

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 412 333**

51 Int. Cl.:

**G07C 9/00**

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **05.08.2009** **E 09167248 (5)**

97 Fecha y número de publicación de la concesión europea: **13.03.2013** **EP 2284803**

54 Título: **Sistema seguro de programación de dispositivos de cerradura de control electrónico mediante acreditaciones acústicas cifradas**

45 Fecha de publicación y mención en BOPI de la traducción de la patente:  
**11.07.2013**

73 Titular/es:

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

72 Inventor/es:

**METIVIER, PASCAL**

74 Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

ES 2 412 333 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Sistema seguro de programación de dispositivos de cerradura de control electrónico mediante acreditaciones acústicas cifradas

5 La invención concierne a los dispositivos de cerradura mandados eléctricamente por medio de un objeto portátil que forma llave, tal como una tarjeta o una tarjeta sin contacto, o igualmente un teléfono móvil equipado con medios de acoplamiento (inductivo, radiofrecuencia, acústico,...) a la cerradura.

10 Por "dispositivo de cerradura" se entenderá no solamente una cerradura en sentido estricto, es decir un mecanismo colocado por ejemplo en una puerta para condenar la apertura, sino igualmente cualquier dispositivo que permita llegar a un resultado comparable, por ejemplo un cilindro de cerradura considerado aisladamente, o un dispositivo de bloqueo más específico que comprenda diversos órganos no reagrupados en una misma caja de cerradura, siendo el objetivo final obtener la condena por medios mecánicos del acceso físico a un lugar o espacio dado, y el acceso a este lugar o espacio por desbloqueo del dispositivo de cerradura, bajo el mando de un usuario, tras la verificación de que este usuario dispone de los derechos de acceso (i) que son propios del mismo y (ii) que son propios del dispositivo de cerradura. El dispositivo de cerradura puede comprender igualmente, o estar asociado con, un sistema de alarma que haya que desactivar para permitir el acceso a un espacio dado, o inversamente activar para proteger este espacio antes o después de haberle dejado.

Para simplificar la descripción, se hablará en lo que sigue simplemente de "cerradura", pero este término debe ser entendido en su sentido más amplio, sin ningún carácter restrictivo en un tipo de equipo particular.

20 La invención concierne de modo más preciso a la programación de estas cerraduras por los "derechos de acceso" que corresponden a las mismas, es decir la indicación de los usuarios autorizados para abrir una u otra cerradura, cada uno de ellos con una definición de los derechos propios de los mismos, derechos que pueden estar limitados por ejemplo en el tiempo (caducidad del derecho de acceso), o limitados a ciertos días de la semana, o a ciertas franjas horarias, etc.

25 En ciertos sistemas, cada cerradura está unida a una red que permite una gestión centralizada de los accesos y del control de los derechos. Estos sistemas están bien adaptados a entornos de empresa u hoteleros, pero mucho menos a aplicaciones de tipo residencial, o bien a la modernización de instalaciones preexistentes en las que difícilmente sería posible crear una red local, especialmente con todas las dificultades de cableado que esto implicaría.

30 La invención se refiere de modo más particular, pero de modo no exclusivo, a otro tipo de instalaciones, en las que las cerraduras son dispositivos autónomos, memorizando internamente cada una de ellas los derechos de acceso que le están vinculados (usuarios autorizados y, para cada uno, eventuales restricciones de acceso).

35 La programación de este tipo de cerradura implica una intervención en el sitio de un operario (en lo sucesivo "usuario maestro") provisto de un aparato que pueda ser acoplado a la cerradura para inscribir en ésta o actualizar los derechos de acceso. La actualización puede concernir igualmente a otros diversos parámetros de funcionamiento de la cerradura tales como fecha y hora, datos de identificación, algoritmos de cálculo, elementos criptográficos, etc.

Los documentos WO 03/093997 A1 y US 5 933 090 A describen tales sistemas de control de acceso programables o reprogramables en función de las necesidades.

40 En la práctica, la programación de tales cerraduras autónomas es una operación delicada, que necesita un equipo específico y caro así como un aprendizaje previo, que obliga casi siempre a recurrir a un operario profesional.

Esos inconvenientes son un freno importante para el establecimiento de estos sistemas de cerradura autónomos.

En este sentido, sería deseable poder disponer de un medio de programación simple de poner en práctica y que no necesite equipo específico, de modo que la programación pueda ser realizada por manipulaciones simples, al alcance de todos.

45 Esto permitiría especialmente desarrollar las aplicaciones residenciales, en las que los clientes deseen poder programar ellos mismos las cerraduras que han adquirido, y/o actualizarlas ellos mismos sin recurrir a un profesional, especialmente cada vez que sea necesario modificar los derechos de acceso o crear unos nuevos.

50 Uno de los objetivos de la presente invención es proponer una nueva técnica de programación de estas cerraduras, que pueda ser puesta en práctica fácilmente por medio de un teléfono móvil, y de un modo suficientemente simple para estar al alcance de un usuario maestro no profesional de habilidad media.

Otro objetivo de la invención es proponer una técnica de programación de cerraduras que presente un nivel de seguridad máximo, una gran flexibilidad de puesta en práctica, y que sea utilizable con cualquier teléfono móvil tradicional, preexistente, sin que el usuario maestro tenga necesidad de recurrir a un dispositivo de programación

particular. De esta manera, el sistema de la invención podrá ser inmediatamente generalizable y utilizable por todos, beneficiándose de la seguridad y de la flexibilidad propias de las técnicas criptográficas modernas.

El principio de la invención se basa en la utilización de acreditaciones acústicas cifradas para la programación de la cerradura. Estas acreditaciones acústicas se presentan por ejemplo en forma de una serie codificada de tonos (tonos DTMF u otros), emitidos por el altavoz de un dispositivo emisor y captados por el micrófono de un dispositivo receptor.

En el caso de la invención, estas acreditaciones acústicas cifradas son acreditaciones “descendentes”, es decir que éstas proceden de un sitio administrador remoto y transmitidas al teléfono móvil del usuario maestro. Para utilizar la acreditación, el usuario maestro aproxima su teléfono a la cerradura e inicia la emisión por el altavoz de su teléfono de la serie de tonos correspondientes a la acreditación acústica cifrada, de manera que estos tonos puedan ser captados por un micrófono incorporado o acoplado a la cerradura. Este último descodifica la acreditación, la verifica y, en caso de conformidad, programa o reprograma los derechos de acceso en su memoria interna.

La utilización de acreditaciones acústicas no es en sí misma nueva, ésta ha sido propuesta ya 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 por un terminal remoto, por ejemplo por 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 sitio de control que forma interfaz con la red a la que se solicita el acceso. Para verificar la autorización del usuario, la red envía una señal sonora (la acreditación acústica) al ordenador remoto que acaba de conectarse, señal que 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 sitio de control remoto a través del operador de red telefónica móvil y “escuchado” por el sitio de control, el cual puede verificar entonces la acreditación y autorizar el acceso del terminal a la red informática. Se observará que en este caso se trata de una acreditación “ascendente”: la acreditación acústica es captada por el micrófono del teléfono, el cual la transmite al sitio de control. Conociendo el destinatario de la llamada telefónica, el sitio de control puede identificar al usuario a través del teléfono móvil utilizado para esta operación, y de esta manera autorizar el acceso lógico a la red por el terminal situado en la proximidad del teléfono así identificado.

De modo más preciso, la presente invención concierne a un sistema del tipo general divulgado por el documento WO03/093997 A1 antes citado, que comprenda los elementos enunciados en el preámbulo de la reivindicación 1.

Para lograr los objetivos indicados anteriormente, la invención propone en este caso los elementos enunciados en la parte característica de la reivindicación 1.

Las subreivindicaciones exponen diversas puestas en práctica posibles de la invención, así como perfeccionamientos ventajosos.

Se van a describir ahora diversos ejemplos de puesta en práctica de la invención refiriéndose a los dibujos anejos en los que las mismas referencias numéricas designan de una figura a otra elementos idénticos o funcionalmente semejantes.

La Figura 1 ilustra de modo esquemático los principales elementos que contribuyen al funcionamiento del sistema de acuerdo con la invención.

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

Se va a explicar el principio y la puesta en práctica de la invención, refiriéndose a las Figuras 1 y 2.

Uno de los elementos esenciales de la invención es un sitio administrador seguro 10 que centraliza en una base de datos DB 12 las informaciones que permiten listar e identificar un cierto número de cerraduras con sus datos de derechos de acceso asociados, que comprende una lista de usuarios autorizados, cada uno con las condiciones de acceso autorizadas: acceso reservado a ciertos días o ciertas franjas horarias, fecha de expiración del derecho de acceso, etc.

Además de los usuarios autorizados, la base de datos lista igualmente para cada cerradura un identificador UID (Unique Identifier) que está atribuido de manera única y permite identificar de modo unívoco la cerradura en los diversos protocolos de intercambio de datos. La cerradura puede ser identificada igualmente por una denominación libre (“entrada”, “garaje”, “bodega”, etc.), especialmente para facilitar la selección por un usuario de una cerradura entre varias, de la misma manera que una etiqueta que estuviera fijada a una llave tradicional.

La base de datos puede conservar igualmente otros datos, especialmente los algoritmos utilizados por la cerradura, una o varias claves criptográficas, etc.

El sitio administrador 10 comprende igualmente un motor criptográfico que forma un generador 14 de datos de acreditación.

De modo característico de la invención, los “datos de acreditación” (credenciales) son acreditaciones acústicas cifradas en forma de señales de audio de uso único constituidas, por ejemplo (pero de modo no limitativo) por una sucesión de tonos dobles DTMF. Estas señales de audio están concebidas de manera que puedan ser transmitidas por canales de transmisión de audio y reproducidas tal cual por transductores acústicos.

La programación de una cerradura implica, en primer lugar, definir o actualizar en la base de datos DB la lista de usuarios autorizados, cada uno con las condiciones de acceso correspondientes. Estas diferentes informaciones serán comunicadas al sitio administrador 10 por un operador autorizado (designado en lo que sigue “usuario maestro”) durante la fase inicial.

Como se explicará en lo que sigue, la programación puede implicar igualmente, además de la determinación de los derechos de acceso, la actualización de otras informaciones propias de la cerradura y relativas a su funcionamiento, tales como: fecha y hora, algoritmo utilizado para el reconocimiento y la descodificación de las acreditaciones acústicas, clave criptográfica, y denominación libre.

La captura por el usuario maestro de la listas de usuarios autorizados y de los derechos de acceso correspondientes puede hacerse cómodamente por medio de un microordenador 16 unido al sitio administrador 10 por un enlace seguro, por ejemplo un enlace IP de tipo https 18.

La utilización de un microordenador 16 no es sin embargo indispensable, pudiendo el operario maestro captar igualmente los datos relativos a los derechos de acceso por medio de su teléfono móvil 20, funcionando éste durante esta fase inicial como terminal conectado al sitio administrador remoto 10 a través de un operador de telefonía móvil.

Una vez captados e introducidos los diversos datos de derechos de acceso en la base de datos 12, conviene programar o reprogramar una cerradura correspondiente 22 con estos derechos de acceso, y/o eventualmente con otras informaciones propias de la cerradura: fecha y hora, algoritmo, clave criptográfica, denominación libre, etc.

El principio de base de la invención consiste en realizar esta programación haciendo reproducir por el altavoz del teléfono móvil 20 del usuario maestro, como señal de audio, una acreditación acústica cifrada que contiene las diferentes informaciones necesarias para la programación, siendo aproximado el teléfono móvil 20 a la cerradura 22 que comprende un micrófono que permite captar esta acreditación acústica cifrada.

Las acreditaciones acústicas, generadas por el motor criptográfico 14, pueden ser enviadas al teléfono móvil 20 a través del operador de telefonía móvil o MNO (Mobile Network Operator) 24, a su vez acoplado al sitio administrador 10 por un enlace seguro, por ejemplo un enlace IP de tipo https, o simplemente por una pasarela telefónica de audio PGW (Phone GateWay) 26 que permita transmitir las acreditaciones acústicas desde el generador 14 hasta el teléfono 20 por los canales de transmisión de audio (canal voz) de la red de telefonía móvil. El aseguramiento del enlace entre la red móvil 24 y el teléfono móvil 20 puede ser realizado por intermedio de un proveedor de servicios de confianza o TSM (Trusted Service Manager), apropiado para asegurar de manera eficaz y segura los diversos procedimientos que se describirán a continuación, de intercambio o de telecarga de informaciones entre el sitio administrador 10 y el teléfono móvil 20 del usuario maestro a través del operador de red móvil 24.

En variante o como complemento, las acreditaciones acústicas cifradas pueden ser transmitidas del sitio administrador 10 al teléfono 20 a través del microordenador 16, por medios de acoplamiento apropiados 28 tales como: enlace por cable (cable USB) o inalámbrico (Bluetooth), a través de un dispositivo de almacenamiento intermedio (tarjeta SD o MicroSD, o dongle USB), o todavía por acoplamiento acústico entre el altavoz del microordenador y el micrófono del teléfono móvil 20 (puesto que las acreditaciones acústicas se presentan en forma de señales de audio).

La Figura 2 ilustra, en forma de esquema de bloques, los principales órganos del teléfono móvil 20 y de la cerradura 22.

El teléfono 20 comprende un microcontrolador 30 acoplado a diversos órganos periféricos tales como circuito de emisión/recepción 32, pantalla 34, teclado 36, memoria de datos 38, tarjeta UICC (Universal Integrated Circuit Card, correspondiente a la “tarjeta SIM” para las funciones de telefonía GSM) 40, y transductor acústico 42.

La cerradura 22, a su vez, comprende un microcontrolador 44 así como un sistema electromecánico 46 que permite mandar el desbloqueo de un pestillo o de una empuñadura 48 bajo la orden del microcontrolador 44. Una memoria de datos 50 conserva diversos datos modificables propios de la cerradura, especialmente:

- la lista de los usuarios autorizados, estando identificado cada uno de estos usuarios listados de modo unívoco por el identificador único UID (Unique Identifier) de una llave constituida por un objeto portátil puesto a disposición del usuario autorizado, objeto que puede ser – de modo no limitativo – una tarjeta o tarjeta de

acoplamiento sin contacto con la cerradura (especialmente de tipo RFID), o bien un mando a distancia de radio o acústico, o también un teléfono móvil identificado por su número de abonado;

- para cada usuario, las condiciones de acceso autorizadas (días o franjas horarias, fecha de expiración del derecho de acceso ...);
  - 5 - el identificador único UID de la cerradura, que es un identificador programable, listado en la base de datos DB del sitio administrador y que permite reconocer la cerradura entre todas, de manera unívoca;
  - una denominación libre ("entrada, garaje",...);
  - algoritmos de reconocimiento y de decodificación;
  - claves criptográficas.
- 10 La cerradura comprende sus propios medios de alimentación en forma de una batería 52, a fin de hacerla autónoma desde el punto de vista eléctrico. No obstante, es posible una alimentación externa.
- De modo característico, la cerradura 22 está provista además de un transductor acústico en forma de un micrófono 54 que permite captar las señales sonoras circundantes, en particular la acreditación acústica que será reproducida por el altavoz 42 del teléfono 20, y transformar las señales acústicas captadas en señales eléctricas aplicadas al
- 15 microcontrolador 44 para decodificación, verificación, y programación o reprogramación en la memoria 50 de los diversos datos modificables indicados anteriormente.

#### **Puesta en práctica de la invención**

Se van a describir ahora varios modos operativos para la puesta en práctica de la invención con los diferentes elementos del sistema que se acaba de describir.

- 20 Previamente, si las listas de usuarios y de derechos de acceso no están todavía en la base de datos DB del sitio administrador 10, o si estos datos deben ser actualizados, el usuario maestro (u otro usuario acreditado por este último) debe captarlas y comunicarlas al sitio administrador, mediante las etapas sucesivas siguientes:
1. acceso seguro (por login + contraseña) al sitio administrador 10;
  2. captura de los UID de las cerraduras y de los UID de las llaves de los usuarios autorizados;
  - 25 3. en su caso, captura de los números de abonados del teléfono móvil de los usuarios autorizados para utilizar un teléfono móvil para abrir las cerraduras (o acreditados para la programación);
  4. asignación eventual de nombres abreviados de puertas a los UID de las cerraduras, y/o de nombres abreviados de usuarios a los UID de las llaves;
  5. asignación de los derechos y condiciones de acceso a los diferentes usuarios;
  - 30 6. validación de las capturas precedentes;
  7. en su caso (véase más abajo), facilitación por el sitio administrador del número o de los números de llamada ascendentes que hay que componer por el usuario maestro para programar cada cerradura, pudiendo serle enviada igualmente esta información por SMS, MSM, e-mail, mensajería instantánea, etc.

- 35 Cuando se desee programar o reprogramar una cerradura, el usuario maestro recibe del sitio administrador 10 los datos que procede inscribir o actualizar en la memoria 50 de la cerradura 22, a través del microordenador 16 y el acoplamiento 28, o bien directamente a través del operador de telefonía móvil 24.

- Como se indicó anteriormente, los datos recibidos del sitio administrador remoto 10 pueden comprender, además de los derechos de acceso vinculados a cada usuario autorizado, un cierto número de informaciones propias de las cerraduras tales como: algoritmo utilizado, clave criptográfica, nombre abreviado, etc. La actualización podrá
- 40 concernir igualmente a la fecha y la hora del reloj interno del microcontrolador 44, a distancia desde el sitio administrador 10.

Los datos de programación pueden comprender igualmente datos que son propios del teléfono móvil 20 del usuario maestro, tales como:

- 45 - la fecha y la hora, cuando se quiere actualizar estas informaciones desde el teléfono móvil en lugar de hacerlo desde el sitio administrador 10);
- el número IMEI que identifica al teléfono de manera única;
- la identificación de la tarjeta UICC 40 (identificador de tarjeta SIM);

- eventualmente, informaciones de localización geográfica que da la posición del teléfono 20 en el momento de la programación (coordenadas GPS si el teléfono está equipado con esta función, o localización aproximada mediante la célula de la red desde la cual emite el teléfono),

5 Para programar la cerradura, el usuario presenta su teléfono 20 delante de la cerradura 22 que desea programar e inicia la emisión, en forma de señal sonora, de la acreditación acústica correspondiente. Esta emisión puede ser iniciada igualmente (como se explicará más adelante) por la simple respuesta o al descolgar en una llamada descendente a la atención del teléfono móvil del usuario maestro que proviene del sitio administrador remoto.

10 La acreditación acústica, captada por el micrófono 54 de la cerradura, es analizada por el microcontrolador 44 que, en caso de conformidad, manda la programación o la actualización de las informaciones correspondientes a la memoria 50.

El hecho de que la acreditación acústica cifrada sea acreditación de uso único impide un fraude por registro y duplicado de la acreditación.

15 Una precaución que permite aumentar la seguridad consiste en prever una validación suplementaria por el usuario, por ejemplo la entrada de un código personal de tipo "PIN code" antes de la facilitación de la acreditación acústica, o una validación de tipo biométrico, por un lector biométrico incorporado al teléfono o por medio de un sistema de reconocimiento de huellas vocales utilizando el micrófono del teléfono (pudiendo ser almacenada la huella biométrica específica en la memoria 38 del teléfono, o bien en la tarjeta UICC 40, o todavía en la base de datos 12).

Ventajosamente, la cerradura 22 está provista de medios que permiten emitir en retorno una señal acústica que valida la buena ejecución de la operación de programación.

20 A tal efecto, es posible utilizar el transductor 54 de la cerradura haciéndola funcionar en modo inverso (para emitir señales sonoras en lugar de captarlas), o bien prever un transductor específico para reproducir señales sonoras.

25 La señal sonora así emitida por la cerradura será captada por el micrófono del teléfono 20 y traducida por un subprograma del teléfono en un mensaje sonoro o visual con destino al usuario maestro para confirmar (o invalidar) la buena ejecución de la programación. El subprograma puede igualmente guardar una traza de las cerraduras que han sido programadas y de las que todavía no lo han sido, por ejemplo por visualización de una lista de cerraduras, para alertar al usuario maestro si éste se ha olvidado de programar algunas de ellas.

30 Ventajosamente, es posible aprovecharse del retorno de informaciones después de la programación de la cerradura para recuperar datos memorizados en esta última, o informaciones de estado tales como señal de batería baja, necesidad de mantenimiento, fallo de funcionamiento, prueba de apertura, etc. Estos datos o informaciones podrán ser traducidos por el subprograma del teléfono en mensajes de alerta ("batería baja", ...) visualizados en la pantalla del teléfono, siendo repetidos estos mensajes si es necesario a intervalos regulares.

35 Por otra parte, estos datos o informaciones podrán ser ventajosamente enviados al sitio administrador por intermedio de la red móvil 24, aprovechándose así del establecimiento por el usuario maestro de un enlace en el sentido descendente (del sitio administrador a la cerradura) para hacer remontar informaciones en sentido inverso (de la cerradura hasta el sitio administrador). En otras palabras, el usuario maestro, durante la programación o reprogramación, pasa a ser para el sistema una fuente de informaciones. Esta manera de proceder es particularmente ventajosa en este caso, porque se trata de cerraduras de tipo stand alone, es decir que funcionan de manera completamente autónoma sin estar conectadas a ninguna red que permita intercambiar datos o transmitir ciertos mensajes de estado o de anomalía.

40 Ventajosamente, antes de realizar la programación propiamente dicha, el teléfono 20 reproduce una acreditación específica de apertura de sesión, apropiada para hacer entrar la cerradura en un modo de programación diferente de su funcionamiento normal. Una vez acabada la programación, otra acreditación acústica específica hace salir la cerradura del modo de programación y la vuelve a colocar en su modo de funcionamiento normal. Esta manera de proceder es particularmente ventajosa para aumentar la seguridad cuando la cerradura es una cerradura de mando  
45 acústico, es decir que el desbloqueo posterior por el usuario autorizado se hará por emisión de una acreditación acústica cifrada, de una naturaleza semejante a la acreditación acústica que haya servido para la programación.

Otro perfeccionamiento pretende evitar un fraude consistente en desmontar una cerradura ya programada para volverla a montar, tal cual, en otro emplazamiento. A tal efecto, la cerradura 22 memoriza las informaciones de localización geográfica (coordenadas GPS u otras) del teléfono 20 en el momento en que éste realiza la programación. La cerradura, por otra parte, comprende medios para recoger las informaciones de localización geográfica del teléfono del usuario que se presentará posteriormente como un usuario autorizado, y comparar estas coordenadas con las que han sido memorizadas en el momento de la programación, y la apertura solamente será autorizada si las informaciones concuerdan, salvo un margen de error dado. En ausencia de cobertura de red o GPS  
50 en el momento en que el usuario solicite el acceso, el dato de localización utilizado será el dato más reciente obtenido antes de la pérdida de contacto, en este caso con un margen de error superior, definido por el administrador del sistema.  
55

Se van a describir ahora varias maneras en las que el sitio administrador 10 puede facilitar la acreditación al teléfono móvil 20, especialmente cuando esta facilitación interviene a través de la red del operador móvil 24.

### 1º) Modo en línea (facilitación directa de la acreditación)

5 Cuando se desee programar la cerradura 22, el usuario maestro entra en contacto con el sitio administrador 10 por cualquier medio apropiado. Esto puede ser obtenido por la llamada de un número telefónico, o por un procedimiento de tipo call back: en este caso, el usuario maestro entra en contacto telefónico o por un mensaje (SMS, MMS, e-mail, mensajería instantánea, etc) con el sitio administrador, el cual no le responde inmediatamente, sino que después de colgar hace sonar el teléfono móvil 20 para que el usuario maestro establezca de nuevo el contacto con el sitio administrador (el siendo el número llamado por el sitio administrador el número de abonado, listado en la base de datos DB, del usuario maestro o de cualquier otro usuario autorizado por este último).

10 Si los parámetros de programación han sido definidos previamente de la manera indicada anteriormente, basta que el usuario maestro valide estos parámetros así como su número de abonado de telefonía móvil ante el sitio administrador 10.

15 La simple respuesta del sitio administrador a la llamada del usuario maestro, o en caso de call back al descolgar este último, provoca la transmisión inmediata y directa de la autorización de la acreditación acústica cifrada.

En este modo de realización, cualquiera que sea la manera en que el usuario maestro entre en contacto con el sitio administrador remoto, éste facilita la acreditación acústica directamente al usuario-maestro, "en línea", sin almacenamiento intermedio.

20 Este modo de realización es particularmente simple de poner en práctica, en la medida en que basta utilizar la infraestructura existente, sin adaptación previa del teléfono, especialmente sin ninguna necesidad de cargar un subprograma o applet, especialmente de tipo midlet o cardlet.

25 De esta manera, la invención puede ser puesta en práctica con cualquier tipo de teléfono móvil, incluso muy simple, y sin ninguna intervención previa en éste. Otra ventaja reside en la posibilidad de verificar en tiempo real la autorización del usuario maestro. Además, gracias a este modo en línea, es posible disponer a nivel del sitio administrador de informaciones sobre la utilización hecha de la acreditación acústica, especialmente la fecha y la hora de la programación, y eventualmente la situación geográfica de esta operación (por identificación de la célula desde la que el usuario maestro llama).

30 Por el contrario, este modo implica disponer de un acceso a la red móvil, lo que no es siempre posible (bodegas, zonas sin cobertura, etc.). Por otra parte, éste no permite en principio disponer, a elección del usuario, de varias acreditaciones correspondientes a varias cerraduras posibles, en la medida en que es necesario tener una correspondencia "uno por uno" entre acreditación y cerradura.

En caso de pluralidad de cerraduras, es posible prever una validación por etapas en cada cerradura, o bien utilizar un número de llamada diferente para cada cerradura.

### 2º) Modo semi en línea (modo en línea diferido con telecarga)

35 Este modo es utilizable especialmente si el acceso a la red no es seguro en el momento de la utilización. En este caso, el usuario maestro se conecta de antemano con el sitio administrador y recibe de éste la acreditación correspondiente a la cerradura que acaba de programar, o varias de estas acreditaciones, en caso de pluralidad de cerraduras que haya que programar. Estas acreditaciones son almacenadas de modo seguro en el teléfono o en una memoria periférica del teléfono (por ejemplo una tarjeta SD o MicroSD).

40 Aquí también, puede establecerse directamente el contacto previo con el sitio administrador 10 con envío al sitio de una petición emitida por el teléfono móvil del usuario maestro, o bien a través de un mensaje descendente emitido por el sitio administrador remoto hacia un número de abonado previamente especificado por el usuario maestro (o el número de cualquier otro usuario autorizado por este último).

45 Cuando el usuario maestro quiera programar una cerradura, éste lanza una aplicación integrada en su teléfono que busca la acreditación correspondiente entre las que han sido almacenadas, la reproduce para programar la cerradura, y después la suprime de la memoria. Y así sucesivamente para utilizar las acreditaciones siguientes.

50 La aplicación que permite esta puesta en práctica es un subprograma conservado en el teléfono, previamente enviado a éste por el operario de red móvil, o bien por telecarga en un soporte externo (tarjeta SD o MicroSD), o también a través de una conexión internet. En el caso de una telecarga a través del operador de red móvil, el sitio administrador habrá enviado previamente un mensaje por ejemplo de tipo "push SMS" o "WAP push" al teléfono, a fin de identificar la marca y el modelo de éste y presentar al usuario maestro un enlace que permita la telecarga del subprograma.

### 3º Modo fuera de línea

En este modo de puesta en práctica, las acreditaciones acústicas son generadas localmente, por el propio teléfono. A tal efecto, el teléfono contiene un subprograma o applet, especialmente de tipo cardlet (almacenado en la tarjeta UICC 40) o midlet (almacenado en la memoria 38 del aparato telefónico). Este subprograma es telecargado por cualquier medio apropiado, de la misma manera que la utilizada en el modo de puesta en práctica precedente: telecarga a través del operador móvil, a través de internet, etc., o bien precargado en el teléfono en el momento de la adquisición de éste.

El sitio administrador 10 envía al teléfono 20 un “dato de acreditación”, que en este caso no es la acreditación acústica propiamente dicha, sino una clave criptográfica, conservada en la tarjeta UICC 40 por razones de seguridad. Esta clave criptográfica, combinada con el subprograma, permitirá constituir un generador criptográfico en el seno del teléfono 20. Cuando se desee programar una cerradura, el usuario maestro manda la generación de la acreditación acústica por el subprograma interno y su reproducción por el transductor de su teléfono.

#### **4º Modo “pieza adjunta”**

Este modo de puesta en práctica es una variante del modo semi en línea.

La diferencia consiste esencialmente en el hecho de que las acreditaciones no son enviadas por el canal vocal de la red de telefonía móvil, sino en forma de un archivo adjunto a un mensaje de tipo e-mail, MMS o mensajería instantánea.

La ventaja de esta solución es utilizar los medios de telecarga de ficheros preexistentes en el teléfono, especialmente con los teléfonos que comprenden funciones elaboradas de tipo smartphone, y esto sin que sea necesario telecargar previamente un subprograma específico, conservar éste en el teléfono y hacerle ejecutar por este último, llegado el momento. El archivo puede igualmente ser telecargado a través del microordenador 16 y el acoplamiento 28 con el teléfono 20.

## REIVINDICACIONES

1. Un sistema seguro de mando de apertura de dispositivos de cerradura, que comprende:
  - un sitio administrador (10) remoto, que comprende:
    - 5 . una base de datos (12) de dispositivos de cerradura y de usuarios autorizados, con un identificador único asociado para cada dispositivo de cerradura, una lista de usuarios autorizados con datos correspondientes de derechos de acceso, y eventualmente datos adicionales;
    - al menos un dispositivo de cerradura (22) que comprende:
      - . una memoria de datos (50) que contiene:
        - 10 i) un identificador único de la cerradura, listado en la base de datos del sitio administrador y que permite reconocer la cerradura entre todas, de manera unívoca;
        - ii) derechos de acceso previamente definidos; y
      - . circuitos electrónicos para el mando condicional de órganos mecánicos de bloqueo/bloqueo en función de lo citados derechos de acceso,
- sistema caracterizado
- 15 porque los citados derechos de acceso están definidos por
  - i) una lista de los usuarios autorizados, cada uno listado de modo unívoco por un identificador único de una llave constituida por un objeto portátil puesto a disposición de esta usuario autorizado; y
  - ii) para cada usuario, las condiciones de acceso autorizadas,
- y porque comprende además:
  - 20 - en el sitio administrador:
    - . un generador (14) de datos de acreditación apropiados para permitir la programación de los dispositivos de cerradura por los derechos de acceso listados en la base de datos, siendo estas acreditaciones, acreditaciones acústicas cifradas en forma de señales de audio de uso único;
  - 25 - un teléfono móvil (20) a disposición del usuario maestro, que comprende un transductor electroacústico (42) apto para reproducir las citadas acreditaciones acústicas; y
  - medios de transmisión seguros de los citados datos de acreditación del sitio administrador al teléfono móvil del usuario maestro;
  - en el dispositivo de cerradura (22):
    - 30 . un transductor electroacústico (54) apto para captar las acreditaciones acústicas reproducidas por el transductor del teléfono previamente colocado en la proximidad del dispositivo de cerradura; y
    - . medios para reconocer, analizar y autenticar las acreditaciones acústicas captadas por el transductor, y realizar, con reconocimiento de una acreditación acústica conforme, una programación o una reprogramación de los derechos de acceso.
- 35 2. El sistema de la reivindicación 1, en el cual los medios de transmisión segura de los datos de acreditación del sitio administrador al teléfono móvil del usuario maestro comprenden medios (28) de acoplamiento de este teléfono móvil con un terminal informático (16) unido al sitio administrador.
3. El sistema de la reivindicación 1, en el cual lo medios de transmisión seguros de los datos de acreditación del sitio administrador al teléfono móvil del usuario maestro comprenden un operador de red móvil (24) acoplado al sitio administrador y al teléfono del usuario maestro.
- 40 4. El sistema de la reivindicación 1, en el cual, para la generación de los datos de acreditación que hay que transmitir al teléfono, el sitio administrador es apto para combinar los datos de derechos de acceso propios de los usuarios autorizados con datos adicionales propios de la cerradura y obtenidos a nivel del sitio administrador, y para generar una acreditación acústica función a la vez de los citados datos de derechos de acceso y de los citados datos adicionales.
- 45 5. El sistema de la reivindicación 1, en el cual el teléfono es apto para combinar los datos de acreditación transmitidos por el sitio administrador con datos adicionales inherentes al teléfono y obtenidos localmente, y para

generar una acreditación acústica función a la vez de los citados datos de acreditación y de los citados datos adicionales.

- 5 6. El sistema de la reivindicación 5, en el cual los citados datos adicionales comprenden además una información de localización geográfica del teléfono en el momento de la operación de programación, y el dispositivo de cerradura comprende además medios para memorizar esta información de localización geográfica en la programación, y compararla posteriormente con una información de localización geográfica de un teléfono de un usuario en el momento de un intento de apertura del dispositivo de cerradura por este usuario.
- 10 7. El sistema de la reivindicación 1, en el cual el teléfono es apto para:
  - previamente a la reproducción de las acreditaciones acústicas de programación de los derechos de acceso, reproducir una acreditación específica de apertura de sesión apropiada para hacer entrar el dispositivo de cerradura en un modo de programación; y
  - eventualmente, tras la reproducción de las citadas acreditaciones acústicas de programación, reproducir una acreditación específica de cierre de sesión apropiada para hacer salir el dispositivo de cerradura del citado modo de programación.
- 15 8. El sistema de la reivindicación 1, en el cual:
  - el dispositivo de cerradura comprende un transductor electroacústico apto para reproducir señales acústicas en retorno, generadas por el dispositivo de cerradura y codificadas por datos propios del dispositivo de cerradura; y
  - el teléfono comprende un transductor electroacústico apto para captar las citadas señales en retorno.
- 20 9. El sistema de la reivindicación 8, en el cual el teléfono comprende además medios para descodificar las citadas señales en retorno y en su caso visualizar un mensaje con destino al usuario función de los citados datos propios del dispositivo de cerradura.
- 25 10. El sistema de la reivindicación 8, en el cual el teléfono comprende además medios para transmitir al sitio administrador las citadas señales en retorno codificadas por los citados datos propios del dispositivo de cerradura.
- 25 11. El sistema de la reivindicación 1, en el cual el teléfono comprende además medios para memorizar y actualizar una lista de dispositivos de cerradura ya programados y de dispositivos de cerradura todavía no programados.
12. El sistema de la reivindicación 1, que comprende además medios para condicionar la reproducción de la acreditación acústica por el transductor del teléfono a la presentación previa de un dato personal de validación facilitada por el usuario maestro al teléfono.
- 30 13. El sistema de la reivindicación 1, que comprende medios aptos para:
  - verificar la autorización del usuario maestro para operar una programación del dispositivo de cerradura;
  - generar una acreditación acústica por el generador (14) del sitio administrador; y
  - transmitir esta acreditación al teléfono, para reproducción directa por el transductor de éste previamente colocado en la proximidad del transductor del dispositivo de cerradura.
- 35 14. El sistema de la reivindicación 1, que comprende medios aptos para:
  - verificar la autorización del usuario maestro para operar una programación del dispositivo de cerradura;
  - generar una acreditación acústica por el generador (14) del sitio administrador; y
  - activar un subprograma interno del teléfono para telecargar la citada acreditación y memorizar ésta en una memoria (32) del teléfono,después, en un segundo tiempo:
- 40
  - activar el subprograma interno para reproducción de la acreditación por el transductor del teléfono previamente colocado en la proximidad del transductor del dispositivo de cerradura.
15. El sistema de la reivindicación 1, que comprende además medios de actualización a distancia, desde el sitio administrador, de la fecha y de la hora del reloj interno del dispositivo de cerradura.
- 45 16. El sistema de la reivindicación 1, que comprende además medios de actualización a distancia, desde el sitio administrador: de algoritmos de reconocimiento y de descodificación, de claves criptográficas y/o de una denominación libre conservada en la memoria de datos (50) del dispositivo de cerradura.

