(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 428 004**

(51) Int. CI.:

***G07C 9/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.09.2009 E 09170475 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.06.2013 EP 2306407**

(54) Título: **Sistema asegurado de gestión de cerraduras de control digital, adaptado a un funcionamiento mediante acreditaciones acústicas cifradas**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**05.11.2013**

(73) Titular/es:

**OPENWAYS SAS (100.0%)**
**5 rue d'Ankara**
**75016 Paris, FR**

(72) Inventor/es:

**METIVIER, PASCAL**

(74) Agente/Representante:

**FÀBREGA SABATÉ, Xavier**

## DESCRIPCIÓN

Sistema asegurado de gestión de cerraduras de control digital, adaptado a un funcionamiento mediante acreditaciones acústicas cifradas

La invención se refiere a dispositivos de cierre controlados eléctricamente por medio de una llave desmaterializada y cifrada, pudiendo esta llave vehicularse mediante un objeto portador ostentado por el usuario, como por ejemplo una tarjeta magnética, una tarjeta chip, un identificador o una tarjeta sin contacto, etc.

Por “dispositivo de cerradura” se entenderá no solamente una cerradura *stricto sensu*, es decir un mecanismo situado por ejemplo sobre una puerta para clausurar la apertura, sino igualmente cualquier dispositivo que permita alcanzar un resultado comparable, por ejemplo, un cilindro de cerradura considerado de forma aislada o un dispositivo de cierre más específico que comprenda diversos órganos no reagrupados en un mismo palastro de cerradura, siendo el objetivo final obtener la clausura por medios mecánicos del acceso físico a un lugar o espacio dado y el acceso a ese lugar o espacio por el desbloqueo del dispositivo de cerradura, sometidos al control de un usuario, tras la verificación de que este usuario dispone efectivamente de los derechos de acceso (i) que le son propios y (ii) que son propios del dispositivo de cerradura. El dispositivo de cerradura puede igualmente comprender, o estar asociado con, un sistema de alarma que se pretende desactivar para permitir el acceso a un espacio dado o, a la inversa, activarlo para proteger este espacio después de haberlo abandonado.

Para simplificar la descripción, se hablará a continuación simplemente de “cerradura”, pero este término debe entenderse en el sentido más amplio, sin ningún carácter restrictivo a un tipo de equipamiento particular.

El objeto portátil cuando se aproxima a la cerradura, desempeña el papel de una llave que permite controlar la apertura por medio de un dato designado a continuación como “acreditación” (*credential)*. Pueden aplicarse diversas técnicas de codificación y de cifrado en la cerradura y/o en el objeto portátil para asegurar una protección contra manipulaciones fraudulentas y asegurar la comunicación entre el objeto portátil y la cerradura. Se conocen numerosos sistemas con tarjetas magnéticas, o incluso con tarjetas o identificadores con microcircuito que aplican a la cerradura un acoplamiento galvánico (tarjeta chip de contactos) o no galvánico (tarjeta de acoplamiento inductivo o tarjeta de tipo RFID). Este acoplamiento asegura una comunicación entre la cerradura y el identificador que permite a la cerradura en particular leer en la memoria del identificador el dato de acreditación con el fin de accionar la apertura si este dato es reconocido como conforme.

Uno de los inconvenientes de esta técnica es la necesidad de disponer de un objeto portátil específico, que debe ser remitido al usuario y que éste debe conservar con él. Esto conlleva además la multiplicación de objetos portátiles, cada uno de ellos correspondiente a una cerradura diferente (domicilio, oficina, puerta de inmueble, garaje, etc.,), lo que hace que todo ello al final sea engorroso y propenso a olvidos.

El documento US 5 933 090 A describe un sistema de este tipo de desbloqueo controlado a distancia y sin contacto físico mediante un objeto específico dedicado a la apertura del tipo concreto de cerradura considerado.

Otro inconveniente está unido a la diversidad de técnicas aplicadas, teniendo cada fabricante sus propias especificaciones tanto al nivel de la capa física (elección tecnológica del acoplamiento: inductivo, RF, magnético, galvánico, etc.) como al nivel del formato de los datos y de los protocolos de intercambio de estos datos entre el lector y el objeto portátil. Esta diversidad de técnicas unida a las elecciones tecnológicas y a las implementaciones propias de los diferentes constructores, constituye un freno a la interoperabilidad, a la estandarización de los materiales y de los procedimientos y a la evolución tecnológica, lo que impide la rápida generalización de estas técnicas, a pesar de sus incontestables ventajas.

Asimismo, el sistema es un sistema estereotipado, pues si se desea actualizar las habilitaciones, suprimir las habilitaciones existentes o crear otras nuevas, es preciso proceder al cambio del objeto portátil, o bien poner al día la memoria de dicho objeto por medio de un protocolo y/o de un lector específico, con la necesidad de manipulaciones físicas y de desplazamientos.

Uno de los objetivos de la invención es proponer una técnica alternativa de gestión y de accionamiento de cerraduras que pueda completar las técnicas existentes, o incluso sustituirlas, sin necesidad de modificaciones sustanciales tanto al nivel del material como del software, y que ofrezca un nivel de seguridad máximo, una alta elasticidad de puesta en práctica y que sea utilizable sin recurrir a un objeto portátil específico. Como se verá a continuación, la técnica de la invención es utilizable por medio de cualquier teléfono móvil convencional que sirva como objeto portátil de vehículo de la llave de accionamiento de la cerradura, sin que el usuario tenga la necesidad de recurrir a un objeto portátil específico y dedicado, como por ejemplo un identificador o una tarjeta.

El documento WO 03/093997 A1 propone un sistema de control de acceso accionado mediante un dispositivo universal a disposición del usuario, como un asistente digital (PDA) o un teléfono móvil. El sistema, y en particular las cerraduras, debe sin embargo estar concebido de manera específica para ser controlado mediante un dispositivo de este tipo.

Desde el punto de vista del fabricante de cerraduras, la técnica de la invención se distingue de este documento

porque permitirá adaptar sin una modificación importante el parque de cerraduras existentes, sin tener que sustituir ni los elementos materiales ni el software ya integrados en la cerradura. Se apreciará, en efecto, que la invención es perfectamente compatible con las técnicas preexistentes aplicadas por los diferentes fabricantes actuales, en la medida en que limita la intervención a una sola capa del protocolo de comunicación (la transmisión de la acreditación a la cerradura), conservando por tanto la misma gestión lógica de los diferentes niveles de seguridad ya previstos por el fabricante.

El principio de la invención descansa en la utilización, para la transmisión del dato de acreditación a la cerradura, de informaciones del tipo de acreditaciones acústicas cifradas.

Estas acreditaciones acústicas se presentan, por ejemplo, en forma de una serie codificada de tonalidades (tonalidades DTMF u otras), emitidas por el altavoz de un dispositivo emisor y captadas por el micrófono de un dispositivo receptor.

Esencialmente, la presente invención consiste en traducir, al nivel de un emplazamiento asegurado, la acreditación convencional utilizada para la gestión de acceso (un bloque de datos que comprende un identificador del fabricante, un identificador único de la cerradura y eventualmente unas informaciones adicionales) y de traducirlas a un formato de acreditación acústica cifrada. Esta acreditación acústica se presenta en forma de una señal de audio que puede transmitirse por unos canales de transmisión de audio, en particular unos canales de transmisión telefónica, y reproducirse tal cual por unos transductores acústicos.

La acreditación acústica se envía de esta manera al teléfono móvil del usuario, que está inscrito en una base de datos del emplazamiento asegurado. Para utilizar la acreditación, el usuario acerca su teléfono a la cerradura y desencadena la emisión por el altavoz de su teléfono de la serie de tonalidades correspondiente a la acreditación acústica cifrada, de manera que estas tonalidades puedan ser captadas por un micrófono incorporado o acoplado a la cerradura. Esta última opera una traducción inversa de la acreditación acústica que permite restituir el formato original de la acreditación convencional, que se aplica después a los circuitos de la cerradura para ser tratada en ellos de la misma forma que si esta acreditación hubiera sido leída por un lector estándar acoplado a la cerradura (lector de tarjetas magnéticas o de chip, lector de acoplamiento inductivo o de RFD, etc.).

La utilización de acreditaciones acústicas no es en sí misma novedosa, ha sido ya propuesta en otros contextos y para otras aplicaciones, por ejemplo por el documento WO 2008/107595 A2 (Tagattitude).

Este documento describe una técnica de aseguramiento del acceso lógico a una red informática mediante un terminal distante, por ejemplo mediante un ordenador unido a esta red a través de Internet. El usuario se conecta a la red con su ordenador, enciende al mismo tiempo su teléfono móvil y llama por medio de éste a un emplazamiento de control situado en interfaz con la red a la que se solicita acceso. Para verificar la habilitación del usuario, la red envía una señal sonora (la acreditación acústica) hacia el ordenador distante que acaba de conectarse y la señal es reproducida por el altavoz del ordenador. Habiendo colocado el usuario su teléfono delante de este altavoz, esta señal sonora es captada por el teléfono, transmitida al emplazamiento de control distante por medio del operador de la red telefónica móvil y “escuchada” por el emplazamiento de control, que puede entonces verificar la acreditación y autorizar el acceso a la red informática por el terminal.

Se observará que en este caso se trata de una acreditación “ascendente”: la acreditación acústica es captada por el micrófono del teléfono, que la retransmite al emplazamiento de control. Conociendo el destinatario de la llamada telefónica, el emplazamiento de control puede identificar al usuario por medio del teléfono móvil utilizado para esta operación y autorizar así el acceso lógico a la red por el terminal situado a proximidad del teléfono así identificado. En el caso de la invención, las acreditaciones acústicas cifradas son, por el contrario, acreditaciones “descendentes”, es decir, que se emiten desde un emplazamiento gestionador distante y se transmiten al teléfono móvil del usuario.

Más exactamente, la invención se refiere, de una forma en sí conocida, a un sistema de seguridad de control de apertura de dispositivos de cerradura, del tipo general divulgado por el documento WO 03/093997 A1 precitado, que comprende los elementos enunciados en el preámbulo de la reivindicación 1.

Para alcanzar los objetivos indicados más arriba, la invención propone combinar los elementos enunciados en la parte caracterizadora de la reivindicación 1.

Las subreivindicaciones exponen diversas aplicaciones posibles de la invención, así como perfeccionamientos ventajosos.

A continuación se describirá un ejemplo de aplicación del dispositivo de la invención con referencia a los dibujos adjuntos, en los que las mismas referencias designan en todas las figuras elementos idénticos o funcionalmente similares.

La Figura 1 ilustra de forma esquemática los principios elementales que contribuyen al funcionamiento del sistema de acuerdo con la invención.

La Figura 2 ilustra más exactamente, en forma de esquema por bloques los principales órganos constitutivos del teléfono móvil y de la cerradura con la que este último está acoplado.

La Figura 3 ilustra las diferentes transformaciones experimentadas por la acreditación en el curso de las etapas desarrolladas por la invención.

La Figura 4 es una serie de cronogramas que ilustran las diversas técnicas de seguridad que permiten asegurar la utilización exclusiva de la acreditación acústica en el marco de la invención.

Se describirán, en primer término, con referencia a las Figuras 1 y 2, los diferentes elementos que sirven para implementar la invención. Se describirán luego las diversas maneras de ponerla en práctica, así como variantes perfeccionadas que permiten reforzar su seguridad.

*Arquitectura general del sistema*

Uno de los elementos esenciales de la invención es un emplazamiento gestor asegurado 10 que centraliza, en una base de datos DB 12, las informaciones que permiten inventariar e identificar un cierto número de cerraduras y de usuarios habilitados para cada una de estas cerraduras. Para cada usuario, la base de datos inscribe un número de teléfono móvil único asociado con este usuario, así como datos del derecho de acceso y condiciones de utilización (acceso reservado a ciertos días o a ciertas franjas horarias, fecha de caducidad de un derecho de acceso, etc.).

Además de los usuarios habilitados, la base de datos realiza también el inventario para cada cerradura de un identificador UID (*Unique IDentifier)* que es atribuido de manera exclusiva y permite identificar de manera unívoca la cerradura en los diversos protocolos de intercambio de datos.

Otros datos pueden ser igualmente ser conservados por la base de datos, especialmente los algoritmos utilizados por la cerradura, una o varias claves criptográficas, una denominación libre simplificada (“entrada”, “garaje”, “bodega”, etc.) para facilitar la selección por un usuario de una cerradura entre varias, etc.

El emplazamiento gestor 10 comprende igualmente un motor criptográfico que forma el generador 14 de datos de acreditación.

Como característica distintiva de la invención, los “datos de acreditación” (*credentials)* son acreditaciones acústicas cifradas o CAC (*Crypto Acoustic Credential)* en forma de señales de audio de uso exclusivo, por ejemplo (pero de forma no limitativa) constituidas por una sucesión de tonalidades dobles DTMF. Estas señales de audio están concebidas para poder transferirse después de su digitalización por unos canales de transmisión de audio telefónico y reproducirse tal cual por unos transductores acústicos.

El emplazamiento gestor 10 está acoplado a una red 16 de un operador de telefonía móvil MNO (*Mobile Network Operator)* por medio de una pasarela telefónica de audio PGW (*Phone GateWay)* 18 y de un enlace asegurado 20, por ejemplo un enlace IP de tipo *https*, para poder transmitir las acreditaciones acústicas desde el generador 14 hasta el teléfono 22 del usuario por los canales de transmisión de audio (canal de voz) de la red de telefonía móvil.

La red de telefonía móvil 16 se utiliza de manera convencional por sus diversos abonados, estando cada usuario en posesión de un teléfono móvil 22 que le es propio, individualizado por las informaciones de la tarjeta SIM contenida en el aparato telefónico o por otro elemento exclusivo si el teléfono opera sin tarjeta SIM. De esta manera, cuando utiliza su teléfono móvil personal, un usuario es reconocido e identificado por la red 16 por medio de su número de abonado y, por tanto, de la misma manera por el emplazamiento gestor 10.

La seguridad del enlace entre la red 16 y el teléfono móvil 22 puede ser operada por medio de un proveedor de servicios de confianza o TSM (*Trusted Service Manager)*, que permite asegurar de manera eficaz y segura los diversos procedimientos que se describirán de intercambio o de transmisión de informaciones entre el emplazamiento gestor 10 y el teléfono móvil 22 a través del operador de la red móvil 16.

En el caso de una llave materializada por un soporte, como una tarjeta o un identificador, una parte importante de la seguridad queda asegurada por la entrega física de este objeto al usuario legítimo, de la misma manera que la entrega de un juego de llaves. Por contra, en el marco de la invención, el objeto utilizado es un teléfono móvil, por tanto un objeto banalizado. Pero éste es reconocido y autenticado por la tarjeta SIM que contiene (o por otro elemento exclusivo) y que, sobre todo, identifica al usuario por medio de su número de teléfono (número de abonado). El emplazamiento gestor 10 puede, por tanto, identificar de este modo dicho teléfono, al que ha sido unido por medio del operador de la red móvil 16, como tratándose efectivamente del teléfono del usuario habilitado, registrado en su base de datos 12.

La puesta en práctica de la invención implica hacer reproducir por el altavoz 24 del teléfono móvil 22, como señal de audio, la acreditación acústica cifrada generada por el generador criptográfico 14 y transmitida en forma de señal vocal por medio de la pasarela telefónica 18 y del operador de la red móvil 16.

La acreditación reproducida por el altavoz 24 del teléfono móvil está destinada a ser captada por un micrófono 26 de una cerradura 28 con el fin de ordenar la apertura de esta cerradura. Se trata de permitir al usuario, detentador del

número de teléfono móvil 22 conocido por la base de datos 12, demostrar a la cerradura 28 que ostenta efectivamente la identidad que proclama y que es beneficiario de los derechos de acceso que permiten la apertura de esta cerradura. La señal sonora reproducida constituye así un justificante de la identidad del usuario y de sus derechos de apertura, de ahí la terminología “acreditación acústica”. Esta acreditación acústica está además cifrada (por medios criptográficos ya conocidos) y es de uso exclusivo con el fin de evitar cualquier fraude por registro y duplicación, pues si no sería muy fácil registrar la señal acústica y reproducirla luego a voluntad.

La Figura 2 ilustra, en forma de un esquema por bloques, los principales órganos del teléfono móvil 22 y de la cerradura 28.

El teléfono 22 incorpora un microcontrolador 30 acoplado a diversos órganos periféricos tales como un circuito de emisión/recepción 32, una pantalla 34, un teclado 36, una memoria de datos 38, una tarjeta UICC (*Universal Integrated Circuit Card,* correspondiente a la “tarjeta SIM” para las funciones de telefonía GSM) 40 y el transductor acústico 24.

Para aumentar la seguridad del proceso pueden adoptarse diversas precauciones, ya conocidas, especialmente mediante una validación suplementaria solicitada por el usuario, por ejemplo la introducción de un código personal del tipo “código PIN” o una validación de tipo biométrico, por un lector biométrico incorporado al teléfono, o por medio de un sistema de reconocimiento de impresiones vocales que utilicen el micrófono del teléfono (pudiendo la impresión biométrica especifica estar almacenada en la memoria 38 del teléfono o bien en la tarjeta UICC 40 o incluso en la base de datos 12).

La cerradura 28, por su parte, comprende un microcontrolador 44 así como un sistema electromecánico 46 que permite controlar el desbloqueo de un pestillo o de un picaporte 48 por orden del microcontrolador 44. Una memoria de datos 50 conserva diversos datos modificables exclusivos de la cerradura, en especial:

- el identificador único UID (*Unique IDentifier)* que permite reconocer esta cerradura entre todas, de manera unívoca;

- algoritmos de reconocimiento y de descodificación;

- claves criptográficas;

- así como otros parámetros específicos para la puesta en práctica de la invención y que se describirán a continuación.

Existen numerosos modelos de cerraduras de este tipo, propuestos por un gran número de fabricantes. La apertura se controla por un módulo lector 52 integrado en la cerradura, que comprende una interfaz de comunicación con una llave o con un identificador, mediante un acoplamiento que puede ser galvánico (lector de tarjeta chip) o no galvánico (lector óptico para identificador que incorpora un código de barras, lector de tarjeta magnética, lector sin contacto de acoplamiento inductivo o de RF, etc.). El lector 52 transmite al microcontrolador 44 una acreditación en datos digitalizados, en lo sucesivo designada DDC (*Digital Data Credential)*, de acuerdo con un formato y un contenido propios de cada fabricante y que comprende típicamente (pero no exclusivamente)), como se ilustra en la línea a de la Figura 3:

- un identificador del fabricante VID (*Vendor ID)*;

- el identificador único UID de la tarjeta,

- y un campo DATA (facultativo) que contiene diversos datos necesarios o útiles para el control del funcionamiento de la cerradura.

Esta acreditación en datos digitales DDC, leída por el módulo 52 en una llave o identificador que el usuario ha acoplado con este módulo, es analizada por el microcontrolador 44, que transmite condicionalmente una autorización de apertura de la cerradura 46 si se satisfacen los criterios requeridos, especialmente la conformidad del identificador UID.

La invención propone sustituir el módulo 52, o completar este módulo 52, por un módulo 54 adecuado para procesar las acreditaciones enviadas a la cerradura en forma de acreditaciones acústicas CAC emitidas por un teléfono móvil 22, en lugar de acreditaciones digitales DDC leídas en una tarjeta o en un identificador acoplado al módulo 52.

El módulo acústico 54 está provisto de un transductor acústico en forma de un micrófono 56 que permite captar las señales sonoras del entorno, en particular la acreditación acústica que será reproducida por el altavoz 24 del teléfono 22, y transformar las señales acústicas captadas en señales digitales aplicadas a una capa 58 que forma el transductor, para convertir las acreditaciones acústicas CAC en señales del mismo formato que las acreditaciones en datos digitales DDC que habría suministrado el módulo 52 por la lectura de un identificador o de una tarjeta.

El módulo acústico 54 comprende igualmente, de manera ventajosa, un transductor 60 que permite reproducir una señal sonora emitida por la capa 58 y audible desde el exterior de la cerradura, pudiendo este transductor 60

comprender un altavoz o, en una versión simplificada, un simple componente de tipo *buzzer* (zumbador). Es asimismo posible utilizar el transductor 46 del módulo acústico 54 haciéndolo funcionar de manera inversa (para emitir señales sonoras en lugar de captarlas).

*Puesta en práctica de la invención*

A continuación se describirán diversos modos operativos para la puesta en práctica de la invención por medio de los diferentes medios del sistema que se acaba de describir.

El primer objetivo de la invención es el de sustituir, o completar, la tecnología “propietaria”, específica del fabricante e implementada en el módulo lector 52, por una tecnología universal a base de acreditaciones acústicas cifradas CAC, que puede ponerse en práctica sin una modificación sustancial de los órganos de la cerradura, tanto materiales como de software.

El principio básico consiste en conservar las acreditaciones en datos digitales (DDC) originales con el contenido y el formato propios del fabricante, y convertir estas acreditaciones DDC en acreditaciones acústicas CAC, transmitir las CAC por teléfono, y a continuación hacer reproducir por el usuario, por medio del altavoz de su teléfono móvil, la acreditación acústica CAC así transmitida. La acreditación captada por el módulo acústico 54 es entonces objeto de una conversión inversa, operada por la capa 58 de traducción incorporada al módulo acústico 54, con el fin de reconstituir la acreditación en datos digitales DDC original a partir de la acreditación acústica CAC que ha sido captada.

Una etapa preliminar consiste, por tanto, en convertir la acreditación digital DDC en una acreditación acústica cifrada CAC.

La acreditación digital DDC puede tener varios orígenes (ver Figura 1), al estar generada:

- en tiempo real por un tercer emplazamiento 62, es decir tras la solicitud del usuario en el momento en que este quiere abrir la cerradura;

- por el tercer emplazamiento 62 en el modo “fuera de línea”, siendo remitidas las acreditaciones de antemano en forma de lotes;

- de forma manual por medio de un lector 64, a partir de una clave o de un identificador convencional 66;

- o bien directamente por el emplazamiento asegurado 10, conservándose la acreditación digital DDC en la base de datos 12.

Estas acreditaciones DDC en forma de bloques de datos digitales son convertidas por el motor criptográfico 14 del emplazamiento asegurado 10 en acreditaciones acústicas CAC.

Como se ilustra en la Figura 3, la conversión puede efectuarse a partir de un bloque de datos en el que los campos VID, UID y DATA se presentan de manera explícita, hacia un campo CORE/CAC de la acreditación acústica CAC (de la línea a hacia la línea c de la Figura 3). Sin embargo, el motor criptográfico puede perfectamente recibir en este estadio la información en una forma no explícita (CORE), que es directamente convertida para dar el campo CORE/CAC de la acreditación acústica CAC (de la línea b hacia la línea c de la Figura 3). En efecto, el conocimiento del contenido de la acreditación digital DDC no es necesario para operar la conversión, que consiste simplemente en crear un “envoltorio” acústico en el que se “desliza” la acreditación digital DDC, con independencia del contenido de esta última, ya que el motor criptográfico 14 no tiene necesidad de conocer la definición de los campos, de la codificación, etc., de la acreditación DDC.

El motor criptográfico 14 añade igualmente al campo CORE/CAC que contiene los datos de acreditación propiamente dichos, un campo variable, diferente en cada generación de una acreditación acústica, con el fin de convertir en exclusiva esta acreditación acústica. Puede tratarse de un dato producido por un generador pseudoaleatorio o, de modo preferente, de un número de secuencia SEQ. El campo SEQ puede ser un contador incrementado en cada generación por una acreditación por el generador criptográfico 14, o incluso un fechado que será funcionalmente equivalente al incremento de un contador.

El generador criptográfico 14 puede asimismo prever la adición a la acreditación acústica CAC de una contraseña PWD que permita aumentar aún más la seguridad del proceso.

Cuando desea lograr la apertura de la cerradura ante la que se encuentra, el usuario entra en contacto con el emplazamiento gestor mediante cualquier medio apropiado. Esto puede conseguirse mediante la llamada de un número telefónico o mediante el envío de un mensaje (SMS, MMS, correo electrónico, mensajería instantánea, etc.) al servidor, que volverá a llamar al teléfono del usuario para transmitirle la autorización en forma de una acreditación acústica cifrada.

En un modo de puesta en práctica “en línea”, la transmisión de esta acreditación se ejecuta inmediata y directamente. Como variante, puede asimismo ejecutarse por un procedimiento de tipo “call back”: en este caso, el

usuario entra en contacto telefónico con el emplazamiento gestor que no le responde inmediatamente, sino que después de volver a colgar hace sonar el teléfono móvil para que el usuario establezca de nuevo el contacto con el emplazamiento, y es en este momento cuando la acreditación acústica le es transmitida. Cualquiera que sea la manera mediante la que el usuario entra en contacto con el emplazamiento distante, éste transmite la acreditación acústica directamente al usuario, sin almacenamiento intermedio.

Este modo es particularmente sencillo de poner en práctica, en la medida en que basta utilizar la infraestructura existente, sin adaptación anterior del teléfono, en concreto sin necesidad alguna de cargar un subprograma o *applet*, en especial del tipo *midlet* o *cardlet*. La invención puede ponerse así en práctica con cualquier tipo de teléfono móvil, incluso muy sencillo y sin ninguna intervención anterior sobre este. Otra ventaja reside en la posibilidad de verificar en tiempo real la validez de la acreditación con, por ejemplo, la posibilidad de tomar en consideración inmediatamente una “lista negra” de usuarios. Además, gracias a este modo en línea, es posible disponer, al nivel del emplazamiento gestor, de un gran número de informaciones sobre la utilización efectuada de la acreditación acústica, especialmente sobre la fecha y la hora de la utilización y eventualmente la situación geográfica del usuario (mediante identificación de la célula de la red desde la que el usuario llama). Por contra, este modo implica disponer de un acceso a la red móvil, lo que no es siempre posible (aparcamientos subterráneos, zonas no cubiertas, etc.). Por otro lado, no permite, en principio, disponer, a elección del usuario, de varias acreditaciones correspondientes a diversas cerraduras posibles, en la medida en que es necesario tener una correspondencia “una por una” entre acreditación y cerradura.

Otro modo de puesta en práctica “fuera de línea” es utilizable en especial si el acceso a la red no está asegurado en el momento de la utilización. En este caso, el usuario se conecta de antemano con el emplazamiento gestor y recibe de éste un número predeterminado de acreditaciones acústicas. Estas acreditaciones son almacenadas de forma segura en el teléfono o en una memoria periférica del teléfono (por ejemplo una tarjeta SD o MicroSD). Cuando el usuario quiere reproducir una acreditación acústica para abrir una cerradura, lanza una aplicación integrada en su teléfono que busca la primera acreditación entre las que se han almacenado, la reproduce para abrir la puerta, después la suprime de la memoria. Y así sucesivamente para utilizar las acreditaciones siguientes. La aplicación que permite esta puesta en práctica es un subprograma conservado en el teléfono, anteriormente enviado a éste a través del operador de la red móvil, o bien por descarga sobre un soporte externo (tarjeta SD o MicroSD), o incluso a través de una conexión con Internet. En el caso de una descarga a través del operador de la red móvil, el emplazamiento gestor habrá enviado anteriormente un mensaje, por ejemplo de tipo “SMS”, “push SMS” o “WAP push” al teléfono con el fin de identificar la marca y el modelo del mismo y presentar al usuario un enlace que permita la descarga del subprograma. Cuando la provisión de acreditaciones almacenadas en el teléfono esté agotada, o esté en vías de agotamiento y el usuario sea capaz de acceder a la red, se recargará esta reserva de acreditaciones para permitir acreditaciones ulteriores. Es posible aprovechar el enlace con la red para, al mismo tiempo, hacer ascender hacia el emplazamiento gestor un cierto número de informaciones, especialmente un historial de la utilización de las acreditaciones precedentes.

En cualquier caso, y con independencia del modo de transmisión de la acreditación acústica cifrada CAC, cuando desea conseguir la apertura de la cerradura, el usuario coloca su teléfono móvil cerca de la cerradura que desea desbloquear y desencadena la emisión, en forma de señal sonora, de la acreditación acústica CAC.

Como se ha explicado anteriormente, el módulo acústico 54 de la cerradura recibe esta acreditación acústica cifrada CAC (correspondiente a la línea c de la Figura 3). La capa de traducción 58 extrae entonces de ello el bloque de datos CORE (línea d de la Figura 3), es decir, en términos de imágenes, “abre el envoltorio (acústico)” que contiene estos datos. Entonces es posible obtener, directamente o después de la descodificación, una acreditación en datos digitales DDC (línea e de la Figura 3) con sus diferentes campos útiles VID, UID y DATA, que es idéntica a la acreditación correspondiente DDC antes de que esta haya sido convertida por el motor criptográfico (línea a de la Figura 3).

La acreditación DDC, que en todos los puntos es idéntica a la que habría sido leída por el módulo 52 a partir de una llave o de un identificador convencional según las prescripciones propias del fabricante, se aplica al microcontrolador 44 para el análisis, verificación y desbloqueo condicional del sistema 46 de control de la cerradura.

Se observará que las diferentes verificaciones operadas por el microcontrolador 44 son idénticas a las que habrían sido efectuadas a partir de informaciones leídas de manera convencional por el módulo 52, según las especificaciones propias de cada fabricante. El papel de la capa traductora 58 es simplemente el de “abrir el envoltorio” de la acreditación acústica CAC para extraer del mismo las informaciones digitales DDC que habían sido antes situadas en este envoltorio por el motor criptográfico 14, pero sin intervenir en el contenido de esta acreditación digital DDC.

*Detección de fraudes por captación de señal*

Pueden contemplarse diversas medidas para evitar fraudes, en especial el que consistiría en registrar la señal de audio reproducida por el teléfono en el momento de la utilización, después utilizar esta señal registrada para abrir otra cerradura o para intentar obtener una nueva apertura de la misma cerradura (mientras que la acreditación es normalmente de uso único y debe renovarse cada vez).

1º) Control de la unicidad de la acreditación acústica: debido a la presencia del campo único SEQ generado de forma que difiera en cada versión de la acreditación acústica CAC, el sistema no debe nunca producir dos acreditaciones acústicas idénticas. De ello se deriva que el módulo acústico de la cerradura debe poder detectar y rechazar una acreditación que ya se haya producido y que sería por tanto una acreditación fraudulenta captada y reutilizada.

Con este fin, en el momento de la inicialización de la cerradura (en el momento de la instalación del módulo acústico 54 o con ocasión de una reinicialización del mismo), se pone a cero un registro del módulo 54. En el momento de la primera utilización, es decir cuando se capta la utilización de la primera acreditación acústica CAC, el módulo 54 memoriza el número de secuencia SEQ incluido en esta acreditación acústica (o la fecha Y la hora, en el caso de un fechado).

En cada utilización ulterior, el módulo 54 verifica que el número de secuencia de la acreditación captada es superior AL número de secuencia que había conservado en memoria en el registro (o verifica que la fecha y la hora son posteriores a las informaciones correspondientes memorizadas). Si no es este el caso, la apertura se rechaza, ya que se trata de un fraude. Por contra, si la condición se cumple, la cerradura se desbloquea y el registro se actualiza con el nuevo número de secuencia (o con los nuevos valores de fecha y hora).

2º) Generación de un marcado temporal por la cerradura: otra medida de precaución, explicada especialmente con referencia a la Figura 4, consiste en hacer emitir por el HP o por el zumbador 60 del módulo acústico 54 durante la recepción de la acreditación acústica CAC o justo después de esta, un parásito acústico o “bip” en un instante predefinido, siempre el mismo para una cerradura determinada pero siempre diferente de una cerradura a otra.

Sobre la línea a del cronograma de la Figura 4 se ha ilustrado la acreditación acústica CAC emitida por el teléfono, y sobre la línea b el bip, designado BEEP1, emitido por el módulo acústico 54 en un instante alejado de $T_1$ con relación al inicio de la recepción de la acreditación CAC.

La señal escuchada cerca del teléfono y, por tanto, susceptible de ser registrada, es esta línea ilustrada c con la superposición de la señal CAC emitida por el teléfono y de la señal BEEP1 emitida por el módulo acústico de la cerradura.

Si un impostor registra esta señal combinada y la presenta en otra cerradura como acreditación acústica, esta otra cerradura va a emitir un parásito BEEP2 según la misma técnica que la primera, pero en una posición temporal $T_2$ diferente (línea d de la Figura 4).

La señal combinada recibida por el modelo acústico de esta otra cerradura será, por tanto, la línea ilustrada e de la Figura 4, es decir, una señal que incorpora dos parásitos acústicos BEEP1 y BEEP2. La presencia de estos dos parásitos será inmediatamente reconocida por el módulo acústico, que rechazará la apertura.

Se observará que, si el impostor había representando sobre la misma cerradura (y no sobre otra cerradura) la acreditación acústica CAC que había registrado, ésta correspondería a la línea f de la Figura 4 con, por tanto, un parásito acústico BEEP1 confundido con el emitido en el mismo momento por el módulo acústico 54. Pero en este caso el número de secuencia SEQ1 sería igual, o inferior, al ya registrado en la memoria del módulo acústico de la cerradura, que podrá así detectar el fraude por el hecho de que este número de secuencia SEQ1 no es conforme.

*Seguridades adicionales con comunicación bidireccional*

Una comunicación bidireccional puede establecerse con el emplazamiento asegurado 10 si al teléfono le es posible obtener un enlace con la red en el momento de la utilización, lo que permite hacer ascender hacia éste informaciones provenientes del teléfono.

En particular, con anterioridad a la generación de la acreditación acústica CAC, el módulo acústico 54 de la cerradura puede producir en forma acústica una contraseña, que es captada por el micrófono del teléfono, después transmitida a la red y al emplazamiento distante 10 para ser incorporada a la acreditación acústica CAC que va a generarse por el motor criptográfico 14 (campo PWD de la línea c de la Figura 3). La acreditación acústica CAC reproducida a continuación por el teléfono incluirá, por tanto, esta contraseña, que podrá entonces ser descodificada por el módulo acústico 54, que verificará que concuerda perfectamente con la que acaba de generarse por este mismo módulo justo antes.

Como variante o como complemento de esta contraseña, otra seguridad consiste en hacer generar por el módulo acústico 54 un valor de retardo o desajuste temporal $\Delta t_1$, diferente cada vez (por ejemplo un retardo aleatorio) y en transmitirlo al emplazamiento asegurado 10, con el fin de que éste añada este desajuste temporal $\Delta t_1$ a la acreditación acústica CAC en el momento de la transmisión de ésta (línea g de la Figura 4). El módulo acústico 54 verifica entonces, al recibir la acreditación acústica CAC, que ésta comienza en efecto con un desajuste temporal $\Delta t_1$, introducido por el servidor distante, que es igual al valor de separación que él mismo había generado justo antes y enviado al servidor.

**REIVINDICACIONES**

1.- Un sistema asegurado de control de apertura de dispositivos de cerradura, que comprende:

- un teléfono móvil (22) a disposición de un usuario habilitado a abrir el dispositivo de cerradura:

- un emplazamiento gestor distante (10), que comprende:

· una base de datos (12) de usuarios habilitados con, para cada usuario, un identificador asociado a un número de teléfono móvil, y

· medios para recibir como entrada datos digitales de acreditación (DDC) adecuados para permitir la apertura de dispositivos de cerradura específicos;

- un operador de red móvil (16), acoplado al emplazamiento gestor y al teléfono móvil, con medios de transmisión segura de informaciones de acreditación del emplazamiento gestor al teléfono móvil del usuario; y

- al menos un dispositivo de cerradura (28) provisto de circuitos electrónicos para el control condicional de órganos mecánicos (46) de bloqueo/desbloqueo a partir de dichos datos digitales de acreditación (DDC), comprendiendo este dispositivo de cerradura:

· medios (44) de reconocimiento, de análisis y de autenticación de dichos datos digitales de acreditación (DDC), y

· medios (44) de control del desbloqueo de los órganos mecánicos tras el reconocimiento de los datos digitales de acreditación (DDC) conformes;

sistema **caracterizado porque**:

- el emplazamiento gestor distante comprende:

· un generador (14) de acreditaciones acústicas cifradas, que incorpora medios de conversión de dichos datos digitales de acreditación (DDC) en acreditaciones acústicas cifradas (CAC) en forma de señales de audio de uso único;

- las informaciones de acreditación transmitidas por el operador de la red móvil son dichas acreditaciones acústicas cifradas (CAC); y

- el teléfono comprende un transductor electroacústico (24) apto para reproducir dichas acreditaciones acústicas cifradas (CAC);

- el dispositivo de cerradura (28) incorpora un módulo acústico (54) que comprende:

· un transductor electroacústico (56) apto para captar dichas acreditaciones acústicas cifradas (CAC) reproducidas por el transductor (24) del teléfono previamente situado en proximidad al dispositivo de cerradura; y

· medios (58) para extraer dichos datos digitales de acreditación (DDC) a partir de las acreditaciones acústicas cifradas (CAC) captadas por el transductor,

con el fin de aplicar a los medios (44) de reconocimiento, de análisis y de autenticación los datos digitales de acreditación (DDC) así extraídos,

y **porque:**

- el módulo acústico (54) comprende además:

· medios para definir un parámetro adicional de transmisión de la acreditación;

· medios para, con anterioridad a cualquier emisión de acreditación acústica, producir un mensaje acústico codificado por dicho parámetro adicional; y

· un transductor electroacústico (56) apto para reproducir dicho mensaje acústico,

- el teléfono (22) comprende un transductor electroacústico apto para captar dicho mensaje acústico y medios para transmitir al emplazamiento gestor (10) un mensaje codificado por este mensaje acústico;

- la acreditación acústica cifrada (CAC) producida por el generador de acreditaciones acústicas (14) incluye dicho parámetro adicional; y

- el módulo acústico comprende igualmente medios para verificar la conformidad del parámetro adicional incluido en la acreditación acústica captada.

2.- El sistema de la reivindicación 1, en el que dicho parámetro adicional es una contraseña (PWD) generada por el módulo acústico (54) y añadida como campo variable a la acreditación acústica (CAC) producida por el generador criptográfico (14).

3.- El sistema de la reivindicación 1, en el que dicho parámetro adicional es un desajuste temporal (Δt1) aplicado a la emisión de la acreditación acústica (CAC) producida por el generador criptográfico (14).

FIG_1

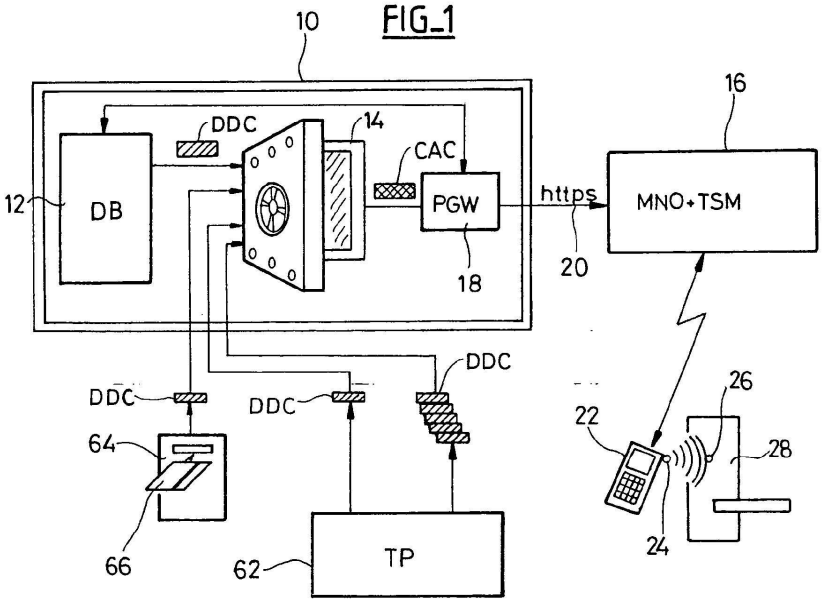

10
16
DDC
14
CAC
12
DB
PGW
https
MNO+TSM
18
20
DDC
DDC
DDC
26
22
64
28
66
62
TP
24

FIG_2

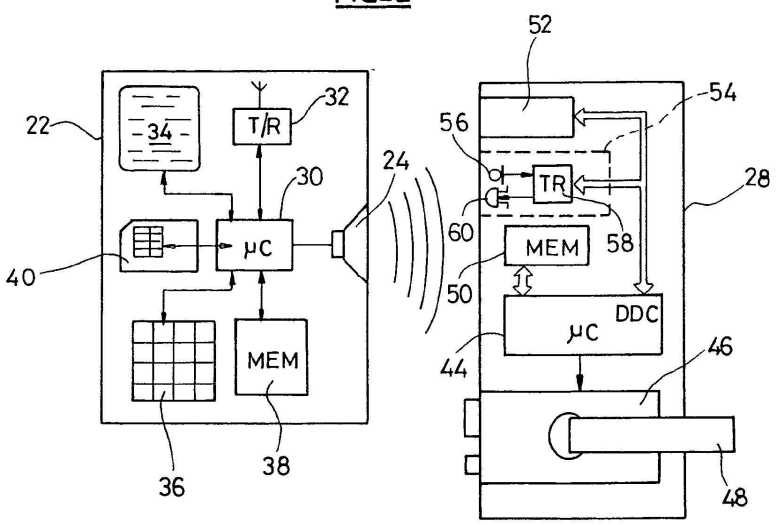

52
54
22
32
T/R
56
34
24
30
28
TR
60
μC
MEM
58
40
50
DDC
μC
44
46
MEM
36
38
48

FIG_3

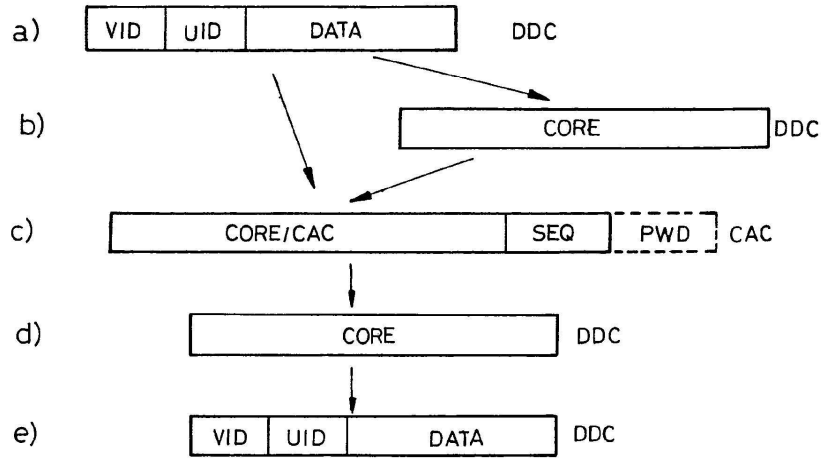
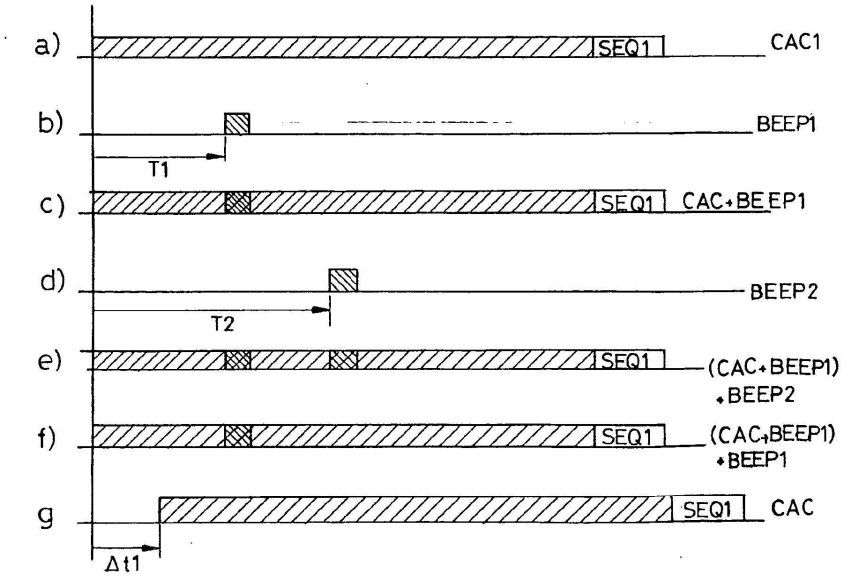

a)
VID
UID
DATA
DDC
b)
CORE
DDC
c)
CORE/CAC
SEQ
PWD
CAC
d)
CORE
DDC
e)
VID
UID
DATA
DDC

FIG_4


a)
SEQ1
CAC1
b)
BEEP1
T1
c)
SEQ1
CAC+BEEP1
d)
BEEP2
T2
e)
SEQ1
(CAC+BEEP1)
+BEEP2
f)
SEQ1
(CAC+BEEP1)
+BEEP1
g
SEQ1
CAC
Δt1