(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 414 089**

(51) Int. CI.:

G08C 17/02 (2006.01)
G07C 9/00 (2006.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.11.2005 E 05819621 (3)**

(97) Fecha y número de publicación de la concesión europea: **24.04.2013 EP 1810093**

(54) Título: **Accionamiento de un sistema de seguridad utilizando un dispositivo inalámbrico**

(30) Prioridad:

10.11.2004 US 985348

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.07.2013

(73) Titular/es:

CORESTREET, LTD. (100.0%)
ONE ALEWIFE CENTER, SUITE 200
CAMBRIDGE, MA 02140, US

(72) Inventor/es:

LIBIN, PHIL

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

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

Accionamiento de un sistema de seguridad utilizando un dispositivo inalámbrico

Antecedentes de la invención

1. Campo Técnico

Esta solicitud está relacionada con el campo de los sistemas de seguridad y, más en particular, con el campo de accionamiento de los sistemas de seguridad, utilizando un dispositivo inalámbrico.

2. Descripción de la técnica relacionada

En muchos casos, una instalación o un grupo de instalaciones puede tener múltiples sistemas diversos de seguridad para el acceso físico, utilizado para proporcionar a los empleados y a otras personas un acceso físico selectivo a zonas restringidas. Cada uno de los sistemas puede utilizar sus propias tarjetas inteligentes exclusivas, placas de identificación, y códigos para proporcionar la entrada a la zona restringida. Los diferentes sistemas pueden haber sido instalados en diferentes momentos y/o comprados a diferentes vendedores. Además, una organización puede adquirir una instalación y heredar los sistemas de seguridad para el acceso físico que ya han sido instalados.

Haciendo referencia a la figura 1, un grupo 20 de sistemas de seguridad de acceso físico, 22, 22', 22'', representa cualquier número de sistemas situados en un solo edificio o en diferentes edificios, incluyendo distintos edificios en zonas geográficamente dispersas. Cada uno de los sistemas puede incluir una puerta 24, 24', 24'' (o similar) que proporciona selectivamente el acceso a una zona restringida. Cada una de las puertas puede ser bloqueada o desbloqueada mecánicamente por medio de un controlador 26, 26', 26'' que envía una señal para accionar un mecanismo de bloqueo para cada una de las puertas 24, 24', 24''.

El documento WO 01/41075 A1 divulga un sistema de control de acceso que permite a los proveedores de bienes o servicios acceder a un lugar, y un método para controlar el acceso a un lugar. El método comprende el almacenamiento de un primer código de acceso que es indicativo de un derecho de acceso predeterminado al lugar y el almacenamiento de un segundo código de acceso en un segundo dispositivo de almacenamiento de un dispositivo con clave electrónica. El método implica además utilizar un dispositivo con clave para solicitar acceso al lugar, transmitiendo el segundo código de acceso a la unidad de control de bloqueo, comparar el segundo código transmitido con el primer código, e iniciar el mecanismo de bloqueo, si el primer código de acceso se corresponde con el segundo código de acceso.

El documento GB 2 364 202 A divulga un dispositivo de acceso que comprende medios para recibir información de una clave y de la validez. El dispositivo de acceso está provisto de la información de claves y de información adicional disponible para el usuario del dispositivo.

Los controladores 26, 26', 26'' determinan si han de accionarse los mecanismos de bloqueo para las puertas 24, 24', 24'' basándose en los códigos de acceso recibidos desde cada una de la pluralidad de tarjetas inteligentes 28, 28', 28''. El término "tarjeta inteligente" puede ser entendido en este caso como que incluye tarjetas de identificación, dispositivos de llavero o cualquier otro mecanismo electrónico portátil convencional capaz de transmitir códigos de acceso a los controladores 26, 26', 26''. Cada uno de los controladores 26, 26', 26'' puede ser programado para aceptar (es decir, desbloquear las puertas 24, 24', 24'') ciertos códigos de acceso desde ciertas tarjetas (dispositivos), mientras que rechaza otros. De forma similar, cada una de las tarjetas inteligentes 28, 28', 28''puede ser programada para accionar ciertos controladores de los controladores 26, 26', 26'' y no los demás. Sin embargo, en algunos casos, si los sistemas 22, 22', 22'' son proporcionados por diferentes fabricantes/vendedores, puede no ser posible, por ejemplo, programar el controlador 26 para aceptar cualquiera de los códigos de las tarjetas 28', 28'' o programar las tarjetas 28', 28'' para accionar el controlador 26. Por tanto, un usuario que tenga permitido, por ejemplo, el acceso a una zona restringida por una puerta 24 y a otra zona restringida por la puerta 24', necesitaría llevar tanto la tarjeta 28 como la tarjeta 28'. Además de las potenciales dificultades logísticas asociadas con la emisión de múltiples tarjetas para los usuarios y programar múltiples sistemas, existen también problemas de seguridad que surgen con respecto a las dificultades asociadas con la necesidad de tener que hacer, por ejemplo, que un empleado cesado devuelva todas sus tarjetas y/o que reprogramar múltiples sistemas para no aceptar las tarjetas del empleado cesado.

Es deseable proporcionar un mecanismo para abordar las deficiencias descritas anteriormente.

Sumario de la invención

De acuerdo con la presente invención, el accionamiento de un sistema de seguridad incluye proporcionar un primer conjunto de códigos de acceso a un dispositivo inalámbrico, y hacer que el dispositivo inalámbrico transmita el primer conjunto de códigos de acceso a un primer controlador que accione el sistema de seguridad. El primer conjunto de códigos de acceso proporcionados al dispositivo inalámbrico puede expirar. El accionamiento de un sistema de seguridad puede incluir también la provisión de fechas de expiración para cada código del primer

conjunto de códigos de acceso proporcionados al dispositivo inalámbrico. El accionamiento de un sistema de seguridad puede incluir también examinar cada una de las fechas de expiración y, como respuesta a una fecha de expiración en particular que es anterior a la fecha actual, borrar del dispositivo inalámbrico un código particular del primer conjunto de códigos de acceso que se corresponde con la fecha particular de expiración. El accionamiento de un sistema de seguridad puede incluir también hacer que se borre un código particular del primer conjunto de códigos de acceso, modificando la correspondiente fecha de expiración del mismo. El accionamiento de un sistema de seguridad puede incluir también proporcionar al dispositivo inalámbrico un valor final que se corresponde con al menos un código del primer conjunto de códigos de acceso, donde el valor final es el resultado de aplicar una pluralidad de veces una función unidireccional de cifrado. El accionamiento de un sistema de seguridad puede incluir también proporcionar periódicamente un valor al dispositivo inalámbrico, aplicando la función unidireccional de cifrado al valor, para obtener un resultado de la misma, y borrar el al menos un código del primer conjunto de códigos de acceso correspondiente al valor final, como respuesta al resultado de que la aplicación de la función de cifrado unidireccional no es igual al valor final. El periodo puede ser un día. El accionamiento de un sistema de seguridad puede incluir también determinar si ha habido alguna manipulación con el dispositivo inalámbrico y, como respuesta a la manipulación, borrar todos los códigos del primer conjunto de códigos de acceso. El accionamiento de un sistema de seguridad puede incluir también determinar un subconjunto del primer conjunto de códigos de acceso que han de ser transmitidos por el dispositivo inalámbrico. Determinar el subconjunto puede incluir utilizar la información transmitida al dispositivo inalámbrico por el primer controlador. Determinar el subconjunto puede incluir utilizar información GPS. Determinar el subconjunto puede incluir alertar al usuario del dispositivo inalámbrico. El accionamiento de un sistema de seguridad puede incluir también realizar un proceso de errores como respuesta a que no hay códigos de acceso en el subconjunto. El accionamiento de un sistema de seguridad puede incluir también proporcionar una primera tabla que contenga los posibles usuarios, y proporcionar una segunda tabla que contenga los posibles códigos de acceso. El accionamiento de un sistema de seguridad puede incluir también recibir información de autorización para un usuario en particular y un subconjunto en particular del primer conjunto de códigos de acceso, y almacenar en el dispositivo inalámbrico el subconjunto particular del primer conjunto de códigos de acceso. La información de autorización puede ser autentificada. El accionamiento de un sistema de seguridad puede incluir también casos de entrada en el sistema del dispositivo inalámbrico que transmite el primer conjunto de códigos de acceso al primer controlador. Los casos pueden entrar en el sistema almacenando datos en el dispositivo inalámbrico y/o en el primer controlador. Los casos pueden ser transmitidos a un procesador central. El dispositivo inalámbrico puede ser un teléfono móvil. El accionamiento de un sistema de seguridad puede accionar una cerradura para permitir el acceso a una zona restringida. El accionamiento de un sistema de seguridad puede incluir proporcionar un segundo conjunto de códigos de acceso al dispositivo inalámbrico y hacer que el dispositivo inalámbrico transmita el segundo conjunto de códigos de acceso a un segundo controlador, donde el primer y el segundo controladores son incompatibles.

De acuerdo además con la presente invención, un producto de programa de ordenador proporcionado en un medio de almacenamiento, incluye código ejecutable que proporciona un primer conjunto de códigos de acceso a un dispositivo inalámbrico, y código ejecutable que hace que el dispositivo inalámbrico transmita el primer conjunto de códigos de acceso a un primer controlador que acciona un sistema de seguridad. El primer conjunto de códigos de acceso proporcionado al dispositivo inalámbrico puede expirar. El producto de programa de ordenador puede incluir también código ejecutable que proporciona fechas de expiración para cada código del primer conjunto de códigos de acceso proporcionado al dispositivo inalámbrico. El producto de programa de ordenador puede incluir también código ejecutable que examina cada una de las fechas de expiración y código ejecutable que borra del dispositivo inalámbrico un código particular del primer conjunto de códigos de acceso que se corresponde con la fecha de expiración particular, como respuesta a una fecha de expiración particular que es anterior a la fecha actual. El producto de programa de ordenador puede incluir también código ejecutable que hace que un código particular del primer conjunto de códigos de acceso sea borrado modificando una correspondiente fecha de expiración del mismo. El producto de programa de ordenador puede incluir también código ejecutable que proporcione al dispositivo inalámbrico un valor final que se corresponda con al menos un código del primer conjunto de códigos de acceso, donde el valor final es el resultado de aplicar una pluralidad de veces una función de cifrado unidireccional. El producto de programa de ordenador puede incluir también código ejecutable que proporcione periódicamente un valor al dispositivo inalámbrico, código ejecutable que aplique la función de cifrado unidireccional al valor, para obtener un resultado de la misma, y código ejecutable que borre el al menos un código del primer conjunto de códigos de acceso correspondiente al valor final, como respuesta al resultado de que la aplicación de la función de cifrado unidireccional no es igual al valor final. El periodo puede ser un día. El producto de programa de ordenador puede incluir también código ejecutable que determine si ha habido manipulación con el dispositivo inalámbrico y código ejecutable que borre todos los códigos del primer conjunto de códigos de acceso, como respuesta a la manipulación. El producto de programa de ordenador puede incluir código ejecutable que determine un subconjunto de una pluralidad de los códigos del primer conjunto de códigos de acceso que han de ser transmitidos por el dispositivo inalámbrico. El código ejecutable que determina el subconjunto puede utilizar información transmitida al dispositivo inalámbrico por el primer controlador. El código ejecutable que determina el subconjunto puede utilizar información GPS. El código ejecutable que determina el subconjunto puede alertar al usuario del dispositivo inalámbrico. El producto de programa de ordenador puede incluir también código ejecutable que realice el proceso de errores como respuesta a que no hay códigos de acceso en el subconjunto. El producto de programa de

ordenador puede incluir también una primera tabla que contenga posibles usuarios almacenados en memoria y una segunda tabla que contenga posibles códigos de acceso almacenados en memoria. El producto de programa de ordenador puede incluir también código ejecutable que reciba información de autorización para un usuario en particular y un subconjunto en particular del primer conjunto de códigos de acceso, y código ejecutable que almacene en el dispositivo inalámbrico el subconjunto en particular del primer conjunto de códigos de acceso. La información de autorización puede ser autenticada. El producto de programa de ordenador puede incluir también código ejecutable que registra los casos en que el dispositivo inalámbrico transmite los códigos de acceso al primer controlador. Los casos pueden ser registrados almacenando datos en el dispositivo inalámbrico. El producto de programa de ordenador puede incluir también código ejecutable que transmita los casos a un procesador central. Los casos pueden ser registrados almacenando los datos en el primer controlador. El producto de programa de ordenador puede incluir también código ejecutable que transmita los casos a un procesador central. El dispositivo inalámbrico puede ser un teléfono móvil. El código ejecutable que acciona el sistema de seguridad puede accionar una cerradura para permitir el acceso a una zona restringida. El producto de programa de ordenador puede incluir también código ejecutable que proporcione un segundo conjunto de códigos de acceso al dispositivo inalámbrico y código ejecutable que haga que el dispositivo inalámbrico transmita el segundo conjunto de códigos de acceso a un segundo controlador, donde el primer y segundo controladores son incompatibles.

De acuerdo además con la presente invención, un teléfono móvil que proporciona el acceso zonas restringidas incluye un medio de almacenamiento, un módulo de transmisión acoplado al medio de almacenamiento, código ejecutable almacenado en el medio de almacenamiento que acepta códigos proporcionados por el teléfono móvil, y código ejecutable que hace que los códigos de acceso sean proporcionados al módulo de transmisión para la transmisión por el teléfono móvil. El teléfono móvil puede incluir también código ejecutable que almacene el valor final en el medio de almacenamiento, donde el valor final se corresponde con al menos un código de acceso y donde el valor final es el resultado de aplicar una pluralidad de veces una función de cifrado unidireccional, código ejecutable que acepte periódicamente un valor, código ejecutable que aplique la función de cifrado unidireccional al valor para obtener un valor del mismo, y código ejecutable que borre los al menos un código de acceso correspondiente al valor final, como respuesta al resultado de que la aplicación de la función de cifrado unidireccional no es igual al valor final.

Breve descripción de los dibujos

La figura 1 ilustra una colección de la técnica anterior de los sistemas de seguridad para el acceso de personas.

La figura 2 ilustra una colección de sistemas de seguridad para el acceso de personas, que pueden ser accionados utilizando un teléfono móvil de acuerdo con el sistema descrito en esta memoria.

La figura 3 ilustra un mecanismo para programar un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 4 ilustra un mecanismo para proporcionar códigos de acceso a una estación de trabajo que es utilizada para programar un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 5 es un diagrama de flujo de datos que ilustra el software de un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 6 es un diagrama de flujo de datos que ilustra el software de un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 7 es un diagrama de flujo que ilustra los pasos realizados por un módulo de transferencia de un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 8 es un diagrama de flujo que ilustra los pasos realizados con respecto a un modo de realización para eliminar códigos de acceso de un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 9 es un diagrama de flujo que ilustra los pasos realizados con respecto a un modo de realización alternativo para eliminar los códigos de acceso de un teléfono móvil, de acuerdo con el sistema descrito en esta memoria.

La figura 10 es diagrama de flujo que ilustra los pasos realizados con respecto a la inicialización de un teléfono móvil con códigos de acceso y otros datos, de acuerdo con un modo de realización del sistema descrito en esta memoria.

La figura 11 es un diagrama que ilustra la generación de códigos de acceso para los teléfonos móviles, de acuerdo con el sistema descrito en esta memoria.

Descripción detallada de diversos modos de realización

Haciendo referencia a la figura 2, un sistema 30 de seguridad incluye las puertas 24, 24', 24'' y los controladores 26,

26', 26'', que se han descrito anteriormente con respecto a la figura 1. El sistema 30 incluye también un teléfono móvil 32 que puede transmitir códigos de acceso a uno o más de los controladores 26, 26', 26'' para hacer que una de las correspondientes puertas 24, 24', 24'' se abra y permita el acceso a una zona restringida. El teléfono móvil 32 transmite códigos de acceso de una manera idéntica o suficientemente similar a los códigos de acceso transmitidos por las tarjetas inteligentes 28, 28', 28''.

Como se ha descrito en otro lugar de esta memoria, el teléfono móvil 32 puede ser programado con códigos de acceso, de manera que cada uno de los controladores 26, 26', 26'' reciben los mismos o similares códigos de acceso desde el teléfono móvil 32 que serían recibidos desde una tarjeta apropiada de las tarjetas inteligentes 28, 28', 28'' para abrir una de las puertas apropiadas 24, 24', 24''. La programación del teléfono móvil 32 con los códigos de acceso se describe con más detalle en otro lugar de esta memoria. El teléfono móvil 32 puede ser programado desde una fuente externa que supervisa y emite códigos de acceso de acuerdo con reglas organizativas apropiadas. En algunos casos, los códigos de acceso pueden expirar o puede hacerse que expiren de una manera que reduzca la probabilidad de que un usuario no autorizado (por ejemplo, un empleado despedido recientemente) pudiera utilizar el teléfono móvil 32 para conseguir acceso no autorizado tras el periodo de expiración.

El sistema 30 proporciona muchas ventajas sobre el sistema 20 descrito anteriormente con respecto a la figura 1. Por ejemplo, un usuario no necesita llevar múltiples tarjetas inteligentes como las tarjetas inteligentes 28, 28', 28'', sino que, en su lugar, puede llevar simplemente un único teléfono móvil 32. Además, como la mayoría de la gente tiene en cualquier caso un teléfono móvil, la utilización del teléfono móvil 32 para proporcionar acceso a diferentes sistemas no genera una incomodidad adicional. En general, el teléfono móvil 32 integra el sistema 30 desde la perspectiva de un usuario del teléfono móvil 32, sin requerir una integración independiente y específica de cada parte potencialmente incompatible del sistema 30. Las partes del sistema pueden ser incompatibles por cualquiera o más de diversas razones, incluyendo estar hecho por fabricantes diferentes, siendo versiones diferentes o modelos diferentes del mismo fabricante, y/o estando instalado en diferentes momentos y/o por diferentes organizaciones o subconjuntos de la misma organización.

El usuario puede utilizar el teléfono móvil 32 como usaría una tarjeta inteligente y muestra su teléfono móvil 32 frente a las partes lectoras de los controladores 26, 26', 26'' para conseguir el acceso. En un modo de realización de esta memoria, el teléfono móvil 32 utiliza la tecnología/chip de Comunicaciones de Campo Cercano (NFC) de Philips para facilitar la transmisión de códigos de acceso a los controladores 26, 26', 26''. La tecnología NFC de Philips está disponible en Philips Corporation y la implementación de la misma en el sistema aquí descrito es directa para una persona de experiencia normal en la técnica, utilizando la información proporcionada por Philips. Sin embargo, obsérvese que puede utilizarse otro hardware y/o software en lugar de la tecnología NFC de Philips, donde la otra tecnología proporcione la misma o similar funcionalidad que la tecnología NFC de Philips para ser capaz de emular uno o más tipos de dispositivos sin contactos.

Haciendo referencia a la figura 3, un diagrama 40 ilustra la programación del teléfono móvil 32, de acuerdo con el sistema descrito en esta memoria. Muchos operadores y fabricantes de teléfonos móviles proporcionan un mecanismo para programar teléfonos móviles y/o proporcionar datos a ellos utilizando Internet, la red telefónica de móviles y/o mecanismos construidos en los teléfonos móviles comercialmente disponibles. En un modo de realización de esta memoria, el usuario utiliza una estación de trabajo informática convencional 42 o equivalente, para iniciar la transferencia de datos y/o la información de programación al teléfono móvil 32, para implementar el sistema descrito en esta memoria. La estación de trabajo 42 está acoplada a una red 44, tal como Internet, que está acoplada también a circuitos 46 de transmisión e interfaz de un teléfono móvil proporcionados por un operador de móviles. Los mecanismos de transferencia integrados y proporcionados por los operadores y los fabricantes de teléfonos móviles permiten transmitir y almacenar datos/programas proporcionados a través de Internet en el teléfono móvil 32.

Los circuitos 46 de transmisión de móviles están acoplados a la torre (antena) 48 de transmisión de móviles que transmite los datos/programas apropiados al teléfono móvil 32. Naturalmente, una red convencional de teléfonos móviles incluye muchas torres de teléfonos móviles y la torre en particular que transmite al teléfono móvil 32 puede incluir, por ejemplo, la torre más cercana al teléfono móvil 32 en el momento de la transferencia.

Haciendo referencia a la figura 4, la estación de trabajo 42 del usuario se ilustra con más detalle estando unida a un lector 52 de tarjetas y a un lector 54 de discos. El lector 52 de tarjetas puede ser utilizado para obtener información de códigos de acceso desde la tarjeta inteligente 28 (u otras tarjetas inteligentes u otros dispositivos de acceso similares). Por tanto, en un modo de realización de esta memoria, la información de códigos de acceso es proporcionada directamente por la tarjeta inteligente 28 al lector 52 de tarjetas, donde el lector 52 de tarjetas proporciona después los datos a la estación de trabajo 42. Después, como se ha descrito en otro lugar de esta memoria, la estación de trabajo 42 proporciona los códigos de acceso (y posiblemente otros datos/programas) al teléfono móvil 32, a través de la red 44.

En otros casos, la información para la programación del teléfono móvil 32 puede ser proporcionada por un disco 56 que puede ser suministrado por un fabricante de un sistema de seguridad para el acceso físico o por alguna otra fuente. El disco 56 se introduce en el lector 54 de discos que proporciona entonces los datos a la estación de trabajo

42 para la programación subsiguiente del teléfono móvil 32 a través de la red 44. Incluso en otros modos de realización, un usuario puede introducir datos directamente en la estación de trabajo 42 utilizando, por ejemplo, el teclado de la estación de trabajo 42, para teclear los códigos de acceso (y/u otra información apropiada) que se suministra subsiguientemente al teléfono móvil 32.

La administración de reglas de seguridad y procedimientos para la estación de trabajo 42 puede ser proporcionada por cualquier mecanismo apropiado, incluyendo cualquiera y todos los mecanismos divulgados en la solicitud de patente de Estados Unidos con el núm. 10/893.126 (solicitud '126) presentada el 16 de Julio de 2004.

Por tanto, por ejemplo, ciertos códigos de acceso pueden no estar disponibles para transferirse al teléfono móvil 32, a menos que el usuario de la estación de trabajo haya emitido las credenciales apropiadas. Obsérvese que la autorización/credenciales para la estación de trabajo pueden ser introducidas a través del teclado, transferidas a la estación de trabajo 42 a través de la red 44, y/o proporcionadas a la estación de trabajo 42 por cualquier medio apropiado.

Haciendo referencia a la figura 5, un diagrama 60 ilustra módulos (software y/o hardware) que pueden ser proporcionados internamente al teléfono móvil 32 para facilitar el uso y la promulgación de códigos de acceso con ellos. Los módulos del teléfono móvil 32 (y otros módulos del teléfono móvil 32 descritos en esta memoria) pueden ser instalados por el fabricante del teléfono móvil 32, instalados por el usuario, descargados (en el caso de software) al teléfono móvil 32 de una manera similar al mecanismo descrito anteriormente con respecto al diagrama 40 de la figura 3, o alguna combinación de los mismos. Los módulos incluyen un elemento 62 de datos de códigos de acceso que contiene los códigos de acceso proporcionados al teléfono móvil 32. El elemento 62 de datos de códigos de acceso está acoplado a un módulo 64 de transmisión que es parte del teléfono móvil e incluye una combinación apropiada de hardware y software para facilitar la transmisión por el teléfono móvil 32 de códigos de acceso desde el elemento 62 de datos de códigos de acceso. El módulo 64 de transmisión puede estar acoplado a la antena del teléfono móvil 32.

En algunos modos de realización, el módulo 64 de transmisión puede recibir datos GPS que indican el lugar geográfico del teléfono móvil 32. Los datos GPS pueden ser recibidos y procesados por un mecanismo interno integrado en el teléfono móvil 32. Como se ha descrito con mayor detalle en otro lugar de esta memoria, en modos de realización en los que el módulo 64 de transmisión recibe datos GPS, el módulo 64 de transmisión puede utilizar los datos GPS para seleccionar los códigos de acceso apropiados desde el elemento 62 de datos de códigos de acceso. Por ejemplo, si el elemento 64 de datos de códigos de acceso contiene códigos para sistemas de seguridad de acceso físico en Boston, Nueva York y Washington, D.C., y si los datos GPS indican que el teléfono móvil 32 está situado en Boston, el módulo 64 de transmisión reduciría el número de posibles códigos de acceso utilizando solamente los códigos de acceso desde el elemento 64 de datos de códigos de acceso que se corresponde a los sistemas de Boston.

En algunos casos, un esquema existente de códigos de acceso puede incluir expiraciones ya integradas de los códigos de acceso. Por ejemplo, para algunos sistemas, los códigos de acceso pueden expirar automáticamente tras una cierta cantidad de tiempo (por ejemplo, un día). Por tanto, siempre que el usuario que tenga posesión del teléfono móvil 32 esté autorizado para un tipo particular de acceso, pueden enviarse periódicamente nuevos códigos de acceso al teléfono móvil 32, según sea apropiado. Cuando el usuario ya no requiera o ya no tenga permitido acceder a una zona en particular, ya no se enviarán nuevos códigos de acceso a esa zona para el teléfono móvil 32. Por tanto, los sistemas con expiraciones integradas para los códigos de acceso permiten la administración de los códigos de acceso decidiendo simplemente si se deben proporcionar o no nuevos códigos de acceso al teléfono móvil 32, tras cada periodo de expiración de los códigos de acceso antiguos. Sin embargo, para algunos sistemas, los códigos de acceso pueden no expirar o, alternativamente, la cantidad de tiempo que se tarda en que expiren los códigos de acceso puede ser más larga que lo deseado. En tales sistemas, puede ser útil proporcionar un mecanismo que haga que se borren los códigos de acceso del teléfono móvil 32.

Haciendo referencia a la figura 6, un diagrama 60' ilustra una versión diferente del software para el teléfono móvil 32. El software incluye el elemento 62 de datos de códigos de acceso y el módulo 64 de transmisión, como se ha descrito anteriormente, con respecto al diagrama 60 de la figura 5. Sin embargo, el diagrama 60' muestra también un elemento 66 de datos de expiración y un módulo 68 de borrado. Para alguno o todos los códigos de acceso del elemento 62 de datos de códigos de acceso, los datos 66 de expiración pueden tener una correspondiente fecha de expiración. El módulo 68 de borrado utiliza los datos de expiración del elemento 66 de datos de expiración para borrar selectivamente los códigos de acceso del elemento 62 de datos de códigos de acceso, de manera que el teléfono móvil 32 ya no pueda ser utilizado para proporcionar el acceso específico concedido por los códigos de acceso borrados. Esto se describe con más detalle en otro lugar de esta memoria.

Haciendo referencia a la figura 7, un diagrama 70 de flujo ilustra los pasos realizados por el software del módulo 64 de transmisión para determinar cuáles de los códigos de acceso del elemento 62 de datos de códigos de acceso deben ser transmitidos. Obsérvese que, para algunos modos de realización, puede ser posible, en cada caso, transmitir simplemente a un lector todos los códigos de acceso del elemento 62 de datos de códigos de acceso. Sin embargo, puede haber inconvenientes con este enfoque, incluyendo posibles compromisos de seguridad y la

posibilidad de que un lector de códigos de acceso pueda dejar de funcionar y deniegue todos los accesos que se intenten (legítimos o no) si el lector recibe demasiados códigos de acceso no válidos. Por tanto, en algunos casos, es deseable hacer que el módulo 64 de transmisión seleccione para la transmisión ciertos códigos de acceso del elemento 62 de datos de códigos de acceso.

El proceso del diagrama 70 de flujo comienza en el paso 72 de comprobación, donde se determina si el lector (es decir, el lector de tarjetas asociado con el controlador 26) ha proporcionado información de localización al teléfono móvil 32. Para algunos modos de realización, es posible hacer que el teléfono móvil 32 reciba información (a través de la antena) desde el lector, para permitir que el teléfono móvil 32 seleccione un subconjunto apropiado de códigos de acceso desde el elemento 62 de datos de códigos de acceso. Si se determina en el paso 72 de comprobación que la información del lector está disponible, se transfiere el control desde el paso 72 al paso 74, donde el número de posibles códigos de acceso se reduce basándose en la información del lector. Es decir, si el lector indica que este lector está en una ciudad en particular, los códigos de acceso para otras ciudades no deben utilizarse, y por tanto se eliminan como posibles códigos de acceso a transmitir (pero no necesariamente borrados del elemento 62 de datos de códigos de acceso).

Si se determina en el paso 72 que no hay disponible información del lector, el control se transfiere desde el paso 72 al paso 76, donde se determina si hay disponible información GPS. Como se ha descrito anteriormente, en algunos casos, es posible proporcionar información GPS al módulo 62 de transferencia utilizando, por ejemplo, la información GPS recibida por el teléfono móvil 32 y procesada en él. Si se determina en el paso 76 que la información GPS está disponible, el control se transfiere desde el paso 76 al paso 77, donde, como en el paso 74 descrito anteriormente, el número de posibles códigos de acceso se reduce.

Después del paso 77, o después del paso 76 si la información GPS no está disponible, hay un paso 78 de prueba donde se determina si hay más de un posible código de acceso que pueda ser proporcionado. Obsérvese que con o sin la información GPS y/o la información del lector, puede seguir habiendo más de un posible código de acceso que pueda ser transmitido por el teléfono móvil 32 (por ejemplo, dos puertas en estrecha proximidad mutua con diferentes códigos de acceso). Obsérvese también que es posible que el teléfono móvil 32 esté programado solamente con un código de acceso, de manera que, independientemente de la disponibilidad de la información GPS y/o la información del lector, solamente habrá un código de acceso en el paso 78. En algunos casos, el teléfono móvil 32 puede ser programado solamente con respecto a un usuario que viaja a un lugar remoto específico y por tanto solamente con los códigos de acceso para ese lugar, en cuyo caso los códigos de acceso pueden ser borrados del teléfono móvil 32 después de que el usuario vuelva desde el lugar remoto. El borrado de los códigos de acceso se describe con más detalle en otro lugar de este memoria.

Si en el paso 78 se determina que hay más de un posible código de acceso, el control se transfiere desde el paso 78 al paso 82, donde se alerta al usuario para que seleccione entre más de un posible código de acceso. La alerta en el paso 82 utiliza la capacidad integrada en el teléfono móvil 32 para presentar una lista de posibles códigos de acceso (o una lista de posibles lugares correspondientes a los códigos de acceso) a partir de la cual el usuario puede seleccionar uno. El teléfono móvil 32 puede utilizar, por ejemplo, el lenguaje (texto) de programación Java y una máquina virtual de Java, o utilizar cualquier otra técnica apropiada para alertar al usuario y recibir respuesta de ello.

Después del paso 82, o después del paso 78 si no hay más de un posible código de acceso, hay un paso 84 de prueba en el que se determina si hay un código de acceso disponible para el uso. Obsérvese que el resultado de filtrar en los pasos 74, 77, 82 puede originar que no haya códigos de acceso utilizables. Obsérvese también que, en algunos modos de realización, puede ser posible que el usuario seleccione “ninguno” (o equivalente) para la alerta proporcionada en el paso 82. También es posible que el teléfono móvil 32 no haya sido programado con ningún código de acceso o al menos no haya sido programado con códigos de acceso consistentes con la información GPS y/o la información del lector.

Si en el paso 84 de comprobación se determina que hay un código de acceso disponible, el control se transfiere desde el paso 84 al paso 86, donde se transmite el código de acceso, por ejemplo, haciendo que el módulo 64 de transmisión proporcione las señales apropiadas a la antena del teléfono móvil 32.

Después del paso 86 está el paso 87, donde se registra el uso del teléfono móvil para el acceso físico. Es posible registrar usos del teléfono móvil 32 para registrar cada uso en el teléfono móvil 32 (es decir, registro de usos dentro del teléfono móvil), registrar cada uso en el lector correspondiente (es decir, registrar usos dentro del lector) o ambas cosas. El registro de usos en el teléfono móvil 32 puede ser facilitado por le lector proporcionando información de identificación al teléfono móvil 32. El registro de usos puede incluir usar cualquiera de los mecanismos de registro descritos en la solicitud de patente de Estados Unidos núm. 10/893.174 presentada el 16 de Julio de 2004. En algunos modos de realización, algunas o todas las entradas del registro en los lectores y/o en el teléfono móvil 32 pueden ser transmitidas a un procesador central, tal como la estación de trabajo 42, para determinar si ha habido algún intento de acceso no autorizado y/o accesos con éxito.

Si en el paso 84 se determina que no hay un código de acceso a transmitir por el teléfono móvil 32, el control se transfiere desde el paso 84 al paso 88, donde se efectúa el proceso de errores. El proceso de errores efectuado en

el paso 88 puede incluir, por ejemplo, proporcionar un mensaje al usuario a través del teléfono móvil 32. El proceso de errores realizado en el paso 88 puede incluir también el registro de intentos de entrada.

En algunos modos de realización, la disponibilidad de la información del lector puede anular la necesidad de información GPS alguna porque, en algunos casos, puede haber un nivel de detalle más utilizable de la información del lector que la que puede proporcionar la información GPS. En tales casos, cuando hay disponible información del lector, puede omitirse la comprobación en el paso 76 de disponibilidad de información GPS. Esto se ilustra con un camino alternativo 89 del flujo desde el paso 74 al paso 78.

Haciendo referencia a la figura 8, el diagrama 90 de flujo ilustra los pasos realizados por el módulo 68 de borrado de la figura 6. El proceso comienza en el primer paso 92, el cual determina si ha habido alguna manipulación con el teléfono móvil 32. En un modo de realización de esta memoria, el teléfono móvil 32 puede estar equipado con medios para detectar la manipulación con él, de manera que un usuario no pueda utilizar el teléfono móvil 32 para conseguir acceso no autorizado. El mecanismo de detección de manipulación del teléfono móvil 32 puede ser cualquier mecanismo apropiado que incluya cualquiera de una pluralidad de mecanismos convencionales de detección de manipulación que pueden ser utilizados con dispositivos electrónicos, como el teléfono móvil 32.

Si en el paso 92 de comprobación se determina que ha habido manipulación con el teléfono móvil 32, el control se transfiere desde el paso 92 de comprobación al paso 94, donde se borran todos los códigos de acceso del teléfono móvil 32, reduciendo así la posibilidad de que el teléfono móvil 32 pueda ser utilizado para el acceso no autorizado. Después del paso 94 está el paso 96, el cual realiza el proceso de errores. El proceso de errores realizado en el paso 96 puede incluir alertar al usuario o a otros, de que se ha detectado una manipulación e inhabilitar las demás posibilidades (por ejemplo, llamada de voz) del teléfono móvil 32. Después del paso 96, el proceso se ha completado. En un modo de realización de esta memoria, una vez que se ha manipulado con el teléfono móvil 32, ya no puede ser utilizado para el acceso, a menos y hasta que se haya detectado la fuente de manipulación y/o el teléfono móvil 32 haya hecho la reposición de una manera segura.

Si en el paso 92 de comprobación se determina que no ha habido manipulación con el teléfono móvil 32, el control se transfiere desde el paso 92 de comprobación al paso 98, donde un índice variable, I, se fija igual a 1. El índice variable I puede ser utilizado para efectuar una iteración a través de los diversos códigos de acceso almacenados en el elemento 62 de datos de códigos de acceso.

Después del paso 98 está el paso 102 de comprobación, el cual determina si el índice variable, I, es mayor que el número de códigos de acceso (es decir, si todos los códigos de acceso han sido examinados). Si es así, el control se transfiere desde el paso 102 de comprobación volviendo al paso 92, para iniciar otra iteración de la comprobación de la expiración de los códigos de acceso. En otro caso, el control se transfiere desde el paso 102 de comprobación hasta el paso 104 de comprobación, el cual determina si el código de acceso de orden I ha expirado. La comprobación en el paso 104 pude ser bastante directa y puede incluir, por ejemplo, la comparación de los datos actuales con los datos de expiración almacenados en el elemento 66 de datos de expiración.

Si en el paso 104 de comprobación se determina que el código de acceso de orden I ha expirado, el control se transfiere desde el paso 104 de comprobación al paso 106, donde se borra el código de acceso de orden I del elemento 62 de datos de códigos de acceso del teléfono móvil 32. Al borrar el código de acceso de orden I del elemento 62 de datos de códigos de acceso del teléfono móvil 32, supone que el teléfono móvil 32 ya no puede ser utilizado para el acceso a una zona que fue accedida previamente utilizando el código de acceso de orden I. Después del paso 106, o después del paso 104 de comprobación si el código de acceso de orden I no ha expirado, hay un paso 108 en el que se incrementa el índice variable I. Después del paso 108, el control se devuelve al paso 102 de comprobación, descrito anteriormente.

Las fechas de expiración asociadas con los códigos de acceso pueden ser proporcionadas con los códigos de acceso (es decir, proporcionadas al teléfono móvil 32 cuando se proporcionan los códigos de acceso) o pueden ser proporcionadas independientemente en momentos diferentes. Obsérvese también que, en algunos casos, puede ser posible hacer que se borren los códigos de acceso modificando la fecha de expiración y utilizando el software que compara la fecha de expiración con la fecha en curso.

En algunos casos, puede ser deseable proporcionar un mecanismo más seguro para ampliar o borrar códigos de acceso en el teléfono móvil 32. Una técnica para reforzar la seguridad puede incluir un mecanismo similar al divulgado en la patente de Estados Unidos 5.666.416. En tal caso, cuando se proporcionan nuevos códigos de acceso al teléfono móvil 32, se proporciona también un valor final (FV). Por tanto, para cada nuevo periodo (por ejemplo, un día) en que los códigos de acceso siguen siendo válidos, se proporciona un nuevo valor que puede ser utilizado con el FV para confirmar que los códigos de acceso siguen siendo válidos.

Haciendo referencia a la figura 9, un diagrama 120 de flujo ilustra un modo de realización alternativo del proceso que puede ser realizado en el teléfono móvil 32 para determinar cuándo borrar un código de acceso. El proceso ilustrado por el diagrama 120 de flujo utiliza el mecanismo divulgado en la patente de Estados Unidos 5.666.416, para hacer que se transmita un nuevo valor al teléfono móvil 32 periódicamente, para mantener la viabilidad de los códigos de

acceso. Es decir, si en cada nuevo periodo el teléfono móvil 32 recibe un valor apropiado, no se borrarán los correspondientes códigos de acceso. En otro caso, si no se recibe el valor apropiado en el teléfono móvil 32, se borrarán los correspondientes códigos de acceso.

El proceso comienza en el primer paso 122 que determina si se ha manipulado con el teléfono móvil 32, como se ha descrito anteriormente con respecto al paso 92 del diagrama 90 de flujo de la figura 8. Si es así, el control se transfiere desde el paso 122 de comprobación al paso 124, donde se borran todos los códigos de acceso del elemento 62 de datos de códigos de acceso. Después del paso 124 está el paso 126, donde se manifiesta un error, como se ha descrito anteriormente con respecto al paso 94 del diagrama 90 de flujo de la figura 8. Después del paso 126, el proceso se ha completado.

Si en el paso 122 de comprobación se determina que no se ha manipulado con el teléfono móvil 32, el control se transfiere desde el paso 122 al paso 128, donde un índice variable, I, se fija igual a uno. El índice variable I puede ser utilizado para efectuar una iteración a través de los códigos de acceso del elemento 62 de datos de códigos de acceso. Después del paso 128 hay un paso 132 de comprobación, el cual determina si el índice variable I es mayor que el número de códigos de acceso. Si es así, el proceso está completo. En otro caso, se transfiere el control desde el paso 132 de comprobación al paso 134, donde el valor más reciente que se ha proporcionado al código de acceso se cifra N veces, donde N es igual al número de periodos. Por tanto, si por ejemplo cada periodo es de un día, y han pasado doce días desde que se suministró inicialmente un código de acceso particular, el valor más reciente se cifra N veces. La función de cifrado puede ser una función de cifrado unidireccional, como se describe en la patente de Estados Unidos núm. 5.666.416. Después del paso 134 hay un paso 136 de comprobación, el cual determina si el resultado de cifrar el valor entrante N veces es igual al valor final, FV, asociado con los códigos de acceso. La comprobación en el paso 136 corresponde al mecanismo divulgado en la patente de Estados Unidos 5.666.416. Si en el paso 136 de comprobación se determina que los valores no son iguales (es decir, el cifrado N-simo del valor más reciente no es igual a FV), el control se transfiere desde el paso 136 de comprobación al paso 138, donde el código de acceso (o conjunto de códigos de acceso) de orden I se borra del elemento 62 de datos de códigos de acceso. Después del paso 138 o después del paso 136 de comprobación si los valores son iguales, hay un paso 142 en el que se incrementa el índice variable, I. Después del paso 142, el control se devuelve al paso 132 descrito anteriormente.

Haciendo referencia a la figura 10, un diagrama 150 de flujo ilustra los pasos realizados con respecto a la recepción de nuevos códigos de acceso que se mantienen en conexión con el proceso realizado por el diagrama 120 de flujo de la figura 9. El proceso comienza en un primer paso 152 en el que se reciben nuevos códigos de acceso y datos adicionales (por ejemplo, el FV). Después del paso 152 hay un paso 154 de comprobación, donde se determina si los códigos de acceso y los datos adicionales han sido firmados por un miembro de confianza. El esquema de la firma utilizado, así como el mecanismo y la política utilizada para determinar quién y quién no es un grupo de confianza, puede ser fijado de acuerdo con las políticas y procedimientos apropiados de una organización. Si se determina en el paso 154 de comprobación que los nuevos códigos de acceso y los datos adicionales no han sido firmados por un grupo de confianza, el control se transfiere desde el paso 154 de comprobación al paso 156, donde se efectúa el proceso de errores. El proceso de errores efectuado en el paso 156 puede incluir, por ejemplo, notificar al usuario que se han recibido nuevos códigos de acceso pero que los códigos de acceso no estaban firmados por un grupo de confianza. Después del paso 156, el proceso se ha completado.

Si en el paso 154 de comprobación se determina que los nuevos códigos de acceso y los datos adicionales proporcionados al teléfono móvil 32 han sido firmados por un grupo de confianza, el control se transfiere desde el paso 154 de comprobación al paso 158, donde los códigos de acceso se almacenan en el teléfono móvil 32, por ejemplo en el elemento 62 de datos de códigos de acceso. Después del paso 158 hay un paso 162 de comprobación, donde el FV utilizado para determinar periódicamente si el acceso sigue siendo autorizado, se almacena también, por ejemplo en el elemento 66 de datos de expiración. Después del paso 162, el proceso está completo.

En algunos casos, es posible no requerir que los nuevos códigos de acceso y los datos adicionales sean firmados por un grupo de confianza. Esto está indicado en el diagrama 150 de flujo por medio de un camino alternativo 164 que muestra la transferencia de control desde el paso 152 al paso 158.

En algunos casos, puede ser posible crear uno o más usuario de propósito especial (por ejemplo, visitantes y/o meta-usuarios) en cada uno de los sistemas de seguridad de acceso físico, donde el usuario de propósito especial puede ser utilizado exclusivamente para el acceso por el teléfono móvil 32. En un modo de realización de esta memoria, se puede crear un usuario de propósito especial para cada posible sistema accedido por el teléfono móvil 32. En otros modos de realización, puede haber más de un usuario de propósito especial para cada sistema de seguridad de acceso físico. Por ejemplo, puede haber muchos usuarios de propósito especial para uno o más sistemas de seguridad de acceso físico, como usuarios potenciales hay del teléfono móvil 32 (o teléfonos móviles similares). También es posible que uno o más sistemas de seguridad de acceso físico incluyan más de una puerta (y por tanto más de un lector, etc.). En tal caso, sería posible tener un usuario de propósito especial independiente para cada puerta posible (o subconjunto de puertas). Tal sistema podría reforzar la seguridad siendo más selectivo con

respecto al acceso, con un correspondiente aumento en la sobrecarga asociada con la administración de códigos de acceso adicionales. En este modo de realización, puede ser útil hacer que el lector (o lectores) proporcionen información de identificación al teléfono móvil 32.

Los usuarios de propósito especial pueden ser cambiados periódicamente para reforzar la seguridad. Por ejemplo, si cada mes se cancelan los antiguos usuarios de propósito especial y se añaden nuevos usuarios de propósito especial, el usuario finalizado/desautorizado que retenga impropiamente los códigos de acceso para un usuario de propósito especial, no podrá utilizar esos códigos después de un mes. La frecuencia en que se deben cambiar los códigos de los usuarios de propósito especial es cuestión de la política que pude derivarse de diversos factores, incluyendo la sensibilidad de una zona protegida por un sistema de seguridad de acceso físico, la dificultad de cambiar códigos de acceso (y promulgar con seguridad los nuevos códigos de acceso), y la tasa esperada de rotación/cancelación de usuarios del teléfono móvil 32 (u otros teléfonos móviles similares). En algunos casos, la creación y eliminación de usuarios de propósito especial puede ser automatizada, de manera que, por ejemplo, los antiguos usuarios de propósito especial sean cancelados y se creen nuevos usuarios de propósito especial en periodos fijos de tiempo, o tras eventos significativos (por ejemplo, después de haber programado N veces el teléfono móvil 32). El cambio automático o manual de usuarios puede ser efectuado con módulos de software adicionales o pre-existentes. Los módulos de software pueden ser utilizados también en casos en los que haya habido un compromiso de seguridad, de manera que, por ejemplo, si se pierde un teléfono móvil que contenga códigos de acceso para un usuario en particular, ese usuario en particular puede ser eliminado (acceso denegado) de cualquier sistema de seguridad de acceso físico.

Haciendo referencia a la figura 11, un diagrama 200 ilustra con más detalle el software que reside en la estación de trabajo 42 para programar el teléfono móvil 32. Una primera tabla 202 tiene una pluralidad de entradas, cada una de las cuales corresponde a un posible usuario del teléfono móvil 32 (o teléfonos móviles similares). Cada entrada incluye información de identificación para el usuario, así como información necesaria para programar el teléfono móvil del usuario. También puede incluirse información de seguridad apropiada.

El diagrama 200 incluye también una segunda tabla 204 de usuarios de propósito especial que puede ser utilizada para acceder a los sistemas de seguridad de acceso físico. Cada una de las entradas incluye información de identificación, así como los correspondientes códigos de acceso. También puede incluirse la información de seguridad apropiada.

Hay un módulo 206 de generación acoplado y recibiendo información tanto desde ambas tablas 202, 204. El módulo 206 de generación recibe también datos de información de autorización que indican al módulo de generación cuál de los usuarios de la primera tabla 202 ha de tener su teléfono móvil programado con qué códigos de acceso de la segunda tabla 204. En algunos modos de realización, la información de autorización puede ser proporcionada solamente por uno o más usuarios autorizados. Los usuarios autorizados pueden firmar digitalmente la información de autorización y/o en otro caso proporcionar una indicación de que la información de autorización es auténtica (es decir, la información está autenticada). En algunos modos de realización, la información de autorización puede incluir datos de seguridad que se combinan con los datos de seguridad almacenados con las entradas de la primera y/o segunda tablas 202, 204 para permitir la activación del teléfono móvil 32 para acceder a los sistemas de seguridad de acceso físico. El módulo 206 de generación tiene un interfaz con la red 44 para proporcionar la información/códigos de acceso de programación apropiados al teléfono móvil 32, como se ha descrito en otro lugar de esta memoria.

Una ventaja del sistema descrito en esta memoria es que, siempre que el teléfono móvil 32 esté accediendo a la red telefónica móvil (es decir, para hacer llamadas de voz), el teléfono móvil 32 puede recibir información sobre los códigos de acceso. Aunque la manipulación con el teléfono móvil 32 puede ser tentadora para un usuario no autorizado, en algunos modos de realización puede utilizarse el hardware a prueba de manipulación para detectar y/o disuadir la manipulación. Obsérvese que algunos o todos los sistemas 22, 22', 22'' pueden ser sistemas que implementan una tecnología como la descrita en la solicitud '126. Naturalmente, algunos o todos los sistemas 22, 22', 22'' pueden implementar alguna otra tecnología no relacionada.

Obsérvese que el mecanismo descrito con respecto al diagrama 120 de flujo puede proporcionar una manera cómoda de eliminar códigos de acceso del teléfono móvil 32, simplemente no proporcionando el siguiente valor periódico necesario para mantener los códigos de acceso. Obsérvese también que el valor necesario para mantener los códigos de acceso en cada periodo no necesita ser transmitido de una manera segura incluso cuando es difícil, si no imposible, que alguien determine independientemente un valor periódico futuro. El sistema descrito en esta memoria puede utilizar también mecanismos descritos en la solicitud '126 (incorporada como referencia anteriormente) para hacer que el teléfono móvil 32 origine activamente códigos de acceso que han de borrarse en ciertas circunstancias. Cualquier otro mecanismo puede ser adaptado también por una persona de experiencia normal en la técnica, de una manera directa para ser utilizada con el sistema descrito en esta memoria, incluyendo, sin limitación los mecanismos descritos en las patentes de Estados Unidos, 5.420.927; 5.604.804; 5.610.982; 6.097.811; 6.301.659; 5.793.868; 5.717.758; 5.717.757; 6.487.658; y 5.717.759.

Aunque el sistema descrito en esta memoria está ilustrado utilizando el teléfono móvil 32, es posible utilizar cualquier

otro dispositivo inalámbrico capaz de recibir códigos de acceso por una red de alcance relativamente largo, y transmitir esos códigos de acceso (quizás de una forma diferente) a un lector de tarjetas sin contactos (o dispositivo similar) con un alcance de transmisión relativamente corto. Tales otros dispositivos inalámbricos pueden incluir un PDA, una combinación de PDA/teléfono móvil, un Blackberry, y otros dispositivos como esos. Obsérvese también que el mecanismo de seguridad ilustrado en esta memoria puede ser utilizado para fines que van más allá del acceso físico y que pueden ser ampliados a sistemas de tiempos de asistencia (por ejemplo, tarjetas electrónicas perforadas), estaciones de observación utilizadas por vigilantes de seguridad para confirmar la revisión de una zona en particular en un momento en particular, y/o a cualquier situación en la que los códigos de acceso puedan ser utilizados para accionar un mecanismo con seguridad.

Aunque la invención ha sido divulgada con respecto a diversos modos de realización, para los expertos en la técnica serán fácilmente evidentes modificaciones a los mismos. Consecuentemente, el alcance de la invención se establece en las reivindicaciones siguientes.

REIVINDICACIONES

1. Un método para accionar un sistema de seguridad, que comprende:

proporcionar un primer conjunto de códigos de acceso a un dispositivo inalámbrico (32);

hacer que el dispositivo inalámbrico (32) transmita al menos alguno del primer conjunto de códigos de acceso al primer controlador (26, 26', 26'') que acciona el sistema de seguridad; y

recibir información adicional en el dispositivo inalámbrico (32), caracterizado por que la información adicional permite la selección de códigos apropiados del primer conjunto de códigos de acceso para que el dispositivo inalámbrico (32) transmita al primer controlador, de acuerdo con un atributo del dispositivo inalámbrico.

2. Un método, de acuerdo con la reivindicación 1, en el que la información adicional es información de localización, y donde el atributo es un lugar geográfico del dispositivo inalámbrico (32).

3. Un método de acuerdo con la reivindicación 1, en el que el primer conjunto de códigos de acceso proporcionado al dispositivo inalámbrico (32) expira, comprendiendo además el método:

proporcionar fechas de expiración para cada uno de los códigos del primer conjunto de códigos de acceso proporcionados al dispositivo inalámbrico (32).

4. Un método de acuerdo con la reivindicación 3, que comprende además:

examinar cada una de las fechas de expiración; y

como respuesta a una fecha de expiración particular anterior a una fecha en curso, borrar del dispositivo inalámbrico el código particular del primer conjunto de códigos de acceso que se corresponde con la fecha de expiración particular.

5. Un método de acuerdo con la reivindicación 4, que comprende además:

hacer que un código particular del primer conjunto de códigos de acceso sea borrado, modificando la correspondiente fecha de expiración del mismo.

6. Un método de acuerdo con la reivindicación 1, que comprende además:

proporcionar al dispositivo inalámbrico un valor final que se corresponde con al menos uno del primer conjunto de códigos de acceso, donde el valor final es el resultado de aplicar una pluralidad de veces una función de cifrado unidireccional.

7. Un método de acuerdo con la reivindicación 6, que comprende además:

proporcionar periódicamente un valor al dispositivo inalámbrico;

aplicar la función de cifrado unidireccional al valor, para obtener el resultado de la misma; y

borrar el al menos un código del primer conjunto de códigos de acceso correspondiente al valor final, como respuesta al resultado de que la aplicación de la función de cifrado unidireccional no es igual al valor final.

8. Un método, de acuerdo con la reivindicación 7, en el que el periodo es un día.

9. Un método, de acuerdo con la reivindicación 1, que comprende además:

determinar si ha habido manipulación con el dispositivo inalámbrico; y

como respuesta a la manipulación, borrar todos los códigos del primer conjunto de códigos de acceso.

10. Un método, de acuerdo con la reivindicación 1, que comprende además:

determinar un subconjunto de una pluralidad de códigos del primer conjunto de códigos de acceso que han de transmitirse por el dispositivo inalámbrico.

11. Un método, de acuerdo con la reivindicación 10, en el que la determinación del subconjunto incluye utilizar información transmitida al dispositivo inalámbrico por el primer controlador.

12. Un método, de acuerdo con la reivindicación 10, en el que la determinación del subconjunto incluye utilizar información GPS.

13. Un método, de acuerdo con la reivindicación 10, en el que la determinación del subconjunto incluye alertar al usuario del dispositivo inalámbrico.

14. Un método, de acuerdo con la reivindicación 10, que comprende además:

efectuar el proceso de errores como respuesta a que no ha habido códigos de acceso en el subconjunto.

15. Un método, de acuerdo con la reivindicación 1, que comprende además:

proporcionar una primera tabla que contiene posibles usuarios; y

proporcionar una segunda tabla que contiene posibles códigos de acceso.

16. Un método, de acuerdo con la reivindicación 15, que comprende además:

recibir información de autorización para un usuario en particular y un subconjunto en particular del primer conjunto de códigos de acceso; y

almacenar en el dispositivo inalámbrico el subconjunto particular del primer conjunto de códigos de acceso.

17. Un método, de acuerdo con la reivindicación 16, en el que la información de autorización está autenticada.

18. Un método, de acuerdo con la reivindicación 1, que comprende además:

registrar casos en que el dispositivo inalámbrico transmite el primer conjunto de códigos de acceso al primer controlador.

19. Un método, de acuerdo con la reivindicación 18, en el que los casos se registran almacenando datos en el dispositivo inalámbrico.

20. Un método, de acuerdo con la reivindicación 19, que comprende además:

transmitir los casos a un procesador central.

21. Un método, de acuerdo con la reivindicación 18, en el que los casos se registran almacenando datos en el primer controlador.

22. Un método, de acuerdo con la reivindicación 21, que comprende además:

transmitir los casos a un procesador central.

23. Un método, de acuerdo con la reivindicación 1, en el que el dispositivo inalámbrico es un teléfono móvil.

24. Un método, de acuerdo con la reivindicación 1, en el que el accionamiento del sistema de seguridad acciona una cerradura para permitir el acceso a una zona restringida.

25. Un método, de acuerdo con la reivindicación 1, que comprende además:

proporcionar un segundo conjunto de códigos de acceso al dispositivo inalámbrico; y

hacer que el dispositivo inalámbrico transmita el segundo conjunto de códigos de acceso a un segundo controlador, donde el primer y el segundo controladores son incompatibles.

26. Un producto de programa informático proporcionado en un medio de almacenamiento, que comprende:

código ejecutable que proporciona un primer conjunto de códigos de acceso a un dispositivo inalámbrico (32);

código ejecutable que hace que el dispositivo inalámbrico (32) transmita al menos algunos códigos del primer conjunto de códigos de acceso a un primer controlador (26, 26', 26'') que acciona un sistema de seguridad, y

código ejecutable que recibe información adicional en el dispositivo inalámbrico (32), caracterizado por que la información adicional permite la selección de códigos apropiados del primer conjunto de códigos de acceso para que el dispositivo inalámbrico (32) transmita al primer controlador, de acuerdo con un atributo del dispositivo inalámbrico (32).

27. Un producto de programa informático, de acuerdo con la reivindicación 26, en el que la información adicional es información de localización, y donde el atributo es un lugar geográfico del dispositivo inalámbrico.

28. Un producto de programa informático, de acuerdo con la reivindicación 26, en el que el primer conjunto de

códigos de acceso proporcionado al dispositivo inalámbrico (32) expira, comprendiendo además el producto de programa informático:

código ejecutable que proporciona fechas de expiración para cada código del primer conjunto de códigos de acceso proporcionado al dispositivo inalámbrico (32).

29. Un producto de programa informático, de acuerdo con la reivindicación 28, que comprende además:

código ejecutable que examina cada una de las fechas de expiración; y

código ejecutable que borra del dispositivo inalámbrico un código particular del primer conjunto de códigos de acceso que se corresponde con la fecha de expiración particular, como respuesta a que la fecha de expiración particular es anterior a la fecha actual.

30. Un producto de programa informático, de acuerdo con la reivindicación 29, que comprende además:

código ejecutable que hace que un código particular del primer conjunto de códigos de acceso se borre modificando una correspondiente fecha de expiración del mismo.

31. Un producto de programa informático, de acuerdo con la reivindicación 26, que comprende además:

código ejecutable que proporciona al dispositivo inalámbrico un valor final que se corresponde al menos a un código del primer conjunto de códigos de acceso, donde el valor final es el resultado de aplicar una pluralidad de veces una función de cifrado unidireccional.

32. Un producto de programa informático, de acuerdo con la reivindicación 31, que comprende además:

código ejecutable que proporciona periódicamente un valor al dispositivo inalámbrico;

código ejecutable que aplica la función de cifrado unidireccional al valor, para obtener un resultado de la misma; y

código ejecutable que borra el al menos un código del primer conjunto de códigos de acceso correspondiente al valor final, como respuesta al resultado de que la aplicación de la función de cifrado unidireccional no es igual al valor final no es igual al valor final.

33. Un producto de programa informático, de acuerdo con la reivindicación 32, en el que el periodo es un día.

34. Un producto de programa informático, de acuerdo con la reivindicación 26, que comprende además:

código ejecutable que determina si ha habido manipulación con el dispositivo inalámbrico; y

código ejecutable que borra el primer conjunto de códigos de acceso como respuesta a la manipulación.

35. Un producto de programa informático, de acuerdo con la reivindicación 26, que comprende además:

código ejecutable que determina un subconjunto de una pluralidad de códigos del primer conjunto de códigos de acceso que ha de transmitirse por el dispositivo inalámbrico.

36. Un producto de programa informático, de acuerdo con la reivindicación 35, en el que el código ejecutable que determina el subconjunto utiliza la información transmitida al dispositivo inalámbrico por el primer controlador.

37. Un producto de programa informático, de acuerdo con la reivindicación 35, en el que el código ejecutable que determina el subconjunto utiliza información GPS.

38. Un producto de programa informático, de acuerdo con la reivindicación 35, en el que el código ejecutable que determina el subconjunto alerta al usuario del dispositivo inalámbrico.

39. Un producto de programa informático, de acuerdo con la reivindicación 35, que comprende además:

código ejecutable que realiza el proceso de errores como respuesta a que no hay códigos de acceso en el subconjunto.

40. Un producto de programa informático, de acuerdo con la reivindicación 26, que comprende además:

una primera tabla que contiene posibles usuarios almacenados en memoria; y

una segunda tabla que contiene posibles códigos de acceso almacenados en memoria.

41. Un producto de programa informático, de acuerdo con la reivindicación 40, que comprende además:

código ejecutable que recibe información de autorización para un usuario en particular y un subconjunto en particular del primer conjunto de códigos de acceso; y

código ejecutable que almacena en el dispositivo inalámbrico el subconjunto particular del primer conjunto de códigos de acceso.

42. Un producto de programa informático, de acuerdo con la reivindicación 41, en el que la información de autorización está autenticada.

43. Un producto de programa informático, de acuerdo con la reivindicación 26, que comprende además:

código ejecutable que registra casos en los que el dispositivo inalámbrico transmite el primer conjunto de códigos de acceso al controlador.

44. Un producto de programa informático, de acuerdo con la reivindicación 43, en el que los casos se registran almacenando datos en el dispositivo inalámbrico.

45. Un producto de programa informático, de acuerdo con la reivindicación 44, que comprende además:

código ejecutable que transmite los casos a un procesador central.

46. Un producto de programa informático, de acuerdo con la reivindicación 43, en el que los casos se registran almacenando datos en el primer controlador.

47. Un producto de programa informático, de acuerdo con la reivindicación 46, que comprende además:

código ejecutable que transmite los casos a un procesador central.

48. Un producto de programa informático, de acuerdo con la reivindicación 26, en el que el dispositivo inalámbrico es un teléfono móvil.

49. Un producto de programa informático, de acuerdo con la reivindicación 26, en el que el código ejecutable que actúa sobre el sistema de seguridad acciona una cerradura para permitir el acceso a una zona restringida.

50. Un producto de programa informático, de acuerdo con la reivindicación 26, que comprende además:

código ejecutable que proporciona un segundo conjunto de códigos de acceso al dispositivo inalámbrico; y

código ejecutable que hace que el dispositivo inalámbrico transmita el segundo conjunto de códigos de acceso a un segundo controlador, donde el primer y segundo controladores son incompatibles.

51. Un teléfono móvil (32) que proporciona acceso a zonas restringidas, que comprende:

un medio de almacenamiento;

un módulo de transmisión acoplado al medio de almacenamiento;

código ejecutable almacenado en el medio de almacenamiento, que acepta códigos de acceso proporcionados al teléfono móvil;

código ejecutable que hace que al menos algunos de los códigos de acceso se proporcionen al módulo de transmisión para su transmisión por el teléfono móvil; y

código ejecutable que recibe información adicional en el teléfono móvil (32), caracterizado por que la información adicional permite la selección de códigos apropiados del primer conjunto de códigos de acceso para que el teléfono móvil (32) los transmita a un primer controlador, de acuerdo con un atributo del teléfono móvil (32).

52. Un teléfono móvil, de acuerdo con la reivindicación 51, que comprende además:

código ejecutable que almacena un valor final en el medio de almacenamiento, donde el valor final se corresponde con al menos un código de acceso y donde el valor final es el resultado de la aplicación de una pluralidad de veces una función de cifrado unidireccional;

código ejecutable que acepta periódicamente un valor;

código ejecutable que aplica la función de cifrado unidireccional al valor, para obtener un resultado de la misma; y

código ejecutable que borra el al menos uno de los códigos de acceso correspondientes al valor final, como respuesta al resultado de que la aplicación de la función de cifrado unidireccional no es igual al valor final.

53. El teléfono móvil de acuerdo con la reivindicación 51, en el que la información adicional es información de localización, y donde el atributo es un lugar geográfico del teléfono móvil.

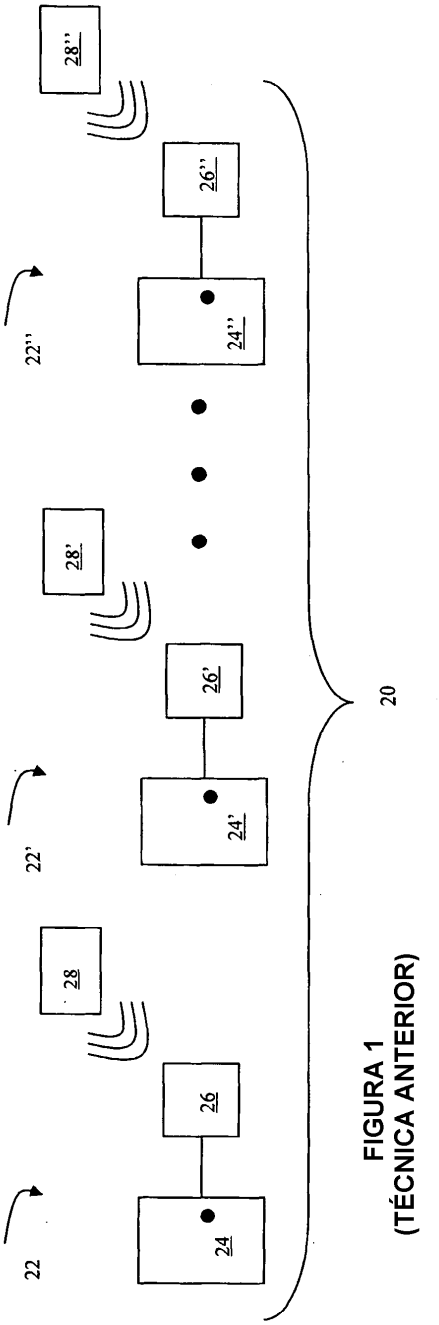

FIGURA 1
(TÉCNICA ANTERIOR)

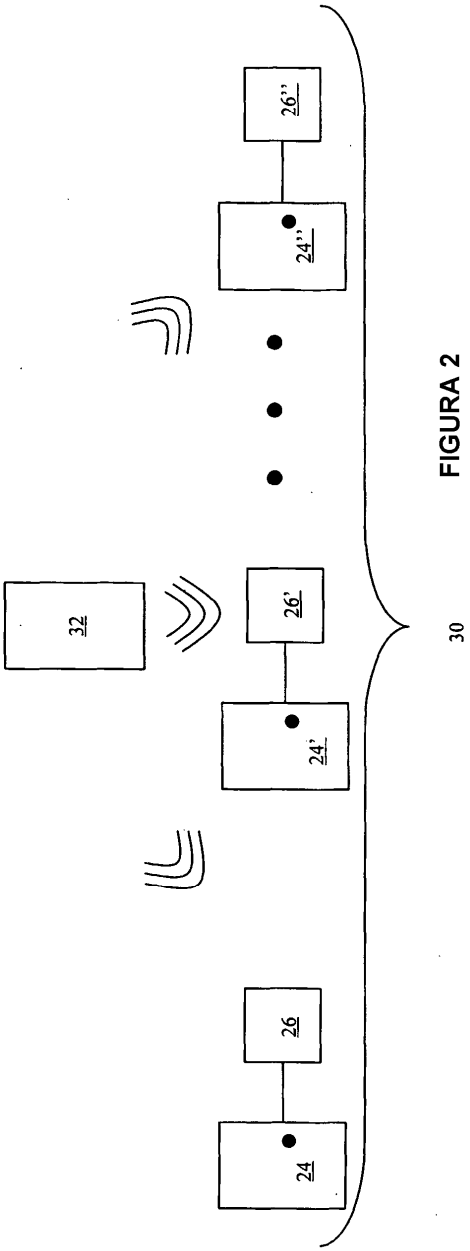

FIGURA 2

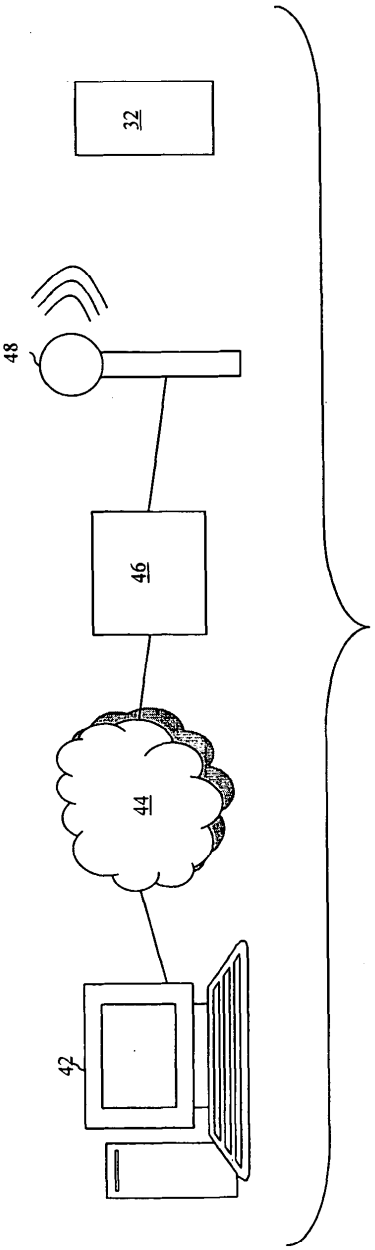

FIGURA 3

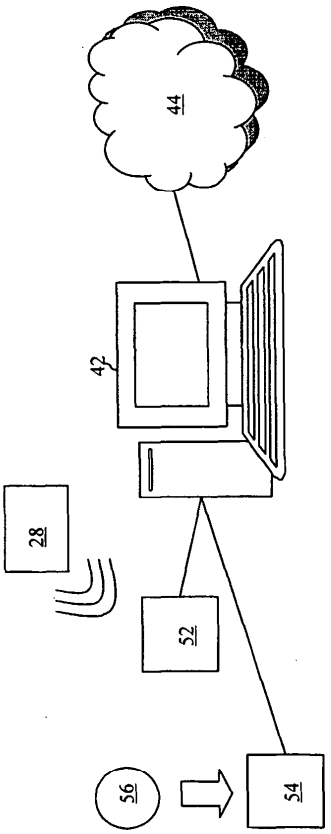

FIGURA 4

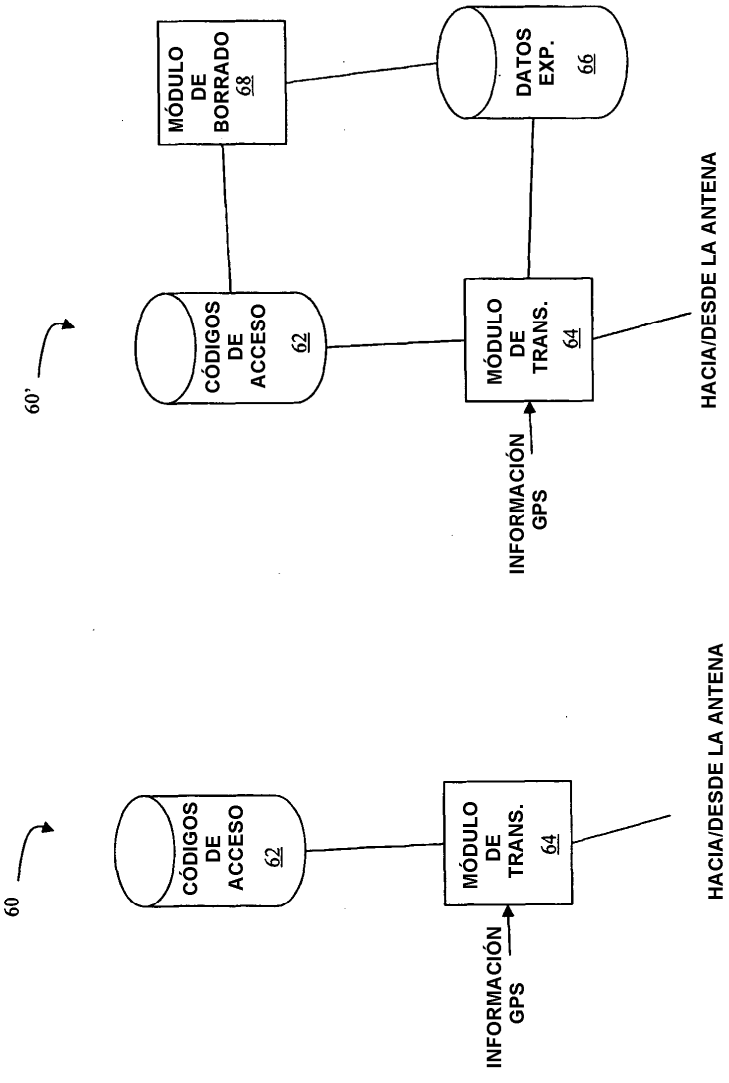

FIGURA 6

FIGURA 5

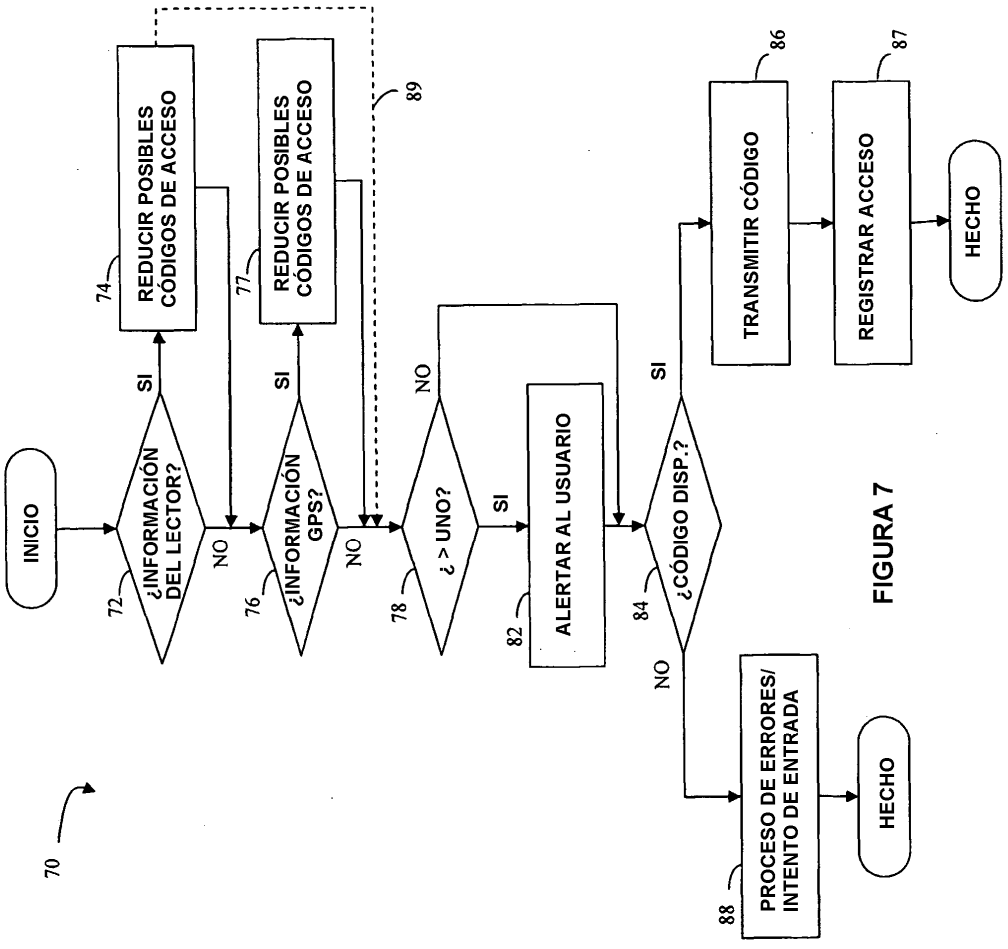
INICIO
¿INFORMACIÓN DEL LECTOR?
SI
NO
REDUCIR POSIBLES CÓDIGOS DE ACCESO
¿INFORMACIÓN GPS?
SI
NO
REDUCIR POSIBLES CÓDIGOS DE ACCESO
¿ > UNO?
NO
SI
ALERTAR AL USUARIO
¿CÓDIGO DISP.?
SI
NO
TRANSMITIR CÓDIGO
REGISTRAR ACCESO
HECHO
PROCESO DE ERRORES/ INTENTO DE ENTRADA
HECHO
70
72
74
76
77
78
82
84
86
87
88
89

FIGURA 7

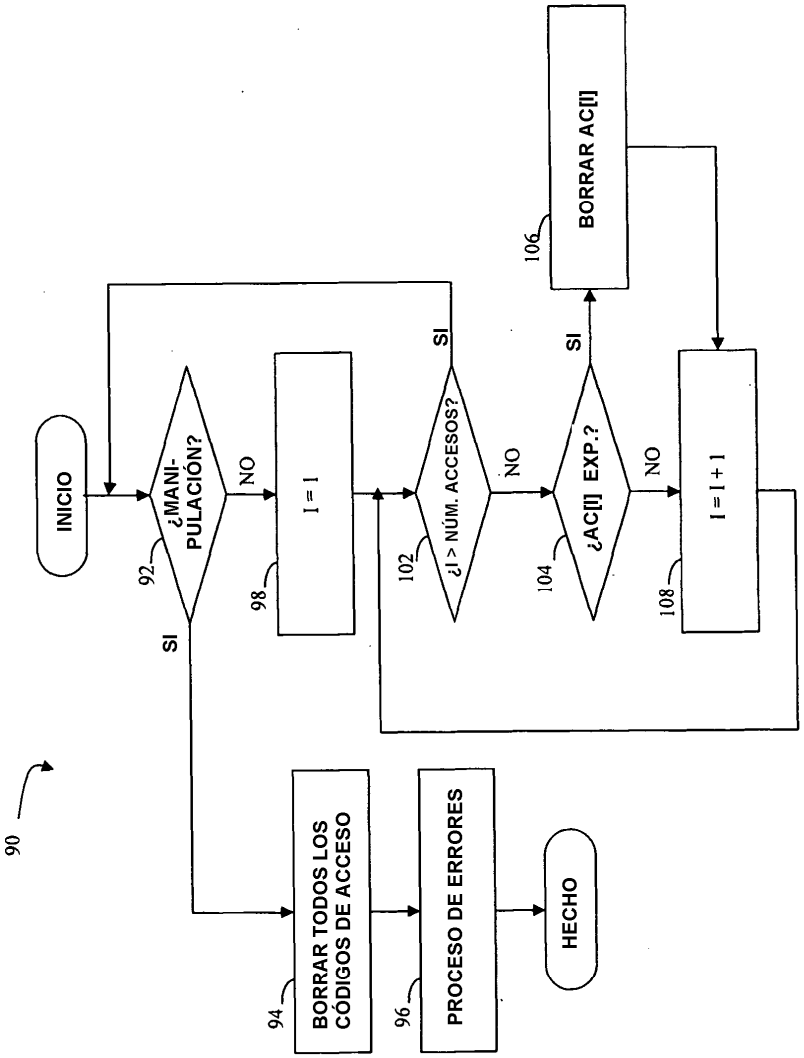
90
INICIO
¿MANI-PULACIÓN?
92
SI
NO
I = 1
98
¿I > NÚM. ACCESOS?
102
SI
NO
¿AC[I] EXP.?
104
SI
NO
BORRAR AC[I]
106
I = I + 1
108
BORRAR TODOS LOS CÓDIGOS DE ACCESO
94
PROCESO DE ERRORES
96
HECHO

FIGURA 8

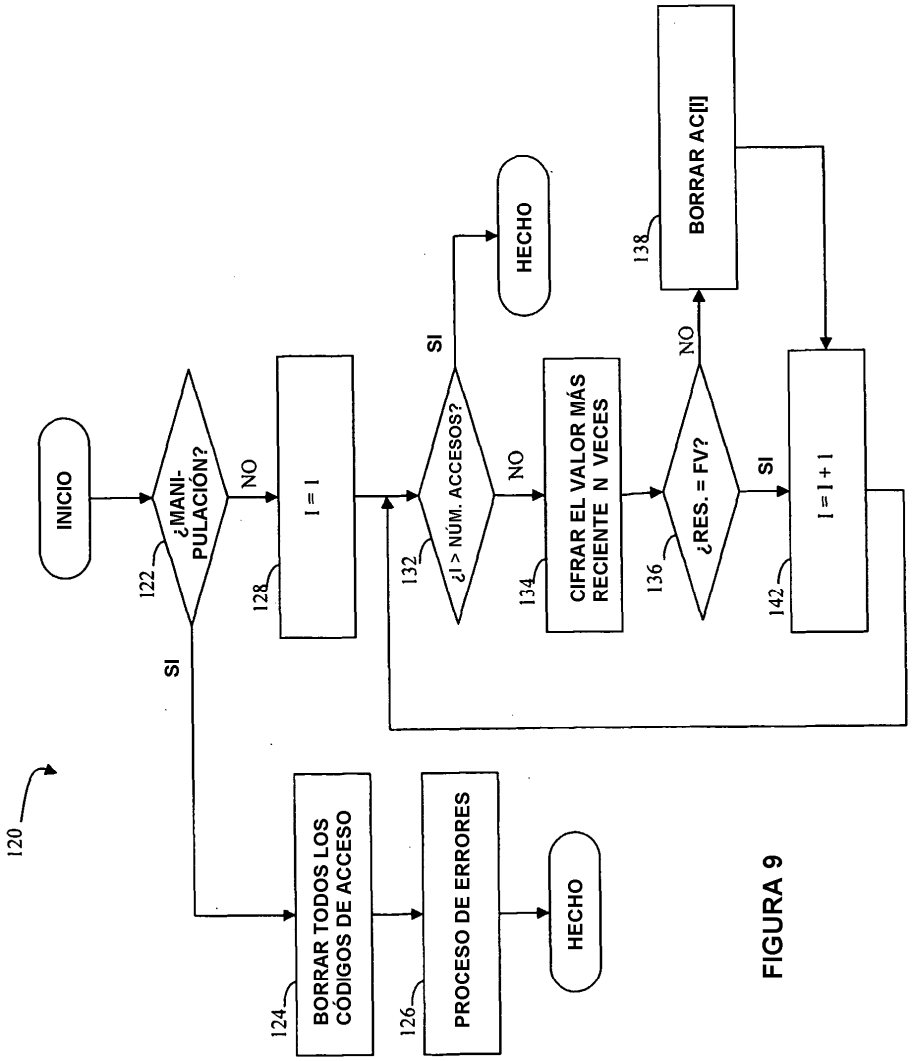
120
INICIO
¿MANI-PULACIÓN?
122
SI
NO
I = 1
128
¿I > NÚM. ACCESOS?
132
SI
HECHO
NO
CIFRAR EL VALOR MÁS RECIENTE N VECES
134
¿RES. = FV?
136
NO
BORRAR AC[I]
138
SI
I = I + 1
142
BORRAR TODOS LOS CÓDIGOS DE ACCESO
124
PROCESO DE ERRORES
126
HECHO

FIGURA 9

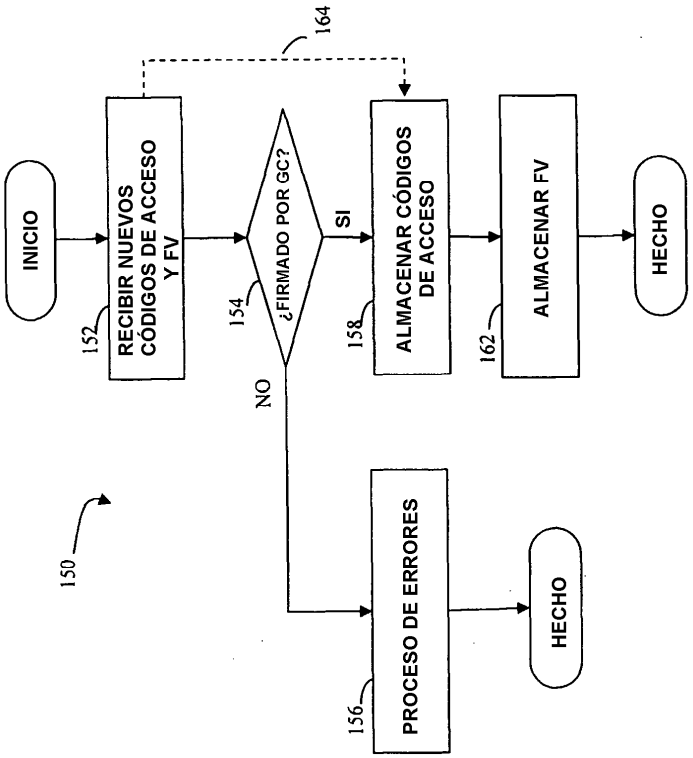
INICIO
RECIBIR NUEVOS CÓDIGOS DE ACCESO Y FV
¿FIRMADO POR GC?
SI
NO
ALMACENAR CÓDIGOS DE ACCESO
ALMACENAR FV
HECHO
PROCESO DE ERRORES
HECHO
150
152
154
156
158
162
164

FIGURA 10

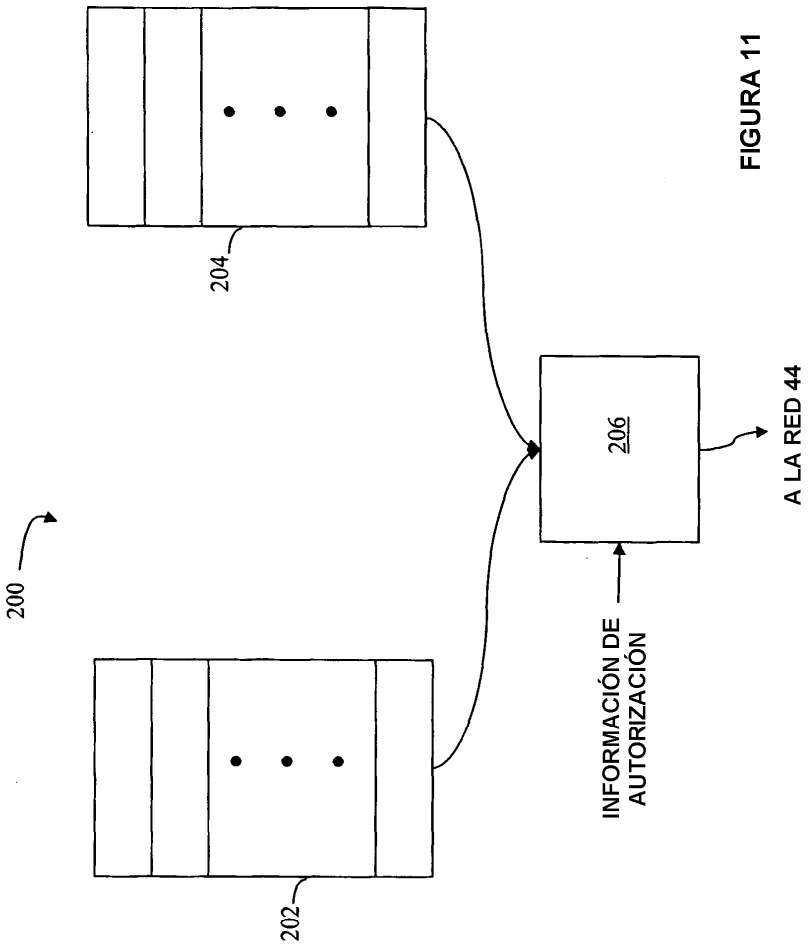

FIGURA 11