(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 874 853**

(51) Int. CI.:

***G07C 9/00*** (2010.01)
***G07C 9/27*** (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.07.2013 PCT/IB2013/002144**

(87) Fecha y número de publicación internacional: **30.01.2014 WO14016699**

(96) Fecha de presentación y número de la solicitud europea: **26.07.2013 E 13785599 (5)**

(97) Fecha y número de publicación de la concesión europea: **14.04.2021 EP 2877983**

(54) Título: **Control de acceso de una caja fuerte en la habitación**

(30) Prioridad:

**27.07.2012 US 201261676827 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**05.11.2021**

(73) Titular/es:

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

(72) Inventor/es:

**LAGERSTEDT, STIG;**
**BERG, DANIEL;**
**BAILIN, DANIEL;**
**ROBINTON, MARK y**
**DAVIS, MASHA LEAH**

(74) Agente/Representante:

**ISERN JARA, Jorge**

## DESCRIPCIÓN

Control de acceso de una caja fuerte en la habitación

Campo de la divulgación

La presente divulgación se refiere, en general, a sistemas, métodos y dispositivos de control de acceso para controlar el acceso en instalaciones de múltiples habitaciones con niveles de acceso en cascada y, más particularmente, a mecanismos de control de acceso bien adecuados para su uso al controlar en cajas fuerte en la habitación con dispositivos aptos para NFC.

Antecedentes

Las instalaciones de múltiples habitaciones o múltiples suites, tales como los hoteles, edificios de apartamentos, complejos de oficinas, dormitorios, edificios de oficinas, aulas, cruceros, instalaciones de laboratorio y estructuras similares tienen muchos dispositivos que, si se monitorizan y/o controlan de una manera que no se hace actualmente, generará nuevas funcionalidades en las áreas de la seguridad de instalaciones, en la eficacia operacional de las instalaciones y el mantenimiento de las instalaciones (para el operador de la instalación y el usuario de la instalación) y generará una reducción de coste global en la gestión y el mantenimiento de la instalación.

Un huésped que visita un hotel puede obtener tarjetas de control de acceso o esquemas similares que se codifican con información tal como la duración de permanencia del huésped, número de habitación y otras preferencias tales como el acceso a habitaciones comunes, spa y servicios añadidos, etc. Estas tarjetas o esquemas similares proporcionan acceso a alguna área general a través de poder abrir el cerrojo o desactivar de otra manera algún mecanismo de control de acceso a esa área general. Sin embargo, en ocasiones, es necesario el control de acceso separado para dispositivos o subáreas dentro de esa área general, por ejemplo, una caja fuerte en una habitación de un huésped.

Por consiguiente, existe una necesidad en la técnica de sistemas, métodos y dispositivos de control de acceso que funcionaran en instalaciones de múltiples habitaciones con niveles de acceso en cascada.

El documento EP1837792 A1 desvela un sistema de gestión que gestiona el uso de un objeto de gestión proporcionado en instalaciones usando un medio de almacenamiento de información de un usuario. Un aparato de gestión de entrada, proporcionado en las cercanías de una entrada de las instalaciones, almacena información de permiso de uso para permitir el uso del objeto de gestión en un medio de almacenamiento de información cuando el usuario entra en las instalaciones. En las instalaciones, un aparato de gestión de uso, proporcionado para cada objeto de gestión, controla la disponibilidad o no disponibilidad del objeto de gestión basándose en la información de permiso de uso almacenada en el medio de almacenamiento de información. Adicionalmente, el aparato de gestión de uso almacena, en el medio de almacenamiento de información, información de uso que muestra que se usa el objeto de gestión.

Sumario

Por lo tanto, es un aspecto de la presente divulgación proporcionar métodos, sistemas y dispositivos para controlar el acceso en instalaciones de múltiples habitaciones con niveles de acceso en cascada. Más específicamente, las realizaciones de la presente divulgación proporcionan un método como se define en la reivindicación 1 y un sistema como se define en la reivindicación 5.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que representa un sistema de control de acceso para una instalación de múltiples habitaciones de acuerdo con realizaciones de la presente divulgación;
La Figura 2 es un diagrama de bloques que representa un módulo de control de acceso de acuerdo con realizaciones de la presente divulgación;
La Figura 3 es un diagrama de bloques que representa una credencial de acceso de acuerdo con realizaciones de la presente divulgación;
La Figura 4 es un diagrama de bloques que representa un módulo de acceso de la caja fuerte de acuerdo con realizaciones de la presente divulgación;
La Figura 5 es un diagrama de flujo que representa un método de control de acceso de acuerdo con realizaciones de la presente divulgación;
La Figura 6 es un diagrama de flujo que representa un método de control de acceso a la caja fuerte de acuerdo con realizaciones de la presente divulgación; y
La Figura 7 es un diagrama de flujo que representa un método de comprobación de estado de la caja fuerte de acuerdo con realizaciones de la presente divulgación.

Descripción detallada

La divulgación se ilustrará a continuación en conjunto con un sistema de control de acceso ilustrativo. Aunque es bien adecuada para su uso con, (por ejemplo, un sistema que usa lectores y/o credenciales de control de acceso), la divulgación no está limitada a usarse con ningún tipo particular de sistema de control de acceso o configuración de elementos de sistema. Los expertos en la materia reconocerán que las técnicas desveladas pueden usarse en cualquier aplicación de mensajería de datos en la que sea deseable aumentar la eficacia o capacidad de deseo de un proceso de acceso, ya incluya tal proceso añadir, terminar o modificar privilegios de acceso.

Los sistemas y métodos ilustrativos de esta divulgación también se describirán en relación con software de análisis, módulos y hardware de análisis asociado. Sin embargo, para evitar oscurecer innecesariamente la presente divulgación, la siguiente descripción omite estructuras, componentes y dispositivos bien conocidos que pueden mostrarse en forma de diagrama de bloques, que son bien conocidos o se resumen de otra manera.

Para propósitos de explicación, se exponen numerosos detalles para proporcionar un entendimiento minucioso de la presente divulgación. Sin embargo, debería apreciarse, que la presente divulgación puede ponerse en práctica en una diversidad de maneras más allá de los detalles específicos expuestos en el presente documento.

Aunque se describirán a continuación diversas realizaciones de la presente divulgación en relación con la actualización de datos de acceso en una credencial de acceso y, en particular, datos de acceso usados dentro de una instalación de múltiples habitaciones, un experto en la materia apreciará que las realizaciones de la presente divulgación son aplicables, en general, para actualizar cualquier tipo de datos en un dispositivo de identificación portátil o en una memoria portátil. Por lo tanto, los mecanismos y métodos analizados en relación con la realización de una actualización de datos de acceso o proceso de codificación pueden aplicarse para actualizar o codificar cualquier otro tipo de datos (por ejemplo, datos de configuración, datos de seguridad, llaves, *etc.)* de una manera similar sin alejarse del alcance de la presente divulgación.

Haciendo referencia de manera inicial a la Figura 1, se representa un sistema 100 de control de acceso ilustrativo de acuerdo con al menos algunas realizaciones de la presente divulgación. El sistema 100 de control de acceso puede incluir una red 104 de comunicación que se conecta a una pluralidad de módulos 116 de control de acceso y un sistema 128 de programación de credenciales a un dispositivo 108 administrativo, que puede también denominarse como un panel de control.

El dispositivo 108 administrativo puede incluir lógica 132 de control de acceso que, en general, es responsable de administrar el sistema 100 de control de acceso de la instalación de múltiples habitaciones. En otras palabras, la lógica 132 de control de acceso del dispositivo 108 administrativo puede proporcionar una ubicación central para administrar la seguridad de la instalación de múltiples habitaciones. Por ejemplo, la lógica 132 de control de acceso puede conectarse a una base de datos 140 centralizada, que incluye información de reserva de huéspedes (por ejemplo, preferencias de huésped, duración de permanencia, preferencias de cliente, información de contacto de huésped y cualquier otra información que confirme reservas de un huésped en una o más habitaciones 112a-N dentro o en recursos de la instalación de múltiples habitaciones). La lógica 132 de control de acceso puede servir como una fuente central de información de seguridad para los diversos otros componentes del sistema 100 de control de acceso.

La lógica 132 de control de acceso puede adaptarse para responder a solicitudes generadas por los módulos 116 de control de acceso y el sistema 128 de programación de credenciales (por ejemplo, proporcionando información solicitada al dispositivo solicitante o confirmando la precisión de la información proporcionada por el dispositivo solicitante). Como alternativa, o, además, la lógica 132 de control de acceso puede adaptarse para proporcionar instrucciones a los módulos 116 de control de acceso y al sistema 128 de programación de credenciales, permitiendo de esta manera que estos dispositivos administren alguno o todo el sistema 100 de control de acceso sin requerir que tales dispositivos se comuniquen con la lógica 132 de control de acceso durante cada transacción.

El sistema 128 de programación de credenciales está ubicado típicamente en un mostrador 118 o alguna otra ubicación centralizada y segura de la instalación de múltiples habitaciones ya que el sistema 128 de programación de credenciales normalmente se proporciona con las capacidades de escritura de datos de acceso para acceder a las credenciales durante el registro de entrada del huésped. Por lo tanto, en general, se prefiere por los propietarios y operadores de la instalación de múltiples habitaciones mantener un cierto nivel de seguridad sobre el sistema 128 de programación de credenciales, ya que tiene la capacidad de escritura de datos de acceso a las credenciales que podría permitir potencialmente a un titular de la credencial acceder a cualquier recurso dentro de la instalación de múltiples habitaciones. Sin algún nivel de control sobre el sistema 128 de programación de credenciales, podría haber un riesgo aumentado de que los huéspedes escribieran datos de acceso en sus credenciales que superaran los permisos de acceso que se hubieran proporcionado de otra manera al invitado. Por esta razón, casi todas las instalaciones de múltiples habitaciones actuales requieren que un huésped haga un registro de entrada en el mostrador 118, de modo que el huésped pueda obtener una credencial de acceso que tenga datos de acceso escritos en la misma de manera apropiada y precisa.

Los módulos 116 de control de acceso, por otra parte, se proporcionan normalmente para asegurar diversos recursos dentro de la instalación de múltiples habitaciones. Por ejemplo, los módulos 116 de control de acceso pueden proporcionarse en puntos de acceso en diversos recursos físicos (por ejemplo, las habitaciones 112a-n, los pasillos

120, los ascensores 124, las cajas fuertes dentro de las habitaciones 150a-n, la instalación de múltiples habitaciones misma, *etc.).* Los módulos 116 de control de acceso pueden proporcionarse también para asegurar recursos lógicos tales como cuentas de dinero, cuentas de cliente en un restaurante dentro de la instalación de múltiples habitaciones o cuentas de ordenador. Por ejemplo, un restaurante dentro de la instalación de múltiples habitaciones puede permitir que los huéspedes de la instalación de múltiples habitaciones "paguen" comidas colocando el saldo debido en una pestaña asociada con la habitación. Después del registro de salida se supone que el huésped liquidará todas las cuentas y pagará el saldo debido por la habitación y tales comidas. Por consiguiente, algunos restaurantes pueden proporcionar un módulo 116 de control de acceso para asegurar tales cuentas y asegurar que los huéspedes asocian su saldo con la habitación apropiada.

Por supuesto, los módulos 116 de control de acceso pueden comprender funcionalidad adicional, y tal funcionalidad adicional será dependiente de los tipos 136 de credenciales usadas, la red 104 de comunicación, el tipo y/o naturaleza física de la instalación (múltiples edificios geográficamente separados), la naturaleza del negocio (hotel o negocio) y otras consideraciones de diseño. De acuerdo con al menos una realización de la presente divulgación, un conjunto de instrucciones (por ejemplo, firmware, software, datos de configuración y/o datos de seguridad) se encuentra residente en el módulo 116 de control de acceso para soportar y controlar las funciones del módulo 116 de control de acceso.

Para facilitar tales políticas de seguridad, los módulos 116 de control de acceso pueden adaptarse para comunicarse con las credenciales 136 de acceso llevadas por los usuarios o huéspedes de la instalación de múltiples habitaciones mediante protocolos de comunicación sin contacto y/o con contacto. Tales comunicaciones permitirán que los módulos 116 de control de acceso identifiquen la credencial 136 de acceso presentada a los mismos, así como que determinen los permisos de acceso para el titular de la credencial 136 de acceso.

Ejemplos de los protocolos de comunicación empleados por un módulo 116 de control de acceso para comunicarse con una credencial 136 de acceso incluyen, sin limitación, comunicaciones basadas en RF (por ejemplo, ISO 14443A, ISO14443B, ISO 15693, comunicaciones de campo cercano, Bluetooth ®), Zigbee ®, WiFi y cualquier otro tipo de protocolo de comunicación que utilice un campo de RF a 125 kHz o 13,56 MHz), comunicaciones magnéticas, comunicaciones lumínicas, comunicaciones alámbricas que incluyen ISO 7816, $I^2C$, SPI, así como otros protocolos de comunicación conocidos o aún por desarrollar.

En algunas realizaciones, los módulos 116 de control de acceso incluyen capacidades de lectura y escritura (codificación) de RF. Tales módulos 116 de control de acceso pueden denominarse como lectores/escritores. Los módulos 116 de control de acceso con capacidades de lectura y escritura incluyen, en general, una antena de RF para intercambiar mensajes de RF con las credenciales 136 de acceso durante las operaciones de lectura y una antena de RF separada para transmitir mensajes de RF, que codifican las credenciales 136 de acceso durante las operaciones de escritura. Sin embargo, un experto en la materia apreciará que un módulo 116 de control de acceso puede comprender una única antena que se use durante las operaciones tanto de lectura como de escritura.

De acuerdo con al menos algunas realizaciones de la presente divulgación, la red 104 de comunicación está adaptada para llevar mensajes entre los componentes conectados a la misma. Por lo tanto, el dispositivo 108 administrativo está permitido a enviar mensajes a y recibir mensajes desde un módulo 116 de control de acceso y/o sistema 128 de programación de credenciales mediante la red 104 de comunicación. La red 104 de comunicación puede comprender cualquier tipo de red de comunicación conocida que incluye combinaciones alámbricas e inalámbricas de las redes de comunicación y puede abarcar distancias largas o pequeñas. Los protocolos usados por la red 104 de comunicación para facilitar las comunicaciones del controlador 116/módulo 116 de control de acceso pueden incluir, pero sin limitación, el protocolo TCP/IP, el Protocolo Simple de Gestión de Red (SNMP), Alimentación de Ethernet (POE), protocolo Wiegand, RS 232, RS 485, Bucle de Corriente, Bluetooth, Zigbee, GSM, SMS, WiFi y combinaciones de los mismos.

Se desvelan detalles adicionales sobre las realizaciones del sistema 100 de control de acceso y la instalación de múltiples habitaciones en la Publicación de Solicitud de Patente de Estados Unidos N.º 2011/0187493 A1 a Elfstrom titulada "Methods and Systems for Permitting Remote Check-in and Coordinating Access Control".

El sistema 100 de control de acceso incluye adicionalmente cajas fuertes 150a-n en las habitaciones 112a-n, respectivamente. Las cajas fuertes 150a-n están acopladas a un respectivo módulo 117 de acceso. El módulo 117 de acceso está configurado para abrir las cajas fuertes 150a-n y está configurado de manera similar como el módulo 116 de control de acceso como se ha descrito anteriormente, pero con funciones específicas para las cajas fuertes 150a-n. Se usa la credencial 136 de acceso para verificar y abrir las cajas fuertes 150a-n mediante el módulo 117 de acceso. Se describirán adicionalmente a continuación las realizaciones de las cajas fuertes 150a-n y el módulo 117 de acceso.

Con referencia ahora a la Figura 2, se describirán detalles de un módulo 116 de control de acceso ilustrativo de acuerdo con al menos algunas realizaciones de la presente divulgación. El módulo 116 de control de acceso comprende, en general, la capacidad para leer automáticamente datos, típicamente en forma de un objeto de mensaje y/o información de validación de una credencial 136. El módulo 116 de control de acceso también puede escribir datos, típicamente en forma de un objeto de mensaje, de vuelta a la credencial 136. Este proceso también es conocido como codificación de la credencial 136. En algunas realizaciones, el módulo 116 de control de acceso puede estar configurado para leer

en primer lugar un identificador de tarjeta de una credencial 136 y a continuación codificar la credencial 136 con datos de acceso durante la misma transacción.

El módulo 116 de control de acceso, de acuerdo con al menos una realización, comprende una interfaz 216 de comunicación de credencial usada para comunicarse de ida y vuelta con la credencial 136. La interfaz 216 de comunicación de la credencial puede comprender una interfaz de comunicación de RF (por ejemplo, una antena de RF), una interfaz de comunicación magnética (por ejemplo, un lector de banda magnética), una interfaz de comunicación óptica (por ejemplo, un detector y transmisor de infrarrojos), una interfaz de comunicación de contacto eléctrico o cualquier otro medio de comunicación de información a/desde una credencial 136.

Se encuentra conectado a la interfaz 216 de comunicación un controlador o procesador 204. En una realización, el procesador 204 incluye un microprocesador, un generador de números aleatorios y un coprocesador criptográfico. El procesador 204 puede modular/demodular datos de manera apropiada enviados a y recibidos desde los dispositivos externos tales como la credencial 136. El procesador 204 controla y determina cómo se comporta el módulo 116 de control de acceso cuando se le presenta una credencial 136. El procesador 204 puede incluir cualquier procesador programable de propósito general, procesador de señales digitales (DSP) o controlador para ejecutar la programación de la aplicación. Como alternativa, el procesador 204 puede comprender un circuito integrado específico de la aplicación (ASIC) especialmente configurado.

El procesador 204 puede proporcionarse también con circuitería de control que puede manipular un dispositivo de control de acceso. El dispositivo de control de acceso está diseñado para asegurar que un punto de acceso se proteja por el módulo 116 de control de acceso. El procesador 204 está habilitado para comunicarse con el dispositivo de control de acceso mediante una interfaz 212 de red o mediante alguna otra interfaz de control de acceso especializada. Ejemplos de un dispositivo de control de acceso típico incluyen, sin limitación, un cerrojo electrónico, un cerrojo magnético o una cerradura eléctrica para una puerta, un cerrojo para un sistema informático, un cerrojo para una base de datos, un cerrojo para una cuenta financiera o un cerrojo en una aplicación informática. En una realización, el procesador 204 acciona el dispositivo de control de acceso enviando una señal al dispositivo de control de acceso mediante la interfaz 212 de red basándose en los resultados de una decisión de acceso realizada por el procesador 204. Opcionalmente, el dispositivo de control de acceso puede ser integral al módulo 116 de control de acceso en una realización, caso en el que no sería necesaria una interfaz de dispositivo de control de acceso. En una realización alternativa, un dispositivo de control de acceso es externo al módulo 116 de control de acceso, necesitando por lo tanto alguna clase de interfaz entre el módulo 116 de control de acceso y el dispositivo de control de acceso. Ejemplos de una interfaz de dispositivo de control de acceso incluyen cualquier tipo de puerto de datos, tal como un puerto USB, puerto de datos serie, puerto de datos paralelo, un cable convencional, un puerto de comunicación inalámbrica, tal como una interfaz de datos de Bluetooth, un puerto de Ethernet o cualquier otro tipo de interfaz de comunicación alámbrica o inalámbrica.

La interfaz 212 de red también se usa para conectar el módulo 116 de control de acceso a la red 104 de comunicación. Por consiguiente, se reciben paquetes o mensajes de comunicación enviados mediante el módulo 116 de control de acceso inicialmente por el módulo 116 de control de acceso en la interfaz 212 de red. Estos mensajes pueden reenviarse al procesador 204 para su análisis y procesamiento adicional (por ejemplo, decodificación, reformateo y/o extracción de datos). La interfaz 212 de red proporciona capacidades de comunicación entre el módulo 116 de control de acceso y servidores externos u otros nodos de red. Una interfaz de comunicación de este tipo puede incluir un puerto USB, un módem alámbrico, un módem inalámbrico, un adaptador de red tal como una tarjeta de Ethernet y puerto de Ethernet, un puerto de datos serie, un puerto de datos paralelo o cualquier otro adaptador de comunicación o puerto conocido en la técnica. Por supuesto, la interfaz 212 de red puede realizarse realmente como múltiples interfaces de red, para facilitar las comunicaciones con múltiples tipos de red, posiblemente mediante diferentes protocolos de comunicación.

El módulo 116 de control de acceso puede comprender adicionalmente una memoria 208. La memoria 208 puede usarse para almacenar firmware o instrucciones de software que soportan la funcionalidad del módulo 116 de control de acceso. Más específicamente, la memoria 208 puede comprender uno o más módulos que proporcionan al módulo 116 de control de acceso con la capacidad para hacer una determinación de si permitir o denegar el acceso de usuario a un recurso controlado por el módulo de control de acceso, así como ejecutar funciones de registro de entrada normalmente reservadas para el sistema de programación de credenciales.

En algunas realizaciones, la memoria 208 incluye un módulo 220 de registro de entrada y lógica 228 de control de acceso. La lógica 228 de control de acceso proporciona al módulo 116 de control de acceso con la capacidad de leer datos de acceso de credenciales 136 y hacer una determinación en cuanto a si el titular de la credencial 136 está permitido o no a acceder a algún recurso controlado por el módulo 116 de control de acceso. Por lo tanto, la lógica 228 de control de acceso puede facilitar operaciones de lectura de datos de acceso, operaciones de verificación de datos de acceso y operaciones asociadas con el permiso de acceso de usuario a un recurso (por ejemplo, abrir el cerrojo de una puerta, proporcionar acceso a una cuenta, *etc.).*

En algunas realizaciones, se proporciona el módulo 220 de registro de entrada para realizar procedimientos de registro de entrada que tradicionalmente se habían reservado para el sistema 128 de programación de credenciales. En

particular, el módulo 220 de registro de entrada puede estar configurado para recibir un identificador de credencial de una credencial 136 de acceso, comparar el identificador de credencial con una lista de identificadores de credenciales, determinar que el identificador de credencial coincide con al menos un identificador de credencial en la lista de identificadores de credenciales, y, basándose en la determinación de que el identificador de credencial coincide con al menos un identificador de credencial en la lista de identificadores, invocar al módulo de control de acceso para codificar la credencial de acceso con datos de acceso que son usables por la credencial de acceso con otros módulos de control de acceso dentro de la instalación de múltiples habitaciones.

Como puede apreciarse por los expertos en la materia, las funciones y características de la lógica 228 de control de acceso pueden incorporarse en el módulo 220 de registro de entrada y viceversa. No hay requisito de que se proporcionen dos módulos separados y distintos para las funciones de control de acceso y las funciones de registro de entrada. En su lugar, puede configurarse un único módulo para proporcionar toda la funcionalidad descrita en el presente documento. También, es posible que se realicen diversas características de la lógica 228 de control de acceso y del módulo 220 de registro de entrada por otros módulos de la memoria 208, sin alejarse del alcance de la presente divulgación.

Debería apreciarse que para completar una operación de lectura/verificación/codificación, tal como la anteriormente descrita en relación con el módulo 220 de registro de entrada, es importante limitar la cantidad de tiempo que ha de presentarse una credencial 136 al módulo 116 de control de acceso. Por ejemplo, un usuario típico generalmente no tolerará presentar una credencial a un módulo 116 de control de acceso durante más de cinco segundos o así. Por consiguiente, el módulo 116 de control de acceso está habilitado para leer un número de identificación desde la credencial 136, confirmar que el número de identificación desde la credencial 136 coincide con un número de identificación asociado con un huésped que ha confirmado la reserva y está permitido a hacer un registro de entrada en una ubicación distinta del mostrador 118, y codificar la credencial 136 con los datos de acceso apropiados en una cantidad mínima de tiempo.

El almacén 232 de imágenes de datos de acceso puede contener una o más imágenes de datos de acceso que pueden escribirse en una credencial 136. En algunas realizaciones, los datos de acceso contenidos dentro del almacén 232 de imágenes de datos de acceso se formatean específicamente para la instalación de múltiples habitaciones (es decir, en un formato reconocido y usado por otros módulos 116 de control de acceso dentro el sistema 100 de control de acceso) y pueden no necesariamente formatearse para su uso por otras instalaciones, incluso si tales instalaciones tienen módulos 116 de control de acceso similares. Esto permite que se usen códigos y protocolos de sistema de la instalación en una forma distribuida sin tener que usar llaves de la instalación y al mismo tiempo se permite el uso de una credencial de huésped (es decir, una credencial no proporcionada por la instalación).

De acuerdo con al menos algunas realizaciones de la presente divulgación, los datos de acceso pueden incluir uno o más de un código de sitio que identifica la instalación de múltiples habitaciones, una clave de encriptación usada sustancialmente de manera exclusiva por la instalación de múltiples habitaciones, un protocolo de comunicación usado por módulos de control de acceso dentro de la instalación de múltiples habitaciones, un identificador de huésped que identifica sustancialmente de manera inequívoca un usuario de la credencial de acceso dentro de la instalación de múltiples habitaciones, duración de permanencia del huésped, número de habitación, identificadores de servicios añadidos y un conjunto de permisos de acceso que definen si un usuario de la credencial de acceso tiene acceso permitido o denegado a recursos particulares de la instalación de múltiples habitaciones. Algunos o todos los datos del almacén 232 de imágenes de datos de acceso pueden escribirse en una credencial 136, dependiendo del usuario de la credencial 136 y la reserva asociada con el usuario de la credencial 136.

En una divulgación no reivindicada proporcionada para entender el contexto de la invención, el módulo 116 de control de acceso puede escribir datos de acceso adicionales en la credencial 136. Aunque la mayoría de las escrituras de datos de acceso se hacen en el proceso de registro de entrada y las lecturas y verificaciones de datos se hacen en los módulos 116 de control de acceso posteriores, un módulo 116 de control de acceso en una puerta de la habitación de hotel, por ejemplo, puede escribir datos de acceso adicionales en la credencial 136 para proporcionar acceso adicional a controles en la habitación (es decir, un módulo de acceso de la caja fuerte). Los datos de acceso escritos adicionales pueden ser del mismo formato que los datos de acceso como se ha descrito anteriormente, o pueden ser de otro formato que únicamente se usa para verificar los datos de acceso con el control de acceso de la puerta de la habitación y los controles de acceso en la habitación. En un aspecto de la realización, el módulo 116 de control de acceso de la puerta puede codificar datos de acceso usando una clave pública-privada exclusivamente emparejada con el control de acceso a la caja fuerte en la habitación cuando el módulo 116 de control de acceso verifica que la credencial 136 dada está permitida a abrir la caja fuerte, tal como cuando se usa la credencial del huésped a diferencia de una credencial de limpieza. De acuerdo con la invención, el módulo 116 de control de acceso puede comunicarse directamente o de manera inalámbrica con los controles de acceso en la habitación para permitir o no permitir estos accesos.

La memoria 208 puede comprender memoria volátil y/o no volátil. Ejemplos de memoria no volátil incluyen Memoria de Sólo Lectura (ROM), ROM programable borrable (EPROM), PROM Eléctricamente Borrable (EEPROM), memoria Flash y similares. Ejemplos de memoria volátil incluyen Memoria de Acceso Aleatorio (RAM), RAM dinámica (DRAM), RAM estática (SRAM) o memoria intermedia. En una realización, la memoria 208 y el procesador 204 están diseñados

para utilizar características de seguridad conocidas para evitar el acceso no autorizado a los contenidos de la memoria 208, tal como análisis de canal secundario y similares.

Puede incluirse también una fuente de alimentación (no representada) en el módulo 116 de control de acceso para proporcionar alimentación a los diversos dispositivos contenidos dentro del módulo 116 de control de acceso. La fuente de alimentación puede comprender baterías internas y/o un convertidor de CA-CC, tal como una fuente de alimentación de modo conmutado o un regulador de tensión conectado a una fuente de alimentación de CA externa.

Se desvelan detalles adicionales sobre las realizaciones del módulo 116 de control de acceso en la Publicación de la Solicitud de Patente de Estados Unidos N.º US2011/0187493 A1 a Elfstrom ("Elfstrom").

Con referencia ahora a la Figura 3, se describirá una credencial 136 de acceso ilustrativa de acuerdo con al menos algunas realizaciones de la presente divulgación. En algunas realizaciones, se proporciona la credencial 136 con un procesador 304, memoria 308 e interfaz 312 de módulo. El procesador 304 puede incluir un microprocesador, un controlador programable o cualquier otro tipo de unidad de procesamiento que pueda ejecutar las instrucciones almacenadas en la memoria 308. Como alternativa, o, además, el procesador 304 puede realizarse como un Circuito Integrado Específico de la Aplicación (ASIC).

El procesador 304 emplea interfaces bidireccionales para comunicarse con la memoria 308 y la interfaz 312 de módulo. En particular, el procesador 304 facilita los intercambios de datos entre la credencial 136 y un módulo 116 de control de acceso. Tales comunicaciones se manejan en el nivel físico por la interfaz 312 de módulo. Similar a la interfaz 216 de credencial, la interfaz 312 de módulo puede comprender una interfaz de comunicación de RF (por ejemplo, una antena de RF), una interfaz de comunicación magnética (por ejemplo, un lector de banda magnética), una interfaz de comunicación óptica (por ejemplo, un detector y transmisor de infrarrojos), una interfaz de comunicación de contacto eléctrico o cualquier otro medio de comunicación de información a/desde un módulo 116 de control de acceso. Como puede apreciarse por un experto en la materia, la interfaz 312 puede incluir una unidad de modulación/demodulación en lugar de basarse en el procesador 304 para realizar las operaciones de codificación/decodificación, funciones de formateo de mensaje y similares.

La credencial 136 puede fabricarse como un dispositivo de sistema en chip (SoC), un dispositivo de sistema en paquete (SiP) o un dispositivo de sistema en módulo (SiM). En el dispositivo SoC, diversos componentes funcionales están integrados en un único molde. Por consiguiente, en dispositivos SiP y SiM, se combinan varios dispositivos SoC en un único paquete (dispositivo SiP) o un conjunto que incluye dispositivos SoC y/o SiP (dispositivo SiM), respectivamente.

Una credencial 136 "pasiva" usa señales de RF (es decir, radiación de RF) emitida por el módulo 116 de control de acceso como una fuente de energía para alimentar la credencial 136 y sus componentes (principalmente el procesador 304). Cuando una credencial 136 pasiva entra en alcance de un módulo 116 de control de acceso de interrogación, el módulo 116 de control de acceso proporciona alimentación a la credencial 136 mediante una señal de RF de consulta. La credencial 136 pasiva convierte una porción de alimentación de RF recogida por la interfaz 312 de módulo (por ejemplo, una antena dentro de la interfaz 312) en alimentación de CC que facilita la operabilidad de la credencial 136. Una credencial 136 de este tipo puede operar únicamente en la zona activa de un módulo 116 de control de acceso de interrogación y está inactiva de otra manera.

Como alternativa, la credencial 136 puede comprender una fuente de alimentación interna (es decir, integrada), por ejemplo, una o varias baterías y/o células solares (credencial "activa"). En otra realización más, la credencial 136 comprende tanto un rectificador de RF como una fuente de alimentación interna (RFID "semi-activa"). Las RFID activas y semiactivas pueden usarse típicamente en distancias mayores de los módulos 116 de control de acceso que las pasivas, así como pueden proporcionarse con capacidades de cálculo y/o de detección adicionales.

En la operación, el módulo 116 de control de acceso y la credencial 136 usan protocolos de comunicación preprogramados. Para aumentar la probabilidad de recepción sin errores, los mismos mensajes pueden repetirse de manera redundante un número predeterminado de veces o durante un intervalo de tiempo predeterminado. Los protocolos y los matices de los mismos pueden definirse dentro de los datos 320 de acceso que se codifican en la credencial 136. En algunas realizaciones, se programan porciones de estos datos 320 de acceso en la credencial 136 antes de que un huésped haga el registro de entrada en la instalación de múltiples habitaciones y se codifican otras porciones de los datos 320 de acceso en la credencial 136 durante el proceso de registro de entrada. Por ejemplo, la información del protocolo de comunicación puede ser datos preprogramados mientras que se programa el número de habitación, duración de permanencia y otros datos usados para determinar privilegios de acceso únicamente durante el proceso de registro de entrada. Esta restricción y separación de programación de datos de acceso permite a la instalación de múltiples habitaciones para mantener un cierto nivel de control sobre el sistema 100 de control de acceso.

El módulo 316 de comunicación puede facilitar las comunicaciones entre la credencial 136 y el módulo 116 de control de acceso. En algunas realizaciones, el módulo 316 de comunicación hace referencia a los datos 320 de acceso para asegurar que se usa el protocolo de comunicación apropiado por la credencial 136 al comunicarse con el módulo 116

de control de acceso. En algunas realizaciones, si la credencial 136 se ha programado únicamente con la cantidad mínima de datos 320 acceso, o no tiene datos 320 de acceso en absoluto (por ejemplo, el usuario de la credencial 136 no ha hecho el registro de entrada con la instalación de múltiples habitaciones), el módulo 316 de comunicación puede proporcionar una UID 324 de credencial a un módulo 116 de control de acceso cuando se interroga la credencial 136 por un módulo 116 de control de acceso. La UID 324 de credencial puede comprender cualquier tipo de número de identificación, nombre, símbolo *etc.* que identifica de manera inequívoca o casi inequívoca la credencial 136 o un titular de la credencial 136 al módulo 116 de control de acceso. Esta UID 324 de credencial puede programarse en la credencial 136 después del aprovisionamiento y puede asegurarse en una porción de sólo lectura de la memoria 308 para asegurar que no se haya modificado o manipulado.

Además, la credencial 136 puede soportar opcionalmente una escritura por el módulo 116 de control de acceso sucesivamente además del proceso de registro de entrada inicial. En una realización ilustrativa, los datos 320 de acceso pueden escribirse para incluir nueva información de acceso o datos de acceso adicionales por un módulo 116 de control de acceso en una puerta de habitación de hotel cuando se presenta la credencial 136 a ese módulo 116 de control de acceso.

Por consiguiente, la memoria 308 puede ser similar a la memoria 208 del módulo 116 de control de acceso, en que la memoria 308 puede incluir una o más de ROM, EPROM, EEPROM, memoria Flash y similares.

Como puede apreciarse por los expertos en la materia, la credencial 136 de acceso puede proporcionarse en cualquier tipo de factor de forma sin alejarse del alcance de la presente divulgación. En algunas realizaciones, la credencial de acceso puede comprender una tarjeta o dispositivo de RFID que tiene funcionalidad similar como un teléfono móvil, teléfono inteligente, tableta, PDA, lector de libro electrónico, reproductor de música portátil o similares. En otras realizaciones, la credencial 136 de acceso puede comprender una tarjeta de banda magnética. En otras realizaciones más, la credencial 136 de acceso puede comprender un llavero. Otros factores de forma conocidos para los expertos en la materia también serán fácilmente evidentes después de revisar la divulgación actual.

Con referencia ahora a la Figura 4, se describirán detalles de un módulo 116 de acceso a la caja fuerte ilustrativo de acuerdo con al menos algunas realizaciones de la presente divulgación. El módulo 117 de acceso a la caja fuerte comprende, en general, la capacidad de leer automáticamente datos, típicamente en forma de un objeto de mensaje y/o información de validación de una credencial 136. El módulo 117 de acceso a la caja fuerte también puede escribir datos, típicamente en forma de un objeto de mensaje, de vuelta a la credencial 136. Este proceso también es conocido como codificación de la credencial 136. En algunas realizaciones, el módulo 116 de acceso a la caja fuerte puede estar configurado para leer en primer lugar un identificador de tarjeta de una credencial 136 y a continuación codificar la credencial 136 con datos de acceso durante la misma transacción. En otras realizaciones, el módulo 136 de acceso a la caja fuerte no necesita escribir necesariamente en la credencial 136.

El módulo 117 de acceso a la caja fuerte, de acuerdo con al menos una realización, comprende una interfaz 416 de comunicación de credencial usada para comunicarse de ida y vuelta con la credencial 136. La interfaz 416 de comunicación de la credencial puede comprender una interfaz de comunicación de RF (por ejemplo, una antena de RF), una interfaz de comunicación magnética (por ejemplo, un lector de banda magnética), una interfaz de comunicación óptica (por ejemplo, un detector y transmisor de infrarrojos), una interfaz de comunicación de contacto eléctrico o cualquier otro medio de comunicación de información a/desde una credencial 136.

Se encuentra conectado a la interfaz 416 de comunicación un controlador o procesador 404. En una realización, el procesador 404 incluye un microprocesador, un generador de números aleatorios y un coprocesador criptográfico. El procesador 404 puede modular/demodular datos de manera apropiada enviados a y recibidos desde los dispositivos externos tales como la credencial 136. El procesador 404 controla y determina cómo se comporta el módulo 117 de acceso a la caja fuerte cuando se le presenta una credencial 136. El procesador r04 puede incluir cualquier procesador programable de propósito general, procesador de señales digitales (DSP) o controlador para ejecutar la programación de la aplicación. Como alternativa, el procesador r04 puede comprender un circuito integrado específico de la aplicación (ASIC) especialmente configurado.

Opcionalmente, el procesador 404 puede proporcionarse también con circuitería de control que puede manipular un dispositivo de control de acceso. El dispositivo de control de acceso está diseñado para asegurar un punto de acceso de que se proteja por el módulo 117 de acceso a la caja fuerte. El procesador 404 está habilitado para comunicarse con el dispositivo de control de acceso mediante una interfaz 414 de red opcional o mediante alguna otra interfaz de control de acceso especializada, tal como la interfaz 422 mecánica. Ejemplos de un dispositivo de control de acceso típico incluyen, sin limitación, un cerrojo electrónico, un cerrojo magnético o una cerradura eléctrica para una puerta, un cerrojo para un sistema informático, un cerrojo para una base de datos, un cerrojo para una cuenta financiera o un cerrojo en una aplicación informática. En una realización, el procesador 404 acciona el dispositivo de control de acceso enviando una señal al dispositivo de control de acceso mediante la interfaz 414 de red basándose en los resultados de una decisión de acceso realizada por el procesador 404. Sin embargo, el dispositivo de control de acceso puede ser integral al módulo 117 de acceso a la caja fuerte en una realización, tal como la interfaz 422 mecánica, caso en el que no sería necesaria una interfaz de dispositivo de control de acceso. En una realización alternativa, un dispositivo de control de acceso es externo al módulo 117 de acceso a la caja fuerte, necesitando por lo tanto alguna clase de

interfaz entre el módulo 117 de acceso a la caja fuerte y el dispositivo de control de acceso. Ejemplos de una interfaz de dispositivo de control de acceso incluyen cualquier tipo de puerto de datos, tal como un puerto USB, puerto de datos serie, puerto de datos paralelo, un cable convencional, un puerto de comunicación inalámbrica, tal como una interfaz de datos de Bluetooth, un puerto de Ethernet o cualquier otro tipo de interfaz de comunicación alámbrica o inalámbrica.

La interfaz 414 de red opcional también se usa para conectar el módulo 117 de acceso a la caja fuerte a la red 104 de comunicación. Por consiguiente, los paquetes o mensajes de comunicación enviados por el módulo 117 de acceso a la caja fuerte se reciben inicialmente por el módulo 117 de acceso a la caja fuerte en la interfaz 414 de red. Estos mensajes pueden reenviarse al procesador 404 para su análisis y procesamiento adicional (por ejemplo, decodificación, reformateo y/o extracción de datos). La interfaz 414 de red proporciona capacidades de comunicación entre el módulo 117 de acceso a la caja fuerte y los servidores externos u otros nodos de red. Una interfaz de comunicación de este tipo puede incluir un puerto USB, un módem alámbrico, un módem inalámbrico, un adaptador de red tal como una tarjeta de Ethernet y puerto de Ethernet, un puerto de datos serie, un puerto de datos paralelo o cualquier otro adaptador de comunicación o puerto conocido en la técnica. Por supuesto, la interfaz 414 de red puede realizarse realmente como múltiples interfaces de red, para facilitar las comunicaciones con múltiples tipos de red, posiblemente mediante diferentes protocolos de comunicación.

El módulo 117 de acceso a la caja fuerte puede comprender adicionalmente una memoria 408. La memoria 408 puede usarse para almacenar firmware o instrucciones de software que soportan la funcionalidad del módulo 117 de acceso a la caja fuerte. Más específicamente, la memoria 408 puede comprender uno o más módulos que proporcionan al módulo 117 de acceso a la caja fuerte con la capacidad para hacer una determinación de si permitir o denegar el acceso de usuario a un recurso controlado por el módulo de control de acceso, así como ejecutar funciones de registro de entrada normalmente reservadas para el sistema de programación de credenciales.

La memoria 408 puede incluir un módulo 431 de seguridad.

En algunas realizaciones, el módulo 431 de seguridad proporciona autenticación de seguridad de la credencial 136 de acceso. Como la interfaz 414 de red puede no estar presente en el módulo 117 de acceso a la caja fuerte, el módulo 117 de acceso a la caja fuerte, a diferencia del módulo 116 de control de acceso, por ejemplo, puede no poder acceder a una lista de identificadores de credenciales a través de la red y de la base de datos central para comparar con la credencial recibida desde la interfaz 416 de credencial. Además, el módulo 117 de acceso a la caja fuerte puede desear no comparar directamente la credencial recibida con la lista de identificadores de credenciales incluso si el módulo 117 de acceso a la caja fuerte tiene la interfaz 414 de red y puede acceder a la red ya que puede haber una necesidad de un protocolo de seguridad más estricto para abrir la caja fuerte y evitar un ataque de hombre en el medio entre la interfaz 414 de red y la red y la base de datos central. En este caso, el módulo 431 de seguridad actúa para verificar que algún otro módulo de acceso, es decir, el módulo 116 de control de acceso en la puerta de la habitación, haya verificado que el módulo 117 de acceso a la caja fuerte conceda acceso a la caja fuerte para la credencial 136 de acceso dada. En un aspecto de la realización, esto puede hacerse con un par de clave pública-privada exclusivo entre el módulo 116 de control de acceso y el módulo 117 de acceso a la caja fuerte. En otros aspectos de la realización, el módulo 116 de control de acceso y el módulo 117 de acceso a la caja fuerte pueden comunicarse directa o inalámbricamente, (es decir, a través de la red de ZigBee según se desvela en la Patente de Estados Unidos N.° 8.102.799 a Alexander et al. titulada "Centralized Wireless Network for Multi-Room Large Properties"), para verificar que la credencial 136 puede abrir la caja fuerte. El módulo 117 de acceso a la caja fuerte usa la interfaz 422 mecánica para operar los mecanismos mecánicos, es decir, abrir el cerrojo de las bisagras que aseguran la puerta de la caja fuerte, para abrir físicamente la caja fuerte.

La memoria 408 puede comprender memoria volátil y/o no volátil. Ejemplos de memoria no volátil incluyen Memoria de Sólo Lectura (ROM), ROM programable borrable (EPROM), PROM Eléctricamente Borrable (EEPROM), memoria Flash y similares. Ejemplos de memoria volátil incluyen Memoria de Acceso Aleatorio (RAM), RAM dinámica (DRAM), RAM estática (SRAM) o memoria intermedia. En una realización, la memoria 408 y el procesador 404 están diseñados para utilizar características de seguridad conocidas para evitar el acceso no autorizado a los contenidos de la memoria 408, tal como análisis de canal secundario y similares.

Una fuente de alimentación (no representada) puede incluirse también en el módulo 117 de acceso a la caja fuerte para proporcionar alimentación a los diversos dispositivos contenidos dentro del módulo 117 de acceso a la caja fuerte. La fuente de alimentación puede comprender baterías internas y/o un convertidor de CA-CC, tal como una fuente de alimentación de modo conmutado o un regulador de tensión conectado a una fuente de alimentación de CA externa.

Haciendo referencia ahora a la Figura 5, se desvela un método ilustrativo de control de acceso con niveles 500 de acceso en cascada de acuerdo con algunas realizaciones de la divulgación. En este punto, habitación hace referencia a una habitación de huésped en una instalación de múltiples habitaciones, pero puede hacer también referencia a otras áreas que están controladas en acceso. De manera similar, caja fuerte hace referencia a un área de almacenamiento cerrada con cerrojo, pero también puede hacer referencia, en general, a otros almacenes o dispositivos controlados en acceso que requieren un nivel de acceso separado dentro de la habitación general.

En primer lugar, el método 500 registra la habitación y la información 510 de acceso a la caja fuerte en una credencial de acceso. En algunas realizaciones, la información de habitación y de acceso a la caja fuerte se almacena en una credencial de acceso durante el proceso de registro de entrada en el que el sistema comprueba que el huésped ha confirmado una reserva a una habitación particular en una instalación de múltiples habitaciones. La información de acceso a esa habitación particular y, normalmente, a la caja fuerte dentro de esa habitación y a otras áreas de la instalación a las que se considera que el huésped tiene acceso, se almacena en la credencial de acceso. En otras realizaciones, la información de acceso puede enviarse electrónicamente a la credencial de acceso (es decir, mediante correo electrónico o mediante otros métodos como es conocido en la técnica).

A continuación, el huésped presenta la credencial de acceso en un módulo 520 de control de acceso de la habitación. En algunas realizaciones, la presentación de la credencial en el módulo de control de acceso hace que la credencial transmita uno o más mensajes al módulo de control de acceso que incluye su número de identificación de credencial y cualquier otra información de identificación pertinente (es decir, la información de acceso registrada en la etapa 510).

A continuación, el módulo de control de acceso lee la información de acceso de credencial y determina privilegios 530 de acceso. El módulo de control de acceso puede tomar decisiones de permiso de acceso basándose en la información de acceso de credencial. En algunas realizaciones, la información de acceso de credencial proporcionará información de acceso necesaria que el módulo de control de acceso puede comprobar contra su lista precargada o a través de una consulta a una base de datos en la red. Como alternativa, la información de acceso incluye información de verificación, como es conocido en la técnica, de manera que la credencial de acceso puede autenticar automáticamente a ese módulo de control de acceso particular, que es la credencial de acceso que pertenece al huésped y que ha dado permiso específico para acceso por el sistema a través de un proceso de registro de entrada apropiado o similar. El fallo de la credencial para proporcionar información de acceso válida dará como resultado que el módulo de control de acceso mantenga su recurso bajo condiciones seguras.

A continuación, el módulo de control de acceso comprueba si está permitido 540 el acceso a la caja fuerte dentro de la habitación. En algunas realizaciones, el módulo de control de acceso podrá determinar privilegios de acceso a la caja fuerte a partir de la lectura de la información de acceso de credencial en la etapa 530. Si el acceso a la caja fuerte no está permitido, a continuación, el módulo de control de acceso permitirá el acceso a la habitación, pero no completará procedimientos adicionales para activar el acceso a la caja fuerte 542.

Si se determina que el acceso a la caja fuerte está permitido en la etapa 540, se activa 541 el acceso a la caja fuerte. El módulo de control de acceso de la habitación envía directamente o de manera inalámbrica instrucciones al módulo de acceso de la caja fuerte para informar al módulo de acceso de la caja fuerte para permitir el acceso a la credencial. En un aspecto de una realización, el acceso a la caja fuerte puede estar limitado adicionalmente por tiempo u otro protocolo de seguridad, por ejemplo, desactivarse automáticamente cuando se presenta una credencial sin acceso a la caja fuerte al módulo de control de acceso de la habitación, para asegurar adicionalmente que el acceso está únicamente activado cuando el huésped está en la habitación, pero no para otros.

Haciendo referencia ahora a la Figura 6, se desvela un método ilustrativo de control de acceso a la caja fuerte 600 de acuerdo con algunas realizaciones de la divulgación.

En primer lugar, se presenta una credencial de acceso al módulo 610 de acceso de la caja fuerte. En algunas realizaciones, la información de acceso de la caja fuerte se almacena en una credencial de acceso durante el proceso de registro de entrada en el que el sistema comprueba que el huésped ha confirmado una reserva en la habitación particular en una instalación de múltiples habitaciones y con permiso de acceso a la caja fuerte dentro de la habitación. En una divulgación no reivindicada proporcionada para entender el contexto de la invención, puede almacenarse la información de activación de acceso a la caja fuerte adicional mediante el módulo de control de acceso de la habitación particular cuando se presenta la credencial de acceso para entrar en la habitación, de manera que la caja fuerte puede activarse únicamente cuando se presenta en primer lugar la credencial para entrar en la habitación. De acuerdo con la invención, el módulo de control de acceso de la habitación envía directamente o de manera inalámbrica información de acceso a la caja fuerte cuando se presenta la credencial al módulo de control de acceso de la habitación.

A continuación, la caja fuerte autentica el acceso a la caja fuerte basándose en la credencial 620 presentada. En algunas realizaciones, el módulo de acceso de la caja fuerte puede comprobar tanto que la credencial tiene permitido el acceso a la caja fuerte como que el módulo de control de acceso de la habitación ha activado el acceso a la caja fuerte. Opcionalmente, puede autenticarse el acceso a la caja fuerte a través de la base de datos en la red 621. Aun opcionalmente, pueden comprobarse los contenidos en la caja fuerte para observar si soportan el acceso 622. Por ejemplo, el sistema puede conceder a alguna otra persona distinta del huésped (es decir una persona de la limpieza, acceso a la caja fuerte únicamente si la caja fuerte está vacía).

Si está permitido 630 el acceso a la caja fuerte, se abre 631 la caja fuerte. Se registra 640 el intento de acceso a la caja fuerte satisfactorio. Si el acceso a la caja fuerte no está permitido 630, no se abre la caja fuerte y se registra 640 el intento de acceso a la caja fuerte no satisfactorio. En algunas realizaciones, pueden registrarse los intentos de acceso en el servidor y puede accederse y visualizarse a través de un dispositivo externo (es decir un ordenador o teléfono). En algunos aspectos de la realización, los intentos de acceso a la caja fuerte no satisfactorios pueden activar

automáticamente una alerta a las personas apropiadas o pueden analizarse por un algoritmo para observar si debería alertarse a las personas apropiadas.

Haciendo referencia ahora a la Figura 7, se desvela un método ilustrativo de la comprobación 700 de estado de contenido de la caja fuerte de acuerdo con algunas realizaciones de la divulgación. En algunos casos, puede ser deseable asegurar que la caja fuerte esté cerrada con cerrojo y asegurada cuando el huésped haya dejado la habitación para proporcionar seguridad adicional debido a los errores humanos.

En primer lugar, el método 700 comprueba si hay algún contenido presente en la caja fuerte y si la caja fuerte está abierta 710 con cerrojo. Puede realizarse la comprobación 710 de contenidos en la caja fuerte mediante sensores como es conocido en la técnica. Si no hay contenido en la caja fuerte o la caja fuerte está cerrada con cerrojo, el método se detiene 740.

A continuación, el método 700 comprueba si el huésped está en la habitación 720. La comprobación 720 puede hacerse mediante diversos sensores en las habitaciones como es conocido en la técnica. En algunas realizaciones, la credencial de acceso usada por el huésped puede conectarse inalámbricamente al sistema de la instalación, es decir, Zigbee; la presencia detectada de la credencial puede indicar que el huésped aún está en la habitación ya que es necesaria la credencial para acceder a diversas partes de la instalación. Si el huésped aún está en la habitación, la comprobación 720 puede realizarse continuamente o en algún intervalo de tiempo hasta que no haya contenido presente en la caja fuerte, la caja fuerte está cerrada con cerrojo o el huésped ha dejado la habitación.

Si el huésped ha dejado la habitación, el huésped está informado del estado de la caja fuerte con el cerrojo abierto con los contenidos 730. El huésped puede estar informado por un método y/o dispositivo preferido elegido previamente (es decir, en el registro de entrada). Por ejemplo, el teléfono del huésped, que puede actuar también como una credencial de acceso, puede estar conectado a una red inalámbrica (es decir, 4G), y puede recibir información acerca del estado de la caja fuerte. En algunas realizaciones, el huésped podrá también emitir comandos limitados mediante este dispositivo inalámbrico en la caja fuerte, tal como cerrar y cerrar con cerrojo la caja fuerte de manera remota.

Aunque se han analizado los diagramas de flujo anteriormente descritos en relación con una secuencia particular de eventos, debería apreciarse que pueden tener lugar cambios en esta secuencia sin afectar de manera material a la operación de la divulgación. Adicionalmente, la secuencia exacta de eventos no es necesario que tenga lugar como se expone en las realizaciones ilustrativas. Las técnicas ilustrativas ilustradas en el presente documento no están limitadas a las realizaciones específicamente ilustradas, sino que pueden utilizarse también con las otras realizaciones ilustrativas y cada característica descrita puede reivindicarse de manera individual y separada.

La presente divulgación, en diversas realizaciones, incluye componentes, métodos, procesos, sistemas y/o aparatos sustancialmente como se representan y describen en el presente documento, que incluyen diversas realizaciones, subcombinaciones y subconjuntos de las mismas. Los expertos en la materia entenderán cómo hacer y usar la presente divulgación después de entender la presente divulgación. La presente divulgación, en diversas realizaciones, incluye proporcionar dispositivos y procesos en ausencia de elementos no representados y/o descritos en el presente documento o en diversas realizaciones del mismo, incluyendo en ausencia de tales elementos como pueden haberse usado en dispositivos o procesos anteriores (por ejemplo, para mejorar el rendimiento, conseguir facilidad y/o reducir el coste de la implementación).

Adicionalmente, los sistemas, métodos y protocolos de esta divulgación pueden implementarse en un ordenador de propósito especial, un microprocesador o microcontrolador programado y elemento o elementos de circuito integrado periféricos, un ASIC u otro circuito integrado, un procesador de señales digitales, un circuito electrónico o lógico preprogramado, tal como un circuito de elemento discreto, un dispositivo de lógica programable, tal como un PLD, PLA, FPGA, PAL, un dispositivo de comunicaciones, tal como un teléfono, cualquier medio comparable o similares. En general, cualquier dispositivo que pueda implementar una máquina de estado que pueda a su vez implementar la metodología ilustrada en el presente documento puede usarse para implementar los diversos métodos, protocolos y técnicas de comunicación de acuerdo con esta divulgación.

El análisis anterior de la divulgación se ha presentado para propósitos de ilustración y descripción. Lo anterior no se pretende que limite la divulgación a la forma o formas desveladas en el presente documento. En la descripción detallada anterior, por ejemplo, se agrupan juntas diversas características de la divulgación en una o más realizaciones para el propósito de simplificar la divulgación. Este método de divulgación no ha de interpretarse como que refleja una intención de que la divulgación reivindicada requiera más características que las expresamente indicadas en cada reivindicación. En su lugar, como reflejan las siguientes reivindicaciones, los aspectos inventivos radican en menos de todas las características de una única realización desvelada anterior. Además, aunque la descripción de la divulgación ha incluido la descripción de una o más realizaciones y ciertas variaciones y modificaciones, otras variaciones y modificaciones se encuentran dentro del alcance de la divulgación (por ejemplo, como puede estar dentro de la experiencia y del conocimiento de los expertos en la materia, después de entender la presente divulgación).

**REIVINDICACIONES**

1. Un método (500, 600) de control de acceso a la caja fuerte, que comprende:

a) un módulo (116) de control de acceso de habitación de una habitación de hotel que determina (520) que un usuario ha presentado una credencial (136) de acceso;
b) leer (530) el módulo (116) de control de acceso de la habitación la información de acceso de la habitación y de la caja fuerte desde la credencial (136) y determinar privilegios basándose en la misma;
c) en caso de información de acceso de la habitación inválida, mantener el módulo (116) de control de acceso de la habitación el control de acceso de la habitación bajo condiciones seguras;
d) en caso de información de acceso de la habitación válida, determinar (540) el módulo (116) de control de acceso de la habitación si está permitido el acceso a la caja fuerte dentro de la habitación, usando la información de acceso de la caja fuerte;
e) si no está permitido el acceso a la caja fuerte dentro de la habitación, permitir el módulo (116) de control de acceso de la habitación el acceso a la habitación, pero no activar el acceso a la caja fuerte (150);
f) si está permitido (540) el acceso a la caja fuerte dentro la habitación, activar el módulo (116) de control de acceso de la habitación el acceso a la caja fuerte (150) enviando directamente o de manera inalámbrica instrucciones al módulo (117) de control de acceso a la caja fuerte de una caja fuerte (150) en la habitación para informar al módulo (117) de control de acceso a la caja fuerte para permitir el acceso a la credencial;
g) determinar (610) el módulo (117) de control de acceso a la caja fuerte que un usuario ha presentado una credencial (136) de acceso;
h) autenticar el módulo (117) de control de acceso a la caja fuerte el acceso (620) a la caja fuerte basándose en la credencial (136) de acceso presentada comprobando que tanto
h1) la credencial tiene acceso a la caja fuerte permitido y
h2) se activó el acceso a la caja fuerte por el módulo (116) de control de acceso de la habitación.

2. El método de la reivindicación 1, en donde la credencial (136) de acceso corresponde a un dispositivo (136) de comunicación móvil.

3. El método de la reivindicación 1, que comprende adicionalmente: accionar un mecanismo de cerrojo de la caja fuerte en la habitación cuando se autentica el acceso a la caja fuerte.

4. El método de la reivindicación 3, en donde el segundo módulo (117) de control de acceso a la caja fuerte intercambia comunicaciones con la credencial (136) de acceso usando comunicaciones de campo cercano (NFC) y comprendiendo el método adicionalmente:

escribir información de registro de control de acceso desde la caja fuerte en la habitación de vuelta a la credencial (136) de acceso para indicar que la credencial (136) de acceso tenía permitida la admisión en la caja fuerte en la habitación.

5. Un sistema de seguridad de habitación de hotel, que comprende un módulo (116) de control de acceso de la habitación configurado para una habitación de hotel y un módulo (117) de control de acceso a la caja fuerte; en donde el módulo (116) de control de acceso de la habitación está configurado para:

a) determinar que un usuario ha presentado una credencial (136) de acceso;
b) leer la información de acceso de la habitación y de la caja fuerte desde la credencial (136) y determinar privilegios basándose en la misma;
c) en caso de información de acceso de la habitación inválida, mantener el control de acceso de la habitación bajo condiciones seguras
d) en caso de información de acceso de la habitación válida, determinar si está permitido el acceso a la caja fuerte dentro de la habitación, usando la información de acceso de la caja fuerte;
e) si el acceso a la caja fuerte dentro la habitación no está permitido, permitir el acceso a la habitación, pero no activar el acceso a la caja fuerte (150);
f) si está permitido (540) el acceso a la caja fuerte dentro de la habitación, activar el acceso a la caja fuerte (150) enviando directamente o de manera inalámbrica instrucciones al módulo (117) de control de acceso a la caja fuerte configurado para que una caja fuerte (150) en la habitación informe al módulo (117) de control de acceso a la caja fuerte para permitir el acceso a la credencial;
y en donde el módulo (117) de control de acceso a la caja fuerte está configurado para:
g) determinar que un usuario ha presentado una credencial (136) de acceso;
h) autenticar el acceso (620) de la caja fuerte basándose en la credencial (136) de acceso presentada comprobando que tanto
h1) la credencial tiene acceso a la caja fuerte permitido y
h2) se activó el acceso a la caja fuerte por el módulo (116) de control de acceso de la habitación.

6. El sistema de la reivindicación 5, en donde la credencial (136) de acceso y el segundo módulo de control de acceso a la caja fuerte están configurados para (117) intercambiar comunicaciones usando comunicaciones de campo cercano (NFC).

7. El sistema de la reivindicación 5, en donde la caja fuerte (150a-n) comprende adicionalmente una interfaz configurada para comunicarse con el módulo (117) de control de acceso a la caja fuerte de la habitación en la que está ubicada la caja fuerte (150a-n).

8. El sistema de la reivindicación 7, en donde la interfaz comprende una interfaz inalámbrica.

9. El sistema de la reivindicación 8, en donde la caja fuerte (150a-n) está configurada para intercambiar uno o más mensajes con el módulo (117) de control de acceso a la caja fuerte para ayudar a determinar si una credencial (136) de acceso presentada a la caja fuerte (150a-n) está permitida a acceder al interior de la caja fuerte (150a-n).

10. El sistema de la reivindicación 5, que comprende adicionalmente un mecanismo de cerrojo que está configurado para accionarse basándose en decisiones recibidas desde el módulo de control de acceso a la caja fuerte.

11. El sistema de la reivindicación 6, en donde la caja fuerte (150a-n) está configurada adicionalmente para escribir un registro de control de acceso de vuelta a la credencial (136) de acceso, en donde el registro de control de acceso de vuelta a la credencial (136) de acceso describe los eventos de control de acceso asociados con la caja fuerte (150a-n).

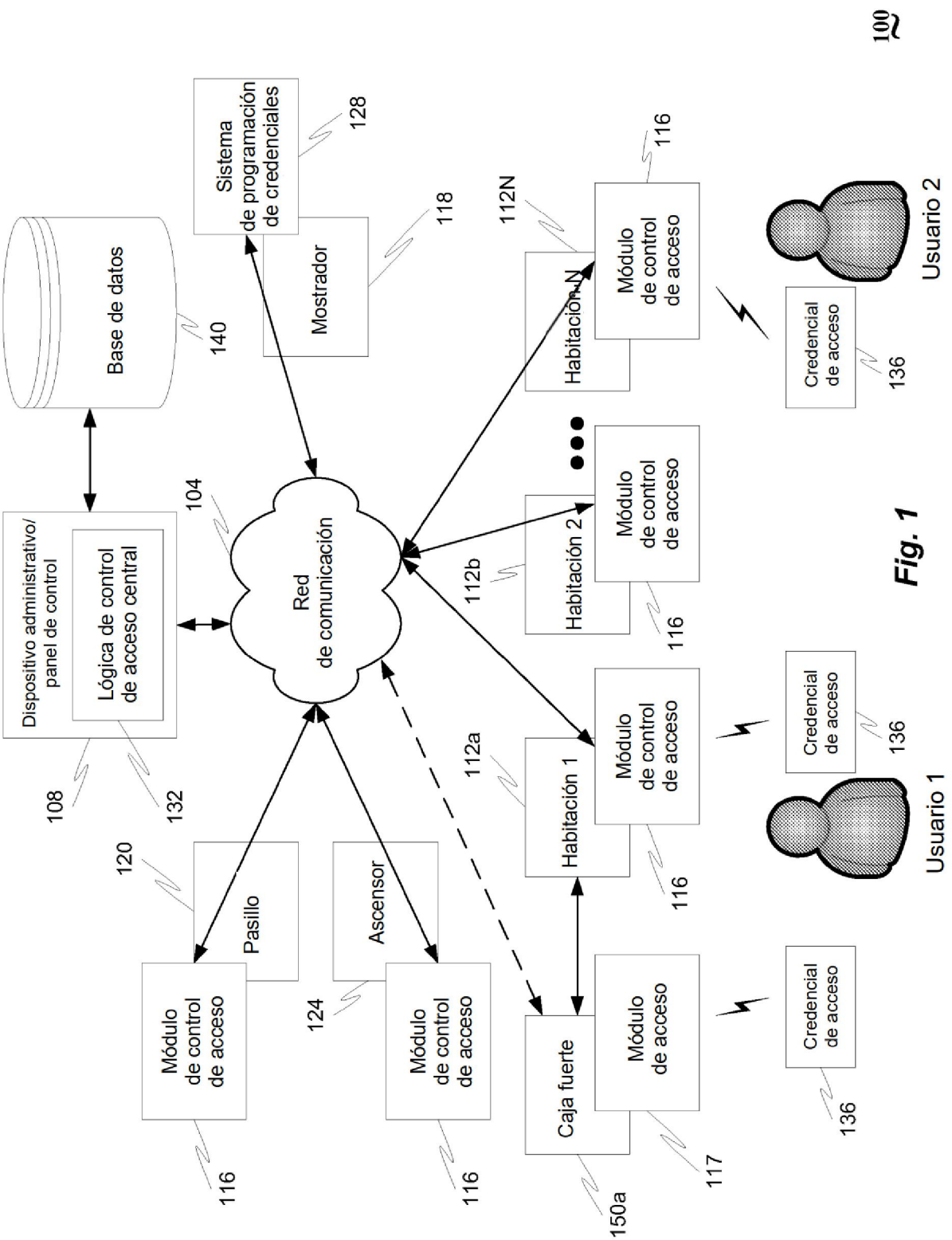

100
Sistema de programación de credenciales
128
Base de datos
140
Mostrador
118
112N
116
Habitación N
Módulo de control de acceso
Usuario 2
Credencial de acceso
136
104
Red de comunicación
Dispositivo administrativo/ panel de control
Lógica de control de acceso central
108
132
112b
Habitación 2
Módulo de control de acceso
116
112a
Habitación 1
Módulo de control de acceso
116
Credencial de acceso
136
Usuario 1
120
Pasillo
Ascensor
124
Módulo de control de acceso
116
Módulo de control de acceso
116
Caja fuerte
Módulo de acceso
117
150a
Credencial de acceso
136

Fig. 1

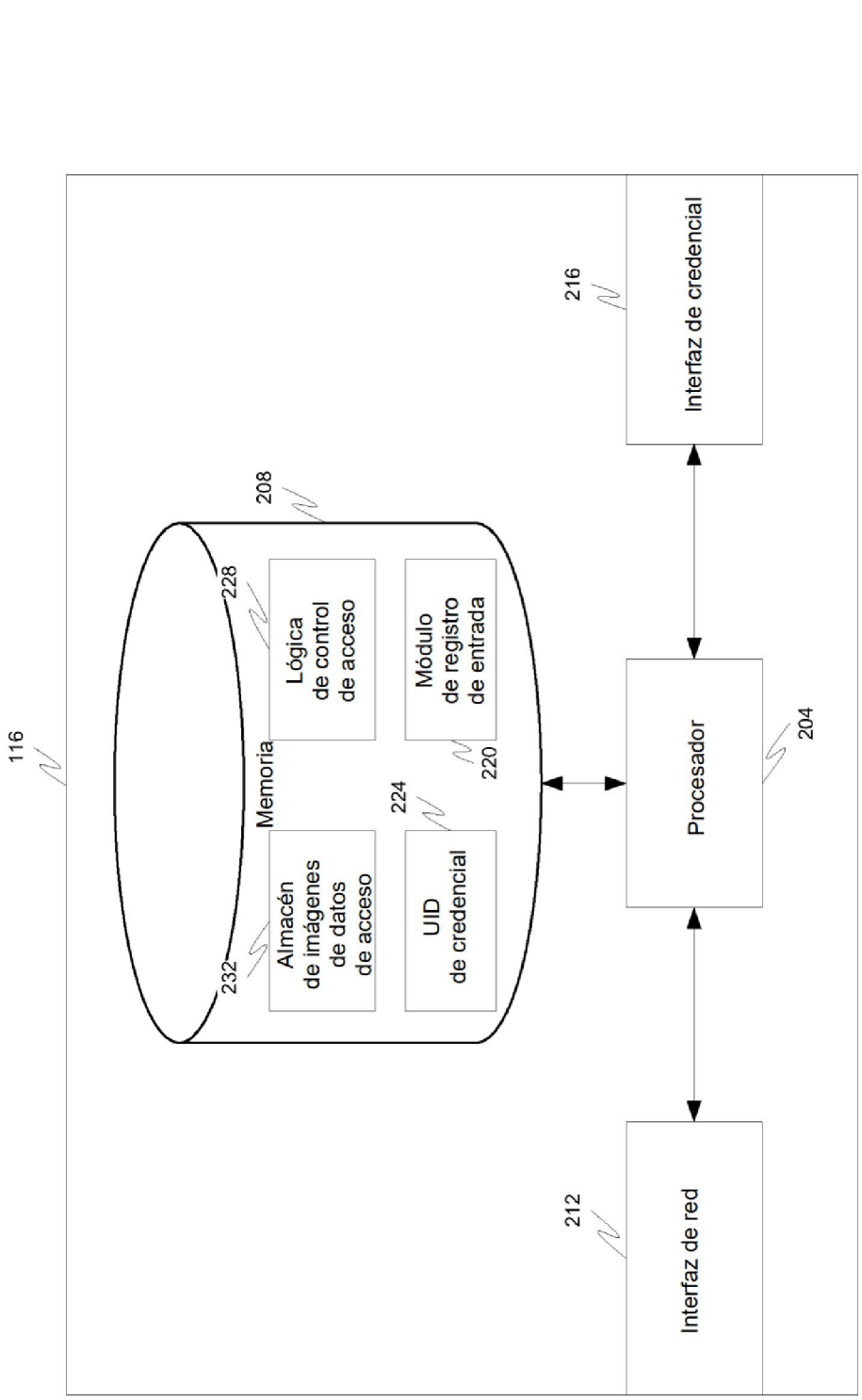

200
116
208
Memoria
228
Lógica de control de acceso
Módulo de registro de entrada
220
224
UID de credencial
Almacén de imágenes de datos de acceso
232
Procesador
204
216
Interfaz de credencial
212
Interfaz de red

*Fig. 2*

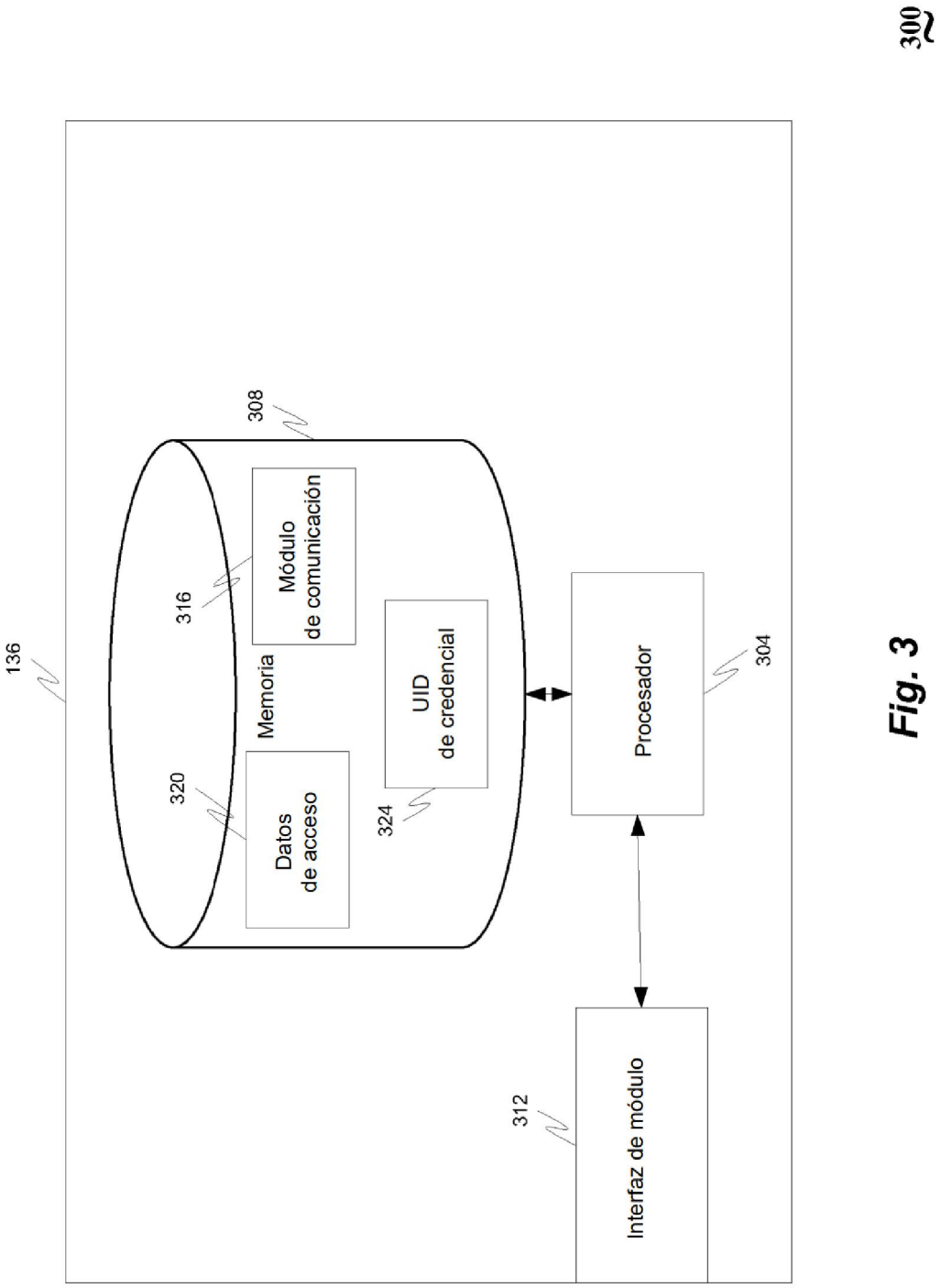

300
136
308
316
Módulo de comunicación
Memoria
320
Datos de acceso
324
UID de credencial
Procesador
304
312
Interfaz de módulo

*Fig. 3*

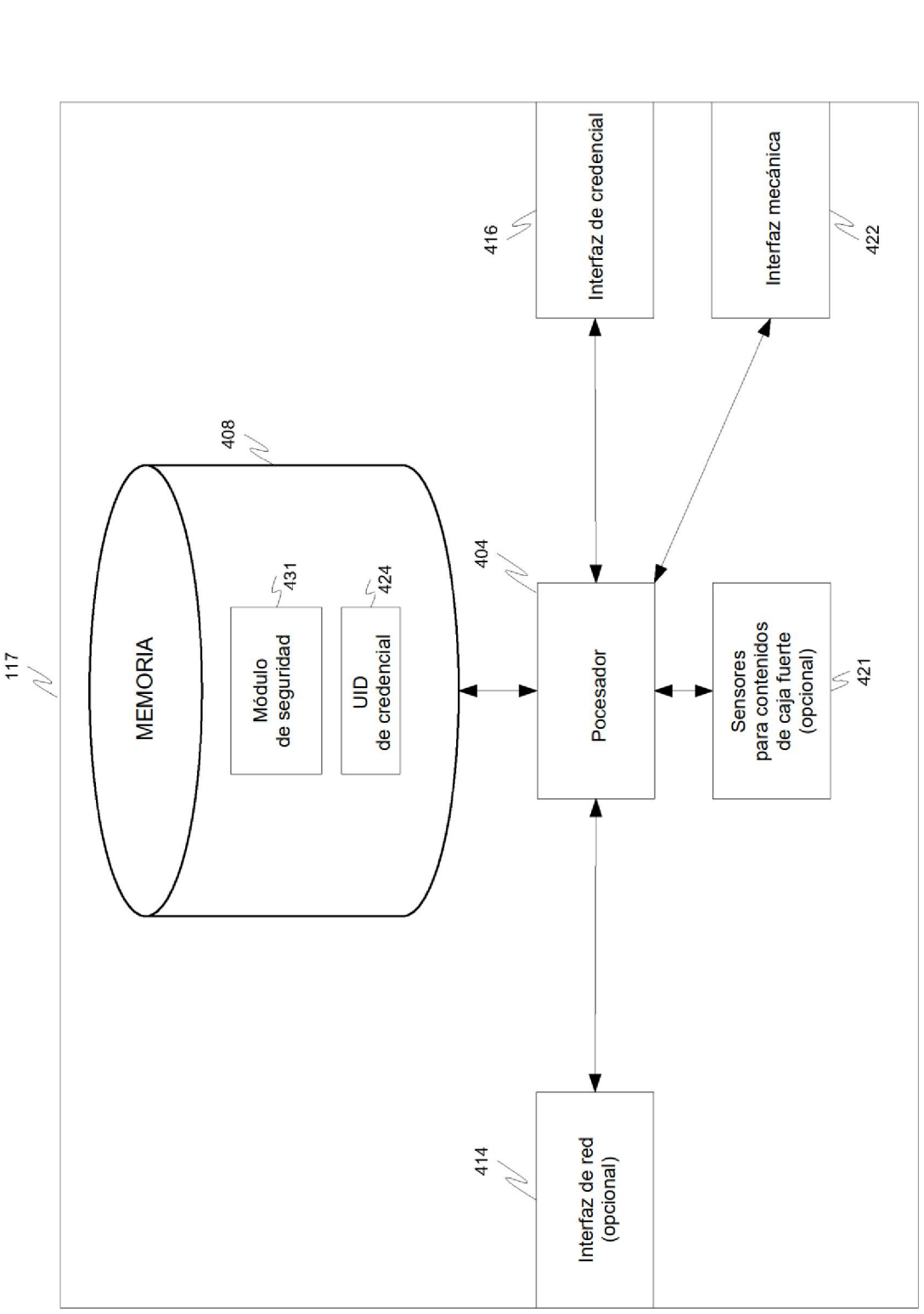

400
117
MEMORIA
408
Módulo de seguridad
431
UID de credencial
424
404
Procesador
416
Interfaz de credencial
422
Interfaz mecánica
421
Sensores para contenidos de caja fuerte (opcional)
414
Interfaz de red (opcional)

Fig. 4

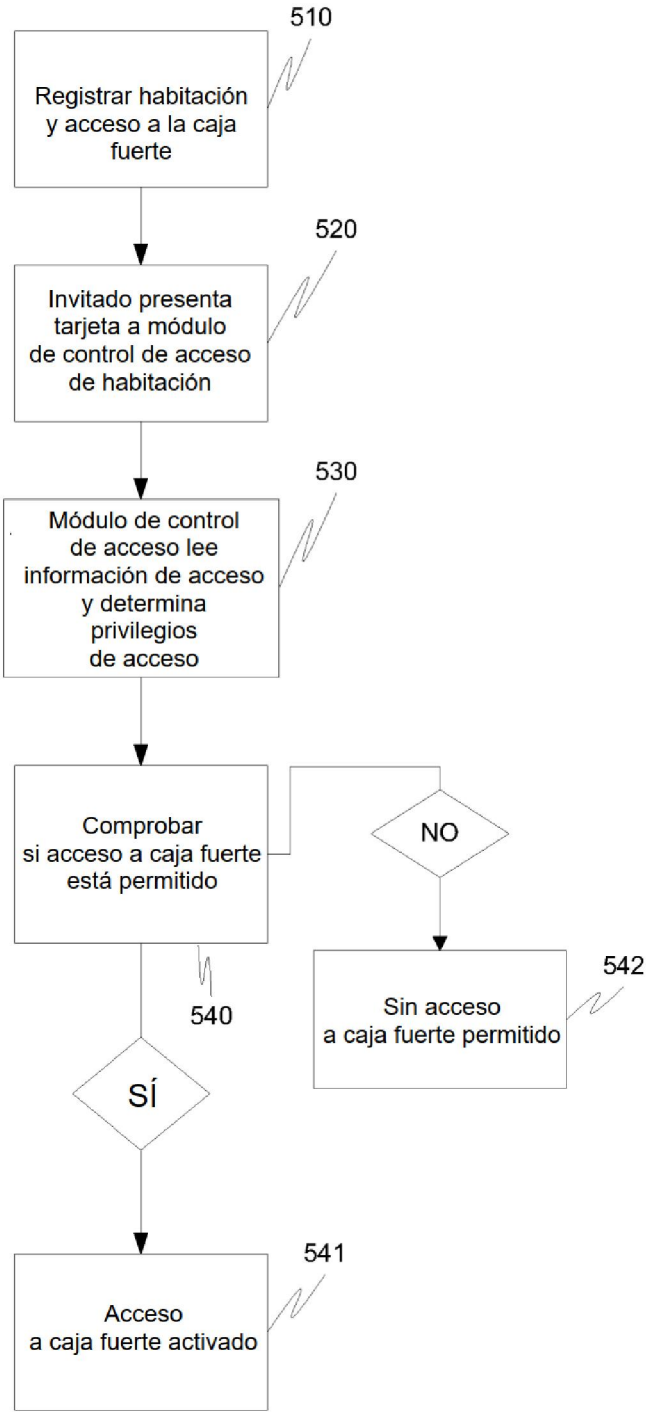

510
Registrar habitación y acceso a la caja fuerte
520
Invitado presenta tarjeta a módulo de control de acceso de habitación
530
Módulo de control de acceso lee información de acceso y determina privilegios de acceso
Comprobar si acceso a caja fuerte está permitido
NO
Sin acceso a caja fuerte permitido
542
540
SÍ
Acceso a caja fuerte activado
541

**Fig. 5**

500

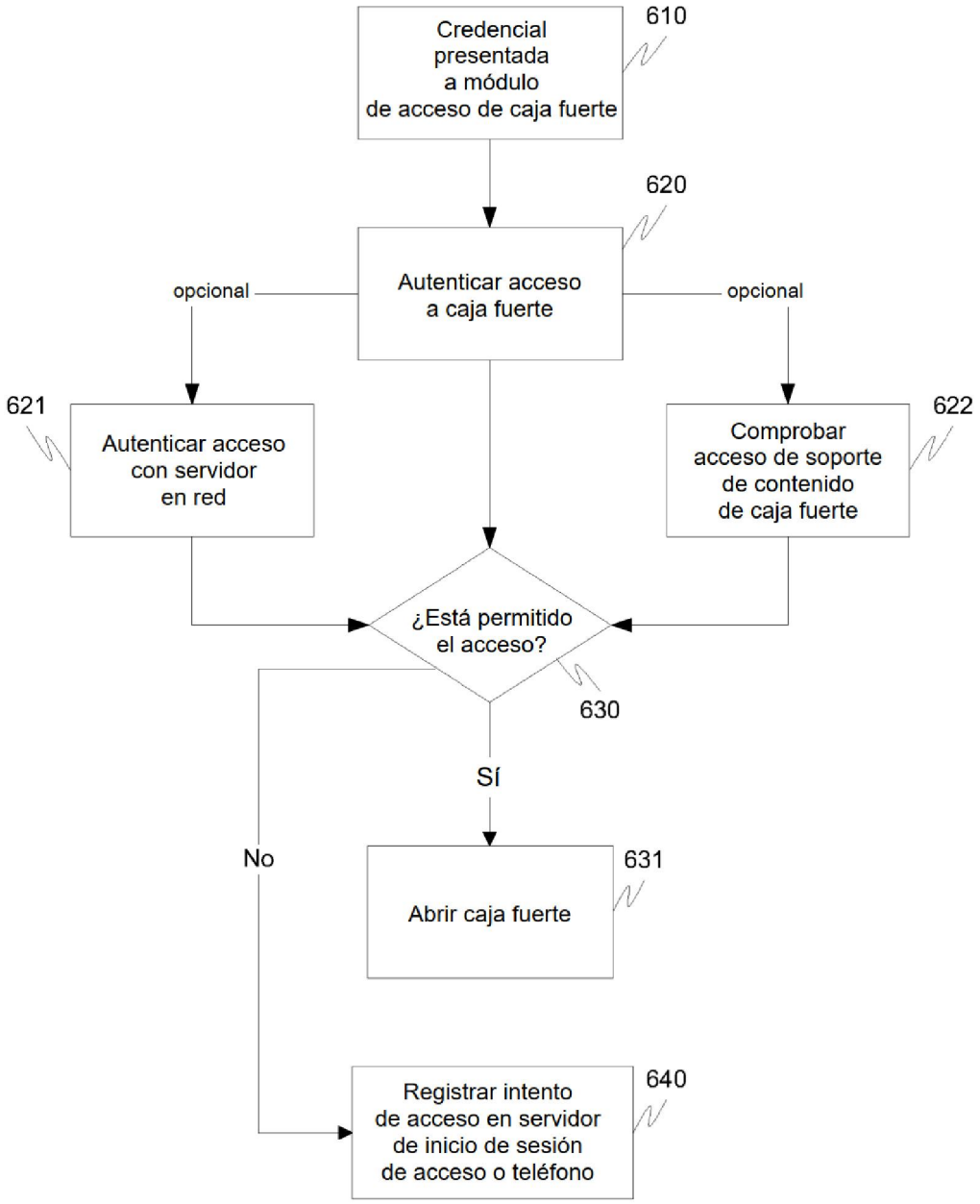
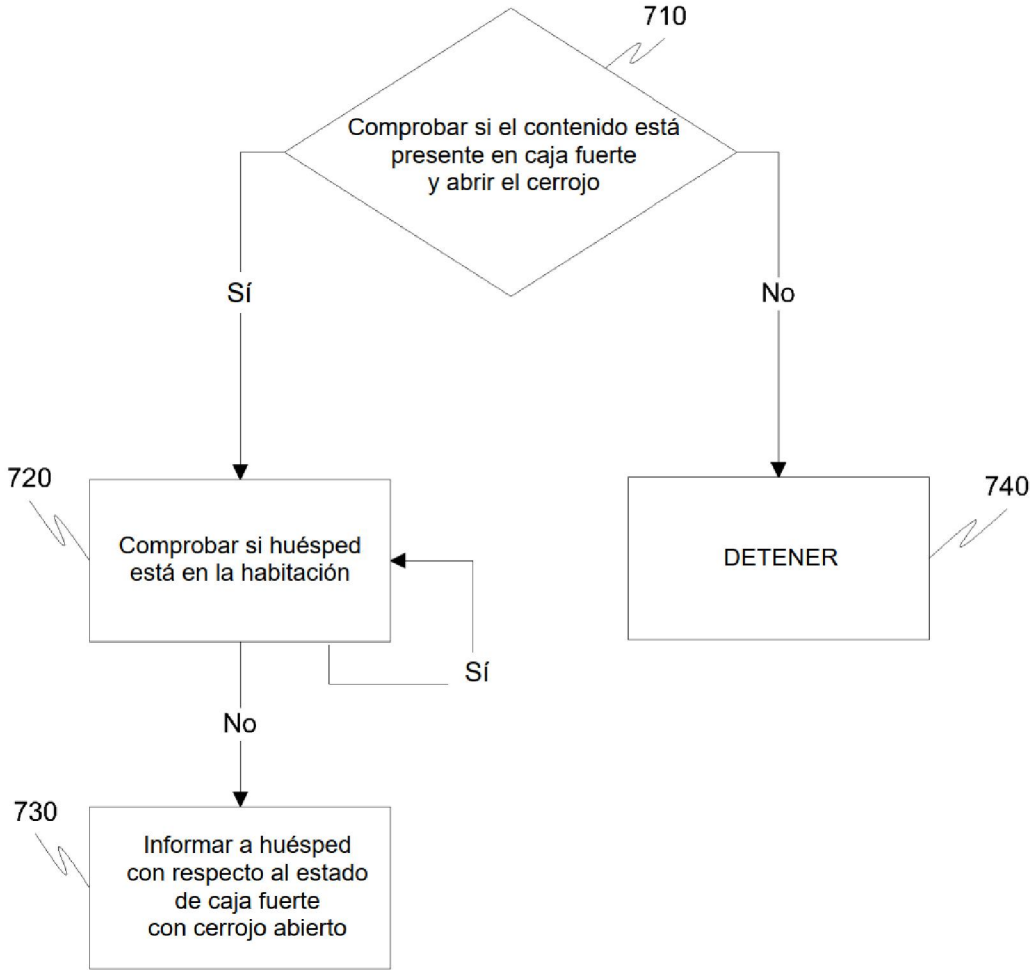

Credencial presentada a módulo de acceso de caja fuerte
610
620
Autenticar acceso a caja fuerte
opcional
opcional
621
Autenticar acceso con servidor en red
622
Comprobar acceso de soporte de contenido de caja fuerte
¿Está permitido el acceso?
630
Sí
No
631
Abrir caja fuerte
640
Registrar intento de acceso en servidor de inicio de sesión de acceso o teléfono
600

*Fig. 6*


710
Comprobar si el contenido está presente en caja fuerte y abrir el cerrojo
Sí
No
720
Comprobar si huésped está en la habitación
Sí
No
740
DETENER
730
Informar a huésped con respecto al estado de caja fuerte con cerrojo abierto

700

*Fig. 7*