(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 399 461**

(51) Int. CI.:

G06F 21/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.01.2008 E 08761971 (4)**

(97) Fecha y número de publicación de la concesión europea: **14.11.2012 EP 2118805**

(54) Título: **Dispositivo portátil de autenticación**

(30) Prioridad:

23.01.2007 FR 0752843

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.04.2013

(73) Titular/es:

DIGIPAY GROUP (100.0%)
46 avenue John Fitzgerald Kennedy
1855 Luxembourg , LU

(72) Inventor/es:

BLOT, PHILIPPE;
RENAUD, JEAN-CHARLES y
BUSCHINI, PHILIPPE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Dispositivo portátil de autenticación.

La presente invención concierne a un sistema que comprende un servidor y un dispositivo portátil y polivalente de autenticación, que permite a un usuario autenticarse, de manera segura y rápida, a través de todos los canales de comunicación existentes (teléfono, Internet…) o directamente en un aparato (autómata, ordenador personal …), para acceder a cualesquiera tipos de servicios y/o de máquinas asegurados.

Para autenticar a un usuario de un servicio o de una máquina, tal como un ordenador personal, es conocido utilizar un dispositivo portátil que facilita una contraseña dinámica o « one time password » (OTP), es decir una contraseña diferente en cada cálculo. Esta contraseña es generada a través de un algoritmo por un procesador, estando basado el algoritmo en una clave secreta única y propia del dispositivo. En tal dispositivo, la clave secreta queda implementada en una memoria durante la fabricación a través del algoritmo de cálculo, lo que, para hacerle funcional, impone la personalización del dispositivo desde la fabricación, de la misma manera que las tarjetas bancarias. Tal limitación plantea especialmente problemas de seguridad (especialmente debido al transporte de dispositivos activos desde su lugar de fabricación), y no permite efectuar actualizaciones de mejora y/o de personalización complementaria del dispositivo, quedando inmovilizadas las informaciones contenidas en fábrica.

Por el documento US 2001/0054148 se conoce transformar un terminal de lectura de tarjeta inteligente por inserción de una tarjeta asegurada en dispositivo de generación de contraseñas de uso único. En este dispositivo conocido, las contraseñas son generadas sobre la base de una clave secreta embarcada en la tarjeta insertada.

Por el documento WO 03/096287 se conoce generar contraseñas de uso único utilizando un registro incrementado de manera monótona y una variable dinámica a fin de obtener una mayor seguridad. El servidor de autenticación divulgado por este documento está en condiciones de generar la misma contraseña de uso único que su cliente, incluso cuando este último ha generado una contraseña que no ha llegado al servidor. Para hacer esto, éste envía una parte del registro utilizado para permitir al servidor detectar esta situación.

El objeto de la invención es mejorar estos sistemas existentes.

La invención parte de la constatación de que es ventajoso poder implementar la clave secreta, entre otras informaciones, lo más tarde posible, y en cualquier caso después de la fabricación (por ejemplo en el momento de la venta), de manera simple y reversible.

Así, la invención concierne a un sistema de acuerdo con la reivindicación 1.

De esta manera, gracias al sistema de acuerdo con la invención, el usuario puede autenticarse de manera segura y rápida facilitando a un prestatario de servicios y/o a un aparato una contraseña dinámica, es decir diferente en cada nueva autenticación. El almacenamiento de la clave secreta que sirve para el cálculo de la contraseña dinámica en una memoria llevada por un circuito electrónico desmontable permite que el dispositivo funcione solamente si la citada memoria está correctamente conectada al dispositivo. La utilización de una memoria desmontable proporciona numerosas ventajas: la personalidad del sistema resulta simplificada porque éste es fabricado en gran serie y personalizado en el último momento, por ejemplo durante la venta, por adición de la memoria que contiene la clave secreta. Además, tal sistema ofrece posibilidades de personalización muy amplias, especialmente la elección de activar o no ciertas funciones. Igualmente, pueden implementarse informaciones complementarias en la memoria y efectuar su actualización. Se puede así hacer evolucionar las capacidades y las funcionalidades del sistema sin tener que reemplazarle.

La seguridad se encuentra igualmente reforzada porque se puede facilitar al usuario los dos elementos por dos canales distintos, efectuando este último a su vez la inserción de la memoria que contiene la clave secreta.

En una realización, la memoria es llevada por un circuito electrónico, de tipo tarjeta SIM o UICC, comprendiendo el dispositivo un conector para acoger al circuito electrónico.

En una realización, el microprocesador es llevado por el mismo circuito electrónico que la memoria en la cual queda almacenada la clave secreta.

En una realización, el dispositivo comprende un módulo de emisión de radiofrecuencias para emitir una señal de radiofrecuencias representativa de la contraseña dinámica.

En una realización, el dispositivo comprende una conexión de tipo USB y puede ser conectado a un aparato equipado con un puerto de tipo USB.

En una realización, el dispositivo comprende una batería recargable, siendo recargada la batería cuando el dispositivo esté conectado a través del puerto USB.

En una realización, la memoria en la cual queda almacenada la clave secreta permite almacenar informaciones complementarias.

En una realización, la contraseña dinámica es facilitada simultáneamente por el dispositivo a través de al menos dos de los medios de comunicación disponibles.

Se describe de maneara no limitativa un ejemplo de realización de la invención en relación con las figuras, en las cuales:

- la figura 1 es un esquema en tres dimensiones de un dispositivo de acuerdo con la invención,
- la figura 2 muestra el dispositivo de la figura 1, visto bajo un ángulo diferente,
- la figura 3 muestra componentes de un dispositivo de acuerdo con la invención,
- la figura 4 muestra los componentes de una variante del dispositivo de la figura 3.

La figura 1 muestra un dispositivo 10 de acuerdo con la invención. Tal dispositivo 10 es un objeto portátil de dimensiones reducidas, formado por una carcasa única y compacta 10_1, en el ejemplo de forma sensiblemente paralelepipédica. En una cara 12 de la carcasa 10_1, denominada cara delantera, está dispuesto un visualizador 14, que permite la visualización de una secuencia de caracteres o de cifras, en el ejemplo una secuencia comprendida entre seis y ocho caracteres. En esta cara delantera 12 del objeto portátil 10 está dispuesta igualmente una tecla 16 que constituye un medio de activación del objeto portátil 10. En variante, la tecla 16 es reemplazada por un sensor biométrico, o por cualquier otro sensor apto para constituir un medio de activación. El contorno de la cara delantera 12 del objeto portátil es sensiblemente rectangular, y el objeto 10 presenta por tanto cuatro caras laterales opuestas dos a dos, dos caras laterales pequeñas 18_1 y 18_2, y dos caras laterales grandes 20_1 y 20_2. Un elemento 22 en saliente sobre una de las caras laterales pequeñas del dispositivo 18_1 comprende un agujero 24 que permite fijar el dispositivo 10, por ejemplo a un portallaves.

La figura 2 muestra el dispositivo 10 visto bajo otro ángulo. En la cara lateral pequeña 18_2, opuesta a la cara lateral pequeña 18_1 que comprende el elemento 21, puede verse una abertura, o ranura 26 que permite la inserción en el interior del dispositivo 10 de un circuito electrónico, o chip, por ejemplo de tipo « tarjeta SIM ».

La figura 3 muestra los componentes dispuestos en el interior del objeto portátil 10. Éste comprende una batería 30 para alimentar los diferentes componentes. En el objeto portátil está integrado un módulo de emisión sonora 34, o « buzzer ». Se trata de un altavoz de tipo piezoeléctrico. Un microprocesador 32 permite efectuar operaciones variadas, entre las cuales el cálculo de una contraseña dinámica, u OTP. El microprocesador 32 efectúa el cálculo de la OTP gracias a un algoritmo basado en una clave secreta y única. Esta clave secreta queda almacenada en una memoria 37, conectada de manera desmontable al objeto 10, a través de un conector 38. En el ejemplo, la memoria 37 es llevada por un circuito electrónico 36 de tipo tarjeta inteligente, que contiene un microcontrolador y una memoria de almacenamiento, como por ejemplo una tarjeta de tipo tarjeta SIM o UICC (« Universal Integrated Circuit Card », tarjeta universal de circuito integrado). De acuerdo con la invención, ésta es introducida en la ranura 26 y conectada al conector 38.

Es ventajoso utilizar una tarjeta de este tipo, porque además de una memoria de almacenamiento, las capacidades de cálculo que ésta proporciona permiten considerar implementar en ella todo o parte del algoritmo de cálculo de la contraseña dinámica, así como funciones suplementarias. En una variante, el microprocesador 32 está integrado en esta tarjeta, y todas las operaciones de cálculo efectuadas por el dispositivo 10 son realizadas por la tarjeta 36. El dispositivo puede comprender en este caso un microprocesador (no representado) dedicado a la gestión de los elementos tal como el visualizador, el módulo de emisión sonora …

Por otra parte, la utilización de una tarjeta de tipo SIM o UICC permite obtener un dispositivo muy compacto. En efecto, las dimensiones de tal tarjeta son muy reducidas en comparación con una tarjeta inteligente clásica con formato de tipo « tarjeta de crédito ». Así, gracias a este tamaño muy reducido, la tarjeta puede ser insertada íntegramente y quedar permanentemente en el interior de la carcasa 10_1 (al tiempo que se mantiene desmontable). Se obtiene así un dispositivo autónomo, que integra todos los elementos necesarios para su funcionamiento, al tiempo que presenta un formato « de bolsillo » comparable con los dispositivos de almacenamiento USB (denominados habitualmente « llaves USB »).

La tarjeta SIM 36 puede ser introducida durante la fabricación o en cualquier momento después de ésta, especialmente durante la remisión del dispositivo a su usuario. El dispositivo no es funcional en tanto que la tarjeta 36 no esté conectada a éste a través del conector 38. La ranura 26 podrá ser sellada después de la introducción de la tarjeta SIM 36 si no se desea que el usuario pueda retirarla él mismo. En este caso, una variante no prevé ranura o abertura en la carcasa 10_1 del dispositivo. Así, la extracción de la tarjeta 36 puede resultar más difícil (haciendo necesario el desmontaje del dispositivo para acceder a la tarjeta), incluso imposible (la tarjeta queda instalada durante la fabricación y el dispositivo no es desmontable).

Cada contraseña dinámica calculada esta destinada a ser visualizada en forma de una secuencia de caracteres alfanuméricos por el visualizador 14 y/o emitida por el buzzer 34 en forma de señales sonoras representativas de esta contraseña dinámica. El visualizador 14 y el buzzer 34 son dos de los medios de comunicación de la OTP de

los que puede disponer el objeto portátil 10. Preferentemente, las señales emitidas y visualizadas comprenden un identificador propio del dispositivo 10 o de la tarjeta 36, así como la OTP.

A continuación se describen variantes de cálculo y de verificación de la OTP. En todas las variantes, la contraseña es generada a través de un algoritmo por el microprocesador 32 y basada en la clave secreta, que es original y única. Esta misma clave queda por otra parte almacenada en una base de datos de un servidor (no mostrado) encargado de la autenticación, para permitir la verificación de una OTP facilitada por un usuario que desee autentificarse.

En una primera variante, la OTP es calculada a través de un algoritmo que toma como argumento, por una parte, la clave secreta almacenada en memoria y, por otra, un contador incrementado una unidad en cada nuevo cálculo, por tanto en cada pulsación de la tecla 16. El incremento del contador facilita así un valor variable que permite que el resultado del cálculo efectuado por el algoritmo sea diferente en cada cálculo: se obtiene así una contraseña dinámica.

Cuando la OTP así calculada es facilitada a la máquina/servidor encargados de la autenticación, por ejemplo en un prestatario de servicios a distancia, ésta va acompañada de un identificador propio del dispositivo 10 (y por tanto propio de su procesador). Gracias al identificador, el servidor extrae de una base de datos interna la clave secreta única asociada al identificador.

No conociendo el servidor el valor del contador incremental utilizado para el cálculo de la OTP, éste busca entonces el último valor conocido de este contador, es decir el utilizado durante la última autenticación, estando almacenado este valor en el servidor. Naturalmente, desde esta ultima autenticación efectiva, el dispositivo habrá podido ser solicitado un cierto número de veces por el usuario sin utilizar las OTP calculadas. Para tener en cuenta esta eventual diferencia, el servidor reproduce sucesivamente el mismo cálculo que el puesto en práctica en el dispositivo, partiendo del último valor conocido del contador incremental aumentado en una unidad e incrementando éste en cada nuevo cálculo, hasta que el cálculo dé un resultado idéntico a la OTP que ha sido facilitada por el usuario.

Por medida de seguridad, el número de iteraciones efectuadas por el servidor será limitado, y si el servidor alcanza el número máximo de iteraciones sin haber podido obtener un resultado idéntico a la OTP facilitada, entonces la autenticación es rechazada. Cuando la OTP ha sido verificada y aceptada, el nuevo valor correcto del contador incremental es almacenado entonces en el servidor para servir durante el próximo intento de autenticación.

En una segunda variante, el algoritmo de cálculo toma como argumento el contador incremental descrito anteriormente y una clave dinámica que varía con el tiempo. Esta clave dinámica se obtiene gracias a un segundo algoritmo que toma como argumento la clave secreta y un valor T dependiente del tiempo. Para obtener de manera simple un valor T dependiente del tiempo, se puede proceder por ejemplo de la manera siguiente: se mide el tiempo transcurrido desde un valor de partida To correspondiente al momento de la personalización del dispositivo (es decir, la introducción inicial de la tarjeta 36), comprendiendo el dispositivo a tal efecto un reloj. El valor T representa entonces el tiempo transcurrido desde To, expresado en unidades de tiempo. La unidad de tiempo utilizada es variable y puede ser elegida durante la personalización del dispositivo (por ejemplo 1, 2, 5 o 10 minutos). Para que la OTP pueda ser verificada por la máquina o el servidor destinatario, es necesario que el referencial tiempo utilizado por el dispositivo sea el mismo que la máquina/servidor destinatario. Con este objetivo, el valor de partida To introducido en memoria durante la personalización es un valor relativo que permite sincronizar el dispositivo con el referencial tiempo de la máquina/servidor destinatario de la OTP.

En esta segunda variante, la verificación de la OTP por el servidor destinatario obedece al mismo principio que el descrito anteriormente, integrando el cálculo de la clave dinámica a partir de la clave secreta y del valor T de los que el servidor dispone igualmente.

El dispositivo de acuerdo con la invención permite realizar la autenticación de su poseedor a través de todos los canales de comunicación existentes (teléfono, Internet …) o directamente en un aparato (autómata, ordenador portátil …). A continuación se describen diferentes ejemplos de procedimientos de autenticación realizables con el dispositivo de acuerdo con la invención, cuando un usuario deba identificarse, ante un prestatario de servicios o una máquina.

Autenticación a través de una red telefónica: en este caso se utiliza la OTP en forma de señales sonoras. El usuario pulsa la tecla 16, y el objeto portátil 10 facilita una OTP en forma de señales acústicas, habiendo situado el usuario previamente su dispositivo 10 en la proximidad del micrófono del teléfono. Las señales acústicas son transmitidas a través de la red telefónica hacia un servidor del prestatario concernido. Se descodifican entonces estas señales, se reconoce al identificador, y se verifica la OTP. La transacción es entonces aceptada o rechazada

Autenticación a través de una red Internet: el usuario es llevado en este caso a introducir su identificador y su OTP. Éste entonces copia la OTP tal como es visualizada por el visualizador 14. Su identificador y su OTP son introducidos en un teclado de un ordenador conectado a un sitio Internet del prestatario. La OTP es verificada entonces por el servidor del prestatario.

Autenticación en un aparato: En un aparato tal como un ordenador portátil, el usuario debe facilitar un identificador y una OTP, como para la autenticación a través de una red.

En todos los casos, el prestatario de servicios podrá añadir al dispositivo un código secreto, tal como un PIN de cuatro cifras, que el usuario deberá facilitar además de la OTP y de su identificador, a fin de reforzar la seguridad de la autenticación.

En una variante no representada, el objeto portátil puede ser conectado a través de un puerto de tipo USB (« Universal Serial Bus ») a un ordenador o a cualquier otro aparato equipado con dicho puerto. Con este objetivo, el dispositivo comprende una toma 40 (véase la figura 4) adaptada al puerto USB. Así, el dispositivo puede facilitar la OTP calculada directamente a través del puerto USB.

Se distinguen entonces dos casos: la contraseña dinámica es facilitada con la activación del dispositivo durante la pulsación de la tecla 16, o ésta es facilitada en respuesta a una interrogación de la máquina anfitrión, por ejemplo a demanda de la aplicación que necesita la autenticación. En este último caso, la interrogación puede ser realizada a intervalos regulares para aumentar la seguridad de la aplicación. En variante, el dispositivo puede igualmente facilitar tras la interrogación de la máquina anfitrión, como complemento de la OTP, un certificado electrónico de autenticación (facilitado previamente por una autoridad habilitada para facilitar tales certificados). En esta variante, el certificado es inscrito en la memoria 37, y no puede ser modificado ni borrado.

En el caso en que el dispositivo esté conectado a través de un puerto de tipo USB, la batería 30 utilizada en el dispositivo 10 puede ser de tipo recargable, siendo recargada ésta entonces a través del puerto USB.

En otra variante no representada, el dispositivo 10 comprende igualmente un módulo de comunicación de radiofrecuencias 42, representado en la figura 4, que permite transmitir sin contacto la OTP calculada, por ejemplo de acuerdo con las normas RFID o NFC.

Ventajosamente, el dispositivo 10 comprenderá todos los componentes necesarios para la puesta en práctica de las diferentes variantes descritas anteriormente, pero sus funcionalidades serán activadas o no durante la personalización del dispositivo. Así, el prestatario de servicios que facilite tal dispositivo a un cliente/usuario podrá elegir, para sus aplicaciones propias, las funcionalidades que éste desee poner en práctica (por ejemplo habida cuenta del tiempo en el cálculo de la OTP o no, utilización de radiofrecuencias o no, utilización del buzzer o no …).

REIVINDICACIONES

1. Sistema que comprende un servidor y un dispositivo portátil de autenticación de un usuario, que comprende una carcasa (10_1) única en la cual están alojados:

- medios (16) de activación del dispositivo, tal como una tecla que debe ser pulsada por el usuario,

- un microprocesador (32) que efectúa un cálculo durante la activación del dispositivo (10), empleando el cálculo un algoritmo basado en una clave secreta almacenada en una memoria (37), y que tiene como resultado una contraseña dinámica;

- siendo el dispositivo (10) tal que la memoria (37) en la cual queda almacenada la clave secreta está dispuesta en el interior de la carcasa (10_1) y conectada al dispositivo de manera desmontable,

- comprendiendo el dispositivo (10) además en combinación un módulo de emisión sonora (34) para facilitar la contraseña dinámica en forma de señales acústicas y un visualizador (14) para una visualización de la contraseña dinámica efectuada simultáneamente con la emisión de la contraseña en forma acústica,

en el cual el cálculo de la contraseña dinámica toma como argumento el valor de un contador incrementado en cada nuevo cálculo, y depende del tiempo.

en el cual, cuando la contraseña dinámica así calculada es facilitada al servidor encargado de la autenticación, ésta va acompañada de un identificador propio del citado dispositivo (10),

en el cual, no conociendo el servidor el valor del contador incremental utilizado para el cálculo de la contraseña dinámica, éste busca entonces el último valor conocido de este contador, es decir el utilizado durante la última autenticación, estando almacenado este valor en el servidor, y en el cual el citado servidor reproduce sucesivamente el mismo cálculo que el puesto en práctica en el citado dispositivo (10), partiendo del último valor conocido del contador incremental aumentado en una unidad e incrementando éste en cada nuevo cálculo, hasta que el cálculo dé un resultado idéntico a la contraseña dinámica que ha sido facilitada por el usuario.

2. Sistema de acuerdo con la reivindicación 1, en el cual la memoria (37) es llevada por una tarjeta, estando situada esta tarjeta íntegramente en el interior de la carcasa (10_1).

3. Sistema de acuerdo con las reivindicaciones 1 o 2, en el cual la memoria (37) es llevada por un circuito electrónico (36) de tipo tarjeta SIM o UICC, comprendiendo el dispositivo un conector (38) para acoger al circuito electrónico (36).

4. Sistema de acuerdo con las reivindicaciones 1 a 3, en el cual el microprocesador (32) es llevado por el mismo circuito electrónico (36) que la memoria (37) en la cual queda almacenada la clave secreta.

5. Sistema de acuerdo con una de las reivindicaciones 1 a 4, que comprende un módulo de emisión de radiofrecuencias (42) para emitir una señal de radiofrecuencias representativa de la contraseña dinámica.

6. Sistema de acuerdo con una de las reivindicaciones 1 a 5, que comprende una conexión (40) de tipo USB y que puede ser conectado a un aparato equipado con un puerto de tipo USB.

7. Sistema de acuerdo con la reivindicación 6, que comprende una batería (30) recargable, siendo recargada la batería cuando el dispositivo esté conectado a través del puerto USB.

8. Sistema de acuerdo con una de las reivindicaciones 1 a 7, en el cual la memoria (37) en la cual queda almacenada la clave secreta permite almacenar informaciones complementarias.

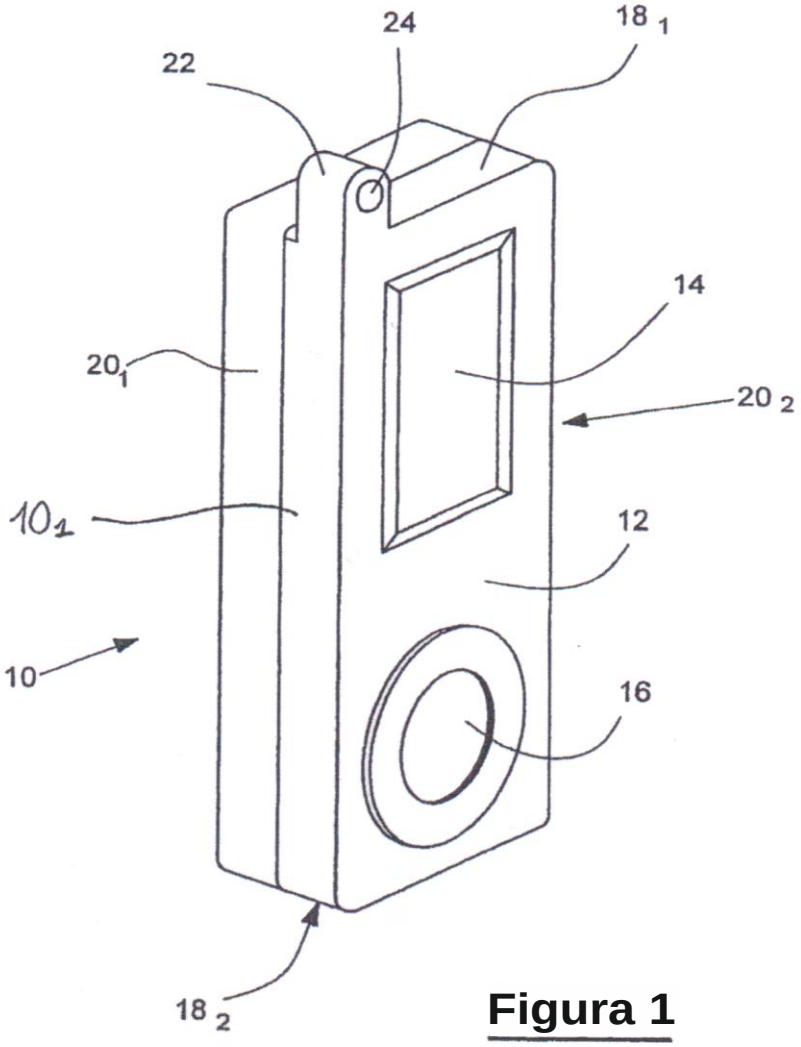

Figura 1

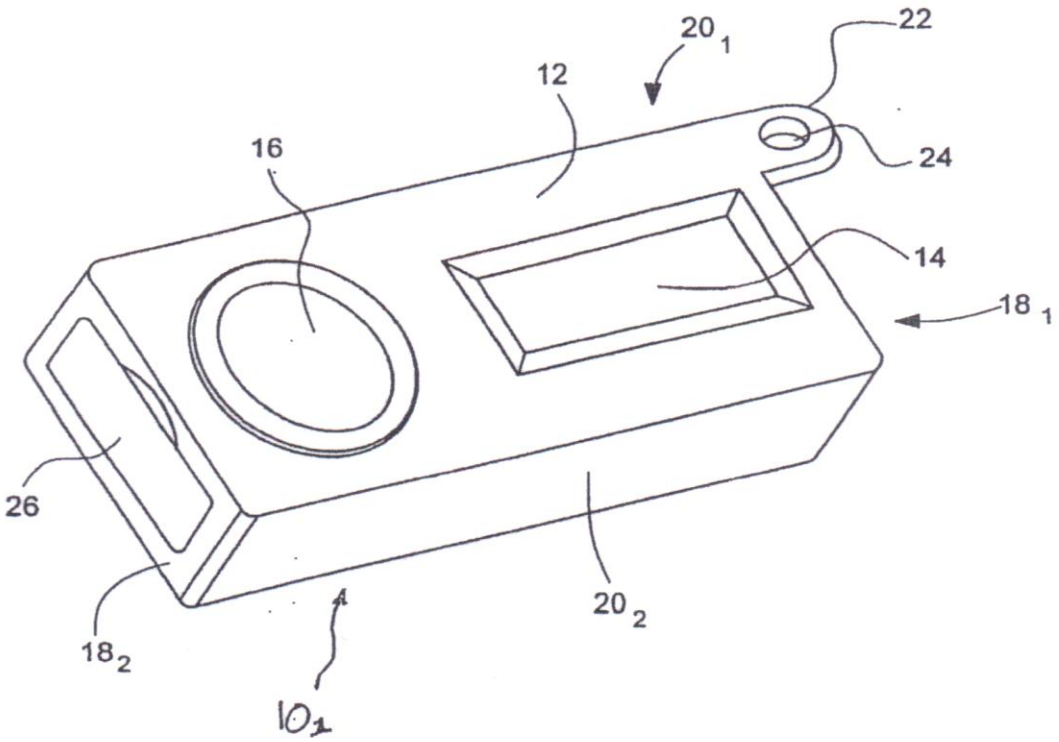

Figura 2

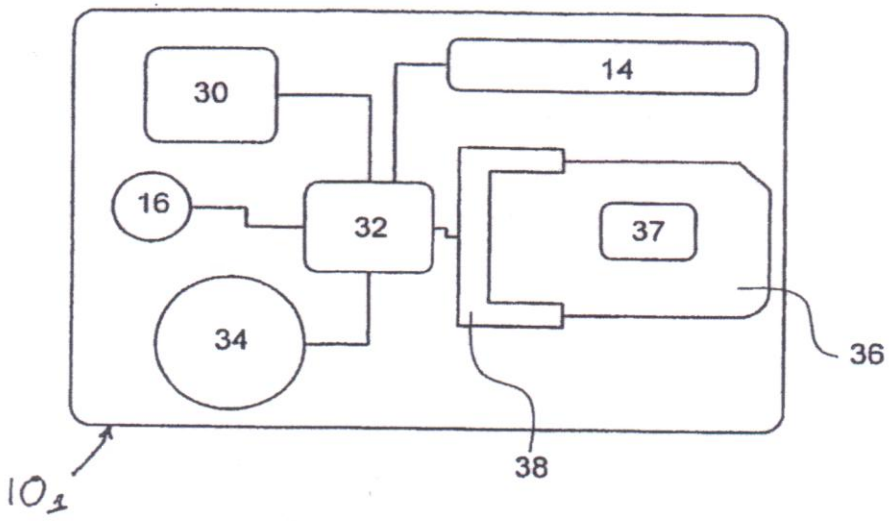

Figura 3

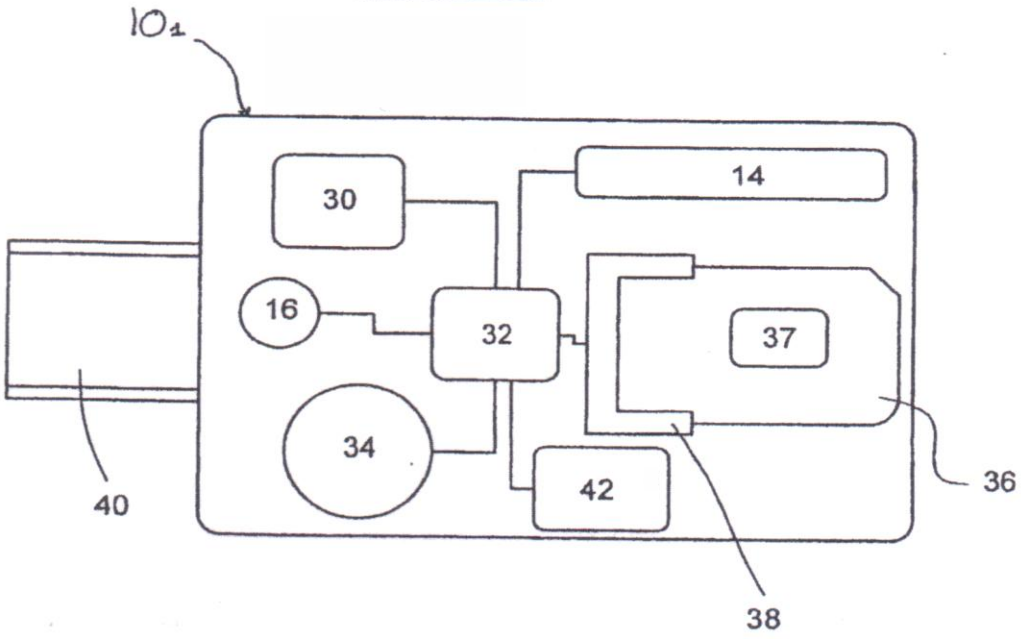

Figura 4