(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 309 708**

(51) Int. Cl.:
G07F 7/10 (2006.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05701817 .8**
(96) Fecha de presentación : **10.01.2005**
(97) Número de publicación de la solicitud: **1706852**
(97) Fecha de publicación de la solicitud: **04.10.2006**

(54) Título: **Tarjeta de identificación y método de identificación del poseedor de la tarjeta con utilización de la misma.**

(30) Prioridad: **09.01.2004 GB 0400428**

(45) Fecha de publicación de la mención BOPI:
16.12.2008

(45) Fecha de la publicación del folleto de la patente:
16.12.2008

(73) Titular/es: **Kinderguard Limited**
Holywood House, Innis Court
County Down, Holywood BT18 9HF, GB

(72) Inventor/es: **Douglas, Raymond**

(74) Agente: **Durán Moya, Carlos**

DESCRIPCIÓN

Tarjeta de identificación y método de identificación del poseedor de la tarjeta con utilización de la misma.

La presente invención se refiere a una tarjeta de identificación y a un método para identificar al poseedor de la tarjeta con utilización de la propia tarjeta, y en particular a una tarjeta de identificación que utiliza características biométricas para la identificación. La expresión poseedor de la tarjeta se refiere a una persona que sostiene la tarjeta entre su dedo índice y su dedo pulgar en condiciones operativas normales. No obstante, se comprenderá que una persona con un problema físico puede sostener la tarjeta entre cualesquiera otras partes adyacentes del cuerpo, tales como los dedos de la mano o de los pies, permitiendo el funcionamiento de la invención.

La biometría ha sido investigada a fondo y parece que virtualmente no existen límites a las partes del cuerpo, las características personales y los métodos de lectura utilizados para la identificación biométrica: dedos, manos, pies, rostro, ojos, orejas, dientes, venas, voces, firmas, estilos de escritura, ADN humano, modo de andar y olores. La biometría aborda las conexiones más débiles de nuestros sistemas y trabaja en la mejora de la seguridad de estos elementos para reducir el riesgo de los ataques contra la seguridad, de los cuales una media del ochenta por ciento, están relacionados con las contraseñas.

Una fotografía instantánea de donde se están utilizando aplicaciones biométricas muestra que el control del acceso físico, es decir, la protección de edificios y de habitaciones contra la entrada sin autorización, se considera que representó aproximadamente la mitad de las ventas de dispositivos biométricos en el año 2001. El control del acceso lógico, es decir, la protección de ordenadores y de redes informáticas, representó el cuarenta por ciento del mercado, y las aplicaciones de tiempo y de espera representaron el resto. Existen muchas tecnologías biométricas que ya están disponibles para ser explotadas. A continuación se resumen las aplicaciones biométricas clave, actualmente desarrolladas y disponibles:

Geometría de la mano - la mano es muy válida y se requiere un daño físico considerable para alterar su forma geométrica de manera significativa. La mano no es muy distintiva, existiendo muchas personas que comparten una representación geométrica común. La mano es accesible ya que es fácil de presentar. La mano es aceptable ya que se opina que no invade la privacidad personal. La disponibilidad de la mano es reducida ya que habitualmente solamente puede presentarse la forma geométrica de una mano, dado que la mano izquierda a menudo es una imagen casi simétrica de la derecha.

Huellas digitales - la huella digital no es muy válida y es susceptible a daños químicos y físicos. La huella digital es muy distintiva, con aplicaciones primarias basadas en la identificación criminal dentro de los organismos de defensa de la ley. La huella digital es accesible, pero a menudo requiere un cierto tiempo de reacción por parte del usuario con respecto a su correcta presentación y puede complicarse debido a enfermedades de la piel. La huella digital es aceptable dado que se opina que no invade la intimidad personal. La disponibilidad de las huellas digitales es elevada ya que habitualmente una persona puede presentar, por lo menos, seis huellas digitales casi independientes. La palma de la mano puede incluirse asimismo dentro de esta categoría pero es raramente utilizada.

La técnica actual en esta área es el resultado de un proyecto (IST-2000-25168) costeado por la UE (Unión europea) con costes compartidos, que finalizó en Junio del año 2002, coordinado por Infineon Technologies AG (Alemania), titulado “Sistema de comparación biométrica y de autentificación en tarjetas (tarjetas de dedos)”.

Rostro - el rostro es válido al ser una zona del cuerpo que está bien protegida. El rostro no es muy distintivo, con aplicaciones primarias basadas en la identificación criminal comparando sospechosos conocidos. El rostro es accesible con sistemas que pueden capturar imágenes a distancia (varios metros) utilizando equipos de video, pero los problemas de orientación distorsionan los datos recogidos. El rostro es aceptable dado que se opina que no invade la intimidad personal. La disponibilidad del rostro es elevada ya que habitualmente una persona puede presentar varias características independientes, pero la orientación puede distorsionarlas. Existe asimismo el coste de la infraestructura técnica asociada a la adquisición de las fuentes de datos del rostro y de otras partes del cuerpo humano, sin mencionar la necesidad de que el ser humano participe en la adquisición de dichos datos permaneciendo de pie en posición correcta o interactuando con determinados dispositivos para obtener los datos.

Ojos - el ojo es muy válido al ser una zona del cuerpo que está bien protegida. El ojo es muy distintivo con aplicaciones primarias basadas en el escaneado de la retina, aunque también se ha desarrollado el escaneado del iris. El ojo es accesible pero puede ser complicado, aunque el escaneado de la retina reduce los problemas de orientación debido a que el ojo se alinea naturalmente por sí mismo cuando enfoca un objetivo iluminado. El escaneado del iris no requiere que la persona interactúe con un dispositivo, pero en cambio utiliza una imagen de video del ojo que puede ser tomada a un pie (30 cm) de distancia. El ojo es aceptable dado que se opina que no invade la intimidad personal. La disponibilidad del ojo se complica por el hecho de que pueden presentarse múltiples zonas de la retina al mover el ojo en diversas direcciones.

Voz - la voz es válida, pero existe una amplia gama de aspectos que impactan en la verificación de la voz, tales como resfriados y gripe, medicación y tensiones. La voz es muy distintiva y muestra una proporción de aceptaciones falsas (FAR) del 0,3%. La voz es accesible pero varía debido a los cambios de posición del cuerpo, el bienestar físico de la persona que habla y el tiempo. La voz es aceptable y es claramente no invasiva, pero no siempre puede ser

apropiada en algunas negociaciones personales o en determinados entornos sociales. La disponibilidad de la voz es elevada ya que está determinada por muchos factores distintos: dimensiones de las cavidades vocales (garganta, boca, nasal) así como de las características de las propias cuerdas vocales, y además está modificada por la forma de hablar; la manera en que se mueven la boca, los labios, la lengua, la mandíbula y los dientes.

Química de la piel - la química de la piel no está bien documentada, con referencias principales a las huellas digitales y a la autentificación de un dedo "real". La principal aplicación que se ha investigado es a través de la Patente IBM (referenciada más adelante) que desarrolla el muestreo del ADN que se sabe que es válido, distintivo, accesible y disponible.

En el área del desarrollo de un sensor biométrico sobre una tarjeta, la Patente US Nº 2002095587 a nombre de IBM titulada: "Tarjeta inteligente con un sensor biométrico integrado" está enfocada al muestreo de huellas digitales, las huellas de las palmas, huellas de voz, de la retina y/o de química de la piel.

La Patente US Nº 6347040 a nombre de Infineon Technologies AG (Alemania), titulada "Dispositivo sensor para detectar características biométricas, en particular características de detalles de los dedos" da a conocer un dispositivo de detección con un chip de detección biométrica. El chip de detección está unido a una placa flexible de un circuito impreso que tiene una capa de un substrato altamente flexible y pistas conductoras aplicadas a la capa de substrato. Las pistas conductoras están en contacto eléctrico con el chip de detección y conducen a una zona de terminales de la placa flexible del circuito impreso. La zona de detección del chip de detección es accesible a través de una abertura en la placa flexible del circuito impreso y la abertura está rodeada, por lo menos parcialmente, por un bastidor puesto a tierra.

La Patente alemana Nº DE10126839 presentada por Infineon Technologies AG (Alemania), titulada "Sensor de huellas digitales para la identificación de personas, que incorpora protección contra descargas electrostáticas y verificación de que el dedo aplicado es un tejido vivo" está enfocada al muestreo de un dedo para identificar la presencia de tejido vivo mediante la derivación de una carga electrostática recibida que es utilizada para la medición de la impedancia en asociación con un circuito de medición. La resistencia de la superficie se determina principalmente mediante la conductividad de un líquido (sudor) que recubre la piel, y esta tecnología intenta abordar el tema de la generación de huellas falsas.

El principal problema asociado con la puesta en práctica de las "tarjetas inteligentes" biométricas desarrolladas recientemente, es un obstáculo financiero debido a la necesidad de instalar programas y equipos informáticos en cada instalación de lectura. Esto no representa ningún problema cuando se instalan por primera vez los lectores de tarjetas desarrollados recientemente, pero en el caso de las máquinas ATM antiguas, por ejemplo, el coste financiero de instalar programas y equipos informáticos en todas las ATMs es prohibitivo en extremo. El problema surge en primer lugar porque la medición biométrica tradicional no puede ser miniaturizada suficientemente de manera económica para adaptarse a los lectores adicionales externos significativos de tarjetas que se requieren, obligando al mercado a la normalización a un tipo de biometría.

El documento WO 01/20538 da a conocer un método y un aparato para autentificar un organismo individual vivo, mediante el reconocimiento de una característica eléctrica interna, y/o magnética, y/o acústica exclusiva, que comprende una firma biométrica, mediante la presentación de una parte del cuerpo a un dispositivo de detección que detecta la firma. La firma biométrica presentada detectada, es comparada con una firma biométrica conocida para autentificar el individuo. Esta autentificación puede ser utilizada a continuación para autorizar una acción por parte del individuo tal como acceder a un equipo o a una zona, o realizar acciones tales como llevar a cabo operaciones financieras. Se utiliza una tarjeta que tiene sensores para detectar la firma biométrica que es leída por medio de un lector de tarjetas y enviada a un lector local o alejado para su comparación.

El documento WO 01/52180 da a conocer un dispositivo activado biométricamente en el cual los datos derivados de la detección de rasgos biométricos exclusivos internos, son almacenados en el interior de dicho dispositivo activado biométricamente, para ser comparados con los datos almacenados relativos a dichos marcadores biométricos o rasgos de un usuario previamente escaneados de dicho dispositivo activado biométricamente. El dispositivo activado biométricamente puede permitir o no permitir el acceso a la información, o facilitar la utilización de datos o de un dispositivo protegido por medio del dispositivo activado biométricamente.

Claramente, existe la necesidad de un nuevo método de identificación humana que utilice una tarjeta de identificación que pueda funcionar también con los sistemas existentes, superando de este modo el problema de las infraestructuras. Dicho sistema no debería requerir una formación adicional por parte del usuario y debería proporcionar esencialmente un método para identificar de manera exclusiva un ser humano.

De acuerdo con ello, la presente invención da a conocer una tarjeta de identificación que tiene medios para generar y transmitir señales en el cuerpo del poseedor de una tarjeta y medios para recibir e interpretar las señales del cuerpo del poseedor de la tarjeta, estando las señales atenuadas por la impedancia bioeléctrica del cuerpo del poseedor de la tarjeta, de tal modo que la interpretación de las señales atenuadas mediante los medios de interpretación proporciona una firma de impedancia bioeléctrica para identificar de manera exclusiva el poseedor de la tarjeta, en la que los medios para generar y transmitir señales en el cuerpo del poseedor de la tarjeta y los medios para recibir e interpretar las señales del cuerpo del poseedor de la tarjeta comprenden un controlador que tiene una unidad central de procesado (UPC) y

una memoria asociada, dos o más electrodos dispuestos en una superficie exterior de la tarjeta de identificación y un conjunto de circuitos electrónicos de control que acoplan eléctricamente los electrodos al controlador, en la que la tarjeta de identificación tiene su propia fuente de energía en la placa capaz de proporcionar suficiente energía para el funcionamiento independiente de la tarjeta de identificación, caracterizada porque los dos o más electrodos están dispuestos en las caras principales opuestas de la tarjeta de identificación y están situados de tal modo que los dedos índice y pulgar están situados naturalmente sobre los mismos cuando la tarjeta está sostenida entre el índice y el pulgar, y la propia fuente de energía de la tarjeta se activa cuando el poseedor de la tarjeta mantiene los electrodos entre sus dedos y el pulgar durante un periodo de tiempo predeterminado.

La impedancia bioeléctrica puede ser medida con instrumentos técnicos simples, lo que facilita la posibilidad de miniaturizar la tecnología de detección biométrica hasta un grado adecuado para la aplicación a una tarjeta.

Preferentemente, el conjunto de circuitos electrónicos de control comprende medios para generar una gama de señales analógicas de corrientes y frecuencias variables.

De manera ideal, las corrientes están comprendidas dentro de una gama de 100 μA a 900 μA.

Preferentemente, la frecuencia de las señales está comprendida dentro de una gama de 1 kHz a 1.350 kHz.

De manera ideal, el conjunto de circuitos electrónicos de control tiene medios para filtrar las señales atenuadas, convirtiendo las señales analógicas en señales digitales y pasando las señales a la UCP para su interpretación.

Preferentemente, los medios para generar e interpretar señales comprenden un módulo de control de la programación almacenado en la memoria del controlador.

De manera ideal, el módulo de control de la programación compara una firma real de la impedancia bioeléctrica con una firma de la impedancia bioeléctrica grabada en la memoria del controlador. Los datos biométricos reales describen la información obtenida mediante la tarjeta de la persona que actualmente sostiene la tarjeta, a diferencia de la información de la persona cuyos datos biométricos fueron grabados originalmente por el organismo emisor de la tarjeta. Dicha comparación se lleva a cabo bajo el control de un módulo de una red neural que observará, aprenderá y verificará los umbrales de los datos biométricos dentro de unos límites de tolerancia aceptables.

Preferentemente, el módulo de control de la programación tiene medios para identificar las características de la impedancia bioeléctrica representativas de la masa grasa, de la masa celular del cuerpo, del agua adicional de las células y de la masa esquelética.

De manera ideal, el módulo de control de la programación es capaz de generar, transmitir, recibir e interpretar señales en un intervalo de tiempo comprendido dentro de una gama de unos pocos segundos para proporcionar al poseedor de la tarjeta identificado o al poseedor de la tarjeta no identificado una salida para permitir o prohibir realizar una operación, respectivamente.

De manera ideal, el intervalo de tiempo es de un segundo aproximadamente.

Preferentemente, el módulo de control de la programación tiene medios para generar una firma exclusiva de la impedancia bioeléctrica para un poseedor específico de una tarjeta, a partir de un conjunto completo de datos que incluyen un bucle único pulgar-índice, la resistividad de la piel, el sudor, la zona geográfica, el peso, la edad, el sexo, la corriente, la medición de la tensión y la gama de frecuencias.

De manera ideal, la tarjeta de identificación tiene medios para transmitir los datos biométricos a través del espacio a una unidad de autorización, por medio de protocolos de comunicaciones.

Preferentemente, la tarjeta de identificación tiene medios para transmitir a través del espacio una señal de autorización generada como respuesta a una identificación con éxito del poseedor de la tarjeta, a una unidad de autorización por medio de protocolos de comunicaciones.

De manera ideal, la firma de la impedancia bioeléctrica de un usuario de una tarjeta autorizada se almacena en la tarjeta de identificación, en una memoria de solo lectura (ROM).

Preferentemente, los medios para la codificación o el encriptado de las firmas de la impedancia bioeléctrica están almacenados en la memoria del controlador.

De manera ideal, la tarjeta de identificación tiene un emisor de radiación incrustado para permitir definir la localización espacial de la tarjeta de identificación en cualquier momento.

De manera ideal, el módulo de control de la programación ejecuta la respuesta a los electrodos de la tarjeta de identificación que está sostenida entre los dedos pulgar e índice del poseedor de la tarjeta durante un periodo de tiempo predeterminado.

Preferentemente, la firma de la impedancia bioeléctrica del poseedor de la tarjeta está almacenada en la tarjeta en una memoria de solo lectura, habiendo sido grabada esta firma durante la inscripción inicial del poseedor de la tarjeta y la calibración primaria de datos en un entorno seguro.

De manera ventajosa, la tarjeta no precisa que la información sea dada a conocer o verificada por ninguna base de datos comparativa exterior o por aplicaciones de lectura, protegiendo los derechos del ciudadano y eliminando la interoperabilidad y los temas de protección de datos infraestructurales.

De manera ventajosa, el lector de tarjetas no requiere ningún equipo adicional de detección.

De manera ideal, el módulo de control de la programación tiene medios para la identificación de errores, para identificar diferencias mínimas en la biometría, en la detección, en la presentación o en la transmisión de la información que se producen incluso cuando la persona inscrita y la persona que está actualmente operando con la tarjeta son la misma.

De manera ventajosa, estos medios de identificación de errores permiten que una operación pueda seguir adelante en caso de diferencias mínimas.

De manera ideal, los medios de identificación de errores comprenden algoritmos diseñados con criterios de validez teniendo en cuenta un bucle único de pulgar-índice, la resistividad de la piel, el sudor, la zona geográfica, el peso, la edad, el sexo, la corriente, la medición de la tensión y la gama de frecuencias.

Preferentemente, la tarjeta tiene medios para indicar cuando el poseedor de la tarjeta ha sido identificado de forma positiva y cuando el poseedor de una tarjeta no ha sido identificado.

De manera ideal, los medios indicativos comprenden un L.E.D. verde y rojo, aunque el método de llevar a cabo el resultado de la fase de verificación puede variar para adaptarse a la arquitectura y al GUI del lector de tarjetas.

De manera ventajosa, esto alerta al poseedor de la tarjeta sobre el hecho de que haya sido identificado favorablemente o no, según sea el caso, y de que ya no es preciso seguir sosteniendo la tarjeta entre los dedos índice y pulgar, permitiéndole introducir totalmente la tarjeta en la ranura del lector de tarjetas, o extraer la tarjeta e intentarlo de nuevo.

De manera ideal, las tarjetas de identificación están fabricadas utilizando la técnica de moldeo por inyección.

Preferentemente, las técnicas de moldeo por inyección comprenden un doble moldeo por inyección marcado en el molde, utilizando impresión de tinta conductora en los orificios pasantes en capas de láminas delgadas de substrato y proporcionando interconectividad entre las capas.

Preferentemente, el módulo de control de la programación dispone de algoritmos con medios para generar una firma de impedancia bioeléctrica exclusiva para el poseedor específico de una tarjeta, a partir de un conjunto completo de datos que incluyen un bucle único de pulgar-índice, la resistividad de la piel, el sudor, la zona geográfica, el peso, la edad, el sexo, la corriente, la medición de la tensión y la gama de frecuencias. Los algoritmos pueden combinar la impedancia con otros datos biométricos según pueda ser preciso (por ejemplo, dado que el usuario muestra el índice y el pulgar en la tarjeta, estas huellas digitales pueden ser capturadas y comparadas formando parte de una firma biométrica).

De manera ideal, los algoritmos son capaces de reducir el tiempo requerido para identificar un poseedor real de una tarjeta mediante la utilización de un subconjunto de datos seleccionados a partir de cualquier combinación de las variables anteriores.

Preferentemente, las tarjetas están dimensionadas para adaptarse a la norma DIN EN 150 9002, es decir, 85,72 mm x 54,03 mm.

A continuación se describirá la invención haciendo referencia al dibujo adjunto que muestra, a modo de ejemplo, una realización de una tarjeta de identificación según la invención.

Haciendo referencia al dibujo, en él se muestra una tarjeta de identificación de impedancia bioeléctrica indicada globalmente mediante el numeral de referencia (1). La tarjeta (1) se compone de una cubierta (2) con una lámina de una capa delgada (3) de un substrato que encapsula una capa de polímero (10). En el interior de la tarjeta (1) está situada una UCP (4) que tiene un electrodo (5) que puede estar conectado al exterior. El conjunto de circuitos electrónicos de control (7) está en comunicación eléctrica con la UCP (4) a través de las conexiones eléctricas (6), y asimismo en comunicación eléctrica con un par de electrodos (8), (9) que pueden conectarse con el exterior. Los electrodos (8), (9)están dispuestos en las superficies principales opuestas de la cubierta (2) de la lámina con la capa delgada de substrato (3). Un electrodo (8) está formado para recibir el pulgar y el otro electrodo (9) está formado para recibir el dedo índice. Por supuesto, los electrodos (8), (9) pueden estar formados de manera idéntica, de manera que sean adecuados para recibir tanto el índice como el pulgar.

Durante la utilización, el poseedor de la tarjeta levante la tarjeta (1) con su pulgar en un electrodo (8) y con su dedo índice en el otro electrodo (9). Cuando el poseedor de la tarjeta sostiene los electrodos (8), (9) entre sus dedos índice y pulgar durante un periodo de tiempo predeterminado, se activa La fuente de energía de la propia tarjeta. Un sistema operativo en la UCP (4) se pone en marcha y se ejecuta un módulo de control de la programación en la UCP (4), generando y transmitiendo señales digitales al conjunto de circuitos electrónicos de control (7), que convierte las señales digitales en corriente analógica y en señales eléctricas de frecuencia variable y transmite estas señales a la mano del poseedor de la tarjeta a través de los electrodos (8), (9). La impedancia bioeléctrica del cuerpo del poseedor de la tarjeta atenúa las señales cuando pasan por el bucle cerrado formado por los dedos pulgar e índice situados sobre los electrodos opuestos (8), (9). Cuando los electrodos reciben las señales atenuadas, las señales pasan al conjunto de circuitos electrónicos de control (7). El conjunto de circuitos electrónicos de control (7), lee los valores de la tensión para cada frecuencia de las señales atenuadas, filtra las señales atenuadas y las convierte de analógicas en digitales, y presenta las señales al módulo de programación que funciona en la UCP (4).

El módulo de control de la programación genera una firma de impedancia bioeléctrica para el poseedor de la tarjeta que está sosteniendo la tarjeta (1) a partir de la información recibida del conjunto de circuitos electrónicos de control (7). Esta firma de impedancia bioeléctrica es comparada a continuación por medio del módulo de control de la programación con una firma de impedancia bioeléctrica que ha sido grabada durante un procedimiento seguro de inscripción del poseedor titular de la tarjeta. Si las firmas se corresponden hasta un grado considerado suficiente, mediante unos algoritmos de comparación versátiles, subyacentes a una rutina de una programación de comparación (agente inteligente), se activa a continuación un indicador en la tarjeta y el poseedor de la tarjeta puede continuar de manera normal con la operación que desee ejecutar, introduciendo completamente la tarjeta en la ranura del lector de tarjetas o transmitiendo la señal de autorización a una unidad operativa situada a distancia. Si las firmas no se corresponden, el poseedor de la tarjeta puede intentarlo de nuevo. Si el proceso de identificación no tiene éxito después de un cierto número de intentos, el poseedor de la tarjeta está intentando utilizar una tarjeta que no está autorizado a utilizar, y se ha impedido una operación potencialmente fraudulenta.

Pueden realizarse variaciones y modificaciones sin apartarse del ámbito de la invención, tal como está definida en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Tarjeta de identificación (1) que tiene medios para generar y transmitir señales en el cuerpo del poseedor de la tarjeta, y medios para recibir e interpretar las señales del cuerpo del poseedor de la tarjeta, estando las señales atenuadas mediante la impedancia bioeléctrica del cuerpo del poseedor de la tarjeta, de tal modo que la interpretación de las señales atenuadas mediante los medios de interpretación proporciona una firma de impedancia bioeléctrica para identificar de manera exclusiva el poseedor de la tarjeta, en la que los medios para generar y transmitir señales en el cuerpo del poseedor de la tarjeta y los medios para recibir e interpretar las señales del cuerpo del poseedor de la tarjeta comprenden un controlador que tiene una unidad central de procesado (UCP) (4) y una memoria asociada, dos o más electrodos (8, 9) dispuestos en una superficie exterior de la tarjeta y un conjunto de circuitos electrónicos de control (7) que acoplan eléctricamente los electrodos (8, 9) al controlador, en la que la tarjeta tiene su propia fuente de energía en la placa, capaz de proporcionar suficiente energía para el funcionamiento independiente de la tarjeta de identificación (1), **caracterizada** porque los dos o más electrodos (8, 9) están dispuestos en las caras principales opuestas de la tarjeta de identificación (1) y están situados de tal manera que el dedo índice y el pulgar están situados de manera natural sobre los mismos cuando la tarjeta está sostenida entre los dedos índice y pulgar, y cuando el poseedor de la tarjeta sostiene los electrodos (8, 9) entre su índice y su pulgar durante un periodo de tiempo predeterminado, se activa la propia fuente de energía de la tarjeta.

2. Tarjeta de identificación (1), según la reivindicación 1, en la que el conjunto de circuitos electrónicos de control (7) comprende medios para generar una gama de señales analógicas de corriente y frecuencia variables.

3. Tarjeta de identificación (1), según la reivindicación 2, en la que las corrientes están comprendidas dentro de una gama de 100 μA a 900 μA.

4. Tarjeta de identificación (1), según las reivindicaciones 2 ó 3, en la que la frecuencia de las señales está comprendida dentro de una gama de 1 kHz a 1.350 kHz.

5. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que el conjunto de circuitos electrónicos de control (7) tiene medios para filtrar las señales atenuadas, convirtiendo las señales analógicas en señales digitales y pasando las señales a la UCP (4) para su interpretación.

6. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que los medios para generar e interpretar señales, comprenden un módulo de control de la programación almacenado en la memoria del controlador.

7. Tarjeta de identificación (1), según la reivindicación 6, en la que el módulo de control de la programación compara una firma real de impedancia bioeléctrica con una impedancia bioeléctrica grabada en la memoria del controlador.

8. Tarjeta de identificación (1), según las reivindicaciones 6 ó 7, en la que el módulo de control de la programación tiene medios para identificar las características de la impedancia bioeléctrica representativas de la masa grasa, de la masa celular del cuerpo, del agua adicional de las células y de la masa esquelética.

9. Tarjeta de identificación (1), según cualquiera de las reivindicaciones 6 a 8, en la que el módulo de control de la programación es capaz de generar, transmitir, recibir e interpretar señales en un intervalo de tiempo comprendido dentro de una gama de unos segundos para proporcionar a un poseedor de la tarjeta identificado, o a un poseedor de la tarjeta sin identificar, una salida para permitir o impedir que una operación se realice, respectivamente.

10. Tarjeta de identificación (1), según cualquiera de las reivindicaciones 6 a 8, en la que el módulo de control de la programación tiene medios para generar una firma exclusiva de impedancia bioeléctrica para un poseedor específico de la tarjeta, a partir de un conjunto completo de datos que incluyen un bucle único de pulgar-índice, la resistividad de la piel, el sudor, la zona geográfica, el peso, la edad, el sexo, la corriente, la medición de la tensión y la gama de frecuencias.

11. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que la tarjeta de identificación (1) tiene medios para transmitir a través del espacio los datos biométricos a la unidad de autorización mediante protocolos de comunicaciones.

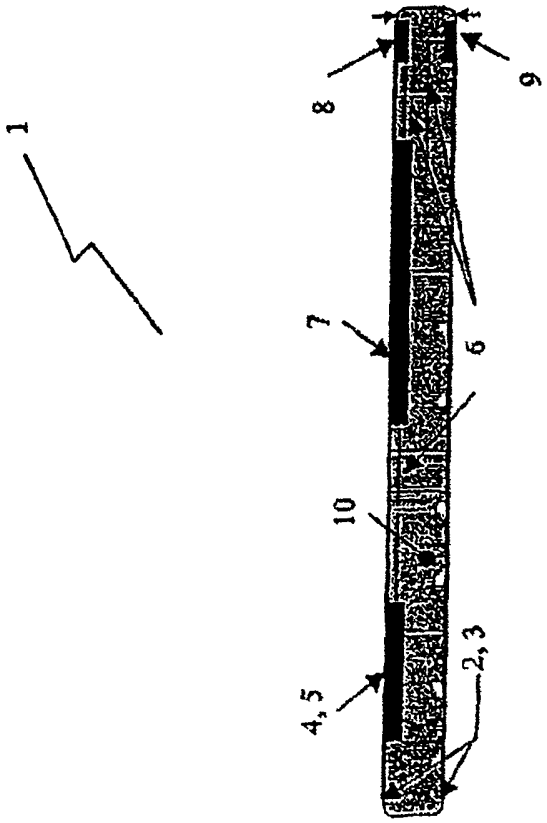
12. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que la tarjeta de identificación (1) tiene medios para transmitir a través del espacio una señal de autorización generada como respuesta a una identificación con éxito del poseedor de una tarjeta a una unidad de autorización, mediante protocolos de comunicaciones.

13. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que la firma de la impedancia bioeléctrica de una tarjeta autorizada de un usuario está almacenada en la tarjeta de identificación (1) en una memoria de solo lectura (ROM).

14. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que los medios para la codificación de las firmas de la impedancia bioeléctrica están almacenados en la memoria del controlador.

15. Tarjeta de identificación (1), según cualquiera de las reivindicaciones anteriores, en la que la tarjeta de identificación (1) tiene un emisor de radiación incrustado, para permitir definir la localización espacial de la tarjeta de identificación (1) en cualquier momento dado.

16. Tarjeta de identificación (1), según cualquiera de las reivindicaciones 6 a 15, en la que el módulo de control de la programación se ejecuta como respuesta a los electrodos (8, 9) de la tarjeta de identificación sostenidos entre los dedos índice y pulgar del poseedor de la tarjeta durante un periodo de tiempo predeterminado.


1
8
9
7
6
10
4, 5
2, 3