



(86) Date de dépôt PCT/PCT Filing Date: 2000/11/30
(87) Date publication PCT/PCT Publication Date: 2001/07/26
(85) Entrée phase nationale/National Entry: 2002/07/18
(86) N° demande PCT/PCT Application No.: EP 2000/012049
(87) N° publication PCT/PCT Publication No.: 2001/054074
(30) Priorité/Priority: 2000/01/19 (100 01 929.3) DE

(51) Cl.Int.⁷/Int.Cl.⁷ G07C 9/00, G07C 9/02

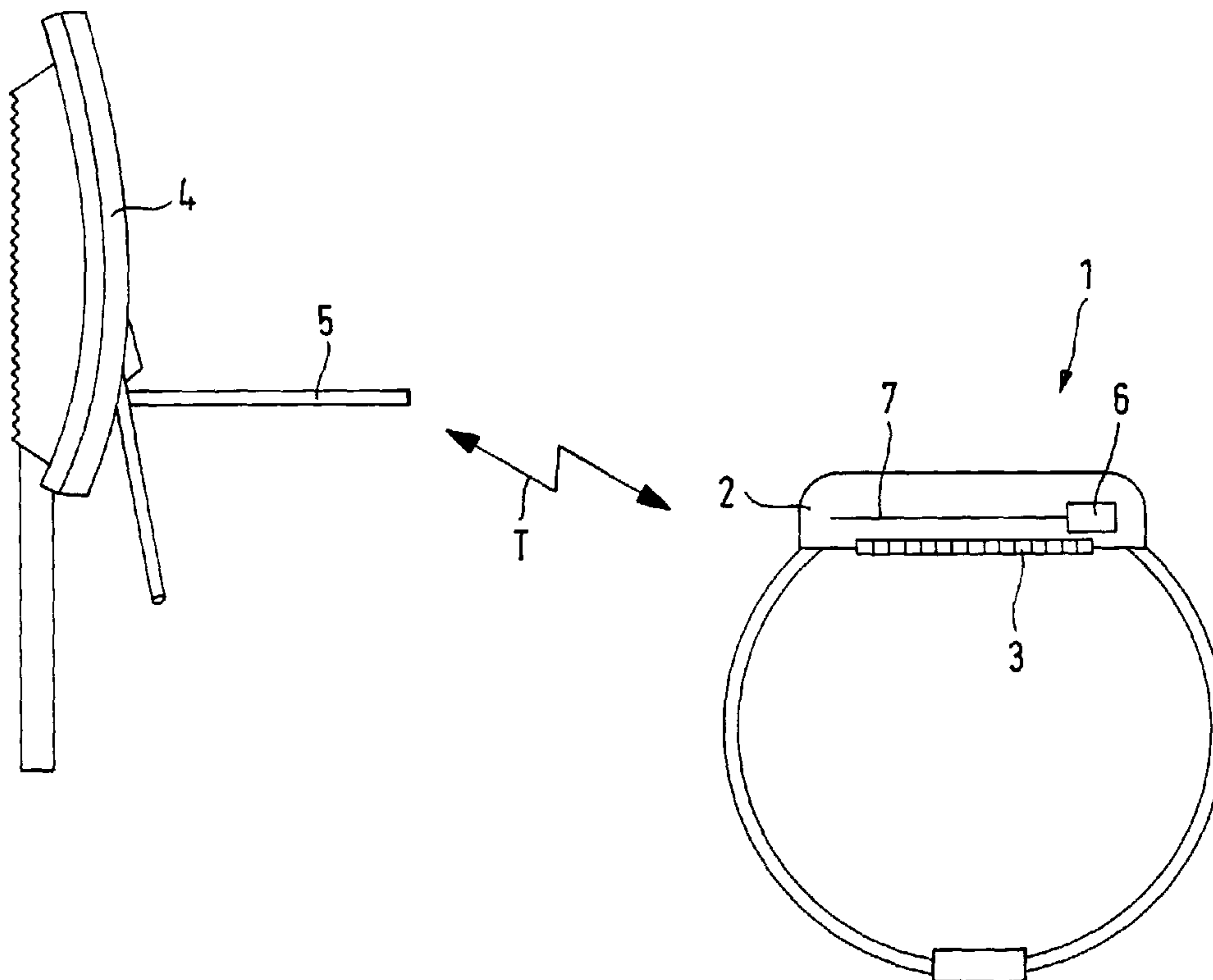
(71) Demandeur/Applicant:
SKIDATA AG, AT

(72) Inventeur/Inventor:
STOCKHAMMER, RUDOLF, AT

(74) Agent: SMART & BIGGAR

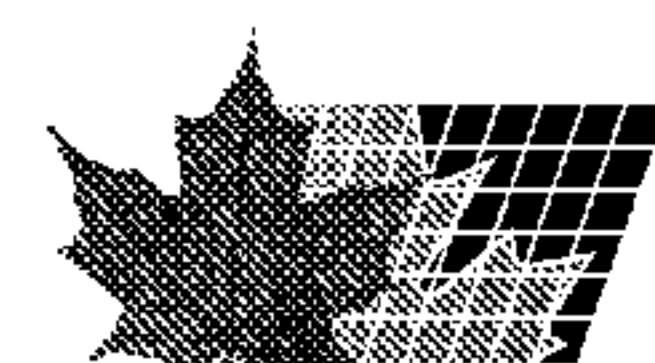
(54) Titre : DISPOSITIF DE CONTROLE D'AUTORISATION

(54) Title: AUTHORIZATION CONTROL DEVICE



(57) **Abrégé/Abstract:**

In order to control the authorization of a person using a service involving a data carrier (1) which communicates in a contactless manner with a read out device (4), said data carrier takes the form of an object which is worn on the skin, a wrist watch for example. Said object which is worn on the skin, e.g. a wrist watch, is provided with a sensor (3) which is used for the detection of biometric skin identification features and is arranged on the lower side thereof. The skin identification features of the authorized person are stored in a memory unit. If the stored biometric identification features tally with the features thus detected, the read out device (4) emits a release signal.



Abstract

In order to control the authorization of a person using a service involving a data carrier (1) which communicates in a contactless manner with a read out device (4), said data carrier takes the form of an object which is worn on the skin, a wrist watch for example. Said object which is worn on the skin, e.g. a wrist watch, is provided with a sensor (3) which is used for the detection of biometric skin identification features and is arranged on the lower side thereof. The skin identification features of the authorized person are stored in a memory unit. If the stored biometric identification features tally with the features thus detected, the read out device (4) emits a release signal.

WO 01/54074

PCT/EP00/12049

Authorization control device

This invention relates to a device for controlling a person's authorization upon utilization of a service with a data carrier that communicates with a reader, according to the preamble of claim 1.

In order to prevent abusive use, data carriers, in particular smart cards, are nowadays combined with a PIN number. Since the user must remember different numbers for different smart cards, there is a danger of him confusing or forgetting them. This increases the error rate in smart card use, which e.g. results in even longer waiting lines than are already caused by PIN entry at peak times.

DE 19648767 A1 discloses a device according to the preamble of claim 1 wherein the data carrier is formed by a smart card in which the authorized person's fingerprint is stored and which is provided with a sensor that detects the user's fingerprint. If the comparison yields a match when the smart card is inserted into the reader, the actual smart-card function, for example access, is released.

It is also known for example from WO 88/04153 and EP 0691822 B1 to identify persons by the patterns of their subcutaneous blood vessels. The relevant person's hand is positioned by the grasping of a handle or the like and the infrared emission spectrum of the back of the hand then measured.

Compared to smart cards and similar data carriers that must be inserted into a reader, contactless-type data carriers, which cooperate with the reader in the radio wave range over a relatively large data transfer distance, have the advantage of being able to be fastened to clothing in the form of a card or integrated into a wristwatch for example, i.e. used "handfree."

Accordingly, contactless-type data carriers are preferably used for example with access control devices of ski lifts and cable cars, which generally have a person singling device, such as a turnstile, which is operated by the reader, i.e. unblocked for a person, when the reader receives corresponding data from the data carrier. Since a PIN code and a fingerprint sensor are out of the question for skiers, if only because of the gloves skiers wear, the nontransferable data carrier is nowadays usually combined with a photo fastened to the skier's clothing in order to prevent transfer to other persons. However, such a photo involves considerable effort.

The problem of the invention is therefore to provide a contactless-type data carrier with nontransferable, personal authorization to utilize a service, for example for the passenger conveyors of a skiing area, which prevents abusive transfer to other persons.

This is obtained according to the invention by forming the contactless-type data carrier by an object worn on the skin and provided with a sensor detecting biometric identification feature of the skin.

The object worn on the skin may be a garment, for example a glove or headband. However, especially preferred objects are ones worn independently of the ambient temperature, for example a bracelet, wristwatch or ring.

The biometric skin identification features detected by the sensor may be of different kinds. For example the skin furrow relief can be detected, its measurement being described e.g. in DE 2719341 C3 or DE 3433194 A1.

However, an infrared sensor is preferably used, being disposed under the object so as to rest on the skin and reliably detect the subcutaneous pattern of arteries, veins, capillaries and other blood vessels thereunder.

Since the hand has a special individual, intensive subcutaneous blood vessel pattern, the inventive object is preferably worn with the sensor in this area. Accordingly, the data carrier used according to the invention is a bracelet, wristwatch, ring or glove, in order to communicate contactlessly with the reader, on the one hand, and for the sensor at the same time to detect the biometric skin identification features in the area of the hand, i.e. the biometric skin identification features on the back of the hand (glove), a finger (ring) or the wrist (bracelet or watch). Compared to other objects worn on the skin, for example a headband, the abovementioned objects worn on the hand have the additional advantage of resulting in a corresponding positioning of the sensor in the hand area whose biometric skin identification data have been stored, since they are more or less always worn at the same place.

The data of the biometric features to be identified can be read and stored in a chip in the wristwatch or other data carrier worn on the skin, which at the same time forms the means for comparing the stored biometric identification feature with those detected. If the comparison yields a match of the biometric data read and stored in the chip with the skin identification features measured by the sensor, a data transaction with the reader is effected with the transponder for noncontacting data transfer in the object worn on the skin, thereby releasing the access control device.

Further, it is possible to store the biometric data to be identified of the access-authorized persons of the relevant access control device in the reader or in a central processing unit with which the reader is connected on- or off-line. Finally, the biometric data to be identified can be stored both in a chip in the particular data carrier worn on the skin and in the reader or central processing unit if especially high security requirements are to be met.

In order to prevent unauthorized readout and changing of the data, the biometric data can be stored in a cryptologically protected memory area that is not freely accessible.

The reader is formed to radiate electromagnetic waves, in particular in the radio wave range. It has for this purpose coils and capacitors, resonant circuits, optocouplers and the like. The data carrier, which is preferably formed as a transponder, likewise has devices such as coils, capacitors, resonant circuits, optocouplers for nongalvanic energy and/or data transfer, so that energy and/or data are transferred between the data carrier and the reader.

The sensor is preferably set in operation by the transponder only when the data carrier is located at the transaction distance from the reader.

The inventive device is employable for example in tourist areas to register authorizations for access to ski lifts, cable cars and other tourist facilities, such as indoor swimming pools, parking garages and values for cashless payment transactions in restaurants, sport stores, etc.

However, the inventive device is of course not limited to tourism. Rather, such a contactless-type data carrier can be used for a great variety of applications, for example the utilization of public transport systems, as an electronic purse and the like, i.e. in particular as a multifunctional data carrier that is employable for as many applications as possible, even as the only personal data carrier with which a person can utilize practically all services that can be controlled with a reader.

In the following, the invention will be explained in more detail by way of example with reference to the enclosed drawing, whose single figure schematically shows a system for controlling personal authorization.

Accordingly, wristwatch 1 shown in partial cross section has infrared sensor 3 on watch case 2 on the underside facing

the wrist (not shown) for detecting the pattern of subcutaneous blood vessels of the relevant person's wrist.

Wristwatch 1 forming the data carrier also has a transponder with chip 6 and antenna coil 7 for the data transaction according to arrow T with reader 4 on access control device 5, which is formed as a turnstile.

The relevant person's subcutaneous blood vessel pattern data measured by sensor 3 are supplied to chip 6 and transferred contactlessly with antenna 7 to reader 4 which is connected on- or off-line with a central processing unit in which the biometric skin identification data of the access-authorized persons are stored. If the comparison yields a match, access control device 5 is released.

-6-

PCT/EP00/12049
SkiData AG

16153 PCT
18 Feb. 2002

New claims

1. A device for controlling a person's authorization upon utilization of a service with a data carrier that communicates contactlessly with a reader (4), and with a sensor (3) for detecting the person's biometric identification features, a memory for the authorized person's biometric identification features and means for comparing the stored biometric identification features with those detected, characterized in that the data carrier is formed as a wristwatch (1), and the sensor (3) is disposed on the side of the wristwatch (1) facing the skin and is formed for detecting the subcutaneous blood vessels of the skin located thereunder as biometric identification features.

2. A device according to claim 1, characterized in that the memory for the biometric identification features is provided in the data carrier (1).

3. A device according to claim 1 or 2, characterized in that the reader (4) is connected with the memory for the biometric identification features.

Smart & Biggar
Ottawa, Canada
Patent Agents

1/1

