(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 976 646**

(51) Int. Cl.:

G07C 9/00 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.09.2015 PCT/IB2015/001926**

(87) Fecha y número de publicación internacional: **17.03.2016 WO16038457**

(96) Fecha de presentación y número de la solicitud europea: **09.09.2015 E 15788185 (5)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2024 EP 3192059**

(54) Título: **Notificación de primera entrada**

(30) Prioridad:

10.09.2014 US 201462048702 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.08.2024

(73) Titular/es:

ASSA ABLOY AB (100.0%)
P.O. Box 70340
107 23 Stockholm, SE

(72) Inventor/es:

AASE, HALVOR

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Notificación de primera entrada

Referencia cruzada a solicitudes relacionadas

La presente solicitud reivindica el beneficio de la solicitud de Patente Provisional de EE. UU. n.º 62/048 702, presentada el 10 de septiembre de 2014.

Campo de la descripción

La presente descripción está dirigida generalmente a un método para operar un sistema de control de acceso.

Antecedentes

Una tarjeta inteligente, una tarjeta con chip o una tarjeta de circuito integrado (ICC) es cualquier tarjeta de bolsillo con circuitos integrados incorporados. Las tarjetas inteligentes se fabrican tradicionalmente de plástico. Un uso común para las tarjetas inteligentes es la seguridad de hoteles y similares.

Los hoteles y otras instalaciones con varias habitaciones suelen emplear sistemas de gestión de la propiedad independientes de los sistemas de control de acceso usados para proteger físicamente las habitaciones de las instalaciones. Por ejemplo, los hoteles tradicionalmente usan sus sistemas de gestión de la propiedad para gestionar y asignar habitaciones a los huéspedes y para realizar un seguimiento de transacciones tales como las compras de los huéspedes en restaurantes, servicio de aparcacoches, minibar y otras compras en la habitación. Por lo general, se crea una nueva cuenta de huésped en el sistema de gestión de la propiedad por habitación durante el registro de los huéspedes en la recepción del hotel. Los documentos EP2736021A2 y WO2014/007870A1 describen métodos de registro en un hotel según la técnica anterior. El documento WO97/45614A1 describe un método para configurar un bloqueo.

Compendio

En entornos donde un huésped puede evitar el proceso de registro en la recepción, el hotel enfrenta nuevos desafíos. Uno de estos desafíos está asociado con completar los procedimientos de registro de los huéspedes en el sistema de gestión de la propiedad, aunque el huésped nunca llegue a la recepción para registrarse. Es deseable permitir a los huéspedes evitar la recepción para que la experiencia del huésped sea mejor y menos onerosa desde el punto de vista administrativo. Sin embargo, sin que el huésped llegue a la recepción, debe haber una manera de comunicar el registro del huésped al sistema de administración de la propiedad desde el sistema de control de acceso, aunque los dos sistemas sean sistemas separados y discretos.

Por lo tanto, se presenta un método según la reivindicación 1 adjunta, para permitir que un sistema de control de acceso detecte, registre y distribuya automáticamente información sobre la primera vez que una llave electrónica determinada llega u obtiene acceso.

Una 'cerradura en línea' es una cerradura con capacidad de red incorporada, que le permite informar automáticamente eventos al sistema de control de acceso. Los eventos típicos pueden ser el uso de llaves, la apertura de puertas, etc. Las redes típicas usadas pueden ser Ethernet cableadas o inalámbricas, redes de radiofrecuencia, etc.

Por el contrario, una "cerradura fuera de línea" es una cerradura que no tiene dicha capacidad de red, por lo tanto, no hay medios previos para informar automáticamente el evento de bloqueo al sistema de control de acceso.

Aunque los ejemplos de la presente descripción se discutirán principalmente en relación con los sistemas de control de acceso de un hotel o un tipo similar de instalación de varias habitaciones, se debe apreciar que las realizaciones de la presente descripción no están tan limitadas. Como algunos ejemplos no limitantes, las realizaciones de la presente descripción podrían usarse en los siguientes tipos de sistemas de control de acceso: hotel (ha llegado un huésped a su habitación); residencial (ha llegado un trabajador a una casa); oficina (ha llegado un miembro del personal para empezar a trabajar), etc.

En un ejemplo específico de un hotel que implementa realizaciones de la presente descripción, pueden ocurrir los siguientes pasos: (1) el operador del hotel organiza para que el sistema de gestión de la propiedad en un hotel solicite la generación de una clave de acceso a la habitación para un huésped; (2) se genera una clave electrónica y se envía a la aplicación del sistema de control de acceso en el teléfono/dispositivo móvil de ese huésped; (3) el huésped llega al hotel y presenta el teléfono para desbloquear la cerradura correspondiente; (4) la información (por ejemplo, Identificador de habitación/Éxito/Primer uso/etc.) se envía de vuelta a la aplicación del teléfono; (5) la aplicación del teléfono envía la información anterior a la parte de origen del sistema de control de acceso; y luego (6) la información también se distribuye al operador del hotel. Una vez recibida por el operador del hotel, la información puede almacenarse en la base de datos del sistema de gestión de la propiedad potencialmente junto con otra información (por ejemplo, qué red transportó la clave electrónica e información de acceso durante (5) hacia/desde el dispositivo móvil). Debe apreciarse que, en algunas realizaciones, algunos de los pasos enumerados anteriormente se pueden

realizar de forma concurrente/simultánea en lugar de secuencialmente. Como ejemplo no limitante, los pasos (4), (5) y/o (6) pueden ocurrir durante la misma transacción que se usa para (3) en donde el huésped presenta su teléfono en la cerradura apropiada, obviando así la necesidad de que el huésped presente su teléfono en la cerradura varias veces.

La presente invención se comprenderá mejor a partir de los dibujos y de la siguiente descripción detallada. Aunque esta descripción establece detalles específicos, se entiende que ciertas realizaciones de la invención pueden practicarse sin estos detalles específicos. También se entiende que, en algunos casos, los circuitos, componentes y técnicas bien conocidos no se han mostrado en detalle para evitar oscurecer la comprensión de la invención.

Breve descripción de los dibujos

La presente descripción se describe junto con las figuras adjuntas:

la Fig. 1 es un diagrama de bloques que representa un sistema de comunicación según realizaciones de la presente descripción;

la Fig. 2 es un diagrama de bloques que representa componentes de un dispositivo móvil según al menos algunas realizaciones de la presente descripción;

la Fig. 3 es un diagrama de bloques que representa los componentes de una cerradura/lector según al menos algunas realizaciones de la presente descripción;

la Fig. 4 es un diagrama de flujo que representa un método para generar y entregar claves a un dispositivo móvil según un ejemplo que no forma parte de la presente invención;

la Fig. 5 es un diagrama de flujo que representa un método para reportar los primeros datos de interacción según realizaciones de la presente descripción;

la Fig. 6 es un diagrama de flujo que representa un método de distribución de primeros datos de interacción según un ejemplo que no forma parte de la presente invención;

la Fig. 7 es un diagrama de flujo que representa los pasos para usar una ruta de entrega de claves y una ruta inversa de entrega de claves según un ejemplo que no forma parte de la presente invención;

la Fig. 8 es un diagrama de flujo que representa un método para realizar procesos de registro en respuesta a recibir una indicación de primera entrada en un sistema de gestión de la propiedad según un ejemplo que no forma parte de la presente invención; y

la Fig. 9 es un diagrama de flujo que representa un método para producir un informe de registro directo a la habitación según un ejemplo que no forma parte de la presente invención.

Descripción detallada

La siguiente descripción proporcionará varias realizaciones o características de un sistema, que puede incluir un sistema de control de acceso que facilita las interacciones entre múltiples componentes. Si bien las realizaciones de la presente descripción se analizan en relación con un sistema de control de acceso que interactúa con un sistema de gestión de la propiedad de un hotel o similar, se debe apreciar que las realizaciones de la presente descripción no están tan limitadas.

Con referencia ahora a las Fig. 1-9, se describirán diversos detalles y características relacionados con un sistema de control de acceso y métodos para operar el mismo según al menos algunas realizaciones de la presente descripción. Con referencia inicial a la Fig. 1, se describirá un sistema 100 de comunicación según al menos algunas realizaciones de la presente descripción. Se muestra que el sistema 100 incluye una o múltiples redes 104 de comunicación, una red 108 de control de acceso y una red 112 de confianza opcional. Aunque se representa como dos redes separadas y distintas, se debe apreciar que las redes 104 de comunicación pueden implementarse como una red única. Asimismo, aunque la red 104 y la red 112 de confianza se representan como redes separadas, se debe apreciar que las redes pueden combinarse o una red (por ejemplo, la red 112 de confianza) puede superponerse sobre la red de comunicación 104, a través de un túnel de comunicación. (por ejemplo, una Red Privada Virtual (VPN), una Red de Área Amplia (WAN) o similar). Por lo tanto, la red 104 de comunicación puede incluir una red 112 de confianza superpuesta a ella sin salirse del alcance de la presente descripción.

La red 108 de control de acceso puede proporcionar conectividad entre uno o más servidores 140 de control de acceso y una pluralidad de lectores 128, dispositivos 148 de registro y otros componentes de un sistema de control de acceso. Por tanto, la red 108 de control de acceso puede permitir la administración e implementación de un Sistema de Control de Acceso Físico (PACS) o similar. La red 108 de control de acceso puede usar cualquier tipo de protocolo de comunicación conocido para transportar información entre componentes conectados a la misma. Los ejemplos no limitantes de los protocolos o redes que pueden usarse dentro de la red 108 de control de acceso incluyen RS-232, RS-485, Wiegand, Ethernet, Alimentación sobre Ethernet (PoE), ZigBee, Wi-Fi (por ejemplo, IEEE 802.11, variantes

del mismo, o extensiones del mismo), una red de Protocolo de Internet (IP), o cualquier otro tipo de protocolo por cable o inalámbrico.

La red 104 de comunicación puede corresponder a una red de comunicación privada, semiprivada o pública usada para transportar información entre dispositivos de comunicación compatibles. En algunas realizaciones, la red 104 de comunicación puede corresponder a una red de comunicación no confiable o no segura. Los ejemplos no limitantes de una red 104 de comunicación incluyen una red telefónica, una red móvil, una red IMS, una Red de Área Amplia (por ejemplo, Internet), una Red de Área Local, una red IP, una red SNMP o cualquier otro tipo de arquitectura de red conocida. . Uno o más de mensajes de correo electrónico, mensajes SMS, mensajes MMS, mensajes SNMP, mensajes transmitidos usando HTTP o SHTTP o variantes de los mismos, mensajes intercambiados usando FTP, mensajes intercambiados usando RTP o UDP, o similares, pueden usarse para transportar información entre un servidor 140 de control de acceso y un dispositivo 116 móvil. En algunas realizaciones, también se puede usar Voz sobre IP (VoIP) o similar para transportar información entre el servidor 140 de control de acceso y el dispositivo 116 móvil.

El lector 128 puede corresponder a cualquier tipo de dispositivo de interacción o conjunto de dispositivos de interacción que limiten o controlen el acceso a uno o más activos protegidos. El lector 128, en algunas realizaciones, puede configurarse para intercambiar comunicaciones directamente con un dispositivo 116 móvil a través de un canal 136 de comunicaciones. El canal 136 de comunicaciones puede ser un canal de comunicaciones sin contacto en algunas realizaciones. El canal 136 de comunicaciones puede ser alternativa o adicionalmente un canal de comunicaciones basado en contacto. En algunas realizaciones, se puede usar radiación electromagnética en forma de ondas de Radiofrecuencia (RF) para transportar información en el canal 136 de comunicaciones. Alternativa o adicionalmente, el canal 136 de comunicaciones puede usar un medio de luz, magnético, acústico o cualquier otro medio para transportar información entre el lector 128 y el dispositivo 116 móvil. El canal 136 de comunicación también puede caracterizarse por el protocolo de comunicación usado para intercambiar información. En algunas realizaciones, la modulación de señal (por ejemplo, modulación de amplitud, modulación de frecuencia, modulación de fase, combinaciones de las mismas, variantes de las mismas o similares) se usa para comunicar datos entre el lector 128 y el dispositivo 116 móvil. Algunos ejemplos no limitantes del protocolo o protocolos que se usan en el canal 136 de comunicación incluyen protocolos definidos en la ISO 14443, ISO 15693, ISO 18092, FeliCa, Comunicaciones de Campo Cercano (NFC), Bluetooth, Wi-Fi (por ejemplo, 802.11N, variantes del mismo o extensiones del mismo), ZigBee, GSM, combinaciones de los mismos, etc. Debe apreciarse además que dependiendo de las capacidades del dispositivo 116 móvil y del lector 128, puede ser posible establecer múltiples canales 136 de comunicación entre los dispositivos. Por ejemplo, el lector 128 y el dispositivo 116 móvil pueden establecer un primer canal de comunicación usando un primer protocolo (por ejemplo, Bluetooth o Bluetooth de Baja Energía (BLE)) así como un segundo canal de comunicación usando un segundo protocolo (por ejemplo, NFC, infrarrojos, o similar). Debe apreciarse que el canal 136 de comunicación puede corresponder a un canal de comunicación basado en proximidad que sólo puede crearse cuando el dispositivo 116 móvil y el lector 128 están a una distancia predeterminada entre sí (por ejemplo, menos de 0,5 metros para NFC, menos de 50 metros para BLE, o menos de 200 metros para Wi-Fi). El canal 136 de comunicación puede caracterizarse además por el protocolo de autenticación usado por los dispositivos (por ejemplo, el lector 128 y el dispositivo 116 móvil) para autenticarse entre sí. Ejemplos de protocolos de autenticación que pueden usarse en el canal 136 de comunicación incluyen SEOS y FIDO.

Aunque el término "lector" se usa en el presente documento para referirse a un dispositivo o conjunto de dispositivos usados para controlar el acceso a un activo protegido (por ejemplo, un activo físico como la puerta de una habitación, una caja fuerte, etc.), se debe apreciar que los términos "lector", "bloqueo" y similares pueden usarse indistintamente. Por ejemplo, un lector 128 en red como se muestra en la Fig. 1 también puede denominarse "cerradura en línea". De manera similar, como se explicará con más detalle en el presente documento, un lector 132 fuera de la red puede denominarse sinónimamente "cerradura fuera de línea". En otras palabras, el uso del término "cerradura", "lector" y otros términos similares puede usarse para describir un dispositivo electromecánico o un conjunto de dispositivos que se usan para proteger y asegurar un activo, tal como un activo físico. Además, el lector o candado como se analiza en el presente documento puede usarse para proteger y asegurar activos lógicos, como cuentas bancarias, recursos de redes informáticas y similares.

Además del lector 128 tradicional que se representa conectado a una red 108 de control de acceso, el sistema 100 de comunicación también incluye uno o más lectores 132 no conectados en red o "cerraduras fuera de línea". Los lectores 132 no conectados en red pueden diferir de los lectores 128 en que los lectores 132 no conectados en red pueden no estar conectados de forma nativa o persistente a la red 108 de control de acceso, lo que posteriormente limita la capacidad del lector 132 no conectado en red para comunicarse con los servidores 140 de control de acceso u otros dispositivos según las necesidades. En consecuencia, las realizaciones de la presente descripción sugieren usar el canal 136 de comunicación para facilitar la comunicación de información desde el lector 132 no conectado en red al dispositivo 116 móvil y eventualmente de regreso a los servidores 140 de control de acceso y otros dispositivos. Por lo tanto, los componentes del lector 132 no conectado en red pueden ser similares o idénticos a los del lector 128 excepto que una interfaz de comunicación con la red 108 de control de acceso puede faltar en el lector 132 no conectado en red o dicha interfaz puede estar deshabilitada/no ser utilizada.

El dispositivo 116 móvil puede corresponder a cualquier tipo de dispositivo electrónico y, como sugiere el nombre, el dispositivo electrónico puede ser de naturaleza portátil. Como algunos ejemplos, el dispositivo 116 móvil puede corresponder a un teléfono móvil o teléfono inteligente llevado por un usuario. Otros ejemplos de un dispositivo 116 móvil incluyen, sin limitación, dispositivos portátiles (por ejemplo, gafas, relojes, zapatos, ropa, joyas, pulseras, pegatinas, etc.). El dispositivo 116 móvil, como se muestra en la Fig. 1, puede estar provisto de una aplicación 120 de control de acceso que almacena una o una pluralidad de claves 124. La clave o claves 132 pueden comunicarse a un lector 128, 132 en conexión con un titular del dispositivo 116 móvil que intenta obtener acceso a un activo protegido por el lector 128, 132. Como ejemplo, el dispositivo 116 móvil puede ser presentado al lector 128, 132 por un usuario o titular del dispositivo 116 móvil.

En algunas realizaciones, la clave o claves 124 pueden entregarse al dispositivo 116 móvil desde el servidor 140 de control de acceso a través de la red 104 de comunicación. En otras realizaciones, la clave o claves 124 pueden entregarse al dispositivo 116 móvil a través de un dispositivo 148 de registro, que recibe las claves desde el servidor o servidores 140 de control de acceso a través de la red 108 de control de acceso. Detalles adicionales del primer mecanismo de entrega de claves se describen en los documentos de Patente de EE.UU. n.º 8,074,271 para Davis et al. y Patente de EE.UU. n.º 7,706,778 para Lowe. Detalles adicionales del segundo mecanismo de entrega de claves (por ejemplo, el uso del dispositivo 148 de registro) se describen en el documento de Patente de EE.UU. n.º 8,730,004 para Elfstrom et al. Los módulos de control de acceso descritos en la patente '004 pueden tener características similares a los lectores 128, 132 descritos en el presente documento. Además, los comportamientos de comunicación y conexión en red de los lectores 128 pueden ser similares a los dispositivos padre e hijo descritos en el documento de Patente de EE.UU. n.º 8,102,799 para Alexander et al.

Si se usa NFC para el canal 136 de comunicación, entonces el lector 128, 132 y el dispositivo 116 móvil pueden tener sus interfaces/antenas acopladas inductivamente entre sí, momento en el cual el lector y/o el dispositivo 116 móvil se autenticarán o se autenticarán mutuamente el uno con el otro. Después de la autenticación, el lector 128, 132 puede solicitar una clave 124 o múltiples claves desde el dispositivo 116 móvil o el dispositivo 116 móvil puede ofrecer una clave 124 o múltiples claves al lector 128, 132. A la clave o claves 124 del dispositivo 116 móvil, el lector 128, 132 puede analizar la clave o claves 124 y determinar si la clave o claves 124 son válidas y, de ser así, permitir al titular/usuario del dispositivo 116 móvil acceder al activo protegido por el lector 128, 132. Debe apreciarse que el dispositivo 116 móvil puede configurarse alternativa o adicionalmente para analizar información recibida desde el lector 128, 132 en relación con la toma de una decisión de control de acceso y/o en relación con la toma de una decisión sobre si proporcionar o no la clave o claves 124 al lector 128, 132.

Si se usa BLE o algún otro protocolo no inductivo (por ejemplo, Wi-Fi) para el canal 136 de comunicación, entonces el lector 128, 132 y el dispositivo 116 móvil pueden realizar una rutina de descubrimiento antes de emparejarse entre sí o conectarse de otro modo a establecer el canal 136 de comunicación. Sin embargo, una vez establecido el canal 136, el lector 128, 132 y el dispositivo 116 móvil pueden entonces autenticarse entre sí e intercambiar información relevante, tal como la clave o claves 124, para permitir que se tome una decisión de control de acceso. Si se toma una decisión positiva de control de acceso (por ejemplo, se determina que la clave o claves 124 son válidas y se permite que el dispositivo 116 móvil acceda al activo protegido por el lector 128, 132), entonces el lector 128, 132 puede iniciar una o más acciones para permitir que el titular/usuario del dispositivo 116 móvil acceda al activo protegido por el lector 128, 132.

Como se analizará con mayor detalle en el presente documento, el envío de información desde un lector 128 en red al servidor 140 de control de acceso y/o a un sistema 144 de gestión de la propiedad es relativamente sencillo. Por ejemplo, cuando un usuario presenta un dispositivo 116 móvil a un lector 128, la información relativa a dicho intercambio puede proporcionarse desde el lector 128 a un servidor de control de acceso 140 o al sistema 144 de gestión de la propiedad a través de la red 108 de control de acceso. Por otro lado, un lector 132 no conectado en red no tiene la capacidad nativa de reportar el mismo tipo de información directamente a los servidores 140 de control de acceso o al sistema 144 de gestión de la propiedad. En consecuencia, puede ser deseable que el lector 132 no conectado en red aproveche el canal 136 de comunicación como un mecanismo para comunicar la información con respecto a una primera interacción (o primer uso de clave o alguna otra información transaccional) de regreso a un servidor 140 de control de acceso o sistema 144 de gestión de la propiedad. Además, una vez que el dispositivo 116 móvil (o más específicamente la aplicación 120 de control de acceso que se ejecuta en el dispositivo 116 móvil) está en posesión de los datos de interacción del lector 132 no conectado en red, el dispositivo 116 móvil puede decidir si reportar la información a los servidores 140 de control de acceso a través de la red 104 de comunicación o si la red 112 de confianza puede y debe utilizarse para reportar la información directamente al sistema 144 de gestión de la propiedad. Como ejemplo no limitante, el lector 132 no conectado en red puede dictar al dispositivo 116 móvil que la red 112 de confianza debe usarse para transmitir los datos de interacción de regreso al sistema 114 de gestión de la propiedad, ya que la red 112 de confianza puede estar bajo el control de la entidad que administra el sistema 144 de gestión de la propiedad (por ejemplo, el operador del hotel). En algunas realizaciones, los datos de interacción pueden ser reportados simultáneamente por un dispositivo 116 móvil tanto al servidor o servidores 140 de control de acceso como a los sistemas de gestión de la propiedad a través de la red 104 de comunicación y la red 112 de confianza (a través de dos mensajes de reporte).

Con referencia ahora a la Fig. 2, se describirán detalles adicionales de un dispositivo 116 móvil según al menos algunas realizaciones de la presente descripción. Se muestra que el dispositivo 116 móvil incluye una memoria 204 informática que almacena uno o más sistemas operativos 208 (O/S) y claves 212, entre otros elementos. También se muestra que el dispositivo 116 móvil incluye un procesador 216, uno o más controladores 220, una interfaz 224 de usuario, una interfaz 228 de lector, una interfaz 232 de red y un módulo 236 de alimentación. Los ejemplos adecuados de un dispositivo 116 móvil incluyen, sin limitación, teléfonos inteligentes, PDA, ordenadores portátiles, PC, tabletas, mini ordenadores, dispositivos portátiles y similares.

La memoria 204 puede corresponder a cualquier tipo de medio no transitorio legible por ordenador. En algunas realizaciones, la memoria 204 puede comprender memoria volátil o no volátil y un controlador para la misma. Los ejemplos no limitantes de memoria 204 que pueden utilizarse en el dispositivo 116 móvil incluyen RAM, ROM, memoria intermedia, memoria flash, memoria de estado sólido o variantes de las mismas.

El O/S 208 puede corresponder a uno o múltiples sistemas operativos. La naturaleza del O/S 208 puede depender del hardware del dispositivo 116 móvil y del factor de forma del dispositivo 116 móvil. El O/S 208 puede verse como una aplicación almacenada en la memoria 204 que es ejecutable por el procesador. El O/S 208 es un tipo particular de aplicación de propósito general que permite que otras aplicaciones almacenadas en la memoria 204 (por ejemplo, un navegador, una aplicación de correo electrónico, una aplicación de SMS, etc.) aprovechen los diversos componentes de hardware y controlador o controladores 220 del dispositivo 116 móvil. En algunas realizaciones, el O/S 208 puede comprender una o más API que facilitan la interacción de una aplicación con ciertos componentes de hardware del dispositivo 116 móvil. Además, el O/S 208 puede proporcionar un mecanismo para ver y acceder a las diversas aplicaciones almacenadas en la memoria 208 y otros datos almacenados en la memoria 208.

Las claves 212 pueden ser similares o idénticas a las claves 124 representadas en la Fig. 1. En algunas realizaciones, la clave o claves 212 pueden almacenarse en la misma memoria 204 física que el O/S 208. En otras realizaciones, la clave o claves 212 pueden almacenarse en una memoria física del ordenador que está separada de la memoria informática usada para almacenar el O/S 208 y otras aplicaciones. Aún más específicamente, la clave o claves 212 pueden mantenerse en una memoria de informática segura o cifrada, evitando así que las claves contenidas en ella sean obtenidas o manipuladas por partes no autorizadas. El acceso a la clave o claves 212 puede depender de ciertos eventos y/o entradas del usuario. Por ejemplo, se le puede solicitar a un usuario que ingrese una contraseña o PIN válido en la interfaz 224 de usuario para que las claves 212 se distribuyan a un lector 128, 132, por ejemplo.

El procesador 216 puede corresponder a uno o varios microprocesadores que están contenidos dentro de la carcasa del dispositivo 116 móvil con la memoria 204. En algunas realizaciones, el procesador 216 incorpora las funciones de la Unidad 116 Central de Procesamiento (CPU) del dispositivo móvil en un solo Circuito integrado (IC) o algunos chips IC. El procesador 216 puede ser un dispositivo programable multipropósito que acepta datos digitales como entrada, procesa los datos digitales según instrucciones almacenadas en su memoria interna y proporciona resultados como salida. El procesador 216 puede implementar lógica digital secuencial ya que tiene memoria interna. Como ocurre con la mayoría de los microprocesadores conocidos, el procesador 216 puede operar con números y símbolos representados en el sistema numérico binario.

Los controladores 220 pueden corresponder a hardware, software y/o controladores que proporcionan instrucciones específicas a los componentes de hardware del dispositivo 116 móvil, facilitando así su funcionamiento. Por ejemplo, la interfaz 224 de usuario, la interfaz 228 de lector y la interfaz 232 de red pueden tener cada una un controlador 220 dedicado que proporciona señales de control apropiadas para efectuar su operación. Los controladores 220 también pueden comprender el software o los circuitos lógicos que garantizan que los diversos componentes de hardware se controlen de forma adecuada y según los protocolos deseados. Por ejemplo, el controlador 220 de la interfaz 228 de lector puede adaptarse para garantizar que la interfaz 228 de lector siga los protocolos basados en proximidad apropiados (por ejemplo, BLE, NFC, infrarrojos, ultrasónico, IEEE 802.11N, etc.) de modo que la interfaz 228 de lector pueda intercambiar comunicaciones. Asimismo, el controlador 220 de la interfaz 232 de red puede adaptarse para garantizar que la interfaz 232 de red siga los protocolos de comunicación de red apropiados (por ejemplo, TCP/IP (en una o más capas en el modelo OSI), UDP, RTP, GSM, LTE, Wi-Fi, etc.) de modo que la interfaz 232 de red pueda intercambiar comunicaciones a través de la red 104 de comunicación, la red 112 de confianza o similares. Como se puede apreciar, los controladores 220 también pueden configurarse para controlar componentes de hardware cableados (por ejemplo, un controlador USB, un controlador Ethernet, etc.).

Como se mencionó anteriormente, la interfaz 224 de usuario puede comprender uno o más dispositivos de entrada de usuario y/o uno o más dispositivos de salida de usuario. Ejemplos de dispositivos de entrada de usuario adecuados que pueden incluirse en la interfaz 224 de usuario incluyen, sin limitación, botones, teclados, ratón, bolígrafo, cámara, micrófono, etc. Ejemplos de dispositivos de salida de usuario adecuados que pueden incluirse en la interfaz 224 de usuario incluyen, sin limitación, pantallas de visualización, luces, altavoces, etc. Debe apreciarse que la interfaz 224 de usuario también puede incluir un dispositivo combinado de entrada y salida de usuario, tal como un elemento de visualización sensible al tacto o similar.

La interfaz 228 de lector puede corresponder al hardware que facilita las comunicaciones entre el dispositivo 116 móvil y un lector 128, 132. La interfaz 228 de lector puede incluir una interfaz Bluetooth (por ejemplo, antena y circuitos asociados), una interfaz Wi-Fi/802.11N (por ejemplo, una antena y circuitos asociados), una interfaz NFC (por ejemplo, una antena y circuitos asociados), una interfaz de infrarrojos (por ejemplo, LED, fotodiodo y circuitos asociados) y/o una interfaz ultrasónica (por ejemplo, altavoz, micrófono y circuitos asociados). En algunas realizaciones, la interfaz 228 de lector se proporciona específicamente para facilitar las comunicaciones basadas en proximidad a través de un canal 136 de comunicación o múltiples canales 136 de comunicación.

La interfaz 232 de red puede comprender hardware que facilita las comunicaciones con otros dispositivos de comunicación a través de la red 104 de comunicación o la red 112 de confianza. Como se mencionó anteriormente, la interfaz 232 de red puede incluir un puerto Ethernet, una tarjeta Wi-Fi, una tarjeta de interfaz de red (NIC), una interfaz móvil (por ejemplo, antena, filtros y circuitos asociados), o similares. La interfaz 232 de red puede configurarse para facilitar una conexión entre el dispositivo 116 móvil y la red 104, 112 de comunicación y puede configurarse además para codificar y decodificar comunicaciones (por ejemplo, paquetes) según un protocolo utilizado por la red 104, 112 de comunicación.

El módulo 236 de alimentación puede incluir una fuente de alimentación incorporada (por ejemplo, batería) y/o un convertidor de energía que facilita la conversión de energía de CA suministrada externamente en energía de DC que se usa para alimentar los diversos componentes del dispositivo 116 móvil. En algunas realizaciones, el módulo 236 de alimentación también puede incluir alguna implementación de circuitos de protección contra sobretensiones para proteger los componentes del dispositivo 116 móvil contra sobretensiones.

Con referencia ahora a la Fig. 3, se describirán detalles adicionales de un lector 132 no conectado en red según al menos algunas realizaciones de la presente descripción. El lector 132 no conectado en red se representa en la Fig. 3, pero debe apreciarse que se pueden incluir componentes similares en un lector 128 en red. La diferencia entre el lector 128 en red y el lector 132 no conectado en red puede corresponder al hecho de que el lector 128 en red tiene una interfaz de red que conecta el lector 128 a la red 108 de control de acceso, ya sea a través de un canal de comunicación por cable o inalámbrico. Sin embargo, el lector 132 no conectado en red carece de una interfaz de red o dicha interfaz está desactivada o no usada por el lector 132 no conectado en red. En algunas realizaciones, un lector que tiene capacidad de comunicación intermitente, pero no continua, con una red puede considerarse un lector 132 no conectado en red. Por lo tanto, cualquier lector sin la capacidad de comunicarse a través de una red de comunicación bajo demanda puede considerarse un lector 132 no conectado en red.

Se muestra que el lector 132 incluye una memoria 304 informática que almacena la lógica 308 de control de acceso, un registro 312 de uso e información 316 de primer uso, entre otros elementos. También se muestra que el lector 132 incluye un procesador 320, uno o más controladores 324, una interfaz 324 de usuario, una interfaz 332 de credenciales y un módulo 336 de alimentación.

En algunas realizaciones, la lógica 308 de control de acceso se implementa como firmware, aunque también puede ser posible implementar la lógica 308 de control de acceso como software o en un Circuito Integrado de Aplicación Específica (ASIC). En algunas realizaciones, el registro 312 de uso puede contener información sobre las interacciones entre el lector 132 y las credenciales, tales como dispositivos 116 móviles y tarjetas de control de acceso tradicionales o llaveros, que pueden denominarse dispositivos de tipo credencial. El tipo de información que puede almacenarse en el registro 312 de uso incluye fechas y horas de interacciones con dispositivos de tipo credencial, si dichas interacciones correspondieron a una primera o posterior interacción con ese dispositivo en particular, qué clave o claves se usaron durante la interacción, los resultados de la decisión de control de acceso tomada por la lógica 308 de control de acceso, etc. Además del registro 312 de uso, la memoria 304 también puede contener información de un primer uso que es específica de instancias de un primer uso de la clave y/o de instancias de una primera interacción entre un dispositivo de tipo credencial particular y el lector 132.

En algunas realizaciones, una clave 124, 212 puede actualizarse después de haber sido usada por primera vez, permitiendo así que todos los lectores posteriores sepan que no está recibiendo una clave 124, 212 como primera instancia del uso de esa clave en el sistema de control de acceso. Como ejemplo, una clave 124, 212 puede actualizarse con una bandera o marcador después de haber sido entregada por primera vez a un lector 128, 132. Todas las transmisiones o usos posteriores de esa clave 124, 212 incluirán la bandera o marcador actualizado que indica que la clave ya no se usa por primera vez. Por lo tanto, cuando un lector 128, 132 recibe una clave 124, 212 y esa clave no está marcada como usada previamente, entonces el lector 128, 132 sabrá que está recibiendo la clave 124, 212 durante su primer uso. Esta información puede almacenarse en la información 316 de primer uso junto con la hora de la transacción, una identidad 116 del dispositivo móvil, una identidad del lector 128, 132 y si se concedió o denegó el acceso. La información 316 del primer uso y/o la información 312 de registro de uso pueden ser transmitidas posteriormente por el lector 132 de vuelta al dispositivo 116 móvil a través del canal 136 de comunicación para su posterior entrega al servidor o servidores 140 de control de acceso y/o al sistema 144 de gestión de la propiedad.

El procesador 320 del lector 132 puede ser de naturaleza similar al procesador de un dispositivo 116 móvil. En algunas realizaciones, las capacidades de procesamiento del procesador 320 pueden estar limitadas en comparación con las capacidades de procesamiento del procesador 216. Como ejemplo, el procesador 320 puede comprender un chip IC o múltiples chips IC configurados para ejecutar el firmware o las instrucciones almacenadas en la memoria 304.

Asimismo, los controladores 324 pueden comprender software, firmware o hardware integrado que facilita las operaciones de los componentes del lector 132. Por ejemplo, la interfaz 328 de usuario puede tener un controlador 324 dedicado. La interfaz 332 de credenciales también puede tener un controlador 324 dedicado. Otros componentes del lector 132 también pueden tener sus propios controladores 324.

La interfaz 328 de usuario puede corresponder a un dispositivo de entrada y/o salida de usuario. En un lector 132, la interfaz 328 de usuario es tradicionalmente un dispositivo relativamente simple, aunque la simplicidad no es un requisito. Por ejemplo, la interfaz 328 de usuario puede comprender un elemento de visualización visual simple (por ejemplo, luz, LED, elemento de visualización de 8 segmentos, etc.) o un elemento de visualización visual más elaborada (por ejemplo, pantalla LCD). Una parte de entrada de usuario de la interfaz 328 de usuario puede comprender un teclado PIN, un sensor de huellas dactilares, un escáner de retina o similares. La interfaz 328 de usuario también puede facilitar interacciones audibles con el lector 132. Por ejemplo, la interfaz 328 de usuario puede comprender un zumbador, altavoz, micrófono, fotodetector, detector de proximidad, etc. Alternativa o adicionalmente, la interfaz 328 de usuario puede comprender un dispositivo de entrada de usuario y salida de usuario combinada, como un elemento de visualización táctil con botones configurables.

La interfaz 332 de credenciales puede comprender el hardware, circuitos o similares que facilitan el establecimiento del canal 136 de comunicación. Como algunos ejemplos no limitantes, la interfaz 332 de credenciales puede comprender una antena, circuitos de sintonización, una antena BLE, un Wi-Fi Antena Fi, lector de banda magnética, fotodetector, emisor de infrarrojos, micrófono, altavoz y similares.

El módulo 336 de alimentación puede corresponder a una fuente de alimentación dedicada y/o un convertidor de energía que facilita la conversión de energía de AC suministrada externamente en energía de DC que se usa para alimentar los diversos componentes del lector 132. En algunas realizaciones, el módulo 336 de alimentación también puede incluir alguna implementación de circuitos de protección contra sobretensiones para proteger los componentes del lector 132 contra sobretensiones.

Con referencia ahora a la Fig. 4, en una descripción no reivindicada proporcionada para comprender el contexto de la invención, se describirá un método para entregar una clave 124, 212 a un dispositivo 116 móvil según al menos algunas realizaciones de la presente descripción. El método comienza cuando se recibe una solicitud de una clave electrónica o un conjunto de claves electrónicas en el sistema 144 de gestión de la propiedad (paso 404). La solicitud puede recibirse en respuesta a que un huésped confirme su deseo de alojarse en un hotel, en respuesta a que un huésped confirme su deseo de entrar en una casa, en respuesta a que un huésped de la oficina confirme su reunión en una oficina, o similares. La solicitud de una clave puede entonces reenviarse desde el sistema 144 de gestión de la propiedad a un servidor 140 de control de acceso. Al recibir la solicitud de la clave electrónica desde el sistema 144 de gestión de la propiedad, el servidor o servidores 140 de control de acceso determinarán si la solicitud es una solicitud válida y procesable (por ejemplo, si la solicitud provino de una fuente de confianza, en un formato de confianza y debería resultar en la creación de una clave electrónica). La autenticación entre el servidor o servidores 140 de control de acceso y el sistema 144 de gestión de la propiedad se puede completar usando cualquier tipo de protocolo de autenticación.

Si la autenticación tiene éxito, entonces el servidor o servidores 140 de control de acceso determinarán los atributos para la clave electrónica (paso 408). Estos atributos pueden incluir una propiedad o código de sitio que se asignará a la clave electrónica, un cifrado para la clave electrónica, una duración de validez para la clave electrónica (que puede ser indefinida o finita) y otros atributos que pertenecerán a la clave. Con base en los atributos, el servidor o servidores 140 de control de acceso generarán la clave o claves electrónicas (paso 412) y luego determinarán uno o más objetivos para las claves (paso 416). Los objetivos para las claves pueden incluir uno o más dispositivos 116 móviles que se identificaron en la solicitud de la clave en el paso 404. Alternativa o adicionalmente, el objetivo para las claves puede incluir credenciales distintas a un dispositivo 116 móvil, como una tarjeta inteligente tradicional, un llavero o similar.

Una vez determinado el objetivo de la clave electrónica, el servidor o servidores 140 de control de acceso determinan si es momento o no de distribuir la clave (paso 420). El momento de la distribución puede basarse en una cantidad de tiempo anterior a la llegada o registro anticipado de un huésped. Alternativa o adicionalmente, el momento de la distribución puede estar basado en eventos o desencadenado por una secuencia de eventos. Por supuesto, la distribución puede basarse tanto en el tiempo como en los eventos. Como ejemplo de distribución basada en el tiempo, la llave electrónica puede no distribuirse al dispositivo objetivo hasta un período de tiempo predeterminado antes del registro anticipado de un huésped en un hotel. Como otro ejemplo de distribución basada en el tiempo, la clave electrónica puede no distribuirse al dispositivo objetivo hasta un período de tiempo predeterminado antes de una reunión programada. Como ejemplo de distribución basada en eventos, la llave electrónica no se puede distribuir hasta que el huésped se encuentre dentro de una distancia o proximidad predeterminada de un hotel, casa o edificio de oficinas. Otro ejemplo de una distribución basada en eventos sería esperar hasta que un dispositivo 116 móvil esté conectado a una red 104 de comunicación predeterminada o una red 112 de confianza. Un ejemplo de una distribución combinada basada en tiempo y basada en eventos sería limitar la distribución de un clave hasta una cantidad de tiempo predeterminada antes del registro anticipado de un huésped y hasta que el dispositivo 116 móvil del huésped se haya conectado a una red 112 de confianza de la propiedad donde el huésped se está registrando.

Si la consulta del paso 420 se responde negativamente, entonces el servidor o servidores 140 de control de acceso continuarán monitorizando eventos, tiempo y otros activadores para determinar un tiempo de entrega apropiado (paso 424). Si la consulta del paso 420 se responde afirmativamente, se determina un protocolo y canal de distribución apropiados para la distribución de la clave o claves electrónicas (paso 428). Por ejemplo, se puede determinar que se puede usar una red móvil y un protocolo de comunicación móvil para entregar las claves al dispositivo 116 móvil a través de la red 104 de comunicación. Como otro ejemplo, se puede determinar que se requiere un canal de entrega más seguro. en cuyo caso puede ser necesaria la red 112 de confianza para la entrega de la clave.

Después de que se hayan determinado el canal y protocolo apropiados, la clave o claves electrónicas se transmiten a su objetivo a través del canal y protocolo determinados (paso 432). La entrega de la clave o claves puede emplear protocolos tradicionales como HTTP/HTTPS, SNMP, FTP, mensajes SMS, mensajes MMS, RTP, UDP, etc. o protocolos no tradicionales/propietarios. En algunas realizaciones, la ruta usada para entregar la clave al objetivo puede denominarse ruta de entrega de clave y puede seguir un conjunto específico de nodos cuando se viaja a través de la red 104 de comunicación o la red 112 de confianza.

Con referencia ahora a la Fig. 5, se describirá un método para reportar los primeros datos de interacción según realizaciones de la presente descripción. El método comienza cuando se presenta un dispositivo 116 móvil a un lector 128, 132 (paso 504). Esto puede implicar colocar el dispositivo 116 móvil dentro de un rango de comunicación del lector 128, 132, emparejar el dispositivo 116 móvil con el lector 128, 132 o similar. Una vez que los dispositivos están dentro de un rango de comunicación entre sí, se puede realizar una autenticación inicial (paso 508). La autenticación puede ser mutua o unidireccional, dependiendo de las preferencias y configuraciones administrativas en el lector 128, 132 y/o el dispositivo 116 móvil. Si la autenticación no tiene éxito (paso 512), entonces el método finalizará o permitirá un reintento de la autenticación (paso 516).

Si la autenticación tiene éxito (paso 512), entonces los dos dispositivos pueden continuar intercambiando información de control de acceso (paso 520). En este paso, el dispositivo 116 móvil puede transmitir una o más claves electrónicas al lector 128, 132 a través del canal 136 de comunicación establecido entre los dos dispositivos. El lector 128, 132 también puede proporcionar información de identificación y/o claves al dispositivo 116 móvil durante este paso. Cualquier otro tipo de información usada en relación con la toma de una decisión de control de acceso se puede intercambiar entre los dos dispositivos (en cualquier dirección) a través del canal 136 de comunicación.

Con base en la información intercambiada en el paso 520, el lector 128, 132 y/o el dispositivo 116 móvil pueden determinar si al titular del dispositivo 116 móvil se le permite o no acceder a un activo protegido por el lector 128, 132 (paso 524). Si esta consulta recibe una respuesta negativa, entonces el lector 128, 132 puede actualizar su registro 312 de uso (paso 528). El lector 128, 132 puede entonces finalizar el intercambio o permitir un reintento (paso 516).

Si la consulta del paso 524 se responde positivamente, entonces el lector 128, 132 determinará si esta es la primera interacción que el dispositivo 116 móvil ha tenido con el sistema de control de acceso (por ejemplo, determinará si esto corresponde a un evento de primera entrada) (paso 532). Esta determinación puede corresponder a determinar si la interacción entre el dispositivo 116 móvil específico y el lector 128, 132 es una primera interacción en general. Esta determinación también puede implicar determinar si la clave usada por el dispositivo móvil corresponde a una primera instancia de uso de esa clave, ya sea globalmente (por ejemplo, entre todos los lectores en el sistema de control de acceso) o localmente (por ejemplo, específica del lector 128, 132 actual). Como se analizó anteriormente, el lector 128, 132 puede analizar propiedades de la clave para determinar si la clave se ha usado previamente o no, por ejemplo analizando la clave para alguna indicación de primer uso (o una indicación de uso posterior mediante el marcado de una bandera de uso en la clave). El análisis de la clave en contraposición al dispositivo 116 móvil puede ser útil, especialmente para situaciones de visitantes frecuentes a una propiedad. Por ejemplo, un huésped puede alojarse en un hotel específico varias veces a lo largo de un año, pero el dispositivo 116 móvil del huésped usará una clave diferente para cada estancia. Si se analizara el propio dispositivo 116 móvil para una primera interacción, entonces todas las estancias posteriores durante el año no se registrarían como un evento de registro. Por otro lado, si se analizan las claves usadas para una estancia concreta, se podrá determinar un registro adecuado para cada instancia de estancia.

También se debe apreciar que el análisis del paso 532 se puede realizar en el paso 528 cuando se le niega el acceso al dispositivo 116 móvil. La ilustración del paso 532 como procedente únicamente de una decisión positiva de control de acceso es para facilitar la comprensión y la simplicidad y no debe interpretarse como realizaciones limitantes de la presente descripción.

Si la interacción corresponde a una primera interacción (o un primer uso de la clave por parte del dispositivo 116 móvil), entonces el lector 128, 132 puede generar un paquete de datos de primera interacción e intentar reportar los primeros datos de interacción al servidor o servidores 140 de control de acceso y/o sistema 144 de gestión de la propiedad. Si el lector es un lector 128 en red, entonces los primeros datos de interacción pueden transmitirse simplemente a través de la red 108 de control de acceso a los servidores 140 de control de acceso y/o sistema 144 de gestión de la propiedad. Por otro lado, si el lector corresponde a un lector 132 que no está en red, entonces el lector 132 proporcionará los primeros datos de interacción al dispositivo 116 móvil (paso 536). En algunas realizaciones, los primeros datos de interacción se devuelven al dispositivo móvil 116 a través del mismo canal 136 de comunicación usado para intercambiar información de control de acceso. Si la determinación en el paso 532 se realiza lo

suficientemente rápido, el lector 132 no conectado en red puede incluso ser capaz de proporcionar los primeros datos de interacción al dispositivo 136 móvil durante el mismo caso de presentación usado para comunicar la información de control de acceso. En otras palabras, es posible que un usuario no necesite presentar el dispositivo 116 móvil al lector 132 dos veces para facilitar las comunicaciones de los pasos 520 y 536. En cambio, los primeros datos de interacción pueden transmitirse eficientemente de vuelta al dispositivo 116 móvil mientras el dispositivo 116 móvil está sostenido frente al lector 132 y esperando una decisión de control de acceso.

Ejemplos no limitativos de los tipos de información que se pueden proporcionar en los primeros datos de interacción incluyen una identidad o número de identificación del lector 132, un identificador de la clave o huésped, una hora de la transacción, un día de la transacción, si la decisión de control de acceso fue positiva o negativa, la temperatura actual, la información del estado del lector 132 (por ejemplo, batería baja), etc.

Posteriormente, el lector 128, 132 concede al dispositivo 116 móvil y a su titular acceso al activo protegido por el lector 128, 132 (paso 540).

Con referencia ahora a la Fig. 6, se describirá un método para distribuir primeros datos de interacción según ejemplos que no forman parte de la invención. El método comienza cuando un dispositivo 116 móvil recibe los primeros datos de interacción desde un lector 132 (paso 604). Los primeros datos de interacción pueden recibirse a través del canal 136 de comunicación usado durante la autenticación y/o durante el intercambio de información de control de acceso.

Cuando el dispositivo 116 móvil recibe los primeros datos de interacción, el dispositivo 116 móvil determina entonces una dirección de destinatario para los primeros datos de interacción (paso 608). Esta información puede estar contenida dentro de los primeros datos de interacción, puede proporcionarse como instrucciones separadas al dispositivo 116 móvil desde el lector 132, o el dispositivo 116 móvil puede comprender la inteligencia para hacer tal determinación (ya que puede incluirse como parte de la lógica 308 de control de acceso). El dispositivo 116 móvil también puede determinar qué canal o vía de comunicación debe usarse para entregar los primeros datos de interacción a la dirección del destinatario (paso 612). En algunas realizaciones, el dispositivo 116 móvil puede determinar que los primeros datos de interacción deben viajar por una ruta inversa de la ruta de entrega de claves. En otras palabras, el dispositivo 116 móvil puede simplemente enviar los primeros datos de interacción a la misma entidad de la que recibió sus claves electrónicas y el dispositivo 116 móvil puede utilizar el mismo canal/red de comunicación para enviar los primeros datos de interacción. En otras realizaciones, un administrador del sistema de control de acceso puede dictar que los primeros datos de interacción se entreguen directamente al sistema 144 de gestión de la propiedad y esta información se pueda entregar a través de una ruta de entrega de la red 112 de confianza en lugar de recorrer una ruta de entrega de clave inversa.

Una vez que se determinan la dirección del destinatario y el canal de comunicación apropiado, el dispositivo 116 móvil genera un mensaje o conjunto de mensajes apropiado para incluir los primeros datos de interacción (paso 616). Luego, el dispositivo 116 móvil envía el o los mensajes a la dirección del destinatario determinada (paso 620).

Con referencia ahora a la Fig. 7, se describirán detalles adicionales de las rutas de comunicación que se pueden usar para entregar claves electrónicas y primeros datos de interacción según al menos algunos ejemplos que no forman parte de la presente invención. El proceso representado en la Fig. 7 comienza cuando el sistema 144 de gestión de la propiedad transmite una solicitud de clave electrónica al servidor o servidores 140 de control de acceso (paso S701). El servidor o servidores 140 de control de acceso, en respuesta a recibir la solicitud, transmiten una o más claves electrónicas a un dispositivo 116 móvil objetivo (paso S702). En algunas realizaciones, la entrega de las claves electrónicas en el paso S702 utiliza la red de comunicación y puede implicar el uso de múltiples tipos de red (por ejemplo, Internet y red de comunicación móvil). En consecuencia, el camino recorrido por el mensaje o mensajes que transportan las claves electrónicas puede atravesar múltiples límites de red y múltiples elementos de borde de red.

Luego, el dispositivo 116 móvil recibe las claves electrónicas y almacena las claves en su aplicación 120 de control de acceso o memoria 204. El dispositivo 116 móvil retiene las claves hasta que se presenta a un lector 132 no conectado en red (o lector 128 en red), en el cual Las comunicaciones puntuales pueden comenzar y puede tener lugar una autenticación entre los dos dispositivos (paso S703). Si se puede establecer una relación de confianza, entonces el canal 136 de comunicación puede usarse para entregar la clave electrónica al lector 132 no conectado en red (paso S704). El lector 132 no conectado en red puede entonces tomar una decisión de control de acceso con base, al menos en parte, en el contenido de la clave electrónica. El lector 132 no conectado en red también puede determinar que su recepción de la clave electrónica desde el dispositivo 116 móvil corresponde a un primer uso de la clave electrónica, en cuyo caso el lector 132 no conectado en red puede generar y entregar primeros datos de interacción al dispositivo 116 móvil, nuevamente a través del canal 136 de comunicación (paso S705). En algunas realizaciones, los pasos S703, S704 y S705 se pueden realizar durante una única presentación del dispositivo 116 móvil al lector 132. Por supuesto, los pasos no se pueden realizar de manera precisamente simultánea, sino a un usuario que sostiene el dispositivo 116 móvil, los pasos pueden realizarse durante un período de tiempo que el usuario percibe como simultáneo. En otras realizaciones, el paso S705 puede ocurrir después de que el dispositivo 116 móvil se presenta por primera vez al lector 132 y el lector 132 puede solicitar al titular del dispositivo 116 móvil que vuelva a presentar el dispositivo 116 móvil al lector 132 para que un proceso de registro puede completarse y el lector 132 puede enviar los primeros datos de interacción al dispositivo 116 móvil.

El dispositivo 116 móvil proporciona entonces una indicación al servidor o servidores 140 de control de acceso de los resultados de la decisión de control de acceso implementada en el lector 132 (paso S706). Además, el dispositivo 116 móvil puede entregar los primeros datos de interacción al servidor o servidores 140 de control de acceso durante el paso S706. El servidor o servidores 140 de control de acceso pueden entonces proporcionar los primeros datos de interacción al sistema 144 de gestión de la propiedad (paso S707). Alternativa o adicionalmente, el dispositivo 116 móvil puede entregar los primeros datos de interacción directamente al sistema 144 de gestión de la propiedad (paso S708). Como puede apreciarse, la ruta de entrega de claves y la ruta de entrega de los primeros datos de interacción pueden coincidir sustancialmente entre sí, pero en orden inverso. En otras realizaciones, la utilización del canal 136 de comunicación puede corresponder al único punto en común entre la ruta de entrega de claves y la ruta de entrega de los primeros datos de interacción.

Con referencia ahora a la Fig. 8, se describirá un método para realizar procesos de registro en respuesta a recibir una indicación de primera entrada en un sistema 144 de gestión de la propiedad según ejemplos que no forman parte de la presente invención. El método comienza cuando se recibe una indicación de la primera entrada de un huésped en el sistema 144 de gestión de la propiedad (paso 804). La indicación puede recibirse en respuesta a que el sistema de gestión de la propiedad reciba los primeros datos de interacción desde el servidor o servidores 140 de control de acceso o desde un dispositivo 116 móvil. Los primeros datos de interacción pueden indicar que un huésped particular (o clave asociada con un huésped) ha llegado a un lector 128, 132 particular y que el lector 128, 132 ha completado una primera instancia de una interacción con el dispositivo 116 móvil del huésped para esta estancia particular.

Al recibir la indicación de la primera entrada, el sistema de gestión de la propiedad inicia un proceso de registro de huéspedes donde se crea una nueva cuenta de usuario para ese usuario, donde la cuenta es específica para la estancia de este huésped en particular y la habitación asignada al huésped (paso 808). Si el huésped tiene una cuenta de huésped frecuente, entonces la cuenta recién generada puede asociarse con la cuenta de huésped frecuente en una base de datos de gestión de relaciones con el cliente. En algunas realizaciones, al menos parte de la información de los primeros datos de interacción se usa para completar la cuenta recién generada (paso 812). Por ejemplo, si los primeros datos de interacción incluyen un identificador del lector 128, 132 con el que el dispositivo 116 móvil interactuó por primera vez y ese lector 128, 132 corresponde a una habitación que está asignada o puede asignarse al huésped (por ejemplo, una habitación vacante), entonces el identificador de lector contenido en los datos de la primera interacción puede incluirse en la cuenta recién generada para identificar la habitación que se ha asignado al huésped. Como otro ejemplo, si el huésped presentó por primera vez el dispositivo 116 móvil a un lector asociado con una máquina de Punto de Servicio (PoS), entonces se puede incorporar un identificador del lector así como datos de transacción para el huésped en la cuenta recién generada.

El método continúa con el sistema 144 de gestión de la propiedad determinando si se requiere un pasaporte para la estancia del huésped (paso 816). Si esta consulta se responde negativamente, entonces el método continúa finalizando otros elementos de registro para la cuenta de ese usuario (por ejemplo, asegurarse de que haya una tarjeta de crédito registrada para el huésped, preparar un itinerario para el huésped, etc.).

Sin embargo, si la consulta del paso 816 se responde positivamente, entonces se le puede pedir al huésped que proporcione información adicional para confirmar su identidad y que posee un pasaporte válido (paso 820). En algunas realizaciones, el huésped puede ingresar la información de su pasaporte a través del lector y/o dispositivo 116 móvil. En algunas realizaciones, el huésped puede proporcionar una imagen de su pasaporte y transmitir esa imagen al sistema 144 de gestión de la propiedad. En algunas realizaciones, se puede enviar a un representante de servicio al cliente del hotel para que se reúna con el huésped en su ubicación conocida (por ejemplo, hacia el lector donde ocurrió la primera interacción) para verificar la información del pasaporte.

Una vez finalizado el análisis del pasaporte (paso 824), el método puede continuar hasta el paso 828 donde se finalizan otros elementos de registro para el huésped.

Con referencia ahora a la Fig. 9, se describirá un método para producir un informe de registro directo a la habitación según ejemplos que no forman parte de la invención. El método comienza determinando que se ha solicitado un registro remoto en el hotel (paso 904). Esta solicitud puede proporcionarse específicamente durante la compra de su habitación por parte de un huésped. Alternativamente, la opción puede proporcionarse al usuario después de que se haya completado la compra y el usuario puede aceptar o rechazar la opción.

Cuando el sistema 144 de gestión de la propiedad determina que el huésped desea el registro remoto, permitiéndole así evitar la recepción, el sistema 144 de gestión de la propiedad asigna una habitación para el huésped antes del registro o llegada anticipada (paso 908). La habitación asignada puede corresponder a una habitación específica o a un conjunto de habitaciones que están disponibles para que el huésped las seleccione. La identificación de la habitación asignada al huésped puede comunicarse al huésped mediante un mensaje transmitido al dispositivo móvil 116 del huésped.

El sistema 144 de gestión de la propiedad crea entonces una cuenta de huésped antes de la llegada del huésped (paso 912). El método espera entonces hasta que se detecta la primera entrada o llegada del huésped (pasos 916 y 920). Una vez que se detecta la llegada del huésped, los primeros datos de interacción asociados con esta primera llegada se envían desde el lector 128, 132 al sistema 144 de gestión de la propiedad (paso 924). El sistema 144 de

gestión de la propiedad produce entonces un informe de registro de entrada directo a la habitación en la recepción del hotel como si acabara de producirse un registro normal (paso 928).

Cabe señalar que las realizaciones se describieron como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama de flujo de datos, un diagrama de estructura o un diagrama de bloques. Aunque un diagrama de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones se pueden realizar en paralelo o simultáneamente. Además, el orden de las operaciones podrá reordenarse sin apartarse del alcance de la presente descripción. Un proceso finaliza cuando se completan sus operaciones, pero podría tener pasos adicionales no incluidos en la figura.

REIVINDICACIONES

1. Un método para comunicar información sobre los primeros datos de interacción con un lector para completar un proceso de registro remoto en una instalación de varias habitaciones, en donde el método está configurado para ser realizado por todos los lectores conectados y no conectados en red de la instalación, en donde el lector es un dispositivo o colección de dispositivos usados para controlar el acceso a un activo protegido, comprendiendo el método:

usar una interfaz de credenciales del lector para establecer un canal de comunicación con un dispositivo (116) móvil;

recibir una clave electrónica desde el dispositivo móvil a través del canal de comunicación;

determinar (532) que la recepción de la clave electrónica corresponde a una primera instancia en donde la clave electrónica ha sido usada por el dispositivo móvil, comprendiendo dicha determinación analizar el contenido de la clave electrónica para obtener una indicación de si la clave electrónica se está presentando al lector por primera vez y no ha sido presentada a ningún otro lector antes de ser presentada al lector, en donde dicho contenido de análisis comprende verificar si la clave electrónica incluye un marcador que indica que la clave electrónica ya ha sido entregada al lector o a cualquier otro lector;

en respuesta a determinar que la recepción de la clave electrónica corresponde a una primera instancia de que la clave electrónica ha sido usada por el dispositivo móvil, generar primeros datos de interacción, en donde los datos de interacción comprenden un identificador de la clave o huésped;

en respuesta a determinar que la recepción de la clave electrónica corresponde a una primera instancia de que la clave electrónica ha sido usada por el dispositivo móvil, actualizar la clave (124, 212) electrónica en el dispositivo (116) móvil con el marcador en la clave electrónica que indica que la llave electrónica ha sido entregada a un lector (128, 132);

transmitir (536) los primeros datos de interacción a un servidor (140) de control de acceso y/o un sistema (144) de gestión de la propiedad para completar un proceso de registro, a través de la red de control de acceso cuando el lector es un lector en red, o al dispositivo móvil a través del canal de comunicación, cuando el lector es un lector no conectado en red;

analizar la llave electrónica con lógica de control de acceso almacenada en una memoria del lector;

y

tomar una decisión de control de acceso al dispositivo móvil con base en el análisis de la llave electrónica.

2. El método de la reivindicación 1, en donde los primeros datos de interacción comprenden además un identificador del lector.

3. El método de la reivindicación 2, en donde los primeros datos de interacción comprenden además un tiempo asociado con la recepción de la clave electrónica en el lector.

4. El método de la reivindicación 3, en donde los primeros datos de interacción comprenden además resultados de una decisión de control de acceso tomada en el lector en respuesta al análisis de la clave electrónica.

5. El método de cualquiera de las reivindicaciones anteriores, en donde los resultados de la decisión de control de acceso se incluyen en los primeros datos de interacción.

6. El método de la reivindicación 1, en donde los primeros datos de interacción se transmiten al dispositivo móvil inmediatamente después de determinar que la recepción de la clave electrónica corresponde a una primera instancia de la clave electrónica que ha sido usada por el dispositivo móvil.

7. El método de la reivindicación 6, en donde los primeros datos de interacción se transmiten a través del canal de comunicación durante la misma presentación del dispositivo móvil al lector no conectado en red que dio como resultado la entrega de la clave electrónica.

8. El método de la reivindicación 1, en donde el canal de comunicación corresponde a un canal de Radiofrecuencia (RF).

9. El método de la reivindicación 8, en donde el dispositivo móvil y el lector no conectado en red utilizan Comunicaciones de Campo Cercano (NFC) y/o Bluetooth para intercambiar información a través del canal de comunicación.

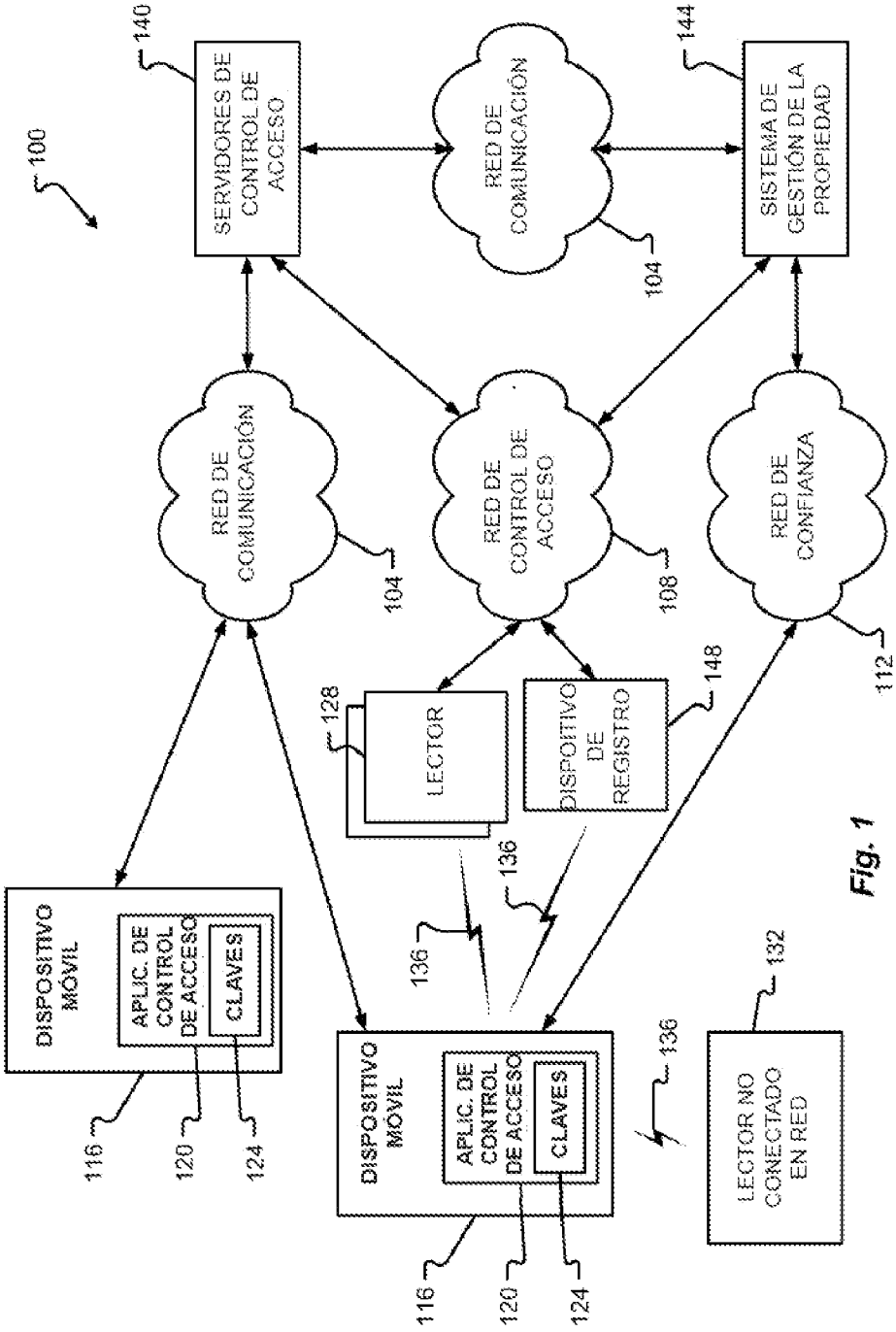
100
140
SERVIDORES DE CONTROL DE ACCESO
RED DE COMUNICACIÓN
104
144
SISTEMA DE GESTIÓN DE LA PROPIEDAD
RED DE COMUNICACIÓN
104
RED DE CONTROL DE ACCESO
108
RED DE CONFIANZA
112
128
LECTOR
DISPOSITIVO DE REGISTRO
148
136
136
DISPOSITIVO MÓVIL
APLIC. DE CONTROL DE ACCESO
CLAVES
116
120
124
DISPOSITIVO MÓVIL
APLIC. DE CONTROL DE ACCESO
CLAVES
116
120
124
136
132
LECTOR NO CONECTADO EN RED

Fig. 1

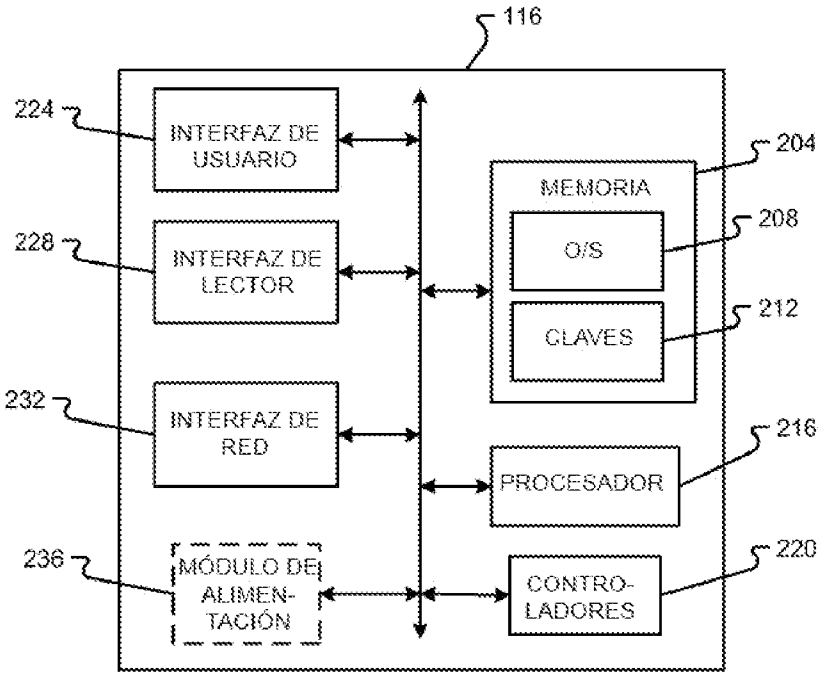
116
224
INTERFAZ DE USUARIO
228
INTERFAZ DE LECTOR
232
INTERFAZ DE RED
236
MÓDULO DE ALIMEN-TACIÓN
MEMORIA
204
O/S
208
CLAVES
212
PROCESADOR
216
CONTRO-LADORES
220

Fig. 2

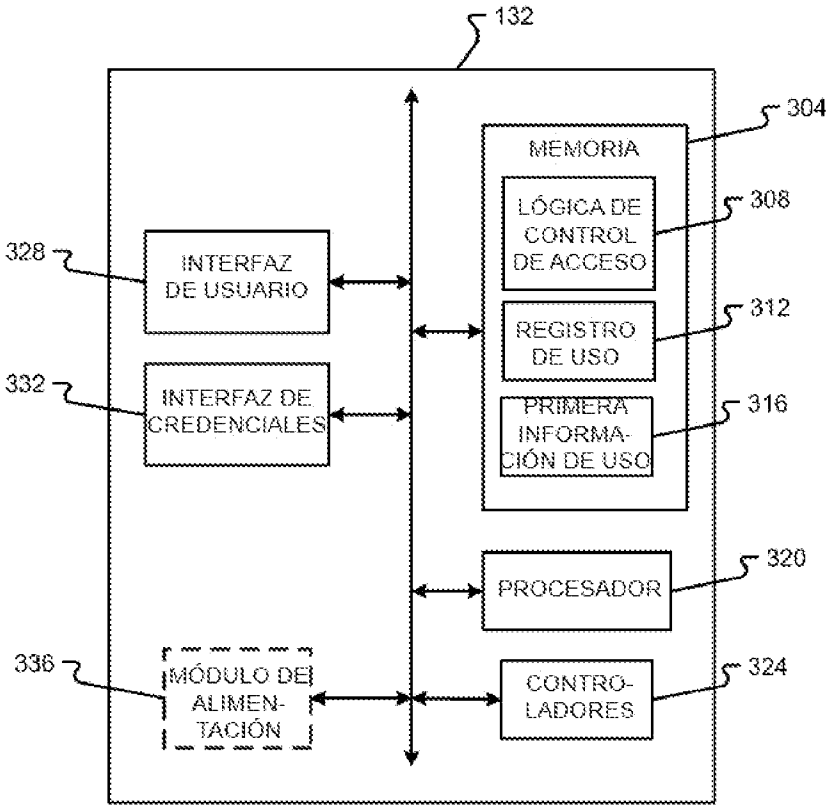
132
304
MEMORIA
LÓGICA DE CONTROL DE ACCESO
308
328
INTERFAZ DE USUARIO
REGISTRO DE USO
312
332
INTERFAZ DE CREDENCIALES
PRIMERA INFORMA-CIÓN DE USO
316
PROCESADOR
320
336
MÓDULO DE ALIMEN-TACIÓN
CONTRO-LADORES
324

Fig. 3

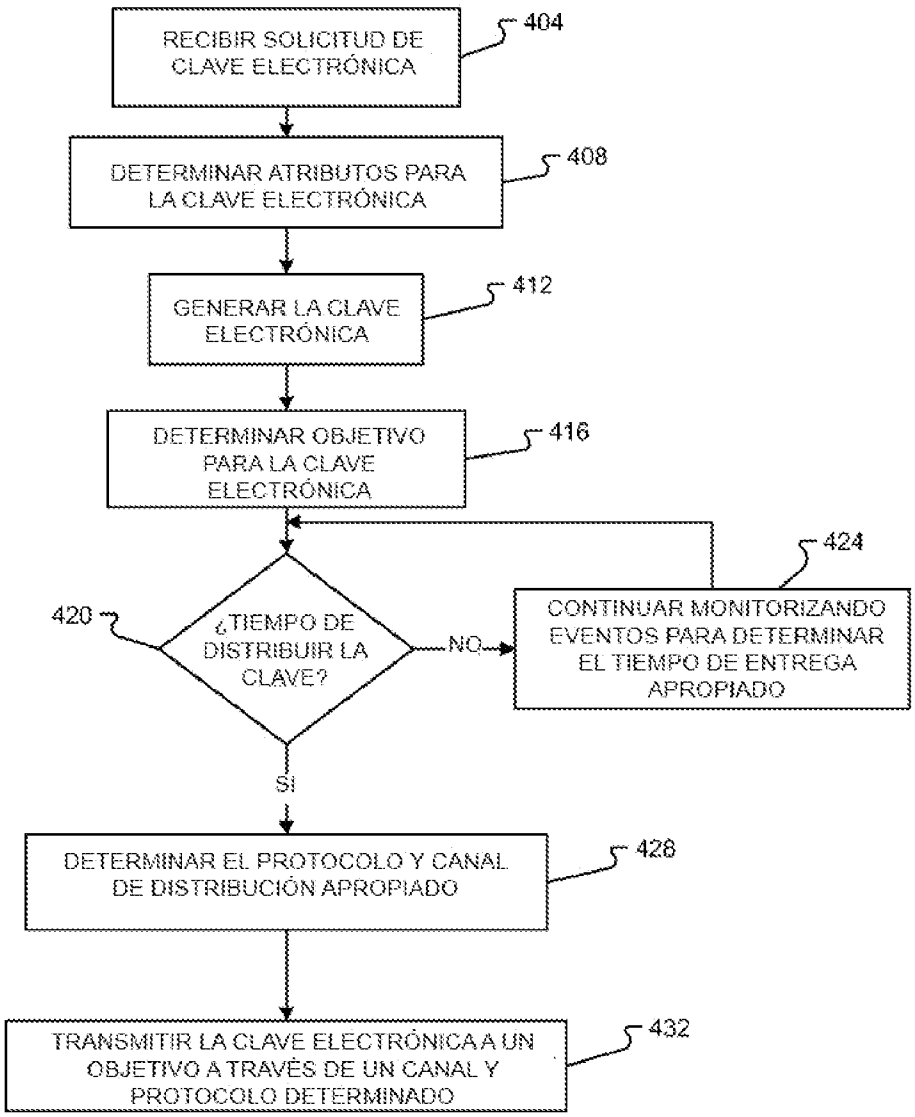
RECIBIR SOLICITUD DE CLAVE ELECTRÓNICA
404
DETERMINAR ATRIBUTOS PARA LA CLAVE ELECTRÓNICA
408
GENERAR LA CLAVE ELECTRÓNICA
412
DETERMINAR OBJETIVO PARA LA CLAVE ELECTRÓNICA
416
424
420
¿TIEMPO DE DISTRIBUIR LA CLAVE?
NO
CONTINUAR MONITORIZANDO EVENTOS PARA DETERMINAR EL TIEMPO DE ENTREGA APROPIADO
SI
DETERMINAR EL PROTOCOLO Y CANAL DE DISTRIBUCIÓN APROPIADO
428
TRANSMITIR LA CLAVE ELECTRÓNICA A UN OBJETIVO A TRAVÉS DE UN CANAL Y PROTOCOLO DETERMINADO
432

Fig. 4

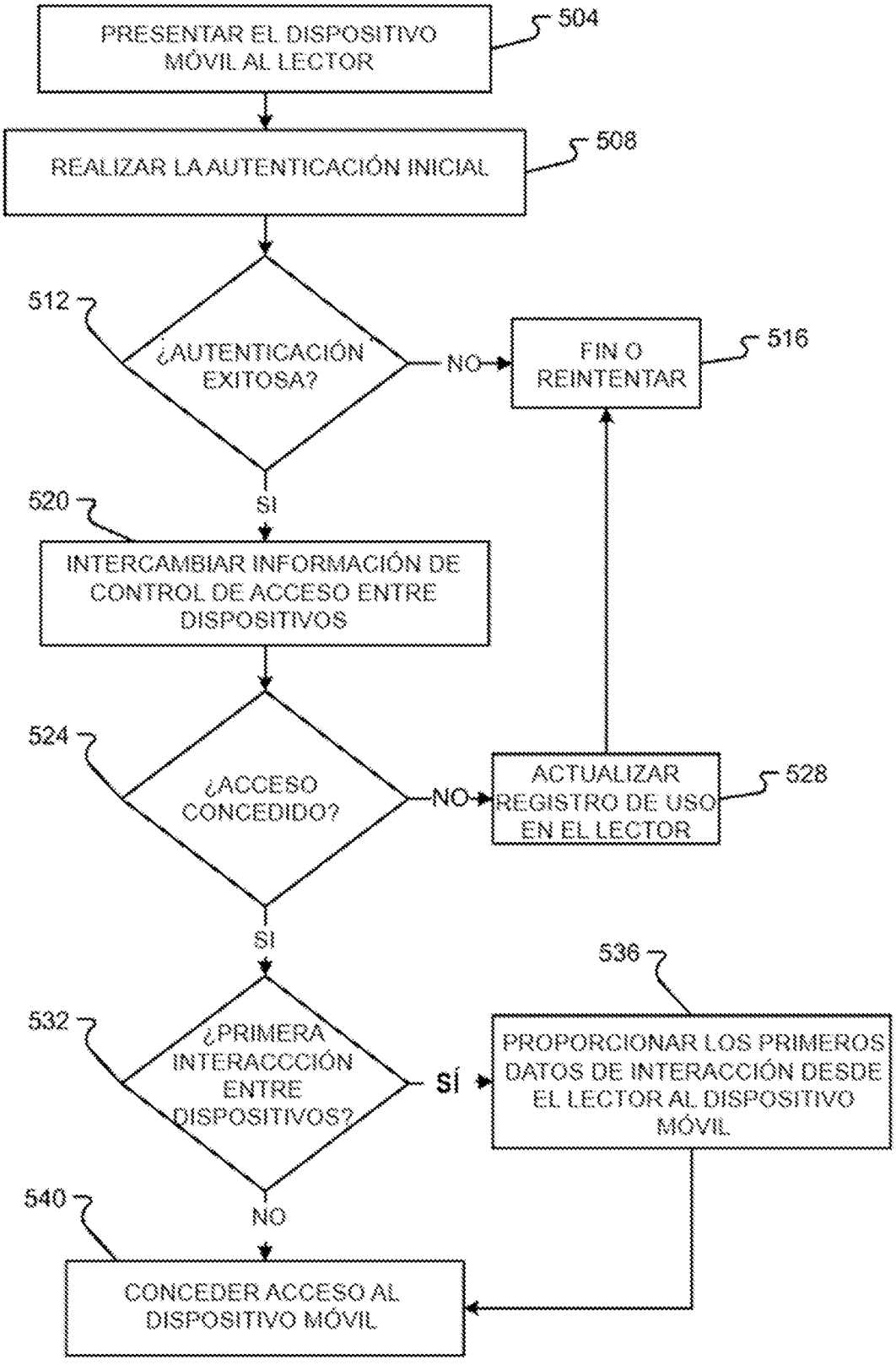
PRESENTAR EL DISPOSITIVO MÓVIL AL LECTOR
504
REALIZAR LA AUTENTICACIÓN INICIAL
508
512
¿AUTENTICACIÓN EXITOSA?
NO
FIN O REINTENTAR
516
SI
520
INTERCAMBIAR INFORMACIÓN DE CONTROL DE ACCESO ENTRE DISPOSITIVOS
524
¿ACCESO CONCEDIDO?
NO
ACTUALIZAR REGISTRO DE USO EN EL LECTOR
528
SI
536
532
¿PRIMERA INTERACCCIÓN ENTRE DISPOSITIVOS?
SÍ
PROPORCIONAR LOS PRIMEROS DATOS DE INTERACCIÓN DESDE EL LECTOR AL DISPOSITIVO MÓVIL
NO
540
CONCEDER ACCESO AL DISPOSITIVO MÓVIL

Fig. 5

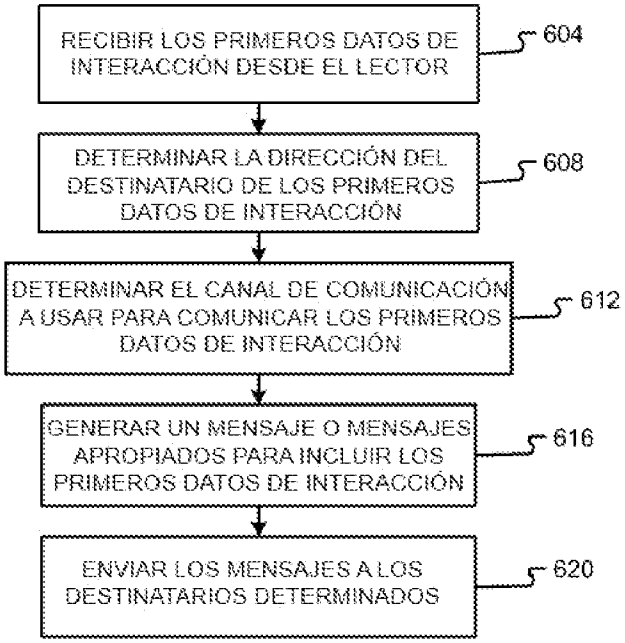
RECIBIR LOS PRIMEROS DATOS DE INTERACCIÓN DESDE EL LECTOR
604
DETERMINAR LA DIRECCIÓN DEL DESTINATARIO DE LOS PRIMEROS DATOS DE INTERACCIÓN
608
DETERMINAR EL CANAL DE COMUNICACIÓN A USAR PARA COMUNICAR LOS PRIMEROS DATOS DE INTERACCIÓN
612
GENERAR UN MENSAJE O MENSAJES APROPIADOS PARA INCLUIR LOS PRIMEROS DATOS DE INTERACCIÓN
616
ENVIAR LOS MENSAJES A LOS DESTINATARIOS DETERMINADOS
620

Fig. 6

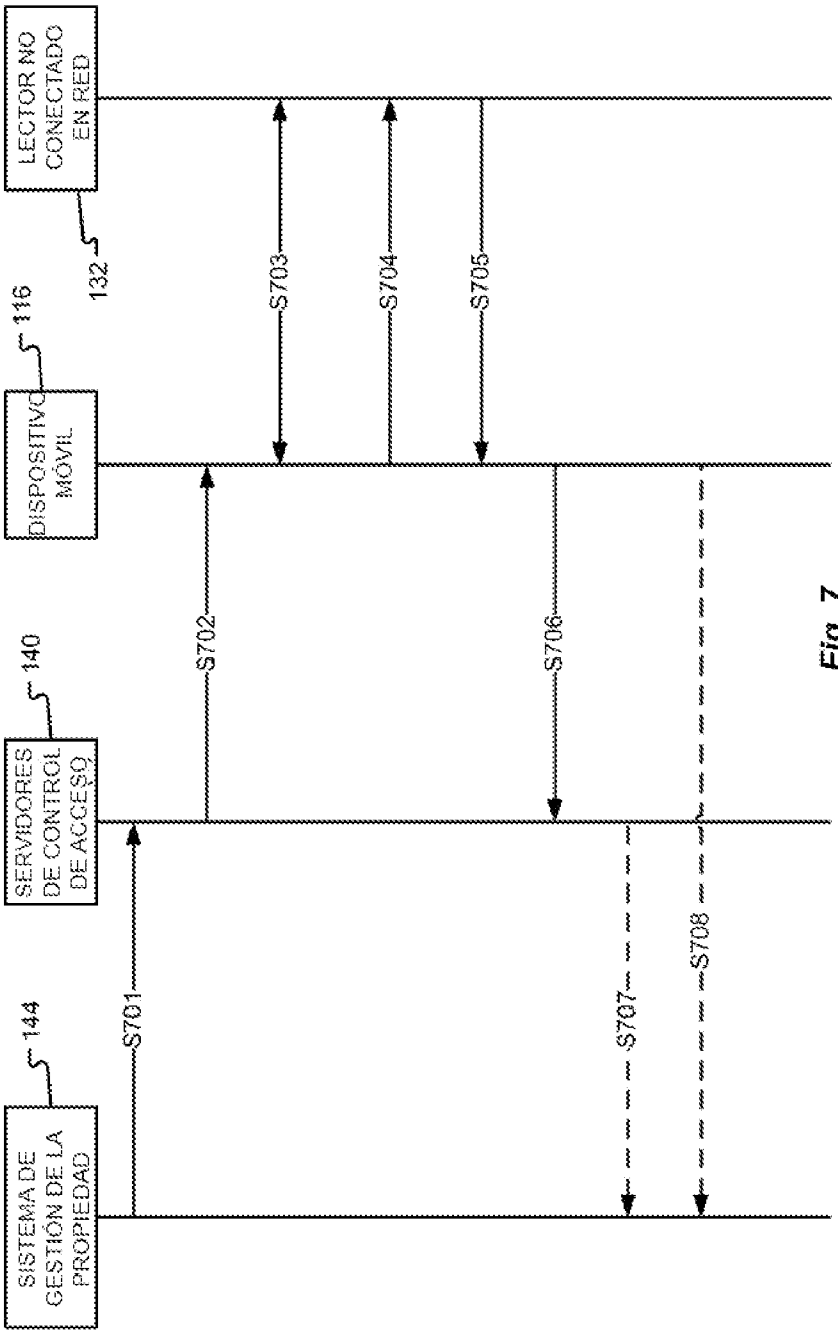
SISTEMA DE GESTIÓN DE LA PROPIEDAD
144
SERVIDORES DE CONTROL DE ACCESO
140
DISPOSITIVO MÓVIL
116
LECTOR NO CONECTADO EN RED
132
S701
S702
S703
S704
S705
S706
S707
S708

Fig. 7

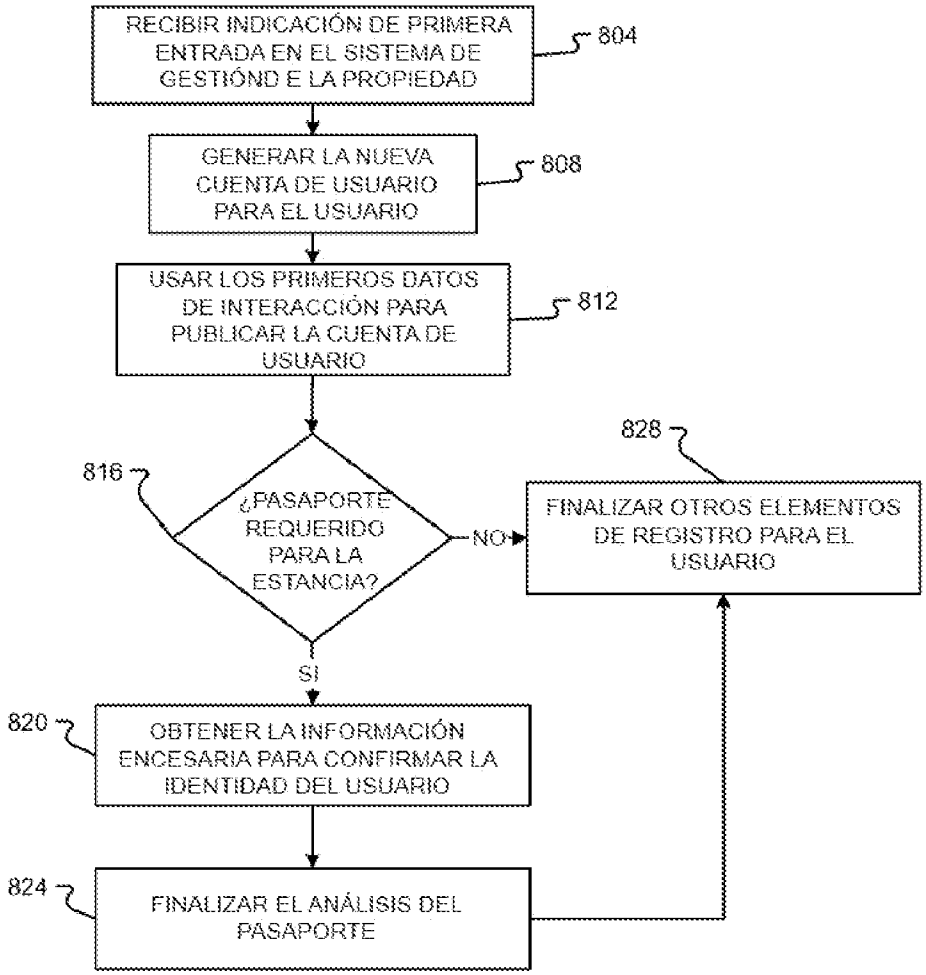
RECIBIR INDICACIÓN DE PRIMERA ENTRADA EN EL SISTEMA DE GESTIÓND E LA PROPIEDAD
804
GENERAR LA NUEVA CUENTA DE USUARIO PARA EL USUARIO
808
USAR LOS PRIMEROS DATOS DE INTERACCIÓN PARA PUBLICAR LA CUENTA DE USUARIO
812
816
¿PASAPORTE REQUERIDO PARA LA ESTANCIA?
NO
828
FINALIZAR OTROS ELEMENTOS DE REGISTRO PARA EL USUARIO
SI
820
OBTENER LA INFORMACIÓN ENCESARIA PARA CONFIRMAR LA IDENTIDAD DEL USUARIO
824
FINALIZAR EL ANÁLISIS DEL PASAPORTE

Fig. 8

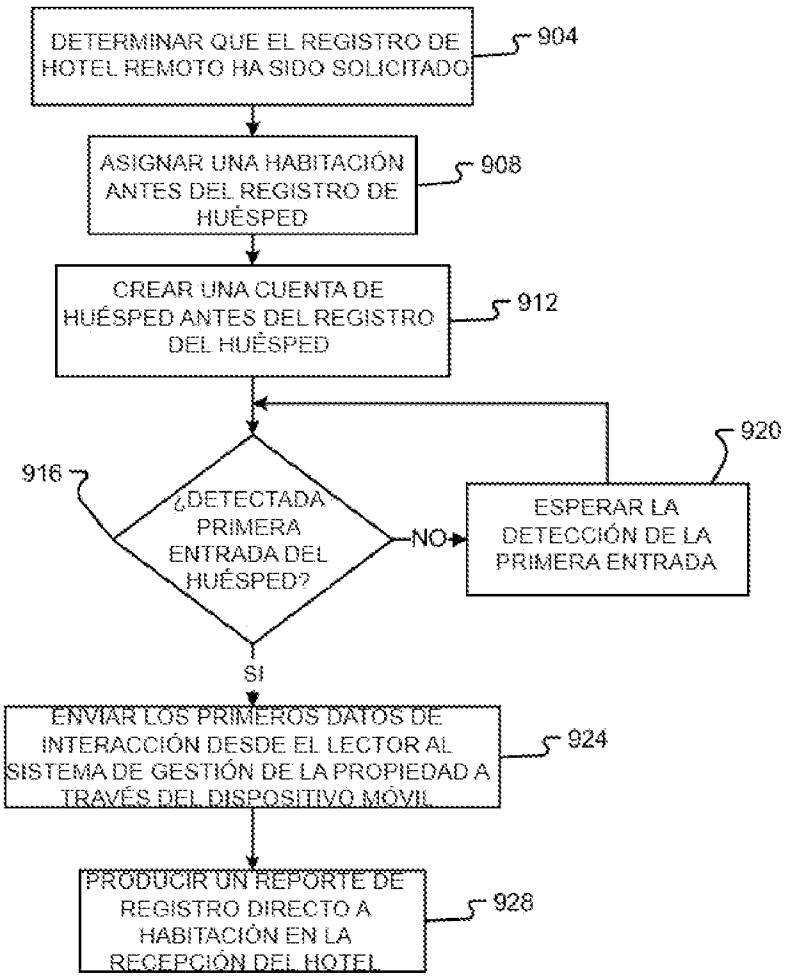
DETERMINAR QUE EL REGISTRO DE HOTEL REMOTO HA SIDO SOLICITADO
904
ASIGNAR UNA HABITACIÓN ANTES DEL REGISTRO DE HUÉSPED
908
CREAR UNA CUENTA DE HUÉSPED ANTES DEL REGISTRO DEL HUÉSPED
912
916
¿DETECTADA PRIMERA ENTRADA DEL HUÉSPED?
NO
ESPERAR LA DETECCIÓN DE LA PRIMERA ENTRADA
920
SI
ENVIAR LOS PRIMEROS DATOS DE INTERACCIÓN DESDE EL LECTOR AL SISTEMA DE GESTIÓN DE LA PROPIEDAD A TRAVÉS DEL DISPOSITIVO MÓVIL
924
PRODUCIR UN REPORTE DE REGISTRO DIRECTO A HABITACIÓN EN LA RECEPCIÓN DEL HOTEL
928

Fig. 9