(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 923 690**

(51) Int. CI.:

H04W 12/08 (2011.01)
H04W 12/069 (2011.01)
G07C 9/00 (2010.01)
G07C 9/27 (2010.01)
H04W 4/02 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.12.2015 PCT/US2015/063148**

(87) Fecha y número de publicación internacional: **09.06.2016 WO16089841**

(96) Fecha de presentación y número de la solicitud europea: **01.12.2015 E 15816968 (0)**

(97) Fecha y número de publicación de la concesión europea: **20.07.2022 EP 3228105**

(54) Título: **Sistema de control de acceso con traspaso de servicio de acreditación móvil automático**

(30) Prioridad:

02.12.2014 US 201462086262 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.09.2022

(73) Titular/es:

CARRIER CORPORATION (100.0%)
One Carrier Place, P.O. Box 4015
Farmington, CT 06034, US

(72) Inventor/es:

KUENZI, ADAM y
HARKEMA, JONAH J.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistema de control de acceso con traspaso de servicio de acreditación móvil automático

Antecedentes

La presente divulgación se refiere, en general, a sistemas de control de acceso y, más en particular, a un sistema y a un método para establecer relaciones de confianza e inicializar un dispositivo móvil para operar en un sistema de acreditación móvil.

Un sistema de control de acceso se opera habitualmente codificando datos en una tarjeta de llave física que indica derechos de acceso. Algunos sistemas de control de acceso son en línea, en donde el lector puede usar algún medio para comunicarse con el sistema de control de acceso. En los sistemas en línea, los derechos de acceso son habitualmente un identificador de referencia. Otros sistemas de control de acceso son fuera de línea y los derechos de acceso se codifican como datos que pueden ser descodificados e interpretados por la cerradura fuera de línea para recuperar los derechos de acceso. Un ejemplo es un sistema de cerradura de hotel en donde una recepción codifica una tarjeta de huésped y una cerradura fuera de línea alimentada por batería en una puerta de habitación de huésped tiene los medios para descodificar la tarjeta y permitir o denegar el acceso basándose en los derechos de acceso codificados. Algunos métodos para codificar derechos de acceso incluyen la secuenciación, en donde derechos de acceso subsiguientes tienen un número de secuencia que es mayor que el de los derechos de acceso anteriores.

Cuando un usuario descarga o carga una aplicación de uso restringido, tal como la que se usa para el control de acceso en un sistema de acreditación móvil, en un dispositivo móvil, se requiere, habitualmente, que el usuario introduzca información de cuenta, por ejemplo, un código de autorización, que es esencialmente una clave de software, clave de instalación o similar. La información de cuenta habilita el uso de una aplicación a través de diversos métodos para autenticar la información de cuenta y el código de autorización encapsula información de cuenta usando cifrado y es introducida en la aplicación por el usuario del dispositivo móvil. Además del código de autorización, el usuario también ha de introducir o seleccionar habitualmente un Nombre de Anfitrión para el servicio deseado.

Un servicio de credenciales móviles, por ejemplo, se puede alojar en diferentes ubicaciones accesibles por la aplicación en el dispositivo móvil, y la información de Nombre de Anfitrión introducida determinaría qué ubicación usar. Además, las ubicaciones separadas podrían ser para la distribución geográfica, para el equilibrado de cargas, para la recuperación ante desastres si cae un servicio primario, etc. Introducir información de cuenta o un código de autorización, que habitualmente puede tener una longitud de 30 dígitos numéricos, y un Nombre de Anfitrión, puede ser engorroso de realizar en un dispositivo móvil. Además, el usuario puede introducir en primer lugar una información de cuenta de fidelidad de hotel y es engorroso que se requiera también introducir un código de autorización y un nombre de Anfitrión para el servicio de credenciales móviles que es usado por la aplicación de fidelidad de hotel para abrir controles de acceso, por ejemplo, cerraduras, para ejercer sus derechos de acceso.

Se divulga técnica anterior en el campo de la acreditación móvil en los documentos EP2620919, US2012/0280783 y US2014/0219453.

Sumario

Un método para inicializar un dispositivo móvil para operar en un sistema de acreditación móvil, el método de acuerdo con una realización no limitante divulgada de la presente divulgación incluye enviar un código de autorización y un Localizador de Recursos Uniforme (URL) de anfitrión a una biblioteca de credenciales móviles de una aplicación móvil en un dispositivo móvil, operable el dispositivo móvil para realizar una primera sincronización con un servicio de credenciales para establecer una relación de confianza continuada entre la biblioteca de credenciales móviles y el servicio de credenciales de tal modo que la aplicación móvil es operable para interaccionar con un control de acceso sin que un usuario del dispositivo móvil conozca ni el código de autorización ni el URL de anfitrión del servicio de credenciales y pasar automáticamente de una primera relación de confianza a la relación de confianza continuada entre la biblioteca de credenciales móviles y el servicio de credenciales, en donde la primera relación de confianza es entre una aplicación de fidelidad y un servicio de hotel, y hay otra relación de confianza entre el servicio de hotel y el servicio de credenciales basándose en una autorización de servicio a servicio.

El servicio de hotel se puede basar en una autorización de cuenta de fidelidad de hotel.

El método puede incluir generar credenciales móviles en el servicio de credenciales para su descarga a la biblioteca de credenciales.

Las credenciales móviles pueden ser para una cuenta de ID de usuario asociada.

El dispositivo móvil puede incluir un teléfono inteligente.

El control de acceso puede ser una cerradura.

El control de acceso puede ser una caja de seguridad.

El servicio de credenciales se puede alojar en una de una multitud de ubicaciones.

Esa una de la multitud de ubicaciones se puede seleccionar para una distribución de cargas geográfica.

El método puede incluir que la biblioteca móvil descifre el código de autorización, que valide el código y que recupere un número de serie de biblioteca móvil contenido en el código de autorización.

El método puede incluir que la biblioteca móvil use información contenida en el código de autorización para realizar la primera sincronización con un servicio de credenciales y para realizar una autenticación.

El método puede incluir que el servicio de credenciales valide la primera información de sincronización y que, entonces, establezca la relación de confianza continuada entre la biblioteca de credenciales móviles y el servicio de credenciales.

Las características y elementos anteriores pueden combinarse en diversas combinaciones sin exclusividad, a menos que se indique expresamente de otra manera. Estas características y elementos, así como el funcionamiento de los mismos, serán más evidentes a la vista de la siguiente descripción y de los dibujos adjuntos. Se debería entender, sin embargo, que la descripción y los dibujos siguientes pretenden ser de naturaleza ilustrativa y no limitantes.

Breve descripción de los dibujos

Diversas características se harán evidentes para los expertos en la materia a partir de la siguiente descripción detallada de la realización no limitante divulgada. Los dibujos que acompañan a la descripción detallada se pueden describir brevemente como sigue:

la figura 1 es un diagrama de sistema esquemático general de un sistema de autenticación de usuarios;

la figura 2 es un diagrama de bloques del sistema de autenticación de usuarios;

la figura 3 es un diagrama de flujo de un método de gestión de credenciales realizado por el sistema de autenticación de usuarios;

la figura 4 es un diagrama de flujo de un método de gestión de credenciales realizado por el sistema de autenticación de usuarios de acuerdo con una realización no limitante divulgada;

la figura 5 es una vista esquemática de una credencial de acuerdo con otra realización no limitante divulgada; y

la figura 6 es un diagrama de flujo de un método de traspaso de servicio de credenciales realizado por el sistema de autenticación de usuarios de acuerdo con una realización no limitante divulgada; y

la figura 7 es un diagrama de flujo de las relaciones de confianza para el método de traspaso de servicio de credenciales de acuerdo con una realización no limitante divulgada.

Descripción detallada

La figura 1 ilustra esquemáticamente un sistema de control de acceso 10. El sistema 10 generalmente incluye un dispositivo móvil 12, un servidor 14 y una pluralidad de controles de acceso 16, ilustrados esquemáticamente como 16a, 16b, ... , 16n. Debería apreciarse que, aunque se definen sistemas particulares de forma separada en los diagramas de bloques esquemáticos, cada uno o cualquiera de los sistemas puede combinarse o separarse de otra manera a través de hardware y/o software.

El dispositivo móvil 12 es un dispositivo de mano con capacidad inalámbrica tal como un teléfono inteligente, que es operable para comunicarse con el servidor 14 y los controles de acceso 16. El servidor 14 puede proporcionar credenciales y otros datos al dispositivo móvil 12, tales como actualizaciones de firmware o software a comunicar a uno o más de los controles de acceso 16. Aunque el servidor 14 se representa en el presente documento como un único dispositivo, debería apreciarse que el servidor 14 se puede materializar, como alternativa, como una multiplicidad de sistemas, a partir de los cuales el dispositivo móvil 12 recibe credenciales y otros datos.

Cada controlad de acceso 16 es un dispositivo con capacidad inalámbrica, de acceso restringido o de uso restringido tal como cerraduras inalámbricas, lectores de control de acceso para la entrada a edificios, controles de banca electrónica, dispositivos de transferencia de datos, dispositivos de dispensación de llaves, dispositivos de dispensación de herramientas y otras máquinas de uso restringido. El dispositivo móvil 12 envía credenciales a los controles de acceso 16, permitiendo de este modo de manera selectiva que un usuario acceda a, o que active, funciones de los controles de acceso 16. Un usuario puede enviar, por ejemplo, una credencial a una cerradura electromecánica para

desbloquear la misma y, de ese modo, conseguir acceso a un área restringida. En otro ejemplo, un usuario puede enviar una credencial a un control de banca electrónica para retirar fondos. En otro ejemplo más, el usuario puede enviar la credencial a una unidad que dispensa tarjetas de llave con datos asociados con la credencial o con datos recuperados de la misma. Un dispositivo móvil 12 puede almacenar credenciales para uno o todos y otros de los ejemplos indicados anteriormente y, además, puede almacenar una pluralidad de credenciales para cada tipo de aplicación al mismo tiempo. Algunas credenciales pueden usarse para múltiples controles de acceso 16. Por ejemplo, una pluralidad de cerraduras electrónicas en una instalación puede responder a la misma credencial. Otras credenciales pueden ser específicas de un único control de acceso 16.

Con referencia a la figura 2, un diagrama de bloques de un sistema de cerradura electrónica 20 de ejemplo incluye el control de acceso 16a, el dispositivo móvil 12 y el servidor 14. El control de acceso 16a generalmente incluye un accionador de cerradura 22, un controlador de cerradura 24, una antena de cerradura 26, un transceptor de cerradura 28, un procesador de cerradura 30, una memoria de cerradura 32, una fuente de alimentación de cerradura 34, un lector de tarjeta de cerradura 90 y un módulo de credenciales 36. El controlad de acceso 16a es receptivo a credenciales del dispositivo móvil 12, y puede, por ejemplo, ser la cerradura de una caja de seguridad, una cerradura de puerta o un bombín de cerradura. Aunque la presente divulgación se centra esencialmente en credenciales para el control de acceso, debería apreciarse que otros sistemas, en donde se transmiten credenciales desde un dispositivo móvil a un control de acceso para identificar el usuario en un sistema en línea o validar permisos o derechos de acceso de usuario en un sistema fuera de línea, se beneficiarán de la misma. Tales sistemas incluyen sistemas de banca virtual o electrónica, sistemas de accionamiento de máquinas, sistemas de dispensación y sistemas de acceso a datos.

Tras recibir y autenticar una credencial apropiada desde el dispositivo móvil 12 usando el módulo de credenciales 36, o después de recibir datos de tarjeta desde el lector de tarjeta de cerradura 90, el controlador de cerradura 24 ordena al accionador de cerradura 22 que bloquee o desbloquee una cerradura mecánica o electrónica. El controlador de cerradura 24 y el accionador de cerradura 22 pueden ser partes de una única unidad de cerradura electrónica o electromecánica, o pueden ser componentes vendidos o instalados de forma separada.

El transceptor de cerradura 28 es capaz de transmitir datos a y de recibir datos desde al menos el dispositivo móvil 12. El transceptor de cerradura 28 puede ser, por ejemplo, un transceptor de comunicación de campo cercano (NFC), Bluetooth o Wi-Fi u otro transceptor inalámbrico apropiado. La antena de cerradura 26 es cualquier antena apropiada para el transceptor de cerradura 28. El procesador de cerradura 30 y la memoria de cerradura 32 son, respectivamente, dispositivos de procesamiento y de almacenamiento de datos. El procesador de cerradura 30 puede ser, por ejemplo, un microprocesador que puede procesar instrucciones para validar datos de tarjeta y determinar los derechos de acceso contenidos en los datos de tarjeta o para pasar mensajes desde un transceptor a un módulo de credenciales 36 y para recibir una indicación de respuesta de vuelta desde el módulo de credenciales 36 con datos de tarjeta. La memoria de cerradura 32 puede ser RAM, EEPROM u otro medio de almacenamiento en el que el procesador de cerradura 30 puede leer y escribir datos, incluyendo, pero sin limitación, opciones de configuración de cerradura y el registro de auditoría de cerradura. El registro de auditoría de cerradura puede ser un registro de auditoría unificado que incluye eventos iniciados accediendo a la cerradura a través del lector de tarjeta de cerradura 90 o del dispositivo móvil 12. La fuente de alimentación de cerradura 34 es una fuente de alimentación tal como una conexión de línea eléctrica, un sistema de recolección de potencia o una batería que alimenta al controlador de cerradura 24. En otras realizaciones, la fuente de alimentación de cerradura 34 solo puede alimentar al controlador de cerradura 24, con el accionador de cerradura 22 alimentado principal o totalmente por otra fuente, tal como un trabajo de usuario (por ejemplo, girando un pasador).

El módulo de credenciales 36 está en comunicación con el procesador de cerradura 30 y es operable para descifrar y validar una credencial para extraer datos de tarjeta virtual comunicados al controlador de cerradura 24 como una "lectura de tarjeta virtual". Es decir, el control de acceso 16a tiene esencialmente dos lectores, un lector 90 para leer una tarjeta de llave física 92 y el módulo de credenciales 36 para comunicarse con el dispositivo móvil 12 a través del procesador de cerradura 30 y el transceptor 28 y la antena 26.

Aunque la figura muestra la antena de cerradura 26 y el transceptor 28 conectados al procesador 30, esto no tiene el fin de limitar otras realizaciones que puedan tener una antena 26 y un transceptor 28 adicionales conectados al módulo de credenciales 36 directamente. El módulo de credenciales 36 puede contener un transceptor 28 y una antena 26 como parte del módulo de credenciales. O el módulo de credenciales 36 puede tener un transceptor 28 y una antena 26 de forma separada del procesador 30 que también tiene un transceptor 28 y una antena 26 separados del mismo tipo o un tipo diferente. En algunas realizaciones, el procesador 30 puede encaminar la comunicación recibida a través del transceptor 28 al módulo de credenciales 36. En otras realizaciones, el módulo de credenciales puede comunicarse directamente con el dispositivo móvil 12 a través del transceptor 28.

El dispositivo móvil 12 generalmente incluye una antena de llave 40, un transceptor de llave 42, un procesador de llave 44, una memoria de llave 46, un receptor de GPS 48, un dispositivo de entrada 50, un dispositivo de salida 52 y una fuente de alimentación de llave 54. El transceptor de llave 42 es un transceptor de un tipo correspondiente al transceptor de cerradura 28, y la antena de llave 40 es una antena correspondiente. En algunas realizaciones, el transceptor de llave 42 y la antena de llave 40 también pueden usarse para comunicarse con el servidor 14. En otras realizaciones, pueden incluirse uno o más transceptores y antenas separados para comunicarse con el servidor 14.

La memoria de llave 46 es de un tipo para almacenar una pluralidad de credenciales localmente en el dispositivo móvil 12. En otras realizaciones, el dispositivo móvil 12 se comunica con el servidor 14 al mismo tiempo que se comunica con el control de acceso 16a. Esta es la configuración en línea y, en esta realización, se recupera una credencial móvil en tiempo real y se pasa al módulo de credenciales 36 sin almacenarse en primer lugar en la memoria de llave 46 en el dispositivo móvil 12.

Con referencia a la figura 3, un método 100 para facilitar la comunicación de una credencial representativa de los datos que normalmente se codificarían físicamente en la tarjeta de llave 92 se recupera en forma digital (la etapa 110), se encapsula en una credencial cifrada (la etapa 112), se descarga al dispositivo móvil 12 (la etapa 114), se pasa de forma segura al módulo de credenciales 36 (la etapa 116) que descifra y valida la credencial (la etapa 118), extrae los datos de tarjeta virtual (la etapa 120), entonces pasa los datos de tarjeta virtual al controlador de cerradura 24 como una "lectura de tarjeta virtual" (la etapa 122). Esto, por ejemplo, permite a un usuario omitir una recepción de un hotel e ir directamente a su habitación, como se describirá adicionalmente. La credencial cifrada puede ser generada por el servidor 14 usando técnicas bien conocidas para la creación y el cifrado de certificados digitales usando algoritmos criptográficos tales como AES, ECC, RSA y similares. Por ejemplo, la credencial puede contener, pero sin limitación, incluir un identificador de credencial, un parámetro que indica el tipo o formato de la credencial, puede contener datos cifrados tales como los datos de tarjeta virtual y puede contener una firma digital. Los datos cifrados se pueden cifrar con una clave de cifrado AES-128 que puede ser conocida por el módulo de credenciales 36. O se pueden cifrar con una clave de cifrado derivada que se puede determinar a partir de información contenida en la credencial. Además, la firma digital puede ser una firma de tipo CBC-MAC basándose en una clave de cifrado AES-128, por ejemplo, que puede ser conocida por el módulo de credenciales 36. O esta podría ser una firma digital basándose en una clave privada conocida por el servidor 14 y puede ser validada por una clave pública conocida por el módulo de credenciales 36. .

Con referencia a la figura 4, un ejemplo de omisión del método de recepción 200 es iniciado por un usuario que, en primer lugar, reserva una habitación de hotel (la etapa 210) a través de cualquier proceso soportado por un hotel, tal como reservas móviles, sitios web, agentes de viajes, etc. Posteriormente, un procedimiento de registro de entrada confirma su estancia (la etapa 212). De nuevo, esto se puede realizar a través de cualquier proceso soportado por el hotel.

A continuación, se asigna una habitación en un sistema de gestión de propiedades de hotel 60 basándose en las preferencias del huésped (o en la selección de habitación) y en la disponibilidad de habitaciones en el momento del registro de entrada (la etapa 214). El sistema de gestión de propiedades de hotel 60 puede usar una interfaz de programación de aplicaciones (API) de software a software proporcionada por una aplicación de recepción 62 para solicitar datos de tarjeta en forma digital (la etapa 216). La aplicación de recepción 62 puede variar desde un codificador autónomo 64 hasta un paquete de software completo en ejecución en una nube que es operable para codificar una tarjeta virtual para la habitación que se seleccionó y devolver los datos de tarjeta virtual al sistema de hotel (la etapa 218).

A continuación, el sistema de gestión de propiedades de hotel 60 hará otra llamada de API de software a software a un servicio de credenciales 70 después de que el sistema de hotel haya autenticado al usuario y haya asignado una reserva de estancia en habitación (la etapa 220). La información pertinente se comunica al servicio de credenciales 70 con una indicación para incluir, por ejemplo, qué propiedad de hotel, qué habitación, qué huésped (por ejemplo, ID de Usuario), qué fechas y también los datos de tarjeta virtual para la estancia.

Simultáneamente o en secuencia con el envío de los datos de tarjeta virtual al servicio de credenciales 70, el servicio de gestión de propiedades de hotel 60 comunica una indicación al usuario (de nuevo, a través de cualquier método convencional) de que el registro de entrada está confirmado y la habitación está asignada (la etapa 222).

A continuación, una aplicación móvil de fidelidad de hotel 80 basada en el dispositivo móvil 12 utilizará una API de software a software en una biblioteca móvil 82 (la etapa 224) para descargar credenciales desde el servicio de credenciales 70 (la etapa 226). La biblioteca móvil 82 se autenticará de forma segura en el servicio de credenciales 70 con un secreto compartido establecido anteriormente que puede cambiar en cada conexión con éxito.

Una vez autenticado, el servicio de credenciales 70 genera en el momento de la comunicación desde la biblioteca móvil 82 las credenciales para el usuario y cifra en las credenciales los datos de tarjeta virtual recibidos en la etapa 220 para el huésped asociado con este caso de la biblioteca móvil. Se genera una credencial para cada puerta o punto de acceso y los datos de tarjeta virtual serán los mismos en cada una de estas credenciales separadas, pero se pueden cifrar con una clave única para la puerta o punto de acceso particular. El método de cifrado puede ser AES, 3DES u otro método de cifrado de este tipo. El método y tipo de credencial usado puede ser un certificado digital comprimido o un certificado basado en normas como X.509 u otro formato de certificado conocido en la técnica. Es decir, por ejemplo, los datos de tarjeta virtual se cifran en la credencial con una clave única conocida por el módulo de credenciales 36 y por el servicio de credenciales 70.

La biblioteca móvil 82 descargará y almacenará la lista de credenciales en el dispositivo móvil 12 usando protecciones de SO nativas y un cifrado adicional de datos con información específica del dispositivo, por ejemplo, direcciones MAC,

IMSI, IMEI, UDID, etc. Ahora que el registro de entrada se ha completado y que la credencial móvil cifrada (con datos de tarjeta virtual) reside en el dispositivo móvil 12 (la figura 2), el usuario puede operar el control de acceso 16 en un modo fuera de línea en cualquier momento posterior sin que se requiera que el dispositivo móvil 12 se conecte al servicio de credenciales 70. Realizaciones adicionales pueden hacer que el dispositivo móvil 12 descargue una credencial al mismo tiempo que el dispositivo móvil se está comunicando con el control de acceso 16 al mismo tiempo que el usuario desea acceder a su habitación, por ejemplo.

Cuando el usuario desea acceder a su habitación (la etapa 228), el usuario indica tal intención a través de un gesto, un clic de un botón, un toquecito en la pantalla, una lectura de huella dactilar, una contraseña, la proximidad a la cerradura, tocar la cerradura, etc. En respuesta a esta intención, la aplicación móvil de fidelidad de hotel 80 llama de nuevo a la API de software a software en la biblioteca móvil 82 para iniciar la transferencia segura de la credencial móvil cifrada al control de acceso 16 (la etapa 230). Mientras la aplicación de fidelidad 80 inicia la transferencia, la biblioteca móvil implementa la transferencia segura de forma separada en la siguiente etapa.

Una transferencia segura de la credencial (la etapa 232) se puede iniciar con un proceso en el que la biblioteca móvil 82 escucha un anuncio de señal, tal como anuncios de Bluetooth de baja energía (BTLE) desde los controles de acceso 16 dentro del alcance. Es decir, los controles de acceso 16 están anunciando su presencia a un ritmo periódico con datos de anuncio que indican un identificador del control de acceso 16 y el dispositivo móvil 12 puede escuchar y conectarse automáticamente sin que la persona tenga que presionar un botón para reactivar una cerradura alimentada por batería 16 en reposo o para salir de un vehículo para interaccionar con un punto de acceso de lector en una puerta de garaje u otro dispositivo. El punto de acceso de lector es otro tipo de la cerradura 16. Otra realización es el uso de Comunicación de Campo Cercano (NFC) y la persona da un 'toquecito' con su dispositivo móvil en la cerradura 16 y un intercambio de credenciales seguro transfiere la credencial móvil al control de acceso 16 (la etapa 232). Los intercambios de credenciales seguros se pueden realizar usando técnicas convencionales tales como el establecimiento de una clave de sesión, el cifrado de mensajes de comunicación y la validación de la autenticidad del remitente y el destinatario del mensaje.

En la realización preferida en la que el control de acceso se anuncia usando Bluetooth de baja energía (BTLE), la biblioteca móvil 82 filtra los anuncios recibidos basándose en el identificador recibido del control de acceso 16 y mediante una comparación con identificadores contenidos en o asociados con cada credencial en la lista de credenciales móviles y basándose en la intención del usuario de acceder a una habitación particular. Una vez que se ha recibido un anuncio para un control de acceso 16 objetivo, la biblioteca móvil 82 inicia una conexión inalámbrica y realiza una transferencia segura de la credencial móvil cifrada (la etapa 232). La transferencia segura puede utilizar una clave de cifrado de sesión única y técnicas y algoritmos criptográficos convencionales. Debería apreciarse que los datos se pueden transmitir de forma segura a través de cualquier enlace inalámbrico, incluyendo, pero sin limitación, BTLE, zigbee, Comunicación de Campo Cercano, etc.

El módulo de credenciales 36 recibirá la credencial móvil cifrada, entonces validará y descifrará la credencial móvil cifrada para recuperar los datos de tarjeta virtual. El descifrado y la validación pueden incluir, pero sin limitación, validar una firma digital, validar el tipo de la credencial, validar que el identificador de credencial coincida con un identificador en la memoria de cerradura 32, validar una fecha de inicio y una fecha de vencimiento de la credencial, validar el origen de la credencial, etc. (la etapa 118; figura 3). Una vez validados y descifrados, se extraen los datos de tarjeta virtual (la etapa 120; figura 3).

Los datos de tarjeta virtual se comunican entonces a través de interfaces de hardware y de software, dependiendo de las realizaciones, al controlador de cerradura 24, que puede descifrar adicionalmente los datos de tarjeta virtual, procesa los datos basándose en reglas de proveedores de cerradura y, entonces, abrir la cerradura si se permite la entrada (la etapa 234). En particular, los datos de tarjeta virtual se comunican al controlador de cerradura 24 como una "lectura de tarjeta virtual" en un formato de datos equivalente al de una tarjeta de llave física. Por lo tanto, esto permite el uso continuado de las tarjetas de llave de huésped 92 tradicionales, tales como la de un miembro de una familia o un huésped que simplemente quiere una copia de la tarjeta de llave física 92, junto con el uso del dispositivo móvil 12.

El registro de auditoría subido por el dispositivo móvil 12 pueden ser simplemente las auditorías generadas por el propio dispositivo móvil 12, o pueden ser las auditorías unificadas que incluyen aperturas por el huésped usando una tarjeta de llave física. Además, cuando se abre la cerradura 16, se puede subir un estado de batería u otra información de mantenimiento de la misma al registro de auditoría desde el dispositivo móvil 12 al servicio de credenciales 70 de tal modo que se pueden notificar condiciones de batería baja al hotel y cambiar de forma proactiva las baterías, o realizar otro mantenimiento. Otra información asociada con el registro de auditoría puede incluir, por ejemplo, aperturas fallidas o intentos fallidos o credenciales cuya validación falló.

El uso de la "lectura de tarjeta virtual" mantiene un registro de auditoría contiguo y también mantiene todos los casos de uso conocidos para el control de acceso que ya se codifican en los datos de tarjeta tradicionales. Además, el módulo de credenciales 36 es independiente del proveedor de cerraduras, de tal modo que los datos de cualquier proveedor de cerraduras se podrían traspasar para permitir que cada proveedor de cerraduras innove de forma independiente con los datos de tarjeta. Además, el módulo de credenciales 36 puede ser suministrado por una empresa diferente de

la de la cerradura 16. Y, asimismo, el servidor 14, el dispositivo móvil 12 y el módulo de credenciales 36 pueden no tener medio alguno para descifrar o validar adicionalmente los datos de tarjeta que no sea tratar estos como un objeto de datos a codificar, cifrar, transferir, recuperar y entregar. Adicionalmente, la "lectura de tarjeta virtual" se puede usar fuera de línea sin requerir que el dispositivo móvil 12 esté en línea con una conexión de Wi-Fi o una conexión en tiempo real a un servicio de credenciales. Es decir, los datos para la "lectura de tarjeta virtual" se almacenan en el dispositivo móvil 12 y se pasan de forma segura al módulo de credenciales 36 en un modo fuera de línea. Esto no tiene el fin de limitar la capacidad de enviar también la "lectura de tarjeta virtual" en un modo en línea. Un beneficio adicional es que cualquier control de acceso 16 puede usar cualquier tipo de tarjeta además de usar un módulo de credenciales 36, en donde los tipos de tarjeta incluyen, pero sin limitación, banda magnética, RFID, proximidad, etc.

En otra realización no limitante divulgada, el módulo de credenciales 36 se puede usar para muchos fines, incluyendo, pero sin limitación, pasar datos a una unidad de dispensación de llaves físicas de autoservicio 98 que genera las tarjetas de llave físicas 92. La unidad de dispensación de llaves físicas 98 tiene un módulo de credenciales 36 que recibe los datos de tarjeta virtual, los descifra, los extrae y los envía a un controlador de cerradura 24 configurado para codificar los datos en una tarjeta de llave física 92. Es decir, los datos de tarjeta virtual en el dispositivo móvil 12 son escritos en una tarjeta de llave física 92 por la unidad 98, y distribuye la tarjeta de llave 92 de forma automática. La unidad 98 no requiere interfaz de usuario alguna aparte del elemento de dispensación para la tarjeta de llave 92 y una fuente de alimentación de unidad, incluyendo, pero sin limitación, baterías, alimentación de la red de distribución eléctrica, recolección de energía y similares. La interfaz de usuario para la unidad 98 es, en realidad, la interfaz del dispositivo móvil 12. Cuando la unidad 98 comienza a quedarse sin tarjetas de llave 92 en blanco, el dispositivo móvil 12 puede subir al servidor de credenciales 70 una indicación del estado que se puede convertir en un informe para notificar al hotel que es necesario rellenar la unidad 98.

En otras realizaciones no limitantes divulgadas, los datos de tarjeta virtual pueden ser datos de tarjeta de control de acceso convencional (es decir, datos de identificación) para sistemas de acceso con placa, o integrarse en una máquina expendedora con los datos de tarjeta virtual como información de tarjeta de crédito, fichas, identificadores de referencia de compra, o similares.

Con referencia a la figura 5, la biblioteca móvil 82 puede incluir un conjunto de credenciales móviles que fueron generadas por el servicio de credenciales 70 basándose en las categorías de acceso 300 (un permiso implícito) además de la credencial móvil con los datos de tarjeta virtual (un permiso explícito) 302 que fue generada por el servicio de credenciales 70 para un control de acceso 16a específico. Las categorías de acceso 300 operan para conceder al usuario acceso a una agrupación particular de los controles de acceso 16b que tienen un significado colectivo. Por ejemplo, una categoría de acceso podría ser 'Salas Públicas' para el acceso a una piscina, un centro de negocios, un ascensor y lectores de pared. En el contexto de una reserva de hotel, cuando el dispositivo móvil 12 se comunica con el servicio de credenciales 70 para descargar la credencial móvil cifrada, el servicio de credenciales 70 genera credenciales para cada cerradura en una o más categorías de acceso a las que se le ha concedido acceso al huésped. Por lo tanto, la credencial móvil cifrada tendrá los mismos datos de tarjeta virtual codificados específicamente para cada punto de acceso especificado, por ejemplo, piscina, centro de negocios, etc. y puede tener, opcionalmente, la categoría de acceso descargada en o con la credencial. Sin embargo, cada credencial móvil se cifrará de forma separada con una clave única para cada control de acceso 16b.

La provisión y el uso de la categoría de acceso 300 por el servicio de credenciales 70 facilita la gestión eficiente de múltiples controles de acceso 16b en un sistema en donde el dispositivo móvil 12 puede abrir multitudes de cerraduras en donde el dispositivo móvil 12 tiene una credencial específica para cada cerradura. Esto es más sencillo en comparación con lo que se requiere convencionalmente, por ejemplo, dos sistemas de control de acceso - uno para el sistema de hotel que genera los datos de tarjeta virtual con toda la técnica actual para las reglas comerciales de acceso del sistema de hotel, y un segundo para conceder acceso con una credencial móvil para cada punto de acceso, por ejemplo, habitación de huésped, lectores de pared, piscina, salón de negocios, etc. En otras palabras, sería necesario duplicar las reglas comerciales para el sistema de hotel en el servicio de credenciales.

La categoría de acceso 300 permite una integración de múltiples proveedores y puede funcionar de forma separada de las reglas comerciales de acceso del sistema de hotel que quedan codificadas en datos de tarjeta virtual. Las credenciales móviles son, por lo tanto, una 'capa' adicional de seguridad "encima de" los datos de tarjeta virtual. La categoría de acceso 300 también permite procedimientos de mantenimiento relativamente más sencillos, tales como, por ejemplo, cuando se reemplaza una cerradura en la Categoría de Acceso 'Público', solo es necesario que la cerradura de reemplazo se asigne a la misma categoría de acceso. Sin embargo, un dispositivo móvil 12 seguiría necesitando comunicarse de nuevo con el servicio de credenciales 70 para descargar un nuevo conjunto de credenciales móviles. No se requiere administración adicional por parte del huésped o sistema aparte de incluir la cerradura de reemplazo en la categoría de acceso correcta, y todos los permisos del huésped seguirán funcionando con fluidez y sin modificaciones, aunque la nueva cerradura tenga claves de cifrado únicas a partir de la cerradura anterior.

Con referencia a la figura 6, en otra realización no limitante divulgada, un método 400 para inicializar un dispositivo móvil para operar en un sistema de acreditación móvil incluye inicialmente descargar una aplicación al dispositivo móvil 12 (la etapa 410). En un ejemplo, la aplicación incluye dos partes compiladas conjuntamente, siendo una parte

la aplicación de fidelidad de hotel 80 y siendo la otra parte una biblioteca de credenciales móviles 82 como se ha descrito anteriormente para proporcionar una experiencia unificada con una única interfaz de usuario. Además, la aplicación de fidelidad de hotel 80 hace uso de la biblioteca de credenciales móviles 82 a través de una interfaz de programación de aplicaciones (API) de software a software proporcionada por la biblioteca de credenciales móviles 80. Otro ejemplo incluye dos aplicaciones separadas, siendo una la aplicación de fidelidad de hotel y siendo la otra una aplicación de credencial móvil que requiere una comunicación de aplicación a aplicación autenticada (por ejemplo, ficha, ID/contraseña, intercambio de certificado bidireccional, etc.) con llamadas entre aplicaciones para realizar las llamadas de API de tal modo que la aplicación de credenciales incluye una interfaz de usuario para la interacción. El método 400 descrito en el presente documento se puede realizar en uno u otro ejemplo.

A continuación, una vez que se ha cargado la aplicación, el usuario autentica su aplicación de fidelidad de hotel 80 (la etapa 420). Esto se inicia habitualmente introduciendo un identificador de cuenta de fidelidad de hotel y una contraseña en la aplicación de fidelidad de hotel 80 en el dispositivo móvil 12.

A continuación, la aplicación de fidelidad de hotel crea una conexión segura con el sistema de gestión de propiedades de hotel 60 y comunica el ID y la contraseña para su validación (la etapa 430). El establecimiento de esta conexión segura y la comunicación o validación del ID y la contraseña se pueden realizar a través de técnicas bien conocidas en el campo de la validación de cuentas de usuario. Por lo tanto, el sistema de gestión de propiedades de hotel 60 está validando la autenticidad de la cuenta de fidelidad de hotel y, por asociación, la autenticidad e identidad del usuario.

A continuación, basándose, por ejemplo, en unas preferencias que indican que la cuenta de fidelidad de hotel está habilitada para la acreditación móvil, y que la aplicación de fidelidad de hotel 80 soporta la acreditación móvil, el sistema de gestión de propiedades de hotel 60 enviará automáticamente una solicitud al servicio de acreditación 70 a través de un interfaz de programación de aplicaciones (API) de software a software para solicitar un código de autorización para este ID de usuario particular (la etapa 440). El servicio de credenciales 70 confía en el sistema de gestión de propiedades de hotel 60 para autenticar en primer lugar el ID de usuario y acepta la llamada de API a través de relaciones de confianza normales, incluyendo, pero sin limitación, una cuenta administrativa del sistema de hotel (ID/contraseña) en el cliente del servicio de credenciales y certificados de SSL de servidor, una VPN, un intercambio de certificados SSL bidireccional, o simplemente por el hecho de que el sistema de gestión de propiedades de hotel 60 y el servicio de credenciales 70 están alojados en el mismo entorno.

A continuación, después de recibir la solicitud de un código de autorización, el servicio de credenciales 70 genera el código de autorización para la cuenta de acreditación móvil identificada (la etapa 450). El código de autorización está cifrado y contiene un identificador de número de serie de biblioteca de credenciales móviles e información para establecer la primera conexión con el servicio de credenciales 70. Este código de autorización puede, por ejemplo, tener una longitud de 30 dígitos o cualquier longitud requerida para incluir la información requerida y proporcionar información aleatoria para garantizar la seguridad y validar la autenticidad del código de autorización.

Además de generar el código de autorización, el servicio de credenciales 70 también desbloquea la cuenta de acreditación móvil asociada con el código de autorización para permitir una 'primera sincronización'. El desbloqueo puede incluir, por ejemplo, un atributo de la cuenta en donde, después de la primera sincronización, el servicio requerirá que un desafío/respuesta desde la biblioteca móvil 82 sea validado por el servicio de credenciales 70 para una comunicación adicional entre la biblioteca móvil 82 y el servicio de credenciales 70 para, por ejemplo, generar credenciales móviles y realizar descargas. Se establecería un secreto compartido en la primera sincronización entre el servicio de credenciales 70 y la biblioteca de credenciales móviles 82 que se podría usar para el desafío/respuesta como es bien conocido en la técnica de la autenticación de un sistema con un secreto compartido. El secreto compartido puede cambiar o 'desplazarse' en sincronizaciones subsiguientes de tal modo que ya no se podría realizar la primera sincronización. Como alternativa, el desbloqueo puede incluir el almacenamiento de información cifrada en el código de autorización que puede ser enviado al servicio de credenciales por la biblioteca de credenciales móviles 82, y se compara en la primera sincronización o se usa con un desafío/respuesta en la primera sincronización como un primer secreto compartido. Una vez que esta información coincide, la misma se cambia en sincronizaciones subsiguientes de tal modo que el código de autorización no pueda ser utilizable de nuevo debido a que ha cambiado la información de la 'primera sincronización'.

A continuación, el código de autorización se devuelve al sistema de gestión de propiedades de hotel 60 y, entonces, se descarga automáticamente a la aplicación de fidelidad de hotel 80 junto con el URL de anfitrión de servicio de credenciales (la etapa 460). El URL de anfitrión se proporciona de tal modo que el sistema de hotel 60 puede indicar a la biblioteca de credenciales móviles 82 que se comunique con un caso específico del servicio de credenciales 70. El servicio de credenciales 70 se podría alojar, por ejemplo, en diferentes ubicaciones para una distribución de cargas geográfica, o alojarse de forma separada para un centro de datos de respaldo en caso de caída del primario. La selección del URL de anfitrión por el sistema de hotel 60 se puede hacer con un parámetro de configuración en el sistema de hotel 60, o se puede hacer por inferencia basándose en la ubicación de la API del servicio de credenciales 70, o se puede hacer basándose en el estado del servicio de credenciales 70, etc.

A continuación, la aplicación de fidelidad de hotel 80 envía el código de autorización y el URL de anfitrión de servicio

de credenciales a la biblioteca de credenciales móviles 82, de nuevo a través de una API de software a software (la etapa 470). Al pasar el código de autorización a la biblioteca de credenciales 82, la aplicación de fidelidad de hotel 80 está traspasando una relación de confianza que se estableció en primer lugar entre la aplicación de fidelidad de hotel 80 y el sistema de gestión de hotel 60 y que se amplió adicionalmente para incluir el servicio de credenciales 70 y que ahora incluirá también la biblioteca móvil 82.

A continuación, la biblioteca móvil 82 descifra el código de autorización, valida el código de autorización y, entonces, recupera un número de serie de biblioteca móvil y otra información contenida en el código de autorización (la etapa 470). La biblioteca móvil 82 usa la información para realizar la primera sincronización con el servicio de credenciales 70 y para realizar una autenticación (la etapa 480). El servicio de credenciales 70 valida la primera información de sincronización y, entonces, establece la relación de confianza continuada entre la biblioteca de credenciales móviles 82 y el servicio de credenciales 70. La primera sincronización se ha descrito anteriormente y, después de esta primera sincronización, la biblioteca móvil 82 tendrá un secreto compartido con el servicio de credenciales 70 que se puede usar para realizar una autenticación en sincronizaciones subsiguientes. Adicionalmente, en la primera sincronización, la biblioteca móvil 82 puede validar la autenticidad del servicio de credenciales 70 validando, por ejemplo, un certificado de SSL desde el anfitrión del servicio de credenciales 70.

Por lo tanto, hay tres relaciones de confianza primarias (la figura 7): una entre la aplicación de fidelidad de hotel 80 y el sistema de gestión de propiedades de hotel 60 que se basa en la autorización de cuenta de fidelidad de hotel; otra entre el sistema de gestión de propiedades de hotel 60 y el servicio de credenciales 70 basándose en una autorización de servicio a servicio tal como un intercambio y validación de certificado de SSL bidireccional; y, ahora, una tercera relación de confianza que ha sido creada por el traspaso automático de la primera relación de confianza a la tercera relación de confianza que es una relación de confianza entre la biblioteca de credenciales móviles 82 y el servicio de credenciales 70. Durante la primera sincronización, y posteriormente, el servicio de credenciales 70 genera credenciales móviles para la biblioteca de credenciales móviles 82 para el usuario asociado.

A continuación, después de la primera sincronización, la biblioteca de credenciales móviles 82 indica a la aplicación de fidelidad de hotel 80 el estado de la primera sincronización, por ejemplo, éxito/fracaso (la etapa 490 de la figura 6). La aplicación de fidelidad de hotel 80 indica entonces un estado de listo para dar servicio (la etapa 495). Ahora que la biblioteca de credenciales móviles 82 está completamente aprovisionada y ha descargado las credenciales móviles, la aplicación 80 se puede usar para abrir cerraduras de habitación de huésped de hotel, interaccionar con dispensadores de llaves, cajas de seguridad de bienes inmuebles y otros usos de computación móvil y de acreditación móvil.

El método 400 para inicializar un dispositivo móvil para operar en un sistema de acreditación móvil opera, por lo tanto, sin que un usuario del dispositivo móvil 12 tenga que conocer ni el código de autorización ni la ubicación del anfitrión para el servicio de credenciales 70. Adicionalmente, la aplicación de fidelidad de hotel 80 puede cambiar la ubicación del anfitrión según sea necesario para equilibrar o regionalizar a los usuarios de todo el mundo para el equilibrado de cargas, o para gestionar los cortes en el servicio sin que se informe al usuario acerca de la ubicación del anfitrión del servicio de credenciales 70. Es decir, el método proporciona una autenticación centralizada y un despliegue descentralizado.

Los elementos descritos y representados en el presente documento, incluyendo los presentes en diagramas de flujo y diagramas de bloques de principio a fin de las figuras, implican límites lógicos entre los elementos. Sin embargo, de acuerdo con prácticas de ingeniería de software o de hardware, los elementos representados y las funciones de los mismos se pueden implementar en máquinas a través de medios ejecutables por ordenador que tengan un procesador capaz de ejecutar instrucciones de programa almacenadas en los mismos como una estructura de software monolítica, como módulos de software autónomos o como módulos que emplean rutinas, código, servicios, y así sucesivamente, de naturaleza externa, o cualquier combinación de estos, y todas las implementaciones de este tipo pueden estar dentro del alcance de la presente divulgación.

Se ha de interpretar que el uso de los términos "un/una", "el/la" y referencias similares en el contexto de la descripción (especialmente, en el contexto de las siguientes reivindicaciones) cubre tanto el singular como el plural, a menos que se indique lo contrario en el presente documento o que se contradiga específicamente por el contexto. El modificador "aproximadamente" usado en relación con una cantidad incluye el valor expuesto y tiene el significado dictado por el contexto (por ejemplo, este incluye el grado de error asociado con la medición de la cantidad particular). Todos los rangos divulgados en el presente documento incluyen los puntos de extremo, y los puntos de extremo son combinables de forma independiente entre sí.

Aunque las diferentes realizaciones no limitantes tienen componentes ilustrados específicos, las realizaciones de la presente invención no se limitan a esas combinaciones particulares. Es posible usar algunos de los componentes o características a partir de cualquiera de las realizaciones no limitantes en combinación con características o componentes a partir de cualquiera de las otras realizaciones no limitantes.

Debería apreciarse que, de principio a fin de los varios dibujos, números de referencia semejantes identifican elementos correspondientes o similares. También debería apreciarse que, aunque en la realización ilustrada se divulga

una disposición de componentes particular, otras disposiciones se beneficiarán de la misma.

Aunque se muestran, se describen y se reivindican secuencias de etapas particulares, se debería entender que las etapas se pueden realizar en cualquier orden, separadas o combinadas, a menos que se indique lo contrario, y se seguirán beneficiando de la presente divulgación.

La descripción anterior es ilustrativa en lugar de ser definida por las limitaciones dentro de la misma. En el presente documento se divulgan diversas realizaciones no limitantes, sin embargo, un experto en la materia reconocería que diversas modificaciones y variaciones a la luz de las enseñanzas anteriores caerán dentro del alcance de las reivindicaciones adjuntas. Por lo tanto, se ha de entender que, dentro del alcance de las reivindicaciones adjuntas, la divulgación se puede poner en práctica de una forma distinta de la descrita específicamente en el presente documento. Por esa razón, las reivindicaciones adjuntas se deberían estudiar para determinar su verdadero alcance y contenido.

REIVINDICACIONES

1. Un método para inicializar un dispositivo móvil (12) para operar en un sistema de acreditación móvil, comprendiendo el método:

enviar un código de autorización y un Localizador de Recursos Universal (URL) de anfitrión a una biblioteca de credenciales móviles (82) de una aplicación móvil en el dispositivo móvil, operable el dispositivo móvil para realizar una primera sincronización con un servicio de credenciales (70) para establecer una relación de confianza continuada entre la biblioteca de credenciales móviles y el servicio de credenciales de tal modo que la aplicación móvil es operable para interaccionar con un control de acceso (16) sin que un usuario del dispositivo móvil conozca ni el código de autorización ni el URL de anfitrión del servicio de credenciales; y
pasar automáticamente de una primera relación de confianza a la relación de confianza continuada entre la biblioteca de credenciales móviles y el servicio de credenciales, en donde la primera relación de confianza es entre una aplicación de fidelidad (80) y un sistema de gestión de propiedades de hotel (60),
y hay otra relación de confianza entre el sistema de gestión de propiedades de hotel (60) y el servicio de credenciales basándose en una autorización de servicio a servicio.

2. El método según la reivindicación 1, en donde el sistema de gestión de propiedades de hotel (60) se basa en una autorización de cuenta de fidelidad de hotel.

3. El método según la reivindicación 1, que comprende además generar credenciales móviles en el servicio de credenciales (70) para su descarga a la biblioteca de credenciales móviles (82).

4. El método según la reivindicación 3, en donde las credenciales móviles son para una cuenta de ID de usuario asociada.

5. El método según la reivindicación 1, en donde el dispositivo móvil (12) incluye un teléfono inteligente.

6. El método según la reivindicación 5, en donde el control de acceso (16) es una cerradura.

7. El método según la reivindicación 5, en donde el control de acceso (16) es una caja de seguridad.

8. El método según la reivindicación 1, en donde el servicio de credenciales (70) está alojado en una de una multitud de ubicaciones.

9. El método según la reivindicación 8, en donde esa una de la multitud de ubicaciones se selecciona para una distribución de cargas geográfica.

10. El método según la reivindicación 1, en donde la biblioteca de credenciales móviles (82) descifra el código de autorización, valida el código y recupera un número de serie de biblioteca móvil contenido en el código de autorización.

11. El método según la reivindicación 10, en donde la biblioteca de credenciales móviles (82) usa información contenida en el código de autorización para realizar la primera sincronización con el servicio de credenciales (70) y para realizar una autenticación.

12. El método según la reivindicación 11, en donde el servicio de credenciales (70) valida la primera información de sincronización y, entonces, establece la relación de confianza continuada entre la biblioteca de credenciales móviles (82) y el servicio de credenciales.

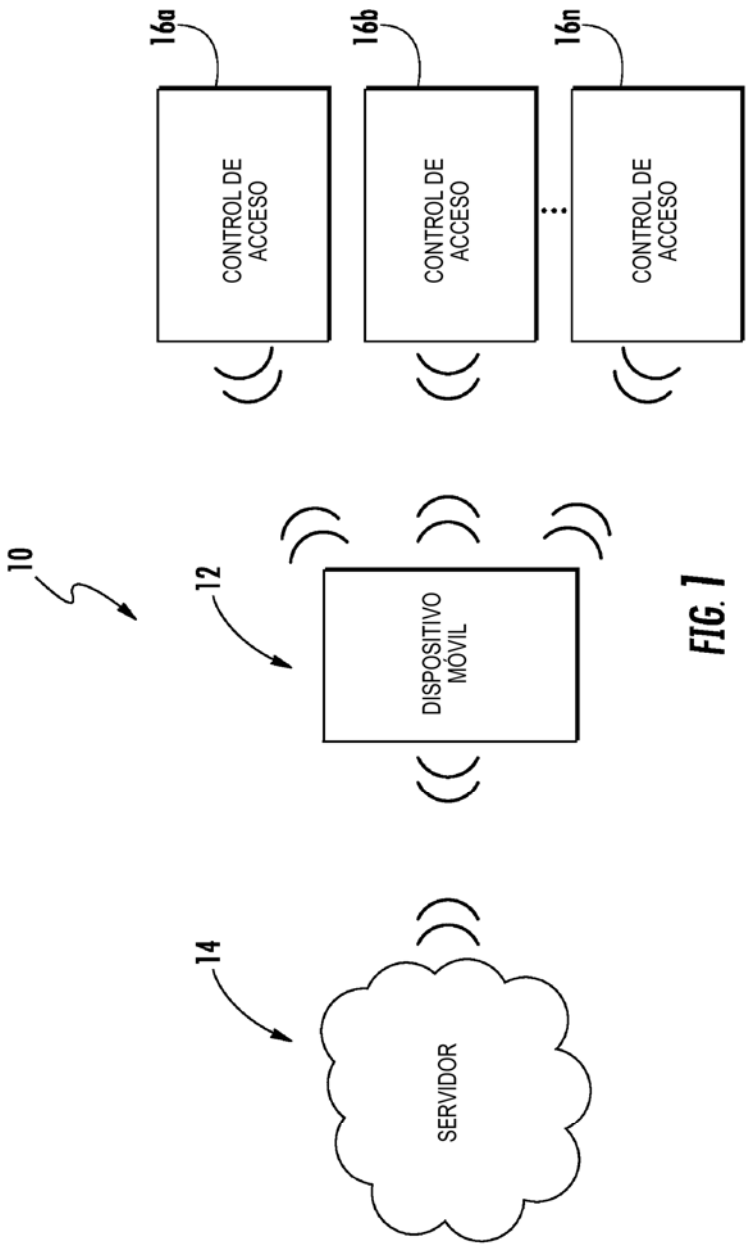
16a
16b
16n
CONTROL DE ACCESO
CONTROL DE ACCESO
CONTROL DE ACCESO
10
12
DISPOSITIVO MÓVIL
14
SERVIDOR

FIG. 1

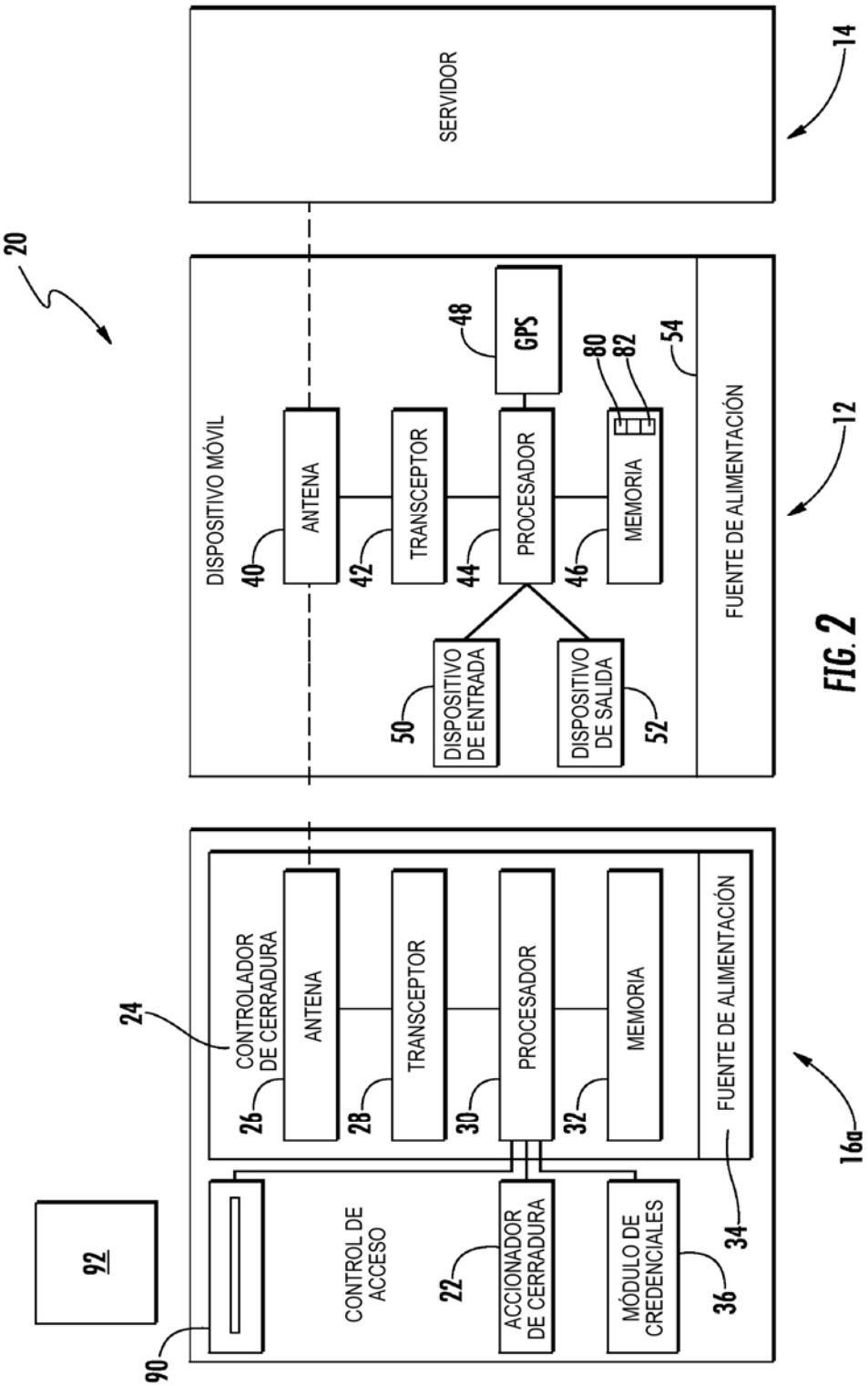
20
SERVIDOR
14
DISPOSITIVO MÓVIL
ANTENA
TRANSCEPTOR
PROCESADOR
MEMORIA
GPS
FUENTE DE ALIMENTACIÓN
12
40
42
44
46
48
80
82
54
DISPOSITIVO DE ENTRADA
DISPOSITIVO DE SALIDA
50
52
24
CONTROLADOR DE CERRADURA
ANTENA
TRANSCEPTOR
PROCESADOR
MEMORIA
FUENTE DE ALIMENTACIÓN
26
28
30
32
16a
92
90
CONTROL DE ACCESO
ACCIONADOR DE CERRADURA
MÓDULO DE CREDENCIALES
22
34
36

FIG. 2

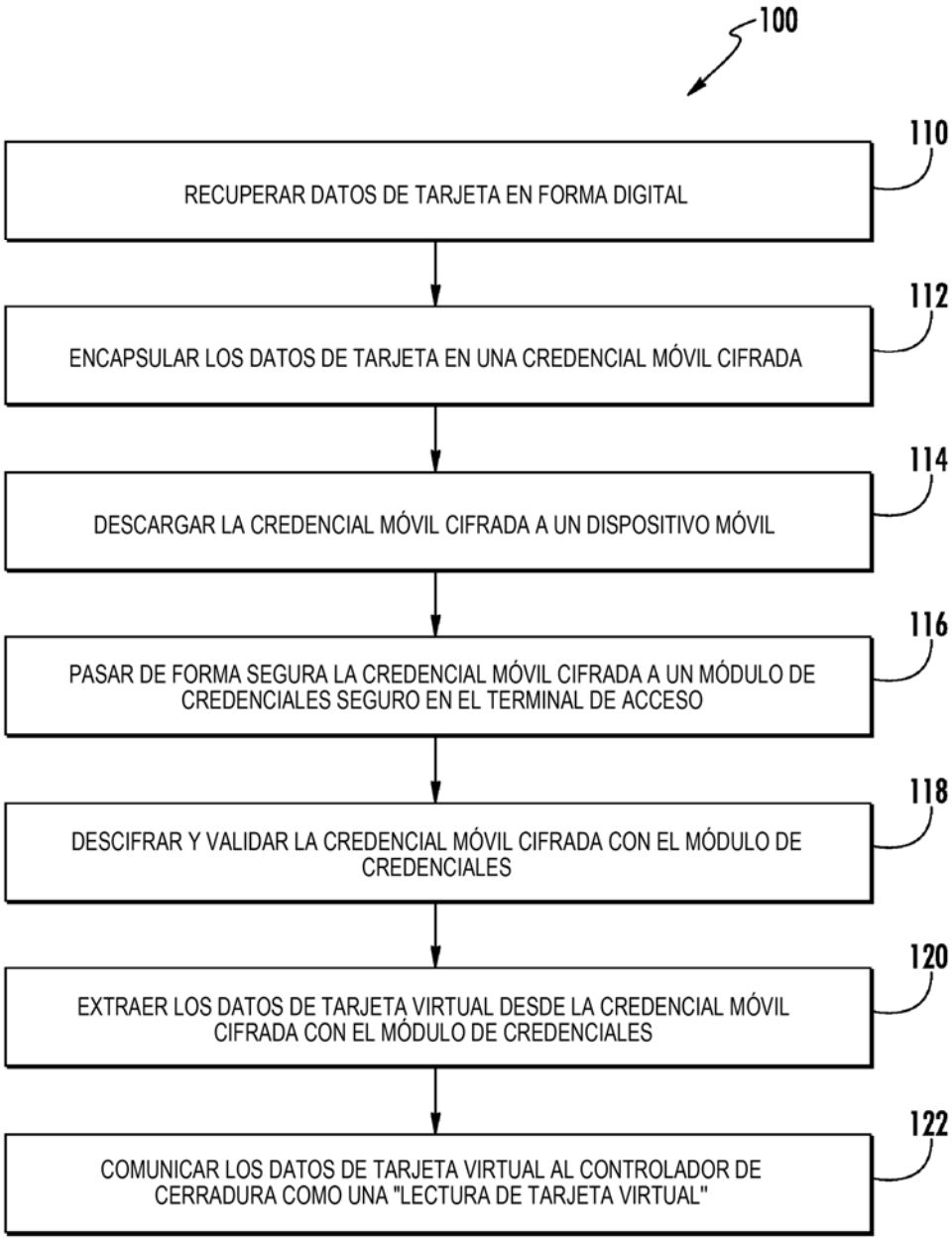
100
110
RECUPERAR DATOS DE TARJETA EN FORMA DIGITAL
112
ENCAPSULAR LOS DATOS DE TARJETA EN UNA CREDENCIAL MÓVIL CIFRADA
114
DESCARGAR LA CREDENCIAL MÓVIL CIFRADA A UN DISPOSITIVO MÓVIL
116
PASAR DE FORMA SEGURA LA CREDENCIAL MÓVIL CIFRADA A UN MÓDULO DE CREDENCIALES SEGURO EN EL TERMINAL DE ACCESO
118
DESCIFRAR Y VALIDAR LA CREDENCIAL MÓVIL CIFRADA CON EL MÓDULO DE CREDENCIALES
120
EXTRAER LOS DATOS DE TARJETA VIRTUAL DESDE LA CREDENCIAL MÓVIL CIFRADA CON EL MÓDULO DE CREDENCIALES
122
COMUNICAR LOS DATOS DE TARJETA VIRTUAL AL CONTROLADOR DE CERRADURA COMO UNA "LECTURA DE TARJETA VIRTUAL"

FIG. 3

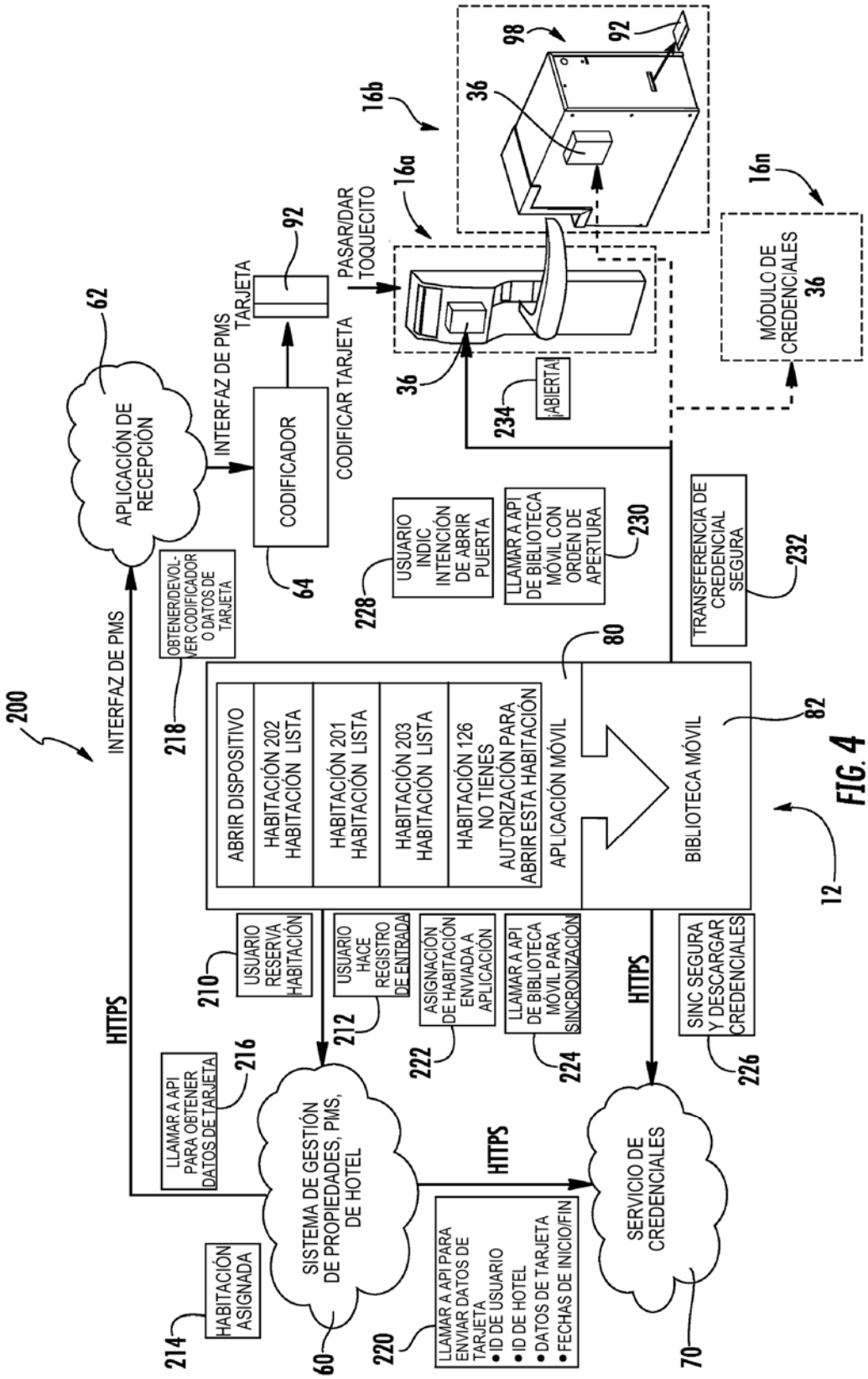
200
INTERFAZ DE PMS
HTTPS
62
APLICACIÓN DE RECEPCIÓN
INTERFAZ DE PMS
CODIFICADOR
CODIFICAR TARJETA
TARJETA
92
PASAR/DAR TOQUECITO
16a
16b
16n
36
98
92
MÓDULO DE CREDENCIALES 36
ABIERTA
234
228
USUARIO INDIC INTENCIÓN DE ABRIR PUERTA
LLAMAR A API DE BIBLIOTECA MÓVIL CON ORDEN DE APERTURA
230
TRANSFERENCIA DE CREDENCIAL SEGURA
232
OBTENER/DEVOLVER CODIFICADOR O DATOS DE TARJETA
218
80
ABRIR DISPOSITIVO
HABITACIÓN 202 HABITACIÓN LISTA
HABITACIÓN 201 HABITACIÓN LISTA
HABITACIÓN 203 HABITACIÓN LISTA
HABITACIÓN 126 NO TIENES AUTORIZACIÓN PARA ABRIR ESTA HABITACIÓN
APLICACIÓN MÓVIL
BIBLIOTECA MÓVIL
82
12
USUARIO RESERVA HABITACIÓN
210
USUARIO HACE REGISTRO DE ENTRADA
212
ASIGNACIÓN DE HABITACIÓN ENVIADA A APLICACIÓN
222
LLAMAR A API DE BIBLIOTECA MÓVIL PARA SINCRONIZACIÓN
224
HTTPS
SINC SEGURA Y DESCARGAR CREDENCIALES
226
LLAMAR A API PARA OBTENER DATOS DE TARJETA
216
HTTPS
SISTEMA DE GESTIÓN DE PROPIEDADES, PMS, DE HOTEL
60
SERVICIO DE CREDENCIALES
70
HABITACIÓN ASIGNADA
214
LLAMAR A API PARA ENVIAR DATOS DE TARJETA
• ID DE USUARIO
• ID DE HOTEL
• DATOS DE TARJETA
• FECHAS DE INICIO/FIN
220

FIG. 4

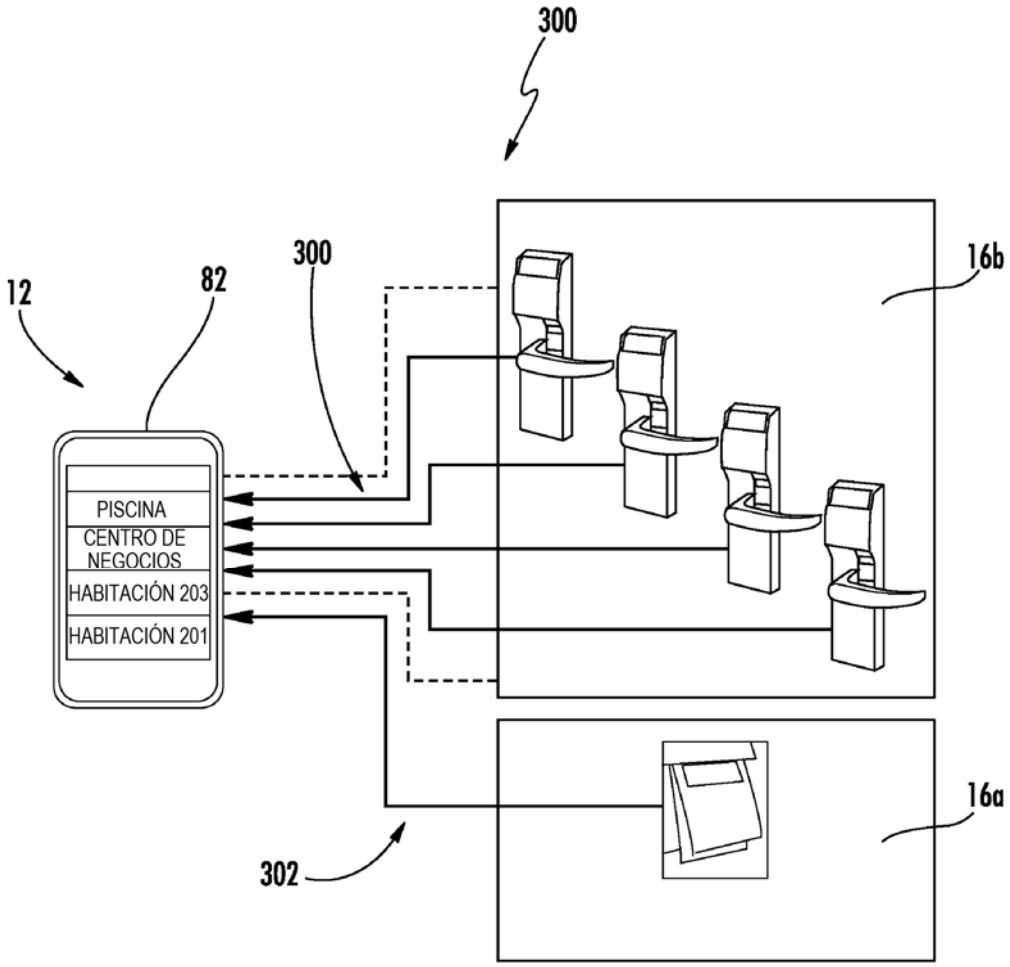
300
12
82
300
16b
PISCINA
CENTRO DE NEGOCIOS
HABITACIÓN 203
HABITACIÓN 201
16a
302

FIG. 5

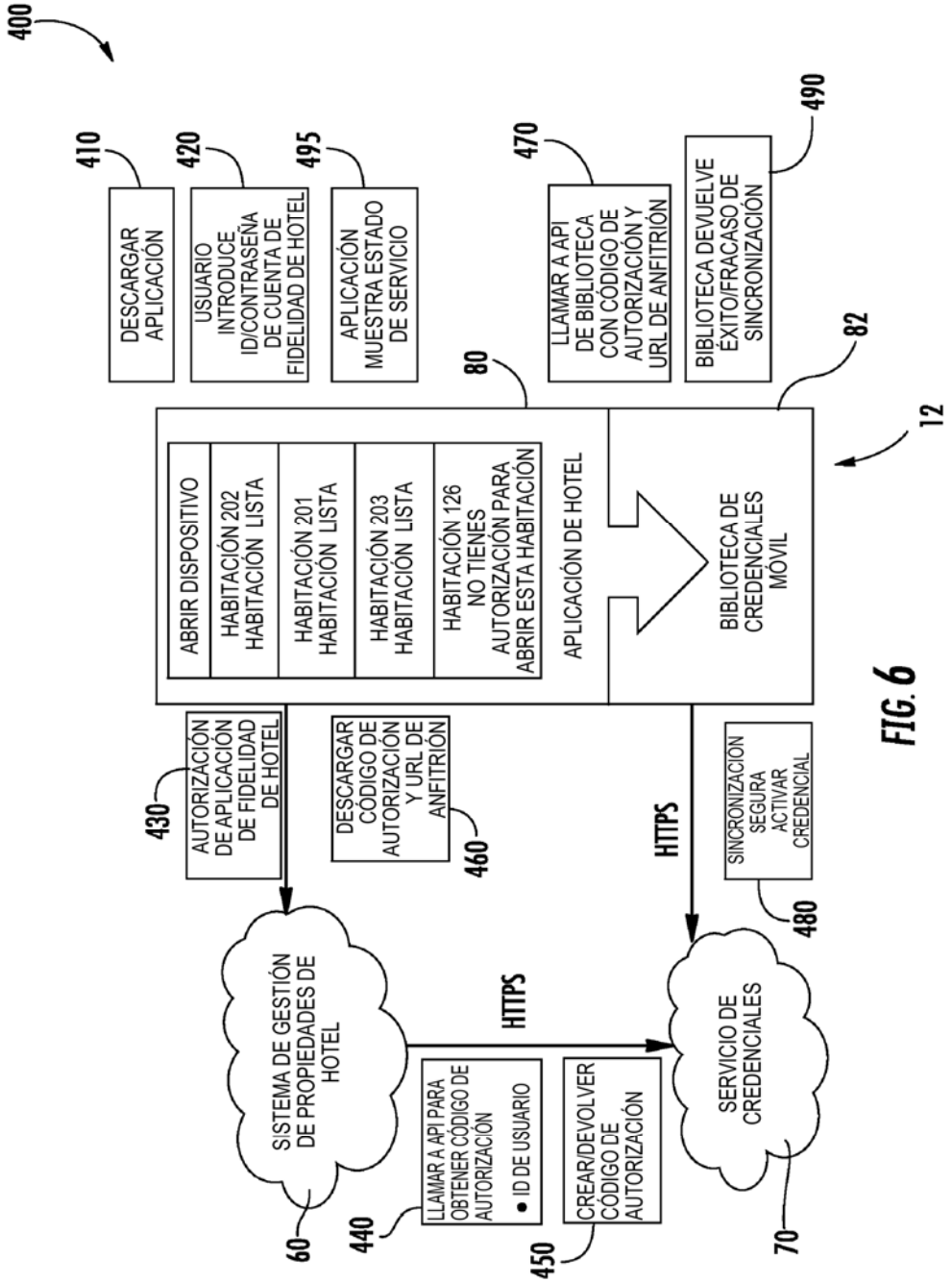
400
410
DESCARGAR APLICACIÓN
420
USUARIO INTRODUCE ID/CONTRASEÑA DE CUENTA DE FIDELIDAD DE HOTEL
495
APLICACIÓN MUESTRA ESTADO DE SERVICIO
470
LLAMAR A API DE BIBLIOTECA CON CÓDIGO DE AUTORIZACIÓN Y URL DE ANFITRIÓN
490
BIBLIOTECA DEVUELVE ÉXITO/FRACASO DE SINCRONIZACIÓN
80
82
12
ABRIR DISPOSITIVO
HABITACIÓN 202 HABITACIÓN LISTA
HABITACIÓN 201 HABITACIÓN LISTA
HABITACIÓN 203 HABITACIÓN LISTA
HABITACIÓN 126 NO TIENES AUTORIZACIÓN PARA ABRIR ESTA HABITACIÓN
APLICACIÓN DE HOTEL
BIBLIOTECA DE CREDENCIALES MÓVIL
430
AUTORIZACIÓN DE APLICACIÓN DE FIDELIDAD DE HOTEL
DESCARGAR CÓDIGO DE AUTORIZACIÓN Y URL DE ANFITRIÓN
460
HTTPS
SINCRONIZACIÓN SEGURA ACTIVAR CREDENCIAL
480
SISTEMA DE GESTIÓN DE PROPIEDADES DE HOTEL
60
HTTPS
SERVICIO DE CREDENCIALES
70
440
LLAMAR A API PARA OBTENER CÓDIGO DE AUTORIZACIÓN
• ID DE USUARIO
450
CREAR/DEVOLVER CÓDIGO DE AUTORIZACIÓN

FIG. 6

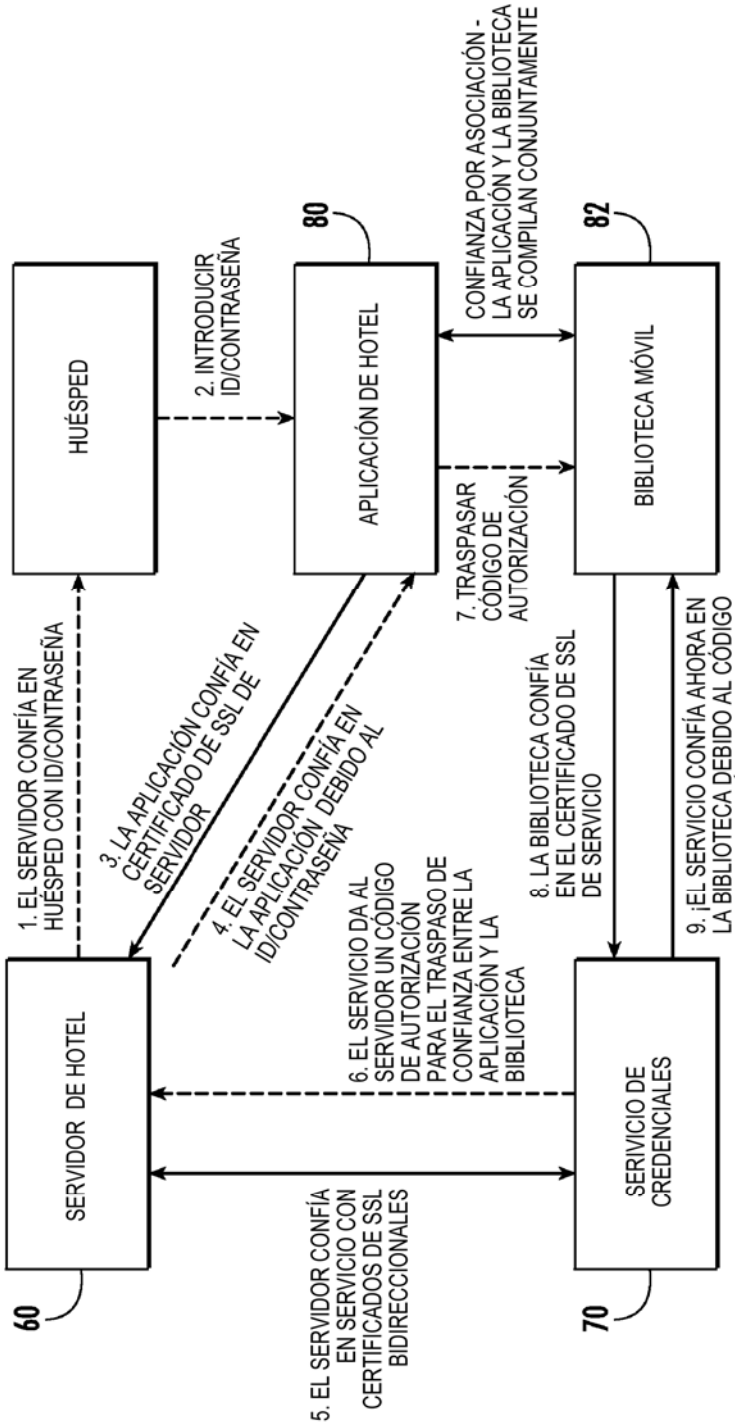
HUÉSPED
APLICACIÓN DE HOTEL
BIBLIOTECA MÓVIL
SERVIDOR DE HOTEL
SERIVICIO DE CREDENCIALES
80
82
60
70
2. INTRODUCIR ID/CONTRASEÑA
CONFIANZA POR ASOCIACIÓN - LA APLICACIÓN Y LA BIBLIOTECA SE COMPILAN CONJUNTAMENTE
7. TRASPASAR CÓDIGO DE AUTORIZACIÓN
1. EL SERVIDOR CONFÍA EN HUÉSPED CON ID/CONTRASEÑA
3. LA APLICACIÓN CONFÍA EN CERTIFICADO DE SSL DE SERVIDOR
4. EL SERVIDOR CONFÍA EN LA APLICACIÓN DEBIDO AL ID/CONTRASEÑA
8. LA BIBLIOTECA CONFÍA EN EL CERTIFICADO DE SSL DE SERVICIO
9. ¡EL SERVICIO CONFÍA AHORA EN LA BIBLIOTECA DEBIDO AL CÓDIGO DE AUTORIZACIÓN!
6. EL SERVICIO DA AL SERVIDOR UN CÓDIGO DE AUTORIZACIÓN PARA EL TRASPASO DE CONFIANZA ENTRE LA APLICACIÓN Y LA BIBLIOTECA
5. EL SERVIDOR CONFÍA EN SERVICIO CON CERTIFICADOS DE SSL BIDIRECCIONALES

FIG. 7