WHITEPAPER BIOMETRIE

Björn Heumann

01.02.2006

Inhaltsverzeichnis

1 Über dieses Dokument

Unvollständige Vorabversion, die in den nächsten Tagen ständig erweitert wird !!!!! Dieses Dokument ist dazu gedacht, dass Sie sich autodidaktisch über des Thema biometrische Verfahren informieren können um dann gegebenenfalls die Entscheidung über das für Sie geeignetste Verfahren treffen zu können. Diese Datei wird kostenlos unter www.biometrie-online.de zum Download angeboten und in naher Zukunft auch in gedruckter Form erhältlich sein. Wenn Texte oder Bilder aus diesem Dokument veröffentlicht werden, ist als Quelle "Björn Heumann - www.biometrie-online.deäm Text bzw. an jedem Bild anzugeben. Bei einer Veröffentlichung in Druckerzeugnissen ist mir ein kostenloses Belegexemplar zu überlassen an:

Biometrie-Online
Björn Heumann
Saalburgstraße 1L
61273 Wehrheim

Alle Bilder wurden von mir selber erstellt und sind auf Nachfrage in besserer Auflösung erhältlich. Abweichungen von den Copyrightbestimmungen sind nach schriftlicher Genehmigung möglich.

2 Biometrie - Grundlagen

2.1 Einleitung - Was ist Biometrie?

Wenn eine Ihnen bekannte Person vor Ihrer Haustür steht, erkennen Sie Ihr Gegenüber anhand besonderer Merkmale, denn unsere Stimme, unser Verhalten, unser Gesicht sind individuell. Hier setzt die biometrische Identifikation an. Biometrie ist aus dem Griechischen abgeleitet und bedeutet biologische Statistik, Zählung und Messung von Lebewesen (*bios* [griechisch] = Leben, *metron* = [griechisch] Maß). Die biometrische Identifikation benutzt anstelle von Schlüsseln, Paßwörtern oder PINs die individuellen Körper- oder Verhaltensmerkmale, welche mit vorher aufgenommenen Referenzdaten verglichen werden. Dabei laufen computergestützt ähnliche Prozesse ab, wie Menschen sie im täglichen Leben anwenden, um ihr Gegenüber zu erkennen. In diesem Zusammenhang können Sensoren aber auch auf für Menschen nicht sicher erfaßbare Merkmale wie die Iris, den Fingerabdruck und viele weitere Eigenschaften als persönliches Merkmal zurückgreifen. Die biometrischen Identifikationsverfahren basieren hierbei auf dem Wiedererkennen der persönlichen Merkmale, welche zu Anfang im Enrolment erfasst wurden und

für den anschließenden Erkennungsvorgang als Referenz zur Verfügung stehen. Im Gegensatz zu PINs oder Passwörtern, welche es unter Umständen auch unberechtigten Personen ermöglichen, im Namen des Berechtigten zu handeln, kann die Biometrie sicherstellen, dass auch wirklich die vorgegebene Person handelt. Biometrische Merkmale können nicht so ohne weiteres an andere Personen übertragen werden. Dies bietet vor allem dort Vorteile, wo man sein Gegenüber nicht direkt sehen kann, z.B. im Internet. Sie sind beständig und bleiben über einen längeren Zeitraum unverändert. Biometrische Merkmale - Systeme Zu den biometrischen Merkmalen, welche heute bereits von Sensoren ausgewertet werden können, gehören zum Beispiel:

- Das Gesicht
- Der Augenhintergrund (Retina)
- Die Handgeometrie
- Das Fingerbild
- Die Unterschrift
- Die Sprache
- Das Tippverhalten (Anschlagdynamik)
- Das Gangverhalten

Am weitesten verbreitet sind die Verfahren Gesichtserkennung, Fingerbilderkennung und Iriserkennung.

2.2 Enrolment - Aufnahme der Referenzdaten

Damit das biometrische System eine Person überhaupt erkennen kann, muss es zunächst die Merkmale dieser Person aufnehmen und als Referenzdatensatz (Template) für spätere Erkennungsvorgänge hinterlegen. Diesen Vorgang nennt man Enrolment. Dem Enrolment kommt bei der biometrischen Identifikation eine besondere Bedeutung zu. Es sollte unter möglichst idealen Bedingungen z.B. bezüglich der Beleuchtung aufgenommen werden, um alle Feinheiten der Merkmale der entsprechenden Person abzudecken, damit eine spätere Erkennung auch unter schlechteren Umgebungsbedingungen noch gewährleistet ist. So ist es z.B. möglich, dass der Finger in einem etwas veränderten Winkel auf den Sensor aufgelegt wird oder dass die Kamera das Gesicht aus einer leicht veränderten Perspektive aufnimmt. Auch in diesen

Fällen sollte die betreffende Person sicher zu verifizieren sein. Da biometrische Merkmale immer leicht variabel sind, z.B. bedingt durch einen 3-Tage-Bart, angeschwollene Finger, etc., kann in der Biometrie nie ein hundertprozentiger 1:1 Vergleich stattfinden. So müssen beispielsweise kleinere Verletzungen des Fingers vom System noch toleriert werden, um einen praktikablen Zutritt zu erreichen, die Gesichtserkennung muss auch dann noch funktionieren, wenn der Benutzer aus einem leicht verändertem Winkel in die Kamera schaut. Bei der Iriserkennung dürfen leichte Lichtreflexe auf den Augen nicht gleich zur Ablehnung einer berechtigten Person führen.

2.3 Die Identifikation - Wer bin ich?

Bei der Identifikation einer Person geht es darum, eine bekannte Person in dem bereits vorhandenem Referenzdatensatz mit den Daten mehrerer Personen zu finden. Das System muss somit seinen gesamten Datenbestand mit allen Templates durchsuchen, bis es in den Referenzdaten Merkmale findet, welche Übereinstimmungen zu den aktuellen Daten des Sensors zeigen. Hierbei handelt es sich nicht um eine 100prozentige Übereinstimmung, sondern um eine "hinreichende"Übereinstimmung, deren Genauigkeit von den vorher festgelegten Toleranzschwellen abhängig ist. Wird in Bezug auf einen Referenzdatensätze der Schwellwert überschritten, dann konnte die entsprechende Person erfolgreich identifiziert werden. Dem System ist nun bekannt, um welche Person dem ihm bekannten Personenkreis (Referenzdatensatz) es sich handelt. Es hat ein 1:n-Vergleich stattgefunden, die Daten einer Person wurden mit einer Vielzahl anderer Daten verglichen.

Abbildung 1: Ablauf der Identifikation

2.4 Die Verifikation - Bin ich der, für den ich mich ausgebe?

Bei der Verifikation gibt sich die Person gegenüber dem System zunächst als eine bestimmte Person zu erkennen. Dies kann z.B. dadurch geschehen, dass mit Hilfe einer Chipkarte eine persönliche ID-Nummer an das System übermittelt wird, das ein Ausweis eingescannt wird oder der Name eingegeben. Der Wahrheitsgehalt dieser Behauptung wird nun durch das System

überprüft, indem es sich den erwarteten Datensatz aus seiner Referenzdatenbank heraussucht und mit den momentanen Livedaten"des Sensors abgleicht. Dazu müssen die Daten innerhalb der vorgegebenen Toleranzschranken, wel-

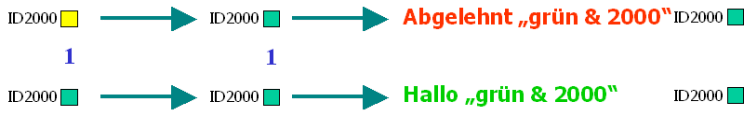

Abbildung 2: Ablauf der Verifikation

che im Programm eingestellt werden können, übereinstimmen. Es wurde somit ein 1:1-Vergleich durchgeführt. Die gewonnenen Daten wurden nur mit einem einzigen Datensatz abgeglichen. Da die aktuellen Daten nur mit einem Referenztemplate abgeglichen werden müssen, ergibt sich ein deutlicher Zeitvorteil gegenüber einer Verfikation, welcher mit zunehmender Größe immer langsamer wird.

3 Erkennungssicherheit

3.1 Festlegung der Erkennungssicherheit (Schwellenanpassung)

Im Gegensatz zu einer PIN oder einem Passwort kann bei biometrischen Identifikationssystemen nie ein 100-Prozent-Abgleich stattfinden (Vgl. Punkt Identifikation). Aus diesem Grund kann in der Erkennungssoftware ein Schwellwert eingerichtet werden, welcher einen Kompromiss aus "höchstmöglicher Sicherheitünd "höchstmöglichem Komfort"bildet. Je mehr man sich einem dieser beiden Punkte nähert, desto mehr Zugeständnisse muss man an den anderen Punkt machen. Aufgrund dieser Tatsache können folgende Szenarien auftreten:

Falsch eingestelltes System

- Eine Berechtigte Person wird abgewiesen, obwohl sie eigentlich Zugang erhalten müsste (zu hohe Sicherheit)
- Eine unberechtigte Person erhält Zugang (zu hoher Komfort)

Richtig eingestelltes System

- Eine Berechtigte Person erhält Zugang
- Eine unberechtigte Person wird abgewiesen

4 Verfahren

4.1 Fingerbilderkennung

4.1.1 Grundlagen

Jeder Mensch hat ein völlig individuelles Fingerbild. Selbst eineiige Zwillinge können anhand ihrer Fingerbilder eindeutig unterschieden werden. Die einzelnen Merkmale eines Fingerbildes wie Gabelungen, Schleifen und Wirbel nennt man Minutien (Minuzien [lat.]: Kleinigkeiten). Diese Minutien bleiben während des ganzen Lebens unverändert und werden deshalb für den Vergleich herangezogen. Dabei sind folgende Merkmale für die Unterscheidung wichtig:

- Breite der Papillarlinien
- Verlauf der Linien

Beim Verlauf der Linien unterscheidet man folgende Typen:

- Schleifen
- Wirbel
- Spiralen
- Ellipsen
- Knotenpunkte
- Gabelungen
- Linienenden
- Inseln

4.1.2 Bildaufnahme des Fingerbildes

Um die Fingerbilderkennung durchzuführen wird der Finger zunächst durch einen Sensor aufgenommen. Hier finden verschiedenen Sensoren Verwendung, die auf kapazitiver, optischer, thermischer oder Ultraschalltechnologie basieren. Die einzelnen Sensortypen werden später gesondert erklärt. Unabhängig von der physikalischen Funktionsweise des einzelnen Sensors entsteht zunächst ein Bild des Fingers in Graustufen, welches die Papillarlinien des zeigt.

Bildaufnahme des Fingerbildes

4.1.3 Normierung des Bildes

Um die Minutien aus dem Bild besser extrahieren zu können, wird das Bild zunächst durch mehrere Bildbearbeitungsfilter so verändert, dass die Paplillarlinien sich klar abheben. Dies geschieht zum Beispiel durch eine Erhöhung des Kontrastes und Entfernung von Bildstörungen.

Normierung des Fingerbildes

4.1.4 Markierung der Minutien

Nun werden die einzelnen Minutien vektoriell und mit ihrer Position eingezeichnet und abgespeichert. Im Beispielbild links wurden 76 Minutien gefunden und markiert. Man sagt, dass für eine sichere Identifikation bereits 14 übereinstimmende Minutien ausreichen. Hier bleibt also noch viel Spielraum für die Identifikation, falls der Finger zum Beispiel leicht verdreht oder verschoben aufgelegt wird und nicht alle Minutien gefunden werden

Markierung der Minutien

5 Gesichtserkennung

5.1 elastic-graph-matching-Verfahren

Viele gebräuchliche Gesichtserkennungssysteme arbeiten nach dem elastic-graph-matching-Verfahren. Hierzu wird das Gesicht zunächst von einer hochauflösenden Kamera erfaßt. Durch eine Bildbearbeitungssoftware wird dann das Gesicht in dem aufgenommen Bild lokalisiert. Nur wenn ein Gesicht gefunden wurde, wird der eigentliche Verifikationsvorgang gestartet. Ein „EyeFinder-Algorithmus“ sucht nun nach den Augen und markiert diese.

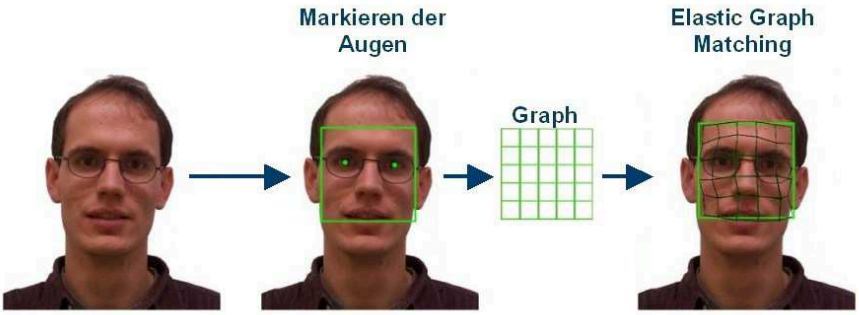

Abbildung 3: elastic-graph-matching

6 Iriserkennung

6.1 Die Iris - Grundlagen

Die Iris (aus dem Griechischen von Iris = Regenbogen) oder auch „Regenbogenhaut“ bildet die Blende des Auges. Wie bei der Blende eine Fotoapparates wird mit der Iris der Lichteinfall geregelt. Die Weite der Pupille wird dabei durch Muskeln in der Iris bestimmt. Die Iris ist auch verantwortlich für die Augenfarbe. Alle Babies z.B. haben zunächst blaue Augen. In den ersten Lebensmonaten kann sich jedoch die Farbe der Regenbogenhaut noch verändern. Dies geschieht durch den Farbstoff Melanin (dunkelbraune, hellbraune und gelbliche Körnchen), welcher gebildet wird und sich in der Iris ablagert. Je nach Mischungsverhältnis dieser Körnchen ergeben sich die verschiedenen Brauntöne. Wenn kaum Farbkörnchen vorhanden sind, dann erscheinen die Augen blau (eigentlich sind sie dann ”durchsichtig bzw. farblos”, es wird jedoch nur das blaue Licht zurückgespiegelt). Ähnlich dem Fingerabdruck ist die Iris bei jedem Menschen verschieden. Ihre Eigenarten (Äderchen, Pigmentkrausen, Streifen usw.) ändern sich im Laufe des normalen menschlichen Lebens nicht. Außnahmen können hier auftreten, wenn es zu einer Erkrankung oder Verletzung des Auges kommt.

6.2 Funktionsweise der Iriserkennung

Bei der Iriserkennung wird zunächst mit einer sehr hochauflösenden Schwarzweiss-Kamera ein Bild der Iris aufgenommen. Dabei wird die Kamera so fokussiert, dass möglichst wenig Reflexe auf der Iris zu erkennen sind. Es wird dabei keine gesundheitsschädliche Lasertechnologie eingesetzt, manche Systeme bedienen sich jedoch einer Infrarotbeleuchtung, um die Empfindlichkeit

der Kamera zu verbessern und Reflexe zu minimieren. Nachdem das Bild aufgenommen wurde, tastet der Rechner mit Hilfe eines Bildbearbeitungsalgorithmus das Auge von aussen nach innen schneckenförmig (in einer Spirale laufend) ab. Jedesmal, wenn er dabei auf ein Äderchen oder eine Pigmentkrause trifft, wird dieser Punkt auf der Spiralstrecke markiert. Wenn man die Spirale am Schluss der Bildbearbeitung äusrollt", erhält man eine Grafik ähnlich einem Barcode, welche alle Eigenarten der Iris wiederspiegelt.

7 Die Unterschrifterkennung

7.1 Die Unterschrift

Im Gegensatz zu vielen anderen biometrischen Identifikationsverfahren wird die Unterschrift nie ungewollt abgegeben. Sie ist international anerkannt und wird seit Jahrhunderten zur Besiegelung von Verträgen verwendet. Die Unterschrifterekennung berücksichtigt Schriftbild und Dynamik.

7.2 Aufnahme der Unterschrift

Zunächst wird die Unterschrift mit einem Grafiktablett, wie es im Handel als Mausersatz erhältlich ist, aufgenommen. Als Beipiel wird hier das Wort "Biometrie"geschrieben.

Abbildung 4: Aufnahme der Unterschrift

7.3 Auswertung der Unterschrift

8 Technik der Fingerbildsensoren

Zur Aufnahme des Fingerbildes mit Sensoren wurden verschiedene physikalische Techniken entwickelt, von denen drei im Folgenden exemplarisch beschrieben werden sollen.

8.1 Kapazitives Verfahren

Als Beispiel soll hier ein kapazitiver Sensor der Firma Siemens gelten. Dieser Sensor besteht aus einem Array mit 224*288 einzelnen Kondensatorzellen auf einer Fläche von xxx * yyy mm. Die physikalische Auflösung des Sensors beträgt somit 513 dpi (dots per inch = Punkte pro Inch; 1 Inch = 2,540 m). Die einzelnen Sensorzellen bilden eine Fläche von 64.512 kleinen Kondensatoren, von welchen jeweils nur eine Platte vorhanden ist. Diese Platte wird mit einer Punktladung vorgeladen. Wird nun ein Finger auf den Sensor aufgelegt, dann Bildet die Haut dieses Fingers die entsprechenden Gegenplatten der Sensorkondensatoren. Durch die Unebenheiten der Haut (Papillarlinien, also Höhen und Tiefen) ergeben sich unterschiedliche Plattenabstände für die einzelnen Minikondensatoren. Aus diesen unterschiedlichen Abständen errechnen sich nach (***FORMEL***) unterschiedliche Kapazitätswerte für die Kondensatoren. Diese Kapazitäten werden durch den Sensor gemessen, abgespeichert und in verschiedene Graustufenwerte umgerechnet. Das dadurch gewonnene Graustufenbild kann sowohl auf dem Monitor angezeigt werden, als auch als Basis für die Erkennungsalgorithmen dienen (siehe Kapitel Fingerbilderkennung").

8.2 Optisches Verfahren

Als Beispiel für das optische Verfahren dient ein Fingerbildsensor der Firma Dermalog. Bei der optischen Aufnahme des Fingerbildes kommt eine herkömmliche CCD-Kamera (Charge-coupled Device). Der Finger wird dabei auf die Oberfläche eines dreieckigen Prismas aufgelegt, welches von unten zusätzlich durch eine LED (Light Emitting Diode bzw. lichtemittierende Diode) beleuchtet wird, um ein besseres Bild zu erhalten. Die Oberfläche des Prismas weist eine spezielle gummiartige Oberflächenvergütung auf, welche die Feuchtigkeit des Fingers abführen und den Kontrast erhöhen soll. Auf der dritten Seite des Prismas befindet sich der CCD-Chip, welcher das Bild aufnimmt. Das aufgenommene Bild wird durch eine Framegrabberkarte (Karte zum Digitalisieren analoger Bildsignale) digitalisiert und in den PC übertragen. Dort dient es als Basis für Erkennungsalgorithmen (siehe Kapitel Fingerbilderkennung").

8.3 Thermisches Verfahren

Im Gegensatz zum optischen und kapazitiven Verfahren wird bei der thermischen Fingerbilderkennung der Finger nicht statisch auf den Sensor aufgelegt, sondern über diesen gezogen. Als Beispiel soll hier ein Sensor der Fir-

ma Thomson dienen. Dieser Sensor besitzt eine Sensorzeile mit den Maßen 1,5 * 14 mm (0,21 cm2), auf welcher insgesamt 30*8400 Pixel angeordnet sind. Daraus ergibt sich rechnerisch eine Auflösung von 500 dpi (dots per inch = Punkte pro Inch; 1 Inch = 2,540 m). Die Sensorzeile wird aufgeheizt und durch den drüberstreichenden Finger wird diese Wärme abgeleitet. An den Erhebungen des Fingers ist ein besserer Kontakt zum Sensor gewährleistet, wodurch mehr Wärme abgeführt werden kann, während in den Rillen weniger Wärme aufgenommen werden kann. Aus den so gewonnenen Wärmeunterschieden errechnet der Sensor Zeilenweise ein Bild welches er dann zu einem gesamten Graustufenbild zusammensetzen kann. Dieses Graustufenbild dient dann, wie auch schon bei den anderen Sensortypen als Basis für Erkennungsalgorithmen (siehe Kapitel Fingerbilderkennung").

9 Forschungsprojekte zur biometrischen Identifikation

9.1 BioTrusT-Projekt

Das BioTrusT-Projekt war eines der größten Forschungsprojekte auf dem Gebiet der biometrischen Identifikationssysteme. Es wurde von der Arbeitsgruppe 6 des TeleTrusT-Vereins gegründet. Der TeleTrusT Deutschland e. V. (QUELLE) wurde 1998 gegründet und hat es sich zur Aufgabe gemacht, die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung zu fördern. Das BioTrusT-Projekt hatte es sich zu Ziel gesetzt, interdisziplinär sowohl die Zuverlässigkeit und Technik der einzelnen biometrischen Identifikationssysteme zu untersuchen, als auch eine Akzeptanzforschung in der Bevölkerung durchzuführen. Gleichzeitig wurden auch Verbraucherschützer und Datenschutzexperten in die Forschungen mit einbezogen. An der Fachhochschule Giessen Friedberg wurden dazu im sogenannten StarGate 12 verschiedene biometrische Systeme installiert. Über 400 Benutzer (Studenten, Professoren und wissenschaftliche Mitarbeiter) wurden auf diese Systeme angelernt (enrollt) und haben sie insgesamt über 75.000 mal benutzt. Durch die Ingenieure an der Fachhochschule konnten viele Fehler in den Systemen aufgedeckt werden, welche in engen Kontakt mit den Herstellern behoben werden konnten. So gab es z.B. Probleme mit diversen USB-Chipsätzen, welche nicht mit den Fingerbildsensoren interagieren konnten. Weiterhin war die Gesichtserkennung anfangs sehr fehleranfällig in Bezug auf Gegenlichtquellen. Insgesamt neun Hersteller von biometrischen Systemen beteiligte sich an dem Test und stellten dafür die entsprechenden Geräte zur Verfügung (u.A. Siemens, Dermalog, Cognitec, Iridian). Abge-

deckt wurden dadurch die Bereiche Gesichtserkennung, Fingerbilderkennung, Sprechererkennung und Iriserkennung.

10 Anwendungsbeispiele

10.1 Zollkontrolle am Flughafen (Frankfurt)

Seit Anfang 2005 können Reisende (Vielflieger) im Non-Schengen-Flugverkehr am Frankfurter Flughafen eine biometrische Grenzkontrolle passieren. Zu diesem Zweck wurden spezielle Schleusen bei der Passkontrolle eingerichtet, in welchen registrierte Passagiere durch eine Iriserkennung verifiziert werden können und dadurch die oftmals langen Warteschlangen an den normalen Zollkontrollen umgehen können.

10.1.1 Enrolment

Um die biometrische Grenzkontrolle nutzen zu können, müssen sich die Passagiere zunächst für die Iriserkennung anlernen (enrolen) lassen. Zu diesem Zweck wurde ein Enrollmentcenter (Registrierngscenter) im Checkinbereich im Terminal 1, Bereich A installiert. Der komplette Enrolmentvorgang dauert ungefähr 15 Minuten. Dazu werden zunächst die persönlichen Daten aus dem Reisepass erfasst und dieser wird maschinenlesbar eingescannt. Dann werden am Iriscangerät insgesamt vier Bilder von jedem Auge aufgenommen, um daraus die Vergleichstemplates zu generieren. Anschließend wird eine Probeverifikation durchgeführt, um sicherzustellen, daß die Person später an der Kontrollschleuse auch erfolgreich wiedererkannt werden kann. Die Ausweisdaten und die Irisdaten werden in einer lokalen Datenbank des Bundesgrenzschutzes gespeichert und verschlüsselt an die Kontrollschleusen übertragen. Knapp 5000 Passagiere haben sich bisher für dieses System enrolen lassen.

10.1.2 Iriskontrollschleuse

Nachdem die Reisenden personalisiert worden, können sie die speziell eingerichteten Kontrollschleusen mit dem Iriserkennungsgerät eigenständig passieren. Dafür legen sie zunächst ihren Reisepass auf einen Scanner auf. Wird ein gültiger Reisepass (zugehörig zu einer bereits vom System enrolten Person) erkannt, dann erhält der Passagier Zutritt zur Schleuse und zum Iriserkennungsgerät.

Hier erfolgt nun die Iris-Verifikation, wobei das System schon vorher mitgeteilt bekommen hat, welche Person nun erwartet wird und somit eine Verifikation (anstelle einer Identifikation) durchführen kann. Nach erfolgter Er-

kennung öffnet sich die Schleuse zum Grenzübertritt. Der gesamte Vorgang zur Grenzüberschreitung dauert ca. 15-20 Sekunden. Sollte die Iriserkennung nicht funktionieren, dann wird die entsprechende Person automatisch durch eine Seitentür in der Schleuse zu einer manuellen Kontrolle durch einen Beamten des Bundesgrenzschutzes geleitet.

10.2 Passwortersatz am PC

Mittlerweile vertreiben viele Hersteller Fingerbildsensoren, welche für den Login am heimischen PC verwendet werden können und die Passwörter ersetzen. Neben Sensoren, welche in die Maus eingebaut sind, gibt es auch stand-alone-Versionen, welche einfach an einen freien USB-Port angeschlossen werden.