(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 215**

(51) Int. CI.:
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **01274860 .4**
(96) Fecha de presentación: **06.12.2001**
(97) Número de publicación de la solicitud: **1454303**
(97) Fecha de publicación de la solicitud: **08.09.2004**

(54) Título: **Dispositivo portátil y método para acceder a dispositivos accionados mediante una clave de datos**

(45) Fecha de publicación de la mención BOPI:
19.07.2012

(45) Fecha de la publicación del folleto de la patente:
19.07.2012

(73) Titular/es:
BIOSCRYPT INC.
5450 EXPLORER DRIVE, SUITE 500
MISSISSAUGA, ONTARIO L4W 5M1, CA

(72) Inventor/es:
HOLLINGSHEAD, Dennis W.

(74) Agente/Representante:
Durán Moya, Luis Alfonso

DESCRIPCIÓN

Dispositivo portátil y método para acceder a dispositivos accionados mediante una clave de datos

SECTOR DE LA INVENCIÓN

La presente invención se refiere a un método para acceder a dispositivos accionados mediante una clave de datos, un dispositivo portátil para acceder dichos dispositivos accionados mediante una clave y un sistema de acceso seguro.

ANTECEDENTES DE LA INVENCIÓN

El acceso a un número cada vez mayor de dispositivos se controla mediante claves de acceso de datos. Por ejemplo, el acceso a un cajero automático (ATM) se controla mediante la entrada mediante teclado numérico de un número de identificación personal adecuado (PIN). De manera similar, el acceso a puertas de alta seguridad se puede controlar mediante la entrada de teclado numérico de un código de acceso. El acceso a los sistemas de seguridad, las redes informáticas y los sistemas de correo de voz también se controlan típicamente mediante un código de acceso. A medida que aumenta el número de dispositivos que demandan una clave de acceso para garantizar el acceso, se vuelve más difícil que un usuario recuerde todas las claves de acceso necesarias. Además, la seguridad de dichos dispositivos accionados mediante una clave pueden verse comprometidos si la clave de acceso no se mantiene en estricto secreto por parte del usuario autorizado.

En el documento US 5.131.038 un transceptor de verificación transmite periódicamente las solicitudes de identidad. Un transceptor de identificación portátil puede recibir dicha solicitud de identidad y, en respuesta, recuperar los datos paramétricos cifrados (por ejemplo, información biométrica tal como altura y peso) de un procesador autorizado desde la memoria y transmitir dichos datos. El transceptor de verificación recibe los datos paramétricos cifrados transmitidos, los descifra y compara los datos paramétricos descifrados con los datos paramétricos medidos de un procesador del transceptor portátil.

En la solicitud EP número 0924657, un dispositivo portátil tiene un sensor para leer datos biométricos, tales como una imagen de huella dactilar, de una persona, y un correlador para comparar los datos detectados con una imagen de referencia almacenada previamente y determinar si coinciden. Si coinciden, el dispositivo genera un valor numérico, tal como un código de redundancia cíclico (CRC), de la imagen de referencia almacenada, cifra el valor numérico y lo transmite a la puerta de una propiedad protegida como confirmación de la identidad de la persona. Al recibir la confirmación de la identidad desde el dispositivo, la puerta compara el valor numérico recibido con uno almacenado anteriormente durante el registro y, si coinciden, garantiza el acceso. En una realización alternativa, el dispositivo envía primero un nombre de usuario a la puerta. Al recibir el nombre de usuario desde el dispositivo, la puerta genera una clave pública y transmite la clave pública al dispositivo. Si el dispositivo ha determinado que existe una coincidencia entre los datos detectados y la imagen de referencia almacenada anteriormente, el dispositivo cifra el CRC que se ha generado utilizando la clave pública de la puerta y lo trasmite a la puerta. La puerta descifra el CRC recibido utilizando su clave privada y determina si existe una coincidencia asociada al nombre de usuario.

Esta invención busca superar los inconvenientes de los sistemas de seguridad conocidos.

CARACTERÍSTICAS DE LA INVENCIÓN

Según la presente invención, se da a conocer un método para acceder a dispositivos accionados mediante una clave de datos que comprende: la recepción de un identificador del dispositivo accionado mediante una clave desde un dispositivo accionado mediante una clave, la recepción de datos biométricos, la determinación de si dichos datos biométricos son datos biométricos autorizados, la comparación de dicho identificador recibido, del dispositivo accionado mediante una clave, con los identificadores de los dispositivos accionados mediante una clave almacenados y, al encontrar una coincidencia con un identificador del dispositivo accionado mediante una clave almacenado y cuando dichos datos biométricos recibidos son datos biométricos autorizados, la recuperación de una clave de acceso almacenada asociada a dicho identificador accionado mediante una clave almacenado coincidente y la transmisión de dicha clave de acceso recuperada.

Según otro aspecto de la invención, se da a conocer un dispositivo de acceso electrónico portátil que comprende: una entrada biométrica, un verificador que reacciona a dicha entrada biométrica para verificar que unos datos biométricos que se introducen a dicha entrada biométrica coinciden con unos datos biométricos autorizados y la disposición de una indicación de la verificación, una memoria que almacena una serie de claves de acceso, cada una para utilizarla para acceder a una serie de dispositivos accionados mediante una clave y una serie de identificadores de dispositivos accionados mediante una clave, un receptor para recibir un identificador de un

dispositivo accionado mediante una clave, un comparador para, en respuesta a una indicación de verificación de dicho verificador, compare un identificador de dispositivo accionado mediante una clave recibido desde un dispositivo accionado mediante una clave con dichos identificadores de los dispositivos accionados mediante una clave almacenada y, al encontrar un identificador del dispositivo accionado mediante una clave que coincide, recuperar una clave de acceso almacenada asociada a dicho identificador del dispositivo accionado mediante una clave almacenado y un transmisor para transmitir una clave de acceso recuperada.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En las figuras que muestran una realización de ejemplo de la invención,

la figura 1 es un diagrama de bloques de un sistema de acceso seguro fabricado según esta invención, y

la figura 2 es un diagrama de flujo de la operación del proceso de la figura 1.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES PREFERENTES

Haciendo referencia a la figura 1, un sistema -10- de acceso seguro comprende un dispositivo -12- accionado mediante una clave de datos y un dispositivo -14- de acceso mediante clave portátil. El dispositivo -12- accionado mediante una clave podría ser una puerta de alta seguridad (vehículo o instalación), un cajero automático (ATM), un sistema de seguridad, una red informática, un sistema de mensajes de voz o cualquier otro dispositivo que requiera una clave de acceso para garantizar el acceso. El dispositivo -14- de acceso mediante una clave comprende un procesador -20- conectado mediante una comunicación bidireccional con un transceptor -22- y mediante una comunicación bidireccional con una memoria -24-. El procesador también recibe señales desde una entrada de huellas dactilares -26-. La memoria -24- es no volátil y almacena una serie de claves de acceso para utilizar cada una para acceder a un dispositivo accionado mediante una clave. La memoria también almacena una serie de identificadores de los dispositivos accionados mediante una clave, cada uno de ellos asociado a una de las diversas claves de acceso almacenadas. El transceptor -22- es inalámbrico y se puede comunicar con el dispositivo accionado mediante una clave a través de transmisiones de radio o transmisiones de infrarrojo. El dispositivo -14- es portátil y preferentemente es alimentado por batería. Un conmutador (no mostrado) puede desconectar la batería cuando el dispositivo no se encuentra en uso para conservar la energía de la batería.

A efectos de utilizar el dispositivo de acceso portátil, un usuario se debe registrar previamente. Para efectuar el registro, el usuario debe pasar una copia digitalizada de su huella dactilar a un ordenador de registro. Esto se puede conseguir haciendo que el usuario aplique su dedo a la entrada de huellas dactilares -26- del dispositivo -14- de acceso cuando el dispositivo se conecta a través de un puerto (no mostrado) al ordenador de registro, de manera que el procesador -20- del dispositivo de acceso es instado a pasar la imagen de la huella dactilar digitalizada al ordenador de registro. De manera alternativa, el usuario puede aplicar su huella dactilar directamente a una entrada de huellas dactilares asociada al ordenador de registro. Este ordenador calcula entonces una plantilla a partir de la huella dactilar del usuario que es una combinación cifrada de la huella dactilar con un código de verificación. Las técnicas adecuadas para obtener dichas plantillas a partir de una huella dactilar y un código, y para recuperar un código a partir de dicha plantilla, se describen en el documento de patente US número 5.680.460 titulado GENERACIÓN DE CLAVE CONTROLADA MEDIANTE DATOS BIOMÉTRICOS de Tomko y otros, los contenidos del cual se incorporan por referencia en este documento. Esta plantilla se carga posteriormente a los dispositivos de acceso portátil y se almacena en una memoria -24-. Además, el ordenador de registro almacena una indicación de verificación en una dirección de la memoria -24- indicada por el código de verificación. Entonces se ha completado el registro.

La operación del sistema -10- de la figura 1 se describe conjuntamente con la figura 1 y la figura 2, que muestra un control de programa para el procesador -20-. El dispositivo -12- accionado mediante una clave transmite periódicamente un identificador de dispositivo. Se prefiere, generalmente, que el tiempo entre dichas transmisiones no sea más de cinco segundos, el alcance de estas transmisiones se prefiere que sea en torno a dos metros. Cuando el dispositivo -14- de acceso portátil se encuentra dentro del alcance de las transmisiones del dispositivo accionado mediante una clave y se conecta, el transceptor -22- recibirá estas transmisiones y pasará el identificador del usuario accionado mediante una clave al procesador -20- (bloque -50-). Si el usuario del dispositivo de acceso portátil aplica entonces su huella dactilar a la entrada de huellas dactilares -26-, la imagen de la huella dactilar también es recibida por el procesador -20- (bloque -52-).

El procesador puede determinar entonces si la huella dactilar que se ha introducido es la del usuario autorizado. Esto se consigue mediante la recuperación por parte del procesador de la plantilla almacenada en la memoria -24- durante el registro y la combinación de ésta con la huella dactilar recientemente introducida desde la entrada -26-. El código de verificación resultante se utiliza como una dirección de memoria en la memoria -24-. Si el procesador encuentra una indicación de verificación en esta dirección de memoria en la memoria -24-, entonces los datos

biométricos se consideran autorizados (bloque -54-). En dicho caso, el procesador compara el identificador del dispositivo accionado mediante una clave recibido con los identificadores de dispositivo accionados mediante una clave en la memoria. Si se encuentra una coincidencia (bloque -56-), el procesador pasa una indicación de usuario válido a un transceptor -22- para la transmisión del dispositivo -12- accionado mediante una clave (bloque -58-). Esta indicación de usuario válido puede comprender el código de verificación o una versión cifrada del mismo. Adicionalmente, el procesador recupera la clave de acceso de la memoria -24- que está asociada al identificador del dispositivo accionado mediante una clave que ha coincidido (bloque -60-).

Cuando el dispositivo -12- accionado mediante una clave recibe una indicación de usuario válido desde el dispositivo de acceso -14-, transmite una clave de cifrado temporal de un solo uso. Ésta es recibida por el transceptor -22- y se pasa al procesador -20-. El procesador -20- utiliza la clave temporal para cifrar la clave de acceso recuperada (bloque -62-). La clave de acceso cifrada se pasa entonces al transceptor -22- y se transmite al dispositivo accionado mediante una clave (bloque -64-). El dispositivo accionado mediante una clave utiliza una clave de descifrado para recuperar la clave de acceso descifrada y, si la clave descifrada resultante es válida, permite el acceso al usuario. En el caso en que el dispositivo accionado mediante una clave es una puerta de alta seguridad, esto da como resultado que se desbloquee la puerta. En el caso en el que el dispositivo accionado mediante una clave es un cajero automático (ATM), esto permitiría al usuario el acceso al dispositivo a través de un teclado numérico que se podría disponer en el dispositivo -14- de acceso portátil.

Se hará evidente que dado que el dispositivo -14- de acceso almacena un número de identificadores de dispositivos accionados mediante una clave, el dispositivo -14- puede ser transportado por parte de un usuario autorizado y utilizado para obtener acceso a un número de diferentes dispositivos accionados mediante una clave sin necesidad de que el usuario memorice una serie de códigos de acceso.

El dispositivo de acceso portátil se puede utilizar con un dispositivo accionado mediante una clave existente modificando el dispositivo para incorporar un transceptor en el mismo y programar el procesador del dispositivo accionado mediante una clave, de manera que el dispositivo funcione de la manera descrita.

Son posibles múltiples modificaciones del sistema que se ha descrito. Por ejemplo, el identificador de usuario válido se puede transmitir tan pronto como se recibe una huella dactilar autorizada mediante el dispositivo -14- de acceso previamente a la determinación de si el identificador del dispositivo accionado mediante una clave recibido coincide con uno de los identificadores almacenados.

Opcionalmente, para aplicaciones de menor seguridad, el dispositivo de acceso portátil no transmite una indicación de usuario válido, ni el dispositivo accionado mediante una clave transmite ninguna clave temporal. En su lugar, para dichas aplicaciones, cuando el dispositivo -14- de acceso determina que un usuario autorizado ha aplicado su huella dactilar a la entrada y al encontrar una clave de acceso para el dispositivo accionado mediante una clave, esta clave de acceso se transmite en una forma sin cifrar al dispositivo accionado mediante una clave.

Otra opción es que el dispositivo -12- accionado mediante una clave envíe un indicador de “seguridad media” cuando quiera acceder al dispositivo -14- para enviar un código de verificación y recibir una clave temporal para descifrar las claves de acceso antes de la transmisión y para enviar un indicador de “baja seguridad”, o ningún indicador de seguridad, cuando quiere el acceso al dispositivo -14- para seguir la opción de baja seguridad descrita.

Una opción de alta seguridad es para que las claves de acceso se cifren en el dispositivo -14- de acceso. Para conseguir esta opción, durante el registro, así como la formación de una plantilla a partir de la huella dactilar del usuario y un código de verificación, se forma una plantilla a partir de la huella dactilar del usuario y una clave especial. La clave especial se utiliza posteriormente para cifrar cada clave de acceso. Durante la operación, cuando el dispositivo -14- de acceso recibe un identificador del dispositivo accionado mediante una clave y una huella dactilar del usuario, recupera cualquier clave de acceso cifrada asociada y ambas plantillas. Si la huella dactilar es la del usuario autorizado, la huella dactilar devuelve con éxito el código de verificación de una plantilla. Esto da como resultado que el dispositivo -14- de acceso envíe una indicación de verificación al dispositivo -12- accionado mediante una clave. El dispositivo accionado mediante una clave responde enviando una clave de cifrado temporal. El dispositivo de acceso utiliza entonces la huella dactilar para devolver la clave especial de la otra plantilla de la huella dactilar y la clave especial se utiliza entonces para descifrar la clave de acceso. El dispositivo -14- de acceso utiliza a continuación la clave temporal para cifrar la clave de acceso y envía la clave de acceso cifrada al dispositivo -12- accionado mediante una clave.

Será evidente para los expertos en la técnica que la transmisión de la clave de acceso recuperada se puede proteger mediante otros medios criptográficos. Por ejemplo, se puede utilizar una Infraestructura de Clave Pública (PKI), de manera que la clave de acceso recuperada es firmada digitalmente en primer lugar utilizando la clave privada del usuario (sinónimo de la clave especial anterior), y posteriormente es cifrada utilizando la clave pública del dispositivo accionado mediante una clave (sinónimo de la clave temporal anterior). Este paquete de datos cifrado se

envía posteriormente al dispositivo accionado mediante una clave. De esta manera, el usuario puede estar seguro de que únicamente la autoridad adecuada puede utilizar adecuadamente los datos transmitidos (dado que sólo ellos tienen la clave privada del dispositivo accionado mediante una clave para descifrar los datos), y el dispositivo accionado mediante una clave puede asegurar, en consecuencia, que el usuario autorizado se encontraba presente (verificando la firma digital de la clave de acceso recuperada utilizando la clave pública del usuario). Esto proporciona una fuerte autenticación mutua (en lugar de únicamente entre el dispositivo de acceso y el dispositivo accionado mediante una clave), dado que la firma digital sólo puede ser iniciada cuando el usuario proporciona una autenticación biométrica positiva. Esta realización proporciona no sólo una línea de transmisión segura entre el dispositivo de acceso electrónico y el dispositivo accionado mediante una clave, sino que también proporciona un elevador grado de responsabilidad de la transacción, dado que el usuario debe encontrarse presente para iniciar la firma digital.

Otros métodos para la transmisión segura de la clave de acceso recuperada serán evidentes para los expertos en la técnica.

Mientras que en la realización descrita el usuario es autorizado únicamente en el dispositivo de acceso portátil, sería posible que el dispositivo accionado mediante una clave participe en esta autorización. Más particularmente, durante el registro, el ordenador de registro puede pasar simplemente la plantilla al dispositivo de acceso portátil y no la indicación de verificación. En dicho caso, cuando se introduce un dato biométrico al dispositivo de acceso, se devuelve un código de verificación y este código se pasa directamente (en una forma cifrada o sin cifrar) al dispositivo accionado mediante una clave. El dispositivo accionado mediante una clave puede pasar entonces el código a una base de datos central que se utilizaría para mirar si el código es indicativo de un usuario válido. En dicho caso, el dispositivo accionado mediante una clave instaría al dispositivo de acceso a continuar. Además, el dispositivo accionado mediante una clave sólo respondería a cualquier clave transmitida por el dispositivo de acceso cuando el dispositivo accionado mediante una clave determina que el usuario es autorizado.

En el caso en el que el dispositivo de acceso transmite una indicación de usuario válido y el dispositivo accionado mediante una clave responde con una clave temporal, la indicación de usuario válido es, convenientemente, el código de verificación recuperado (cifrado o sin cifrar) y el dispositivo accionado mediante una clave insta, convenientemente, a la clave temporal.

Aunque el dispositivo -14- se muestra para ser utilizado con una entrada de huella dactilar, se pueden utilizar igualmente otros datos biométricos del usuario. Por ejemplo, el dispositivo de acceso -14- puede escanear el iris de un usuario.

Dado que cualquier dispositivo de verificación de datos biométricos tendrá una tasa de aceptación falsa distinta de cero, preferentemente, los dispositivos -14- accionados mediante una clave se programan para cerrarse o emitir un código de alarma tras un número predeterminado de intentos fallidos de verificación consecutivos por parte del usuario.

Otras modificaciones serán evidentes para los expertos en la técnica y, por tanto, la invención se define en las reivindicaciones.

REIVINDICACIONES

1. Método para acceder a dispositivos accionados mediante una clave que comprende

la recepción de un identificador del dispositivo accionado mediante una clave desde un dispositivo accionado mediante una clave (12);

la determinación de si dichos datos biométricos recibidos son datos biométricos autorizados;

la comparación de dicho identificador del dispositivo accionado mediante una clave recibido, con los identificadores de los dispositivos accionados mediante una clave almacenados y, al encontrar un identificador del dispositivo accionado mediante una clave coincidente y cuando dicho dato biométrico recibido es un dato biométrico autorizado, la recuperación de una clave de acceso almacenada asociada con dicho identificador del dispositivo accionado mediante una clave coincidente, y la transmisión de dicha clave de acceso recuperada.

2. Método, según la reivindicación 1, que comprende además:

la recepción de una clave temporal; y

el cifrado de dicha clave de acceso recuperada con dicha clave temporal antes de la transmisión de dicha clave de acceso recuperada.

3. Método, según la reivindicación 2, que comprende además:

la respuesta a la determinación de dichos datos biométricos es un dato biométrico autorizado, transmitiendo inicialmente una indicación de usuario válida.

4. Método, según la reivindicación 3, en el que dicha clave temporal se recibe en consecuencia a la transmisión de dicha indicación de usuario válido.

5. Método, según la reivindicación 3 o la reivindicación 4, en el que cuando se transmite inicialmente una indicación de usuario válido depende de encontrar un identificador del dispositivo accionado mediante una clave almacenado que coincide con dicho identificador del dispositivo accionado mediante una clave recibido.

6. Método, según cualquiera de las reivindicaciones 2 a 5, en el que cada una de dichas claves de acceso almacenadas se cifra y se incluye realizando una operación de descifrado sobre un clave de acceso recuperada antes de cifrar dicha clave de acceso recuperada con dicha clave temporal.

7. Método, según la reivindicación 6, en el que cada una de dichas claves de acceso almacenadas se cifra con una clave especial y en el que dicha realización de la operación de descifrado comprende la recuperación de una plantilla y el intento de recuperar dicha clave especial de dicha plantilla utilizando dichos datos biométricos recibidos.

8. Método, según cualquiera de las reivindicaciones 1 a 6, que comprende, además, la recuperación de una plantilla y el intento de recuperar una clave especial de dicha plantilla utilizando dichos datos biométricos, para utilizar dicha clave especial en la realización de la operación criptográfica.

9. Método, según la reivindicación 8, en el que dicha operación criptográfica implica al menos una de dichas claves de acceso.

10. Método, según cualquiera de las reivindicaciones 3 a 5, en el que dicha transmisión inicial de una indicación de usuario válido depende de encontrar un identificador del dispositivo accionado mediante una clave almacenado que coincide con dicho identificador del dispositivo accionado mediante una clave recibido.

11. Método, según cualquiera de las reivindicaciones 1 a 10, en el que dicha determinación de si los datos biométricos recibidos son unos datos biométricos autorizados comprende la utilización de una plantilla que comprende dichos datos biométricos autorizados y un código de verificación, de manera que la presencia de dichos datos biométricos permite la recuperación de dicho código de verificación.

12. Dispositivo (14) de acceso electrónico portátil que comprende:

una entrada de datos biométricos (26);

un transmisor (22) para transmitir una señal:

un receptor (22);

una memoria (24);

un verificador (20) que responde a dicha entrada de datos biométricos (26) para verificar que unos datos biométricos que se introducen en dicha entrada de datos biométricos (26) coincide con unos datos biométricos autorizados y proporciona una indicación de verificación;

caracterizado porque:

dicha memoria (24) almacena una serie de claves de acceso, para utilizar cada una de ellas para acceder a un dispositivo (12) accionado mediante una clave y una serie de identificadores de dispositivos accionados mediante una clave, asociado cada uno de ellos con una de dicha serie de claves de acceso;

dicho receptor (22) recibe un identificador de dispositivo accionado mediante una clave de acceso;

y dicho dispositivo (14) comprende, además:

un comparador (20) para, en respuesta a dicha indicación de verificación de dicho verificador, comparar un identificador de dispositivo accionado mediante una clave de un dispositivo accionado mediante una clave (12) con dichos identificadores de dispositivo accionados mediante una clave almacenados y, al encontrar un identificador de dispositivo accionado mediante una clave almacenado que coincide, recuperar una clave de acceso almacenada asociada con dicho identificador de dispositivo accionado mediante una clave almacenado coincidente, y

en el que dicha señal transmitida por dicho transmisor (22) es dicha clave de acceso recuperada.

13. Dispositivo (14), según la reivindicación 12, en el que dichas claves de acceso almacenadas se cifran y que incluye un aparato de descifrado para descifrar una clave de acceso recuperada antes de que dicha clave de acceso se transmita por dicho transmisor (22).

14. Dispositivo (14), según la reivindicación 12, en el que dicha memoria (24) también sirve para almacenar una plantilla de clave especial, dichas claves de acceso se cifran con una clave especial y dicho aparato de descifrado responde a dicha entrada de datos biométricos (26) para realizar una operación de recuperación de la clave especial en dicha plantilla de clave especial utilizando dichos datos biométricos introducidos y una posterior operación de descifrado de dicha clave de acceso recuperada utilizando una clave de acceso especial recuperada.

15. Dispositivo (14), según la reivindicación 12 o de la reivindicación 13, en el que dicha memoria (24) también sirve para almacenar una plantilla de clave especial que comprende dichos datos biométricos autorizados y una clave especial, para utilizar dicha clave especial en la realización de una operación criptográfica.

16. Dispositivo (14), según cualquiera de las reivindicaciones 12 a 15, en el que dicho verificador sirve para acceder una plantilla almacenada que comprende dichos datos biométricos autorizados y un código de verificación, para intentar la recuperación de dicho código de verificación a partir de unos datos biométricos de entrada y para utilizar dicho código de verificación para obtener dicha indicación de verificación.

17. Dispositivo (14), según cualquiera de las reivindicaciones 12 a 16, en el que dicho receptor (22) también sirve para recibir una clave temporal e incluye un aparato de cifrado para cifrar dicha clave de acceso recuperada con dicha clave temporal antes de la transmisión de dicha clave de acceso recuperada mediante dicho transmisor (22).

18. Dispositivo (14), según cualquiera de las reivindicaciones 12 a 17, en el que dicho transmisor (22) también sirve para transmitir inicialmente una indicación de usuario válido en respuesta a dicho verificador proporcionando dicha indicación de verificación.

19. Dispositivo (14), según la reivindicación 17, en el que dicho transmisor (22) también sirve para transmitir inicialmente una indicación de usuario válido en respuesta a dicho verificador proporcionando dicha indicación de verificación y en el que dicha clave temporal se recibe una vez dicho transmisor ha transmitido dicha indicación de usuario válido.

20. Dispositivo (14), según cualquiera de las reivindicaciones 12 a 19, en el que dicho receptor (22) comprende un receptor de radio y un receptor de infrarrojos y dicho transmisor (22) comprende un transmisor de radio y un transmisor de infrarrojos.

21. Sistema (10) de acceso seguro que comprende:

un dispositivo (12) accionado mediante una clave de datos para transmitir una señal;

un dispositivo (14) de acceso portátil que comprende:

una entrada de datos biométricos (26);

un transmisor (22) para transmitir una señal;

una memoria (24);

un receptor (22) para recibir dicha señal transmitida por dicho dispositivo accionado mediante una clave (12);

un verificador (20) que responde a dicha entrada (26) de datos biométricos para verificar que unos datos biométricos que se introducen coinciden con unos datos biométricos autorizados y

proporcionar una indicación de verificación;

caracterizado porque:

dicha memoria (24) almacena una serie de claves de acceso, para utilizar cada una de ellas para acceder a un dispositivo (12) accionado mediante una clave y una serie de identificadores de dispositivos accionados mediante una clave de acceso, asociado cada uno de ellos con una de dichas claves de acceso; dicha señal transmitida por dicho dispositivo accionado mediante una clave (12) es transmitida periódicamente y dicha señal transmitida por dicho dispositivo (12) accionado mediante una clave es un identificador de dispositivo accionado mediante una clave; y

dicho dispositivo (14) portátil comprende, además:

un comparador (20) para, en respuesta a dicha indicación de verificación de dicho verificador (20), comparar un identificador de dispositivo accionado mediante una clave recibido desde dicho dispositivo (12) accionado mediante una clave con dichos identificadores de dispositivo accionados mediante una clave almacenados y, si se encuentra una coincidencia, recuperar una clave de acceso asociada con dicho identificador de dispositivo accionado mediante una clave almacenado y cuando dicha señal transmitida por dicho transmisor (22) es dicha clave de acceso recuperada a dicho dispositivo accionado mediante una clave.

22. Sistema (10), según la reivindicación 21, en el que dicho receptor (22) sirve para recibir una clave temporal y en el que dicho dispositivo de acceso (14) incluye un aparato de cifrado para cifrar dicha clave de acceso recuperada con dicha clave temporal antes de la transmisión de dicha clave de acceso recuperada por dicho transmisor (22).

23. Sistema (10), según la reivindicación 21 ó 22, en el que dicho transmisor (22) sirve también para transmitir inicialmente una indicación de usuario válido en respuesta a dicho verificador (20) que proporciona dicha indicación de verificación a dicho dispositivo de acceso (14) y en el que dicho dispositivo accionado mediante una clave (12) sirve también, en respuesta a la recuperación de dicha indicación de usuario válido, para la transmisión de dicha clave temporal.

24. Sistema (10), según cualquiera de las reivindicaciones 21 a 23, en el que dicha memoria (24) sirve también para almacenar una plantilla y en el que dicho verificador (20) sirve también para intentar recuperar una clave especial de dicha plantilla utilizando dichos datos biométricos, para utilizar dicha clave especial en la realización de una operación criptográfica.

25. Sistema (10), según cualquiera de las reivindicaciones 21 a 24, en el que dicho transmisor (22) es un transmisor de radio y dicho receptor (22) es un receptor de radio.

26. Sistema (10), según cualquiera de las reivindicaciones 21 a 25, en el que dicho verificador (20) es para acceder a una plantilla almacenada que comprende dichos datos biométricos autorizados y un código de verificación, para intentar recuperar dicho código de verificación desde unos datos biométricos de entrada y para utilizar dicho código de verificación para obtener dicha indicación de verificación.

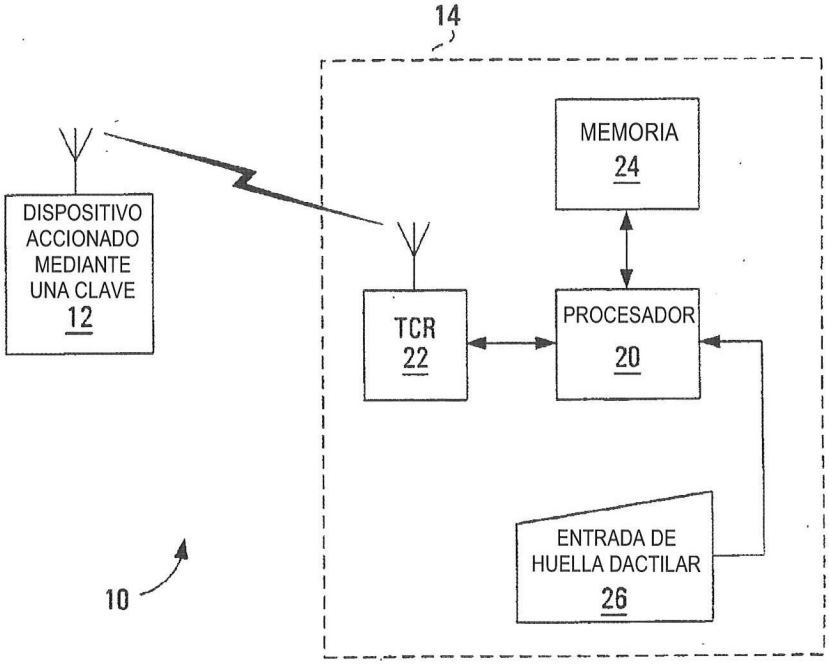
14
MEMORIA
24
DISPOSITIVO ACCIONADO MEDIANTE UNA CLAVE
12
TCR
22
PROCESADOR
20
ENTRADA DE HUELLA DACTILAR
26
10

FIG. 1

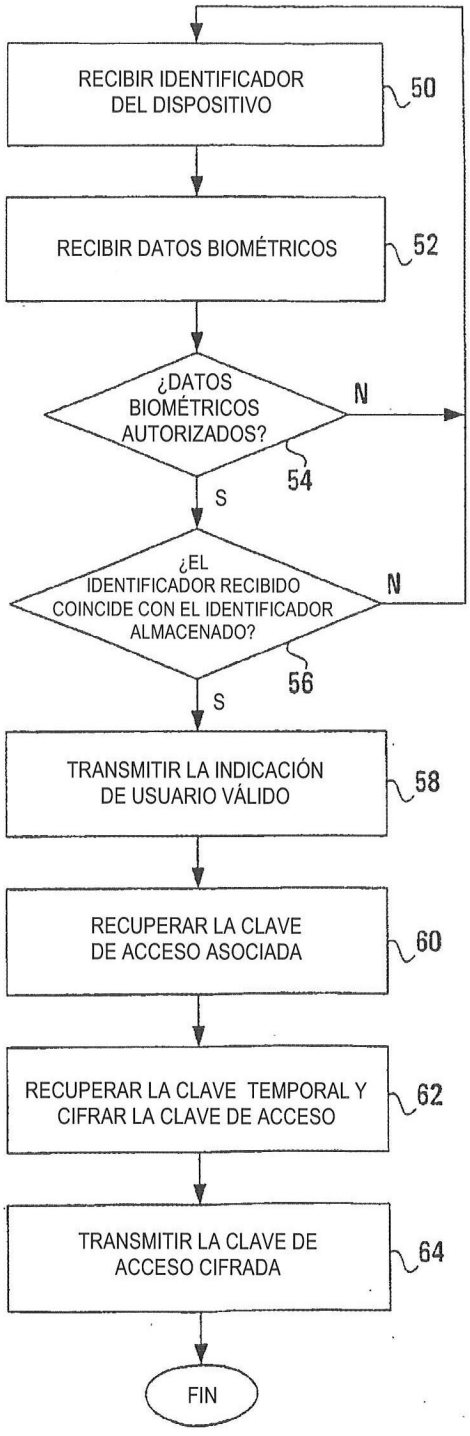
RECIBIR IDENTIFICADOR DEL DISPOSITIVO
50
RECIBIR DATOS BIOMÉTRICOS
52
¿DATOS BIOMÉTRICOS AUTORIZADOS?
54
N
S
¿EL IDENTIFICADOR RECIBIDO COINCIDE CON EL IDENTIFICADOR ALMACENADO?
56
N
S
TRANSMITIR LA INDICACIÓN DE USUARIO VÁLIDO
58
RECUPERAR LA CLAVE DE ACCESO ASOCIADA
60
RECUPERAR LA CLAVE TEMPORAL Y CIFRAR LA CLAVE DE ACCESO
62
TRANSMITIR LA CLAVE DE ACCESO CIFRADA
64
FIN

FIG. 2