



(11)

EP 1 669 941 B1

(12)

EUROPÄISCHE PATENTSCHRIFT

(45) Veröffentlichungstag und Bekanntmachung des
Hinweises auf die Patenterteilung:
13.06.2012 Patentblatt 2012/24

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

(21) Anmeldenummer: **05008968.9**

(22) Anmeldetag: **23.04.2005**

(54) Zugangskontrollsystem

Access control system

Système de contrôle d'accès

(84) Benannte Vertragsstaaten:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR**

(30) Priorität: **10.12.2004 DE 102004059608**

(43) Veröffentlichungstag der Anmeldung:
14.06.2006 Patentblatt 2006/24

(73) Patentinhaber: **SkiData AG
5083 Gartenau (AT)**

(72) Erfinder:
• **Wallerstorfer, Kurt
5204 Irrsdorf (AT)**

• **Ponert, Gregor
A-5020 Salzburg (AT)**

(74) Vertreter: **Karakatsanis, Georgios et al
Haft - Karakatsanis
Siegesstrasse 13
80802 München (DE)**

(56) Entgegenhaltungen:
**US-A- 5 095 196 US-A1- 2002 016 740
US-B1- 6 801 907**

EP 1 669 941 B1

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

Beschreibung

[0001] Die Erfindung bezieht sich auf ein System mit wenigstens einer Zugangskontrollvorrichtung mit einer Leseeinrichtung für Datenträger, auf denen eine Zugangsberechtigung und Identifikationsdaten abgelegt sind.

[0002] Systeme zur Zugangskontrolle werden beispielsweise bei Seilbahnen und Liften verwendet. Insbesondere zum Wintersport werden neben Einzelfahrten Tageskarten, Wochenkarten und Saisonkarten und dergleichen längerfristige Berechtigungen ausgegeben, oft für ganze Regionen mit einer Vielzahl von Seilbahnen und Liften. Für die längerfristigen Berechtigungen werden dabei gegenüber Einzelfahrten erhebliche Preisnachlässe gewährt, sie sind dafür jedoch nicht auf andere Personen übertragbar.

[0003] Die unberechtigte Übertragung längerfristiger Karten ist jedoch weit verbreitet. So kommt es häufig vor, dass ein Skifahrer, der frühmorgens eine Tageskarte gekauft hat, das Skifahren gegen Mittag einstellt und dann die Karte beispielsweise einem Bekannten gibt, gegebenenfalls auch einer fremden Person, z.B. am Parkplatz. Dadurch entsteht den Liftbetreibern ein erheblicher finanzieller Schaden. Um die Übertragung zu verhindern, wird daher beim Kauf der Karte ein Identitätsfoto des Käufers angefertigt, das auf der gekauften Karte angebracht wird, so dass das Kontrollpersonal das Foto auf der Karte mit der Person vergleichen kann, die den Zugang benutzt. Das Anfertigen und Aufbringen der Fotos auf den Karten ist jedoch zeitaufwändig und kostspielig, so dass damit nur Karten hoher Wertigkeiten, wie Wochen- oder Saisonkarten gesichert werden können.

[0004] Ferner ist es bekannt, ein digitalisiertes Bild des Kartenkäufers zusammen mit Identifikationsdaten für die betreffende Karte in einer Datenbank abzuspeichern und am Zugang ein Endgerät mit einem Bildschirm vorzusehen, auf das nach Eingabe der Identifikationsdaten der Karte durch das Kontrollpersonal das Bild des Karteninhabers von der Datenbank auf das Endgerät übertragen und mit dem Bildschirm dargestellt wird, also die Kontrollperson den Zugangsberechtigten mit dem Bild auf dem Bildschirm vergleichen kann. So eine Ausführung ist aus US 6,801,907 bekannt. Dieser Überprüfungsvorgang ist jedoch zeitaufwändig.

[0005] Aus US 2002/016740 A1 ist ein Shopping-System mit einer Kunden-ID-Karte bekannt. Dabei wird am Eingang mit einer Kamera ein Bild des Kunden aufgenommen und die ID-Karte des Kunden ausgelesen. Die ID-Daten werden mit den in einer Datenbank gespeicherten Kundenprofilen verknüpft und zusammen mit dem aufgenommenen Bild des Kunden an ein Endgerät übermittelt. Damit können in dem Geschäft insbesondere kaufkräftige Kunden von den Verkäufern gezielt angesprochen werden.

[0006] Aus US 5,095,196 A ist ein Zutrittssystem für eine Sicherheitszone bekannt, bei der die Bilder und Identifikationsdaten der zutrittsberechtigten Personen in

einer Datenbank abgespeichert sind. Am Eingang der Sicherheitszone ist eine Leseeinrichtung für einen Datenträger mit Identifikationsdaten und eine Kamera zur Aufnahme eines Bildes der jeweiligen Person vorgesehen. Die ausgelesenen Daten und das aufgenommene Bild werden mit den Identifikationsdaten und dem Bild in der Datenbank verglichen und bei Übereinstimmung der Zugang freigegeben.

[0007] Aufgabe der Erfindung ist es, einen Missbrauch von nicht übertragbaren Zugangsberechtigungsdaten-trägern zu verhindern.

[0008] Dies wird erfindungsgemäß mit dem in Anspruch 1 beschriebenen System erreicht. In den Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung wiedergegeben.

[0009] Das erfindungsgemäße System weist eine oder mehrere Zugangskontrollvorrichtungen auf. Dabei kann es sich um beliebige Personenvereinzelungseinrichtungen handeln, beispielsweise Drehsperren, Lichtschranken und dergleichen. An der Zugangskontrollvorrichtung befindet sich eine Leseeinrichtung, die bei gültiger Lesung einer Zugangsberechtigung den Zugang freigibt, d.h. z.B. bei einer von einem Motor angetriebenen Drehsperre den Motor ansteuert, so dass der Benutzer des Datenträgers die Drehsperre passieren kann. Die Leseeinrichtung kann eine kontaktbehaftete Leseeinrichtung, beispielsweise für Barcode-, Magnet- oder Chipkarten als Datenträger oder eine berührungslos wirkende Leseeinrichtung, insbesondere für RFID-Transponder als Datenträger sein. Auch kann die Zugangsberechtigung im Mobiltelefon des Zugangsberechtigten abgelegt sein. Die Zugangsberechtigung kann beispielsweise an einer Kassa beim Kauf des Datenträgers auf den Datenträger aufgezeichnet oder darauf abgespeichert werden.

[0010] Der Datenträger ist mit Identifikationsdaten versehen, die eine eindeutige Referenz oder Kennung für den jeweiligen Datenträger bilden. Dabei kann es sich um visuelle Daten, beispielsweise auf das Ticket aufgedruckte alphanumerische Daten handeln, z.B. den Namen des Käufers des Datenträgers. Auch können die Identifikationsdaten durch einen Barcode gebildet oder auf die Magnet- oder Chipkarte aufgezeichnet sein. Bei Karten mit einem Chip, d.h. kontaktbehafteten Chipkarten oder RFID-Transpondern, können die Identifikationsdaten auch z.B. die Seriennummer des Chips sein. Die Identifikationsdaten können auch mit den Zugangsberechtigungsdaten übereinstimmen, sofern es sich bei letzteren um eine eindeutige Kennung handelt.

[0011] Um die Zugangskontrollvorrichtung freizugeben, muss der Benutzer über eine Zugangsberechtigung verfügen. Dazu wird den Identifikationsdaten, die auf dem Datenträger abgelegt sind, eine Zugangsberechtigung zugeordnet. Die Zugangsberechtigung kann zusammen mit den Identifikationsdaten auf dem Datenträger abgelegt sein. Es ist jedoch auch möglich, dass die Zugangsberechtigung in der Datenbank abgelegt ist, wobei die Identifikationsdaten auf dem Datenträger eine Referenz zum Auslesen der Zugangsberechtigung aus der

Datenbank bilden.

[0012] Mit dem erfindungsgemäßen System kann der Zugang zu beliebigen Einrichtungen kontrolliert werden, beispielsweise zu Veranstaltungen, Stadien oder Schwimmbädern. Es ist jedoch insbesondere für Personenbeförderungsanlagen bestimmt, vor allem für Lifte, Seilbahnen und dergleichen Personenbeförderungseinrichtungen in einem Wintersportgebiet. Dabei sind meistens in einer Wintersportregion eine Vielzahl von derartigen Personenbeförderungseinrichtungen mit einem Datenträger mit einer Zugangsberechtigung benutzbar. Die Zugangsberechtigungsleser der Zugangskontrollvorrichtungen an den einzelnen Liften, Bergbahnen und dergleichen Personenbeförderungseinrichtungen sind dabei mit einer zentralen Datenbank vernetzt, in der bei jedem Zugang die Identifikationsdaten des jeweiligen Datenträgers und weitere Zugangsdaten, wie der Zeitpunkt des Zugangs und die Daten zur Identifizierung der jeweiligen Zugangskontrollvorrichtung gespeichert werden.

[0013] Nach der Erfindung befindet sich am Zugang, insbesondere an der Zugangsspur im Bereich der Dreh Sperre oder dergleichen Zugangskontrollvorrichtung, eine Kamera, mit der beim Zugang ein Bild, vorzugsweise ein Brustbild des Datenträger-Benutzers aufgenommen und in digitalisierter Form in der Datenbank abgespeichert wird.

[0014] Bei der Kamera kann es sich beispielsweise um eine einfache Webcam handeln, die z.B. in dem Gehäuse des Zugangsberechtigungslesers vorgesehen sein kann. Dazu braucht das Gehäuse nur eine kleine Öffnung für das Objektiv aufzuweisen, so dass die Kamera praktisch nicht wahrnehmbar ist. Die Kamera wird vorzugsweise durch den Zugangsberechtigungsleser ausgelöst, wenn dieser einen Datenträger liest.

[0015] Die Auslösung der Kamera und die Abspeicherung des Bildes kann bei jedem Zugang erfolgen. Um die Anzahl der aufzunehmenden und in der Datenbank abzuspeichernden Bilder zu reduzieren, ohne die Effektivität der Kontrolle nennenswert herabzusetzen, ist vorzugsweise eine Selektionsprogramm vorgesehen.

[0016] So können nur die Bilder der Benutzer von Datenträgern mit höherer Wertigkeit ausgewählt und abgespeichert werden, beispielsweise nur Wochen- oder Saisonkarten.

[0017] Da in der Datenbank die Zugangsdaten für den jeweiligen Datenträger abgespeichert werden, also insbesondere die Zugangszeitpunkte, kann ferner eine Verhaltensmuster-Analyse des Benutzers durchgeführt und danach eine Auswahl der aufzunehmenden und abzuspeichernden Bilder getroffen werden.

[0018] So besteht ein typischer Missbrauch eines Datenträgers mit nicht übertragbarer Zugangsberechtigung, z.B. einer Tageskarte, beim Wintersport darin, dass der Benutzer, der die Tageskarte frühmorgens gekauft hat, zunächst mit dem Lift, der Bergbahn oder dergleichen in höhere Regionen fährt, dort den Vormittag verbringt und gegen Mittag ins Tal abfährt, um die Karte

dort z.B. am Parkplatz an einen anderen zu übergeben. Wenn ein solches Verhalten anhand der Datenbank festgestellt worden ist, kann mit der Kamera an der Zugangskontrollvorrichtung im Tal ein Bild von dem Benutzer aufgenommen und in der Datenbank abgespeichert werden. Es kann dann mit einem zuvor z.B. bei Erstbenutzung des Datenträgers aufgenommenen Bild verglichen werden.

[0019] Bei dem erfindungsgemäßen System geht es also nicht darum, nicht den Zugang sondern den Missbrauch von nicht übertragbaren Zugangsberechtigungsdatenträgern zu verhindern, wozu, wie das vorstehende Beispiel zeigt, ein unberechtigter Zugang zwar zugelassen, jedoch später aufgedeckt wird.

[0020] Weiters können statistische Verfahren verwendet werden, um mit der Kamera Bilder der Datenträger-Benutzer aufzunehmen und in der Datenbank abzuspeichern. So kann beispielsweise das AQUIL (Acceptable Quality Level) - Stichprobensystem, ein internationales Qualitätssicherungssystem, zur Auswahl der Benutzerbilder herangezogen werden, welches bei einer Annahmen-Stichprobenprüfung die obere Grenze einer zufriedenstellenden mittleren Qualitätslage beschreibt.

[0021] Um die Datenmengen zu reduzieren, die in der Datenbank abgespeichert wird, kann ferner ein Computerprogramm verwendet werden, das den Kopf des Datenträger-Benutzers findet, ihn sozusagen ausschneidet und damit nur ein digitales Bild des Kopfes des Benutzers übertragen bzw. abgespeichert wird.

[0022] Die Kamera wird zur Aufnahme des Bildes des Benutzers beim Zugang durch das Lesen des Datenträgers mit der Leseeinrichtung oder beispielsweise durch das Vorrücken des Benutzers ausgelöst, das durch Sensoren erfasst wird.

[0023] Nach der Erfindung sind die in der Datenbank abgespeicherten Benutzer-Bilder mit einem Endgerät mit Bildschirm abrufbar, das von einer Kontrollperson bedient wird. Das Endgerät, das vorzugsweise als Handgerät ausgebildet ist, kommuniziert dazu mit der Datenbank gegebenenfalls über ein Modem. Vorzugsweise erfolgt die Kommunikation des Handgeräts mit der Datenbank jedoch über Funk, insbesondere mit GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunication System) oder einer anderen Mobilfunktechnik zur schnellen Datenübertragung. Die Kommunikation des Handgeräts mit der Datenbank kann statt über das öffentliche Telekommunikationsnetz auch durch Wireless LAN über ein internes Netzwerk der Einrichtung erfolgen, deren Zugänge erfindungsgemäß überwacht werden sollen.

[0024] Zur Überprüfung der rechtmäßigen Benutzung eines Datenträgers werden mit dem vorzugsweise tragbaren, insbesondere als Handgerät ausgebildeten Endgerät zunächst die Identifikationsdaten des zu überprüfenden Datenträgers erfasst. Wenn das Endgerät eine Tastatur aufweist und die Identifikationsdaten durch alphanumerische Daten gebildet werden, können die Identifikationsdaten mit der Tastatur eingegeben werden.

Wenn die Identifikationsdaten durch einen Barcode gebildet oder auf einer Magnet- oder Chipkarte aufgezeichnet oder im Chip eines RFID-Transponders oder in anderer Weise maschinenlesbar abgelegt sind, kann stattdessen das Endgerät auch eine Leseeinrichtung aufweisen, um die Identifikationsdaten zu erfassen.

[0025] Die so erfassten Identifikationsdaten werden an die Datenbank vorzugsweise per Funk übermittelt, worauf gegebenenfalls sämtliche in der Datenbank abgelegten Bilder, die dem Datenträger mit diesen Identifikationsdaten zugeordnet sind, vorzugsweise per Funk an das Endgerät übertragen werden.

[0026] Die Kontrollperson kann damit die Bilder auf dem Bildschirm des Endgeräts, die in der Datenbank von dem Benutzer des Datenträgers abgespeichert worden sind, visuell mit der Person vergleichen, die den Datenträger gerade besitzt. Die Kontrollperson blättert mit dem Endgerät diese Bilder sozusagen durch und kann damit durch Sichtvergleich feststellen, ob die Bilder auf dem Bildschirm stets die Person zeigen, die sie gerade prüft. Die in der Datenbank abgespeicherten Bilder können dabei von einer Kamera bei der Benutzung der Zugangskontrollvorrichtung und/oder an einer anderen Stelle, z.B. an einer Kassa beim Kauf des Datenträgers, aufgenommen worden sein. D.h., das abgespeicherte Bild kann auch schon vor längerer Zeit aufgenommen worden sein, was insbesondere bei Saisonkarten und dergleichen Datenträgers mit längerfristigen Zugangsberechtigungen von Interesse sein kann.

[0027] Bei fehlender Übereinstimmung eines Bildes auf dem Bildschirm mit der gerade geprüften Person können entsprechende Maßnahmen ergriffen, beispielsweise der Datenträger eingezogen werden.

[0028] Da vorzugsweise zusammen mit den Bildern und den Identifikationsdaten des jeweiligen Datenträgers auch weitere Zugangsdaten, wie Zugangszeitpunkt und Daten der jeweiligen Zugangskontrollvorrichtung in der Datenbank abgespeichert werden, kann die Kontrollperson beispielsweise bei fehlender Übereinstimmung eines Bildes auf dem Bildschirm mit der gerade geprüften Person zudem feststellen, zu welchen Zeitpunkt und an welcher Zugangskontrollvorrichtung der Datenträger von einer anderen Person verwendet worden ist.

[0029] Erfindungsgemäß kann auch lediglich bei der Erstbenutzung des Datenträgers an der Zugangskontrollvorrichtung mit der dort angeordneten Kamera ein Bild aufgenommen und in der Datenbank zusammen mit den Identifikationsdaten abgespeichert und dieses Bild zum Sichtvergleich auf das Endgerät mit dem Bildschirm übertragen werden. Dabei kann der Datenträger auch über das Internet gekauft und mit den Identifikationsdaten versehen werden.

[0030] Nachstehend ist die Erfindung anhand der beigefügten Zeichnung beispielhaft näher erläutert, deren einzige Figur schematisch eine Ausführungsform des erfindungsgemäßen Systems zeigt.

[0031] Danach weist eine als Drehsperre ausgebildete Zugangskontrollvorrichtung 1 mit einer Drehsperre mit

zwei um eine Achse 2 drehbaren Sperrarmen 3 eine Leseeinrichtung in einem Gehäuse 4 auf. In das Kartenmaul 5 der als Einsteckleser ausgebildeten Leseeinrichtung wird ein als Karte ausgebildeter Datenträger 8 mit einer nicht übertragbaren Zugangsberechtigung gesteckt, beispielsweise mit einem Barcode. Bei gültiger Lesung der Zugangsberechtigung auf dem Datenträger 8 mit dem Einsteckleser wird die Drehsperre gedreht, so dass der Zugang 6 freigegeben wird.

[0032] Wenn der Datenträger 8 in das Kartenmaul 5 gesteckt wird, wird mit einer Kamera in dem Gehäuse 4, von der nur das Objektiv 7 zu sehen ist, ein Bild von dem Datenträger-Benutzer aufgenommen. Der Datenträger ist mit Identifikationsdaten, z.B. "752" versehen, die von der Leseeinrichtung gelesen werden. Diese Identifikationsdaten werden zusammen mit dem digitalisierten Bild, das mit der Kamera 7 von dem Kartenbenutzer aufgenommen worden ist, in einer Datenbank 9 abgespeichert.

[0033] Die in der Datenbank 9 abgespeicherten Bilder sind mit einem Handgerät 11 mit einem Bildschirm 12 und einer Tastatur 13 über Funk 14 von einer Kontrollperson, von der nur die Hand 15 dargestellt ist, abrufbar.

[0034] Zur Überprüfung der rechtmäßigen Benutzung eines Datenträgers erhält die Kontrollperson 15 von der Person 16, die sie gerade überprüft, die Identifikationsdaten, also z.B. "752" des Datenträgers 8, die sie mit der Tastatur 13 in das Handgerät 11 eingibt. Die Identifikationsdaten werden dann per Funk 14 der Datenbank 9 übermittelt, die daraufhin alle abgespeicherten, diesen Identifikationsdaten zugeordneten Bilder an das Handgerät 11 überträgt, die mit dem Bildschirm 12 betrachtet werden können.

[0035] Die Kontrollperson 15 blättert diese Bilder durch und kann damit durch Sichtvergleich feststellen, ob die Bilder stets die Person 16 zeigen, die sie gerade kontrolliert.

Patentansprüche

1. System mit wenigstens einer Zugangskontrollvorrichtung (1) mit einer Leseeinrichtung (4) für Datenträger (8), auf denen Identifikationsdaten abgelegt sind, denen eine Zugangsberechtigung zugeordnet ist, über die der Benutzer verfügen muss, damit die Zugangskontrollvorrichtung freigegeben wird, wobei eine Kamera (7) an der Zugangskontrollvorrichtung (1), die digitalisierte Bilder von den Benutzern der Zugangskontrollvorrichtung (1) aufnimmt, welche zusammen mit den Identifikationsdaten in einer Datenbank (9) abgespeichert werden sowie wenigstens ein von einer Kontrollperson (15) bedienbares, mit der Datenbank (9) kommunizierendes Endgerät (11) mit Bildschirm (12) vorgesehen sind, wobei das Endgerät (11) zum Erfassen der identifikationsdaten des zu prüfenden Datenträgers (8) eine Tastatur (13) aufweist, sofern die Identifikationsdaten des Datenträgers (8) durch alphanumerische Daten gebildet

- werden, oder, wenn die Identifikationsdaten des Datenträgers (8) durch einen Barcode gebildet oder auf einer Magnet- oder Chipkarte aufgezeichnet oder im Chip eines RFID-Transponders oder in anderer Weise maschinenlesbar abgelegt sind, eine Leseeinrichtung aufweist, wobei die in der Datenbank (9) abgespeicherten Bilder, die dem Datenträger (8) mit diesen Identifikationsdaten zugeordnet sind, an das Endgerät (11) übertragen werden, so dass die Kontrollperson (15) die Bilder auf dem Bildschirm (12) des Endgeräts (11), die in der Datenbank (9) von dem Benutzer des Datenträgers (8) abgespeichert worden sind, visuell mit der Person (16) vergleichen kann, die den Datenträger (8) gerade besitzt, um durch Sichtvergleich, festzustellen, ob die Bilder auf dem Bildschirm (12) stets die gleiche Person zeigen, die sie gerade prüft.
2. System nach Anspruch 1, **dadurch gekennzeichnet, dass** das bei der Erstbenutzung des Datenträgers (8) an der Zugangskontrollvorrichtung (1) mit der Kamera (7) aufgenommene und abgespeicherte Bild des kontrollierten Benutzers (16) des Datenträgers (8) zum Sichtvergleich übertragbar ist.
3. System nach Anspruch 1, **dadurch gekennzeichnet, dass** die bei den einzelnen Zugängen zu der Zugangskontrollvorrichtung (1) mit der Kamera (7) aufgenommenen und abgespeicherten Bilder des kontrollierten Benutzers (16) des Datenträgers (8) zum Sichtvergleich übertragbar sind.
4. System nach Anspruch 1, **dadurch gekennzeichnet, dass** die Kommunikation des Endgerätes mit der Datenbank über Funk (14) erfolgt.
5. System nach Anspruch 4, **dadurch gekennzeichnet, dass** die Kommunikation des Endgerätes mit der Datenbank (9) mit GPRS, UMTS oder einer anderen Mobilfunktechnik zur schnellen Datenübertragung erfolgt.
6. System nach Anspruch 4, **dadurch gekennzeichnet, dass** die Kommunikation des Endgerätes mit der Datenbank (9) durch Wireless LAN über ein internes Netzwerk erfolgt.
7. System nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** das Endgerät als Handgerät (11) ausgebildet ist.
8. System nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** ein Selektionsprogramm bestimmte Datenträger (8) auswählt, um mit der Kamera (7) ein Bild vom Benutzer des Zugangs (6) aufzunehmen und in der Datenbank (9) abzuspeichern.

9. System nach Anspruch 8, **dadurch gekennzeichnet, dass** das Selektionsprogramm die Datenträger (8) nach ihrer Wertigkeit, aufgrund einer Verhaltensmuster-Analyse der Datenträger-Benutzer und/oder statistisch auswählt.
10. System nach Anspruch 1, **dadurch gekennzeichnet, dass** die Kamera (7) zur Aufnahme des Bildes des Benutzers durch das Lesen des Datenträgers (8) mit der Leseeinrichtung (4) und/oder durch das Vorrücken des Benutzers ausgelöst wird, das mit Sensoren erfasst wird.
11. System nach Anspruch 1, **dadurch gekennzeichnet, dass** in der Datenbank (9) ein Bild des Benutzers des Datenträgers (8) zusammen mit den Identifikationsdaten des Datenträgers (8) abgelegt ist und mit dem Endgerät erfassbar ist, das mit einer Kamera vor dem Zugang des Benutzers zu der Zugangskontrollvorrichtung (1) aufgenommen worden ist.

Claims

1. A system with at least one access checking device (1) with a reader (4) for data carriers (8) on which identification data are stored, to which an access right is assigned, which the user must have in order that the access checking device is enabled, wherein a camera (7) on the access checking device (1), which records digitised images of the users of the access checking device (1) which are stored together with the identification data in a database (9), and also at least one terminal (11) with a monitor (12), which terminal can be operated by a checking person (15) and communicates with the database (9), are provided, wherein the terminal (11) has a keypad (13) for capturing the identification data of the data carrier (8) to be tested if the identification data of the data carrier (8) are formed by alphanumeric data, or, if the identification data of the data carrier (8) are formed by a barcode or are recorded on a magnet or a chip card or are stored in the chip of an RFID transponder or in a machine readable manner in some other way, has a reader, wherein the images stored in the database (9), which are assigned to the database (8) with the same identification data, are transmitted to the terminal (11) so that the checking person (15) can visually compare the images on the monitor (12) of the terminal (11), which have been stored in the database (9) by the user of the data carrier (8), with the person (16) who currently possesses the data carrier (8), in order to determine by visual comparison whether the images on the monitor (12) always show the same person, whom they are currently checking.

2. The system according to Claim 1, **characterised in that** the image of the checked user (16) of the data carrier (8), which is recorded at the access checking device (1) with the camera (7) and stored during the first use of the data carrier (8), can be transmitted for visual comparison. 5
3. The system according to Claim 1, **characterised in that** the images of the checked user (16) of the data carrier (8) recorded during the individual instances of access to the access checking device (1) using the camera (7) and stored can be transmitted for visual comparison. 10
4. The system according to Claim 1, **characterised in that** the communication of the terminal with the database takes place wirelessly (14). 15
5. The system according to Claim 4, **characterised in that** the communication of the terminal with the database (9) takes place using GPRS, UMTS or another mobile communications technology for fast data transmission. 20
6. The system according to Claim 4, **characterised in that** the communication of the terminal with the database (9) takes place by means of wireless LAN via an internal network. 25
7. The system according to one of the preceding claims, **characterised in that** the terminal is constructed as a handheld device (11). 30
8. The system according to one of the preceding claims, **characterised in that** a selection program selects certain data carriers (8) in order to record an image of the user of the access (6) with the camera (7) and to store the same in the database (9). 35
9. The system according to Claim 8, **characterised in that** the selection program selects the data carriers (8) in accordance with their value on the basis of a behaviour-pattern analysis of the data carrier users and/or statistically. 40
10. The system according to Claim 1, **characterised in that** the camera (7) for recording the image of the user is triggered by means of the reading of the data carrier (8) with the reader (4) and/or by means of the advancing of the user, which is detected using sensors. 45
11. The system according to Claim 1, **characterised in that** an image of the user of the data carrier (8) is stored in the database (9) together with the identification data of the data carrier (8) and can be captured using the terminal, which image has been recorded using a camera before the access of the user to the 50

access checking device (1).

Revendications

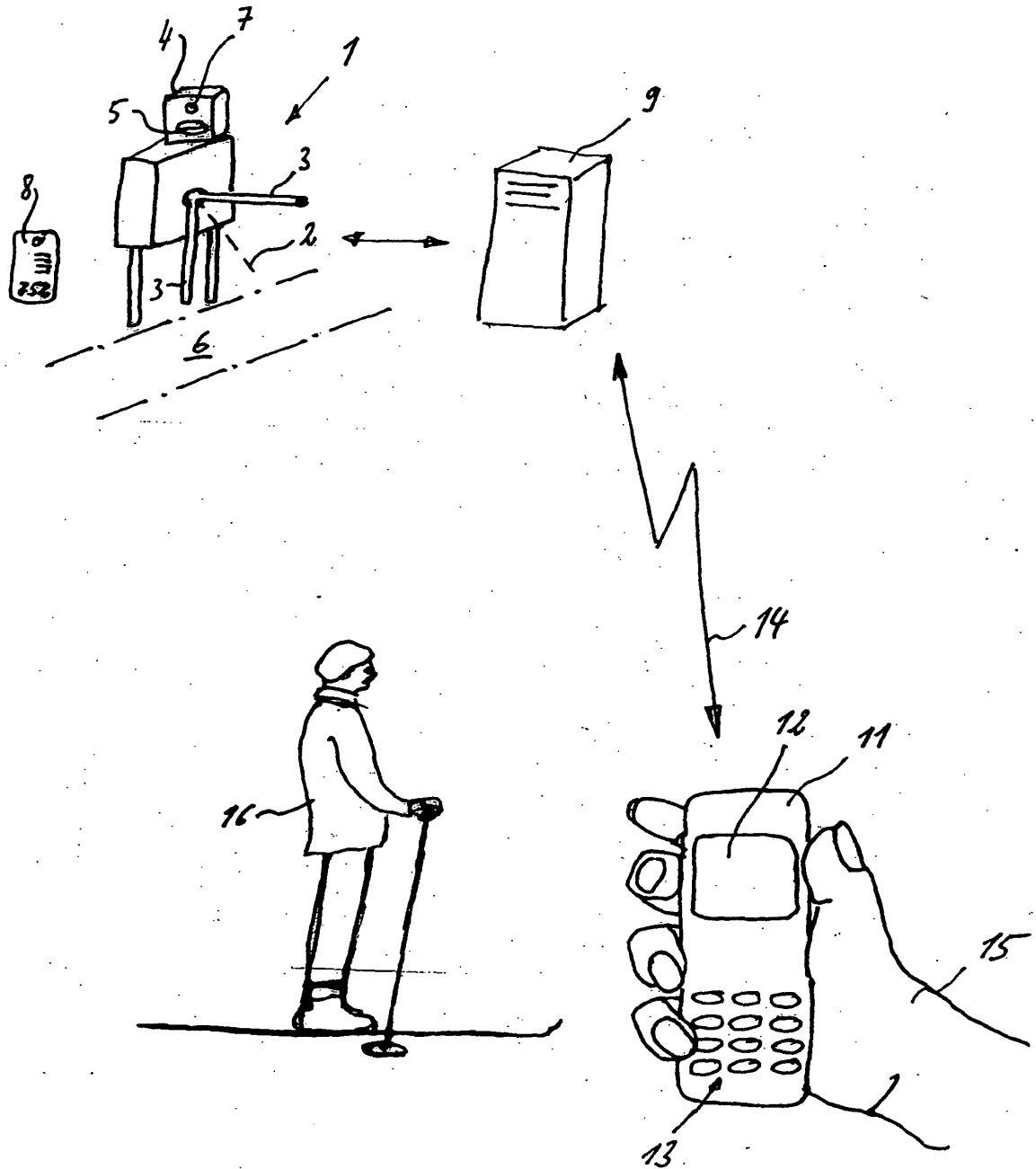
1. Système comportant au moins un dispositif de contrôle d'accès (1) avec un dispositif de lecture (4) de supports de données (8), sur lesquels des données d'identification sont stockées, auxquelles une autorisation d'accès est coordonnée, dans lequel une caméra (7) sur le dispositif de contrôle d'accès (1), qui prend des images numérisées des utilisateurs du dispositif de contrôle d'accès (1), qui sont mémorisées conjointement aux données d'identification dans une banque de données (9) et au moins un terminal (11) pouvant être manipulé par un personnel de contrôle (15), communiquant avec la banque de données (9) sont pourvus d'un écran (12), dans lequel le terminal (11) présente, pour détecter les données d'identification du support de données (8) à contrôler, un clavier (13), dans la mesure où les données d'identification du support de données (8) sont formées par des données alphanumériques ou, quand les données d'identification du support de données (8) sont formées par un code-barres ou sont enregistrées sur un aimant ou une carte à puce ou sont stockées dans la puce d'un transpondeur RFID ou peuvent être lues par une machine d'une autre manière, présente un dispositif de lecture, dans lequel les images mémorisées dans la banque de données (9), qui sont coordonnées au support de données (8) avec ces données d'identification, sont transmises au terminal (11), de sorte que le personnel de contrôle (15) puisse comparer visuellement les images sur l'écran (12) du terminal (11), qui ont été mémorisées dans la banque de données (9) par l'utilisateur de support de données (8) avec la personne (16), que le support de données (8) possède déjà, et s'assurer par comparaison visuelle, que les images sur l'écran (12) affichent constamment la même personne, qui est en train d'être contrôlée. 55
2. Système selon la revendication 1, **caractérisé en ce que** lors de la première utilisation du support de données (8) sur le dispositif de contrôle d'accès (1) l'image prise et mémorisée avec la caméra (7) de l'utilisateur contrôlé (16) du support de données (8) peut être transmise à des fins de comparaison visuelle.
3. Système selon la revendication 1, **caractérisé en ce que** les images de l'utilisateur contrôlé (16) du support de données (8) prises et mémorisées avec la caméra (7) lors des accès individuels au dispositif de contrôle d'accès (1) peuvent être transmises à des fins de comparaison visuelle.
4. Système selon la revendication 1, **caractérisé en**

ce que la communication du terminal a lieu par radio (14) avec la banque de données.

5. Système selon la revendication 4, **caractérisé en ce que** la communication du terminal avec la banque de données (9) a lieu avec GPRS, UMTS ou une autre technique radio mobile à des fins de transmission de données rapide. 5
6. Système selon la revendication 4, **caractérisé en ce que** la communication du terminal avec la banque de données (9) a lieu par LAN sans fil ou par un réseau interne. 10
7. Système selon une des revendications précédentes, **caractérisé en ce que** le terminal est réalisé comme un appareil portatif (11). 15
8. Système selon une des revendications précédentes, **caractérisé en ce que** un programme de sélection sélectionne des supports de données (8) déterminés, afin de prendre avec la caméra (7) une image de l'utilisateur de l'accès (6) et la mémoriser dans la banque de données (9). 20
9. Système selon la revendication 8, **caractérisé en ce que** le programme de sélection sélectionne les supports de données (8) selon leur valeur, sur la base d'une analyse de modèle de comportement de l'utilisateur du support de données et/ou statistiquement. 25 30
10. Système selon la revendication 1, **caractérisé en ce que** la caméra (7) pour prendre l'image de l'utilisateur est déclenchée par la lecture du support de données (8) avec le dispositif de lecture (4) et/ou par l'avancée de l'utilisateur, qui est détectée avec des capteurs. 35
11. Système selon la revendication 1, **caractérisé en ce que** dans la banque de données (9) une image de l'utilisateur du support de données (8) est stockée conjointement aux données d'identification du support de données (8) et peut être détectée avec le terminal, laquelle a été prise avec une caméra avant l'accès de l'utilisateur au dispositif de contrôle d'accès (1). 40 45

50

55



IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- US 6801907 B [0004]
- US 2002016740 A1 [0005]
- US 5095196 A [0006]