Einsatzmöglichkeiten für Biometrie und Smartcards

Diplomarbeit

Zur Erlangung des Grades eines Diplom-Ökonomen der
Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

Vorgelegt von

Name: Zhang Vorname: Jue

in: Shanghai V.R.China

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover,
den 17.01.2005

Inhaltsverzeichnis

1. Einleitung

In der heutigen modernen Informationsgesellschaft werden immer mehr neue moderne Informations- und Kommunikationstechnologien eingesetzt, so dass neue Chancen entstehen, die den Informationsaustausch und Wirtschaft fördern.[1]

Dabei gewinnen Biometrische Verfahren und Chipkarten immer mehr Bedeutung. Diese beiden Technologien werden heute in allen Lebensbereichen eingesetzt. Ziel dieser Diplomarbeit ist, dass diese beiden Technologien beschrieben werden, und die Einsatzmöglichkeiten für diese beiden Technologien erläutert werden.

Im zweiten Kapitel werden Grundlagen der Biometrie beschrieben. Im dritten Kapitel werden bestimmte biometrische Verfahren erläutert. Im vierten Kapitel werden Einsatzbeispiele verschiedener biometrischer Verfahren beschrieben. Im fünften Kapitel und sechsten Kapitel geht es um Angriffsmöglichkeiten auf biometrische Verfahren und Datenschutz. Im siebten Kapitel werden Grundlagen der Chipkarten beschrieben. Im achten Kapitel werden Anwendungsmöglichkeiten der Chipkarten erläutert. Im letzten Kapitel folgt eine Zusammenfassung und ein Ausblick.

2. Grundlagen der Biometrie

2.1 Begriffsklärung der Biometrie

Biometrie ist ein Begriff, der aus dem Griechischen stammt und wird aus den zwei Wörtern Bios (Leben) und Metron (Maß) zusammengesetzt.[2] Laut Duden ist die Biometrie die Wissenschaft von der Zählung und Körpermessung an Lebewesen. Lebewesen werden als Menschen interpretiert, deren körperliche Merkmale, die gemessen werden können, die Grundlage der biometrischen Verfahren bilden.[3]

Eine bestimmte Person kann durch biometrische Erkennung von anderen Personen unterschieden werden, indem ein spezifisches Merkmal der betroffenen Personen gemessen und verglichen wird.[4]

---

[1] Vgl. Albrecht (2003, S.19)
[2] Vgl. Nolde (2002, S.20)
[3] Vgl. Nolde (2002, S.20)
[4] Vgl. Albrecht (2003, S.31)

Es gibt biometrische Verfahren und biometrische Systeme.[5] Ein biometrisches Verfahren ist eine Methode, die die Menschen authentisieren können, indem geeignete Geräte angewendet werden, so dass die persönlichen biologischen Eigenschaften der betroffenen Menschen gemessen werden können.[6] Ein biometrisches Verfahren enthält normalerweise folgende Komponenten:[7] Sensoren, Kameras, Mikrophone und Scanner sind die technischen Instrumente, die die individuellen biometrischen Merkmale erfassen können. Die Daten, die gefasst werden, werden mit der Hilfe von mathematischen und statistischen Methoden behandelt und als Referenzmuster gespeichert. Danach werden Vergleichsalgorithmen erstellt. Der ganze Prozess läuft automatisch. In einem biometrischen System werden Hard- und Software-Gefüge miteinander kombiniert .[8]

2.2 Geschichtliche Entwicklung der Biometrie

Schon seit mehr als ein tausend Jahr wurde biometrisches Verfahren angewendet.[9] In China wurde schon in der Tang-Dynastie das Verfahren von Fingerabdruckerkennung im Geschäftsleben eingesetzt, während Verträge von Geschäftsleute abgeschlossen wurden.[10] 1858 wurde zum ersten Mal vorgeschlagen, dass das Verfahren zur Fingerabdruckerkennung angewendet werden soll, um gegen die Kriminalität zu bekämpfen.[11] 1879 wurde ein System der Messung von Alphonse Bertillon entwickelt, das versucht, die Identifikation der Personen auf der Basis von physiologischen Merkmalen zu ermöglichen.[12] 1892 wurde von Francis Galton herausgefunden, dass jedes Individuum einen einzigartigen Fingerabdruck besitzt und dieser Fingerabdruck grundsätzlich im ganzen Leben nicht verändert wird.[13] 1897 wurden die ersten Verbrecher von New Scotland dadurch identitifiziert.[14] 1903 wurde die Methode des Fingerabdrucks in Deutschland eingesetzt.[15] In den siebziger Jahren wurden Handgeometrie-erkennungssysteme entwickelt.[16] John Daugman entwickelte am Ende der achtziger Jahre die

---

[5] Vgl. Albrecht (2003, S.31)
[6] Vgl. Albrecht (2003, S.31)
[7] Vgl. Nolde (2002, S.20)
[8] Vgl. Albrecht (2003, S.32)
[9] Vgl. Albrecht (2003, S.33)
[10] Vgl. Albrecht (2003, S.33)
[11]Vgl. Albrecht (2003, S.34)
[12] Vgl. Albrecht (2003, S.34)
[13] Vgl. Albrecht (2003, S.34)
[14] Vgl. Albrecht (2003, S.34)
[15] Vgl. Busch (2002, S.8)
[16] Vgl. Albrecht (2003, S.34)

Methode der Iriserkennung und erwarb darauf das Patent.[17] Eine Reihe biometrischer Systeme, die auf der Basis von neuronaler Netzen aufgebaut werden, werden seit ungefähr 1995 eingesetzt.[18] Danach kamen viele Produkte biometrischer Systeme für kommerzielle Zwecken auf dem Markt.[19]

2.3 Funktionsweise biometrischer Verfahren

Biometrische Merkmale haben in der Regel drei Eigenschaften.[20] Die erste Eigenschaft ist :[21] die biometrischen Merkmale sind genetisch bedingt und können somit zum Teil vererbt werden. Die zweite Eigenschaft ist, dass Die biometrischen Merkmale bilden sich in Zufallsprozessen während einer embryonalen Phase und werden sich ein Leben lang grundsätzlich nicht verändern.[22] Die dritte Eigenschaft ist, dass die biometrischen Merkmale trotz ihrer genotypischer und randotypischer Eigenschaften vom Verhalten gesteuert werden könne und somit zum Teil anerziehbar und veränderbar sein können. [23]

Biometrische Verfahren lassen sich in der Regel in zwei Arten unterteilen[24] : Die eine Art basiert auf physiologische Merkmale und die andere Art basiert auf verhaltensbezogene Merkmale. Die physiologischen Merkmale sind zum Beispiel Gesicht, Iris, Retina, Finger oder Hand.[25] Die verhaltensbezogenen Merkmale sind zum Beispiel Handschrift und Stimme.[26]

Der Prozess eines biometrisches Verfahren läuft in der Regel unabhängig von verschiedenen technischen Strukturen wie folgend: Zuerst wird der Nutzer in das System registriert (Enrollment), dann werden Datensätze (Templates) erstellt und gespeichert und schließlich werden im Erkennungsprozess die gespeicherten Datensätze mit Datensätzen, die geprüft werden sollen, verglichen (Matching). [27]

2.3.1 Die Auswahl von Merkmalen

---

[17] Vgl. Albrecht (2003, S.34)
[18] Vgl. Busch (2002, S.8)
[19] Vgl. Albrecht (2003, S.34)
[20] Vgl. Albrecht (2003, S.34)
[21] Vgl. Behrens (2001, S.55)
[22] Vgl. Albrecht (2003, S.35)
[23] Vgl. Busch (2002, S.4)
[24] Vgl. Albrecht (2003, S.35)
[25] Vgl. Albrecht (2003, S.35)
[26] Vgl. Albrecht (2003, S.35)
[27] Vgl. Nolde/Leger (2002,S.22)

Für die Auswahl von Merkmalen werden folgende Anforderungen gestellt:[28] Universalität bedeutet, dass ein Merkmal bei jeder Person vorzufinden ist.
Mit Einzigartigkeit wird verstanden, dass ein Merkmal von jeder Person unterschiedlich präsentiert wird. Permanenz bedeutet, dass ein Merkmal sich im Laufe der Zeit nicht verändert.
Erfassbarkeit bedeutet, dass ein Merkmal quantitativ erhoben werden kann. Es wäre ideal, wenn ein Merkmal alle Anforderungen erfüllen kann. Für die jeweiligen biometrischen Verfahren werden auch Anforderungen gestellt:[29] Technische Umsetzbarkeit bedeutet, dass ein Verfahren geeignet sein müssen, um eine bestimmte große Menge von Menschen zu erkennen.
Ökonomische Machbarkeit bedeutet, dass die Kosten sich im Rahmen halten und getragen werden können. Überlistungsresistenz bedeutet, dass ein Verfahren gegen verschiedene Angriffsmöglichkeiten gut bewahrt werden kann.
Akzeptanz bedeutet, dass die betroffenen Personen bereit sein müssen, dass ein Merkmal von ihnen für das Verfahren erhoben wird.

2.3.2 Die Messung von Merkmalen

Die Messung von Merkmalen muss unbedingt die Anforderung der Genauigkeit erfüllen. Zum Beispiel beim Verfahren der Gesichtserkennung muss die Auflösung des aufgenommenen Bildes sehr genau festgelegt werden, wenn digitale CCD-Kameras eingesetzt werden.[30] Wenn die betroffene Person ihre Mimik verändert oder sich bewegt, wird die Genauigkeit möglicherweise beeinflusst.[31]
Die Lichtverhältnisse und die Reflexe, die im Verlauf des Tages verändern, könnten auch dazu führen, dass verschiedene Probleme bei der Auswertung eintreten.[32]
Vergleichbare Probleme können bei allen biometrischen Verfahren eintreten, und somit ist ein geeignetes Toleranzintervall hilfreich.[33]
In der Praxis ist es nicht ungewöhnlich, dass ein Merkmal bei einer bestimmten Person oder einer bestimmten Gruppe nicht stark genug ausgeprägt ist oder überhaupt nicht existiert. Deshalb ist es rational, dass nicht nur ein biometrisches Verfahren eingesetzt wird, sondern

---

[28] Vgl. Behrens/Roth (2001, S.11-12)
[29] Vgl. Behrens/Roth (2001, S.12) in : Biometrische Identifikation
[30] Vgl. Behrens/Roth (2001, S.14) in: Biometrische Identifikation
[31] Vgl. Behrens/Roth (2001, S.14) in: Biometrische Identifikation
[32] Vgl. Behrens/Roth (2001, S.14) in : Biometrische Identifikation
[33] Vgl. Behrens/Roth (2001, S.14) in: Biometrische Identifikation

mehrere Verfahren kombiniert angewendet werden, so dass es vermieden werden kann, dass bestimmte Personen diskriminiert werden.[34]

2.3.3 Identifikation und Verifikation

Am Anfang funktioniert immer zunächst ein Prozess, das Enrollment heißt. Dieser Prozess läuft wie folgt ab:[35] Die Merkmale, die wichtig sind, werden aufgenommen. Innerhalb von Rahmenbedingungen, die unterschiedlich sind, werden die wichtigen Merkmale mehrmals erfasst. Die aufgenommenen Daten werden dann verarbeitet, zusammengefasst und schließlich als Template gespeichert.

Identifikation bedeutet, dass eine Person von einer Menge unterschieden wird (1:n).[36] Ein neuer aufgenommener Datensatz wird mit vielen gespeicherten Referenzdatensätzen verglichen, und er gilt als identifiziert, wenn einer von diesen Referenzdatensätzen die Ähnlichkeit, die innerhalb eines vorher festgelegten Toleranzintervalls liegt, vorweist.[37]

Bei Verifikation (1:1) wird der Datensatz mit genau einem Referenzdaten verglichen. Er wird entweder als wahr oder als falsch ausgewiesen.[38]

3. Bestimmte biometrische Verfahren

3.1 Fingerabdruckerkennung

Die Fingerabdrücke jedes Menschen sind einzigartig und verändern sich im ganzen Leben nicht.[39]

Es gibt verschiedene Sensorentypen, die eingesetzt werden können, um die Fingerabdrücke zu erfassen.[40] Bei optische Sensoren werden die Fingerabdrücke mit der Hilfe von Kameras oder Scannern aufgenommen.[41]

Mit der Hilfe von speziellen Chips funktionieren kapazitive Sensoren.[42] Ultraschallsensoren, thermische Sensoren und andere Möglichkeiten erweitern die Möglichkeiten, durch die die Fingerabdrücke erfasst werden können.[43]

---

[34] Vgl. Behrens/Roth (2001, S.15) in: Biometrische Identifikation
[35] Vgl. Behrens/Roth (2001, S.15) in: Biometrische Identifikation
[36] Vgl. Behrens/Roth (2001, S.10) in: Biometrische Identifikation
[37] Vgl. Behrens/Roth (2001, S.16) in: Biometrische Identifikation
[38] Vgl. Behrens/Roth (2001, S. 10) in: Biometrische Identifikation
[39] Vgl. Behrens/Heumann (2001, S.82) in: Biometrische Identifikation
[40] Vgl. Breitenstein (2002, S.36) in: Biometrische Verfahren
[41] Vgl. Breitenstein (2002, S.36) in: Biometrische Verfahren
[42] Vgl. Breitenstein (2002, S.36) in: Biometrische Verfahren
[43] Vgl. Breitenstein (2002, S.36) in: Biometrische Verfahren

Wenn die Mitarbeiter eine Pause machen, nehmen sie ihre Chipkarte aus dem Kartenleser aus und der Zugang wird wieder geschlossen, so dass die Sicherheit gewährleistet wird und die Chipkarte kann weiter in der Cafeteria für die Zahlung eingesetzt werden.[434]
Wenn der letzte Mitarbeiter einer Abteilung seine Abteilung verlässt hat, beziehungsweise per Chipkarte bei dem Zeiterfassungsterminal abgebucht hat, werden das Licht und die Be- und Entlüftung in dieser Abteilung automatisch ausgeschaltet, während die manuelle Ausschaltung selbstverständlich weiterhin funktioniert.[435]
Mit dieser Chipkarte wird die Zeiterfassung optimiert und erleichtert, wobei die Informationen über Nacht verarbeitet werden, und die Mitarbeiter können am nächsten Tag bei dem Terminal alle wichtige Daten der Zeiterfassung einfach abbrufen, wodurch viele Freiheiten für die Mitarbeiter geschaffen werden.[436]
Wenn es notwendig ist, können die Mitarbeiter selbst durch ihren PC die Fehler, die bei der Zeiterfassung eingetreten sind, wahrhaft korrigieren und anschließend wird der Chef automatisch informiert.[437]
In der Cafeteria sind alle Zahlungen inklusiv der Rücknahme der Flaschen nur mittels dieser Chipkarte möglich, wobei sie bei einem Automaten bei Bedarf aufgeladen werden kann. [438] Es ist ebenfalls möglich, dass die Zahlungen direkt mit dem Gehalt abgerechnet werden können, wobei diese Möglichkeit nicht zum Einsatz kommt, weil aus der Sicht des Datenschutzes die Personalabteilung keine entsprechende Möglichkeiten bekommen soll.[439]

9. Zusammenfassung und Ausblick

Biometrie ist ein Begriff, der aus dem Griechischen stammt und wird aus den zwei Wörtern Bios(Leben) und Metron (Maß) zusammengesetzt. Laut Duden ist die Biometrie die Wissenschaft von der Zählung und Körpermessung an Lebewesen.
Ein biometrisches Verfahren ist eine Methode, die Menschen authentisieren können, indem geeignete Geräte angewendet werden, so dass die persönlichen biologischen Eigenschaften der betroffenen Menschen gemessen werden können. Ein biometrisches Verfahren enthält normalerweise folgende Komponenten: Sensoren, Kameras, Mikrophone und Scanner sind die technischen Instrumente, die die individuellen biometrischen Merkmale erfassen können.

---

[434] Vgl. Siemering (2002, S.63)
[435] Vgl. Siemering (2002, S.63-64)
[436] Vgl. Siemering (2002, S.64)
[437] Vgl. Siemering (2002, S.64)
[438] Vgl. Siemering (2002, S.64)
[439] Vgl. Siemering (2002, S.64)

Die Daten, die erfasst werden, werden mit der Hilfe von mathematischen und statistischen Methoden behandelt und als Referenzmuster gespeichert.
Biometrische Verfahren lassen sich in der Regel in zwei Arten unterteilen: Die eine Art basiert auf physiologische Merkmale und die andere Art basiert auf verhaltensbezogene Merkmale. Die physiologischen Merkmale sind zum Beispiel das Gesicht, Iris, Retina, Finger oder die Hand. Die verhaltensbezogenen Merkmale sind zum Beispiel Handschrift und Stimme.
Der Prozess eines biometrischen Verfahren läuft in der Regel unabhängig von verschiedenen technischen Strukturen wie folgend: Zuerst wird der Nutzer in das System registriert (Enrollment), dann werden Datensätze (Templates) erstellt und gespeichert, und schließlich werden im Erkennungsprozess die gespeicherten Datensätze mit Datensätzen, die geprüft werden sollen, verglichen (Matching).
Identifikation bedeutet, dass eine Person von einer Menge unterschieden wird (1:n). Ein neu aufgenommener Datensatz wird mit vielen gespeicherten Referenzdatensätzen verglichen und er gilt als identifiziert, wenn einer von diesen Referenzdatensätzen die Ähnlichkeit, die innerhalb eines vorher festgelegten Toleranzintervalls liegt, vorweist. Bei Verifikation (1:1) wird der Datensatz mit genau einem Referenzdaten verglichen. Er wird entweder als wahr oder als falsch ausgewiesen.
Im Verfahren der Fingerabdruckerkennung vergleicht man bei der Verifikation die Referenzdaten, die schon gespeichert wurden, mit den neu aufgenommenen Daten. Jede Minutie kann aufgrund ihrer Distanz und ihrer Orientierung zu den anderen Minutien identifiziert werden. Darüber hinaus werden die Informationen, die den Typ der Minutie und die relative Richtung der Minutie beschrieben, hinzugezogen. Innerhalb eines Toleranzintervalls wird die Ähnlichkeit als Übereinstimmung positiv bewertet.
Bei der Identifikation werden nur die Fingerbilder, die die gleichen Muster und Strukturen vorweisen, in Betracht gezogen, und anschließend wird ein entsprechendes Ergebnis durch das Vergleichen jeder Minutie erzielt.
Die FAR (False Acception Rate) wird von den meisten Produzenten von weniger als 0.0001 Prozent angegeben, und FRR (False Rejection Rate) wird von weniger als ein Prozent angegeben. In der Praxis liegt die Zahl jedoch höher.
Die Einsatzmöglichkeiten werden folgt genannt: Der Pin vom Mobiltelefon kann ersetzt werden und auch der Pin bei der Wegfahrsperre im PKW kann ersetzt werden. Außerdem können der PC-Arbeitsplatz oder das allgemeine IT-Umfeld ersetzt werden.

Es kann des weiteren dazu angewendet werden, um Missbrauch von Sozialhilfeansprüchen zu verhindern. Für die Wählerregistrierung, die Zutrittskontrolle, den Computer und den Führerschein kann dieses Verfahren ebenfalls verwendet werden.
Der ganze Prozess der Gesichtserkennung läuft in der Regel in zwei Phasen: Die erste Phase heißt Face Detection, in der das gesuchte Gesicht in der gesamten Umgebung entdeckt wird und anschließend fokussiert wird, so dass es unabhängig vom Hintergrund sein wird. In der zweiten Phase beginnt der eigentlicher Prozess der Gesichtserkennung, in dem die betroffene Person identifiziert oder verifiziert wird.
Die Einsatzmöglichkeiten werden wie folgt genannt: Für den Zugangsschutz von PC-Systemen und Zutrittskontrolle kann es eingesetzt werden. In Kaufhäusern kann es angewendet werden, um Ladendiebe zu entdecken. Bei der Führerschein-Erteilung, oder der Zutrittskontrolle zu Sicherheitsbereichen in Atomkraftwerken ist es ein wirksames Instrument. Es kann außerdem in Flughäfen und Stadtvierteln oder bei Großveranstaltungen eingesetzt werden, um die Funktion der Überwachung zu erfüllen. Für die Wähler-Registrierung ist es auch ein geeignetes Mittel.
Im Prozess der Iriserkennung wird die Iris in der Regel optisch von einer Videokamera erfasst. Das aufgenommene Bild der Iris wird zuerst digitalisiert. Auf der Basis der gesamten Struktur der Iris wird ein Iriscode mittels eines Algorithmus erstellt. Durch Abstandsberechnungen auf den Iriscode werden zwei Irismuster verglichen, um den Hamming-Abstand zu erzielen.
Die Einsatzmöglichkeiten werden wie folgend genannt: Weil dieses Verfahren berührungslos ist, kann es eingesetzt werden, um die Sicherheit von Hochsicherheitsbereichen oder dem IT-Umfeld gewährleisten zu können.
Sensible Dokumente am PC können ebenfalls durch diese Methode geschützt werden.
Bei Geldausgabenautomaten, Lebensmittelgeschäften, Gefängnissen oder Flughäfen ist es ein geeignetes Instrument.
Bei dynamischer Unterschriftserkennung wird die Unterschrift von dem Anwender abgegeben und eingelernt. Die eingelernten Daten werden verschlüsselt und mit Uhrzeit und Datum versehen. Anschließend werden diese Daten zum Vergleichen weitergeleitet.
Die Einsatzmöglichkeiten werden wie folgt genannt: Für das IT-Umfeld ist es ein gutes Instrument. Bei Schecks und Überweisungen kann es angewendet werden, um Unterschriften zu prüfen. Im Workflow- und Dokumentenmanagement wird die Berechtigung der Unterschriften anhand dieses Verfahren überprüft.

Es kann auch innerhalb einer bestimmten bekannten Benutzergruppe eingesetzt werden, um die Funktion der Zutrittskontrolle zu erfüllen.
Bei Stimmerkennung kann die Erfassung durch Mikrofone durchgeführt werden, und die erfasste Stimme wird in analoge Signale umgewandelt. Es gibt zwei Methoden für die Erkennung, die textabhängig und nicht textabhängig sind. Bei der ersten Methode werden ein Wort, ein Satz oder eine Serie von Zahlen vorher genau vorgegeben, und bei der zweiten Methode wird dagegen keine Festlegung bezüglich Wort oder Satz vorgegeben.
Die Einsatzmöglichkeiten werden wie folgt genannt: Es wird dazu eingesetzt, um eine Berechtigungsüberprüfung über die Telefonnetze zu ermöglichen. Für das IT-Umfeld, Telefonbanking, PC-Zugangskontrolle, Zutrittskontrolle ist es auch geeignet.
Um die Personen, die unter Hausarrest stehen, zu kontrollieren, kann es ebenfalls angewendet werden.
Bei der Handgeometrieerkennung wird der Umriss der Hand mittels CCD-Kameras erfasst, und die weiteren Bestandsteile des Erkennungssystems sind eine Oberfläche, die beleuchtet ist und von der Hand aufgelegt wird, Stäbchen, die dazu dienen, dass die Hand auf der richtigen Position legen kann, Seitenspiegel, die ermöglichen, dass ein Seitenprofil der Hand aufgenommen werden kann.
Die Einsatzmöglichkeiten werden wie folgt beschrieben: Es kann eingesetzt werden, für Zutrittskontrolle, Grenzkontrolle, Passagierabfertigung und die PC-Zugangssicherung. Weiterhin kann es angewendet werden, um die Berechtigung der geprüften Person zu Prüfen, ob diese Person sensible Medikamenten bekommen darf.
Der Kartenkörper einer Chipkarten enthält eine Schaltung, in der Elemente vorhanden sind, die dazu dienen, dass Datenübertragung, Datenspeicherung und Datenverarbeitung ermöglicht werden. Es gibt Speicherkarte und Mikroprozessorkarten. Bei Speicherkarten wird es wie folgt beschrieben: Im Speicher werden die Informationen, die für die jeweiligen Anwendungen entscheidend sind, gespeichert. Mittels Sicherheitslogik wird gewährleistet, dass Angriffsversuche abgewehrt werden können. Die Anwendungsbeispiele sind : Telefonkarten, die vorher schon bezahlt werden. Krankenversichertenkarte, Öffentlicher Verkehr, Verkaufsautomaten, Kantinen, Schwimmbäder, Parkgebühren usw.
Bei Mikroprozessorkarten wird es wie folgend erläutert: Der Prozessor ist am wichtigsten und funktioniert mit weiteren vier Komponenten, die das Masken-ROM, das EEPROM, das RAM und die I/O-Schnittstelle sind.

Die Anwendungsmöglichkeiten sind im folgenden Bereichen zu finden: im Bankenbereich, im Mobilfunkbereich, als Ausweiskarten, für Zugangskontrolle, für elektronische Unterschrift, für elektronische Geldbörse usw.
Es gibt sowohl kontaktlose Speicherkarte als auch kontaktlose Mikroprozessorkarten.
Der Mikrocontroller ist ein selbständiger Computer, der einen Prozessor und Speicher besitzt, und durch eine Schnittstelle mit der Außenwelt kommuniziert, und alle Aktivitäten werden von ihm gesteuert, initiiert und überwacht.
Im Bankenwesen wird die Chipkarte in der Regel im Zahlungsverkehr angewendet. Es gibt verschiedene Anwendungsmöglichkeiten bezüglich der Chipkarte.
Die erste Anwendungsmöglichkeit ist electronic cash offline. Die zweite Anwendungsmöglichkeit ist die Geldkarte. Die dritte Anwendungsmöglichkeit ist HBCI(Home Banking Computer Interface).
Mit der Geldkarte können die Kunden ihre Zahlungen im Internet realisieren.
Eine Displaycard ist eine intelligente Banking-Chipkarte, auf der ein LC-Display installiert wird. Durch dieses Display können die Informationen der Banking-Transaktionen, die durchgeführt werden, erläutert und erkundet werden.
Außerhalb von Bankenbereichen können diese Chipkarten auch im Hotels, Clubs, Casinos, Airlines, Supermärkte oder im öffentlichen Nahverkehr eingesetzt werden.
In der Telekommunikation werden Smartcards hauptsächlich bei Mobiltelefon angewendet. Die Smartcards, die im GSM-Netzen eingesetzt werden, heißen SIM(Subscriber Identity Module). Diese SIM-Karte, die in GSM-Telefon integriert werden kann, hat einen Prozessor, ROM, RAM, und ein EEPROM.
Die Aufgaben der SIM-Karte sind die Folgenden: Der Zugriff bezüglich von Netzwerkdiensten wird durch sie kontrolliert. Die Dienste werden personalisiert. Sie bestimmt die Wahl des Netzes.
Seit dem 7.April 2003 wird die Chipkarte, die Padersprinter Card heißt, in Paderborn und Nord- und Kirchborchen eingesetzt, womit die Fahrgäste ohne Bargeld die Dienstleistungen der öffentlichen Verkehrsmittel benutzen können.
Noch früher wurde 1999 in Köln schon die kontaktlose Chipkarte beim Verkehr eingesetzt, die bei der Benutzung von den Fahrgästen mit einem Abstand, der bis 10 cm gültig ist, die Kartenlesergeräte vorbeigeführt werden, und schon wird alles notwendiges erledigt.
Die Chipkarte, die in den nächsten Jahren im Gesundheitswesen eingeführt werden soll, heißt die elektronische Gesundheitskarte, die auch als Patienten-Chipkarte gekennzeichnet wird.

Auf dieser Chipkarte wird das Photo des Patienten integriert, und die notwendigen medizinischen Informationen von den betroffenen Patienten werden mit ihrer Genehmigung auf der Chipkarte gespeichert.
Die Elektronische Gesundheitskarte hat Fünfhauptfunktionen. Die erste Funktion ist die Ausweisfunktion. Die zweite Funktion ist die Erklärungsfunktion. Die dritte Funktion ist Dokumentations-oder Speicherfunktion. Die vierte Funktion ist die Übermittlungsfunktion. Die fünfte Funktion ist Verschlüsselungsfunktion.
Seit 1999 wird eine Chipkarte von der Deutschen Telekom angeboten, mit der E-Mails, Interneteinkäufe, Verträge, Arztrezepte, Gerichtsurteile, und Steuererklärungen elektronisch unterschrieben werden können.
Diese Anwendung finden heutzutage nicht nur bei Militär, Geheimdiensten und Banken statt, sondern wird auch längst von der Bevölkerung und den deutschen Behörden als Normalität akzeptiert.
Der Dienstausweis, der bei dem Rückversicherer Swiss Re in Unterföhring bei München von den Mitarbeitern benutzt wird, ist eine Chipkarte, die verschiedene Aufgaben erfüllen kann: Zutrittskontrolle, Zeiterfassung, Zahlung in der Cafeteria, Zugang zu PC usw.
Für die Zukunft bezüglich biometrischer Verfahren und der Chipkarte bin ich der Meinung, dass der Einsatz biometrischer Chipkarte immer mehr Bedeutung gewinnen wird. Die Chipkarte wird eine Multifunktionalitäten vorweisen, die bisherigen getrennten Einsatzmöglichkeiten in sich vereinigen wird. Die Prognose der zukünftigen Umsätze bezüglich dieser zwei Themen möchte ich hier nicht weiter verfolgen, weil alle bisherige Prognosen, die veröffentlicht werden, als falsch erwiesen haben.

Literaturverzeichnis

Albrecht,A: Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 1.Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2003.

Behrens,M/Roth,R.(Hrsg.): Biometrische Identifikation, 1.Auflage, Friedr.Vieweg& Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 2001.