(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. Juli 2005 (28.07.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/069534 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32, G07C 9/00

(21) Internationales Aktenzeichen: PCT/EP2005/000173

(22) Internationales Anmeldedatum:
11. Januar 2005 (11.01.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 001 855.3 13. Januar 2004 (13.01.2004) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BEINLICH, Stephan** [DE/DE]; Niebelungenstrasse 12, 80639 München (DE). **MARTINI, Ullrich** [DE/DE]; Zeppelinstrasse 61, 81669 München (DE).

(74) Anwalt: **KLUNKER.SCHMITT-NILSON.HIRSCH**; Winzererstrasse 106, 80797 München (DE).

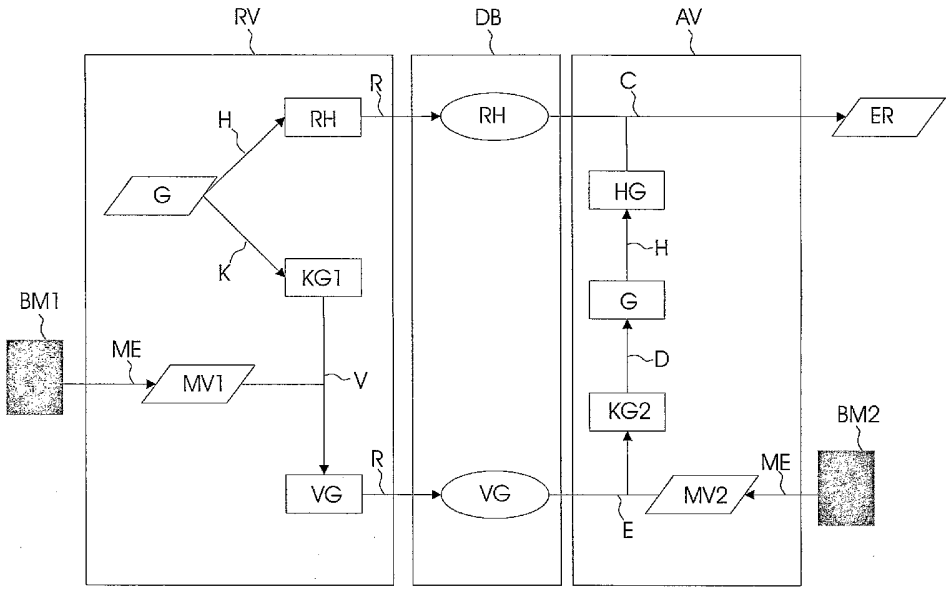
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

[Fortsetzung auf der nächsten Seite]

(54) Title: BIOMETRIC AUTHENTICATION

(54) Bezeichnung: BIOMETRISCHE AUTHENTISIERUNG



(57) Abstract: Disclosed are methods and devices for securely registering a person by means of a selected biometric feature (BM, BM1) and securely authenticating said person with the aid of the same biometric feature (BM, BM2). According to the invention, an individual secret (G) that is associated with said person is coded with a key (MV1) obtained from the biometric feature (BM, BM1), and a non-decipherable reference hash value (RH) of the secret (G) is formed. The coded secret (VG) is deciphered using a second key (MV2) of the person's same biometric feature (BM, BM2) while a hash value (HG) that is calculated therefrom is compared to the reference hash value (RH) during the authentication process.

[Fortsetzung auf der nächsten Seite]

WO 2005/069534 A1

GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Es werden Verfahren sowie Vorrichtungen zum sicheren Registrieren einer Person mittels einer ausgewählten biometrischen Eigenschaft (BM, BM1) und zum sicheren Authentisieren dieser Person mittels der gleichen biometrischen Eigenschaft (BM, BM2) beschrieben. Dabei wird ein dieser Person zugeordnetes, individuelles Geheimnis (G) mit einem aus der biometrischen Eigenschaft (BM, BM1) gewonnenen Schlüssel (MV1) verschlüsselt (VG) und ein nicht entschlüsselbarer Referenz-Hash-Wert (RH) des Geheimnisses (G) gebildet. Bei der Authentisierung wird das verschlüsselte Geheimnis (VG) mittels eines zweiten Schlüssels (MV2) der gleichen biometrischen Eigenschaft (BM, BM2) der Person entschlüsselt und ein daraus errechneter Hash-Wert (HG) mit dem Referenz-Hash-Wert (RH) verglichen.

Biometrische Authentisierung

Die Erfindung betrifft Verfahren und Vorrichtungen zum sicheren Authentisieren und Registrieren von Personen mittels biometrischer Verschlüsselung.

Für Verfahren und Vorrichtungen dieser Art existieren vielfältige gewerbliche Verwendungsmöglichkeiten, beispielsweise bei elektronischen Geldtransaktionen und Vertragsschlüssen im Banken- und Kreditkartenwesen und im Online-Handel (E-Commerce), in der elektronisch unterstützten Verwaltung (E-Governance) und dem Betrieb von elektronischen Kommunikationsnetzen aller Art. Die gewerbliche Relevanz derartiger Verfahren ist allein schon daraus ableitbar, daß der Umsatz beim Online-Shopping im Jahre 2002 in der Europäischen Union 4,3 Mrd. Euro betrug.

Eine zuverlässige elektronische Kommunikations-Infrastruktur muß im wesentlichen zwei Bedingungen erfüllen: Sie muß für jeden Kommunikationspartner eindeutig und reproduzierbar feststellen, daß er derjenige ist, der er vorgibt zu sein, also dessen Authentisierung ermöglichen, und sie muß die auszutauschenden Daten vor Manipulation oder Abhören durch Dritte schützen, d. h. deren Integrität sicherstellen.

Beide Ziele können durch den Einsatz geeigneter (symmetrischer oder asymmetrischer) Verschlüsselungsverfahren erreicht werden, mit denen eine Person eine Nachricht mit einem personalisierten Schlüssel zum Sicherstellen ihrer Integrität verschlüsseln kann, die von einem Kommunikationspartner nur mit demselben Schlüssel (symmetrische Verschlüsselung) oder einem speziellen korrespondierenden Schlüssel (asymmetrische Verschlüsselung) zu entschlüsseln ist. Andererseits kann eine Person eine elektronische Signatur generieren, die die zu sendende Nachricht und den personalisierten Schlüssel der Person kodiert, und mit der sich die Person durch Anhängen

der Signatur an die betreffende Nachricht eindeutig als Verfasser der Nachricht ausweist und somit authentisiert.

Bei symmetrischen Verschlüsselungsverfahren (z. B. dem „Data Encryption Standard" DES oder dem „International Data Encryption Algorithm" IDEA mit Schlüssellängen von 168 Bit und 128 Bit) besteht das Problem, daß aufgrund der Identität des Verschlüsselungs- und des Entschlüsselungsschlüssels eine Übergabe des Schlüssels an den Empfänger der verschlüsselten Nachricht erforderlich ist und dies einen Ansatzpunkt für kryptoanalytische Angriffe darstellt. Demgegenüber bietet ein asymmetrisches Verfahren (z. B. der RSA/PGP-Algorithmus mit einer Schlüssellänge von bis zu 2084 Bit) mit einem privaten Verschlüsselungsschlüssel für den sich authentisierenden Sender und einem öffentlichen Entschlüsselungsschlüssel für dessen Kommunikationspartner in der Regel zusätzliche Sicherheit. Denn der private Schlüssel kann selbst bei Kenntnis einer unverschlüsselten Nachricht, der entsprechenden verschlüsselten Nachricht und des öffentlichen Schlüssels mit den heute zur Verfügung stehenden Mitteln nicht errechnet werden.

Nachteilig ist bei asymmetrischen Signatur- und Verschlüsselungsverfahren jedoch, daß bei der Authentisierung zwar von einer empfangenen Nachricht über den öffentlichen Entschlüsselungsschlüssel eindeutig auf die Echtheit des privaten Verschlüsselungsschlüssels zurückgeschlossen werden kann, die eindeutige Zuordnung zwischen dem Verschlüsselungsschlüssel und der sendenden Person aber dadurch nicht unbedingt sichergestellt ist. Um einen Mißbrauch des privaten Schlüssels zu verhindern, wird dieses letzte Glied in der Authentisierungskette beispielsweise dadurch geschlossen, daß der private Schlüssel durch ein Kennwort (eine sogenannte „Passphrase" bzw. eine persönliche Identifikationsnummer PIN) geschützt wird, welches ausschließlich dem rechtmäßigen Besitzer des privaten Schlüssels bekannt ist.

Wegen der vielfachen Verwendung von Kennworten und PINs werden sie erfahrungsgemäß häufig von den Benutzern niedergeschrieben, woraus sich wiederum ein weiteres Angriffspotential zum Korrumpieren des Verschlüsselungs- bzw. Signatursystems ergibt. Erlangt eine unbefugte Person durch Diebstahl das legitimierende Kennwort eines Anderen, so kennt sie ohne weiteres dessen privaten Schlüssel und kann Nachrichten unter dessen Identität versenden, ohne daß dies für den Empfänger der Nachricht erkennbar wäre.

Eine Möglichkeit, die angesprochenen Probleme herkömmlicher Verschlüsselungsverfahren zu lösen zeigt WO 01/15378 A1 auf. Hierbei wird zunächst aus einer geeigneten biometrischen Eigenschaft einer Person, beispielsweise aus ihrem Fingerabdruck oder Irismuster, mittels geeigneter (Bildverarbeitungs-) Algorithmen ein Merkmalsvektor als Schlüssel extrahiert, der eine bestimmte Anzahl von charakterisierenden, numerischen Werten der biometrischen Eigenschaft repräsentiert. Eine Möglichkeit zur Extraktion geeigneter Merkmale einer biometrischen Eigenschaft offenbart beispielsweise WO 98/48538. Hierbei werden digitale Bilder der biometrischen Eigenschaft mittels der Fourier-Transformation in den (komplexwertigen) Ortsfrequenzraum transformiert und daraus durch die Interaktion mit bestimmten Filterfunktionen Merkmale bzw. Merkmalsvektoren errechnet.

Die WO 01/15378 A1 offenbart weiterhin, daß der aus der digitalisierten biometrischen Eigenschaft extrahierte Merkmalsvektor zur biometrischen Verschlüsselung eines Geheimnisses - beispielsweise des Kennwortes des persönlichen Schlüssels eines asymmetrischen Verschlüsselungsverfahrens – in einem Registrierungsprozeß verwendet wird. Bei der Benutzung des privaten Schlüssels kann sich der legitime Benutzer in einem Authentisie-

rungsprozeß durch erneutes Scannen der betreffenden biometrischen Eigenschaft, Extraktion eines gleichartigen Merkmalsvektors, Entschlüsselung des Kennwortes und Vergleich mit einem auf dem System gespeicherten Kennwort authentisieren. Für einen Kommunikationspartner ist dadurch eine eindeutige Zuordnung einer erhaltenen Nachricht zu dem tatsächlichen Absender im Rahmen der Fälschungssicherheit der biometrischen Eigenschaft des Senders gegeben. Nachteil dieses Verfahrens ist jedoch, daß aus der vollständigen Entschlüsselung des Geheimnisses bzw. dessen unverschlüsselter Speicherung ein erhebliches und für viele Anwendungen inakzeptables Angriffspotential erwächst.

Ein flexibler Einsatz derartiger biometrischer Systeme wird ermöglicht, indem eine berechtigte Person ihre biometrischen Daten in Form des biometrisch verschlüsselten Geheimnisses auf einem separaten digitalen Datenträger, beispielsweise einer Chip-Karte oder Smart-Card, mit sich führt. Damit ist die Authentisierung möglich, indem die Person das auf der Smart-Card gespeicherte biometrisch verschlüsselte Kennwort bzw. die PIN auf ein Terminal lädt, mit ihrer biometrischen Eigenschaft das Kennwort/die PIN entschlüsselt und dadurch Zugang zu ihrem privaten Schlüssel erhält.

In der Praxis möchte man jedoch bei den meisten Anwendungen der automatischen, elektronischen Authentisierung, insbesondere bei den wirtschaftlich hochrelevanten Bezahl- und Anmeldesystemen, aus Kosten- und Praktikabilitätsgründen auf die Verwendung von personalisierten Smart-Cards oder ähnlichen portablen digitalen Medien verzichten.

Demzufolge liegt der vorliegenden Erfindung die Aufgabe zugrunde, die sichere biometrische Authentisierung von Personen zu ermöglichen, ohne daß sicherheitsrelevante Daten unverschlüsselt vorliegen und ohne daß dazu

über die üblichen Ausweisdokumente einer Person hinausgehende zusätzliche personalisierte Medien benötigt werden.

Diese Aufgabe wird erfindungsgemäß durch Verfahren und Vorrichtungen mit den Merkmalen der unabhängigen Ansprüche gelöst. In davon abhängigen Ansprüchen sind vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung angegeben.

Die im folgenden beschriebenen erfindungsgemäßen Verfahren und Vorrichtungen bestehen prinzipiell aus zwei interagierenden Komponenten. Bevor eine Person die Möglichkeit hat, eine personalisierte Dienstleistung – z. B. bargeldloses Bezahlen durch biometrische Legitimierung, Abgeben einer authentisierten Erklärung, Beantragen begrenzter Ressourcen, etc. - durch biometrische Authentisierung in Anspruch zu nehmen, muß die Person der entsprechenden Infrastruktur bekannt sein, d. h. sie muß zunächst durch Aufnahme ihrer zur biometrischen Authentisierung verwendeten biometrischen Eigenschaft in einem Register registriert werden. Da sich die beiden Komponenten „Registrierung" und „Authentisierung" in allen Ausführungsformen der Erfindung jeweils entsprechen, werden korrespondierende Verfahrens- und Vorrichtungsmerkmale im folgenden parallel beschrieben.

Dementsprechend wird eine Person im Sinne der Erfindung registriert, indem zunächst ein diese Person identifizierendes Geheimnis, d. h. eine PIN oder ein Kennwort, bereitgestellt wird. Hierbei ist es einerseits möglich, das Geheimnis als individuelle Identifikationsnummer, insbesondere als zufällige Zeichenfolge, automatisch erzeugen zu lassen und der sich registrierenden Person vorzuenthalten. Andererseits kann die Person das Geheimnis auch selbst auswählen und zur Registrierung benennen.

Eine erfindungsgemäße Registrierung umfaßt desweiteren die digitale Aufnahme einer geeigneten biometrischen Eigenschaft der Person in Form eines digitalen Bildes. Für den genannten Zweck eignen sich beispielsweise die Fingerabdrücke, also die Papillarstruktur bestimmter Finger, die Irismuster der Augen oder das Spektralmuster einer Sprachäußerung der Person. Aus der digitalisierten biometrischen Eigenschaft wird anschließend ein biometrischer Schlüssel extrahiert, der das komplexe biometrische Muster mittels mathematischer oder signaltheoretischer Algorithmen auf eine Anzahl charakteristischer, numerischer Merkmale reduziert. Mit einem aus diesen Merkmalen gebildeten Merkmalsvektor wird das automatisch erzeugte oder frei gewählte Geheimnis im nächsten Schritt verschlüsselt und für die Person registriert. Ein derart biometrisch verschlüsseltes Geheimnis kann solange risikolos zwischen lokalen Registrierungs- bzw. Authentisierungsterminals und beispielsweise einer zentralen Datenbank übertragen werden, wie der biometrische Schlüssel bzw. die zugrundeliegende biometrische Eigenschaft ausschließlich der berechtigten Person bekannt ist und insbesondere nicht unverschlüsselt übertragen wird.

Zusätzlich zu dem biometrisch verschlüsselten Geheimnis wird im Zuge der erfindungsgemäßen Registrierung mittels einer sogenannten Hash-Funktion ein Referenz-Hash-Wert des Geheimnisses berechnet und ebenfalls für die Person registriert. Hash-Funktionen sind spezielle Einwegfunktionen $h(x)=y$, bei denen es praktisch unmöglich ist, aus einem gegebenen Funktionswert y das zugehörige Argument x zu rekonstruieren. Damit sie für kryptographische Zwecke nutzbar sind, müssen sie zudem „kollisionsfrei" sein, d. h. die Wahrscheinlichkeit, daß ein Paar von Argumenten x, x' auf denselben Hash-Wert $h(x)=h(x')$ abgebildet wird, muß (nahezu) 0 sein. Der Hash-Wert des Geheimnisses ist dem Geheimnis also eineindeutig zugeordnet, während das Geheimnis aus dem Hash-Wert nicht rekonstruiert werden kann. Aufgrund

dieser Eigenschaften können Hash-Werte ebenso risikolos über einen Kanal übertragen werden wie das biometrisch verschlüsselte Geheimnis, ohne die Entschlüsselung des Geheimnisses befürchten zu müssen.

Mit der sicheren Speicherung des biometrisch verschlüsselten Geheimnisses und des aus dem Geheimnis berechneten Referenz-Hash-Wertes ist die Registrierung der Person abgeschlossen.

Zur erfindungsgemäßen Authentisierung einer registrierten Person, beispielsweise an einem lokalen Authentisierungsterminal, das mit einer Datenbank verbunden ist, die alle registrierten Datensätze speichert, wird zunächst die gleiche biometrische Eigenschaft digitalisiert aufgenommen, die bereits bei der Registrierung zur Verschlüsselung verwendet wurde. Aus dieser wird mittels der bereits bei der Registrierung verwendeten Methoden ein Merkmalsvektor berechnet, das der Person zugehörige registrierte biometrische Geheimnis angefordert und mit dem Merkmalsvektor entschlüsselt. Von dem auf diese Weise entschlüsselten Geheimnis wird schließlich der Hash-Wert berechnet, wozu dieselbe Hash-Funktion verwendet wird, mit der bei der Registrierung bereits der Referenz-Hash-Wert berechnet wurde. Schließlich wird dieser Hash-Wert mit dem Referenz-Hash-Wert verglichen. Bei einer Identität der beiden Hash-Werte gilt die betreffende Person als korrekt authentisiert.

Die beschriebenen erfindungsgemäßen Registrierungs- und Authentisierungsverfahren ermöglichen vorteilhaft die zentrale Speicherung der Registrierungsdaten (des biometrisch verschlüsselten Geheimnisses und des Referenz-Hash-Wertes) und deren sichere Übertragung über Kommunikationsnetze zu und von lokalen Registrierungs- und Authentisierungsterminals, da Hash-Werte prinzipiell nicht entschlüsselbar sind und für die Entschlüsse-

lung des biometrisch verschlüsselten Geheimnisses der biometrische Schlüssel bekannt sein muß. Dieser Schlüssel - der Merkmalsvektor -, bzw. die ihm zugrundeliegende biometrische Eigenschaft wird jedoch an keiner Stelle unverschlüsselt abgelegt oder gespeichert und ist somit besonders vorteilhaft vor Angriffen von Dritten geschützt. Weder auf das Geheimnis noch auf die biometrische Eigenschaft kann aus den zwischen einem Terminal und dem zentralen Datenbank-Server übertragenen und somit potentiell abhörbaren Daten rückgeschlossen werden. Darüberhinaus wird die Authentisierung einer Person nur mittels ihrer biometrischen Eigenschaften und ohne die Verwendung spezieller, zusätzlicher digitaler Datenträger wie Chipkarten oder Smart-Cards ermöglicht.

Bei einer ersten vorteilhaften Ausführungsform wird die obige Erfindung eingesetzt, um Personen das bargeldlose Bezahlen von Waren und Dienstleistungen zu ermöglichen, ohne daß sie hierfür spezielle Chipkarten benötigen, wie z. B. Eurocheck- oder Kreditkarten. Hierzu werden erfindungsgemäße Registrierungsvorrichtungen zum Registrieren von Person, beispielsweise spezielle Registrierungsterminals in Bankfilialen oder bei Dienstleistungsanbietern eingerichtet. Zur Erzeugung eines individuellen Geheimnisses für eine Person ist in der Registrierungsvorrichtung ein Zufallsgenerator vorgesehen. Alternativ hierzu kann eine Person ihr Geheimnis auch selbst wählen. Hierzu wird dann eine geeignete Eingabeeinrichtung zum Eingeben des Geheimnisses benötigt, z. B. eine Tastatur oder ein Touch-Screen.

Ferner besitzt die Registrierungsvorrichtung eine Scan-Einrichtung, um eine geeignete biometrische Eigenschaft der Person aufnehmen und digitalisieren zu können. Eine Recheneinrichtung des lokalen Registrierungsterminals extrahiert aus der digitalisierten biometrischen Eigenschaft einen Merkmalsvek-

tor als biometrischen Schlüssel, mit dem das persönliche Geheimnis verschlüsselt wird.

Bei einer ersten Variante kann die Registrierung nur direkt bei einer zentralen Registrierungsstelle vorgenommen werden, die die registrierten Daten (das biometrisch verschlüsselte Geheimnis und den Referenz-Hash-Wert) ohne weitere Übertragung über Kommunikationsnetze an Ort und Stelle in einem Register oder Speicher ablegt.

Bei einer zweiten, für die Praxis relevanteren und deshalb besonders vorteilhaften Variante kann die Registrierung im Rahmen einer Client-Server-Architektur auch an einem lokalen Registrierungsterminal, z. B. in Bank-Filialen oder den diesen Service anbietenden Geschäften und Einrichtungen, vorgenommen werden. Derartige Registrierungsterminals besitzen eine Kommunikationsverbindung zu einer zentralen Speichereinrichtung - dem Datenbank-Server -, um die zu registrierenden Daten an den Server übertragen zu können. Prinzipiell kann das verschlüsselte Geheimnis und der Referenz-Hash-Wert in getrennten Registern abgelegt werden (die möglicherweise sogar in unterschiedlichen Datenbanken abgelegt sind) oder durch Ablegen in einem gemeinsamen Register auf dem Datenbank-Server registriert werden. Da das Geheimnis dabei einerseits biometrisch verschlüsselt und andererseits als Referenz-Hash-Wert übertragen wird, ist eine sichere Kommunikation zwischen dem lokalen Registrierungsterminal und dem zentralen Datenbank-Server sichergestellt. Mit der sicheren Speicherung ist die Registrierung der Person abgeschlossen.

Da zur Identifikation verwendbare biometrische Eigenschaften höchst komplexe und nicht notwendigerweise vollständig zeitinvariante Muster repräsentieren, die zudem bei jeder Verwendung leicht verändert aufgenommen

werden können, sind auch die aus ihnen extrahierten Merkmale (als Komponenten des Merkmalsvektors) in gewissen Grenzen variabel und deshalb oft nicht ohne weiteres zum Ver- und Entschlüsseln wichtiger Daten geeignet. Diese leichte Varianz der numerischen Merkmale kann jedoch in einer vorteilhaften Ausgestaltung der Erfindung ausgeglichen werden, indem das Geheimnis bei der Registrierung der Person an einem erfindungsgemäßen Registrierungsterminal vor der Verschlüsselung fehlertolerant kodiert wird, z. B. durch eine Hamming-Kodierung. Diese Kodierung fügt der Information des zu kodierenden Geheimnisses (den sogenannten Nachrichtenbits) redundante Information (sogenannte Kontrollbits) bei.

Im Falle einer fehlerhaften Entschlüsselung des kodierten, verschlüsselten Geheimnisses aufgrund leicht abweichender Merkmalsvektoren sind diese Fehler in den Kontrollbits kodiert und werden bei der Dekodierung des zu diesem Zeitpunkt zwar entschlüsselten aber noch kodierten Geheimnisses kompensiert. Der Grad der Fehlerkorrektur kann dabei über die verwendete Kodierung (bzw. die Redundanz) frei gewählt werden, so daß mittelbar die erlaubte Abweichung der beiden Aufnahmen der biometrischen Eigenschaft und der resultierenden Merkmalsvektoren eingestellt werden kann.

Bei dieser ersten Ausführungsform der Erfindung kann sich jede registrierte Person, beispielsweise zum bargeldlosen Bezahlen ohne Chip-Karte, an einem Authentisierungsterminal authentisieren, das z. B. in Geschäften als eigenständiger Geldautomat oder als Teil der vorhandenen Kassenanlage installiert sein kann. Dazu wird an dem Authentisierungsterminal durch eine entsprechende Aufnahme- und Digitalisierungseinrichtung zunächst die gleiche biometrische Eigenschaft digitalisiert aufgenommen, die bereits bei der Registrierung zur Verschlüsselung verwendet wurde. Das der Person zugehörige biometrisch verschlüsselte Geheimnis wird bei dem Datenbank-

Server angefordert und von einer speziellen Kommunikationseinrichtung des lokalen Authentisierungsterminals empfangen. Aus dieser wird dann von der Recheneinrichtung des Authentisierungsterminals mittels der bereits bei der Registrierung verwendeten Extraktionsalgorithmen ein Merkmalsvektor extrahiert, mit dem das vom Server empfangene biometrisch verschlüsselte Geheimnis lokal entschlüsselt wird und - falls es bei der Registrierung fehlertolerant kodiert wurde – zusätzlich fehlerkorrigierend dekodiert.

Schließlich berechnet die Recheneinrichtung des Authentisierungsterminals den Hash-Wert des entschlüsselten und dekodierten Geheimnisses, fordert den bei der Registrierung gebildeten Referenz-Hash-Wert vom Datenbank-Server an und vergleicht diese beiden Werte. Bei einer Identität der beiden Hash-Werte gilt die betreffende Person als korrekt authentisiert. Damit ist die Authentisierung der Person abgeschlossen, und die bargeldlose Bezahlung durch entsprechende Transaktionen des Authentisierungsterminals oder einer damit verbundenen Einrichtung kann durchgeführt werden.

In einer besonders vorteilhaften Ausgestaltung der Erfindung können Registrierungs- und Authentisierungsterminals in eine bauliche Einheit zusammengeführt werden und einige Komponenten gemeinsam benutzen, z. B. die Aufnahme- und Digitalisierungseinrichtung, die Recheneinrichtung oder auch die Kommunikationsmittel zum Datenaustausch mit dem Datenbank-Server.

Das beschriebene Authentisierungsverfahren ermöglicht vorteilhaft die Authentisierung einer Person nur mittels ihrer biometrischen Eigenschaften und ohne zusätzliche Hilfsmittel wie Chipkarten oder Smart-Cards. Die zentrale Speicherung und die damit zusammenhängende Übertragung der

Registrierungsdaten ist durch die biometrische Verschlüsselung und die Hash-Wert-Bildung ausreichend sicher, da Hash-Werte prinzipiell nicht entschlüsselbar sind und für die Entschlüsselung des biometrisch verschlüsselten Geheimnisses der biometrische Schlüssel bekannt sein muß. Dieser Schlüssel – der Merkmalsvektor - , bzw. die ihm zugrundeliegende biometrische Eigenschaft wird jedoch an keiner Stelle unverschlüsselt abgelegt oder gespeichert und ist somit besonders vorteilhaft vor Angriffen von Dritten geschützt. Weder auf das Geheimnis noch auf die biometrische Eigenschaft kann aus den zwischen einem Terminal und dem zentralen Datenbank-Server übertragenen und somit potentiell abhörbaren Daten rückgeschlossen werden.

Bei einer Abwandlung dieser ersten Ausführungsform wird nicht der Referenz-Hash-Wert vom Datenbank-Server an das Authentisierungsterminal übertragen, sondern es wird umgekehrt der vom Authentisierungsterminal berechnete Hash-Wert an den Datenbank-Server übertragen und der Vergleich des errechneten Hash-Wertes auf dem Datenbank-Server mit dem dort registrierten Referenz-Hash-Wert von einer dafür vorgesehenen Recheneinrichtung durchgeführt. Das Ergebnis des Vergleichs, also die Zulassung oder Verweigerung der von der Peson initiierten Transaktion, wird abschließend an die lokale Authentisierungseinrichtung gemeldet. Diese Abwandlung ermöglicht es, einen etwaigen Vergleich eines von der Authentisierungseinrichtung erzeugten Hash-Wertes mit einer Vielzahl von zentral gespeicherten Referenz-Hash-Werten von dem Server durchführen zu lassen. Durch das lediglich einmalige Senden des Hash-Wertes zum Datenbank-Server wird die Kommunikationslast gegenüber dem umgekehrten Fall reduziert, bei dem der Vergleich vom Authentisierungsterminal durch geführt wird und demzufolge alle Referenz-Hash-Werte vom zentralen Datenbank-Server angefordert werden müssen.

Gemäß einer zweiten bevorzugten Ausführungsform der Erfindung wird die Beantragung und Erteilung von zentral verwalteten und begrenzten Ressourcen automatisch kontrolliert. Dabei handelt es sich z. B. um staatliche oder kommunale Leistungen, wie Visa oder Sozialleistungen, oder auch um beschränkte Leistungen privater Dienstleister, beispielsweise im Mobilfunkbereich. Bei dieser zweiten Ausführungsform wird für eine zu vergebende Leistung eine zentrale Datenbank eingerichtet, in der die biometrischen Registrierungsdaten, also das biometrisch verschlüsselte Geheimnis und der zugehörige Referenz-Hash-Wert, aller Personen gespeichert werden, die die betreffende Leistung bereits mindestens einmal empfangen haben. Das zur Generierung dieser Registrierungsdaten benötigte Geheimnis wird gleichzeitig mit der ersten Leistungsbeantragung von der Registrierungseinrichtung als zufällige Zahlen- oder Zeichenkombination erzeugt und die Registrierungsdaten werden ebenfalls bei der ersten Leistungsbeantragung berechnet und in der zentralen Datenbank hinterlegt. Auch bei dieser Ausführungsform bietet sich ein Client-Server-Modell an, bei dem ein zentraler Datenbank-Server mit lokalen Authentisierungs- und Registrierungsterminals kommuniziert.

Falls nun eine Person eine Leistung beantragt, wird überprüft, ob sich die biometrischen Registrierungsdaten dieser Person bereits auf dem Datenbank-Server befinden. Falls dies nicht der Fall ist, wird ihre Registrierung - wie beschrieben - vorgenommen und die Leistung bewilligt. Andernfalls wird der Antrag der Person abgelehnt. Bei dieser Ausführungsform ist die Unterscheidung zwischen Registrierung und Authentisierung für eine Person nicht ersichtlich. Deshalb ist es in einer vorteilhaften Ausgestaltung sinnvoll, gemeinsame Registrierungs- und Authentisierungsterminals bzw. Clients vorzusehen.

Wenn eine Person an einem derartigen Terminal eine Leistung beantragt, wird zunächst ihre biometrische Eigenschaft digital aufgezeichnet und ein entsprechender Merkmalsvektor daraus extrahiert. Mit dem Merkmalsvektor werden alle registrierten, biometrisch verschlüsselten Geheimnisse nacheinander entschlüsselt, die entsprechenden Hash-Werte daraus gebildet und diese mit den den jeweiligen biometrisch verschlüsselten Geheimnissen zugeordneten Referenz-Hash-Werten verglichen. Dieser Prozeß wird solange durchgeführt, bis entweder eine Übereinstimmung des individuellen Hash-Wertes mit einem der Referenz-Hash-Werte festgestellt wird oder alle Referenz-Hash-Werte erfolglos überprüft wurden. Im letzteren Fall hat sich die Person, da sie die Leistung bisher noch nicht in Anspruch genommen hat, als berechtigt authentisiert und ihre Daten werden in die Datenbank übernommen und dadurch registriert. Die Authentisierung einer Peson ist bei dieser Ausführungsform also gerade dann möglich, wenn sie noch nicht registriert ist.

Da eine Übertragung von Hash-Werten prinzipiell sicher ist, kann der Vergleich der errechneten Hash-Werte mit den jeweiligen Referenz-Hash-Werten dann entweder von dem Terminal oder vom Server durchgeführt werden. Im zweitgenannten Fall werden die vom Terminal errechneten und an die Datenbank übertragenen Hash-Werte mit den entsprechenden Referenz-Hash-Werten verglichen und entweder werden alle Vergleichsergebnisse wieder an das Terminal gesendet oder es wird nur bei übereinstimmenden Werten eine Bestätigung an das Terminal geschickt.

Bei dem Einsatz von lokalen Terminals ist es aus Sicherheitsgründen sinnvoll, weder das unverschlüsselte digitale Bild der biometrischen Eigenschaft noch den Merkmalsvektor von einem Authentisierungs-/ Registrierungs-

terminal an den Datenbank-Server zu übertragen, sondern umgekehrt die bereits registrierten, biometrisch verschlüsselten Geheimnisse und deren zugehörige Referenz-Hash-Werte vom Server an das lokale Terminal zur dortigen Überprüfung zu schicken.

Um den dadurch entstehenden Datentransfer auf ein Minimum zu reduzieren, kann bei einer vorteilhaften Ausgestaltung dieser zweiten Ausführungsform von dem Datenbank-Server eine Vorauswahl der relevanten und potentiell zu berücksichtigenden Datensätze durch eine Vorsortierung dieser Datensätze anhand bestimmter charakteristischer und eindeutig reproduzierbarer Auswahlmerkmale der zugrundeliegenden biometrischen Eigenschaft vorgenommen werden.

So ist beispielsweise bei der Verwendung des Irismusters als biometrische Eigenschaft die Augenfarbe in der Regel eindeutig reproduzierbar und einer von wenigen Auswahlklassen (z. B. blau, braun, grün) zweifelsfrei zuzuordnen. Gemäß der verschiedenen Werte dieses Auswahlmerkmals – die nicht notwendigerweise numerisch sein müssen, sondern, wie z. B. bei der Augenfarbe, auch symbolisch sein können – werden die Datensätze durch Abspeichern (Registrieren) des Auswahlmerkmals – entweder in einem separaten Register oder in einem gemeinsamen Register zusammen mit den Registrierungsdaten - in Auswahlklassen eingeteilt und dadurch vorsortiert.

Bei einer Authentisierung wird dann der Wert des betreffenden Auswahlmerkmals aus der digitalisierten biometrischen Eigenschaft ermittelt und an den Datenbank-Server geschickt. Dieser wählt daraufhin zur Überprüfung nur diejenigen Datensätze aus, deren assoziiertes Auswahlmerkmal dem ermittelten Wert entspricht, und sendet nur diese an das Terminal zur Überprüfung zurück.

Auf diese Weise wird die Auswahl der für eine Überprüfung relevanten Datensätze vorteilhaft eingeschränkt und der Vorgang beschleunigt. Natürlich können bei weiteren Varianten die Datensätze auch anhand mehrerer numerischer oder symbolischer Auswahlmerkmale vorsortiert bzw. strukturiert und die jeweils relevanten Datensätze dadurch weiter eingeschränkt werden. Sie können beispielsweise in Form einer hierarchischen Datenstruktur organisiert werden, die in einer relationalen Datenbank gemeinsam mit weiteren personenbezogenen Daten abgelegt sind. Prinzipiell können die Auswahlmerkmale auch mit einigen der numerischen Merkmale des zur Entschlüsselung verwendeten Merkmalsvektors übereinstimmen.

Die Vorsortierung relevanter Datensätze auf dem Datenbank-Server anhand bestimmter charakteristischer und eindeutig reproduzierbarer Auswahlmerkmale der zugrundeliegenden biometrischen Eigenschaft ist im gleichen Maße sinnvoll, um bei der vorbeschriebenen ersten Ausführungsform das Auffinden der registrierten Daten einer sich authentisierenden Person zu ermögliche bzw. zu beschleunigen.

In manchen Fällen, insbesondere bei kommunalen oder ortsgebundenen Leistungen, kann es auch sinnvoll sein bei dieser zweiten Ausführungsform vom Client-Server-Modell abzusehen und das gemeinsame Registrierungs- und Authentisierungsterminal mit einer integrierten Datenbank auszustatten, um dadurch jeglichen Datentransfer zu unterbinden und dadurch eine hohe Sicherheit herzustellen.

Prinzipiell können neben der beschriebenen Speicherung der Registrierungsdaten in einer zentralen Datenbank viele weitere Speichertechniken eingesetzt werden. Eine dritte erfindungsgemäße Ausführungsform sieht

beispielsweise die Speicherung durch Aufbringen der Daten auf Dokumenten und sonstigen Schriftstücken vor. Dieses Prinzip der Registrierung und Authentisierung wird vorteilhaft zur biometrischen Identifikation von Personen eingesetzt, beispielsweise bei Grenz- oder sonstigen Ausweiskontrollen.

Dazu wird das biometrisch verschlüsselte Geheimnis und der zugehörige Referenz-Hash-Wert nicht von einem zentralen Datenbank-Server gespeichert, sondert auf ein Ausweisdokument, beispielsweise auf den Personalausweis, Reisepaß, Führerschein oder Dienstausweis einer Person, gedruckt oder gestanzt oder auf eine beliebige andere Weise hinterlegt. Derartige Dokumente werden typischerweise von zentralen staatlichen oder auch staatlicherseits dazu legitimierten privaten Stellen ausgefertigt. Entsprechende Registrierungseinrichtungen zumindest zum Aufnehmen und Digitalisieren der benötigten biometrischen Eigenschaft können z. B. an den diese Dokumente ausgebenden Stellen eingerichtet werden. Eine Kommunikation mit einer zentralen Stelle ist bei dieser Ausführungsform nicht notwendig, da die biometrischen Daten nicht zentral gespeichert werden sondern eine Person allein durch das Aufbringen der Daten auf die entsprechenden Dokumente registriert wird.

Dementsprechend kann die spätere Authentisierung einer derart registrierten Person an einem lokalen Authentisierungsterminal erfolgen, ohne daß eine Datenfernübertragung bzw. die hierfür benötigten technischen Voraussetzungen bereitgestellt werden müssen. Die Authentisierung erfolgt bei dieser Ausführungsform also nur durch die biometrische Eigenschaft der Person und ein übliches Ausweisdokument, das die Person ohnehin mit sich führt, bzw. sogar dazu verpflicht ist es mitzuführen. Zusätzliche digitale Da-

tenträger wie z. B. Chip-Karten, Smart-Cards, oder optische Medien werden zur Authentisierung nicht benötigt.

Ein entsprechendes Authentisierungsterminal besitzt Einrichtungen zum Aufnehmen und Digitalisieren der biometrischen Eigenschaft und zum Lesen und Erkennen der Registrierungsdaten von dem Dokument. Eine Recheneinrichtung wird dann das biometrisch verschlüsselte Geheimnis entschlüsseln, dessen Hash-Wert berechnen und mit dem von dem Dokument gelesenen Referenz-Hash-Wert vergleichen. Bei Übereinstimmung hat sich die Person als die auf dem Dokument genannten Person ausgewiesen.

Auf die gleiche Art und Weise können andere wichtige Dokumente, z. B. Wertdokumente wie Urkunden, persönliche Dokumente, Aktien und dergleichen, durch irreversibles Aufbringen der Registrierungsdaten einer oder mehrerer Personen personalisiert werden und deren authentisierte Besitzerschaft von einer Authentisierungseinrichtung zweifelsfrei nachgewiesen werden.

Die Vorteile dieser Ausführungsform liegen darin, daß individuelle biometrische Daten fälschungssicher und maschinenlesbar auf Ausweis- und Wertdokumenten hinterlegt werden können und diese Personen dadurch zweifelsfrei und auf einfache Weise identifizierbar sind. Aus den prinzipiell öffentlich zugänglichen, auf dem Dokument angebrachten Daten kann weder auf das im Referenz-Hash-Wert enthaltene Geheimnis noch auf die biometrische Information oder den Schlüssel rückgeschlossen werden.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung verschiedener erfindungsgemäßer Ausführungsbeispiele

und Ausführungsalternativen. Es wird auf die Figuren verwiesen, die zeigen:

Figur 1 ein Ausführungsbeispiel eines erfindungsgemäßen Verfahrens zum bargeld- und kartenlosen Bezahlen,

Figur 2 ein Ausführungsbeispiel eines erfindungsgemäßen Systems zur Kontrolle von Mehrfachbeantragungen begrenzter Leistungen und

Figur 3 ein Ausführungsbeispiel eines erfindungsgemäßen Systems zum Identifizieren von Personen.

Figur 1 illustriert schematisch den Informationsfluß bei einem erfindungsgemäßen Registrierungs- und Authentisierungsverfahren, realisiert durch ein Client-Server-System, zum bargeldlosen und kartenlosen Bezahlen durch biometrische Authentisierung. Bei diesem Ausführungsbeispiel kommunizieren zwei Clients, die Registrierungsvorrichtung RV und die Authentisierungsvorrichtung AV, mit einem Datenbank-Server DB. Eine Person kann sich an dem System über die Registrierungsvorrichtung RV durch Abgabe einer biometrischen Eigenschaft BM1, hier ihres Fingerabdrucks, anmelden. Daraus werden Registrierungsdaten RH, VG für die Person berechnet, die auf dem zentralen Datenbank-Server DB gespeichert werden. Bei jeder Authentisierung der Person werden die Registrierungsdaten RH, VG von dem Datenbank-Server DB an das lokale Authentisierungsterminal AV zur Überprüfung übertragen.

Bei der Registrierung der Person wird zunächst ihr Fingerabdruck aufgenommen und liegt in Form des digitalen Bildes BM1 zur Merkmalsextraktion ME bereit. Durch die Merkmalsextraktion ME werden bestimmte, mög-

lichst individuelle Charakteristika der biometrischen Eigenschaft BM1 durch numerische Werte ausgedrückt, die als Merkmalsvektor MV1 die diskriminative Information der biometrischen Eigenschaft BM1 repräsentieren. Der Merkmalsvektor MV1 wird im weiteren Verlauf des Registrierungsprozesses als Schlüssel einer biometrischen Verschlüsselung V verwendet.

Der Merkmalsvektor MV1 soll die biometrische Eigenschaft BM1 einerseits hinreichend genau beschreiben und muß andererseits weitestgehend reproduzierbar sein, d. h. eine erneute Merkmalsextraktion ME muß zumindest ähnliche Merkmalswerte erzeugen. Deshalb werden Algorithmen zur Merkmalsextraktion ME verwendet, die entsprechend robuste Merkmale erzeugen (z. B. Filterantworten, Spektralkoeffizienten, Momente, Verteilungsparameter, Formfaktoren, etc.) und die bezüglich der obligatorischen natürlichen Abweichungen einer biometrischen Quelle eine möglichst geringe (Interklassen-) Varianz besitzen und bei unterschiedlichen biometrischen Quellen gleichzeitig eine möglichst hohe (Intraklassen-) Varianz aufweisen und demzufolge hinreichend diskriminativ sind.

Neben dem Merkmalsvektor MV1 wird als zweites personenindividuelles Datum mittels eines Zufallsgenerators ein Geheimnis G generiert. Dieses Geheimnis bleibt selbst der Person, der es zugeordnet ist, unbekannt. Deshalb kann es, im Gegensatz zu herkömmlichen PINs und Kennworten, aus einer komplexen, nicht ohne weiteres merkbaren Zeichenfolge bestehen.

Da die nachfolgende biometrische Verschlüsselung V des Geheimnisses G mit dem Merkmalsvektor MV1 aufgrund der natürlichen Unschärfe biometrischer Eigenschaften BM1 beim Authentisierungsprozeß nicht eindeutig rückgängig gemacht werden kann, wird das Geheimnis G vor der Verschlüsselung V durch eine fehlertolerante Kodierung K in ein kodiertes Geheimnis

KG1 transformiert. Das kodierte Geheimnis KG1 unterscheidet sich vom unkodierten Geheimnis G durch eine bestimmte Anzahl zusätzlicher redundanter Bits, die biometriebedingte Entschlüsselungsfehler in bestimmtem Umfang zu korrigieren vermögen.

Die auf dem Datenbank-Server DB zu speichernden Registrierungsdaten VG, RH werden schließlich von dem Registrierungsterminal RV durch eine Verschlüsselung V des kodierten Geheimnisses KG1 in ein verschlüsseltes Geheimnis VG und durch die Bildung H eines Referenz-Hash-Wertes RH aus dem unverschlüsselten Geheimnis G erzeugt. Mit der Übertragung R der Registrierungsdaten VG, RH an den Datenbank-Server DB und der dortigen Speicherung der Daten VG, RH ist der Registrierungsprozeß abgeschlossen.

Bei der Authentisierung der Person mittels des Authentisierungsterminals AV wird der Fingerabdruck der Person erneut aufgenommen und liegt nun in Form eines digitalen Bildes BM2 vor, das sich aufgrund vielerlei technischer und bio-physiologischer Einflüsse von dem bei der Registrierung aufgenommenen Bild BM1≈BM2 leicht unterscheidet. Die Gründe hierfür liegen in der grundsätzlichen Unschärfe biometrischer Messungen, sowie in veränderlichen Aufnahmebedingungen. Dementsprechend liefert die anschließende Merkmalsextraktion ME auch einen Merkmalsvektor MV2, der leicht von dem zum Verschlüsseln verwendeten Merkmalsvektor MV1≈MV2 abweicht. Aus diesem Grunde weicht nach der Entschlüsselung E des verschlüsselten Geheimnisses VG auch das Ergebnis, also das zwar entschlüsselte aber immer noch kodierte Geheimnis KG2, von seinem Pendant, dem bei der Registrierung generierten kodierten Geheimnis KG1≈KG2, leicht ab. Dieser leichte Abweichungsfehler wird nun im nächsten Schritt, dem fehlerkorrigierenden Dekodieren D des kodierten Geheimnisses KG2, korrigiert und führt zu dem nunmehr unverschlüsselten Geheimnis G. Mit Hilfe der Kodierung K bzw.

der Dekodierung D wird also die obligatorische biometrische Meßunschärfe biometrischer Merkmal BM1, BM2 kompensiert, sofern diese in einem bei der Kodierung einstellbaren Rahmen bleibt. Abweichungen, die über die Korrekturkapazität der fehlertoleranten (De-) Kodierung K/D hinausgehen, also insbesondere die grundsätzlich unterschiedlichen biometrischen Eigenschaften verschiedener Personen, werden nicht kompensiert und führen zum Scheitern der Authentisierung.

Das auf diese Weise entschlüsselte Geheimnis G wird sofort wieder durch die Hash-Wert-Bildung H in den Hash-Wert HG transformiert. Dieser wird abschließend anhand eines Vergleiches C mit dem von dem Datenbank-Server DB angeforderten Referenz-Hash-Wert RH verglichen und das Ergebnis ER des Vergleichs C beispielsweise über einen Bildschirm mitgeteilt bzw. intern weiter verarbeitet. Falls die beiden Hash-Werte RH und HG identisch sind, hat sich die betreffende Person korrekt authentisiert. Bei unterschiedlichen Werten bleibt ihr der elektronische Zugang zu einem Konto zum bargeldlosen Bezahlen verwehrt.

Dieses Ausführungsbeispiel realisiert somit die sichere Registrierung und Authentisierung einer Person an einem System zum elektronischen Bezahlen nur aufgrund persönlicher biometrischer Daten BM1, BM2. Ein weiteres digitales Speichermedium, z. B. eine Chip-Karte wird hierfür nicht benötigt. Der Transfer von Daten zum/vom Datenbank-Server DB ist ausreichend sicher, da einerseits dem Referenz-Hash-Wert RH aufgrund der Einweg-Eigenschaft der verwendeten Hash-Funktion H das Geheimnis G nicht zu entnehmen ist. Andererseits ist das verschlüsselte Geheimnis VG nur bei Kenntnis der biometrischen Eigenschaft BM1, BM2 zu entschlüsseln, die jedoch an keiner Stelle und zu keinem Zeitpunkt auf einem Permanentspeicher niedergelegt wird.

Figur 2 zeigt ein weiteres Ausführungsbeispiel der Erfindung. Das dort abgebildete System kontrolliert die Beantragung und Gewährung von Leistungen und Ressourcen, die einer Person nur einmal zustehen und verhindert die unberechtigte Doppelbeantragung derartiger Leistungen.

Da die Trennung zwischen der Registrierung und der Authentisierung bei diesem Ausführungsbeispiel in der bisher beschriebenen Art und Weise nicht zweckmäßig ist, wird ein kombiniertes Registrierungs- und Authentisierungsterminal RV/AV verwendet, das mit einem zentralen Datenbank-Server DB kommuniziert und über die jeweiligen Transfereinrichtungen TE die Registrierungsdaten VG, RH austauscht.

Eine Person beantragt zunächst eine Leistung durch die Abgabe einer biometrischen Eigenschaft BM, die von einer Digitalisierungseinrichtung DE des Terminals RV/AV aufgenommen und in Form eines digitalen Bildes der Recheneinrichtung RE zur Extraktion des zugehörigen Merkmalsvektors zur Verfügung gestellt wird.

Um die Berechtigung der Person festzustellen, muß zunächst überprüft werden, ob für diese Person bereits Registrierungsdaten VG, RH auf dem Datenbank-Server DB gespeichert sind. Falls dies der Fall ist, hat die Person die betreffende Leistung bereits einmal empfangen und eine weitere Inanspruchnahme ist nicht möglich. Andernfalls wird die Leistung gewährt und die Registrierungsdaten VG, RH der Person werden von der Recheneinrichtung RE generiert und von dem Datenbank-Server DB gespeichert bzw. registriert.

Zur Überprüfung des Vorhandenseins von Registrierungsdaten VG, RH für die betreffende Person müssen die auf dem Datenbank-Server DB vorhandenen verschlüsselten Geheimnisse VG der Reihe nach mit dem Merkmalsvektor der Person entschlüsselt werden, aus dem entschlüsselten Geheimnis G ein Hash-Wert berechnet und dieser Hash-Wert mit dem dem verschlüsselten Geheimnis VG zugeordneten Referenz-Hash-Wert RH verglichen werden.

Damit dieser Prozeß nicht für alle Registrierungsdaten VG, RH durchgeführt werden muß, sind die Registrierungsdaten VG, RH auf dem Datenbank-Server DB anhand des Wertes eines eindeutig zugeordneten Auswahlmerkmals AM vorsortiert. Das Auswahlmerkmal AM ist ein charakteristisches, numerisches oder symbolisches Merkmal der biometrischen Eigenschaft BM und ergibt sich eindeutig aus dieser. Bei der Leistungsbeantragung der Person muß also nur die Auswahl A derjenigen Registrierungsdaten VG, RH überprüft werden, deren zugeordnetes Auswahlmerkmal AM mit dem von der Recheneinrichtung RE berechneten Auswahlmerkmal AM der Person übereinstimmen. Für den Fall, daß als biometrische Eigenschaft BM das Irismuster einer Person verwendet wird, kann als (symbolisches) Auswahlmerkmal AM beispielsweise die daraus eindeutig berechenbare Augenfarbe der Person verwendet werden.

Nachdem für eine Person das Auswahlmerkmal AM aus deren biometrischer Eigenschaft BM extrahiert wurde, wird es über die Transfereinrichtung TE des Terminals RV/AV an den Datenbank-Server DB gesendet und von dessen Transfereinrichtung TE empfangen. Das Auswahlmerkmal AM kann dabei im Hinblick auf Datenschutz und Datenintegrität risikolos unverschlüsselt bleiben, da es keinerlei eindeutig zuzuordnende Information über die betreffende Person repräsentiert.

Die Recheneinrichtung RE des Datenbank-Servers DB wählt anschließend aus allen dort gespeicherten Datensätzen DS die Auswahl A derjenigen Datensätze DS aus, deren Auswahlmerkmal AM den gleichen Wert aufweist, wie das von dem Terminal RV/AV empfangene Auswahlmerkmal AM. Aus den Datensätzen DS dieser Auswahl A werden anschließend die entsprechenden Registrierungsdaten VG, RH (nicht jedoch das Auswahlmerkmal AM, da es nicht weiter benötigt wird) entnommen und über die Transfereinrichtungen TE an das Terminal RV/AV zur weiteren Überprüfung geschickt.

Die Recheneinrichtung RE des Terminals RV/AV entschlüsselt alle von dem Datenbank-Server DB empfangenen verschlüsselten Geheimnisse VG der Auswahl A mit dem bereits berechneten Merkmalsvektor, berechnet von dem daraus resultierenden Geheimnis G den Hash-Wert und vergleicht diesen mit dem dem jeweiligen verschlüsselten Geheimnis VG zugeordneten Referenz-Hash-Wert RH. Sobald hierbei eine Übereinstimmung zwischen einem Hash-Wert und einem Referenz-Hash-Wert RH festgestellt wird, wird der Authentisierungsprozeß abgebrochen und die beantragte Leistung verweigert, da sie offensichtlich bereits einmal empfangen wurde. Falls nach Überprüfung aller Registrierungsdaten VG, RH der Auswahl A keine derartige Übereinstimmung aufgetreten ist, wird die von der Person beantragte Leistung bewilligt. Das jeweilige Ergebnis ER der Überprüfung wird auf einer Anzeigeeinrichtung AE des Terminals RV/AV bekannt gegeben.

Im Anschluß an die Bewilligung einer Leistung muß die Person registriert werden, damit eine zweite, unberechtigte Bewilligung der gleichen Leistung ausgeschlossen wird. Hierzu wird von einem Zufallsgenerator ZG ein Geheimnis G als zufällige Zeichenfolge generiert, dieses von der Recheneinrichtung RE des Terminals RV/AV mit dem Merkmalsvektor biometrisch ver-

schlüsselt und ein Referenz-Hash-Wert RH des Geheimnisses G errechnet. Zusammen mit dem bereits bei in der Authentisierungsphase errechneten Auswahlmerkmal AM wird schließlich das verschlüsselte Geheimnis VG und der Referenz-Hash-Wert RH zur Registrierung an den Datenbank-Server DB geschickt. Dieser neue Datensatz DS (VG, RH, AM) wird dort entsprechend dem Wert seines Auswahlmerkmals AM abgelegt und somit registriert.

In Abwandlungen dieses zweiten Ausführungsbeispiels ist es generell auch möglich, auf die gleiche Weise Leistungen zu verwalten, die eine Person mehrfach, aber in begrenzter Anzahl empfangen darf. Hierbei ist zumindest die Anzahl der Leistungsempfänge zusätzlich zu registrieren.

Figur 3 zeigt ein drittes Ausführungsbeispiel der Erfindung zur biometrischen Unterstützung von Personenidentifikationen bei Ausweiskontrollen beispielsweise im Grenz- oder Flugverkehr.

Die Registrierung wird an einem entsprechenden Registrierungsterminal RV vorgenommen, indem die biometrische Eigenschaft BM1 der Person mittels einer Digitalisierungseinrichtung DE, z. B. einer hochauflösenden CCD-Kamera, aufgezeichnet wird. Das dabei erzeugte digitale Bild sowie eine durch einen Zufallsgenerator ZG erzeugte Zufallszahl - das Geheimnis G - werden an die Recheneinrichtung RE des Registrierungsterminals RV weitergegeben. Diese berechnet aus der biometrischen Eigenschaft BM1 einen Merkmalsvektor, mit dem als biometrischem Schlüssel das Geheimnis G verschlüsselt wird. Es entsteht das zur Registrierung benötigte verschlüsselte Geheimnis VG. Ebenso bildet die Recheneinrichtung RE einen Hash-Wert des Geheimnisses G, der als Referenz-Hash-Wert RH zur Registrierung verwendet wird.

Der eigentliche Registrierungsprozeß wird von der Prägeeinrichtung PE des Registrierungsterminals RV durchgeführt, indem das verschlüsselte Geheimnis VG und der Referenz-Hash-Wert RH in maschinenlesbarer Form auf ein Ausweisdokument ID aufgebracht werden. Dies kann vorzugsweise durch Auf- oder Einprägen geschehen, aber auch durch Stanzen oder verschiedene Drucktechniken, sowie durch Speicherung auf einem Speicherchip, falls er in das Ausweisdokument ID integriert ist und sich nicht auf einem zusätzlichen digitalen Datenträger befindet.

Obwohl die Registrierungsdaten VG, RH auf dem Ausweisdokument ID sichtbar oder zumindest auslesbar und dadurch prinzipiell öffentlich sind, ist durch die biometrische Verschlüsselung bzw. die Hash-Wert-Bildung eine Entschlüsselung des Geheimnisses G oder der biometrischen Eigenschaft BM1 ausgeschlossen.

Die Authentisierung der Person, also der biometrische Nachweis, daß die Person, die das Ausweisdokument ID mit sich führt, mit der dort genannten Person identisch ist, wird an einem Authentisierungsterminal AV durchgeführt, das an entsprechenden Grenz- und Kontrollstellen eingerichtet ist oder vom Kontrollpersonal portabel mitgeführt werden kann.

Das Authentisierungsterminal verfügt über eine Leseeinrichtung LE, die die auf dem Ausweisdokument ID hinterlegten maschinenlesbaren Registrierungsdaten RH, VG scannt und in von der Recheneinrichtung RE weiterverarbeitbare digitale Daten VG, RH umsetzt. Die Recheneinrichtung RE erhält zusätzlich die digitalisierte biometrische Eigenschaft BM2, deren mögliche marginale Abweichung von der zur Registrierung verwendeten biometri-

schen Eigenschaft BM1 prinzipiell durch fehlerkorrigierende (De-) Kodierung ausgeglichen werden kann.

Die Recheneinrichtung RE des Authentisierungsterminals AV extrahiert einen Merkmalsvektor aus der digitalisierten biometrischen Eigenschaft BM2, entschlüsselt mit diesem das verschlüsselte Geheimnis VG und errechnet daraus einen Hash-Wert zum Vergleichen mit dem Referenz-Hash-Wert RH. Das Ergebnis ER des Vergleichs, also die Bestätigung oder Bezweiflung der Identität der ausweisführenden Person, wird der kontrollierenden Person abschließend auf einer Anzeigeeinrichtung mitgeteilt.

Sowohl die Recheneinheit RE des Registrierungsterminals RV als auch die Recheneinheit RE des Authentisierungsterminals AV können, in diesem wie in allen anderen Ausführungsbeispielen, spezialisierte Co-Prozessoren zum Extrahieren der Merkmalsvektoren und/oder zum Verschlüsseln des Geheimnisses G bzw. zur Hash-Wert-Bildung besitzen.

Dieses Ausführungsbeispiel ermöglicht die einfache und effektive Kodierung biometrischer Information und deren Verwendung auf Ausweisdokumenten ID und anderen Wertpapieren einer Person. Dabei werden neben dem Ausweisdokument ID keine zusätzlichen digitalen Datenträger, z. B. Chip-Karten, benötigt. Trotz des quasi öffentlichen Zugangs der Registrierungsdaten RH, VG kann weder auf das in ihnen enthaltene Geheimnis G noch auf die biometrische Information rückgeschlossen werden.

Patentansprüche

1. Verfahren zum Authentisieren einer registrierten Person, umfassend die folgenden Schritte:

- Ermitteln (ME) eines biometrischen Schlüssels (MV2) aus einer biometrischen Eigenschaft (BM; BM2) der Person,
- Entschlüsseln (E) eines verschlüsselten Geheimnisses (VG) mit dem ermittelten biometrischen Schlüssel (MV2),

gekennzeichnet durch die folgenden weiteren Schritte:

- Berechnen (H) eines Hash-Wertes (HG) des entschlüsselten Geheimnisses (G),
- Vergleichen (C) des berechneten Hash-Wertes (HG) mit einem für die registrierte Person individuellen Referenz-Hash-Wert (RH).

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß der Schritt des Ermittelns (ME) des biometrischen Schlüssels (MV2) das Extrahieren (E) numerischer Merkmale aus der biometrischen Eigenschaft (BM; BM2) der Person umfaßt.

3. Verfahren nach Anspruch 1 oder 2, **gekennzeichnet durch** den weiteren Schritt des fehlertoleranten Dekodierens (D) des entschlüsselten Geheimnisses (KG2) vor dem Schritt des Berechnens (H) des Hash-Wertes (HG).

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, daß das Verfahren von einer lokalen Authentisierungsvorrichtung (AV) durchgeführt wird, wobei das verschlüsselte Geheimnis (VG) von einer zentralen Speichereinrichtung (DB) an die lokale Authentisierungsvorrichtung (AV) übermittelt wird und die Schritte des Entschlüsselns (E) und des Be-

rechnens (H) von der lokalen Authentisierungsvorrichtung (AV) durchgeführt werden.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, daß der Referenz-Hash-Wert (RH) von der zentralen Speichereinrichtung (DB) an die lokale Authentisierungsvorrichtung (AV) übermittelt wird und der Schritt des Vergleichens (C) von der lokalen Authentisierungsvorrichtung (AV) durchgeführt wird.

6. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, daß der berechnete Hash-Wert (HG) an die zentrale Speichereinrichtung (DB) übermittelt wird und der Schritt des Vergleichens (C) von der zentralen Speichereinrichtung (DB) durchgeführt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, daß eine Auswahl (A) von unterschiedlichen verschlüsselten Geheimnissen (VG) von jeweils verschiedenen Personen mit dem für die Person ermittelten biometrischen Schlüssel (MV2) entschlüsselt werden, zu jedem entschlüsselten Geheimnis (G) ein Hash-Wert (HG) berechnet wird und jeder dieser Hash-Werte (HG) mit einem individuellen Referenz-Hash-Wert (RH) der jeweils verschiedenen Personen verglichen wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet**, daß die Auswahl (A) von unterschiedlichen verschlüsselten Geheimnissen (VG) anhand zumindest eines charakteristischen Auswahlmerkmals (AM) aus einer Vielzahl von verschlüsselten Geheimnissen (VG) ausgewählt wird.

9. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** daß das verschlüsselte Geheimnis (VG) und der Referenz-Hash-Wert (RH) einem Dokument (ID) der Person entnommen werden.

10. Verfahren zum Registrieren einer Person, umfassend die folgenden Schritte:

- Bereitstellen eines Geheimnisses (G),
- Ermitteln (ME) eines biometrischen Schlüssels (MV1) aus einer biometrischen Eigenschaft (BM; BM1) der Person,
- Verschlüsseln (V) des Geheimnisses (G) mit dem ermittelten biometrischen Schlüssel (MV1),
- Registrieren (R) des verschlüsselten Geheimnisses (VG) für die Person,

gekennzeichnet durch die folgenden weiteren Schritte:

- Berechnen (H) eines Referenz-Hash-Wertes (RH) des unverschlüsselten Geheimnisses (G),
- Registrieren (R) des Referenz-Hash-Wertes (RH) für die Person.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet,** daß der Schritt des Ermittelns (ME) des biometrischen Schlüssels (MV1) das Extrahieren numerischer Merkmale aus der biometrischen Eigenschaft (BM; BM1) der Person umfaßt.

12. Verfahren nach Anspruch 10 oder 11, **gekennzeichnet durch** den weiteren Schritt des fehlertoleranten Kodierens (K) des Geheimnisses (G) vor dem Schritt des Verschlüsseln (V).

13. Verfahren nach einem der Ansprüchen 10 bis 12, **dadurch gekennzeichnet,** daß das Geheimnis (G) in Form einer individuellen Identifikationsnummer der Person bereitgestellt wird.

14. Verfahren nach einem der Ansprüchen 10 bis 13, **dadurch gekennzeichnet,** das das Geheimnis (G) in Form einer individuell erzeugten Zufallszahl bereitgestellt wird.

15. Verfahren nach einem der Ansprüche 10 bis 14, **dadurch gekennzeichnet,** daß sowohl der Schritt des Registrierens (R) des verschlüsselten Geheimnisses (VG) als auch der Schritt des Registrierens (R) des Referenz-Hash-Wertes (RH) durch das Speichern des verschlüsselten Geheimnisses (VG) und des Referenz-Hash-Wertes (RH) in einer zentralen Speichereinrichtung (DB) erfolgt.

16. Verfahren nach Anspruch 15, **dadurch gekennzeichnet,** daß das Verfahren von einer lokalen Registrierungsvorrichtung (RV) durchgeführt wird, wobei das verschlüsselte Geheimnis (VG) und der Referenz-Hash-Wert (RH) zur Registrierung (R) an die zentrale Speichereinrichtung (DB) übertragen werden.

17. Verfahren nach Anspruche 16, **dadurch gekennzeichnet,** daß zumindest ein charakteristisches Auswahlmerkmal (AM) aus der biometrischen Eigenschaft (BM; BM1) der Person extrahiert und durch Speichern in der zentralen Speichereinrichtung (DB) registriert wird.

18. Verfahren nach einem der Ansprüche 10 bis 14, **dadurch gekennzeichnet,** daß sowohl der Schritt des Registrierens (R) des verschlüsselten Geheimnisses (VG) als auch der Schritt des Registrierens (R) des Referenz-Hash-Wertes (RH) durch das Hinterlegen des verschlüsselten Geheimnisses (VG) und des Referenz-Hash-Wertes (RH) auf einem Dokument (ID) der Person erfolgt.

19. Verfahren Anspruch 18, **dadurch gekennzeichnet**, daß das Dokument (ID) ein Ausweisdokument ist.

20. Registrierungs- und Authentisierungsverfahren, **dadurch gekennzeichnet**, daß das Registrieren mit einem Verfahren nach einem der Ansprüche 10 bis 19 und das Authentisieren mit einem Verfahren nach einem der Ansprüche 1 bis 9 durchgeführt wird.

21. Vorrichtung zum Authentisieren (AV) einer registrierten Person, umfassend eine Recheneinrichtung (RE) zum Ermitteln eines biometrischen Schlüssels (MV2) aus einer biometrischen Eigenschaft (BM; BM2) der Person und zum Entschlüsseln (E) eines für diese Person registrierten, verschlüsselten Geheimnisses (VG) mit dem ermittelten biometrischen Schlüssel (MV2), **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, einen Hash-Wert (HG) des entschlüsselten Geheimnisses (G) zum Vergleich (C) mit einem für die Person individuellen Referenz-Hash-Wert (RH) zu berechnen.

22. Vorrichtung nach Anspruch 21, **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, numerische Merkmale aus der biometrischen Eigenschaft (BM; BM2) als biometrischen Schlüssel zu extrahieren.

23. Vorrichtung nach Anspruch 21 oder 22, **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, das entschlüsselte Geheimnis (G) vor dem Berechnen (H) des Hash-Wertes (HG) fehlertolerant zu dekodieren.

24. Vorrichtung nach einem der Ansprüche 21 bis 23, **dadurch gekennzeichnet**, daß sie eine Transfereinrichtung (TE) zum Empfangen des ver-

schlüsselten Geheimnisses (VG) von einer zentralen Speichereinrichtung (DB) besitzt.

25. Vorrichtung nach Anspruch 24, **dadurch gekennzeichnet**, daß die Transfereinrichtung (TE) auch den Referenz-Hash-Wert (RH) von einer zentralen Speichereinrichtung (DB) empfängt und die Recheneinrichtung (RE) eingerichtet ist, den berechneten Hash-Wert (HG) mit dem Referenz-Hash-Wert (RH) zu vergleichen.

26. Vorrichtung nach Anspruch 24, **dadurch gekennzeichnet**, daß die Transfereinrichtung (TE) eingerichtet ist, den berechneten Hash-Wert (HG) an die zentrale Speichereinrichtung (DB) zu versenden zum dortigen Vergleich (C) mit dem Referenz-Hash-Wert (RH).

27. Vorrichtung nach einem der Ansprüche 24 bis 26, **dadurch gekennzeichnet**, daß

die Transfereinrichtung (TE) eingerichtet ist, eine Auswahl (A) von verschlüsselten Geheimnissen (VG) jeweils verschiedener Personen von der zentralen Speichereinrichtung (DB) zu empfangen, und

die Recheneinrichtung (RE) eingerichtet ist, die Auswahl (A) von verschlüsselten Geheimnissen (VG) mit dem für die Person ermittelten biometrischen Schlüssel (MV2) zu entschlüsseln und zu jedem entschlüsselten Geheimnis (G) einen Hash-Wert (HG) zum Vergleich (C) mit einem individuellen Referenz-Hash-Wert (RH) der jeweils verschiedenen Personen zu berechnen.

28. Vorrichtung nach Anspruche 27, **dadurch gekennzeichnet**, daß die Transfereinrichtung (TE) eingerichtet ist, die berechneten Hash-Werte (HG)

an die zentrale Speichereinrichtung (DB) zum dortigen Vergleich (C) mit dem Referenz-Hash-Wert (RH) zu versenden.

29. Vorrichtung nach Anspruche 27, **dadurch gekennzeichnet**, daß die Transfereinrichtung (TE) eingerichtet ist, die individuellen Referenz-Hash-Werte (RH) der jeweils verschiedenen Personen von der zentralen Speichereinrichtung (DB) zu empfangen, und die Recheneinrichtung (RE) eingerichtet ist, die Hash-Werte (HG) der entschlüsselten Geheimnisse (G) mit den individuellen Referenz-Hash-Werten (RH) der jeweils verschiedenen Personen zu vergleichen.

30. Vorrichtung nach einem der Ansprüche 27 bis 29, **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, zumindest ein charakteristisches Auswahlmerkmal (AM) der biometrischen Eigenschaft (BM, BM2) der Person zu ermitteln, und die Transfereinrichtung (TE) eingerichtet ist, das zumindest eine charakteristische Auswahlmerkmal (AM) zum Auswählen der Auswahl (A) von verschlüsselten Geheimnissen (VG) aus einer Vielzahl von verschlüsselten Geheimnissen (VG) an die zentrale Speichereinrichtung (DB) zu versenden.

31. Vorrichtung nach Anspruch 30, **dadurch gekennzeichnet**, daß die zentrale Speichereinrichtung (DB) eingerichtet ist, die Auswahl (A) von verschlüsselten Geheimnissen (VG) anhand des von der Transfereinrichtung (TE) empfangenen, zumindest einen charakteristischen Auswahlmerkmals (AM) aus einer Vielzahl von Geheimnissen auszuwählen.

32. Vorrichtung nach einem der Ansprüche 21 bis 25, **dadurch gekennzeichnet**, daß die Transfereinrichtung (TE) eingerichtet ist, das verschlüsselte

Geheimnis (VG) und den Referenz-Hash-Wert (RH) einem Dokument (ID) der Person zu entnehmen.

33. Vorrichtung zum Registrieren (RV) einer Person, umfassend eine Einrichtung (ZG) zum Bereitstellen eines Geheimnisses, eine Recheneinrichtung (RE) zum Ermitteln (ME) eines biometrischen Schlüssels (MV1) aus einer biometrischen Eigenschaft (BM; BM1) der Person und zum Verschlüsseln (V) des bereitgestellten Geheimnisses (G) mit dem ermittelten biometrischen Schlüssel (MV1) und ein erstes Register zum Registrieren (R) des verschlüsselten Geheimnisses (VG), **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, einen Referenz-Hash-Wert (RH) des unverschlüsselten Geheimnisses (G) zu berechnen, und weiter gekennzeichnet durch ein zweites Register zum Registrieren (R) des Referenz-Hash-Wertes (RH).

34. Vorrichtung nach Anspruch 33, **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, numerische Merkmale aus der biometrischen Eigenschaft (BM; BM1) als biometrischen Schlüssel (MV1) zu extrahieren.

35. Vorrichtung nach Anspruch 33 oder 34, **dadurch gekennzeichnet**, daß die Recheneinrichtung (RE) eingerichtet ist, das unverschlüsselte Geheimnis (G) vor dem Verschlüsseln (V) fehlertolerant zu kodieren.

36. Vorrichtung nach einem der Ansprüche 33 bis 35, **dadurch gekennzeichnet**, daß die Einrichtung (ZG) zum Bereitstellen des Geheimnisses (G) eingerichtet ist, das Geheimnis in Form einer individuellen Identifikationsnummer der Person bereitzustellen.

37. Vorrichtung nach einem der Ansprüche 33 bis 36, **dadurch gekennzeichnet,** daß die Einrichtung (VG) zum Bereitstellen des Geheimnisses (G) das Geheimnis in Form einer individuell erzeugten Zufallszahl bereitstellt.

38. Vorrichtung nach einem der Ansprüche 33 bis 37, **dadurch gekennzeichnet,** daß sowohl das erste Register als auch das zweite Register auf einer zentralen Speichereinrichtung (DB) gespeichert ist.

39. Vorrichtung nach einem der Ansprüche 33 bis 38, **dadurch gekennzeichnet,** daß die Recheneinrichtung (RE) eingerichtet ist, zumindest ein charakteristisches Auswahlmerkmal (AM) der biometrischen Eigenschaft (BM; BM1) der Person zu ermitteln, und die Vorrichtung ein drittes Register zum Registrieren dieses zumindest einen charakteristischen Auswahlmerkmals (AM) umfaßt.

40. Vorrichtung nach Anspruch 39 mit Anspruch 38, **dadurch gekennzeichnet,** daß das dritte Register auf der zentralen Speichereinrichtung (DB) gespeichert ist.

41. Vorrichtung nach einem der Ansprüche 33 bis 37, **dadurch gekennzeichnet,** daß die Speichereinrichtung (DB) ein Dokument (ID) der Person ist.

42. System zum Registrieren und Authentisieren von Personen, umfassend eine Vorrichtung (AV) zum Authentisieren nach einem der Ansprüche 21 bis 26 und eine Vorrichtung (RV) zum Registrieren nach einem der Ansprüche 33 bis 38.

43. System zum Registrieren und Authentisieren von Personen, umfassend eine Vorrichtung (AV) zum Authentisieren nach einem der Ansprüche 27 bis 31 und eine Vorrichtung (RV) zum Registrieren nach Anspruch 39 oder 40.

44. System zum Registrieren und Authentisieren von Personen, umfassend eine Vorrichtung (AV) zum Authentisieren nach Anspruch 32 und eine Vorrichtung (RV) zum Registrieren nach Anspruch 41.

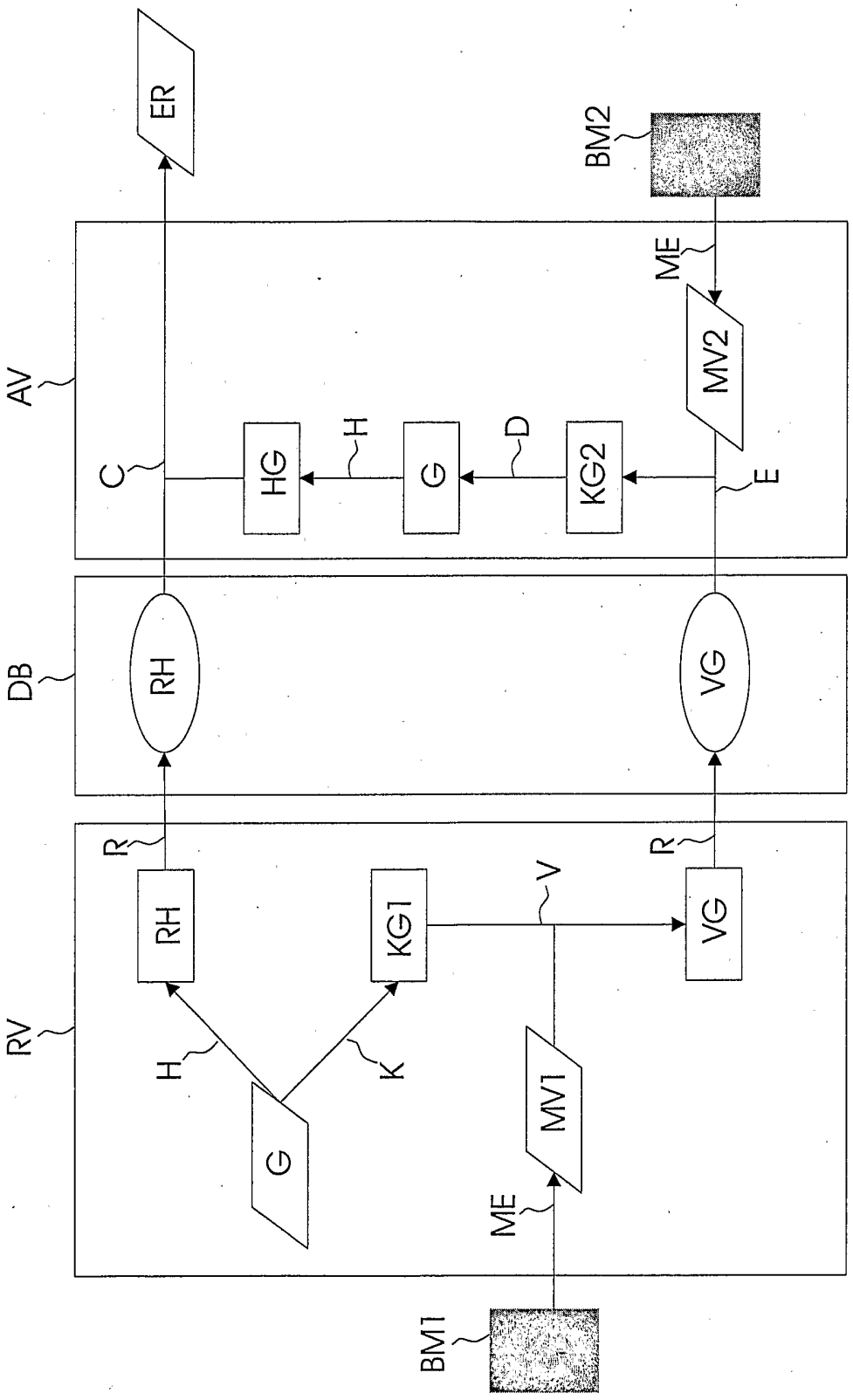

ER
BM2
ME
MV2
AV
C
HG
H
G
D
KG2
E
DB
RH
VG
R
R
RH
KG1
V
VG
RV
H
K
G
MV1
ME
BM1

Fig. 1

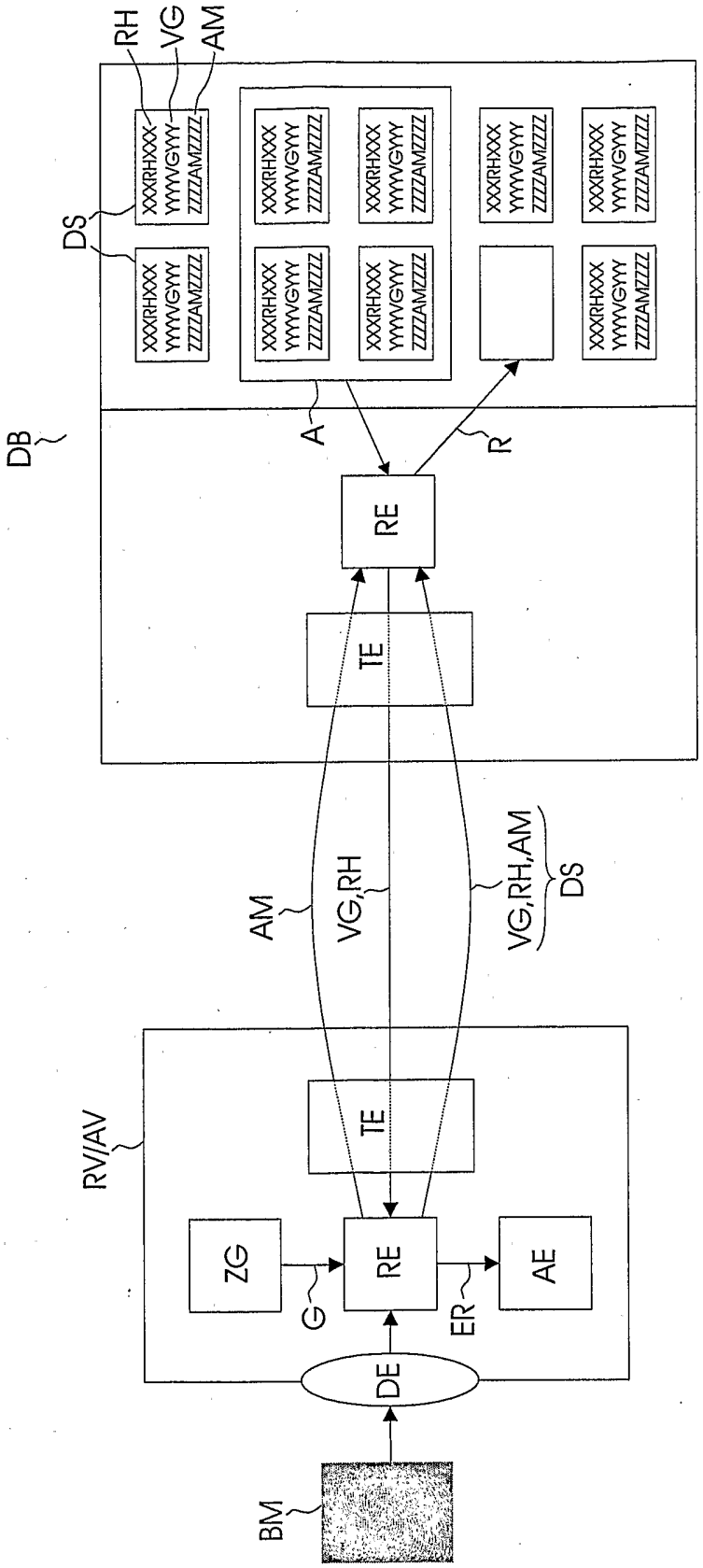

RH
VG
AM
DS
XXXRHXXX
YYYVGYYY
ZZZZAMZZZZ
DB
A
R
RE
TE
AM
VG,RH
VG,RH,AM
DS
RV/AV
TE
ZG
RE
AE
G
ER
DE
BM

Fig. 2

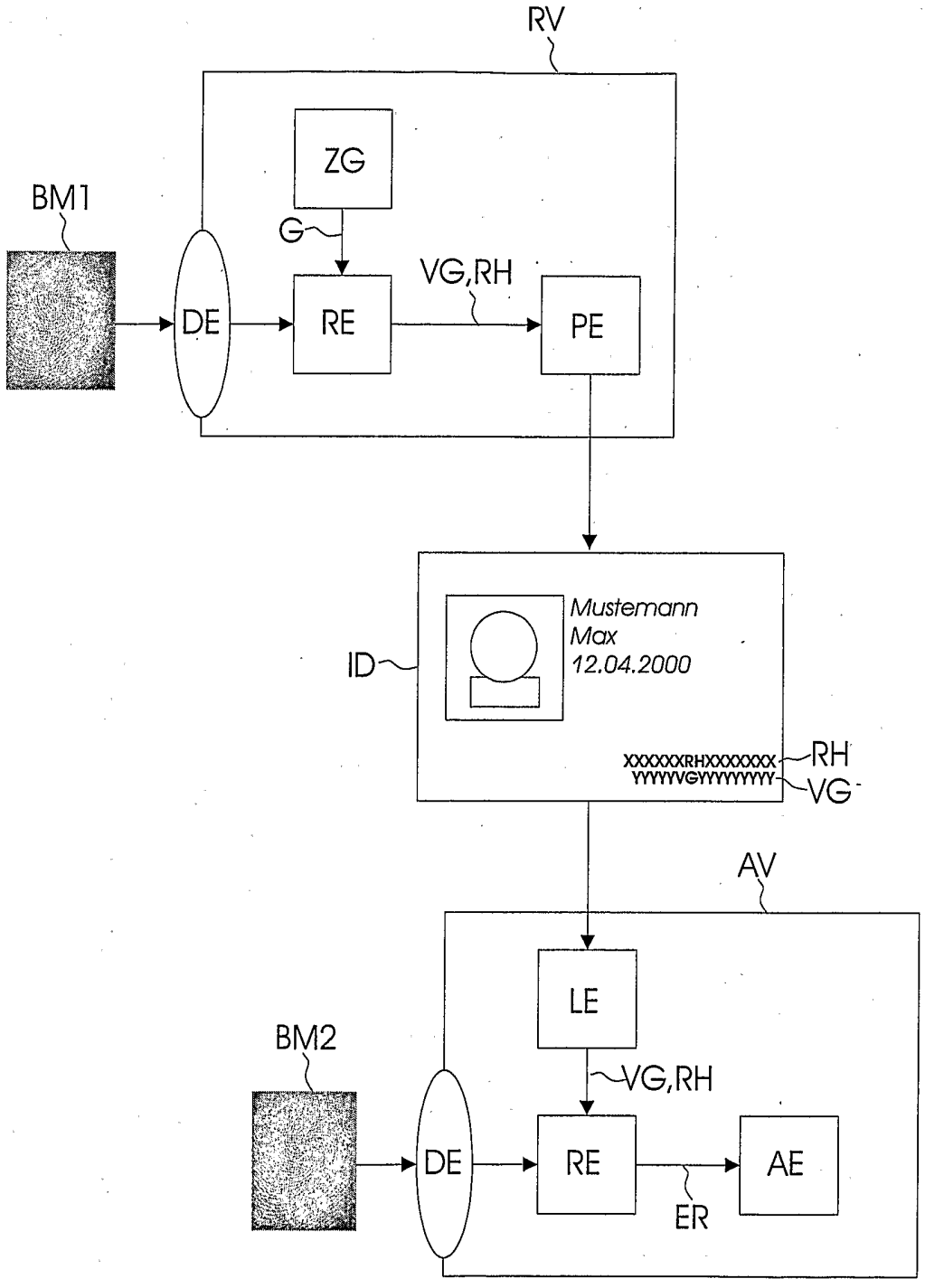

RV
ZG
BM1
G
VG,RH
DE
RE
PE
ID
Mustermann
Max
12.04.2000
XXXXXXRHXXXXXXX
YYYYYVGYYYYYYYY
RH
VG
AV
LE
BM2
VG,RH
DE
RE
AE
ER

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/000173

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G07F G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/48538 A (MYTEC TECHNOLOGIES INC) 29 October 1998 (1998-10-29) abstract; claims 1,5-7,12; figures 1,3 page 4, paragraph 3 - page 5, paragraph 2 page 20, paragraph 2	1-44
X	WO 03/100730 A (NCIPHER, CORPORATION, LTD) 4 December 2003 (2003-12-04) abstract; claims; figures 3a,3b,6,7 page 6, paragraph 1 - page 7, paragraph 1	1-44
X	US 6 038 315 A (STRAIT ET AL) 14 March 2000 (2000-03-14) abstract; figures 1,2 column 3, line 6 - column 4, line 24	1-44

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 May 2005	18/05/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/000173

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/36566 A (KONINKLIJKE PHILIPS ELECTRONICS N.V) 22 June 2000 (2000-06-22) abstract; figures	1,10,21, 33,42-44
A	WO 01/15378 A (CIFRO GESELLSCHAFT FUER SICHERHEIT IN DATENNETZEN MBH IM GRUENDUNGSZEN) 1 March 2001 (2001-03-01) cited in the application abstract; claims 1,2; figures 1,5,7	1,10,21, 33,42-44

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/000173

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9848538 A	29-10-1998	CA 2203212 A1	21-10-1998
		CA 2209438 A1	21-10-1998
		AU 7020898 A	13-11-1998
		CA 2286749 A1	29-10-1998
		WO 9848538 A2	29-10-1998
		DE 19882328 T0	13-07-2000
		GB 2339518 A ,B	26-01-2000
		US 6219794 B1	17-04-2001
WO 03100730 A	04-12-2003	US 2003219121 A1	27-11-2003
		AU 2003238596 A1	12-12-2003
		WO 03100730 A1	04-12-2003
US 6038315 A	14-03-2000	NONE	
WO 0036566 A	22-06-2000	US 2002124176 A1	05-09-2002
		CN 1297553 A	30-05-2001
		WO 0036566 A1	22-06-2000
		EP 1057145 A1	06-12-2000
		JP 2002532997 T	02-10-2002
		TW 472217 B	11-01-2002
WO 0115378 A	01-03-2001	DE 19940341 A1	01-03-2001
		AU 7272400 A	19-03-2001
		CN 1382332 A	27-11-2002
		WO 0115378 A1	01-03-2001
		EP 1214812 A1	19-06-2002
		JP 2003507964 T	25-02-2003
		ZA 200201303 A	18-10-2002

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/000173

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07C G07F G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 98/48538 A (MYTEC TECHNOLOGIES INC) 29. Oktober 1998 (1998-10-29) Zusammenfassung; Ansprüche 1,5-7,12; Abbildungen 1,3 Seite 4, Absatz 3 - Seite 5, Absatz 2 Seite 20, Absatz 2	1-44
X	WO 03/100730 A (NCIPHER, CORPORATION, LTD) 4. Dezember 2003 (2003-12-04) Zusammenfassung; Ansprüche; Abbildungen 3a,3b,6,7 Seite 6, Absatz 1 - Seite 7, Absatz 1	1-44
X	US 6 038 315 A (STRAIT ET AL) 14. März 2000 (2000-03-14) Zusammenfassung; Abbildungen 1,2 Spalte 3, Zeile 6 - Spalte 4, Zeile 24	1-44

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
4. Mai 2005	18/05/2005

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Formblatt PCT/ISA/210 (Blatt 2) (Januar 2004)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 00/36566 A (KONINKLIJKE PHILIPS ELECTRONICS N.V) 22. Juni 2000 (2000-06-22) Zusammenfassung; Abbildungen	1,10,21, 33,42-44
A	WO 01/15378 A (CIFRO GESELLSCHAFT FUER SICHERHEIT IN DATENNETZEN MBH IM GRUENDUNGSZEN) 1. März 2001 (2001-03-01) in der Anmeldung erwähnt Zusammenfassung; Ansprüche 1,2; Abbildungen 1,5,7	1,10,21, 33,42-44

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2005/000173

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9848538	A	29-10-1998	CA	2203212 A1	21-10-1998
			CA	2209438 A1	21-10-1998
			AU	7020898 A	13-11-1998
			CA	2286749 A1	29-10-1998
			WO	9848538 A2	29-10-1998
			DE	19882328 T0	13-07-2000
			GB	2339518 A ,B	26-01-2000
			US	6219794 B1	17-04-2001
WO 03100730	A	04-12-2003	US	2003219121 A1	27-11-2003
			AU	2003238596 A1	12-12-2003
			WO	03100730 A1	04-12-2003
US 6038315	A	14-03-2000	KEINE		
WO 0036566	A	22-06-2000	US	2002124176 A1	05-09-2002
			CN	1297553 A	30-05-2001
			WO	0036566 A1	22-06-2000
			EP	1057145 A1	06-12-2000
			JP	2002532997 T	02-10-2002
			TW	472217 B	11-01-2002
WO 0115378	A	01-03-2001	DE	19940341 A1	01-03-2001
			AU	7272400 A	19-03-2001
			CN	1382332 A	27-11-2002
			WO	0115378 A1	01-03-2001
			EP	1214812 A1	19-06-2002
			JP	2003507964 T	25-02-2003
			ZA	200201303 A	18-10-2002