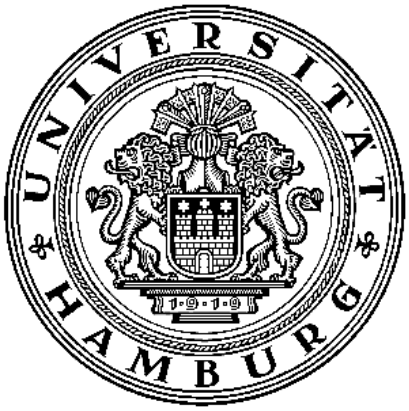
Verfahren der biometrischen Authentisierung und deren Unterstützung durch Chipkarten



Studienarbeit vorgelegt von

Stefan Henke

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich für Anwendungen der Informatik
in Geistes- und Naturwissenschaft

Juli 1999

Betreuerin: Dr. Kathrin Schier

1 Einleitung

Biometrie ist die Kunst, Leben zu (ver-)messen. Biometrische Verfahren ermöglichen Personenidentifikationen über Spracherkennung, Erkennung von Handgeometrie, Gesicht, Fingerabdruck, Iris oder Retina, die schon vor Jahren in "James Bond" Filmen zu bewundern waren. Diese Verfahren sind heute in realen Systemen erhältlich.

Ziel dieser Arbeit ist, die biometrischen Verfahren zu beschreiben und zu zeigen, wie eine Authentisierung mit ihrer Hilfe durchgeführt werden kann. Es soll auch gezeigt werden, wie Chipkarten systemunabhängig eine gesicherte Speicherung und Übertragung von Daten ermöglichen. Sie können Bindeglied zwischen einem biometrischen System und einem System sein, an dem sich authentisiert werden soll.

Biometrische Verfahren können auch mißbraucht werden, um personenbezogene Daten zu sammeln und systemübergreifend Benutzerprofile zu erstellen. Daher findet der Datenschutz besondere Beachtung und es wird eine Möglichkeit vorgestellt, wie Authentisierung anonym erfolgen kann.

Die Anwendungen biometrischer Verfahren, die ursprünglich auch Inhalt der Studienarbeit sein sollten, wie zum Beispiel die SIZ-Geldkarte oder die Bürgerkarte Berlin, konnten mangels Information oder mangels Zustandekommen des Projektes aufgrund fehlender finanzieller Mittel nicht behandelt werden. Statt dessen wird in stärkerem Maße auf die technischen Aspekte von Chipkarten und biometrischen Verfahren eingegangen.

2 Biometrische Verfahren

Biometrie ist eine Sammelbezeichnung für die zahlenmäßige Erfassung und Bearbeitung (besonders mit den Methoden der mathematischen Statistik) von Meß- und Zählwerten in allen Bereichen der Biologie, Medizin und Landwirtschaft. [Brockhaus87]

In der Informationstechnologie werden biometrische Verfahren zur Überprüfung der Identität einer Person zwecks Zugangsbeschränkung in sicherheitsrelevanten Bereichen eingesetzt.

Im Verlauf dieses Kapitels werden verschiedene biometrische Verfahren beschrieben sowie deren Eignung für Identifizierung und Authentisierung von Benutzern untersucht. Weiterhin wird auf Kriterien eingegangen, die für den Vergleich der biometrischen Verfahren verwendet werden können. Wenn von der Sicherheit eines biometrischen Systems geredet wird, so bezieht sich das nicht auf das umliegende System, in das das biometrische System eingebettet ist, sondern nur auf das biometrische System selbst. Die Sicherheit, die durch biometrische Verfahren zur Verfügung gestellt wird, darf nur als Bestandteil eines übergeordneten Sicherheitskonzeptes gesehen werden. Ein Sicherheitskonzept identifiziert und organisiert die Sicherheitsbetätigungen für ein System. Die Sicherheitspolitik ist Teil eines Sicherheitskonzepts. Sie beschreibt, wer auf welche Weise Zugriff auf welche Ressourcen erhalten darf [Pfleeger97].

2.1 Einführung

Authentisierung bedeutet „Bezeugung der Echtheit“. Ein Benutzer bezeugt seine Echtheit (seine Identität) gegenüber einem System, um zum Beispiel eine Leistung in Anspruch nehmen zu können.

Es gibt verschiedene Möglichkeiten der Authentisierung. Diese sind Authentisierung durch

- Wissen
- Besitz
- biometrische Eigenschaften.

Authentisierung durch Wissen oder Besitz oder einer Kombination aus beidem wird in vielen Bereichen verwendet. Für den Zugang zu einem Computer genügt meistens ein Benutzername und das zugehörige Paßwort. Eine Magnetkarte dient in vielen Parkhäusern als Nachweis dafür, daß der Benutzer berechtigt ist, das Parkhaus zu verlassen. Gegenüber einem Geldautomaten authentisiert sich ein Kunde mittels Magnetkarte und PIN.

Paßworte sollten aus Sicherheitsgründen für jedes System, bei dem ein Benutzer sich anmeldet, verschieden sein, damit der Verlust eines Paßwortes nicht mehrere Systeme kompromitieren kann. Dazu kommt, daß die Sicherheitspolitik oftmals vorschreibt, in regelmäßigen Abständen ein neues Paßwort zu wählen, das mit vorherigen Paßworten nicht übereinstimmen darf. Dies kann zu einer immer größeren Zahl von Paßworten führen, so daß ein Benutzer sich mehr und mehr Paßworte und PINs merken muß und so zum Teil dazu übergeht, sich die Paßworte zu notieren, wodurch die Sicherheit der betroffenen Systeme vermindert wird. Ebenso können Paßworte oder PINs verwechselt werden. Nach der dritten Eingabe einer vermeindlich richtigen PIN am Geldautomaten wird die Magnetkarte eingezogen, am Mobiltelefon wird die Chipkarte gesperrt.

Ein weiteres Problem kann in der Art liegen, in der ein Paßwort gewählt wird. Ein Wort, daß in einem Wörterbuch vorkommt oder Namen, wie der des Ehepartners sind unsicher, da sie durch einen Wörterbuchangriff oder durch Ausspähen in Erfahrung gebracht werden können. Ebenso ungeeignet sind das eigene Geburtsdatum oder das des Partners als PIN, sofern diese frei wählbar ist.

Die Authentisierung durch Besitz birgt den Nachteil, daß Besitz verloren, vergessen oder gestohlen werden kann.

Sowohl Wissen, als auch Besitz ist übertragbar. Bei Authentisierung über diese Merkmale kann nicht sichergestellt werden, daß die Person, die sich authentisiert auch tatsächlich dazu berechtigt ist.

Authentisierung durch biometrische Eigenschaften eröffnet die Möglichkeit, zum Beispiel auf das Wissen in Form eines Paßwortes oder einer PIN zu verzichten. Es werden personengebundene – und nicht nur personenbezogene Merkmale erfaßt. Biometrische Authentisierungsverfahren benutzen physiologische oder verhaltenstypische Charakteristika des Benutzers zu dessen Authentisierung ([TeleTrusT98] S.1). Durch Biometrie kann hinreichend sichergestellt werden, daß zum Beispiel der Benutzer einer Chipkarte auch der rechtmäßige Besitzer der Karte ist.

Biometrische Authentisierungsverfahren eignen sich überall dort, wo ein hoher Sicherheitsbedarf besteht. Dies umfaßt Bereiche wie Geldautomaten, Zeiterfassung, physikalischer Zugang zu sicherheitsrelevanten Bereichen, Zugriff auf Computersysteme, Zugang zu finanziellen staatlichen Leistungen oder auch Electronic Commerce. Zu Electronic Commerce gehört jede Transaktion, die per Telekommunikationstechnik elektronisch durchgeführt wird [Schier99]. Sie können Ersatz für Wissen und zum Teil auch Ersatz für Besitz sein und werden zum Beispiel zur Zugangskontrolle in Atomkraftwerken bereits über das Experimentierstadium hinaus eingesetzt.

Wie auch bei der in Kapitel 3.4.2 beschriebenen Authentisierung von Chipkarte – Lesegerät – Terminal sollte die Datenübertragung zwischen biometrischem Sensor und Terminal verschlüsselt werden, um einen Angriff auf das Gesamtsystem über das wiedereinspielen abgehörter Daten zu verhindern. Zu dem Zweck bietet sich das Challenge-Response-Verfahren an.

Biometrische Verfahren lassen sich in statische und dynamische Verfahren untergliedern. Statische Verfahren lesen ein Merkmal des Benutzers ein, das sich während des Vorgangs nicht verändert, also statisch ist. Zu den statischen Verfahren gehören unter anderem die Merkmale Fingerabdruck, Hand, Gesicht, Iris und Retina. Dynamische Verfahren sind solche, die sich während des Einlesevorgangs verändern. Dazu gehören die Merkmale Stimme, Unterschrift, und Tippdynamik, aber auch die Lippenbewegung beim Sprechen.

Es kann zwischen Authentisierung durch Verifikation und Authentisierung durch Identifikation unterschieden werden (siehe 4.1 / 4.2). Bei der Identifikation wird zu den eingelesenen Daten der passende Benutzer gesucht. Es findet also ein *1:n*-Vergleich von eingelesenen Daten und gespeicherten Daten statt. Bei der Verifikation wird getestet, ob ein Benutzer der ist, der er behauptet zu sein. Es findet also ein *1:1*-Vergleich von eingelesenen Daten und gespeicherten Daten statt. Dazu muß dem System angegeben werden, mit welchem Datensatz die eingelesenen Daten verglichen werden sollen. Dies kann zum Beispiel durch

Eingabe eines Benutzernamens erfolgen. Eine andere Möglichkeit wäre, das Referenzmuster auf einer Chipkarte zu speichern, von der es zum Vergleich geladen werden kann.

Bei Authentisierung mit biometrischen Verfahren handelt es sich grundsätzlich um ein Mustererkennungsproblem zur Trennung von zwei Klassen, den Originalen und den Fälschungen. Dabei muß ein System einerseits beträchtliche Variabilitäten in den Originaldaten akzeptieren um den Zutritt zur gewünschten Applikation für berechtigte Nutzer zu garantieren, während Fälschungen, die Originalen nahe kommen, zurückgewiesen werden müssen [DuD1].

2.1.1 Ablauf einer biometrischen Authentisierung

Gemeinsam ist den verschiedenen biometrischen Verfahren der in Abbildung 1 dargestellte prinzipielle Ablauf einer biometrischen Verifikation oder Identifikation.

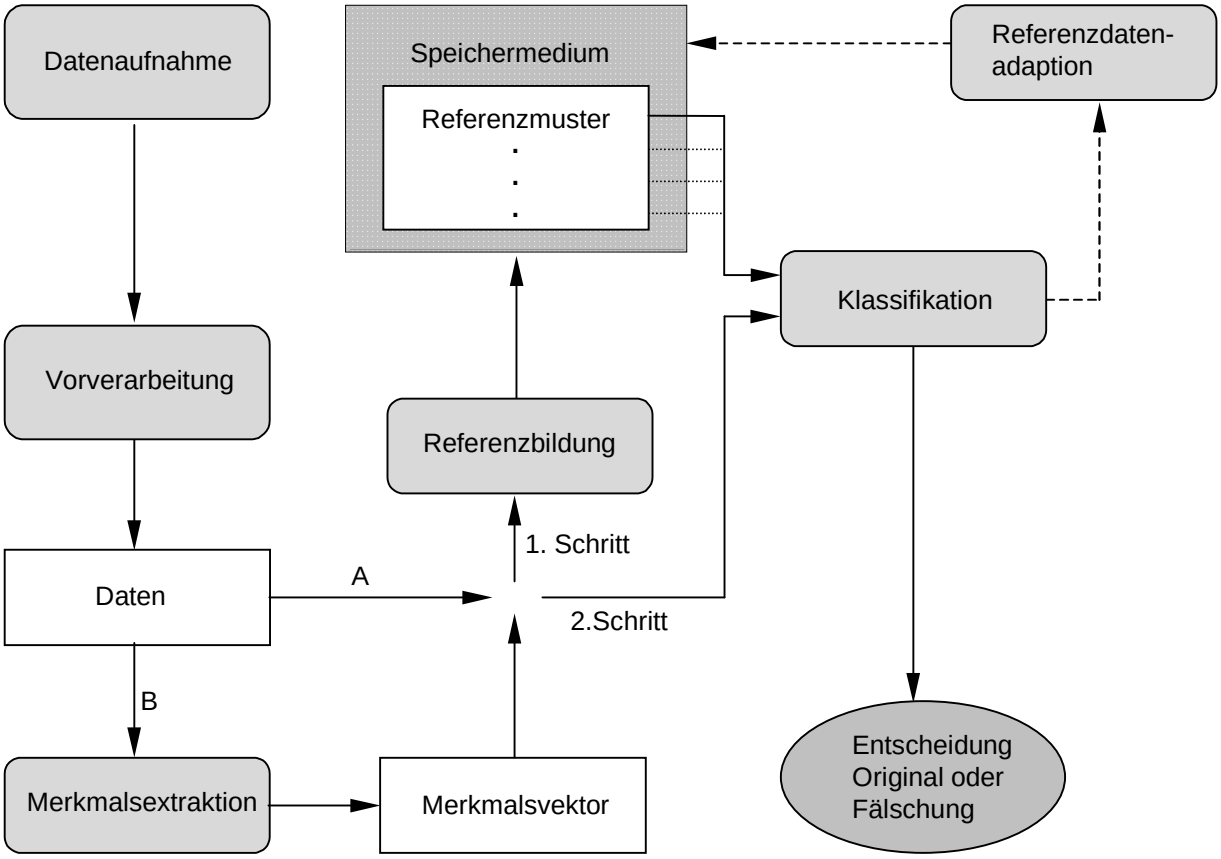


Abbildung 1: Ablauf einer biometrischen Verifikation oder Identifikation (Quelle: [TeleTrusT 98] S. 3)

Bei jedem der Verfahren werden in der *Datenaufnahme* über einen Sensor biometrische Daten des Benutzers eingelesen und in der *Vorverarbeitung* normalisiert, das heißt, die Daten werden in eine für das jeweilige Verfahren erforderliche Normalform gebracht. Der Sensor ist, je nach biometrischem System, zum Beispiel eine Kamera, ein Mikrofon oder auch die Tastatur des Computers.

Für die weiteren Schritte können im Fall *A* die normalisierten Daten verwendet werden oder es wird im Fall *B* aus diesen Daten in der *Merkmalsextraktion* ein *Merkmalsvektor* erzeugt. Bei der Bildung eines Merkmalsvektors werden aus den eingelesenen biometrischen Daten besondere Punkte herausgenommen und miteinander verbunden, so daß ein Netz entsteht. Dieses Netz bildet den Merkmalsvektor. Der umgekehrte Weg, also aus einem Merkmalsvektor wieder die biometrischen Daten zu erhalten ist nicht möglich, weil bei der Bildung eines Merkmalsvektors durch die herausnahme nur einiger Punkte Information verlorenen geht. Besondere Punkte können bei der Gesichtserkennung (siehe 2.8) zum Beispiel Kinn, Mund oder Nase sein, bei der Handgeometrie (siehe 2.4) die Fingerenden.

Die *Referenzbildung* ist der Prozeß des initialen Erlernens der biometrischen Charakteristika durch das System [DuD1]. Für einen neuen Benutzer werden im 1. Schritt die bis hier erfolgten Schritte eine festzulegende Anzahl von Malen wiederholt, um dann in der *Referenzbildung* das *Referenzmuster* zu erstellen. Im 2. Schritt werden für bereits registrierte Benutzer bei einem Authentisierungsversuch in der *Klassifikation* die Eingangsdaten aus Fall *A* oder *B* bei Verifikation mit dem entsprechenden Referenzmuster (1:1), bei Identifikation mit allen Referenzmustern (1:n) verglichen. Die Eingangsdaten werden dort als Original oder Fälschung klassifiziert. In Verfahren, die Adaption verwenden (siehe Kapitel 4), gehen die Daten aus Fall *A* oder *B* wieder in das Referenzmuster ein, sofern das System diese als Original erkannt hat. Auf diese Weise werden Änderungen von Verhalten oder physischen Merkmalen eines Benutzers berücksichtigt.

2.1.2 Notwendige Eigenschaften biometrischer Merkmale

Um für biometrische Authentisierung geeignet zu sein, muß ein biometrisches Merkmal einige wichtige Eigenschaften aufweisen ([TeleTrusT98] S. 5). Diese sind

- Einzigartigkeit
  Für verschiedene Menschen muß das muß das Merkmal hinreichend verschieden sein. Ein biometrisches Merkmal, daß nur 100 verschiedene Ausprägungen besitzt, wäre nicht sinnvoll einsetzbar. Um nachzuweisen, daß ein Merkmal geeignet ist, sollte die Einzigartigkeit eines Merkmals durch theoretische Berechnungen nachgewiesen - und durch praktische Versuche bestätigt werden.
- Konstanz
  Das Merkmal sollte sich im Laufe der Zeit möglichst wenig ändern. Kleinere Änderungen, sie können besonders bei dynamischen Verfahren auftreten, können durch adaptive Verfahren ausgeglichen werden.
- Verbreitung
  Das Merkmal muß bei möglichst vielen Personen, die das System benutzen sollen, vorhanden sein. Die Iriserkennung ist zum Beispiel für blinde Menschen ebenso ungeeignet, wie die Spracherkennung für Stumme. Auch gibt es Menschen, die für biometrische Verfahren keine hinreichend ausgeprägten Fingerabdrücke haben. Um die diskriminierung dieser „biometrischen Randgruppen“ zu vermeiden, sollten alternative Erkennungsmethoden angeboten werden.

2.2 Vergleichbarkeit biometrischer Verfahren

2.2.1 Fehlerraten

Damit ein Benutzer bei der Authentisierung über Benutzername und Paßwort Zugang zum System erhält, müssen die von ihm eingegebenen Zugangsdaten immer identisch sein. Das System nimmt einen 1:1 Vergleich der eingegebenen Zugangsdaten mit den gespeicherten Zugangsdaten vor, um die Echtheit des Benutzers zu bestätigen. Abweichungen werden nicht akzeptiert.

Anders ist dies bei der biometrischen Authentisierung. Das Verhalten eines Benutzers, zum Beispiel bei auf Motorik basierenden Systemen (siehe 2.10), variiert leicht von Login zu Login. Bei Authentisierung über physiologische Charakteristika können ebenfalls Abweichungen auftreten, zum Beispiel eine veränderte Stimmlage durch Heiserkeit, unreine oder feuchte Fingerabdrücke oder Lichtreflexionen im optischen Sensor. Jedes biometrische System muß also bei der Authentisierung tolerant sein, da die eingelesenen Daten beziehungsweise der daraus erzeugte Merkmalsvektor nur selten zu 100% mit dem gespeicherten Referenzmuster übereinstimmen (siehe Abbildung 1). Dies wird über einen Toleranzwert gelöst, mit dem eingestellt wird, um wieviel Prozent die Daten in der Klassifikation voneinander abweichen dürfen. Ist die Abweichung der eingelesenen Daten von den gespeicherten Daten größer als der eingestellte Toleranzwert des Systems, so schlägt die Authentisierung durch Verifikation des Benutzers fehl und der Benutzer wird zurückgewiesen. Bei Authentisierung durch Identifikation wird in dem Fall solange zum jeweils nächsten gespeicherten Datensatz übergegangen, bis der passende Datensatz gefunden wurde oder alle Datensätze überprüft wurden und der Benutzer zurückgewiesen wird.

Je niedriger der Toleranzwert des Systems ist, desto häufiger werden Benutzer fälschlicherweise zurückgewiesen, desto häufiger werden aber auch unautorisierte Zugriffe verhindert.

Aus statistischer Sicht läßt sich ein Zugangssystem über zwei Fehlerraten charakterisieren. Die eine Fehlerrate ist die „False Rejection Rate“ (FRR), die andere Fehlerrate ist die „False Acceptance Rate“ (FAR). Die FRR berechnet sich als Quotient aus der Summe fälschlich zurückgewiesener Zugriffe (fzz) und der Summe der berechtigten Zugriffsversuche (bz). Die FAR ist der Quotient aus der Summe der vom System fälschlich akzeptierten Zugriffe (faz) und der Summe der gesamten unberechtigten Zugriffsversuche (uz). Sowohl die FAR als auch die FRR werden in Prozent angegeben.

$$FRR = \frac{fzz}{bz} \times 100 \qquad FAR = \frac{faz}{uz} \times 100$$

In Abhängigkeit zum Toleranzwert läßt sich für die beiden Fehlerraten die in Abbildung 2 dargestellte stilisierte Grafik erstellen:

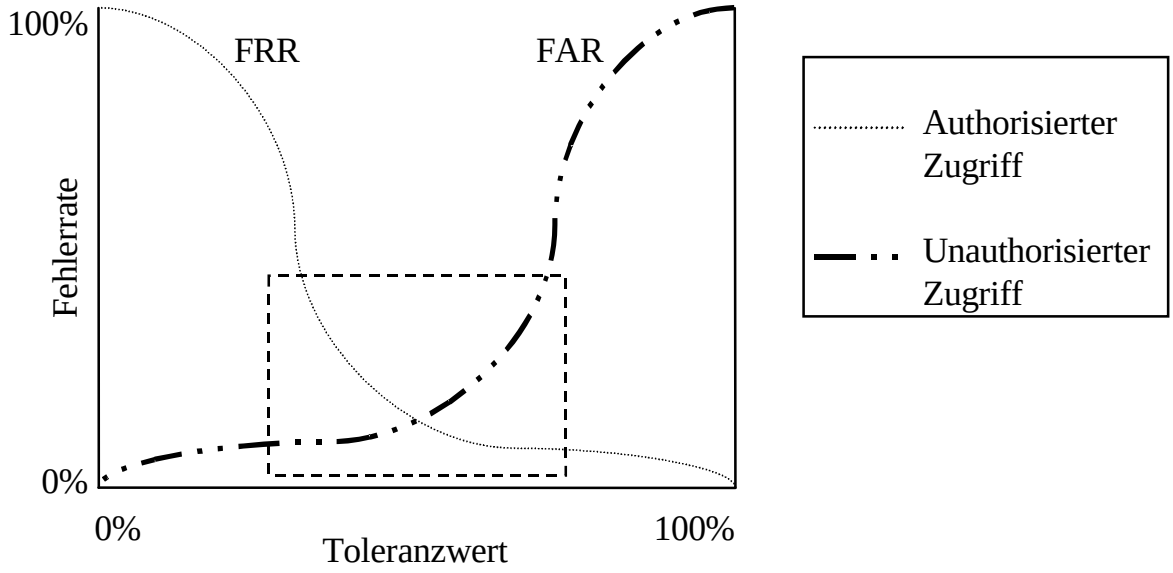


Abbildung 2: Die Fehlerraten des autorisierten Zugriffs (FRR) und des unautorisierten Zugriffs (FAR) in Abhängigkeit zum Toleranzwert

Der durch das gestrichelte Kästchen dargestellte Ausschnitt wird in Abbildung 3 genauer analysiert. Betrachten wir einen Extremwert in Abbildung 2, den Toleranzwert von 100%. Bei diesem Wert wird jeder Benutzer vom System akzeptiert. Dadurch liegt die FRR bei 0%, da kein autorisierter Benutzer abgewiesen wird und die FAR bei 100%, denn auch jeder unautorisierte Zugriff wird akzeptiert. Je weiter der Toleranzwert verkleinert wird, desto seltener werden unautorisierte Zugriffsversuche akzeptiert – die FAR sinkt – und desto häufiger kann es vorkommen, daß autorisierte Benutzer abgewiesen werden – die FRR steigt. Bei einem Toleranzwert von 0% geht die FRR gegen 100% und die FAR gegen 0%, ohne daß diese Grenzwerte erreicht werden. Die FRR erreicht nie 100%, da es durchaus vorkommen kann, daß die eingelesenen Daten zu 100% mit den gespeicherten Daten eines Benutzers übereinstimmen. Die Tatsache, daß die FAR nie 100% erreicht, begründet sich in der statistisch sehr geringen Wahrscheinlichkeit, daß die eingelesenen biometrischen Daten, beziehungsweise der daraus gewonnene Merkmalsvektor zweier Menschen identisch sind. Diese Wahrscheinlichkeit ist zwar sehr gering, aber dennoch vorhanden (siehe folgende Abschnitte und Kapitel 4). Wie hoch die Toleranz eines biometrischen Systems eingestellt wird und welche der Fehlerraten somit minimiert wird, hängt von der Anwendung ab, in der das System eingesetzt werden soll. Je kritischer die Sicherheit für ein System ist, desto eher kann von einem Benutzer verlangt werden, eine fälschliche Abweisung hinzunehmen. Dagegen ist bei Systemen, die als Massenanwendung eingesetzt werden sollen, die Benutzerakzeptanz, die bei häufiger fälschlicher Rückweisung sinkt, von größerer Bedeutung (siehe 2.2.2).

An dem Punkt, wo die Kurven für FAR und FRR sich schneiden, liegt die Equal Error Rate (EER) oder auch Gleichfehlerrate. Je niedriger die EER ist, desto niedriger sind FAR *und*

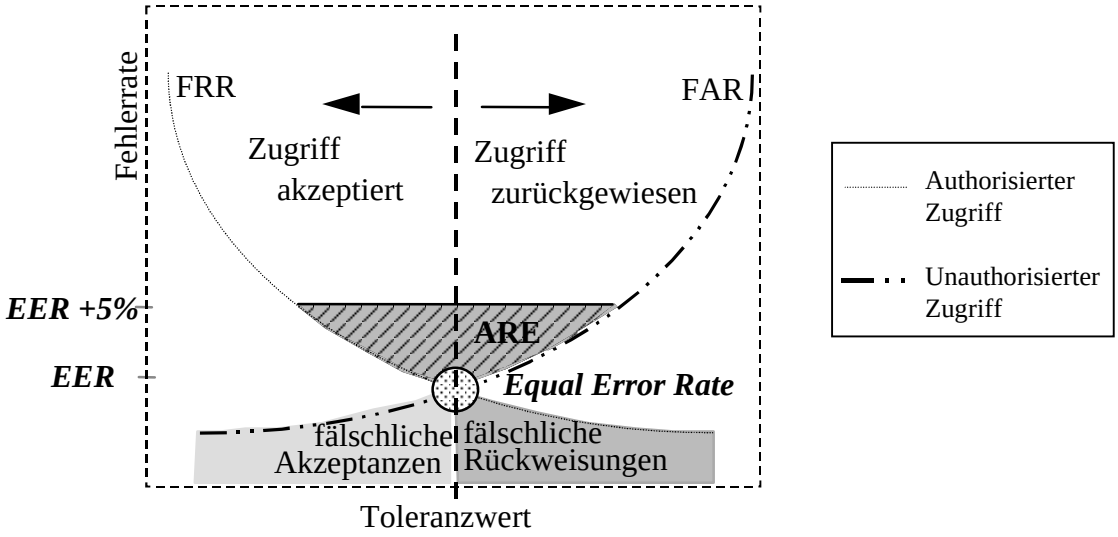


Abbildung 3: EER, ARE & Co (Quelle: [TeleTrusT98] S. 9)

FRR, desto weniger fälschliche Akzeptanzen oder Rückweisungen treten auf. Die EER beschreibt die Trennfähigkeit eines Systems zwischen Originalen und Fälschungen.

Die Bestimmung der EER ist nur im Falle klassifizierter Originale und Fälschungen als theoretische Evaluierung der Leistungsfähigkeit eines Systems möglich. Beim tatsächlichen Systemeinsatz muß die Zulassungstoleranz entsprechend den gewünschten Fehlerraten aus den Referenzdaten geschätzt und gegebenenfalls adaptiert werden. Es ist dann zu prüfen, wie weit die tatsächlichen Fehlerraten von den theoretischen abweichen ([TeleTrusT] S. 9).

Je nach Anwendung kann der Toleranzwert abweichend von seinem theoretisch idealen Wert am Schnittpunkt von FAR und FRR eingestellt werden (siehe 2.2.2). Es ist also wichtig, auch das Systemverhalten um dem idealen Punkt herum zu betrachten. Veschiedene Systeme können in ihrem Verhalten um diesen Punkt deutlich voneinander abweichen. Bei einem System mit stark ansteigender Kurve der FAR führt zum Beispiel eine Erhöhung des Toleranzwertes zugunsten einer besseren FRR zu einer stärkeren verschlechterung der FAR als bei einem System, in dem die Kurve der FAR nur schwach ansteigt. Zur Charakterisierung eines Systems sollten deshalb neben der Angabe der EER als eindeutige Kenngröße des Systems die charakteristischen FAR- und FRR-Fehlerkurven gemeinsam dargestellt werden, so daß das Verhalten um den kritischen Punkt visualisiert werden kann.

Eine weitere Möglichkeit ein System genauer charakterisieren zu können, ist die Betrachtung der Fläche zwischen den Fehlerkurven, der EER und der EER + 5%. Dieser Bereich, ARE genannt, ist in Abbildung 3 als schraffierte Fläche dargestellt. Steigen die Kurven der Fehlerraten links und rechts der EER stark an, so ist die ARE kleiner als wenn die Kurven nur leicht ansteigen. Je größer die ARE ist, desto besser ist die Trennfähigkeit eines Systems zwischen Originalen und Fälschungen. Die Angabe der ARE eines Systems kann die Darstellung der Fehlerkurven ergänzen.

Von den Herstellern biometrischer Systeme angegebene Werte für FAR und FRR liegen

- für die FAR zwischen 10^{-4} und 10^{-1} %
- für die FRR zwischen 10^{-3} und 1 %
- für die EER zwischen 10^{-3} und 10^{-1} %

Um über statistische Daten diskutieren zu können, ist eine minimale Datensatzgröße notwendig. Das heißt für

- eine Sicherheit von 95%,
- eine EER von 3% sowie
- eine maximale Abweichung der realen von der geschätzten Fehlerwahrscheinlichkeit von 0,5 %

benötigt man mindestens 4.500 Datensätze. ([TeleTrusT98] S. 7)

Untersuchungen über die Fehlerraten eines Systems sollten möglichst alle relevanten Originaldatenvariabilitäten abdecken. Für den praktischen Einsatz sollten insbesondere natürliche Variationen an den Originaldaten nicht zur Verwechslung mit Fälschungen führen und daher im Test enthalten sein. Eine Mindestvoraussetzung ist daher die Streuung der Sammlung der Originale über einen relevanten Sammlungszeitrahmen ([TeleTrusT98] S. 14). Neben der Zahl der Messungen sollte auch die Zahl der verschiedenen Personen, an denen gemessen wurde, bekannt sein. Dazu auch der Zeitraum über den die Messungen durchgeführt wurden, da sich einige Merkmale mit der Zeit ändern können. Je breiter die Datenbasis ist, anhand der die Fehlerraten getestet werden, desto genauer kann das Ergebnis sein.

Wenn ein System auf fehlerhafte Akzeptanz getestet wird, kann dies mit zufälligen oder mit geübten Fälschungen geschehen.

Zufällige Fälschungen sind die Verwendungen anderer Originale als Fälschungen. Sie können dadurch entstehen, daß bei Authentisierung durch Verifikation (siehe 4.1) zum Beispiel versehentlich eine falsche Identifikationsnummer eingegeben wurde oder bei Authentisierung durch Identifikation (siehe 4.2) das Muster einer dem System unbekannten Person mit der Referenzdatenbank verglichen wird.

Geübte Fälschungen werden mit Aufwand und der Intention erzeugt, bestimmten Originalen so ähnlich wie möglich zu sein ([TeleTrusT98] S. 14). Bei statischen Verfahren mit impliziter oder expliziter Lebenderkennung (siehe 2.3-2.12) sind solche Fälschungen nicht oder nur unter sehr hohem Aufwand durchfühbar. Ohne die Lebenderkennung wäre es durchaus denkbar, daß der Wachsabdruck eines fremden Fingers, ein Foto oder eine künstliche Hand vom System akzeptiert werden. Dynamische Verfahren erlauben vom Grundsatz her den Versuch, das Verhalten eines anderen Benutzers bei der Authentisierung zu imitieren.

In den meisten Fällen sind die Fehlerraten biometrischer Systeme aufgrund theoretischer Gegebenheiten des biometrischen Merkmals geschätzt und täuschen eine Genauigkeit vor, die in der Realität möglicherweise gar nicht erreicht wird. Da noch keine standardisierten Testdatenbanken existieren, sind die Fehlerraten verschiedener Systeme meist auch nicht miteinander vergleichbar. Ein System läßt sich nicht nur über die in Abbildung 3 genannten Größen charakterisieren, da sich die Eigenarten des verwendeten biometrischen Merkmals

nicht in den Fehlerraten wiederspiegeln. Somit ist ein Vergleich zweier biometrischer Systeme nur anhand ihrer Fehlerraten ungenau.

2.2.2 Einfluß auf die Benutzerakzeptanz

Die Wahl, welches biometrische Verfahren eingesetzt werden sollte, hängt sowohl von der gegebenen Anwendung ab, als auch von der zu erwartenden Benutzerakzeptanz [DuD1].

Für die Akzeptanz, die ein Benutzer einem System entgegenbringen soll, kommt es auf mehrere Faktoren an ([TeleTrusT] S. 24). Diese sind unter anderem

- Komfort bei der Benutzung

  Der Benutzungskomfort umfaßt den Zeitaufwand im Normalfall bei der Authentisierung am System und im Fall der fehlerhaften Rückweisung. Die Anwendung sollte möglichst einfach zu bedienen sein. Wichtig ist auch, ob es Ersatzmöglichkeiten für das biometrische Merkmal gibt, sollte dieses einmal zeitweilig ausfallen (zum Beispiel eine aufgrund einer Verletzung bandagierte Hand. Auch die Erstellung des Referenzmusters sollte schnell und ohne großen zusätzlichen Aufwand vonstatten gehen. Wenn ein Erfassungsstelle zur Erstellung des Referenzmusters notwendig ist, sollte diese schnell erreichbar sein.

- Vertrautheit und Transparenz

  Die Transparenz oder Durchschaubarkeit eines biometrischen Verfahrens ist Voraussetzung für einen Benutzer, um sich ein eigenes Urteil bilden zu können [Meyer90]. Die Vertrautheit mit bereits bekannten und etablierten Vorgängen steigert die Akzeptanz, wenn diese Vorgänge durch Biometrie erfüllt werden sollen. Wenn die Zusammenhänge und der Abläufe leicht verständlich sind, der Benutzer also versteht, was bei der biometrischen Authentisierung passiert, wird dies die Bereitschaft zur Kooperation beim Benutzer steigern. Wenn ein Benutzer ein biometrisches System nicht akzeptieren will, weil er es zum Beispiel nicht richtig versteht, dann ist er auch nicht gewillt, sein biometrisches Merkmal gemäß den jeweiligen Anforderungen zu präsentieren. Dadurch kann sich die FRR für diesen Benutzer erhöhen, was sich wiederum negativ auf die Akzeptanz auswirkt.

- Belästigung

  Unter den Punkt Belästigung fallen die Aspekte Hygiene und Invasivität. Wenn das System berührungsfrei arbeitet, wird sich ein Benutzer auch nicht von einem verschmutzten Sensor belästigt fühlen. Nicht leicht vorhersagbar ist, inwiefern die Biometrie in die persönliche Schutzsphäre des Benutzers eindringt. Es ist zu vermuten, daß ein System, das zum Beispiel die Geometrie der Hand einliest, eine weniger große Belästigung darstellt, als ein System, das den Verlauf der Blutgefäße auf der Retina vermißt.

- Vorurteile und Ängste

  Es können Vorurteile gegen die Registrierung oder die Benutzung eines biometrischen Systems bestehen. Auch ist nicht ausgeschlossen, daß einige Benutzer Angst haben, ihre biometrischen Daten könnten zum Beispiel zur Erstellung von Profilen oder zur Rasterfahndung mißbraucht werden.

Der Faktor „Vorurteile und Ängste“ wird in Kapitel 4 im Zuge der Datenschutzverfahren behandelt.

Biometrische Verfahren können eingesetzt werden um

- eine bestehende, bereits akzeptierte Anwendung zu erweitern oder
- eine neue oder unzureichend akzeptierte Anwendung zu realisieren.

Die erste der beiden Möglichkeiten soll in bezug auf die Benutzerakzeptanz anhand eines Beispiels erläutert werden.

Das Abheben von Geld an einem Geldautomaten läuft zur Zeit in folgenden Schritten ab:

1. Einführen der Magnetkarte in den Automaten
2. Eingabe der PIN
3. Eingabe des auszugebenden Geldbetrages
4. Entnahme von Karte und Geld falls die PIN korrekt eingegeben wurde, ansonsten maximal 2 weitere Authentisierungsversuche ab Schritt 2.

Bei der Nutzung von Biometrie am Geldautomaten wird die bislang verwendete PIN aus Schritt 2 durch ein biometrisches Merkmal oder durch eine Kombination von Merkmalen ersetzt. Das Einlesen der biometrischen Merkmale sollte nur einen Bedienschritt in Anspruch nehmen, ebenso wie dies bislang bei der Eingabe einer PIN erforderlich war. Realisierbar wäre dies zum Beispiel durch Kombinationen wie Handgeometrie und Fingerabdruck oder Gesicht und Stimme. Für den Benutzer bedeutet dies keine große Umstellung, da auch bisher, nachdem die Karte eingeführt wurde, eine Eingabe erforderlich war.

Die Erfassung und Verarbeitung der biometrischen Daten sollte nicht länger dauern, als die Eingabe einer PIN, also weniger als 5 Sekunden, damit die Dauer des gesamten Vorgangs nicht größer wird. Dies gilt genauso für den Fall, daß ein Benutzer fehlerhaft abgewiesen wird, was der falschen Eingabe einer PIN entspricht.

Die Anzahl der Fälle, in denen ein berechtigter Benutzer abgewiesen wird, sollte minimiert werden. Das entspricht der Minimierung der FRR, die zumindest kleiner 1% sein sollte. Der Benutzer wird das System weniger akzeptieren, wenn er häufiger zurückgewiesen wird, als dies zuvor der Fall war. Angenommen ein Benutzer hebt einmal pro Woche Geld an einem Automaten ab. Dann bedeutet eine FRR von 1%, daß der Benutzer im Schnitt etwa alle zwei Jahre fälschlich zurückgewiesen wird.

Ebenfalls wichtig ist, daß der Aufwand, der zur Erstellung des Referenzmusters nötig ist, möglichst gering gehalten wird. Wünschenswert ist eine Erfassungsstelle in jeder Filiale und die rechtzeitige Ausgabe der für das gewählte biometrische Verfahren geeigneten Karte. Das ist entweder eine Magnetkarte oder, was wahrscheinlicher ist, eine Chipkarte, die der Magnetkarte gegenüber erheblich sicherer ist. Die rechtzeitige Ausgabe der Karte ist erforderlich, damit jedem Benutzer die Möglichkeit gegeben wird, seine Bank zur Öffnungszeit zu erreichen.

Wie und ob das System den Ausfall eines erforderlichen biometrischen Merkmals kompensieren kann, hängt vom verwendeten Verfahren ab. Es ist denkbar, einen zweiten Finger oder die jeweils andere Hand biometrisch registrieren zu lassen um dadurch Ersatz zu schaffen oder auch ein Verfahren aus drei Merkmalen zu verwenden, das den Ausfall eines der Merkmale toleriert.

Aus Sicht der Betreiber biometrischer Systeme, in diesem Fall der Banken, stehen den zusätzlichen Anschaffungs-, Betriebs- und Wartungskosten die eingesparten Kosten gegenüber, die zur Zeit durch Mißbrauch von EC-Karten entstehen. Wenn zu erwarten ist, daß durch die Einführung biometrischer Verfahren Kosten gespart werden können, ist der Anreiz zu deren Implementierung vorhanden.

2.3 Fingerabdruck

Die angegebenen Werte zu Datensatzgrößen der Muster, Erkennungsgeschwindigkeiten und FAR / FRR sind Angaben verschiedener Hersteller zu ihren Produkten. Die Testbedingungen, unter denen sie ermittelt wurden, sind im Regelfall von den Herstellern nicht oder nicht detailliert veröffentlicht worden. Dies gilt für alle biometrischen Merkmale.

2.3.1 Verfahrensbeschreibung

Der menschliche Fingerabdruck ist das biometrische Merkmal, das schon seit mehr als 100 Jahren zur Identifizierung von Individuen verwendet wird [FBI84]. Fingerabdrücke werden noch vor der Geburt gebildet und verändern sich während des Lebens nicht ([Roddy99] S. 4). Auf der Haut der Fingerspitzen bilden Erhebungen ein Linienmuster. In den Erhebungen befinden sich Poren, die Schweiß absondern. Dieser Schweiß bildet entlang der Erhebungen einen Film. Kommt der Finger mit einer Oberfläche in Berührung, wird ein Teil des Schweißfilms auf der Oberfläche zurückgelassen, wodurch ein Fingerabdruck entsteht.

Das Verfahren ist nicht berührungslos. Zur Authentisierung wird ein Finger, dessen Referenzmuster dem System bekannt ist, auf einen Sensor gelegt. Der Sensor liest die Merkmale ein und vergleicht sie mit den gespeicherten Referenzmustern (1:n) oder mit einem angegebenen Referenzmuster (1:1) (siehe 2.1).

Verschiedene Faktoren können die Authentisierung erschweren oder verhindern. Diese sind

- zuviel oder zuwenig Feuchtigkeit auf dem Finger
- Schmutz auf dem Finger oder auf dem Sensor
- temporäre Veränderungen am Finger
- fehlerhafte Positionierung des Fingers auf dem Sensor

Abbildung 4: Zu feuchter-, zu trockener- und beschädigter Fingerabdruck

Ist ein Finger zu feucht, dann befindet sich in den Rillen des Fingers so viel Feuchtigkeit, daß zwischen einzelnen Erhebungen Flächen entstehen und die Struktur somit verfälscht wird.

Bei zuwenig Feuchtigkeit können einige Sensoren das Linienmuster der Erhebungen nicht mehr vollständig erfassen, wobei zum Teil auch wichtige Charakteristika unerfaßt bleiben.

Schmutz kann die Linienstruktur überdecken.

Einschnitte oder Abschürfungen können den Fingerabdruck bis zur Heilung verfälschen oder komplett unleserlich machen.

Bei Fingerabdrücken kann man zwischen drei Grundformen unterscheiden: Wirbel, Schleifen und Bögen.

Abbildung 5: Die verschiedenen Arten von Fingerabdrücken (Quelle: [Jasperinc99])

Etwa 5% aller Fingerabdrücke sind Bögen, 30% sind Wirbel und 65 % sind Schleifen. [Jasperinc99]. Die weißen Punkte in den Fingerabdrücken in Abbildung 5 sind Poren, die sich in den Erhebungen befinden.

Für die Klassifikation eines eingelesenen Fingerabdrucks in Original oder Fälschung wird für eine Verifikation im Mittel eine Sekunde benötigt, für eine Identifikation in Abhängigkeit zur Größe der Datenbank und Geschwindigkeit der verarbeitenden Einheit entsprechend länger. Die gesamte Dauer der Verifikation eines Benutzers, von der Ankunft am Gerät bis zu dessen Verlassen beträgt im Mittel etwa 7 Sekunden ([Sandia91] S.20).

Die Größe eines Datensatzes liegt zwischen 256 Bytes und 2000 Bytes. Bei heutigen Speichermedien, auch bei Chipkarten, stellt diese Platzanforderung kein Problem dar.

Eine Authentisierung kann ausgelöst werden, in dem ein Finger auf dem Sensor plaziert wird. Der Fingerabdruck ist ein statisches Merkmal und erfordert während der Authentisierung selbst keine Aktion des Benutzers. Dadurch ist es bei hohem Sicherheitsbedarf erforderlich, dem Sensor einen Scanner hinzuzufügen, der überprüft, ob es sich um einen echten, lebendigen Finger handelt. Diese Lebenderkennung soll verhindern, daß das System von einem Wachsfinger oder einem auf einen Finger aufgebrachten Latexabdruck getäuscht werden kann. Es kann zum Beispiel überprüft werden, ob in dem aufgelegten Finger Blut pulsiert.

Geräte zur Erkennung von Fingerabdrücken sind in verschiedenen Variationen am Markt erhältlich. Es gibt sie wandmontiert als Zugangskontrolle zu Räumen oder Gebäuden, als eigenständiges Gerät, das zum Beispiel über die serielle Schnittstelle an einen PC angeschlossen werden kann, aber auch integriert in Eingabegeräte wie Tastatur oder Maus. Das

Sensorfeld, das einen Fingerabdruck einliest, ist normalerweise etwa so groß, wie der Fingerabdruck selbst. Es gibt aber bereits Sensoren, die so Breit sind, wie ein Finger, aber wesentlich kürzer. Bei solchen Sensoren, die zum Beispiel in Mobiltelefonen zum Einsatz kommen sollen, muß der Finger über den Sensor bewegt werden, der die einzelnen Abschnitte intern wieder zusammensetzt, um so das komplette Bild des Fingerabdrucks zu erhalten.

2.3.2 Sensorprinzipien

Um einen Fingerabdruck auszulesen, können verschiedene Arten von Sensoren zum Einsatz kommen. Es gibt

- kapazitive Sensoren,
- Infrarot-Sensoren und
- optische Sensoren.

Kapazitive Sensoren nutzen eine kleine Sensorplatte bestehend aus vielen einzelnen Kondensatoren. Wird ein Finger auf diese Platte gelegt, so kommen nur die Erhebungen der Fingerspitze in Kontakt mit der Platte. Überall dort, wo ein solcher Kontakt entsteht, entladen sich die Kondensatoren. Der Zustand der Kondensatoren, also ob sie geladen oder entladen sind, ergibt das Bild des Fingerabdrucks.

Infrarot-Sensoren funktionieren ähnlich wie die kapazitiven, nur daß bei dem Kontakt des Fingers mit dem Sensor keine Ladung, sondern Wärme ausgetauscht wird. Die Erhebungen geben, da sie Kontakt haben, die Wärme besser ab, als die Rillen. Die Wärmedifferenzen auf dem Sensor ergeben das Bild des Fingerabdrucks.

Optische Sensoren senden einen Lichtstrahl in einem Winkel von 45 Grad zum aufgelegten Finger. Anhand der Reflexion des Lichts kann der Sensor die Linienstruktur des Fingerabdrucks erkennen.

2.3.3 Merkmalscharakteristika

Es gibt verschiedene Methoden, mit denen aus dem Fingerabdruck ein Vergleichsmuster erstellt werden kann:

- Die einfachste Methode ist, die Grauwertbilder des Fingerabdrucks und des Musters zu verwenden. Dies ist aus datenschutzrechtlicher Sicht bedenklich, da Grauwertbilder Rückschlüsse auf den Besitzer des entsprechenden Fingerabdrucks erlauben. Es wäre zum Beispiel möglich, ein Grauwertbild mit Fingerabdrücken einer Verbrecherkartei zu vergleichen.
- Eine weitere Methode ist die Ermittlung von Minutiae. Minutiae sind besondere Punkte im Linienmuster eines Fingerabdrucks wie zum Beispiel [Jasperinc99]

  - Verzweigungen 
  - Endungen 
  - Inseln 

Wie in Abbildung 6 gezeigt, kann ein Muster aus Minutiae gebildet werden. Dieses am häufigsten verwendete Verfahren benötigt eine Sensorauflösung von ca. 500 dpi [Veridicom99]. Die Minutiae werden über Vektoren miteinander verbunden und nur das resultierende Muster wird gespeichert und für den Vergleich verwendet. Für eine juristisch eindeutige Identifikation einer Person sind zwölf Minutienpaare ausreichend.

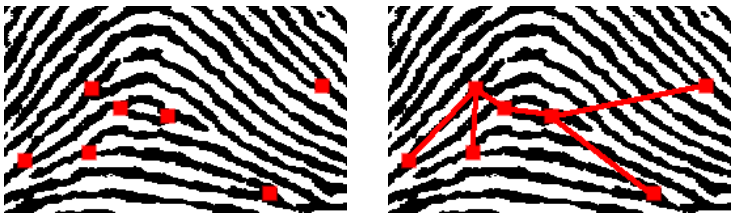


Abbildung 6: Bildung eines Musters aus einzelnen Minutiae

- Statt Minutiae können Poren für die Mustererstellung genutzt werden. Für ein auf Poren basierendes Verfahren ist eine Auflösung von ca. 800 dpi notwendig ([Roddy99] S.18). Da ein Fingerabdruck etwa 25 Minutiae enthält, aber ein Vielfaches davon an Poren, genügt es, einen kleineren Bereich des Fingerabdrucks zur Musterbildung heranzuziehen. Erkennung über Poren ist genauer, als über Minutiae. Dadurch sinkt die FAR, allerdings steigt auch die FRR an.

2.3.4 Bewertung

Die Vorteile der Fingerabdruckerkennung liegen in

- der langen Erfahrung auf diesem Gebiet,
- der potentiell sehr kleinen Scannergröße und
- der weiten Verbreitung des Merkmals, denn theoretisch besitzt jeder Mensch, der Finger hat, auch Fingerabdrücke.

Nachteile liegen in

- einem möglicherweise gestörten Hygieneempfinden der Benutzer, denn nicht jeder empfindet es als angenehm, seinen Finger auf einen Sensor zu legen, den schon viele andere Benutzer angefaßt haben. Dieses Problem tritt bei allen nicht-berührungslosen Verfahren auf.
- möglichen Akzeptanzproblemen wegen der Assoziation von Fingerabdrücken mit einer Verbrecherkartei.

Um hohen Sicherheitsansprüchen gerecht zu werden, sollte das Verfahren eine sichere Lebenderkennung enthalten.

2.4 Handgeometrie

Bei den Handgeometriescannern gibt es zwei Hersteller, die in dieser Arbeit betrachtet werden. Der eine ist BioMet (www.biomet.ch) mit einem System, das die Geometrie von Zeige- und Mittelfinger einer Hand vermißt, der andere ist Recogsys (www.recogsys.com) mit einem System, das die Geometrie von vier Fingern einer Hand vermißt.

2.4.1 Verfahrensbeschreibung

Handgeometrieverfahren nutzen optische Systeme, um wichtige geometrische Merkmale der Topographie der Hand abzubilden.

Das Verfahren ist nicht Berührungslos. Zur Authentisierung werden die Finger einer Hand in einen Sensor gelegt. Der Sensor liest die Merkmale ein und vergleicht sie mit einem angegebenen Referenzmuster. Das Muster befindet sich auf einer Chipkarte oder im Speicher des Scanners beziehungsweise eines externen Servers.

Feinheiten der Fingeroberfläche, wie Fingerabdrücke, Linien, Narben, Schmutz oder auch die Fingernägel werden vom Scanner nicht beachtet. Nach einer positiven Verifizierung der Identität, wird eine Handlung ausgeführt, wie zum Beispiel das Öffnen einer Tür oder die Weitergabe der Daten zwecks Zeiterfassung [Zunkel99].

Die Handgeometrie ist ein statisches Merkmal. Deshalb ist hier, wie auch beim Fingerabdruckverfahren eine Lebenderkennung notwendig, damit das System vor Nachbildungen einer realen Hand geschützt ist.

Die Größe eines Datensatzes liegt bei 9 beziehungsweise 20 Bytes und ist damit der kleinste aller betrachteter Verfahren. Die benötigte Zeit für eine Verifikation beträgt unter einer Sekunde. Die gesamte Dauer der Verifikation eines Benutzers, von der Ankunft am Gerät bis zu dessen Verlassen dauert im Mittel etwa 5 Sekunden ([Sandia91] S.20).

Die Equal Error Rate (EER) liegt nach Angaben der Hersteller bei 0,1%. Der Wert ist das Resultat eines Feldtests, der in [Sandia91] beschrieben wird.

Die Scanner arbeiten entweder mit einer Tastatur und internem oder externem Speicher, oder mit einer Chipkarte, auf der das Muster gespeichert ist.

Es ist notwendig, daß die Finger im Sensor gespreizt werden, da sonst die einzelnen Finger nicht korrekt vom Scanner erkannt werden könnten und somit die Authentisierung fehlschlägt [Sandia98]. Durch geeignete Maßnahmen kann die Fingerspreizung erreicht werden, ohne die kein Authentisierungsversuch gestartet wird. So ist zum Beispiel bei dem Scanner von Biomet eine breite Säule in der Mitte des Scanners, der Zeige- und Mittelfinger voneinander trennt. Bei dem Scanner von Recogsys muß jeder der vier Fingerspitzen eine kleine Säule berühren, die, entsprechend angeordnet, die Spreizung erreichen. Bedingt durch die Größe der Hände und der zum Einsatz kommenden Scannertechnik, sind die Geräte, in denen sich der Scanner befindet, relativ groß.

Authentisierung über Handgeometrie findet, bedingt durch die Größe des Geräts, hauptsächlich bei der Zugangskontrolle zu Räumen oder Gebäuden Anwendung. Das Gerät von Recogsys wird zum Beispiel bei etwa 50% der Kernkraftwerke in den USA oder zur Beschleunigung der Formalitäten bei der Einreise in die USA für Personen, die mindestens dreimal pro Jahr einreisen, eingesetzt.

2.4.2 Sensorprinzipien

Um die Handgeometrie auszulesen, wird eine optische Kamera verwendet. Die Firma Recogsys verwendet in ihrem System zum Beispiel eine 32000-Pixel CCD Digitalkamera, um über 90 Messungen an der Hand vorzunehmen. Die dreidimensionale Form der Hand wird aus Umrißbildern aufgenommen, die in den Scanner projiziert wurden.

2.4.3 Merkmalscharakteristika

Die Fingerlänge, -breite und -höhe wird vermessen ebenso wie Erhebungen der Handfläche.

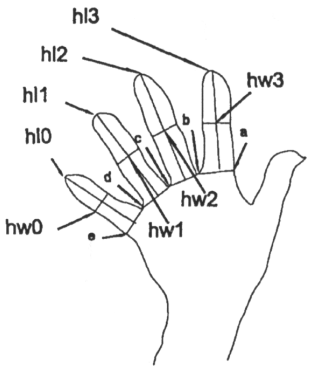


Abbildung 7: Merkmale der Handgeometrie (Quelle: [Sandia91] S.25)

Ein mögliches Verfahren ermittelt die Fingerspitzen und die Täler (a-e, von rechts) zwischen den Fingern. Die Länge der Finger hl0-3 ist die Strecke zwischen der jeweiligen Fingerspitze und dem entsprechenden Mittelpunkt der Strecken ab, bc, cd und de. Die Breite der Finger ist die kürzeste Verbindung quer über den Finger genau auf der halben Länge. Weiterhin kann das Dreieck mit den Kanten bc, cd und bd als Merkmal verwendet werden.

2.4.4 Bewertung

Die Vorteile der Handgeometrieerkennung liegen in

- einer hohen Benutzerakzeptanz [Sandia91],
- der kleinen Datensatzgröße,
- der schnellen Verifizierung,
- der Robustheit in bezug auf Verschmutzung der Finger und
- der weiten Verbreitung des Merkmals.

Nachteile liegen in

- einem möglicherweise gestörten Hygieneempfinden der Benutzer

Um hohen Sicherheitsansprüchen gerecht zu werden, sollte das Verfahren eine sichere Lebenderkennung enthalten.

2.5 Augen: Iris

2.5.1 Verfahrensbeschreibung

Iriserkennungsverfahren nutzen optische Systeme, um die Besonderheiten der Iris abzubilden. Die Iris ist die Regenbogenhaut des Auges (siehe Abbildung 9). Sie kann sich ausdehnen oder zusammenziehen und kontrolliert so die Größe der Pupille. Die Anzahl der Pigmente in der Iris bestimmt ihre Färbung, von blau bis hin zu schwarz [Encyclopaedia99].

Mit einer Kamera wird das Gesicht des Benutzers gesucht und die Exakte Position der Augen bestimmt. Das Muster der Iris wird erfaßt und in ein Binärmuster umgewandelt. Die Erkennung findet, je nach Sensortyp, aus einer Entfernung von 10-50 cm statt.

Das Verfahren ist Berührungslos und somit ist die Erkennung auch von der Umgebung des Sensors abhängig. Bei der Iriserkennung ist die Helligkeit der Umgebung wichtig, da diese Einfluß auf die Größe der Pupille hat. Außerdem muß es hell genug sein, damit der Sensor die Merkmale eindeutig erkennen kann.

Die benötigte Zeit für eine Verifikation beträgt in Abhängigkeit zur Größe der Datenbank etwa 2 Sekunden.

Die Iris ist ein statisches Merkmal. Eine Lebenderkennung ist notwendig, um das System vor Nachbildungen, wie zum Beispiel ein Glasauge oder das Foto eines Benutzers, zu schützen.

Es gibt theoretisch 10^{78} verschiedene Irismuster. Um diese eindeutig in einem Datensatz abbilden zu können, müßte jeder Datensatz mindestens 2^{260}, also 260 Bit ≈ 33 Bytes groß sein. Die tatsächliche Größe eines Datensatzes beträgt etwa 512 Bytes. Bei einer Erdbevölkerung von $6*10^{9}$ kann die Iris als eindeutig angesehen werden.

Die Größe eines Irisscanners variiert je nach Anwendungsgebiet. Es gibt sie etwa handgroß für den Einsatz zum Beispiel am PC oder auch wandmontiert oder integriert in Geldautomaten.

Die Equal Error Rate ist nach Angaben der Hersteller < 10^{-2} % beziehungsweise < 10^{-4} %. Probleme könnten sich bei Personen ergeben, die farbige Kontaktlinsen oder eine getönte Brille tragen. Auch wechselnde Lichtverhältnisse könnten sich negativ auf die Erkennung auswirken.

2.5.2 Merkmalscharakteristika

Eine Kamera nimmt ein Bild des Auges in schwarzweiß auf. Über das Bild wird ein Gitter gelegt. Ein Algorithmus generiert aus den hellen und dunklen Bereichen der Iris innerhalb des Gitters einen „menschlichen Barcode“, der eindeutig ist. Dieser Barcode ist das Muster, das dann mit dem Referenzmuster verglichen werden kann (siehe Abbildung 8).

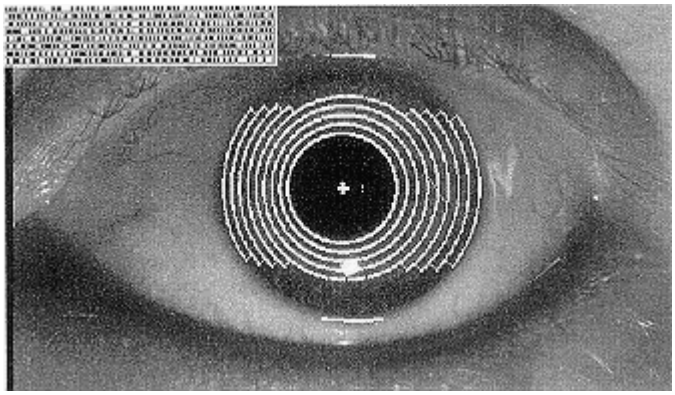


Abbildung 8: Erzeugung eines Iriscodes
(Quelle: www.iriscan.com)

2.5.3 Bewertung

Die Vorteile der Iriserkennung liegen in

- der hohen Erkennungsgenauigkeit,
- der berührungsfreien Benutzung und
- der weiten Verbreitung des Merkmals.

Ein Nachteil liegt darin, daß bei blinden Menschen diese Form der biometrischen Authentisierung nicht funktioniert.

Um hohen Sicherheitsansprüchen gerecht zu werden, sollte das Verfahren eine sichere Lebenderkennung enthalten.

2.6 Augen: Retina

2.6.1 Verfahrensbeschreibung

Die Retina ist eine komplexe Nervengewebeschicht, die sich über die hinteren zwei Drittel des Augapfels erstreckt (siehe Abbildung 9). Von hier werden empfangene Lichtimpulse an den Sehnerv weitergeleitet und von dort direkt weiter in das Gehirn [Encyclopaedia99].

Die natürlichen reflektierenden und absorbierenden Eigenschaften der Retina werden dazu genutzt, um ein Muster zu bilden. Der Benutzer blickt in ein schwach erleuchtetes Ziel. Der Scanner erfaßt und analysiert Informationen in Form von von der Retina reflektiertem Licht und speichert diese in einem 96 Byte großen Datensatz [EyeDentify99]. Die benötigte Zeit für eine Verifikation beträgt etwa 1,5 Sekunden.

Das Verfahren ist nicht berührungslos. Das zu erfassende Auge muß an einen Scanner gelegt werden. Kontaktlinsen beeinträchtigen die Erkennung nicht, nur muß eine eventuell vorhandene Brille vor der Erfassung abgenommen werden.

Die FRR wird mit 0,1% angegeben, die FAR mit 10^{-4} %, beides in Abhängigkeit zum definierten Toleranzwert (siehe 2.2.1). Variationen sind durch Erschöpfung oder Temperatur möglich.

Die Retina ist ein statisches Merkmal. Eine Lebenderkennung ist nicht extra notwendig, da eine Nachbildung der Retina nicht oder nur unter extremen Aufwand vorstellbar ist.

2.6.2 Merkmalscharakteristika

Der Scanner ist eine Kamera, die Reflexionen aufnimmt. Im Beispiel des Retinascanners von "EyeDentify" blickt der Benutzer auf einen farbigen Ring, der sich grün füllt, wenn die Erfassung beginnt. Aus den aus der Reflexion erhaltenen Daten werden 400 Referenzpunkte gebildet, von denen nach einer Analyse noch 192 übrig bleiben, die dann in ein spezifisches Datenformat übertragen- und gespeichert werden.

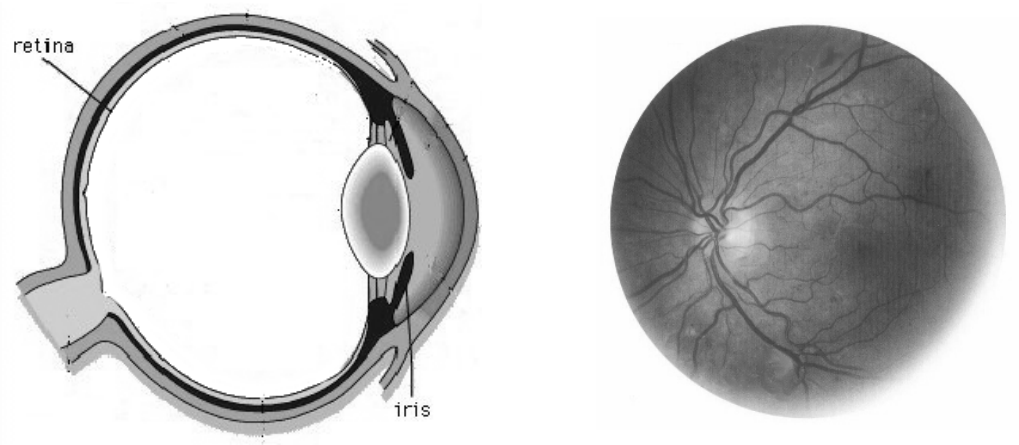


Abbildung 9: Das Auge mit Lage von Iris und Retina und das Bild einer Retina (Quelle: [Encyclopaedia99] und [EyeDentify99])

2.6.3 Bewertung

Vorteile der Retinaerkennung liegen in

- der Fälschungssicherheit,
- keinen Fehlerraten bei exakter Fokussierung [Sandia91] und
- in der kleinen Datensatzgröße.

Nachteile liegen in

- einer potentiell niedrigen Benutzerakzeptanz [Sandia91], durch das Eindringen in einen als intim betrachteten Bereich und gesundheitlicher Bedenken gegen den Kontakt der Augenpartie mit einem Fremdkörper (dem Scanner) und der Ausleuchtung der Retina mit einem Laser und
- einem vergleichsweise hohen Preis [Spence99].

2.7 Sprache

2.7.1 Verfahrensbeschreibung

Spracherkennungsverfahren vergleichen textabhängige oder textunabhängige Sprachproben basierend auf personencharakteristischen Sprachmerkmalen.

Die Sprachverarbeitung geschieht nicht im Sinne von der Erkennung der gesprochenen Worte, sondern es wird aus den aufgezeichneten Frequenzen ein Muster gebildet, das zwecks Authentisierung mit dem Referenzmuster verglichen wird.

Das Verfahren ist berührungslos. Die benötigte Zeit für den gesamten Vorgang einer Verifikation betrug in [Sandia91] fast 20 Sekunden. Diese Zahl relativiert sich aber durch die von 1991 bis heute stark gestiegene Rechenleistung aktueller Prozessoren.

Die Datensatzgröße liegt zwischen 1000 und 8000 Bytes. Die EER liegt nach Angaben eines Herstellers bei 1,7%, bei dem in [Sandia91] getesteten System bei etwa 5%.

Als Scanner kommt ein Mikrophon zum Einsatz, das, je nach Ausführung, sehr klein sein kann.

Die Sprache ist ein dynamisches Merkmal. Die Sprachfrequenzen variieren von mal zu mal, die Charakteristik der Sprache bleibt jedoch gleich. Eine Lebenderkennung ist dennoch notwendig, um sich vor Wiedereinspielung einer mit Tonband aufgezeichneten Authentisierung zu schützen. Dies gilt auch für den Fall, daß verschiedene Wörter oder Zahlen in variabler Reihenfolge gesagt werden müssen, da, sobald jedes Wort nach einer Anzahl von Authentisierungen mindestens einmal von einem Benutzer gesagt wurde, alle Informationen für einen Angriff vorhanden wären.

Dieses Verfahren kann überall dort angewendet werden, wo ein Mikrophon angeschlossen werden kann. Auch für telefonische Transaktionen, wie zum Beispiel das Ordern von Aktien oder der telefonische Einkauf mit Kreditkarte bietet sich die Spracherkennung an, weil so die Identität des Benutzers sicherer überprüft werden kann, als dies mit einem Paßwort möglich ist.

Verschiedene Faktoren können die Authentisierung erschweren oder verhindern ([Hübener97] S. 11ff). Diese sind

- Variabilität durch Sprecherunabhängige Faktoren, wie zum Beispiel Husten, Heiserkeit, emotionale Verfassung, Trunkenheit
- artikulationsabhängige Faktoren, also ob Wörter zusammengezogen oder einzeln gesprochen werden
- umgebungsabhängige Faktoren, wie zum Beispiel verschiedene Räumlichkeiten, Hintergrundgeräusche, Reflexionen oder die unbewußte Anpassung an die jeweilige akustische Umgebung.

2.7.2 Merkmalscharakteristika

Von jedem gesprochenen Wort wird sowohl die Lautstärke, als auch das Frequenzspektrum (siehe Abbildung 10) analysiert und daraus ein Frequenz-Lautstärke-Profil für den Benutzer erstellt. Aus jedem Wort werden 14 Merkmale extrahiert, die den Merkmalsvektor des Wortes bilden. Eine Abfrage von drei Ziffern ergibt somit einen Vektor aus 42 Merkmalen.

Abbildung 10: Frequenzspektrum des Satzes "Spracherkennung - die Stimme ist das Passwort"

2.7.3 Bewertung

Vorteile der Spracherkennung liegen in

- der Möglichkeit der Authentisierung via Telefon und
- bei vorhandener Hardwareplattform den niedrigen zusätzlichen Hardwarekosten für ein Mikrophon.

Nachteile liegen in

- der relativ langsamen Verifikation und der damit verbundenen geringen Benutzerakzeptanz mit Ausnahme von Telefonanwendungen, wo kein anderes Verfahren möglich ist und
- der relativ hohen Fehlerrate.

2.8 Gesichtserkennung: Visuell

2.8.1 Verfahrensbeschreibung

Bei der visuellen Gesichtserkennung nimmt eine Kamera ein Bild des Gesichts auf und analysiert es anhand verschiedener Kriterien.

Dieses statische Verfahren ist berührungslos. Eine Lebenderkennung ist notwendig, um das System vor Nachbildungen, wie zum Beispiel einem Foto, zu schützen. Auch gegen äußere

Veränderungen des Gesichts wie ein Bart oder eine Sonnenbrille muß das System unempfindlich sein.

Die Scannergröße ist variabel und reicht, je nach Einsatzgebiet, von der Größe einer Webcam für den Rechnerzugang bis hin zu über einen Meter hohen, schmalen Säulen, in die die Kamera in einem schräg nach oben zeigenden Winkel montiert ist für den Zugang zu Räumen oder Gebäuden.

Die EER liegt bei etwa 0,5%. Bei der Erkennung ist auf eine ausreichende Beleuchtung zu achten. Für eine Verifikation wird etwa eine Sekunde benötigt.

Die Größe eines Datensatzes beträgt etwa 2-4 Kilobytes, wobei ein eventuell zu Audit-Zwecken gespeichertes Originalbild 16 Kilobytes belegt.

2.8.2 Merkmalscharakteristika

Es gibt verschiedene Möglichkeiten, wie aus dem Bild eines Gesichts ein Merkmalssatz erstellt werden kann. So können verschiedene markante Punkte, wie zum Beispiel Haaransatz, Augenbrauen, Augen, Nase, Mund und Kinn verwendet werden. Diese Punkte werden über Vektoren miteinander verbunden und das resultierende Muster wird gespeichert und für den Vergleich verwendet.

Eine weitere Methode legt eine Art Gitter über das Gesicht (siehe Abbildung 11). Die dreidimensionalen Eigenschaften des Gesichts werden in das Gitter übertragen, das dann zur Erzeugung eines Merkmalssatzes verwendet wird.

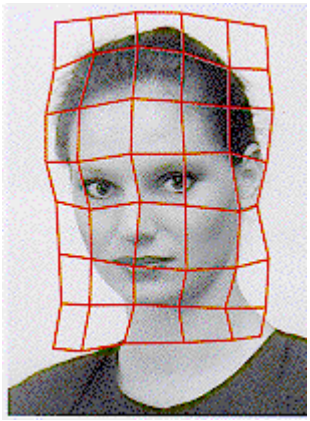


Abbildung 11: Bildung eines Merkmalssatzes mit Hilfe eines Gitters (Quelle: [www.zn-gmbh.com])

2.8.3 Bewertung

Vorteile der visuellen Gesichtserkennung liegen in

- einer potentiell hohe Benutzerakzeptanz, da das System berührungslos, unaufdringlich und einfach bedienbar ist
- niedrige Anschaffungskosten für Hardware für den Zugang zu einem Computer.

Ein Nachteil der visuellen Gesichtserkennung liegt in der Anfälligkeit gegen zu geringe Beleuchtung.

2.9 Gesichtserkennung: Thermisch

2.9.1 Verfahrensbeschreibung

Bei der thermischen Gesichtserkennung zeichnet eine Infrarot-Kamera ein Bild des Gesichts auf. Bedingt durch den Verlauf der Blutgefäße im Gesicht und deren unterschiedliche Nähe zur Hautoberfläche ergibt sich ein Temperaturmuster mit einer benutzerspezifischen Rotfärbung. Ein Algorithmus erstellt aus dem Muster ein Gesichtsthermogramm und digitalisiert, speichert und vergleicht es mit dem Referenzmuster [Betac99]. Die Wärmeemissionen von Ohren und Nase werden nicht berücksichtigt, da diese relativ stark auf Änderungen der Umgebungstemperatur reagieren.

Das Verfahren ist, wie auch die visuelle Gesichtserkennung, berührungslos. Die Größe eines Datensatzes beträgt 2-4 Kilobytes. Das Verfahren ist statisch. Eine Lebenderkennung ist durch die Verwendung einer Infrarot-Kamera nicht erforderlich, da Fälschungen nahezu ausgeschlossen sind.

2.9.2 Bewertung

Vorteile der thermischen Gesichtserkennung liegen in

- der Unabhängigkeit von der Beleuchtung und
- der Fälschungssicherheit bezüglich Verkleidung oder plastischer Chirurgie.

Ein Nachteil ist der relativ hohe Preis für die Hardware.

2.10 Motorik: Unterschrift

2.10.1 Verfahrensbeschreibung

Beim biometrischen Unterschriftsverfahren wird die Unterschrift eines Benutzers in geeigneter Weise aufgezeichnet, um daraus ein Muster zu erstellen. Der reine zweidimensionale Vergleich zweier Unterschriften auf Papier ist nicht sicher. Daher werden bei diesem Verfahren weitere Kriterien hinzugezogen.

Das Verfahren ist dynamisch und nicht berührungslos. Die benötigte Zeit für die Verifikation beträgt etwa eine Sekunde. Die Fehlerraten sind nicht vom Hersteller genannt worden. Zumindest die false rejection rate (FRR) ist benutzerspezifisch, denn ein immer annähernd identisch unterschreibender Benutzer wird auch nicht fälschlicherweise zurückgewiesen werden.

Die Unterschrift einzelner Benutzer kann sich im Laufe der Zeit ändern. Das Verfahren ist deshalb adaptiv (siehe 2.1.1), um die möglichen Änderungen berücksichtigen zu können.

Probleme bei der Authentisierung können auftreten, wenn ein Benutzer zum Beispiel durch kaltes Wetter klamme Finger hat und dadurch die Unterschrift von seinem Muster deutlich abweichen kann.

Die Größe eines Datensatzes beträgt 1-2 Kilobytes.

Dieses Verfahren bietet sich als Ersatz für herkömmliche Unterschriftsprüfung an. So könnten auf diese Weise zum Beispiel in der Bank Transaktionen autorisiert werden.

2.10.2 Sensorprinzipien

Um eine Unterschrift auszulesen, können zwei verschiedene Arten von Sensoren zum Einsatz kommen. Es gibt

- einen speziellen Stift oder
- eine spezielle Unterlage.

In beiden Sensortypen sind einzelne Sensoren implementiert, die die Bewegung des Stifts bei der Unterschrift auslesen und digitalisieren. Im ersten Fall befinden sich diese Sensoren im Stift selbst, im zweiten Fall in der Unterlage, auf der mit einem beliebigen Stift unterschrieben werden kann.

2.10.3 Merkmalscharakteristika

Die bei einer Unterschrift werden vier verschiedene Merkmale aufgezeichnet:

- Die Bewegung des Stiftes in X-Richtung
- Die Bewegung des Stiftes in Y-Richtung
- Der Druck, den der Stift auf die Unterlage ausübt
- Die Zeit, die in Abbildung 12 die Größe der X-Achse bestimmt.

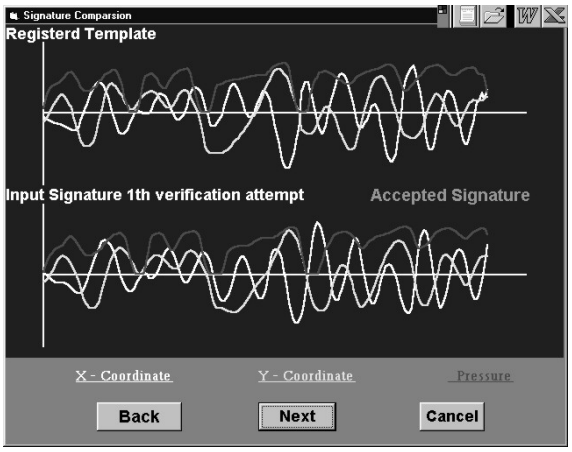


Abbildung 12: Zwei digitale Unterschriften im Vergleich (Quelle: [www.cybersign.com])

Die daraus resultierenden Kurven werden ausgewertet und zur Erstellung eines Merkmalsvektors verwendet.

2.10.4 Bewertung

Vorteile der biometrischen Unterschriftserkennung liegen in

- der allgemeinen Akzeptanz der Unterschrift als Mittel zur Authentisierung.

Nachteile liegen in

- einer potentiell hohen FRR.

2.11 Motorik: Tastenanschlag

2.11.1 Verfahrensbeschreibung

Das Tastenanschlagsverfahren benutzt eine gewöhnliche Computertastatur, um den benutzerspezifischen Tipprhythmus zu ermitteln und daraus ein Muster zu errechnen [BioPassword99].

Das Verfahren ist dynamisch und nicht berührungslos. Die benötigte Zeit für die Verifikation (und nur die ist mit diesem Verfahren möglich) ist praktisch nicht länger, als der Paßwortvergleich, der in anderen geschützten Systemen zur Authentisierung benötigt wird. Die Fehlerraten sind nicht vom Hersteller genannt worden. Zumindest die false rejection rate (FRR) ist benutzerspezifisch, denn ein immer annähernd identisch tippender Benutzer wird auch nicht fälschlicherweise zurückgewiesen werden.

Das Tippverhalten einzelner Benutzer kann sich im Laufe der Zeit ändern, zum Beispiel durch häufigeres Schreiben an der Tastatur, wodurch das Auffinden verschiedener Tasten schneller vonstatten gehen kann. Das Verfahren ist deshalb adaptiv (siehe 2.1.1), um die möglichen Änderungen berücksichtigen zu können.

Das Anwendungsgebiet dieses Verfahrens ist der Zugang zu Computersystemen, indem die normale Paßwortabfrage durch die biometrische ersetzt wird.

2.11.2 Merkmalscharakteristika

Beim Login in ein System wird die Tastatur 1000 mal pro Sekunde abgefragt. Die Identifikation basiert auf der Zeit, die ein Benutzer braucht, Tasten in verschiedenen Bereichen der Tastatur zu drücken. Das benutzerspezifische Muster bildet sich aus zwei Hauptparametern [BioPassword99]. Diese sind

- die "Haltezeit", die eine Taste gedrückt ist und
- die "Flugzeit", die benötigt wird, um die nächste Taste zu drücken.

Der daraus resultierende Tipprhythmus bildet den Merkmalsvektor des Benutzers.

2.11.3 Bewertung

Vorteile des Tastenanschlagsverfahrens liegen

- darin, daß keine zusätzliche Hardware benötigt wird, als bei einem Computer bereits vorhanden ist und
- in der geringen Umgewöhnung an das System.

Nachteile liegen in

- einer potentiell hohen FRR.

2.12 Hybridverfahren

2.12.1 Verfahrensbeschreibung

Hybridverfahren kombinieren mehrere biometrische Authentisierungsverfahren, um so eine höhere Sicherheit zu erreichen. Grundsätzlich sind die Kombinationen beliebig, jedoch wird die Benutzerakzeptanz niedrig sein, wenn die Verfahren einfach seriell hintereinander gehängt sind und sich somit jeder Benutzer mehrfach nacheinander authentisieren müßte.

Sinnvolle Verfahrenskombinationen wären zum Beispiel

- Iris- und Gesichtserkennung,
- Handgeometrie mit integriertem Fingerabdruckscanner,
- Gesichts- und Stimmerkennung.

Bei dem System von BioID [www.bioid.com] werden Gesicht, Stimme und die Lippenbewegung während des Sprechens als biometrische Merkmale miteinander kombiniert.

Als Sensor hierfür werden eine Kamera und ein Mikrophon benötigt. Die drei einzelnen, aus den Mustern erzeugten Merkmalsvektoren werden in einem Datensatz gespeichert, der größer als 10 Kilobytes ist.

Das Verfahren vereint dynamische und statische Merkmale und ist berührungslos. Zu schützen ist das System gegen die Wiedereinspielung einer auf Video aufgezeichneten Authentisierung als einzige Fälschungsmöglichkeit, da die Lippenbewegung nicht anders zu imitieren wäre.

Die Authentisierung erfolgt über eine 2 aus 3 Entscheidung, daß heißt mindestens zwei der drei Merkmalsvektoren müssen innerhalb der Toleranz mit den Referenzvektoren übereinstimmen.

2.12.2 Bewertung

Vorteile des Hybridverfahrens von BioID liegen in

- der hohen Fälschungssicherheit und
- der Unanfälligkeit des Systems gegen temporäre Veränderungen eines der Merkmale.

Ein Nachteil ist, daß sich die Probleme, die es in den einzelnen Verfahren gibt, in der Kombination der Verfahren summieren. Insbesondere die Kamera, die Gesicht und Lippen aufnimmt, muß gegen Reflexionen zum Beispiel von Brillengläsern und Änderungen in der Beleuchtung weitgehend resistent sein.

2.13 Sonstige Verfahren

Es gibt noch weitere Verfahren, die in dieser Arbeit zwar keine Berücksichtigung finden, da sie sich zum Teil noch in einem experimentellen Stadium befinden, aber hier genannt werden sollen. Diese sind

- Venenerkennung – hier wird der Verlauf der Venen im Handrücken analysiert,
- Ohrerkennung – untersucht die Form und den Knorpelverlauf des menschlichen Ohres[1],
- Geruchserkennung – identifiziert Menschen an ihrem individuellen Geruch,
- DNA-Analyse – hier werden Teile der menschlichen DNA zur Identifizierung verwendet. Die Erkennungsgesschwindigkeit liegt hier eher im Bereich von Stunden als von Sekunden und ist somit zu Zwecken der Authentisierung nicht geeignet.

[1] In Hamburg konnten 1999 zwei Einbrechern eine Reihe von Taten nachgewiesen werden, da diese beim Lauschen an den Haustüren einen Abdruck ihres Ohres hinterließen.

3 Chipkarten-Grundlagen

3.1 Geschichte der Chipkarten

Anfang der 50er Jahre wurden in den USA erste Vollplastik-Karten aus PVC produziert. Sie hatten gegenüber anderen Materialien den Vorteil der Robustheit und Langlebigkeit, wodurch sie besser für den täglichen Gebrauch geeignet waren.

Von Diners-Club, später auch von VISA und Mastercard, wurden Karten für den überregionalen Zahlungsverkehr ausgegeben. Diese Kreditkarten, bei denen man „mit seinem guten Namen“ bezahlte, fanden zunächst in den USA und später auch in Europa rasche Verbreitung. Die Vorteile lagen unter anderem in der Sicherheit gegenüber Bargeld und dem entfallenden Geldumtausch im Ausland.

Die benutzerspezifischen Merkmale, wie Name und Kartennummer, wurden durch Hochprägung auf die Karte gebracht, allgemeine Informationen, zum Beispiel der Name des Kartenausgebers, wurden aufgedruckt. Als weitere Merkmale für Sicherheit gegen Manipulation und Betrug dienten Unterschriftsfeld, Sicherheitsdruck und Hologramm.

Als erste Erweiterung der Funktionalität der Karten wurde ein Magnetstreifen aufgebracht, auf den Benutzerdaten, aber auch weitere Informationen, wie Benutzungsbeschränkungen oder Fehlbedienungszähler, maschinenlesbar gespeichert werden konnten. Dadurch wurde die Bearbeitungszeit verkürzt und weitere Anwendungen ermöglicht, so die Benutzung von Geldausgabeautomaten. Die Sicherheit hingegen wurde nur unwesentlich erhöht, da die gespeicherten Daten von jedem mit einem Schreib- / Lesegerät ausgelesen und manipuliert werden können. Magnetkarten sind einfach duplizierbar und anfällig gegen starke magnetische Felder. Die Speicherung geheimer Daten ist aus diesen Gründen nicht sinnvoll.

Das Patent für eine Karte mit darauf untergebrachtem integrierten Schaltkreis zur Aufnahme von Daten, also eine Chipkarte, stammt in Deutschland aus dem Jahr 1968 von J. Dethloff und H. Gröttrup. In den 70er Jahren ermöglichten Fortschritte in der Mikroelektronik, integrierte Schaltungen zu vertretbaren Preisen zu liefern und somit Chipkarten zu entwickeln. Den Durchbruch schafften die Chipkarten nicht bei den Bankkarten, sondern auf einem neuen Gebiet - den Telefonkarten, wodurch keine Rücksicht auf ein bestehendes System genommen werden mußte und die technischen Möglichkeiten voll ausgeschöpft werden konnten. 1984 wurden in Frankreich und ca. drei Jahre später auch in Deutschland Chipkarten als Telefonkarten eingeführt, von denen heute mehr als hundert Millionen im Umlauf sind. Ebenfalls sehr weit verbreitet ist in Deutschland die Krankenversichertenkarte mit Chip, die jeder gesetzlich Versicherte besitzt.

In der Herstellung sind Magnetkarten deutlich günstiger als Chipkarten. Deshalb und auch durch die zur Zeit bestehenden, auf Magnetkarten basierenden Systeme werden Magnetkarten auf unbestimmte Zeit erhalten bleiben.

Die Vorteile von Chipkarten gegenüber Magnetkarten liegen neben der Sicherheit in

- der deutlich größeren Speicherkapazität von zum Teil über 20 kByte gegenüber 226 Zeichen (nach ISO 7811) auf dem Magnetstreifen
- der Flexibilität dadurch, daß die Programmierung bestehender Chipkarten auch nachträglich angepaßt und erweitert werden kann

- der Multifunktionalität, d.h. eine Karte kann für mehrere unterschiedliche Funktionen genutzt werden.

Anwendungsbeispiele und bestehende Systeme werden im Kapitel 3.5 behandelt.

3.2 Arten von Chipkarten

Bei dem Begriff „Chipkarte“ wird in dieser Arbeit von kontaktbehafteten ausgegangen. Kontaktlose Chipkarten sind immer auch als solche betitelt und werden im Kapitel 3.2.3 behandelt.

Für Chipkarten gibt es drei in den ISO-Normen festgelegte Formate: ID-1, ID-00 und ID-000. ID steht dabei für Identifikationskarte. Die Norm für das häufigste Format ID-1 stammt aus ISO 7810 von 1985 und ist das Format, in dem z.B. auch EC- und Kreditkarten vorliegen. Die Übereinstimmung im Format hat den Vorteil, daß neue Karten bestehender Systeme mit einem Chip ausgerüstet werden können (siehe 3.5.3). Die drei Formate, die elektrische Belegung und Numerierung der Kontaktfelder einer Chipkarte, sowie mögliche Anordnungen von Chip, Magnetstreifen und Hochprägefeld sind in ISO 7816-2 beschrieben.

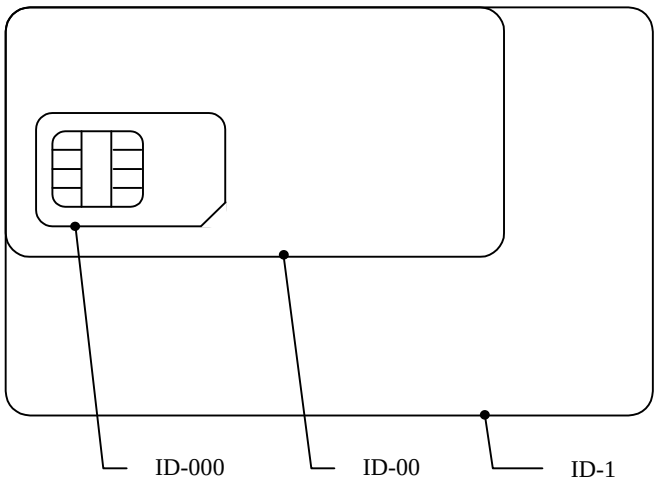


Abbildung 13: Die Kartenformate ID-1, ID-00, ID-000
(Quelle: [RANKL96] S. 40)

Es ist möglich, die Formate ID-00, auch „Mini-Karte“-, und ID-000, auch „Einschubkarte“ genannt, aus dem größeren Format ID-1 auszustanzen. Dies bietet Vorteile in der Produktion und zum Teil auch in der Handhabung. Einschubkarten finden unter anderem Verwendung in Mobiltelefonen.

Die acht Kontakte eines Chips sind folgendermaßen belegt (siehe Abbildung 14):

Der Kontakt C1 (Vcc) ist für die Versorgungsspannung des Chips, die bei heutigen Karten 5 Volt ±10% beträgt. Neuere Standardisierungsbestrebungen sehen zusätzlich Karten mit einer Versorgungsspannung von 3V vor (siehe 3.5). Der Spannungsbereich dieser Karten reicht dann von 2,7V bis 5,5V (3-5V ±10%). Reine 3V Chips hätten den Nachteil, daß sie nur in speziellen Terminals verwendet werden könnten, da ein normales Terminal mit der Vcc von 5V den Chip zerstören würde.

Der Kontakt C2 (RST) löst, auf high gesetzt, einen Reset auf der Karte aus. Der Inhalt des RAM wird gelöscht und der integrierte Adreßzähler zurückgesetzt.

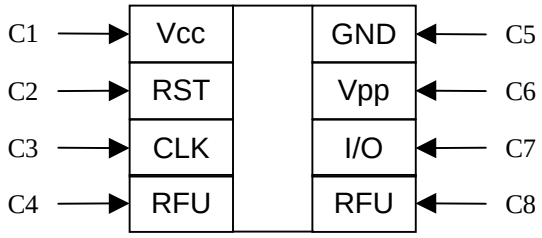


Abbildung 14: Die Belegung der Kontaktfelder einer Chipkarte nach ISO 7816-2

Der Kontakt C3 (CLK) versorgt den Chip mit einem Taktsignal.

Die Kontakte C4 und C8 (RFU) sind „reserved for future use“. Zur Zeit gibt es noch keine Standardisierung für sie, somit dürfen sie auf ISO-konformen Karten nicht verwendet werden. Einige Hersteller von Chipkarten, zum Beispiel Oldenbourg, verzichten aus Kostengründen vollständig auf diese beiden Kontakte.

Der Kontakt C5 (GND) ist Ground, das Bezugspotential des Chips, per Definition 0V.

Der Kontakt C6 (Vpp) ist für die Programmierspannung und wird nur bei alten Chips noch gebraucht. Um einen EEPROM zu programmieren, werden Spannungen von 12,5V – 25V benötigt. Auf neuen Karten wird diese Spannung mittels einer Ladungspumpe generiert. Dabei werden Kondensatoren in Parallelschaltung aufgeladen und in Reihenschaltung wieder entladen, wodurch sich ihre Spannungen auf benötigtes Niveau addieren. Durch schnelles Umschalten von Parallel- und Reihenschaltung wird so eine pulsierende Gleichspannung erzeugt, die durch einen weiteren Kondensator geglättet wird. Für andere Zwecke kann der Kontakt nicht genutzt werden, ohne von der ISO-Norm abzuweichen.

Der Kontakt C7 (I/O) schließlich ist die bidirektionale Datenleitung zum Austausch von Nutzinformationen mit der Chipkarte im Halbduplex-Verfahren. Ein 20kΩ Widerstand verhindert, daß durch gleichzeitiges Senden von Terminal und Chipkarte die resultierenden Spannungsschwankungen auf der I/O-Leitung die Schnittstellenbausteine zerstören.

Bei der Übertragung und Speicherung von Daten können Fehler auftreten. Um diese zu erkennen und ggf. zu korrigieren, gibt es verschiedene Möglichkeiten:

Man kann ein Paritätsbit an ein Datenbyte anhängen, um so 1-Bit-Fehler zu erkennen. Die Nachteile liegen darin, daß die normale Speicherstruktur byteweise organisiert ist und es dadurch schwierig ist, zusätzliche Paritätsbits einzubringen. Bei der Datenübertragung stellt dies zwar kein Problem dar, aber der Overhead ist mit 12,5% recht groß.

Diesen Overhead kann man deutlich reduzieren, indem über einen Datenblock einer beliebigen Anzahl von Bytes eine Prüfsumme gebildet wird. Bei der XOR-Prüfsumme werden alle Datenbytes mit XOR verknüpft und das Ergebnisbyte im Anschluß an den Block gesendet / gespeichert. Dieses Verfahren ist sehr schnell, da die logische XOR-Operation direkt als Maschinenbefehl im Prozessor vorhanden ist und der Algorithmus in Assemblercode nur

etwa 20 Byte Speicherplatz benötigt. Allerdings werden auch hier keine Mehrbitfehler erkannt.

Anders bei der CRC-Prüfsumme. CRC steht für „cyclic redundancy check“. Hier werden die Datenbits eines Blocks über einem Polynom ausgewertet. Mit diesem Verfahren werden auch Mehrbitfehler und Bytevertauschungen erkannt, allerdings ist die Berechnung etwa um Faktor 200 langsamer als beim XOR. Gemeinsam ist den Verfahren, daß eine Fehlerkorrektur nicht möglich ist. Für eine genauere Beschreibung der Verfahren siehe ([Rankl96] S. 82ff).

Eine Fehlerkorrektur kann mittels Mehrfachablage der Daten erreicht werden, entweder 3fach mit einer 2 aus 3 Entscheidung oder doppelt mit doppelter Prüfsumme. Ob die hohen Kosten und der Aufwand gerechtfertigt sind, ist im Einzelfall zu prüfen.

3.2.1 Speicherkarten

Als Speicherkarten oder auch synchrone Karten werden Chipkarten ohne Mikroprozessor bezeichnet. Der Aufbau solcher Karten ist in Abbildung 15 zu sehen. Der Logikbaustein ist dabei optional und auf der Telefonkarte vorhanden, auf der Krankenversichertenkarte hingegen nicht (siehe 3.5).

Im ROM (read only memory) stehen Identifizierungsdaten, wie zum Beispiel die

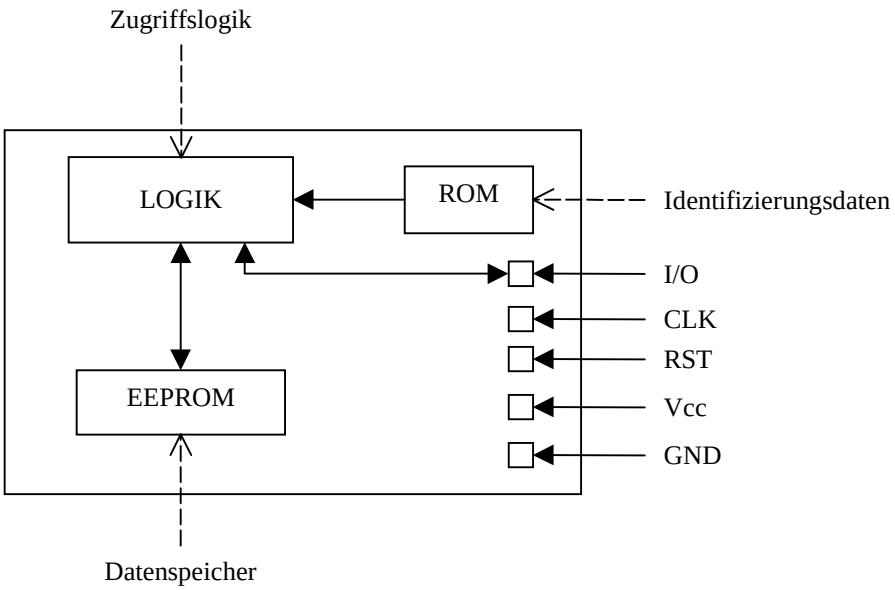


Abbildung 15: Schematischer Aufbau von Speicherkarten (Quelle: [RANKL96] S. 32)

Kartennummer. Der beschreibbare Speicher wird meistens durch ein EEPROM realisiert. Bei einigen Telefonkarten (nicht in Deutschland) wird statt dessen ein EPROM verwendet. Um ein EEPROM zu beschreiben, ist die Programmierspannung Vpp notwendig, die entweder über den Kontakt C6 zugeführt wird oder intern über die Ladungspumpe aus der Versorgungsspannung Vcc generiert wird. Das genaue Verfahren der Programmierung eines EEPROM ist zum Beispiel in ([Rankl96] S.71ff) beschrieben.

Der Logikteil des Chips umfaßt die Funktionen Adreßzähler-, Reset-, Programmier- und ggf. Sicherheitslogik. Die Programmierlogik erzeugt die für die Änderung des Speicherinhalts notwendige Programmierspannung Vpp und über die Sicherheitslogik lassen sich Speicherbereiche vom freien Zugriff ausnehmen, die dann nur unter bestimmten Voraussetzungen gelesen oder geändert werden können.

Die Datenübertragung läuft nach folgendem Verfahren ab, das in ISO 7816-3 beschrieben ist:

Nachdem GND Kontakt mit dem Terminal hat, wird die Versorgungsspannung Vcc und ggf. die Programmierspannung Vpp angelegt und anschließend RST auf high gesetzt. Der integrierte Adreßzähler wird dadurch zurückgesetzt. Der Chip bekommt über CLK seinen ersten Taktimpuls, bevor RST wieder auf low gesetzt wird. Daraufhin sendet die Karte über I/O ihr erstes Bit, nach jedem Taktimpuls dann ein weiteres. Die Datenübertragung läuft also synchron ab, deshalb spricht man auch von synchronen Karten.

Die ersten 16 bzw. 32 Bit sind die „Answer-to-reset"-Daten, kurz ATR. Sie dienen zur Klassifizierung der Karte. Die eigentlichen Datenbits erhält man, indem nach dem Erhalt der ATR weitergetaktet wird. Wenn der Adreßzähler den gültigen Bereich überschreitet, wird er von der Adreßzähler-Logik automatisch auf 0 zurückgesetzt.

Synchrone Karten sind zwar unflexibel, weil sie meist für eine bestimmte Anwendung optimiert sind, sind aber in der Produktion besonders kostengünstig und haben sich dadurch bei Anwendungen mit hohen Stückzahlen durchgesetzt, wie zum Beispiel bei Telefonkarten oder der Krankenversichertenkarte (siehe 3.5).

3.2.2 Mikroprozessorkarten

Im Kern bestehen Mikroprozessorkarten, auch asynchrone Karten genannt, aus CPU, ROM, EEPROM und RAM (siehe Abbildung 16). Die CPU – die „central processing unit" – ist der Prozessor der Karte. In ihr finden mit Hilfe der Befehle des Betriebssystems, das größtenteils im ROM gespeichert ist, Berechnungen unterschiedlicher Art statt. Im EEPROM kann dazu Programmcode gespeichert sein, der von der CPU ausgeführt wird. Eine genaue Darstellung der einzelnen Speicherarten ist in [Volpe96] zu finden.

Das RAM (random access memory) ist der Arbeitsspeicher der CPU, der von der Versorgungsspannung Vcc abhängig ist, d.h. wenn Vcc nicht anliegt, geht der Inhalt des RAM verloren.

Bei asynchronen Karten handelt es sich um einen kompletten Mikrocontroller, der alle Aktivitäten steuert, initiiert und überwacht. Der Datentransfer geschieht hier asynchron und mit einer Vielzahl von Befehlen im Gegensatz zu den synchronen Karten mit einem übertragenen Bit nach jedem Taktimpuls. Jedes Datenbyte wird verpackt in ein Startbit am Anfang, sowie ein Paritätsbit und zwei Stopbits am Ende. Die ATR wird innerhalb der ersten oder zweiten 40000 Taktzyklen von der Karte generiert, je nach Typ des Chips. Zwei typische Taktfrequenzen sind 3,579 MHz und 4,9152 MHz.

Der Platzbedarf eines Bauteils ist bei der Produktion von Chipkarten ein wichtiger Kostenfaktor. So ist RAM etwa 4x größer als EEPROM und etwa 16x größer als ROM. Allerdings ist die Zeit, in der eine Speicherzelle des RAM beschrieben werden kann mit <70ns um Faktor 10^5-10^6 kleiner als bei einem EEPROM. Gerade bei aufwendigen Berechnungen, wie sie

zum Beispiel bei der Kryptographie anfallen, kann aus Geschwindigkeitsgründen nicht auf RAM verzichtet werden. Als Beispiel für die Proportionen verwendeten Speichers wird bei dem SLE44C80 Chip von Siemens 16kByte ROM, 8kByte EEPROM und nur 256 Byte RAM verwendet ([Schütt96] S.76).

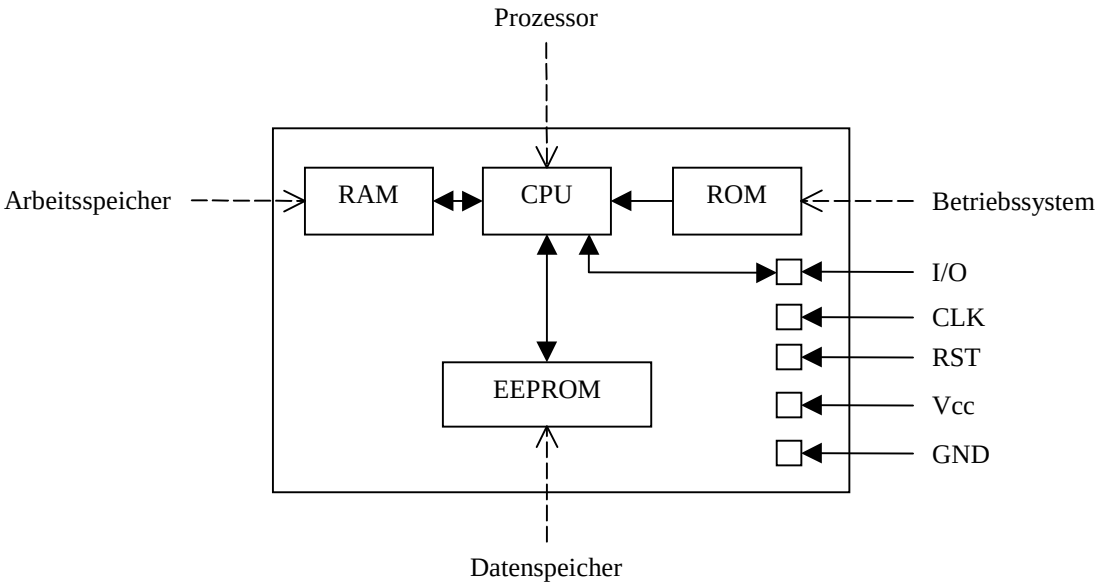


Abbildung 16: Schmatischer Aufbau von Mikroprozessorkarten (Quelle: [RANKL96] S. 32)

In den nächsten Jahren könnte Flash-EEPROM normalen EEPROM ersetzen, da durch ein anderes Verfahren die Schreibzeit pro Speicherzelle von ca. 3-10ms auf 10µs gesenkt werden konnte und Flash-EEPROM auch nur etwa halb so groß ist.

Einige Hersteller bieten als zusätzliche Hardware auf dem Chip zum Beispiel Coprozessoren oder Zufallszahlengeneratoren an, um Funktionen bereitzustellen, die von Software nicht, oder nur unzureichend erfüllt werden können (siehe 3.4.2 / 3.4.4).

Die Vorteile von Mikroprozessorkarten gegenüber reinen Speicherkarten liegen in der Flexibilität, da die Karten nicht auf eine bestimmte Anwendung festgelegt sind, sondern durch die Programmierung angepaßt werden können. Es ist auch möglich, eine Karte für mehr als nur eine Anwendung zu programmieren und somit eine Multifunktionalität zu erreichen. Außerdem können Daten auf Mikroprozessorkarten sicher gespeichert werden (siehe 3.4). Die Produktionskosten liegen allerdings höher als bei Speicherkarten.

3.2.3 Kontaktlose Chipkarten

Der Standard für kontaktlose Chipkarten ist in ISO 10536 beschrieben. Durch folgende mögliche Anordnung der Elemente wird die Kompatibilität zu ISO 7816 gewährleistet:

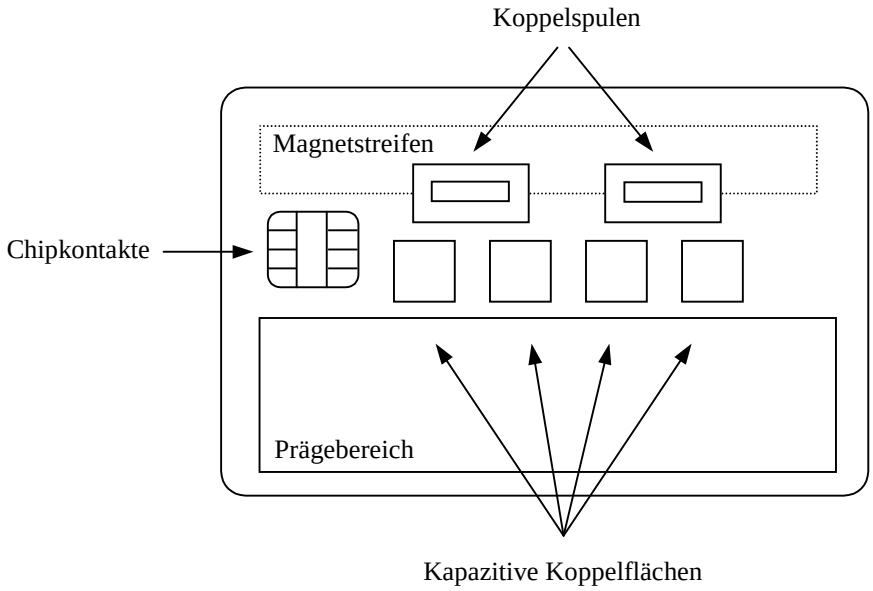


Abbildung 17: Flächenaufteilung der Funktionselemente kontaktloser Chipkarten (Quelle: [SCHÜTT96] S. 127)

Die kapazitiven Koppelflächen reichen zur Energieversorgung nicht aus, werden aber bei einigen Karten zur Datenübertragung verwendet. Die Koppelspulen der Chipkarte dienen der induktiven Übertragung. Sie ist das zur Zeit am weitesten verbreitete Verfahren, mit dem sich sowohl die Datenübertragung als auch die Stromversorgung realisieren läßt. Dabei wird an jede der beiden Koppelspulen eine frequenzgleiche Wechselspannung induziert.

Diese vom Terminal induzierten Wechselspannungen werden genutzt zur

- Erzeugung der Spannungen Vcc und Vpp
- Generierungung des Systemtaktes CLK
- Datenübertragung mittels Modulation der Phase, Amplitude oder Frequenz.

Bei der Amplitudenmodulation, sie wird für die Übertragung zum Terminal genutzt, wird von der Karte durch das Datensignal ein Spannungsabfall erzeugt, der im Terminal erkannt und ausgewertet werden kann ([Rankl96] S.44).

Für die Übertragung vom Terminal zur Karte wird Phasenmodulation eingesetzt. Dabei wird eine der beiden Wechselspannungen um 90^{o} in der Phase relativ zur anderen verschoben, was in der Karte in ein Datensignal umgewandelt wird ([Schütt96] S.128).

Kontaktlose Chipkarten werden von der Semantik her genauso angesprochen wie kontakt-behaftete mit dem Unterschied, daß die kontaktlose Übertragungsstrecke als physikalische

Transportschicht dient ([Schütt96] S.125). Das bedeutet, daß ein und dieselbe Anwendung problemlos auf beiden Kartentypen laufen kann.

Die Leistungsaufnahme des Chips bestimmt den maximalen Abstand zwischen Terminal und Karte, da sich die abgestrahlte Leistung des Terminals aufgrund von Postvorschriften nicht beliebig erhöhen läßt. Man spricht auch von Close - und Remote Coupling Cards ([Rankl96] S.45). Kontaktlose Speicherkarten benötigen im reinen Lesebetrieb ca. 10µW, im Schreibbetrieb hingegen ca. 100µW, weil u.a. die Programmierspannung Vpp erzeugt werden muß. Die Reichweite dieser Remote Coupling Cards liegt bei 1m bzw. 10cm. Mikroprozessorkarten haben mit ca. 100mW Leistungsaufnahme eine auf wenige Millimeter begrenzte Reichweite, d.h. diese Close Coupling Card muß dem Lesegerät aufgelegt oder eingeführt werden. Lage und Richtung der Karte haben dabei keine Auswirkungen auf die Funktion.

Kontaktlose Chipkarten haben eine Reihe von Vorteilen gegenüber den kontaktbehafteten:

- Verzichtet man auf Chipkontakte, Magnetstreifen und Hochprägung (siehe Abbildung 17), dann sind die Oberflächen der Karte frei gestaltbar.
- Es gibt keinen Verschleiß von Kontakten oder mechanischen Teilen im Terminal.
- Es sind keine Kartenschlitze am Terminal nötig, wodurch ein Angriffspunkt für Vandalismus entfällt.
- Die Lage der Karte zum Terminal ist nicht vorgeschrieben und somit frei wählbar.
- Die Abwicklungsgeschwindigkeit, zum Beispiel bei der Zugangskontrolle, kann sich deutlich erhöhen.

Diese Vorteile können die Ausfallsicherheit des Systems verbessern und die Akzeptanz beim Benutzer erhöhen.

Es gibt auch einige Nachteile kontaktloser Chipkarten:

- Sie sind teuer in der Produktion.
- Ihre Zuverlässigkeit ist noch nicht bewiesen.
- Es ist eine unbewußte Kontrolle und Profilbildung der Benutzer möglich.
- Die Abbuchung von Beträgen einer Karte mit Zahlungsfunktion könnte automatisch -, und somit auch ungewollt und unberechtigt erfolgen.

Auf die Sicherheit von Chipkarten wird in Kapitel 3.4 genauer eingegangen.

Kontaktlose Chipkarten können zum Beispiel zur Zugangskontrolle, als elektronischer Fahrschein im öffentlichen Nahverkehr oder auch als elektronische Geldbörse verwendet werden (siehe 3.5).

3.3 Betriebssysteme

3.3.1 Aufgabe von Betriebssystemen

Es ist Aufgabe eines Betriebssystems, dem Benutzer ein Äquivalent einer virtuellen Maschine zu präsentieren, die leichter zu programmieren ist, als die darunterliegende Hardware ([Tanenbaum95] S.6). Das Betriebssystem hat weiterhin die Aufgabe der Verwaltung aller Bestandteile eines komplexen Systems ([Tanenbaum95] S.7). Somit fungiert das

Betriebssystem als Schnittstelle zwischen dem Benutzer und der Hardware. Es macht durch Abstraktion einen komplizierten Vorgang, wie zum Beispiel das Beschreiben einer EEPROM-Zelle, durch einen einfachen Befehl zugänglich und stellt allen Anwendungen die vorhandene Hardware zur Verfügung.

Ein Chipkarten-Betriebssystem hat folgende Hauptaufgaben ([Rankl96] S.123):

- Datenübertragung von und zur Chipkarte
- Ablaufsteuerung der Kommandos
- Dateiverwaltung
- Verwaltung und Ausführung kryptographischer Algorithmen

Von seiner Aufgabenstellung her ist ein Chipkarten-Betriebssystem immer ein Sicherheitssystem, das Informationen vor allem geheimhalten muß. Es darf keine Möglichkeit geben, Daten am Betriebssystem vorbei unautorisiert auszulesen, denn dann kann keine Sicherheit mehr gewährleistet werden. Zum Beispiel werden erst nach erfolgreicher Authentisierung Speicherbereiche für lesenden oder auch schreibenden Zugriff freigegeben (siehe 3.4.2).

3.3.2 Besonderheiten von Chipkarten-Betriebssystemen

Bei der Personalisierung werden alle Daten, die einer einzelnen Person oder Karte zugeordnet sind, in die Karte ein- bzw. aufgebracht ([Rankl96] S.334). Zum Beispiel werden die Kartennummer und gegebenenfalls Erweiterungen für das Betriebssystem in einem speziellen Bereich des EEPROM gespeichert, der nur einmal geschrieben aber mehrfach ausgelesen werden kann.

Betriebssysteme wie Windows NT oder Linux benötigen mehrere Megabyte an Speicherplatz. Ein Chipkarten-Betriebssystem muß sich hingegen auf wenige kByte beschränken. Der Großteil des Programmcodes von Chipkarten-Betriebssystemen ist in ROM-Code geschrieben. Dadurch können nach der Produktion des Chips, spätestens aber nach der Personalisierung keine Änderungen mehr vorgenommen werden, im Gegensatz zu einigen Betriebssystemen auf PCs durch sogenannte „Service Releases“. Die Korrektur von Fehlern ist zeitaufwendig und kostenintensiv, da die komplette Hardware – die Chipkarte – ausgewechselt werden muß ([Rankl96] S.122).

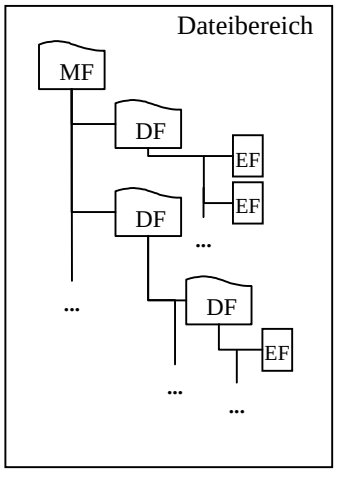


Abbildung 18: Dateibereich eines EEPROMS mit den verschiedenen Dateitypen in einer Chipkarte (Quelle: [Rankl96] S. 134)

Der Speicherplatz für Chipkarten-Betriebssysteme ist sehr begrenzt. Es kann nicht immer die gesamte Menge der genormten Befehle und Datenstrukturen implementiert werden. Aus diesem Grund gibt es Profile von Chipkarten. In einem Profil ist eine Untermenge der genormten Befehle und Datenstrukturen aufgeführt, die das Profil mindestens enthalten muß. Profile sind eine Empfehlung der ISO 7816-4 an die Betriebssystemdesigner.

Die Dateistruktur einer Chipkarte ist ähnlich der von DOS oder UNIX. Es gibt ein Master File (MF), ein oder mehrere Dedicated Files (DF) und Elementary Files (EF) (siehe Abbildung 18). MF entspricht der

Wurzel, DF den Verzeichnissen und EF den Dateien. Die Anzahl der DF und EF ist durch den geringen Platz begrenzt. Jeder Datei, die erzeugt wird, wird ein zusammenhängender Speicherbereich zugewiesen, der in Größe und physikalischem Speicherort nicht nachträglich änderbar ist. Dieser Speicherbereich besteht aus Dateispeicher und Freispeicher. In den Dateispeicher wird der Programmcode der Datei geschrieben. Der Freispeicher dient als Puffer für mögliche Änderungen der Größe einer Datei. Er kann bei MF und DF auch dazu genutzt werden, neue Dateien zu erzeugen.

Unter DOS und UNIX wird der Speicher als doppelt verkettete Liste verwaltet, eine Liste für den belegten -, eine für den freien Speicherplatz. Der Aufwand für die Dateiverwaltungsprogramme und der Overhead in den Dateideskriptoren wäre bei einem Chipkarten-Betriebssystem nicht gerechtfertigt ([Rankl96] S.132).

Ein Beispiel für ein Chipkarten-Betriebssystem ist STARCOS:

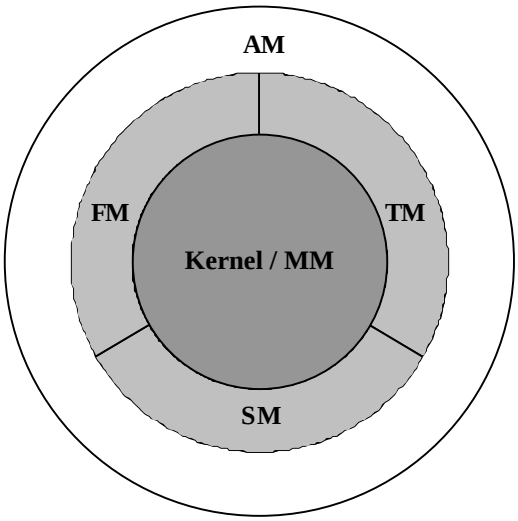


Abbildung 19 : Aufbau des Chipkarten-Betriebs systems STARCOS (Quelle: [Schütt96] S.73)

AM = Aplication Manager
FM = File Manager
MM = Memory Manager
SM = Security Manager
TM = Transmission Manager

Die Speicherverwaltung wird vom Memory Manager übernommen. Er sorgt unter anderem dafür, daß einzelne Anwendungen den ihnen zugeteilten Speicherbereich nicht verlassen können. Wenn eine Datei gelöscht wird, weist der Memory Manager den frei werdenden Speicherplatz dem Freispeicher der physikalisch benachbarten Datei zu, so daß ein größerer physikalisch zusammenhängender Freispeicher entsteht. Der Transmission Manager ist für die Datenübertragung und die ATR zuständig. Der File Manager verwaltet das Dateisystem und die verschiedenen Dateitypen. Der Security Manager übernimmt Verschlüsselung und Zugriffskontrolle. Dazu ist der DES-Algorithmus implementiert, der für Challenge-Response und zur verschlüsselten Datenübertragung eingesetzt wird (siehe 3.4.2 / 3.4.3). Der Application Manager schließlich dient als Schnittstelle zu den Anwendungen.

3.4 *Sicherheit von Chipkarten*

Es ist Aufgabe sowohl der Software wie auch der Hardware dafür zu sorgen, daß Vertraulichkeit und Integrität der Daten auf einer Chipkarte gewährleistet sind. Für die Kontrolle der Echtheit einer Karte ist oft auch der Mensch der Entscheidungsfaktor. Dieses Kapitel stellt verschiedene Methoden vor, die die Sicherheit von Chipkarten gewährleisten sollen.

3.4.1 Äußere Sicherheitsmerkmale

Bei der Produktion von Karten werden verschiedene Folien laminiert, aus denen der Kartenkörper ausgestanzt wird [Kuratorium97]. Vor dem eigentlichen Laminieren werden in die Folien passende Löcher gestanzt, in die der Chipkörper eingesetzt wird. Der Chip kann aus der fertigen Karte nicht mehr entfernt werden, ohne ihn zu zerstören. Diese Eigenschaft haben auch die beiden anderen Produktionsverfahren ([Schütt96] S. 58).

Die Sicherheit einer Chipkarte wird durch mehrere Faktoren bestimmt. Es gibt maschinenlesbare Merkmale, die zum Beispiel in Hardware oder Software implementiert sind. Damit eine Karte von Menschen auf Echtheit überprüft werden kann, müssen optische Merkmale auf der Karte vorhanden sein. Sie sollen verhindern, daß eine Karte hergestellt werden kann, die das gleiche Aussehen und die gleiche Funktionalität einer bereits existierenden Karte aufweist. Die optischen Merkmale stützen sich darauf, daß sie nur mit hohem technischen Aufwand und nur mit einem bestimmten Verfahren hergestellt werden können und somit nicht kopierbar sind. Ein Manipulationsversuch kann die Zerstörung des Merkmals bewirken.

Beispiele für solche Merkmale sind:

- Unterschriftsstreifen: Hier wird vom *Eigentümer* der Karte eine Unterschriftsprobe hinterlegt. Diese kann mit der Unterschrift verglichen werden, die der *Besitzer* bei der Benutzung der Karte geben muß, wie zum Beispiel bei der Ausstellung eines Euroschecks.
- UV-Bedruckung: Karten können mit einer UV-aktiven Farbmischung versehen werden, die nur unter einer UV-Lampe wieder sichtbar wird [Kuratorium97].
- Guillochen: Dies sind nicht reproduzierbare, kunstvoll verschlungene Linienstrukturen, die zum Beispiel auch auf Geldscheinen vorhanden sind.
- Hologramm: Ein Bild mit „3D-Eindruck“, dessen Echtheit durch Veränderung des Blickwinkels festgestellt werden kann. Das Hologramm wird mit Laserstrahlen auf eine aluminiumbedampfte Folie aufgetragen, die dann untrennbar mit der Karte verbunden wird. Es ist auch möglich, ein holographisches Overlay in die Karte einzubinden, bei dem das Hologramm in einer Schicht der Karte selbst erzeugt wird [Kuratorium97].
- Mikroschrift: Diese Schrift stellt sich für das Auge als feine Linie dar, kann aber zum Beispiel durch eine Lupe erkennbar werden.

Um die Sicherheit zu erhöhen, können die optischen Merkmale miteinander kombiniert werden.

3.4.2 Authentisierung

Um zu verhindern, daß unautorisiert geheime Daten einer Karte oder eines Terminals ausgelesen werden können oder eine sonstige Funktionalität unerlaubt genutzt wird, gibt es das Verfahren der Authentisierung (siehe [Rankl96] Kapitel 8.1-8.5). Es wird zur Feststellung von Identität und Authentizität des Benutzers, der Karte und des Terminals verwendet. Um dies zu erreichen, wird zwischen Karte und Terminal ein Geheimnis abgefragt, das beide Seiten kennen. Das Terminal könnte zum Beispiel eine in der Karte gespeicherte PIN (personal identification number) abfragen und mit der gespeicherten Nummer in einer internen Datenbank vergleichen. Der entscheidende Nachteil bei dieser Art der Identifikation ist, daß die

Datenübertragung im Klartext erfolgt. Ein potentieller Angreifer kann die Kommunikation abhören, das Geheimnis in Erfahrung bringen und sich genauso wie die echte Karte dem System gegenüber authentisieren.

Die Lösung dieses Problems liegt im Challenge-Response-Verfahren. Am Anfang jeder Sitzung stellt das System dem Benutzer eine Frage (Challenge) und entscheidet anhand der Antwort (Response) über die Authentizität. Die Frage kann zum Beispiel eine Zufallszahl sein, die als Eingabe für eine kryptographische Funktion dient. Der dabei verwendete Schlüssel ist das gemeinsame Geheimnis.

Die Authentisierung erfolgt

- einseitig oder gegenseitig
- symmetrisch oder asymmetrisch
- statisch oder dynamisch.

Bei einseitiger Authentisierung beweist nur die Karte ihre Identität gegenüber dem Terminal. Bei der gegenseitigen geschieht dies auch umgekehrt. Dadurch kann nicht durch ein unautorisiertes Terminal auf interne Karteninformationen zugegriffen werden.

Symmetrische oder asymmetrische Authentisierung bezieht sich auf das verwendete kryptographische Verfahren (siehe 3.4.3 / 3.4.4), mit dem die Response - und bei gegenseitiger Authentisierung auch die Challenge verschlüsselt wird. Im Bereich der Chipkarten werden hauptsächlich symmetrische Kryptoalgorithmen verwendet.

Bei der statischen Authentisierung werden vor Ausgabe der Karte verschiedene kartenindividuelle, unveränderbare Informationen mit einem Verfahren verschlüsselt und auf der Karte gespeichert. Das Terminal liest die kartenindividuellen Informationen aus und verschlüsselt sie mit demselben Verfahren (und demselben Schlüssel). Das Ergebnis ist die zu erwartende

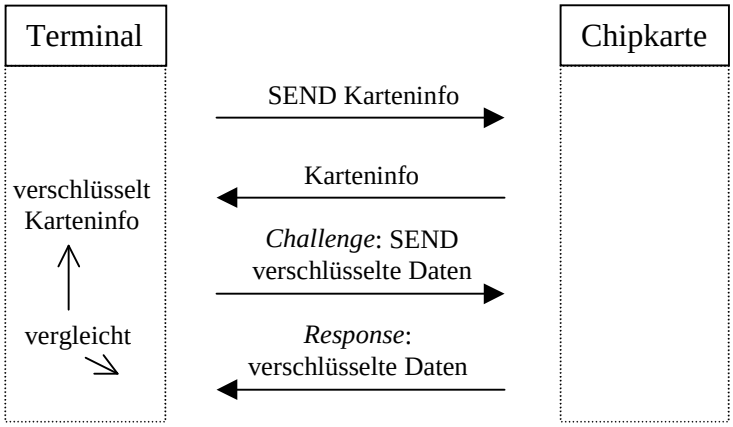


Abbildung 20: Ablauf einer statischen Authentisierung

Response der Karte. Die Challenge besteht aus der Aufforderung an die Karte, die gespeicherten verschlüsselten Daten zu senden. Das Ergebnis der Berechnung wird mit der Response verglichen und somit die Authentizität ermittelt (siehe Abbildung 20).

Das Problem von statischer Authentisierung ist, daß Challenge und Response immer gleich sind. Das Verfahren bietet keinen Schutz gegen Wiedereinspielung einer zuvor abgehörten Authentisierung. Der Vorteil liegt in den geringeren Produktionskosten der Chipkarte, die nicht in der Lage sein muß, verschlüsseln zu können. Dadurch ist aber nur einseitige Authentisierung möglich.

Eine sicherere Methode ist daher die gegenseitige symmetrische oder asymmetrische dynamische Authentisierung.

Eine Sitzung bezeichnet den Zeitraum zwischen Verbindungsaufbau und Verbindungsende von Terminal und Chipkarte. Bei der dynamischen Authentisierung gibt es bei jeder Sitzung andere Challenge-Response-Daten, wodurch ein Angriff über Wiedereinspielung unmöglich ist. Dies wird erreicht über die Verwendung von Zufallszahlen.

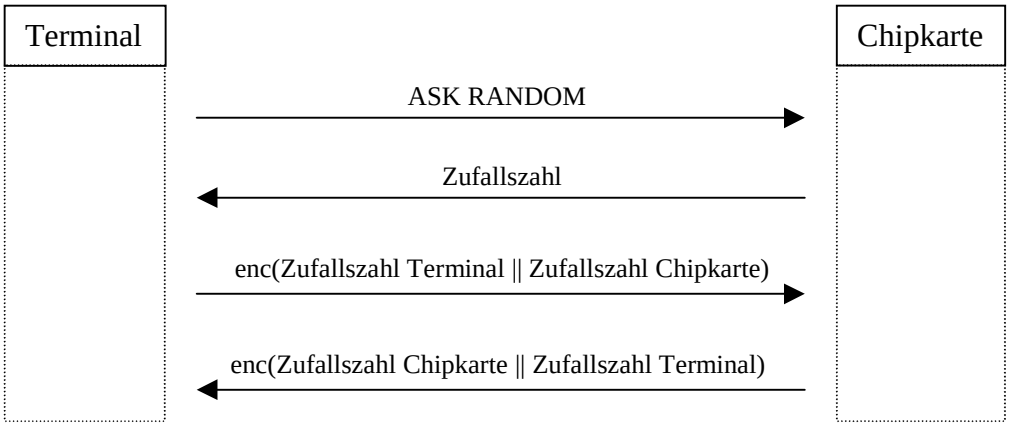


Abbildung 21: Gegenseitige Authentisierung mit einem symmetrischen Kryptoalgorithmus (Quelle: [Rankl96] S. 272)

Zufallszahlen sind von einem Zufallszahlengenerator, von äußeren Einflüssen unabhängig erzeugte Zahlen, die nicht vorhersagbar oder beeinflußbar sind. Natürliche Zufallszahlen sind Produkt realer physikalischer Prozesse wie zum Beispiel der Zerfall radioaktiver Substanzen. Sie sind sehr schwer zu erzeugen und nach dem Stand der Technik bei Chipkarten fast unmöglich. Es werden mit Hilfe von Software sogenannte „Pseudozufallszahlen“ erzeugt. Pseudozufallszahlen sind das Ergebnis deterministischer Prozesse. Man kann mit Kenntnis des verwendeten Verfahrens und der Eingangswerte die Zahlen voraussagen. Zufallszahlengeneratoren sollen in praktisch endloser Folge voneinander unabhängige Zufallszahlen erzeugen, die zufällig und nicht stellenweise gehäuft in der Folge auftreten ([Page91] S.102ff). Die Karten einer Produktionsreihe müssen unterschiedliche Zufallszahlen erzeugen. Dazu wird bei der Produktion von Chipkarten in das EEPROM jeder Karte ein unterschiedlicher Startwert geschrieben. Bei jeder Sitzung muß eine andere Reihe von Zufallszahlen erzeugt werden. Gewährleistet wird dies durch die Speicherung eines neuen Startwertes nach jeder Erzeugung einer Zufallszahl. Implementieren kann man einen Zufallszahlengenerator zum Beispiel mit dem DES-Algorithmus oder durch Zusatzhardware.

Wenn die Echtheit von Terminal und Karte bestätigt ist, kann noch geprüft werden, ob der Benutzer der Karte autorisiert ist. Die herkömmliche Methode hierfür ist den Benutzer aufzufordern, eine PIN einzugeben. In der Entwicklung befinden sich auch biometrische

Verfahren, bei denen die Person selbst und nicht ein Geheimnis (die PIN) identifiziert wird (siehe Kapitel 2). Biometrische Verfahren können auf Grundlage von einzigartigen, individuellen und biologischen Merkmalen eine Person eindeutig identifizieren ([Rankl96] S.260). Biometrische Merkmale sind zum Beispiel Fingerabdruck, Iris und Netzhaut ([Rankl96] S.265f).

3.4.3 Symmetrische Kryptoalgorithmen

Verschlüsselungsverfahren, bei denen derselbe Schlüssel zur Ver- und Entschlüsselung dient, nennt man symmetrisch. Ein Klartext wird mit dem geheimen Schlüssel chiffriert und der resultierende Schlüsseltext dann übermittelt. Aus dem Schlüsseltext kann dann wieder mit demselben Schlüssel der Klartext gewonnen werden.

Es ist wichtig, daß die Sicherheit eines Verschlüsselungsverfahrens nicht auf der Geheimhaltung des Algorithmus, sondern alleine auf der Geheimhaltung des verwendeten Schlüssels beruht (Kerckhoff-Prinzip). Die Akzeptanz bei den Benutzern wird deutlich erhöht, wenn der Algorithmus offengelegt und seine Sicherheit hinreichend bewiesen wurde. Der am häufigsten genutzte symmetrische Kryptoalgorithmus ist der DEA (Data Encryption Algorithm), auch als DES (Data Encryption Standard) bekannt. Das Kerckhoff-Prinzip und auch zwei weitere Prinzipien für Kryptoalgorithmen, das der Konfusion und der Diffusion, werden vom DES erfüllt. Diffusion besagt, daß jedes Bit des Klartextes und des Schlüssels möglichst viele Bits des Schlüsseltextes beeinflussen soll. Der Klartext wird sozusagen im Schlüsseltext verstreut. Ist das Prinzip der Konfusion erfüllt, dann kann nicht vorhergesagt werden, welche Änderungen im Schlüsseltext von der Änderung eines einzigen Zeichens des Klartextes hervorgerufen werden. Eine detaillierte Beschreibung von DES findet sich zum Beispiel in ([Pfleeger97] S.100ff).

Ein DES-Schlüssel besteht aus 64 Bit. Die Daten werden in Blöcke zu je 8 Bytes zerlegt und dann mit DES verschlüsselt. Klartext und Schlüsseltext haben dieselbe Länge, abgesehen vom letzten Block, der gegebenenfalls auf 8 Bytes aufgefüllt wird. Es gibt DES-Bausteine, die die Verschlüsselung eines 8-Byte-Blocks innerhalb von 64 ns ermöglichen. Bei Chipkarten wird DES als Software implementiert. Eine der möglichen Softwarerealisierungen in Assemblercode benötigt 10-20 ms pro Block und 1920 Bytes Speicherplatz ([Volpe96] S.59).

Jedes achte Bit eines DES-Schlüssels dient als Paritätsbit. Die Sicherheit des Schlüssels beruht also auf 56 Bit. Daraus ergeben sich $2^{56} \approx 7{,}2*10^{16}$ verschiedene Möglichkeiten für die Wahl eines Schlüssels. Seit dem Jahr 1977, aus dem der DES stammt, ist die Rechenleistung so stark angewachsen, daß mit einem Brute-Force-Angriff, also einem Durchprobieren aller 2^{56} möglichen Schlüssel, innerhalb sehr kurzer Zeit ein Schlüssel gebrochen werden kann. Dazu muß lediglich ein Klartext-Schlüsseltext-Paar bekannt sein. Im Juli 1998 benötigte ein 250000 Dollar teurer Spezialcomputer drei Tage, um einen DES-Schlüssel zu knacken. Dabei wurden etwa $9{,}2*10^{10}$ Schlüssel pro Sekunde ausprobiert [c't16/98].

Jeder Teilnehmer eines Systems, hier die Chipkarte und das Terminal, verfügt über denselben Schlüssel. Daraus ergibt sich zum Beispiel das Problem, daß ein gebrochener, also durch einen Angriff bekannt gewordener Schlüssel das gesamte, auf ihm aufbauende System kompromittiert. Sowohl Daten, als auch die Kommunikation können ausgespäht und manipuliert werden. Auch die Authentizität eines Teilnehmers kann dann nicht mehr

gewährleistet werden. Bei Chipkarten kann die individuelle Kartennummer in die Berechnung des Schlüssels mit eingehen und somit ein kartenindividueller geheimer Schlüssel erzeugt werden. Das Terminal liest die Kartennummer aus und errechnet den Schlüssel, der für die Kommunikation mit dieser Karte verwendet werden muß.

Die Sicherheit eines Systems kann erhöht werden, wenn statt DES Triple-DES verwendet wird. Bei Triple-DES wird der Klartext zunächst mit Schlüssel 1 chiffriert, dann mit Schlüssel 2 dechiffriert und anschließend mit Schlüssel 1 wieder chiffriert. Dadurch wird der Schlüsselraum von 2^{56} auf 2^{112} vergrößert. Die Kompatibilität zu DES ist gegeben, wenn Schlüssel 1 und 2 identisch sind. Der einzige Nachteil von Triple-DES gegenüber DES ist der höhere Zeitaufwand für die Ver- und Entschlüsselung (und 8 Byte zusätzlicher Speicher für Schlüssel 2).

3.4.4 Asymmetrische Kryptoalgorithmen

Ein Problem symmetrischer Kryptoalgorithmen ist, daß mit Bekanntwerden des Schlüssels das auf ihm aufbauende System kompromittiert ist. Um dieses Problem zu vermeiden, werden bei asymmetrischen Kryptoalgorithmen zwei verschiedene Schlüssel zur Ver- und Entschlüsselung verwendet. Der eine Schlüssel ist privat, der andere ist öffentlich und wird nicht geheim gehalten. Der am meisten verwendete asymmetrische Kryptoalgorithmus ist RSA, benannt nach seinen Erfindern Rivest, Shamir und Adelman. Er eignet sich sowohl für Verschlüsselung, als auch für digitale Signaturen (siehe 3.4.5).

Der öffentliche Schlüssel wird aus e und n gebildet, der private Schlüssel aus d und n. Der Schlüsseltext S entsteht, indem der Klartext K mit e potenziert wird und das Ergebnis modulo n gerechnet wird ($S=K^e \bmod n$). Die Entschlüsselung erfolgt auf gleiche Weise mit dem privaten Schlüssel ($K=S^d \bmod n$). Daraus folgt, daß e und n öffentlich bekannt sein müssen und d geheim ist. d, e und n sind ganzen Zahlen und werden folgendermaßen gebildet ([Pfleeger97] S.93):

- Man wähle zwei Primzahlen p und q, die beide möglichst groß sein sollen (>100 Ziffern). Der öffentliche Modulo n ist das Produkt der Zahlen p und q ($n=p*q$). p und q dürfen nicht veröffentlicht werden, da sonst die Schlüsselerzeugung nachvollzogen werden kann.
- Die Zahl e wird so gewählt, daß sie kleiner ist als n und zu dem Produkt $(p-1)*(q-1)$ prim ist, das heißt, e hat keine gemeinsamen Primfaktoren mit $(p-1)*(q-1)$, anders ausgedrückt ist der größte gemeinsame Teiler der beiden Zahlen gleich eins ($ggt(e,(p-1)*(q-1))=1$). Wird e als Primzahl größer $(p-1)$ und $(q-1)$ gewählt, dann ist diese Eigenschaft auf jeden Fall erfüllt.
- Die Zahl d wird so gewählt, daß $e*d \bmod ((p-1)*(q-1))=1$.

Die zu verschlüsselnde Nachricht wird in Blöcke zerlegt, die kleiner als n sind und die dann verschlüsselt werden. Die Blöcke sollten mit Zufallswerten auf die Größe von n aufgefüllt werden ([Schneier96] S.539). Es ist nicht notwendig, die gesamte Exponentation K^e vor der Modulo-Berechnung auszuführen, da nach der Reduzierbarkeitsregel $a*b \bmod n = (a \bmod n) * (b \bmod n) \bmod n$ ist ([Pfleeger97] S.95). Somit werden die Zahlen in der Berechnung nie viel größer als n. Dies ist besonders bei Chipkarten wichtig, da diese nur wenig Speicherplatz haben.

Wie aus dem Erzeugungsprozeß ersehbar, ist die Schlüssellänge bei RSA variabel (anders als bei DES mit 64 Bit). Je größer *p* und *q* gewählt werden, desto größer werden die Schlüssel, desto höher wird die Sicherheit, desto größer wird der Zeitaufwand zur Ver- und Entschlüsselung. Gängige Schlüssellängen sind 512, 768, 1024 Bit, in einigen Bereichen auch 2048 Bit.

Hardwareimplementierungen von RSA sind, bezogen auf 512 Bit Schlüssellänge, etwa 1000 mal langsamer als DES, Sofwareimplementierungen von RSA sind etwa 100 mal langsamer als DES ([Schneier96] S.535). Die höhere Sicherheit von RSA gegenüber DES ist mit einem deutlich höheren Zeitaufwand verbunden. Dieser kann aber gerechtfertigt sein durch die Anforderungen einer Anwendung, für die Sicherheit von kritischer Bedeutung ist. Die Verschlüsselung mit dem öffentlichen Schlüssel kann beschleunigt werden, wenn *e* geschickt gewählt wird. Typische Werte von *e* sind 3, 17 und 65537 ($=2^{16}+1$). Jeder dieser Werte enthält in seiner Binärdarstellung nur zwei Einsen, wodurch sich die Potenzierung sehr schnell ausführen läßt.

Die Sicherheit von RSA basiert auf dem mathematischen Problem der Faktorisierung großer Zahlen. Der schnellste bekannte Algorithmus, der eine Zahl in seine Primfaktoren zerlegt, ist von exponentieller Zeitkomplexität, das heißt, der benötigte Zeitaufwand wächst exponentiell zur Größe der Zahl, die faktorisiert werden soll ([Pfleeger97] S.92). Es wird vermutet, daß die Wiederherstellung des Klartextes K aus dem öffentlichen Schlüssel und dem Schlüsseltext äquivalent zur Faktorisierung von *n* ist ([Schneier96] S.532).

3.4.5 Digitale Signaturen

Um die Authentizität einer Nachricht festzustellen, ist es meistens zu zeitaufwendig, die gesamte Nachricht zu verschlüsseln. Statt dessen wird sie signiert. Dazu wird eine Hash-Funktion verwendet, die von der Nachricht einen Hash-Wert erzeugt, der dann verschlüsselt

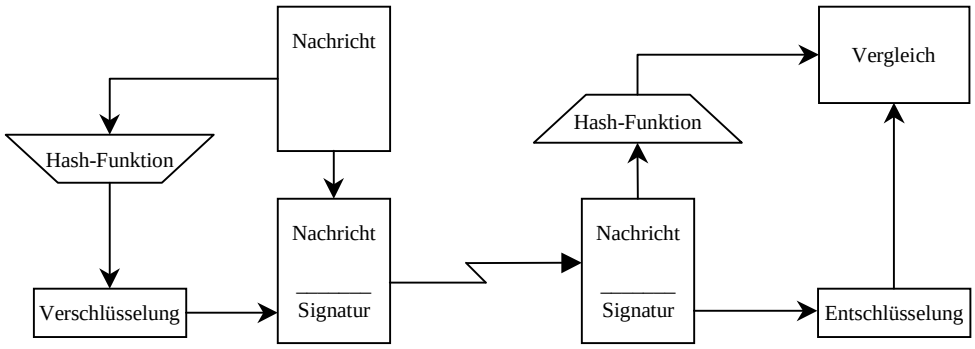


Abbildung 22: Erzeugung einer Signatur zur Authentitätsprüfung

wird. Der verschlüsselte Hash-Wert ist die Signatur der Nachricht und wird an die Nachricht angehängt. Zur Prüfung der Signatur wird von der Nachricht wieder der Hash-Wert gebildet und mit der entschlüsselten Signatur verglichen. Sind sie identisch, ist die Nachricht authentisch (siehe Abbildung 22). Wenn der Hash-Wert asymmetrisch verschlüsselt wird, zum Beispiel mit RSA, dann spricht man von einer digitalen Signatur, sonst von einer kryptographischen Prüfsumme oder einem Message Authentication Code (MAC).

Eine Hash-Funktion ist eine Einwegfunktion, die eine Nachricht (fast) beliebiger Länge auf eine feste Länge reduziert (oder erweitert bei sehr kleinen Nachrichten). Das Resultat ist der Hash-Wert der Nachricht. Diese Reduktion ist verlustbehaftet, das heißt, es ist nicht möglich, aus dem Hash-Wert die ursprüngliche Nachricht zu erzeugen. Da bei der Bildung eines Hash-Wertes viele Bits auf wenige abgebildet werden, ist es grundsätzlich möglich, daß zwei verschiedene Nachrichten denselben Hash-Wert besitzen. Deswegen ist Voraussetzung für eine gute Hash-Funktion, daß das Problem, zwei Nachrichten zu erzeugen, die denselben Hash-Wert haben, von exponentieller Komplexität ist. Je größer der Hash-Wert ist, desto geringer ist die Wahrscheinlichkeit, zwei Nachrichten mit identischem Hash-Wert zu finden. Zwei gängige Hash-Funktionen sind MD5 (Message Digest algorithm number 5) und SHA (Secure Hash Algorithm). MD5 erzeugt Hash-Werte von 128 Bit, SHA von 160 Bit. Die maximale Nachrichtenlänge beträgt beim SHA 2^{64} Bits ([Pfleeger97] S.98).

Für digitale Signaturen ist es wichtig, nur den Hash-Wert einer Nachricht und nicht die ganze Nachricht zu signieren, da sonst die digitale Unterschrift auf einem anderen Dokument gefälscht werden könnte ([Schneier96] S.538). Außerdem sollte bei RSA eine Nachricht immer erst unterschrieben werden, bevor sie mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wird ([Schneier96] S.540).

3.5 Anwendungen von Chipkarten

Zwei in Deutschland weit verbreitete Chipkarten werden im Folgenden vorgestellt. Dies sind die Telefonkarte und die Krankenversichertenkarte. Da Chipkarten im Zahlungsverkehr von wachsender Bedeutung sind, wird auch die Geldkarte behandelt.

3.5.1 Die Telefonkarte der Deutschen Telekom

Von Dezember 1986 bis Mai 1989 lief in 16 deutschen Großstädten ein erfolgreicher Feldversuch mit auf Speicherkarten basierenden Kartentelefonen. 1996 gab es über 50000 Kartentelefone und 150 Millionen verkaufte Guthabenkarten pro Jahr ([Rankl96] S.393).

Im Chip der Telefonkarte sind folgende Daten gespeichert ([Rankl96] S. 395f) :

- Die ersten 5 der 7 Ziffern der *Seriennummer*. Sie stehen in einem nicht änderbaren Bereich des EEPROM. Da die Nummer nicht vollständig gespeichert ist, lassen sich nur Gruppen von 100 Karten sperren (siehe unten).
- Das *Herstelldatum* des Chips, das nicht änderbar ist.
- Die *Herstellerkennung*, die ebenfalls nicht änderbar ist.
- Der *Anfangswert*, das ist der Wert in Pfennigen, mit dem die Karte ausgegeben wird.
- Das *Restguthaben*. Im EEPROM ist ein irreversibler Zähler implementiert, der in seinem Wert nur verkleinert (dekrementiert) werden kann. Er besteht aus 5 Byte je 8 Bit und gibt den Restwert der Karte in Pfennigen an. Jedes gesetzte Bit des ersten Bytes stellt einen Wert von 4096 Pfennigen dar, jedes Bit des zweiten Bytes 512 Pfennige, des dritten 64, des vierten 8 und des letzten Bytes 1 Pfennig. Das bedeutet, daß der maximale Wert einer Telefonkarte 374,48 DM betragen könnte.

Um die Gebühr für eine Einheit abzubuchen, wird der entsprechende Betrag durch Löschen der Bits vom Restguthaben abgezogen. Sind alle Bits eines Bytes gelöscht, dann wird ein Bit

eines höherwertigen Bytes gelöscht und alle Bits des niederwertigen Bytes gesetzt. Eine Sicherheitslogik auf der Karte verhindert, daß ein Bit gesetzt wird, bevor ein Bit eines höherwertigen Bytes gelöscht wurde [c't12/94].

Bei der Kartenproduktion wird der Restguthabenzähler auf den Anfangswert dekrementiert. Da der Wert in Pfennigen und nicht in Gesprächseinheiten implementiert ist, war die Gebührenänderung vom Januar 1997 problemlos durchführbar, ohne daß sich bei älteren Karten das Restguthaben veränderte. Die Kosten je Einheit wurden von 30 auf 20 Pfennige reduziert, dafür wurde die Länge einer Gesprächseinheit stark verkürzt.

Bei den aktuellen Telefonkarten werden nur die Kontakte C1-C3, C5 und C7 verwendet. C4 und C8 fehlen aus Kostengründen oftmals (siehe 3.2). Ein in seiner Funktion geheimes Hardwaremerkmal der Karte dient zum Schutz vor gefälschten Karten. In Zukunft sollen Speicherbausteine eingesetzt werden, die eine einseitige Authentisierung der Karte gegenüber dem Telefon ermöglichen.

Nur wenn sich der Eingabeschlitz des Telefons nach dem Einführen der Karte schließt, funktioniert das Telefon. So wird verhindert, daß die Kommunikation zwischen Karte und Telefon zum Beispiel durch eine gefälschte Karte mit Kabelverbindung nach außerhalb abgehört wird.

Beim Verbindungsaufbau zwischen Kartentelefon und entferntem Gesprächsteilnehmer schickt das Kartentelefon die Seriennummer der Chipkarte an die nächsthöhere Verbindungsinstanz, wo sie mit einer Sperrliste verglichen wird. Von dieser Instanz bekommt das Telefon auch den Gebührenimpuls, den es an die Karte weitergibt, wo dann der Restguthabenzähler dekrementiert wird.

3.5.2 Die Krankenversichertenkarte

Ende 1994 wurde in Deutschland die Krankenversichertenkarte (KVK) eingeführt. Sie ersetzt den Krankenschein, der für Mitglieder gesetzlicher Krankenkassen oder Ersatzkassen erforderlich war und dient gleichzeitig zur Identifikation des Patienten gegenüber dem Arzt ([Rankl96] S.400). Die KVK ist eine einfache Speicherkarte. Die Produktionskosten der Chipkarte und der Lesegeräte in den Arztpraxen konnten dadurch niedrig gehalten werden. Die Daten auf dem Chip der KVK verhalten sich nach außen hin wie ein einzelnes EF, auf das wahlfrei zugegriffen werden kann. Es ist kein Schutz vor dem unberechtigten Auslesen der Daten vorhanden. Einige zusätzliche Anwendungen, wie zum Beispiel ein Notfallpaß, sind daher ausgeschlossen, weil dazu vertrauliche Daten gespeichert werden müßten ([Schütt96] S.97) ([Rankl96] S.401).

Die Daten der KVK können von den normalen Kartenlesern nur gelesen werden. Die Software der Kartenleser verhindert, daß Daten auf der Karte auch geschrieben und somit manipuliert werden können. Nur die ausgebenden Krankenkassen selbst können natürlich die KVK auch beschreiben.

Die KVK beherrscht keine Art der Authentisierung. Ein gefälschtes Terminal kann nicht erkannt werden. Somit können auch mit einem geeigneten, nicht autorisierten Terminal die Daten der KVK verändert werden, um sich zum Beispiel Arztleistungen unerlaubt in Anspruch zu nehmen.

Auf der Krankenversichertenkarte ist vorhanden:

- Titel, Vorname, Familienname, Namenszusatz, Geburtsdatum, Status, Kartennummer, Nummer, und die genaue Adresse des Versicherten
- Name und Nummer der Krankenkasse
- Rechtskreis Ost / West und das Gültigkeitsdatum der Karte.

Abgesichert werden die Daten durch eine XOR-Prüfsumme (siehe 3.2).

Unveränderliche und personenbezogene Daten sind außen auf der Karte vermerkt, veränderliche wie zum Beispiel die Adresse des Versicherten, sind nur im Chip gespeichert.

3.5.3 Die Geldkarte

Die Chipkarte ist das zur Zeit einzige Kartenmedium, mit dem sich Daten relativ sicher speichern lassen. Diese Daten können auch Geld repräsentieren. Somit eignet sich die Chipkarte als elektronische Geldbörse, die in Deutschland als Geldkarte eingeführt wurde. Sie soll keine der vorhandenen Zahlungsmethoden, wie zum Beispiel EC- oder Kreditkarte ersetzen, sondern die Barzahlung ergänzen. Auf einer Geldkarte lassen sich maximal 400,- DM speichern. Sie ist eine Debitbörse, das heißt, das elektronische Guthaben der Karte ist mit realem Geld im Voraus bezahlt worden.

Die Vorteile der Geldkarte auf Benutzerseite liegen in dem beschleunigten Bezahlvorgang an Kassen oder Automaten und darin, daß das Problem des benötigten, aber nicht vorhandenen Kleingeldes entfällt.

Händler können ebenfalls von dem beschleunigten Bezahlvorgang profitieren. Elektronisches Geld läßt sich über Telekommunikation transferieren, so daß seine Verrechnug und der Eingang echten Geldes auf dem Bankkonto schneller und unkomplizierter erfolgen kann, als über herkömmliche Wege, wie zum Beispiel die Abgabe von „Geldbomben“ im Nachttresor einer Bank. Anders als bei EC- oder Kreditkarte fallen bei Bezahlung mit der Geldkarte keine Gebühren für jede einzelne Transaktion an. Die Bezahlung erfolgt offline und die gesammelten Einzeltransaktionen werden über eigens dafür eingerichtete Evidenzstellen mit dem Kartenausgeber verrechnet. Für die vom Kartenausgeber garantierte Verrechnung des elektronischen Geldes muß der Händler Gebühren in Höhe von 0,3% der Verrechnungssumme bezahlen.

Der Betreiber eines Geldkarten-Systems hat zwar die Kosten für die Chipkarten und die Ladestationen zu tragen, im Gegenzug bekommt er aber echtes Geld für elektronisches Geld. Unter der Annahme von 10 Millionen ausgegebenen Geldkarten mit einem durchschnittlichen Guthaben von 150 DM und einem Zinssatz von 5%, beträgt der jährliche Zinsgewinn 75 Millionen DM pro Jahr, der Zinsverlust der Benutzer dagegen bei erträglichen 7,50 DM ([Rankl96] S.352).

Die Nachteile für den Benutzer liegen darin, daß, solange nicht auch „der Bäcker von nebenan“ über ein Geldkarten-Terminal verfügt, immer auch Bargeld mitgeführt werden muß, wodurch eine höhere Kapitalbindung entsteht.

Nur wenn es möglich ist, die Vorteile der Geldkarte intensiv zu nutzen, wird sie von den Benutzern akzeptiert werden. Dies setzt voraus, daß es möglichst viele Händler gibt, bei denen mit der Geldkarte bezahlt werden kann, und daß auch möglichst viele Terminals existieren, an denen die Geldkarte aufgeladen werden kann. Das Risiko defekter Karten

sollte in erster Linie vom Betreiber getragen werden. Die Bezahlung mit Geldkarte sollte anonym sein, denn dies ist bei Barzahlung gegeben. Diese Anonymität ist bei kontogebundenen Geldkarten, deren Verbreitung dadurch gesteigert wird, daß neue EC-Karten für den Benutzer kostenlos mit einem Geldkarten-Chip ausgerüstet werden, nicht gegeben. Bei kontogebundenen Geldkarten wird der aufzuladende Betrag direkt vom zugehörigen Konto abgebucht, bei nicht-kontogebundenen Geldkarten wird er in Bar gezahlt.

Jede Geldkarte enthält eine Kartennummer. Für diese Kartennummer wird vom Betreiber eine Art Konto geführt, auf dem die Bezahlvorgänge mit den aufgeladenen Beträgen abgeglichen werden. Dadurch ist zwar ein gewisses Maß an Kontrolle möglich, diese dient aber zur Absicherung des Betreibers gegen Mißbrauch. Der Aufladevorgang ist schematisch in Abbildung 23 dargestellt.

In Schritt 4 schickt die Chipkarte neben ihren Kartendaten und dem aufzuladenden Betrag auch eine Signatur *S1* über verschiedene Daten an das Terminal. Das Sicherheitsmodul des Betreibers prüft die Signatur und schickt im positiven Fall die Auftragsfreigabe und eine Signatur *S2* zurück. Diese Signatur wird von der Chipkarte geprüft, womit die gegenseitige Authentisierung vollständig ist. Die mit *S3* signierte Aufladequittung bestätigt den korrekten Vorgang, der mit der Aufforderung an den Benutzer endet, die Karte zu entnehmen.

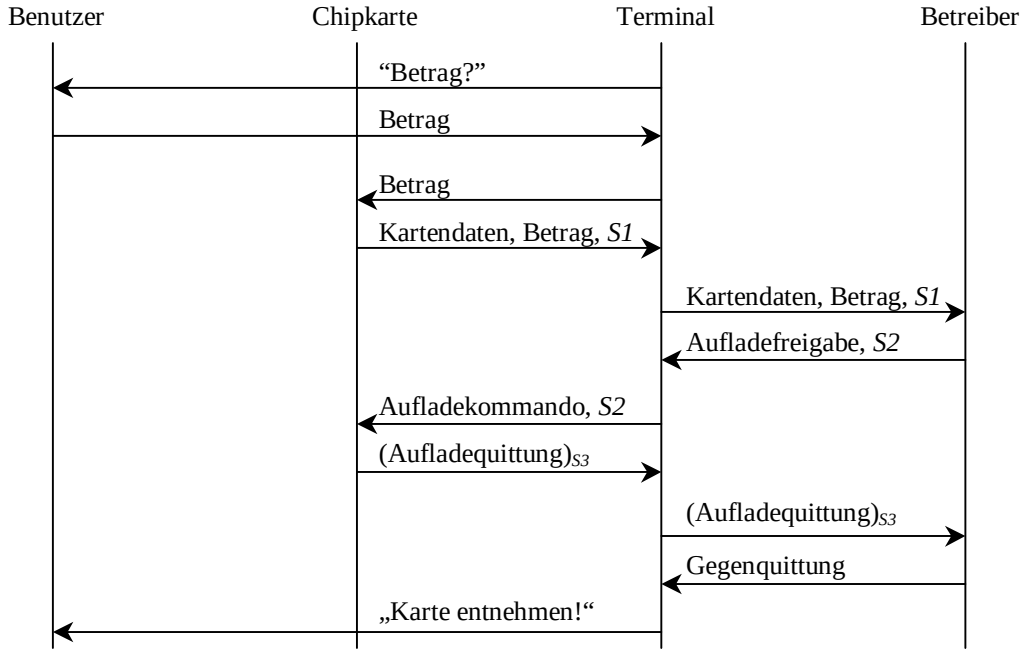


Abbildung 23: Message Sequence Chart für das Aufladen einer elektronischen Geldbörse (Quelle: [Schütt96] S. 111)

Die gesamte Sicherheit der Geldkarte beruht auf einem kryptographischen Algorithmus, der die im Klartext ausgetauschten Nachrichten zwischen Karte und Terminal signiert. Wird der zugehörige, geheime Schlüssel gebrochen, dann ist es möglich, in gewissem Rahmen Geld zu erzeugen.

4 Datenschutzverfahren: Sicherheit und Akzeptanz

Die personenbezogenen Daten eines Benutzers dürfen zweckgebunden gespeichert, übermittelt und ausgewertet werden, sofern dies durch das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift erlaubt oder angeordnet wird ([BDSG] §4) oder der Benutzer explizit einwilligt. Dies kann im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses geschehen. Darüber hinaus muß dies zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich sein und es darf kein Grund zu der Annahme bestehen, daß das schutzwürdige Interesse des Benutzers an dem Ausschluß der Verarbeitung oder Nutzung überwiegt ([BDSG] §28).

Das BDSG bietet eine gute Grundlage für den Schutz personenbezogener Daten vor Mißbrauch. Es verbietet die vom Benutzer nicht ausdrücklich genehmigte Zusammenführung von Daten. Die unerlaubte Erstellung eines Benutzerprofils ist somit illegal.

Ein Benutzerprofil ist eine Sammlung von Daten einen Benutzer betreffend, die aus einer oder mehreren Quellen zusammengetragen wurde.

Detaillierte Benutzerprofile können zum Beispiel dazu verwendet werden, gezielt auf die Person abgestimmte Werbung zu versenden oder auch Vertreterbesuche zu organisieren. Es könnten Staatsangehörigkeiten, Religionszugehörigkeiten, polizeiliche Führungszeugnisse oder andere sensitive Daten zusammengestellt werden, die gezielt zum Nachteil des Betroffenen mißbraucht werden könnten.

Es kann entweder auf die Erhebung personenbezogener Daten verzichtet werden, oder die erhobenen Daten sind in geeigneter Weise vor Mißbrauch zu schützen. Die Verhinderung des Mißbrauchs personenbezogener Daten, zum Beispiel, in dem bei dem Vorgang der Authentisierung nichts protokolliert wird, ist dem bloßen Verbot vorzuziehen und würde sich auch in der Benutzerakzeptanz positiv widerspiegeln.

Sofern eine Protokollierung aus Datensicherheitsgründen nötig ist, muß sich diese auf den erforderlichen Umfang beschränken ([TeleTrusT98] S. 19). In der Sicherheitspolitik eines Systems muß klar definiert sein, unter welchen Voraussetzungen wer welche protokollierten Daten einsehen darf und wann diese zu löschen sind (siehe 2).

Möglicher Mißbrauch kann durch Anwendung des Vieraugenprinzips eingeschränkt werden. Es besagt, daß mindestens zwei berechtigte Benutzer der Aktion zustimmen müssen. Realisierbar wäre dies zum Beispiel dadurch, daß die personenbezogenen Daten verschlüsselt gespeichert werden (siehe 3.4.3) und der zugehörige Schlüssel derart unter den berechtigten Benutzern aufgeteilt wird, daß zwei Benutzer erforderlich sind, um ihn wieder zusammenzusetzen ([DuD2] S. 153). Bei n Benutzern bekommt jeder Benutzer $(n-1)/n$ Teile des Schlüssels, wobei jedem Benutzer ein anderer Teil des Schlüssels fehlt.

Bei 3 Benutzern - Alice, Bob und Claire - könnte ein kryptographischer Schlüssel (1 2 3) folgendermaßen in drei Teile aufgeteilt werden:

Alice : 2 3
Bob : 1 3
Claire : 1 2

Alice fehlt der erste Teil des Schlüssels, Bob fehlt der mittlere Teil und Claire fehlt der letzte Teil. Da Alice, Bob und Claire den fehlenden Schlüsselteil der jeweils anderen beiden Benutzer haben, können zwei Benutzer den Schlüssel wieder zusammensetzen. Die Schlüssellänge ist geeignet groß zu wählen, damit der unbekannte Schlüsselraum möglichst groß ist (siehe 3.4.3). Die kryptographische Sicherheit des Schlüssels ist somit gewährleistet, da der jeweils fehlende Teil nicht leicht von einem der Benutzer herausgefunden werden kann.

Kein Benutzer darf zu irgendeinem Zeitpunkt Zugriff auf den kompletten Schlüssel erhalten, weil sonst das Vieraugenprinzip nicht mehr erfüllt ist. Zum Beispiel könnte dann Alice alleine die personenbezogenen Daten entschlüsseln. Wenn die Daten entschlüsselt wurden, für die der zusammengesetzte Schlüssel erforderlich war, muß dieser wieder gelöscht werden.

Verschiedene Anwendungen, in denen biometrische Authentisierung zum Einsatz kommt, sollten mehrere verschiedene Verfahren der biometrischen Authentisierung verwenden. Eine solche heterogene „Verfahrenslandschaft“ kann die Akzeptanz eines Benutzers erhöhen, denn dadurch kann zum einen die Abhängigkeit von *einem* Hersteller biometrischer Verfahren verhindert werden. In verschiedenen Verfahren der biometrischen Authentisierung werden die Referenzmuster der Benutzer unterschiedlich repräsentiert. Dadurch wird zum anderen verhindert, daß allein durch Kenntnis eines Referenzmusters eines Benutzers personenbezogene Daten dieses Benutzers anwendungsübergreifend unerlaubt zusammengeführt werden.

Es kann zwischen Hard- und Softwareimplementierungen von biometrischen Verfahren unterschieden werden. Hardware ist vom Grundsatz her sicherer, da es sich um ein abgeschlossenes System handelt, dessen Sicherheit nicht von der Implementierung des umgebenden Systems abhängt. Bei einer Hardwarelösung kann durch klar definierte Schnittstellen physikalisch die Trennung von biometrischer Einheit und umgebenden System vorgenommen werden. Hingegen bei Softwareimplementierungen erfolgt diese Trennung nur auf logischer Ebene, das heißt im System selbst.

Ein weiterer Aspekt für die Benutzerakzeptanz ist Beeinflußbarkeit eines Systems. Sie beinhaltet

- die aktive Auslösung der biometrischen Erkennung, die bei jeder Authentisierung durch Verifikation, bei dynamischen- oder nicht-berührungslosen biometrischen Verfahren vorhanden ist (siehe 2.3-2.12).
- die mögliche Auswahl einer von mehreren angebotenen Leistungen eines Systems (siehe 4.3.2).

Für einige der biometrischen Verfahren bietet sich die Adaption von als Original klassifizierten Referenzdaten an (siehe 2.1.1). Dies betrifft alle dynamischen Verfahren und die, bei denen das biometrische Merkmal im Laufe der Zeit natürlichen Veränderungen ausgesetzt ist (siehe 2.3-2.12). Ein Problem, das mit Datenadaption insbesondere bei dynamischen Verfahren theoretisch auftreten könnte, ist die Adaption einer fremden Identität. Mit Hilfe geübter Fälschungen (siehe 2.2.1) ist es denkbar, daß ein Angreifer unerlaubt Zutritt zum

System erhält. Sein Muster wurde dann vom System fälschlicher Weise als Original klassifiziert und geht über die Referenzdatenadaption wieder in das originale Referenzmuster ein (siehe Abbildung 1). Wird dieser Vorgang hinreichend oft wiederholt, kann sich das originale Referenzmuster immer mehr der Fälschung angleichen, bis es der Fälschung näher ist, als dem eigentlichen Original selbst.

Ähnlich wie durch das Kerckhoff-Prinzip für Kryptographie beschrieben (siehe 3.4.3), sollten die biometrischen Verfahren derart dokumentiert sein, daß sie von unabhängiger Seite bezüglich Sicherheit und Erfüllung der datenschutzrechtlichen Anforderungen analysiert werden können. Ihre Sicherheit sollte nicht auf der Geheimhaltung des Algorithmus basieren.

Bei der Erstellung eines Merkmalsvektors geht Information verloren (siehe 2.1.1). Dadurch steigt die Wahrscheinlichkeit, daß sich die Referenzmuster zweier Benutzer ähnlicher sind und weniger Unterschiede aufweisen, als die biometrischen Merkmale selbst. Ist der Informationsverlust zu groß, dann besteht die Gefahr, daß sich Benutzer A als Benutzer B authentisieren kann. Ein biometrisches Verfahren muß daher sicherstellen, daß die Merkmalsvektoren von hinreichend vielen Punkten gebildet werden.

Beim Referenzbildungsprozeß werden die biometrischen Daten eines neuen Benutzers vom System erlernt (siehe 2.1.1). Die Identität des Benutzers muß dabei überprüft werden, um sicherzustellen, daß die Person zur Nutzung des Systems autorisiert ist und daß die Person die ist, die sie vorgibt zu sein. Eine Möglichkeit hierfür ist ein amtlicher Lichtbildausweis.

Der Referenzdatenbildungsprozeß basiert auf einer ungenügenden Anzahl von Originaldatensätzen. Ein Referenzmuster wird aus drei bis zehn Datensätzen gebildet (siehe 2.3-2.12), die in einem sehr kurzen Zeitraum, nämlich bei der Ersterfassung eines Benutzers, gesammelt werden. Von äußeren Einflüssen bedingte Variabilitäten, die auftreten können, werden dabei nicht berücksichtigt. Dadurch wird die Klassifizierung biometrischer Eingangsdaten in Originale und Fälschungen erschwert. Um dies im Laufe der Zeit zu verbessern, könnte Adaption dazu verwendet werden, das Referenzmuster zu "festigen". In dem Fall müssen aber bei jeder Authentisierung die selben Sicherheitsmaßnahmen getroffen werden, wie bei der ersten Erstellung des Referenzmusters.

Ein Referenzmuster kann auf zwei verschieden Arten gebildet werden - direkt aus eingelesenen biometrischen Daten oder aus Merkmalsvektoren (siehe 2.1.1). Werden keine Merkmalsvektoren verwendet, so hat dies zur Folge, daß

- das Referenzmuster größer ist und somit die Zeit für einen Vergleich steigt
- unter Umständen ein Bezug zwischen einem gespeicherten Referenzmuster und der Identität eines Benutzers hergestellt werden kann. Wenn zum Beispiel bei der Gesichtserkennung (siehe 2.8) ein Foto des Gesichts eines Benutzers als Referenzmuster dient, kann jeder, der den Benutzer kennt und Zugriff auf das Referenzmuster erhält, den Bezug herstellen. Dies gilt ebenso für andere Verfahren wie Spracherkennung oder Fingerabdruck.

Ist ein solcher Bezug bei mehr als einem System herstellbar, dann können system- oder auch verfahrensübergreifend personenbezogene Daten zusammengeführt werden. Die Möglichkeit, aus den biometrischen Referenzdaten unmittelbar auf die dahinterstehende natürliche Person rückschließen zu können, sollte erschwert oder ausgeschlossen werden ([TeleTrusT98] S. 18). Dazu sollten die Referenzmuster der Benutzer verschlüsselt abge-

speichert, und sie sollten aus Merkmalsvektoren, und nicht direkt aus den biometrischen Daten gebildet werden.

Je dauerhafter die Verbindung zwischen den biometrischen Daten und der Person besteht, desto wichtiger ist der Schutz der Daten ([DuD1] S. 133). Bei statischen Verfahren ist diese Bindung stärker gegeben, als bei dynamischen.

Zusammenfassend läßt sich folgendes feststellen:

Bei der Erstellung eines Referenzmusters ist die Identität des Benutzers zu überprüfen. Referenzmuster sollten verschlüsselt gespeichert werden und aus möglichst vielen Merkmalsvektoren gebildet sein. Die Speicherung des Musters in einer Chipkarte ist der Speicherung in einer Datenbank vorzuziehen, weil damit die Sicherheit erhöht, und der Benutzer selbst über die Verwendung seiner Daten bestimmt (siehe 4.1). Wenn biometrische Daten übertragen werden, muß sichergestellt sein, daß Absender und Empfänger der Daten authentisch sind. Dies gilt sowohl für die Übertragung über ein Netzwerk, als auch für die Übertragung zwischen biometrischem Sensor und System (siehe 4.3.2). Der Zugriff auf die Daten darf nur autorisierten Personen gestattet sein. Das Vieraugenprinzip kann dabei möglichem Mißbrauch vorbeugen.

Wie in Kapitel 2.1 beschrieben, kann zwischen Authentisierung durch Verifikation und Authentisierung durch Identifikation unterschieden werden.

4.1 Authentisierung durch Verifikation

Vorteile:

- Schnellere Erkennungszeit durch den 1:1-Vergleich

  Die Notwendigkeit, alle gespeicherten Referenzmuster mit den eingelesenen Daten zu vergleichen, entfällt.

- Potentiell höhere Benutzerakzeptanz

  Es kann keine unbemerkte Erfassung stattfinden, sondern es ist immer zuerst eine Aktion des Benutzers notwendig.

  Wird das Referenzmuster in einer Chipkarte gespeichert und verläßt dieses die Karte nicht, dann kann ein Benutzer selbst über die Verwendung seines Musters entscheiden. Hierdurch wird dem Recht auf informationelle Selbstbestimmung am besten Rechnung getragen. Dieses Recht leitet sich aus dem Grundgesetz Artikel 2 Absatz 1 und Artikel 1 Absatz 1 ab und besagt, daß der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen darf ([BfD91] S. 76).

- Möglichkeit des Offline-Betriebs

  Wenn das Referenzmuster auf einer Chipkarte gespeichert ist, dann ist es nicht erforderlich, Verbindung zu einem zentralen Datenbankserver aufzunehmen, sofern das System beziehungsweise die Anwendung dies nicht verlangt. Dadurch wird eine mögliche Störungsquelle für den Betrieb des Systems ausgeschaltet. Weiterhin gibt es dann keine biometrische Datenbank, die angegriffen werden könnte.

- Möglichkeit zu anonymer Biometrie (siehe 4.3.2)

Nachteile:

- Erforderlichkeit einer Eingabeschnittstelle

  Es muß, in Form einer Nummer oder eines Namens oder ähnlichem, eine Identifikation eingegeben werden, oder der Benutzer braucht zum Beispiel eine Karte, auf der das Referenzmuster gespeichert ist. Das bedeutet für den Betreiber eines Systems, daß eventuell auch zusätzliche Hardware erforderlich ist wie zum Beispiel ein Kartenleser oder ein Ziffernpad.

- Für den Betreiber eines Systems eventuell erforderlicher Zusatzaufwand für die Administration von Chipkarten

Werden die Referenzmuster der Benutzer auf Chipkarten gespeichert, ist sicherzustellen, daß die Muster nicht unberechtigt ausgelesen werden können.

Bei einer Erweiterung der Zugangskontrolle eines bestehenden Systems durch Biometrie (siehe 2.2.2) kommt es für die Benutzerakzeptanz auch darauf an, wie sich ein Benutzer zuvor bei der Zugangskontrolle authentisiert hat. Wenn auch bisher eine Karte oder ein Schlüssel, eine Identifikationsnummer oder –name erforderlich war, stellt Authentisierung

durch Verifikation keine große Umstellung und keinen niedrigeren Komfort für den Benutzer dar.

4.2 Authentisierung durch Identifikation

Vorteile:

- Höherer Komfort für den Benutzer

  Weder Wissen, noch Besitz sind bei dieser Form der Authentisierung notwendig (siehe 2.1). Ein Benutzer muß also weder einen Namen oder eine Nummer eingeben, noch eine Karte mit sich führen.

- Höhere Sicherheit gegenüber Angriffen anderer, dem System bekannten Benutzer

  Es kann nicht ausprobiert werden, welcher Benutzer ein ähnliches Muster hat, wie der Angreifer selbst.

Nachteile:

- Langsamere Erkennungszeit

  Es müssen *alle* gespeicherten Muster mit dem aktuell eingelesenen Muster verglichen werden, denn wenn es zwei Benutzer Alice und Bob gibt, deren Muster ähnlich sind könnte sonst Alice als Bob identifiziert werden, wenn

  - die Toleranzschwelle des Systems niedriger eingestellt ist, als die Abweichung der beiden Muster ist und
  - der Referenzdatensatz von Bob eher mit den eingelesenen Daten verglichen wird, als der von Alice.

  Die Tatsache, daß die eingelesenen Daten vielleicht zu 99% mit dem Referenzmuster von Alice übereinstimmen, würde dann außer Acht gelassen. Bei Datenbanken mit hoher Zahl an Referenzmustern kann sich die Notwendigkeit, alle gespeicherten Muster mit dem aktuell eingelesenen Muster zu vergleichen, durch eine langsamere Erkennungszeit negativ bemerkbar machen.

- Mögliche unbemerkte Identifizierung

  Da zur Identifizierung über einige biometrische Verfahren keine Aktion eines Benutzers erforderlich ist, kann diese Identifizierung auch unbemerkt und unerlaubt stattfinden. Eine aktive Mitwirkung des Benutzers, wie sie bei Authentisierung durch Verifikation erforderlich ist, kann das Verfahren für ihn verständlicher und durchschaubarer machen und dürfte Ängste abbauen sowie zur Akzeptanz des Verfahrens beitragen ([TeleTrusT98] S. 18).

  Als ein Beispiel wäre es möglich, in einem Stadion unbemerkt biometrische Daten zu erheben, diese mit einer Verbrecherkartei 1:n zu vergleichen und, wenn der Vergleich negativ war, die Daten zu löschen. Sie werden dann zwar weder gespeichert, noch übermittelt, wohl aber genutzt, was durch [BDSG] §28 ebenfalls verboten ist. Ein Benutzer muß sich einer möglichen Überprüfung bewußt sein und dieser zugestimmt haben.

4.3 Pseudonyme und anonyme Biometrie

Unter der Leistung eines Systems wird hier ein Dienst verstanden, der einem Benutzer zur Verfügung gestellt werden kann. Dies umfaßt den Zugriff auf Informationen, den physikalischen Zugang zu Gebäudebereichen und alles, wofür eine Authentisierung erforderlich ist (siehe 2.1).

Ein Benutzer will eine Leistung eines Systems in Anspruch nehmen und authentisiert sich zu diesem Zweck über ein biometrisches Verfahren. Überall dort, wo nicht unbedingt erforderlich ist, daß ein Systembetreiber Kenntnis von der Identität eines sich authentisierenden Benutzers erhält, kann auf die Möglichkeit der Zuordnung von Identität und Benutzername verzichtet werden. Diese Maßnahme kann auch die Benutzerakzeptanz für betroffene Systeme erhöhen, denn wo keine personenbezogenen Daten gespeichert werden, können diese auch nicht mißbraucht werden. Ein Ansatz, dies zu erreichen, ist pseudonyme Biometrie, eine weitere ist anonyme Biometrie.

4.3.1 Pseudonyme Biometrie

Für pseudonyme Biometrie meldet sich ein Benutzer unter einem Pseudonym, zum Beispiel einer selbst gewählten Nummer, an einem System an.

Die geheimen Zugangsdaten werden folgendermaßen erzeugt (siehe Abbildung 24):

1. Ein Zufallszahlengenerator (siehe 3.4.2) erzeugt eine Zufallszahl, die zusammen mit dem gewählten Pseudonym die öffentlichen Steuerdaten bildet.
2. Die biometrischen Daten werden eingelesen, normalisiert und zur Bildung eines Merkmalsvektors verwendet (siehe 2.1.1).
3. Dieser Merkmalsvektor bildet zusammen mit einem Teil der Zufallszahl die Eingabe für eine Hash-Funktion, die diese Eingabe in irreversibler Weise auf eine Ausgabe fester Länge abbildet (siehe 3.4.5).

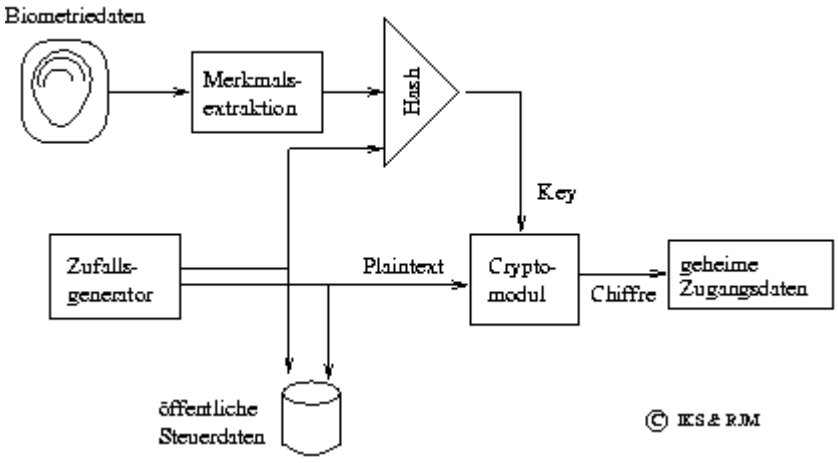


Abbildung 24: Erlernen der Biometriequelle (Quelle: [DuD2] S. 152)

4. Die Ausgabe der Hash-Funktion bildet den Schlüssel für eine symmetrische Verschlüsselungsfunktion, in der der zweite Teil der Zufallszahl verschlüsselt wird.
5. Das Ergebnis bildet die geheimen Zugangsdaten.

Ein Schwachpunkt dieses Verfahrens liegt in dem Teil „Merkmalsextraktion“. Darin müssen die eingelesenen Daten sehr stark vereinfacht werden, denn nur bei 100% Übereinstimmung dieses Merkmalsvektors mit dem, der bei der Erstellung des Pseudonyms erzeugt wurde, kann von der Hash-Funktion auch der korrekte Schlüssel erzeugt werden.

Um Zugang zu einem System zu erlangen, gibt ein Benutzer sein Pseudonym als Loginnamen dem System bekannt. Daraufhin wird die zugehörige Zufallszahl aus den öffentlichen Steuerdaten extrahiert, die zur Generierung der Zugangsdaten verwendet wird. Ein Teil der Zahl erzeugt zusammen mit den eingelesenen biometrischen Daten über die Hash-Funktion den kryptographischen Schlüssel, mit dem der zweite Teil der Zahl verschlüsselt wird (siehe Abbildung 24). Die so generierten geheimen Zugangsdaten werden in ein dem System verständliches Format, zum Beispiel ASCII, gewandelt und bilden das dem Pseudonym zugehörige Paßwort, dessen Gültigkeit vom System überprüft wird.

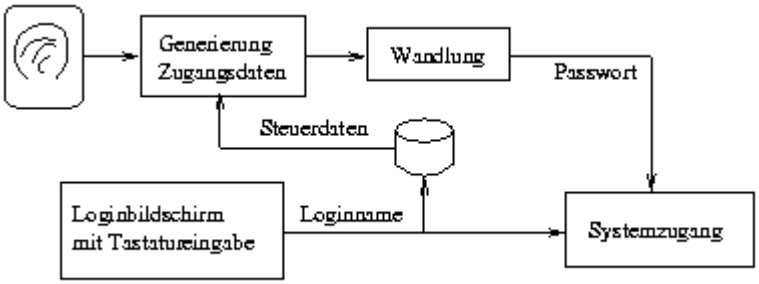


Abbildung 25: Biometrische Zugangskontrolle (Quelle: [DuD2] S. 153)

Es wäre auch möglich, die geheimen Zugangsdaten als Schlüssel für die symmetrische Verschlüsselung von Dateien zu verwenden. Zusammen mit der so verschlüsselten Datei muß der Steuerdatendatz gespeichert werden. Aus den Daten ist nicht ersichtlich, wessen und welches biometrische Merkmal zur Entschlüsselung der Datei erforderlich ist.

Bei jeder Authentisierung gibt ein Benutzer dem System sein aktuelles Pseudonym bekannt. Wenn dieses aufzeichnet, welches Pseudonym, wann was im System gemacht hat und, falls der Benutzer sein aktuelles Pseudonym wechselt, auch dieses speichert, so hinterläßt der Benutzer eine Spur, die unter Umständen zurückverfolgt werden kann. Wenn jetzt, zum Beispiel durch Social Engineering, eine Verbindung zwischen der wahren Identität eines Benutzers und einem seiner Pseudonyme hergestellt wird, kann die Identität auch allen anderen Pseudonymen der Person zugeordnet werden, solange sich die Spur zurückverfolgen läßt.

Wenn verhindert werden soll, daß eine Spur hinterlassen wird, gibt es zwei Möglichkeiten. Zum einen kann auf die Aufzeichnung von Daten, die bei der Authentisierung anfallen, verzichtet werden. Es würde genügen, nicht aufzuzeichnen, welches Pseudonym sich

authentisiert hat. Dadurch ist der Benutzer aber darauf angewiesen, auf die aus dieser Sicht korrekte Implementierung des Login im System zu vertrauen.

Zum anderen kann der Vorgang der Authentisierung anonymisiert werden, wenn dem System gar keine personen- oder pseudonymbezogenen Daten überlassen werden.

4.3.2 Anonyme Biometrie

Anonyme biometrische Authentisierung kann zum Beispiel durch folgenden Aufbau realisiert werden:

Benötigt werden eine Chipkarte, ein Chipkarten-Lesegerät, eine unabhängige biometrische Einheit und ein System, an dem die Geräte angeschlossen werden können, zum Beispiel ein PC.

Das biometrische Referenzmuster des Benutzers wird auf einer Chipkarte in einem Bereich gespeichert, der gegen unbefugtes Auslesen gesichert ist. Wenn ein System mehr als eine Leistung anbietet und nicht jeder Benutzer auf jede der Leistungen Zugriff erhalten soll, dann kann in dem geschützten Speicherbereich der Chipkarte auch eine Auswahl der möglichen Leistungen gespeichert werden, für die die Chipkarte autorisiert werden soll. Das Chipkarten-Lesegerät ist physikalisch mit der biometrischen Einheit verbunden. Diese ist wiederum mit dem System verbunden, allerdings nur in eine Richtung, das heißt, das System kann nicht auf die biometrische Einheit oder Chipkarte und Lesegerät zugreifen.

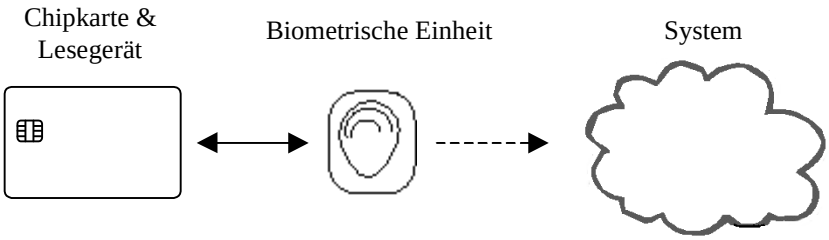


Abbildung 26: Aufbau für anonyme Biometrie

Unter diesen Voraussetzungen kann der Ablauf für eine anonyme biometrische Authentisierung folgendermaßen realisiert werden:

1. Leistungsauswahl

   Sofern mehr als eine Leistung verfügbar ist, wird eine der angebotenen Leistungen des Systems ausgewählt. Diese Auswahl könnte zum Beispiel über ein Ziffernpad auf dem Chipkarten-Lesegerät erfolgen.

2. Prüfung der Authentizität der Chipkarte

   Mit Hilfe des Challenge-Response-Verfahrens kann die Echtheit von Chipkarte und Lesegerät über gegenseitige Authentisierung überprüft werden (siehe 3.4.2). Anschließend prüft das Lesegerät gegebenenfalls, ob die Chipkarte für die angeforderte Leistung autorisiert ist. Dabei wird ein kryptographischer Schlüssel vereinbart, der für die Dauer der Transaktion gültig ist. Die Kommunikation zwischen Karte und Lesegerät findet verschlüsselt statt.

3. Verbindungsaufnahme mit der biometrischen Einheit

   Wie auch in Schritt 2 wird mit dem Challenge-Response-Verfahren die Echtheit des Lesegerätes und der biometrischen Einheit bestätigt und ein kryptographischer Schlüssel vereinbart.

4. Einlesen der biometrischen Daten

   Von Schritt 3 initiiert, werden von der biometrischen Einheit die biometrischen Daten eingelesen und normalisiert und gegebenenfalls wird daraus ein Merkmalsvektor erzeugt (siehe Abbildung 1).

5. Vergleich mit dem Referenzmuster

   Die eingelesenen biometrischen Daten werden mit dem Referenzmuster verglichen, um die Authentizität des Benutzers der Chipkarte zu überprüfen. Diese Überprüfung kann entweder in der biometrischen Einheit oder in der Chipkarte selbst erfolgen. Im ersten Fall wird von der Chipkarte das Referenzmuster angefordert, im zweiten Fall sendet die biometrische Einheit die vorverarbeiteten biometrischen Daten an die Chipkarte. Dies hätte den Vorteil, daß das Referenzmuster die Chipkarte nie verläßt. Allerdings werden dadurch hohen Anforderungen an die Leistungsfähigkeit der Chipkarte gestellt.

6. Verbindungsaufnahme mit dem System

   Wenn die eingelesenen biometrischen Daten innerhalb der festgelegten Toleranzen mit dem Referenzmuster übereinstimmen, so war die Authentisierung erfolgreich. An das System kann jetzt eine Aufforderung zur Freigabe der angeforderten Leistung gesendet werden. Diese Aufforderung sollte mit einem Zeitstempel versehen und signiert werden, um die Authentizität der Aufforderung sicherzustellen und die Nachricht für eine Wiedereinspielung unbrauchbar zu machen.

Das System erhält weder auf das Referenzmuster, noch auf die eingelesenen biometrischen Daten Zugriff. Es ist nicht notwendig, den Namen des Benutzers oder irgendeine Identifikationsnummer in elektronischer Form auf der Karte zu vermerken, denn von der Chipkarte beziehungsweise der Biometrischen Einheit wird dem System bestätigt, daß der Besitzer der benutzten Chipkarte auch zu deren Benutzung autorisiert ist, da sein Referenzmuster sich auf der Chipkarte befindet. Vom System selbst kann nur Datum und Zeit, sowie die angeforderte Leistung aufgezeichnet werden. Unter der Voraussetzung, daß auch das Chipkarten-Lesegerät und die biometrische Einheit keine Aufzeichnungen tätigen können, ist sichergestellt, daß die biometrische Authentisierung anonym ist.

5 Schlußbetrachtung

Als Benutzer informationstechnischer Systeme muß man sich bewußt sein, daß neue Technologien zwar normalerweise Verbesserungen mit sich bringen, aber nie der Weisheit letzter Schluß sind. Die Verwendung von Verfahren der biometrischen Authentisierung anstelle von Authentisierung durch Wissen oder Besitz kann die Sicherheit von Systemen erhöhen. Allerdings macht Authentisierung nur einen Teil der Sicherheit eines Systems aus. Somit ist es falsch zu glauben, Biometrie alleine könnte ein System sicher machen.

Ebenso verhält es sich mit dem Ersatz von Magnetkarten durch Chipkarten. Während ein Magnetstreifen leicht auslesbar ist, bieten Chipkarten die Möglichkeit, Daten in gesicherten Bereichen zu speichern. Das bedeutet jedoch nicht, daß es kein Verfahren gibt oder geben wird, auch diese Daten auszulesen oder zu manipulieren. Fälschungen von Chipkarten sind ebenfalls mit unterschiedlich hohem Aufwand herstellbar, wie Beispiele aus den letzten Jahren gezeigt haben.

Unabhängig davon sind Chipkarten ein technischer Fortschritt, der, unter anderem durch die Integration eines Mikroprozessors auf dem Chip, weitergehende Anwendungen und Funktionalitäten ermöglicht, die mit Magnetkarten nicht realisierbar wären.

Steigende Leistungsfähigkeit der Mikroprozessoren und ein Speichervolumen von vielen Megabyte ermöglichen Chipkarten in Zukunft Datenträger für viele Applikationen, zum Beispiel im elektronischen Zahlungsverkehr, zu sein.

Erfahrungen aus bereits im Einsatz befindlichen biometrischen Systemen, wie auch noch in neuen Feldversuchen zu testenden Systemen werden dazu beitragen, Authentisierungen sicherer gestalten zu können.

Die hohe Sicherheit, die viele biometrische System bieten und die mögliche Eindämmung der "Paßwortflut", mögen manche Anwender euphorisch stimmen. Es muß aber darauf geachtet werden, daß der Schutz persönlicher Daten gewährleistet ist, um den "gläsernen Menschen" niemals Wirklichkeit werden zu lassen.

6 Literaturverzeichnis

[BDSG] Bundesdatenschutzgesetz (Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990, BGB1. I S. 2954, 2955)

[BfD91] Der Bundesbeauftragte für den Datenschutz: Bundesdatenschutzgesetz – Text und Erläuterung –. Bonn, 1991.

[BioPassword99] http://www.biopassword.com

[Brockhaus87] Brockhaus Enzyklopädie, Mannheim, 1987.

[c't12/94] Meyer, C.; Volpe, F. P.; Volpe, S.: Plaste und Elaste – Interna der wichtigsten Chipkarten, in: c't Heft 12/1994, S.310-318.

[c't16/98] Endres, J.: Krypto-Standard DES untauglich, in: c't Heft 16/1998, S.27.

[DuD1] Wirtz, B.: Biometrische Verfahren – Überblick, Evaluierung und aktuelle Themen, in: Datenschutz und Datensicherheit Heft 3/99, S129-134. Verlag Vieweg, Wiesbaden.

[DuD2] Donnerhacke, L.: Anonyme Biometrie, in: Datenschutz und Datensicherheit Heft 3/99, S151-154. Verlag Vieweg, Wiesbaden.

[Encyclopaedia99] Encyclopaedia Britannica, http://www.eb.com

[EyeDentify99] http://www.eyedentify.com

[FBI84] Federal Bureau of Investigation: The science of Fingerprints: Classification and Uses, U.S. Government Printing Office, Washington D.C., 1984.

[Hübener97] Hübener, K.: Akustische Segmentierung zur Erkennung gesprochener Sprache. Dissertation zur Erlangung des Doktorgrades am Fachbereich Informatik der Unversität Hamburg, 1997.

[Jasperinc99] http://www.jasperinc.com/english/profile/brief.html

[Kuratorium97] Kuratorium Deutsche Kartenwirtschaft: „Die Karte".

[Meyer90] Meyers großes Taschenlexikon: in 24 Bänden, 3. und aktualisierte Auflage, Mannheim, 1990.

[Page91] Page, B.: Diskrete Simulation. Springer-Verlag, Berlin (u.a.), 1991.

[Pfleeger97] Pfleeger, C. P.: Security in Computing (Second Edition). Prentice Hall PTR, Upper Saddle River, NJ07458, 1997.

[Rankl96] Rankl, W.; Effing, W.: Handbuch der Chipkarten: Aufbau, Funktionsweise, Einsatz von Smart Cards (2. Auflage). Carl Hanser Verlag, München, Wien, 1996.

[Roddy99] Roddy and Stosz: Fingerprint Features – Statistical Analysis and System Performance Estimates. http://www.biometrics.org/Reports/IEEE_pre.pdf

[Sandia91] James P. Holmes, Larry J. Wright, Russell L. Maxwell, Sandia National Laboratories: A Performance Evaluation of Biometric Identification Devices. Albuquerque, New Mexico, 1991.

[Sandia98] Dr. Jeffrey J. Carlson and Dr. Ann M. Bouchard, Sandia National Laboratories: Sensor-Fusion-Based Biometric Identity Verification. Albuquerque, New Mexico, 1998.

[Schier99] Schier, K.: Vertrauenswürdige Kommunikation im elektronischen Zahlungsverkehr. Dissertation zur Erlangung des Doktorgrades am Fachbereich Informatik der Universität Hamburg, 1999.

[Schneier96] Schneier, B.: Angewandte Kryptographie. Addison-Wesley, Bonn (u.a.), 1996.

[Schütt96] Schuett, S.; Kohlgraf, B.: Chipkarten: Technische Merkmale, Normung, Einsatzgebiete. R. Oldenbourg Verlag, München, Wien, 1996.

[Spence99] Bill Spence: Biometrics In Physical Access Control: Issues, Status and Trends. http://www.recogsys.com/rsi_public_html/rsitech/white2.html

[Tanenbaum95] Tanenbaum, A.: Moderne Betriebssysteme (2.Auflage). Prentice Hall International Inc., London; Carl Hanser Verlag, München, Wien, 1995.

[TeleTrusT98] TeleTrusT: Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren. Berlin, 1998.

[Veridicom99] http://www.veridicom.com/fps100frames.htm

[Volpe96] Volpe, F. P.; Volpe, S.: Chipkarten: Grundlagen, Technik, Anwendungen. Heinz Heise Verlag GmbH & Co KG, Hannover, 1996.

[Zunkel99] Dick Zunkel, Technical Editor: Hand Geometry Today. http://www.recogsys.com/rsi_public_html/rsitech/white1.html