

81.928

REPUBLICA DE COLOMBIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIVISION DE NUEVAS CREACIONES

CONTESTACION A REPAROS - OBSERVACIONES
APORTACION DE NUEVA DOCUMENTACION A
UNA SOLICITUD DE PATENTE DE INVENCION O
MODELO DE UTILIDAD O DISEÑO INDUSTRIAL

SUPERINDUSTRIA Y COMERCIO
Radicacion : 00009725 00000001 Folios: 43
Fecha (AMD): 2000-05-16 17:07:47
Trámite : 002 PATENTES D 1 REGISTRO/ 467 SOLICITUD
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Solicitud de Patente
Expediente No. 00 009.725

CONTESTACION: Reparos ☐
Observaciones ☐
Otros ☒
NUEVA DOCUMENTACION APORTADA ☒

☒ PATENTE ☐ MODELO DE UTILIDAD ☐ DISEÑO INDUSTRIAL

TITULO: **PROCEDIMIENTO Y DISPOSITIVO PARA LA PERSONALIZACION Y VERIFICACION DE DOCUMENTOS
DE IDENTIDAD Y SEGURIDAD ASI COMO UN DOCUMENTO DE IDENTIDAD Y SEGURIDAD**

SOLICITANTE: **BUNDESDRUCKEREI GmbH**

INDICE DE DOCUMENTOS QUE SE ACOMPAÑAN

- 1 Solicito PRORROGA DEL TERMINO con el fin de ☐ Patentes de la primera solicitud presentada para la
dar cumplimiento al Auto No.0399 notificado por ☐ misma invención, de la cual REIVINDICAMOS PRIORI-
estado el 30 de Marzo del año 2000, para cuyo ☐ DAD, junto con su correspondiente traducción al
efecto anexamos recibo oficial de caja No.27128 ☐ español.
por este concepto. ☐
2 Copia certificada por la Oficina Alemana de ☐

APODERADO: RAMIRO CASTRO DUQUE Código 340

DOMICILIO: Cra. 7 No. 16-56 Piso 9

TEL: 2-812424

FIRMA:

NUMERO DE HOJAS 43

RADICADO POR: Nombres y Apellidos

Mayo 03, 2000
GCB/nr.



Industria y Comercio

SUPERINTENDENCIA

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 27,128
FECHA : MAYO 3 DE 2000

SUPER INDUSTRIA Y COMERCIO
Radicacion : 88889725 88888831 Folios: 43
Fecha (ACID): 2000-05-16 17:07:47
Tramite : 882 PATENTES D 1 REGISTRO/ 467 SOLICITUD
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	SUCURSAL	CUENTA	Nº. PAGO	Vr. PAGO
BRIGARD & CASTRO LTDA	CONSIGNACION	BANCO POPULAR	BOGOTA	050-00024-9	719806	8,952,000.00

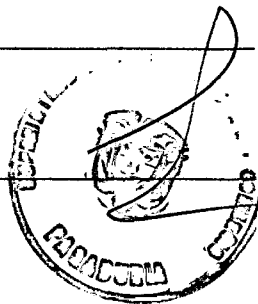
***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-08	PRORROGA DE TERMINOS	31 PRORROGA DE TERMINOS
			50,000.00
		TOTAL :	\$ 50,000.00

SON: CINCUENTA MIL PESOS

RESPONSABLE :

RECIBO DE CAJA APLICADO AL EXPEDIENTE No.



81928
1A
32



Bescheinigung

Die Bundesdruckerei GmbH in Berlin/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Vorrichtung zur Personalisierung und Verifizierung von Identitäts- und Sicherheitsdokumenten sowie ein damit verwendbares Identitäts- und Sicherheitsdokument"

am 16. Februar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 06 K und B 42 D der Internationalen Patentklassifikation erhalten.

München, den 20. März 2000

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Dzierzon

Aktenzeichen: 199 06 388.5

5

10

12502.0-B1517N-54

12. Februar 1999

Anmelder: Bundesdruckerei GmbH
Oranienstrasse 91, 10958 Berlin

15

**Verfahren und Vorrichtung zur Personalisierung und Verifizierung von
Identitäts- und Sicherheitsdokumenten sowie ein damit verwendbares
Identitäts- und Sicherheitsdokument**

20 Gegenstand der Erfindung ist ein Verfahren und eine Vorrichtung zur
Personalisierung und Verifizierung von Identitäts- und Sicherheitsdokumenten
sowie ein damit verwendbares Identitäts- und Sicherheitsdokument.

Hochsichere Identitätsdokumente wie Ausweise, Passports, Lizenzen,
25 Führerscheine, Kfz-Scheine, Mitgliedskarten, Betriebs- und Dienstaussweise,
Kreditkarten und dergleichen bestehen aus einem unpersonalisierten
Dokumentenkörper auf und/oder in welchem die persönlichen Daten des Inhabers
in vom Dokumentenkörper untrennbarer Weise eingebracht werden. Hierzu sind
mehrere Verfahren bekannt, wobei z.B. fotografische Prozesse, Lasergravur,
30 Thermotransfer, Dye-Sublimation, xerografische Laserverfahren, Ink-Jet
Verfahren etc. zu nennen sind.

Die Dokumentenkörper selbst können aus verschiedenen Materialien,
Kombinationen, Konstruktionen von Materialien, Formaten und Zusätzen
35 bestehen. Beispiele für Materialien sind: Identitäts- und Sicherheitspapiere,
Kunststoffe wie Polycarbonat und Polyvinylchlorid. Beispiele für Formate sind:
ID0, ID1 [ICAO und ISO-Normen, z.B. ISO 7816]

5

Besagte Identitätsdokumente werden aus Sicherheitsgründen in einem Unternehmen der Wert- und Sicherheitstechnik zentral hergestellt und personalisiert. Bei der Personalisierung werden die Personaldaten des Inhabers mit Hilfe verschiedener Verfahren in den Dokumentenkörper eingebracht.

10

Grundsätzlich lassen sich zwei Klassen von Personaldaten unterscheiden: alphanumerische und grafische Personaldaten. Alphanumerische Personaldaten bestehen grundsätzlich aus Buchstaben, Ziffern und Sonderzeichen der verschiedenen Zeichensätze (Fonts). Ein Beispiel für den Umfang eines Zeichensatzes des europäischen Sprachraums ist in der ISO 8859 dargestellt. Es bestehen daneben jedoch weitere Zeichensätze für z. B. arabische oder asiatische Schriften. Eine besondere Ausprägung stellen die OCR-Schriftsätze in den ICAO-Zeilen von Identitätsdokumenten dar, da sie maschinenlesbar sind. Damit ist es möglich, mit Hilfe eines Lesegeräts (Scanner) alphanumerische Daten des Identitätsdokuments auszulesen und zu verifizieren.

20

Typische grafische Daten eines Identitätsdokuments sind: Portraits, Unterschriften, Fingerabdrücke, Barcodes, Hoheitszeichen und Logos. Diese Grafikdaten werden mittels moderner fotografischer oder digitaler Druck- und Graviervverfahren in das Identitätsdokument eingebracht. Damit ist gewährleistet, daß die Personaldaten untrennbar mit dem Dokument verbunden sind.

25

Für die alphanumerischen Personaldaten sind automatische Verfahren bekannt, die z. B. auf Flughäfen die ICAO-Zeilen mit Hilfe entsprechender Lesegeräte (Scanner) einlesen und mit den Einträgen in einem elektronischen

30

Personenarchiv (Datenbank) vergleichen können. Dieses Verfahren setzt jedoch die Online-Verbindung zwischen dem Scanner und einer zentralen Datenbank voraus und läßt sich bisher nicht auf grafische Daten anwenden, da diese eine hohe Komplexität und damit ein hohes Datenvolumen aufweisen. Die hohe Komplexität bedingt eine hohe Prozessorleistung der beteiligten

35

Informationsverarbeitungsanlagen zur Übertragung und Verarbeitung des Datenvolumens. Wegen des großen Datenvolumens wird ein hoher Speicherbedarf und eine breitbandige Übertragungsleistung der angeschlossenen

- 5 Kommunikationseinrichtungen benötigt. Selbst unter Ausnutzung modernster Informationsverarbeitungsanlagen würden hier im praktischen Einsatz unvertretbar lange Verarbeitungs- und Antwortzeiten entstehen.

10 Ein weiterer Nachteil des oben geschilderten Verfahrens ist die Notwendigkeit der ständigen Online-Verfügbarkeit der zentralen Personendatenbank. In der Praxis bedeutet dies, daß ständig komplexe, ausfallsichere und teure Informationsverarbeitungsanlagen verfügbar und betriebsbereit sein müssen, und daß beispielsweise einem Polizist in einem Streifenwagen oder in einer örtlichen Wache die genannten notwendigen Prüfmöglichkeiten nicht zur Verfügung
15 stehen.

Kritisch sind in diesem Zusammenhang auch nationale juristische Restriktionen, z. B. des Personendatenschutzes, die die maschinengestützte Identitätsfeststellung von Personen verbieten, da die Gefahr besteht, daß die Daten ausgewertet und daraus Bewegungsprofile erstellt werden können.
20

Aufgabe der Erfindung ist, ein Verfahren und eine Vorrichtung zur Personalisierung und Verifizierung von Sicherheitsdokumenten sowie ein geeignetes Sicherheitsdokument bereitzustellen, welches es erlaubt, die Echtheit insbesondere von grafischen Personaldaten mit verhältnismäßig einfachen Mitteln
25 automatisch verifizieren zu können. In der Praxis bedeutet dies, daß eine Authorisierungsperson wie z. B. ein Polizei- oder Grenzkontrollbeamter feststellen können muß, ob z. B. das Portrait eines vorgelegten Identitätsdokuments zu diesem gehört.

- 30 Diese Aufgabe wird durch die kennzeichnenden Merkmale der unabhängigen Patentansprüche gelöst.

Die erfindungsgemäße Lösung umfasst im wesentlichen folgende Merkmale und Vorteile:

- 35
- die Verifizierung ist mit verhältnismäßig einfachen Mitteln möglich,
 - die Verifizierung findet Offline, d. h. ohne Verbindung zu einer zentralen

5 Datenbank statt,

- die Verifizierung führt zu dem Ergebnis, daß die grafischen Daten des bei der Prüfung vorgelegten Identitätsdokuments echt sind, also zu diesem gehören und
- die Verifizierung verstösst nicht gegen geltende Rechtsbestimmungen.

10

Der visuelle Vergleich zwischen der Präsentation des Gesichts einer Person und der bildlichen Darstellung z. B. als fotografisches Lichtbild oder in gedruckter Form gilt als die klassische Erkennungsmethode schlechthin. Aus diesem Grund wird die Verfahrenslösung im folgenden beispielhaft für das Portrait als

15

Identifikationsmethode beschrieben. Selbstverständlich gelten die Ausführungen in angepaßter Form auch für andere grafische Personaldaten, wie z. B. Fingerabdrücke. In einer weiteren Ausführung sind auch akustische Vergleichsmethoden zur Identitätsfeststellung wie z. B. der menschlichen Stimme anwendbar.

20

Bei der Personalisierung von Identitätsdokumenten werden Portraits zunehmend mit Hilfe von digitalen Druckverfahren in einem zentralen Wert- und Sicherheitsdruckbetrieb hergestellt. Diese Methode bietet den Vorteil, daß die Produktion auf Datenverarbeitungsanlagen durchgeführt wird, bei der das Portrait in einem rechnergestützten Format vorliegt (Pixeldaten) und für eine

25 Weiterverarbeitung effizient genutzt werden kann. Das Volumen eines Portraits für den Einsatz in Identitätsdokumenten beträgt bei einer akzeptable Reproduktionsqualität etwa 70 bis 100 kBytes. Diese Zahlen sind u.a. abhängig von den geometrischen Abmessungen, der Farbe, der Farbtiefe und vom

30 Kompressionsfaktor.

30

Der Lösungsweg geht über die Idee, diese graphischen Daten in der herkömmlichen gedruckten und einer zweiten maschinenlesbaren Form in das Identitätsdokument einzubringen. Damit besteht die Möglichkeit bei einer

35

Identitätsprüfung beide Formen des Portraits miteinander zu vergleichen und bei erfolgreichem Vergleich die Echtheit des Dokuments zu bestätigen.

- 5 In einer bevorzugten Ausführungsform ist vorgesehen, die Portraitdaten, d.h. die Vergleichsdaten in einem elektronischen Speicherchip abzulegen. Dieser Chip ist Bestandteil des Identitätsdokuments. Als Ausführungsform können Chipkarten nach ISO 7816 oder kontaktlose (Transponder)Karten eingesetzt werden. Weitere Möglichkeiten die Grafikdaten in einer zweiten Form abzuspeichern, bieten
- 10 Barcodes, insbesondere 2D-Barcodes wie z. B. der PDF 417 der Fa. Symbol.

Beim Einsatz von Halbleiterspeichern beträgt der beschreibbare Speicherbereich von geeigneten Chipkarten mit Prozessorfunktionalität derzeit typisch 16 kByte für kontaktbehaftete Karten. Die o. g. Datenmenge eines Portraits ist um ein

15 Vielfaches größer als der verfügbare Speicherplatz. Damit ist es zur Zeit nicht möglich, die Pixeldaten eines Portraits in unkomprimierter Form in einer Chipkarte abzulegen. Abgesehen davon würde die Dauer des Auslesens einer derartigen Datenmenge unakzeptabel lange dauern.

Der wesentliche Nachteil einer unkomprimierten Speicherung besteht jedoch

20 darin, daß die reinen Pixeldaten einen einfachen Fälschungsangriff ermöglichen, da ein Angreifer den Chip eines Identitätsdokumentes mit gefälschten Daten überschreiben könnte. Aus diesem Grund muß die Speicherung der Porträttdaten folgende Bedingungen erfüllen:

- die Speichergröße d.h. der Grad der Kompression der Daten muß in einem

25 optimalen Verhältnis von Qualität und Realisierbarkeit stehen und

- die Abspeicherung der grafischen Daten muß in einem unverfälschbaren Format durchgeführt werden.

Um die erste Bedingung zu erfüllen, erfolgt eine entsprechende Aufbereitung der

30 grafischen Daten. Die bei der Produktion des Sicherheitsdokuments vorliegenden Grafikdaten entsprechen einer Pixeldarstellung des Portraits. Mit Hilfe dieses Datenstromes wird die Personalisierungseinrichtung angesteuert, um das Bild auf das Dokument zu drucken. Bei einer automatischen Inspektion muß das Bild von einem Verifizierungsgerät aufgenommen werden. Hierzu lassen sich Scanner

35 oder Kameras mit CCD-Technologie (CCD: Charge Coupled Devices) einsetzen. Das gescannte Bild liefert jedoch stets einen anderen Datenstrom als der zur Personalisierung eingesetzte. Dies liegt u. a. daran, daß die Farbwerte des

- 5 Portraits nie genau rekonstruiert werden können und daß die ursprüngliche Pixelauflösung aufgrund der geometrischen Toleranzen nie genau genug getroffen werden kann.

Aus diesem Grund wird ein Verfahren eingesetzt, welches auf einem biometrischen Verfahren zur Generierung des Datensatzes basiert. Hintergrund
10 ist, daß es bei dem Vergleich zweier Portraits nicht auf die reinen Pixeldaten ankommt, sondern daß bestimmte körperliche Merkmale entscheidend sind. Dies entspricht im übrigen auch der Verfahrensweise, wie ein Polizist das Portrait auf der Karte mit dem Gesicht eines Bürgers vergleicht. Ausgewertet werden Merkmale wie z. B.:

- 15 - Abstandsverhältnisse zwischen Augen, Nase, Ohren, Mund ,
- Größenverhältnisse der Sinnesorgane,
- Ausprägungen der Kopfform und einzelnen Teilen, etc..

Diese biometrischen Merkmale werden aus den Portraitdaten gewonnen und
20 führen zu einem variablen individuellen Datensatz. Je genauer die biometrischen Merkmale ausgewertet werden, desto Umfangreicher wird der Datensatz. Hersteller solcher Systeme geben eine Größe von 1.000 bis 2.000 Byte an, mit der das Portrait einer Person eindeutig charakterisiert werden kann. Damit steht ein Datenformat bzw. eine Datenmenge zur Verfügung, welche optimal den
25 Forderungen zur Speicherung auf einem Kartenchip genügt. Bei der folgenden Ausführung wird dieser Referenzdatensatz, der die charakteristischen Merkmale eines Portraits beschreibt, Bio-Datensatz (Bio-ref) genannt.

Um die zweite, oben genannte Bedingung zu erfüllen ist vorgesehen, ein
30 Verfahren einzusetzen, welches auf der Basis einer asymmetrischen Kryptoverschlüsselung die Unverfälschbarkeit des Bio-Datensatzes garantiert. Asymmetrische Verschlüsselungsverfahren basieren auf einem Schlüsselpaar mit einem privaten und einem öffentlichen Schlüssel. Die Verschlüsselung wird mit dem privaten Schlüssel und die Entschlüsselung mit dem öffentlichen Schlüssel
35 durchgeführt. Der Hersteller der Identitätsdokumente besitzt den zertifizierten privaten Schlüssel des asymmetrischen Kryptoverfahrens wie z. B. RSA. Eine wesentliche Voraussetzung ist, daß dieser private Schlüssel unberechtigten

5 Dritten niemals bekannt wird, da sonst das Gesamtsystem angreifbar wird. Aus diesem Grund darf der private Schlüssel niemals die Kryptobox des Produktionssystems des Sicherheitsbetriebes verlassen. Sogar die Generierung dieses Schlüssels findet innerhalb der Kryptobox statt. Eine Schlüssellänge von 1024 Bit wird derzeit als unangreifbar betrachtet.

10

Der im Produktionssystem aus den Pixeldaten gewonnene Bio-Datensatz wird mit dem privaten Schlüssel des asymmetrischen Kryptoverfahrens verschlüsselt. Im Ergebnis liegt ein verschlüsselter Bio-Datensatz vor, der aufgrund der Verfahrensinhärenz nur durch die Kryptobox des Sicherheitsbetriebes generiert werden kann. Dieser verschlüsselte Bio-Datensatz wird im Speicher des Chips des Identitätsdokumentes abgelegt. Die Entschlüsselung des Datensatzes ist möglich unter Zuhilfenahme des öffentlichen Schlüssels. Dieser darf bekannt sein, da sich die asymmetrische Kryptoverfahren dadurch auszeichnen, daß sich im Gegensatz zu den symmetrischen Verfahren aus der Bekanntheit eines Schlüssels der andere nicht ableiten läßt.

15

20

Die Erfindung beschreibt den Einsatz eines asymmetrischen Kryptoverfahrens wie z. B: RSA zum Ver- und Entschlüsseln des biometrischen Datensatzes. Diese Verfahren sind allgemein bekannt. Eine Standardbeschreibung der Verfahren findet sich in "Applied Cryptography" von Bruce Schneier, ISBN 0-471-11709-9.

25

Gegenstand der Erfindung ist ebenfalls ein Prüfgerät, welches im Feld die Echtheit eines Identitätsdokumentes insbesondere von grafischen Daten feststellt.

30

Aus Effizienzgründen kann bei der Datensatzgenerierung ein Hash-Algorithmus (z.B. RIPEMD160) eingesetzt werden, welcher aus dem vorliegenden bis zu 2 kByte grossen Bio-Datensatz einen z.B. 160 Bit grossen Hashwert bildet. Dies bietet den Vorteil, daß für die Speicherung der Daten auf den Sicherheitsdokument sehr wenig Speicherplatz benötigt wird und das Verfahren des Prüfens des Identitätsdokuments in der Praxis schneller durchgeführt werden kann.

35

5 Nachfolgend wird die Erfindung anhand eines Ausführungsbeispiels unter Bezugnahme auf mehrere Zeichnungsfiguren näher erläutert. Dabei gehen aus den Zeichnungen und der zugehörigen Beschreibung weitere Merkmale und Vorteile der Erfindung hervor.

10 Figur 1 zeigt eine einfache stilistische Darstellung eines Portraits mit einigen eingetragenen biometrischen Merkmalen;

Figur 2 zeigt schematisch den Verfahrensablauf und den Datenfluss bei der Personalisierung und Verifizierung eines Sicherheitsdokuments;

15

Figur 3 zeigt einen möglichen Aufbau eines Verifizierungsgeräts mit eingebrachtem Sicherheitsdokument.

20 In Figur 1 ist ein Portrait dargestellt, in welchem einigen körperliche (biometrische) Merkmale eingetragen sind:

- A: Ohrenabstand
- B: Augenabstand
- C: Mundbreite
- D: Augen-Mund-Abstand
- 25 E: Nase-Augen-Abstand

Natürlich gibt es eine Vielzahl von weiteren Merkmalen, die zur Generierung des Bio-Datensatzes herangezogen werden können, z.B. Form des Kinnbereichs, Form der Nase, Narben, Leberflecke etc.

30

In der Biometrie (Lehre von der Vermessung lebender Merkmale) sind verschiedene Verfahren bekannt, die z. B. Gesichtsmerkmale erkennen, zuordnen und vermessen. Im Ergebnis steht ein charakteristischer Datensatz zur Verfügung. Die Qualität des Datensatzes ist von der Verfahrensart und der Menge der Daten abhängig. Diese biometrischen Verfahren sind Stand der Technik und deren Arbeitsweise soll hier nicht näher erläutert werden.

35

- 5 Ein Portrait in CMYK-Farbdarstellung mit Paßbildgröße und einer digitalen Auflösung von 600 dpi benötigt ca. 3,5 Mio. Bytes in unkomprimierter Darstellung. Gängige Verfahren wie TIFF, JPEG, Wavelet oder Fraktale Kompression ermöglichen die Reduktion der o. g. Datenmenge. Allerdings sind sie auch immer mit Qualitätsverlusten der Ausgangsdaten behaftet, die eine eindeutige
- 10 Erkennbarkeit für ein Verifizierungssystem nicht mehr zulassen.

Die biometrischen Verfahren lösen das Problem, weil sie lediglich die wesentlichen körperlichen Merkmale betrachten. Beispiel: Soll der Augenabstand in einem Wertebereich von 20 mm mit einer Genauigkeit von 0,1 mm bestimmt

15 werden, so läßt sich das Ergebnis in nur einem Byte angeben. Unter Berücksichtigung von z.B. tausend solcher biometrischen Merkmale läßt sich ein Portrait mit einer extrem niedrigen Fehlerwahrscheinlichkeit in nur einem kByte Speicherplatz beschreiben.

- 20 Das biometrische Verfahren wird bei der Erfindung an zwei Stellen eingesetzt. Bei der Personalisierung wird mit dem biometrischen Verfahren der Bio-Datensatz (Bio-ref) erzeugt, der verschlüsselt und im Chip-Speicher des ID-Dokuments abgelegt wird. Im Prüfgerät (Verifikationsgerät) wird mit Hilfe des selben biometrischen Verfahrens aus dem gescannten Portrait ein zweiter Bio-Datensatz
- 25 (Bio-scan) generiert. Ein Vergleich beider Bio-Datensätze ergibt das Verifizierungsergebnis.

Der Datenfluss bei der Personalisierung und bei der Verifizierung des Identitätsdokuments ist in Figur 2 dargestellt.

- 30 Bei der Personalisierung des ID-Dokuments liegt zunächst die Datei 1 mit den Pixelportraitdaten einer Person vor. Diese Daten werden einem geeigneten Biometrischen Verfahren 2 unterzogen, wobei sich ein im Datenumfang stark reduzierter Bio-Datensatz (Bio-ref) ergibt. Dieser Bio-Datensatz wird mit Hilfe
- 35 eines asymmetrischen Verschlüsselungsverfahrens 3 unter Verwendung eines privaten Schlüssels verschlüsselt und in einem auf den ID-Dokument angeordneten Speicherchip 4 gespeichert.

5

Bei der Verifizierung wird das ID-Dokument in ein Prüfgerät eingeführt. Das Prüfgerät verfügt über eine optische Leseeinrichtung mittels welcher das bildliche Portrait auf dem ID-Dokument gescannt wird, so daß sich eine Pixelportraitdatei 5 ergibt, die in einem Speicher des Prüfgeräts abgelegt wird. Diese Pixeldatei wird dem selben biometrischen Verfahren 6 unterzogen, wie es bereits bei der Personalisierung des Dokuments verwendet wurde, wobei sich ein biometrischer Datensatz 7 (Bio-scan) ergibt, der ebenfalls im Speicher des Prüfgerätes abgelegt wird. Das Prüfgerät verfügt über eine kontakthaftete und/oder kontaktlose Auslesevorrichtung, mit welcher die Bio-ref-Daten aus dem Speicherchip des ID-Dokuments ausgelesen, entschlüsselt und im Speicher des Prüfgerätes gespeichert werden können.

Im Prüfgerät liegen nun beide Bio-Datensätze, Bio-ref und Bio-scan, vor, die nun mittels eines Verifizierungsverfahrens 8 von einem im Prüfgerät vorhandenen Mikrocomputers verglichen werden. Dieser Vergleich führt zu einem Ergebnis 9, welches dem Benutzer optisch und/oder akustisch angezeigt wird. Stimmen die beiden Bio-Datensätze in hohem Masse überein, so ist die Echtheit des ID-Dokuments bewiesen. Stimmen sie nicht ausreichend überein, so ist von einem gefälschten Dokument auszugehen.

Figur 3 zeigt einer Ausführungsform des Prüfgeräts 10 mit einem Gehäuse 11 etwa in der Größe einer Videokassette. Das Prüfgerät 10 verfügt an einer schmalen Seite über eine Positionierungseinheit, mit deren Hilfe das Identitätsdokument 13 in eine definierte Lage gebracht werden kann. Dies kann z. B. ein Einschubschlitz 12 oder eine Auflagefläche sein. Die korrekte Positionierung kann automatisch durch eine Sensorik erkannt werden, die den Start der Prüfung einleitet. Der Start kann jedoch auch manuell durch die Betätigung eines Tasters ausgelöst werden. Geometrisch gegenüber der zu prüfenden Grafik (hier: Portrait 15) befindet sich eine Aufnahmeeinheit, z. B. ein Scanner 16 oder eine Kamera. Der Mikrochip 14, auf dem die Bio-Referenzdaten gespeichert sind, wird über eine Kontaktierungseinheit 17 elektrisch angeschlossen. In einer besonderen Ausführungsform erfolgt der Anschluß kontaktlos über ein elektromagnetisches Antennensystem. Das Prüfgerät 10

- 5 verfügt über einen Mikrocomputer 18 an den der Scanner 16 und die Chipkontaktierungseinheit 17 angeschlossen sind. Der Mikrocomputer 18 führt die digitalen Prüffunktionen aus und gibt über eine Anzeigeeinheit (nicht dargestellt) das berechnete Prüfergebnis aus.
- 10 Die Funktionen laufen wie folgt ab. Nach Positionierung des Identitätsdokuments 13 und der Startauslösung wird das Portrait 15 über den Scanner 16 aufgenommen und in digitale Signale umgewandelt. Damit liegt das Portrait 15 als Pixeldatei in ähnlicher Form vor, wie es zur Personalisierung des Identitätsdokuments im Sicherheitsbetrieb eingesetzt wurde. Diese Pixeldatei wird
- 15 im Speicher des Mikrocomputers 18 abgelegt. Der Prozessor generiert nach dem gleichen Algorithmus wie bei der Personalisierung aus dieser Pixeldatei einen zweiten Bio-Datensatz (Bio-scan), der auch im Speicher des Mikrocomputers 18 abgelegt wird.
- 20 In einem weiteren Schritt liest der Prozessor den verschlüsselten Bio-Datensatz (Bio-ref) aus dem Chip 14 des Identitätsdokumentes 13 aus und legt ihn im Speicher des Mikrocomputers 18 des Prüfgeräts 10 ab. In diesem Speicher steht aufgrund der Initialisierung des Mikrocomputers 18 der öffentliche Schlüssel des kryptologischen Systems zur Verfügung. Mit Hilfe dieses Schlüssels wird der erste
- 25 Bio-Datensatz (Bio-ref) aus dem Chip 14 entschlüsselt. Damit liegen beide Bio-Datensätze (Bio-ref und Bio-scan) in vergleichbarer Form im Prüfgerät 10 vor und die Verifikation kann durchgeführt werden.
- Wie bereits beschrieben, können die beiden Bio-Datensätze aufgrund der
- 30 Aufnahmetoleranzen des gescannten Portraits 15 nicht absolut identisch sein. Ähnliche Verfahren der biometrischen Verifikation liefern Ergebnisse mit Abweichungsraten im Subpromille-Bereich. Unter der Berücksichtigung eines Schwellwertes aus diesem Bereich werden diese Abweichungen toleriert. Festzuhalten ist, daß die Abweichungsraten deutlich niedriger liegen als
- 35 beispielsweise bei einem visuellen Vergleich eines Portraits mit einer lebenden Person z. B. durch einen Inspektionsbeamten.

- 5 Das Verifikationsergebnis stellt der Prozessor über eine Ausgabeeinheit an der Oberfläche des Prüfgeräts 10 zur Verfügung. Dies kann im einfachsten Fall eine Rot/Grün-Leuchteinheit sein, aber auch die digitale Darstellung des Verifikationsergebnisses z. B. in Prozentangabe der Übereinstimmung der Daten oder auch ein akustisches „OK“-Signal.
- 10 Durch geeignete Auswahl der mechanischen und elektronischen Komponenten insbesondere des Mikrocomputers 18 läßt sich der Prüfvorgang auf die Dauer von einigen Sekunden einschränken. Der Aufbau des Prüfgeräts 10 ist so ausgelegt, daß es für einen mobilen Einsatz geeignet ist. Aus diesen Gründen verfügt es
- 15 über eine Energieversorgung aus Batterien oder nachladbaren Akkus und/oder über einen Anschluß an einen Netzadapter oder das 12-Volt-Versorgungsnetz eines PKW.

45

5

Zeichnungslegende

- | | | |
|----|----|------------------------------------|
| | 1 | Datei |
| | 2 | Biometrisches Verfahren |
| | 3 | Verschlüsselung |
| 10 | 4 | Speicherchip mit Bio-ref Datensatz |
| | 5 | Pixelportraitdaten |
| | 6 | Biometrisches Verfahren |
| | 7 | Biometrischer Datensatz (Bio-scan) |
| | 8 | Vergleich |
| 15 | 9 | Ergebnis |
| | 10 | Prüfgerät |
| | 11 | Gehäuse |
| | 12 | Einschubschlitz |
| | 13 | ID-Karte |
| 20 | 14 | Mikrochip |
| | 15 | Portrait |
| | 16 | Scanner |
| | 17 | Kontaktiereinheit |
| | 18 | Mikrocomputer |

25

5

Patentansprüche

1. Identitäts- oder Sicherheitsdokument, welches personenbezogene Daten aufweist, die in alphanumerischer und/oder graphischer Form auf dem Dokument aufgebracht und/oder in dieses eingebracht sind,
dadurch gekennzeichnet,
daß die personenbezogenen Daten (15) und/oder mit diesen korrelierte Daten in einer zweiten, maschinenlesbaren Form auf/in dem Dokument vorhanden sind.
2. Identitäts- oder Sicherheitsdokument nach Anspruch 1, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten nach einem biometrischen Verfahren generierte Daten sind.
3. Identitäts- oder Sicherheitsdokument nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten in komprimierter Form vorliegen.
4. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten in verschlüsselter Form vorliegen.
5. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß es ein nichtflüchtiges elektronisches Speichermedium (14) umfasst.
6. Identitäts- und Sicherheitsdokument nach Anspruch 5, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten in dem elektronischen Speichermedium (14) gespeichert sind.

- 5 7. Identitäts- oder Sicherheitsdokument nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß das Speichermedium Anschlusskontakte zum Einlesen und/oder Auslesen der darauf gespeicherten Daten aufweist.
- 10 8. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, daß das Speichermedium Mittel zum drahtlosen Einlesen und/oder Auslesen der darauf gespeicherten Daten aufweist.
- 15 9. Identitäts- oder Sicherheitsdokument nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten im Form eines Barcodes auf/in das Dokument eingebracht sind.
- 20 10. Verfahren zum Personalisieren eines Identitäts- oder Sicherheitsdokuments, bei dem personenbezogene Daten in alphanumerischer und/oder graphischer Form auf dem Dokument aufgebracht und/oder in dieses eingebracht werden, dadurch gekennzeichnet,
daß die personenbezogenen Daten und/oder mit diesen korrelierte Daten in einer zweiten, maschinenlesbarer Form auf das Dokument aufgebracht und/oder in dieses eingebracht werden.
- 25 11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß personenbezogene Daten in digital verarbeitbarer Form verwendet werden.
- 30 12. Verfahren nach einem Anspruch 10 oder 11, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbarer Form vorhandenen Daten mittels eines biometrischen Verfahrens aus den personenbezogene Daten generiert werden.
- 35 13. Verfahren nach einem der Ansprüche 10 bis 12, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbarer Form vorhandenen Daten mittels eines asymmetrischen Verschlüsselungsverfahrens verschlüsselt werden.

- 5 14. Verfahren nach einem der Ansprüche 10 bis 13, dadurch gekennzeichnet, daß
die in der zweiten, maschinenlesbarer Form vorhandenen Daten komprimiert
werden.
- 10 15. Verfahren nach einem der Ansprüche 10 bis 14, dadurch gekennzeichnet, daß
die in der zweiten, maschinenlesbarer Form vorhandenen Daten in einem auf/in
dem Dokument vorhandenen nichtflüchtigen elektronischen Speichermedium
gespeichert werden.
- 15 16. Verfahren nach einem der Ansprüche 10 bis 15, dadurch gekennzeichnet, daß
die in der zweiten, maschinenlesbarer Form vorhandenen Daten als Barcode
in/auf dem Dokument abgelegt werden.
- 20 17. Vorrichtung zum Verifizieren eines Identitäts- oder Sicherheitsdokuments,
gekennzeichnet durch:
ein Positioniermittel (12) zum lagerichtigen Positionieren des Identitäts-
und/oder Sicherheitsdokuments (13);
ein erstes Abtastmittel (16) zum Erfassen von auf dem Identitäts- oder
Sicherheitsdokument an-/aufgebrachten personenbezogenen Daten (15);
ein zweites Abtastmittel (17) zum Erfassen von auf dem Identitäts- oder
25 Sicherheitsdokument vorhandenen Vergleichsdaten;
Mittel (18) zum Speichern, Aufbereiten und Verarbeiten der erfassten Daten
und zur Ausgabe und Anzeige von Ergebnisdaten.
- 30 18. Vorrichtung nach Anspruch 17, dadurch gekennzeichnet, daß Mittel (18) zur
Aufbereitung der personenbezogenen Daten mittels eines biometrischen
Verfahrens vorhanden sind.
- 35 19. Verfahren zum Verifizieren eines Identitäts- oder Sicherheitsdokuments,
welches personenbezogene Daten aufweist, die in alphanumerischer
und/oder graphischer Form auf dem Dokument aufgebracht und/oder in
dieses eingebracht werden,
gekennzeichnet, durch folgende Schritte:

- 5 Abtasten/Auslesen der personenbezogenen Daten und Speichern dieser Daten in digitaler Form;
Auslesen von auf dem Dokument abgelegten Vergleichsdaten;
Vergleichen der personenbezogenen Daten mit den Vergleichsdaten;
Ausgeben des Ergebnisses des Vergleichs.
- 10 20. Verfahren nach Anspruch 19, dadurch gekennzeichnet, daß die personenbezogenen Daten mittels eines biometrischen Verfahrens aufbereitet und die daraus resultierenden biometrischen Daten abgespeichert werden.
- 15 21. Verfahren nach Anspruch 19 oder 20, dadurch gekennzeichnet, daß die biometrischen Daten mit auf/in dem Dokument vorhandenen biometrischen Vergleichsdaten verglichen werden.
- 20 22. Verfahren nach einem der Ansprüche 19 bis 21, dadurch gekennzeichnet, daß die personenbezogenen Daten mittels eines optischen Bildaufnehmers vom Dokument ausgelesen werden.
- 25 23. Verfahren nach einem der Ansprüche 19 bis 22, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten aus einem auf dem Dokument vorhandenen elektronischen Speichermedium ausgelesen werden.
- 30 24. Verfahren nach einem der Ansprüche 19 bis 23, dadurch gekennzeichnet, daß die in der zweiten, maschinenlesbaren Form vorhandenen Daten als Barcode auf dem Dokument vorliegen und mittels eines optischen Bildaufnehmers ausgelesen werden.

50

5

Zusammenfassung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Personalisierung und Verifizierung von Identitäts- und Sicherheitsdokumenten sowie ein damit verwendbares Sicherheitsdokument. Das Identitäts- oder Sicherheitsdokument weist personenbezogene Daten auf, die in alphanumerischer und/oder graphischer Form auf dem Dokument aufgebracht und/oder in dieses eingebracht sind. Erfindungsgemäss sind die personenbezogenen Daten und/oder mit diesen korrelierte Daten in einer zweiten, maschinenlesbarer Form auf/in dem Dokument vorhanden und können zusammen mit den personenbezogenen Daten mittels eines entsprechenden Prüfgerätes vom Dokument ausgelesen und auf Übereinstimmung überprüft werden.

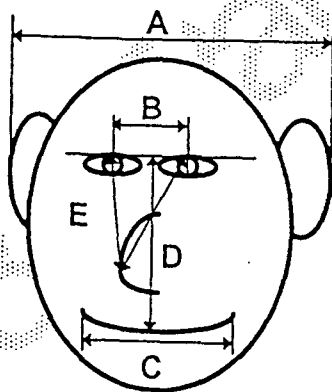


Fig. 1

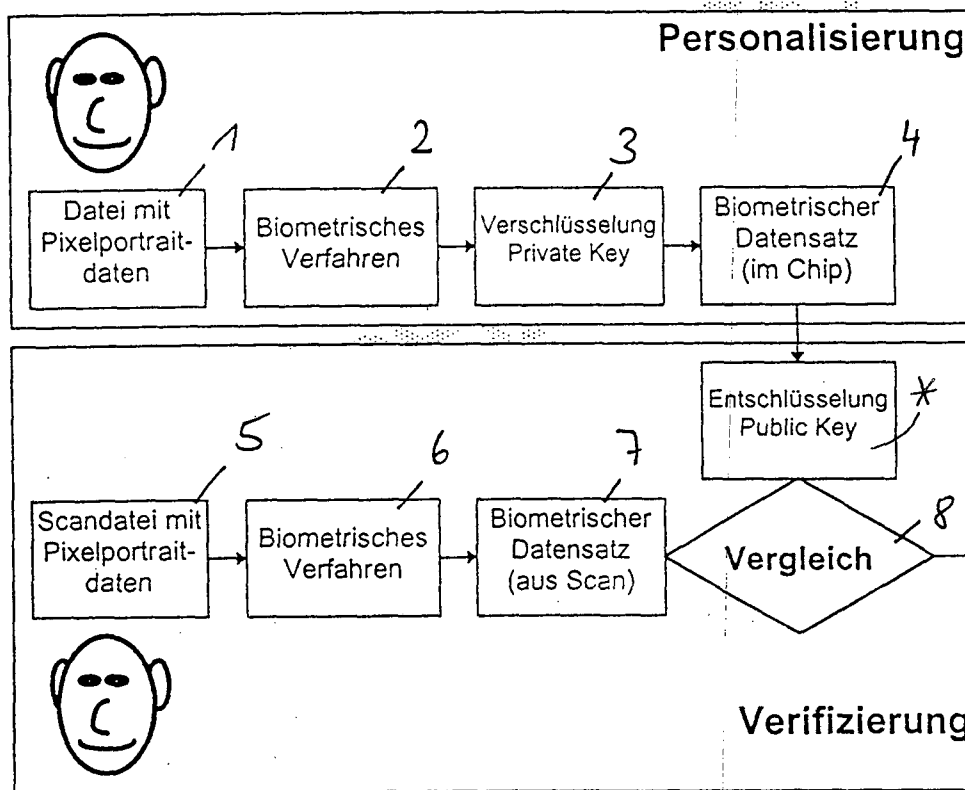


Fig. 2

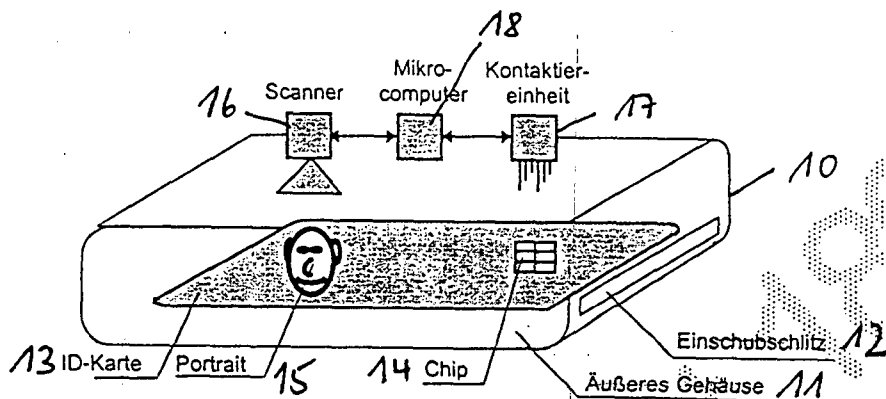


Fig. 3

52

REPUBLICA FEDERAL DE ALEMANIA

Certificación

La compañía Bundesdruckerei GmbH domiciliada en Berlín, República Federal de Alemania, presentó el día 16 de Febrero de 1999 ante la Oficina Alemana de Patentes y Marcas una solicitud de patente bajo el título

"Procedimiento y dispositivo para la personalización y verificación de documentos de identidad y de seguridad, así como también un documento de identidad y de seguridad utilizable con dicho procedimiento y dicho dispositivo".

Los documentos adjuntos son una copia fiel y exacta de los documentos originales de esta solicitud de patente.

La solicitud recibió provisionalmente en la Oficina Alemana de Patentes y Marcas los símbolos G 06 K y B 42 D de la clasificación internacional de patentes.

Munich, 20 de Marzo del 2000

El Presidente de la Oficina Alemana de Patentes y Marcas

Por encargo: Dzierzon

(Firma y Sello Oficial)

Número de referencia: 199 06 388.5

S3

Procedimiento y dispositivo para la personalización y verificación de documentos de identidad y de seguridad, así como también un documento de identidad y de seguridad utilizable con dicho procedimiento y dicho dispositivo

El Objeto de la invención es un procedimiento y un dispositivo para la personalización y verificación de documentos de identidad y de seguridad, así como también un documento de identidad y de seguridad utilizable con dicho dispositivo y dicho documento.

Los documentos de alta seguridad, tales como cédulas de ciudadanía, pasaportes, licencias, pases de conducción, tarjetas de membrecía, documentos de identidad de empresas, tarjetas de crédito y similares, consisten en un cuerpo del documento sobre/en el cual se incorporan de forma inseparable los datos personales del titular del documento. Para ello se conocen varios procedimientos, por ejemplo procesos fotográficos, grabado láser, termotransferencia, sublimación de tintes, procedimientos xerográficos láser, procedimientos de inyección de tinta, etc.

El cuerpo mismo del documento puede consistir en diferentes materiales, combinaciones de materiales, construcciones de materiales, formatos y aditivos. Entre los ejemplos de materiales están: papeles de identidad y de seguridad, plásticos tales como policarbonato y polivinilcloruro. Entre los ejemplos de formato están: ID0, ID1 [normas ICAO e ISO, por ejemplo ISO 7816].

Por razones de seguridad, los documentos mencionados se elaboran y se personalizan centralmente en una compañía de técnica de valores y seguridad. Para la personalización, los datos personales del titular se incorporan al cuerpo de documento con la ayuda de distintos procedimientos.

Básicamente se distinguen dos clases de datos personales: los datos personales alfanuméricos y los datos personales gráficos. Los datos personales alfanuméricos consisten básicamente en letras, cifras y signos especiales del conjunto de signos (fuentes). La norma alemana ISO 8859 es un ejemplo de un conjunto de signos para el área lingüística europea. Pero existen además otros conjuntos de signos, por ejemplo para las escrituras árabes o asiáticas. Los conjuntos de escrituras OCR en los renglones ICAO de documentos de identidad constituyen una acuñación especial ya que son legibles automáticamente. Con ellos es posible leer y verificar los datos alfanuméricos del documento de identidad con la ayuda de un aparato lector (scanner). Datos gráficos típicos de un documento de identidad son: retratos, firmas, huellas dactilares, códigos de barras, insignias y logotipos. Dichos datos gráficos se incorporan al documento de identidad mediante modernos procedimientos de impresión y grabado fotográficos o digitales. Se garantiza así que los datos personales estén unidos inseparablemente al documento.

Para los datos personales alfanuméricos se conocen procedimientos automáticos que, por ejemplo en los aeropuertos, pueden leer los renglones ICAO con la ayuda de los apropiados aparatos lectores (scanners) y compararlos con los registros existentes en un archivo electrónico de datos personales (banco de datos). Pero este procedimiento requiere la conexión en línea entre el scanner y un banco central de datos y hasta el presente no se puede usar con datos gráficos ya que éstos presentan una alta complejidad y por ende un elevado volumen de datos. Para la transmisión y el procesamiento del volumen de datos, esa alta complejidad hace necesaria una alta capacidad procesadora de los dispositivos procesadores de información participantes. Debido al gran volumen de datos se requiere que los dispositivos de comunicación conectados tengan una elevada

capacidad de memoria y una amplia capacidad de transmisión. En la práctica se requerirían tiempos de procesamiento y de respuesta demasiado largos incluso si se utilizaran los más modernos dispositivos procesadores de información.

Otra desventaja del procedimiento descrito arriba es que el banco central de datos personales tiene que estar permanentemente disponible en línea. En la práctica esto significa que permanentemente tienen que estar disponibles dispositivos procesadores de información complejos, a prueba de apagones y muy costosos, y también significa que las posibilidades de verificación no son accesibles por ejemplo para un policía que se encuentra en una patrulla o en una estación de policía local. En este contexto también tienen importancia crítica las restricciones jurídicas nacionales, por ejemplo leyes de protección de datos personales que prohíben verificar por medios automáticos la identidad de personas ya que existe el peligro de que los datos sean analizados y a partir de ellos se puedan elaborar perfiles de movimiento.

La tarea de la invención es poner a disposición un procedimiento y un dispositivo para la personalización y la verificación de documentos de seguridad, así como también poner a disposición un apropiado documento de seguridad que permita verificar automáticamente por medios relativamente sencillos la autenticidad en especial de datos personales gráficos. En la práctica esto significa que una persona autorizada, por ejemplo un policía o un funcionario de control fronterizo, debe poder verificar por ejemplo si el retrato colocado en un documento de identidad efectivamente pertenece a este documento.

Esta tarea se soluciona mediante las características específicas de las reivindicaciones de patente independientes.

La solución inventiva comprende esencialmente las siguientes características y ventajas:

- la verificación es posible por medios relativamente sencillos,
- la verificación se efectúa off-line, es decir sin comunicación con un banco central de datos,
- la verificación conduce al resultado de que los datos gráficos del documento de identidad sometido a prueba son auténticos, es decir pertenecen a dicho documento, y
- la verificación no infringe las disposiciones legales vigentes.

El método clásico de identificación es la comparación visual entre la cara de una persona y su representación gráfica como retrato fotográfico o en forma impresa. Por esta razón la solución procedimental descrita a continuación utiliza el retrato fotográfico como método de identificación. Obviamente las explicaciones son válidas también en forma adaptada para otros datos personales gráficos como por ejemplo huellas dactilares. En otra forma de realización se pueden emplear también métodos de comparación acústica para verificar la identidad, por ejemplo la voz humana.

Para la personalización de documentos de identidad, los retratos se elaboran cada vez más mediante procedimientos de impresión digitales. Este método ofrece la ventaja de que la producción se lleva a cabo en computadores, en los que el retrato se presenta en un formato apoyado por computador (datos en pixels) y puede ser empleado eficientemente para un procesamiento ulterior. Para su utilización en documentos de identidad el volumen de un retrato con una calidad de reproducción aceptable tiene aproximadamente de 70 hasta 100 kbytes. Estas cifras dependen entre otras cosas de las dimensiones geométricas, de los colores, de la intensidad de los colores y del factor de compresión.

La solución abarca la idea de incorporar al documento de identidad estos datos gráficos en la forma impresa tradicional y también en una segunda forma legible por medios automáticos. Existe así la posibilidad de que para una verificación de identidad se pueden comparar entre sí ambas formas del retrato y, si dicha comparación resulta exitosa, confirmar la autenticidad del documento.

En una forma preferida de realización se ha previsto depositar los datos del retrato, es decir los datos de comparación, en un chip electrónico de memoria. Este chip es elemento constitutivo del documento de identidad. Como forma de realización se pueden utilizar tarjetas chip según la norma alemana ISO 7816 o tarjetas (transpondedoras) sin-contacto. Otra posibilidad para memorizar los datos gráficos en una segunda forma son los códigos de barras, en especial los códigos de barras 2D, por ejemplo el símbolo de compañía PDF 417.

Si se usan memorias semi-conductoras, en la actualidad el área de memoria de tarjetas chip apropiadas con funcionalidad procesadora es típicamente de 16 kbytes para tarjetas con-contacto. La cantidad de datos de un retrato -ya mencionada anteriormente- es varias veces mayor que el área de memoria disponible. Por tanto actualmente no es posible depositar en forma no-comprimida en una tarjeta chip los datos en pixels de un retrato. Aparte de ello, la lectura de tal cantidad de datos tendría una duración inaceptablemente larga.

Pero el inconveniente fundamental de una memorización no-comprimida consiste en que los puros datos en pixels permiten una falsificación sencilla puesto que el falsificador podría sobre-escribir con datos falsos el chip de un documento de identidad. Por tal razón la memorización de los datos del retrato debe llenar los siguientes requisitos:

- el tamaño de la memoria, es decir el grado de compresión de

los datos, tiene que estar en una relación óptima de calidad y realizabilidad, y

- la memorización de los datos gráficos tiene que efectuarse en un formato infalsificable.

Para llenar el primer requisito los datos gráficos son preparados adecuadamente. Los datos gráficos disponibles para la producción del documento de seguridad corresponden a una representación del retrato en pixels. El dispositivo de personalización se dirige con esta corriente de datos para imprimir el retrato sobre el documento. Para una inspección automática el retrato tiene que ser registrado por el aparato verificador. Para ello se pueden emplear cámaras con tecnología CCD (CCD = Dispositivos Acoplados de Carga). Pero el retrato escaneado proporciona siempre una corriente de datos diferente a la utilizada para la personalización. Esto se debe entre otras cosas al hecho de que los valores de color del retrato no pueden ser reconstruidos exactamente y de que, debido a las tolerancias geométricas, la resolución de pixels no se puede hallar o reproducir con suficiente exactitud.

Por este motivo se utiliza un procedimiento que se basa en un procedimiento biométrico para generar el conjunto de datos. La razón es que para la comparación de dos retratos lo importante no son los puros datos de pixels, sino el hecho de que lo decisivo son determinadas características corporales. Esto por lo demás corresponde a la manera en que p. ej. un policía compara el retrato del documento con la cara de quien presenta dicho documento. Se analizan características como p. ej.:

- proporciones de distancia entre ojos, nariz, oídos, boca,
- proporciones de tamaño de los órganos de los sentidos,
- forma de la cabeza y de cada una de las partes, etc.

Estas características biométricas se obtienen a partir de los datos del retrato y dan como resultado un conjunto de datos

individuales variable. Entre más exactamente se analicen las características biométricas, más grande será el conjunto de datos. Los fabricantes de tales sistemas indican que el retrato de una persona se puede caracterizar de manera unequivoca con un tamaño de 1.000 a 2.000 bytes. De este modo está disponible un formato de datos o una cantidad de datos que satisfaga óptimamente los requisitos para la memorización en una tarjeta chip. En la siguiente explicación el conjunto de datos biométricos de referencia que describe los rasgos característicos de un retrato se denominan conjunto de bio-datos (bio-ref).

Para llenar el segundo requisito arriba mencionado se ha previsto utilizar un procedimiento que sobre la base de un cifrado o encriptado asimétrico garantiza la infalsificabilidad del conjunto de bio-datos. Los procedimientos de cifrado asimétrico se basan en una pareja de claves con una clave privada y una clave pública. El cifrado se efectúa con la clave privada y el desciframiento se hace con la clave pública. El fabricante de los documentos de identidad posee la clave privada certificada del procedimiento de cifrado asimétrico, por ejemplo el procedimiento RSA. Un requisito fundamental es que dicha clave privada no sea conocida nunca por terceros no autorizados, ya que de lo contrario todo el sistema sería vulnerable a una falsificación. Por esta razón no se puede permitir que la clave privada salga de la oficina de cifrado del sistema de producción de la compañía de seguridad que elabora los documentos de identidad. Incluso la generación de esta clave tiene lugar dentro de la oficina de cifrado. Actualmente se considera que una clave con una longitud de 1024 es inexpugnable.

El conjunto de bio-datos obtenido en el sistema de producción a partir de los datos de pixels se encifra o encripta con la clave privada del sistema de cifrado asimétrico. El resultado

es un conjunto de bio-datos cifrado que por el procedimiento mismo no puede ser generado sino por la oficina de cifrado de la compañía de seguridad. Este conjunto de bio-datos cifrado se deposita en la memoria del chip del documento de identidad. El desciframiento del conjunto de datos es posible con la ayuda de la clave pública. La clave publica puede ser conocida puesto que los procedimientos de cifrado asimétrico se caracterizan porque, al contrario de los sistemas simétricos, el hecho de conocer una de las claves no permite deducir la otra.

La invención describe el empleo de un procedimiento de cifrado asimétrico, como por ejemplo el procedimiento RSA, para cifrar y descifrar el conjunto de datos biométricos. Estos procedimientos son conocidos en general. Una descripción estandarizada de dichos procedimientos se encuentra en "Applied Cryptography" de Bruce Schneier, ISBN 0-471-11709-9.

Objeto de la invención es también un aparato verificador, el cual determina in situ la autenticidad de un documento de identidad y en especial la autenticidad de los datos gráficos.

Por razones de eficiencia se puede emplear un algoritmo parcializado (por ejemplo RIPEMD160), que a partir del presente conjunto de bio-datos de tamaño de hasta 2 kbyte conforma por ejemplo un valor parcializado de un tamaño de 160 bits. Este ofrece la ventaja de que se necesita muy poco espacio de memoria para el almacenamiento de los datos en el documento de seguridad, y de que en la práctica el examen del documento de identidad puede efectuarse más rápidamente.

A continuación se describe más en detalle la invención con la ayuda de un ejemplo de realización y haciendo referencia a varias Figuras ilustrativas. De las Figuras y de su correspondiente descripción se derivan otras características y ventajas de la invención.

La Figura 1 muestra una representación estilística sencilla de un retrato con algunas características biométricas registradas.

La Figura 2 muestra esquemáticamente el curso del procedimiento y el flujo de datos en la personalización y verificación de la autenticidad de un documento de seguridad.

La Figura 3 muestra una posible estructura de un aparato verificador con documento de identidad posicionado.

En la Figura 1 se representa un retrato en el cual están registradas algunas características corporales (biométricas):

- A: Distancias entre los oídos
- B: Distancia entre los ojos
- C: Anchura de la boca
- D: Distancia entre ojos y boca
- E: Distancia entre nariz y ojos

Obviamente hay una multiplicidad de otras características que pueden ser utilizadas para la generación del conjunto de biodatos, por ejemplo forma de la zona de la quijada, forma de la nariz, cicatrices, manchas hepáticas, etc.

En biometría (la ciencia de la medición de las características vivientes) se conocen distintos procedimientos por ejemplo para identificar las características de la cara, para clasificarlas y para medirlas. El resultado es un conjunto de datos característico. La calidad del conjunto de datos depende del tipo de procedimiento y de la cantidad de datos. Dichos datos biométricos forman parte del estado de la técnica y aquí no se explicará en detalle su forma de trabajo.

Un retrato tamaño pasaporte y con representación de color CMYK y resolución de 600 dpi necesita aproximadamente 3,5 millones de bytes en representación no-comprimida. Procedimientos usuales, tales como TIFF, JPEG, Wavelet o Compresión Fractal, permiten la reducción de la cantidad de datos arriba mencionada.

Aunque dichos procedimientos van asociados siempre con pérdidas de calidad de los datos de partida, pérdidas las cuales ya no permiten una identificabilidad inequívoca para un sistema de verificación.

Los procedimientos biométricos resuelven el problema pues toman en consideración solamente las características corporales esenciales. Ejemplo: Si la distancia que hay entre los ojos se ha de determinar en un ámbito de valor de 20 mm con una precisión de 0,1 mm entonces el resultado se puede indicar en solamente un byte. Si por ejemplo se toman en consideración mil de tales características biométricas, entonces un retrato se puede describir con una probabilidad de error sumamente baja en tan sólo un kbyte de espacio de memoria.

El procedimiento biométrico se emplea en la presente invención en dos lugares. En la personalización el conjunto de bio-datos (bio-ref) se produce con el procedimiento biométrico, se cifra y se deposita en el chip de memoria del documento de identidad. Con la ayuda del mismo procedimiento biométrico y a partir del retrato escaneado se genera en el aparato verificador un segundo conjunto de bio-datos (bio-scan). Una comparación de estos dos conjuntos de bio-datos produce el resultado de la verificación.

En la Figura 2 se ilustra el flujo de datos en la personalización y en la verificación del documento de identidad.

Para la personalización del documento de identidad se encuentran en primer lugar el archivo 1 con los datos de pixels del retrato de una persona. Estos datos se someten a un adecuado procedimiento biométrico 2, resultando un conjunto de bio-datos (bio-ref) intensamente reducido en su volumen. Este conjunto de bio-datos se cifra con la ayuda de un procedimiento de cifrado asimétrico 3 y empleando una clave privada y se de-

posita en el chip de memoria 4 dispuesto en el documento de identidad.

Para la verificación, el documento de identidad se introduce en el aparato verificador. El aparato verificador cuenta con un dispositivo lector óptico, mediante el cual se escanea el retrato colocado en el documento de identidad, de tal manera que se produce un archivo del retrato en pixels 5 que es depositado en una memoria del aparato verificador. Este archivo en pixels se somete al mismo procedimiento biométrico 6 empleado ya en la personalización del documento, se produce así un conjunto de datos biométricos (7) (bio-scan) que también es depositado en la memoria del aparato verificador. El dispositivo verificador tiene un dispositivo lector con-contacto y/o sin-contacto, con el cual el conjunto de datos biométricos de referencia (bio-ref) del chip de memoria del documento de identidad se puede leer, descifrar y almacenar en la memoria del aparato verificador.

Ambos conjuntos de bio-datos (bio-ref y bio-scan) están ahora en el aparato verificador y un microcomputador dispuesto en el aparato verificador los puede comparar mediante un procedimiento de verificación 8. Esta comparación produce el resultado 9, que se le indica óptica y/o acústicamente al usuario. Si los dos conjuntos de bio-datos concuerdan en alto grado entonces queda probada la autenticidad del documento de identidad. Pero si los dos conjuntos de datos no concuerdan suficientemente entonces se puede suponer que el documento de identidad es falso.

La Figura 3 muestra una forma de realización del aparato verificador 10 con una armadura que tiene más o menos el mismo tamaño que un videocassette. El aparato verificador 10 tiene en un lado angosto una unidad de posicionamiento, con cuya ayuda se puede colocar el documento de identidad 13 en una posición

definida. Dicha unidad de posicionamiento puede ser por ejemplo una ranura de introducción 12 o una superficie de colocación. El posicionamiento correcto puede ser reconocido automáticamente mediante un sensor que entonces pone en marcha la verificación. La puesta en marcha también puede ser iniciada manualmente oprimiendo un botón. Geométricamente en frente del retrato 15 se encuentra una unidad registradora, por ejemplo un scanner 16 o una cámara. El microchip 14, en el que se encuentran almacenados los datos biométricos de referencia, se conecta eléctricamente mediante la unidad de contacto 17. En una forma especial de realización la conexión tiene lugar sin contacto a través de un sistema de antena electromagnético. El aparato verificador 10 dispone de un microcomputador 18, al cual están conectados el scanner 16 y la unidad de contacto del chip 17. El microcomputador 18 ejecuta las funciones digitales de verificación y presenta a través de una unidad indicadora (no representada) el resultado del procesamiento verificador.

Las funciones se desarrollan del siguiente modo. Luego del posicionamiento del documento de identidad 13 y de la puesta en marcha del proceso de verificación, el retrato 15 es registrado por el scanner 16 y transformado en señales digitales. De esta manera el retrato 15 está ahora como archivo en pixels, es decir en forma similar a la empleada en la personalización del documento. Este archivo en pixels se deposita en la memoria del microcomputador 18. De acuerdo con el mismo algoritmo que en la personalización del documento, a partir de este archivo en pixels el procesador genera un segundo conjunto de bio-datos (bio-scan), el cual también es depositado en la memoria del microcomputador 18.

En un paso ulterior el procesador lee el conjunto cifrado de bio-datos (bio-ref) en el chip 14 del documento de identidad 13 y lo deposita en la memoria del microcomputador 18 del apa-

65

rato verificador 10. En esta memoria, debido a la inicialización del microcomputador 18, está a disposición la clave pública del sistema criptológico. Con la ayuda de esta clave se descifra el primer conjunto de bio-datos (bio-ref) del chip 14. De esta manera ambos conjuntos de bio-datos (bio-ref y bio-scan) están ahora en forma comparable en el aparato verificador 10 y se puede efectuar la verificación.

Tal como ya describió, ambos conjuntos de bio-datos no pueden ser absolutamente idénticos debido a las tolerancias de registro del retrato 15 escaneado. Procedimientos similares de verificación biométrica proporcionan resultados con tasas de desviación en un ámbito inferior a las milésimas. Tales desviaciones se toleran tomando en consideración un valor umbral de dicho ámbito. Hay que señalar que las tasas de desviación son claramente inferiores respecto por ejemplo a la comparación visual que un funcionario inspector hace entre un retrato y una persona viviente.

El procesador pone a disposición el resultado de la verificación mediante una unidad de salida colocada en la superficie del aparato verificador 10. En el caso más sencillo dicha unidad de salida puede ser una unidad luminosa rojo/verde, pero también puede ser una representación digital del resultado de la verificación por ejemplo en porcentaje de la concordancia de los datos, o también una señal acústica de "OK".

La elección adecuada de los componentes mecánicos y electrónicos, en especial del microcomputador 18, permite limitar el proceso de verificación a unos cuantos segundos. La estructura del aparato verificador está concebida de tal manera que éste puede ser utilizado moviblemente. Por esta razón él posee una alimentación de energía por baterías o por acumulador recargable y/o mediante conexión a un adaptador de red o a la red alimentadora de 12 voltios de un automóvil.

Lista de Referencia

- 1 Archivo
- 2 Procedimiento biométrico
- 3 Enciframiento
- 4 Chip de memoria con conjunto de datos biométricos de referencia (bio-ref)
- 5 Datos del retrato en pixels
- 6 Procedimiento biométrico
- 7 Conjunto de datos biométricos (bio-scan)
- 8 Comparación
- 9 Resultado
- 10 Aparato verificador
- 11 Armadura
- 12 Ranura de entrada
- 13 Documento de identidad
- 14 Microchip
- 15 Retrato
- 16 Scanner
- 17 Unidad de contacto
- 18 Microcomputador

Reivindicaciones de Patente

1. Documento de identidad o de seguridad que presenta datos personales los cuales están incorporados en forma alfanumérica y/o gráfica sobre/en el documento, caracterizado porque los datos personales (15) y/o datos correlacionados con éstos se encuentran disponibles en el documento en una segunda forma legible por medios automáticos.
2. Documento de identidad o de seguridad de acuerdo con la reivindicación 1, caracterizado porque los datos disponibles en la segunda forma legible por medios automáticos son generados de acuerdo con un procedimiento biométrico.
3. Documento de identidad o de seguridad de acuerdo con la reivindicación 1 o 2, caracterizado porque los datos disponibles en la segunda forma legible por medios automáticos se encuentran en forma comprimida.
4. Documento de identidad o de seguridad de acuerdo con una de las reivindicaciones 1 hasta 3, caracterizado porque los datos disponibles en la segunda forma legible por medios automáticos se encuentran en forma cifrada.
5. Documento de identidad o de seguridad de acuerdo con una de las reivindicaciones 1 hasta 4, caracterizado porque comprende un medio de memoria electrónico no-volátil.
6. Documento de identidad y de seguridad de acuerdo con la reivindicación 5, caracterizado porque los datos disponibles en la segunda forma legible por medios electrónicos están almacenados en el medio electrónico de memoria (14).
7. Documento de identidad o de seguridad de acuerdo con la reivindicación 5 o 6, caracterizado porque el medio de memoria presenta contactos de conexión para la lectura de los datos allí almacenados.

8. Documento de identidad o de seguridad de acuerdo con una de las reivindicaciones 5 hasta 7, caracterizado porque el medio de memoria presenta medios para la lectura inalámbrica de los datos allí almacenados.

9. Documento de identidad o de seguridad de acuerdo con una de las reivindicaciones 1 hasta 8, caracterizado porque los datos disponibles en la segunda forma legible por medios automáticos se han incorporado al documento en forma de un código de barras.

10. Procedimiento para la personalización de un documento de identidad o de seguridad en el que los datos personales se han incorporado al documento en forma alfanumérica y/o gráfica, caracterizado porque los datos personales y/o datos correlacionados con éstos se han incorporado al documento en una segunda forma legible por medios automáticos.

11. Procedimiento de acuerdo con la reivindicación 10, caracterizado porque los datos personales se utilizan en una forma procesable digitalmente.

12. Procedimiento de acuerdo con la reivindicación 10 u 11, caracterizado porque los datos disponibles en una segunda forma legible por medios automáticos se generan a través de un procedimiento biométrico a partir de los datos personales.

13. Procedimiento de acuerdo con una de las reivindicaciones 10 hasta 12, caracterizado porque los datos disponibles en una segunda forma legible por medios automáticos se encifran mediante un procedimiento de cifrado asimétrico.

14. Procedimiento de acuerdo con una de las reivindicaciones 10 hasta 13, caracterizado porque se comprimen los datos disponibles en la segunda forma legible por medios automáticos.

15. Procedimiento de acuerdo con una de las reivindicaciones 10 hasta 14, caracterizado porque los datos disponibles en la

segunda forma legible por medios automáticos están almacenados en medios de memoria electrónicos no-volátiles dispuestos en el documento.

16. Procedimiento de acuerdo con una de las reivindicaciones 10 hasta 15, caracterizado porque los datos disponibles en una segunda forma legible por medios automáticos se depositan en el documento como código de barras.

17. Dispositivo para la verificación de un documento de identidad o de seguridad, caracterizado por:

un medio de posicionamiento (12) para el posicionamiento correcto del documento de identidad y/o de seguridad (13);

un primer medio detector (16) para registrar los datos personales (15) incorporados al documento de identidad o de seguridad;

un segundo medio detector (17) para registrar los datos de comparación disponibles en el documento de identidad o de seguridad;

medios (18) para almacenar, preparar y procesar los datos registrados y para emitir y mostrar los datos del resultado.

18. Dispositivo de acuerdo con la reivindicación 17, caracterizado porque están disponibles medios (18) para la preparación de datos personales mediante un procedimiento biométrico.

19. Procedimiento para la verificación de un documento de identidad o de seguridad que presenta datos personales incorporados al documento en forma alfanumérica y/o gráfica, caracterizado por los siguientes pasos:

detección/lectura de los datos personales y almacenamiento de estos datos en forma digital;

lectura de los datos de comparación depositados en el documento;

comparación de los datos personales con los datos de comparación;

emisión de los resultados de la comparación.

20. Procedimiento de acuerdo con la reivindicación 19, caracterizado porque los datos personales se preparan mediante un procedimiento biométrico y los datos biométricos de allí resultantes se almacenan.

21. Procedimiento de acuerdo con la reivindicación 19 o 20, caracterizado porque los datos biométricos se comparan con datos de comparación biométricos disponibles en el documento.

22. Procedimiento de acuerdo con una de las reivindicaciones 19 hasta 20, caracterizado porque los datos personales se leen del documento mediante un registrador gráfico óptico.

23. Procedimiento de acuerdo con una de las reivindicaciones 19 hasta 22, caracterizado porque los datos disponibles en una segunda forma legible por medios automáticos se leen de un medio de memoria electrónico disponible en el documento.

24. Procedimiento de acuerdo con una de las reivindicaciones 19 hasta 23, caracterizado porque los datos disponibles en una segunda forma legible por medios automáticos están en forma de código de barras en el documento y son leídos mediante un registrador gráfico óptico.

Resumen

La invención se refiere a un procedimiento y a un dispositivo para la personalización y verificación de documentos de identidad y de seguridad, así como también a un documento de seguridad utilizable con dicho procedimiento y dicho dispositivo. El documento de identidad o de seguridad presenta datos personales incorporados al documento en forma alfanumérica y/o gráfica. De acuerdo con la invención, en el documento están dispuestos en una segunda forma legible por medios automáticos datos personales y/o datos correlacionados con éstos y, mediante un aparato verificador apropiado, pueden ser leídos del documento junto con los datos personales incorporados al documento en forma alfanumérica y/o gráfica y ser examinados respecto a su concordancia.

72

Leyenda de las Figuras

Figura 2:

Personalización

- 1 Archivo con datos del retrato en pixels
- 2 Procedimiento biométrico
- 3 Enciframiento - Clave privada
- 4 Conjunto de datos biométricos (en el chip)

Verificación

- * Desciframiento - Clave pública
- 5 Archivo de escaneo con datos del retrato en pixels
- 6 Procedimiento biométrico
- 7 Conjunto de datos biométricos (del escaneo)
- 8 Comparación
- 9 Resultado

Figura 3:

- 10 Aparato verificador
- 11 Armadura externa
- 12 Ranura de introducción
- 13 Documento de identidad
- 14 Chip
- 15 Retrato
- 16 Scanner
- 17 Unidad de contacto
- 18 Microcomputador