(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 507 548**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.05.2002 E 02771817 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.07.2014 EP 1423826**

(54) Título: **Sistema de seguridad**

(30) Prioridad:

22.05.2001 US 862879

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.10.2014

(73) Titular/es:

ERICSSON INC. (100.0%)
6300 LEGACY DRIVE MS EVW 2-C-2
PLANO, TX 75024, US

(72) Inventor/es:

DENT, PAUL y
SKUBIC, JANEZ

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema de seguridad

ANTECEDENTES DE LA INVENCIÓN

La presente invención se refiere en general a sistemas de seguridad para proporcionar seguridad a una tarea de protección y, más en particular, a un sistema de seguridad que usa un protocolo de consulta/respuesta para proporcionar seguridad a las tareas de protección.

Las cerraduras tradicionales emplean una llave o una combinación para limitar el acceso a la propiedad. Presumiblemente, sólo las personas con derecho a acceder a la propiedad poseen la llave o combinación necesarias para manejar la cerradura. Éste método tradicional aún se usa extensamente. Más recientemente, las cerraduras de llave tradicional y de combinación han sido reemplazadas por sistemas de bloqueo electrónico activados por tarjetas de plástico con cinta magnética. Este tipo de cerradura electrónica se usa comúnmente en los hoteles. En este tipo de sistema, un tirador de puerta y un sistema de bloqueo electromagnético están integrados con un lector de tarjeta magnética dentro de una robusta envolvente metálica. El lector de tarjeta magnética lee la tarjeta Insertada, la coteja con un código clave y activa el mecanismo de bloqueo para desbloquear la puerta si se ha proporcionado el código clave correcto.

También se conoce del pasado el uso de algún tipo de identificación, tal como un código PIN, huella digital o exploración del iris para proporcionar un mecanismo de bloqueo para desbloquear una puerta. Uno de tales dispositivos se describe en la patente U.S. número 6,038.666 concedida a Hsu y otros. Esta patente describe un método inalámbrico de hacer funcionar una cerradura de puerta usando datos de huella digital. La cerradura de puerta debe primero estar cargada con datos de la huella digital de un usuario autorizado y la clave pública cifrada del usuario. Un dispositivo móvil transportado por el usuario autorizado está cargado también con los mismos datos de huella digital y se comunica inalámbricamente con la cerradura de la puerta. El nombre del usuario se trasmite de forma no cifrada a la cerradura de la puerta. La cerradura de la puerta genera un par de claves cifradas pública/privada aleatorias y envía la clave pública al dispositivo del usuario. El dispositivo del usuario cifra doblemente los datos de la huella digital usando la clave privada del dispositivo del usuario y la clave pública de la cerradura de la puerta en un orden arbitrario y transmite el resultado a la puerta. La puerta descifra los datos recibidos de la huella digital y los compara con los datos de la huella digital almacenada, desbloqueando la puerta si los datos de la huella digital coinciden.

La patente U.S. número 5,602.536 describe una o más cerraduras o unidades de clave de un sistema de seguridad de entrada, que está provisto de un receptor de radio. El receptor permite que una memoria en la cerradura o en la unidad de clave se actualice con nuevos datos que van modulados sobre una señal de radiofrecuencia.

La solicitud de patente Europea EP 0870889 describe un sistema de entrada sin llave de vehículos a motor e ignición. Un usuario activa un control remoto para seleccionar una tarea a realizar por el vehículo a motor. Cuando se producen una primera y una segunda indicaciones de verificación, un circuito de control emite una señal que hace que el vehículo a motor realice la tarea seleccionada.

La patente U.S. 5,897.598 describe un transpondedor portátil, tal como una llave, que cuando envía datos no válidos a una cerradura, recibe una señal de consulta. La llave envía en respuesta una palabra código a la cerradura. La cerradura comprueba la palabra código y si coincide con la palabra código deseada calcula un nuevo código para un siguiente ciclo de apertura, creando por consiguiente un código alternativo.

BREVE SUMARIO DE LA INVENCIÓN

La presente invención se refiere a un método de habilitar o activar una tarea de protección de acuerdo con la reivindicación 1 y a un sistema de seguridad que proporciona seguridad de acuerdo con la reivindicación 9, por ejemplo, para una tarea de protección tal como desbloquear una puerta. De acuerdo con la presente invención, la tarea a proteger está controlada por un dispositivo de control de accesos. Los miembros autorizados para acceder a la tarea a proteger utilizan un dispositivo de comunicación inalámbrica, tal como un radio teléfono móvil, para comunicarse con el dispositivo de control de accesos. Un código de autorización válido por un periodo especificado de tiempo se almacena en el dispositivo de comunicación inalámbrica. Para acceder a la tarea asegurada, el miembro autorizado hace que el dispositivo de comunicación inalámbrica transmita una petición de acceso al dispositivo de control de accesos. El dispositivo de control, en respuesta a la petición de acceso, transmite una consulta de autenticación a los dispositivos de comunicación inalámbrica. La consulta de comunicación comprenderá típicamente al menos un número aleatorio y puede incluir una indicación de la hora. El dispositivo de comunicación inalámbrica genera una respuesta de autenticación combinando partes seleccionadas de la consulta de autenticación (por ejemplo, el número aleatorio) con el código de autorización almacenado en su memoria y transmite la respuesta de autenticación al dispositivo de control de accesos. El dispositivo de control de accesos compara la respuesta de autenticación recibida con una respuesta de autenticación esperada y habilita o activa la tarea de protección si la respuesta de autenticación recibida coincide con la respuesta de autenticación esperada.

El controlador central puede también cambiar los códigos de autorización cuando sea necesario. En una realización, el dispositivo de control de accesos es un dispositivo autónomo programado con un código maestro. El dispositivo de control de accesos utiliza el código maestro almacenado para calcular códigos de autorización para diferentes periodos de tiempo. El controlador central, con un conocimiento *a priori* del código maestro usado por el dispositivo de control de accesos puede también calcular códigos de autorización para cualquier periodo de tiempo.

El sistema de control de accesos de la presente invención se puede usar, por ejemplo, en un hotel para controlar el acceso a las habitaciones del hotel para predeterminados periodos de tiempo. Los expertos en la técnica encontrarán numerosos usos diferentes para el sistema de control de accesos de la presente invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un diagrama esquemático del sistema inalámbrico de cerradura de puerta de acuerdo con la presente invención.

La figura 2 es un diagrama funcional de bloques de un dispositivo de comunicación inalámbrica usado por un miembro autorizado para comunicarse con un dispositivo de control de accesos.

La figura 3 es un diagrama funcional de bloques de un módulo de seguridad que se puede usar en un dispositivo de control de accesos, en un dispositivo de comunicación inalámbrica o en un controlador central.

La figura 4 es un diagrama funcional de bloques que ilustra una realización de ejemplo de un dispositivo de control de accesos de acuerdo con la presente invención. En esta realización, el dispositivo de control de accesos tiene la forma de una cerradura electrónica de puerta.

La figura 5 es un diagrama funcional de bloques de un controlador central usado para emitir códigos de autorización a un dispositivo de comunicación inalámbrica.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

La figura 1 ilustra un sistema de seguridad, indicado en general por el número 10, de acuerdo con la presente invención. El sistema de seguridad 10 consta de un dispositivo de control de accesos 20, un controlador central 40 y un dispositivo de comunicación inalámbrica 100 para activar las tareas protegidas aseguradas por el dispositivo de control de accesos 20. En la realización ilustrativa que se describe más adelante, el sistema de seguridad 10 es un sistema de cerradura de puerta inalámbrica para un hotel y el dispositivo de control de accesos 20 consiste en una cerradura electrónica de puerta. Por consiguiente, para el resto de la descripción, el dispositivo de control de accesos 20 se refiere en este documento como cerradura electrónica de puerta 20.

De acuerdo con el ejemplo presente, al dispositivo de comunicación inalámbrica 100 se le habilita con un código de autorización por el controlador central 40. Una vez habilitado, el dispositivo de comunicación inalámbrica 100 se puede usar para “desbloquear” la puerta. Para desbloquear la puerta, el dispositivo de comunicación inalámbrica 100 transmite una petición de acceso a la cerradura electrónica de puerta 20 (es decir, al dispositivo de control de accesos). La cerradura electrónica de puerta 20 transmite una petición de autenticación al dispositivo de comunicación inalámbrica 100 en respuesta a la petición de acceso. La petición de autenticación incluye, al menos, una cadena de bits aleatoria o un número que no puede ser conocido con anterioridad por el dispositivo de comunicación inalámbrica 100. El dispositivo de comunicación inalámbrica 100 combina partes seleccionadas de la petición de autenticación, incluyendo la cadena de bits aleatoria, con el código de autorización almacenado usando un predeterminado algoritmo de combinación para generar una respuesta de autenticación y transmitir la respuesta de autenticación a la cerradura electrónica de puerta 20. La cerradura electrónica de puerta 20 calcula una respuesta de autenticación esperada usando el mismo algoritmo de combinación. Si la respuesta de autenticación recibida coincide con la respuesta de autenticación esperada, la puerta es desbloqueada para permitir el acceso a la habitación del hotel.

El controlador central 40 se comunica con el dispositivo de comunicación inalámbrica por medio de un interfaz inalámbrico, tal como un interfaz BLUETOOTH, para proporcionar los códigos de autorización al dispositivo de comunicación inalámbrica 100. Alternativamente, el dispositivo de comunicación inalámbrica 100 puede estar incluido dentro de una plataforma de conexión o conectado por medio de cable a un interfaz normalizado en el controlador central 40 para permitir el intercambio de datos. El controlador central 40 puede también comunicarse con la cerradura electrónica de puerta 20 para cargar o cambiar códigos de autorización para la cerradura electrónica de puerta 20. No es esencial, sin embargo, que el controlador central 40 se comunique con la cerradura electrónica de puerta 20. Como se describirá más adelante, la cerradura electrónica de puerta 20 puede estar programada con un código maestro secreto que se usa para calcular códigos de autorización para diferentes periodos de tiempo. Conociendo este código maestro y un número del dispositivo asociado a la cerradura electrónica de puerta 20, el controlador central 40 puede calcular, en cualquier momento dado, el código válido de autorización de la cerradura electrónica de puerta 20.

La comunicación entre el dispositivo de comunicación inalámbrica 100 y la cerradura electrónica de puerta 20 se hace por medio de un interfaz inalámbrico, tal como un interfaz de radio frecuencia de corto alcance conforme a la norma BLUETOOTH. La norma BLUETOOTH permite la comunicación inalámbrica de datos y voz en enlaces inalámbricos de corto alcance entre ambos dispositivos móviles y fijos. El interfaz BLUETOOTH es un interfaz de radio universal en la banda de frecuencias de 2,45 GHz, que permite que los dispositivos portátiles electrónicos se conecten y comuniquen inalámbricamente por medio de redes de corto alcance, ad hoc. A aquellos interesados en diferentes detalles con respecto a la tecnología BLUETOOTH, se les remite al artículo titulado “The Bluetooth Radio System” de Jaap Haartsen,

que se puede encontrar en IEEE Personal Communications, de Febrero de 2000, cuya descripción del mismo se incorpora en este documento como referencia. Aunque la presente invención se explica este documento con referencia a la norma BLUETOOTH, se advierte que se pueden usar también otras normas para interfaces inalámbricos de corto alcance.

La norma BLUETOOTH proporciona el cifrado y descifrado de datos, que permite que los datos se comuniquen con seguridad. Usando la norma BLUETOOTH, el dispositivo de comunicación inalámbrica 100 puede comunicarse con seguridad con la cerradura electrónica de puerta 20 y con el controlador central 40 sin descubrir la información secreta.

La figura 2 es un diagrama funcional de bloques que muestra una realización de ejemplo de un dispositivo de comunicación inalámbrica 100 de acuerdo con la presente invención. En la realización de ejemplo, el dispositivo de comunicación inalámbrica 100 es un terminal móvil equipado con BLUETOOTH, tal como un radio teléfono celular o un asistente personal digital (PDA). El dispositivo de comunicación inalámbrica 100 consta de un procesador principal 101, un dispositivo de entrada 102, una pantalla 103, un interfaz inalámbrico 104, una batería 105 y un módulo de seguridad 110. El procesador 101 controla el funcionamiento del dispositivo de comunicación inalámbrica 100. Un dispositivo de entrada 102, tal como un teclado o un puntero, permiten al usuario introducir datos y comandos. La pantalla 103 permite que el usuario vea la información, tal como los ajustes y mensajes del dispositivo. El interfaz inalámbrico 104 permite la comunicación con los dispositivos externos, tales como la cerradura electrónica de puerta 20 y posiblemente el controlador central 40. La batería 105 suministra energía al dispositivo inalámbrico de comunicación 100. El módulo de seguridad 110 puede contener datos de la suscripción necesarios para activar el dispositivo inalámbrico de comunicación 100. Además, el módulo de seguridad 110 puede almacenar variables de seguridad, tales como claves de cifrado públicas y privadas, para facilitar las transacciones seguras.

La figura 3 ilustra el módulo de seguridad 110 con mayor detalle. El módulo de seguridad 110 comprende un procesador seguro 111, una memoria de programa 112, una memoria de datos 113, una memoria de acceso aleatorio 114 y un interfaz de entrada/salida 115. El módulo de seguridad 110 puede incluir opcionalmente un co-procesador 116 y un generador de bits o de ruido aleatorio 117. El procesador 111 ejecuta sólo los programas seleccionados almacenados en la memoria de programa 112. La memoria de datos 113 se utiliza como almacenamiento de larga duración para los datos generados después de la fabricación, tales como las claves secretas específicas del usuario. La memoria de acceso aleatorio 114 se utiliza como almacenamiento temporal para los cálculos. El interfaz de entrada/salida 115 interconecta el módulo de seguridad 110 con el procesador principal 101 en el dispositivo de comunicación inalámbrica 100. El co-procesador 116, si existe, acelera ciertos cálculos, tales como cálculos criptográficos que impliquen multiplicación, raíz cuadrada o exponenciación de valores enteros grandes. El generador de ruido aleatorio 117, si existe, proporciona a un tiempo la generación de pares de claves pública/privada y consultas de autenticación ad hoc, como se describirá a continuación: El co-procesador 116 y el generador de ruido aleatorio 117 no son necesarios para la realización de la invención, pero pueden ser útiles para el aspecto relativo a la verificación de la identidad del usuario.

El módulo de seguridad 110 puede estar contenido, por ejemplo, en una tarjeta inteligente extraíble. Las solicitudes de patentes U.S. relativas al uso de tarjetas inteligentes incluyen la solicitud de patente U.S. número de serie 09/695964 presentada el 25 de octubre de 2000 titulada "Method of Bi-Lateral Identity Authentication Over the Internet" y la solicitud de patente U.S. número de serie 09/696450, titulada "Method of Establishing a Symmetric Cipher Key" presentada el 25 de octubre de 2000 que se han Incorporado en el presente documento como referencia. La solicitud mencionada en primer lugar describe cómo utilizar un dispositivo de comunicación inalámbrica 100 que contiene una tarjeta inteligente para establecer mutuamente la identidad de dos dispositivos de comunicación y para establecer una clave de sesión temporal para una comunicación eficiente, segura entre los dispositivos. La segunda solicitud describe un método para establecer con seguridad una clave secreta y almacenar la clave secreta en una tarjeta inteligente. Las técnicas que se describen en estas aplicaciones se pueden utilizar para verificar la identidad electrónica, incluyendo la identidad de crédito de un posible huésped del hotel para establecer una clave secreta con la que los códigos de autorización se transfieren desde el controlador central 40 al dispositivo de comunicación inalámbrica 100 para ser cifrada, evitando de este modo su interceptación.

La figura 4 muestra una realización de ejemplo de la cerradura electrónica de puerta 20 con más detalle. La cerradura electrónica de puerta 20 comprende un dispositivo de accionamiento 22, una unidad de control 24, un reloj interno 26, un Interfaz inalámbrico 28, un interfaz de red 30, un módulo de seguridad 110 y una batería 34. El interfaz inalámbrico 28 permite que la cerradura electrónica de puerta 20 se comunique con el dispositivo de comunicación inalámbrica 100. Como se ha mencionado anteriormente, el interfaz inalámbrico 28 puede ser un interfaz BLUETOOTH. La cerradura electrónica de puerta 20 puede incluir además un interfaz de red 30 para conectar la cerradura electrónica de puerta 20 al controlador central 40 por medio de una red de área local en ciertas realizaciones. El interfaz de red 30 puede ser un interfaz normalizado para comunicaciones cableadas, tal como un interfaz serie o un interfaz Ethernet, o puede ser un interfaz inalámbrico. Alternativamente, un simple interfaz inalámbrico 28 puede ser utilizado para las comunicaciones, tanto con el dispositivo de comunicación inalámbrico 100 como con el controlador central 40. El reloj en tiempo real 26 proporciona una referencia de tiempo para la unidad de control 24. La cerradura de electrónica de puerta 20 puede incluir además un módulo de seguridad 110 del tipo mostrado en la figura 3 que proporciona almacenamiento seguro para la información secreta y realiza cálculos criptográficos que se describirán más adelante. La energía para la

cerradura electrónica de puerta 20 la suministra una batería 34 u otra fuente de alimentación.

La figura 5 es un diagrama funcional de bloques del controlador central 40, que puede estar situado en el mostrador de recepción del hotel o conectado a una plataforma de recepción a través de una red de área local. El controlador central 40 normalmente comprende cualquier tipo de ordenador personal o de sobremesa que tiene un procesador 41, un dispositivo de entrada 42, una pantalla 43, un reloj 44, un interfaz de red 45 y un módulo de seguridad 110. El controlador central 40 puede incluir además un interfaz 46, tal como un interfaz inalámbrico, para comunicarse con el dispositivo de comunicación inalámbrica 100, transportado por el cliente. El funcionamiento puede ser restringido sólo al personal autorizado de acuerdo con los procedimientos normales de identificación usando contraseñas, etc. El funcionamiento de los programas de seguridad puede estar además protegido usando contraseñas inversas generadas en el módulo de seguridad 110 como se describe en la solicitud de patente U.S. número de serie 09/727062 presentada el 30 de noviembre de 2000 titulada "AntiSpoofing Password Protection", que se incorpora como referencia en el presente documento. Esta solicitud describe un método para proteger contra las falsas informaciones que invitan al usuario a introducir contraseñas, que luego serían enviadas inocentemente a un miembro no autorizado.

El modulo de seguridad 110 suele encontrarse en una caja segura, a prueba de manipulaciones y puede ser del tipo ilustrado en la figura 3. El modulo de seguridad 110 puede almacenar información secreta usada para derivar códigos de autorización como se describe a continuación, así como claves pública y privada utilizadas para el cifrado y descifrado. El interfaz de red 45, tal como un interfaz Ethernet, conecta el controlador central 40 a una red de área local dentro del hotel, que puede proporcionar los medios para comunicarse con el sistema de cerradura electrónica de puerta 20. La red de área local puede además incluir una pasarela (no mostrada) para comunicarse con redes externas, tales como Internet. El interfaz inalámbrico 46 puede, por ejemplo, comprender un interfaz BLUETOOTH que permite la comunicación de corto alcance y de redes ad hoc con otros dispositivos. El controlador central 40 puede comunicarse con el dispositivo de comunicación inalámbrica 100 a través del interfaz inalámbrico 46. Alternativamente, el interfaz inalámbrico 46 puede ser sustituido por un interfaz normalizado, tal como una interfaz serie o un interfaz USB.

En una realización, no es necesaria la comunicación entre la cerradura electrónica de puerta 20 y el controlador central 40 después de la instalación de la cerradura electrónica de puerta 20. La cerradura electrónica de puerta 20 está programada con un código maestro, un identificador del dispositivo (que puede ser, por ejemplo, el número de la puerta) y un valor inicial para su reloj interno 26. Cada cerradura electrónica de puerta 20 puede generar un nuevo código de autorización a una hora de salida especificada, determinada por su reloj interno 26 mediante la combinación del código maestro con su identificador del dispositivo y la fecha utilizando un algoritmo de combinación predeterminado. El controlador central 40 también puede generar un código de autorización para cualquier puerta y fecha mediante la combinación de las mismas variables de entrada utilizando el mismo algoritmo de combinación, que luego se puede suministrar al dispositivo de comunicación inalámbrica 100 del huésped.

Al utilizarlo, un huésped del hotel que lleva un dispositivo de comunicación inalámbrica 100 se presenta en el mostrador de recepción del hotel. Si el dispositivo de comunicación inalámbrica 100 incluye un interfaz Bluetooth, el dispositivo de comunicación inalámbrica 100 puede ya haber establecido comunicación con el controlador central 40. Los detalles de cómo se establecen las comunicaciones entre dos dispositivos BLUETOOTH no son relevantes para esta invención y no se describirán en este documento. Por medio del uso de tecnología de cifrado, el interfaz BLUETOOTH proporciona un canal de comunicación segura entre el dispositivo de comunicación inalámbrica 100 y el controlador central 40. Durante el procedimiento de admisión, al huésped se le puede pedir el equivalente electrónico de una tarjeta de crédito de cara a la facturación. El controlador central 40, bajo la dirección del empleado del hotel, transmite una petición de identificación del crédito al dispositivo de comunicación inalámbrica 100 del huésped. El controlador central 40 y el dispositivo de comunicación inalámbrica 100 pueden entonces ejecutar un procedimiento de autenticación como el descrito en la solicitud de patente U.S. número de serie 09/696450. El propósito del procedimiento de autenticación es comprobar o autenticar la identidad de crédito del huésped. El procedimiento de autenticación puede incorporar un procedimiento de establecimiento de clave para establecer una clave de sesión para posteriores comunicaciones. Tras la autenticación de la identidad crédito reclamada, el controlador central 40 transmite códigos de autorización e indicaciones de hora asociadas al dispositivo de comunicación inalámbrica 100, que pueden ser cifradas utilizando la clave de sesión acordada. Se necesitan indicaciones de la hora cuando se transfieren múltiples códigos de autorización para diferentes períodos de tiempo de forma que el dispositivo de comunicación inalámbrico 100 sepa qué código usar para cualquier período de tiempo determinado.

Los códigos de autorización y la clave de sesión se almacenan en el dispositivo de comunicación inalámbrica 100. Los códigos de autorización y la clave de sesión pueden, por ejemplo, estar almacenados en la memoria a prueba de manipulaciones dentro del módulo de seguridad 110 o de forma protegida en la memoria 113. Un método de proteger un código de autorización almacenado en una memoria insegura es borrar dígitos seleccionados del código de autorización basándose en un código PIN proporcionado por el usuario. El código de autorización, en este caso no es operativo para desbloquear la puerta a menos que el código PIN, que sólo conoce el usuario, sea suministrado para rellenar los dígitos que faltan del código de autorización.

El dispositivo de comunicación inalámbrica 100 del cliente, ahora programado con códigos de autorización e indicaciones asociadas de la hora, se puede utilizar para desbloquear una puerta del hotel equipada con la cerradura

electrónica de puerta 20 de la presente invención. El dispositivo de comunicación inalámbrica 100 transmite una petición de acceso a la cerradura electrónica de puerta 20 para desbloquear la puerta del hotel. La petición de acceso puede incluir un identificador del dispositivo que direcciona en particular la cerradura electrónica de puerta 20 (por ejemplo, “358” para la habitación 358). El identificador del dispositivo puede direccionar múltiples cerraduras electrónicas de puerta 20 usando un grupo identificador como el que se describirá a continuación. Tras la recepción de la petición de acceso, la cerradura electrónica de puerta 20 genera una consulta de autenticación en el módulo de seguridad 110. Alternativamente, la cerradura electrónica de puerta 20 puede recibir una consulta de autenticación desde el controlador central 40 específica para esa cerradura electrónica de puerta 20 en particular y transmitir la consulta de autenticación al dispositivo de comunicación inalámbrica 100. La consulta de autenticación transmitida por la cerradura electrónica de puerta 20 puede comprender una cadena aleatoria de bits generada localmente o un número obtenido a partir de un generador de ruido aleatorio 117, que puede estar situado en la cerradura electrónica de puerta 20 o accesible a través de una red de área local. La consulta de autenticación puede incluir además la indicación de la hora actual, que puede ser suministrada por el controlador central 40 o por un reloj interno 28 en la cerradura electrónica 20.

Una vez recibida la consulta de autenticación, el dispositivo de comunicación inalámbrica 100 combina al menos la cadena de bits aleatoria de la consulta de autenticación con el código de autorización apropiado para el período de tiempo actual para conformar una respuesta de autenticación. La indicación de la hora en la consulta de autenticación (si existe) puede ser utilizada por el dispositivo de comunicación inalámbrica 100 para seleccionar el código de autorización apropiado de entre una pluralidad de códigos o el dispositivo de comunicación inalámbrica 100 puede utilizar una indicación de la hora proporcionada por un reloj interno (no mostrado). El dispositivo de comunicación inalámbrica 100 transmite la respuesta de autenticación a la cerradura electrónica de puerta 20.

La cerradura electrónica de puerta 20 compara la respuesta de autenticación recibida con una respuesta de autenticación esperada calculada por la cerradura electrónica de puerta 20. Si la respuesta de autenticación recibida coincide con la respuesta de autenticación esperada, la cerradura electrónica de puerta 20 acciona el mecanismo de bloqueo electrónico 22 para desbloquear la puerta.

El código de autorización suministrado por el controlador central 40 al dispositivo de comunicación inalámbrica 100 puede comprender una combinación de códigos maestros secretos con al menos una indicación del periodo de tiempo durante el cual el código de autorización es válido. El usuario del dispositivo de comunicación inalámbrica 100 es, por lo tanto, incapaz de producir códigos de autorización por un período de tiempo elegido por el usuario, ya que el usuario no posee el código maestro secreto. Opcionalmente, el identificador del dispositivo puede ser usado para generar el código de autorización y/o la respuesta de autenticación.
El identificador de dispositivo puede estar combinado por el controlador central 40 con el código maestro secreto y la indicación de la hora para generar el código de autorización. Del mismo modo, el identificador del dispositivo puede estar combinado por el dispositivo de comunicación inalámbrica 100 con el código de autorización y partes seleccionadas de la consulta de autenticación para generar la respuesta de autenticación. El uso de un identificador del dispositivo para generar la respuesta de autenticación en el dispositivo de comunicación inalámbrica 100 se puede hacer cuando el hotel utiliza diferentes códigos maestros de autorización para producir códigos de autorización para diferentes puertas. Si se utilizan los mismos códigos maestros para generar códigos de autorización para todas las puertas, entonces el dispositivo de comunicación inalámbrica 100 podría abrir cualquier puerta sustituyendo un identificador del dispositivo suministrado al usuario cuando se calcula la respuesta de autenticación, lo cual no es deseable.

Un usuario autorizado con determinados privilegios, tal como el personal del hotel, puede recibir un dispositivo de comunicación inalámbrica 100 programado con un código de autorización maestro para abrir cualquier puerta. Un código de autorización maestro es aquel que abre dos o más puertas. Tal código de autorización maestro lo genera el controlador central 40 utilizando el código maestro y un identificador de grupo. El código de autorización maestro también puede ser generado basándose en una indicación de la hora asociada con un período de tiempo deseado. Un identificador de grupo es un código que direcciona más de una cerradura electrónica de puerta 20. Por ejemplo, la cadena de bits para "353" puede direccionar la cerradura electrónica de puerta de la habitación 353. La cadena de bits para "35-" (donde - representa un dígito en blanco) se puede utilizar para direccionar las cerraduras electrónicas de puerta de las habitaciones 350 – 359. La cadena de bits"3--" se puede utilizar como un identificador de grupo para todas las habitaciones del tercer piso, y la cadena de bits"---" puede utilizarse como un identificador de grupo para todas las habitaciones del hotel.

Para utilizar un código de autorización maestro, el dispositivo de comunicación inalámbrica 100 transmite un identificador de grupo a la cerradura electrónica de puerta 20 como parte de una petición de acceso. La petición de acceso puede estar dirigida a una cerradura electrónica de puerta 20 en particular para evitar activar otras cerraduras electrónicas de puerta 20 dentro del alcance del dispositivo de comunicación inalámbrica 100. Por ejemplo, la petición de acceso a la cerradura electrónica de puerta 20 de la habitación número 303 podría comprender la cadena 303 codificado 3- dentro de los bits para indicar a la cerradura electrónica de puerta 20 que la respuesta de autenticación se va a basar en un código de autorización maestro para el grupo que comprende todas las habitaciones del tercer piso. De manera semejante, una petición de acceso a la cerradura electrónica de puerta 20 de la habitación 358 incluiría la cadena 358 3-. La cerradura electrónica de puerta 20 respondería con una consulta de autenticación y el dispositivo de

comunicación inalámbrica 100 del usuario autorizado calcularía una respuesta de autenticación con aquel código maestro de autorización del usuario. El código de autorización maestro lo calcula el controlador central 40, usando el identificador de grupo en lugar de un dispositivo identificador. Es decir, el identificador de grupo se combina con el código maestro y, posiblemente, con una indicación de la hora. La cerradura electrónica de puerta 20 calcula una respuesta de autenticación esperada basándose en el código de autorización maestro para el grupo designado y compara la respuesta de autenticación recibida del dispositivo de comunicación inalámbrica 100 del usuario autorizado con la respuesta esperada de autenticación. Tras la coincidencia, la puerta se desbloquearía.

El método descrito anteriormente desbloquearía cualquier puerta de habitación que comenzara con el número "3" y, por ello, proporcionaría una clave maestra para las habitaciones de la tercera planta, por ejemplo. Una clave maestra universal podría ser calculada por el equipo de seguridad del hotel basándose en el código maestro y en una indicación de la hora, y en el patrón de bits para ---, que se refiera a cualquier puerta. Cuando se abre una puerta por medio de dichas claves maestras, el reloj interno 26 de la cerradura de puerta se puede poner en hora transmitido desde el dispositivo de comunicación inalámbrica 100 del usuario autorizado mediante la transmisión de un comando de puesta a cero de manera que cualquier desviación o inexactitud se corrige de acuerdo con la hora exacta del hotel.

El método de combinar datos secretos del hotel con indicación de la hora, identificadores de dispositivos u otras variables para producir códigos de autorización con partes seleccionadas de consultas de autenticación, ya sea en el dispositivo de comunicación inalámbrica 100 o en la cerradura electrónica de puerta 20, utiliza una función no reversible. El propósito de una función no reversible es hacer imposible o impracticable la determinación del código maestro o del código de autorización dada la salida de la función y todas las demás variables de entrada no secretas. Asimismo, la función no reversible hace impracticable la generación de códigos de autorización para otra puerta u otro período de tiempo dados los códigos de autorización para una puerta o período de tiempo, o dados el código de autorización para muchas otras puertas y/o periodos de tiempo. Un buen algoritmo de combinación que tiene las propiedades deseadas se describe en la Patente U.S. número 5091942 que se incorpora aquí para referencia. Por lo general, esta función no reversible se proporciona mediante el uso de cifrado de bloques, usando los datos secretos al introducir la clave y otros bits de datos como la entrada de "los datos a cifrar". Se puede usar el cifrado de bloques, conocido como DES. Por ejemplo, se considera adecuada la seguridad proporcionada por claves secretas de 56 bits. Por lo demás, el cifrado iterativo de bloques descrito en la patente anterior se puede extender a cualquier clave deseada o longitud variable.

A pesar de las provisiones de seguridad descritas anteriormente, embaucadores sofisticados pueden intentar entrar a una habitación del hotel atrayendo a un individuo con un dispositivo de comunicación inalámbrica 100 autorizado para pedir acceso a la habitación, retransmitiendo la petición de acceso a la cerradura electrónica de puerta 20, retransmitiendo la consulta de autenticación de la cerradura electrónica de puerta 20 al dispositivo de comunicación inalámbrica 100 del usuario autorizado y retransmitiendo la respuesta de autenticación recibida del dispositivo de comunicación inalámbrica 100 del usuario autorizado a la cerradura electrónica de puerta 20. Por ejemplo, dos embaucadores pueden colaborar para atraer a un huésped del hotel para desbloquear de forma remota su puerta de la habitación del hotel para cometer un robo. Uno de los embaucadores, equipado con un dispositivo de comunicación inalámbrica modificado, puede merodear cerca de una puerta que desea desbloquear, mientras que el otro, que tiene un segundo dispositivo de comunicación inalámbrica 100 similarmente modificado, traba conversación con el huésped desprevenido. El segundo embaucador atrae o trata de timar al huésped demostrándole cómo se utiliza el dispositivo de comunicación inalámbrica 100 para abrir una puerta. De este modo, el huésped puede ser engañado para transmitir una petición de acceso para abrir la puerta, cuya petición es recibida por el dispositivo inalámbrico del segundo embaucador y retransmitida inmediatamente al primer embaucador. El dispositivo inalámbrico del primer embaucador retransmite la petición de acceso a la cerradura electrónica de puerta 20 a corta distancia y recibe a cambio la consulta de autenticación, que se retransmite al segundo embaucador. El dispositivo inalámbrico del segundo embaucador retransmite la consulta de autenticación al dispositivo de comunicación inalámbrica 100 del huésped. El dispositivo de comunicación inalámbrica 100 del huésped puede responder con la respuesta correcta de autenticación, que recibe entonces el dispositivo inalámbrico del segundo embaucador y lo retransmite al primer embaucador. El dispositivo inalámbrico del primer embaucador retransmite entonces la respuesta de autenticación a la cerradura electrónica de puerta 20, obteniendo con ello el acceso a la habitación del hotel del huésped. Tal fraude puede ser perpetrado aunque el huésped esté a kilómetros de distancia del hotel.

No hay forma de que el dispositivo comunicación inalámbrica 100 del huésped distinga una consulta de autenticación reenviada desde una consulta directa desde la cerradura electrónica de puerta 20 basándose en características de la señal. La consulta de autenticación transmitida por la cerradura electrónica de puerta 20 puede ser reproducida con exactitud y retransmitida al dispositivo de comunicación inalámbrica 100 a largas distancias. Del mismo modo, no hay forma de que la cerradura electrónica de puerta 20 distinga una respuesta de autenticación retransmitida de una respuesta directa basándose en características de la señal. Por lo tanto, se debe aplicar un protocolo para impedir tales intentos fraudulentos. Las siguientes medidas de seguridad se pueden incorporar para dificultar el fraude con la ayuda involuntaria de un dispositivo de comunicación inalámbrica 100 autorizado.

1. El dispositivo de comunicación inalámbrica 100 autorizado no debe responder a una consulta de autenticación a menos que haya sido realizada por el usuario al transmitir una solicitud de acceso.
2. El dispositivo de comunicación inalámbrica 100 autorizado no debe responder automáticamente a una consulta

de autenticación a menos que el usuario indique que debe hacerlo así, por ejemplo, pulsando una tecla "sí" en respuesta a una pregunta del dispositivo de comunicación inalámbrica 100.

3. El dispositivo de comunicación inalámbrica 100 autorizado no debe transmitir una solicitud de acceso hasta que el usuario haya introducido un código de seguridad, tal como un código PIN. Por otra parte, durante un preámbulo en el protocolo para establecer inicialmente la comunicación con la cerradura electrónica de puerta 20, el usuario puede ser solicitado para que introduzca un código de seguridad en un punto adecuado antes de continuar.

4. El dispositivo de comunicación inalámbrica 100 autorizado puede mostrar una indicación de que se ha establecido la comunicación con la cerradura electrónica de puerta 20, que sería una sorpresa para el usuario si está a kilómetros de distancia del hotel.

5. La cerradura electrónica de puerta 20 puede poner límites al retardo de tiempo a la recepción de una respuesta de autenticación después de emitir una consulta de autenticación, lo suficientemente corto como para obstaculizar los intentos de retransmitir la consulta de autenticación a un dispositivo remoto autorizado. Se podría diseñar un algoritmo de cálculo de la respuesta de autenticación de modo que ningún cálculo parcial pueda comenzar ventajosamente hasta la recepción del último bit de la consulta que se va a transmitir. La respuesta de autenticación se debe calcular tan rápido como sea posible y transmitirla tan pronto como sea posible a partir de entonces, lo que permite que se especifiquen y se impongan los menores límites al retardo.

6. El protocolo de comunicación de salto de frecuencia BLUETOOTH dificulta intrínsecamente intentos de fraude por su configuración de emplear para cada enlace, únicamente una secuencia de frecuencia aleatoria, ad hoc. Si es necesario, la cerradura electrónica de puerta 20 y el dispositivo de comunicación inalámbrica 100 autorizado pueden hacer que la respuesta de autenticación dependa de alguna manera de un parámetro que describa la secuencia del salto de frecuencia. Este procedimiento requeriría que los dispositivos fraudulentos Introdujeran esencialmente retardo cero, lo cual es muy difícil cuando se tiene que operar bl-direccionalmente utilizando división dúplex en el tiempo.

Con cualquiera o con todas las garantías anteriores, el huésped puede estar protegido en contra de que abran, sin saberlo, la puerta desde una ubicación remota.

La invención anterior se ha descrito con respecto a una aplicación típica en el negocio hotelero en el que a los huéspedes temporales se les otorga acceso a las habitaciones durante un período determinado. Sin embargo, la invención se puede usar en cualquier circunstancia en que se requiera que una persona o dispositivo sea autorizado para realizar funciones, tener acceso físico a zonas o tener acceso electrónico a la información y la autorización pueda ser controlada por un miembro autorizado, incluida la limitación de la zona o el periodo el tiempo a los cuales se concede tal autorización. Tales variaciones de la invención caen dentro del alcance de la invención tal como se describe en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de habilitar o activar una tarea de protección, comprendiendo el método:

almacenar una pluralidad de códigos de autorización y las indicaciones de tiempo asociadas en un dispositivo de comunicación inalámbrica (100), en el que los códigos de autorización y las indicaciones de tiempo asociadas se reciben en el dispositivo de comunicación inalámbrica de un controlador central (40), indicando cada indicación de tiempo un período de tiempo para el correspondiente código de autorización durante el cual es válida la utilización;
calcular los códigos de autorización para diferentes períodos de tiempo utilizando un código maestro almacenado en un dispositivo de control de acceso;
transmitir una petición de acceso desde el dispositivo de comunicación inalámbrica al dispositivo de control de accesos; recibir la petición de acceso desde el dispositivo de comunicación inalámbrica en el dispositivo de control de accesos; transmitir una consulta de autenticación desde el dispositivo de control de accesos al dispositivo de comunicación inalámbrica en respuesta a la petición de acceso;
recibir la consulta de autenticación desde el dispositivo de control de accesos en el dispositivo de comunicación inalámbrica en respuesta a la petición de acceso;
calcular una respuesta de autenticación basándose en la consulta de autenticación y en el código de autorización apropiado para el periodo actual de tiempo; y
transmitir la respuesta de autenticación desde el dispositivo de comunicación inalámbrica al dispositivo de control de accesos;
recibir la respuesta de autenticación basándose en la consulta de autenticación y en el código de autorización para el periodo de tiempo actual;
calcular una respuesta de autenticación esperada basándose en la consulta de autenticación y en el código de autorización apropiado para el período de tiempo actual;
comparar la respuesta de autenticación recibida con la respuesta de autenticación esperada; y
generar una señal de control para permitir el acceso a la tarea de protección si la respuesta de autenticación recibida coincide con la respuesta de autenticación esperada.

2. El método de la reivindicación 1, en el que cada uno de los códigos de autorización está asociado a un período diferente de tiempo.

3. El método de las reivindicaciones 1 o 2, en el que la tarea de protección es desbloquear una puerta.

4. El método de cualquiera de las reivindicaciones 1 a 3, en el que calcular una respuesta de autenticación basándose en la consulta de autenticación y en el código de autorización comprende combinar partes seleccionadas de la consulta de autenticación y del código de autorización con una función no reversible.

5. El método de cualquiera de las reivindicaciones 1 a 4, en el que la consulta de autenticación incluye al menos un número aleatorio y en el que calcular la respuesta de autenticación basándose en la consulta de autenticación y en el código de autorización comprende combinar el número aleatorio de la consulta de autenticación y el código de autorización.

6. El método de cualquiera de las reivindicaciones 1 a 5 que comprende además almacenar los códigos de autorización recibidos en el dispositivo de control de accesos.

7. El método de la reivindicación 6, en el que almacenar los códigos de autorización calculados en el dispositivo de control de accesos comprende almacenar una pluralidad de códigos de autorización en el dispositivo de control de accesos, siendo válido cada código de autorización para un periodo de tiempo definido.

8. El método de cualquiera de las reivindicaciones 1 a 7, que comprende además calcular los códigos de autorización basándose en una combinación del código maestro y de una indicación de la hora.

9. Un sistema para habilitar o activar una tarea de protección, comprendiendo el sistema un dispositivo de comunicación inalámbrica (100) que incluye:

almacenar en memoria una pluralidad de códigos de autorización e indicaciones de hora asociadas en el dispositivo de comunicación inalámbrica (100), en el que los códigos de autorización y las indicaciones de hora asociadas se reciben en el dispositivo de comunicación inalámbrica desde un controlador central (40), indicando cada indicación de la hora un periodo de tiempo para el correspondiente código de autorización durante el cual es válido el código de autorización;

un transmisor inalámbrico adaptado para transmitir una petición de acceso y una respuesta de autenticación a un dispositivo de control de accesos (20);
un receptor inalámbrico adaptado para recibir una consulta de autenticación del dispositivo de control de accesos como respuesta a la petición de acceso;
un procesador adaptado para calcular una respuesta de autenticación basándose en la consulta de autenticación y en el código de autorización apropiado para el periodo de tiempo actual; y
estando además el transmisor inalámbrico adaptado para transmitir la respuesta de autenticación desde el dispositivo de comunicación inalámbrica al dispositivo de control de accesos, comprendiendo además el sistema un dispositivo de control de accesos (20) para asegurar una tarea de protección, incluyendo el dispositivo de control de accesos:

un transceptor inalámbrico para comunicarse con el dispositivo de comunicación inalámbrica;
un procesador programado para:

calcular códigos de autorización para diferentes periodos de tiempo usando un código maestro almacenado en el dispositivo de control de accesos;
recibir la petición de acceso del dispositivo de comunicación inalámbrica en el dispositivo de control de accesos; transmitir la consulta de autenticación del dispositivo de control de accesos al dispositivo de comunicación inalámbrica en respuesta a la petición de acceso;
recibir la respuesta de autenticación basándose en la consulta de autenticación y en el código de autenticación para el periodo de tiempo actual;
calcular una respuesta de autenticación esperada basándose en la consulta de autenticación y en el código de autorización apropiado para el período de tiempo actual;
comparar la respuesta de autenticación recibida con la respuesta de autenticación esperada; y
generar una señal de control para permitir el acceso a la tarea de protección si la respuesta de autenticación esperada coincide con la respuesta de autenticación recibida.

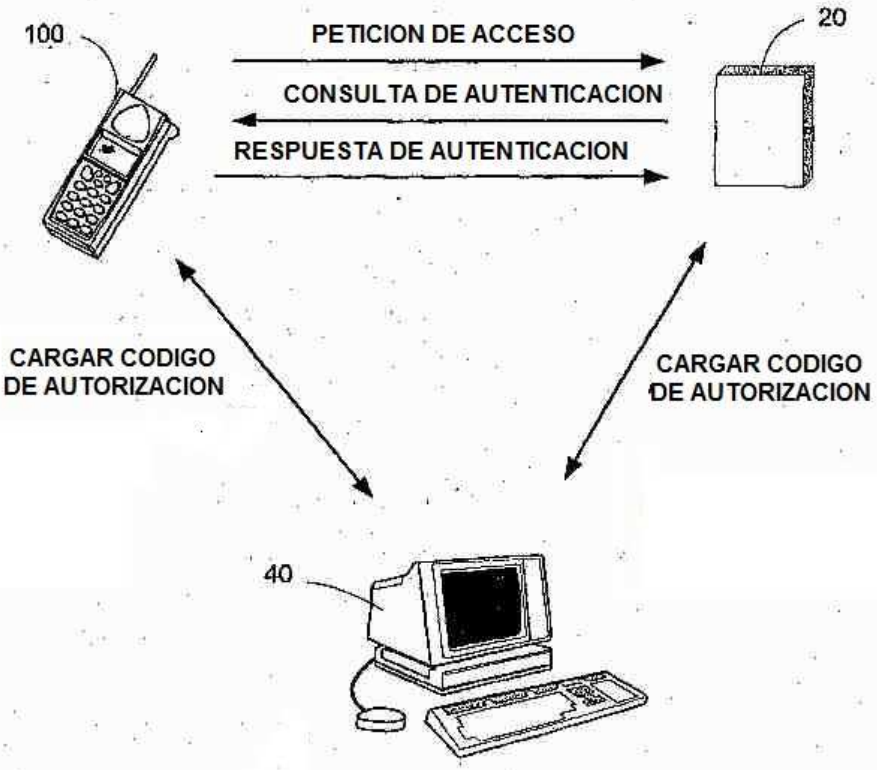
100
PETICION DE ACCESO
20
CONSULTA DE AUTENTICACION
RESPUESTA DE AUTENTICACION
CARGAR CODIGO
DE AUTORIZACION
CARGAR CODIGO
DE AUTORIZACION
40

FIG. 1

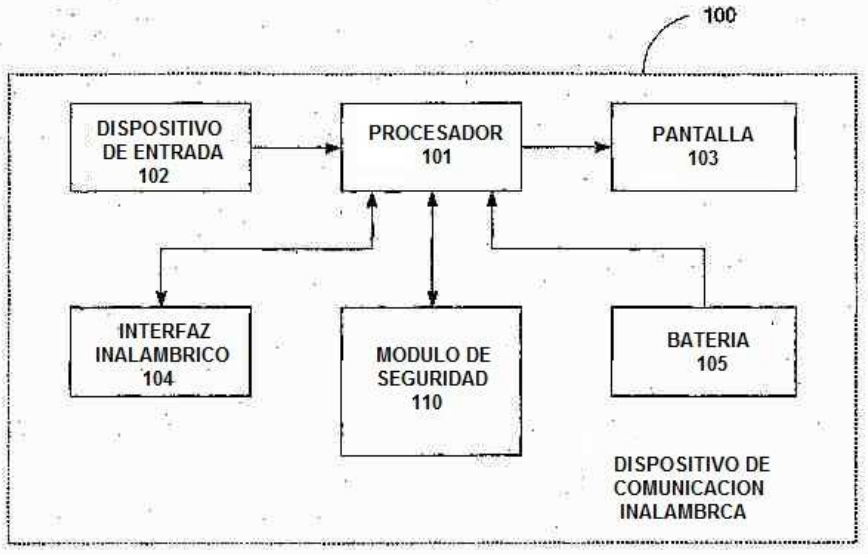
100
DISPOSITIVO DE ENTRADA 102
PROCESADOR 101
PANTALLA 103
INTERFAZ INALAMBRICO 104
MODULO DE SEGURIDAD 110
BATERIA 105
DISPOSITIVO DE COMUNICACION INALAMBRCA

FIG. 2

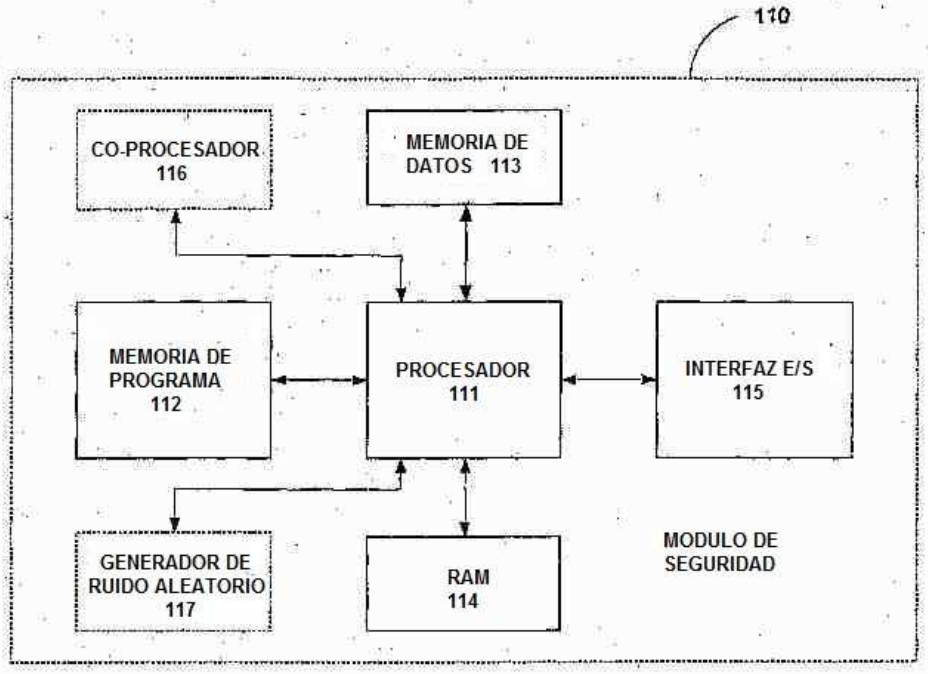
110
CO-PROCESADOR
116
MEMORIA DE
DATOS 113
MEMORIA DE
PROGRAMA
112
PROCESADOR
111
INTERFAZ E/S
115
GENERADOR DE
RUIDO ALEATORIO
117
RAM
114
MODULO DE
SEGURIDAD

FIG. 3

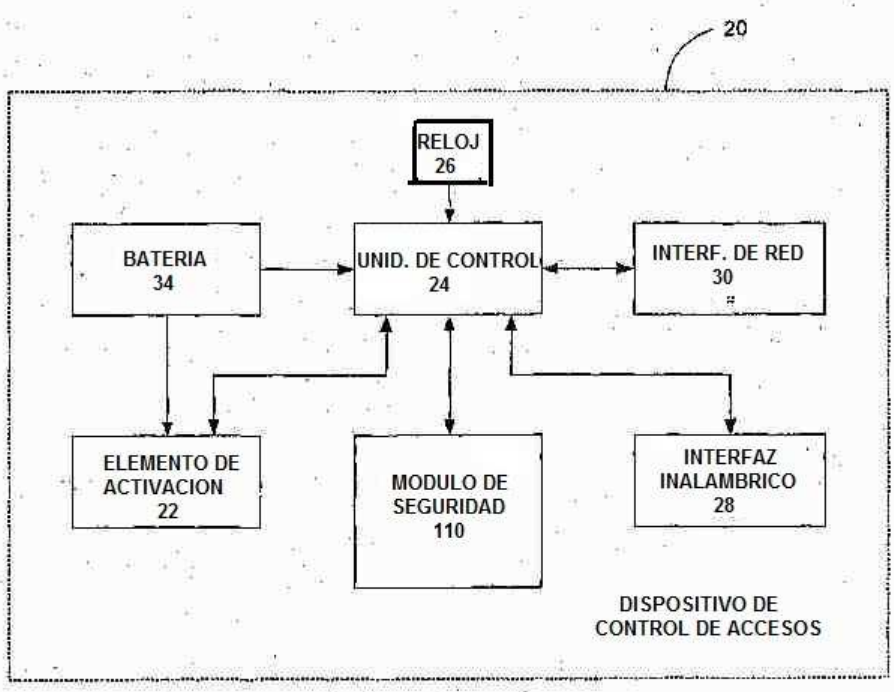
20
RELOJ
26
BATERIA
34
UNID. DE CONTROL
24
INTERF. DE RED
30
ELEMENTO DE
ACTIVACION
22
MODULO DE
SEGURIDAD
110
INTERFAZ
INALAMBRICO
28
DISPOSITIVO DE
CONTROL DE ACCESOS

FIG. 4

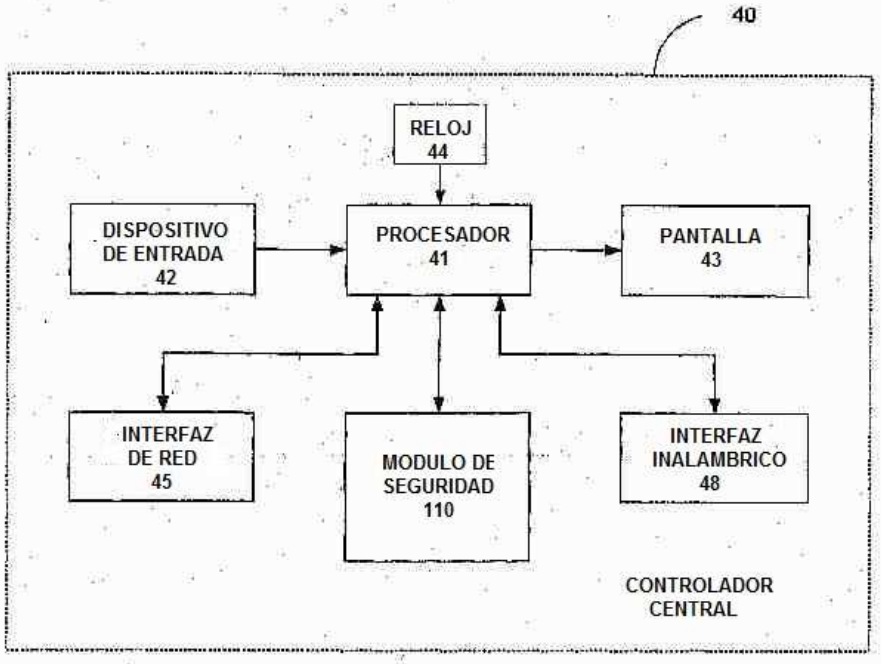
40
RELOJ
44
DISPOSITIVO
DE ENTRADA
42
PROCESADOR
41
PANTALLA
43
INTERFAZ
DE RED
45
MODULO DE
SEGURIDAD
110
INTERFAZ
INALAMBRICO
48
CONTROLADOR
CENTRAL

FIG. 5