(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 817 795**

(51) Int. CI.:

G06F 21/32 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2010 PCT/FR2010/052767**

(87) Fecha y número de publicación internacional: **14.07.2011 WO11083241**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2010 E 10810772 (3)**

(97) Fecha y número de publicación de la concesión europea: **24.06.2020 EP 2517141**

(54) Título: **Tarjeta inteligente multiaplicativa con validación biométrica**

(30) Prioridad:

22.12.2009 FR 0959414

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2021

(73) Titular/es:

MEREAL BIOMETRICS (100.0%)
141 bis rue de Saussure
75017 Paris, FR

(72) Inventor/es:

PARTOUCHE, PATRICK;
BLOT, PHILIPPE y
MOBETIE, DIDIER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Tarjeta inteligente multiaplicativa con validación biométrica

La presente invención concierne al ámbito técnico de los dispositivos de acceso seguro o de comunicación segura. La misma encuentra una aplicación particularmente interesante, pero no exclusivamente, en la tecnología de las tarjetas inteligentes con o sin contacto tales como las tarjetas inteligentes RFID (Identificación por Radio Frecuencia o « Radio Frequency Identification » en inglés). La invención concierne especialmente a una tarjeta inteligente sin contacto de tipo NFC, Mifare, ISO 14443 o 15693, es decir que tiene una antena RF y que emite cuando se encuentra en un campo electromagnético apropiado.

De modo general, una tarjeta inteligente comprende uno (o varios) chips electrónicos de silicio que contienen informaciones más o menos sensibles y relativas al portador de la tarjeta. A modo de ejemplo, en la tecnología RFID, el chip está generalmente conectado a una antena. Una tarjeta RFID puede tener el formato de una tarjeta inteligente clásica, pero igualmente puede revestir diferentes formas tales como una placa, una etiqueta (« tag »), un portallaves u otro,... Puede estar prevista una batería integrada con el fin de extender las funcionalidades de la tarjeta.

La tecnología RFID, basada en el principio de inducción electromagnética, está cada vez más expandida en la vida cotidiana. Esta tecnología, utilizada inicialmente para la gestión de stocks, se ha expandido masivamente en el ámbito del control de accesos. La misma está en pleno auge en el ámbito de los pasaportes y del pago. En Japón por ejemplo, es muy utilizada como medio de pago por el protocolo Felica. En los Estados Unidos de Norteamérica, se han desplegado los primeros terminales de pago basados en el protocolo ISO14443A. El despliegue en Francia está en curso actualmente.

Desgraciadamente, el entusiasmo por esta tecnología se hace en detrimento del aspecto de la seguridad. En efecto, una persona malintencionada puede acceder libremente a las informaciones contenidas en un chip RFID. Y la entidad que dispone de un lector RFID no está segura de que el poseedor de la tarjeta RFID es la persona cuyos datos confidenciales están almacenados en la tarjeta.

Se conocen sistemas que permiten autenticar a una persona utilizando un circuito biométrico.

Se conoce el documento US20070016940 que describe una tarjeta dotada de un circuito biométrico para identificar al portador de la tarjeta y de medios de control de acceso por contraseña. El documento WO03084124 describe una tarjeta inteligente dotada de un circuito biométrico para autenticar al usuario y de un botón de selección para seleccionar sus contenidos en la tarjeta; permitiendo un circuito RFID la comunicación con el exterior. El documento US20080234985 describe un circuito con detectores.

La presente invención tiene por objetivo una solución alternativa a las soluciones existentes de aseguramiento de datos contenidos en una tarjeta.

La presente invención es de un ámbito más amplio puesto que la misma tiene por objetivo una nueva tarjeta inteligente capaz de integrar numerosas funcionalidades. La presente invención aspira a tener numerosas aplicaciones en la tecnología inalámbrica y/o con contacto.

Otro objetivo de la invención es un dispositivo enriquecido capaz de tener en cuenta el entorno en el cual se encuentra el mismo.

Al menos uno de los objetivos antes citados se consigue con un dispositivo de comunicación inalámbrica, que comprende:

- una pluralidad de circuitos aplicativos que están asociados cada uno al menos a un servicio aplicativo contenido de modo seguro en el seno del dispositivo, siendo cada circuito aplicativo apto para ser excitado por una señal externa,

- una unidad de control:

- para identificar un circuito aplicativo excitado,

- para identificar un servicio aplicativo asociado a un circuito aplicativo excitado, y

- para activar el citado servicio aplicativo excitado en respuesta a una autorización de activación, y

- un circuito biométrico para autenticar al usuario de modo que genere la citada autorización de activación.

Un servicio aplicativo puede comprender una aplicación informática que se ejecuta cuando se activa este servicio aplicativo.

La activación de un servicio aplicativo consiste especialmente en hacerle accesible desde el exterior, ejecutar un algoritmo o bien desbloquear una aplicación o datos.

Con el dispositivo según la invención, se realiza una doble verificación antes de activar un servicio aplicativo. La primera verificación es ambiental puesto que se trata de detectar una señal que viene del entorno exterior. La segunda verificación es biométrica. Se dispone así de un sistema seguro, inteligente y económico en energía. El dispositivo según la invención es inteligente porque es autoadaptativo. El mismo es capaz de reconocer el entorno en el cual es utilizado y activar el mecanismo de reconocimiento biométrico que autorizará o no el servicio aplicativo correspondiente. El dispositivo según la invención tiene múltiples aplicaciones y puede elegir de modo automático el servicio aplicativo adecuado.

El dispositivo según la invención determina la acción o el canal de comunicación adaptado frente a un estímulo y hace validar la activación por el portador del dispositivo gracias a su firma biométrica.

Según una característica ventajosa de la invención, los circuitos aplicativos comprenden un emisor-receptor de señales de radiofrecuencia. Puede tratarse de una antena de radiofrecuencia.

El servicio aplicativo que es activado puede ser cualquier tipo de aplicación que utilice una antena de radiofrecuencia. Se puede utilizar una señal de radiofrecuencia por ejemplo para abrir una puerta en hoteles u otros, o activar una máquina tragamonedas. La unidad de control puede comprender un chip de tipo chip RFID.

Según la invención, estos circuitos aplicativos pueden comprender al menos un conector metálico para comunicación con un lector por ejemplo.

Ventajosamente, los circuitos aplicativos comprenden al menos un detector ambiental. Este detector ambiental puede ser uno de los elementos siguientes:

- un detector acústico
- un detector térmico,
- un detector olfativo,
- un fotodetector,
- un detector de presión, y
- un acelerómetro.

En particular estos detectores pueden ser realizados utilizando sensores MEMS.

Se puede prever que la unidad de control identifique un circuito aplicativo excitado solo cuando la excitación llegue a un umbral predeterminado. Su puede considerar también el hecho de que la señal externa de excitación esté codificada de modo que la unidad de control solamente considera la excitación después de análisis del código. Este código puede igualmente servir para identificar un servicio aplicativo entre varios servicios aplicativos posibles. Este código puede manifestarse especialmente en forma de una melodía particular en el ámbito de un detector acústico, de una onda o frecuencia de señal luminosa particular en el caso del fotodetector, de una señal RFID codificada, y así sucesivamente.

Preferentemente, el circuito biométrico comprende un sensor biométrico asociado a una unidad de cálculo para tratar datos biométricos. Los datos de identificación de uno o varios usuarios pueden ser almacenados en la unidad de cálculo o en una memoria asociada en el transcurso de una etapa de inscripción. En funcionamiento, a cada solicitud del circuito biométrico, el usuario interacciona con el sensor biométrico el cual transmite los datos detectados hacia la unidad de cálculo para una comparación y una autenticación.

El circuito biométrico puede así generar directamente la autorización de activación. Pero, cuando el circuito biométrico no comprende una unidad de cálculo, la comparación puede hacerse en el seno de la unidad de control.

Ventajosamente, el dispositivo según la invención comprende una interfaz hombre-máquina para indicar un estado de funcionamiento. Puede tratarse de indicadores sonoros para emitir un sonido particular, una voz o música a partir de un elemento piezoeléctrico. Puede tratarse de indicadores visuales que comprendan DELS, diodos electroluminiscentes. La interfaz hombre-máquina puede igualmente proponer por ejemplo una pantalla de visualización, un teclado, un micrófono y altavoces, para acceder a la unidad de control.

El dispositivo según la invención puede ser alimentado por una batería integrada o preferentemente una pila que sea flexible o no, recargable o no. Se puede considerar por ejemplo un sensor solar para recargar una pila fotovoltaica integrada en el dispositivo. Dicho de otro modo, se puede utilizar una alimentación por una fuente externa, especialmente cuando se utilicen dispositivos poco móviles.

Preferentemente, el dispositivo es un elemento portátil en un formato de tarjeta inteligente, de llave USB, o de etiqueta electrónica.

Según otro aspecto de la invención, se propone un procedimiento puesto en práctica en una tarjeta de comunicación inalámbrica que comprende una pluralidad de circuitos aplicativos, una unidad de control y un circuito biométrico; comprendiendo este procedimiento las etapas siguientes:

se detecta una señal externa de excitación por medio de uno de los circuitos aplicativos, estando asociado cada circuito aplicativo al menos a un servicio aplicativo contenido de modo seguro en el seno de la tarjeta,

en el seno de la unidad de control, se identifica el circuito aplicativo excitado y el servicio aplicativo asociado a este circuito aplicativo excitado, y se inicia un proceso de autenticación por comparación biométrica en el seno del circuito biométrico, y después se activa el citado servicio aplicativo excitado en respuesta a una autorización de activación que proviene del circuito biométrico.

Naturalmente, las diferentes características, formas y variantes de realización de la invención pueden ser asociadas una a otra según diversas combinaciones en la medida en que las mismas no sean incompatibles o exclusivas una de otra.

Por otra parte, otras diversas características de la invención se deducirán de la descripción que sigue efectuada en referencia a los dibujos anejos, los cuales ilustran formas no limitativas de realización de una tarjeta inteligente RFID autoadaptativa que integra un circuito biométrico.

Las Figuras 1 a 4 son esquemas simplificados que ilustran el principio general de puesta en práctica de un dispositivo según la invención,

Las Figuras 5 a 8 son sistemas simplificados que ilustran un modo de puesta en práctica del dispositivo según la invención aplicado a un circuito RFID,

La Figura 9 es una vista general de una tarjeta inteligente según la invención.

En las Figuras 1-9, los diferentes elementos comunes a las diversas variantes o formas de realización llevan las mismas referencias.

El principio de una tarjeta autoadaptativa según la invención está ilustrado esquemáticamente en las Figuras 1 a 4, en las cuales se distingue una tarjeta inteligente 1 que comprende por una parte un conjunto de circuitos aplicativos 2 a 4 y, por otra, un circuito biométrico 5.

La tarjeta inteligente 1 puede comprender numerosos circuitos aplicativos, aquí solo están representados tres de ellos. Las referencias 2 a 4 representan respectivamente los circuitos aplicativos n-1, n y n+1. Un circuito aplicativo puede estar constituido por un emisor-receptor asociado a un servicio aplicativo. Cada circuito aplicativo es sensible a un fenómeno físico dado que caracteriza el entorno en el cual se encuentra la tarjeta. Estos fenómenos físicos pueden comprender el térmico, el tacto (contacto), la luz, el olfativo, el acústico, la presión, el campo electromagnético,… Cuando la tarjeta está inmersa en un entorno « n », el circuito aplicativo n detecta la presencia de este entorno que le está directamente asociado, pero no activa el servicio aplicativo n correspondiente. Este servicio aplicativo puede ser un protocolo de intercambio con este entorno « n » o la ejecución de un programa particular.

Los otros circuitos aplicativos n-1 y n+1 permanecen insensibles: el entorno « n » no es reconocido por estos circuitos aplicativos.

A continuación se transmite una solicitud de autorización hacia el circuito biométrico 5 como se ve en la Figura 2. Desde la recepción de esta solicitud de autorización, el circuito biométrico inicia el proceso de autenticación con objeto de reconocer e identificar al usuario de la tarjeta. Para hacer esto, el circuito biométrico comprende un sensor biométrico que puede ser de diferentes tipos: por análisis de características físicas (huella digital, imagen del iris, imagen de la retina,…), por análisis de comportamiento (análisis vocal, firma,…).

El usuario debe entonces someterse a la detección biométrica de modo que el circuito biométrico recupere datos que son comparados después con datos contenidos en la tarjeta. Cuando la comparación es satisfactoria, el reconocimiento biométrico es entonces positivo y se envía una señal de acuerdo para activar el servicio aplicativo n como se ve en la Figura 3. Una vez activado el servicio aplicativo, el circuito aplicativo n puede interactuar con el entorno como se ve en la Figura 4.

En las Figuras 5 a 8, se ve un ejemplo de realización de un dispositivo según la invención. La tarjeta sigue estando designada por la referencia 1. Los circuitos aplicativos 2 a 4 son respectivamente un circuito acústico, un circuito térmico y un circuito RFID.

En este ejemplo de realización, el entorno está representado por un lector RFID 6, el cual genera un campo electromagnético o campo RF hacia la tarjeta inteligente 1. El circuito RFID detecta este campo RF y transmite en la Figura 6 una solicitud de autorización hacia el circuito biométrico 5. Esta solicitud de autorización tiene por objetivo activar un servicio de comunicación RFID entre el circuito RFID 4 y el lector RFID 6. El circuito biométrico 5 autentica al usuario y después transmite una señal de acuerdo o de desacuerdo hacia el circuito RFID. En caso de acuerdo tal como está representado en la Figura 7, el circuito RFID activa el servicio de comunicación que permite especialmente

la transferencia de datos o de consigna hacia el lector RFID 6 como está ilustrado en la Figura 8. El lector RFID 6 puede estar asociado a una puerta, a una máquina tragamonedas o a cualquier otro sistema de modo que la recepción de una consigna que proviene de la tarjeta inteligente pueda provocar la apertura de la puerta, la activación de la máquina tragamonedas, la puesta en tensión o en vigilancia de un sistema,…

La consigna puede comprender datos personales del usuario así como instrucciones codificadas o no destinadas al lector RFID 6.

La señal del entorno detectado por un circuito aplicativo puede ser una señal codificada o no que permita especialmente distinguir qué servicio aplicativo necesita ser activado cuando por ejemplo varios servicios aplicativos son susceptibles de ser activados a través de este servicio aplicativo.

Se puede considerar que el servicio aplicativo activado lance una comunicación con una máquina tragamonedas por campo RF para por ejemplo acreditar una cuenta del usuario en la máquina tragamonedas o recuperar ganancias realizadas por el usuario, especialmente en tiempo real.

La Figura 9 es un esquema de bloques simplificado de un ejemplo de realización de una tarjeta inteligente según la invención. Se distingue un emisor-receptor acústico 7 asociado a un solo servicio aplicativo A1. El emisor receptor térmico 8 está asociado a un solo servicio aplicativo A2. El emisor-receptor RFID 9 está asociado a un solo servicio aplicativo A3. Se puede imaginar un sistema más complejo en el cual un emisor-receptor esté asociado a varios servicios aplicativos. Se puede incluso prever utilizar varias señales de excitación detectadas simultáneamente por varios emisores-receptores para determinar un servicio aplicativo adecuado para el entorno en curso.

Como está ilustrado en la Figura 9, en cada conexión entre el emisor-receptor y su servicio aplicativo asociado, se introduce respectivamente un interruptor controlado 11, 12 y 13, de modo que un servicio aplicativo solo se activa cuando el interruptor controlado asociado esté cerrado.

En la Figura 9 cada emisor-receptor 7, 8 y 9 está conectado a una unidad de control 10 la cual genera el conjunto de los componentes y programas informáticos de la tarjeta inteligente 1. La unidad de control 10 es un microcontrolador equipado:

- con una memoria flash que contiene las aplicaciones informáticas para su propio funcionamiento y destinadas a controlar el circuito biométrico 5,

- con una memoria RAM,

- con un reloj, y

- con varias entradas/salidas.

La misma está en forma de un chip integrado en la tarjeta y presenta un consumo reducido. La unidad de control 10 está configurada para cerrar uno de los interruptores 11, 12 y 13 en respuesta a un acuerdo de activación emitido por el circuito biométrico 5.

Una interfaz hombre-máquina IHM 17 comprende medios de visualización, de entrada, de difusión sonora y visual. La difusión visual puede hacerse a través de los diodos electroluminiscentes DELs. Una batería integrada 16 alimenta el conjunto de los componentes de la tarjeta 1.

El circuito biométrico 5 comprende un sensor biométrico 14 que se encarga de la entrada de datos biométricos brutos. Se utiliza un sensor de huella digital. El circuito biométrico 5 comprende igualmente una unidad de cálculo 15 capaz de tratar los datos biométricos con el fin de realizar la inscripción y las comparaciones de huellas.

La inscripción se desarrolla de la manera siguiente:

- el usuario activa la tarjeta a través del circuito de control,

- el circuito de control activa el circuito biométrico poniéndole en modo « inscripción »,

- el usuario coloca su dedo sobre el sensor de huella, el cual envía informaciones correspondientes hacia la unidad de cálculo, y

- cuando estas informaciones son transferidas a, y almacenadas en, la unidad de cálculo, la unidad de control informa al usuario que la inscripción se ha realizado bien a través de la interfaz IHM 17.

El funcionamiento de la tarjeta puede ser el siguiente. Cuando una señal de excitación es detectada por uno de los emisores-receptores 7, 8 o 9, por ejemplo el emisor-receptor 7, la unidad de control 10 es activada y se inicia un proceso de autenticación:

- el circuito de control activa el circuito biométrico poniéndole en modo « autenticación »,

- el usuario coloca su dedo sobre el sensor de huella, el cual envía informaciones correspondientes hacia la unidad de cálculo,

- la unidad de cálculo compara estas informaciones con informaciones previamente almacenadas durante la fase de inscripción, y

- después de la autenticación, la unidad de control informa al usuario del resultado y desactiva el circuito biométrico.

En caso de respuesta positiva (autenticación satisfactoria), la unidad de control cierra entonces el interruptor 11 de modo que permita la comunicación del servicio aplicativo A1 con el entorno exterior a través del emisor-receptor 7. Naturalmente, los interruptores controlados 11, 12 y 13 pueden ser realizados en forma informática, siendo obtenido el acceso a los servicios aplicativos después de la recepción de un acuerdo de autenticación.

Naturalmente, la invención no está limitada a los ejemplos que se acaban de describir y a estos ejemplos se pueden aportar numerosas disposiciones sin salirse del marco de la invención. El dispositivo puede aplicarse a diferentes ámbitos tales como:

El ámbito bancario,

La identificación de individuos,

El ámbito del juego,

La llave digital para apertura de puertas,

El ámbito del registro/lectura de mensajes,

La restitución de datos,

El ámbito médico por ejemplo para el análisis de sangre o del ADN.

REIVINDICACIONES

1. Dispositivo de comunicación de acceso seguro, que comprende:

- una pluralidad de circuitos aplicativos que están asociados cada uno al menos a un servicio aplicativo contenido de modo seguro en el seno del dispositivo, comprendiendo cada circuito aplicativo al menos un detector ambiental y siendo apto para ser excitado por una señal externa que caracteriza el entorno en el cual se encuentra el dispositivo, comprendiendo el dispositivo de comunicación un emisor-receptor de señales de radiofrecuencia para la comunicación con el exterior,

- una unidad de control que permite identificar el circuito aplicativo excitado y el servicio aplicativo asociado, y activar el citado servicio en respuesta a una autorización de activación, y

- un circuito biométrico para autenticar al usuario de modo que genere la citada autorización de activación; utilizando el servicio aplicativo asociado el citado emisor-receptor de señales de radiofrecuencia para comunicar con el exterior.

2. Dispositivo según una cualquiera de las reivindicaciones precedentes, caracterizado por que los circuitos aplicativos comprenden al menos uno de los elementos siguientes:

- un detector acústico;

- un detector térmico;

- un detector olfativo,

- un fotodetector;

- un detector de presión;

- un acelerómetro.

3. Dispositivo según una cualquiera de las reivindicaciones precedentes, caracterizado por que el circuito biométrico comprende un sensor biométrico asociado a una unidad de cálculo para tratar datos biométricos.

4. Dispositivo según una cualquiera de las reivindicaciones precedentes, caracterizado por que comprende una interfaz hombre-máquina para indicar un estado de funcionamiento del dispositivo o para acceder a la unidad de control.

5. Dispositivo según una cualquiera de las reivindicaciones precedentes, caracterizado por que es alimentado por una pila flexible o no, recargable o no.

6. Dispositivo según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que es alimentado por una fuente externa.

7. Dispositivo según una cualquiera de las reivindicaciones precedentes, caracterizado por que está en un formato de tarjeta inteligente, de llave USB, o de etiqueta electrónica.

8. Procedimiento de puesta en práctica en un dispositivo de comunicación de acceso seguro que comprende una pluralidad de circuitos aplicativos, una unidad de control y un circuito biométrico; comprendiendo este dispositivo, las etapas siguientes:

- detectar una señal externa de excitación por medio de uno de los circuitos aplicativos, comprendiendo cada circuito aplicativo al menos un detector ambiental y siendo apto para ser excitado por una señal externa, que caracteriza el entorno en el cual se encuentra el dispositivo, y estando asociado al menos a un servicio aplicativo contenido de modo seguro en el seno del dispositivo de comunicación de acceso seguro

- en el seno de la unidad de control, identificar el circuito aplicativo excitado y el servicio aplicativo asociado a este servicio aplicativo excitado, e iniciar un proceso de autenticación por comparación biométrica en el seno del circuito biométrico, y activar después el citado servicio aplicativo excitado en respuesta a una autorización de activación que proviene del circuito biométrico, estando asegurada la comunicación con el exterior por un emisor-receptor de señales de radiofrecuencia dispuesto en el dispositivo de comunicación de acceso seguro.

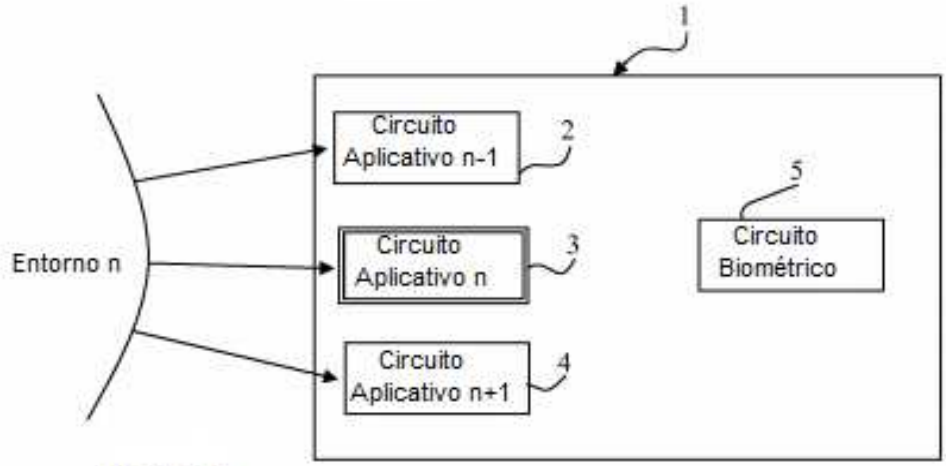

FIGURA 1

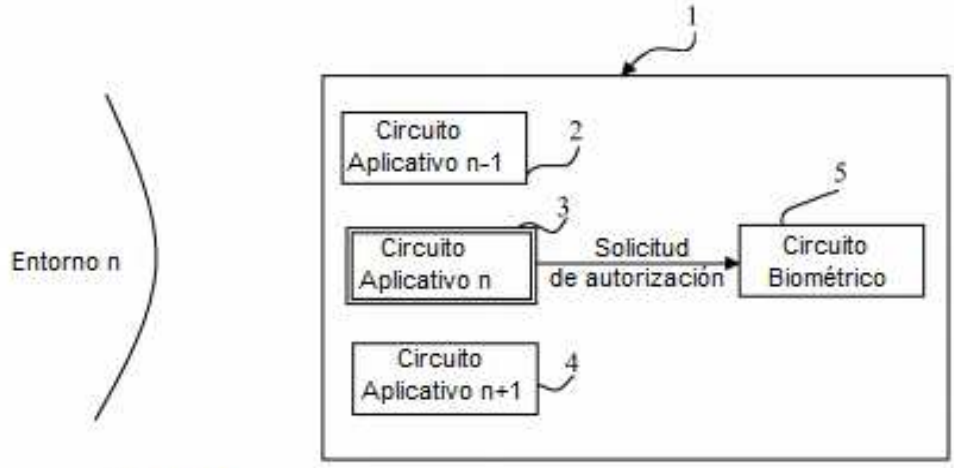

FIGURA 2

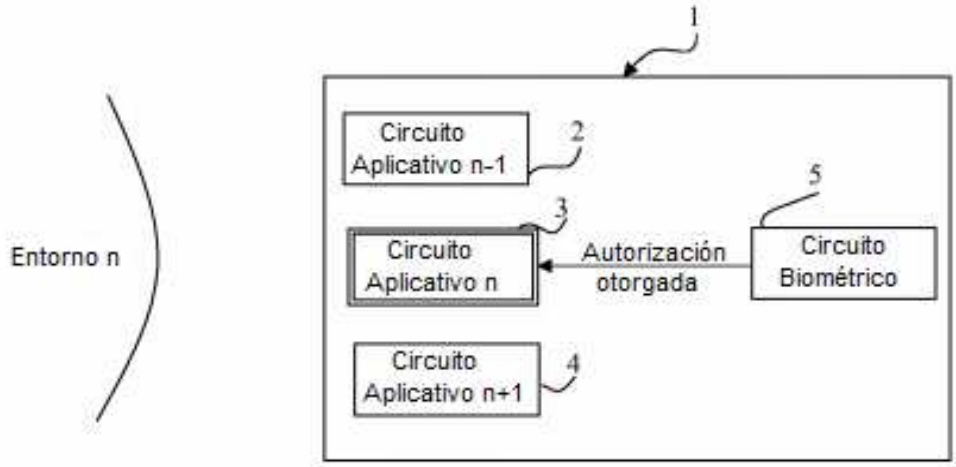

FIGURA 3

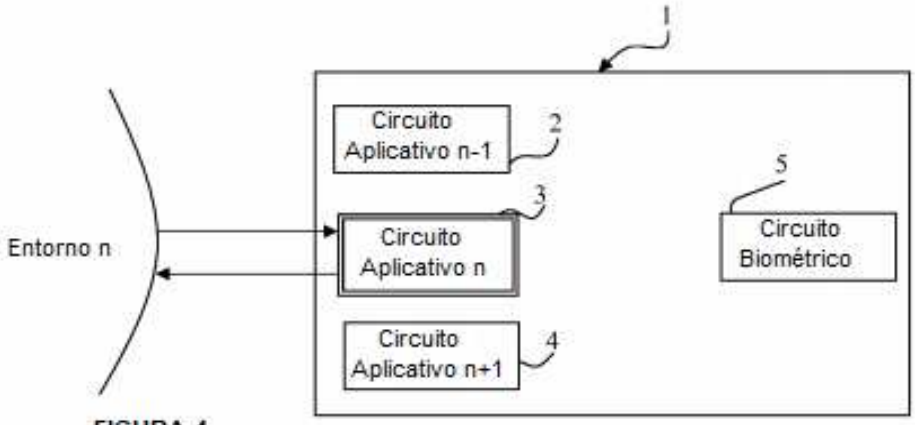

FIGURA 4

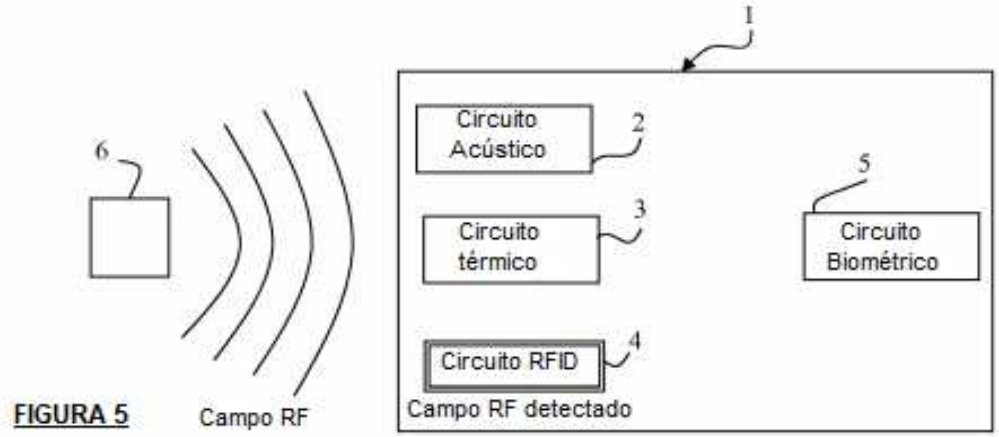

FIGURA 5

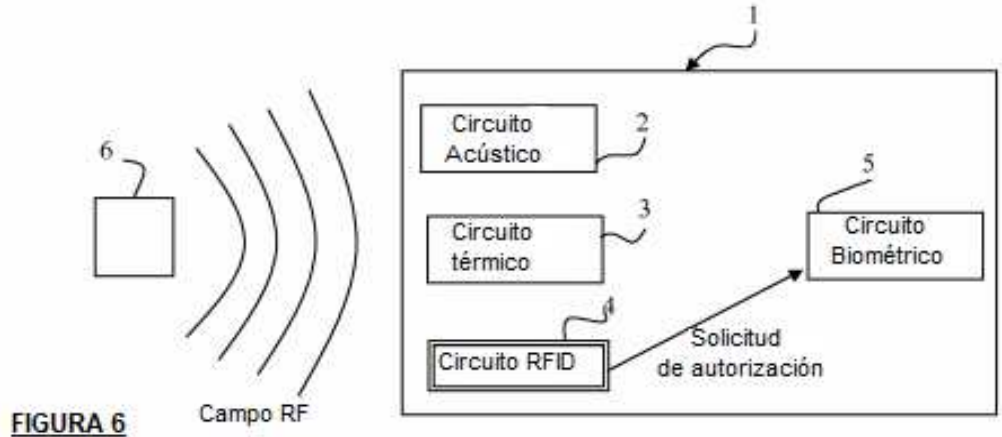

FIGURA 6

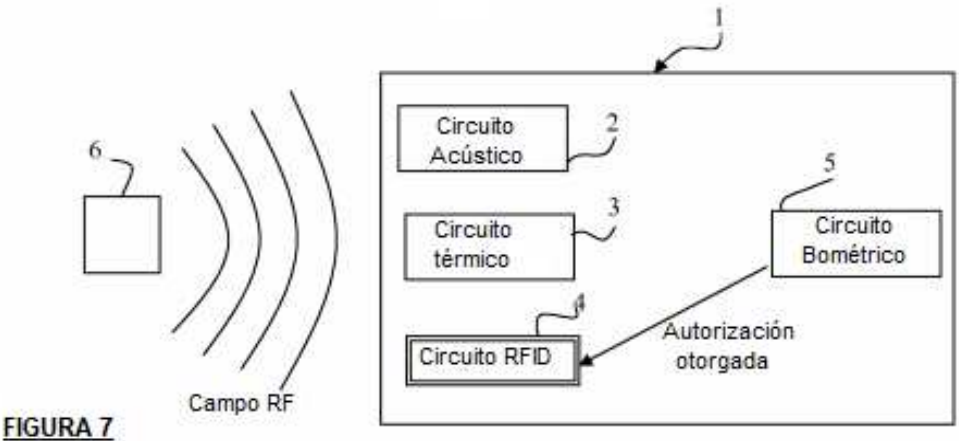

FIGURA 7

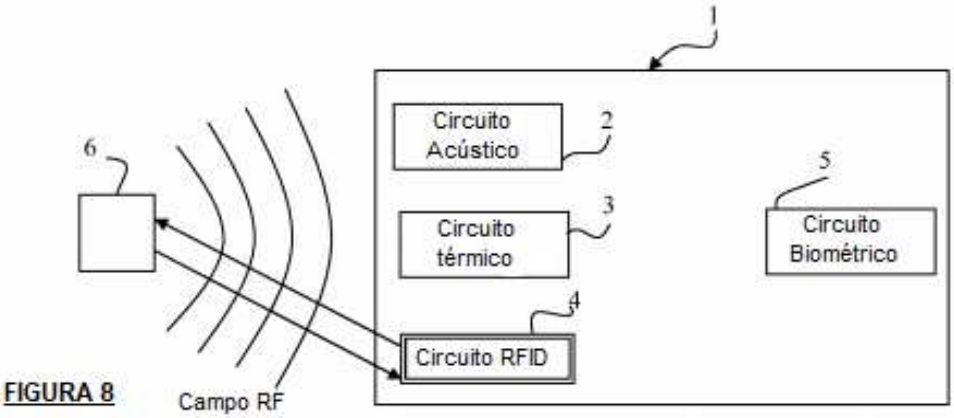

FIGURA 8

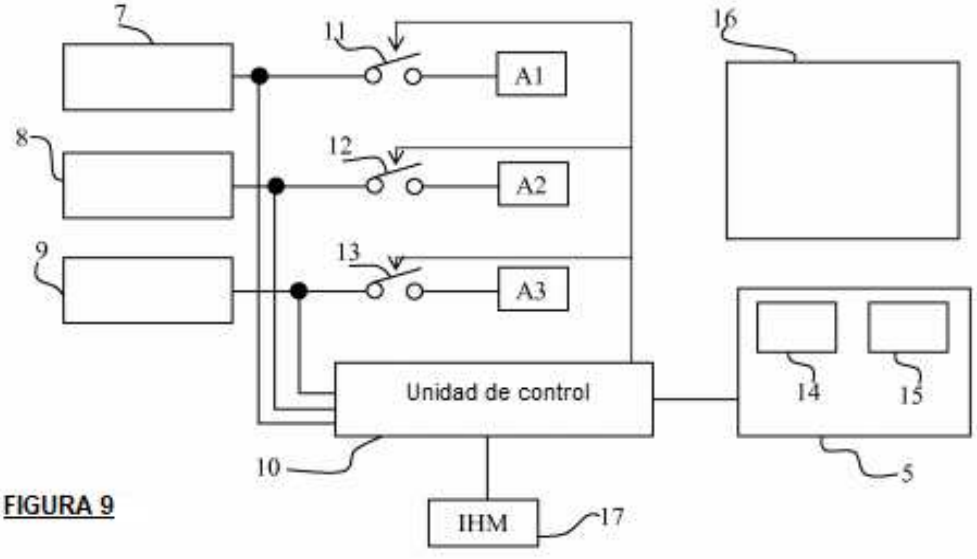

FIGURA 9