(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 102 216 B1

(12) **EUROPÄISCHE PATENTSCHRIFT**

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
16.08.2006 Patentblatt 2006/33

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Anmeldenummer: **99125349.3**

(22) Anmeldetag: **21.12.1999**

(54) **System und Verfahren zur automatisierten Kontrolle des Passierens einer Grenze**

System and method for automatically checking the passage of a frontier

Système et procédé de contrôle automatique du passage d'une frontière

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priorität: **19.11.1999 DE 19957283**

(43) Veröffentlichungstag der Anmeldung:
23.05.2001 Patentblatt 2001/21

(73) Patentinhaber: **Accenture GmbH**
61476 Kronberg (DE)

(72) Erfinder: **Hellenthal,Markus**
56154 Boppard (DE)

(74) Vertreter: **Rocke, Carsten et al**
Müller-Boré & Partner
Grafinger Strasse 2
81671 München (DE)

(56) Entgegenhaltungen:
EP-A- 0 599 291
EP-A- 0 762 340
WO-A-99/16024
US-A- 4 586 441
US-A- 4 847 485
US-A- 4 993 068
US-A- 5 095 196

EP 1 102 216 B1

Printed by Jouve, 75001 PARIS (FR)

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein System und ein Verfahren zur automatisierten Kontrolle des Passierens einer Grenze.

[0002] Grenzkontrollen z. B. an Flughäfen, aber auch im Bereich der Land- und Fährverkehre sind für den grenzüberschreitenden Personenverkehr zeitkritisch. Gleichzeitig ist der Aufwand der Kontrollbehörden - unter anderem wegen des Schengener Abkommens in den vergangenen Jahren überproportional zur Anzahl der Reisenden gestiegen. Die seit Jahren steigende Mobilität der Menschen und wachsende Passagierzahlen im internationalen Flugverkehr führen zu neuen Anforderungen im Personenbeförderungswesen. Andererseits sind die personellen und finanziellen Ressourcen der staatlichen Kontrollbehörden, der Luftverkehrsunternehmen und der Flughafenbetreiber sowie die räumlichen Gegebenheiten auf vielen internationalen Verkehrsflughäfen zunehmend begrenzt.

[0003] Durchgengsschleuse sind von US-A-458 64 41 bekannt.

[0004] Der Erfindung liegt somit die Aufgabe zugrunde, die Geschwindigkeit des Passagierverkehrs zu erhöhen.

[0005] Erfindungsgemäß wird diese Aufgabe gelöst durch ein System zur automatisierten Kontrolle des Passierens einer Grenze, mit:

- einer Einrichtung zur Erfassung von Personendaten von Systembenutzern,
- einer Einrichtung zur Erfassung von biometrischen Daten der Systembenutzer,
- einer Einrichtung zur Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank und Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,
- einer Einrichtung zum Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,
- einer vor einer Grenze angeordneten Durchgangsschleuse zum Regulieren des Durchgangs der Systembenutzer mit einem Eingang und einem Ausgang, wobei der Eingang und der Ausgang in Grundstellung verschlossen sind,
- einer vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zur Vereinzelung der Systembenutzer,
- einer hinter der Vereinzelungseinrichtung, aber vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zum automatisierten Lesen der auf den Identifikationsmedien gespeicherten Daten,
- einer vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zur automatisierten Überprüfung der Echtheit der Identifikationsmedien,
- einer vor dem Eingang der Durchgangsschleuse angeordneten Einrichtung zur automatisierten Überprüfung des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- einer Einrichtung zum automatisierten Öffnen des Eingangs der Durchgangsschleuse, wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt wurden,
- einer in der Durchgangsschleuse befindlichen Einrichtung zum automatisierten Erfassen von biometrischen Daten eines hineingelassenen Systembenutzers,
- einer Einrichtung zum automatisierten Vergleich der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- einer Einrichtung zum automatisierten Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- einer Einrichtung zur automatisierten Weitergabe der Personendaten an die Fahndungsdatenbank und zur automatisierten Abfrage, ob der Systembenutzer auf einer Fahndungsliste steht, und
- einer Einrichtung zum automatisierten Öffnen des Ausgangs der Durchgangsschleuse und Ermöglichen eines Grenzübertritts des Systembenutzers, wenn das Ergebnis der Fahndungsabfrage negativ ist, und zur automatisierten Auslösung eines Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

[0006] Weiterhin wird die Aufgabe gelöst durch ein Verfahren zur automatisierten Kontrolle des Passierens einer Grenze, das die folgenden Schritte umfaßt:

- Erfassen von Personendaten von Systembenutzern,
- Erfassen von biometrischen Daten der Systembenutzer,

- Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank und Vornahme einer Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,

- Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,

- Vereinzelung der einen Grenzübertrittsversuch unternehmenden Systembenutzer vor einer Durchgangsschleuse mit einem Eingang und einem Ausgang, wobei der Eingang und der Ausgang in Grundstellung geschlossen sind,

- automatisiertes Lesen der auf dem Identifikationsmedium gespeicherten Daten,

- automatisierte Überprüfung der Echtheit des jeweiligen Identifikationsmediums,

- automatisiertes Überprüfen des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,

- automatisiertes Öffnen des Eingangs der Durchgangsschleuse, wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt werden,

- automatisiertes Erfassen von biometrischen Daten eines in die Durchgangsschleuse hineingelassenen Systembenutzers,

- automatisiertes Vergleichen der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,

- automatisiertes Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,

- automatisiertes Weitergeben der Personendaten an die Fahndungsdatenbank und automatisiertes Abfragen, ob der Systembenutzer auf einer Fahndungsliste steht, und

- automatisiertes Öffnen des Ausgangs der Druchgangsschleuse, wenn das Ergebnis der Fahndungsabfrage negativ ist, bzw. automatisiertes Auslösen eine Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

[0007] Insbesondere kann bei dem System vorgesehen sein, daß die Einrichtung zur Erfassung von Personendaten von Systembenutzern eine Einrichtung zum automatischen Einlesen der Personendaten aufweist. Beispielsweise kann die Einrichtung zum automatischen Einlesen der Personendaten ein Scanner sein.

[0008] Vorteilhafterweise umfaßt die Einrichtung zur Erfassung von biometrischen Daten eine Einrichtung zur Erfassung eines Fingerabdruckes und/oder der Netzhautstruktur und/oder der Gesichtsmerkmale und/oder der Stimme und/oder Sprache eines jeweiligen Systembenutzers.

[0009] Eine weitere besondere Ausführungsform des Systems ist gekennzeichnet durch eine Einrichtung zur Verarbeitung der erfaßten biometrischen Daten und Umrechnung in ein oder mehrere repräsentative(s) Datenmerkmal(e), anhand dessen/derer eine Wiedererkennung des Systembenutzers bei der Kontrolle möglich ist.

[0010] Auch kann vorgesehen sein, daß die Einrichtung zur Speicherung von Daten eine Einrichtung zur Verschlüsselung der Personen- und/oder Identifikationsmediumdaten und zur Erzeugung eines identifikationsmediumspezifischen Schlüssels aufweist.

[0011] Ferner kann auch vorgesehen sein, daß die Verschlüsselungseinrichtung ein lokal vorgesehenes Sicherheitsmodul ist oder sich in einem Hintergrundsystem befindet, das über eine On-Line-Datenverbindung verbunden ist.

[0012] Vorzugsweise weist die Einrichtung zur Speicherung der Daten eine Einrichtung zur elektrischen Personalisierung der verschlüsselten Daten in dem Identifikationsmedium und/oder eine Einrichtung zum Aufbringen der Personendaten und gegebenenfalls eines Fotos sowie der Unterschrift des jeweiligen Systembenutzers auf das Identifikationsmedium auf. Beispielsweise können die Personendaten im Thermotransfer-Druck auf das Identifikationsmedium aufgebracht werden.

[0013] Günstigerweise weist die Einrichtung zur Speicherung der Daten eine Einrichtung zum Überziehen des Identifikationsmediums mit einer Laminatfolie auf. Durch die Laminatfolie wird das Identifikationsmedium fälschungssicher.

[0014] Vorzugsweise sind die Identifikationsmedien Smart Cards.

[0015] Günstigerweise ist in der Durchgangsschleuse mindestens eine Videokamera vorgesehen. Dies ermöglicht eine Überwachung der Durchgangsschleuse insbesondere hinsichtlich der Vornahme einer wirksamen Vereinzelung.

[0016] Weiterhin kann vorgesehen sein, daß die Einrichtung zum Lesen der auf den Identifikationsmedien gespeicherten Daten eine Einrichtung zum Berechnen des identifikationsmediumspezifischen Schlüssels aus den verschlüsselten Identifikationsmediumdaten und Verifikation desselben aufweist. Damit ist die Vornahme einer Kartenlegitimationsprüfung möglich.

[0017] Weiterhin weist die Einrichtung zum Lesen der auf dem Identifikationsmedium gespeicherten Daten vorzugsweise eine Einrichtung zum Entschlüsseln der verschlüsselten Personendaten und Verifikation derselben auf Dies ermöglicht eine Personenlegitimationsprüfung.

[0018] Eine weitere besondere Ausführungsform der Erfindung ist gekennzeichnet durch eine Einrichtung zur Erzeugung und Verteilung von Schlüsseln für die Datenverschlüsselungen und Überwachung des Systembetriebes. Eine derartige Einrichtung erfüllt die Funktion eines TrustCenter.

[0019] Eine weitere besondere Ausführungsform der Erfindung ist gekennzeichnet durch eine Einrichtung zur Verwaltung und Überwachung insbesondere der Lebensdauer aller an Systembenutzer ausgegebener Identifikationsmedien.

[0020] Schließlich ist eine weitere besondere Ausführungsform der Erfindung gekennzeichnet durch eine Einrichtung zur kryptographischen Verschlüsselung von zwischen Einrichtungen des Systems und/oder zwischen dem System und externen Einrichtungen übertragenen Daten. Dies soll vor einem unerlaubten Zugriff auf die übertragenen Daten schützen.

[0021] Die Unteransprüche 17 bis 26 betreffen vorteilhafte Weiterentwicklungen des erfindungsgemäßen Verfahrens.

[0022] Der Erfindung liegt die überraschende Erkenntnis zugrunde, daß durch eine Integration der behördlichen Kontrollen in den Gesamtablauf wobei ein Teil der Kontrolle im Prinzip vorgezogen wird, eine Beschleunigung und Vereinfachung der Abwicklung des Grenzverkehrs erzielt wird, ohne daß darunter die Qualität der Kontrolle leidet. Durch die zumindest zum Teil vorgezogene Kontrolle kann die Kontrolle an der Grenze hinsichtlich der bereits vorab kontrollierten, unproblematischen Reisenden vereinfacht und verkürzt werden, wodurch eine Konzentration der Polizei- und Kontrollkräfte auf potentielle Täter und Gefahren möglich wird.

[0023] Die vorab durchgeführte Kontrolle erlaubt eine maschinelle Überprüfung des polizeilich unproblematischen grenzüberschreitenden Reisendenverkehrs mit all den Einzelkomponenten, die auch eine Grenzkontrolle durch Polizeibeamte beinhaltet, nämlich Personenvergleich, Echtheitsprüfung von Grenzübertrittsdokumenten, Fahndungsabfrage, Gestattung des Grenzübertritts. Dabei werden unter Berücksichtigung aller nationalen, Schengener und EU-Anforderungen zuvor aus polizeilicher Sicht unproblematische eingestufte Reisende nach Antragstellung und auf freiwilliger Basis mittels auf ihren Identifikationsmedien gespeicherten Personendaten und biometrischen Daten beim Grenzübertritt jeweils aktuell maschinell identifiziert und über eine On-Line-Fahndungsabfrage polizeilich überpüft.

[0024] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus den Ansprüchen und aus der nachstehenden Beschreibung, in der ein Ausführungsbeispiel anhand der schematischen Zeichnungen im einzelnen erläutert ist. Dabei zeigt:

Figur 1 eine Draufsicht eines Teils eines Systems gemäß einer besonderen Ausführungsform der vorliegenden Erfindung; und

Figur 2 schematisch wesentliche Einrichtungen und Einrichtungsblöcke des Systems;

[0025] Figur 1 zeigt eine Draufsicht eines Teils eines Systems gemäß einer besonderen Ausführungsform der Erfindung. Der gezeigte Teil betrifft die Kontrolle von Systembenutzern direkt an einer Grenze (z. B. Landesgrenze). Figur 1 zeigt eine Durchgangsschleuse 10 mit einem Eingang 12 und einem Ausgang 14. Der Eingang 12 und der Ausgang 14 sind jeweils mit einer Drehtür 16 bzw. 18 versehen. Vor der Drehtür 16 am Eingang 12 befindet sich eine Einrichtung zur Vereinzelung der Systembenutzer (nicht gezeigt). Die Vereinzelung kann mechanisch, aber auch z. B. optisch durchgeführt werden. Beispielsweise kann dazu eine Ampel verwendet werden. Wenn die Ampel auf Grün steht darf eine einzelne Person passieren. Wenn eine Person bei Rot weitergeht, wird ein optischer und/oder akustischer Alarm ausgelöst. Zwischen dieser Einrichtung und der Drehtür 16 befindet sich ein Kartenlesegerät 20 zum Lesen von Smart Cards. Die Drehtür 16 ist in Grundstellung arretiert und verschließt somit den Eingang 12. In der Durchgangsschleuse 10 befindet sich ein Biometriedatenlesegerät 22. Das Kartenlesegerät 20 und das Biometriedatenlesegerät 22 sind mit einem lokalen Server des Bundesgrenzschutzes (nicht gezeigt) verbunden. In der Durchgangsschleuse 10 befindet sich darüber hinaus noch eine Videokamera 24 zur Überwachung der mechanischen Vereinzelung der Systembenutzer.

[0026] In Figur 2 sind schematisch die wesentlichen Einrichtungen einzeln bzw. in Blöcken des Systems gezeigt. Ein Systemblock, der mit dem Bezugszeichen 26 versehen ist, betrifft die Beantragung und Ausgabe einer Karte (sogenanntes Enrolment Center). Die Karte in Form einer Smart Card 28 dient als Berechtigungsausweis für jeden Systembenutzer. Sie wird beim Grenzübertritt in dem in Figur 1 gezeigten Teil des Systems, der hier als dezentrales automatisiertes Grenzkontrollsystem 30 bezeichnet ist, überprüft. Das dezentrale automatisierte Grenzkontrollsystem 30 umfaßt einen lokalen Server des Bundesgrenzschutzes, der über einen Dienststellen-Server 32 des Bundesgrenzschutzes mit einer Fahndungsdatenbank 34 der INPOL, einem Trust Center 36, einer zentralen Datenverwaltungseinrichtung 38 des Bundesgrenzschutzes und dem Enrolment Center 26 in Verbindung steht.

[0027] In dem Enrolment Center 26 kann eine Kartenbeantragung vorgenommen werden. Diese umfaßt alle Prozeßschritte, die zur Erfassung der potentiellen Systembenutzer, also insbesondere die Erfassung ihrer Personen- und biometrischen Daten, notwendig sind. Es können mehrere Enrolment Center vorgesehen sein, die an verschiedenen Orten errichtet sind. Zur Kartenbeantragung legen die potentiellen Systembenutzer ihr

Grenzübertrittsdokument vor, von dem der Bediener eines PCs, auf dem die Erfassungssoftware läuft, die Daten automatisch oder manuell erfaßt. Der Datensatz wird auf einem Formblatt ausgedruckt und vom antragstellenden, potentiellen Systembenutzer unterschrieben. Das Formblatt enthält unter anderem folgende weitere Angaben:

- eine Beschreibung des Systems,
- die Personalien des potentiellen Systembenutzers,
- die Bedingungen für die freiwillige Teilnahme am System,
- die notwendigen datenschutzrechtlichen Erklärungen zur Erhebung, Speicherung, Übermittlung und Verarbeitung der Personendaten des antragstellenden, potentiellen Systembenutzers im Zusammenhang mit der automatisierten Grenzkontrolle,
- einen Hinweis auf die Pflicht des Systembenutzers, bei jedem Grenzübertritt ein gültiges Grenzübertrittsdokument mit sich zu führen, und
- Hinweise zu den anerkannten Reisezwecken, für die das System genutzt werden darf.

[0028] In einem nächsten Schritt wird der Fingerabdruck des potentiellen Systembenutzers mittels eines Fingerabdrucklesegerätes (nicht gezeigt) erfaßt. Die vom Fingerabdrucklesegerät gewonnen Daten werden durch die Verarbeitungssoftware in ein oder mehrere repräsentative Datenmerkmale umgerechnet, anhand derer eine Wiedererkennung des Systembenutzers bei der Grenzkontrolle möglich wird. Dann wird ein Test auf Duplikate vorgenommen, das heißt es wird überprüft, ob der Antragsteller bereits im System erfaßt ist. Die zuvor erfaßten Personendaten werden um die biometrischen Daten ergänzt und zur Verschlüsselung gegeben. Diese erfolgt entweder am lokalen System in einem dafür vorgesehenen Sicherheitsmodul oder in einem Hintergrundsystem, zu welchem für diesen Zweck eine On-Line-Datenverbindung geschaltet wird. Die verschlüsselten Daten werden im Enrolment Center in einen Smart Card-Rohling elektrisch personalisiert und die Personendaten auf dem Smart-Card-Körper im Thermotransfer-Druck aufgebracht. Zusätzlich können gegebenenfalls ein Foto des Systembenutzers sowie seine Personalien (beides erforderlichenfalls als Grundlage für eine manuelle Überprüfung, z. B. im Rahmen von Stichprobenkontrollen), seine Unterschrift und der Name des ausstellenden Enrolment Centers aufgedruckt werden. Anschließend wird der Smart-Card-Körper mit einer fälschungssicheren Laminatfolie überzogen. All diese Schritte laufen in einer Maschine ab und werden vom PC überwacht. Nach einer Funktionskontrolle an einem Terminal im Enrolment Center wird die Smart Card dem Systembenutzer ausgehändigt. Das gesamte Enrolment dauert weniger als 10 Minuten. Die Kartenbeantragung und -ausgabe kann auch gleichzeitig mit der erstmaligen Benutzung des Systems an der Grenze vor Ort vorgenommen werden.

[0029] Alle hoheitlichen Schritte - die Durchführung der vorgezogenen Grenzkontrolle entsprechend der nationalen, Schengener und EU-Anforderungen und die Freigabe der Smart Card - sind einem Beamten der Grenzkontrollbehörde vorbehalten. Er wird gegebenenfalls unterstützt durch Personal bzw. Beauftragte des Betreibers. Für die Mitarbeiter in den Enrolment Center werden ebenfalls geeignete Zugangskontrollen vorgesehen.

[0030] Darüber hinaus stellt die Erfassungssoftware sicher, daß Smart Cards nur mit Zutun legitimierter Grenzkontrollbeamter, nur nach erfolgreichem Verlaufen aller erforderlichen Schritte und nur für visumsbefreite Angehörige bestimmter zugelassener Staaten ausgestellt werden, die im Besitz eines gültigen Reisedokumentes sind.

[0031] Die Kartenkontrolle umfaßt alle Prozesse, die bei der Prüfung des Karteninhabers im Rahmen der Einreise durchgeführt werden. Die Kartenkontrolle findet innerhalb einer Durchgangsschleuse 10 (siehe Figur 1) statt, welche die zu kontrollierende Person betreten muß.

[0032] Die Durchgangsschleuse selbst kann problemlos in die bestehende Infrastruktur integriert werden, das heißt es sind nur geringfügige bauliche Veränderungen notwendig. Der lokale Server dient zur Ablaufsteuerung und zur Kommunikation mit externen Rechnern.

[0033] Vor der Durchgangsschleuse 10 findet zunächst eine mechanische Vereinzelung mittels einer Einrichtung zur mechanischen Vereinzelung (nicht gezeigt) statt, um das Eintreten von Unberechtigten sowie mehreren Personen zur gleichen Zeit zu verhindern. Diese Maßnahme wird durch den Einsatz einer Videokamera 24 in der Durchgangsschleuse 10 und entsprechender Bildauswertungssoftware ergänzt.

[0034] Hinter der Einrichtung zur Vereinzelung, aber vor dem Eingang 12 wird die zu überprüfende Person zum Einführen der Smart Card in ein Kartenlesegerät 20 aufgefordert. In dem Kartenlesegerät 20 befindet sich ein Sicherheitsmodul (nicht gezeigt) zur Echtheitsüberprüfung der Smart Card sowie der darauf gespeicherten Personendaten. Jede authentische Smart Card besitzt einen Smart Card-spezifischen Schlüssel, der basierend auf bestimmten Smart Card Daten von dem Sicherheitsmodul im Kartenlesegerät 20 berechnet und sodann verifiziert werden kann. Die Kommunikation zwischen der Smart Card und dem Sicherheitsmodul in dem Kartenlesegerät 20 wird zusätzlich mit einem temporären Schlüssel geschützt, der vorher zwischen der Smart Card und dem Sicherheitsmodul ausgehandelt worden ist.

[0035] Danach werden die Personendaten einschließlich biometrischen Daten aus der Smart Card gelesen und eine angehängte Signatur (MAC) mit Hilfe des öffentlichen Schlüssels im Sicherheitsmodul auf Echtheit überprüft. So können illegale Datenmanipula-

tionen sicher erkannt werden.

[0036] Wenn die Echtheit der Karte und das Vorliegen keiner Datenmanipulation verifiziert worden sind, läßt sich die Drehtür 16 drehen, so daß die Person in die Durchgangsschleuse gelangen kann. In der Durchgangsschleuse 10 wird mittels des Biometriedatenlesegerätes 22 der Fingerabdruck des Systembenutzers erhoben und ein Vergleich mit den auf seiner Smart Card gespeicherten biometrischen Daten vorgenommen. Dazu werden aus den lokal gewonnen Daten Extrakte gebildet und mit den in der Smart Card gespeicherten Datenmerkmalen verglichen.

[0037] Durch dieses zweistufige Überprüfungsverfahren am Eingang der Durchgangsschleuse und innerhalb derselben wird zweierlei erreicht:

- es wird festgestellt, daß es sich bei der Person, der aufgrund der am Eingang der Durchgangsschleuse geprüften Smart Card der Einlaß gewährt wurde, um einen berechtigten Systembenutzer handelt;

- unberechtigten Personen wird der Eintritt in die Durchgangsschleuse verwehrt; hier dürfte es ausreichen, auf einem Bildschirm am Kartenlesegerät am Eingang der Durchgangsschleuse einen Hinweis zu geben, sich der regulären Grenzkontrolle zu unterziehen.

- Mißbräuchliche Benutzer oder durch das System fälschlicherweise zurückgewiesene Berechtigte (dies läßt sich durch kein technisches System zu 100 % ausschließen) werden spätestens in der Durchgangsschleuse zuverlässig festgestellt. Hier wäre - nach einer entsprechenden automatischen Alarmauslösung durch das System - ein Eingreifen durch die Grenzkontrollbehörde oder einen Beauftragten erforderlich, um die Person aus der Durchgangsschleuse zu befreien und einer regulären Grenzkontrolle zuzuführen.

[0038] Im nächsten Schritt werden die erforderlichen Personendaten über den lokalen Server des Bundesgrenzschutzes zur Überprüfung an eine Fahndungsdatenbank der INPOL weitergeleitet.

[0039] Wenn alle vorab beschriebenen Schritte beanstandungslos durchlaufen werden, wird der Ausgang der Durchgangsschleuse freigegeben. Im Falle einer Beanstandung oder eines fehlerhaften Verhaltens des System wird ein Alarm ausgelöst und mit der Überprüfung der Person durch Personal des Bundesgrenzschutzes fortgefahren.

[0040] Die Gestaltung der Durchgangsschleuse, die Art der verwendeten Vereinzelungstechnik und der Freigabe am Ausgang der Durchgangsschleuse können in Abhängigkeit von z. B. der Ergonomie und der Führung großer Verkehrsströme bestimmt werden.

[0041] Das Trust Center 36 dient als zentrale Systemkomponente zur Verwaltung aller sicherheitsrelevanten Aspekte des Systems, also insbesondere zur Erzeugung und Verteilung von Schlüsseln und Überwachung des laufenden Systembetriebes.

[0042] Die zentrale Datenverwaltungseinrichtung 38 des Bundesgrenzschutzes dient zur Verwaltung aller ausgegebenen Smart Cards mit Funktionen zur Überwachung des Card Life Cycle. Die Kartenverwaltung beinhaltet auch die Funktionen zur Antragsbearbeitung, also der Erfassung der Personendaten und der biometrischen Daten.

[0043] Die besondere Sensibilität der Daten der Smart Cards und der damit verbundenen Funktionalität erfordern ein hohes Maß an Schutz gegen:

- Verfälschung der Personendaten auf der Smart Card

- Verfälschung der biometrischen Daten

- Verfälschung der Verbindung zwischen biometrischen Daten und den Personaldaten

- Manipulationen an einem Kontrollterminal

- Manipulationen bei der Erfassung der Personendaten bzw. der biometrischen Daten und

- Angriffe auf die kryptographischen Funktionen im System.

[0044] Zur umfassenden Absicherung dieser Risiken ist eine schalenartige Sicherheitsarchitektur zur Absicherung zentraler Informationen und Funktionen ratsam. Ziel der Architektur ist, die Errichtung mehrerer Hürden, die ein potentieller Angreifer überwinden muß, um das System zu manipulieren.

[0045] Den Kern bilden die Personendaten zusammen mit den biometrischen Daten. Diese Daten werden im System als eine Einheit betrachtet, das heißt biometrische Daten sind ein Element des Personendatensatzes. Über den Personendatensatz wird zunächst mit Hilfe eines Secure Hash-Verfahrens, z. B. dem SHA-1 Algorithmus, eine kryptographische Prüfsumme erzeugt. Dieser 160 Bit lange Wert hat die typischen Eigenschaften eines guten Hash-Algorithmus, das heißt, er ist im wesentlichen kollisionsfrei. Das Ergebnis des Algorithmus wird als ein Teil der Kryptogrammbildung verwendet, da der gesamte Personendatensatz als Eingabedatum der Verschlüsselung zu groß ist. Der Hash-Wert komprimiert den Inhalt des Personendatensatzes auf eine stark reduzierte Form. Dabei kann vom Hash-Wert nicht auf die ursprünglichen Daten geschlossen werden. Änderungen im Personendatensatz ergeben zwangsläufig eine Änderung im Hash-Wert. Das Secure Hash-Verfahren ist kein Verschlüsselungsverfahren, das heißt, es verwendet keine Schlüssel.

[0046] In der zweiten Schale werden wesentliche Extrakte aus den Personendaten (z. B. Name, Geburtsda-

tum und Geburtsort), insbesondere also die Daten für die Abfrage bei der INPOL-Fahndungsdatenbank, zusammen mit dem Hash-Wert mit einem Private Key-Verfahren verschlüsselt Als Private Key-Verfahren sollen - abhängig von der weiteren Detailabstimmung - RSA mit einer Schlüssellänge von mindestens 1.024 Bit oder elliptische Kurven mit hinreichender Schlüssellänge genutzt werden.

[0047] Für die Verschlüsselung des Extraktes wird der private Schlüssel einer Ausgabestelle oder der private Schlüssel einer zentralen Instanz verwendet Im letzteren Fall muß der Personendatensatz zur Verschlüsselung an die zentrale Instanz versandt werden und er kann erst dann in die Smart Card personalisiert werden (z. B. durch On-Line-Anfrage).

[0048] Für die Entschlüsselung des Extraktes wird der öffentliche Schlüssel benötigt. Dieser wird in den Kontrollterminals hinterlegt. Eine Entschlüsselung liefert zunächst die Personendaten für die INPOL-Abfrage und den Hash-Wert. Der Hash-Wert wird mit einem erneut berechneten Hash-Wert verglichen. Bei Gleichheit kann von einem unverfälschten Datensatz ausgegangen werden.

[0049] Innerhalb des Verfahrens sind eine Reihe von Varianten möglich, deren Nutzung von den konkreten Rahmenbedingungen abhängt:

- Eine eindeutige Smart Card-Nummer könnte in den Personendatensatz aufgenommen und dadurch mit diesem verknüpft werden. Eine Übertragung der Daten auf ein andere Smart Card wäre damit nicht möglich. Eine sinnvolle Nutzung dieser Option setzt eine On-Line-Personalisierung voraus, bei der Personendaten und die Smart Card-Nummer verschlüsselt und direkt in die Smart Card personalisiert werden.

- Die Verschlüsselung des Personendatensatzes kann mit dem privaten Schlüssel der Ausgabestelle durchgeführt werden. Diese würde dann ihren öffentlichen Schlüssel in der Smart Card speichern. Eine Kontrollstation würde dann zur Verifikation des Extraktes den von der Smart Card gelieferten öffentlichen Schlüssel der Ausgabestelle nutzen. Zur Verhinderung des Mißbrauches, etwa der Einspielung von gefälschten öffentlichen Schlüsseln einer Ausgabestelle, müssen die Schlüsselpaare der Ausgabestelle von einer zentralen Instanz elektronisch signiert werden. Ein solches Verfahren erlaubt die Ausgabe der Smart Card ohne Zugriff und Authorisierung durch ein Zentralsystem.

[0050] Jede Smart Card im System erhält bei der Herstellung eine eindeutige Seriennummer. Diese Seriennummer ist Grundlage der kryptographischen Verfahren, die aktiv durch die Smart Card ausgeführt werden. Die Smart Card enthält einen durch Ableitung der Seriennummer unter einem Masterschlüssel gewonnen smartcardspezifischen Schlüssel zur Authentisierung.

[0051] Die Authentisierung erfolgt implizit durch das Auslesen der Personendaten im sogenannten PRO-Mode. Der PRO-Mode ist eine in ISO7816 eingeführte Variante des Lesezugriffs, bei dem die an das Terminal übertragenen Daten durch einen Message Authentication Code (MAC) gesichert werden. Dieser MAC wird dynamisch bei jedem Lesezugriff neu erzeugt, um einen sogenannten Replay-Angriff, also das erneute Einspielen bereits gelesener Daten, auszuschließen.

[0052] Die Erzeugung des MAC erfolgt innerhalb des Betriebssystems der Smart Card unter Nutzung des kartenindividuellen Authentisierungsschlüssels und einer durch das Terminal gelieferten Zufallszahl. Das Terminal enthält hierzu in einem Sicherheitsmodul (z. B. eine weitere Smart Card) einen Zufallszahlengenerator und den Masterschlüssel, welche für die Ableitung des Smart Card-Schlüssels unter der Smart Card-Seriennummer benutzt wird. Das Terminal überprüft selbständig und unmittelbar nach dem Auslesen der Smart Card-Daten den MAC und weist eine Karte mit fehlerhaftem MAC ab.

[0053] Wichtig ist in diesem Zusammenhang, daß der MAC dynamisch durch die Smart Card erzeugt wird. Der dazu notwendige Schlüssel muß in der Smart Card vorhanden sein. Eine Manipulation der Smart Card, z. B. durch Duplizieren, erfordert Zugriff auf diesen Kartenschlüssel, welches nur unter hohem finanziellen Aufwand möglich ist.

[0054] Auch für diese Schutzstufe gibt es eine Variante, die jedoch eine leistungsfähigere Smart Card voraussetzt. Statt einem symmetrischen Verfahren für die MAC-Bildung (in der Regel Triple DES) kann das asymmetrische Verfahren der elliptischen Kurven Anwendung finden. Bei diesem Verfahren wird in der Karte der private, kartenindividuelle Schlüssel auslesegeschützt gespeichert und der öffentliche Schlüssel lesbar gemacht. Der öffentliche Schlüssel muß dazu mit dem privaten Schlüssel des Systembetreibers signiert werden. Ein Kontrollterminal braucht nun nur den weniger sicherheitskritischen, öffentlichen Schlüssel des Systembetreibers zu speichern und mit ihm die Echtheit des kartenindividuellen öffentlichen Schlüssel zu überprüfen.

[0055] Das Auslesen der Daten erfolgt analog dem symmetrischen Verfahren, mit der Abweichung, daß der MAC durch den asymmetrischen Algorithmus erzeugt wird.

[0056] Solche Verfahren auf Basis asymmetrischer Kryptographie finden aufgrund ihrer hohen Anforderungen an die Rechenleistung nur begrenzten Einsatz in Smart Cards. Im Detail muß hier sicher noch das Antwort-Zeitverhalten einer solchen Lösung betrachtet werden.

[0057] Die Übertragung der Daten zwischen Einrichtungen des Systems, insbesondere die Übertragung der Daten bei der Kartenausgabe soll durch kryptographische Verfahren abgesichert werden. Hierzu bieten sich Verfahren der Line-Verschlüsselung an, mit denen sich geschützte, transparente Datenkanäle aufbauen lassen.

[0058] Mit diesen Verfahren läßt sich die Integrität der Daten und die Vertraulichkeit sicherstellen. Letztere ist

insbesondere bei der Erzeugung und Verteilung der Systemschlüssel von Bedeutung.

[0059] Ein wesentlicher, oft unterschätzter Mechanismus zur Sicherung von Informationssystemen ist die Einbettung der technischen Systeme in eine zuverlässige Ablauforganisation (5. Schale). Die besten und längsten Schlüsselverfahren der Welt nützen nichts, wenn die Schlüssel einfach zugänglich sind. Technische Verfahren können hier nur einen begrenzten Schutz herstellen, einem Angriff von innen sind sie oft schutzlos ausgeliefert.

[0060] Ein weiteres Merkmal der 5. Schale ist die Absicht, alle sicherheitsrelevanten Systemeinrichtungen in die Obhut der Grenzkontrollbehörde zu stellen. Dadurch soll aus Sicht der Behörde gewährleistet werden, daß ein Zugriff auf diese Systemeinrichtungen ohne ihr Zutun und unter keinen Umständen möglich ist. Dazu müssen sich nicht alle Systemeinrichtungen tatsächlich in den Räumlichkeiten der Behörde selbst befinden. Der technischen Betrieb könnte auch bei einem Beauftragten der Behörde durchgeführt werden, solange durch entsprechende vertragliche Gewährleistungsklauseln ein unerlaubter Zugriff durch Dritte (einschließlich dem Betreiber) unmöglich ist.

[0061] Eine zusätzliche organisatorische Schutzvorkehrung besteht darin, daß alle hoheitlichen Schritte - das heißt die Durchführung der vorgezogenen Grenzkontrolle entsprechend den nationalen, Schengener und EU-Anforderungen und die Freigabe der Smart Card - einem Beamten der Grenzkontrollbehörde vorbehalten sind. Für ihn sowie für die anderen Mitarbeiter in dem Enrolment Center bestehen geeignete Zugangskontrollen.

[0062] Darüber hinaus stellt die Erfassungssoftware sicher, daß Smart Cards

- nur auf der Basis im System bereits bekannter Smart Card-Rohlinge (jeder Smart Card-Rohling besitzt eine ein-eindeutige Kartennummer),
- nur mit Zutun im System legitimierter Grenzkontrollbeamter,
- nur nach erfolgreichem Durchlaufen aller erforderlichen Schritte und
- nur für Angehörige bestimmter zugelassener Staaten ausgestellt werden, die im Besitz eines gültigen Reisedokumentes sind.

[0063] Die erfindungsgemäßen Systeme haben einige Vorteile, die es von verschiedenen anderen, bislang erfolglosen Versuchen zur flächendeckenden Einführung automatisierter Grenzkontrollen unterscheiden:

- Das System stellt eine wirksame und sparsame Möglichkeit dar, Grenzkontrollbehörden effizienter zu machen. Das System erlaubt es den Grenzkontrollkräften, sich auf einen eher polizeilich relevanten Personenkreis zu fokussieren. Damit können sie mit weniger Aufwand mehr für Sicherheit und Service leisten.
- Die gemäß einer besonderen Ausführungsform der Erfindung eingesetzte Smart Card erlaubt die Speicherung auch sensibler Daten ohne das Risiko eines Mißbrauchs durch unerlaubte Veränderungen oder von Fälschungen.
- Das Verfahren erlaubt kürzestmögliche Transaktionszeiten (im wesentlichen nur abhängig vom Antwort-Zeitverhalten der Abfrage bei der INPOL-Fahndungsdatenbank).
- Das Verfahren erlaubt geringstmögliche Transaktionskosten.
- Das Verfahren birgt keine datenschutzrechtliche Problematik (der Besitzer trägt seine vor unberechtigtem Zugriff sicher geschützten personenbezogenen Daten mit sich).
- Die in einer besonderen Ausführungsform der Erfindung verwendete Smart Card enthält ausreichende Speicherkapazität für diese und gegebenenfalls weitere zukünftige Anwendungen mit zusätzlichen Nutzpotentialen.
- Auf der gemäß einer besonderen Ausführungsform der Erfindung verwendeten Smart Card befindet sich ausreichend Platz, um gegebenenfalls weitere Sicherheitsmerkmale (z. B. maschinenlesbares Hologramm mit Mikroschrift) oder andere Speichervarianten gleichzeitig zu nutzen.

Bezugszeichenliste

[0064]

8	Grenze
10	Durchgangsschleuse
12	Eingang
14	Ausgang
16,18	Drehtür
20	Kartenlesegerät
22	Biometriedatenlesegerät
24	Videokamera
26	Enrolment Center
28	Smart Card
30	dezentrales automatisiertes Grenzkontrollsystem
32	Dienststellen-Server
34	Fahndungsdatenbank
36	Trust Center
38	zentrale Datenverwaltungseinrichtung

Patentansprüche

1. System zur automatisierten Kontrolle des Passierens einer Grenze, mit:

- einer Einrichtung (26) zur Erfassung von Personendaten von Systembenutzern,
- einer Einrichtung (26) zur Erfassung von biometrischen Daten der Systembenutzer,
- einer Einrichtung (26) zur Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank (34) und Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,
- einer Einrichtung (26) zum Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium (26) und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,
- einer vor einer Grenze (8) angeordneten Durchgangsschleuse (10) zum Regulieren des Durchgangs der Systembenutzer mit einem Eingang (12) und einem Ausgang (14), wobei der Eingang (12) und der Ausgang (14) in Grundstellung verschlossen sind,
- einer vor dem Eingang (12) der Durchgangsschleuse (10) angeordneten Einrichtung zur Vereinzelung der Systembenutzer,
- einer hinter der Vereinzelungseinrichtung, aber vor dem Eingang (12) der Durchgangsschleuse (10) angeordneten Einrichtung (20) zum automatisierten Lesen der auf den Idenfifikationsmedien gespeicherten Daten,
- einer vor dem Eingang (12) der Durchgangsschleuse (10) angeordneten Einrichtung (20) zur automatisierten Überprüfung der Echtheit der Identifikationsmedien,
- einer vor dem Eingang (12) der Durchgangsschleuse (10) angeordneten Einrichtung (20) zur automatisierten Überprüfung des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- einer Einrichtung zum automatisierten Öffnen des Eingangs (12) der Durchgangsschleuse (10), wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt wurden,
- einer in der Durchgangsschleuse (10) befindlichen Einrichtun (22) zum automatisierten Erfassen von biometrischen Daten eines hineingelassenen Systembenutzers,
- einerEinrichtung (22) zum automatisierten Vergleich der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- einer Einrichtung zum automatisierten Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- einer Einrichtung zur automatisierten Weitergabe der Personendaten an die Fahndungsdatenbank (34) und zur automatisierten Abfrage, ob der Systembenutzer auf einer Fahndungsliste steht, und
- einer Einrichtung zum automatisierten Öffnen des Ausgangs der Durchgangsschleuse (10) und Ermöglichen eines Grenzübertritts des Systembenutzers, wenn das Ergebnis der Fahndungsabfrage negativ ist, und zur automatisierten Auslösung eines Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist. 1

2. System nach Anspruch 1, **dadurch gekennzeichnet, daß** die Einrichtung (26) zur Erfassung von Personendaten von Systembenutzern eine Einrichtung zum automatischen Einlesen der Personendaten aufweist.

3. System nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** die Einrichtung (22,26) zur Erfassung von biometrischen Daten eine Einrichtung zur Erfassung eines Fingerabdruckes und/oder der Netzhautstruktur und/oder der Gesichtsmerkmale und/oder der Stimme und/oder Sprache eines jeweiligen Systembenutzers aufweist.

4. System nach einem der Ansprüche 1 bis 3, **gekennzeichnet durch** eine Einrichtung zur automatisierten Verarbeitung der erfaßten biometrischen Daten und automatisierten Umrechnung in ein oder mehrere repräsentative(s) Datenmerkmal(e), anhand dessen/derer eine automatisierten Wiedererkennung des Systembenutzers bei der Kontrolle möglich ist.

5. System nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, daß** die Einrichtung (26) zur Speicherung von Daten eine Einrichtung zur Verschlüsselung der Personen- und/oder Identifikationsmediumdaten und zur Erzeugung eines identifikationsmediumspezifischen Schlüssels aufweist.

6. System nach Anspruch 5, **dadurch gekennzeichnet, daß** die Verschlüsselungseinrichtung ein lokal vorgesehenes Sicherheitsmodul ist oder sich in einem Hintergrundsystem befindet, das über eine On-Line-Datenverbindung verbunden ist.

7. System nach Anspruch 5 oder 6, **dadurch gekennzeichnet, daß** die Einrichtung (26) zur Speicherung

der Daten eine Einrichtung zur elektrischen Personalisierung der verschlüsselten Daten in dem Identifikationsmedium und/oder eine Einrichtung zum Aufbringen der Personendaten und gegebenenfalls eines Fotos sowie der Unterschrift des jeweiligen Systembenutzers auf das Identifikationsmedium aufweist.

8. System nach Anspruch 7, **dadurch gekennzeichnet, daß** die Einrichtung (26) Speicherung der Daten eine Einrichtung zum Überziehen des Identifikationsmediums mit einer Laminatfolie aufweist.

9. System nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, daß** die Identifikationsmedien Smart Cards (28) sind.

10. System nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, daß** in der Durchgangsschleuse (10) mindestens eine Videokamera (24) vorgesehen ist.

11. System nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, daß** die Einrichtung (20) zum automatisierten Lesen der auf den Identifikationsmedien gespeicherten Daten eine Einrichtung zum Berechnen des identifikationsmediumspezifischen Schlüssels aus den verschlüsselten Identifikationsmediumdaten und Verifikation desselben aufweist

12. System nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet, daß** die Einricthung (20) zum automatisierten Lesen der auf dem Identifikationsmedium gespeicherten Daten eine Einrichtung zum Entschlüsseln der verschlüsselten Personendaten und Verifikation derselben aufweist.

13. System nach einem der vorangehenden Ansprüche, **gekennzeichnet durch** eine Einrichtung (36) zur Erzeugung und Verteilung von Schlüsseln für die Datenverschlüsselungen und Überwachung des Systembetriebes.

14. System nach einem der vorangehenden Ansprüche, **gekennzeichnet durch** eine Einrichtung zur Verwaltung und Überwachung insbesondere der Lebensdauer aller an Systembenutzer ausgegebener Identifikationsmedien.

15. System nach einem der vorangehenden Ansprüche, **gekennzeichnet durch** eine Einrichtung zur kryptographischen Verschlüsselung von zwischen Einrichtungen des Systems und/oder zwischen aus dem System und externen Einrichtungen übertragenen Daten.

16. Verfahren zur automatisierten Kontrolle des Passierens einer Grenze, das die folgenden Schritte umfaßt:

- Erfassen von Personendaten von Systembenutzern,
- Erfassen von biometrischen Daten der Systembenutzer,
- Weitergabe der Personendaten der Systembenutzer an eine Fahndungsdatenbank und Vornahme einer Abfrage, ob der jeweilige Systembenutzer auf einer Fahndungsliste steht,
- Speichern von Daten, die die Personendaten und biometrischen Daten des jeweiligen Systembenutzers umfassen, auf einem für jeden Systembenutzer vorgesehenen Identifikationsmedium und gegebenenfalls identifikationsmediumspezifischer Daten, wenn das Ergebnis der Fahndungsabfrage negativ ist,
- Vereinzelung der einen Grenzübertrittsversuch unternehmenden Systembenutzer vor einer Durchgangsschleuse mit einem Eingang und einem Ausgang, wobei der Eingang und der Ausgang in Grundstellung geschlossen sind,
- automatisiertes Lesen der auf dem Identifikationsmedium gespeicherten Daten,
- automatisierte Überprüfung der Echtheit des jeweiligen Identifikationsmediums,
- automatisiertes Überprüfen des Vorliegens einer Manipulation der Daten auf dem jeweiligen Identifikationsmedium,
- automatisiertes Öffnen des Eingangs der Durchgangsschleuse, wenn die Echtheit des jeweiligen Identifikationsmediums und keine Manipulation der Daten auf dem jeweiligen Identifikationsmedium festgestellt werden,
- automatisiertes Erfassen von biometrischen Daten eines in die Durchgangsschleuse hineingelassenen Systembenutzers,
- automatisiertes Vergleichen der erfaßten biometrischen Daten mit den auf dem Identifikationsmedium des hineingelassenen Systembenutzers gespeicherten biometrischen Daten,
- automatisiertes Auslösen eines Alarmsignals, wenn die erfaßten und die auf dem jeweiligen Identifikationsmedium gespeicherten biometrischen Daten nicht übereinstimmen,
- automatisiertes Weitergeben der Personendaten an die Fahndungsdatenbank und automatisiertes Abfragen, ob der Systembenutzer auf einer Fahndungsliste steht, und
- automatisiertes Öffnen des Ausgangs der Druchgangsschleuse, wenn das Ergebnis der Fahndungsabfrage negativ ist, bzw. automatisiertes Auslösen eine Alarmsignals, wenn das Ergebnis der Fahndungsabfrage positiv ist.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, daß** die Personendaten der Systembenut-

zer durch automatisches Einlesen erfaßt werden.

18. Verfahren nach Anspruch 16 oder 17, **dadurch gekennzeichnet, daß** der Fingerabdruck und/oder die Netzhautstruktur und/oder die Gesichtsmerkmale und/oder die Stimme und/oder die Sprache eines jeweiligen Systembenutzers erfaßt wird/werden.

19. Verfahren nach einem der Ansprüche 16 bis 18, **dadurch gekennzeichnet, daß** die erfaßten biometrischen Daten verarbeitet und in einer oder mehrere repräsentative(s) Datenmerkmal(e) umgerechnet werden, anhand dessen/derer eine Wiedererkennung des Systembenutzers bei der Kontrolle möglich ist.

20. Verfahren nach einem der Ansprüche 16 bis 19, **dadurch gekennzeichnet, daß** die Personen- und/oder Identifikationsmediumdaten verschlüsselt werden und ein idenfifikationsmediumspezifischer Schlüssel erzeugt wird.

21. Verfahren nach einem der Ansprüche 16 bis 20, **dadurch gekennzeichnet, daß** die verschlüsselten Daten in dem Identifikationsmedium elektrische personalisiert und/oder die Personendaten und gegebenenfalls ein Foto sowie Unterschriften des jeweiligen Systembenutzers auf das Identifikationsmedium aufgebracht werden.

22. Verfahren nach einem der Ansprüche 16 bis 21, **dadurch gekennzeichnet, daß** die Identifikationsmedien mit einer Laminatfolie überzogen werden.

23. Verfahren nach einem der Ansprüche 16 bis 22, **dadurch gekennzeichnet, daß** als Identifikationsmedium Smart Cards verwendet werden.

24. Verfahren nach einem der Ansprüche 16 bis 23, **dadurch gekennzeichnet, daß** die Durchgangsschleuse mittels einer Videokamera überwacht wird.

25. Verfahren nach einem der Ansprüche 16 bis 24, **dadurch gekennzeichnet, daß** aus den verschlüsselten Identifikationsmediumdaten ein identifikationsmediumspezifischer Schlüssel berechnet und verifiziert wird.

26. Verfahren nach einem der Ansprüche 16 bis 25, **dadurch gekennzeichnet, daß** die verschlüsselten Personendaten entschlüsselt und verifiziert werden.

Claims

1. System for automated border-crossing control, with:

- a device (26) for recording personal data of system users,
- a device (26) for recording biometric data of system users,
- a device (26) for transmitting the personal data of system users to a wanted persons database (34) and inquiring whether the corresponding system user is on a wanted persons list,
- a device (26) for storage of data, comprising the personal data and biometric data of the corresponding system user, on an identification medium (28) provided for each system user and optionally data specific to the identification medium, when the result of the wanted persons inquiry is negative,
- a transit gate (10) arranged in front of a boundary (8) to control the passage of system users, with an entrance (12) and an exit (14), in which the entrance (12) and exit (14) are closed in the base position,
- a device for isolation of system users arranged in front of the entrance (12) of transit gate (10),
- a device (20) for the automated reading of the data stored on the identification media, said device (20) being arranged behind the isolation device, but in front of the entrance (12) to the transit gate (10),
- a device (20) for the automated checking of the authenticity of the identification media, said device (20) being arranged in front of the entrance (12) of transit gate (10),
- a device (20) for the automated checking of the presence of data manipulation on the corresponding identification medium, said device (20) being arranged in front of the entrance (12) of the transit gate (10),
- a device for the automated opening of the entrance (12) of transit gate (10), when the authenticity of the corresponding identification medium and no data manipulation on the corresponding identification medium have been established,
- a device (22) for the automated recording of biometric data of an admitted system user, said device (22) being situated in the transit gate (10),
- a device (22) for automated comparison of the recorded biometric data with the biometric data stored on the identification medium of the admitted system user,
- a device for the automated triggering of an alarm signal, when the recorded biometric data and the biometric data stored on the corresponding identification medium do not correspond,
- a device for the automated transmitting of personal data to the wanted persons database (34) and automated inquiring as to whether the system user is on a wanted persons list, and
- a device for the automated opening of the exit of the transit gate (10) and permitting border-crossing of the system user, when the result of

the wanted persons inquiry is negative, and for the automated triggering of an alarm signal, when the result of the wanted persons inquiry is positive.

2. System according to Claim 1, **characterized in that** the device (26) for recording the personal data of system users has a device for automatic entry of personal data.

3. System according to Claim 1 or 2, **characterized in that** the device (22, 26) for recording biometric data has a device for recording a fingerprint and/or retinal structure and/or facial features and/or voice and/or language of a corresponding system user.

4. System according to one of Claims 1 to 3, **characterized by** a device for automated processing of recorded biometric data and automated conversion to one or more representative data features, by means of which automated recognition of the system user is possible during control.

5. System according to one of the preceding claims, **characterized in that** the device (26) for storage of data has a device for encryption of the personal and/or identification medium data and for generation of an identification medium-specific code.

6. System according to Claim 5, **characterized in that** the encryption device is a locally provided security module or is situated in a background system that is connected via an online data connection.

7. System according to Claim 5 or 6, **characterized in that** the device (26) for storage of data has a device for electrical personalization of the encrypted data in the identification medium and/or a device for application of personal data and optionally a photo, as well as signature of the corresponding system user, to the identification medium.

8. System according to Claim 7, **characterized in that** the device (26) for storage of data has a device for coating the identification medium with a laminate film.

9. System according to one of the preceding claims, **characterized in that** the identification media are Smart Cards (28).

10. System according to one of the preceding claims, **characterized in that** at least one video camera (24) is provided in the transit gate (10).

11. System according to one of the preceding claims, **characterized in that** the device (20) for the automated reading of the data stored in the identification media has a device for calculating the identification medium-specific code from the encrypted identification medium data and verification of it.

12. System according to one of the preceding claims, **characterized in that** the device (20) for the automated reading of the data stored on the identification medium has a device for decoding the encrypted personal data and verification of it.

13. System according to one of the preceding claims, **characterised by** a device (36) for generation and distribution of codes for the data encryption and monitoring of system operations.

14. System according to one of the preceding claims, **characterized by** a device for management and monitoring, especially of the lifetime of all identification media issued to system users.

15. System according to one of the preceding claims, **characterized by** a device for encryption of data transferred between devices of the system and/or between the system and external devices.

16. Method for the automated control of border-crossing, comprising the following steps:

- recording of personal data of system users,
- recording of biometric data of system users,
- transfer of personal data of system users to a wanted persons database and performance of an inquiry, whether the corresponding system user is on a wanted persons list,
- storage of data, comprising the personal data and biometric data of the corresponding system user, on an identification medium provided for each system user and optionally identification medium-specific data, if the result of the wanted persons inquiry is negative,
- isolation of system users undertaking a border-crossing attempt in front of a transit gate with an entrance and an exit, in which the entrance and exit are closed in the base state,
- automated reading of data stored in the identification medium,
- automated checking of the authenticity of the corresponding identification medium,
- automated checking of the presence of data manipulation on the corresponding identification medium,
- automated opening of the entrance of the transit gate when the authenticity of the corresponding identification medium and no data manipulation on the corresponding identification medium are established,
- automated recording of biometric data of a system user admitted to the transit gate,

- automated comparison of the recorded biometric data with the biometric data stored on the identification medium of the admitted system user,
- automated triggering of an alarm signal, when the recorded biometric data and the data stored on the corresponding identification medium do not correspond,
- automated transmission of personal data to the wanted persons database and automated inquiry whether the system user is on a wanted persons list, and
- automated opening of the exit of the transit gate, when the result of the wanted persons inquiry is negative, or automated triggering of an alarm signal, when the result of the wanted persons inquiry is positive.

17. Method according to Claim 16, **characterized in that** the personal data of system users are recorded by automatic entry.

18. Method according to Claim 16 or 17, **characterized in that** the fingerprint and/or retinal structure and/or facial features and/or voice and/or language of a corresponding system user is/are recorded.

19. Method according to one of Claims 16 to 18, **characterized in that** the recorded biometric data are processed and converted to one or more representative data features, by means of which recognition of the system user is possible during control.

20. Method according to one of Claims 16 to 19, **characterized in that** the personal and/or identification medium data are encrypted and an identification medium-specific code is generated.

21. Method according to one of Claims 16 to 20, **characterized in that** the encrypted data are electrically personalized in the identification medium and/or the personal data and optionally a photo, as well as signatures of the corresponding system user, are applied to the identification medium.

22. Method according to one of Claims 16 to 21, **characterized in that** the identification media are coated with a laminate film.

23. Method according to one of Claims 16 to 22, **characterized in that** Smart Cards are used as identification medium.

24. Method according to one of Claims 16 to 23, **characterized in that** the transit gate is monitored by means of a video camera.

25. Method according to one of Claims 16 to 24, **characterized in that** an identification medium-specific code is calculated and verified from the encrypted identification medium data.

26. Method according to one of Claims 16 to 25, **characterized in that** the encrypted personal data are decoded and verified.

Revendications

1. Système de contrôle automatique du passage d'une frontière avec :

- un équipement (26) d'enregistrement des données personnelles d'utilisateurs du système,
- un équipement (26) d'enregistrement des données biométriques des utilisateurs du système,
- un équipement (26) de transmission des données personnelles des utilisateurs du système vers une banque de données de recherche (34) et interrogation pour savoir si l'utilisateur présent du système se trouve sur une liste de recherche,
- un équipement (26) de mémorisation de données englobant les données personnelles et les données biométriques de l'utilisateur présent du système, sur un moyen d'identification (28) prévu pour chaque utilisateur du système et le cas échéant des données spécifiques au moyen d'identification, lorsque le résultat de la demande de recherche est négatif,
- un sas de transit (10) disposé avant une frontière (8) pour réguler le transit des utilisateurs du système avec une entrée (12) et une sortie (14), l'entrée (12) et la sortie (14) étant fermées en position normale,
- un équipement disposé avant l'entrée (12) du sas de transit (10) pour isoler les utilisateurs du système,
- un équipement (20) disposé derrière l'équipement d'isolement mais avant l'entrée (12) du sas de transit (10) pour la lecture automatique des données mémorisées sur le moyen d'identification,
- un équipement (20) disposé avant l'entrée (12) du sas de transit (10) pour la vérification automatique de l'authenticité des moyens d'identification,
- un équipement (20) disposé avant l'entrée (12) du sas de transit (10) pour la vérification automatique de l'existence d'une manipulation des données sur le présent moyen d'identification,
- un équipement pour l'ouverture automatique de l'entrée (12) du sas de transit (10) lorsque l'authenticité des moyens d'identification présents a été constatée et qu'aucune manipulation des données sur le présent moyen d'identifica-

tion n'a été constatée,
- un équipement (22) disposé dans le sas de transit (10) pour l'enregistrement automatique de données biométriques d'un utilisateur du système qu'on aura laissé pénétrer,
- un équipement (22) pour la comparaison automatique des données biométriques enregistrées avec les données biométriques mémorisées sur le moyen d'identification de l'utilisateur du système qu'on aura laissé pénétrer,
- un équipement pour le déclenchement automatique d'un signal d'alarme lorsque les données biométriques enregistrées ne concordent pas avec les données biométriques mémorisées sur le moyen d'identification présent,
- un équipement pour la transmission automatique des données personnelles vers la banque de données de recherche (34) et pour l'interrogation automatique pour savoir si l'utilisateur du système se trouve sur une liste de recherche, et
- un équipement pour l'ouverture automatique de la sortie du sas de transit (10) et pour permettre à l'utilisateur du système de passer la frontière lorsque le résultat de l'interrogation de la recherche est négatif, et pour le déclenchement automatique d'un signal d'alarme lorsque le résultat de l'interrogation de la recherche est positif.

2. Système selon la revendication 1, **caractérisé en ce que** l'équipement (26) d'enregistrement des données personnelles d'utilisateurs du système comporte un équipement pour la lecture automatique des données personnelles.

3. Système selon la revendication 1 ou 2, **caractérisé en ce que** l'équipement (22, 26) d'enregistrement des données biométriques comporte un équipement pour l'enregistrement d'une empreinte digitale et/ou de la structure de la rétine et/ou des caractéristiques du visage et/ou de la voix et/ou de la langue d'un utilisateur présent.

4. Système selon une des revendications 1 à 3, **caractérisé par** un équipement de traitement automatique des données biométriques enregistrées et conversion automatique en une ou plusieurs donnée(s) caractéristique(s) représentative(s), permettant une reconnaissance automatique de l'utilisateur du système lors d'un contrôle.

5. Système selon une des revendications précédentes, **caractérisé en ce que** l'équipement (26) pour la mémorisation de données comporte un équipement pour l'encodage des données personnelles et/ou des données du moyen d'identification et pour la génération d'une clé spécifique du moyen d'identification.

6. Système selon la revendication 5, **caractérisé en ce que** l'équipement pour l'encodage est un module de sécurité prévu en local ou bien se trouve dans un système à l'arrière-plan relié par une liaison de données en ligne.

7. Système selon la revendication 5 ou 6, **caractérisé en ce que** l'équipement (26) pour la mémorisation des données possède un équipement pour la personnalisation électrique des données encodées sur le moyen d'identification et/ou un équipement pour l'introduction des données personnelles et le cas échéant une photo ainsi que la signature de l'utilisateur présent du système sur le moyen d'identification.

8. Système selon la revendication 7, **caractérisé en ce que** l'équipement (26) pour la mémorisation des données possède un équipement pour la couverture du moyen d'identification avec une feuille laminée.

9. Système selon une des revendications précédentes, **caractérisé en ce que** les moyens d'identification sont des cartes à puces (28).

10. Système selon une des revendications précédentes, **caractérisé en ce qu'**au moins une caméra vidéo (24) est prévue dans le sas de transit (10).

11. Système selon une des revendications précédentes, **caractérisé en ce que** l'équipement (20) pour la lecture automatique des données mémorisées sur les moyens d'identification comporte un équipement pour le calcul de la clé spécifique du moyen d'identification à partir des données encodées du moyen d'identification et la vérification de celle-ci.

12. Système selon une des revendications précédentes, **caractérisé en ce que** l'équipement (20) pour la lecture automatique des données mémorisées sur le moyen d'identification comporte un équipement pour le décodage des données personnelles encodées et la vérification de celles-ci.

13. Système selon une des revendications précédentes, **caractérisé par** un équipement (36) pour la génération et la distribution de clés pour les encodages des données et la surveillance du fonctionnement du système.

14. Système selon une des revendications précédentes, **caractérisé par** un équipement pour la gestion et la surveillance notamment de la durée de vie de tous moyens d'identification fournis à des utilisateurs du système.

15. Système selon une des revendications précédentes, **caractérisé par** un équipement pour l'encodage

cryptographique de données transmises entre des équipements du système et/ou entre des équipements du système et des équipements externes.

16. Procédé de contrôle automatique du passage d'une frontière comportant les étapes suivantes :

- enregistrement des données personnelles d'utilisateurs du système,
- enregistrement des données biométriques des utilisateurs du système,
- transmission des données personnelles des utilisateurs du système vers une banque de données de recherche et entreprendre l'interrogation pour savoir si l'utilisateur présent du système se trouve sur une liste de recherche,
- mémorisation de données englobant les données personnelles et les données biométriques de l'utilisateur présent du système, sur un moyen d'identification prévu pour chaque utilisateur du système et le cas échéant des données spécifiques au moyen d'identification, lorsque le résultat de la demande de recherche est négatif,
- isolation des utilisateurs du système entreprenant un passage de frontière devant un sas de transit avec une entrée et une sortie, l'entrée et la sortie étant fermées en position normale,
- lecture automatique des données mémorisées sur le moyen d'identification,
- vérification automatique de l'authenticité des moyens d'identification,
- vérification automatique de l'existence d'une manipulation des données sur le présent moyen d'identification,
- ouverture automatique de l'entrée du sas de transit lorsque l'authenticité du moyen d'identification présent a été constatée et qu'aucune manipulation des données sur le présent moyen d'identification n'a été constatée,
- enregistrement automatique de données biométriques d'un utilisateur du système qu'on aura laissé pénétrer,
- comparaison automatique des données biométriques enregistrées avec les données biométriques mémorisées sur le moyen d'identification de l'utilisateur du système qu'on aura laissé pénétrer,
- déclenchement automatique d'un signal d'alarme lorsque les données biométriques enregistrées ne concordent pas avec les données biométriques mémorisées sur le moyen d'identification présent,
- transmission automatique des données personnelles vers la banque de données de recherche et interrogation automatique pour savoir si l'utilisateur du système se trouve sur une liste de recherche, et
- ouverture automatique de la sortie du sas de transit lorsque le résultat de l'interrogation de la recherche est négatif, respectivement déclenchement automatique d'un signal d'alarme lorsque le résultat de l'interrogation de la recherche est positif.

17. Procédé selon la revendication 16, **caractérisé en ce que** les données personnelles des utilisateurs du système sont enregistrées par lecture automatique.

18. Procédé selon la revendication 16 ou 17, **caractérisé en ce que** l'empreinte digitale et/ou la structure de la rétine et/ou les caractéristiques du visage et/ou la voix et/ou la langue d'un utilisateur présent est/sont enregistré(s).

19. Procédé selon une des revendications 16 à 18, **caractérisé en ce que** les données biométriques enregistrées sont traitées et converties en une ou plusieurs donnée(s) caractéristique(s) représentative(s), permettant une reconnaissance automatique de l'utilisateur du système lors d'un contrôle.

20. Procédé selon une des revendications 16 à 19, **caractérisé en ce que** les données personnelles et/ou les données du moyen d'identification sont encodées et qu'une clé spécifique du moyen d'identification est générée.

21. Système selon une des revendications 16 à 20, **caractérisé en ce que** les données encodées sont électriquement personnalisées dans le moyen d'identification et/ou les données personnelles et le cas échéant une photo ainsi que les signatures de l'utilisateur présent du système sont introduites dans le moyen d'identification.

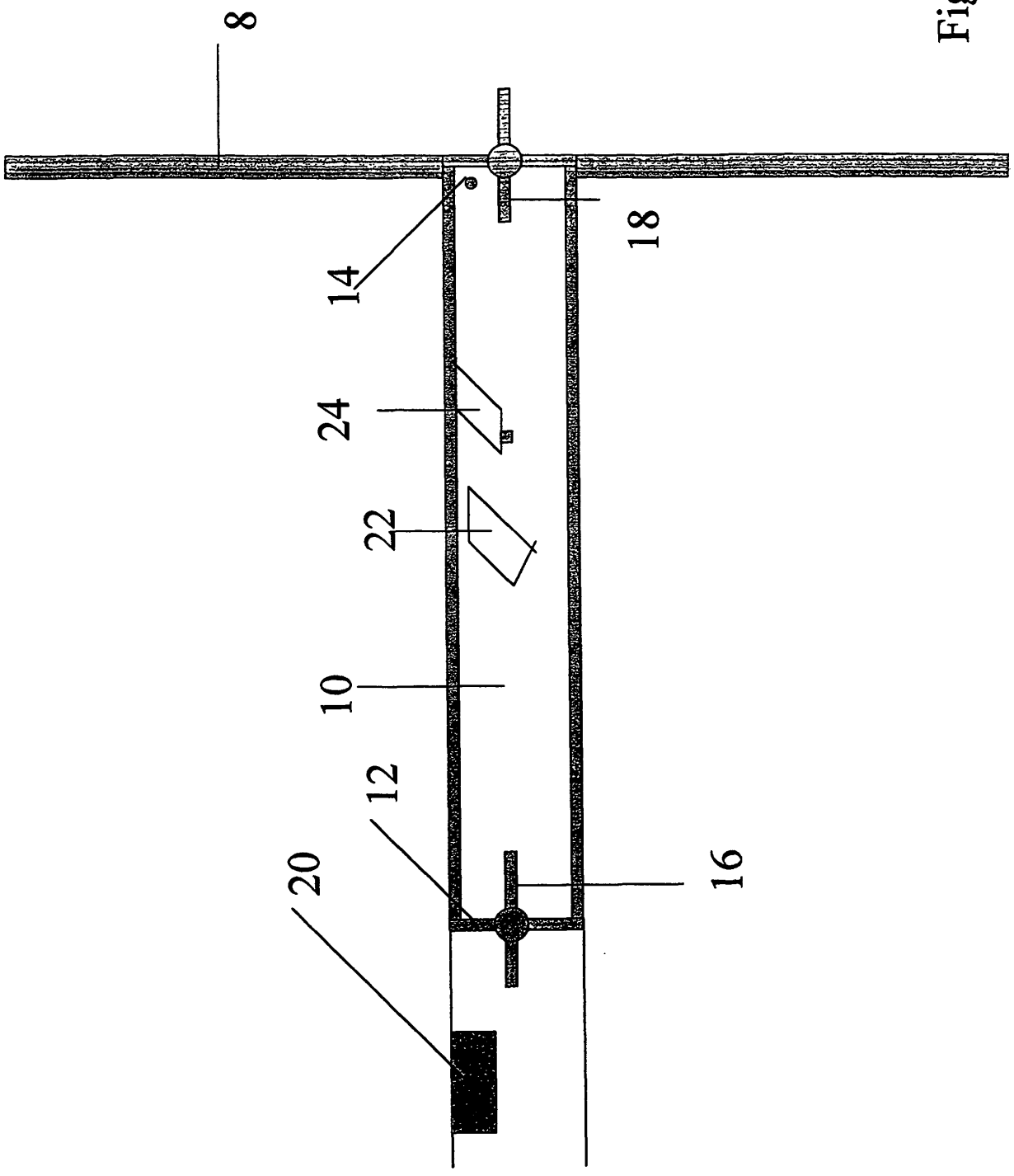
22. Procédé selon une des revendications 16 à 21, **caractérisé en ce que** le moyen d'identification est revêtu d'une feuille laminée.

23. Procédé selon une des revendications 16 à 22, **caractérisé en ce que** des cartes à puces sont utilisées comme moyen d'identification.

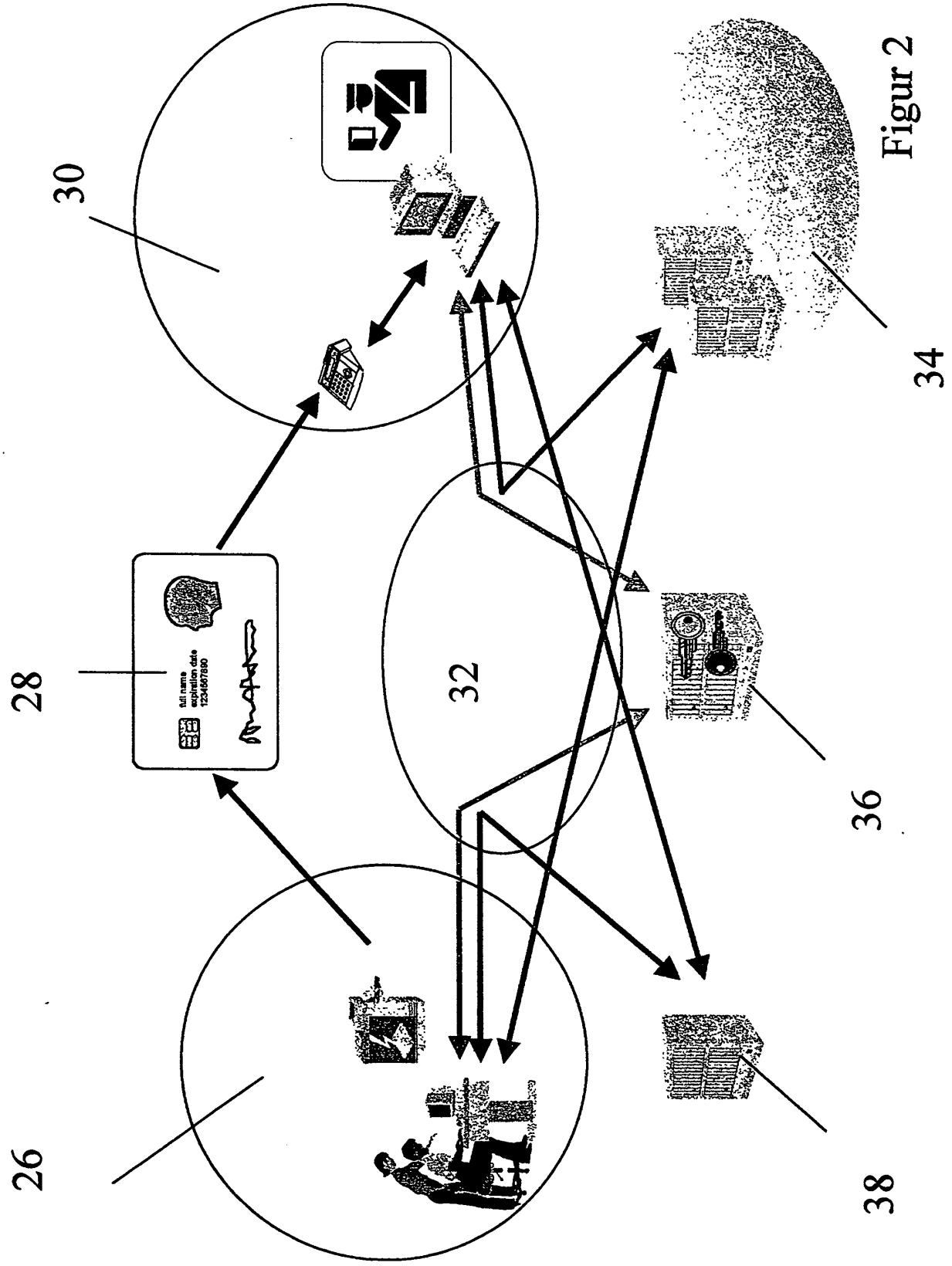
24. Procédé selon une des revendications 16 à 23, **caractérisé en ce que** le sas de transit est surveillé par une caméra vidéo.

25. Procédé selon une des revendications 16 à 24, **caractérisé en ce qu'**on calcule et qu'on vérifie une clé spécifique du moyen d'identification à partir des données encodées du moyen d'identification.

26. Procédé selon une des revendications 16 à 25, **caractérisé en ce que** les données personnelles encodées sont décodées et vérifiées.



Figur 1



Figur 2