(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
31 de Enero de 2008 (31.01.2008)

PCT

(10) Número de Publicación Internacional
WO 2008/012389 A1

(51) Clasificación Internacional de Patentes:
G07C 9/00 (2006.01) *A61B 5/117* (2006.01)
G06K 9/00 (2006.01)

(21) Número de la solicitud internacional:
PCT/ES2007/000456

(22) Fecha de presentación internacional:
25 de Julio de 2007 (25.07.2007)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(30) Datos relativos a la prioridad:
P200602018 27 de Julio de 2006 (27.07.2006) ES

(71) Solicitante *(para todos los Estados designados salvo US)*: **TECISA 74, S.L.** [ES/ES]; Bubierca, 6, E-50013 Zaragoza (ES).

(72) Inventor; e

(75) Inventor/Solicitante *(para US solamente)*: **LANUZA FERNÁNDEZ, Ignacio** [ES/ES]; Bubierca, 6, E-50013 Zaragoza (ES).

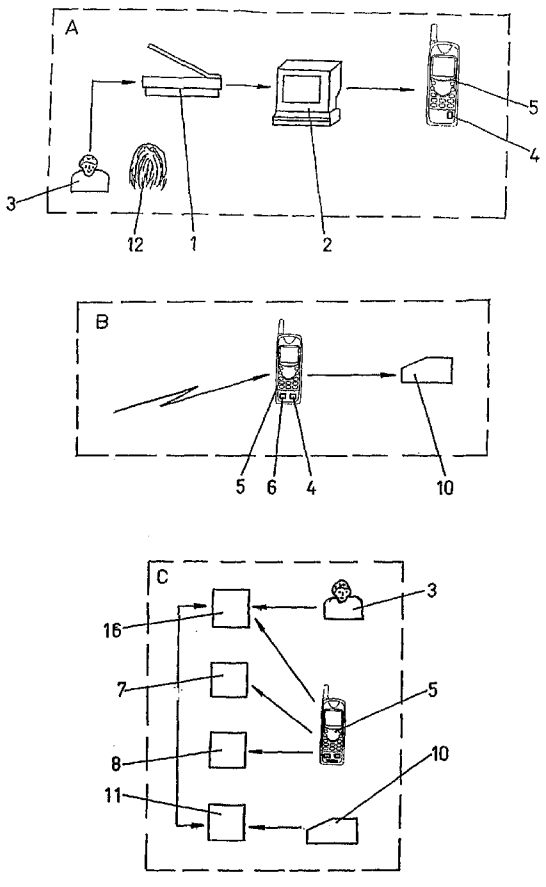
(74) Mandatario: **UNGRÍA LÓPEZ, Javier**; Avenida Ramón y Cajal, 78, E-28043 Madrid (ES).

(81) Estados designados *(a menos que se indique otra cosa, para toda clase de protección nacional admisible)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Continúa en la página siguiente]

(54) **Title:** TEMPORARY BIOMETRIC ACCREDITATION SYSTEM

(54) **Título:** SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL



(57) Abstract: The invention relates to a temporary biometric accreditation system which is used to enable people to access pre-determined locations. The system includes: a computer biometric accreditation device (A), information loading means (B), and an access control device (C), none of which are connected. The computer device is connected to a computer (2) which is used to generate and save the biometric characteristics of the individual (3) to be accredited in a memory element (4) of a mobile telephone (5). The information loading means (B) include a message which can be stored in a memory element (6) of the mobile telephone (5) and which, together with the stored biometric characteristics, generates information that has been encrypted using a two-dimensional barcode and/or a radio frequency. The access control device (C) includes: a biometric data reader (16), a radio frequency transmitter and receiver (7) for receiving radio frequency transmitted by the mobile telephone (5) and/or a barcode reader on the screen (9) of the mobile telephone (5) reader for obtaining access.

(57) Resumen: El sistema previsto para su aplicación en el acceso de personas a determinados lugares comprende: un equipo informático (A) de acreditación biométrica; unos medios (B) de carga de información y- un equipo (C) de control de acceso, sin conexión entre ellos. El equipo informático conectado a un ordenador (2), mediante el que se generan y guardan las características biométricas del sujeto (3) a acreditar en una memoria (4) d en teléfono móvil (5). Los medios (B) de carga de información comprenden un mensaje almacenable en una memoria (6) del teléfono móvil (5), que junto con las características biométricas guardadas generan una información encriptada según un código de barras de dos dimensiones y/o una radio-frecuencia. El equipo (C) de control de acceso incluye: un lector (16) de datos biométricos; un emisor-receptor (7) de radio-frecuencia emitida por el teléfono móvil (5) y/o un lector de código de barras presentado en pantalla (9) del lector del teléfono móvil (5) para obtener en acceso.

WO 2008/012389 A1

(84) Estados designados *(a menos que se indique otra cosa, para toda clase de protección regional admisible)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publicada:

— *con informe de búsqueda internacional*

— *antes de la expiración del plazo para modificar las reivindicaciones y para ser republicada si se reciben modificaciones*

Para códigos de dos letras y otras abreviaturas, véase la sección "Guidance Notes on Codes and Abbreviations" que aparece al principio de cada número regular de la Gaceta del PCT.

SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL.

OBJETO DE LA INVENCIÓN.

La siguiente invención, según se expresa en el enunciado de la presente memoria descriptiva, se refiere a un sistema de acreditación biométrica temporal, el cual tiene como objetivo esencial permitir el control de acceso con total seguridad a zonas de acceso restringido de, únicamente, aquellos usuarios que estén acreditados.

Así, el sistema se basa en un equipo informático de acreditación biométrica personalizada, unos medios de carga de la información y un equipo de control de acceso, independientes entre sí, de forma que al no precisar una base de datos de almacenaje de todos los posibles usuarios a acreditar, se permite el incremento de usuarios del sistema sin que ello conlleve una mayor complejidad del mismo.

Para ello, mediante el equipo informático de acreditación se genera la acreditación biométrica personalizada que es guardada en memoria en un teléfono móvil; mediante los medios de carga de la información se guarda en memoria en el propio teléfono móvil y mediante el segundo equipo de control de acceso se permite el paso de acceso.

CAMPO DE APLICACIÓN.

En la presente memoria se describe un sistema de acreditación biométrica temporal, el cual tiene un amplio campo de aplicación para controlar el acceso a muy diferentes lugares, en base al reconocimiento de una característica biométrica, tal como la huella digital, el iris u otros.

Así, el sistema puede ser de aplicación para el control de acceso a conjuntos residenciales, casas rurales, empresas e industrias, chalets, despachos, oficinas, viviendas particulares, etc., dada la sencillez y economía de instalación.

ANTECEDENTES DE LA INVENCIÓN.

Por un lado, haciendo referencia al ámbito de acceso a viviendas, como es conocido el mismo se viene produciendo mediante la correspondiente llave, siendo cada día más frecuente que, al trabajar fuera, se disponga de diferentes servicios a los que se les deba de aportar un acceso a las viviendas cuando no hay nadie presente en ella.

Así, cuando se requiere servicios tales como de limpieza, planchado u otros a la empresa que los presta se le debe de facilitar una llave de acceso, perdiendo fiabilidad por el hecho de no ser siempre la misma persona la que acuda a realizar la tarea correspondiente.

Esta misma situación se produce en numerosas oficinas, industrias, empresas, organismos públicos, etc. en los que diferentes trabajos, tales como los de limpieza, se suelen llevar a cabo en horario fuera de trabajo.

Por otra parte, como es conocido, en el ámbito industrial, el control de acceso a determinados lugares, como por ejemplo industrias, empresas, organismos públicos, etc., se ha venido llevando a cabo en un puesto de control mediante la simple identificación de las personas que vayan a acceder, esto es, facilitando su identidad, de forma que, en este caso, se precisa de la presencia física de, al menos, una persona en el puesto de control.

Asimismo, con el paso del tiempo, se han venido implantando nuevos sistemas de control de acceso que no precisen la presencia física de una persona, y, así, para acceder a zonas de uso común, como puede ser garajes, se ha popularizado el uso de "mandos a distancia" codificados.

Este sistema presenta ciertos inconvenientes como es su poca o nula fiabilidad al no ser un sistema

individualizado, de forma que en el momento que accede un usuario autorizado al disponer del correspondiente mando, simultáneamente, pueden acceder personas ajenas.

Así, con obviar de estos inconvenientes, en determinados lugares, se han ido implantando medidas de control más rigurosas, de forma que en aquellos casos en los que se ha precisado llevar a cabo un riguroso control de acceso se ha aplicado el reconocimiento de huella dactilar, el cual se ha reservado, en general, a sistemas relacionados con alta seguridad y los cuales se basan en una comparación de la medida biométrica obtenida en el control de acceso con una base de datos en la que están almacenados los datos de los usuarios que pueden acceder. Así, si los datos obtenidos en el control de acceso coinciden con alguno de los datos almacenados en la base de datos se permite el acceso.

Por otra parte, podemos citar la existencia del Modelo de Utilidad ES 1062278 en el que se presenta un *"Dispositivo de mando a distancia multiuso"*, el cual es susceptible de emitir diferentes códigos con objeto de poder acceder a diferentes lugares, de acuerdo a cada uno de los códigos que puede emitir.

Asimismo, podemos citar el Modelo de Utilidad ES 1062274 en el que se presenta un *"Dispositivo para el control de identidad"*, el cual se basa en una unidad central de proceso, asociada a uno o más sistemas de lectura biométrica, a una pantalla LCD o similar, a una unidad controladora y ésta a una pluralidad de sensores que actúan a modo de pulsadores.

DESCRIPCIÓN DE LA INVENCIÓN.

En la presente memoria se describe un sistema de acreditación biométrica temporal, siendo del tipo de sistemas de acreditación para el acceso a determinados lugares basados en el control de una característica biométrica, de manera que en el lugar de acceso se

dispone de un lector de datos biométricos para su comparación con los datos almacenados en una base de datos de un ordenador central con el cual esta comunicado, de forma que el nuevo sistema comprende un equipo informático de acreditación biométrica; unos medios de carga de la información (lugar y tiempo de acceso) y un equipo de control de acceso, no estando conectados entre sí, de manera que el independiente equipo informático de acreditación biométrica se constituye por:

- un lector de datos biométricos conexionado a un ordenador mediante el cual se genera y guarda las deseadas características biométricas del usuario a acreditar en una memoria de su teléfono móvil;

en tanto que los medios de carga de la información, relativa al lugar y tiempo de acceso, se constituyen por:

- un mensaje que se almacena en una memoria del teléfono móvil, que junto con las características biométricas guardadas en la correspondiente memoria del teléfono móvil generan una información encriptada, según un código de barras de dos dimensiones y/o una radio frecuencia;

mientras que el independiente equipo de control de acceso se constituye por:

- un lector de datos biométricos;
- un emisor receptor de radio frecuencia emitida por el teléfono móvil y/o,
- un lector del código de barras presentado en la pantalla del teléfono móvil para obtener el acceso

De esta forma, la información encriptada resultante de la información almacenada en las memorias del teléfono móvil, relativas a la memoria que guarda las

características biométricas del usuario acreditado y la memoria que guarda el mensaje recibido puede ser impresa, según un código de barras, en un soporte en papel convencional.

Asimismo, el equipo de control podrá incorporar un lector para leer la información, basada en un código de barras, almacenada en el soporte de papel convencional.

Los lectores de características biométricas se constituyen, preferentemente, por un lector de huella digital y/o iris.

Igualmente, el equipo de control de acceso puede incorporar una cámara de control montada en el lugar de acceso, mediante la cual se podrá controlar a la persona que acceda al interior de la zona a controlar.

Por otra parte, en una variante de ejecución practica de la invención, el sistema comprende un equipo informático de acreditación biométrica y un equipo de control de acceso, no estando conectados entre sí, de manera que el equipo informático de acreditación biométrica se constituye por:

- un lector de datos biométricos conexionado a un ordenador y una impresora mediante la cual se genera un soporte en papel con un código de barras que guarda las deseadas características biométricas del usuario; y,

en tanto que el equipo de control de acceso se constituye por:

- un lector de características biométricas del usuario a acreditar; y,
- un lector del soporte de papel basado en una tecnología de código de barras de dos dimensiones, provisto de una base de datos para almacenar los accesos producidos y estando conexionado con el lector de

características biométricas de este equipo de control de acceso.

De estas forma, el teléfono móvil, así como el soporte en papel que contienen la información generada están personalizados para uso exclusivo por la persona acreditada en el lugar y el tiempo predeterminado.

Además, el propio papel convencional de uso diario se utilizará de soporte para almacenar la información deseada quedando almacenado el lugar al que se podrá acceder y el tiempo de uso.

Cuando la información esté almacenada en un teléfono móvil el equipo de control de acceso, además del lector de datos biométricos, incorporará un receptor emisor de radio frecuencia y/o un lector del código de barras presentado en la pantalla del propio teléfono móvil, permitiendo el acceso por ambas opciones.

Por otra parte, el lector del soporte en papel, relativo al control de acceso, lee el código de barras bidimensional acreditando:

- la autenticidad de la información almacenada por medio de la firma digital;
- los datos almacenados de acceso, estando referidos al lugar y el posible plazo horario de acceso; y,
- la característica biométrica almacenada comparándola con la leída por el lector de características biométricas relativo al control de acceso.

En una ejecución practica los lectores de características biométricas se pueden constituir, preferentemente, por lectores de huella digital y/o iris.

Asimismo, el segundo equipo de control de acceso puede incorporar una cámara de control instalada en el lugar de acceso con objeto de poder controlar el acceso a la zona a controlar.

De esta forma, el sistema descrito presenta como una primer y muy importante ventaja el hecho de que el equipo informático de acreditación biométrica y el equipo de control de acceso son total y absolutamente independientes entre sí, ya que, toda la información de las personas acreditadas esta almacenada en el teléfono móvil y/o en el soporte en papel y no es necesario disponer de un sistema centralizado de bases de datos, permitiendo el incremento del número de usuarios sin que ello implique un incremento en la complejidad del sistema.

Para complementar la descripción que seguidamente se va a realizar, y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña a la presente memoria descriptiva, de un juego de planos, en cuyas figuras de forma ilustrativa y no limitativa, se representan los detalles más característicos de la invención.

BREVE DESCRIPCIÓN DE LOS DISEÑOS.

Figura 1. Muestra una vista esquemática de una ejecución practica del sistema objeto de la invención constituido por un equipo informático de acreditación biométrica, unos medios de carga de la información y un equipo de control de acceso, independientes entre sí.

Figura 2. Muestra una vista esquemática de una segunda ejecución practica del sistema objeto de la invención constituido por un equipo informático de acreditación biométrica y un equipo de control de acceso, independientes entre sí.

DESCRIPCIÓN DE UNA REALIZACIÓN PREFERENTE.

A la vista de las comentadas figuras y de acuerdo con la numeración adoptada podemos observar como el sistema de acreditación biométrica temporal se constituye por un equipo informático A de acreditación biométrica; unos medios B de carga de la información relativa al

lugar y tiempo de acceso y un equipo C de control de acceso, no estando conectados entre sí.

Así, el independiente equipo informático A de acreditación biométrica se constituye por un lector 1 de datos biométricos conexionado a un ordenador 2 mediante el cual se genera y guarda las deseadas características biométricas, preferentemente la huella digital 12, del usuario 3 a acreditar en una memoria 4 de un teléfono móvil 5, de forma que esta operación deberá ser realizada por aquellas personas que estén acreditadas para ello.

Por otra parte, los medios B de carga de la información, relativa al lugar y tiempo de acceso, se constituyen por un mensaje que se almacena en una memoria 6 del teléfono móvil 5, que junto con las características biométricas guardadas en la memoria 4 generan una información encriptada, según un código de barras de dos dimensiones y/o una radio frecuencia.

El independiente equipo C de control de acceso se constituye por un lector 16 de características biométricas, un emisor receptor 7 de radio frecuencia emitida por el teléfono móvil 5 y/o un lector 8 del código de barras presentado en la pantalla 9 del teléfono móvil 5 para obtener el acceso.

Así, en el punto de acceso el usuario acreditado deberá acreditar su huella digital mediante el lector 16 y podrá emitir, a través del teléfono móvil 5, una radio frecuencia para activar un receptor emisor 7 de radio frecuencia, o bien podrá disponer la pantalla 9 en la que se presenta un código de barras encriptado con la información ante un lector 8 de código de barras. De esta forma, la huella de la persona a acreditar deberá coincidir con la información obtenida por el teléfono móvil.

Mediante el sistema descrito un usuario 3 acreditado a través de su móvil 5, por ejemplo, podrá

contactar vía Internet para solicitar unos días de estancia en una casa rural, de forma que de acuerdo a su solicitud (días de estancia) recibirá un mensaje en su teléfono móvil que junto con la información guardada en la memoria 4 de sus característica biométricas generará un información encriptada.

Así, al desplazarse a la casa rural por medio del teléfono móvil 5, además de acreditar su huella digital mediante el lector 16, activará una radio frecuencia y el receptor emisor 7, si es correcta, permitirá el acceso, esto es, abrirá la puerta de paso. De igual forma ocurriría si el control de acceso se llevase a cabo por medio de un código de barras en su pantalla 9 que contiene la información y que al ser leído por el lector 8, igualmente, se facilitaría el acceso.

Asimismo, mediante el teléfono móvil 5 se podría imprimir en un soporte 10 de papel convencional el código de barras de dos dimensiones para ser utilizado como medio de acceso para lo cual en el control de acceso se deberá incorporar un lector 11 de código de barras.

En una variante de ejecución practica de la invención, el equipo informático A de acreditación biométrica se puede constituir por un lector 1, tal como un escáner, de datos biométricos, preferiblemente de la huella digital 12 del usuario 3 a acreditar, conexionado a un ordenador 2 y una impresora 13 de chorro de tinta para generar un soporte 10 en papel de uso diario.

En dicho soporte 10 se almacenarán las deseadas características biométricas (huella digital 12) de la persona 3 a acreditar, la información del lugar y tiempo de acceso permitido y la firma digital del emisor del soporte 10, estando basada la información almacenada en el soporte 10 en una tecnología de código de barras de dos dimensiones.

Por otra parte, el equipo C de control de acceso,

independiente del equipo A de acreditación biométrica, se constituirá por un lector 14 de características biométricas (huella digital 12) de la persona 3 a acreditar y un lector 15 del soporte 10 en papel convencional, estando dotado el lector 15 de una base de datos para almacenar los accesos producidos y estando conexionado el citado lector 15 de tarjetas con el lector 14 de las características biométricas de este equipo C de control de acceso.

El lector 1, el lector 14 y el lector 16 de las características biométricas pueden ser iguales o diferentes, dando ello una mayor versatilidad al sistema.

De esta forma, cuando se vaya a acreditar a un usuario 3 éste posicionará un dedo sobre el escáner 1, con objeto de capturar los datos biométricos de su huella digital 12 por el acreditador que rellenará un formulario recogiendo los datos personales del nuevo usuario, los datos físicos y temporales de acceso, esto es, puntos a los que se autoriza el acceso y el horario de acceso y la firma digital del acreditador, de forma que el sistema encriptará la información en un sistema de código de barras de dos dimensiones que se imprimirá, mediante una impresora 13 de chorro de tinta, en un soporte 10 de papel estándar creando un código de barras de dos dimensiones.

Así, en el correspondiente control de acceso C, cuando el usuario 3 desee acreditarse aproximará el soporte 10 en papel convencional al lector 15 de código de barras y posicionará su huella digital 12 en el lector 14 de datos biométricos, de forma que el lector 15 leerá el código de barras de dos dimensiones del soporte 10 comprobando, de manera inequívoca, la autenticidad de la información y su origen, a través de la firma digital del acreditador.

Asimismo, comprueba los datos físicos y

temporales de acceso y compara los datos biométricos, huella digital 12, almacenados en el soporte 10 con los datos leídos, huella digital 12, por el lector 14 de datos biométricos.

Así, si los datos físicos y temporales leídos se corresponden con los datos almacenados de acceso y la huella digital también se corresponde con la almacenada se registrará el acceso siguiendo un protocolo de seguridad y a continuación se abrirá la puerta de paso.

Preferentemente, los lectores de características biométricas se constituyen por lectores de huella digital, pudiendo ser iguales o diferentes, o por lectores de iris u otras características.

Tal como se ha indicado el equipo C de control de acceso puede incorporar una cámara de control, de forma que mediante ella se podrá controlar el acceso de la persona autorizada, pudiendo ser esta ejecución de gran utilidad en viviendas particulares para controlar el acceso de personal de reparto a domicilio. En esta ejecución, asimismo, el sistema puede estar interrelacionado con el teléfono móvil del propietario de la vivienda.

Esta ejecución aporta una gran ventaja hoy en día cuando al trabajar fuera de casa se requiere diferentes servicios a domicilio y al no estar presente se facilite el acceso a la vivienda, presentando, en primer lugar, la ventaja de poder tener identificada a la persona de acceso al estar perfectamente personalizado el acceso, y, en segundo lugar, se pueda controlar el acceso por medio de una cámara.

Por otra parte, el sistema permite un uso generalizado a un mínimo coste y permite trabajar con la información biométrica de los usuarios sin que el acreditador deba almacenar en una base de datos las huellas dactilares de los usuarios acreditados, con lo

cual se evita atentar contra la protección de datos de carácter personal y contra la sensibilidad de las personas, que sienten mayor confianza y seguridad a dar la información de su huella sabiendo que no se hará un uso fraudulento de la misma.

Por otra parte, tal como hemos indicado, el sistema propuesto tiene una amplia aplicación siendo de especial utilidad en aquellos lugares de acceso en los que no siempre se encuentre presente una persona de control y que el acceso se debe de confiar a los posible usuarios, normalmente, facilitando una llave con los inconvenientes que ello representa, como puede ser por la perdida de la misma.

Así, el sistema aplicado para el acceso a "casas rurales" presenta importantes ventajas, ya que, es frecuente que no se encuentre, de forma permanente, una persona por lo que a los usuarios se les facilita una llave, de manera que con el sistema preconizado se obtiene un acceso de control totalmente personalizado.

De esta forma, a los usuarios se les podrá facilitar mediante su propio teléfono móvil 5 o mediante un soporte 10 en papel convencional un plazo determinado, por ejemplo una semana, y, si se desea, con un horario determinado, de forma que transcurrido dicho plazo queda inutilizable.

R E I V I N D I C A C I O N E S.

1ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, siendo del tipo de sistemas de acreditación para el acceso a determinados lugares basados en el control de una característica biométrica, de manera que en el lugar de acceso se dispone de un lector de datos biométricos para su comparación con los datos almacenados en una base de datos de un ordenador central con el cual esta comunicado, caracterizado porque el sistema comprende un equipo informático (A) de acreditación biométrica; unos medios (B) de carga de la información y un equipo (C) de control de acceso, no estando conectados entre sí, de manera que el independiente equipo informático (A) de acreditación biométrica se constituye por:

- un lector (1) de datos biométricos conexionado a un ordenador (2) mediante el cual se genera y guarda las deseadas características biométricas del usuario (3) a acreditar en una memoria (4) de un teléfono móvil (5);

en tanto que los medios (B) de carga de la información, relativa al lugar y tiempo de acceso, se constituyen por:

- un mensaje que se almacena en una memoria (6) del teléfono móvil (5), que junto con las características biométricas guardadas en la memoria (4) generan una información encriptada, según un código de barras de dos dimensiones y/o una radio frecuencia;

mientras que el independiente equipo (C) de control de acceso se constituye por:

- un lector (16) de características biométricas;
- un emisor receptor (7) de radio frecuencia emitida por el teléfono móvil (5) y/o,
- un lector (8) del código de barras presentado en

la pantalla (9) del teléfono móvil (5) para obtener el acceso

2ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, según reivindicación 1ª, caracterizado porque la información encriptada resultante de la información almacenada en la memoria (4) relativa a las características biométricas y en la memoria (6) relativa al lugar y tiempo de acceso del teléfono móvil puede ser impresa, según un código de barras, en un soporte (10) en papel convencional.

3ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, según reivindicaciones 1ª y 2ª, caracterizado porque el teléfono móvil (5) y el soporte (10) que contienen la información están personalizados para uso exclusivo del usuario (3) acreditado en el lugar y el tiempo predeterminado.

4ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, según reivindicaciones 1ª y 2ª, caracterizado porque el equipo (C) de control puede incorporar un lector (11) para leer la información almacenada en el soporte (10) de papel convencional.

5ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, según reivindicación 1ª, caracterizado porque, en una variante de ejecución practica de la invención, el sistema comprende un equipo informático (A) de acreditación biométrica y un equipo (C) de control de acceso, no estando conectados entre sí, de manera que el equipo informático (A) de acreditación biométrica se constituye por:

- un lector (1) de datos biométricos conexionado a un ordenador (2) y una impresora (13) mediante la cual se genera un soporte (10) en papel con un código de barras que guarda las deseadas características biométricas del usuario (3); y,

en tanto que el equipo (C) de control de acceso se

constituye por:

- un lector (14) de características biométricas del usuario (3) a acreditar; y,
- un lector (15) de códigos de barras para la lectura del código de barras impreso en los soportes (10) de papel, estando provisto de una base de datos para almacenar los accesos producidos y estando conexionado con el lector (14) de características biométricas de este equipo (C) de control de acceso.

6ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, según reivindicaciones 1ª y 5°, caracterizado porque los lectores (1), (14) y (16) de características biométricas se constituyen por un lector de huella digital (12) y/o iris.

7ª.- SISTEMA DE ACREDITACIÓN BIOMÉTRICA TEMPORAL, según reivindicaciones 1ª y 5°, caracterizado porque el equipo (C) de control de acceso puede incorporar una cámara de control montada en el lugar de acceso.

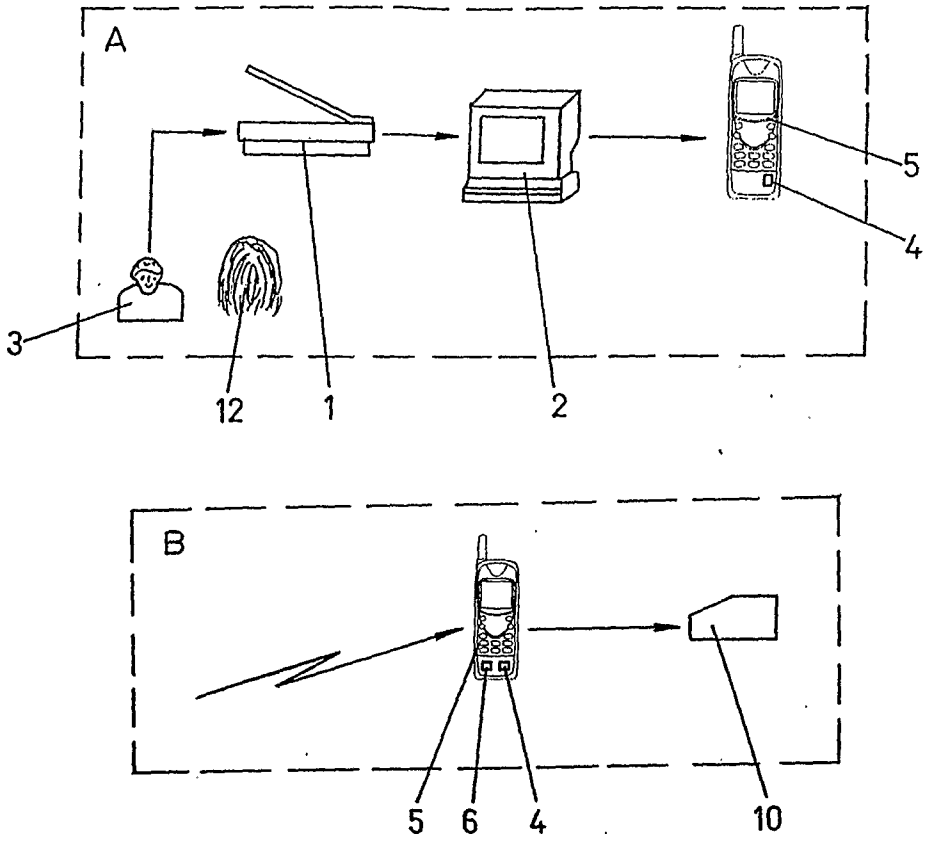


Fig. 1

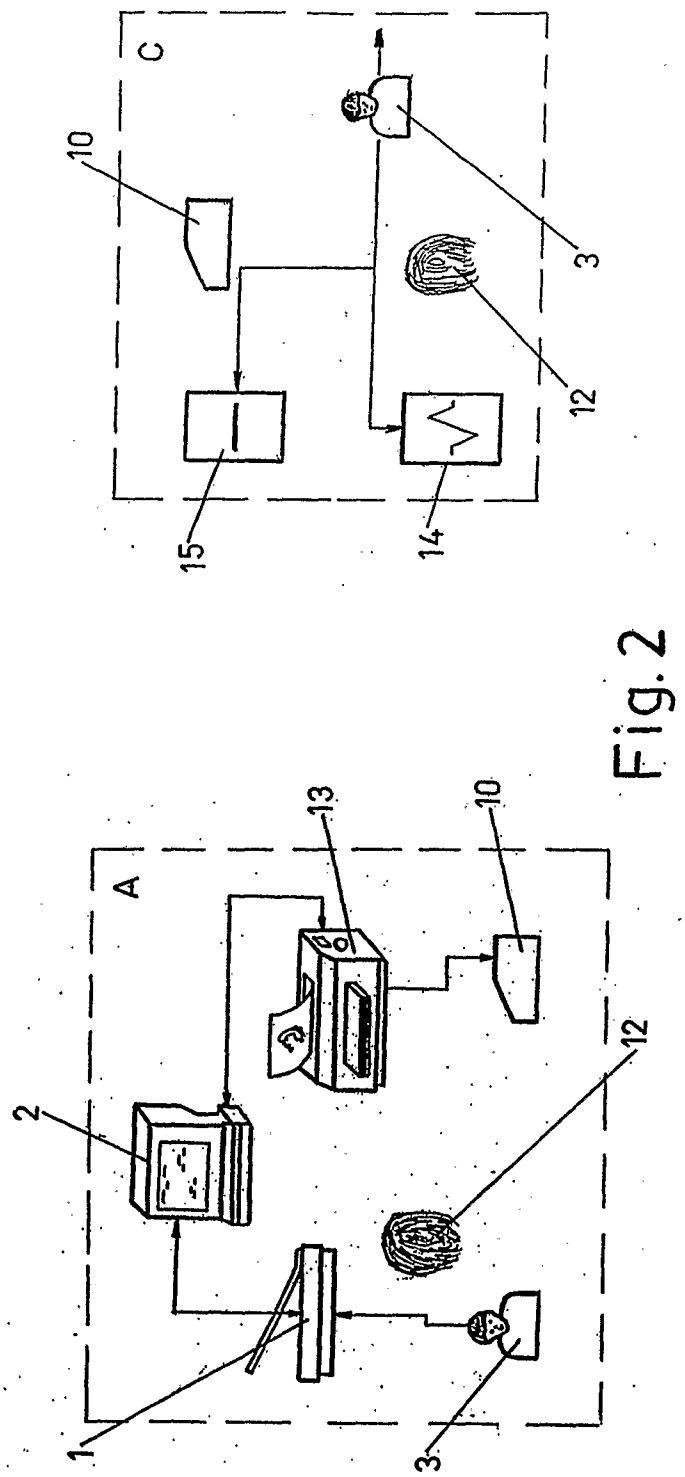


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES 2007/000456

A. CLASSIFICATION OF SUBJECT MATTER

see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G07C, G06K, A61B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CIBEPAT, EPODOC, WPI, TXTE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005242921 A1 (ZIMMERMAN et al.) 03.11.2005, abstract; paragraphs [37-55]; paragraphs [125-136]; figures 2, 9 and 10.	1-7

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance.
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure use, exhibition, or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other documents , such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 December 2007 (11.12.2007)	(21/12/2007)
Name and mailing address of the ISA/ O.E.P.M. Paseo de la Castellana, 75 28071 Madrid, España. Facsimile No. 34 91 3495304	Authorized officer A. Figuera González Telephone No. +34 91 349 55 16

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/ ES 2007/000456

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
US 2005242921 A	03.11.2005	NONE	----------

INTERNATIONAL SEARCH REPORT

International application No.

PCT/ ES 2007/000456

CLASSIFICATION OF SUBJECT MATTER

G07C 9/00 (2006.01)
G06K 9/00 (2006.01)
A61B 5/117 (2006.01)

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº

PCT/ ES 2007/000456

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

Ver hoja adicional

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G07C, G06K, A61B

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

CIBEPAT, EPODOC, WPI, TXTE

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
X	US 2005242921 A1 (ZIMMERMAN et al.) 03.11.2005, resumen; párrafos [37-55]; párrafos [125-136]; figuras 2, 9 y 10.	1-7

☐ En la continuación del Recuadro C se relacionan otros documentos ☒ Los documentos de familias de patentes se indican en el Anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional.	Fecha de expedición del informe de búsqueda internacional
11 Diciembre 2007 (11.12.2007)	21 de diciembre de 2007 (21/12/2007)
Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M. Paseo de la Castellana, 75 28071 Madrid, España. Nº de fax 34 91 3495304	Funcionario autorizado A. Figuera González Nº de teléfono +34 91 349 55 16

INFORME DE BÚSQUEDA INTERNACIONAL

Información relativa a miembros de familias de patentes

Solicitud internacional nº

PCT/ES 2007/000456

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
US 2005242921 A	03.11.2005	NINGUNO	----------

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº

PCT/ ES 2007/000456

CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

G07C 9/00 (2006.01)
G06K 9/00 (2006.01)
A61B 5/117 (2006.01)