(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 940 450**

(51) Int. CI.:

G07C 9/00 (2010.01)
G06Q 10/00 (2012.01)
G07C 9/22 (2010.01)
G07C 9/27 (2010.01)
G06Q 10/02 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.04.2010 E 20195767 (7)**

(97) Fecha y número de publicación de la concesión europea: **14.12.2022 EP 3806046**

(54) Título: **Método y sistema para permitir el registro remoto y coordinar el control de acceso**

(30) Prioridad:

29.01.2010 US 697044

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.05.2023

(73) Titular/es:

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

(72) Inventor/es:

ELFSTRÖM, JAN;
KJÄLLMAN, MARTIN;
ALEXANDER, ARNON y
AASE, HALVOR

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método y sistema para permitir el registro remoto y coordinar el control de acceso

Campo de la invención

La presente invención se relaciona en general con sistemas, métodos y dispositivos de control de acceso y, más en particular, con mecanismos de control de acceso adecuados de forma correcta para su uso en instalaciones de múltiples habitaciones.

Antecedentes de la invención

Las instalaciones de múltiples habitaciones o *suites*, como hoteles, edificios de apartamentos, complejos de oficinas, dormitorios, edificios de oficinas, aulas, cruceros, instalaciones de laboratorios y estructuras similares tienen muchos dispositivos que, si se monitorean y/o controlan de una manera que actualmente no se ha hecho, generará nuevas funcionalidades en las áreas de seguridad de la instalación, eficiencia operativa de la instalación y mantenimiento de la instalación (para el operador de la instalación y el usuario de la instalación) y generará una reducción general de costes en la gestión y el mantenimiento de la instalación.

Un problema que se encuentra con frecuencia al visitar un hotel como huésped es la molestia de hacer fila en la recepción, particularmente durante el registro. Dado que las cerraduras de hotel estándar requieren que las tarjetas estén codificadas de forma única con información tal como la duración de la estadía del huésped, el número de habitación y otras preferencias, tales como el acceso a las salas comunes, el spa y los servicios adicionales, etc., usualmente no hay otra alternativa que registrarse en la recepción para que un huésped obtenga una tarjeta de acceso debidamente codificada.

El documento US 2009/066476 A1 divulga un método de control de acceso por autoservicio para huéspedes frecuentes de una instalación de alojamiento. El documento GB 2 251 266 A1 divulga un sistema codificado de cerradura/llave con desactivación. El documento US 2007/176739 A1 divulga un método y sistema multifuncional sin llaves y sin tarjetas para operar y administrar de manera segura instalaciones de alojamiento con cerraduras electrónicas para puertas. El documento US 2003/208386 A1 divulga reservas, registros, controles de acceso, salidas y pagos inalámbricos.

Breve descripción de la invención

Por lo tanto, un aspecto de la presente divulgación es proporcionar un mecanismo más inteligente para administrar el funcionamiento de una instalación de múltiples habitaciones. Más específicamente, los aspectos de la presente divulgación proporcionan métodos, sistemas y dispositivos que permiten a un huésped o usuario de una instalación de múltiples habitaciones registrarse de forma remota y evitar la molestia de hacer fila en la recepción.

La presente divulgación proporciona mecanismos que permiten a un huésped que ya ha confirmado reservas de forma remota para que proceda a un módulo de control de acceso dentro de la instalación de múltiples habitaciones (es decir, un lector de credenciales de acceso que no se encuentra en los servicios para huéspedes o en el mostrador de recepción) y tener datos de acceso automáticamente por escrito en su credencial de acceso. En consecuencia, un huésped no solo puede pasar por alto la recepción para registrarse, sino que también puede hacer que sus datos de acceso personalizados a las instalaciones se escriban en su credencial de acceso personal mediante módulos de control de acceso ubicados dentro de las instalaciones de múltiples habitaciones.

De acuerdo con la invención, se proporciona un método de acuerdo con la reivindicación 7 adjunta.

De acuerdo con la invención, se proporciona un módulo de control de acceso de acuerdo con la reivindicación 1 adjunta.

La breve descripción de la invención no pretende ni debe interpretarse como representativa de la dimensión y el alcance completos de la presente invención. La presente invención se establece en diversos niveles de detalle y la breve descripción, así como en los dibujos adjuntos y en la descripción detallada de la invención y no se pretende limitar el alcance de la presente invención según se define en las reivindicaciones adjuntas por la inclusión o la no inclusión de elementos, componentes, etc., en la breve descripción de la invención. Aspectos adicionales de la presente invención resultarán más evidentes a partir de la descripción detallada, particularmente cuando se toman en conjunto con los dibujos.

Breve descripción de los dibujos

La Fig. 1 es un diagrama de bloques que representa una instalación de múltiples habitaciones de acuerdo con aspectos de la presente divulgación;

la Fig. 2 es un diagrama de bloques que representa un módulo de control de acceso de acuerdo con realizaciones de la presente invención;

la Fig. 3 es un diagrama de bloques que representa una credencial de acceso de acuerdo con realizaciones de la presente invención;

la Fig. 4 es un diagrama de bloques que representa un método de confirmación de reserva de acuerdo con aspectos de la presente divulgación;

la Fig. 5 es un diagrama de flujo que representa un método de registro del huésped de acuerdo con realizaciones de la presente invención; y

la Fig. 6 es un diagrama de flujo que representa un método de control de acceso de acuerdo con realizaciones de la presente invención.

Descripción detallada de la invención

La invención se ilustrará a continuación en conjunto con un sistema de control de acceso ejemplar. Aunque es adecuada para su uso con, por ejemplo, un sistema que utiliza lectores de control de acceso y/o credenciales, la invención no se limita al uso con ningún tipo particular de sistema de control de acceso o configuración de elementos del sistema. Los expertos en la técnica reconocerán que las técnicas divulgadas se pueden usar en cualquier aplicación de mensajería de datos en la que sea deseable aumentar la eficacia o la conveniencia de un proceso de acceso, ya sea que tal proceso incluya agregar, terminar o alterar los privilegios de acceso.

Los sistemas y métodos ejemplares de esta invención también se describirán en relación con el *software* de análisis, los módulos y el *hardware* de análisis asociado. Sin embargo, para evitar oscurecer innecesariamente la presente invención, la siguiente descripción omite estructuras, componentes y dispositivos bien conocidos que pueden mostrarse en forma de diagrama de bloques, que son bien conocidos o que se describen brevemente de otro modo.

Se establecen numerosos detalles con fines de explicación a fin de proveer una comprensión minuciosa de la presente invención. Debe apreciarse, sin embargo, que la presente invención se puede practicar en una diversidad de formas más allá de los detalles específicos que se establecen en este documento.

A pesar de que a continuación se describirán diversas realizaciones de la presente invención en relación con la actualización de los datos de acceso en una credencial de acceso y, en particular, los datos de acceso usados dentro de una instalación de múltiples habitaciones, un experto en la técnica apreciará que las realizaciones de la presente invención son generalmente aplicables a la actualización de cualquier tipo de datos en un dispositivo portátil de identificación o memoria portátil. De este modo, los mecanismos y métodos expuestos en relación con la realización de un proceso de codificación o actualización de datos de acceso se pueden aplicar para actualizar o codificar cualquier otro tipo de datos (por ejemplo, datos de configuración, datos de seguridad, claves, etc.) de manera similar sin alejarse del alcance de la presente invención.

Con referencia inicial a la Fig. 1, se representa un sistema de control de acceso 100 de ejemplo de acuerdo con al menos algunos aspectos de la presente divulgación. El sistema de control de acceso 100 puede incluir una red de comunicación 104 que conecta una pluralidad de módulos de control de acceso 116 y un sistema de programación de credenciales 128 a un dispositivo administrativo 108, que también puede denominarse un panel de control.

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

La lógica de control de acceso 132 se puede adaptar para responder a las solicitudes generadas por los módulos de control de acceso 116 y el sistema de programación de credenciales 128 (por ejemplo, al proporcionar la información solicitada al dispositivo solicitante o al confirmar la precisión de la información proporcionada por el dispositivo solicitante). Alternativamente, o además, la lógica de control de acceso 132 se puede adaptar para proporcionar instrucciones a los módulos de control de acceso 116 y al sistema de programación de credenciales 128, permitiendo de esa manera que estos dispositivos administren parte o la totalidad del sistema de acceso seguro 100 sin requerir que tales dispositivos se comuniquen con la lógica de control de acceso 132 durante cada operación.

El sistema de programación de credenciales 128 usualmente se encuentra en una recepción 118 o en alguna otra ubicación centralizada y segura de la instalación de múltiples habitaciones, dado que el sistema de programación de credenciales 128 usualmente está provisto con la capacidad de escribir datos de acceso para acceder a las credenciales durante el registro del huésped. De este modo, los propietarios y operadores de la instalación de múltiples habitaciones

generalmente prefieren mantener un cierto nivel de seguridad sobre el sistema de programación de credenciales 128, dado que tiene la capacidad de escribir datos de acceso a las credenciales que podrían permitirle al titular de la credencial acceder a cualquier activo dentro de la instalación de múltiples habitaciones. Sin algún nivel de control sobre el sistema de programación de credenciales 128, podría haber un mayor riesgo de que los invitados escriban datos de acceso en sus credenciales que excedan los permisos de acceso que de otro modo se proporcionarían al invitado. Por esta razón, casi todas las instalaciones actuales de múltiples habitaciones requieren que un huésped se registre en la recepción 118 de forma que el huésped pueda obtener una credencial de acceso que tenga datos de acceso escritos en esta de forma correcta y precisa.

Por otro lado, los módulos de control de acceso 116, usualmente se proporcionan para asegurar diversos activos dentro de la instalación de múltiples habitaciones. Por ejemplo, los módulos de control de acceso 116 se pueden proporcionar en los puntos de acceso a diversos activos físicos (por ejemplo, habitaciones 112a-N, pasillos 120, ascensores 124, cajas fuertes dentro de las habitaciones, la propia instalación de múltiples habitaciones, etc.). Los módulos de control de acceso 116 también se pueden proporcionar para asegurar activos lógicos tales como cuentas de dinero, cuentas de clientes 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” las comidas al colocar el saldo adeudado en una pestaña asociada con la habitación. Al momento de la salida, se asume que el huésped saldará todas las cuentas y pagará el saldo adeudado por la habitación y tales comidas. En consecuencia, algunos restaurantes pueden proporcionar un módulo de control de acceso 116 para asegurar tales cuentas y garantizar que los invitados asocien su saldo con la habitación apropiada.

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

Para facilitar tales políticas de seguridad, los módulos de control de acceso 116 se pueden adaptar para comunicarse con las credenciales de acceso 136 que llevan los usuarios o invitados de la instalación de múltiples habitaciones a través de protocolos de comunicación sin contacto y/o basados en contacto. Tales comunicaciones permitirán que los módulos de control de acceso 116 identifiquen la credencial de acceso 136 que se les presentó, así como determinar los permisos de acceso para el titular de la credencial de acceso 136.

Ejemplos de protocolos de comunicación empleados por un módulo de control de acceso 116 para comunicarse con una credencial de acceso 136 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, por ejemplo), comunicaciones basadas en magnetismo, comunicaciones basadas en luz, comunicaciones por cable, incluidas ISO 7816,1^{2}C, SPI, así como otras comunicaciones conocidas o protocolos de comunicación aún por desarrollar.

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

De acuerdo con al menos algunos aspectos de la presente divulgación, la red de comunicación 104 está adaptada para llevar mensajes entre los componentes conectados a esta. De este modo, el dispositivo administrativo 108 puede enviar y recibir mensajes desde un módulo de control de acceso 116 y/o un sistema de programación de credenciales 128 a través de la red de comunicación 104. La red de comunicación 104 puede comprender cualquier tipo de red de comunicación conocida, incluidas redes de comunicación por cable e inalámbricas o combinaciones de redes de comunicación y puede abarcar distancias largas o cortas. Los protocolos usados por la red de comunicación 104 para facilitar las comunicaciones del controlador 116/módulo de control de acceso 116 pueden incluir, pero no se limitan a estos, protocolo TCP/IP, protocolo simple de administración de red (SNMP [por sus siglas en inglés]), alimentación de ethernet (POE [por sus siglas en inglés]), Protocolo Wiegand, RS 232, RS 485, CurrentLoop, Bluetooth, Zigbee, GSM, SMS, WiFi y combinaciones de estos.

Con referencia ahora a la Fig. 2, se describirán los detalles de un módulo de control de acceso 116 ejemplar de acuerdo con al menos algunas realizaciones de la presente invención. El módulo de control de acceso 116 generalmente comprende la capacidad de leer datos automáticamente, usualmente en la forma de un objeto de mensaje y/o de información de validación, desde una credencial 136. El módulo de control de acceso 116 también es capaz de escribir de regreso datos en la credencial 136, usualmente en la forma de un objeto de mensaje. Este proceso también se conoce como codificación de la credencial 136. El módulo de control de acceso 116 está configurado para leer primero un

identificador de tarjeta de una credencial 136 y después codificar la credencial 136 con datos de acceso durante la misma operación.

El módulo de control de acceso 116, de acuerdo con al menos una realización, comprende una interfaz de comunicación de credencial 216 usada para comunicarse de ida y vuelta con la credencial 136. La interfaz de comunicación de credencial 216 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 interfaz, o cualquier otro medio para comunicar información a/desde una credencial 136.

Conectado a la interfaz de comunicación 216 hay 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 es capaz de modular/demodular adecuadamente los datos enviados y recibidos desde dispositivos externos tales como la credencial 136. El procesador 204 controla y determina cómo se comporta el módulo de control de acceso 116 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 aplicaciones. Alternativamente, el procesador 204 puede comprender un circuito integrado específico de aplicación (ASIC [por sus siglas en inglés]) especialmente configurado.

El procesador 204 también puede estar provisto de circuitería de control capaz de manipular un dispositivo de control de acceso. El dispositivo de control de acceso está diseñado para asegurar un punto de acceso protegido por el módulo de control de acceso 116. El procesador 204 está habilitado para comunicarse con el dispositivo de control de acceso a través de una interfaz de red 212 o a través de alguna otra interfaz de control de acceso dedicada. Los ejemplos de un dispositivo usual de control de acceso incluyen, sin limitación, una cerradura electrónica, una cerradura magnética o una cerradura eléctrica para una puerta, un bloqueo para un sistema informático, un bloqueo para una base de datos, un bloqueo para una cuenta financiera o un bloqueo en una aplicación informática. En una realización, el procesador 204 activa el dispositivo de control de acceso mediante el envío de una señal al dispositivo de control de acceso a través de la interfaz de red 212 con base en los resultados de una decisión de acceso realizada por el procesador 204. Opcionalmente, el dispositivo de control de acceso puede ser parte integral del módulo de control de acceso 116 en una realización, en cuyo caso 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 de control de acceso 116, por lo que necesita algún tipo de interfaz entre el módulo de control de acceso 116 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, un puerto de datos en serie, un puerto de datos paralelo, un cable convencional, un puerto de comunicación inalámbrica, tal como una interfaz de datos Bluetooth, un puerto Ethernet o cualquier otro tipo de interfaz de comunicación por cable o inalámbrica.

La interfaz de red 212 también se usa para conectar el módulo de control de acceso 116 a la red de comunicación 104. En consecuencia, los paquetes de comunicación o mensajes enviados por el módulo de control de acceso 116 son recibidos inicialmente por el módulo de control de acceso 116 en la interfaz de red 212. Estos mensajes se pueden reenviar al procesador 204 para su posterior análisis y procesamiento (por ejemplo, decodificación, reformateo y/o extracción de datos). La interfaz de red 212 proporciona capacidades de comunicación entre el módulo de control de acceso 116 y servidores externos u otros nodos de red. Tal interfaz de comunicación puede incluir un puerto USB, un módem con cable, un módem inalámbrico, un adaptador de red tal como una tarjeta Ethernet y un puerto Ethernet, un puerto de datos en serie, un puerto de datos paralelo o cualquier otro adaptador o puerto de comunicación conocido en la técnica. Por supuesto, la interfaz de red 212 de hecho se puede materializar como múltiples interfaces de red, para facilitar las comunicaciones con múltiples tipos de redes, posiblemente a través de diferentes protocolos de comunicación.

El módulo de control de acceso 116 comprende además una memoria 208. La memoria 208 se usa para almacenar instrucciones de *firmware* o *software* que admiten la funcionalidad del módulo de control de acceso 116. Más específicamente, la memoria 208 comprende uno o más módulos que proporcionan al módulo de control de acceso 116 la capacidad de tomar una determinación para permitir o denegar el acceso del usuario a un activo controlado por el módulo de control de acceso, así como ejecutar funciones de registro normalmente reservadas para el sistema de programación de credenciales.

La memoria 208 incluye un módulo de registro 220 y una lógica de control de acceso 228. La lógica de control de acceso 228 proporciona al módulo de control de acceso 116 la capacidad de leer los datos de acceso de las credenciales 136 y determinar si el titular de la credencial 136 tiene permitido o no acceder a cualquiera de los activos controlados por el módulo de control de acceso 116. De este modo, la lógica de control de acceso 228 facilita las operaciones de lectura de datos de acceso, las operaciones de verificación de datos de acceso y las operaciones asociadas con permitir el acceso de un usuario a un activo (por ejemplo, desbloquear una puerta, proporcionar acceso a una cuenta, etc.).

El módulo de registro 220 se proporciona para realizar procedimientos de registro que tradicionalmente se han reservado al sistema de programación de credenciales 128. En particular, el módulo de registro 220 está configurado para recibir un identificador de credencial de una credencial de acceso 136, comparar el identificador de credencial con una lista de identificadores de credencial, determinar que el identificador de credencial coincide con al menos un identificador de credencial en la lista de identificadores de credencial y, con base en la determinación de que el identificador de

credenciales coincide con al menos un identificador de credenciales en la lista de identificadores, invocar el módulo de control de acceso para codificar la credencial de acceso con datos de acceso que la credencial de acceso puede utilizar con otros módulos de control de acceso dentro de la instalación de múltiples habitaciones.

Como se pueden apreciar por los expertos en la técnica, las funciones y características de la lógica de control de acceso 228 se pueden incorporar en el módulo de registro 220 y viceversa. No existe ningún requisito de que se proporcionen dos módulos separados y distintos para las funciones de control de acceso y las funciones de registro. Más bien, se puede configurar un solo módulo para proporcionar toda la funcionalidad que se describe en este documento. Además, es posible que otros módulos de memoria 208 puedan realizar varias características de la lógica de control de acceso 228 y el módulo de registro 220 sin alejarse del alcance de la presente invención.

Debe apreciarse que para completar una operación de lectura/verificación/codificación, tal como la descrita anteriormente en relación con el módulo de registro 220, es importante limitar la cantidad de tiempo que se debe presentar una credencial 136 al módulo de control de acceso 116. Por ejemplo, un usuario típico generalmente no tolerará presentar una credencial a un módulo de control de acceso 116 durante más de cinco segundos, o así sucesivamente. En consecuencia, el módulo de control de acceso 116 está habilitado para leer un número de identificación de la credencial 136, confirmar que el número de identificación de la credencial 136 coincide con un número de identificación asociado con un huésped que tiene reservas confirmadas y que tiene permitido registrarse en un lugar distinto de la recepción 118, y codificar la credencial 136 con los datos de acceso adecuados en una cantidad mínima de tiempo.

La presente invención proporciona al módulo de control de acceso 116 una lista de números de identificación única (UID [por sus siglas en inglés]) de registro que se mantiene de forma local 224 y un almacén de imágenes de datos de acceso local 232 para permitir que el módulo de control de acceso 116 complete la operación de lectura/verificación/codificación en una cantidad mínima de tiempo. Por lo tanto, cuando se realizan funciones de registro (por ejemplo, verificación del número de identificación de la credencial y codificación de la credencial 136 con datos de acceso), el módulo de registro 220 es capaz de hacer referencia a la lista de UID de registro 224 que se mantiene de forma local y dar lugar a que los datos de acceso adecuados tengan acceso al almacén de imágenes de datos de acceso 232 para ser codificados en la credencial 136. Estos datos se pueden conservar de manera persistente en la credencial 136 o renovarse automáticamente después de una cantidad de tiempo predeterminado.

De acuerdo con al menos algunas realizaciones de la presente invención, los datos almacenados en la lista de UID de registro 224 se mantienen en un formato relativamente simple, pero de búsqueda fácil. Por ejemplo, la lista puede ser simplemente una lista de números de identificación asociados con una tarjeta que ha sido autorizada para registrarse en un lugar que no sea la recepción 118. En algunas realizaciones, se agregan números a la lista 224 al recibir un mensaje de la lógica de control de acceso central 132 que incluye un número de identificación de credencial, el módulo de registro 220 actualiza la lista 224 para incluir el número de identificación de credencial recién recibido. Por el contrario, cuando el módulo de registro 220 ha completado un proceso de registro para una credencial 136 y ha confirmado que el registro ha sido exitoso, el módulo de registro 220 puede eliminar el número de identificación de la credencial correspondiente de la lista 224 (o eliminarlo de la lista después de la salida, en caso de que haya problemas durante la estancia).

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

De acuerdo con al menos algunas realizaciones de la presente invención, los datos de acceso pueden incluir uno o más de un código de sitio que identifica la instalación de múltiples habitaciones, una clave de cifrado usada sustancialmente de forma 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 identifique sustancialmente de manera única a un usuario de la credencial de acceso dentro de la instalación de múltiples habitaciones, la duración de la estadía del huésped, el número de habitación, los identificadores de servicios agregados y un conjunto de permisos de acceso que definen si se permite o deniega el acceso a activos particulares de la instalación de múltiples habitaciones a un usuario de la credencial de acceso. Algunos o todos los datos del almacén de imágenes de datos de acceso 232 se pueden escribir en una credencial 136, según el usuario de la credencial 136 y las reservas asociadas con el usuario de la credencial 136.

La memoria 208 puede comprender memoria volátil y/o no volátil. Ejemplos de memoria no volátil incluyen memoria de sólo lectura (ROM [por sus siglas en inglés]), ROM programable borrable (EPROM [por sus siglas en inglés]), PROM borrable electrónicamente (EEPROM [por sus siglas en inglés]), memoria flash y similares. Los ejemplos de memoria volátil incluyen memoria de acceso aleatorio (RAM [por sus siglas en inglés])), RAM dinámica (DRAM [por sus siglas en inglés])), RAM estática (SRAM [por sus siglas en inglés])) o memoria temporal. En una realización, la memoria 208 y el procesador 204 están diseñados para usar funciones de seguridad conocidas para evitar el acceso no autorizado al

contenido de la memoria 208, tal como el análisis de canales laterales y similares.

También se puede incluir una fuente de alimentación (no se representa) en el módulo de control de acceso 116 para proporcionar energía a los diversos dispositivos contenidos dentro del módulo de control de acceso 116. La fuente de alimentación puede comprender baterías internas y/o un convertidor CA-CC, como una fuente de alimentación conmutada o un regulador de voltaje conectado a una fuente de alimentación de CA externa.

Con referencia ahora a la Fig. 3, se describirá una credencial de acceso 136 ejemplar de acuerdo con al menos algunas realizaciones de la presente invención. En algunas realizaciones, la credencial 136 se proporciona con un procesador 304, una memoria 308 y una interfaz de módulo 312. El procesador 304 puede incluir un microprocesador, un controlador programable o cualquier otro tipo de unidad de procesamiento capaz de ejecutar las instrucciones almacenadas en la memoria 308. Alternativamente, o además, el procesador 304 se puede materializar como un circuito integrado de aplicación específica (ASIC).

El procesador 304 emplea interfaces bidireccionales para comunicarse con la memoria 308 y con la interfaz de módulo 312. En particular, el procesador 304 facilita los intercambios de datos entre la credencial 136 y un módulo de control de acceso 116. Tales comunicaciones son manejadas a nivel físico por la interfaz de módulo 312. De modo parecido a la interfaz de credencial 216, la interfaz de módulo 312 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 interfaz, o cualquier otro medio para comunicar información a/desde un módulo de control de acceso 116. Como puede apreciar un experto en la técnica, la interfaz 312 puede incluir una unidad de modulación/desmodulación en lugar de depender del procesador 304 para realizar operaciones de codificación/descodificación, funciones de formateo de mensajes y similares.

La credencial 136 se puede fabricar como un dispositivo de sistema en chip (SoC [por sus siglas en inglés]), un dispositivo de sistema en paquete (SiP [por sus siglas en inglés]) o un dispositivo de sistema en módulo (SiM [por sus siglas en inglés]). En el dispositivo SoC, están integrados diversos componentes funcionales en una sola hilera. En consecuencia, en los dispositivos SiP y SiM, se combinan muchos dispositivos SoC en un solo paquete (dispositivo SiP) o un conjunto que incluye dispositivos SoC y/o SiP (dispositivo SiM), respectivamente.

Una credencial “pasiva” 136 usa señales de RF (es decir, radiación de RF) emitidas por el módulo de control de acceso 116 como fuente de energía para alimentar la credencial 136 y sus componentes (principalmente el procesador 304). Cuando una credencial pasiva 136 entra dentro del alcance de un módulo de control de acceso de interrogación 116, el módulo de control de acceso 116 proporciona energía a la credencial 136 a través de una señal de RF de interrogación. La credencial pasiva 136 convierte una parte de la potencia de RF recopilada por la interfaz de módulo 312 (por ejemplo, una antena dentro de la interfaz 312) en potencia de CC que facilita la operatividad de la credencial 136. Tal credencial 136 solo puede operar en la zona activa de un módulo de control de acceso de interrogación 116 y de otra manera está inactiva.

Alternativamente, la credencial 136 puede comprender una fuente de alimentación interna (es decir, en placa), por ejemplo, una o varias baterías y/o celdas solares (credencial “activa”). Incluso en otra realización, la credencial 136 comprende un rectificador de RF y una fuente de alimentación interna (RFID “semiactiva”). Las RFID activas y semiactivas se pueden usar normalmente a mayores distancias de los módulos de control de acceso 116 que las pasivas, y también se pueden proporcionar capacidades adicionales informáticas y/o de detección.

Cuando está en funcionamiento, el módulo de control de acceso 116 y la credencial 136 usan protocolos de comunicación preprogramados. Para aumentar la probabilidad de recepción sin errores, los mismos mensajes se pueden repetir de forma redundante un número predeterminado de veces o durante un intervalo de tiempo predeterminado. Los protocolos y matices de estos se pueden definir dentro de los datos de acceso 320 que están codificados en la credencial 136. En algunas realizaciones, partes de estos datos de acceso 320 se programan en la credencial 136 antes de que un huésped se registre en la instalación de múltiples habitaciones y otras partes de los datos de acceso 320 se codifican en la credencial 136 durante el proceso de registro. Por ejemplo, la información del protocolo de comunicación pueden ser datos programados con anterioridad, al mismo tiempo que el número de habitación, la duración de la estadía y otros datos usados para determinar los privilegios de acceso solo se programan durante el proceso de registro. Esta restricción y separación de la programación de datos de acceso permite que la instalación de múltiples habitaciones mantenga un cierto nivel de control sobre el sistema de control de acceso 100.

El módulo de comunicación 316 puede facilitar las comunicaciones entre la credencial 136 y el módulo de control de acceso 116. En algunas realizaciones, el módulo de comunicación 316 se refiere a los datos de acceso 320 para garantizar que la credencial 136 use el protocolo de comunicación adecuado al comunicarse con el módulo de control de acceso 116. En algunos aspectos de la divulgación, si la credencial 136 solo ha sido programada con la cantidad mínima de datos de acceso 320, o no tiene ningún dato de acceso 320 (por ejemplo, el usuario de la credencial 136 no se ha registrado en la instalación de múltiples habitaciones), el módulo de comunicación 316 es capaz de proporcionar un UID de credencial 324 a un módulo de control de acceso 116 cuando la credencial 136 es interrogada por un módulo de control de acceso 116. El UID de credencial UID 324 puede comprender cualquier tipo de número de identificación, nombre, símbolo, etc.,

que identifique de manera única o casi única la credencial 136 o un titular de la credencial 136 con el módulo de control de acceso 116. Este UID de credencial 324 se puede programar en la credencial 136 al momento de proporcionarla y se puede proteger en una porción de solo lectura de la memoria 308 para garantizar que no se altere o manipule.

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

Como pueden apreciar los expertos en la técnica, la credencial de acceso 136 se puede proporcionar en cualquier tipo de factor de forma sin alejarse del alcance de la presente invención. En algunas realizaciones, la credencial de acceso puede comprender una tarjeta o dispositivo RFID que tenga una funcionalidad similar como un teléfono móvil, una agenda personal (PDA), un lector de libros electrónicos, un reproductor de música portátil o similar. En otras realizaciones, la credencial de acceso 136 puede comprender una tarjeta de banda magnética. Aún en otras realizaciones, la credencial de acceso 136 puede comprender un control remoto encriptado (keyfob). Otros factores de forma conocidos por los expertos en la técnica también resultarán fácilmente evidentes después de revisar la actual divulgación.

Con referencia ahora a la Fig. 4, se describirá un método ejemplar para confirmar reservas de huéspedes de acuerdo con al menos algunos aspectos de la presente divulgación. Inicialmente, las reservas de invitados para uno o más activos (por ejemplo, habitaciones 112a-N, servicios y similares) en la instalación de múltiples habitaciones se confirman en la lógica de control de acceso central 132. Esta información de reserva se puede mantener en la base de datos 140 y puede ser recuperada por la lógica de control de acceso 132 o puede haber sido escrita en la base de datos 140 por la lógica de control de acceso 132.

Al confirmar las reservas de los huéspedes, el método continúa con la lógica de control de acceso generando uno o más mensajes para el registro 118 en un lugar distinto de la recepción (paso 408). En algunos aspectos, esta característica (es decir, el registro en un lugar distinto de la recepción) puede ser un servicio por el cual el huésped paga un cargo adicional. En otros aspectos, solo los clientes preferentes (es decir, clientes con cuentas y/o tarjetas de fidelización) tienen permitido acceder a esta función. En otros aspectos, esta función puede estar disponible para todos los huéspedes de la instalación de múltiples habitaciones. En consecuencia, la determinación de si tal mensaje es generado o no por la lógica de control de acceso 132 dependerá de las preferencias operativas del operador de la instalación de múltiples habitaciones y no altera necesariamente el alcance de la presente invención.

Una vez generada, la lógica de control de acceso 132 da lugar a que los mensajes se transmitan a uno o más módulos de control de acceso autorizados 116 dentro del sistema de acceso seguro 100 (paso 412). En algunos aspectos, los mensajes se transmiten a todos los módulos de control de acceso 116 dentro del sistema de acceso seguro 100. En otros aspectos, los mensajes solo se transmiten a los módulos de control de acceso 116 que tienen un módulo de registro 220. En otros aspectos, solo un subconjunto de módulos de control de acceso 116 que tienen un módulo de registro 220 reciben un mensaje que permite el registro en un lugar distinto de la recepción.

Por ejemplo, si un huésped ha confirmado reservas y se ha identificado que una habitación en particular está reservada para ese huésped (por ejemplo, la habitación 678), entonces solo el módulo de control de acceso 116 asociado con la habitación 678 puede recibir el mensaje que permite el registro en un lugar distinto a la recepción. En este escenario particular, se le puede notificar al huésped del identificador de la habitación (es decir, la habitación 678) y las instrucciones para llegar a la habitación 678 al llegar, o antes de la llegada, a la instalación de múltiples habitaciones. Estas instrucciones se pueden proporcionar electrónicamente al huésped (por ejemplo, a través de mensajes de texto SMS, correo electrónico, correo de voz o similar) o por correo tradicional. Al llegar a la instalación de múltiples habitaciones, se permite al huésped ir directamente a la habitación 678 y completar el proceso de registro, una vez que el módulo de control de acceso 116 asociado con la habitación 678 ha recibido el mensaje que permite el registro en un lugar distinto de la recepción.

En el escenario anterior, también puede ser posible proporcionar el número de identificación de la credencial a uno o más módulos de control de acceso 116 entre la entrada de la instalación de múltiples habitaciones y la habitación 678 para permitir que el huésped continúe a través de la instalación de múltiples habitaciones hasta la habitación. 678. Por ejemplo, si se debe atravesar un ascensor 124 o pasillo 120 para llegar a la habitación 678, se puede proporcionar un módulo de control de acceso 116 asociado con tal ascensor 124 o pasillo 120 con el número de identificación de la credencial. Sin embargo, estos módulos de control de acceso 116 se pueden no comprender necesariamente un módulo de registro 220 como el módulo de control de acceso 116 asociado con la habitación 678. Si este es el caso, los módulos de control de acceso 116 asociados con el ascensor 124 o el pasillo 120 pueden permitir el acceso a su activo asociado si se proporciona el número de identificación de la credencial al módulo de control de acceso 116, pero puede ser que estos módulos no completen necesariamente el proceso de registro. Sin embargo, si uno o más de estos módulos de control de acceso 116 comprenden un módulo de registro 220, entonces el proceso de registro puede completarse antes de que el huésped llegue a la habitación 678.

De regreso al diagrama de flujo de la Fig. 4, una vez que los mensajes de habilitación han sido transmitidos a los módulos de control de acceso apropiados 116, la lógica de control de acceso 132 confirma la recepción segura de los mensajes (paso 416). Esto generalmente se hace al requerir que el módulo de control de acceso 116 transmita un mensaje de recepción a la lógica de control de acceso 132. En ausencia de la recepción de un recibo del módulo de control de acceso 116, la lógica de control de acceso 132 generalmente no confirmará la recepción de tales mensajes. Alternativamente, el

personal administrativo puede llevar una tarjeta física a los módulos de control de acceso deseados 116 y esta tarjeta física, cuando la lee el módulo de control de acceso 116, puede dar lugar a que el módulo de control de acceso 116 escriba números de identificación de credenciales adicionales en su lista que se mantiene de forma local 224. De este modo, el proceso de registro en un lugar distinto de la recepción se puede habilitar de forma automática o manual, según las preocupaciones de seguridad de la instalación de múltiples habitaciones.

Después de que se ha confirmado la recepción del mensaje, la lógica de control de acceso 132 puede dar lugar a que se transmitan uno o más mensajes (por ejemplo, electrónicos y/o físicos) al huésped para notificarle sobre la disponibilidad del registro, así como con instrucciones para el registro en lugares que no sean la recepción 118 (paso 420).

Con referencia ahora a la Fig. 5, se describirá un método de registro de acuerdo con al menos algunas realizaciones de la presente invención. El método se inicia cuando un invitado presenta una credencial de acceso 136, tal como una tarjeta RFID, en un módulo de control de acceso 116 habilitado con un módulo de registro 220 (paso 504). El método continúa con el módulo de control de acceso 116 que invoca al módulo de registro 220 a que determine un número de identificación de credencial 324 que ha sido proporcionado desde la credencial 136 al módulo de control de acceso 116 durante el intercambio de mensajes inicial (paso 508). El módulo de registro 220 también puede estar adaptado para determinar un tipo de credencial como un punto de datos adicional para confirmar la identidad de la credencial 136.

Una vez que se ha obtenido el número de identificación de la credencial, y posiblemente la información del tipo de credencial, el módulo de registro 220 busca en la lista de UID del registro que se mantiene de forma local 224 (paso 512). El módulo de registro 220 compara el número de identificación de la credencial y/o la información del tipo de credencial con la información que se mantiene en la lista 224 en busca de coincidencias (paso 516).

Si no se encuentra ninguna coincidencia entre la información proporcionada por la credencial 136 y la información mantenida en la lista 224, entonces el módulo de control de acceso 116 continúa inmediatamente solicitando datos de acceso, si tales datos no se han obtenido ya de la credencial 136, y se han determinado los privilegios de acceso para la credencial 136 (o más específicamente un titular de la credencial 136) en base a los datos de acceso recibidos (paso 532). Con base en este paso, el módulo de control de acceso 116 determinará si el titular de la credencial 136 tiene permitido o no el acceso a algún activo controlado a través del módulo de control de acceso 116. Si se confirman los permisos, entonces el módulo de control de acceso 116 liberará o pondrá a disposición de otra manera tales activos para el titular de la credencial 136. Si no se confirma el permiso, entonces el módulo de control de acceso 116 puede no hacer nada o proporcionar un mensaje de intento de acceso fallido al titular de la credencial de acceso 136 (por ejemplo, al emitir un pitido, destellando o proporcionando algún otro indicio que pueda ser percibido por el titular).

Con referencia de nuevo al paso 516, si se determina una coincidencia entre la información proporcionada por la credencial 136 y la información mantenida en la lista 224, el módulo de registro 220 continúa dando lugar a que el módulo de control de acceso 116 codifique la credencial 136 con los datos de acceso adecuados (paso 520). En algunas realizaciones, el tipo de datos de acceso codificados en la credencial 136 puede ser específico del titular de la credencial 136 e incluso más específico para las reservas del titular. Por ejemplo, los datos de acceso codificados en la credencial 136 pueden incluir un número de habitación (que identifica una habitación en la que el huésped tiene reservas confirmadas), servicios disponibles (que identifican los servicios a los que se permite el acceso del huésped y si tales servicios son gratuitos, prepagados, o facturables a la cuenta del huésped), y la duración de la estancia (identificando una fecha de salida o una fecha de caducidad de los datos de acceso).

Después de que los datos de acceso hayan sido codificados en la credencial 136, el módulo de control de acceso 116 confirma la precisión de los datos de acceso al solicitar que la credencial 136 proporcione los datos de acceso al módulo de control de acceso 116 (paso 524). Si los datos de acceso recibidos de la credencial 136 coinciden con los datos que se suponía que debía escribir el módulo de control de acceso 116, entonces el módulo de control de acceso 116 confirma la codificación exitosa.

Posteriormente, el módulo de registro 220 actualiza la lista que se mantiene de forma local 224 para reflejar que el huésped se ha registrado (paso 528). Este paso de actualización incluye eliminar los datos coincidentes de la lista 224 (es decir, eliminar el número de identificación de la credencial y/o la información del tipo de credencial de la lista 224), asegurando de este modo que el módulo de control de acceso 116 no intente realizar el proceso de registro en la misma credencial 136 o en otra credencial 136 para la misma persona. También durante este paso, el módulo de control de acceso 116 genera y transmite un mensaje a la lógica de control de acceso 132 que indica que ha completado recientemente un proceso de registro. Este mensaje puede incluir el número de identificación de la credencial con la que se realizó el registro y cualquier otro dato necesario para confirmar el registro (por ejemplo, hora de registro, ubicación, etc.).

Al recibir el mensaje, la lógica de control de acceso 132 puede generar y enviar mensajes a otros módulos de control de acceso 116 dentro del sistema de acceso seguro 110 al solicitar que esos módulos 116 actualicen sus listas 224 que se mantienen internamente para reflejar el registro reciente. Por ejemplo, la lógica de control de acceso 132 puede notificar a cualquier módulo de control de acceso 116 que recibió un mensaje en el paso 412. Al recibir tal mensaje, los módulos de control de acceso 116 que no realizaron el procedimiento de registro pueden actualizar sus listas 224 que se mantienen internamente al eliminar el número de identificación de credencial adecuado y/o la información de tipo de credencial. En este punto, todos los módulos de control de acceso 116 confirmarán los privilegios de acceso para la credencial registrada

recientemente 136 con base en los datos de acceso 320 mantenidos en la credencial 136 y no necesariamente el número de identificación de la credencial 324.

Con referencia ahora a la Fig. 6, se describirá un método de control de acceso de acuerdo con al menos algunas realizaciones de la presente invención. El método se inicia cuando un invitado presenta una credencial 136 a un módulo de control de acceso 116 que no tiene un módulo de registro 220 y/o permisos para confirmar el registro para la credencial presentada al mismo (paso 604). Por ejemplo, el módulo de control de acceso 116 puede estar asociado con un pasillo 120, un ascensor 124 o similar. La presentación de la credencial 136 al módulo de control de acceso 116 da lugar a que la credencial 136 transmita uno o más mensajes al módulo de control de acceso 116 que incluye su número de identificación de credencial 324 y cualquier otra información de identificación pertinente (por ejemplo, tipo de credencial).

El módulo de control de acceso 116 analiza el mensaje o mensajes recibidos de la credencial 136 y determina el número de identificación de la credencial 324 junto con cualquier otra información de identificación de la credencial (paso 608). Esta información se compara con la lista que se mantiene de forma local de números de identificación 224 para ayudar al módulo de control de acceso 116 a determinar si se permite a la credencial 136 acceder al activo asociado con dicho módulo (pasos 612 y 616). Si se determina una coincidencia de información en la lista que se mantiene de forma local 224, el módulo de control de acceso 116 permite que el titular de la credencial 136 acceda al activo asegurado por el módulo de control de acceso (paso 620). Si no se determina una coincidencia, entonces el módulo de control de acceso 116 continúa leyendo los datos de acceso de la credencial 136, si tales datos no se han obtenido previamente durante otras transacciones, y determina los privilegios de acceso para la credencial 136 en función de tales datos de acceso (paso 624). En consecuencia, el módulo de control de acceso 116 es capaz de tomar decisiones de permisos de acceso con base en la información de identificación de credenciales 324 o, en ausencia de confirmación de permisos con tales datos, en función de los datos de acceso 320. Si la credencial 136 no logra proporcionar información de identificación de credencial válida o datos de acceso, el módulo de control de acceso 136 mantendrá su activo en condiciones seguras. El método anteriormente descrito también permite que un huésped continúe a través de ciertos caminos, tal vez caminos definidos, dentro de la instalación de múltiples habitaciones antes del registro; de este modo permite que el huésped posiblemente complete el proceso de registro en ubicaciones distintas a la recepción 118.

Mientras que los diagramas de flujo descritos anteriormente se han expuesto en relación con una secuencia particular de eventos, debe apreciarse que pueden tener lugar cambios en esta secuencia sin llevar a cabo de forma material la operación de la invención. Adicionalmente, no es necesario que ocurra la secuencia exacta de eventos como se establece en las realizaciones ejemplares. Las técnicas ejemplares ilustradas en este documento no se limitan a las realizaciones ilustradas específicamente, sino que también se pueden utilizar con las otras realizaciones ejemplares y cada característica descrita se puede reivindicar individualmente y por separado.

La presente invención, en diversas realizaciones, incluye componentes, métodos, procesos, sistemas y/o aparatos sustancialmente como se representa y describe en este documento, incluidas diversas realizaciones, subcombinaciones y subconjuntos de estas. Los expertos en la técnica comprenderán cómo realizar y utilizar la presente invención después de comprender la presente divulgación. La presente invención, en diversas realizaciones, incluye proporcionar dispositivos y procesos en ausencia de elementos no representados y/o descritos en el presente o en varias realizaciones de este, incluso en ausencia de elementos que puedan haber sido utilizados en dispositivos o procesos anteriores, por ejemplo, para mejorar el rendimiento, lograr la facilidad de uso y/o reducir los costes de implementación.

Además, los sistemas, métodos y protocolos de esta invención se pueden implementar en un ordenador de propósito especial, un microprocesador o microcontrolador programado y elemento o elementos de circuito integrado periférico, un ASIC u otro circuito integrado, un procesador de señal digital, un circuito electrónico o lógico, tal como un circuito de elementos discretos, un dispositivo lógico programable, tal como PLD, PLA, FPGA, PAL, un dispositivo de comunicaciones, tal como un teléfono, cualquier medio comparable o similares. En general, cualquier dispositivo capaz de implementar una máquina de estados que a su vez sea capaz de implementar la metodología que se ilustra en este documento se puede usar para implementar los diversos métodos, protocolos y técnicas de comunicación de acuerdo con esta invención.

La anterior exposición de la invención se ha presentado con fines ilustrativos y de descripción. Lo anterior no pretende limitar la invención a la forma o formas divulgadas en este documento. En la descripción detallada anterior, por ejemplo, diversas características de la invención se agrupan en una o más realizaciones con el fin de simplificar la divulgación. Este método de divulgación no debe interpretarse como reflejo de la intención de que la invención reivindicada requiera más características de las que se mencionan expresamente en cada reivindicación. Más bien, como reflejan las reivindicaciones siguientes, los aspectos inventivos radican en menos que todas las características de una sola realización divulgada anteriormente.

REIVINDICACIONES

1) Un módulo de control de acceso (116) configurado para usarse en una instalación, el módulo de control de acceso comprende:

una lógica de control de acceso (228) configurada para hacer una determinación para permitir o denegar el acceso del usuario a un activo controlado por el módulo de control de acceso en donde la lógica de control de acceso (228) proporciona al módulo de control de acceso (116) la capacidad de leer los datos de las credenciales de acceso (136) y de hacer la determinación depermitir o no al titular de la credencial de acceso (136) el tener acceso a cualquier activo controlado por el módulo de control de acceso (116); y
un módulo de registro (220) está configurado para recibir un identificador de credencial de una credencial de acceso (136), comparar el identificador de credencial con una lista de identificadores de credencial almacenada en el módulo de control de acceso (116), determinar que el identificador de credencial coincide con al menos un identificador de credencial en la lista de identificadores de credencial y, con base en la determinación de que el identificador de credenciales coincide con al menos un identificador de credenciales en la lista de identificadores, invocar el módulo de control de acceso (116) para codificar la credencial de acceso con datos de acceso que comprende un conjunto de permiso de acceso que definen si se permite o se deniega el acceso de la credencial de acceso a un activo particular de la instalación;
en donde el módulo de registro (220) está configurado para invocar al módulo de control de acceso para codificar la credencial de acceso con los datos de acceso después de determinar que el identificador de credenciales coincide con al menos un identificador de credencial en la lista de identificadores y en donde el módulo de registro está configurado además para que, después de determinar que el identificador de credenciales coincide con al menos un identificador de credencial en la lista de identificadores, confirmar que la credencial de acceso se ha codificado de forma exitosa con los datos de acceso, eliminar el identificador de credencial de la lista de identificadores e informar de un registro exitoso a una lógica de control de acceso central.

2) El módulo de control de acceso de la reivindicación 1), en donde los datos de acceso codificados en la credencial de acceso están formateados específicamente para su uso por otros módulos de control de acceso dentro de la instalación y que no está formateado necesariamente de forma específica para su uso por los módulos de control de acceso dentro de otras instalaciones.

3) El módulo de control de acceso de la reivindicación 2, en donde los datos de acceso codificados en la credencial de acceso comprende uno o más de un código de sitio que identifica la instalación, una clave de cifrado usada sustancialmente de forma exclusiva por la instalación, un protocolo de comunicación usado por módulos de control de acceso dentro de la instalación, un identificador de huésped que identifique sustancialmente de manera única correlacionado con la credencial de acceso dentro de la instalación, la duración de la estadía del huésped, el número de habitación, los identificadores de servicios autorizados y un conjunto de permisos de acceso que definen si se permite o deniega el acceso a activos particulares de la instalación de múltiples habitaciones.

4) El módulo de control de acceso 1), en donde el activo controlado por el módulo de control de acceso comprende una o más habitaciones dentro de la instalación, un corredor dentro de la instalación y un ascensor dentro de la instalación un puerto de entrada/salida a la instalación.

5) El módulo de control de acceso de la reivindicación 1), en donde el módulo de control de acceso comprende una interfaz de credencial que facilita las comunicaciones de RF con credenciales de acceso y en donde el módulo de control de acceso está configurado para recibir el identificador de credencial en un mensaje transmitido desde la credencial de acceso a la interfaz de credencial y para proporcionarle al módulo de registro el identificador de credencial después de que el mensaje se ha demodulado y que se ha determinado el identificador de credencial.

6) El módulo de control de acceso de la reivindicación 1, en donde el módulo de control de acceso está configurado para cambiar los permisos de autorización/acceso en la credencial.

7) Un método para operar un módulo de control de acceso (116) de una instalación, en donde el módulo de control de acceso comprende una lógica de control de acceso (228) configurada para hacer una determinación para permitir o denegar acceso de usuario a una instalación controlada por el módulo de control de acceso en donde la lógica de control de acceso (228) proporciona al módulo de control de acceso (116) la capacidad de leer los datos de acceso de las credenciales de acceso (136) y hacer la determinación si el titular de la credencial de acceso (136) tiene permitido o no el acceso a cualquiera de los activos controlados por el módulo de control de acceso (116), el método comprende:
recibir, en un módulo de registro (220) del módulo de control de acceso (116), un identificador de credencial de una credencial de acceso (136);
comparar el identificador de credencial con una lista de identificadores de credenciales almacenada en el módulo de control de acceso (116);
determinar que el identificador de credencial coincide con al menos un identificador de credencial en la lista de identificadores de credencial;
invocar, con base en la determinación de que el identificador de credencial coincide al menos con un identificador de credencial en la lista de identificadores, el módulo de control de acceso (116) para codificar la credencial de acceso con los datos de acceso que comprenden un conjunto de permisos de acceso que definen si se permite o se deniega el acceso

a la credencial de acceso a activos particulares de la instalación;
en donde invocar, en el módulo de registro (220), al módulo de control de acceso para codificar la credencial de acceso con los datos de acceso se realiza después de determinar que el identificador de credencial coincide con al menos un identificador de credencial en la lista de identificadores;
confirmar que la credencial de acceso ha sido codificada de forma exitosa con los datos de acceso;
determinar después que la credencial de acceso ha sido codificada de forma exitosa con los datos de acceso, eliminando el identificador de credencial de la lista de identificadores;
informar de un registro exitoso a una lógica de control de acceso central.

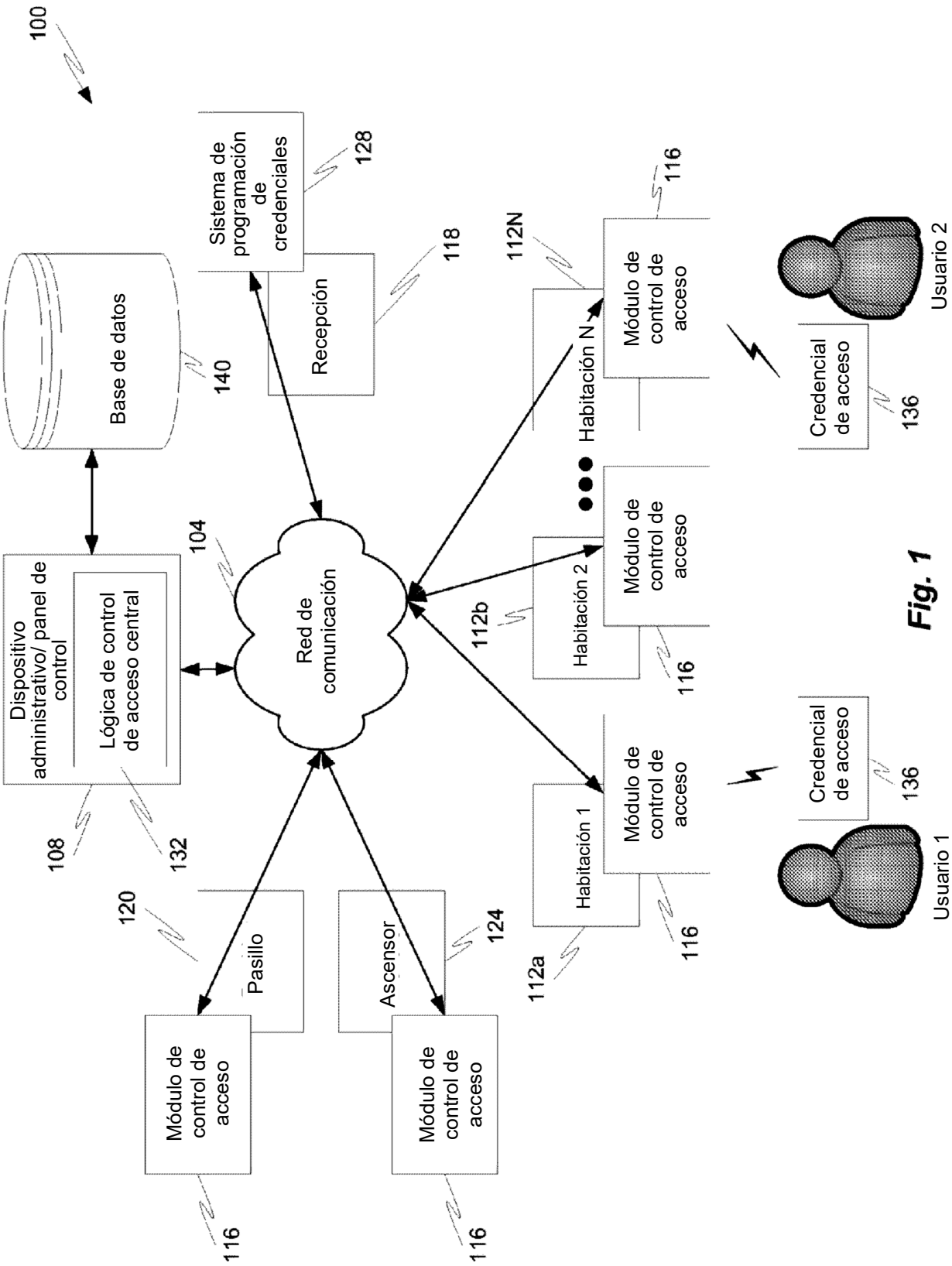
100
Sistema de programación de credenciales
128
Base de datos
140
Recepción
118
112N
Habitación N
Módulo de control de acceso
116
Credencial de acceso
136
Usuario 2
104
Red de comunicación
Dispositivo administrativo/ panel de control
Lógica de control de acceso central
108
132
112b
Habitación 2
Módulo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

Fig. 1

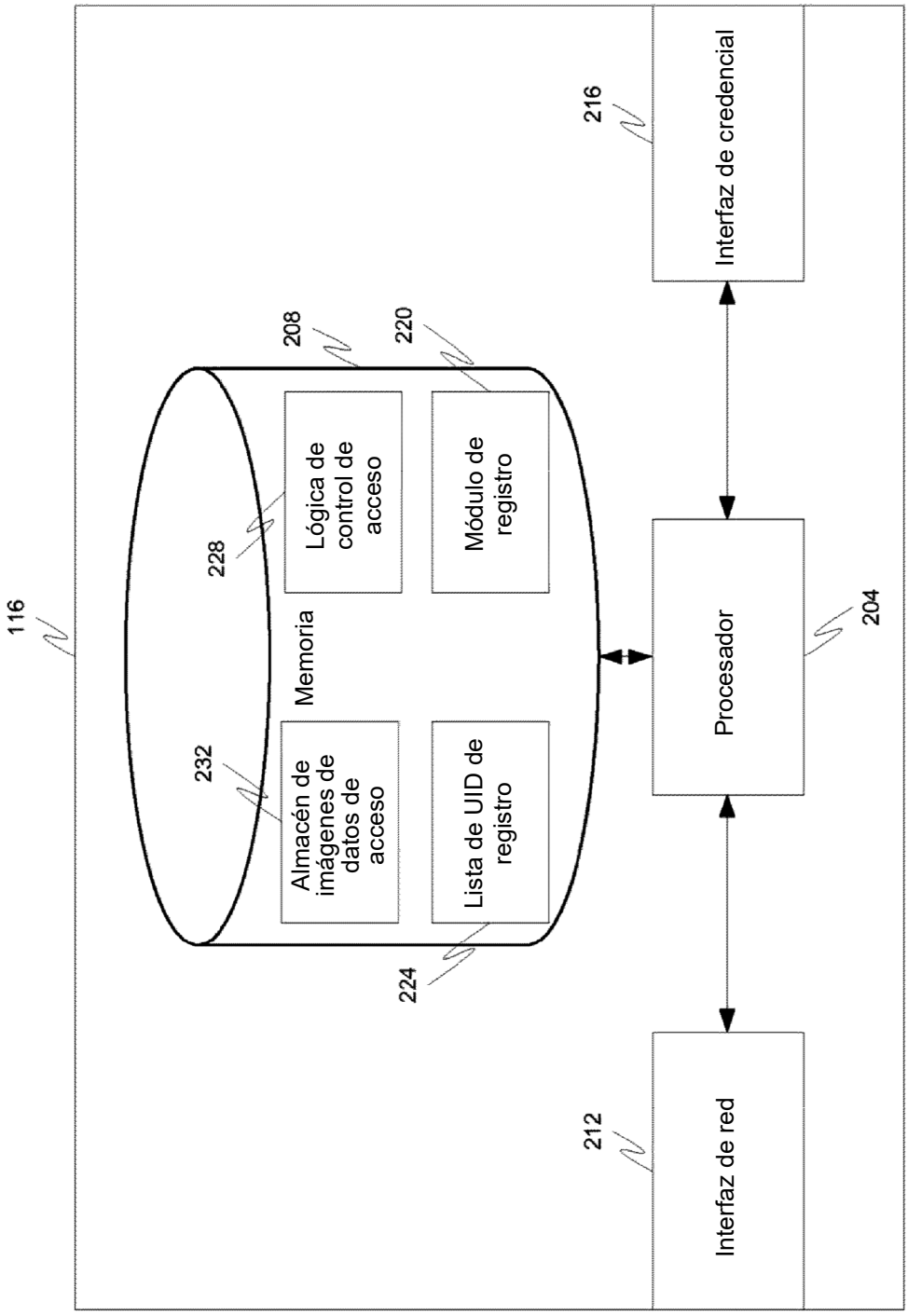
116
Interfaz de credencial
216
208
220
Lógica de control de acceso
Módulo de registro
228
Memoria
Procesador
204
232
Almacén de imágenes de datos de acceso
Lista de UID de registro
224
Interfaz de red
212

Fig. 2

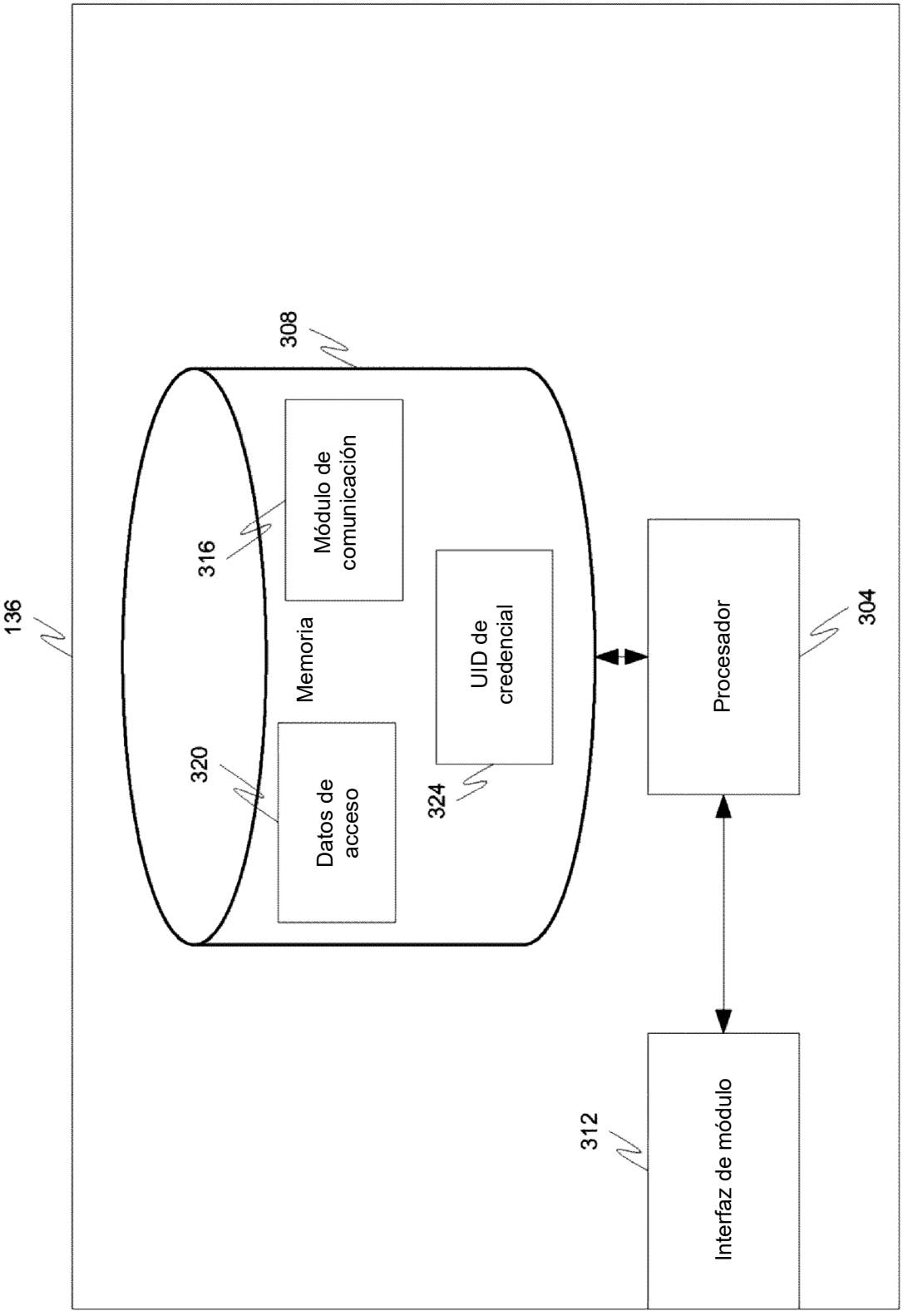
136
308
316
Módulo de comunicación
Memoria
320
Datos de acceso
324
UID de credencial
Procesador
304
312
Interfaz de módulo

Fig. 3

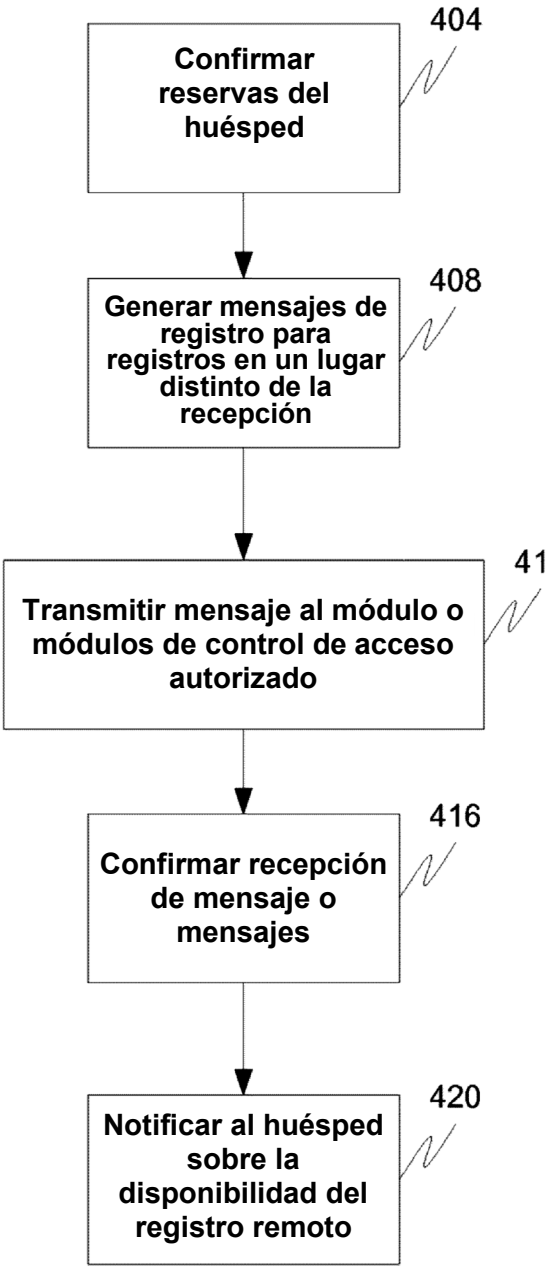
404
Confirmar reservas del huésped
408
Generar mensajes de registro para registros en un lugar distinto de la recepción
41
Transmitir mensaje al módulo o módulos de control de acceso autorizado
416
Confirmar recepción de mensaje o mensajes
420
Notificar al huésped sobre la disponibilidad del registro remoto

Fig. 4

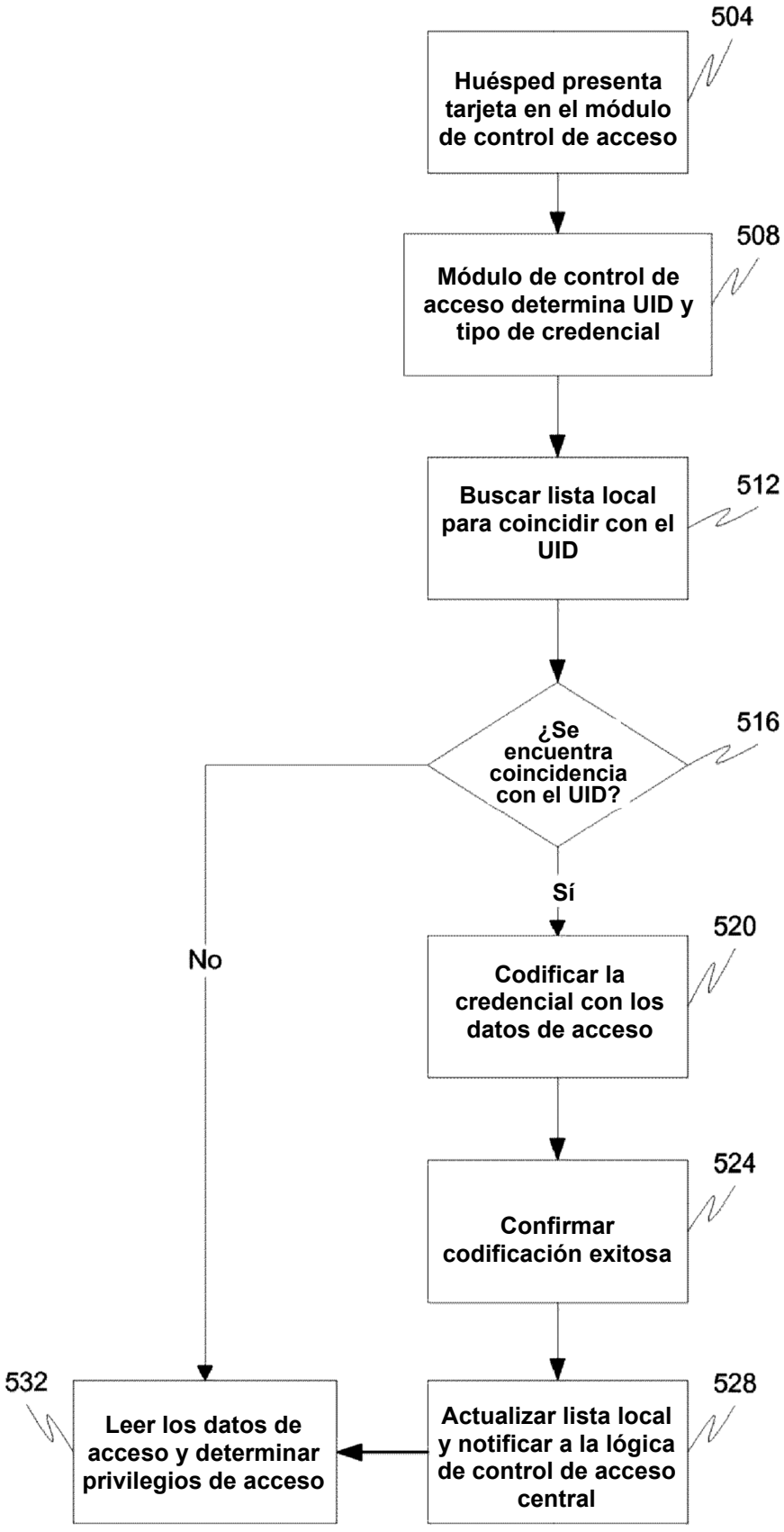
504
Huésped presenta tarjeta en el módulo de control de acceso
508
Módulo de control de acceso determina UID y tipo de credencial
512
Buscar lista local para coincidir con el UID
516
¿Se encuentra coincidencia con el UID?
Sí
No
520
Codificar la credencial con los datos de acceso
524
Confirmar codificación exitosa
528
Actualizar lista local y notificar a la lógica de control de acceso central
532
Leer los datos de acceso y determinar privilegios de acceso

Fig. 5

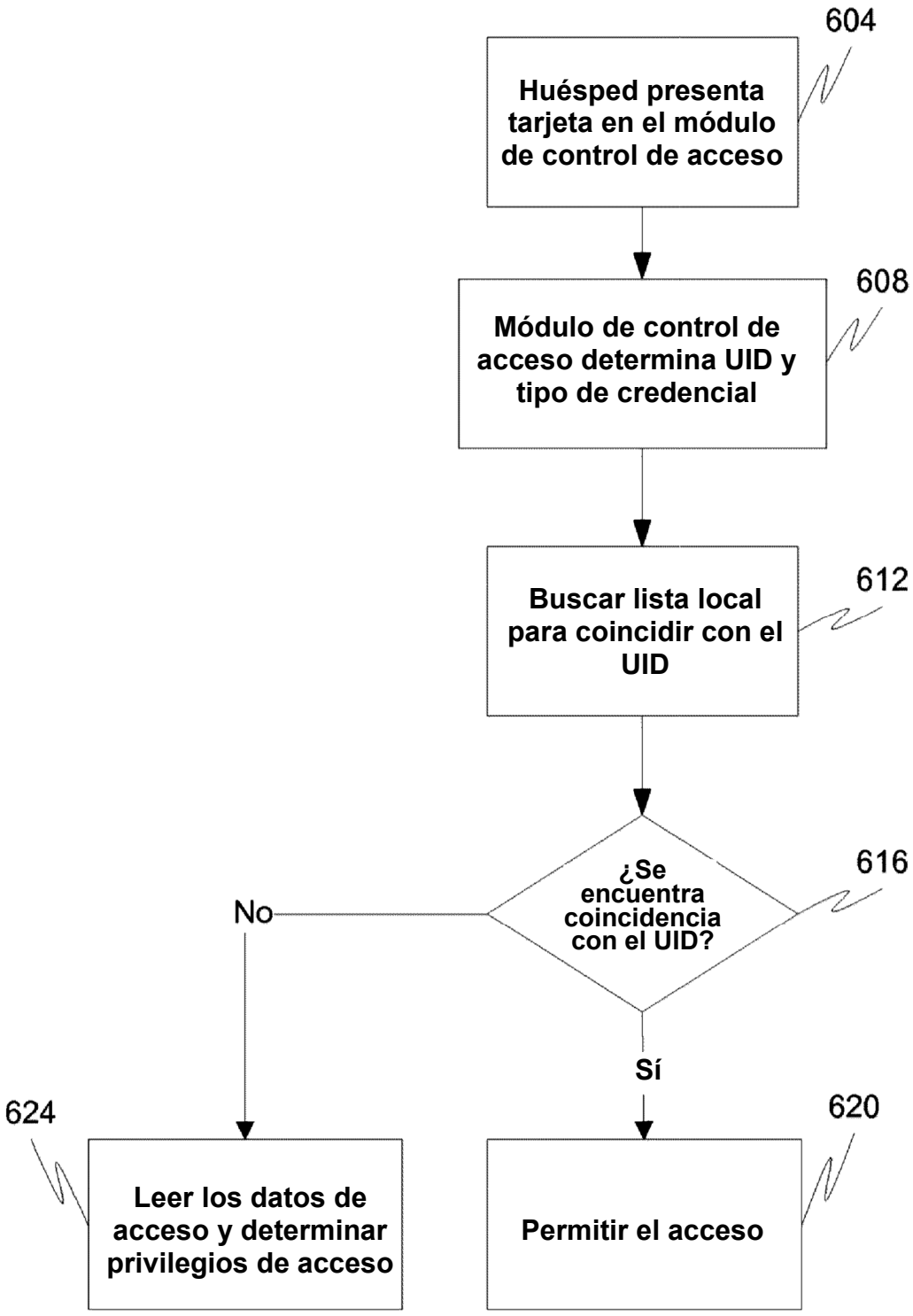
604
Huésped presenta tarjeta en el módulo de control de acceso
608
Módulo de control de acceso determina UID y tipo de credencial
612
Buscar lista local para coincidir con el UID
616
¿Se encuentra coincidencia con el UID?
No
Sí
624
Leer los datos de acceso y determinar privilegios de acceso
620
Permitir el acceso

Fig. 6