaket erstellt werden, das neue Anmeldedaten analysiert und feststellt, ob der Benutzer autorisiert ist auf das System zuzugreifen oder nicht. Es können auch neue Authentikationspakete erstellt werden, die Standardanmeldedaten verwenden, jedoch neue Sicherheitsalgorithmen implementieren.

5.1.13 Kerberos

Das Kerberos-Authentifizierungsprotokoll definiert die Interaktionen zwischen einem Client und einem Netzwerkauthentifizierungsdienst, der als Schlüsselverteilungscenter (Key Distribution Center, kurz KDC) bezeichnet wird.

Bei Kerberos handelt es sich um ein Authentifizierungsprotokoll mit gemeinsam genutzten Kennwörtern, da Benutzer und KDC beide das Benutzerkennwort kennen, bzw. (im Fall des KDCs) das unidirektional verschlüsselte Kennwort.

Das Kerberos-Protokoll definiert eine Reihe von Austauschvorgängen zwischen den Clients, dem KDC und den Servern, um Kerberos-Tickets zu erhalten und zu verwenden. Wenn ein Benutzer eine Anmeldung bei Windows initiiert, erhält das Kerberos-SSP ein Kerberos-Anfangsticket (TGT), das auf einer Hashverschlüsselung des Benutzerkennwortes basiert.

Das Kerberos-Authentifizierungprotokoll stellt folgende Funktionen bereit:

- schnellere Serverauthentifizierung beim ersten Herstellen der Verbindung
- Delegierung der Authentikation für mehrstufige Client/Server-Anwendungsarchitekturen
- transitive Vertrauensstellungen für die Authentifizierung zwischen Domänen

Windows 2000 speichert das Kerberos-Anfangsticket (TGT) in einem Ticket-Zwischenspeicher auf der Arbeitsstation, die dem Anmeldekontext des Benutzers zugeordnet ist. Wenn ein Clientprogramm versucht, auf einen Netzwerkdienst zuzugreifen, überprüft die Kerberos-Laufzeitkomponente den Ticket-Zwischenspeicher auf ein gültiges Sitzungsticket für den Server. Ist kein Ticket verfügbar, wird das TGT an das „Key Distribution Center“, kurz KDC, gesendet und ein Sitzungsticket angefordert, das einen Zugriff auf den Server zulässt.
Bei der ersten Verbindungsmeldung wird das Kerberos-Sitzungsticket dem Remotedienst präsentiert. Teile des Sitzungstickets werden mithilfe eines geheimen Schlüssels verschlüsselt, der von dem Dienst und dem KDC gemeinsam verwendet wird. Der Server kann den Client in kurzer Zeit authentifizieren, indem das Sitzungsticket ohne den Authentifizierungsdienst verifiziert wird, da die Kerberos-Laufzeitkomponente des Servers über ein zwischengespeichertes Exemplar des geheimen Serverschlüssels verfügt.
Das Sitzungsticket wird zum Ticket-Zwischenspeicher hinzugefügt und kann für spätere Verbindungen zu dem selben Server wieder verwendet werden, bis das Ticket abläuft. Die Ablaufzeit für das Ticket wird durch die Domänensicherheitsrichtlinie bestimmt. Läuft das Sitzungsticket in der Mitte einer aktiven Sitzung ab, gibt der Kerberos-Sicherheitsanbieter entsprechende Fehlerwerte zurück, die es Client und Server ermöglichen, das Ticket zu aktualisieren, einen neuen Sitzungsschlüssel zu erzeugen und die Verbindung wieder aufzunehmen.

Kerberos-Sitzungstickets enthalten einen eindeutigen Sitzungsschlüssel, der vom KDC erstellt wird und für eine symmetrische Verschlüsselung der Authentifizierungsinformationen sowie für die zwischen Client und Server übertragenen Daten verwendet wird.

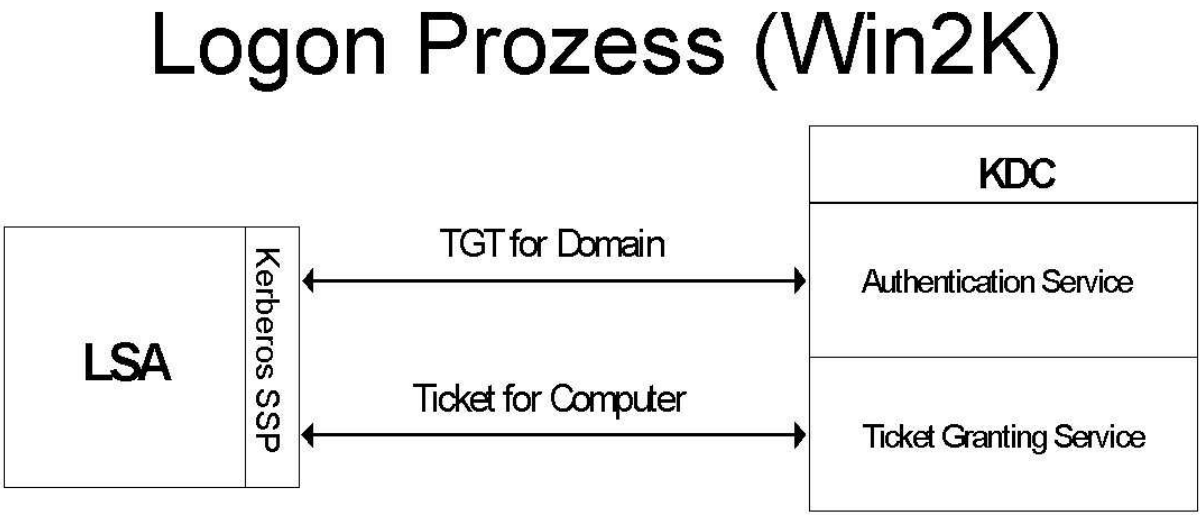


Abbildung 50 – Logon Prozess unter Windows 2000

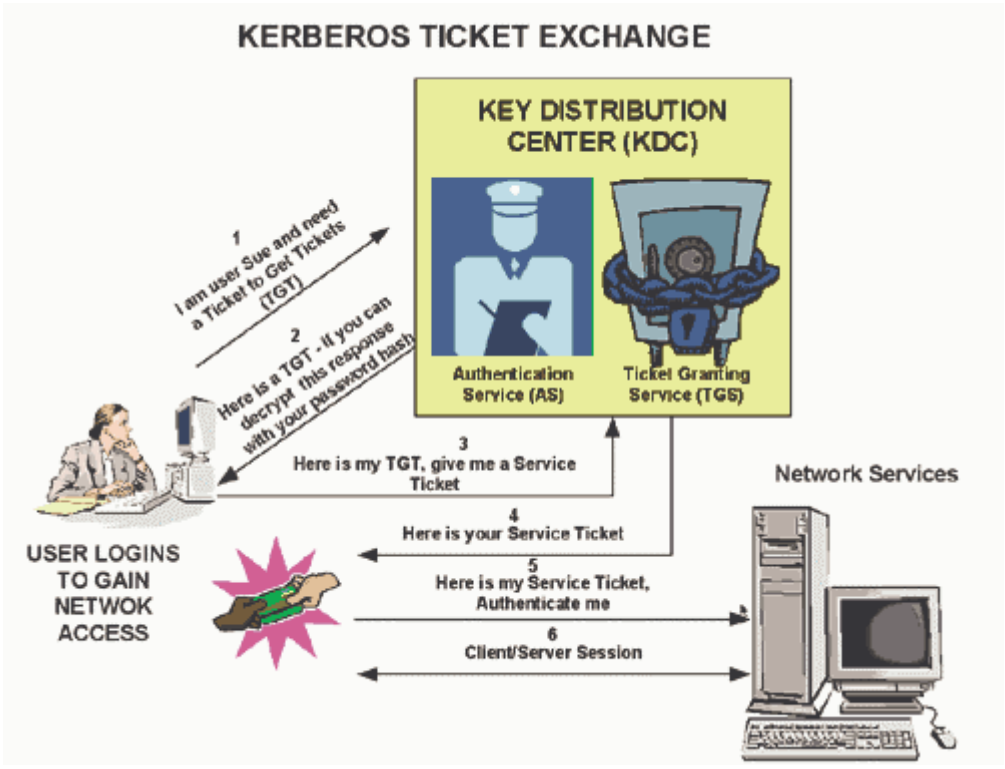


Abbildung 51 – Kerberos Ticket Exchange

Unter Windows NT/2K/XP lässt sich eine biometrische Authentikation in Verbindung mit Kerberos nur dann nutzen, wenn eigene Sicherheitskomponenten (wie z.B. „My Kerberos Authentication Package“) programmiert und somit neu definiert/spezifiziert werden.

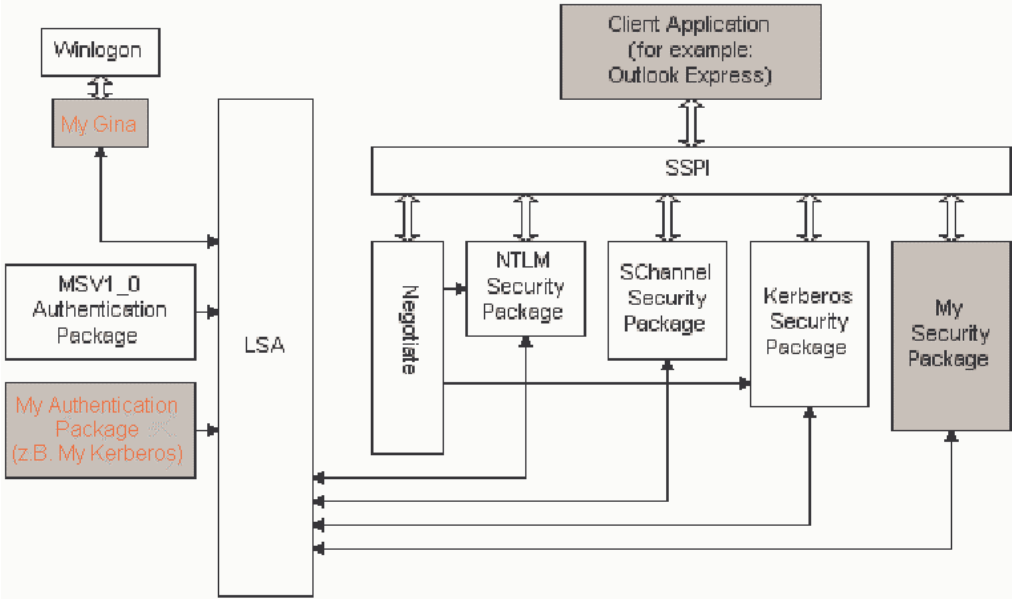


Abbildung 52 - W2K-Sicherheitsarchitektur (modifiziert)

Ohne diese eigenen Komponenten arbeitet Kerberos nur mit Benutzernamen und Passwort zur Authentikation.

5.2 FaceVACS 2.1 – Logon

PC-Zugang über automatische Gesichtserkennung unter Windows 2000

5.2.1 Produktbeschreibung des Herstellers: „Cognitec“

FaceVACS-Logon sichert den Zugang zum PC, indem die Authentizität der Benutzer festgestellt wird. Unterschiedliche Betriebsarten gewährleisten einen flexiblen Einsatz.
So lässt sich z. B. bei hohen Sicherheitsanforderungen die automatische Identifizierung von FaceVACS – Logon mit der Eingabe eines herkömmlichen Passwortes kombinieren. Das Gesicht des Benutzers wird mit einer Videokamera aufgenommen, wofür bereits eine einfache Webcam ausreicht. Verschiedene Bildverarbeitungsalgorithmen berechnen aus den digitalisierten Daten der Kameraaufnahme einen Merkmalsdatensatz, der mit dem im Rechner abgelegten und der Person eindeutig zugeordneten Datensatz auf Übereinstimmung geprüft wird. Die Authentikation kann beim Anmelden am System und beim Freischalten eines Bildschirmschoners oder gesperrten Bildschirms erfolgen.

Features:

- flexible Betriebsarten, z.B. Stand-alone oder in Kombination mit Passwort
- Gesichtserkennung beim Logon, zum Freischalten des Screen Lock und des Bildschirmschoners
- Morphing Editor für Bildschirmschoner
- Unterstützung von Windows 98, Windows Me, Windows NT und Windows 2000/XP
- für die Bildaufnahme ist bereits eine einfache Webcam ausreichend

Betriebsarten:

Für die Anmeldung am System kann unter vier verschiedenen Funktionen gewählt werden:

- Benutzer wird, ohne Abfrage von Name und Passwort, automatisch nach positiver Identifikation durch FaceVACS-Logon am System angemeldet

- Benutzername wird eingegeben, die Gesichtserkennung ersetzt die Passworteingabe
- Benutzername und Passwort werden eingegeben, zusätzlich wird die Authentizität des Benutzers durch die Gesichtserkennung überprüft
- Standardanmeldung am System ohne Gesichtserkennung.
- für Domain-User und Novell-User ist die Authentisierung beim Logon unter Windows 98 und Windows Me nur eingeschränkt möglich.

Computer, deren Zugang durch manuelles Sperren, Stand-by Modus oder Aktivierung des Bildschirmschoners mit Passwortschutz gesperrt wurde, können mit Hilfe von FaceVACS-Logon bequem freigeschaltet werden:

- automatisch durch Blick des Benutzers in die Kamera oder
- nach Aufforderung bei Mausbewegung oder Tastendruck.

Falls für das Sperren der Arbeitsstation ein Bildschirmschoner verwendet wird, kann gewählt werden zwischen:

- einem beliebigen auf dem System installierten Standard-Bildschirmschoner
- dem Live-Bild der Kamera
- einem selbst gewählten Bild, in das das Gesicht aus dem Live-Bild der Kamera eingefügt wird

Systemanforderungen:

- Intel 686 kompatibler PC, mindestens 64 MB RAM, mindestens 400 Mhz
- Betriebssystem Windows 98, Windows Me, Windows NT4.0 (mit Servicepack4 oder höher), Windows 2000 oder Windows XP
- bei Windows NT/2000: NTFS-Dateisystem

- Kamera/Webcam mit Treibern für Video for Windows bzw. DirectShow, bei Verwendung einer Analog-Kamera wird ein Framegrabber benötigt, der eine dieser Schnittstellen unterstützt

5.2.2 Testumgebung

Testsystem 1:

- Intel PII-350Mhz
- 128 MB RAM
- Windows 2000
- Medion USB-Kamera
- FaceVacs Version 2.1 für W2K

Testsystem 2:

- Notebook Intel PIII-900Mhz
- 128MB RAM
- Windows XP
- Philips Vesta Pro USB-Kamera
- FaceVacs Version 2.1 für Windows XP

Testsystem3

- AMD Athlon Thunderbird 1 Ghz
- 768 MB RAM
- Windows XP
- Philips Vesta Pro USB-Kamera
- FaceVacs Version 2.1 für Windows XP

5.2.3 Softwaretest – FaceVacs 2.1

Die Software „ersetzt“, durch Anpassung der Registry, die MSGina.dll und fügt drei weitere Dateien ins Systemverzeichnis (\System32) des bestehenden Betriebssystems hinzu. In diesem Fall, also W2K bzw. Windows XP Professional:

- fvauth.dll
- fvgina.dll → ersetzt die Standard msgina.dll
- qt230.dll

Alle weiteren Dateien befinden sich im gewählten Installationsverzeichnis (in unserem Fall in „C:\Programme\Fvacs\“).

Durch die modifizierte Gina.dll (fvgina.dll) wird es unter anderem ermöglicht den Videostrom der in diesem Fall genutzten USB-Kamera abzuzweigen, um eine Gesichtserkennung durchführen zu können.

Abbildung 53 - FaceVacs Logon

Aus Abbildung [53] wird deutlich, inwieweit die modifizierte gina.dll den Anmeldedialog zunächst rein optisch verändert hat. Der Standardanmeldebildschirm wurde komplett neu gestaltet.

Nach der Installation fordert die Software zum Anlegen eines Enrollments auf. Dafür werden in der Regel 8 Aufnahmen des Gesichtes gemacht. Jedes Foto wird gleichzeitig qualitativ

überprüft. Die Bilder werden im .ppm-Format in einer Log-Datei abgelegt. Bei jedem Authentikationsvorgang kommen weitere Bilddaten hinzu, die mit der Endung .fvi abgespeichert werden. Diese Daten werden weder verschlüsselt noch anderweitig gesichert.

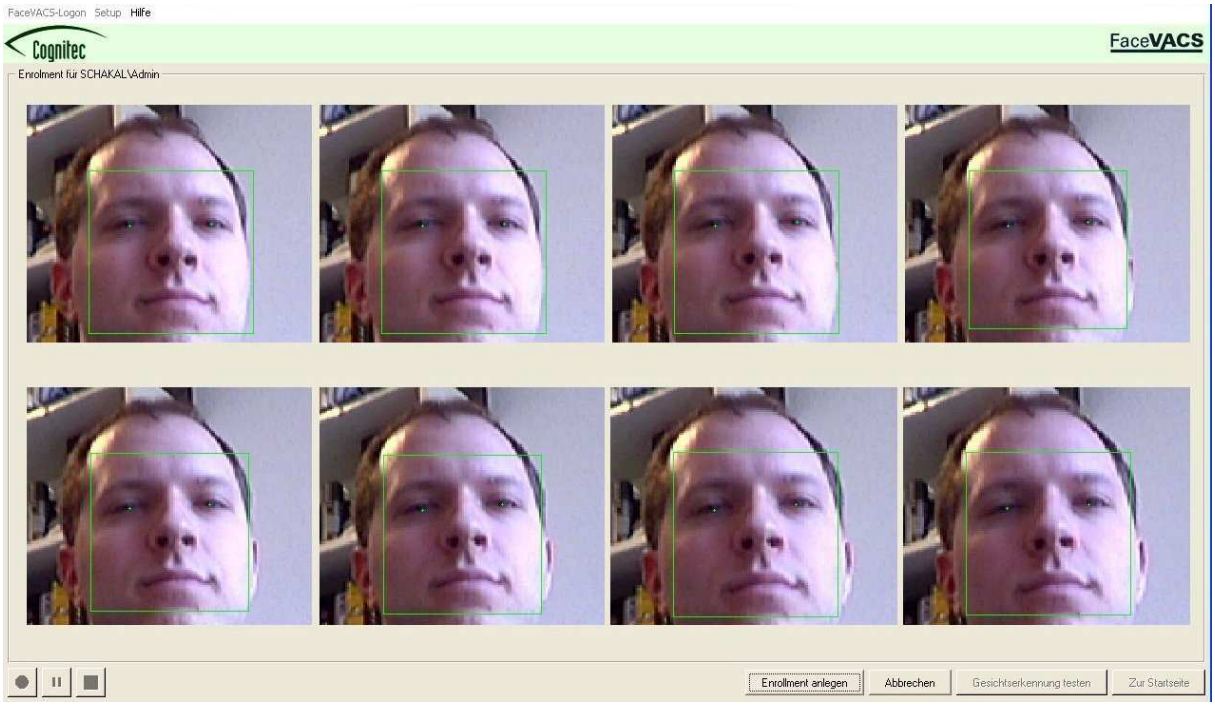


Abbildung 54 - FaceVacs: Enrollment

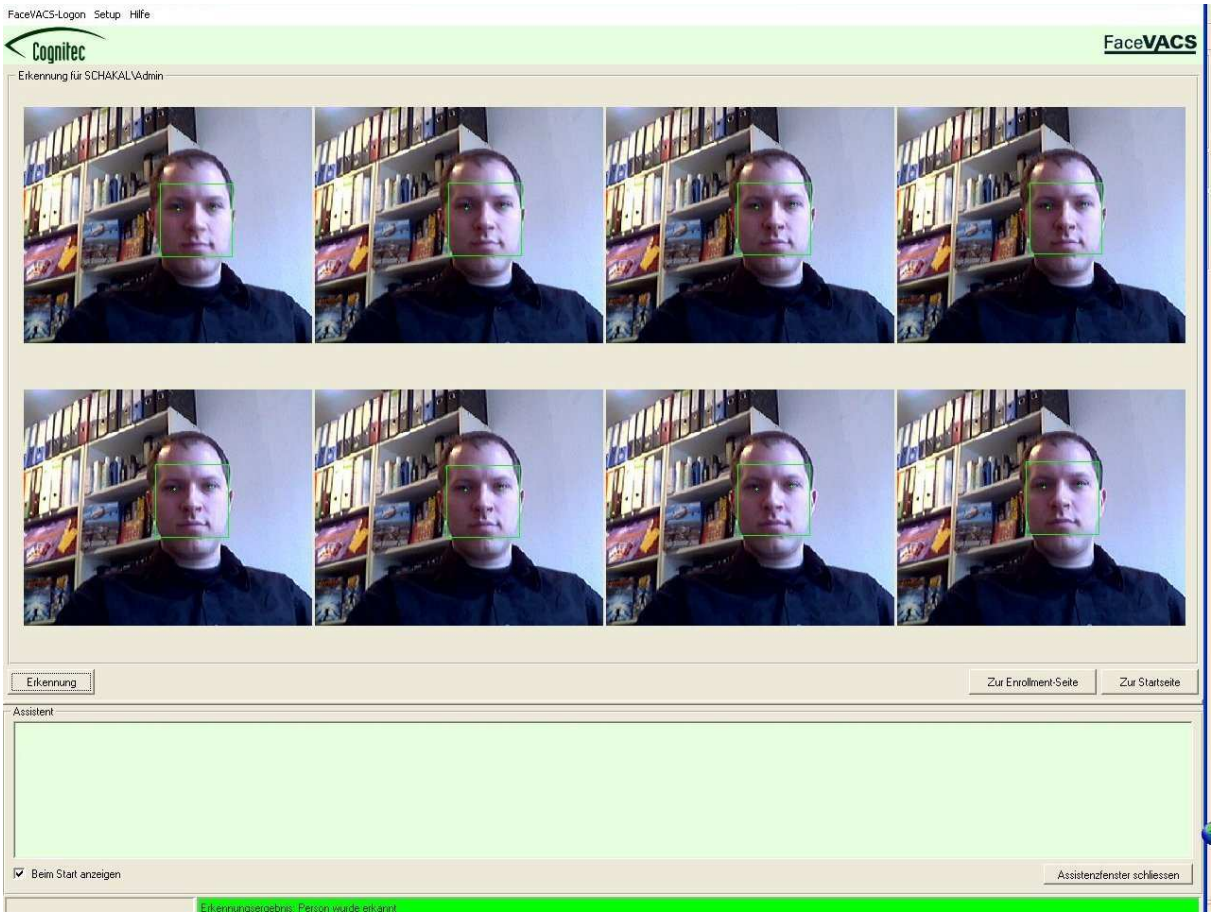


Abbildung 55 - FaceVacs: Erkennung

Die Software erkennt das Gesicht selbständig und vergrößert den relevanten Bereich automatisch. Auch die Augen werden problemlos selektiert [54].

Nach Abschluss des Enrollments und damit der Generierung eines Templates war es problemlos möglich, sich mittels biometrischer Gesichtserkennung ins System einzuloggen. Die Software erkennt den jeweiligen, zuvor eingelernten, Benutzer ganz ohne Eingabe von Benutzernamen und Passwort. Die Erkennungszeit beträgt dabei gerade mal ein bis drei Sekunden.

5.2.4 Sicherheitstest

Bei biometrischen Verfahren besteht natürlich die Gefahr, dass die neue Bequemlichkeit auf Kosten der Sicherheit geht. Wie gut schützen biometrische Zugangskontrollen vor dem Eindringen Unbefugter?

FaceVacs führt standardmäßig keinen Livecheck aus. In diesem Test war es demnach problemlos möglich die Software mit Hilfe des Fotos eines eingelernten Benutzers täuschen.

Das Foto war von relativ schlechter Qualität:

- Snapshot mit einer Auflösung von 352x288 Pixel
- selektierte Bildgröße: 255x270 Pixel
- Ausdruck auf HP-Desjket 970Cxi mit 600x600 dpi

Das System erkannte das Gesicht auf dem Foto auf Anhieb und authentisierte uns mittels Ausdruck (siehe auch Abbildung [56]).

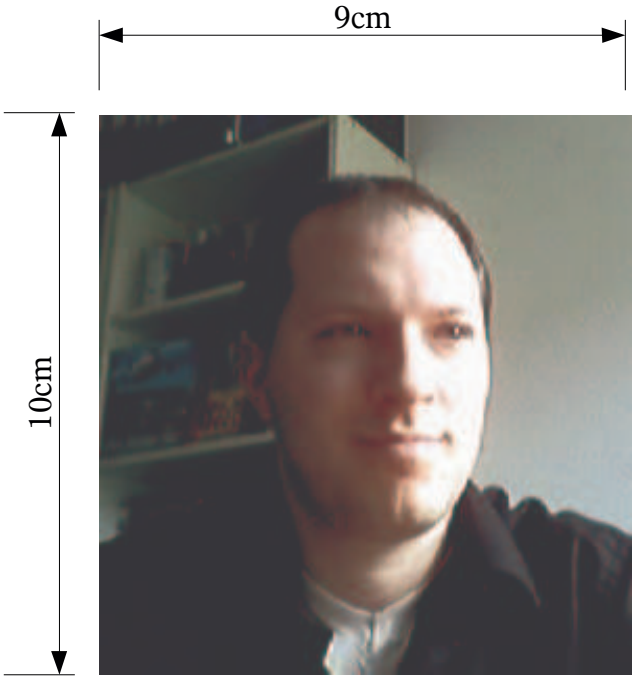


Abbildung 56 - FaceVacs - Snapshot in Originalgröße

Erst die Aktivierung des so genannten „Livecheck“ im Optionsmenü, brachte deutlich mehr Sicherheit. Der Benutzer muss nun zur erfolgreichen Authentikation seinen Kopf von links nach rechts drehen. Dabei werden mehrere Snapshots aufgenommen und mit dem gespeicherten Template verglichen. Der Loginvorgang mit zugeschaltetem Livecheck erfordert deutlich mehr Einlernzeit für den Benutzer, sollte aber aus Sicherheitsgründen in jedem Falle aktiviert werden!

Auch die Aktivierung des Livecheck stellte letztlich kein Hindernis dar. Mit Hilfe einer Webcam wurde ein kurzes Video eines eingelernten Benutzers aufgenommen, in dem dieser seinen Kopf ein wenig hin und her bewegte. Mit Hilfe eines Notebooks wurde der USB-Kamera im Anschluss die kurze Videosequenz vorgespielt. FaceVacs erkannte in der abgespielten Videosequenz tatsächlich einen sich bewegenden „echten“ Kopf und authentisierte uns erfolgreich.

Eine weitere Angriffsmöglichkeit bieten die ungeschützt abgespeicherten Gesichtsbilder der eingelernten Benutzer. Man kann demnach bei Zugang zum Rechner die Bilddaten auslesen und ggf. manipulieren. Zudem kann man anhand der Logfiles erkennen, welche Daten qualitativ gut sind, d. h. über dem Schwellwert für die Erkennung liegen. Aufgrund dieser Lücke konnten wir die Daten von dem Rechner auf ein Notebook überspielen und dem System diese Bilder präsentieren. Wir konnten uns meist schon nach dem ersten Versuch mit Hilfe der „gestohlenen“ Bilder erfolgreich über FaceVacs anmelden.

Aus einem uns nicht bekannten Grund ist es nicht möglich, auf verschlüsselte Dateien des NTFS zuzugreifen, wenn die Systemanmeldung via biometrischer Authentikation erfolgt ist. Nur nach Anmeldung via Passwort und Benutzername ist ein Zugriff auf diese möglich!!!

Personen die (zeitweise) eine Brille tragen, sollten beim Enrollment darauf achten, dass mindestens eine Aufnahme mit Brille erfolgt. Ansonsten kann es zu Erkennungsproblemen kommen bzw. die Brille muss für die Authentikation abgenommen werden. Die Hersteller haben hierfür eine Pausetaste im Enrollment-Dialog implementiert. Es können so ohne Probleme und in aller Ruhe, Aufnahmen mit und ohne Brille erstellt werden.

Abbildung 57 - FaceVacs - Enrollment - Aufnahmesteuerung

Es ist vorerst empfehlenswert die biometrische Authentikation mit der Benutzer/Passworteingabe zu kombinieren um die Sicherheit zu erhöhen. FaceVacs bietet hierfür extra eine Option an. Der Benutzer gibt also zunächst seinen „Benutzernamen“ und anschließend sein Passwort ein und wird anschließend von der Software biometrisch überprüft.

Laut Cognitec handelt es sich bei FaceVacs um eine Software, die nicht für den Einsatz in Hochsicherheitsbereichen gedacht ist. Es stellt sich aber dennoch die Frage, ob eine Sicherheitsanwendung, deren Schutzfunktion sich mit den simpelsten Tricks aushebeln lässt, eine Investition wert ist.

6 ZUSAMMENFASSUNG & AUSBLICK

Die in dieser Studienarbeit aufgezeigten biometrischen Verfahren lassen sich in der Regel fast ausnahmslos aushebeln. Besonders einfach ist dies beispielsweise bei handelsüblichen Zugangssicherungen auf der Basis von Fingerabdruckerkennungssystemen. Hier kann man z.B. mit Hilfe von etwas Silikon und Gelatine die meisten Fingerabdruckscanner überlisten. In einen kleinen Klumpen Silikon wird ein Finger gedrückt. In die entstandene Mulde wird anschließend in Wasser gelöste Gelatine gegeben. Im Kühlfach entsteht so ein neuer Kunstfinger.

Um biometrische Systeme unter Realbedingungen nun wirklich zu überlisten, muss man das obige Verfahren ein wenig erweitern. Zunächst benötigt man einen Fingerabdruck eines eingelernten Benutzers. Diesen macht man mit Hilfe von etwas Graphitpulver sichtbar. Von diesem sichtbaren Abdruck wird nun ein digitales Foto erstellt und mittels Bildbearbeitungsprogramm eventuell Kontraste verstärkt. Der Abdruck wird auf Folie ausgedruckt und als Maske für die Belichtung einer Leiterplatine verwendet [58]. Auf diese Art und Weise erhält man ein Relief des Fingerabdrucks. Anschließend wird in Wasser gelöste Gelatine darüber gegeben [59]. So entsteht letztlich im Kühlschrank ein Kunstfingerüberzug.

Alle gängigen und bezahlbaren Fingerabdruckerkennungssysteme lassen sich mit diesem Verfahren überlisten. Da Gelatine ähnlich physikalische Eigenschaften wie menschliches Gewebe aufweist, funktioniert der Gelatinefinger auch auf Systemen die mit einem LiveCheck ausgestattet sind. Diese Verfahren stammen von dem japanischen Mathematiker „Tsutomo Matsumoto“.

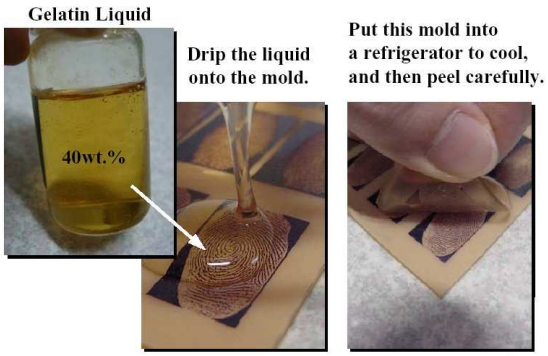
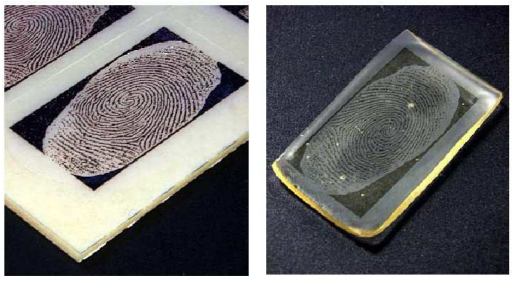


Abbildung 58 - Generierung eines künstlichen Fingerabdrucks I



Mold: 70JPY/piece
(Ten molds can be obtained in the PCB.)

Gummy Finger: 50JPY/piece

Abbildung 59 - Generierung eines künstlichen Fingerabdrucks II

Es stellt sich nun natürlich die Frage, inwieweit teurere Systeme sicherer sind – oder sind sie gar noch nie ernsthaft geprüft worden? Zum jetzigen Zeitpunkt gibt es also noch viel zu tun, bevor an den Ersatz von Passwörtern und PINs durch biometrische Verfahren zu denken ist. Derzeitige biometrische Systeme sollten also aus Sicherheitsgründen nur in Kombination mit den klassischen Passwortverfahren eingesetzt werden.

LITERATURVERZEICHNIS

[1, Datenschutz Berlin 1998] aus http://www.datenschutz-berlin.de/jahresbe/98/teil3-5.htm

[2, Schwiderski-Grosche 2002] **EU-Studie: "Usability of Biometrics in Relation to Electronic Signatures".** Dr. Scarlet Schwiderski-Grosche, GMD-Forschungszentrum Informationstechnik, Institut für sichere Telekooperation

[Biguen 1997] Audio- and video-based biometric person authentication : first international conference, AVBPA '97, Crans-Montana, Switzerland, March 12 - 14, 1997 ; proceedings / Josef Biguen ... (eds.) Beteiligt: Josef Biguen Koerperschaft: AVBPA (1, 1997, Crans-Montana) Kongress: International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA) ; 1 (Crans-Montana) : 1997.03.12-14 Erschienen: Berlin [u.a.] : Springer, 1997 Umfang: XII, 450 S. : Ill., graph. Darst. ; 24 cm Schriftenreihe: Lecture notes in computer science ; 1206Anmerkung: LiteraturangabenISBN: 3-540-62660-3 *kart.

[Bigun, Smeraldi 2001] Josef Bigun; Fabrizio Smeraldi: Audio- and video-based biometric person authentication : third international conference, Halmstad, Sweden, June 6 - 8, 2001 ; proceedings / AVBPA 2001. (eds.) (3, 2001, Halmstad) International Association for Pattern Recognition Kongress: International Conference on Audio- and Video-Based Biometric Person Authentication Erschienen: Berlin [u.a.] : Springer, 2001 Schriftenreihe: Lecture notes in computer science ; ISBN: 3-540-42216-1*kart.

[Bolle, Pankanti, Nalini, Ratha 2000] Evaluation techniques for biometric-based authentication systems (FRR) / Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha Verfasser: Ruud M. Bolle ; Sharath Pankanti ; Nalini K. Ratha Erschienen: Yorktown Heights, NY : IBM Watson Research Center, 2000 Umfang: 7 S. Schriftenreihe: Research Report / IBM Research Division, Watson Research Center : RC ; 21759 = 98007Computer science/mathematics Report-Nr.: RC 21759

[Brömme 2001] Arslan Brömme : A Discussion on Privacy Needs and (Mis)Use of Biometric IT-Systems & Overheadpapers , Faculty of Informatics, University of Hamburg.

[Brömme 2001] Arslan Brömme: Politik-gewollte Anwendungen der Biometrik:Fahndung, Ausweise, Terrorbekämpfung. Eine Diskussion unter Berücksichtigung des Datenschutzes Universität Hamburg Fachbereich InformatikArbeitsbereich AGN 1. Nov. 2001

[Daugman 2002] John Daugman, PhD, OBE: How Iris RecognitionWorks University of Cambridge, The Computer Laboratory, Cambridge CB2 3QG, U.K. (http://www.CL.cam.ac.uk/users/jgd1000/) – Stand: Februar 2002
[EU-Studie "Usability of Biometrics in Relation to Electronic Signatures] http://sit.gmd.de/SICA/papers/WS_01/Beitrag_Schwiderski.pdf – Stand: Februar 2002

[heise.de 2002] Heise.de c't

- http://www.heise.de/newsticker/data/anw-20.05.02-004/
- http://www.heise.de/ct/02/11/114/
- http://www.heise.de/ct/02/05/146/default.shtml

[IBG 2001] International Biometric Group: LLC Biometrics Explained, (http://www.biometricgroup.com) - Stand: Februar 2002

[Mass 2000] Kluwer Academic, 2000 Schriftenreihe: The Kluwer international series on Asian studies in computer and information science ; 7 Anmerkung: Includes bibliographical references and index, ISBN: 0-7923-7856-3 : NLG 305.00

[Matsumoto, Tsutomo 2002] Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies – A Case Study for User Identification (http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf)

[Microsoft - MS-Whitepaper 2002] Windows 2000 Security in an E-Commerce Environment (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/ecommerce/maintain/operate/sececomm.asp) - Stand: Februar 2002

[Microsoft - Platform SDK 2001] Microsoft Platform Software Developer Kit – Stand: November 2000

[Microsoft - MSDN 2002] Microsoft Developer Network (http://msdn.microsoft.com/library/) - Stand: Februar 2002

[Zhang 2000] David D. Zhang : Automated biometrics : technologies and systems, Boston

ABBILDUNGSVERZEICHNIS

Alle Internetbildquellen sind Stand: Februar-Mai 2002