(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 664 947**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **24.10.2005 E 05109900 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2018 EP 1780680**

(54) Título: **Procedimiento de control de bloqueo de cerradura, y cerradura**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2018

(73) Titular/es:

DORMAKABA SCHWEIZ AG (100.0%)
Mühlebühlstrasse, Kempten
8623 Wetzikon, CH

(72) Inventor/es:

PELLATON, PIERRE

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Procedimiento de control de bloqueo de cerradura, y cerradura.

Campo técnico

La presente invención se refiere a un procedimiento de control de bloqueo de cerradura electrónica. La presente invención se refiere asimismo a una cerradura electrónica útil para la realización de este procedimiento. La presente invención se refiere en particular a una cerradura que ofrece el nivel de seguridad requerido para cajeros automáticos (ATM, *Automatic Teller Machines*) o cajas fuertes.

Estado de la técnica

Las cerraduras convencionales se bloquean o se desbloquean por medio de llaves mecánicas o electrónicas. La distribución de las llaves está restringida a los usuarios autorizados a acceder al contenido protegido por la cerradura. El nivel de protección depende de la facilidad con la cual se pueden falsificar las llaves y de la confianza otorgada a los portadores de la llave.

En el caso de cajeros de banco, el acceso por la cara frontal se salvaguarda por medio de un lector de tarjetas y de un teclado que permiten que diferentes usuarios se identifiquen antes de extraer un número limitado de billetes. El acceso a la cara posterior del cajero está cerrado en cambio, generalmente, por medio de una cerradura de llave convencional. Los empleados de banca, los profesionales del transporte de fondos encargados de reponer el cajero y los técnicos de reparación se reparten, todos ellos, copias de la misma llave que permite acceder a cajas fuertes que contienen, frecuentemente, decenas de miles de euros en efectivo o dentro de un contenedor. El riesgo de que una de estas llaves se pierda o sea robada y que la misma caiga en malas manos es importante. Además, resulta extremadamente difícil encontrar al culpable en caso de robo por parte de un empleado desaprensivo cuando una llave se distribuye a numerosos usuarios.

Con el fin de remediar estos problemas, la compañía Kaba Mas (marca registrada) propone, desde hace varios años, una cerradura comercializada con el nombre de Cencon System 2000 (marca registrada). Esta cerradura se puede abrir por medio de una llave electrónica convencional, que permite identificar a su portador, y de un código secreto de un solo uso OTC (*One Time Combination*, marca registrada). El código OTC se comunica al usuario desde una central por ejemplo a través de una llamada telefónica. Solamente un usuario que logre presentar a la vez una llave electrónica y un código OTC válido, está autorizado a acceder al contenido del cajero protegido.

Sin embargo, esta solución adolece del inconveniente de que requiere siempre unas llaves físicas asociadas a cada cajero. Un transportista de fondos necesita tantas llaves como cajeros a reabastecer en el transcurso de su jornada, o sino una llave programada para abrir varios cajeros en combinaciones con diferentes códigos OTC. La gestión y la programación de las llaves destinadas a distribuir a los diferentes usuarios es un rompecabezas administrativo, en particular cuando se pierde una llave.

Por otra parte, un usuario que haya adquirido fraudulentamente una llave podría intentar llamar a la central usurpando la identidad del portador autorizado de la llave, con el fin de obtener un código OTC válido. Por tanto, la seguridad ofrecida es insuficiente.

Por otra parte, el lector de llaves electrónicas comprende unos elementos eléctricos, electrónicos y/o electromecánicos que ofrecen unas posibilidades de manipulaciones y de fraudes adicionales.

La solicitud de patente EP 0 546 701 describe un procedimiento de control de desbloqueo de cajas fuertes en el que la seguridad se garantiza por medio de diferentes códigos PIN y de mensajes codificados que el usuario debe introducir en un terminal que le pertenece. A continuación, este terminal se conecta a la caja fuerte protegida, con el fin de provocar su desbloqueo. El terminal que se encuentra habitualmente en las manos del usuario constituye un blanco para piratas informáticos tentados de examinarlo o de fabricar un terminal compatible para acceder a cajas fuertes no autorizadas.

La solicitud de patente EP 0 935 041 describe un dispositivo de mando de acceso físico o lógico que se puede aplicar a una cerradura (acceso físico). En este caso, un primer circuito electrónico está montado en un zócalo solidario a la cerradura, y un segundo circuito electrónico está montado en una caja separada. Cuando la caja se introduce en el zócalo, el primer circuito electrónico se conecta el segundo circuito electrónico. Un primer código aleatorio es generado por estos primer y segundo circuitos electrónicos asociados, es transmitido a continuación hacia un centro de mando distante que procede a realizar unas verificaciones antes de generar, y a continuación entregar, un segundo código aleatorio al primer y al segundo circuitos electrónicos asociados. La introducción de este segundo código aleatorio permite, cuando es correcto, desbloquear la cerradura. Al constituir la posesión de la caja, por parte de un estafador, un factor determinante para acceder a la apertura de la cerradura, este procedimiento no permite, por tanto, tener en cuenta una eventual situación de coacción.

La patente US nº 5.774.058 describe un sistema de acceso para el desbloqueo de cerraduras a distancia. Un ordenador distante comprende un receptáculo destinado a recibir una llave física que permite a un primer usuario la entrada efectiva en el sistema de mando de la cerradura a distancia, mientras que una pantalla y un teclado situados en la cerradura permiten a un segundo usuario interaccionar en particular con la cerradura. Sin embargo, se prevé siempre, necesariamente, el uso de una llave física, lo cual plantea problemas en caso de pérdida como ya se ha expuesto anteriormente.

Es por tanto un objetivo de la presente invención proponer un procedimiento y una cerradura que permitan evitar los inconvenientes de los procedimientos y de las cerraduras de la técnica anterior.

Según la invención, estos objetivos se logran en particular por medio de un procedimiento de control de bloqueo de una cerradura electrónica, de acuerdo con la reivindicación 1.

Este procedimiento tiene en particular la ventaja de obligar al usuario a transmitir una pregunta planteada por la cerradura del cajero a la central. Esta operación adicional permite prever unas pruebas adicionales, por ejemplo para verificar en la central si la pregunta planteada es definitivamente válida.

Asimismo, este procedimiento tiene la ventaja de basar la identificación del usuario ya no necesariamente en una llave física, sino por ejemplo por medio de una contraseña, un PIN, o de datos biométricos, más difíciles de robar.

En el caso de una identificación del usuario por medio de una contraseña o de un PIN, este procedimiento tiene la ventaja de permitir distribuir, sustituir o invalidar más fácilmente contraseñas, a distancia mediante simples manipulaciones lógicas desde una central.

En una variante, el código secreto utilizado para identificar el usuario es verificado por la central 1, y no por la cerradura. Se evita así la transmisión de listas de usuarios autorizados a las diferentes cerraduras.

Este procedimiento tiene también la ventaja de que todos los datos y todos los códigos necesarios para desbloquear la cerradura se pueden introducir directamente en la misma, sin pasar por un equipo intermedio que ofrezca una vulnerabilidad adicional a los ataques.

La presente invención se refiere también a una cerradura electrónica según la reivindicación 17.

Esta cerradura está adaptada al procedimiento anterior; presenta además la ventaja de no necesitar obligatoriamente un lector de llaves, vulnerable y costoso.

La presente invención se refiere también a un procedimiento para una central de gestión de un parque de cerraduras electrónicas según la reivindicación 26.

Este procedimiento se puede realizar de manera totalmente automática mediante un ordenador programado para estas diferentes tareas, o de manera asistida por un operador humano, o un grupo de operadores humanos, utilizando un ordenador.

Breve descripción de los dibujos

Se indican unos ejemplos de realización de la invención en la descripción ilustrada por las figuras adjuntas, en las cuales:

La figura 1 ilustra, en forma de esquema de bloques, un sistema que realiza el procedimiento y la cerradura de la invención.

La figura 2 ilustra, en forma de diagrama de flujo, los intercambios de información en el transcurso del proceso de la invención.

Ejemplo(s) de modo de realización de la invención

La figura 1 ilustra, en forma de esquema de bloques, un sistema que comprende una central 1 a la cual se pueden conectar diferentes usuarios 4 con la ayuda de un equipo móvil 3, a través de una red 2. El sistema comprende además una o varias cerraduras 5 para proteger unos dispositivos no representados, por ejemplo cajeros automáticos, cajas fuertes, salas u otros espacios protegidos.

La central 1 puede estar constituida por ejemplo por una central de llamadas, dirigida por varios operadores humanos, o un servidor o grupo de servidores que ejecuta una aplicación específica. La red 2 es por ejemplo una red de telecomunicaciones por ejemplo una red telefónica convencional, una red de tipo Internet o Intranet, o,

preferentemente, una red celular móvil. Los usuarios se pueden conectar a la central 1 estableciendo una comunicación de voz o de datos a través de la red 2.

En una variante preferida, los usuarios se conectan a la central 1 a través de una red celular móvil 2 y enviando datos por ejemplo SMS (*Short Message System),* correos electrónicos o paquetes de datos IP a través de una red 2 de tipo GSM, GPRS, HSCSD, EDGE o GPRS, por ejemplo. La central recibe, preferentemente de manera automática, datos por medio de un módem o de un rúter adaptado, y puede responder, también, al usuario enviándole sus propios datos a través de un mismo canal, o de un canal diferente. Los datos intercambiados en uno de los sentidos, o en los dos sentidos, pueden firmarse electrónicamente y/o cifrarse por parte de la central 1 y/o por parte del equipo móvil 3 por ejemplo utilizando una tarjeta chip en el equipo móvil 3.

En otra variante, los usuarios 4 se conectan a la central 1 por medio de una comunicación de voz. La central 1 utiliza, en este caso, operadores humanos para reaccionar a esta llamada de voz, y/o un sistema de reconocimiento de voz IVR (Interactive Voice Response) para analizar el contenido de las peticiones y/o de los códigos DTMF del usuario y para sintetizar una respuesta vocal.

La central 1 comprende además un banco de datos 10 de usuarios autorizados, que contiene, para cada usuario, por lo menos un código personal -o datos de verificación de código personal- así como autorizaciones por ejemplo una lista de cerraduras para cuya apertura está autorizado el usuario. El registro correspondiente a cada usuario puede indicar además unas ventanas temporales durante las cuales se autoriza un acceso a una o a varias cerraduras, un perfil de usuario, que incluye por ejemplo su nombre, sus coordenadas, claves criptográficas de comunicación con cada usuario, un historial de utilización del sistema (número de ensayos satisfactorios, de ensayos insatisfactorios, fechas, horas, etc.), y otros datos de identificación o de autenticación, incluyendo por ejemplo un número de comunicante MSISDN correspondiente a su equipo móvil 3, datos biométricos, etc.

Unos medios de cálculo 11 en la central 1 permiten ejecutar un programa aplicativo para gestionar los diferentes usuarios y sus derechos en el banco de datos 10. Los medios de cálculo permiten además ejecutar un algoritmo que permite calcular la respuesta a una pregunta (“challenge”) recibida de un usuario. Este algoritmo por ejemplo puede consultar una tabla de correspondencia en memoria ROM que indica la respuesta a cada pregunta esperada, o, preferentemente, puede calcular una función matemática a partir de cada pregunta. La función ejecutada se selecciona, preferentemente, de tal manera que el conocimiento de un número cualquiera de respuestas a preguntas anteriores no permite predecir cuál será la respuesta a la próxima pregunta (función pseudoaleatoria). El algoritmo seleccionado, o los valores que permiten parametrizarlo (por ejemplo, el valor semilla en el caso de una función pseudoaleatoria), preferentemente se mantienen confidenciales. Además, preferentemente se utiliza un algoritmo diferente, o valores diferentes, para cada cerradura 5, y/o incluso para cada usuario 4.

La central 1 puede comprender además un banco de datos de cerraduras (no representado), que comprende, para cada cerradura 5, un perfil con informaciones tales como la ubicación geográfica, el tipo de dispositivo protegido, claves criptográficas de comunicación, etc.

El equipo móvil 3 depende del tipo de red utilizada. En una variante preferente, este equipo está constituido por un equipo móvil celular por ejemplo un teléfono celular o un asistente personal, un teléfono inteligente o un ordenador personal dotado de una tarjeta de conexión a una red celular, de un módem o de un rúter. También es posible utilizar un aparato de comunicación dedicado a este uso.

El equipo móvil 3 puede comprender unos medios de geolocalización 30 por ejemplo un receptor satelital de tipo GPS que permita determinar su posición y, eventualmente, transmitirla a la central 1. Un equipo de protección del trabajador aislado (PTI) 31 permite verificar si el usuario 4 del equipo móvil 3 está despierto por ejemplo verificando si el mismo se mueve, si está en vertical, si reacciona a solicitudes de respuesta, etc. El equipo móvil 3 puede comprender además unos medios de identificación y/o de autenticación 32 adicionales por ejemplo una tarjeta chip (por ejemplo, tarjeta SIM), de medios de introducción y de verificación de códigos PIN, de un sensor biométrico, etc. La identificación y/o la autenticación del usuario 4 se puede efectuar localmente, es decir, en el equipo móvil o en una tarjeta chip introducida en el equipo, o a distancia, es decir por ejemplo en la central 1 que dispone, entonces, de medios de verificación de los datos de la tarjeta chip, de los códigos PIN y/o de los datos biométricos introducidos. El equipo móvil 3 puede ser por ejemplo portátil o puede estar instalado en un vehículo.

No obstante, es posible utilizar un teléfono móvil convencional como equipo móvil en el ámbito de la invención; solamente es necesario que el usuario se pueda poner en contacto, por medio de este equipo, con una central 1 para enviar una pregunta y recibir una respuesta correspondiente. Resulta incluso ventajoso, para aumentar la seguridad, el establecimiento de las comunicaciones entre los diferentes usuarios y la central mediante canales de tipo diferente. La central puede utilizar por ejemplo esta información adicional y convenir con un transportista de fondos por ejemplo que la pregunta se deberá transmitir oralmente, incluso si el transportista de fondos dispone de un equipo que permite una comunicación de datos.

El usuario 4 es por ejemplo un empleado de banca, un transportista de fondos, un técnico de reparación, o cualquier persona física autorizada por la central 1 a abrir la cerradura 5. El usuario 4 tiene conocimiento de un código personal secreto que le ha sido transmitido por la central 1, y, con el cual, se puede identificar con respecto a una o varias cerraduras 5 de un parque de cerraduras gestionadas por la central 1. Además, el usuario 4 está capacitado, preferentemente, para identificarse con respecto a su equipo móvil 3 por medio de otro código secreto por ejemplo el código PIN del teléfono y/o de la tarjeta SIM. En el ámbito de la invención son concebibles otros medios de identificación del usuario 4 con respecto a la cerradura 5 y/o con respecto al equipo móvil 3; por ejemplo, el usuario podría demostrar su identidad presentando un objeto personal, tal como una llave o una tarjeta chip, o por identificación biométrica con la ayuda de huellas dactilares, del iris, de la retina, de la voz, de la cara, etc. Evidentemente, pueden ponerse en práctica procedimientos diferentes para identificar o autentificar el usuario 4 con respecto al equipo móvil 3 y con respecto a la cerradura 5. Es además posible combinar varios procedimientos de identificación. Por otra parte, los datos de identificación introducidos en el equipo móvil 3 se pueden transmitir a la central 1 para su verificación.

La cerradura 5 comprende un elemento electromecánico 52 por ejemplo un pestillo, cuya posición es controlada por un dispositivo lógico en el interior de la cerradura 5 para actuar sobre un mecanismo mecánico (“varillaje”) que permite bloquear o, por el contrario, desbloquear el acceso al espacio protegido, por ejemplo al interior de un cajero. La cerradura está destinada, preferentemente, a utilizarse en combinación con un dispositivo que contiene un espacio a proteger por ejemplo con un cajero automático o una caja fuerte; no constituye, por tanto, en sí misma, una caja fuerte del tipo mencionado, y no comprende un espacio protegido, sino que dispone de medios no representados para asociarla mecánicamente y/o eléctricamente, de manera difícilmente desmontable, con una caja fuerte o un cajero del tipo mencionado.

Un teclado numérico o alfanumérico 51 asociado a la cerradura 5 permite que el usuario introduzca su código personal y la respuesta a las preguntas planteadas. En la cerradura 5 pueden preverse, eventualmente, otros elementos de introducción de datos (no representados) por ejemplo un sensor biométrico, una cámara, un micrófono, etc. La cerradura comprende además una pantalla 50 para visualizar mensajes en modo texto o matricial, incluyendo preguntas, invitaciones para introducir una respuesta, y mensajes de estado.

La cerradura comprende además preferentemente, una o varias interfaces 53 opcionales que le permiten intercambiar datos con el dispositivo que debe proteger por ejemplo un cajero de banca electrónica, y/o con la central 1 a través de cualquier red adaptada por ejemplo una red telefónica o Internet. La comunicación de datos con el dispositivo a proteger en el que está montada la cerradura permite en particular mejorar la seguridad, gracias al intercambio de informaciones que permiten detectar fraudes probables con la ayuda de combinaciones de índices, y gracias a la generación de los archivos de registros que tienen en cuenta datos recopilados tanto por la cerradura como por el dispositivo protegido. Llegado el caso, esta comunicación también puede utilizarse para controlar la cerradura 5 por medio del teclado del cajero, visualizar mensajes dependientes del funcionamiento de la cerradura 5 sobre la pantalla del cajero, transmitir alarmas activadas por la cerradura por medio del cajero, o activar otras acciones efectuadas por el cajero. La comunicación, preferentemente bidireccional, entre la cerradura 5 y la central 10 permite por ejemplo modificar a distancia la lista de los usuarios autorizados a identificarse con respecto a cada cerradura 5 (a no ser que esta verificación sea realizada por la central), modificar los algoritmos de verificación de respuesta a distancia, consultar los archivos de registros generados por la cerradura, y detectar a distancia otros eventos vinculados a la utilización de la cerradura. Esta comunicación con la central 1 también puede efectuarse a través del dispositivo protegido por la cerradura por ejemplo utilizando un módem o un rúter de este dispositivo. En un modo de realización, los datos intercambiados por la cerradura y la central 1 son firmados y cifrados electrónicamente por ejemplo a través de un túnel privado virtual (VPN, *virtual private network*) para preservar su confidencialidad y su autenticidad incluso con respecto al cajero a proteger.

La cerradura 5 comprende además preferentemente, un reloj electrónico 54 que le permite determinar la fecha y la hora de manera autónoma, y calcular intervalos de tiempo. Unos medios de cálculo no representados por ejemplo un microcontrolador, un microprocesador con una memoria, un microordenador industrial, un circuito de tipo asic y/o un circuito FPGA, etc., permiten gestionar los diálogos con el usuario, y controlar el dispositivo electromecánico que provoca el bloqueo o el desbloqueo de la cerradura. Los medios de cálculo comprenden además preferentemente, un módulo por ejemplo un módulo lógico, para generar, y a continuación visualizar, una pregunta como respuesta a la introducción de un código de identificación personal aceptado, y un módulo por ejemplo lógico, para verificar si una respuesta a la pregunta es correcta, y para provocar el desbloqueo de la cerradura en caso de respuesta correcta.

Preferentemente, los medios de cálculo están protegidos contra las manipulaciones físicas o lógicas y por ejemplo pueden autodestruirse, manteniendo la cerradura cerrada, durante manipulaciones fraudulentas. Además, la cerradura 5 puede comprender unos elementos de conexión inalámbricos con el equipo móvil 3 por ejemplo una interfaz de tipo Bluetooth, con el fin por ejemplo de detectar y de verificar la presencia de este equipo en las proximidades; sin embargo, se puede renunciar a estos medios en caso de que los mismos introduzcan una vulnerabilidad adicional.

Preferentemente, la cerradura 5 es autónoma eléctricamente y se alimenta con la ayuda de pilas o de una batería; permanece mecánicamente cerrada cuando las pilas o baterías están descargadas. La recarga o la sustitución de las pilas o baterías se puede efectuar, por tanto, sin desbloquear la cerradura. En una variante, la cerradura se alimenta eléctricamente por el dispositivo en el que está montada por ejemplo un cajero automático. Todavía en otra variante, se alimenta por medio de un generador accionado por el usuario; el reloj 54 utiliza, en este caso, su propia fuente de energía con el fin de mantener la hora incluso cuando el resto del sistema ya no se alimente eléctricamente.

A continuación se va a describir, con la ayuda de la figura 2, un ejemplo de puesta en práctica del procedimiento de la invención.

Inicialmente, un usuario 4 que desea desbloquear la cerradura 5 se encuentra físicamente delante de esta cerradura e introduce, en el transcurso de la etapa 100, un código personal en el teclado 51 por ejemplo un código numérico o alfanumérico por ejemplo un código de 6 cifras.

En el transcurso de la etapa 101, los medios de cálculo en la cerradura verifican el código personal introducido. En una primera variante, el código personal se compara con una lista de códigos aceptados (“lista blanca”) almacenada en la cerradura. Sin embargo, esta variante tiene el inconveniente de tener que transmitir dicha lista a la cerradura por ejemplo a través de una red de telecomunicaciones, o por medio de transportistas de fondos. Una transmisión de este tipo está sujeta a riesgos de interceptación o de espionaje. Con el fin de evitar este riesgo, en una segunda variante preferente, basta con que la cerradura verifique, en el transcurso de la etapa 101, si el código personal introducido es plausible por ejemplo si el formato del código es admisible, si un eventual código de paridad es correcto, o si el código personal introducido no pertenece a una lista de códigos rechazados (“lista negra”) por inexistentes o pertenecientes a usuarios rechazados. La verificación del código personal particular introducido por el usuario se delega, en esta segunda variante, a la central, a la cual se deberá transmitir de manera implícita o explícita el código posteriormente.

Si la cerradura, en el transcurso de la etapa 101, detecta que el código personal introducido no es válido, el mismo es rechazado, y, en la pantalla de visualización 50, se puede visualizar un mensaje de error para informar al usuario e invitarle a introducir un código nuevo. Con el fin de impedir ataques por “fuerza bruta”, es decir, probando sucesivamente un número elevado de códigos diferentes, es posible por ejemplo introducir un tiempo entre cada tentativa y/o limitar el número de tentativas insatisfactorias posibles antes de bloquear la cerradura durante un periodo más prolongado, o hasta la introducción de una maniobra de desbloqueo.

En una de las variantes, el usuario se identifica con respecto a la cerradura demostrando la posesión de un objeto por ejemplo una llave, una llave electrónica, una tarjeta chip, etc. El propio objeto presentado puede estar protegido por un código, en particular en el caso de una tarjeta chip. Sin embargo, esta solución tiene el inconveniente de necesitar una organización para distribuir y gestionar los objetos a presentar. El usuario también se puede identificar por medio de datos biométricos adquiridos por medio de un sensor biométrico por ejemplo con la ayuda de sus huellas dactilares, del iris, de la retina, de la cara, de la voz, etc. No obstante, estos datos biométricos tienen el inconveniente de no poderse sustituir con la facilidad de un código personal que se puede transmitir en el último momento al usuario; además, se requiere un registro del usuario para adquirir sus datos biométricos de referencia.

Además, pueden combinarse diferentes procedimientos de identificación. Es también posible reclamar una identificación adicional o diferente según las circunstancias; por ejemplo, puede exigirse una identificación biométrica, o por clave, cuando la identificación por código personal no haya funcionado después de un número de intentos predeterminado, o cuando la cantidad disponible en el espacio protegido supera una cierta cantidad, o cuando otras circunstancias imponen un aumento de la seguridad.

Si el código personal es válido, los medios de cálculo de la cerradura (o, posteriormente, los de la central) verifican los derechos de acceso vinculados al usuario identificado por este código. Los derechos de acceso pueden depender del tiempo; por ejemplo, es posible no autorizar un desbloqueo de la cerradura más que durante una ventana temporal limitada correspondiente a la hora a la cual se espera al usuario. Esta ventana temporal puede estar codificada, con otras informaciones, en la respuesta de la central que se describe más abajo.

Según el objeto protegido, es también posible permitir un acceso a partes diferentes del espacio protegido para diferentes usuarios; es concebible por ejemplo autorizar a un técnico el acceso únicamente a diferentes órganos de un cajero por ejemplo para reponer el papel, extraer ficheros de registros o efectuar otras operaciones de mantenimiento, mientras que el acceso a la caja fuerte se reserva para otros usuarios identificados con la ayuda de otros códigos.

Según la invención, la cerradura 5 verifica también si se ha efectuado una manipulación particular durante la introducción del código personal por parte del usuario 4, con el fin de señalar que el mismo se encuentra bajo coacción por ejemplo porque un asaltante está obligándole a introducir el código. La manipulación particular

puede implicar por ejemplo la introducción de un código personal diferente, la presión de una tecla o de un órgano adicional, un apoyo prolongado sobre una tecla, u otras manipulaciones identificables sin ambigüedades por la cerradura 5, aunque difíciles de detectar para un asaltante que observe la maniobra. La detección de una manipulación particular conlleva un comportamiento diferente de la cerradura, tal como se verá más abajo.

En caso de identificación válida, la cerradura 5 visualiza, a continuación, en el transcurso de la etapa 102, una pregunta en la pantalla de visualización 50. La pregunta visualizada puede depender de la hora, de la fecha, del usuario identificado, de la cerradura, de otros parámetros recogidos por la cerradura, y/o de una eventual detección de manipulación para señalar una coacción. Por otra parte, la elección de la pregunta puede depender de un factor aleatorio. Preferentemente, cada pregunta se visualiza una sola vez y no se vuelve a utilizar, o por lo menos no para el mismo usuario. La pregunta visualizada puede ser generada por una función matemática por ejemplo una función pseudoaleatoria, y/o se puede seleccionar en una tabla de preguntas predefinidas. En una variante preferente, la función pseudoaleatoria depende, por lo menos parcialmente, del valor de un contador incrementado en cada apertura del cofre y/o en cada tentativa de desbloqueo; el contador no se puede decrementar nunca, y el valor máximo que se puede contar es suficiente para garantizar que el contador no entra en bucle. También será posible utilizar la hora que cuenta el reloj de la cerradura para inicializar la función pseudoaleatoria; sin embargo, un reloj debe poder ponerse en hora, y, por lo tanto, debe poder atrasarse, lo cual podría usarse para “retroceder en el tiempo” con el fin de obligar a la cerradura a generar nuevamente una pregunta cuya respuesta ya es conocida.

Las identificaciones satisfactorias y las tentativas de identificaciones insatisfactorias se registran, preferentemente, en un archivo de registro en la cerradura, con la fecha y la hora del evento. Este archivo puede ser consultado por un técnico por ejemplo introduciendo un código particular en el teclado 51, conectando un ordenador a un conector en la cara frontal de la cerradura, y/o a distancia desde la central 1 a través de una red de comunicaciones.

El usuario 4 lee la pregunta visualizada en el transcurso de la etapa 103, y a continuación la introduce en el transcurso de la etapa 104 en el teclado de su equipo móvil 3. Como la pregunta visualizada en la pantalla de visualización 50 es impredecible, y es posible distinguir las preguntas posibles de las preguntas no lícitas, se garantiza así que el usuario 4 se encuentra claramente en las proximidades de la cerradura 5 a abrir.

En el transcurso de la etapa 105, la pregunta introducida por el usuario es transmitida por el equipo móvil 3 a la central por ejemplo en forma de mensaje corto por ejemplo de SMS, de correo electrónico, de paquetes de datos, de código DTMF, o de mensaje de voz pronunciado por el usuario.

El equipo móvil 3 puede ejecutar una aplicación dedicada por ejemplo una miniaplicación Java (marca registrada), para facilitar la introducción de la pregunta y su transmisión hacia la central 1. En una variante, la pregunta es simplemente introducida por el usuario y se transmite a un número telefónico o hacia una dirección de correo electrónico conocida del usuario.

El acceso al equipo móvil 3, o a la aplicación del equipo móvil, puede estar protegido por una contraseña, un código PIN, o puede requerir otras medidas de identificación o de autentificación del usuario 4.

Además de la pregunta introducida por el usuario, el mensaje transmitido a la central 1 en el transcurso de la etapa 105 puede incluir otras informaciones, incluyendo por ejemplo una identificación del equipo móvil 3 utilizado (por ejemplo, un número de comunicante MSISDN), datos de identificación del usuario (incluyendo su código personal, aunque también por ejemplo una contraseña, un código PIN, datos biométricos, datos extraídos de una tarjeta chip en el equipo móvil, etc.), informaciones de posiciones suministradas por el módulo de geolocalización 30, informaciones suministradas por el módulo PTI 31, etc. El mensaje puede firmarse además electrónicamente por medio de una tarjeta chip en el equipo móvil 3, con el fin de demostrar su autenticidad y su integridad, y/o se puede cifrar con el fin de garantizar su confidencialidad.

En el transcurso de la etapa 106, la central 1 recibe el mensaje transmitido por el usuario y lo verifica. La verificación implica por ejemplo controlar si la pregunta transmitida es una pregunta lícita, en función del usuario que la utiliza, de la cerradura delante de la cual se encuentra, de la hora, etc. Si el código personal del usuario se ha transmitido con la pregunta, o si el mismo está contenido implícitamente en la pregunta, la central 1 también puede asegurarse de que este usuario está efectivamente autorizado a acceder a esta cerradura en ese momento por ejemplo en función de un plan de ruta establecido previamente para un transportista de fondos que se desplaza entre varias cerraduras. Otras verificaciones pueden tener en cuenta la ubicación geográfica del usuario, datos suministrados por el dispositivo PTI, eventuales datos suministrados directamente por la cerradura, verificaciones de información que señalen una manipulación para indicar una coacción, etc.

Si las verificaciones efectuadas en el transcurso de la etapa 106 permiten determinar que la pregunta es una pregunta legítima transmitida en el momento adecuado por un usuario autorizado, se determinan preferentemente los derechos de este usuario. Cuando el usuario posee por lo menos ciertos derechos, se calcula una respuesta a esta pregunta en el transcurso de la etapa 107, por medio de un algoritmo desconocido

para los usuarios y ejecutado por los medios de cálculo 11. Preferentemente, la respuesta está constituida por una sucesión numérica o alfanumérica que no permite que un usuario determine inmediatamente si la misma contiene instrucciones implícitas para la cerradura.

En el caso contrario en el que la pregunta recibida no es válida, o si la misma ha sido transmitida por un usuario no autorizado, o cuando el usuario no posee los derechos de acceso necesarios, o cuando se han detectado otras anomalías, no se calcula ninguna respuesta. En una de las variantes, un mensaje de error que informa al usuario es transmitido entonces al equipo móvil 3 y visualizado por este último, con el fin por ejemplo de permitir que el usuario corrija una errata durante la introducción de la pregunta. Alternativamente, la central puede suministrar una respuesta modificada que conlleve un comportamiento modificado de la cerradura. La reacción de la central y la respuesta enviada puede depender también de la anomalía detectada, del número de intentos insatisfactorios, o de otras condiciones.

Si la central, a partir de la pregunta recibida, detecta que el usuario ha efectuado una manipulación particular para indicar que se encuentra bajo coacción, la misma calcula una respuesta modificada con respecto a la respuesta normal, con el fin de provocar un comportamiento particular de la cerradura. Diferentes respuestas modificadas pueden ser seleccionadas automáticamente o por operadores humanos según las circunstancias, con el fin de desencadenar diferentes reacciones.

En la respuesta se pueden codificar otras informaciones complementarias por ejemplo para definir los derechos de acceso del usuario a la cerradura por ejemplo en función del tiempo.

La respuesta a la pregunta se transmite, a continuación, al equipo móvil en el transcurso de la etapa 108, y a continuación se visualiza y es leída por el usuario en el transcurso de la etapa 109. La respuesta puede comprender por ejemplo un código numérico o alfanumérico y la misma es introducida por el usuario 4 en el teclado 51 de la cerradura 5 en el transcurso de la etapa 110.

En el transcurso de la etapa 111, los medios de cálculo en la cerradura 5 verifican si la respuesta recibida es correcta. En una variante, esta verificación implica una comparación con una respuesta calculada por la propia cerradura, ejecutando el mismo algoritmo que el correspondiente ejecutado por la central 1. En una variante, la verificación de la respuesta recibida es efectuada sin volver a calcularla independientemente por ejemplo verificando la respuesta recibida por medio de una clave de verificación que permite distinguir la o las respuestas posibles a la pregunta con respecto a respuestas no válidas, en función de la pregunta y/o de otros parámetros. Esta variante tiene la ventaja de no requerir copias del algoritmo en una multitud de cerraduras diseminadas sobre un territorio; es además compatible con algoritmos susceptibles de suministrar varias respuestas válidas a una misma pregunta.

Los medios de cálculo 5 verifican además en el transcurso de la etapa 111, si la respuesta recibida tiene en cuenta una detección de manipulación por un usuario bajo coacción, o si se han codificado otros parámetros en esta respuesta.

En una variante no reivindicada, el usuario indica un estado de coacción a la cerradura 5 durante la introducción de la respuesta en el teclado en el transcurso de la etapa 110 por ejemplo introduciendo una cifra adicional, etc. Sin embargo, esta solución es menos segura ya que un usurpador podría introducir él mismo la respuesta, sin efectuar una manipulación adicional. Además, a la central no se le informa de una manipulación.

En una variante adicional no reivindicada, la cerradura 5 detecta directamente un estado de coacción a partir de sensores o de datos adicionales, de datos transmitidos por el cajero al cual está asociada la cerradura, o de datos transmitidos directamente por la central 1.

Si la cerradura, en el transcurso de la etapa 111, determina que la respuesta introducida es correcta, y que no se corresponde con un estado de coacción, la cerradura se desbloquea en el transcurso de la etapa 112, hasta el próximo bloqueo manual o durante un intervalo de tiempo limitado. El usuario puede, así, acceder al espacio protegido, o a una parte de este espacio. Este evento se protocoliza en el archivo de registro, indicando la hora y el intervalo de tiempo del desbloqueo. Por otra parte, el contador utilizado para inicializar la función pseudoaleatoria se incrementa de manera irreversible.

Si, en el transcurso de la etapa 111, la cerradura determina que la respuesta introducida es incorrecta, la cerradura queda cerrada, y, en la pantalla de visualización 50, se puede visualizar un mensaje de error. Después de un número predeterminado de intentos insatisfactorios, puede activarse localmente una alarma o la misma se puede enviar a la central 1 o hacia otra dirección predeterminada. En una variante, los billetes en el interior del cajero son destruidos automáticamente o marcados con una tinta indeleble.

Si, en el transcurso de la etapa 111, la cerradura determina que la respuesta introducida es correcta, pero que se corresponde con un estado de coacción, efectúa una de las acciones siguientes según la respuesta:

- mantenimiento del bloqueo, eventualmente incluso si se introduce posteriormente una respuesta correcta durante un intervalo de tiempo limitado,

- desbloqueo retardado de la cerradura después de un tiempo breve, aunque mayor que el tiempo habitual

- desbloqueo retardado de la cerradura después de un tiempo largo por ejemplo superior a tres minutos,

- visualización de un mensaje particular en la pantalla de visualización 50 de la cerradura por ejemplo para indicar al asaltante que ha sido detectado,

- activación de una alarma por ejemplo una alarma sonora o

- destrucción del contenido del espacio protegido por la cerradura por ejemplo por marcado de los billetes o por medio de una tinta indeleble.

Sin embargo, las dos últimas opciones se deben utilizan con moderación para evitar el riesgo de que el usuario legítimo sea tomado como rehén o víctima de represalias.

Además, estas medidas diferentes se pueden combinar.

Después de la introducción de una respuesta correcta, o de una respuesta que indica una manipulación, en el transcurso de una etapa adicional no ilustrada se visualiza preferentemente un código de recibo en la pantalla de visualización 50. El usuario, a continuación, introduce este código de recibo en su equipo móvil y lo transmite a la central 1, de la misma manera que la pregunta anterior, con el fin de indicar a la central el fin de su misión. El código de recibo requerido es, preferentemente, único e impredecible de antemano, para garantizar que el usuario lo ha leído bien tras la manipulación y que no lo ha deducido de otra manera. No obstante, la central está en condiciones de verificar si el código de recibo transmitido es lícito.

De nuevo, el código de recibo generado por la cerradura o reintroducido por el usuario puede contener indicaciones que le señalen a la central eventos particulares por ejemplo para indicar si la cerradura ha sido abierta, un nuevo estado de coacción, o cualquier otro evento. Además, el código de recibo transmitido, de la misma manera que la pregunta anterior, se puede firmar, cifrar, y acompañar con datos tales como la fecha, la hora, la identificación del usuario, de equipo móvil, de posición geográfica, etc. Así, la central puede verificar estos datos, o detectar la ausencia de envío de mensaje de recibo después de un tiempo predeterminado, para decidir una acción adecuada, incluyendo la activación de una alarma, la activación de una intervención, y/o el bloqueo de otras cerraduras próximas o sobre el trayecto previsto del usuario incluso en caso de maniobra correcta.

Preferentemente, el código de recibo generado depende, de la misma manera que la pregunta o la respuesta, del usuario en curso, de la cerradura en curso y/o de otros parámetros tales como la fecha, la hora, la detección de manipulaciones eventuales.

En el procedimiento anterior de la presente, una autorización de desbloqueo de una cerradura particular por un usuario particular se puede modificar por parte de la central 1, de una de las formas siguientes:

- Comunicando un nuevo código personal al usuario por ejemplo por medio de una llamada telefónica, de un SMS, de un correo electrónico o de otro mensaje enviado al equipo móvil 3, o transmitido oralmente al usuario

- Modificando los códigos personales aceptados por las cerraduras 5 por ejemplo enviando listas nuevas de códigos aceptados (lista blanca; solamente en la variante en la que estas listas se almacenan en la cerradura), listas nuevas de códigos sospechosos, que requieren verificaciones adicionales (lista gris), o modificando los derechos de acceso asociados a estos códigos. Las listas de códigos y los derechos de acceso pueden ser transmitidos por un canal de telecomunicaciones a través de una interfaz de telecomunicaciones en la cerradura, y/o por medio de una interfaz de telecomunicaciones vinculada al dispositivo protegido por la cerradura, o pueden ser introducidos directamente, a través de un soporte de datos físico, por un técnico encargado del mantenimiento.

- Modificando los códigos personales aceptados por la central, en función de listas blancas, grises o negras, o de otros parámetros tales como el plan de ruta previsto del usuario.

- Modificando la respuesta dada a una pregunta transmitida por un usuario, o negándose responder a estas preguntas.

- Enviando una orden directamente a la cerradura por ejemplo una orden de mantener el bloqueo durante un intervalo.

Por otra parte, independientemente del comportamiento de la central, la propia cerradura 5 puede autorizar o denegar el desbloqueo en función de parámetros adquiridos directamente o a través del dispositivo protegido por ejemplo con la ayuda de sensores, cámaras o micrófonos asociados a la cerradura o al dispositivo, obtenidos analizando las manipulaciones del usuario sobre el teclado 5, o según un historial interno de las manipulaciones de este usuario y/o de la cerradura 5.

Es posible, sin embargo, en el ámbito de la invención, prever solamente una parte de las posibilidades de autorización de desbloqueo mencionadas anteriormente en la presente.

La cerradura descrita anteriormente en la presente se puede utilizar para proteger otros espacios que no sean cajeros automáticos por ejemplo armeros utilizados en las comisarías o por el ejército, cajas fuertes, u otros espacios cuyo bloqueo o desbloqueo por parte de un usuario local debe ser autorizado por una central a distancia.

Por otra parte, la cerradura de la invención se puede programar en cualquier momento por ejemplo desde la central y/o con la ayuda de un código particular introducido por un usuario en las proximidades, para funcionar en un modo diferente al modo interactivo descrito más arriba. Por ejemplo, sería posible reprogramar esta cerradura para autorizar su desbloqueo por ciertos usuarios, o incluso por todos los usuarios, sin establecer una conexión con la central.

REIVINDICACIONES

1. Procedimiento de control de bloqueo de una cerradura electrónica (5), que comprende las siguientes etapas:

un usuario (4) se identifica ante la cerradura electrónica (5) introduciendo un código personal en unos medios de introducción de datos (51) de la cerradura,

la cerradura electrónica (5) visualiza una pregunta,

el usuario transmite la pregunta con la ayuda de un equipo móvil a una central (1),

la central calcula la respuesta a la pregunta y transmite esta respuesta al equipo móvil del usuario para que sea visualizada en el mismo y después leída por el usuario,

el usuario introduce la respuesta en la cerradura,

la cerradura verifica si la respuesta es correcta y decide, en función de esta respuesta, el desbloqueo de la cerradura,

en el que

dicho usuario (4) efectúa una manipulación particular cuando tiene lugar la introducción de su código personal cuando desea señalar que se encuentra bajo coacción,

la cerradura detecta si se efectúa una manipulación particular cuando tiene lugar la introducción del código personal del usuario,

la cerradura genera y visualiza una pregunta que depende de una eventual detección de manipulación particular,

dicha central (1) reacciona entonces generando una respuesta modificada a dicha pregunta, siendo dicha respuesta modificada diferente de la respuesta generada cuando no se efectúa dicha manipulación particular,

cuando dicho usuario introduce dicha respuesta modificada, dicha cerradura efectúa por lo menos una de las siguientes acciones:

mantenimiento del bloqueo de la cerradura (5);

temporización del desbloqueo de la cerradura (5) mediante desbloqueo después de un tiempo más prolongado que el tiempo habitual;

visualización de un mensaje en la pantalla de visualización (50) de dicha cerradura (5);

activación de una alarma;

destrucción o marcado del contenido del dispositivo protegido por dicha cerradura (5).

2. Procedimiento según la reivindicación 1, en el que al final de la manipulación, un código de recibo es visualizado por dicha cerradura (5) y transmitido por dicho usuario a la central (1) con la ayuda de un equipo móvil (3).

3. Procedimiento según una de las reivindicaciones 1 o 2, en el que se visualiza una pregunta diferente en cada acceso a la cerradura.

4. Procedimiento según una de las reivindicaciones 1 a 3, en el que dicha central verifica si dicha pregunta es válida.

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que las preguntas visualizadas dependen de dichos usuarios.

6. Procedimiento según una de las reivindicaciones 1 a 5, en el que dicha respuesta a dicha pregunta se calcula por medio de un algoritmo en dicha central (1), y en el que dicha cerradura verifica, por medio del o de un algoritmo ejecutado en la cerradura, si dicha respuesta es correcta.

7. Procedimiento según una de las reivindicaciones 1 a 6, en el que dicho usuario (4) transmite dicha respuesta a dicha central por medio de una comunicación establecida a través de una red celular (2) independiente de dicha

cerradura.

8. Procedimiento según la reivindicación 7, en el que dicho usuario (4) transmite dicha respuesta a dicha central (1) por medio de un equipo móvil (3) apto para conectarse en una red celular,

determinando dicho equipo móvil la posición de dicho usuario por medio de un dispositivo de geolocalización (30),

siendo dicha posición transmitida a dicha central (1),

verificando dicha central dicha posición antes de transmitir dicha respuesta a dicha pregunta.

9. Procedimiento según una de las reivindicaciones 7 a 8, utilizando dicho equipo móvil (3) un equipo de protección de trabajador aislado (31) con el fin de determinar si dicho usuario está vivo y/o si está despierto.

10. Procedimiento según una de las reivindicaciones 7 a 9, autentificando dicho equipo móvil (3) a dicho usuario por medio de una tarjeta chip, de un código personal y/o de datos biométricos (32).

11. Procedimiento según la reivindicación 10, siendo la identidad de dicho usuario (4) determinada en dicho equipo móvil (3) transmitida a dicha central (1) para su verificación.

12. Procedimiento según una de las reivindicaciones 1 a 11, en el que dicho usuario (4) se identifica ante la cerradura electrónica (5) por medio de un código personal introducido en un teclado (51) de la cerradura (5).

13. Procedimiento según la reivindicación 12, en el que un nuevo código personal es transmitido por dicha central a dicho usuario (4).

14. Procedimiento según una de las reivindicaciones 1 a 13, que comprende una etapa previa de definición de derechos de acceso de los usuarios identificados a dicha cerradura.

15. Procedimiento según una de las reivindicaciones 2 a 14, en el que se visualiza un código de recibo diferente al final de cada manipulación.

16. Procedimiento según una de las reivindicaciones 2 a 15, en el que dicho código de recibo depende del usuario en curso, de la apertura de la cerradura, de la cerradura en curso, de la fecha, de la hora, y/o de la detección de manipulaciones eventuales.

17. Cerradura electrónica (5) que comprende:

unos medios de introducción de datos (51) para la introducción de un código de identificación personal por un usuario,

unos medios para detectar una manipulación particular efectuada por el usuario cuando tiene lugar la introducción de su código personal cuando desea señalar que se encuentra bajo coacción,

un módulo configurado para generar y después visualizar una pregunta en respuesta a la introducción de un código de identificación personal, dependiendo dicha pregunta generada de una eventual detección de manipulación particular cuando tiene lugar la introducción del código de identificación personal y que corresponde a un estado de coacción,

un módulo (11) configurado para verificar si una respuesta a dicha pregunta introducida por dichos medios de introducción de datos (51) es correcta, y para provocar el desbloqueo de dicha cerradura en caso de respuesta correcta, permitiendo dicho módulo (11) verificar además si dicha respuesta es una respuesta modificada correspondiente a un estado de coacción,

unos medios para temporizar el desbloqueo de la cerradura (5) después de un tiempo más largo que el tiempo habitual o para mantener el bloqueo de la cerradura (5) o para visualizar un mensaje o para activar una alarma o para destruir o marcar el contenido del dispositivo protegido por dicha cerradura en caso de introducción de respuesta modificada.

18. Cerradura según la reivindicación 17, que comprende unos medios para generar y visualizar un código de recibo después de una tentativa de desbloqueo.

19. Cerradura según una de las reivindicaciones 17 a 18, que comprende unos medios para verificar la plausibilidad de dicho código personal, estando dichos medios desprovistos de lista de usuarios autorizados.

20. Cerradura según una de las reivindicaciones 17 a 19, que comprende un archivo de registro para clasificar los eventos provocados por dichos usuarios.

21. Cerradura según una de las reivindicaciones 17 a 20, que comprende un reloj alimentado permanentemente para determinar la hora y la fecha.

22. Cerradura según una de las reivindicaciones 17 a 21, que comprende un contador incrementable de manera irreversible para inicializar una función pseudoaleatoria utilizada para generar dicha pregunta.

23. Cerradura según una de las reivindicaciones 17 a 22, que comprende una interfaz para intercambiar datos con un dispositivo protegido por dicha cerradura.

24. Cerradura según una de las reivindicaciones 17 a 23, que comprende una interfaz para intercambiar datos con una central a distancia.

25. Procedimiento para una central (1) de gestión de parque de cerraduras electrónicas según una de las reivindicaciones 17 a 24, que comprende las etapas siguientes:

distribución de códigos personales a una pluralidad de usuarios (4) con el fin de permitirles identificarse con respecto a por lo menos ciertas de dichas cerraduras,

determinación de los derechos de acceso de cada usuario (4) a cada cerradura (5),

recepción de una pregunta transmitida por dicho usuario a través de una red de telecomunicaciones (2) con la ayuda de un equipo móvil de dicho usuario,

verificación de la plausibilidad de dicha pregunta,

cálculo de una respuesta a dicha pregunta por medio de un algoritmo confidencial,

transmisión de dicha respuesta a dicho equipo móvil del usuario,

caracterizado por una etapa de detección de indicaciones en dicha pregunta de que dicho usuario (4) se encuentra bajo coacción, y de modificación de dicha respuesta en este caso, de manera que cuando dicho usuario introduce dicha respuesta modificada, dicha cerradura efectúa por lo menos una de las acciones siguientes:

mantenimiento del bloqueo de la cerradura (5);

temporización del desbloqueo de la cerradura (5) por desbloqueo después de un tiempo más prolongado que el tiempo habitual;

visualización de un mensaje en la pantalla de visualización (50) de dicha cerradura (5);

activación de una alarma;

destrucción o marcado del contenido del dispositivo protegido por dicha cerradura (5).

26. Procedimiento según la reivindicación 25, en el que dicho algoritmo es diferente para cada usuario (4).

27. Procedimiento según una de las reivindicaciones 25 a 26, que comprende una etapa de verificación de la posición geográfica de dicho usuario con la ayuda de informaciones transmitidas por este último.

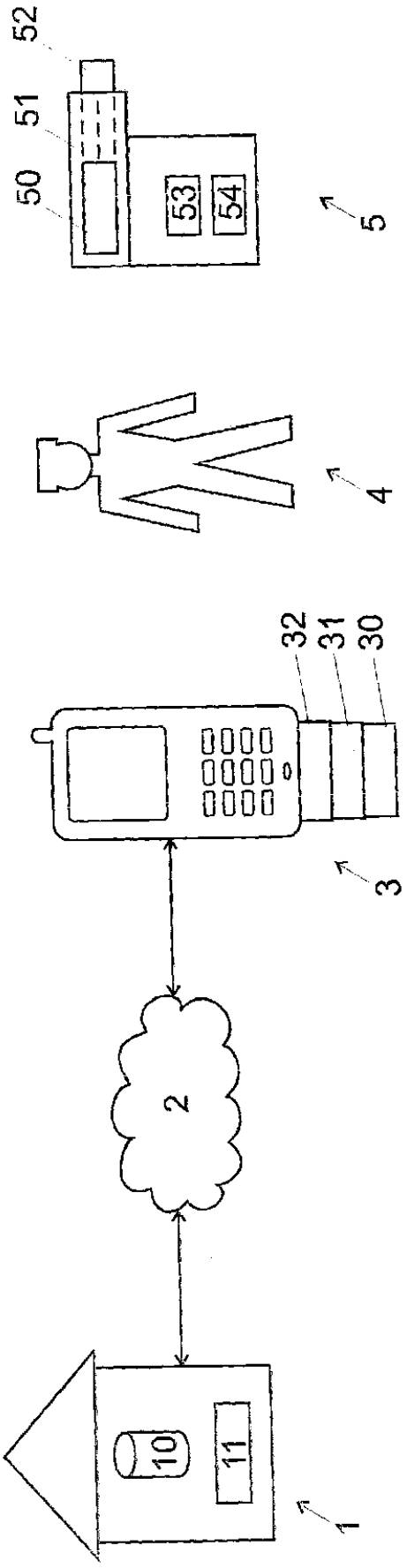

Fig. 1

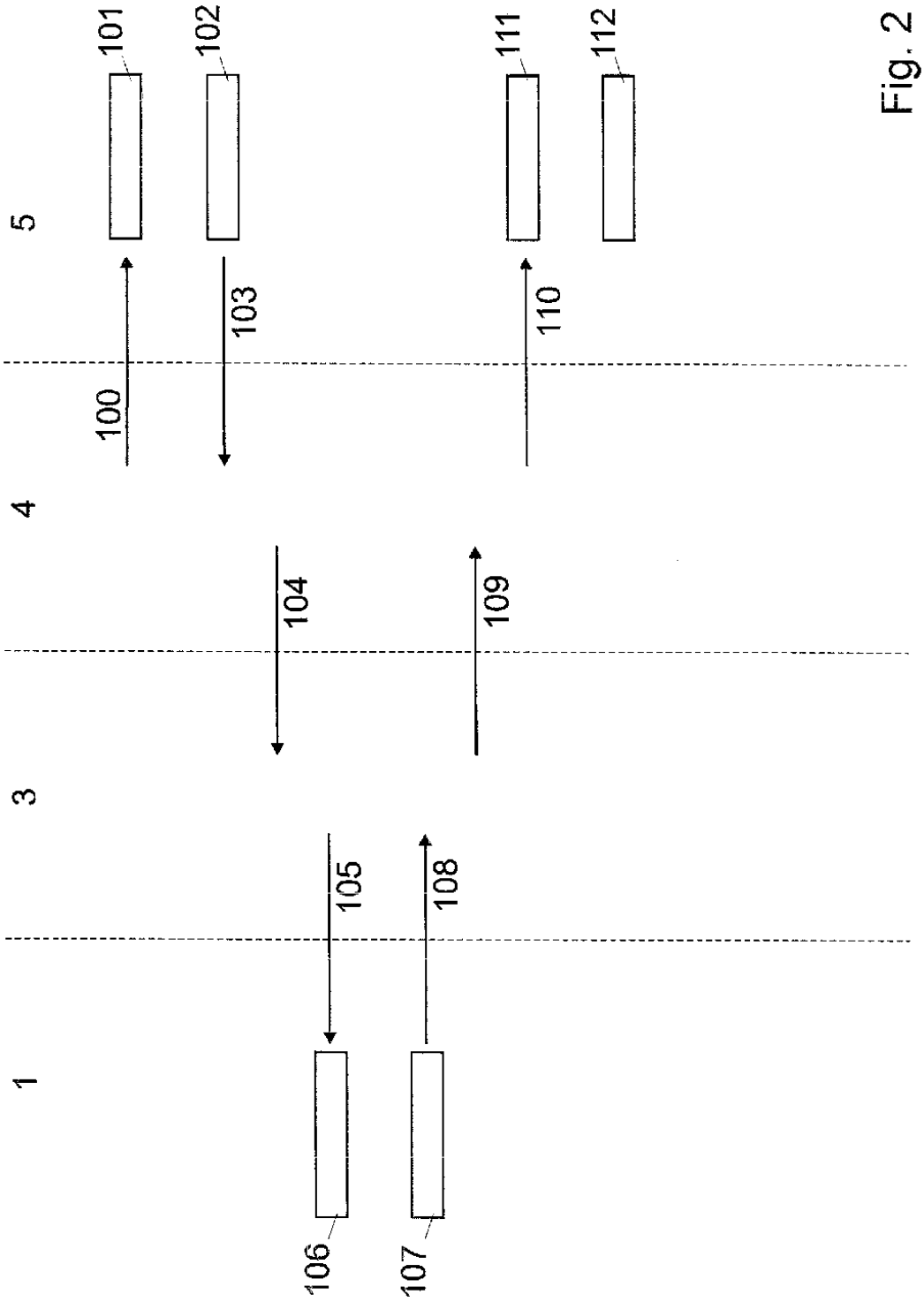

Fig. 2