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

(11) EP 1 669 941 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
14.06.2006 Patentblatt 2006/24

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

(21) Anmeldenummer: **05008968.9**

(22) Anmeldetag: **23.04.2005**

(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
Benannte Erstreckungsstaaten:
AL BA HR LV MK YU

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

(71) Anmelder: **SkiData AG**
5083 Gartenau (AT)

(72) Erfinder:
- **Wallerstorfer, Kurt**
  A-5020 Salzburg (AT)
- **Ponert, Gregor**
  A-5020 Salzburg (AT)

(74) Vertreter: **Haft, von Puttkamer, Berngruber, Czybulka**
Patentanwälte
Franziskanerstrasse 38
81669 München (DE)

(54) Zugangskontrollsystem

(57) An einer Zugangskontrollvorrichtung (1) mit einer Leseeinrichtung (4) für Datenträger (8), auf denen eine Zugangsberechtigung und Identifikationsdaten abgelegt sind, ist eine Kamera (7) vorgesehen, die digitalisierte Bilder von den Benutzern der Zugangskontrollvorrichtung (1) aufnimmt, welche zusammen mit den von der Leseeinrichtung (4) beim Lesen des Datenträgers (8) gelesenen Identifikationsdaten in einer Datenbank (9) abgespeichert werden. Eine Kontrollperson (15) bedient ein mit der Datenbank (9) kommunizierendes Endgerät mit Bildschirm (12), mit dem die Identifikationsdaten des Datenträgers (8) erfassbar sind und an das das abgespeicherte Bild des Benutzers des Datenträgers (8) mit den jeweiligen Identifikationsdaten, das bei dem Zugang zu der Zugangskontrollvorrichtung (1) von dem Benutzer mit der Kamera (7) aufgenommen worden ist, zum Sichtvergleich mit dem kontrollierten Benutzer (16) übertragbar ist.

EP 1 669 941 A2

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, nach dem Oberbegriff des Anspruchs 1.

[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 Zugangsbenutzer mit dem Bild auf dem Bildschirm vergleichen kann. Dieser Überprüfungsvorgang ist jedoch zeitaufwändig.

[0005] Aufgabe der Erfindung ist es, einen Missbrauch von nicht übertragbaren Zugangsberechtigungsdatenträgern zu verhindern.

[0006] Dies wird erfindungsgemäß mit dem in Anspruch 1 gekennzeichneten System erreicht. In den Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung wiedergegeben.

[0007] 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 Zugangbenutzers abgelegt sein. Die Zugangsberechtigung kann beispielsweise an einer Kassa beim Kauf des Datenträgers auf den Datenträger aufgezeichnet oder darauf abgespeichert werden.

[0008] Der Datenträger ist mit Identifikationsdaten versehen, die ein 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.

[0009] 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.

[0010] 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.

[0011] 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.

[0012] 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.

[0013] 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.

[0014] So können nur die Bilder der Benutzer von Datenträgern mit höherer Wertigkeit ausgewählt und abgespeichert werden, beispielsweise nur Wochen- oder Saisonkarten.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] Weiters können statistische Verfahren verwendet werden, um mit der Kamera Bilder der Datenträger-Benutzer aufzunehmen und in der Datenbank abzuspeichern. So kann beispielsweise das AQUL (Acceptable Qualitity Level) - Stichprobensystem, ein internationales Qualitätssicherungssystem, zur Auswahl der Benutzerbilder herangezogen werden, welches bei einer Annahmen-Stichprobenprüfung die obere Grenze einer zufriedenstellenden mittleren Qualitätslage beschreibt.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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.

[0023] 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.

[0024] 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 Zugangs-

kontrollvorrichtung 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.

[0025] Bei fehlender Übereinstimmung eines Bildes auf dem Bildschirm mit der gerade geprüften Person können entsprechende Maßnahmen ergriffen, beispielsweise der Datenträger eingezogen werden.

[0026] 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.

[0027] 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.

[0028] Nachstehend ist die Erfindung anhand der beigefügten Zeichnung beispielhaft näher erläutert, deren einzige Figur schematisch eine Ausführungsform des erfindungsgemäßen Systems zeigt.

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] 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, und mit einer Datenbank (9), in der ein Bild des Benutzers des Datenträgers (8) zusammen mit den Identifikationsdaten des Datenträgers (8) abgelegt ist, **gekennzeichnet durch** wenigstens eine Kamera (7) an der Zugangskontrollvorrichtung (1), die digitalisierte Bilder von den Benutzern der Zugangskontrollvorrichtung (1) aufnimmt, welche zusammen mit den Identifikationsdaten in der Datenbank (9) abgespeichert werden, sowie wenigstens ein von einer Kontrollperson (15) bedienbares, mit der Datenbank (9) kommunizierendes Endgerät mit Bildschirm (12), mit dem die Identifikationsdaten des Datenträgers (8) erfassbar sind und an das das abgespeicherte Bild des Benutzers des Datenträgers (8) mit den jeweiligen Identifikationsdaten, das bei dem Zugang zu der Zugangskontrollvorrichtung (1) mit der Kamera (7) aufgenommen worden ist, zum Sichtvergleich mit dem kontrollierten Benutzer (16) des Datenträgers (8) übertragbar ist.

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 zum Erfassen der Identifikationsdaten eine Tastatur (13) und/oder eine Leseeinrichtung aufweist.

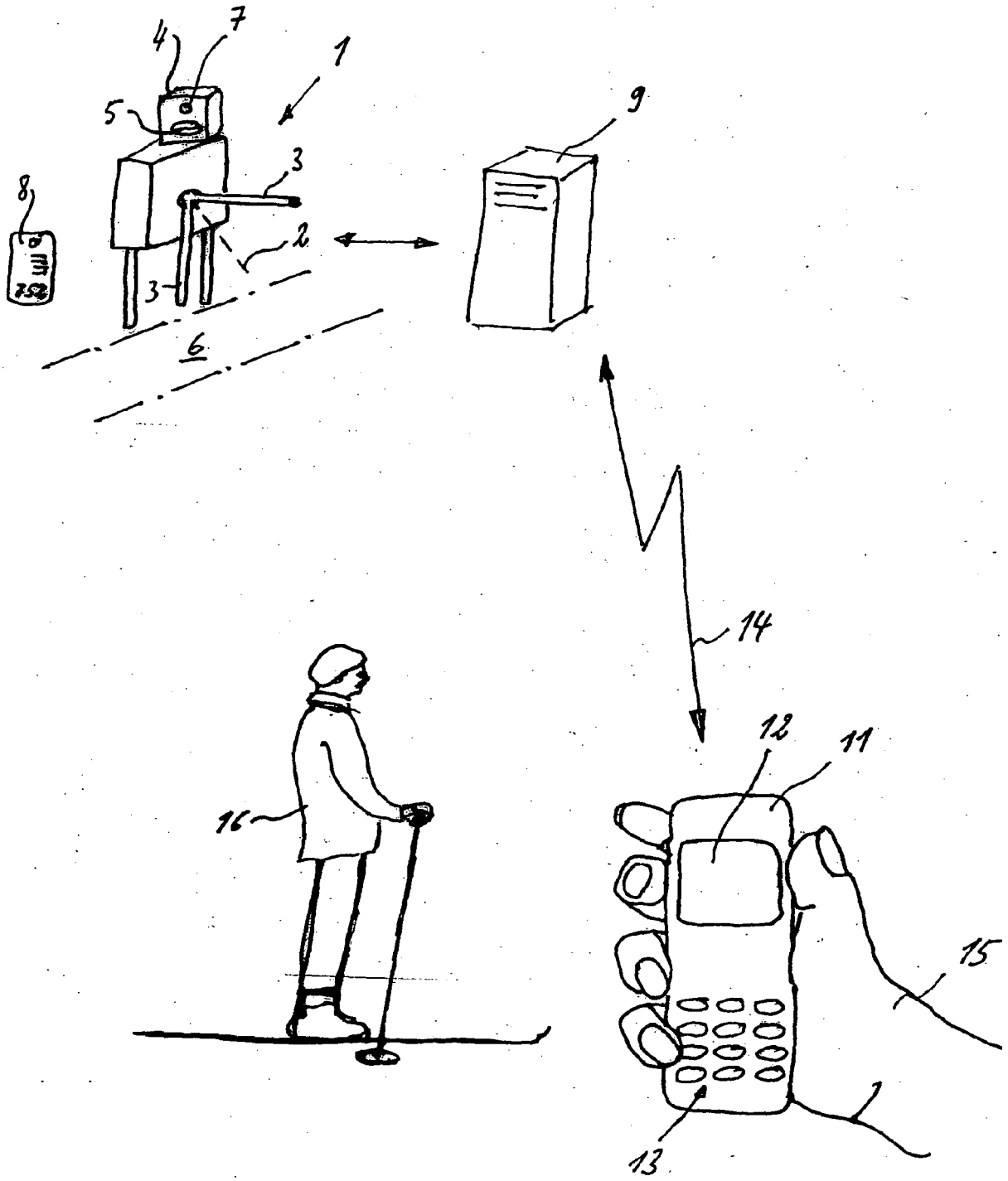
8. System nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet, dass** das Endgerät als Handgerät (11) ausgebildet ist.

9. 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.

10. System nach Anspruch 9, **dadurch gekennzeichnet, dass** das Selektionsprogramm die Datenträger (8) nach ihrer Wertigkeit, aufgrund einer Verhaltensmuster-Analyse der Datenträger-Benutzer und/oder statistisch auswählt.

11. 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.

12. 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.


4
7
1
5
9
3
8
2
3
6
14
12
11
16
15
13