(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 695 33 939 T2** 2005.12.22

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 777 890 B1**
(21) Deutsches Aktenzeichen: **695 33 939.7**
(86) PCT-Aktenzeichen: **PCT/AU95/00545**
(96) Europäisches Aktenzeichen: **95 929 664.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 96/006409**
(86) PCT-Anmeldetag: **25.08.1995**
(87) Veröffentlichungstag der PCT-Anmeldung: **29.02.1996**
(97) Erstveröffentlichung durch das EPA: **11.06.1997**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **19.01.2005**
(47) Veröffentlichungstag im Patentblatt: **22.12.2005**

(51) Int Cl.[7]: **G06K 19/067**
G09F 3/03, G07C 9/00

(30) Unionspriorität:

PM769094	**25.08.1994**	**AU**
PN470295	**09.08.1995**	**AU**

(73) Patentinhaber:
P-Seven Holdings PTY Ltd., Brisbane, AU

(74) Vertreter:
derzeit kein Vertreter bestellt

(84) Benannte Vertragsstaaten:
DE, FR, GB, IT

(72) Erfinder:
CHAPMAN, P., Bryan, Clayfield, AU

(54) Bezeichnung: **IDENTIFIZIERUNGSVERFAHREN**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

[0001] Diese Erfindung betrifft ein Verfahren zum Bereitstellen einer Identifikation.

[0002] Diese Erfindung hat eine bestimmte, aber nicht ausschließliche, Anwendung auf ein Verfahren und eine Vorrichtung zum Identifizieren von Personen und einzigartigen Artikeln, die eine Lebenslange ausgeprägte Identität beibehalten, wie Gemälde und andere Kunstobjekte. Derartige Personen und Artikel werden nachstehend kollektiv als „eine Person oder Personen" bezeichnet.

[0003] Eine positive Identifikation von Personen ist wichtig, um einen nichtautorisierten Zugang oder einen Durchgang von gewählten Orten oder Einrichtungen, wie Banken, Konten etc. und eingeschränkten Gebieten, wie gesicherten Gebäuden und Flughafen-Terminals und dergleichen, zu verhindern. Eine positive Identifikation von Personen ist besonders wichtig für Entscheidungen auf der Regierungsebene bezüglich des Zugangs von Reisenden zu Ländern, insbesondere von internationalen Reisenden.

[0004] Internationale Reisende sind oft unterbrechenden und übermäßigen Verzögerungen auf eine Ankunft an und/oder bei einem Abflug von Flughafen-Terminals ausgesetzt, da Beamte versuchen die Gutgläubigkeit von jedem Reisenden dadurch festzustellen, dass jeder Reisende manuell befragt wird und die Person, die gerade befragt wird, mit der verfügbaren Identifikation, wie Pässen, Speicherlisten und Computerdateien und dergleichen, verglichen wird, mit dem Ziel irgendeinen Reisenden zu identifizieren, der nicht autorisiert ist das Land zu betreten, oder dessen Einzelheiten auf Listen von beschränkten Personen sind. Diese Eintrittsüberprüfung wird auch verwendet, um Einzelheiten einer Bewegung von reisenden Personen in ein und von einem jeweiligen besuchten Land aufzuzeichnen.

[0005] Die gegenwärtig verfügbaren Methoden für eine positive Identifikation einer Person umfassen typischerweise Pässe, die Kenntnis einer eingeschränkten Information, wie ein Kennwort, den Besitz eines eingeschränkten Artikels, wie einen Durchlassschlüssel, oder das physikalische Erscheinungsbild der Person, wie in einem Referenzfoto porträtiert.

[0006] Eine Sicherheit auf Grundlage der Kenntnis von eingeschränkter Information oder einen Besitz eines eingeschränkten Artikels kann ohne eine Entdeckung durchbrochen werden, da die Information von ihrem rechtmäßigen Eigentümer erhalten werden kann. Demzufolge stellt eine derartige Information nicht ein zufriedenstellendes Verfahren für eine positive Identifikation einer Person in sämtlichen Fällen bereit, insbesondere dann, wenn eine derartige Identifikation schnell durchgeführt werden muss.

[0007] Methodologien, die sich auf das physikalische Erscheinungsbild beziehen, wobei diese gewöhnlicherweise als biometrische Techniken bezeichnet werden, wie die Fingerabdruck-Analyse, Thermogramme und die DNA Analyse, werden als weniger empfindlich gegenüber einer falschen Identität angesehen und sind deshalb für Autoritäten attraktiv, aber bislang ist es schwierig gewesen sie erfolgreich zu verwenden. In den meisten Fällen erfordern derartige Methodologien eine immense Datenbank, die die bestimmten biometrischen Daten enthält, wobei eine Lokalisierung und ein Zugriff darauf schwierig und/oder langsam sein kann.

[0008] Ein bekanntes Verfahren zum Verwenden von biometrischen Techniken um für eine Identifikation einer Person für den Zweck der Beschränkung eines Zutritts zu einem Gebiet nur für autorisierte Personen umfasst, dass jede der autorisierten Personen mit einer Karte versehen wird, die biometrische Daten enthält, die spezifisch für jede Person sind. Die Karte kann an einer Lesestation angeboten werden, wo die biometrischen Daten durch einen Kartenleser oder dergleichen gelesen und mit der Person, die die Karte anbietet, verglichen werden. Eine hohe Korrelation zwischen den Kartendaten und den vorübergehend gesammelten Daten der Person, die die Karte anbietet, führt zu einem Zugang und eine niedrige Korrelation führt zu einer Ablehnung. Dieses System verhindert jedoch nicht, dass nicht autorisierte Karten hergestellt werden, die verwendet werden können, um einen nicht autorisierten Zugang zu einer Einrichtung zu erhalten.

[0009] Ein anderes bekanntes Verfahren umfasst das Vergleichen der biometrischen Daten auf einer Karte, die durch eine Person angeboten wird, mit einer früher geschaffenen Datenbank von biometrischen Daten von autorisierten Personen. Ein derartiges System kann durch Personen überlistet werden, die eine Karte von ihrem rechtmäßigen Besitzer erhalten haben.

[0010] Die WO 94/10659, gegenüber der die Ansprüche abgegrenzt sind, offenbart ein Kreditkartenbetrugs-Beseitigungssystem mit einer Datenbank mit Fingerabdruckdaten, die zu einer Kontonummer gehören. In einem Registrierungsschritt füllt der Kunde eine Fingerabdruckform (die versendet wird) aus, deren Daten digitalisiert und durch die Finanzinstitution gespeichert wird. In einem Laden wird die Kontonummer von der Kreditkarte gelesen. Ein Fingerabdruck des Benutzers wird an dem Terminal gescannt und an den zentralen Computer für einen Vergleich mit vorher gespeicherten Daten, die zu der Kontonummer gehören, gesendet. Der Kaufmann (ebenfalls identifiziert) weist einen Fingerabdruckleser (ein festes Terminal oder eine mobile Kartenüberprüfungs-

vorrichtung) auf, die mit der Finanzinstitution verbunden ist (über eine Leitung oder über Funk), um den Kartenhalter-Fingerabdruck mit den vorher gespeicherten Daten zu vergleichen.

[0011] Die EP-A-520 455 beschreibt einen Gepäckanhänger zur Verwendung mit einem computerisierten Flugzeuggepäck-Verwaltungssystem; er umfasst einen Signalprozessor zur Speicherung von Information und eine TX-RX Einrichtung zur Kommunikation mit einem Gepäckbehandlungscomputer. Anhänger werden aus Daten erzeugt, die auf einem Boarding-Ticket gespeichert sind. Gepäck wird in Übereinstimmung mit Daten, die in dessen Anhänger aufgezeichnet sind, an das richtige Flugzeug und einen richtigen Container geleitet. Ein Anhänger-Leser vor dem Container überträgt Daten an einen Hostcomputer über eben aufgenommenes Gepäck. An dem Boarding-Gate wird Information an den Hostcomputer über irgendwelche eben eingestiegene Passagiere übertragen. Der Hostcomputer führt eine Gepäcküberprüfung aus und nimmt ein Gepäckstück, welches zu nicht eingestiegenen Passagieren gehört, heraus.

[0012] Das US Patent 4495496 offenbart ein Personen überwachungs- und -lokalisierungssystem zur Verwendung in Minen, unter Verwendung von RFID Anhängern, deren Antworten auf das Abfragesignal zeitlich verzögert ist, um Interferenzen zu vermeiden.

[0013] Das US Patent 5189396 betrifft einen elektronischen Sicherheitsverschluss für Transportcontainer.

[0014] Die vorliegende Erfindung zielt darauf ab wenigstens einen der obigen Nachteile zu beseitigen und ein Verfahren zum Bereitstellen einer Identifikation bereitzustellen, welches bei der Verwendung zuverlässig und effizient sein wird.

[0015] Diese Erfindung in einem Aspekt besteht in einem Verfahren zum Bereitstellen einer Identifikation einer Person, wie in dem Anspruch 1 aufgeführt.

[0016] Die Identifikationsdaten, die in der Datenbank enthalten sind, umfassen eine biometrische Information, beispielsweise Thermogramme, Fingerabdrücke, Fotografien, Sprachproben; DNA Sequenzen oder dergleichen. Die biometrische Information ist eine Information, die nicht-invasiv ermittelt werden kann, und geeigneterweise eine Information, die durch Abbilden einer Person von einem entfernten Ort ermittelt oder eingefangen werden kann. Wenn die Person nicht ein lebender Organismus ist, dann können andere identifizierbare Attribute, wie Oberflächenbilder oder akustische Antwortmuster verwendet werden und die Daten, die diese Attribute darstellen, können von Zeit zu Zeit aktualisiert werden, um eine Verschlechterung oder Änderungen in dem Artikel zu berücksichtigen.

[0017] Vorzugsweise enthält die Datenbank ein geschütztes Paket von Identifikationsdaten in Bezug auf jede Person. Das geschützte Paket von Identifikationsdaten kann mehr als ein identifizierbares Attribut, wie ein Thermogramm oder einen Fingerabdruck, darstellen. Jedes Paket kann zu einem oder mehreren Nur-Hinzufügungs (add/on)-Dateien gehören, die historische oder andere Informationen aufzeichnen können, zum Beispiel medizinische Einzelheiten wie die Blutgruppe für den Fall einer Person.

[0018] Die Datenbank kann angeordnet werden, um existierende Daten zu überprüfen, bevor eine Eingabe eines identifizierbaren Attributs, das sich auf eine Person bezieht, genehmigt wird, um so sicherzustellen, dass Daten, die spezifisch für jede Person sind, mit nur einer einzigartigen Beschreibung verknüpft sind und/oder eine Anordnung kann getroffen werden, um kontinuierlich die Daten zu scannen, wobei nach irgendwelchen Fehlübereinstellungen oder definierten Ähnlichkeiten geprüft wird, die die Existenz von mehr als einer Beschreibung für eine Person anzeigen können, das heißt einen Betrug.

[0019] Die einzigartige Beschreibung kann irgendeine Information oder Daten, wie beispielsweise eine Adresse in einer Datenbank, und ausreichend zum Isolieren einer Datei in Bezug auf eine Person in einer Datenbank sein und kann den Namen der Person, den Geburtstag, die Nationalität und ähnliche Charakteristiken einschließen. Vorzugsweise ist die einzigartige Beschreibung jedoch ein einzigartiger Dateicode, der zu der Person gehört. Die einzigartige Beschreibung kann in Übereinstimmung mit einem internationalen Standard angeordnet werden, um so eine positive Identifikation von Personen auf einer globalen Grundlage zu ermöglichen.

[0020] Vorzugsweise ist die einzigartige Beschreibung nur von einer Maschine lesbar und von einem Typ, der durch eine Schutzeinrichtung geschützt werden kann. Die Schutzeinrichtung kann eine Codierung oder Verschlüsselung der einzigartigen Beschreibung sein oder sie kann ein gesicherter Zugangscode oder ein Zugangsstil sein oder umfassen.

[0021] Vorzugsweise wird die Identifikationseinrichtung eine Identifikationseinrichtung wie nachstehend beschrieben.

[0022] Eine Identifikationseinrichtung umfasst:
eine Trägereinrichtung, und
eine einzigartige Beschreibung, die durch die Trägereinrichtung geführt wird.

[0023] Die Trägereinrichtung kann eine Karte, ein Token, eine Plakette oder dergleichen sein und die einzigartige Beschreibung kann darauf in irgend ei-

ner lesbaren Form enthalten sein. Vorzugsweise ist die einzigartige Beschreibung von einem entfernten Ort über eine Maschine lesbar. Zum Beispiel kann die einzigartige Beschreibung durch ein entferntes Abbildungssystem oder einen Laser- oder einen Infrarot-Strahlungsscanner oder dergleichen lesbar sein. Vorzugsweise ist die Identifikationseinrichtung ansprechend auf ein Funkfrequenzsignal, wobei die einzigartige Beschreibung für einen Empfang durch eine entfernte Empfangsstation übertragen wird.

[0024] Die Trägereinrichtung kann andere Informationen als die einzigartige Beschreibung tragen bzw. führen. Zum Beispiel kann sie Informationen darüber führen, welche von mehreren Datenbanken die Identifikationsdaten führt die bestimmte Person, die unter Untersuchung steht, enthält, wodurch einer Lesestation ermöglicht wird die relevante Datenbank schnell zu lokalisieren. Eine derartige zusätzliche Information kann auch mit der einzigartigen Beschreibung übertragen werden. Vorzugsweise trägt jedoch die Trägereinrichtung in geeigneter Weise keine Information vom Wert über irgendeine andere Person als die Person, für die sie ausgegeben wurde, wobei die Einrichtung nur ermöglicht, dass ein Zugang zu den Identifikationsdaten in Bezug auf diese Person erhalten wird.

[0025] Die Identifikationseinrichtung kann auch eine Unterscheidungseinrichtung einschließen, mit der eine Empfangsstation die Identifikationseinrichtung von anderen üblicherweise getragenen programmierbaren Karten und ähnlichen Einrichtungen unterscheiden kann. Die Unterscheidungseinrichtung kann eine eingebaute Zeitverzögerung einschließen, wobei andere Einrichtungen ihre Signale vor der Übertragung durch die Identifikationseinrichtung übertragen, wodurch einem Empfänger erlaubt wird diese Signale von den Signalen, die durch die programmierbaren Karten übertragen werden, und ähnlichen von denjenigen, die durch die Identifikationseinrichtung übertragen werden, zu unterscheiden und diese entsprechend zu löschen.

[0026] Die Identifikationseinrichtung kann eine Zugriffseinrichtung umfassen, die dafür ausgelegt ist, um einen Zugriff bzw. einen Zugang auf die Empfangsstation bereitzustellen, so dass die Empfangsstation sich selbst vorbereitet, um die einzigartige Beschreibung nur nach dem sie durch die Zugriffseinrichtung geöffnet ist, zu empfangen. Zum Beispiel kann die Zugriffseinrichtung einen spezifischen Signalstrom umfassen der durch die Empfangsstation erkannt wird. Die Identifikationseinrichtung kann ferner eine Validierungseinrichtung umfassen, um die Gültigkeit der Information zu überprüfen, die in früheren Signalen enthalten ist. Vorzugsweise ist die Validierungseinrichtung derart angeordnet, dass irgendein Herumhantieren oder eine Manipulation an der einzigartigen Beschreibung oder einer anderen Information, die in der Identifikationseinrichtung enthalten ist, oder irgendeine Herumhantierung bzw. Manipulation von Komponenten der Identifikationseinrichtung dazu führen wird, dass die Identifikationseinrichtung für eine Untersuchung gekennzeichnet wird und gleichzeitig einen Empfang von irgendeiner verfügbaren Information durch die Empfangsstation für eine Speicherung an der Empfangsstation in der Nur-Hinzuführung (add-on)-Datei ermöglichen wird.

[0027] Die Identifikationseinrichtung umfasst eine Verschlüsselungseinrichtung, wobei Information, die von der Identifikationseinrichtung an eine Empfangsstation übertragen wird, nur durch eine Empfangsstation verstanden werden kann, die eine entsprechende Dekodierungseinrichtung verwendet.

[0028] Wenn die Trägereinrichtung eine Kartenidentifikation ist, werden Daten, die spezifisch für jede ausgegebene Karte sind, vorzugsweise in einer Datenbank geführt, die in geeigneter Weise mit einer Datenbank verknüpft/assoziiert sein kann, die Identifikationsdaten enthält, die spezifisch für die Person sind, für die die Karte ausgegeben wurde. Derartige spezifische Kartendaten können zum Beispiel ein Muster oder eine Orientierung umfassen, die auf eine Stirnfläche der Karte angewendet und durch ein Bildlesegerät lesbar ist. Alternativ können die kartenspezifischen Daten ein individuelles Signal sein, welches in einem Transponder enthalten ist und von einem entfernten Ort lesbar ist.

[0029] Damit sich diese Erfindung leichter verstehen lässt und um diese in der Praxis umzusetzen, werden nachstehend auf die beiliegenden Zeichnungen Bezug genommen, die eine bevorzugte Ausführungsform der Erfindung darstellen. In den Zeichnungen zeigen:

[0030] **Fig.** 1a eine Diagrammdarstellung einer Identifikationskarte gemäß der Erfindung, und

[0031] **Fig.** 1b eine Diagrammdarstellung einer anderen Identifikationskarte gemäß der Erfindung,

[0032] Fig. 2 eine diagrammartige Darstellung eines Verfahrens zum Erleichtern der Reise von autorisierten Personen gemäß der Erfindung und

[0033] Fig. 3 und Fig. 4 diagrammartige Darstellungen der Zwischenverbindung von relevanten funktionalen Gebieten und Datenbanken für die Implementierung eines Systems gemäß der Erfindung.

[0034] Die auf eine Funkfrequenz ansprechende Identifikationskarte **10** die in **Fig.** 1a dargestellt ist, umfasst eine flexible Plastikbasisschicht **11** in Brieftaschengröße, die um eine zentral angeordnete Halterungslinie **12** faltbar ist, die die Karte in einen Infor-

mationsabschnitt **13** und einen Validierungsabschnitt **14** aufteilt. Der Informationsabschnitt **13** umfasst eine schaltungsartige Antenne **15**, die in der Basisschicht **11** zum Empfangen von Signalen eingebettet ist. Die Antenne **15** ist betriebsmäßig mit einem Eingabetransponder **16**, einem Beschreibungstransponder **17** und einem Validierungstransponder **18** verbunden. Der Validierungstransponder ist auf dem Validierungsabschnitt **14** angeordnet, wobei die Verbindung dazu über die Halterungslinie **12** durch leitende Bahnen **19** und **20** geht. Eine Zeitverzögerungskomponente **21** ist angeordnet, um eine Zeitverzögerung zwischen einem Empfang eines Funkfrequenzsignals und einer Aussendung eines Antwortsignals bereitzustellen.

[0035] Die Transponder **16**, **17** und **18** sind angeordnet, um in einer Sequenz im Ansprechen auf ein Funkfrequenzsignal, das von einer angrenzenden Sende- und Empfangstation übertragen wird, zu berichten.

[0036] Der Eingabetransponder **16** umfasst eine Eingabeschlüsselkomponente **22**, die konfiguriert ist, um einen Lesestations-Zugriffscode an die Empfangsstation zu übertragen, wodurch die Empfangsstation über einen gültigen Signalteil gewarnt wird. Die Empfangsstation wird dadurch vorbereitet zum Empfangen von weiteren Signalteilen von den Transpondern **16**, **17** und **18**. Die Komponente **22** verhindert effektiv die Empfangsstations-Verarbeitung von irgendeinem Signal, welches nicht mit dem Zugriffscode beginnt. Der Transponder **16** enthält auch Informationen darüber, welche Datenbank die Personen-Identifikationsdatei enthält.

[0037] Der Beschreibungstransponder **17** ist eine integrierte Schaltung, die ein Signal überträgt, das die einzigartige Beschreibung, die der Person zugewiesen wird, für die die Karte ausgegeben wird, und eine Identifikation der Ausgabestation, die die Karte ausgegeben hat, anzeigt. Der Beschreibungstransponder **17** überträgt sein Signal direkt nach dem Transponder **16**.

[0038] Der Transponder **18** ist eine integrierte Schaltung, die einen Validierungs- und Verschlüsselungscode enthält. Der Verschlüsselungscode ist für die Karte einzigartig und arbeitet mit dem Dateinortscode zusammen, sodass das Signal, das durch die Empfangsstation aufgezeichnet wird, ein Paket von Informationen mit einem einzigartigen Identifizierer ist, der durch eine entsprechende Dekodierungseinrichtung dekodiert werden muss, die zu der Empfangsstation gehört.

[0039] Die auf eine Funkfrequenz ansprechende Identifikationskarte **10**, die in **Fig.** 1b dargestellt ist, umfasst Komponenten, wie in Bezug auf **Fig.** 1a beschrieben. Jedoch umgibt in dieser Ausführungsform der Validierungsabschnitt den Informationsabschnitt, wobei die leitenden Bahnen **19** und **20** effektiv die Antenne **15** umgeben.

[0040] Bei der Verwendung überträgt die Sende- und Empfangsstation, die typischerweise sowohl an der Abfahrtstation als auch der Ankunftsstation angeordnet ist, ein Befähigungssignal mit einer bestimmten Frequenz für eine vorgegebene Zeitperiode. Sämtliche Karten, die bei dieser Frequenz und innerhalb des bestimmten Bereichs oder der bestimmten Zone arbeiten, wie derartige, die durch eine einzelne Person getragen werden, können durch das Befähigungssignal aktiviert werden. Die Identifikationskarte wird durch das Signal aktiviert, antwortet aber im Gegensatz zu den anderen Karten nicht sofort wegen der eingebauten Antwortzeitverzögerung. Die Länge der Zeitverzögerung wird so eingestellt, um eine ausreichende Zeit bereitzustellen, damit sämtliche Karten, die bei der gleichen Frequenz unter Umständen aktiviert werden sollen, ihre Nachrichten übertragen, um so zu ermöglichen, dass ein Signal, welches danach durch die Identifikationskarte übertragen wird, identifiziert und klar und ununterbrochen durch die Empfangsstation empfangen wird.

[0041] An dem Ende der bestimmten Zeitverzögerung überträgt der Eingabe- bzw. Eintritts-Transponder **16** sein Signal an die Empfangsstation, die dann Vorbereitungen zum Empfangen eines Nachrichtensignals von dem Beschreibungstransponder **17** und eines Validierungssignals von dem Validierungstransponder **18** trifft.

[0042] Wenn das Validierungssignal wie erwartet empfangen wird, arbeitet der Verschlüsselungscode, der in dem Signal enthalten ist, das durch den Validierungstransponder **18** übertragen wird, mit den Nachrichten von den Transpondern **16** und **17** zusammen, um eine verschlüsselte Nachricht bereitzustellen, die als ein Paket einer Fertig-zum-Senden-Information durch die Empfangsstation empfangen wird. Wenn der Validierungstransponder **18** nicht antwortet oder eine Diskrepanz in dem Signal von dem Beschreibungstransponder **17** anzeigt, dann ist es nicht möglich, dass die durch den Transponder **17** übertragene Nachricht durch den einzigartigen Verschlüsselungscode, der von dem Transponder **18** getragen wird, verschlüsselt wird. Jedoch wird die Nachricht danach durch einen Verschlüsselungscode verschlüsselt, der spezifisch für die bestimmte Empfangsstation ist, die die Karte liest. Demzufolge wird die Nachricht als ein gekennzeichnetes Paket von Information vorbereitet, wobei eine Anzeige bereitgestellt wird, dass die Person eine weitere Untersuchung erfordert.

[0043] Die Erleichterung der Reise durch autorisierte Personen ist schematisch in den Fig. 2, Fig. 3 und Fig. 4 dargestellt und wird nachstehend beschrieben. Personen, die international reisen wollen, beantra-

gen eine Identifikationskarte des voranstehend beschriebenen Typs und erhalten diese. Die Karte wird durch eine Kartenausgabestation ausgegeben, an der die geeignete eineinzigartige Beschreibung in die Karte einprogrammiert wird. Entweder gleichzeitig oder danach werden die biometrischen Daten der Wahl, die einzigartig für jede Person sind, und in geeigneter Weise ein Thermogramm vorbereitet und (vorzugsweise in digitaler Form) in der Datenbank der Datei-Haltestation an einen Dateiort, der durch die einzigartige Beschreibung bestimmt wird, gespeichert. Das Thermogramm ist in einer geeigneten Weise von dem Typ, der in dem US Patent Nr. 5163094 von Prokowski beschrieben wird.

[0044] Die Person kann danach den Wunsch anzeigen nach Australien zu reisen. Ein derartiger Wunsch kann zum Beispiel durch den Kauf eines Fluglinientickets oder durch einen Antrag für ein Visum angezeigt werden. Die Personenidentifikationskarte kann zu dieser Zeit gelesen werden und das Fluglinienticket würde in den Namen der Person, für den die Karte ausgegeben wurde, erstellt werden.

[0045] Zu dieser Zeit würde die add-on Datei der Person in der nationalen Datenbank aktualisiert werden, um zu zeigen, dass er/sie für eine Reise nach Australien autorisiert ist und dort über eine spezifische Zeitperiode bleiben. Auf eine Aktualisierung dieser add-on Datei hin kann der Person eine geeignete Empfangsbestätigung oder ein Ticket für ihren eigenen Nutzen und eigene Aufzeichnungen gegeben werden, obwohl eine derartige Empfangsbestätigung nicht für irgendeinen offiziellen Zweck verwendet werden würde.

[0046] In einer bevorzugten Ausführungsform wird das Thermogramm von Personen oder andere biometrische Daten aus der Datenbank ausgelesen oder zu dieser Zeit vorbereitet und in einer Abfahrtsstations-Datenbank gespeichert, die angeordnet ist, um Thermogramme in Bezug auf Personen, die für jeden bestimmten Flug per Ticket vorgesehen sind, zu vergleichen. Demzufolge wird eine Information, die spezifisch für jede Person ist, so wie eine Information in Bezug auf eine autorisierte Länge des Besuches und dergleichen oder eine andere Information, die einen schnellen und einfachen Zugriff auf diese Information erlaubt, in Bezug auf jede Person auf einem bestimmten Flug als ein Paket von Identifikationsdaten vor der Zeit einer Abfahrt (eines Abflugs) erstellt.

[0047] Wenn sich Passagiere in Richtung auf die Abfluglounge hin oder durch die Abflug-Gates bewegen, werden sie zum Beispiel durch einen entfernten Scanner gescannt, um ein gegenwärtiges Thermogramm zu schaffen, welches sofort mit dem Thermogramm verglichen werden kann, welches in die Abflugstations-Datenbank geladen ist, um positiv jeden Passagier zu identifizieren.

[0048] Diejenigen Passagiere, die positiv als autorisierte Passagiere durch eine ausreichende Korrelation zwischen dem gegenwärtigen Thermogramm und dem Abfahrtsstations-Datenbankenthermogramm als autorisiert identifiziert werden, erhalten einen nicht unterbrochenen Durchgang zu den ablegenden Flugzeug. Diejenigen Passagiere, für die die Korrelation unter dem erforderlichen Niveau ist, werden an ein bestimmtes Gebiet für eine weitere Identifikation geführt. Dieser Prozess wird für sämtliche Personen ausgeführt, die das Flugzeug besteigen (ein Boarding durchführen).

[0049] Die Abfahrt- bzw. Abflugstation kann auch eine Datenbank mit verbotenen Personen enthalten, auf die vorzugsweise zum Vergleich mit sämtlichen Passagieren zugegriffen wird. Irgendeine Person, die als ein verbotener Passagier identifiziert wird, kann davon abgehalten werden ein Boarding des Flugzeugs durchzuführen.

[0050] Gleichzeitig oder in einer zeitgerechten Weise während des Flugs wird das Paket von Informationsdaten, die sämtliche Passagierdaten enthalten, an die Zielstation übertragen, wo es in der Zielstations-Datenbank gespeichert wird. Diejenigen Personen, die nicht positiv in der kurzen Periode vor einem Boarding identifiziert werden und denen erlaubt wird einzusteigen werden weiter während der relativen langen Periode untersucht, in der sich das Flugzeug in Transit befindet. Demzufolge werden diejenigen Passagiere, für die eine Autorisierung schließlich hergestellt wird, mit einem einfachen Zutritt zu dem Zielflughafen versehen, und diejenigen, die nicht positiv identifiziert worden sind, werden für eine weitere Identifikation interniert.

[0051] An dem Zielflughafen gehen sämtliche Passagiere an einer Scanstation vorbei, wo die Identifikationskarte jedes Passagiers entfernt gelesen wird, wodurch ermöglicht wird, dass das gespeicherte Thermogramm für diese Karte zurück gewonnen wird. Jeder Passagier wird gleichzeitig durch einen entfernten thermografischen Scanner, der auf die Person fokussiert ist, die die erfasste Karte trägt, als Thermogramm abgebildet. Die Thermogramme werden verglichen und wenn eine ausreichende Korrelation erreicht wird, gehen derartige Personen weiter zu ihrem Zielort ohne eine weitere Unterbrechung durch Beamte durch Wähl-Gates, die durch das Überwachungsgerät automatisch betätigt werden können. In geeigneter Weise fangen die Auswahl-Gates in einer unauffälligen Weise nicht autorisierte Personen für eine sichere weitere Untersuchung ein. Die add-on (Hinzuführungs-) Datenbank kann zu dieser Zeit automatisch aktualisiert werden, um die Ankunft von jedem Passagier in dem Zielland aufzuzeichnen.

[0052] Alternativ kann der Abflug-Flughafen die Information, die auf den Identifikationskarten von Personen enthalten ist, auf einem Flug verpacken und diese an die Ankunfts-Zielstelle senden, die das Paket von Identifikationsdaten für deren Verwendung, um einen freien Durchgang von gutgläubigen aussteigenden Reisenden zu erleichtern, zusammenstellt.

[0053] Vorzugsweise weist jede Station, die auf die Datenbank zugreifen kann, einen individuellen Stationszugriffscode auf und jeder Betreiber, der eine derartige Station bemannt, hat einen individuellen Betreibercode. In geeigneter Weise wird diese Information zu der Nur-Hinzufügungs(add-on)-Datei jedes Mal hinzugefügt, wenn ein Zugriff durchgeführt oder versucht wird. In geeigneter Weise wird eine Autorisierung für einen Zugriff auf die Datenbank in einer ähnlichen Weise bereitgestellt, wobei eine biometrische Korrelation benötigt wird. Demzufolge wird eine Auditaufzeichnung von Aktionen geführt und eine Aufzeichnung von autorisierten Bewegungen von jeder Person wird in einer derartigen Weise aufgezeichnet, dass ein Geschichtsbericht mit Einzelheiten des Betreibers, der die Datei aktualisiert, festgestellt werden kann.

[0054] Ausländische Reisende in einem Host-Land müssen nur ihre Identifikationskarten tragen. Wenn sie gefragt werden, ob sie autorisiert sind in dem bestimmten Land zu sein, müssen sie nur einen Regierungsbeamten an eine Lesestation begleiten, wo ein gegenwärtiges Thermogramm herausgenommen werden kann und wo deren Identifikationskarten verwendet werden können, um auf die nationale Datenbank zuzugreifen, um ein Thermogramm jeder Person und autorisierte Reise-Einzelheiten auszulesen.

[0055] Zusätzlich zu den voranstehenden Ausführungen könnte diese Erfindung verwendet werden, um Personen zu überwachen, die in ein gesichertes Gebiet eintreten und dieses verlassen, beispielsweise zur Überwachung von Grenzüberschreitungen oder von Gefängnissen. Ferner kann das Verfahren zum Bereitstellen einer Identifikation verwendet werden, um die Identität von Personen festzustellen, die eine medizinische Behandlung durchlaufen. Zum Beispiel kann die Datenbank eine Information in Bezug auf eine medizinische Bedingung, eine Blutgruppe oder dergleichen einschließen und eine derartige Information kann von Krankenhausangestellten auf einen Empfang einer Bestätigung einer Identität einer verletzten Person hin verwendet werden, anstelle dass sofort Bluttests ausgeführt werden, um die Blutgruppe der Person zu bestimmen In vorteilhafter Weise wird ein derartiges Verfahren Zeit einsparen. Alternativ könnte ein Mediziner Medikamente oder eine Behandlung für einen entfernten Patienten auf die Feststellung der Identität des Patienten durch das voranstehende Verfahren sicher bei der Kenntnis verschreiben, das die Identität der Person richtig festgestellt worden ist.

Patentansprüche

1. Verfahren zum Bereitstellen einer Identifikation von einer Person, umfassend die folgenden Schritte:
Führen einer Datenbank von Identifikationsdaten, die jeweils wenigstens einen Typ von nicht-invasiv bestimmbarem biometrischem Attribut einschließen, das in der Lage ist jeweilige Personen zu unterscheiden, wobei einige der Personen eingeschränkte Personen sind, um eine Identifikation einer Person mit Hilfe der Identifikationsdaten zu ermöglichen,
Versehen der jeweiligen Identifikationsdaten mit einer einzigartigen Beschreibung,
Bereitstellen einer Identifikationseinrichtung für eine Mitführung durch jede besagte Person und enthaltend die einzigartige Beschreibung,
Bereitstellen einer Empfangsstation in Kommunikation mit der Datenbank,
wobei die Empfangsstation:
wenigstens ein nicht-invasiv bestimmbares biometrisches Attribut der Person eines Typs gespeichert durch die Datenbank bestimmt,
die einzigartige Beschreibung, die in der Identifikationseinrichtung enthalten ist, die von der Person mitgeführt wird, liest,
auf die Datenbank zugreift, um die Identifikationsdaten zu bestimmen, die der einzigartigen Beschreibung entsprechen,
das Attribut, das durch die Empfangsstation bestimmt wird, mit dem entsprechenden Attribut, das in den Identifikationsdaten auf der Datenbank eingeschlossen ist, vergleicht, und
den Weitergang der Person, wenn eine ausreichende Korrelation zwischen dem Attribut, das durch die Empfangsstation bestimmt wird, und dem Attribut auf der Datenbank nicht gefunden wird, unterbricht,
dadurch gekennzeichnet, dass
die einzigartige Beschreibung so gewählt und verschlüsselt wird, dass sie die Identifikationsdaten durch eine nicht autorisierte Verarbeitung oder Entschlüsselung nicht hervorbringen kann, um dadurch die Identifikationseinrichtung für eine andere Person als die Person, an die die Identifikationseinrichtung herausgegeben wird, wertlos zu machen,
die Identifikationseinrichtung ferner eine Validierungseinrichtung einschließt, die angeordnet ist, um eine Herumhantierung an der einzigartigen Beschreibung zu erfassen, zum Ausgeben eines Validierungssignals, das anzeigt, ob herumhantiert worden ist,
und einen Transponder zum Übertragen der einzigartigen verschlüsselten Beschreibung und des Validierungssignals,
und die Empfangsstation ausgelegt ist, um den Transponder zu triggern, um die einzigartige verschlüsselte Beschreibung und das Validierungssignal zu übertragen, und um einen Verifizierfehler durch die Validierungseinrichtung anzuzeigen, um den Wei-

tergang der Person zu unterbrechen.

2. Verfahren nach Anspruch 1, wobei die Identifikationseinrichtung eine Karte umfasst.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Karte eine Oberfläche mit einem Muster oder einem Ornament, angebracht an einer Stirnfläche der Karte und ausgelegt, um durch einen Bildleser gelesen zu werden, einschließt.

4. Verfahren nach Anspruch 1, 2 oder 3, gekennzeichnet durch den weiteren Schritt zum Bereitstellen eines Prüfpfads von Datenbanktransaktionen, an denen Daten beteiligt sind, die sich auf eine besagte Person beziehen.

5. Verfahren nach irgendeinem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Identifikationseinrichtung ferner eine Unterscheidungseinrichtung einschließt, mit der eine Empfangsstation die Identifikationseinrichtung von anderen auf Funkfrequenzen ansprechende Einrichtungen unterscheiden kann.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass die Unterscheidungseinrichtung eine eingebaute Zeitverzögerung zum Verzögern der Übertragung eines Signals durch den Transponder einschließt.

7. Verfahren nach Anspruch 6, gekennzeichnet durch eine Zugriffseinrichtung, die dafür ausgelegt ist, um ein Zugriffssignal an der Empfangsstation bereitzustellen.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass die Zugriffseinrichtung einen spezifischen Signalstrom einschließt.

9. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass eine verschlüsselte Information, die von der Identifikationseinrichtung an eine Empfangsstation übertragen wird, nur durch eine Empfangsstation verstanden werden kann, die einen entsprechenden Entschlüsselungscode verwendet, der zum Decodieren der verschlüsselten Information geeignet ist.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

Fig. 1(a)

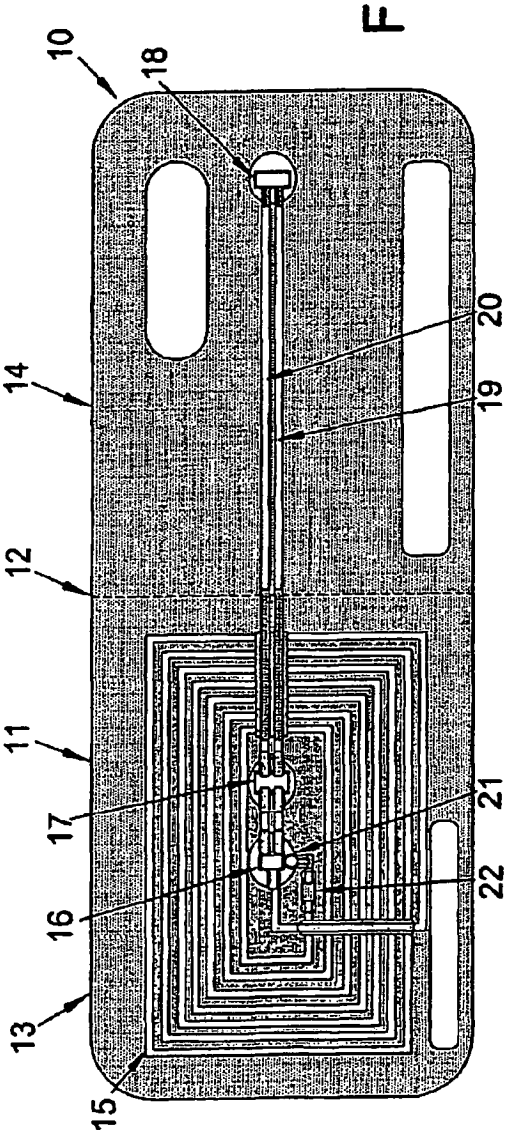
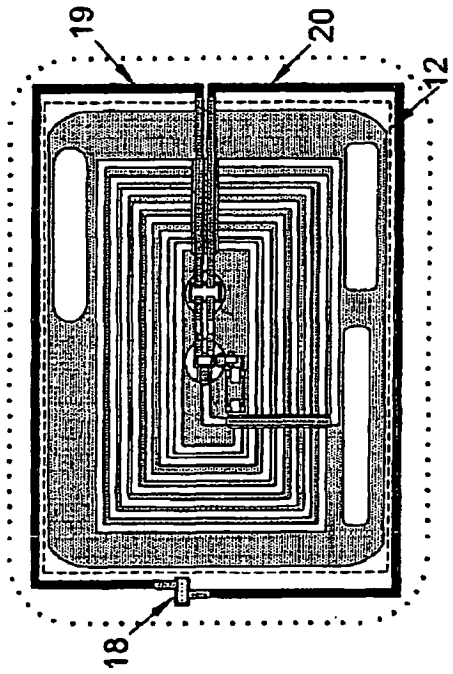


Fig. 1(b)



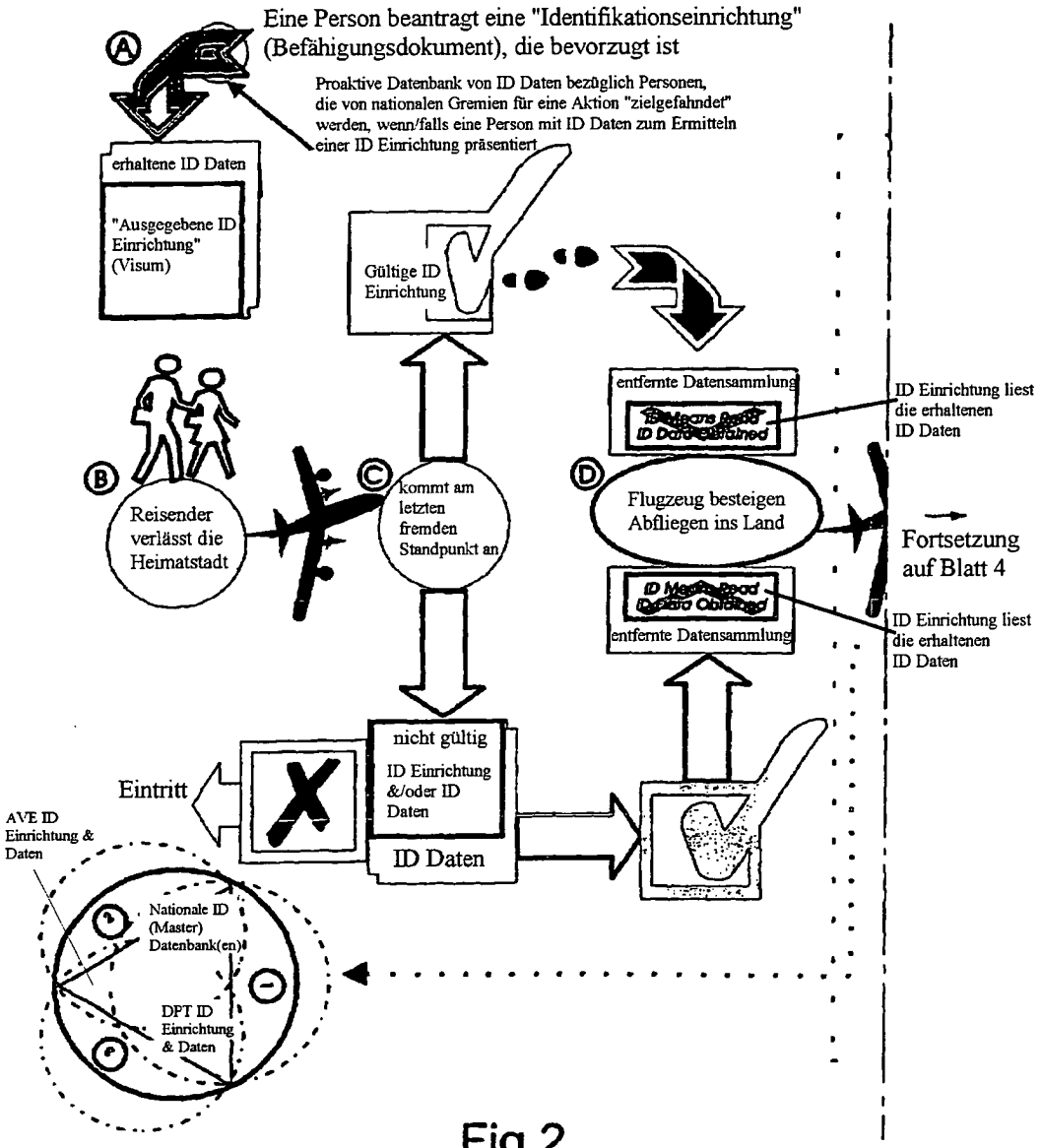

Eine Person beantragt eine "Identifikationseinrichtung" (Befähigungsdokument), die bevorzugt ist
Proaktive Datenbank von ID Daten bezüglich Personen, die von nationalen Gremien für eine Aktion "zielgefahndet" werden, wenn/falls eine Person mit ID Daten zum Ermitteln einer ID Einrichtung präsentiert
A
erhaltene ID Daten
"Ausgegebene ID Einrichtung" (Visum)
Gültige ID Einrichtung
entfernte Datensammlung
ID Einrichtung liest die erhaltenen ID Daten
B
Reisender verlässt die Heimatstadt
C
kommt am letzten fremden Standpunkt an
D
Flugzeug besteigen Abfliegen ins Land
Fortsetzung auf Blatt 4
entfernte Datensammlung
ID Einrichtung liest die erhaltenen ID Daten
nicht gültig
ID Einrichtung &/oder ID Daten
ID Daten
Eintritt
AVE ID Einrichtung & Daten
Nationale ID (Master) Datenbank(en)
DPT ID Einrichtung & Daten

Fig.2

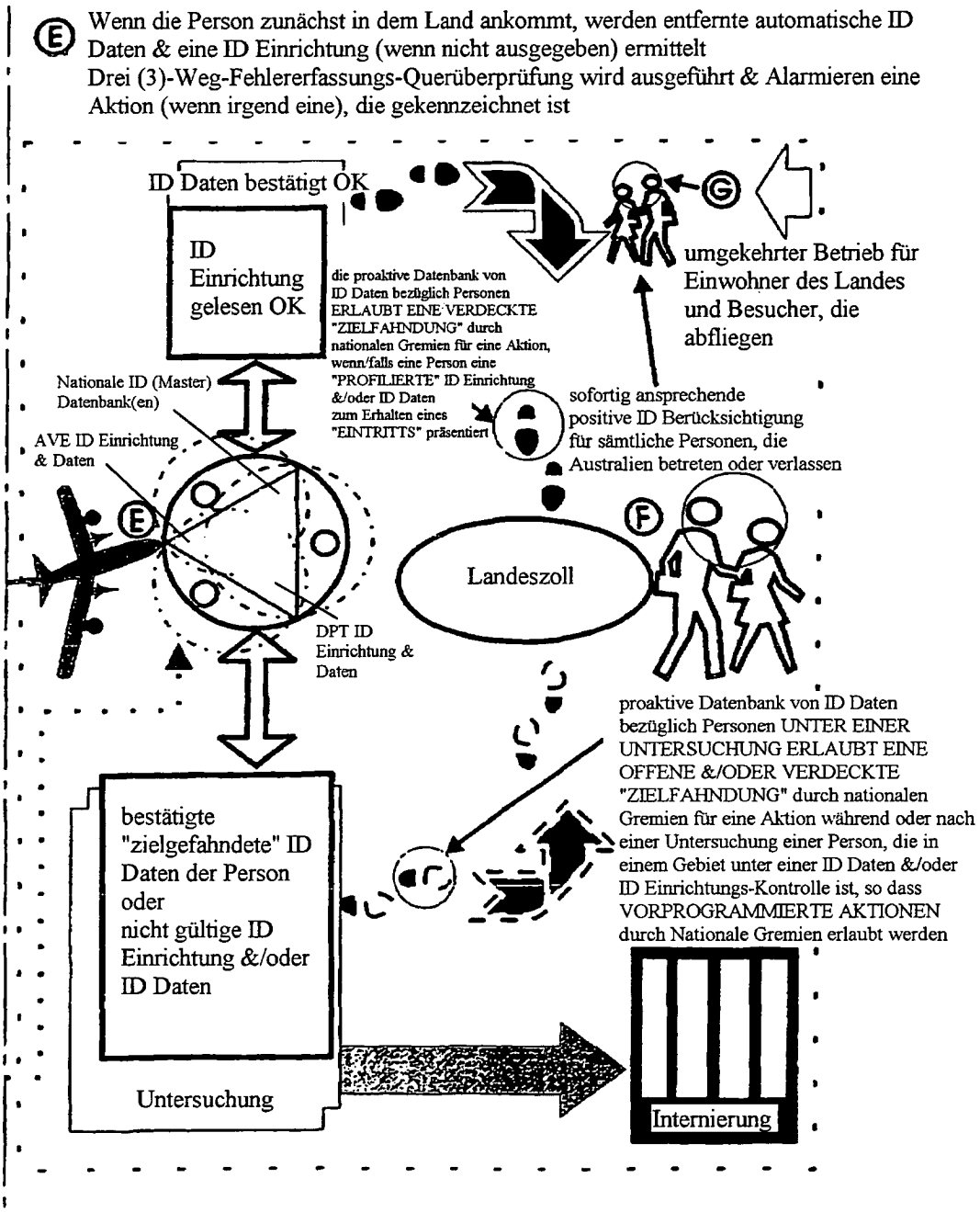

Ⓔ Wenn die Person zunächst in dem Land ankommt, werden entfernte automatische ID Daten & eine ID Einrichtung (wenn nicht ausgegeben) ermittelt
Drei (3)-Weg-Fehlererfassungs-Querüberprüfung wird ausgeführt & Alarmieren eine Aktion (wenn irgend eine), die gekennzeichnet ist
ID Daten bestätigt OK
ID Einrichtung gelesen OK
die proaktive Datenbank von ID Daten bezüglich Personen ERLAUBT EINE VERDECKTE "ZIELFAHNDUNG" durch nationalen Gremien für eine Aktion, wenn/falls eine Person eine "PROFILIERTE" ID Einrichtung &/oder ID Daten zum Erhalten eines "EINTRITTS" präsentiert
umgekehrter Betrieb für Einwohner des Landes und Besucher, die abfliegen
Nationale ID (Master) Datenbank(en)
AVE ID Einrichtung & Daten
sofortig ansprechende positive ID Berücksichtigung für sämtliche Personen, die Australien betreten oder verlassen
Landeszoll
DPT ID Einrichtung & Daten
proaktive Datenbank von ID Daten bezüglich Personen UNTER EINER UNTERSUCHUNG ERLAUBT EINE OFFENE &/ODER VERDECKTE "ZIELFAHNDUNG" durch nationalen Gremien für eine Aktion während oder nach einer Untersuchung einer Person, die in einem Gebiet unter einer ID Daten &/oder ID Einrichtungs-Kontrolle ist, so dass VORPROGRAMMIERTE AKTIONEN durch Nationale Gremien erlaubt werden
bestätigte "zielgefahndete" ID Daten der Person oder nicht gültige ID Einrichtung &/oder ID Daten
Untersuchung
Internierung

Fig.2 (cont.)

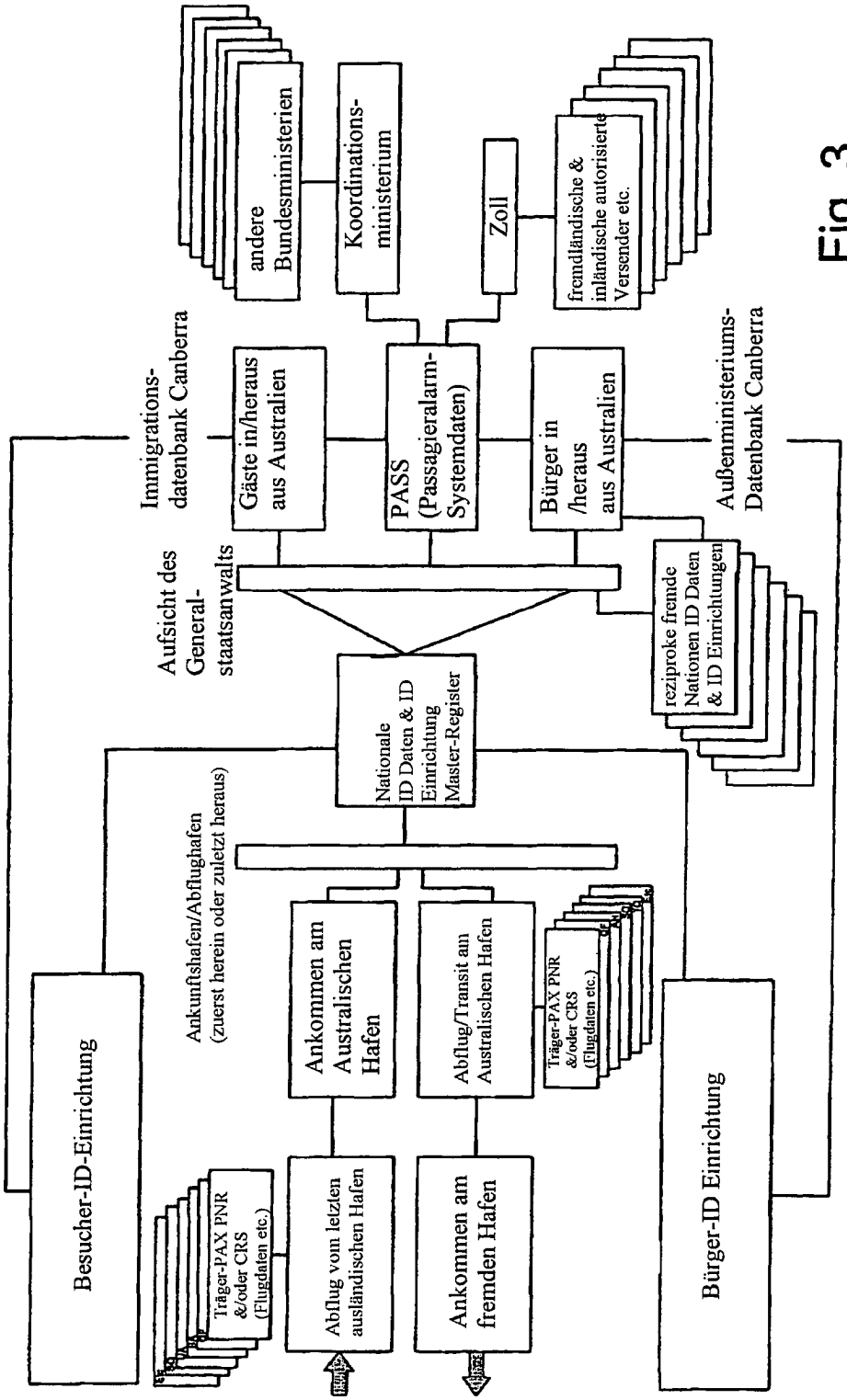

andere Bundesministerien
Koordinations-ministerium
Zoll
fremdländische & inländische autorisierte Versender etc.
Immigrations-datenbank Canberra
Gäste in/heraus aus Australien
PASS (Passagieralarm-Systemdaten)
Bürger in /heraus aus Australien
Außenministeriums-Datenbank Canberra
Aufsicht des General-staatsanwalts
reziproke fremde Nationen ID Daten & ID Einrichtungen
Nationale ID Daten & ID Einrichtung Master-Register
Ankunftshafen/Abflughafen (zuerst herein oder zuletzt heraus)
Besucher-ID-Einrichtung
Ankommen am Australischen Hafen
Abflug/Transit am Australischen Hafen
Träger-PAX PNR &/oder CRS (Flugdaten etc.)
Träger-PAX PNR &/oder CRS (Flugdaten etc.)
Abflug vom letzten ausländischen Hafen
Ankommen am fremden Hafen
Bürger-ID Einrichtung

Fig. 3

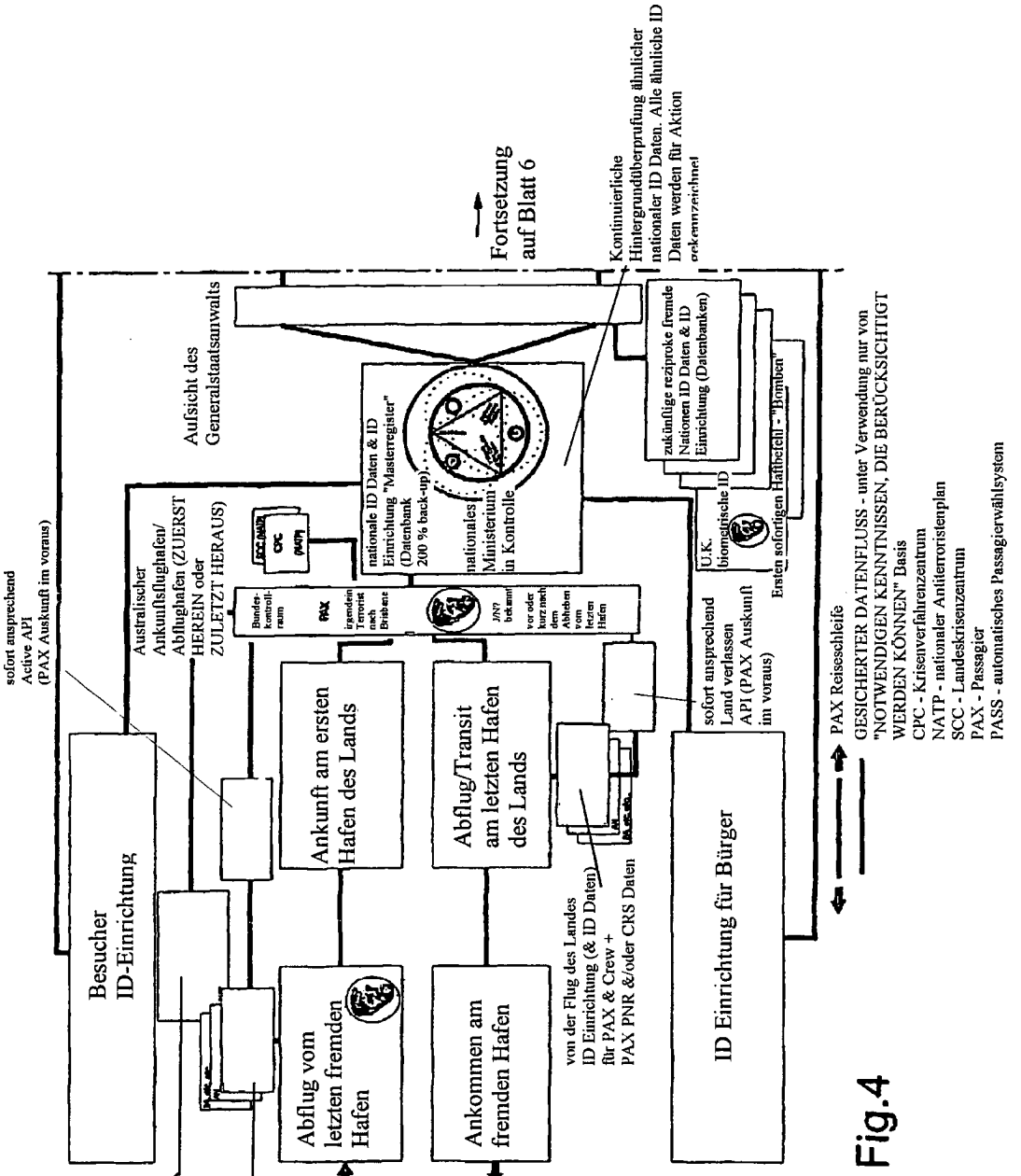

Fortsetzung auf Blatt 6
Kontinuierliche Hintergrundüberprüfung ähnlicher nationaler ID Daten. Alle ähnliche ID Daten werden für Aktion gekennzeichnet
Aufsicht des Generalstaatsanwalts
sofort ansprechend Active API (PAX Auskunft im voraus)
Australischer Ankunftsflughafen/ Abflughafen (ZUERST HEREIN oder ZULETZT HERAUS)
nationale ID Daten & ID Einrichtung "Masterregister" (Datenbank 200 % back-up)
nationales Ministerium in Kontrolle
zukünftige reziproke fremde Nationen ID Daten & ID Einrichtung (Datenbanken)
U.K. biometrische ID
Ersten sofortigen Haftbefehl - "Bomben"
Besucher ID-Einrichtung
Ankunft am ersten Hafen des Lands
Abflug/Transit am letzten Hafen des Lands
Abflug vom letzten fremden Hafen
Ankommen am fremden Hafen
ID Einrichtung für Bürger
sofort ansprechend Land verlassen API (PAX Auskunft im voraus)
von der Flug des Landes ID Einrichtung (& ID Daten) für PAX & Crew + PAX PNR &/oder CKS Daten
Länder ID Datensammlung überprüfung mit Warnliste proaktives abgelehntes Boarding PAX &/oder FRÜHEN WARNUNG [mit geheimen Datenprofil]
zur Austr. Flug Einrichtung (& ID Daten) für PAX & Crew + PAX PNR &/oder CRS Daten
PAX Reiseschleife
GESICHERTER DATENFLUSS - unter Verwendung nur von "NOTWENDIGEN KENNTNISSEN, DIE BERÜCKSICHTIGT WERDEN KÖNNEN" Basis
CPC - Kriseinverfahrenzentrum
NATP - nationaler Antiterroristenplan
SCC - Landeskrisenzentrum
PAX - Passagier
PASS - automatisches Passagierwählsystem

Fig.4

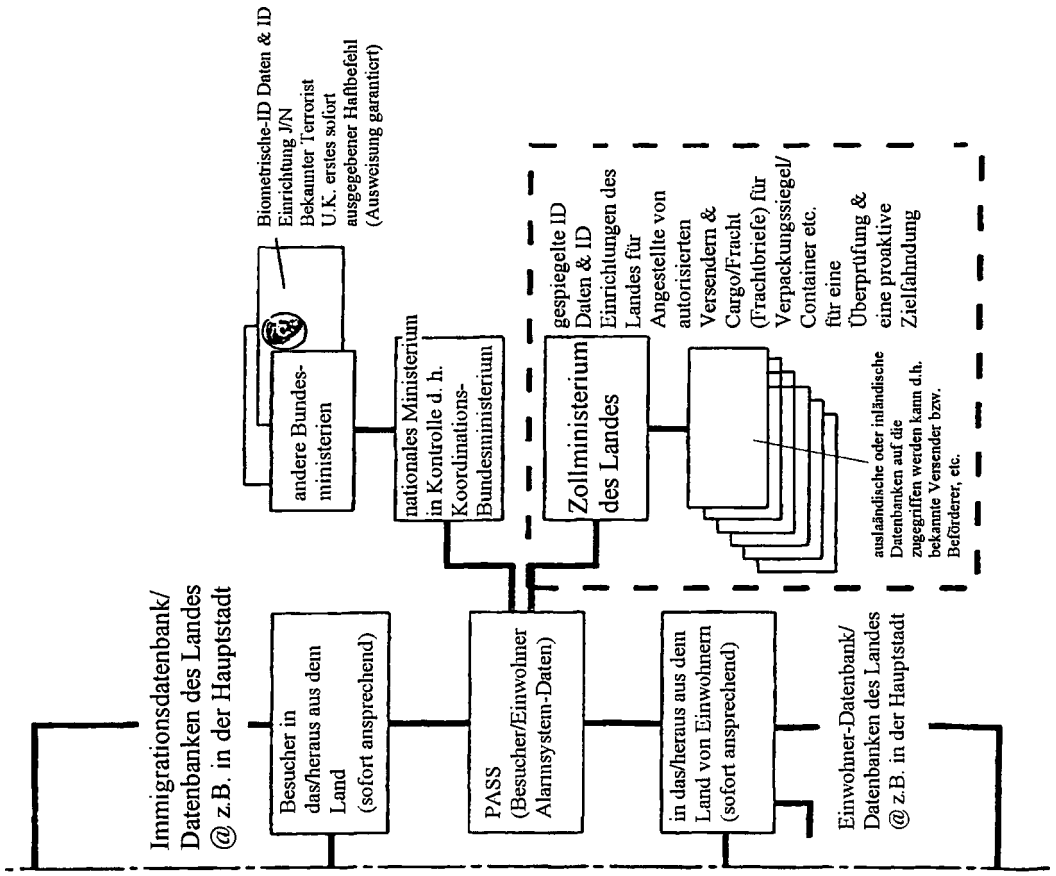


Fig.4 (Fortsetzung)