(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
15. April 2010 (15.04.2010)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2010/040162 A1

(51) Internationale Patentklassifikation:
G07C 9/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/AT2009/000388

(22) Internationales Anmeldedatum:
7. Oktober 2009 (07.10.2009)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 1570/2008 7. Oktober 2008 (07.10.2008) AT

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **NANOIDENT TECHNOLOGIES AG** [AT/AT]; Untere Donaulände 21-25, A-4020 Linz (AT).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **SCHRÖTER, Klaus** [DE/DE]; Pommersche Strasse 11, 10707 Berlin (DE). **CHANG, Ho B.** [CA/CH]; Auf Oberrüthi 13, CH-6048 (CH).

(74) Anwalt: **ANWÄLTE BURGER UND PARTNER RECHTSANWALT GMBH**; Rosenauerweg 16, A-4580 Windischgarsten (AT).

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

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

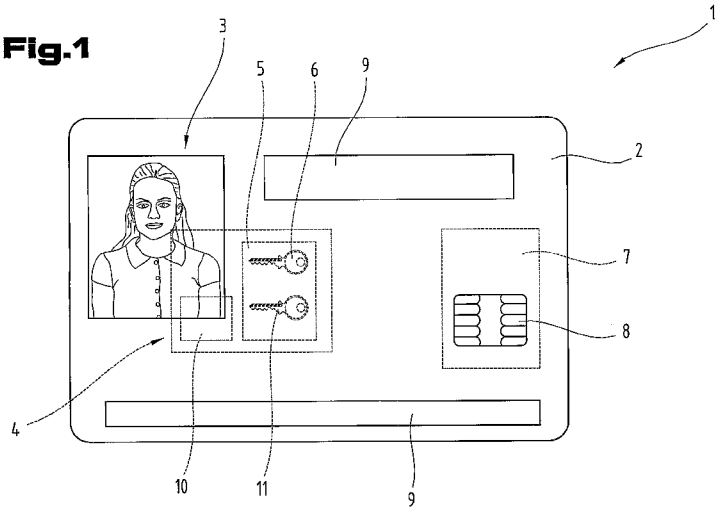
Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) Title: IDENTIFICATION FEATURE

(54) Bezeichnung : IDENTIFIKATIONSMERKMAL

Fig.1



(57) Abstract: The invention relates to an identification feature (1) for authenticated person identification, comprising a carrier layer (2), an authentication device (4) having a storage means (5) designed as a non-volatile, rewritable semiconductor memory, a person-related feature (3), a communication device (7) having a communication connection (8), wherein in the storage means (5) a first electronic key (6) is deposited, which is linked to the person-related feature (3). The invention further relates to an identification feature for authenticated person identification, comprising an electronic data record, in which an electronic image of a person-related feature (3) and a first electronic key (6) are deposited, wherein the first electronic key (6) is linked to the person-related feature (3). The invention further relates to a method for identifying and authenticating a person using an identification feature.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2010/040162 A1

Die Erfindung betrifft ein Identifikationsmerkmal (1) zur authentifizierten Personenidentifikation, umfassend eine Trägerlage (2), eine Authentifizierungseinrichtung (4) mit einem Speichermittel (5), das als nicht-flüchtiger, wiederbeschreibbarer Halbleiterspeicher ausgebildet ist, ein personenbezogenes Merkmal (3), eine Kommunikationseinrichtung (7) mit einem Kommunikationsanschluss (8), wobei im Speichermittel (5) ein erster elektronischer Schlüssel (6) hinterlegt ist, welcher mit dem personenbezogenen Merkmal (3) verknüpft ist. Die Erfindung betrifft ferner ein Identifikationsmerkmal zur authentifizierten Personenidentifikation, umfassend einen elektronischen Datensatz, in dem ein elektronisches Abbild eines personenbezogenen Merkmals (3) und ein erster elektronischer Schlüssel (6) hinterlegt sind, wobei der erste elektronische Schlüssel (6) mit dem personenbezogenen Merkmal (3) verknüpft ist. Des Weiteren betrifft die Erfindung ein Verfahren zur Identifikation und Authentifikation einer Person mit einem Identifikationsmerkmal.

Identifikationsmerkmal

Die Erfindung betrifft ein persönliches Identifikationsmerkmal zur authentifizierten Personenidentifikation umfassend eine Trägerlage, eine Authentifizierungseinrichtung mit einem Speichermittel, das als nicht-flüchtiger, wiederbeschreibbarer Halbleiterspeicher ausgebildet ist, ein personenbezogenes Merkmal und eine Kommunikationseinrichtung mit einem Kommunikationsanschluss. Des Weiteren betrifft die Erfindung ein Identifikationsmerkmal zur authentifizierten Personenidentifikation umfassend einen elektronischen Datensatz, in dem ein elektronisches Abbild eines personenbezogenen Merkmals und ein erster elektronischer Schlüssel hinterlegt sind. Die Erfindung betrifft ferner ein Verfahren zur Identifikation und Authentifikation einer Person mit einem Identifikationsmerkmal.

Identifikationsmerkmale zur Identifikation einer Person sind allgemein bekannt und basieren zumeist auf einer optischen Prüfung der Übereinstimmung von Merkmalen einer Person, welche das Identifikationsmerkmal bei sich trägt bzw. einer überprüfenden Autorität präsentiert, mit Personendaten, welche im Identifikationsmerkmal hinterlegt sind. Diese Überprüfung der Übereinstimmung wird zumeist von einer Person durchgeführt, es ist jedoch auch bekannt, dass ein Identifikationsmerkmal zumindest teilweise durch ein automatisiertes System ausgelesen und verarbeitet werden kann. In der optisch visuellen Vergleichsprüfung durch eine Person liegt nun auch ein wesentlicher Nachteil der bekannten Informationsmerkmale, da es einem potentiellen Angreifer möglich ist, ein derartiges Merkmal zu verfälschen und somit ein gültiges Identifikationsmerkmal dahingehend zu manipulieren, dass es von einer anderen Person in missbräuchlicher Absicht benutzt werden kann. Des Weiteren hängen die Bewertungskriterien der Übereinstimmung von der teilweise subjektiven Einschätzung einer Person ab und sind insbesondere auch von der jeweiligen Tagesverfassung abhängig. Eine objektive Prüfung kann daher nicht sichergestellt werden.

Der folgenden Erfindung liegt nun die Aufgabe zugrunde, ein Identifikationsmerkmal zu schaffen, mit dem die Identität und Authentizität einer Person eindeutig sichergestellt werden kann.

Die Aufgabe der Erfindung der Erfindung wird dadurch gelöst, dass im Speichermittel des Identifikationsmerkmals ein erster elektronischer Schlüssel hinterlegt ist, der mit dem personenbezogenen Merkmal verknüpft ist.

Diese Ausbildung stellt nun in besonders vorteilhafter Weise sicher, dass ein personenbezogenes Merkmal weitestgehend vor einer Manipulation geschützt ist, da ein potentieller Angreifer sowohl das personenbezogene Merkmal, als auch die Verknüpfung und ggf. den ersten elektronischen Schlüssel manipulieren müsste, um Erfolg zu haben. Da der erste elektronische Schlüssel im Speichermittel und somit in der Authentifizierungseinrichtung hinterlegt ist, müsste ein potentieller Angreifer somit die Authentifizierungseinrichtung manipulieren, was trotz eines außerordentlich hohen Aufwands, nur geringe Erfolgsaussichten bringt.

Der erste elektronische Schlüssel kann bspw. durch einen pseudozufälligen Code gebildet sein, bspw. als alphanumerischer Code. Derartige Schlüssel lassen sich mit einem Algorithmus definiert erzeugen, wirken aber auf einen Betrachter wie eine zufällige Anordnungen von Zeichen. Insbesondere lassen sich so eindeutige elektronische Schlüssel ausbilden, die sich auch durch eine so genannte brute-force Attacke nicht umgehen lassen. Insbesondere würde der notwendige Aufwand zur Prüfung aller möglichen Kombinationen eines derartigen Schlüssels, die technischen und zeitlichen Möglichkeiten eines Angreifers übersteigen.

Durch die Verknüpfung des personenbezogenen Merkmals mit dem elektronischen Schlüssel ist eine Merkmalskombination geschaffen, die die Vorteile eines elektronischen Schlüssels im Bezug auf die Fälschungssicherheit, mit einem personenbezogenen Merkmal kombiniert. Somit wird das Identifikationsmerkmal derart vorteilhaft ausgebildet, dass eine deutliche Steigerung der Sicherheit einer eindeutigen Personenidentifikation bzw. Authentifikation erreicht wird.

Eine weitere Ausbildung des Identifikationsmerkmals löst die Aufgabe der Erfindung auch mit einem elektronischen Datensatz, wobei auch hier der erste elektronische Schlüssel mit dem personenbezogenen Merkmal verknüpft ist. Der Vorteil dieser weiteren Ausbildung liegt nun insbesondere darin, dass ein elektronischer Datensatz von einem automatisierten Erfassungssystem, welches bevorzugt eine Datenverarbeitungseinrichtung umfasst, direkt verarbeitet werden kann. Insbesondere ist zur Durchführung einer Identitätsprüfung eine Erfassungs-

vorrichtung zur Herstellung einer Kommunikationsverbindung mit dem Identifikationsmerkmal nicht erforderlich. Ein weiterer Vorteil dieser Ausbildung liegt ferner darin, dass das Identifikationsmerkmal auf datentechnischem Weg verbreitet und verarbeitet werden kann. Insbesondere stehen somit eine Vielzahl bekannter und weit verbreiteter Einrichtungen zur Verfügung, um eine Identifikation und/oder Authentifikation einer Person, basierend auf dem hinterlegten personenbezogenen Merkmal durchführen zu können.

Da es aus gesetzlichen bzw. rechtsstaatlichen Grundsätzen erforderlich sein kann, dass eine Person ein Identifikationsmerkmal mit sich trägt, ist gemäß einer Weiterbildung die Trägerlage als Ausweisdokument ausgebildet. Das Identifikationsmerkmal kann nun beispielsweise als Lenkberechtigung für ein Fahrzeug ausgebildet sein, es ist jedoch auch eine Ausbildung als Reisedokument zum grenzüberschreitenden Reisen möglich. Im Hinblick auf eine Vernetzung der Kontrollstellen zur Erhöhung einer Sicherheit der Personenidentifikation, kann das Identifikationsmerkmal auch derart ausgebildet sein, dass es von einer automatisierten Erfassungseinrichtung verarbeitet werden kann. Insbesondere kann das personenbezogene Merkmal den Anforderungen an eine maschinenlesbare Erfassung genügen. Beispielsweise ist es für eine optische Erfassung eines personenbezogenen Merkmals möglich, dieses derart auszubilden, dass Merkmalskomponenten in unterschiedlichen Spektralkomponenten aufgebracht sind. Somit ist eine Überprüfung des personenbezogenen Merkmals beispielsweise nicht nur im optisch sichtbaren Bereich möglich, sondern es lassen sich auch Merkmalskomponenten im nicht sichtbaren Bereich ausbilden und zum Vergleich erfassen, beispielsweise im IR- bzw. UV-Bereich. Die Ausbildung als maschinenlesbares Ausweisdokument hat den weiteren Vorteil, dass die Prüfung des personenbezogenen Merkmals stets nach den gleichen reproduzierbaren Kriterien erfolgt und somit ein möglicher Unsicherheitsfaktor durch individuelle Bewertungskriterien einer Begutachtungsperson ausgeschlossen werden.

Von besonderem Vorteil ist auch die Weiterbildung, nach der die Trägerlage als scheckkartenartige Datenkarte ausgebildet ist, wobei eine Ausbildung als Chipkarte besonders bevorzugt wird. Die anspruchsgemäße Weiterbildung hat den besonderen Vorteil, dass eine Scheckkarte besonders kompakt ausgebildet ist und somit von einer Person permanent mitgeführt werden kann, ohne dass es aufgrund der Größe und/oder Formgebung zu einer Beeinträchtigung der Bewegungsfreiheit kommt. Insbesondere hat die Ausbildung als Scheckkarte

den Vorteil, dass diese in einem Gegenstand untergebracht sein kann, der von einer Person üblicherweise immer mitgeführt wird, beispielsweise in einer Geldtasche.

Die Trägerlage kann auch durch einen mobilen Datenspeicher gebildet sein bspw. durch einen USB-Stick oder eine Speicherkarte, wie sie dem Fachmann bekannt sind. Aufgrund des technischen Fortschritts werden derartige mobile Datenspeicher bei reduzierter Baugröße immer leistungsfähiger, bieten also immer größere Speicherkapazitäten. Daher werden diese mobilen Datenspeicher bereits von einer Vielzahl von Benutzern mitgeführt und bieten sich somit als Trägerlage für das erfindungsgemäße Identifikationsmerkmal in besonders vorteilhafter Weise an.

Nach einer Weiterbildung ist das personenbezogene Merkmal durch ein Abbild einer Person gebildet. Ein Abbild einer Person, insbesondere ein Foto, erlaubt eine sehr schnelle Kontrolle der Übereinstimmung des personenbezogenen Merkmals mit der Person, die das Identifikationsmerkmal präsentiert. Durch die erfindungsgemäße Verknüpfung mit dem ersten elektronischen Schlüssel wird ein personenbezogenes Merkmal derart vorteilhaft weitergebildet, dass ein einfacher und schneller optischer Vergleich möglich ist, jedoch das personenbezogene Merkmal bzw. das Identifikationsmerkmal nur äußerst schwer zu manipulieren ist.

Bevorzugt ist auf der Trägerlage eine Darstellung des personenbezogenen Merkmals angeordnet. Dies hat den Vorteil, dass eine schnelle visuelle Kontrolle der Person möglich ist, in dem die Darstellung mit der physisch anwesenden Person verglichen wird.

Im Hinblick auf eine zuverlässige Erkennung und somit einer zuverlässigen Identifikation und Authentifikation einer Person mittels eines Abbilds derselben, ist eine Weiterbildung von ganz besonderem Vorteil, nach der das Abbild einem international anerkannten Standard zur Abbildung von Personen genügt. Bevorzugt finden die Anforderungen der International Civil Aviation Organization (ICAO) Anwendung. Von der ICAO ist dabei insbesondere festgelegt, wie das Gesicht einer Person abzubilden ist und welche Anforderungen hinsichtlich der Mimik der Person einzuhalten sind. Durch diese international anerkannte Standardisierung ist es beispielsweise möglich, Personenabbilder automatisiert verarbeiten zu können. Ein weiterer wesentlicher Vorteil liegt auch darin, dass durch die internationale Standardisierung eine uni-

verselle Anwendbarkeit sichergestellt ist und somit weltweit einheitliche Vergleichsmerkmale Anwendung finden.

Neben dem Abbild einer Person als personenbezogenes Merkmal, kann das personenbezogene Merkmal auch durch ein biometrisches Merkmal gebildet sein, was den Vorteil hat, dass biometrische Merkmale nur äußerst schwierig bzw. nicht zu manipulieren sind und somit eine ganz besonders hohe Sicherheit der Personenidentifikation- bzw. Authentifikation bieten. Als biometrisches Merkmal kann bspw. ein Fingerabdruck, ein Iris-Abbild, eine Haut- bzw. Venenstruktur oder auch die Stimme verwendet werden. Das biometrische Merkmal wird dabei in eine elektronische Repräsentation übergeführt, um am erfindungsgemäßen Identifikationsmerkmal hinterlegt werden zu können.

Im Hinblick auf die Sicherheit des Identifikationsmerkmals ist eine Weiterbildung von Vorteil, nach der der erste Schlüssel durch einen Schlüssel einer Authentifizierungs- bzw. Zertifizierungseinrichtung gebildet ist. Derartige Einrichtungen sind zumeist international anerkannte Organisationen, die insbesondere einen sehr hohen Standard hinsichtlich der Vergabe und Verwaltung elektronischer Schlüssel erfüllen. Von wesentlicher Bedeutung ist jedoch, dass derartige Einrichtungen die Schlüsselvergabe und Verwaltung unabhängig von anderen Organisationen durchführen und somit ein sehr hohes Maß an Eigenständigkeit und damit einen sehr geringen Beeinflussungsgrad sicherstellen. Beispielsweise kann der erste elektronische Schlüssel Teil eines so genannten Public Key Systems sein, wobei ein Schlüsselteil öffentlich bekannt ist, der private Schlüsselteil jedoch nur dem registrierten Benutzer der Authentifizierungs- und Zertifizierungseinrichtung bekannt ist.

Beispielsweise kann nun der erste elektronische Schlüssel bzw. die Verknüpfung derart ausgebildet sein, dass ein potentieller Angreifer durch einen Manipulationsversuch den ersten Schlüssel bzw. die Verknüpfung unwiederbringlich zerstört.

Da der erste Schlüssel und das personenbezogene Merkmal im Speichermittel der Authentifizierungseinrichtung hinterlegt sind, ist es von Vorteil, wenn die Authentifizierungseinrichtung eine Datenverarbeitungseinrichtung bzw. ein Kryptografiemodul aufweist, da somit ein direkter Zugriff auf die hinterlegten Merkmale verhindert werden kann. Aus sicherheitstechnischen Gründen ist es von besonderer Bedeutung, wenn eine externe Prüfeinrichtung, bspw. eine

automatisierte Personenidentifikationseinrichtung, keinen direkten Zugriff auf den hinterlegten Schlüssel, das personenbezogene Merkmal bzw. die Verknüpfung hat. Mit der anspruchsgemäßen Weiterbildung lassen sich die hinterlegten Merkmale derart verschlüsseln, dass ein potentieller Angreifer daraus keinen Vorteil gewinnen kann. Insbesondere hat die Ausbildung den Vorteil, dass die hinterlegten Merkmale weitestgehend verborgen gehalten werden kann und somit die Möglichkeit eines missbräuchlichen Zugriffs verhindert wird. Beispielsweise kann der elektronische Schlüssel mittels eines Einweg-Krypto-Algorithmus verschlüsselt werden. Beim Zugriff auf das Identifikationsmerkmal zur Prüfung des personenbezogenen Merkmals muss daher die Personenidentifikationseinrichtung der Authentifizierungseinrichtung das korrekte Schlüsselergebnis präsentieren, um einen datentechnischen Zugriff auf das Identifikationsmerkmal gestattet zu bekommen. Bei einer butre-force Attacke versucht ein Angreifen durch probieren möglicher Schlüsselergebnisse, einen Zugriff zu erlangen. Nach einem mehrfachen fehlerhaften Zugriffsversuch mit einem falschen Schlüsselergebnis, kann die Authentifizierungseinrichtung einen Schutzmechanismus aktivieren, der bspw. den Zugriff völlig sperrt und eine erneute Verknüpfung des ersten elektronischen Schlüssels mit dem personenbezogenen Merkmal erforderlich macht. Es ist jedoch auch möglich, dass die Authentifizierungseinrichtung das Identifikationsmerkmal unbrauchbar macht, bspw. in dem der erste Schlüssel und/oder das personenbezogene Merkmal zerstört wird.

Im Hinblick auf einen möglichst benutzerfreundlichen Einsatz bzw. Anwendung des erfindungsgemäßen Identifikationsmerkmals ist eine Weiterbildung von Vorteil, nach der der Kommunikationsanschluss zur drahtlosen Kommunikation ausgebildet ist. Dadurch ist es beispielsweise möglich, dass ein Benutzer, der das erfindungsgemäße Identifikationsmerkmal bei sich trägt, eine Erfassungsvorrichtung passiert, wobei die Erfassungsvorrichtung über die Kommunikationseinrichtung drahtlos mit der Authentifizierungseinrichtung kommuniziert und so beispielsweise den ersten Schlüssel und/oder gegebenenfalls weitere personenbezogene Merkmale ausgetauscht bzw. verifiziert werden. Gerade in Bereichen mit einem erhöhten Personenaufkommen hat diese Ausbildung den besonderen Vorteil, dass der Personenstrom nicht durch ein Präsentieren des Identifikationsmerkmals verlangsamt wird. Die Personen passieren beispielsweise die Erfassungseinrichtung, welche die relevanten Merkmale ausliest und gegebenenfalls eine automatisierte Personenidentifikation bzw. Authentifikation durchführt.

In einer Weiterbildung könnte die Erfassungsvorrichtung beispielsweise mit einer Datenverarbeitungseinrichtung verbunden sein, die nach Auslesen bzw. Prüfen des ersten elektronischen Schlüssels auf eine zentrale Datenspeichereinrichtung zugreift und dort hinterlege Referenzdaten des Identifikationsmerkmals ausliest. Diese Referenzmerkmale können anschließend einer Kontrollperson zur Anzeige gebracht werden, die diese Merkmale mit denen der aktuell anwesenden Person vergleicht.

Im Hinblick auf eine zuverlässige Authentifikation und Identifikation einer Person erreicht man eine besondere Steigerung der Sicherheit des Identifikationsmerkmals, wenn ein zweiter elektronischer Schlüssel hinterlegt ist. Dieser kann in einer ersten Ausbildung im Speichermittel der Authentifizierungseinrichtung hinterlegt sein, oder in einer zweiten Ausbildung im elektronischen Datensatz hinterlegt sein. Dieser zweite elektronische Schlüssel ist vom ersten elektronischen Schlüssel unabhängig und ermöglicht es somit mittels einer weiteren Authentifizierungs- bzw. Zertifizierungseinrichtung, ein zusätzliches Sicherheitsmerkmal am Identifikationsmerkmal hinterlegen zu können. Somit hat eine Kontrollinstanz bei der Überprüfung des erfindungsgemäßen Identifikationsmerkmals die Möglichkeit, zwei elektronische Schlüssel unabhängig voneinander überprüfen zu können und so eine Person mit einer erhöhten Sicherheit identifizieren und authentifizieren zu können. Durch diese Ausbildung wird es auch für einen potentiellen Angreifer bedeutend schwieriger das erfindungsgemäße Identifikationsmerkmal zu manipulieren, da dieser nun zwei elektronische Schlüssel gleichzeitig und in definierter Art und Weise manipulieren müsste, um so eine falsche Identität vorspiegeln zu können.

Eine besonders vorteilhafte Weiterbildung erhält man, wenn der zweite mit dem ersten Schlüssel verknüpft ist, da somit eine eindeutige und unverrückbare Verbindung der beiden Schlüssel hergestellt wird, was insbesondere im Hinblick auf die Zuverlässigkeit der Identifikation und Authentifikation einer Person von ganz besonderem Vorteil ist. Des Weiteren wir dadurch ein möglicher Manipulationsversuch wesentlich erschwert. Die Verknüpfung kann beispielsweise derart ausgebildet sein, dass ein nicht umkehrbares Schlüsselprodukt gebildet wird, dass also aus dem Ergebnis der Verknüpfung nicht auf die beiden Teilschlüssel zurück geschlossen werden kann.

Die Verknüpfung des personenbezogenen Merkmals mit dem ersten Schlüssel kann durch eine Einweg-Operation gebildet sein, bei der aus dem Ergebnis der Verknüpfung, nicht wieder auf die ursprünglichen Ausgangsprodukte zurück geschlossen werden kann. Bei einer Einweg-Verknüpfung wird insbesondere nur das Ergebnis der Verknüpfung hinterlegt. Bei der Identifikation bzw. Authentifikation einer Person wird von einer Authentifizierungsstelle mittels eines entsprechenden Prüfalgorithmus bspw. die Verknüpfung erneut hergestellt bzw. generiert und mit der hinterlegten Verknüpfung verglichen. Somit kann auf eine eindeutige Übereinstimmung geprüft werden, ohne die spezifischen und sicherheitsrelevanten wesentlichen Merkmale selbst überprüfen zu müssen.

Von ganz besonderem Vorteil ist eine Weiterbildung, nach der der erste und/oder zweite elektronische Schlüssel durch einen elektronischen Schlüssel einer juristischen Autorität gebildet ist. Eine juristische Autorität ist beispielsweise ein Rechtsanwalt oder Notar, jedenfalls eine Person, die Kraft ihres rechtlichen Status eine rechtsverbindliche Aussage über die Authentizität eines Identifikationsmerkmals treffen kann. Eine Person wird beispielsweise das Identifikationsmerkmal einer juristischen Autorität präsentieren, die nach einer Legitimation der Person, durch Hinterlegen des eigenen elektronischen Schlüssels, das Identifikationsmerkmal eindeutig einer Person zuordenbar bestätigt. Wesentlich dabei ist, dass durch diese einmalige Bestätigung durch eine juristische Autorität, eine eindeutige und nachvollziehbare Zuordnung des Identifikationsmerkmals zu einer Person festgelegt ist und diese eindeutige Zuordnung bei nachfolgenden Identifikations- bzw. Authentifikationsvorgängen der Person eindeutig abrufbar ist. Einem Dritten ist es somit durch Prüfung des Identifikationsmerkmals möglich, eine Person, die ein derartiges Identifikationsmerkmal präsentiert, eindeutig und zuverlässig zu identifizieren und authentifizieren, insbesondere ist eine rechtlich verbindliche Identifikation und Authentifikation möglich.

Die juristische Autorität kann insbesondere durch jede Einrichtung gebildet sein, die eine in hohem Maß anerkannte und insbesondere rechtlich verbindliche Aussage über die Identität einer Person treffen kann. Beispielsweise kann dies auch durch eine national und/oder international tätige Autorisierungs- bzw. Zertifizierungseinrichtung erfolgen.

Im Hinblick auf die Sicherheit des Identifikationsmerkmals ist eine Weiterbildung von ganz besonderem Vorteil, nach der ein digitales Abbild des personenbezogenen Merkmals im Spei-

chermittel hinterlegt ist. Ein potentieller Angreifer könnte beispielsweise die Trägerlage des Identifikationsmerkmals derart manipulieren, dass ein verfälschtes personenbezogenes Merkmal aufgebracht bzw. angeordnet ist. Wird nun zusätzlich zum personenbezogenen Merkmal auf der Trägerlage, ein digitales Abbild dieses Merkmals im Speichermittel der Authentifizierungseinrichtung hinterlegt, steht bei einem späteren Zugriff zur Authentifizierung einer Person stets ein Referenzabbild zur Verfügung, das mit dem aktuell auf der Trägerlage angeordneten Merkmal verglichen werden kann und somit einen Manipulationsversuch sofort erkennbar macht. Diese Ausbildung hat insbesondere den Vorteil, dass eine so genannte Offline-Authentifikation einer Person möglich wird, da das zu prüfende bzw. zu vergleichende Referenzmerkmal am Identifikationsmerkmal vorhanden ist und somit keine Kommunikationsverbindung zu einer zentralen Zertifizierungs- bzw. Autorisierungseinrichtung erforderlich ist.

Durch einen entsprechenden Zugriffsschutz der Authentifizierungseinrichtung kann beispielsweise zusätzlich sicher gestellt werden, dass ein Zugriff auf dieses Referenzmerkmal nur lesend möglich ist, dass insbesondere ein Schreibender Zugriff durch technische Merkmale und Sicherheitseinrichtungen der Authentifizierungseinrichtung verhindert wird. In einer Weiterbildung könnte die Authentifizierungseinrichtung auch derart ausgebildet sein, dass ein Schreibender Zugriff auf das hinterlegte Merkmal zur Zerstörung der hinterlegten Information, der Verknüpfung und gegebenenfalls auch zur Zerstörung des Identifikationsmerkmals führt.

Eine ganz besonders vorteilhafte Weiterbildung erhält man, wenn der erste elektronische Schlüssel im digitalen Abbild codiert hinterlegt ist. Beispielsweise kann eine derartige Codierung mittels eines steganografischen Verfahrens durchgeführt werden, was den Vorteil hat, dass der erste elektronische Schlüssel derart im digitalen Abbild hinterlegt wird, das bei optischer Betrachtung des hinterlegten Abbilds der codierte Schlüssel nicht in Erscheinung tritt. Weiters von Vorteil ist, dass das digitale Abbild nicht manipuliert werden kann, da jeder Manipulationsversuch automatische die Verknüpfung des personenbezogenen Merkmals mit dem ersten elektronischen Schlüssel ungültig machen würde. Insbesondere hat diese Ausbildung den besonderen Vorteil, dass ein derartiges Codierungsverfahren zumeist nicht umkehrbar ist, also dass es zu Manipulationszwecken nicht möglich ist, die Codierung aufzuheben, das per-

sonenbezogene Merkmal zu verändern und anschließend die Codierung bzw. die Verknüpfung erneut durchzuführen.

Gemäß einer Weiterbildung ist der elektronische Datensatz in einem Speichermittel einer Datenverarbeitungseinrichtung hinterlegt. Zur Sicherung des hinterlegten elektronischen Datensatzes kann die Datenverarbeitungseinrichtung bspw. in einem Sicherheitsbereich angeordnet sein, zu dem nur eine ausgewählte Personenschar Zutritt hat. In der Datenverarbeitungseinrichtung können nun ggf. auch mehrere elektronische Datensätze hinterlegt sein. Beispielsweise können so elektronische Datensätze mehrere Personen verwaltet werden.

Von Vorteil ist eine Weiterbildung, nach der die Datenverarbeitungseinrichtung einen Kommunikationsanschluss aufweist, der dazu ausgebildet ist, einer entfernten Datengegenstelle einen Zugriff auf den elektronischen Datensatz zu ermöglichen. Beispielsweise kann die Datenverarbeitungseinrichtung durch einen Server gebildet sein, der eine Mehrzahl unterschiedlicher elektronischer Datensätze als Identifikationsmerkmale hinterlegt hat und über ein globales Kommunikationsnetzwerk zugänglich ist. Dadurch können eine Mehrzahl von Identifikations- und Authentifikationseinrichtungen auf die Identifikationsmerkmale zugreifen und so die Personenidentifikation- bzw. Authentifikation durchführen.

Im Hinblick auf eine Vereinfachung der Anwendung und um dem Umstand Rechnung zu tragen, dass das erfindungsgemäße Identifikationsmerkmal bevorzugt mitgeführt werden soll, ist eine Weiterbildung von Vorteil, nach der der elektronische Datensatz in einem mobilen Datenspeicher hinterlegt ist. Wie bereits beschrieben gehören mobile Datenspeicher bereits überwiegend zu Einrichtungen des täglichen Gebrauchs und werden daher meist mitgeführt.

Die Aufgabe der Erfindung wird auch durch ein Verfahren zur Identifikation und Authentifikation einer Person gelöst, welches die nachfolgend beschriebenen Verfahrensschritte umfasst.

Durch Hinterlegen personenbezogener Merkmale in einem Speichermittel oder einem elektronischen Datensatz, wird ein Identifikationsmerkmal geschaffen, das von einem Benutzer mitgeführt werden kann bzw. jederzeit zugreifbar ist und jederzeit eine Identifikation der Person ermöglicht.

Zur Sicherstellung der Identität einer Person wird diese durch eine juristische Autorität legitimiert. Dies kann bspw. dadurch erfolgen, dass die Person der juristischen Autorität ein rechtsgültiges Dokument vorlegt, das die Identität der Person belegt.

Durch Hinterlegen eines ersten Schlüssels einer juristischen Autorität im Speichermittel des Informationsmerkmals oder dem elektronischen Datensatz und anschließender Verknüpfung des ersten Schlüssels mit dem personenbezogenen Merkmal, wird eine rechtsgültige Beziehung zwischen dem physischen Identifikationsmerkmal und der Person als Träger bzw. Besitzer dieses Merkmals hergestellt.

Die Person kann nachfolgend durch Präsentation des Identifikationsmerkmals rechtsgültig die Identität authentifiziert belegen. Bei der Präsentation des Identifikationsmerkmals vor einem Dritten, kann dieser somit davon ausgehen, insbesondere rechtsverbindlich davon ausgehen, dass diese Person eindeutig derjenigen entspricht, die von der juristischen Autorität diesem spezifischen Identifikationsmerkmal zugeordnet wurde.

Die Präsentation des Identifikationsmerkmals kann nun nach der ersten Ausbildung des Identifikationsmerkmals bedeuten, dass die Trägerlage einer prüfenden Person und/oder einer Prüfeinrichtung vorgewiesen wird. Nach der zweiten Ausbildung als elektronischer Datensatz kann der Prüfeinrichtung bzw. prüfenden Person ein Verweis auf den Speicherort des Datensatzes präsentiert werden, wonach über einen Kommunikationsweg auf das Identifikationsmerkmal zugegriffen werden kann.

Zur Erhöhung der Sicherheit bzw. zur Bereitstellung eines mehrstufigen Authentifikationsverfahrens ist eine Ausbildung von Vorteil, bei der ein zweiter elektronischer Schlüssel einer Authentifizierungs- bzw. Zertifizierungseinrichtung hinterlegt wird. Diese Ausbildung bringt eine deutliche Steigerung der Sicherheit der Identifikation und Authentifikation einer Person, da ein Dritter, dem das Identifikationsmerkmal präsentiert wird, durch Prüfen des Schlüssels bei der ausgebenden bzw. ausstellenden Authentifizierungs- bzw. Zertifizierungseinrichtung prüfen kann, ob die Person, die das Identifikationsmerkmal präsentiert, mit jener Person übereinstimmt, die den zweiten elektronischen Schlüssel beantragt hat. Da eine derartige Einrichtung zumeist ein besonderes nationales, bevorzugt jedoch ein internationales anerkanntes Ansehen hat, wird die Feststellung der Identität bzw. Authentizität einer Person einmal mittels

des ersten elektronischen Schlüssels, der durch eine juristische Autorität hinterlegt wurde und ein zweites mal durch den zweiten elektronischen Schlüssel einer Authentifizierungs- bzw. Zertifizierungseinrichtung bestätigt, was einen ganz besonderen Vorteil im Hinblick auf eine zuverlässige Personenerkennung und eine große Akzeptanz des erfindungsgemäßen Verfahrens bringt.

Diese Ausbildung ermöglicht auch die Realisierung unterschiedlicher Sicherheitsstufen. Beispielsweise kann für einfachere, sicherheitstechnisch unkritische Anwendung die Authentifikation mittels des zweiten Schlüssels ausreichen. Ist eine erhöhte Sicherheit erforderlich, kann auch noch der erste Schlüssel geprüft werden.

Für eine deutliche Steigerung der Sicherheit des erfindungsgemäßen Verfahrens, im Hinblick auf die zuverlässige Identifikation und Authentifikation einer Person, sowie auf eine möglichst rasche Durchführung des Verfahrens, ist eine Weiterbildung von Vorteil, nach der in einer externen Speichereinheit ein Referenzsatz personenbezogener Daten hinterlegt wird. Diese externe Speichereinheit könnte beispielsweise durch eine zentrale Datenverarbeitungseinrichtung gebildet sein, die mit Vorrichtungen verbunden ist, um personenbezogene Merkmale bzw. elektronische Schlüssel, sowie deren Verschlüsselungsprodukte aus Identifikationsmerkmalen auslesen zu können. Beispielsweise kann der Referenzsatz ein Abbild der personenbezogenen Merkmale des Identifikationsmerkmals aufweisen, wodurch bei einer Personenauthentifikation jederzeit auf jenen ursprünglichen Merkmalsatz zugegriffen werden kann, der bei Legitimierung durch die juristische Autorität mit dem personenbezogenen Merkmal verknüpft wurde. Ein potentieller Angreifer könnte beispielsweise das Identifikationsmerkmal manipulieren, hat auf den hinterlegten Referenzsatz keinen Zugriff, so dass der Manipulationsversuch bei der nächsten Personenauthentifikation sofort erkannt werden würde. Zur Authentifikation einer Person steht somit immer ein nicht bzw. nur äußerst schwer manipulierbarer Referenzsatz zu Verfügung, wodurch sich für einen Dritten eine bedeutende Steigerung der Sicherheit und Zuverlässigkeit der Personenidentifikation ergibt.

Ebenfalls im Hinblick auf eine Steigerung der Zuverlässigkeit und Akzeptanz des erfindungsgemäßen Verfahrens ist eine Weiterbildung von Vorteil, bei der am Identifikationsmerkmal, insbesondere im Speichermittel, ein Referenzsatz personenbezogener Daten hinterlegt wird. Diese Ausbildung ist insbesondere dann von Vorteil, wenn eine Erfassungseinrichtung „offli-

ne“ betrieben wird, also keinen direkten Zugang zu einer zentralen Verwaltungseinrichtung hat.

In Weiterbildungen kann dieser Referenzsatz selbstverständlich verschlüsselt bzw. entsprechend kodiert hinterlegt werden bspw. durch eine Einwegverschlüsselung, was für einen potentiellen Angreifer eine weitere Sicherheitshürde darstellt.

Gemäß einer Weiterbildung wird zur Identifikation und Authentifikation einer Person, das hinterlegte personenbezogene Merkmal mit einem erfassten Merkmal verglichen. Durch diese Ausbildung ist in vorteilhafter Weise sicher gestellt, dass das erfindungsgemäße Identifikationsmerkmal eine ausreichende Merkmalsicherheit bietet, um anhand eines erfassten Merkmals und Vergleich desselben mit dem hinterlegten Merkmal, eine zuverlässige Identifikation und/oder Authentifikation einer Person zu ermöglichen. Dieser Vergleich kann von einer Kontrollperson und/oder einer automatisierten Kontrolleinrichtung durchgeführt werden, insbesondere wird diese Prüfung dann durchgeführt, wenn eine Person, die ein Identifikationsmerkmal trägt bzw. eine Referenz präsentiert, dieses gegenüber einem Dritten vorweist und sich identifizieren und authentifizieren möchte. Eine Erfassungseinrichtung kann dann personenbezogene Merkmale erfassen, diese an eine Verarbeitungseinrichtung bzw. eine Kontrollperson übermitteln, welche die aktuell erfassten Daten mit hinterlegten Referenzdaten vergleicht. Bei Übereinstimmung ist somit sichergestellt, dass die aktuell anwesende physische Person mit derjenigen übereinstimmt, für die das Identifikationsmerkmal durch eine juristische Autorität bestätigt bzw. zugeordnet wurde.

Eine ganz besondere Steigerung der Sicherheit des Identifikationsmerkmals erreicht man durch eine Weiterbildung, nach der das personenbezogene Merkmal sofort nach der Erfassung mit dem ersten elektronischen Schlüssel verknüpft wird. Somit ist eindeutig sichergestellt, dass das personenbezogene Merkmal zwischen der Erfassung und der Hinterlegung und Verknüpfung nicht manipuliert werden kann.

Eine weitere besondere Steigerung der Sicherheit bei der Erfassung des personenbezogenen Merkmals zur Hinterlegung und Verknüpfung mit dem ersten elektronischen Schlüssel liegt darin, dass das personenbezogene Merkmal in Echtzeit vor bzw. durch die Juristische Autorität erfasst wird, wodurch die Authentizität des erfassten personenbezogenen Merkmals ein-

deutig bestätigt ist. Da das personenbezogene Merkmal das wesentliche Merkmal des Identifikationsmerkmals ist, bringt diese Ausbildung eine ganz besondere Erhöhung der Sicherheit, da das erfasste Merkmal unter Aufsicht erfasst wird und ohne Möglichkeit einer Manipulation hinterlegt und mit dem Schlüssel verknüpft wird.

Zum besseren Verständnis der Erfindung wird diese anhand der nachfolgenden Figuren näher erläutert.

Es zeigen jeweils in stark schematisch vereinfachter Darstellung:

Fig. 1 Ein Ausbildung des erfindungsgemäßen Identifikationsmerkmals;

Fig. 2 Die Verfahrensschritte zur Bildung eines Identifikationsmerkmals zur eindeutigen Identifikation und Authentifikation einer Person;

Fig. 3 Eine Vorrichtung zur Zutrittssicherung unter Prüfung der Identität einer Person;

Fig. 4 Eine Vorrichtung zur Authentifizierung eines Identitätsmerkmals.

Einführend sei festgehalten, dass in den unterschiedlich beschriebenen Ausführungsformen gleiche Teile mit gleichen Bezugszeichen bzw. gleichen Bauteilbezeichnungen versehen werden, wobei die in der gesamten Beschreibung enthaltenen Offenbarungen sinngemäß auf gleiche Teile mit gleichen Bezugszeichen bzw. gleichen Bauteilbezeichnungen übertragen werden können. Auch sind die in der Beschreibung gewählten Lageangaben, wie z.B. oben, unten, seitlich usw. auf die unmittelbar beschriebene sowie dargestellte Figur bezogen und sind bei einer Lageänderung sinngemäß auf die neue Lage zu übertragen. Weiters können auch Einzelmerkmale oder Merkmalskombinationen aus den gezeigten und beschriebenen unterschiedlichen Ausführungsbeispielen für sich eigenständige, erfinderische oder erfindungsgemäße Lösungen darstellen.

Sämtliche Angaben zu Wertebereichen in gegenständlicher Beschreibung sind so zu verstehen, dass diese beliebige und alle Teilbereiche daraus mit umfassen, z.B. ist die Angabe 1 bis 10 so zu verstehen, dass sämtliche Teilbereiche, ausgehend von der unteren Grenze 1 und der

oberen Grenze 10 mitumfasst sind, d.h. sämtliche Teilbereich beginnen mit einer unteren Grenze von 1 oder größer und enden bei einer oberen Grenze von 10 oder weniger, z.B. 1 bis 1,7, oder 3,2 bis 8,1 oder 5,5 bis 10.

Fig. 1 zeigt eine Ausbildung des erfindungsgemäßen Identifikationsmerkmal 1, umfassend eine Trägerlage 2, ein personenbezogenes Merkmal 3, insbesondere ein Abbild der Person, sowie eine Authentifizierungseinrichtung 4 mit einem Speichermittel 5, in dem ein erster elektronischer Schlüssel 6 hinterlegt ist. Das Identifikationsmerkmal 1 weist zusätzlich eine Kommunikationseinrichtung 7 mit einem Kommunikationsanschluss 8 auf. Am Identifikationsmerkmal 1 können noch weitere personenbezogene oder institutionelle Merkmale 9 angeordnet und/oder integriert sein.

Das Identifikationsmerkmal 1, insbesondere die Trägerlage ist bevorzugt als Ausweisdokument ausgebildet, um einen Träger dieses Identifikationsmerkmals einen Zugriff bzw. einen Zutritt zu nicht allgemein zugänglichen Bereichen bzw. Informationen zu ermöglichen. Da das erfindungsgemäße Identifikationsmerkmal gegebenenfalls permanent mitgeführt werden muss, ist die Trägerlage bevorzugt scheckkartenartig ausgebildet, so dass es zu keiner Einschränkung der Bewegungsfreiheit bzw. zu keiner strukturellen Gefährdung des Identifikationsmerkmals aufgrund der personeneigenen Bewegung kommen kann. Insbesondere hat eine scheckkartenartige Ausbildung den Vorteil, dass das Identifikationsmerkmal in einer üblicherweise mitgeführten Ausweis- bzw. Geldtasche angeordnet werden kann. Eine Ausbildung als Chipkarte hat den weiteren besonderen Vorteil, dass derartige Karten besonders weit verbreitet sind und daher besonderes kostengünstig verfügbar sind und insbesondere Komponenten bzw. Module aufweisen, die für die Durchführung des erfindungsgemäßen Identifikations- und Authentifikationsverfahrens von besonderer Bedeutung sind und somit von einer Erfassungsvorrichtung zur Identitäts- bzw. Authentizitätsprüfung nicht bereitgestellt werden müssen.

Bei bekannten Identifikationsmerkmalen besteht zumeist das Problem, dass ein personenbezogenes Merkmal 3, 9, insbesondere das Abbild der dem Identifikationsmerkmal zugeordneten Person, in missbräuchlicher Absicht manipuliert werden kann und somit das Identifikationsmerkmal zur Vorspielung einer falschen Identität verwendet werden kann. Insbesondere in Bereichen mit einem hohen Personenaufkommen kann es bei einer optischen Prüfung eines

personenbezogenen Merkmals durch eine Kontrollperson zu Fehlern kommen, wodurch sich ein Angreifer Zugriff auf gegebenenfalls sensible Bereiche schaffen kann. Der ganz besondere Vorteil des erfindungsgemäßen Identifikationsmerkmals liegt nun darin, dass der erste elektronische Schlüssel 6 mit dem personenbezogenen Merkmal 3 sowie gegebenenfalls einem weiteren Merkmal 9 verknüpft ist. Das personenbezogene Merkmal 3 ist bevorzugt durch ein Abbild der Person gebildet, was den Vorteil hat, dass zusätzlich ein visueller Vergleich der Person, die das Identifikationsmerkmal präsentiert, mit dem hinterlegten Abbild 3 möglich ist. Die Verknüpfung des elektronischen Schlüssels 6 mit dem personenbezogenen Merkmal 3 erfolgt beispielsweise dadurch, dass eine elektronische Repräsentation des personenbezogenen Merkmals 3 erzeugt wird und beispielsweise mit dem ersten elektronischen Schlüssel 6 verschlüsselt im Speichermittel 5 hinterlegt wird. Bevorzugt ist jedoch eine Ausbildung, bei der ein eine digitale Repräsentation eines Personenabbilds 3 im Speichermittel 5 hinterlegt wird und mittels eines steganographischen Verfahrens das digitale Abbild mit dem ersten elektronischen Schlüssel 6 verknüpft wird, wodurch der erste elektronische Schlüssel im digitalen Abbild verborgen wird. Es ist jedoch auch möglich, dass beispielsweise aus dem digitalen Abbild eine Prüfsumme ermittelt wird, die mit dem ersten elektronischen Schlüssel verschlüsselt und anschließend im digitalen Abbild verborgen wird. Dies sind nur beispielhafte Ausbildungen einer Verknüpfung eines elektronischen Schlüssels mit einem personenbezogenen Merkmal. Dem Fachmann sind diesbezüglich weitere Möglichkeiten bekannt, um einen elektronischen Schlüssel mit einem personenbezogenen Merkmal, welches bevorzugt in elektronisch verarbeitbarer Form vorliegt, derart zu verknüpfen, dass ein Manipulationsversuch wesentlich erschwert wird. Insbesondere hat die erfindungsgemäße Verknüpfung des ersten elektronischen Schlüssels 6 mit einem personenbezogenen Merkmal 3 den ganz besonderen Vorteil, dass bei einem Manipulationsversuch des personenbezogenen Merkmals 3 die Verknüpfung mit dem ersten elektronischen Schlüssel 6 ungültig wird und somit der Manipulationsversuch eindeutig erkennbar wird.

Zur datentechnischen Kommunikation des Identifikationsmerkmals 1 mit einer Erfassungseinrichtung weist das Identifikationsmerkmal ein Kommunikationsmittel 7 mit einem Kommunikationsanschluss 8 auf. Gemäß der bevorzugten Ausbildung als scheckkartenartige Smart-Card, beispielsweise nach dem Standard ISO/IEC 7810, ist die Anordnung des Kommunikationsanschlusses 8 auf der Trägerlage 2, sowie die Ausbildung der Trägerlage selbst festgelegt. Der Kommunikationsanschluss 8 kann neben einer kontaktbehafteten Ausbildung auch draht-

los ausgebildet sein und ermöglicht somit eine Durchführung der Authentifizierung ohne dass das Identifikationsmerkmal in einer Erfassungseinrichtung angeordnet werden muss. Beispielsweise legt der Standard ISO/IEC 14443 die Ausbildung für kontaktlos auslesbare Chipkarten fest.

Die Authentifizierungseinrichtung 4 kann nun dazu ausgebildet sein, charakteristische Merkmale der Verknüpfung zwischen dem personenbezogenen Merkmal 3 und dem ersten elektronischen Schlüssel 6, über die Kommunikationseinrichtung 7 einer Erfassungseinrichtung bereit zu stellen. Es ist jedoch auch möglich, dass die Authentifizierungseinrichtung ein aktuell erfasstes personenbezogenes Merkmal mit dem hinterlegten personenbezogenen Merkmal vergleicht und eine erkannte Übereinstimmung an die Erfassungseinrichtung übermittel. In dieser Ausbildung wird in vorteilhafter Weise kein Merkmal der Verknüpfung bzw. des ersten Schlüssels vom Identifikationsmerkmal nach außen übermittelt.

Im Hinblick auf eine Sicherung des hinterlegten elektronischen Schlüssels bzw. eines gegebenenfalls hinterlegten Abbilds des personenbezogenen Merkmals weist gemäß einer Weiterbildung die Authentifizierungseinrichtung 4 eine Datenverarbeitungseinrichtung bzw. ein Kryptographiemodul 10 auf. Die Authentifizierungseinrichtung 4 kann dazu ausgebildet sein, die hinterlegten Merkmale bzw. elektronischen Schlüssel derart zu sichern, dass ein Angreifer selbst bei Zugriff auf die hinterlegten Merkmale bzw. Schlüssel keinen Vorteil aus diesem Zugriff gewinnen kann. Dies wird beispielsweise durch eine Einwegverschlüsselung erreicht, die von einem Kryptographiemodul durchgeführt wird und bei der aus dem Ergebnis der Sicherung nicht auf die ursprünglichen Merkmale rückgeschlossen werden kann. Die Authentifizierungseinrichtung kann jedoch auch komplexe Aufgaben übernehmen, beispielsweise eine mehrstufige Merkmalsprüfung mit einer gegebenenfalls erforderlichen Ermittlung personenspezifischer Merkmale, wobei von Vorteil ist, wenn die Authentifizierungseinrichtung eine Datenverarbeitungseinrichtung umfasst, da eine derartige Vorrichtung zumeist komplexe Bearbeitungsschritte ausführen kann. Wie bereits beschrieben hat dazu eine Ausbildung als Chipkarte oder SmartCard den Vorteil, dass eine derartige Datenverarbeitungseinrichtung zumeist ein integrierter Teil einer solchen Karte ist.

Als weiteres Sicherheitsmerkmal kann im Speichermittel 5 der Authentifizierungseinrichtung 4 ein zweiter elektronischer Schlüssel 11 angeordnet sein. Das Wesen des ersten und/oder

zweiten elektronischen Schlüssels liegt darin, dass dieser von einer Authentifizierungs- bzw. Zertifizierungsstelle ausgegeben bzw. bereitgestellt wird, wobei diese Zertifizierungs- bzw. Autorisierungseinrichtung einem hohen internationalen Standard hinsichtlich der Zuverlässigkeit der generierten elektronischen Schlüssel genügt. Insbesondere erfüllen derartige Einrichtungen besondere Anforderungen an die Erstellung und Verwaltung der Benutzerdaten zur Generierung der elektronischen Schlüssel.

Fig. 2 zeigt eine Prinzipdarstellung des Verfahrens zur Ausbildung eines erfindungsgemäßen Identifikationsmerkmals 1, welches eine eindeutige Identifizierung und Authentifizierung einer Person ermöglicht. In einem ersten Schritt 12 wird ein unpersonalisiertes Identifikationsmerkmal 13 mit personenbezogenen Merkmalen 3, 9 personalisiert, es werden also die Merkmale 3, 9 am Identifikationsmerkmal 13 angeordnet bzw. hinterlegt. In einem zweiten Schritt 14 bringt der Benutzer 15 das personalisierte Identifikationsmerkmal 16 zusammen mit einem rechtsstaatlich gültigen Dokument 17 zur Feststellung der Identität der Person 15 einer Autorisierungsinstanz 18. Die Autorisierungsinstanz 18 ist bevorzugt durch eine juristische Autorität gebildet, beispielsweise durch einen Rechtsanwalt bzw. Notar. Dieser prüft die Identität der Person 15 mittels des beigebrachten Dokuments 17 und hinterlegt anschließend den eigenen ersten elektronischen Schlüssel 6 im personalisierten Identifikationsmerkmal 16, insbesondere im Speichermittel, wodurch dieses legitimiert wird. Der wesentliche Schritt des erfindungsgemäßen Verfahrens liegt nun darin, dass die Authentifizierungsautorität 18 den im Identifikationsmerkmal 16 hinterlegten ersten elektronischen Schlüssel 6 mit einem personenbezogenen Merkmal 3, 9 verknüpft und somit eine unwiderrufliche Verbindung 19 ausbildet.

Die Verfahrensschritte zur Durchführung der Personalisierung 12 bzw. der Autorisierung 14 des Identifikationsmerkmals erfordern es, dass das Identifikationsmerkmal in einer, nicht dargestellten, Zugriffssteuerung und Kontrolleinrichtung angeordnet wird, wobei diese durch eine Datenverarbeitungseinrichtung mit einer kommunikativ gekoppelten Kommunikationseinrichtung gebildet sein kann, die über den Kommunikationsanschluss 8 eine datentechnische Verbindung mit der Authentifizierungseinrichtung 4 herstellt. Der wesentliche technische Effekt dieses erfindungsgemäßen Verfahrens liegt nun darin, dass ein Identifikationsmerkmal 1 geschaffen wird, das ein personenbezogenes Merkmal 3 mit einem ersten elektronischen Schlüssel 6 derart verknüpft 19, dass durch diese Verknüpfung eine Manipulation des

Identifikationsmerkmals weitestgehend verhindert wird und somit die Identität und Authentizität einer Person eindeutig und rechtsgültig feststellbar ist.

Gegebenenfalls kann die Personalisierung 12 des Identifikationsmerkmals 13 noch einen Schritt umfassen, bei dem ein zweiter elektronischer Schlüssel 11 im Speichermittel 5 der Authentifizierungseinrichtung 4 hinterlegt wird. Der erste 6 und gegebenenfalls zweite 11 elektronische Schlüssel wird bevorzugt von einer externen Zertifizierungs- bzw. Autorisierungseinrichtung 20, 21 bereitgestellt bzw. verwaltet. Wie bereits zuvor beschrieben, weist diese Einrichtung einen hohen Grad an Akzeptanz ihrer Sicherheit im Hinblick auf die Generierung bzw. Verwaltung der elektronischen Schlüssel auf. Beispiele für derartige Einrichtungen sind: RSA oder VeriSign. Diese Einrichtungen verwalten einen Satz elektronischer Schlüssel, der eindeutig einem registrierten Benutzer zugeordnet ist. Bevorzugt wird dabei ein Schlüsselsatz nach einem so genannten Public Key System verwendet, der aus einem privaten und einem öffentlichen Schlüssel besteht. Auf eine detaillierte Beschreibung wird hier verzichtet, da Public Key Systeme dem kundigen Fachmann bekannt sind. Der Vorteil derartiger Schlüsselsysteme liegt insbesondere darin, dass es Dritten jederzeit möglich ist, die Authentizität eines elektronischen Schlüssels von einer unabhängigen Zertifizierungs- und Authentifizierungseinrichtung 20, 21 feststellen zu lassen.

Fig. 3 zeigt eine Anwendung des erfindungsgemäßen Verfahrens zur eindeutigen Identifikation und Authentifikation einer Person 15, mittels des erfindungsgemäßen Identifikationsmerkmals 1. Beispielsweise kann der Zutritt zu einer nicht allgemein zugänglichen Einrichtung mittels einer Zutrittskontrolleinrichtung 22 gesichert sein. Für die Freigabe der Zutrittskontrolleinrichtung 22 ist eine eindeutige Identifikation und Authentifikation einer Person 15 erforderlich. Dazu präsentiert die Person 15 das Identifikationsmerkmal 1 einer Erfassungseinrichtung 23, welche dieses auswertet. Beispielsweise wird das Identifikationsmerkmal 1 in einer Auslesevorrichtung 24 angeordnet, wobei über den Kommunikationsanschluss 8 eine Kommunikationsverbindung mit der Authentifizierungseinrichtung aufgebaut wird. Die Erfassungseinrichtung 23 kann nun beispielsweise zur automatisierten Identifikation und Authentifikation einer Person ausgebildet sein, beispielsweise in dem mit einem Erfassungsmittel 25, bevorzugt einer optischen Bilderfassungseinrichtung, ein Abbild der Person erfasst wird und von einem Auswerte- und Vergleichsmodul 26 mit den, am Identifikationsmerkmal 1 hinterlegten personenbezogenen Merkmalen verglichen wird. Da ein personenbezogenes

Merkmal 3 bevorzugt als Abbild gemäß einem international anerkannten Standard gebildet ist, insbesondere nach ICAO, kann das Auswerte- und Vergleichsmodul 26 überwiegend vollautomatisch einen Vergleich das aktuell erfassten Abbilds mit dem hinterlegten personenbezogenen Merkmal durchführen. Um sicherzustellen, dass das Identifikationsmerkmal 1 nicht manipuliert wurde, kann die Erfassungseinrichtung 23 bei einer externen Zertifizierungs- bzw. Autorisierungseinrichtung 21 die Gültigkeit und Authentizität des ersten elektronischen Schlüssels 6 prüfen. Ebenso ist auch die Prüfung eines zweiten elektronischen Schlüssels 11 durch eine weitere Zertifizierungs- bzw. Autorisierungseinrichtung 20 möglich.

In einer Weiterbildung ist es jedoch auch möglich, dass am Identifikationsmerkmal 1 hinterlegte personenbezogene Merkmale von der Erfassungseinrichtung 23 nicht ausgelesen werden, sondern dass ein aktuell erfasstes Abbild der Person aufbereitet und verarbeitet wird, beispielsweise von einem Kryptografiemodul 27 der Erfassungseinrichtung 23, und anschließend an das Identifikationsmerkmal 1 übermittelt. Die Authentifizierungseinrichtung des Identifikationsmerkmals 1 prüft anschließend, ob das erfasste und entsprechend aufbereitete Abbild der Person, mit dem hinterlegten personenbezogenen Merkmal 3 übereinstimmt und generiert darauf basierend ein entsprechendes Freigabesignal, welches an die Erfassungseinrichtung 23 zurück übermittelt wird, welche dann die Zutrittskontrolleinrichtung 22 freigibt.

Fig. 4 zeigt eine Vorrichtung zur Bildung des erfindungsgemäßen Identifikationsmerkmals 1, insbesondere um ein personenbezogenes Merkmal mit einem ersten elektronischen Schlüssel zu verknüpfen und am Identifikationsmerkmal zu hinterlegen. Die Verfahrensschritte zur Personalisierung und Authentifizierung eines Identifikationsmerkmals werden dabei bevorzugt mittels einer Datenverarbeitungseinrichtung 28 durchgeführt, da eine derartige Einrichtung weit verbreitet ist und insbesondere allgemein ausgebildete Eigenschaft zur Verarbeitung von elektronischen bzw. digitalen Informationseinheiten ausgebildet ist. Insbesondere umfasst eine derartige Einrichtung ein Bildaufbereitungsmodul 29, welches ein, von einer Bilderfassungseinrichtung 30 erfasstes Abbild einer Person 15 in eine weiterverarbeitbare Darstellungsform 31 überführt. Die Bilderfassungseinrichtung 30 bspw. eine Kamera, ist dabei über einen Kommunikationsanschluss mit der Datenverarbeitungseinrichtung 28 verbunden. Da das Abbild bevorzugt anerkannten Standards zur automatisierten Bilderfassung genügen muss, insbesondere nach ICAO, kann das Bildaufbereitungsmodul 29 die Bilderfassungseinrichtung 30 derart kontrollieren, dass die standardgemäß erforderliche Abbildung erreicht

wird. Bevorzugt führt das Bildaufbereitungsmodul die erfasste Bildinformation in ein standardisiertes Bilddatenformat über, welches von einer Mehrzahl von Datenverarbeitungssystemen verarbeitbar ist.

Ein wesentliches Merkmal des erfindungsgemäßen Identifikationsmerkmals bzw. des Verfahrens liegt darin, dass ein elektronischer Schlüssel, der hohen Anforderungen hinsichtlich einer Verfälschungssicherheit genügt, mit dem personenbezogenen Merkmal, insbesondere dem Abbild, verknüpft wird. Nachfolgend sind mehrere Beispiele für eine mögliche Verknüpfung aufgeführt, es wird jedoch auf das Fachwissen des kundigen Technikers verwiesen, welche Verfahren zur Verknüpfung eines elektronischen Schlüssels mit einem personenbezogenen Merkmal, welches in einer datentechnisch verarbeitbaren Form vorliegt, zu Verfügung stehen. Beispielsweise kann der erste elektronische Schlüssel 6 mittels eines steganografischen Verfahrens in digitalen Bilddaten angeordnet werden. Dies hat den Vorteil, dass das personenbezogene Merkmal bei Betrachtung durch eine Person keine Beeinträchtigungen aufweist, der erste elektronische Schlüssel über die gesamten Bilddaten integriert angebracht ist. Es ist jedoch auch möglich, dass aus dem aufbereiteten Abbild ein charakteristischer Referenzwert beispielsweise ein Hash-Wert ermittelt wird, der beispielsweise zusammen mit dem ersten elektronischen Schlüssel ein Kryptografiemodul 32 durchläuft und daraus ein kryptografisches Ergebnis gebildet wird. Dieses kryptografische Ergebnis kann nun so gebildet sein, dass daraus nicht wieder auf die ursprünglichen Bilddaten bzw. den elektronischen Schlüssel zurück geschlossen werden kann. Diese Ausbildung hat den Vorteil, dass nach der Authentifizierung des Identifikationsmerkmals durch eine Autorität, das personenbezogene Merkmal nicht wieder abgefragt werden muss, sondern dass bei einer anschließenden Identifikation und Authentifikation einer Person durch einen Dritten ein Abbild der Person erfasst wird, und mittels der gleichen kryptografischen Verschlüsselungsmethode bearbeitet wird, wobei wiederum ein kryptografisches Ergebnis entsteht. Dieses Ergebnis kann nun mit dem am Identifikationsmerkmal hinterlegten kryptografischen Ergebnis verglichen werden, um die Identität der Person authentifizieren zu können. Die Authentifizierungseinrichtung 4 des Identifikationsmerkmals 1 bzw. das Speichermittel der Authentifizierungseinrichtung kann auch derart ausgebildet sein, dass ein Zugriff auf hinterlegte personenbezogene Merkmale um diese verändern bzw. bearbeiten zu können, nur einer Autorität möglich ist, die Besitzer des ersten elektronischen Schlüssels ist. Gemäß einer vorteilhaften Weiterbildung kann der erste elektronische Schlüssel 6 Teil eines Schlüsselsystems sein, welches von einer Zertifizierungs-

bzw. Autorisierungseinrichtung bereitgestellt und/oder verwaltet wird. Diese Zertifizierungs- bzw. Autorisierungseinrichtung kann nun Teil der Datenverarbeitungseinrichtung 28 sein bzw. mit dieser lokal verbunden sein 33. Es ist jedoch auch eine entfernte Zertifizierungs- und Autorisierungseinrichtung 21 möglich, die beispielsweise mit der Datenverarbeitungseinrichtung 28 über ein öffentliches Kommunikationsmedium, beispielsweise dem Internet, kommunikativ verbunden ist. Beispielsweise kann hier ein so genanntes Public Key System verwendet werden, wobei die Autorität bei der Authentifizierung des Identifikationsmerkmals das Abbild mit seinem privaten Schlüssel verknüpft und am Identifikationsmerkmal hinterlegt. Da ein potentieller Angreifer niemals den privaten Schlüssel der Autorität kennt, ist eine Manipulation des personenbezogenen Merkmals nicht möglich, da dadurch auch die Verknüpfung mit dem ersten elektronischen Schlüssel ungültig werden würde. Ein Dritter kann nun die Identität und Authentizität einer Person, die das Identifikationsmerkmal präsentiert, dadurch feststellen, dass beispielsweise das verschlüsselte personenbezogene Abbild der Zertifizierungs- und Autorisierungseinrichtung 21 präsentiert, welche vollautomatisch die Authentizität des am Identifikationsmerkmal hinterlegten personenbezogenen Merkmals bestätigen kann. Durch Überprüfung der charakteristischen Merkmale der physisch anwesenden Person mit dem am Identifikationsmerkmal hinterlegten Referenzmerkmal lässt sich nun die Identität der physisch anwesenden Person eindeutig authentifizieren.

Zum Zugriff auf die hinterlegten Referenzmerkmale bzw. zur Hinterlegung der Referenzmerkmale und Durchführung der Verknüpfung mit dem ersten elektronischen Schlüssel ist das Identifikationsmerkmal 1 in einer Zugriffseinrichtung 34 angeordnet, wobei diese über die Kommunikationseinrichtung und insbesondere über den Kommunikationsanschluss 8 eine datentechnische Verbindung zwischen der Datenverarbeitungseinrichtung 26 und der Authentifizierungseinrichtung 4 des Identifikationsmerkmals 1 herstellt.

Eine weitere Ausbildung des erfindungsgemäßen Identifikationsmerkmals kann auch darin bestehen, dass die zugeordnete Person selbst weitere Merkmale authentifiziert. Dazu kann die Person bspw. ein Abbild mittels einer Bilderfassungseinrichtung einer Datenverarbeitungseinrichtung erfassen und durch Vergleich mit dem hinterlegten Merkmal, die eigene Identität authentifizieren. Dabei ist es gleichgültig, ob es sich um ein Identifikationsmerkmal gemäß der Ausbildung mit einer Trägerlage, oder einem elektronischen Datensatz handelt. Nach erfolgreicher Authentifikation kann die Person bspw. ein weiteres Identifikationsmerkmal

erstellen. Eine weit verbreitete Datenverarbeitungseinrichtung weist zumeist alle erforderlichen Komponenten auf, um die Verfahrensschritte nach dieser Weiterbildung durchführen zu können.

Die Ausführungsbeispiele zeigen mögliche Ausführungsvarianten des Identifikationsmerkmals bzw. des Verfahrens zur Authentifizierten Identifikation einer Person, wobei an dieser Stelle bemerkt sei, dass die Erfindung nicht auf die speziell dargestellten Ausführungsvarianten derselben eingeschränkt ist, sondern vielmehr auch diverse Kombinationen der einzelnen Ausführungsvarianten untereinander möglich sind und diese Variationsmöglichkeit aufgrund der Lehre zum technischen Handeln durch gegenständliche Erfindung im Können des auf diesem technischen Gebiet tätigen Fachmannes liegt. Es sind also auch sämtliche denkbaren Ausführungsvarianten, die durch Kombinationen einzelner Details der dargestellten und beschriebenen Ausführungsvariante möglich sind, vom Schutzumfang mit umfasst.

Der Ordnung halber sei abschließend darauf hingewiesen, dass zum besseren Verständnis des Aufbaus des Identifikationsmerkmals bzw. des Verfahrens dieses bzw. deren Bestandteile teilweise unmaßstäblich und/oder vergrößert und/oder verkleinert dargestellt wurden.

Die den eigenständigen erfinderischen Lösungen zugrundeliegende Aufgabe kann der Beschreibung entnommen werden.

Vor allem können die einzelnen in den Fig. 1 bis 4 gezeigten Ausführungen den Gegenstand von eigenständigen, erfindungsgemäßen Lösungen bilden. Die diesbezüglichen, erfindungsgemäßen Aufgaben und Lösungen sind den Detailbeschreibungen dieser Figuren zu entnehmen.

Bezugszeichenaufstellung

1 Identifikationsmerkmal
2 Trägerlage
3 Personenbezogenes Merkmal
4 Authentifizierungseinrichtung
5 Speichermittel
6 Erster elektronischer Schlüssel
7 Kommunikationseinrichtung
8 Kommunikationsanschluss
9 Personenbezogenes oder institutionelles Merkmal
10 Datenverarbeitungseinrichtung, Kryptographiemodul
11 Zweiter elektronischer Schlüssel
12 Identifikationsmerkmal personalisieren
13 Unpersonalisiertes Identifikationsmerkmal
14 Identifikationsmerkmal authentifizieren
15 Person
16 Personalisiertes Identifikationsmerkmal
17 Dokument
18 Authentifizierungsautorität
19 Verknüpfung
20 Zertifizierungseinrichtung, Autorisierungseinrichtung
21 Zertifizierungseinrichtung, Autorisierungseinrichtung
22 Zutrittskontrolleinrichtung
23 Erfassungseinrichtung
24 Auslesevorrichtung
25 Erfassungsmittel
26 Auswerte- und Vergleichsmodul
27 Kryptographiemodul
28 Datenverarbeitungseinrichtung
29 Bildaufbereitungsmodul
30 Bilderfassungseinrichtung
31 Aufbereitete Bilddaten, digitales Abbild
32 Kryptographiemodul
33 Lokale Zertifizierungseinrichtung, Autorisierungseinrichtung
34 Zugriffseinrichtung

Patentansprüche

1. Identifikationsmerkmal (1) zur authentifizierten Personenidentifikation, umfassend eine Trägerlage (2), eine Authentifizierungseinrichtung (4) mit einem Speichermittel (5), das als nicht-flüchtiger, wiederbeschreibbarer Halbleiterspeicher ausgebildet ist, ein personenbezogenes Merkmal (3), eine Kommunikationseinrichtung (7) mit einem Kommunikationsanschluss (8), dadurch gekennzeichnet, dass im Speichermittel (5) ein erster elektronischer Schlüssel (6) hinterlegt ist, welcher mit dem personenbezogenen Merkmal (3) verknüpft ist.

2. Identifikationsmerkmal zur authentifizierten Personenidentifikation, umfassend einen elektronischen Datensatz, in dem ein elektronisches Abbild eines personenbezogenen Merkmals (3) und ein erster elektronischer Schlüssel (6) hinterlegt sind, dadurch gekennzeichnet, dass der erste elektronische Schlüssel (6) mit dem personenbezogenen Merkmal (3) verknüpft ist.

3. Identifikationsmerkmal nach Anspruch 1, dadurch gekennzeichnet, dass die Trägerlage (2) gebildet ist aus der Gruppe umfassend Ausweisdokument, scheckkartenartige Datenkarte, mobiler Datenspeicher,

4. Identifikationsmerkmal nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das personenbezogene Merkmal (3) durch ein Abbild einer Person gebildet ist.

5. Identifikationsmerkmal nach Anspruch 4, dadurch gekennzeichnet, dass das Abbild (3) einem international anerkannten Standard zur Abbildung von Personen genügt, insbesondere dass es den Anforderungen der ICAO genügt.

6. Identifikationsmerkmal nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das personenbezogene Merkmal (3) durch ein biometrisches Merkmal gebildet ist.

7. Identifikationsmerkmal nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der erste elektronische Schlüssel (6) durch einen Schlüssel einer Authentifizierungs- bzw. Zertifizierungseinrichtung (21) gebildet ist.

8. Identifikationsmerkmal nach einem der Ansprüche 3 bis 7, dadurch gekennzeichnet, dass die Authentifizierungseinrichtung (4) eine Datenverarbeitungseinrichtung bzw. ein Kryptografiemodul (10) aufweist.

9. Identifikationsmerkmal nach einem der Ansprüche 3 bis 7, dadurch gekennzeichnet, dass der Kommunikationsanschluss (8) zur drahtlosen Kommunikation ausgebildet ist.

10. Identifikationsmerkmal nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass ein zweiter elektronischer Schlüssel (11) hinterlegt ist.

11. Identifikationsmerkmal nach Anspruch 10, dadurch gekennzeichnet, dass der zweite (11) mit dem ersten (6) elektronischen Schlüssel verknüpft ist.

12. Identifikationsmerkmal nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Verknüpfung durch eine Einweg-Operation gebildet ist.

13. Identifikationsmerkmal nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass der erste (6) und/oder zweite (11) elektronische Schlüssel durch einen elektronischen Schlüssel einer juristischen Autorität (18) gebildet ist.

14. Identifikationsmerkmal nach einem der Ansprüche 3 bis 13, dadurch gekennzeichnet, dass ein digitales Abbild (31) des personenbezogenen Merkmals (3) im Speichermittel (5) hinterlegt ist.

15. Identifikationsmerkmal nach Anspruch 14, dadurch gekennzeichnet, dass der erste elektronische Schlüssel (6) im digitalen Abbild (31) codiert hinterlegt ist.

16. Identifikationsmerkmal nach einem der Ansprüche 2 bis 15, dadurch gekennzeichnet, dass der elektronische Datensatz in einem Speichermittel einer Datenverarbeitungseinrichtung hinterlegt ist.

17. Identifikationsmerkmal Anspruch 16, dadurch gekennzeichnet, dass die Datenverarbeitungseinrichtung einen Kommunikationsanschluss aufweist, der dazu ausgebildet ist, einer entfernten Datengegenstelle einen Zugriff auf den elektronischen Datensatz zu ermöglichen.

18. Identifikationsmerkmal nach einem der Ansprüche 2 bis 17, dadurch gekennzeichnet, dass der elektronische Datensatz in einem mobilen Datenspeicher hinterlegt ist.

19. Verfahren zur Identifikation und Authentifikation einer Person mit einem Identifikationsmerkmal, insbesondere nach einem der Ansprüche 1 bis 18, umfassend die Schritte:
Hinterlegen eines personenbezogenen Merkmals (3, 9) in einem Speichermittel (5) oder einem elektronischen Datensatz;
Legitimieren einer Person (15) durch eine juristische Autorität (18);
Hinterlegen eines ersten Schlüssels (6) einer juristischen Autorität (18) im Speichermittel (5) oder im elektronischen Datensatz,
Verknüpfen (19) des ersten Schlüssels (6) mit dem personenbezogenen Merkmal (3).

20. Verfahren nach Anspruch 19, dadurch gekennzeichnet, dass im Speichermittel (5) oder im elektronischen Datensatz ein zweiter elektronischer Schlüssel (11) einer Authentifizierungs- bzw. Zertifizierungseinrichtung (20) hinterlegt wird.

21. Verfahren nach Anspruch 19 oder 20, dadurch gekennzeichnet, dass in einer externen Speichereinheit ein Referenzsatz personenbezogener Daten hinterlegt wird.

22. Verfahren nach einem der Ansprüche 19 bis 21, dadurch gekennzeichnet, dass am Identifikationsmerkmal (1), insbesondere im Speichermittel (5), ein Referenzsatz personenbezogener Daten hinterlegt wird.

23. Verfahren nach einem der Ansprüche 21 oder 22, dadurch gekennzeichnet, dass ein hinterlegter Referenzsatz personenbezogener Daten mit einem präsentierten personenbezogenen Datensatz verglichen wird.

24. Verfahren nach einem der Ansprüche 19 bis 23, dadurch gekennzeichnet, dass zur Identifikation und Authentifikation einer Person, das hinterlegte personenbezogene Merkmal (3, 9) mit einem erfassten Merkmal verglichen wird.

25. Verfahren nach einem der Ansprüche 19 bis 24, dadurch gekennzeichnet, dass das personenbezogene Merkmal sofort nach der Erfassung mit dem ersten elektronischen Schlüssel (6) verknüpft wird.

26. Verfahren nach Anspruch 25, dadurch gekennzeichnet, dass das personenbezogene Merkmal in Echtzeit vor bzw. durch die Juristische Autorität erfasst wird.

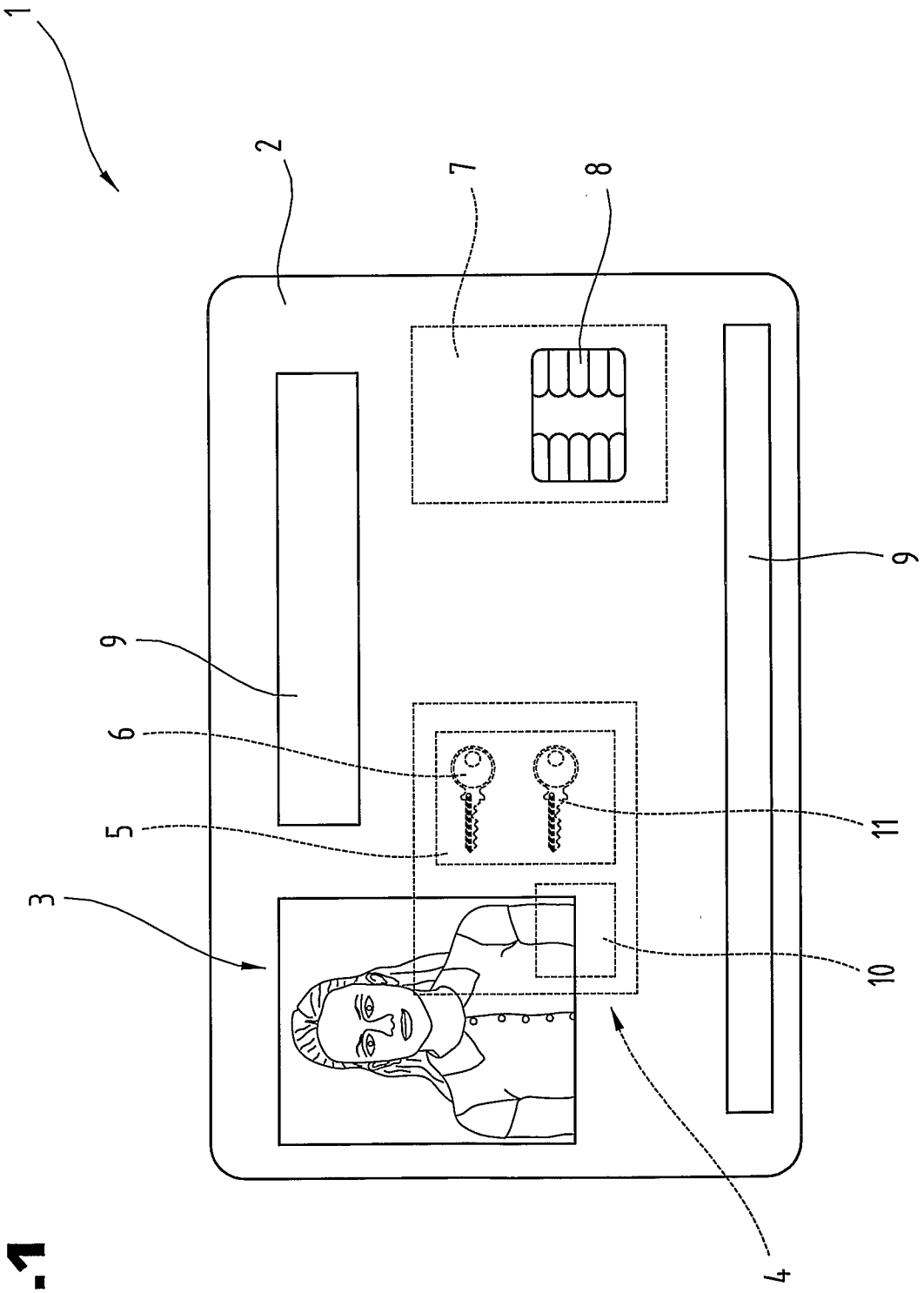


Fig.1

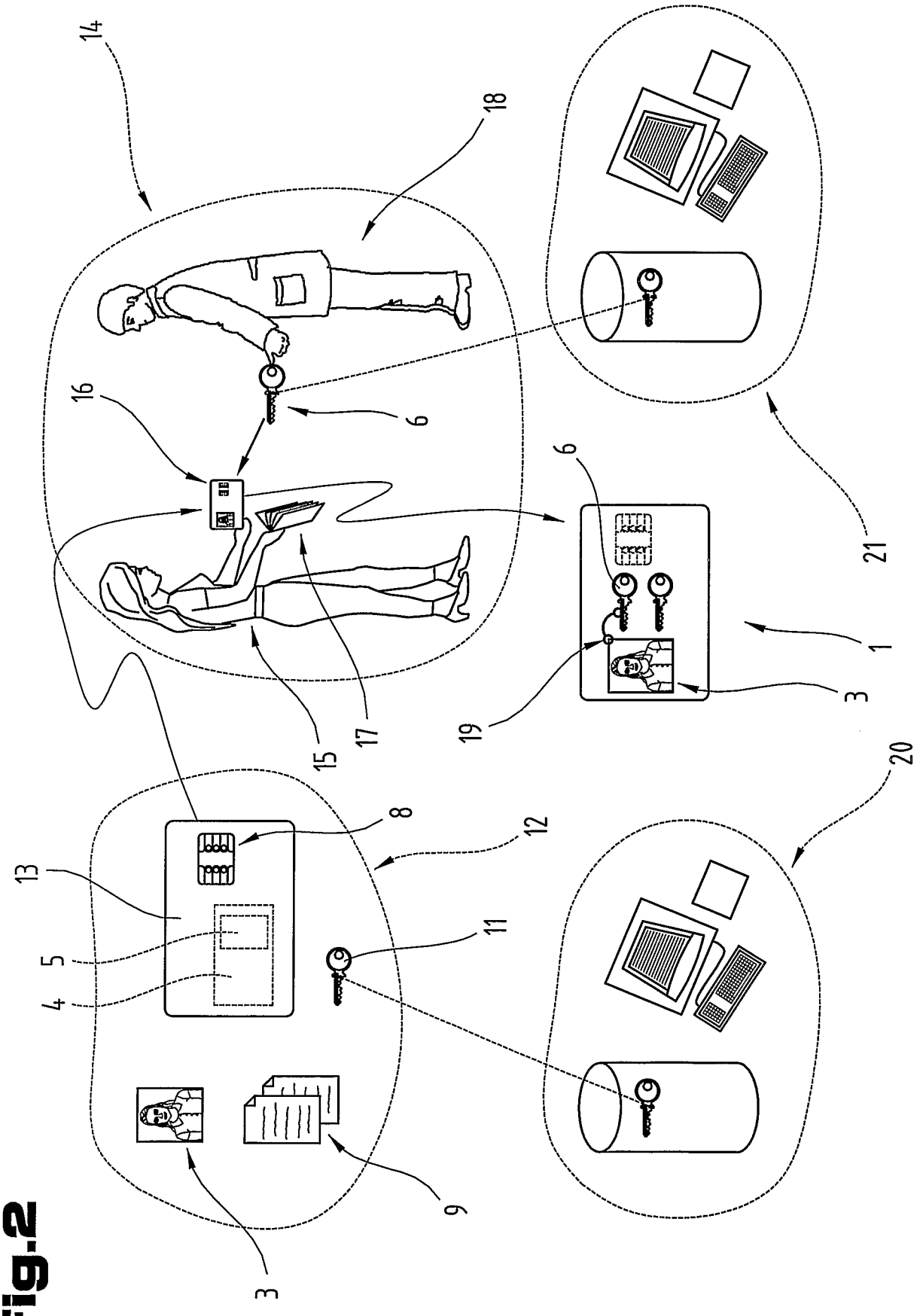


Fig.2

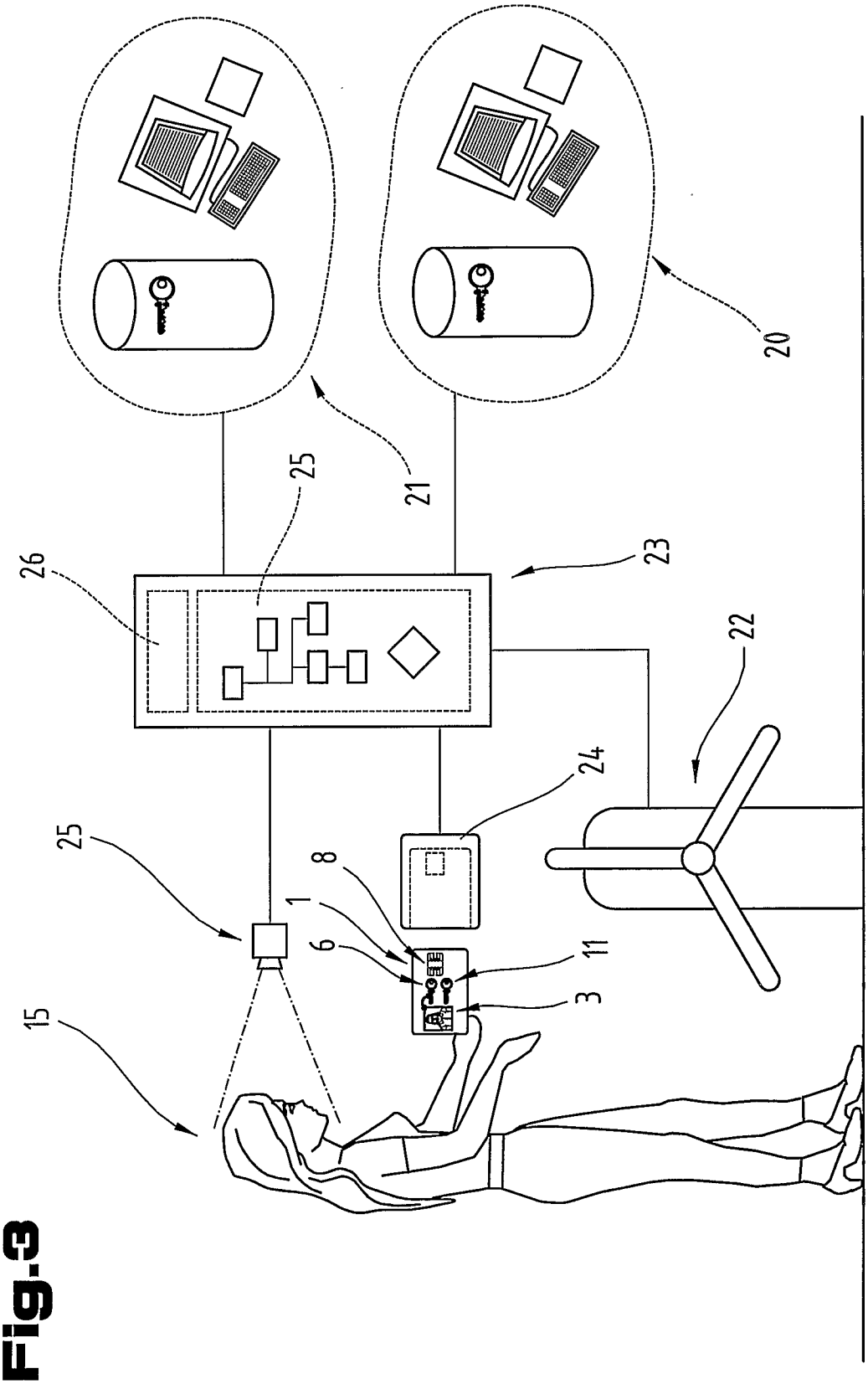


Fig.3

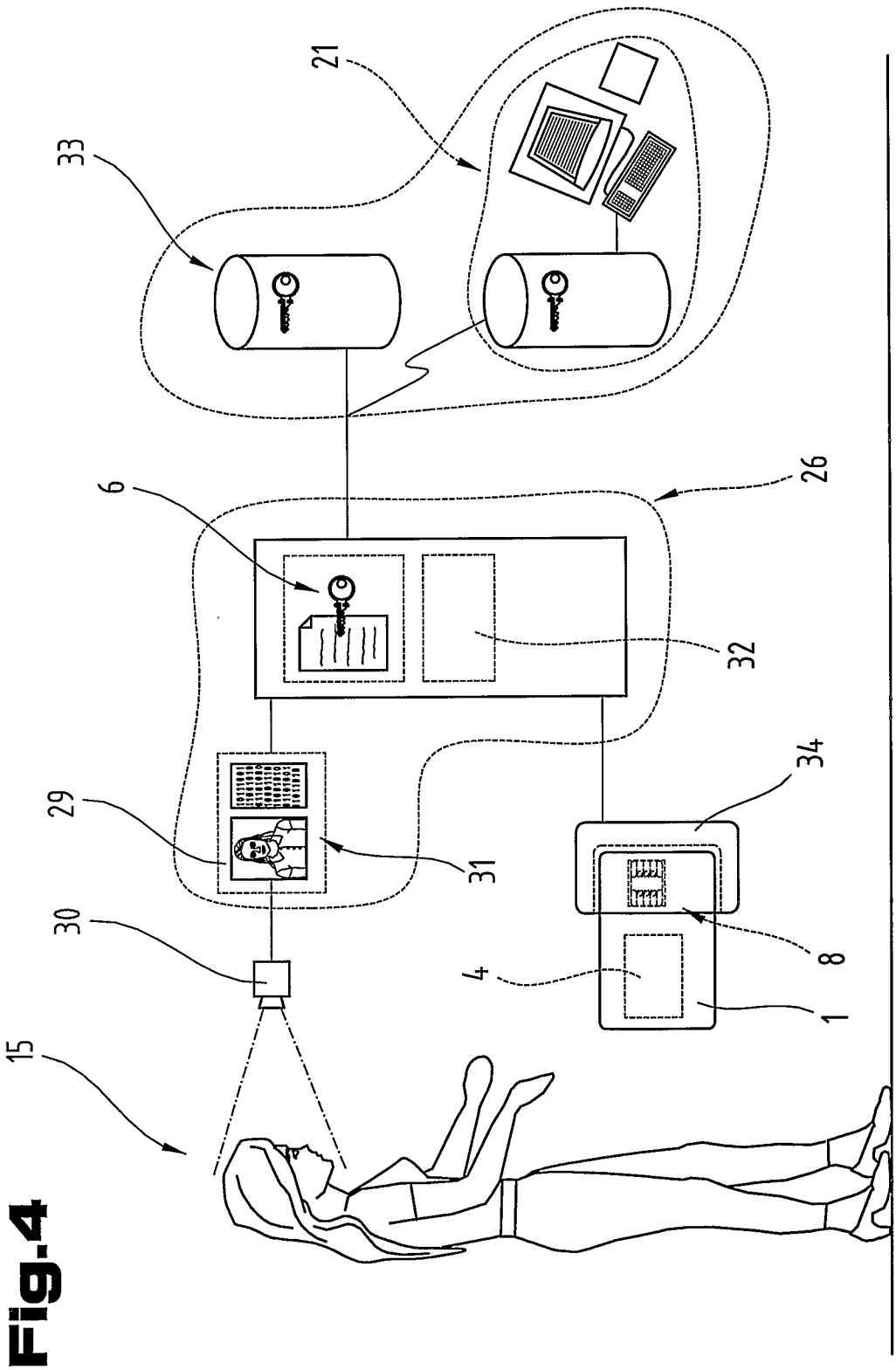


Fig.4

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2009/000388

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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)
G07C

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/269043 A1 (LAUNAY NATHALIE [FR] ET AL) 22 November 2007 (2007-11-22) the whole document	1-26
A	US 6 883 716 B1 (DE JONG EDUARD KAREL [NL]) 26 April 2005 (2005-04-26) abstract; claims 1-7; figures 1-4 column 2, line 56 - column 4, line 5 column 6, line 9 - column 7, line 2	1-26
A	US 2007/204162 A1 (RODRIGUEZ TONY F [US]) 30 August 2007 (2007-08-30) abstract; claim 1; figures paragraphs [0007], [0008], [0011], [0012], [0031] - [0044]	1-26

-/--

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

[X] See patent family 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
19 Januar 2010	26/01/2010

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, Fax: (+31-70) 340-3016	Rother, Stefan

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2009/000388

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/132194 A1 (WARD JEAN R [US]) 16 June 2005 (2005-06-16) abstract; claim 1; figures 1-3 paragraphs [0087] - [0092] paragraphs [0095] - [0097], [0103], [0112]	1-26
A	US 2006/136997 A1 (TELEK MICHAEL J [US] ET AL) 22 June 2006 (2006-06-22) abstract; claims; figures 1,2 paragraph [0028]	1,2,19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/AT2009/000388

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007269043 A1	22-11-2007	CN 101061494 A	24-10-2007
		EP 1653395 A2	03-05-2006
		WO 2006038075 A1	13-04-2006
		JP 2008515311 T	08-05-2008
US 6883716 B1	26-04-2005	AU 777437 B2	14-10-2004
		AU 1586700 A	18-06-2001
		BR 9917573 A	06-08-2002
		CA 2393642 A1	14-06-2001
		CN 1398385 A	19-02-2003
		DE 69932643 T2	05-04-2007
		EP 1236181 A1	04-09-2002
		JP 2003516572 T	13-05-2003
		WO 0143080 A1	14-06-2001
US 2007204162 A1	30-08-2007	WO 2007101076 A2	07-09-2007
US 2005132194 A1	16-06-2005	NONE	
US 2006136997 A1	22-06-2006	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2009/000388

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G07C9/00

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G07C

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2007/269043 A1 (LAUNAY NATHALIE [FR] ET AL) 22. November 2007 (2007-11-22) das ganze Dokument	1-26
A	US 6 883 716 B1 (DE JONG EDUARD KAREL [NL]) 26. April 2005 (2005-04-26) Zusammenfassung; Ansprüche 1-7; Abbildungen 1-4 Spalte 2, Zeile 56 - Spalte 4, Zeile 5 Spalte 6, Zeile 9 - Spalte 7, Zeile 2	1-26
A	US 2007/204162 A1 (RODRIGUEZ TONY F [US]) 30. August 2007 (2007-08-30) Zusammenfassung; Anspruch 1; Abbildungen Absätze [0007], [0008], [0011], [0012], [0031] - [0044]	1-26

-/--

[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
19. Januar 2010	26/01/2010

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Rother, Stefan

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 2005/132194 A1 (WARD JEAN R [US]) 16. Juni 2005 (2005-06-16) Zusammenfassung; Anspruch 1; Abbildungen 1-3 Absätze [0087] - [0092] Absätze [0095] - [0097], [0103], [0112]	1-26
A	US 2006/136997 A1 (TELEK MICHAEL J [US] ET AL) 22. Juni 2006 (2006-06-22) Zusammenfassung; Ansprüche; Abbildungen 1,2 Absatz [0028]	1,2,19

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/AT2009/000388

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2007269043 A1	22-11-2007	CN 101061494 A	24-10-2007
		EP 1653395 A2	03-05-2006
		WO 2006038075 A1	13-04-2006
		JP 2008515311 T	08-05-2008
US 6883716 B1	26-04-2005	AU 777437 B2	14-10-2004
		AU 1586700 A	18-06-2001
		BR 9917573 A	06-08-2002
		CA 2393642 A1	14-06-2001
		CN 1398385 A	19-02-2003
		DE 69932643 T2	05-04-2007
		EP 1236181 A1	04-09-2002
		JP 2003516572 T	13-05-2003
		WO 0143080 A1	14-06-2001
US 2007204162 A1	30-08-2007	WO 2007101076 A2	07-09-2007
US 2005132194 A1	16-06-2005	KEINE	
US 2006136997 A1	22-06-2006	KEINE	