(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 658 219**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
G06F 21/31 (2013.01)
G06F 21/32 (2013.01)
G06F 21/41 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.07.2013 PCT/EP2013/066132**

(87) Fecha y número de publicación internacional: **06.02.2014 WO14020087**

(96) Fecha de presentación y número de la solicitud europea: **31.07.2013 E 13744539 (1)**

(97) Fecha y número de publicación de la concesión europea: **01.11.2017 EP 2880585**

(54) Título: **Autenticación biométrica de una persona**

(30) Prioridad:

31.07.2012 FR 1257409

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2018

(73) Titular/es:

IONOSYS (100.0%)
11, boulevard de la Vanne
94240 L'Hay les Roses, FR

(72) Inventor/es:

BLONDEAU, STÉPHANE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Autenticación biométrica de una persona

Campo de la invención

La invención se refiere a la autenticación biométrica de personas.

Antecedentes

Existen muchos medios de identificación física y autenticación para lograr transacciones seguras. Por ejemplo, una tarjeta inteligente permite autenticar a un usuario introduciendo por el usuario un código secreto a través de un terminal dedicado, siendo este código comparado con un código esperado aguardado por un protocolo seguro. Sin embargo, tal tarjeta no protege contra un uso, típicamente de manera fraudulenta, por alguien distinto del usuario auténtico si esa persona fuese capaz de obtener el código secreto.

Tal inconveniente se puede compensar implantando un chip subcutáneo bajo la piel del usuario. Tal implantación asegura la autenticidad del usuario. Sin embargo, ésta es una solución particularmente intrusiva en la medida que requiere un acto especializado y en la medida que el usuario no puede retirarlo fácilmente.

Otra solución conocida consiste en usar datos biométricos únicos para el usuario auténtico. Una posibilidad es de esta manera realizar una comprobación biométrica de dichos datos, mediante un dispositivo que comprende un lector de estos datos (por ejemplo, una huella dactilar) formando una base dedicada, siempre que el usuario desee realizar una operación. Sin embargo, la seguridad de tal sistema se puede considerar como limitada. En particular, en términos de seguridad, la identificación y la autenticación son totalmente dependientes de una medición realizada por la base. De esta manera, durante cada autenticación, es necesario reproducir la medición biométrica. Además, tal sistema puede realizar la autenticación del usuario solamente sobre la base de datos biométricos particulares (por ejemplo, una huella digital) que la base usada para la autenticación es capaz de medir.

A partir del documento US2004/064728A1 se conoce un módulo para autenticar a un portador que comprende un circuito de procesamiento con una memoria de autenticación, un sensor de un parámetro fisiológico del portador, un medio de inactivación del circuito de procesamiento capaz de inactivar este circuito cuando el sensor no recibe una señal fisiológica esperada, un circuito de comunicaciones inalámbricas de campo cercano con una base para recibir datos de dicha base, y medios para transmitir o recibir señales de validación de presencia.

El documento US 6 695 207 B1 describe un módulo en forma de pulsera con detección de detección de proximidad de la persona que lleva puesto el módulo y la abertura de la pulsera, realizando el módulo una autenticación biométrica del portador.

El documento EP 1 914 656 A1 describe un módulo de autenticación que proporciona, a través del cuerpo de una persona que lleva puesto el módulo, datos biométricos de referencia, a una base que realiza la autenticación biométrica de la persona.

Compendio de la invención

Un objetivo de la invención es permitir una identificación y autenticación altamente seguras al tiempo que ofrece una gran flexibilidad y facilidad de uso y una gran facilidad de uso, y en particular para asegurar de una manera clara y fiable que la persona a ser autenticada efectivamente es la persona que lleva puesto el modulo.

Para este fin, se proporciona una combinación como se define en las reivindicaciones.

Breve descripción de las figuras

Otras características, objetivos y ventajas de la invención aparecerán a partir de la siguiente descripción de una realización. En los dibujos anexos:

- la Figura 1a muestra la arquitectura de un módulo de autenticación de personas según una realización de la invención,

- la Figura 1b muestra una posible realización práctica del módulo de la Figura 1,

- la Figura 2a muestra un conjunto que comprende un módulo y un soporte según una realización de la invención,

- la Figura 2b muestra una posible realización práctica del conjunto de la Figura 2a, así como una base de autenticación de personas,

- la Figura 3 muestra una arquitectura práctica de un conjunto según una realización de la invención,

- la Figura 4 muestra una arquitectura de la base de autenticación de una persona según una realización de

la invención,

- la Figura 5 muestra una arquitectura de una base de autenticación de personas según una realización de la invención, y

- la Figura 6 muestra una combinación de un módulo de autenticación y una base de autenticación según una realización de la invención.

Descripción detallada de la invención

1) Ejemplo de un módulo llevado puesto

a) Parte de módulo

Con referencia a las Figuras 1a y 1b, se describe un módulo 10 para autenticar a una persona.

Este módulo 10 está destinado a ser llevado puesto por un usuario, denominado “portador” del módulo.

El módulo 10 incluye un circuito 102 de procesamiento que comprende una memoria de autenticación o memoria 104 segura.

- *Sensor de parámetro fisiológico*

El módulo 10 también incluye un sensor 106 de un parámetro fisiológico del usuario que lleva el módulo.

Por parámetro fisiológico se entiende cualquier parámetro fisiológico que se puede medir directamente en el portador.

Cuando se lleva puesto el módulo por el usuario, el sensor 106 mide el parámetro fisiológico. Esta medición certificará que el módulo 10 está colocado en el cuerpo del portador.

Tal parámetro fisiológico puede ser un parámetro biométrico, es decir, adaptado para permitir la identificación biométrica del portador como es conocido por los expertos, pero también puede ser un parámetro del portador que no permite una identificación biométrica, particularmente no una identificación única o no una identificación con un nivel de precisión correspondiente a una identificación biométrica.

El parámetro fisiológico es, por ejemplo, la temperatura corporal, la frecuencia cardíaca o la conductividad de la piel.

- *Medios de inactivación*

El sensor 106 está asociado con un medio 108 para inactivar el circuito 102 de procesamiento que es sensible a la información proporcionada por el sensor 106 y capaz de inactivar el circuito 102 de procesamiento cuando dicho sensor 106 no recibe una señal fisiológica esperada. En realidad, la memoria 104, conectada al sensor 106, puede contener un tipo o formato esperado de información biométrica.

El medio 108 de inactivación, por ejemplo, comprende un circuito de inactivación que incluye un microcontrolador.

El conjunto formado por la memoria 104, el sensor 106 y el medio 108 de inactivación forma de esta manera un medio autónomo de autenticación del portador.

Este conjunto cumple de esta manera una primera función, es decir, la inactivación selectiva del módulo (que se activó inicialmente por cualquier medio conocido en sí mismo).

El sensor 106 puede operar de forma continua o realizar mediciones en intervalos regulares y/o en momentos predefinidos. Alternativamente, la activación del sensor 106 puede estar condicionada a la detección de una señal de alerta. Esta señal de alerta se origina, por ejemplo, a partir de un conjunto llevado puesto en el que está incluido el módulo 10. La señal de alerta es, por ejemplo, una señal de detección de la apertura de una correa 40 sobre la cual está montado el módulo 10, como se describe en mayor detalle a continuación.

- *Circuito de comunicación inalámbrica*

El módulo 10 incluye un circuito 110 para comunicación inalámbrica de campo cercano con una base 20. El circuito 110 de comunicación es capaz de comunicarse con dicha base 20 según un protocolo que implica datos almacenados en una memoria del módulo (típicamente la memoria 104).

La base 20 es, por ejemplo, una base 20 que permite la activación del módulo 10. Por activación, se entiende la activación inicial del módulo 10, durante la cual el módulo 10 se puede personalizar almacenando datos o activaciones sucesivas en la memoria. Durante estas activaciones sucesivas, los datos almacenados están implicados en el momento de la activación del módulo.

Estos datos preferiblemente son datos biométricos, pero pueden incluir más generalmente cualquier dato relacionado con el usuario y permitir su identificación. El circuito 110 de comunicación inalámbrica, que implica una comunicación según un protocolo que usa datos de identificación, típicamente datos biométricos, forma de esta manera un medio para autenticar al portador, aquí frente a frente con la base 20.

Los datos de identificación pueden ser representativos de un parámetro biométrico o una pluralidad de parámetros biométricos. Los datos biométricos tienen una exactitud que es suficiente para permitir la implementación de una identificación biométrica como es conocido por los expertos, particularmente con la certeza requerida para tales mediciones según el conocimiento de los expertos.

Estos datos biométricos son preferiblemente distintos de dicho parámetro fisiológico medido por el sensor 106, es decir, los datos biométricos son representativos de al menos un parámetro biométrico del portador, siendo el parámetro diferente del medido por el sensor 106.

Por lo tanto, la distinción se hace a nivel del parámetro representado, y por lo tanto puede implicar un formato diferente, así como datos en sí mismos diferentes como que son representativos de un parámetro identificado diferente. Por ejemplo, el parámetro fisiológico puede ser la conductividad de la piel y los datos biométricos pueden ser representativos del iris del ojo o una huella dactilar del portador.

Los datos biométricos pueden incluir, por ejemplo, datos biométricos representativos del parámetro fisiológico medido por el sensor 106, si este último permite un reconocimiento biométrico, y datos biométricos representativos de un parámetro diferente.

Es posible, de esta manera, obtener un aumento de seguridad por que la autenticación se puede basar, en particular, en al menos dos parámetros distintos, siendo uno medido por el módulo 10 y siendo usado por el medio 108 de inactivación, y siendo el otro usado por el protocolo de comunicación inalámbrica.

Los datos biométricos distintos de dicho parámetro fisiológico medidos por el sensor 106 se pueden medir por otro sensor, o almacenar previamente en una memoria de módulo (memoria 104 como se ha mencionado anteriormente).

En el caso donde los datos biométricos estén almacenados previamente, es posible de esta manera usar datos tales como una imagen de un iris o de las redes venosas de una retina. En cada activación, estos datos se pueden comparar con los datos obtenidos a partir de las mediciones hechas por la base 20 durante la misma activación.

Además, de esta manera es posible asegurar que una activación inicial del módulo 10 por una base 20 implica una medición biométrica realizada por esta base 20 y almacenada en forma de datos biométricos en el módulo 10 durante la activación. La activación, de esta manera, tendrá que ser realizada usando una base 20 dedicada, que permitirá aumentar aún más el nivel de seguridad asociado con el uso del módulo 10.

Los datos, preferiblemente los datos biométricos, están almacenados en el módulo 10. Los datos relacionados con el mismo parámetro biométrico también se pueden medir por la base 20 con propósitos de activación.

La comunicación inalámbrica entre el módulo y la base se puede llevar a cabo directamente entre el módulo 10 y la base 20, o de otro modo a través de un equipo personal tal como un teléfono 30. La comunicación inalámbrica es, por ejemplo, una comunicación de tipo NFC o “Bluetooth”.

Los expertos determinarán fácilmente las características técnicas del circuito de comunicación inalámbrica de campo cercano para permitir que el módulo 10 comunique con la base 20. Estas características pertenecen a la técnica de comunicaciones inalámbricas a través de dispositivos y protocolos electrónicos, en particular protocolos seguros, que se pueden asociar con tales tipos de comunicación.

Esta comunicación permite comprobar que el módulo y la base tengan los mismos datos biométricos (o más generalmente datos de identificación) y de esta manera autenticar al usuario tras la activación.

- *Medios de validación de presencia*

El sistema formado por la base 20 y el módulo 10 permite comprobar que el módulo 10 se lleve puesto por el portador. Por propietario del módulo 10, se entiende, por ejemplo, la persona cuyos datos están almacenados en la memoria del módulo 10.

Una persona se puede definir como propietaria del módulo 20 durante su activación inicial, en particular almacenando los datos biométricos de esta persona en la memoria del módulo 10.

Esta validación de presencia se puede considerar, por lo tanto, como la validación de la identidad del portador del módulo.

El módulo 10 también comprende como medios para transmitir o recibir, o para recibir y transmitir, señales de validación de presencia.

El módulo 10 puede incluir medios de validación de presencia que comprenden medios para transmitir y/o recibir señales de validación de presencia. Los medios de validación de presencia pueden comprender o consistir en un dispositivo de validación de presencia, por ejemplo, un circuito electrónico que permita tal validación.

Según una primera alternativa, el módulo 10 comprende medios 112 para transmitir señales de validación de presencia a dicha base 20.

Según una segunda alternativa, el módulo 10 comprende medios para recibir señales de validación de presencia. De esta manera, según esta segunda alternativa, el módulo 10 comprende medios 112 para recibir las señales de validación de presencia de dicha base 20.

Estos medios 112 de transmisión o recepción son distintos de dicho circuito de comunicación 110.

Por ejemplo, los medios 112 de transmisión o recepción incluyen un receptor o transmisor que es independiente del circuito 110 de comunicación, y pueden transmitir o recibir señales independientemente y/o separadamente del circuito 110 de comunicación.

Las señales de validación de presencia permiten validar la presencia del propietario como portador del módulo 10.

La validación se puede realizar por el módulo 10 y/o la base 20 y permite asegurar que el portador sea en realidad el propietario.

Por validación, se puede entender la comprobación de un criterio dado, esto es, la transmisión y/o recepción de señales. Esta comprobación de un criterio dado implica, por ejemplo, una respuesta de validación o invalidación, típicamente en forma de un booleano. Tal respuesta se proporciona, por ejemplo, siguiendo a una entrada dada, por ejemplo, siguiendo a la provisión de un valor de variable de entrada después de un tiempo dado.

Por señal de validación, sabemos que se entiende, de esta manera, una señal, la recepción, la falta de recepción, la transmisión, la falta de transmisión y/o el contenido del cual, permite que sea comprobado tal criterio.

La comprobación del criterio se puede determinar mediante un sistema electrónico, por ejemplo, mediante la base 20 y/o el módulo 10, por ejemplo, mediante medios informáticos de la base 20 y/o el módulo 10.

De esta manera, los expertos implementarán fácilmente una señal con propósitos de validación, denominada señal de validación.

En particular, los expertos sabrán cómo implementar una señal de validación que permita validar la presencia del portador, el propietario y/o el módulo 10.

Según una realización particular, su presencia, entendida como detección a una cierta distancia de la base 20, se puede entender en particular como detección en un área específica, por ejemplo, un área de autenticación.

Es posible, de esta manera, aumentar aún más el nivel de seguridad asociado con el módulo 10 de autenticación y/o la base 20, asegurando que el módulo 10 se activará únicamente si lo lleva puesto una persona que es su propietaria.

Las señales de validación de presencia permiten de esta manera una validación de la autenticación del portador.

Las señales de validación de presencia pueden ser señales acústicas o eléctricas adaptadas para ser transportadas por el cuerpo del portador. Las señales de validación de presencia pueden ser alternativamente señales ópticas, tales como ondas de luz transmitidas por la base 20 para ser recibidas por el módulo 10, o viceversa. Los medios 112 de transmisión o recepción comprenden típicamente una fuente de señal y un receptor adaptado para detectar y validar tales señales.

Este segundo medio de inactivación es sensible a un medio para detectar la presencia del módulo sobre o en un soporte 40 para dicho módulo 10 en el cuerpo de un portador.

Los expertos determinarán fácilmente las características técnicas para la implementación de los medios 112 para transmitir señales a dicha base 20 y/o para recibir señales que se originan desde dicha base 20. Estas características pertenecen a la técnica de comunicación y procesamiento de señales y protocolos, particularmente protocolos seguros, posiblemente asociados juntos.

De manera similar, los expertos determinarán fácilmente las características técnicas del módulo 10 de modo que el circuito 110 de comunicación inalámbrica permita una comunicación con una base 20 y de modo que los medios 112 para transmisión y/o recepción de señales transmitan una señal para la misma base 20 y/o reciban una señal que se origina desde la misma base 20. Los expertos saben cómo determinar las características técnicas de manera que cada uno de estos medios esté asociado con una base 20, y es suficiente de esta manera que las características técnicas respectivas de cada uno de los medios permitan comunicación con la misma base 20.

Por comunicación con la misma base 20, se entiende que puede ser una base 20 dada como cualquier base 20 que tenga una serie de características dadas, de la misma forma que una tarjeta inteligente o tarjeta de banda magnética está adaptada para comunicarse con múltiples terminales sin necesitar, sin embargo, almacenar información relacionada con cada terminal en la tarjeta bancaria.

Según una realización, es posible de esta manera comprobar que la persona autenticada mediante sus datos biométricos (siendo la autenticación habilitada por el circuito o los circuitos de comunicación inalámbrica que forman los medios de comunicación inalámbrica) es en realidad el que lleva puesto el módulo 10.

En realidad, la medición del parámetro biométrico de los datos biométricos se puede seleccionar y realizar por la base, y la medición de validación de presencia se puede seleccionar y realizar de modo que la persona que se autentica mediante sus datos biométricos sea la que intenta validar su presencia. Por ejemplo, los datos biométricos pueden ser una huella dactilar y la validación de presencia puede ser una medición de conductividad por el módulo en respuesta a la transmisión de un campo eléctrico por la base de modo que el campo eléctrico sea conducido por el dedo presentado para la medición de huella dactilar por la base.

b) *Conjunto llevado puesto*

Con referencia a las Figuras 2a y 2b, el módulo puede estar incluido en un conjunto 70 comprendiendo el módulo 10 y un soporte 40 para dicho módulo 10.

El soporte 40 está, por ejemplo, en forma de una correa adaptada para ser unida a la muñeca. La correa 40 puede comprender medios 402 conectados al módulo para determinar el cierre de la correa 40 sobre sí misma. Los medios 402 de determinación de cierre se pueden seleccionar de un grupo que consiste en dispositivos de contacto eléctrico y dispositivos que se basan en de un material cuyas propiedades eléctricas varían en función de su deformación, tales como un elastómero que contiene carbono. De esta manera, es posible saber si la correa 40 se ha retirado y deshabilitar posteriormente el circuito 102 de procesamiento.

La correa 40 está adaptada para ser llevada puesta por el usuario o el portador para permitir su identificación en función de los datos grabados previamente en la memoria 104 de autenticación.

El módulo 10 puede ser una unidad de interfaz unida de manera retirable o fija a la correa 40.

c) *Realización práctica del conjunto*

Con referencia a la Figura 3, la correa 40 y el módulo 10 se pueden poner juntos en el mismo conjunto 70 comprendiendo un circuito 702 sensor que incluye el sensor 106 y opcionalmente el sensor 402 de detección de cierre. El circuito 702 sensor también puede incluir un circuito electrónico para validar la presencia del portador y autenticar al mismo.

El conjunto 70 que es accionado por una unidad 704 central incluye un microcontrolador 706 de baja potencia alimentado y sincronizado apropiadamente y conectado al circuito 702 sensor comprendiendo el sensor 106 y posiblemente el sensor 402 de detección de cierre.

El conjunto que incluye una etapa 710 de NFC implementa el circuito 110 de comunicación inalámbrica, y opcionalmente una etapa 712 para comunicarse con un dispositivo 30 personal, por ejemplo a través de un protocolo de comunicaciones “Bluetooth”.

La unidad central puede incluir un segundo microcontrolador 708 con una potencia de procesamiento y tamaño de memoria apropiados para formar el circuito 102 de procesamiento, gestionar la copia de seguridad de los datos en la memoria 104 de autenticación, gestionar la etapa 710 de comunicaciones inalámbricas, gestionar la etapa 712 opcional de comunicaciones inalámbricas con un dispositivo 30 personal, etc.

El conjunto 70 también comprende opcionalmente una etapa 714 de interfaz de usuario comprendiendo un visualizador 716. El visualizador 716 puede tener una funcionalidad de pantalla táctil para permitir la interacción entre el portador y el conjunto 70. El visualizador 716 es por ejemplo una pantalla táctil de 1,5 pulgadas con una resolución de 240 dpi. Alternativamente o además, el módulo tiene uno o más botones de control.

El conjunto 70 comprende además una etapa 718 de fuente de alimentación para alimentar el dispositivo 7, por ejemplo, una batería que se puede recargar por cable, inalámbricamente o por inducción, con una autonomía adecuada.

2) Ejemplo de una base

Con referencia a las Figuras 2b y 4, se describirá la base 20 de autenticación capaz de cooperar con el módulo 10.

La base 20 puede incluir medios 202 para interconectarse con un dispositivo 30 digital personal. El dispositivo 30 digital personal es, por ejemplo, un asistente digital personal, un ordenador o un teléfono. Los medios 202 de interfaz pueden ser inalámbricos o cableados, por ejemplo, a través de una conexión USB. Los medios 202 de interfaz

incluyen un circuito de interfaz perteneciente a un módulo de interfaz.

La base 20 también puede incluir un circuito 206 para comunicación inalámbrica de campo cercano con dicho módulo 10 en respuesta a los medios 204 de control.

Alternativamente, un dispositivo distinto de la base 20, tal como el dispositivo 30 digital personal, puede comprender el circuito 206 para comunicación inalámbrica de campo cercano con dicho módulo 10 como tal, siendo este último controlado por los medios 204 de control de la base 20.

De esta manera, los medios 204 de control pueden ser medios 204 de control adaptados para permitir una comunicación inalámbrica de campo cercano con dicho módulo 10, por ejemplo, medios 204 para controlar un circuito 206 para comunicación inalámbrica de campo cercano con dicho módulo 10, siendo dicho circuito 206 un circuito de la base 20, o enlazado con la base 20, por ejemplo conectado con la base 20, por ejemplo un circuito de un dispositivo externo tal como dispositivo 30 digital personal conectado con la base 20, por ejemplo, por medio de una conexión cableada.

Los medios 204 de control comprenden, por ejemplo, un microcontrolador que tiene circuitos de entrada/salida. La tecnología de comunicación inalámbrica es, por ejemplo, una comunicación de campo cercano, llamada NFC para “Comunicación de Campo Cercano”.

La base 20 comprende además medios para adquirir y almacenar datos 208 biométricos de un portador del módulo 10. Los medios 208 de adquisición y almacenamiento típicamente están en forma de un módulo de adquisición y almacenamiento comprendiendo un sensor y medios de procesamiento asociados con una memoria. Los datos biométricos son los mencionados anteriormente en relación con el circuito 110 de comunicación del módulo. Los medios 208 de adquisición de datos biométricos pueden estar implicados con o sin contacto corporal con un portador.

Los datos biométricos pueden ser, por ejemplo, huellas dactilares o un patrón de vena de la palma del portador.

Con referencia a la Figura 5, se describe una arquitectura ejemplar de la base 20. La base 20 comprende una etapa 212 de microprocesador que recupera los datos de los medios 208 de adquisición. La etapa 212 de microprocesador también controla el circuito 206 de comunicación inalámbrica de campo cercano cerca para realizar comunicaciones de datos con el módulo 10.

La base 20 puede incluir una etapa 214 de identificación que permite la identificación del portador a partir de los datos biométricos adquiridos.

La base 20 puede incluir una etapa 216 de acondicionamiento de sensor que realiza el acondicionamiento analógico para adquirir datos biométricos o para validar la presencia del portador comparando los datos adquiridos con los del módulo 10.

La base 20 comprende una etapa 218 de potencia para alimentar los componentes de la base 20.

3) Cooperación módulo/base

Con referencia a la Figura 6, un módulo 10 de autenticación y una base 20 de autenticación como se ha descrito anteriormente pueden cooperar (lo cual se ilustra esquemáticamente por la referencia 50) para autorizar el acceso a los datos biométricos, en particular para autorizar al módulo 10, o respectivamente la base 20 para acceder a los datos biométricos, en particular los datos biométricos en la base 20, o respectivamente en el módulo 10, solamente cuando la presencia del módulo 10, preferentemente del módulo y su propietario, se detecta válidamente en la base (véase la descripción a continuación).

Los datos biométricos en la base 20 se pueden adquirir directamente en el portador.

Según otra realización, los datos biométricos en la base 20 se pueden almacenar por los medios 208 de adquisición y almacenamiento de la base 20, por ejemplo en una memoria de la base 20.

Los datos biométricos en el módulo se pueden almacenar en una memoria del módulo 10.

Esta detección se realiza mediante un procesamiento 502 de datos en el módulo y/o un procesamiento 502’ de datos en la base.

Por detectado válidamente, se entiende una detección a través de validación como se ha descrito anteriormente, por ejemplo, por los medios 112 para transmitir señales de validación de presencia a dicha base 20 y para recibir señales de validación de presencia desde dicha base 20.

Esta cooperación implica una comparación 504 de los datos biométricos adquiridos por la base con los datos biométricos de referencia. Según una realización, esta comparación se realiza tras la activación del módulo que ha sido previamente sometido a activación inicial.

Los medios 504 de comparación se pueden proporcionar en el módulo 10, en la base 20, y/o en un dispositivo distinto del módulo 10 y la base 20.

Los medios 504 de comparación pueden estar situados en el módulo 10, con los datos biométricos adquiridos por la base 20 siendo transmitidos al módulo 10 a través de circuitos 206 de comunicación inalámbrica de campo cercano provistos en la base 20 o en el dispositivo 30 digital personal. Alternativamente, se pueden situar medios 504 de comparación en la base 20, con los datos biométricos de referencia siendo almacenados en el módulo 10 y transmitidos a la base 20 a través de circuitos 206 de comunicación inalámbrica de campo cercano.

Además, se pueden proporcionar medios 504 de comparación en un dispositivo distinto del módulo 10 y la base 20, conectado al módulo 10 y/o a la base 20.

La memoria 104 de autenticación en el módulo 10 puede ser capaz de almacenar conjuntos de datos de autenticación capaces de ser comunicados a dicha base 20 y/o al dispositivo 30 digital personal interconectados a través de circuitos 206 de comunicación inalámbrica de campo cercano con el propósito de realizar transacciones con dispositivos digitales conectados a dicha base 20.

4) Inactivación del circuito de procesamiento del módulo

La inactivación del circuito 102 de procesamiento del módulo 10 se implementa mediante un medio 108 de inactivación del circuito 102 sensible a dicho sensor 106 y es capaz de inactivar el circuito 102 cuando dicho sensor 106 no recibe una señal fisiológica esperada.

Tal medio 108 de inactivación puede, por ejemplo, estar basado en una medición de la conductividad de la piel. La medición de la conductividad de la piel permite estimar la actividad de las glándulas sudoríparas en la piel. De esta manera, una alta actividad de estas glándulas se asociará con una alta conductividad de la piel y una baja actividad se asociará con baja conductividad. La medición de la conductividad de la piel se lleva a cabo generalmente en las extremidades (manos y pies) en la medida que el número de glándulas sudoríparas es mayor en estas zonas. La medición se puede hacer a partir de dos electrodos en los que se inyecta una corriente de baja magnitud (DC o AC) y entonces se mide el voltaje generado a través de los electrodos. Los electrodos usados para realizar la medición pueden ser electrodos hechos de Ag/AgCl.

El hecho de que un valor de conductividad medido por el sensor 106 sea menor que un umbral determinado (posiblemente programable) puede indicar por lo tanto una separación entre el módulo 10 y el portador, el medio 108 de inactivación realizando entonces una inactivación del circuito 102 de procesamiento, impidiendo el uso del módulo 10. Tal medición asegura alta fiabilidad y alta seguridad del módulo 10.

El medio 108 de inactivación alternativamente puede basarse en la medición de una conductividad eléctrica distribuida. La conductividad eléctrica distribuida, medida por un sensor piezoeléctrico, permite comprobar que el módulo 10 esté en una posición generalmente estable. Si se retira la correa 40, la conductividad eléctrica cambiará, permitiendo de esta manera detectar una posible apertura (*realización práctica a ser especificada*).

El medio 108 de inactivación también se puede basar en una medición de la variación de la capacitancia de un polímero elástico del conjunto 70, por ejemplo de la correa 40. El propósito aquí es medir la deformación elástica del material de la correa, la cual indicaría la retirada del conjunto 70. El material es, por ejemplo, un polímero electroactivo. El polímero electroactivo es un material cuya forma o tamaño cambia cuando se coloca en un campo eléctrico o que puede presentar un cambio en su resistencia o capacidad eléctrica cuando se somete a un cambio en su geometría. De esta manera, cuando el material se estira, ocurre allí una variación en su capacidad la cual se detecta por un circuito de detección para causar la inactivación.

El medio 108 de inactivación también puede incluir medios para medir variaciones de resistencia eléctrica, por ejemplo en un sensor contenido en el conjunto 70, por ejemplo de la correa 40. El propósito aquí es medir la deformación elástica del material de la correa la cual indicaría una retirada de conjunto 70. El sensor es, por ejemplo, un sensor de curvatura en forma de banda cuya resistencia varía en función del diámetro al que se dobla el sensor. El sensor se complementa de manera útil mediante un circuito de detección para causar la inactivación.

5) Asociación base/módulo

También se proporcionan según una realización de la invención, medios para comprobar en la base 20 que está presente un módulo 10 esperado. Estos medios forman de esta manera medios para validar la presencia de la base 20.

Una primera realización de estos medios puede implicar una medición de la conductividad de la piel tanto en el módulo 10 como en la base 20, siendo las dos señales comparadas entonces o bien en la base 20 (después de la transmisión a la base de las señales detectadas en el módulo por los medios de comunicación inalámbrica) o bien en el módulo 10 (después de la transmisión al módulo de las señales detectadas en la base por los medios de comunicación inalámbrica).

Alternativamente, estos medios pueden implicar una medición de la frecuencia cardíaca del portador mediante fotopletismografía. La medición se lleva a cabo usando una fuente de luz y un fotodiodo. La fuente de luz ilumina un área específica del cuerpo del portador (preferiblemente en un dedo, que tiene la propiedad de estar altamente vascularizado), por ejemplo con un primer diodo emisor de luz que tiene una longitud de onda de 660 nm y un segundo diodo emisor de luz que tiene una longitud de onda de 940 nm para mejorar el rendimiento de la medición, y los cambios en el volumen de sangre generan una variación en la intensidad de la luz medida por el fotodiodo. La medición se puede realizar en el dispositivo 70, por ejemplo, por reflexión de la luz por la sangre, y en la base 20, por ejemplo, por transmisión, para permitir luego una comparación con una referencia con el fin de obtener una validación.

Según una realización, la base 20 incluye medios 210 para transmisión o recepción de señales validando la presencia del módulo 10, distinto del circuito 206 de comunicación. Las señales de validación de presencia destinadas a dicho módulo y/o que se originan desde dicho módulo pueden ser típicamente señales acústicas, eléctricas u ópticas moduladas.

En el caso donde la adquisición de datos 208 biométricos se implementa por contacto con el cuerpo de un portador (en particular el caso de huellas dactilares), las señales son preferiblemente señales acústicas o eléctricas transportadas por el cuerpo del portador, entre la muñeca (zona donde está unido el conjunto 70) y la punta del dedo. Para este fin, el conjunto 70 o base 20 comprende un transductor acústico, por ejemplo, de tipo piezoeléctrico o un electrodo para aplicar al área del cuerpo con la cual está en contacto señales que están moduladas según un patrón de modulación predeterminado. Estas señales, después de haber viajado a través del dedo del usuario, se detectan por un sensor correspondiente (otro transductor acústico u otro electrodo), proporcionado respectivamente en la base 20 o en el conjunto 70. Si se detecta la modulación esperada (que también puede codificar información), entonces la presencia del conjunto 70 se valida por la base. En el caso donde es el conjunto 70 el que recibe las señales, el procesamiento se puede realizar en el módulo 10 y transmitir la validación a la base por el circuito de comunicación inalámbrica.

En el caso donde los medios 208 de adquisición de los datos biométricos se llevan a cabo sin contacto con el cuerpo del usuario (por ejemplo una cámara que toma una imagen de la red venosa palmar), las señales destinadas a permitir la validación de la presencia del módulo son ventajosamente señales ópticas. Estas señales ópticas pueden estar constituidas por una señal óptica modulada, recogida por la cámara antes mencionada además de la red venosa, o de otro modo por un patrón gráfico generado, por ejemplo, en una pantalla de tipo LCD proporcionada en el módulo, siendo este patrón capturado al mismo tiempo que el sistema venoso para su validación.

En todos los casos, si las señales esperadas no están presentes, esto significa que no está presente el módulo 10 esperado, y no están activas las funcionalidades de identificación y/o autentificación del sistema de la invención.

6) Ejemplos de funcionalidades de identificación/autenticación

a) *Identificación de un usuario autorizado en un ordenador en sustitución del nombre de usuario y de la contraseña requerido convencionalmente por un sistema operativo*

El usuario instala un programa dedicado en el ordenador o los ordenadores en los que desea identificarse a sí mismo.

Conecta la base 10 a través de un cable USB (u otro protocolo, cableado o inalámbrico) al ordenador.

El programa le invita a llevar su conjunto 70 que se lleva en la muñeca cerca de la base 20, y entonces se carga un archivo cifrado en la memoria del módulo 10, este archivo que contiene el nombre de usuario y la contraseña para este ordenador.

En el siguiente uso, el usuario simplemente tendrá que llevar su muñeca provista con el conjunto 70 cerca de la base 20 para lograr la apertura de sesión.

Opcionalmente, el usuario puede parametrizar una duración para que la sesión permanezca abierta.

b) *Identificación mediante almacenamiento de nombres de usuario y contraseñas de diferentes sitios web seguros visitados por medio de un navegador*

El usuario instala un complemento para su navegador de Internet.

Este complemento cargará automáticamente los nombres de usuario y las contraseñas pregrabadas por el navegador y las almacenará de una forma cifrada en la memoria 104 segura del módulo 10. El usuario tendrá, de esta manera, en cualquier ordenador con un navegador que tenga este complemento instalado, la posibilidad de tener sus nombres de usuario y contraseñas rellenados previamente automáticamente cuando se establezca una conexión con estos sitios seguros, y simplemente necesitará validar, por ejemplo mediante una pulsación del ratón.

c) *Autenticación en sitios web compatibles*

El usuario visita un sitio web ofreciendo una miniaplicación de identificación compatible con el sistema de la invención.

En su primer inicio de sesión, se sugiere al usuario que introduzca su información de contacto (como para un usuario convencional), pero no introduce ningún nombre de usuario o contraseña. Siguiendo a la validación del registro por el usuario, la miniaplicación carga un archivo cifrado en la memoria 104 segura del módulo 10, permitiéndole ser identificado automáticamente usando el conjunto 70 que lleva en posteriores visitas al sitio.

Para permitir algún grado de control al usuario, puede ventajosamente, en cualquier momento, cambiar el estado de identificación entre los siguientes:

- *siempre autorizado*: el usuario sólo necesita llevar el conjunto 70 (llevado puesto en la muñeca) cerca de la base 20 para que la autenticación sea realizada automáticamente;

- *autorizado de una forma caso por caso*: el usuario debe presentar su conjunto 70 y luego realizar la validación en la interfaz del módulo para lograr la autenticación;

- *denegado*: todos los intentos de lectura serán ignorados. El usuario por lo tanto será capaz de acceder solamente a la parte del sitio que no requiera identificación;

- *revocado*: tras un intento de lectura, el módulo 10 transmite una solicitud de revocación a la miniaplicación del sitio web que (según las reglamentaciones locales) tendrá que borrar los datos personales del usuario de sus servidores.

d) *Cargar un medio de pago legible sin contacto o tarjeta de fidelidad*

El usuario en posesión de un instrumento de pago legible sin contacto o una tarjeta de fidelidad (por ejemplo, una tarjeta bancaria legible por NFC de PayPass) puede transferir este instrumento de pago al módulo 10.

Para este propósito, instala una aplicación dedicada en su ordenador e introduce los datos de identificación vinculados a esta tarjeta de pago. También debe poner la tarjeta y entonces su módulo 10 (llevado puesto en la muñeca) dentro del alcance del lector de NFC de la base 20. Después de estas comprobaciones, el programa carga los datos de la tarjeta de pago en la memoria segura del módulo 10.

Entonces, cuando el usuario quiere hacer un pago, lleva el conjunto 70 que lleva puesto en su muñeca cerca de un terminal de pago de NFC para realizar la transacción, por ejemplo, con un débito automático para un pago pequeño o la necesidad de validar el transacción a través de la interfaz del módulo 10 (botón o pantalla táctil) para un pago mayor.

Naturalmente, todas las funcionalidades están inactivadas (inactivación de la unidad 102 central) cuando el conjunto de módulo/correa no se lleva puesto por el usuario y, cuando está implicada la base 20, cuando no se logra la asociación módulo/base (véase anteriormente).

7) Uso

a) *Configuración*

Para configurar el sistema, se sugiere al usuario colocar el módulo en la correa (a menos que ya formen un todo – el conjunto 70 – desde el comienzo) y colocar el conjunto en su muñeca.

El módulo se inicia y detecta si necesita los parámetros fisiológicos correspondientes a la muñeca del usuario (temperatura, frecuencia cardíaca, conductividad de la piel) y entra en modo de inicialización.

En paralelo, la base se conecta a una fuente de alimentación.

Según una realización, el usuario, colocando su dedo sobre la base 20, causa entonces una transmisión de la señal de validación de presencia, tal como una señal modulada transportada a través de la piel entre el dedo y la muñeca a través de un transmisor de la base 20 sobre la cual se coloca el dedo del usuario y a través del sensor del módulo 10, ubicado en sí mismo en la muñeca del usuario. La comparación entre las señales transmitidas y medidas, cuando da como resultado una coincidencia entre las señales, desencadena la lectura de su huella dactilar o de su red venosa, y la imagen digital correspondiente se transmite al módulo a través de los circuitos de comunicación inalámbrica para ser almacenada en el mismo. El módulo 10 entonces conmuta al estado activo.

b) *Espera activa y reactivación*

Llevar el módulo 10 al modo de espera activa o inactivo por el usuario se realiza simplemente retirando el conjunto 70, por ejemplo, durante la noche. Esto implica la posibilidad de reactivarlo. El usuario usa la base 20 con este propósito. Coloca el conjunto en su muñeca y causa una transmisión de la señal de validación de presencia y una medición de esta señal, una comparación de las señales transmitidas y medidas y entonces, en caso de

coincidencia, una lectura de su huella dactilar en la base 2. Se envía al módulo 10 a través de los circuitos de comunicación inalámbrica. Si ésta coincide con el perfil de huella dactilar almacenado, el módulo 10 se activa. De otro modo, no pasa nada.

c) *Copia de seguridad de datos*

En caso de pérdida, robo o mal funcionamiento del módulo 10, el usuario debe tener derecho a continuar accediendo a los servicios.

Para este fin, la base 20 tiene un controlador de unidad de memoria (por ejemplo, en forma de una memoria USB). Tras cada reactivación, los datos contenidos en la memoria segura del módulo 10 se almacenan en forma cifrada en esta unidad de memoria (incluyendo el perfil de huella dactilar asociado). El usuario puede realizar tantas copias de seguridad como desee (a través de tantas reactivaciones). Para restaurar estos datos, el usuario sólo necesita inicializar un nuevo módulo 10 con su huella dactilar. Si hay una coincidencia con el perfil de huella dactilar almacenado en la unidad de memoria, los datos de esta unidad se descifrarán y transferirán a la memoria segura del nuevo módulo. El usuario puede usar de nuevo los servicios.

d) *Usos fraudulentos*

Para impedir el uso fraudulento de una unidad 10 perdida o robada, siguiendo a esta restauración de servicios, cada identidad almacenada se etiqueta como una identidad “recuperada”. Durante una identificación, la miniaplicación del sitio web visitado será informada de este estado. Entonces será capaz de proporcionar una nueva identidad para su almacenamiento en la memoria segura del módulo, y revocar la identidad previa.

Esta funcionalidad es posible, por supuesto, solamente con identificaciones hechas en sitios que tienen la miniaplicación compatible. Para los otros identificadores almacenados, el usuario posiblemente tendrá un software que le permita ser guiado para sustituir manualmente sus contraseñas corruptas.

En caso de pérdida, robo o mal funcionamiento de la base, se puede sustituir con una nueva base sin dificultad, al menos con respecto a la realización donde no contiene ningún dato.

8) Variantes de parámetros biológicos/biométricos

Como recordatorio de las posibilidades descritas anteriormente y además de las mismas, el sistema puede implicar una o más de las siguientes mediciones:

- conductividad de la piel: la conductividad se mide a intervalos regulares. Una discontinuidad se considera una condición anormal;

- temperatura y proximidad: un sensor de infrarrojos mide a intervalos regulares la proximidad y la temperatura del usuario. Una discontinuidad también se identificará como una condición anormal;

- frecuencia cardíaca: un sensor mide la frecuencia cardíaca del usuario. Una pérdida de información se percibirá como una condición anormal.

Además, con el fin de evitar falsos positivos, se puede implementar un programa para controlar la coincidencia de dos o más de estas condiciones anormales para indicar al controlador 102 si debe conmutar al modo inactivo.

9) Realización alternativa

a) *Medios de recepción de señal de validación del módulo*

Según otra realización, el módulo 10 de autenticación de personas puede incluir, alternativamente o además de los medios de transmisión y/o recepción de señal de validación de presencia descritos anteriormente, medios que forman segundos medios de señales de validación de presencia del cuerpo del portador.

En particular, el módulo 10 se puede configurar de modo que los medios de validación de presencia puedan incluir estos segundos medios para recibir señales de validación de presencia del cuerpo del portador.

Los segundos medios para recibir señales de validación de presencia se pueden configurar de modo que las señales de validación de presencia sean distintas de las señales transmitidas y/o recibidas por el circuito de comunicación inalámbrica cuando se comunica con la base según un protocolo que implica datos biométricos.

Estos segundos medios de recepción de señales de presencia pueden ser de esta manera distintos de dicho circuito 110 de comunicación.

b) *Medios para recibir señales de validación de presencia en la base*

Además, la base 20 también puede comprender, alternativamente o además de los medios para transmisión de las señales de validación de presencia a dicho módulo y/o para recibir señales de validación descritas anteriormente,

segundos medios para recibir señales de validación de presencia del cuerpo del portador.

En particular, la base 20 se puede configurar de modo que los medios de validación de presencia puedan incluir estos segundos medios para recibir señales de validación de presencia del cuerpo del portador.

Los segundos medios para recibir señales de validación de presencia se pueden configurar de modo que las señales de validación de presencia sean distintas de las señales transmitidas y/o recibidas por el circuito 206 de comunicación inalámbrica cuando se comunica con el módulo 10 según un protocolo que implica datos biométricos.

Estos segundos medios para recibir señales de presencia de esta manera pueden ser distintos de dicho circuito 110 de comunicación.

Los segundos medios para recibir señales de validación de presencia en el módulo 10 y/o la base 20 pueden, por ejemplo, comprender o estar formados cada uno por un sensor de señales de validación de presencia, por ejemplo un sensor de una señal fisiológica del portador.

c) *Medios de comparación de señales*

Los medios de validación de presencia en el módulo 10 y/o la base 20 pueden incluir medios de comparación de señales para habilitar permitir la validación de la presencia del portador y/o del módulo 10 cerca de la base 20.

En realidad, el módulo 10 y la base 20 pueden recibir señales a través de sus segundos medios de recepción. Estas señales entonces se pueden comparar por los medios de comparación para validar la presencia del portador y del módulo 10 cerca de la base 20.

Si las señales son idénticas, o lo suficientemente similares, uno puede considerar de esta manera que la persona es en realidad la que lleva puesta el módulo 10, y permitir el acceso a la base 20 o la activación del módulo 10 por la base 20.

Según una realización, la persona en juego es la persona cuyos datos biométricos coinciden con los datos biométricos grabados en la memoria del módulo 10, tal comparación habiendo sido permitida por el circuito o los circuitos de comunicaciones inalámbricas.

Según esta realización, es posible de esta manera comprobar que la persona autenticada por sus datos biométricos, siendo la autenticación permitida por el circuito o los circuitos de comunicaciones inalámbricas de formación de los medios de comunicaciones inalámbricas, es en realidad el que lleva puesto el módulo 10.

En realidad, la medición del parámetro biométrico de los datos biométricos se puede seleccionar y realizar por la base, y la medición de validación de presencia se puede seleccionar y realizar de modo que la persona que es autenticada por sus datos biométricos es la que intenta validar su presencia.

Por ejemplo, los datos biométricos pueden ser una huella dactilar y la validación de presencia una medición de la frecuencia cardíaca por el módulo y la base simultáneamente con propósitos de comparación, de modo que la frecuencia cardíaca se mide por la base en el dedo presentado para la medición de la huella dactilar por la base.

En una realización particular, la persona en juego es una persona en las inmediaciones de la base 20.

Por ejemplo, las señales recibidas por el módulo 10 se pueden transmitir al módulo 20, o viceversa. La transmisión/recepción se puede lograr por medio de la comunicación inalámbrica descrita anteriormente, por ejemplo, según el protocolo que implica los datos biométricos o según un protocolo diferente.

Los medios de comparación de señales pueden, por ejemplo, comprender o estar formados por un dispositivo de comparación de señales, por ejemplo, un circuito electrónico que permita tal comparación.

d) *Medios para controlar el tipo de señal*

Los medios de validación de presencia del módulo 10 y/o la base 20 pueden incluir medios para controlar el tipo de señales recibidas por los segundos medios de recepción de señales de validación de presencia del módulo 10 y/o la base 20.

Antes o después de que se comparen las señales, las señales obtenidas de las mediciones realizadas simultáneamente por los segundos medios de recepción de señales de validación de presencia del módulo 10 y la base 20 se pueden someter a un paso de comprobación para verificar que corresponden a la señal de validación de presencia del portador.

Por ejemplo, la señal esperada puede ser el pulso cardíaco del portador y los medios de validación de presencia del módulo 10 y/o la base pueden verificar que las mediciones hechas corresponden a un pulso cardíaco.

En otro ejemplo, se puede lograr una medición de la conductividad de la piel tanto en el módulo 10 como en la base 20 mediante los segundos medios de validación de presencia, siendo las dos señales comparadas entonces o bien

en la base 20, después de transmitir a la base, por ejemplo, a través del circuito de comunicación inalámbrica que forma los medios de comunicación inalámbrica, las señales recogidas en el módulo, o en el módulo 10, después de transmitir al módulo, por ejemplo, a través del circuito de comunicación inalámbrica formando los medios de comunicación inalámbrica, las señales recogidas en la base.

Es posible, de esta manera, en particular, evitar que las señales correspondientes a un módulo que no está en contacto con un portador y con una base a la que el portador no se haya introducido a sí mismo, por ejemplo, señales nulas idénticas, se comparan y/o permiten validar erróneamente la presencia de un portador.

Los medios para verificar el tipo de señales recibidas pueden, por ejemplo, incluir o estar formados por un dispositivo para verificar el tipo de las señales recibidas, por ejemplo, un circuito electrónico que permita tal verificación.

Por supuesto, la presente invención no está limitada a las realizaciones descritas y mostradas, y los expertos serán capaces de llevar a la misma muchas variantes y modificaciones con su conocimiento general.

REIVINDICACIONES

1. Una combinación de un conjunto de un módulo (10) para autenticar a un portador y un soporte para el módulo, en forma de una correa (40), y una base (20), comprendiendo la combinación las siguientes características:

- un circuito (102) de procesamiento proporcionado en el módulo y comprendiendo una memoria (104) de autenticación,

- medios (402) conectados al módulo (10) para detectar la apertura de la correa (40),

- un medio (108) para inactivar el circuito (102) de procesamiento cuando los medios de detección de apertura detectan una apertura de la correa, siendo este medio proporcionado en el módulo,

- un sensor (106) de un parámetro fisiológico del portador proporcionado en el módulo,

- un sensor del mismo parámetro fisiológico proporcionado en la base,

- medios (208) para adquirir y almacenar datos biométricos de un portador del módulo (10), distintos de dicho parámetro fisiológico, siendo estos medios proporcionados en la base,

- medios (504) para comparar los datos biométricos adquiridos por la base (20) con los datos biométricos de referencia contenidos en la memoria de autenticación,

- circuitos (110) para comunicaciones inalámbricas de campo cercano provistas en el módulo y en la base (20) y controladas por medios de control, capaces de permitir que el módulo y la base se comuniquen según un protocolo que permita transmitir o recibir los datos biométricos,

- medios para validar la presencia del portador en base a señales de validación de presencia constituidas por el parámetro fisiológico proporcionado por dicho sensor del módulo y proporcionado por el sensor de la base, capaces de autorizar al módulo o la base para acceder a los datos biométricos solamente en caso de validación, y

- medios (202) para interconectar la base (20) con un dispositivo digital personal.

2. Una combinación según la reivindicación 1, en donde las señales de validación de presencia comprenden una señal de temperatura corporal o una señal de frecuencia cardíaca o una señal de conductividad de la piel.

3. Una combinación según la reivindicación 1 o 2, en donde los datos biométricos son datos de huellas dactilares.

4. Una combinación según la reivindicación 1 o 2, en donde los datos biométricos son datos de la red venosa, en particular datos de la red venosa palmar.

5. Una combinación según una cualquiera de las reivindicaciones 1 a 4, comprendiendo además medios (502) para autorizar al módulo (10) o la base (20) para acceder a los datos biométricos solamente cuando las señales de validación de presencia transmitidas por dicho módulo (10) son detectadas válidamente por dicha base (20).

6. Una combinación según una cualquiera de las reivindicaciones 1 a 4, comprendiendo además medios (502') para autorizar al módulo (10) o la base (20) para acceder a los datos biométricos solamente cuando las señales de validación de presencia transmitidas por dicha base (20) son detectadas válidamente por dicho módulo (10).

7. Una combinación según una cualquiera de las reivindicaciones 1 a 6, en donde los medios (504) de comparación están situados en el módulo, los datos biométricos adquiridos por la base (20) siendo transmitidos al módulo (10) a través de los circuitos (206) de comunicación inalámbrica de campo cercano.

8. Una combinación según una cualquiera de las reivindicaciones 1 a 6, en donde los medios (504) de comparación están situados en la base, siendo los datos biométricos de referencia transmitidos a la base (20) a través de los circuitos (206) de comunicación inalámbrica de campo cercano.

9. Una combinación según una cualquiera de las reivindicaciones 1 a 8, en donde la memoria (104) de autenticación del módulo (10) es capaz de almacenar conjuntos de datos de autenticación capaces de ser comunicados a dicha base (20) a través de los circuitos (206) de comunicación inalámbrica de campo cercano con el propósito de transacciones con dispositivos digitales conectados a dicha base (20).

10. Una combinación de un conjunto de un módulo (10) para autenticar a un portador y un soporte para el módulo, en forma de una correa (40), y una base (20), la combinación que comprende las siguientes características:

- un circuito (102) de procesamiento proporcionado en el módulo y comprendiendo una memoria de autenticación (104),

- un sensor (106) de un parámetro fisiológico del portador, proporcionado en el módulo,

- un medio (108) para inactivar el circuito (102) sensible a dicho sensor (106) y capaz de inactivar el circuito (102) cuando dicho sensor no recibe una señal fisiológica esperada, este medio que se proporciona en el módulo,

- medios (208) para adquirir y almacenar datos biométricos de un portador del módulo (10), distintos de dicho parámetro fisiológico, siendo estos medios proporcionados en la base,

- medios (504) para comparar los datos biométricos adquiridos por la base (20) con los datos biométricos de referencia contenidos en la memoria de autenticación,

- circuitos (110) para comunicaciones inalámbricas de campo cercano proporcionadas en el módulo y en la base (20) y controlados por medios de control, capaces de permitir que el módulo y la base se comuniquen según un protocolo que permita transmitir o recibir los datos biométricos,

- medios para validar la presencia del portador en base a las señales de validación de presencia transmitidas por el módulo a la base o transmitidas por la base al módulo de una manera distinta de dichos circuitos (110) de comunicación, capaces de autorizar al módulo o a la base para acceder a los datos biométricos solamente en caso de validación, y

- medios (202) para interconectar la base (20) con un dispositivo digital personal.

11. Una combinación según la reivindicación 10, en donde las señales de validación son señales acústicas capaces de ser conducidas por el cuerpo del portador, o señales eléctricas capaces de ser conducidas por el cuerpo del portador, o señales ópticas.

12. Una combinación según la reivindicación 11, en donde los medios (208) de adquisición de datos biométricos implican un contacto con el cuerpo de un portador, y las señales de validación de presencia destinadas a dicho módulo y/o que se originan desde dicho módulo (10) son señales acústicas o eléctricas.

13. Una combinación según la reivindicación 12, en donde los datos biométricos son datos de huellas dactilares.

14. Una combinación según la reivindicación 11, en donde los medios (208) de adquisición de datos biométricos operan sin contacto con el cuerpo de un portador, y en donde los medios (210) para transmitir y/o recibir señales de validación de presencia comprenden medios para transmitir y/o detectar señales ópticas.

15. Una combinación según la reivindicación 14, en donde las señales ópticas comprenden una señal óptica modulada y/o un patrón gráfico.

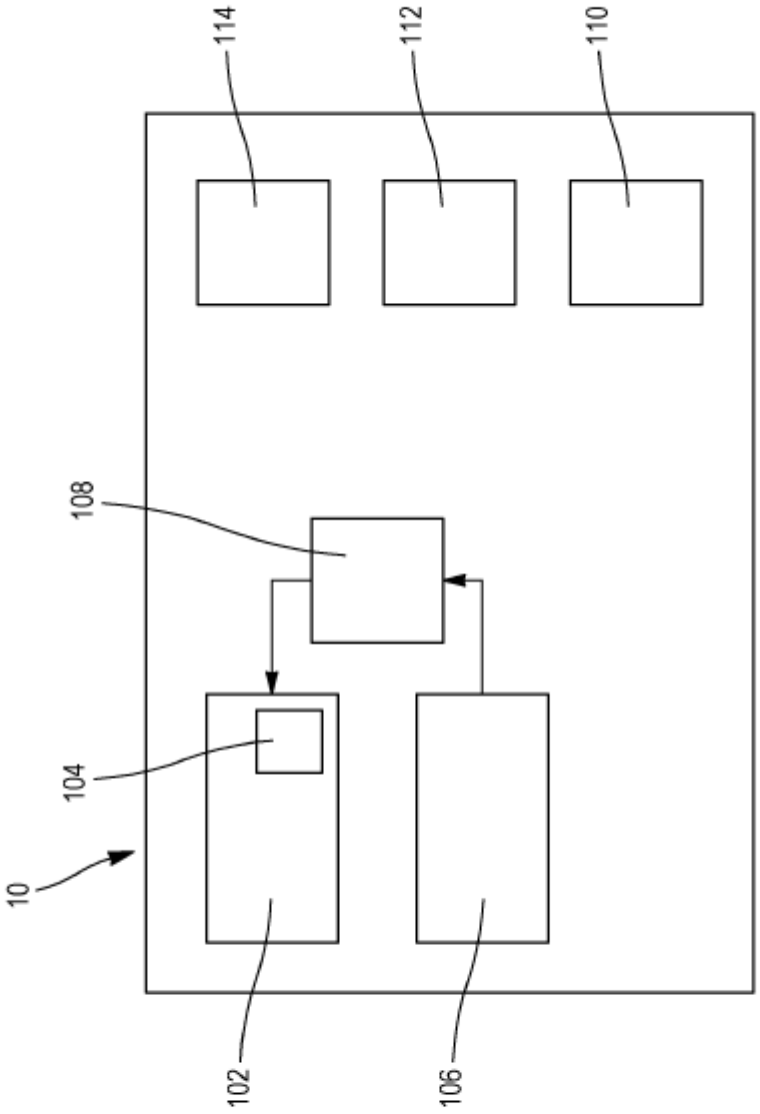

FIG. 1a

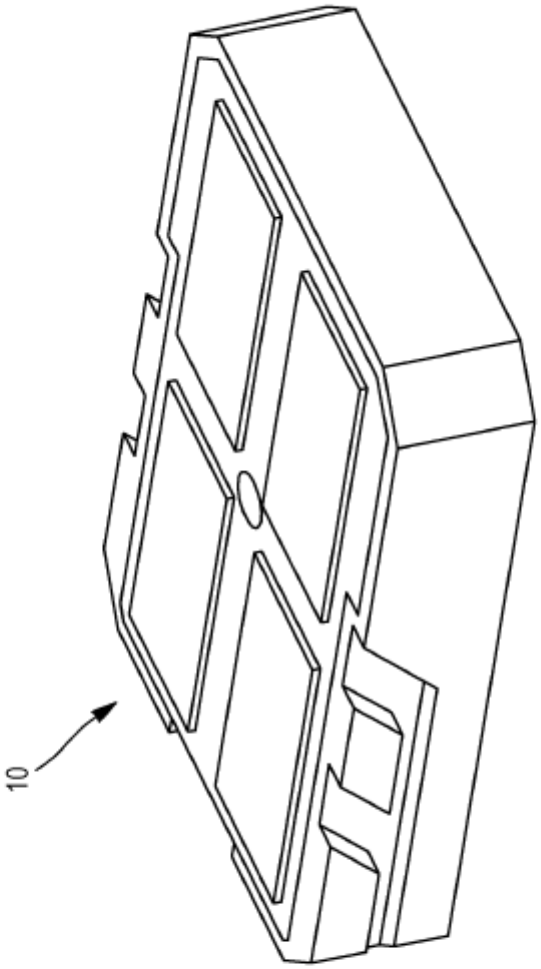

FIG. 1b

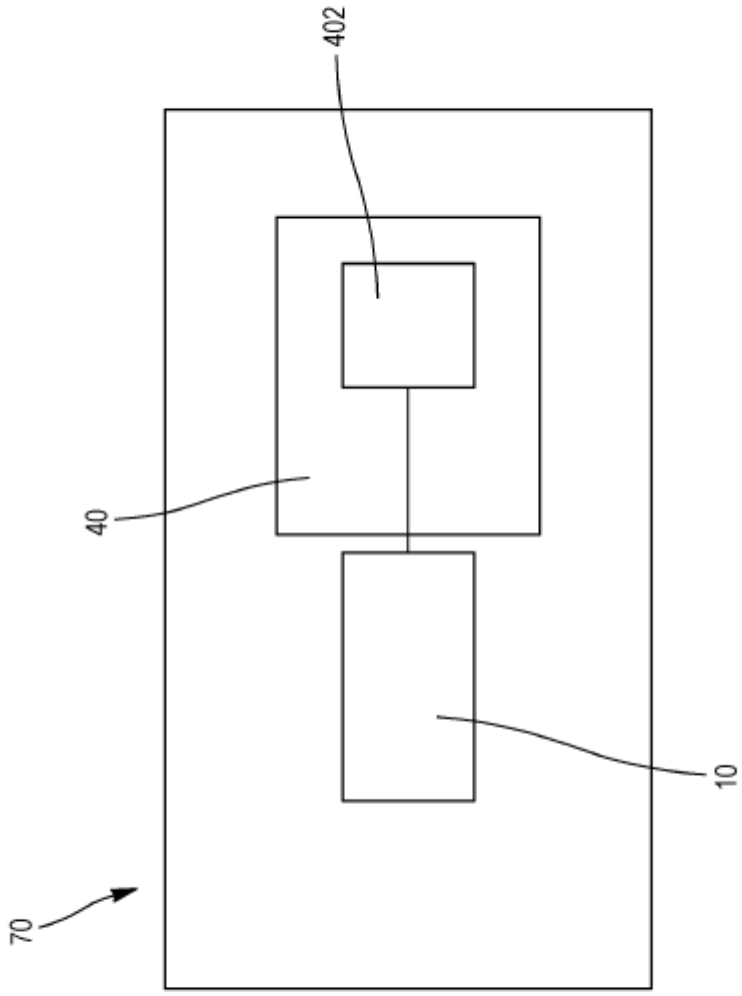

FIG. 2a

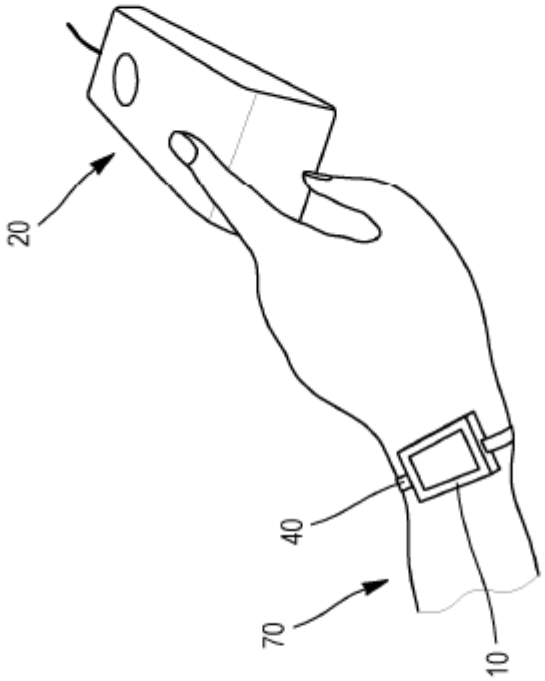

FIG. 2b

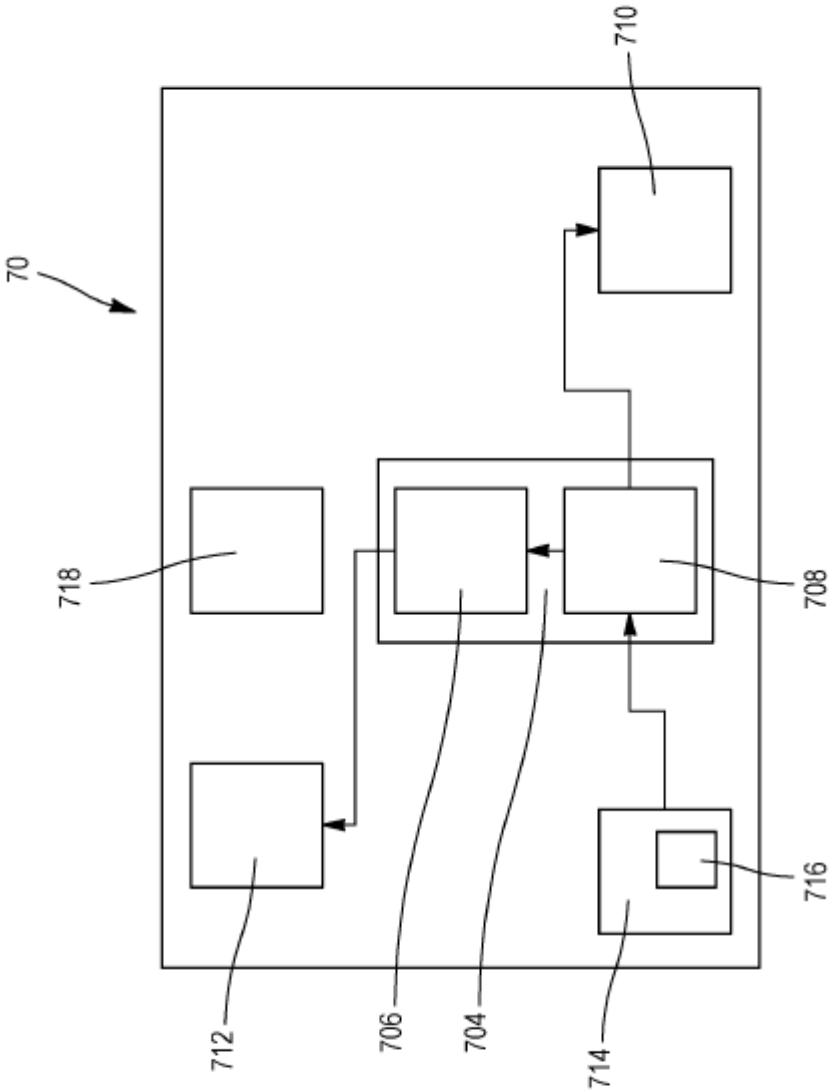

FIG. 3

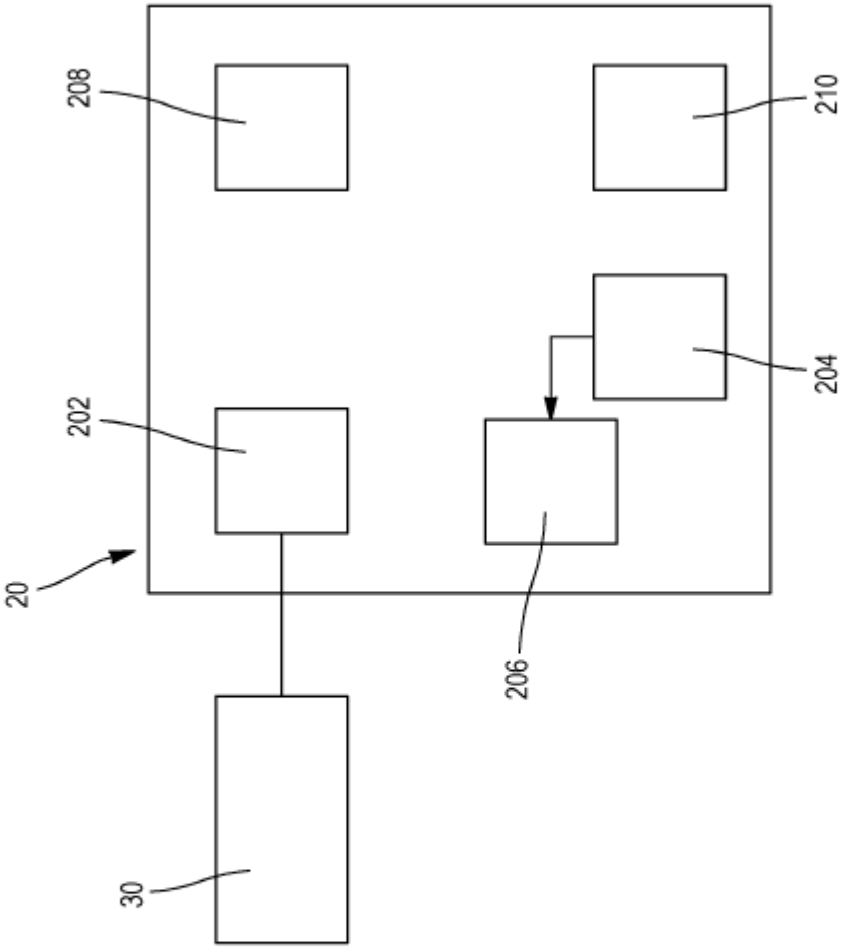

FIG. 4

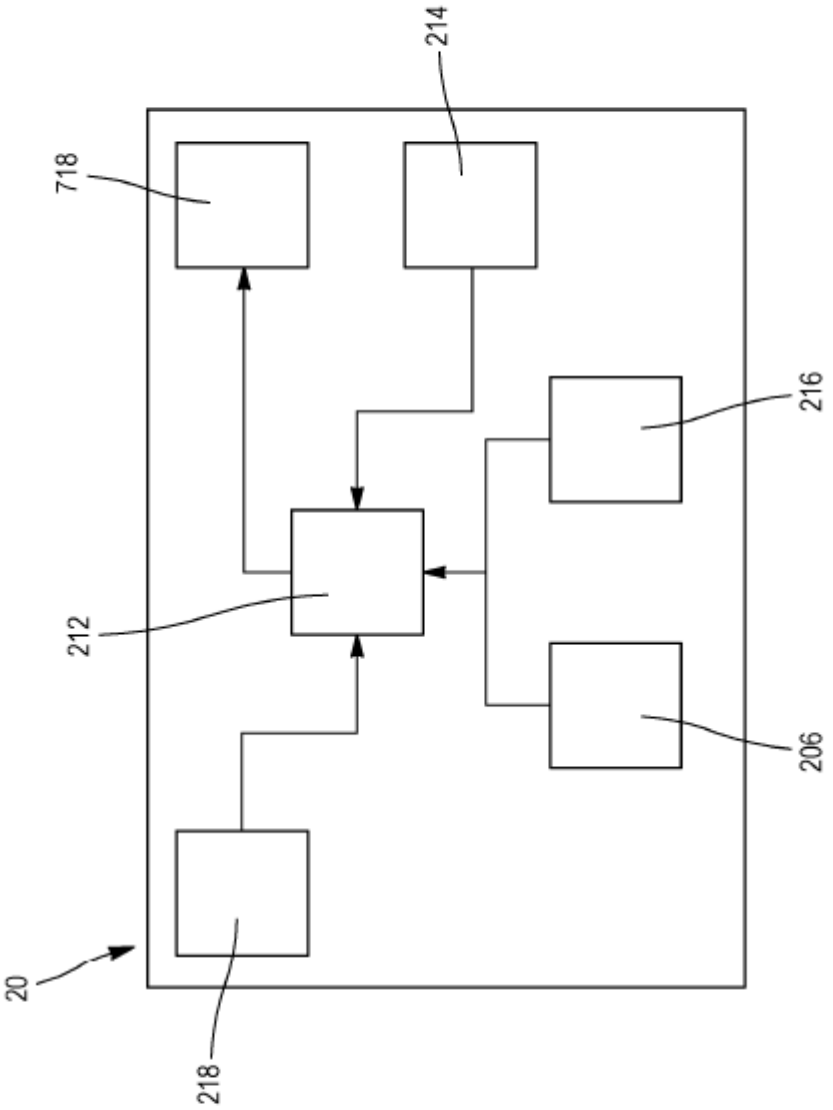

FIG. 5

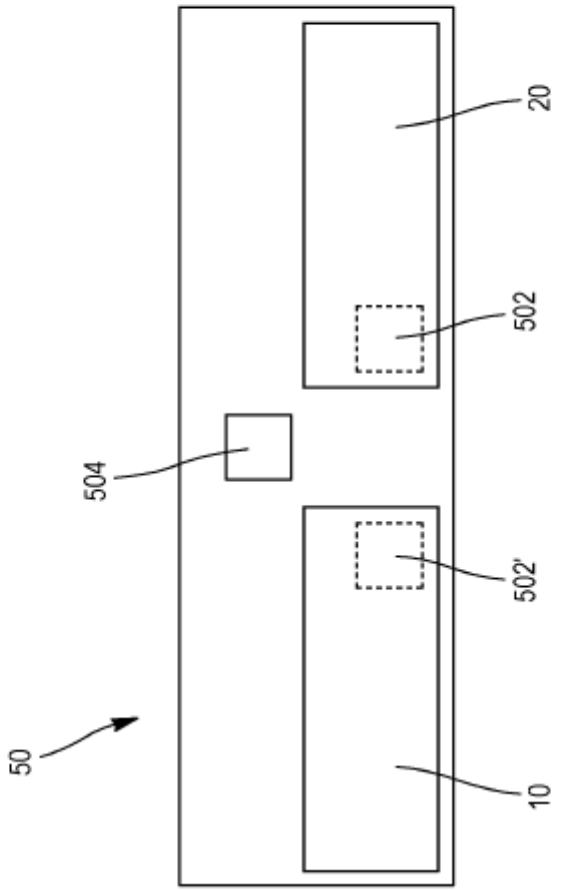

FIG. 6