(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. Februar 2007 (15.02.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/017275 A1

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

(21) Internationales Aktenzeichen: PCT/EP2006/007896

(22) Internationales Anmeldedatum:
9. August 2006 (09.08.2006)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2005 038 092.1 11. August 2005 (11.08.2005) DE

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

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **NESS, Werner** [DE/DE]; Lena-Christ-Strasse 5, 85716 Unterschleissheim (DE).

(74) Anwalt: **DENDORFER, Claus**; Wächtershäuser & Hartz, Weinstrasse 8, 80333 Munich (DE).

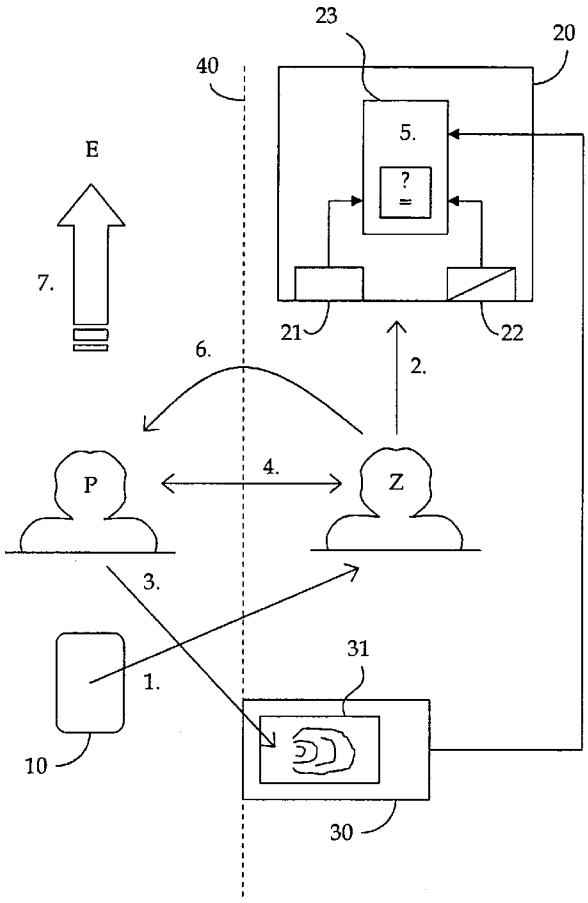
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD AND DEVICE FOR CHECKING AN ELECTRONIC PASSPORT

(54) **Bezeichnung:** VERFAHREN UND EINRICHTUNG ZUR PRÜFUNG EINES ELEKTRONISCHEN PASSES



(57) Abstract: The invention relates to a method for carrying out a machine checking of electronically stored personal data in a passport booklet (10). The data are transmitted in a concealed form to a reading device (20) after the passport (10) is presented to this reading device (20), and the accuracy of the concealment is firstly verified and the concealment is then removed. A positive signal is issued in the event of a successful verification. The restored personal data is subsequently checked for authenticity. The verification and removing of the concealment (109) as well as the checking for authenticity (111) ensue in a time-staggered manner after the passport booklet (10) has been removed from the reading device (20) by a verifying person (Z) in order to conduct further checks.

(57) Zusammenfassung: Vorgeschlagen wird ein Verfahren zur maschinellen Prüfung von in einem Paßbuch (10) elektronisch gespeicherten personenbezogenen Daten. Die Daten werden nach Präsentation des Passes (10) an einem Lesegerät (20) in verschleierter Form an dieses übertragen, wo zunächst die Richtigkeit der Verschleierung geprüft und anschließend die Verschleierung entfernt wird. Bei erfolgreicher Prüfung ergeht ein Gutsignal. Nachfolgend werden die wiederhergestellten personenbezogenen Daten auf Authentizität geprüft. Das Prüfen und Entfernen der Verschleierung (109) sowie die Prüfung auf Authentizität (111) erfolgen dabei erst zeitversetzt, nachdem das Paßbuch (10) zur Durchführung von weiteren Prüfungen durch eine Prüfperson (Z) wieder von dem Lesegerät (20) entfernt und wurde.

WO 2007/017275 A1

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

Erklärung gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii)*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

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

Verfahren und Einrichtung zur Prüfung eines elektronischen Passes

Die Erfindung geht aus von einem elektronischen Paß wie er beispielsweise aus der US 2003/0168514 A1 entnehmbar ist. Der darin beschriebene Paß hat die Gestalt eines Paßbuches, in dessen Deckel eine RFID-Anordnung mit einem Chip zur Aufnahme von Daten sowie einer Antenne als Schnittstelle zur Außenwelt hin eingearbeitet ist. Der beschriebene Paß kann maschinell berührungslos ausgelesen werden.

Aus der JP 05-035935 ist ein Verfahren zur vollautomatischen Durchführung bestimmter Prüfungen mithilfe eines Passes entnehmbar, der über einen nichtflüchtigen Speicher verfügt, welcher elektronisch auslesbar ist. Die Prüfung umfaßt einen Vergleich einer von dem Besitzer des Passes genommenen Bildinformation mit einer aus dem Paß ausgelesenen Bildinformation. Anhand einer aus dem nichtflüchtigen Speicher ausgelesenen Prüfinformation wird ferner die Authentizität des Passes festgestellt. Im Zusammenhang mit der Prüfung können in den Paß auch Prüfinformationen eingeschrieben werden. Vorteil des Verfahrens ist, daß die Anwesenheit einer Prüfperson entfällt. Allerdings bedingen die vorgeschlagenen Schritte einigen Datenverarbeitungsaufwand, der einer schnellen Durchführbarkeit entgegensteht.

EP 1 170 705 A2 offenbart ein besonders für die Abfertigung von Flugpassagieren geeignetes vollautomatisches Einlaßsystem, bei dem Informationen aus einem Paßbuch genutzt werden, um zum einen die Identität des Reisenden festzustellen und zum anderen die Legitimation des Passes zu prüfen. Die Personenidentitätsprüfung erfolgt durch datentechnischen Vergleich eines mittels einer automatischen Kamera von einem Reisenden aufgenommenen Fotos mit einem von dem im Paß befindlichen Bild abgenommenen Foto. Zur Prüfung der Paßlegitimation werden im Paß befindliche maschinenlesbare Daten ausgelesen und mit einer „schwarzen" Liste verglichen.

Das vorgeschlagene System erübrigt die persönliche Präsenz von Prüfpersonen an Einlaßsystem, arbeitet durch die zweimal notwendige Umsetzung von Fotos in Daten aber vergleichsweise langsam oder erfordert eine sehr leistungsstarke und damit teure Datenverarbeitungsanlage. Die vollständige Herausnahme von Prüfpersonen aus dem Kontrollprozeß ist aus Sicherheitsgründen zudem häufig gerade nicht erwünscht; besonders gilt dies für Grenzkontrollen. Für eine Anordnung, die eine Prüfperson einschließt, eignet sich das vorgeschlagene System wegen seiner vergleichsweise langsamen Arbeitsgeschwindigkeit aber nicht.

DE 199 61 403 C2 ist ein Verfahren zur Personenkontrolle durch Prüfung eines elektronischen Berechtigungsausweises in Gestalt einer Smart Card bekannt, der formale und biometrische Personendaten enthält. Eine zu kontrollierende Person wird dabei nacheinander durch zwei Schleusen dirigiert. In der ersten Schleuse erfolgt eine Prüfung der Echtheit der Smart Card und der Personendaten, in der zweiten eine Prüfung der den biometrischen Daten zugrundeliegenden biometrischen Merkmale der Person. Die Prüfung der Personendaten geschieht kryptographisch gesichert unter Verwendung von sogenannten MACs (*Message Authentication Code*). Das Verfahren erlaubt eine beschleunigte automatische Abwicklung von Personenkontrollen.

Gegenwärtig werden die zum Auslesen von personenbezogenen Daten aus elektronischen Pässen auszuführenden Schritte durch Normen festgelegt. Danach ist vorgesehen, daß das Auslesen über eine gesicherte Datenverbindung erfolgt. Die Sicherung wird durch Anwendung der bekannten Technik des „secure messaging" erreicht. Secure messaging beruht auf der Verwendung von sogenannten „session keys", die zu Beginn einer Datenübertragung zwischen den beteiligten Partnern, hier: zwischen einem Paß und einem Lesegerät, ausgehandelt werden. Zur weiteren Sicherung der Datenübertragung durch Diversifizierung ist im Paß und im Lesegerät ferner je-

weils ein Sendefolgezähler SSC (*sense sequence counter*) vorgesehen, der bei jedem Austausch eines Datenpaketes innerhalb einer Datenübertragung erhöht wird. Durch Verschlüsselung mit Hilfe der session keys und des Sendefolgezählers werden Kommandos des Lesegerätes und Antworten des Passes für die Datenübertragung verschleiert.

Für elektronisch auslesbare Pässe ist ferner regelmäßig behördlich vorgegeben, daß die Richtigkeit der Durchführung der Verschleierung der von einem Paß gelieferten Antworten in dem Lesegerät nachgeprüft wird. Die Nachprüfung kann insbesondere mittels des bekannten Konzeptes des MACs (*Message Authentication Code*) erfolgen. Dabei wird von einem Paß über eine verschleierte Antwort jeweils ein MAC gebildet und zusammen mit der Antwort an das Lesegerät übertragen. Das Lesegerät bildet nach Erhalt der Antwort über die erhaltenen verschleierten Daten ebenfalls einen MAC* und vergleicht diesen mit dem in der Antwort des Passes übertragenen MAC.

Aufgrund der üblicherweise bei der Kommunikation eingesetzten Protokolle und der durch die physikalischen Eigenschaften der Schnittstelle bedingten Begrenztheit des Datenaustausches zwischen Lesegerät und Paß erfolgt die Datenübertragung vom Paß zum Lesegerät beim Auslesen regelmäßig in Teilen in mehreren Datenpaketen. Jedes übertragene Datenpaket wird im Lesegerät unmittelbar nach Eingang auf Richtigkeit nachgeprüft, etwa durch MAC-Vergleich Bei erwiesener Richtigkeit wird das nächste Teilpaket von dem Paß angefordert. Tritt ein Fehler auf, wird das Auslesen der Daten aus einem Paß unmittelbar abgebrochen. Das Verfahren ist sicher, bedingt aber entsprechend lange Auslesezeiten.

Aufgabe der Erfindung ist es, ein Verfahren zur Prüfung eines elektronischen Passes anzugeben, das die Einschaltung einer Prüfperson vorsieht und dabei trotzdem hinreichend schnell ausgeführt werden kann.

Diese Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Hauptanspruchs sowie durch ein Prüfsystem mit den Merkmalen des unabhängigen Systemanspruchs.

Das erfindungsgemäße Verfahren hat den Vorteil, daß in einer Paßkontrolle bei noch vertretbarem Zeitaufwand sowohl eine Überprüfung elektronischer Daten wie eine Sichtprüfung durch eine Person erfolgen kann. Erreicht wird dies, indem zu prüfende elektronische Daten aus dem zu kontrollierenden Paß zunächst nur ausgelesen werden, die eigentliche Überprüfung der Richtigkeit und der Authentizität der Daten aber erst nachgelagert erfolgt, während zur gleichen Zeit die Sichtprüfung durch eine Person durchgeführt wird.

Beim Auslesen der elektronischen Daten aus dem Paß erfolgt vorzugsweise nur eine Prüfung der ausgelesenen Daten auf Plausibilität. Die Prüfung kann insbesondere in einer Prüfung auf Einhaltung bestimmter syntaktischer Vorgaben bestehen oder in einer Prüfung auf bestimmte Datenmengen. Ein Ausführungsbeispiel der Erfindung wird nachfolgend unter Bezugnahme auf die Zeichnung näher erläutert.

Es zeigen:

Fig. 1 den Aufbau eines elektronischen Passes,

Fig. 2 eine Prüfanordnung zum Prüfen eine elektronischen Passes, und

Fig. 3 ein Flußdiagramm des Ablaufs der Prüfung eines elektronischen Passes.

Fig. 1 zeigt einen elektronischen Paß in Gestalt eines Paßbuches 10, das aus einem Buchdeckel mit den beiden Buchdeckelhälften 11 und 12 besteht. Zwischen die Buchdeckelhälften 11 und 12 sind eine nach Art einer Kunststoffkarte ausgeführte Seite 13 aus Plastik sowie mehrere Seiten 14 aus Papier eingebunden. In die Deckelseite 11 ist eine Chip-Spulenanordnung 15, 16 eingearbeitet, wobei in dem Chip 15 personenbezogene Daten eines Paßbuchbesitzers P eingespeichert sind und die Spule 16 als Schnittstelle zu einem Lesegerät 20 dient. Die personenbezogenen Daten beinhalten paßbuchtypische Angaben wie insbesondere Name, Wohnort, Geburtsdatum usw. eines Paßbuchbesitzers P. Desweiteren sind in dem Chip 15 als personenbezogene Daten biometrische Merkmale des Paßbuchbesitzers P abgespeichert, etwa ein Fingerabdruck und/oder ein Irisabbild.

Auf der Plastikseite 13 sind ein Foto 17 des Paßbuchbesitzers sowie personenbezogene Daten 18 im Klartext aufgebracht. Desweiteren befindet sich auf der Seite 13 ein Feld 19 mit besonderen maschinenlesbaren Daten, die zur Prüfung der Echtheit des Paßbuches dienen. Das Feld 19 hat typischerweise die Gestalt einer bekannten, sogenannten MRZ (*Machine Readable Zone*).

Der insoweit beschriebene Aufbau des Paßbuches 10 ist an sich bekannt und kann, in ebenfalls bekannter Weise, eine Reihe von Abwandlungen aufweisen. Unter anderem kann die Chip-Spulenanordnung 14, 15 auf einer anderen Seite 12, 13, 14 angebracht sein oder kann anstelle einer Spule 16 eine andere Schnittstelle, etwa eine kontaktbehaftet arbeitende, vorgesehen sein. Weiter können auf der aus Plastik ausgeführten Seite 13 weitere Felder vorgesehen sein, etwa Felder mit der Wiedergabe von biometrischen Merkma-

len, etwa eines Fingerabdrucks oder weitere Felder mit personenbezogenen Angaben. Grundsätzlich muß die Seite 13 zudem nicht aus Plastik sondern kann aus einem beliebigen anderen Material, insbesondere auch Papier bestehen. Die die Chip-Spulenanordnung 14, 15 enthaltende Seite, d.h. je nach Ausführung die Plastikseite 13 , die Deckelseite 11 oder eine andere Seite 12, 15, wird zweckmäßig nach Art einer Chipkarte oder zumindest unter Verwendung der Fertigungsmethoden zur Herstellung von Chipkarte hergestellt.

In einer praktisch bedeutsamen Ausführungsvariante kann das Paßbuch 10 auch auf eine einzelne Seite reduziert sein, die dann vorzugsweise in Gestalt einer Chipkarte ausgeführt ist. Diese Ausführungsvariante kommt insbesondere für Identitätskarten zur Anwendung..

Fig. 2 veranschaulicht eine Prüfanordnung zum Prüfen eines elektronischen Passes und das Zusammenwirken der beteiligten Komponenten. Die Anordnung umfaßt insgesamt ein nachfolgend einfach als Paß bezeichnetes Paßbuch 10, ein Lesegerät 20 sowie eine damit verbundene Vorrichtung 30 zur Abnahme eines biometrischen Merkmales von einer zu kontrollierenden Person, d.h. eines Paßbuchbesitzers P.

Das Lesegerät 20 umfaßt eine Vorrichtung 21 zum Lesen der maschinenlesbaren Daten im Feld 19 eines Passes 10, eine Schnittstelle 22 zur Kommunikation mit der Spule 16 in dem Paß 10 sowie eine zentrale Verarbeitungseinheit 23, welche mit der Vorrichtung 21, der Schnittstelle 22 sowie der Abnahmevorrichtung 30 verbunden ist. Die zentrale Verarbeitungseinheit 23 führt insbesondere Datenverarbeitungen durch, um die Authentizität eines vorgelegten Passes 10 sowie die Legitimation einer Person P zu prüfen. Das Lesegerät 20 ist zweckmäßig für eine Person P, deren Paß 10 zu kontrollieren ist, nicht zugänglich und von dieser durch eine Barriere 40 getrennt. Die

Komponenten 21, 22, 23 des Lesegerätes 20 können räumlich verteilt angeordnet sein. Typischerweise ist zentrale Verarbeitungseinheit 23 räumlich von den Schnittstellen 21, 22 getrennt. Die Schnittstelle 22 dient zweckmäßig ausschließlich zur Datenaufnahme. Die gesamte Prüfung erfolgt in der zentralen Verarbeitungseinheit 23.

Die Abnahmevorrichtung 30 dient zur Abnahme eines biometrischen Merkmals einer zu kontrollierenden Person P und verfügt entsprechend über geeignete Mittel zur Gewinnung eines biometrischen Merkmals. Wie in Fig. 2 angedeutet, kann die Abnahmevorrichtung 30 z.B. einen Fingerabdruckaufnehmer 31 aufweisen; alternativ oder ergänzend kann z.B. eine Fotokamera vorgesehen sein. Die Abnahmevorrichtung 30 steht im Zugriff der zu kontrollierenden Person 1.

Weitere Komponente der Prüfanordnung ist eine anwesende Prüfperson Z, etwa ein Grenzbeamter oder ein Zöllner, die die Identität einer zu kontrollierenden Person P durch eine Sichtprüfung überprüft.

Durch die numerierten Pfeile ist das Zusammenwirken der Komponenten der Prüfanordnung angedeutet. Eine zu kontrollierende Person P bewegt sich dabei in einer Richtung E an der Abnahmevorrichtung 30, der Prüfperson Z sowie dem Lesegerät 20 vorbei, von denen sie dabei durch die Barriere 40 getrennt ist. Wie durch den Pfeil 1 angedeutet übergibt die zu kontrollierende Person beim Passieren der Prüfanordnung zunächst der Prüfperson Z ihren Paß 10, welcher von der Prüfperson Z daraufhin, Pfeil 2, an den Schnittstellen 21 und 22 des Lesegerätes 20 präsentiert wird. In der Zeit. während der Paß 10 an den Schnittstellen 21, 22 ausgelesen wird, präsentiert, Pfeil 3, die zu prüfende Person P ein bestimmtes biometrisches Merkmal, etwa ihren Fingerabdruck, an der Abnahmevorrichtung 30, welche das präsentierte biometrische Merkmal in Referenzdaten umsetzt und diese an das

Lesegerät 20 übermittelt. Sowie die Datenübertragung aus dem Paß 10 an das Lesegerät 20 abgeschlossen ist, entfernt die Prüfperson Z den Paß 10 von dem Lesegerät 20 und führt eine Sichtprüfung der zu kontrollierenden Person P durch. Typischerweise erfolgte diese Sichtprüfung durch Vergleich der Person P mit dem im Paß 10 befindlichen Foto 17.

Während der Sichtprüfung wertet die zentrale Verarbeitungseinrichtung 23 die über die Schnittstellen 21 und 22 aus dem Paß 10 ausgelesenen Daten sowie die von der Abnahmevorrichtung 30 übermittelten Referenzdaten aus. Das Ergebnis teilt das Lesegerät 20 über geeignete Anzeigemittel, etwa ein Display oder farbige Leuchten, der Prüfperson Z mit. Fällt das Ergebnis positiv aus, erzeugt das Lesegerät 20 ein Gutsignal. Die Prüfperson Z gibt daraufhin der zu kontrollierenden Person P den Paß 10 zurück, woraufhin diese die Prüfanordnung in Richtung E verläßt. Ergibt die Auswertung, daß die über die Schnittstellen 21 und 22 aus dem Paß 10 ausgelesenen Daten und die von der Abnahmevorrichtung 30 übermittelten Referenzdaten nicht zueinander passen, erzeugt das Lesegerät 20 eine Fehlermeldung.

Fig. 3 veranschaulicht die im Zuge der Prüfung einer zu kontrollierenden Person P durchzuführenden Schritte in Form eines Flußdiagrammes. Der Kontrollvorgang setzt ein mit dem Erscheinen der zu kontrollierenden Person P an der Prüfanordnung, Schritt 100. Die zu kontrollierende Person P übergibt zunächst ihren Paß 10 an die Prüfperson Z, Schritt 101. Weiter präsentiert die zu kontrollierende Person P ein bestimmtes vorzuweisendes biometrisches Merkmal an der Abnahmevorrichtung 30, Schritt 102, welche daraus Referenzdaten erzeugt und diese an das Lesegerät 20 sendet.

Der übergebene Paß 10 wird von der Prüfperson Z zunächst an der Schnittstelle 21 präsentiert, welche aus dem Feld 19 die maschinenlesbaren Daten ausliest, Schritt 103. Sodann präsentiert die Prüfperson Z den Paß 10 an der

Schnittstelle 22, wo die in dem Chip 14 gespeicherten personenbezogenen Daten ausgelesen werden, Schritt 104.

Das Auslesen der personenbezogenen Daten erfolgt über eine gesicherte Datenverbindung. Die Sicherung wird vorzugsweise, wie eingangs beschrieben, durch „secure messaging" in Verbindung mit der Verwendung von Sendefolgezählern SSC (*sense sequence counter*) erreicht. Durch Verschlüsselung mit Hilfe der session keys und des Sendefolgezählers werden Kommandos des Lesegerätes 20 und Antworten des Passes 10 für die Datenübertragung verschleiert.

Die Richtigkeit der Durchführung der Verschleierung der von einem Paß 10 gelieferten Antworten wird in dem Lesegerät 20 nachgeprüft. Vorzugsweise geschieht die Nachprüfung durch eine MAC (*Message Authentication Code*) - Prüfung. Von dem Paß 10 wird dabei über eine verschleierte Antwort jeweils ein MAC gebildet und mit der Antwort an das Lesegerät 20 übertragen. Das Lesegerät 20 bildet nach Erhalt der Antwort über die erhaltenen verschleierten Daten ebenfalls einen MAC* und vergleicht diesen mit dem in der Antwort des Passes 10 übertragenen MAC.

Die Übertragung der aus dem Paß 10 auszulesenden Daten erfolgt regelmäßig, wie eingangs beschrieben, in mehreren Datenpaketen.

Erfindungsgemäß ist nun vorgesehen, daß das Auslesen der Daten aus dem Paß 10 und die Nachprüfung der Richtigkeit der Verschleierung im Lesegerät 20 nicht mehr datenpaketweise unmittelbar sondern zeitlich getrennt durchgeführt werden, wobei zunächst alle auszulesenden, für eine Prüfung erforderlichen Daten vollständig übertragen werden, bevor die Nachprüfung der Richtigkeit der Verschleierung erfolgt.

Im Schritt 104 erfolgt entsprechend nur das vollständige Auslesen aller Daten aus dem Paß 10. Die Überprüfung der Richtigkeit der Verschleierung und die Wiederherstellung der personenbezogenen Daten erfolgen hingegen unmittelbar noch nicht. Nach Eingang eines Datenpaketes im Lesegerät 20 wird vielmehr unmittelbar das nächste Datenpaket von dem Paß 10 angefordert. Um dennoch eine erste Absicherung zu erzeugen, daß die aus dem Paß 10 ausgelesenen Daten voraussichtlich in richtiger Weise übertragen wurden und der Paß 10 authentisch ist, erfolgt beim Auslesen unmittelbar eine Plausibilitätsprüfung der im Lesegerät 20 eingehenden Daten, Schritt 105. Dabei wird geprüft, ob die Struktur der eingehenden Daten einer bestimmten Syntax entspricht. Desweiteren wird geprüft, ob die Menge der übertragenen Daten einer zu erwartenden Länge entspricht. Weiter kann geprüft werden, ob alle erwarteten Datenobjekte übertragen wurden. Ergibt die Prüfung in Schritt 105, daß die ausgelesenen Daten plausibel sind, wird dies durch das Lesegerät 20 der Prüfperson Z signalisiert.

Diese entfernt daraufhin den Paß 10 von dem Lesegerät 20, Schritt 106, und führt eine Sichtkontrolle der zu kontrollierenden Person P durch. Die Sichtkontrolle besteht vorzugsweise in bekannter Weise in einem Vergleich des in dem Paß befindlichen Fotos 17 mit der Person P. Zusätzlich oder alternativ zu einer Sichtkontrolle können von der Prüfperson weitere Aktivitäten ausgeführt werden. Beispielsweise kann die Richtigkeit eines Visums geprüft werden. Weiter können zu diesem Zeitpunkt Informationen in den Paß 10 eingetragen werden, beispielsweise können in die Seiten 14 Stempel eingebracht werden, Schritt 108.

Parallel zur Durchführung der Schritte 106 und 107 führt die zentrale Verarbeitungseinheit 23 des Lesegerätes 20 die Überprüfung der Richtigkeit und die Entfernung der Verschleierung der aus dem Paß 10 ausgelesenen Daten durch, Schritt 109. Hierzu bildet sie zunächst über die ausgelesenen ver-

schleierten Daten einen MAC* und prüft, ob dieser mit dem in der Antwort des Passes 10 übertragenen MAC übereinstimmt. Ist das der Fall, entfernt sie durch Entschlüsselung die Verschleierung von den ausgelesenen Daten und stellt dadurch die in den ausgelesenen Daten enthaltenen personenbezogenen Daten wieder her. Dem Lesegerät 20 stehen damit die in dem Paß 10 gespeicherten personenbezogene Daten der zu kontrollierenden Person P bereit, die insbesondere biometrisch nachprüfbare Daten wie die Daten eines Fingerabdruckes oder eines Paßbildes umfassen, Schritt 110.

Die biometrisch überprüfbaren Daten prüft die zentrale Verarbeitungseinrichtung 23 sodann auf Authentizität. Hierzu vergleicht sie die biometrisch überprüfbaren Daten mit den Referenzdaten, die ihr in der Zwischenzeit von der Abnahmevorrichtung 30 nach Ausführung des Schrittes 102 zugesandt wurden, Schritt 111. Ergibt der Vergleich in Schritt 111, daß die verglichenen Daten aus den Schritten 110 und 102 übereinstimmen, stellt das Lesgerät 30 Authentizität fest und signalisiert der Prüfperson Z durch ein Gutsignal, daß die zu kontrollierende Person P berechtigt ist.

Waren sowohl die Prüfung in Schritt 107 wie die Prüfung in Schritt 111 erfolgreich, Schritt 112, gibt die Prüfperson Z abschließend der zu kontrollierenden Person P den Paß 10 zurück, Schritt 113.

Ergibt sich bei der Durchführung der Schritte 109 oder 111 eine Nichtübereinstimmung der verglichenen Daten, erzeugt das Lesegerät 20 eine Fehlermeldung.

Unter Beibehaltung des grundlegenden Gedankens, die Kontrolle einer Person anhand von in einem Paßbuch elektronisch gespeicherten personenbezogenen Daten durchzuführen, wobei die personenbezogenen Daten zunächst in einem Lesegerät nur ausgelesen, der Paß anschließend unmittelbar

wieder freigegeben wird und parallel zur Vornahme weiterer Kontrollmaßnahmen die maschinelle Prüfung der Richtigkeit der ausgelesenen personenbezogenen Daten erfolgt, gestattet die vorbeschriebene Erfindung eine Reihe von nicht im Detail beschriebenen Ausgestaltungen. Beispielsweise kann vorgesehen sein, daß die Abnahme des biometrischen Merkmales an der Abnahmevorrichtung 30 schon erfolgt, bevor der Paß 10 zum Auslesen der elektronischen Daten an die Prüfperson Z übergeben wird; diese Variante bietet sich an, wenn sich regelmäßig Schlangen von zu kontrollierenden Personen P bilden. Ebenso kann die Rückgabe des Passes 10 erfolgen, bevor die Prüfung der biometrisch überprüfbaren Daten mit Schritt 111 abgeschlossen ist. Die Prüfanordnung kann ohne weiteres auch weitere Komponenten umfassen, etwa mehrere Abnahmevorrichtungen zur Abnahme unterschiedlicher biometrischer Merkmale oder Auswahlmittel, mittels derer die Prüfperson Z unter verschiedenen angebotenen biometrischen Merkmalen eines auswählt, das dann in der zentralen Verarbeitungseinrichtung 23 geprüft wird. Desweiteren kann anstelle der Technik des secure messagings eine andere Technik zur Verschleierung der Datenübertragung zwischen Paß 10 und Lesegerät 20 eingesetzt werden. Ebenso kann zum Nachweis der richtigen Durchführung der Verschleierung eine andere Technik als die der Verwendung von MACs eingesetzt werden.

Patentansprüche

1. Verfahren zur maschinellen Prüfung von in einem Paßbuch elektronisch gespeicherten personenbezogenen Daten, die nach Präsentation des Paßbuches (10) an einem Lesegerät (30) in verschleierter Form an dieses übertragen werden, wobei die Verschleierung bei Eingang der Daten im Lesegerät auf Richtigkeit geprüft und bei gegebener Richtigkeit wieder entfernt wird, und wobei nachfolgend die wiederhergestellten personenbezogenen Daten auf Authentizität geprüft und bei erfolgreicher Prüfung ein Gutsignal ausgegeben wird, dadurch **gekennzeichnet**, daß das Entfernen der Verschleierung (109) und die Prüfung auf Authentizität (111) erst erfolgen, nachdem alle aus dem Paßbuch (10) auszulesenden personenbezogenen Daten vollständig an das Lesegerät (20) übertragen wurden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Übertragung der auszulesenden personenbezogenen Daten in mehreren Datenpaketen erfolgt.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Entfernen der Verschleierung (109) und die Prüfung auf Authentizität (111) erst erfolgen, nachdem das Paßbuch (10) wieder von dem Lesegerät (20) entfernt wurde.

4. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die an das Lesegerät (20) übertragenen Daten bei Eingang im Lesegerät (20) einer Plausibilitätsprüfung unterzogen werden.

5. Verfahren nach Anspruch 4, dadurch **gekennzeichnet**, daß die Plausibilitätsprüfung durch Prüfung erfolgt, ob die an das Lesegerät (20)

übertragenen Daten eine bestimmte Syntax besitzen.

6. Verfahren nach Anspruch 4, dadurch **gekennzeichnet**, daß die Plausibilitätsprüfung durch Prüfung erfolgt, ob die im Lesegerät (20) eingegangenen Daten einer bestimmten zu erwartenden Menge entsprechen.

7. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Verschleierung der personenbezogenen Daten bei der Übertragung an das Lesegerät (20) durch Anwendung der Technik des Secure Messagings erfolgt.

8. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Prüfung der Verschleierung auf Richtigkeit durch Erzeugung eines MAC* über die übertragenen verschleierten Daten und Vergleich mit einem mit den übertragenen Daten mitübertragenen MAC erfolgt.

9. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Prüfung auf Authentizität durch Vergleich der wiederhergestellten personenbezogenen Daten mit vor Ort aufgenommenen Referenzdaten erfolgt.

10. Verfahren nach Anspruch 9, dadurch **gekennzeichnet**, daß die zur Authentizitätsprüfung herangezogenen personenbezogenen Daten und die Referenzdaten biometrische Daten sind.

11. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die Übertragung der personenbezogenen Daten erst erfolgt, wenn zuvor maschinenlesbare Daten aus dem Paßbuch (10) ausgelesen wurden.

12. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die personenbezogenen Daten in dem Paßbuch (10) in einem Chip (15) gespeichert und über eine mit dem Chip (15) verbundene Spule (16) kontaktlos ausgelesen werden.

13. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß die personenbezogenen Daten in dem Paßbuch (10) in einem Chip (15) gespeichert und über eine mit dem Chip (15) verbundene kontaktbehaftet arbeitende Schnittstelle ausgelesen werden.

14. Prüfeinrichtung mit einer Schnittstelle zum Auslesen von elektronisch gespeicherten personenbezogenen Daten aus einem Paßbuch sowie einer zentralen Verarbeitungseinrichtung zur Prüfung der Richtigkeit und der Authentizität ausgelesener Daten, dadurch **gekennzeichnet**, daß die Verarbeitungseinrichtung (23) die Prüfung der Authentizität (109) der ausgelesenen Daten erst nach Entfernen des Paßbuches (10) von der Schnittstelle (22) durchführt.

15. Prüfeinrichtung nach Anspruch 14, dadurch **gekennzeichnet**, daß die zentrale Verarbeitungseinrichtung (23) übertragene personenbezogene Daten nach Eingang unmittelbar auf Plausibilität prüft.

16. Prüfeinrichtung nach Anspruch 14, dadurch **gekennzeichnet**, daß die Schnittstelle (22) zum Auslesen von Daten aus einem Paßbuch (10) räumlich von der zentralen Datenverarbeitungseinreichtung (23) getrennt angeordnet ist und die Prüfung der ausgelesenen Daten vollständig in der zentralen Datenverarbeitungseinrichtung (23) erfolgt.

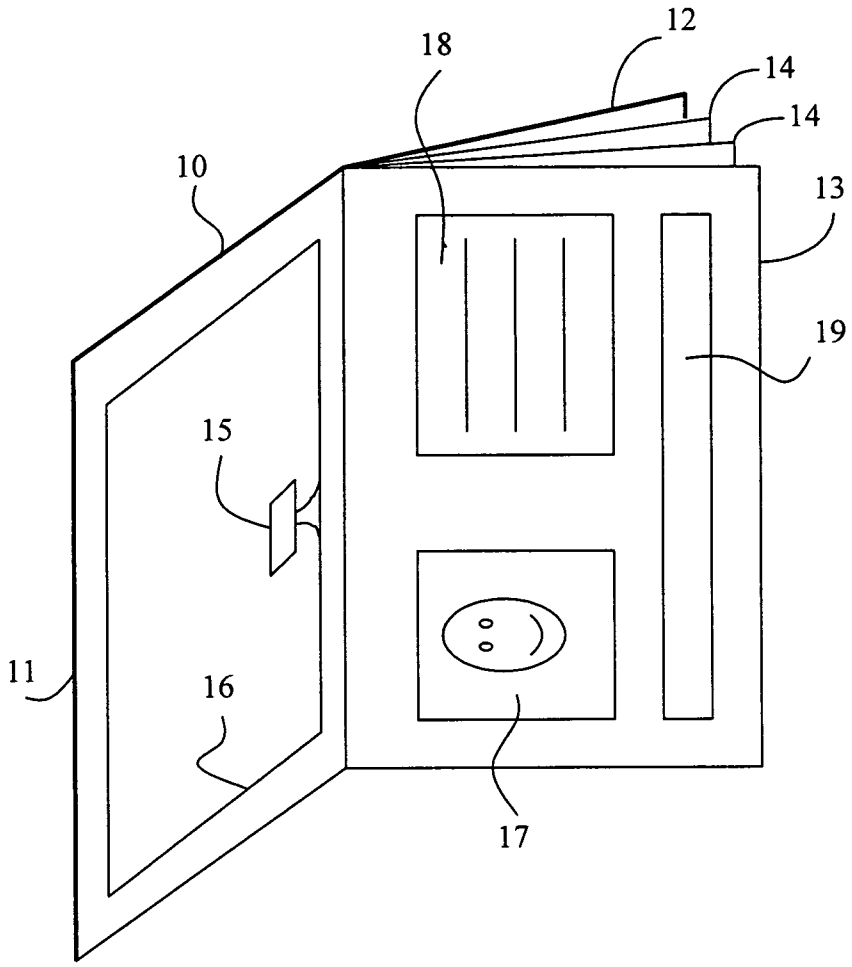


Fig. 1

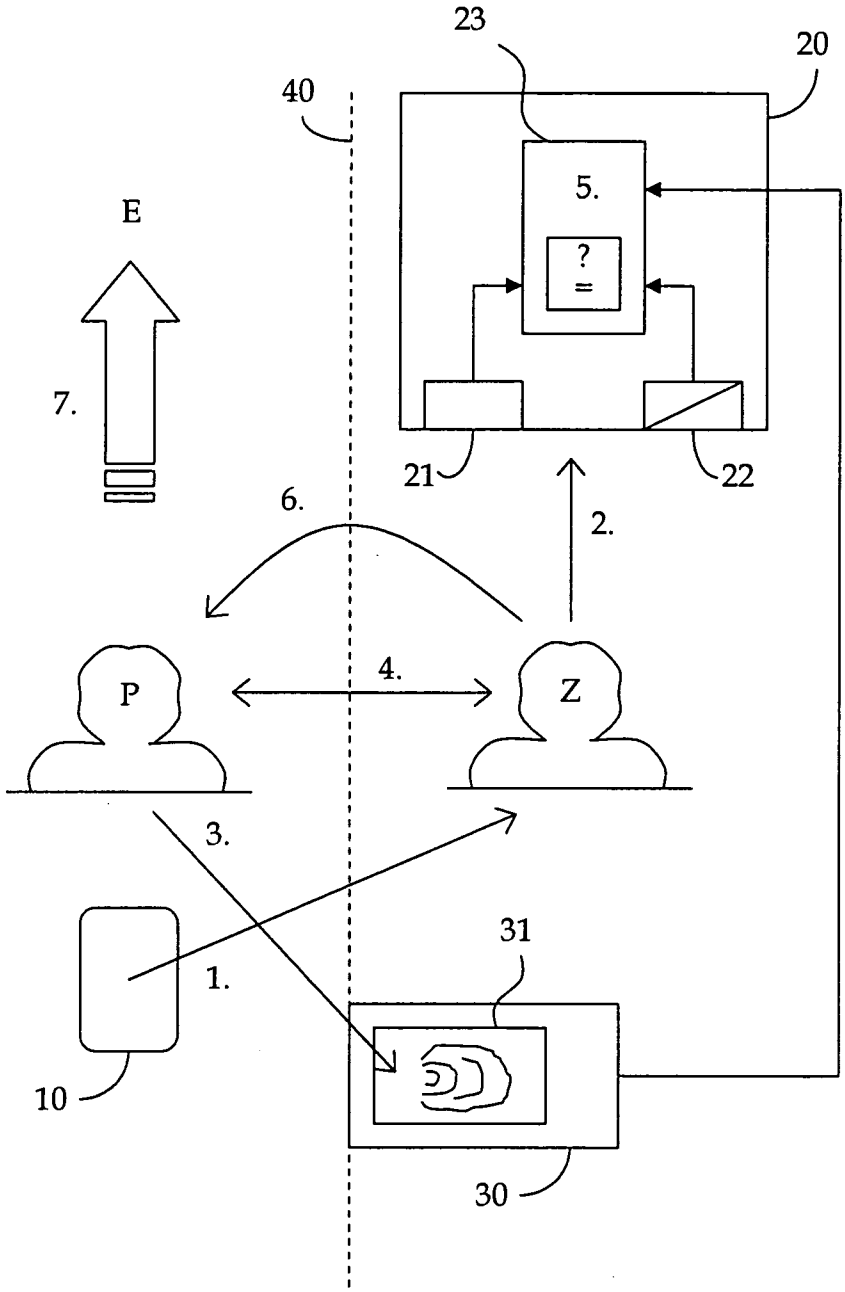


Fig. 2

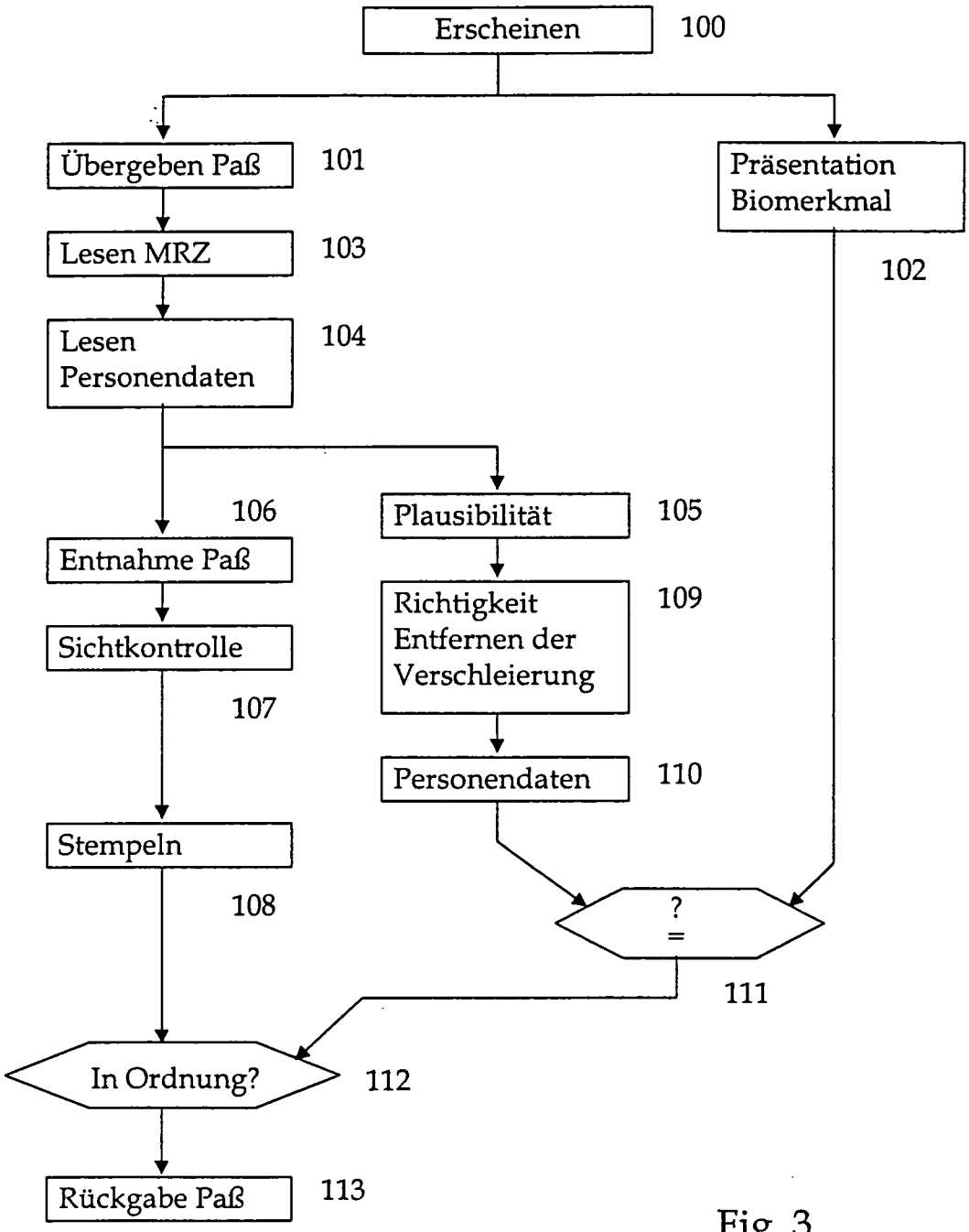

Erscheinen
100
Übergeben Paß
101
Präsentation Biomerkmal
102
Lesen MRZ
103
Lesen Personendaten
104
106
Plausibilität
105
Entnahme Paß
Richtigkeit Entfernen der Verschleierung
109
Sichtkontrolle
107
Personendaten
110
Stempeln
108
?
=
111
In Ordnung?
112
Rückgabe Paß
113

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/007896

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 993 068 A (PIOSENKA GERALD V [US] ET AL) 12 February 1991 (1991-02-12) abstract figure 3b column 7, line 7 - column 8, line 64	1-16
A	WO 2004/017265 A1 (ENSCHEDE SDU B V [NL]; D AGNOLO CARLO ANTONIO GIOVANN [NL]) 26 February 2004 (2004-02-26) the whole document	1-16
A	NL 1 010 443 C2 (ROBERT ARNOUT VAN DER LOOP ING [NL]; ALEXANDER LEONARDUS MARIA DE R [N) 3 May 2000 (2000-05-03) the whole document	1-16

☐ Further documents are listed in the continuation of Box C.

☒ 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
15 November 2006	28/11/2006

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/007896

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4993068 A	12-02-1991	NONE	
WO 2004017265 A1	26-02-2004	AU 2003285786 A1	03-03-2004
		CA 2490208 A1	26-02-2004
		EP 1514244 A1	16-03-2005
		IS 7655 A	19-01-2005
		JP 2005534125 T	10-11-2005
		NL 1020903 C2	22-12-2003
		NZ 537305 A	29-09-2006
		US 2006179481 A1	10-08-2006
NL 1010443 C2	03-05-2000	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2006/007896

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, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 4 993 068 A (PIOSENKA GERALD V [US] ET AL) 12. Februar 1991 (1991-02-12) Zusammenfassung Abbildung 3b Spalte 7, Zeile 7 - Spalte 8, Zeile 64	1-16
A	WO 2004/017265 A1 (ENSCHEDE SDU B V [NL]; D AGNOLO CARLO ANTONIO GIOVANN [NL]) 26. Februar 2004 (2004-02-26) das ganze Dokument	1-16
A	NL 1 010 443 C2 (ROBERT ARNOUT VAN DER LOOP ING [NL]; ALEXANDER LEONARDUS MARIA DE R [N) 3. Mai 2000 (2000-05-03) das ganze Dokument	1-16

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ 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
15. November 2006	28/11/2006

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

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2006/007896

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 4993068 A	12-02-1991	KEINE	
WO 2004017265 A1	26-02-2004	AU 2003285786 A1	03-03-2004
		CA 2490208 A1	26-02-2004
		EP 1514244 A1	16-03-2005
		IS 7655 A	19-01-2005
		JP 2005534125 T	10-11-2005
		NL 1020903 C2	22-12-2003
		NZ 537305 A	29-09-2006
		US 2006179481 A1	10-08-2006
NL 1010443 C2	03-05-2000	KEINE	