(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 700 476**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.07.2014 E 14178592 (3)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 2977964**

(54) Título: **Procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato a través de un terminal móvil**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2019

(73) Titular/es:

SKIDATA AG (100.0%)
Untersbergstrasse 40
5083 Grödig/Salzburg, AT

(72) Inventor/es:

WENNINGER, CHRISTIAN y
DUCHAC, BERND

(74) Agente/Representante:

RUO , Alessandro

DESCRIPCIÓN

Procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato a través de un terminal móvil

[0001] La presente invención se refiere a un procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato a través de un terminal móvil según el preámbulo de la reivindicación 1.

[0002] Por el estado de la técnica se conocen aparatos, por ejemplo mecanismos de cierre que pueden ser controlados a través de un terminal móvil de un usuario. Para el control del aparato desde el terminal móvil se establece un enlace de datos local con el aparato, adquiriéndose la autorización para el control del aparato mediante una interacción entre el terminal móvil y un servidor, generalmente a través de Internet.

[0003] Por ejemplo, el documento WO2013/181682A1 describe un procedimiento para el control de un mecanismo de cierre por un usuario con un terminal móvil, estableciéndose por el terminal móvil, para el control del mecanismo de cierre, un enlace de datos local al mecanismo de cierre y realizándose, para la emisión de una clave para abrir el mecanismo de cierre con el terminal móvil, una conexión por Internet a un proveedor de identidad.

[0004] En el procedimiento conocido, el usuario se autentica al proveedor de identidad a través del terminal móvil, siendo enviada por el proveedor de identidad una información de autenticación al terminal móvil, que es enviada por el terminal móvil a una instancia de autorización en una red. Tras una verificación de la información de autenticación por la instancia de autorización se emite una clave con la que se abre el mecanismo de cierre. Para obtener la clave para abrir el mecanismo de cierre se establece un enlace con un proveedor de identidad existente. A continuación, la clave es transmitida por el terminal móvil al mecanismo de cierre a través de un enlace de datos local entre el terminal móvil y el mecanismo de cierre.

[0005] En este procedimiento conocido así, como en todos los procedimientos conocidos por el estado de la técnica, para el control que requiere autorizaciones referidas al usuario, de un aparato a través de un terminal móvil, la autorización necesaria para el control del aparato o los comandos de control acoplados a las autorizaciones necesarias se almacenan en el terminal móvil y se transmiten al aparato que ha de ser controlado. Esto, sin embargo, puede resultar desventajoso, porque por una parte, las autorizaciones o los comandos acoplados a las autorizaciones, para el control del aparato, están acoplados a un aparato móvil y, por otra parte, el almacenamiento local de las autorizaciones o de los comandos de control acoplados a las autorizaciones en un terminal móvil supone un riesgo de seguridad en caso de que el terminal móvil sea empleado por personas no autorizadas para el control del aparato.

[0006] El acoplamiento a un terminal móvil de las autorizaciones para el control del aparato o de los comandos para el control de un aparato, acoplados a dicha autorización, supone también una pérdida de confort: por esta concepción por ejemplo no es posible depositar una bicicleta en un depósito de bicicletas y prever que la bicicleta pueda ser utilizada por otra persona con otro terminal móvil tras abrir el mecanismo de cierre correspondiente.

[0007] En el documento US2011/0311052 se describe un procedimiento para aumentar la seguridad en un sistema inalámbrico para el control del acceso a un aparato que ha de ser controlado por medio de un aparato electrónico móvil, según el cual sus comandos de control codificados para el aparato que ha de ser controlado son transmitidos por un servidor de autenticación, a través del aparato electrónico móvil, al aparato que ha de ser controlado, y cuando ha transcurrido un intervalo de tiempo predefinido, los comandos de control se vuelven inutilizables. Los comandos de control recibidos por el aparato que ha de ser controlado no se verifican en cuanto a la autorización del usuario para utilizar los comandos de control.

[0008] Por lo tanto, la presente invención tiene el objetivo de proporcionar un procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato a través de un terminal móvil, mediante cuya realización se eviten las desventajas mencionadas, conocidas por el estado de la técnica. Además, el procedimiento debe poder realizarse también en caso de que sean posibles no sólo un comando de control, sino varios comandos de control.

[0009] Este objetivo se consigue mediante las características de la reivindicación 1. Más realizaciones ventajosas resultan de las reivindicaciones subordinadas.

[0010] Por tanto, se propone un procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato a través de un terminal móvil, por medio de un enlace de datos entre el terminal móvil y el aparato que ha de ser controlado, en el que los comandos de control, que requieren autorizaciones referidas al usuario, para el aparato que ha de ser controlado son generados mediante una interacción preferentemente basada en Internet entre el terminal móvil y un servidor de autenticación y/o de administración de aparatos y son transmitidos por el servidor de autenticación y/o de administración de aparatos, a través del terminal móvil, al aparato que ha de ser controlado, y en el que los comandos de control, que requieren autorizaciones referidas al usuario, para el aparato que ha de ser controlado no se almacenan en el terminal móvil.

[0011] Los comandos de control para el aparato que ha de ser controlado son recibidos por el terminal móvil y, a continuación, son transmitidos al aparato para el control del mismo. Una vez realizada la transmisión al aparato, se borran en caso de estar presentes aún en la memoria RAM del aparato.

[0012] Según la invención está previsto que los comandos de control transmitidos del terminal móvil al aparato que ha de ser controlado, no son verificados por el aparato que ha de ser controlado, en cuanto a la autorización del usuario para utilizar los comandos de control. De esta manera, el procedimiento se realiza rápidamente y se ahorran recursos de cálculo. Tras la recepción de un comando de control o, dado el caso, tras una descodificación o verificación de una signatura del mismo en caso de que el comando de control esté codificado o signado, este es ejecutado por el aparato que ha de ser controlado.

[0013] Según la invención, el enlace de datos local entre el terminal móvil y el aparato que ha de ser controlado se establece a través de un estándar Bluetooth-Low-Energy (BLE). Esto resulta por una parte en la ventaja de un bajo consumo de corriente a través de una batería convencional y, por otra parte, en la utilización de la característica “de difusión” de este estándar, por lo que el aparato que ha de ser controlado indica al terminal móvil que puede ser controlado por el mismo. La señal de difusión contiene de manera ventajosa una ID de aparato (ID de hardware) del aparato que ha de ser controlado, mediante la que el aparato puede ser identificado de forma unívoca. Alternativamente, para establecer un enlace de datos local entre el terminal móvil y el aparato que ha de ser controlado pueden usarse otros estándares conocidos por el estado de la técnica para la comunicación de datos inalámbrica o por cable, y cuando no está disponible ninguna señal de difusión, la ID de aparato del aparato que ha de ser controlado es consultada de forma activa por el terminal móvil.

[0014] El aparato que ha de ser controlado puede ser, por ejemplo, un dispositivo de cierre para una puerta, un depósito de bicicletas, una consigna automática, un armario, una cerradura de esquí o una taquilla, o bien, un dispositivo de control de acceso de personas, por ejemplo para estadios etc. Además, puede ser una máquina automática para dispensar productos predeterminados.

[0015] A continuación, la invención se describe en detalle a título de ejemplo con la ayuda de las figuras adjuntas. Muestran:

la figura 1 muestra un diagrama de bloques para la ilustración de componentes necesarios para la realización de una variante del procedimiento según la invención;

la figura 2 muestra un diagrama de secuencia para la ilustración de los pasos de procedimiento para el control de un aparato, en el que se puede generar un comando de control, al ejemplo de la apertura de un aparato realizado como mecanismo de cierre, para un diagrama de bloques según la figura 1; y

la figura 3 muestra un diagrama de secuencia para la ilustración de los pasos de procedimiento para el control de un aparato en el que pueden generarse varios comandos de control, para un diagrama de bloques según la figura 1.

[0016] En la figura 1, por 1 está designado el aparato que ha de ser controlado, estando designados por 2 un microcontrolador para el procesamiento de los comandos de control y por 3 un módulo BLE. El microcontrolador 2 y el módulo BLE son alimentados de energía por una batería estándar convencional. Además, puede estar previsto un sensor de proximidad, y cuando el sensor de proximidad se atenúa, el microcontrolador 2 y el módulo BLE 3 pasan de un modo de reposo a un modo activo.

[0017] En las figuras 1 y 2, por 8 está designado un usuario que maneja un terminal móvil 4 que puede estar realizado como smartphone, tablet, etc., pudiendo establecerse una ruta de comunicación BLE 10 entre el terminal móvil 4 y el microcontrolador 2 para el control del aparato 1 que ha de ser controlado a través del terminal móvil 4 y del módulo BLE 3.

[0018] El terminal móvil 4 puede comunicar, a través de una conexión de Internet 9, con el servidor de autenticación 5 en el que están creados datos de usuario y está implementado software para la autenticación del usuario. En el servidor de autenticación 5 no se almacenan autorizaciones de usuario. Además, el terminal móvil 4 puede comunicar, a través de una conexión de Internet 9, con un servidor de administración de aparatos 6 en el que están almacenadas informaciones relativas a los aparatos que han de ser controlados y están depositadas asignaciones entre uno o varios usuarios y un aparato que ha de ser controlado.

[0019] Por 7 está designado un módulo de codificación que recibe, verifica y signa comandos de control. El módulo de codificación puede estar integrado en el servidor de administración de aparatos 6. El servidor de autenticación 5 y el servidor de administración de aparatos 6 pueden estar reunidos en un servidor. Además, el servidor de autenticación 5 y el servidor de administración de aparatos 6 pueden estar interconectados para la comunicación de datos, a través de una conexión de red que puede estar realizada como conexión LAN 11. En función de los datos de transacción entre el usuario 8 y el servidor de administración de aparatos 6 está previsto un módulo de facturación B2C (“Business to Consumer” / Negocio a Consumidor) o B2B (“Business to Business” / Negocio a

Negocio) según el estado de la técnica.

[0020] Haciendo referencia a la figura 2, el usuario 8 inicia un software correspondiente en su terminal móvil 4 que puede estar implementado como llamada App (paso s1), y en el siguiente paso s2, por medio de un enlace entre el terminal móvil 4 y el servidor de autenticación 5 se realiza un registro o un alta del usuario 8, y una vez realizados el alta o el registro es enviada por el servidor de autenticación 5 una ID de sesión de usuario al terminal móvil 4 (paso s3).

[0021] En un siguiente paso s4.1, el usuario 8 selecciona a través del terminal móvil 4 un aparato 1 que ha de ser controlado, y mediante una interacción BLE entre el terminal móvil 4 y el módulo BLE 3 del aparato 1 que ha de ser controlado es enviada por el módulo BLE 3 al terminal móvil 4 una llamada señal de difusión que contiene la ID de hardware del aparato 1 que ha de ser controlado (paso s4.2).

[0022] En un siguiente paso s5 se establece un enlace entre el terminal móvil 4 y el servidor de administración de aparatos 6, durante el cual se consulta el estado del aparato 1 que ha de ser controlado, que puede ser identificado con la ayuda de su ID de hardware. Durante un siguiente paso de procedimiento s6, en el caso de que el CA 1 pueda ser controlado por el servidor de administración de aparatos 6 al terminal móvil 4, es enviada una señal que indica la aptitud para ser controlado del aparato 1 que ha de ser controlado a través del terminal móvil 4. Dado que en el aparato 1, realizado como mecanismo de cierre son posibles dos comandos de control, a saber, “Abrir” y “Cerrar”, y el servidor de administración de aparatos 6 conoce el estado del aparato 1, puede ejecutarse sólo un comando en cada momento, en el presente caso el comando “Abrir” para la apertura del mecanismo de cierre.

[0023] A continuación, se establece, a través del módulo BLE 3 y del microcontrolador 2, un enlace de datos BLE entre el terminal móvil 4 y el aparato 1 que ha de ser controlado (paso s7), y en un siguiente paso s8, estando cerrado el mecanismo de cierre, el microcontrolador 2 signa un paquete de datos (DataString) con una clave pública SK1 del servidor de administración de aparatos 6 y, en un siguiente paso s9, lo envía al terminal móvil 4.

[0024] El paquete de datos (DataString) signado se envía, junto a la ID de sesión de usuario y la ID de hardware del aparato 1 que ha de ser controlado, al servidor de administración de aparatos 6, solicitando el comando de control disponible, en el presente caso, un comando Abrir para el mecanismo de cierre 1 (s10).

[0025] En un siguiente paso s11, por el servidor de administración de aparatos 6 es verificada, mediante una interacción con el servidor de autenticación 5, la ID de sesión de usuario recibida en el paso s10, y en caso de una ID de sesión de usuario (s12) válida, por el módulo de codificación 7 se solicita un paquete de datos de respuesta (DataStringResponse) como reacción al paquete de datos (DataString) contenido (paso s13). El módulo de codificación 7 verifica el paquete de datos (DataString) signado por el microcontrolador 2 mediante una clave privada PK del servidor de administración de aparatos 6 (paso s14) y genera un paquete de datos de respuesta (DataStringResponse) (paso s15) que contiene el comando de control y que, junto al paquete de datos (DataString) contenido, es signado por el módulo de codificación 7 con una clave pública SK2 del microcontrolador 2 (paso s16). En el caso de que sea posible sólo un comando de control, el paquete de datos de respuesta puede estar vacío.

[0026] En un siguiente paso s17, el paquete de datos de respuesta (DataStringResponse) signado se transmite, junto al paquete de datos (DataString) signado contenido, al servidor de administración de aparatos 6, y a continuación, en el paso s18, el paquete de datos de respuesta (DataStringResponse) signado se conduce, junto al paquete de datos (DataString) signado contenido, al microcontrolador 2 a través de Internet, del terminal móvil 4 y del enlace de datos BLE entre el terminal móvil 4 y el microcontrolador 2, sin almacenarse en el terminal móvil 4.

[0027] El paquete de datos (DataString) contenido se reenvía, junto al paquete de datos de respuesta (DataStringResponse) al microcontrolador 2, para que el microcontrolador 2 pueda verificar que el comando de control contenido debe ser ejecutado por el aparato 1. Si el paquete de datos (DataString) no se corresponde con el paquete de datos generado originalmente y enviado al servidor de administración de aparatos 6, el comando de control no se ejecuta, ya que no puede ser asignado al aparato 1. Esto resulta ventajoso especialmente si son administrados varios aparatos por el servidor de administración de aparatos 6, ya que de esta manera se puede excluir que un aparato ejecute accidentalmente un comando de control que está destinado a otro aparato. El paquete de datos (DataString) puede ser, por ejemplo, un número biunívoco generado de forma aleatoria.

[0028] En un siguiente paso s19, el paquete de datos de respuesta (DataStringResponse) signado recibido y el paquete de datos (DataString) reenviado son verificados por el microcontrolador 2 con la ayuda de una clave privada PK2 y una vez realizada la verificación, se produce la reacción del microcontrolador 2, correspondiente al paquete de datos de respuesta (DataStringResponse) (paso s20), que envía el comando correspondiente al aparato 1 que ha de ser controlado (paso s21). En un último paso, una vez ejecutado el comando de control se envía al servidor de administración de aparatos 6, a través del enlace de datos BLE, del terminal móvil 4 y de Internet 9, una información de estado que se necesita para una nueva realización del procedimiento.

[0029] El procedimiento se ha descrito con la ayuda de sólo un comando de control generable posible, en el

presente caso con la ayuda de un comando de control Abrir para la apertura de un aparato 1 realizado como mecanismo de cierre. En el caso de un comando de control Cerrar se procede de manera correspondiente.

[0030] En función de la funcionalidad y del estado del aparato 1 que ha de ser controlado pueden generarse comandos de control adicionales, y en el caso de que sean posibles varios comandos de control, según la invención y haciendo referencia a la figura 3, después de los pasos s1 a s5 según la figura 2, en el paso s6 el usuario 8 recibe del servidor de administración de aparatos 6 a través del terminal móvil 4 una señal que indica la aptitud para ser controlado del aparato 1 que ha de ser controlado a través del terminal móvil 4 y adicionalmente los comandos de control posibles (Lista de comandos).

[0031] En este caso, a través del terminal móvil 4, el usuario 8 selecciona, de entre una pluralidad de comandos de control posibles, el comando de control deseado que ha de ser generado (paso adicional s4.3), siendo enviada esta información por el terminal móvil 4 en un paso adicional s5' al servidor de administración de aparatos 6 que en el paso adicional s6' confirma la selección. El comando de control seleccionado para el aparato 1 se almacena en el servidor de administración de aparatos 6 y se asigna a la ID de hardware del aparato 1 (paso s7').

[0032] Los demás pasos de procedimiento corresponden a los pasos de procedimiento según la figura 2 con la diferencia de que en el paso s13, por el módulo de codificación 7, se solicita un paquete de datos de respuesta (DataStringResponse) que corresponda, al o contenga, el comando de control seleccionado deseado. Un aparato 1 en el que pueden generarse varios comandos de control puede ser, por ejemplo, una máquina dispensadora de bebidas que ofrezca varias posibilidades de selección.

REIVINDICACIONES

1. Procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato (1) a través de un terminal móvil (4), por medio de un enlace de datos local a través de un estándar Bluetooth-Low-Energy (BLE) entre el terminal móvil (4) y el aparato (1) que ha de ser controlado, en el que los comandos de control, que requieren autorizaciones referidas al usuario, para el aparato (1) que ha de ser controlado son generados mediante una interacción entre el terminal móvil (4) y un servidor de autenticación (5) y/o un servidor de administración de aparatos (6) y son transmitidos por el servidor de autenticación y/o de administración de aparatos (5, 6), a través del terminal móvil (4), al aparato (1) que ha de ser controlado, y en el que los comandos de control recibidos por el aparato (1) que ha de ser controlado no son verificados en cuanto a la autorización del usuario (8) para utilizar los comandos de control, **caracterizado por que** los comandos de control, que requieren autorizaciones referidas al usuario, para el aparato (1) que ha de ser controlado son recibidos por el terminal móvil (4) y, a continuación, son transmitidos al aparato (1) que ha de ser controlado para el control del mismo y no se almacenan en el terminal móvil (4), y si puede generarse sólo un comando de control posible, el procedimiento comprende los siguientes pasos:

- el inicio (s1) por parte del usuario (8) de un software en el terminal móvil (4);
- la realización (s2) de un registro o un alta del usuario (8) por medio de un enlace entre el terminal móvil (4) y el servidor de autenticación (5), y tras la realización (s3) del alta o del registro es enviada por el servidor de autenticación (5) una ID de sesión de usuario al terminal móvil (4);
- la selección (s4.1) de un aparato (1) que ha de ser controlado por el usuario (8) a través del terminal móvil (4), siendo enviada por un módulo BLE (3) al terminal móvil (4), mediante una interacción BLE entre el terminal móvil (4) y el módulo BLE (3) del aparato (1) que ha de ser controlado, una señal de difusión que contiene la ID de hardware del aparato (1) que ha de ser controlado (s4.2);
- el establecimiento (s5) de un enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6), durante el cual se consulta el estado del aparato (1) que ha de ser controlado que puede ser identificado con la ayuda de su ID de hardware, y el envío (s6), del servidor de administración de aparatos (6) al terminal móvil (4), de una señal que indica la aptitud para ser controlado del aparato (1) que ha de ser controlado a través del terminal móvil (4);
- el establecimiento (s7) de un enlace de datos BLE entre el terminal móvil (4) y el aparato (1) que ha de ser controlado través del módulo BLE (3) y de un microcontrolador (2) del aparato (1) que ha de ser controlado, y en un siguiente paso (s8), el microcontrolador (2) signa un paquete de datos (DataString) con una clave pública del servidor de administración de aparatos (6) y lo envía (s9) al terminal móvil (4);
- el envío (s10) al servidor de administración de aparatos (6) del paquete de datos (DataString) signado, junto a la ID de sesión de usuario y la ID de hardware del aparato (1) que ha de ser controlado, solicitando el comando de control;
- la verificación (s11, s12) de la ID de sesión de usuario por el servidor de administración de aparatos (6) mediante una interacción con el servidor de autenticación (5), y en caso de una ID de sesión de usuario (s13) válida, la solicitud (s13) de un paquete de datos de respuesta (DataStringResponse) por un módulo de codificación (7);
- la verificación (s14) por el módulo de codificación (7) del paquete de datos (DataString) signado por el microcontrolador (2) mediante una clave privada del servidor de administración de aparatos (6) y la generación (s15) de un paquete de datos de respuesta (DataStringResponse) que contiene el comando de control y que, junto al paquete de datos (DataString) contenido, es signado (s16) por el módulo de codificación (7) con una clave pública del microcontrolador (2);
- la transmisión (s17) al servidor de administración de aparatos (6) del paquete de datos de respuesta (DataStringResponse) signado se transmite, junto al paquete de datos (DataString) signado contenido, y a continuación, en el paso (s18), el paquete de datos de respuesta (DataStringResponse) signado se conduce, junto al paquete de datos (DataString) signado contenido, al microcontrolador (2) a través de un enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6), el terminal móvil (4) y el enlace de datos BLE entre el terminal móvil (4) y el microcontrolador (2), sin almacenarse en el terminal móvil (4);
- la verificación (s19, s20) por el microcontrolador (2) del paquete de datos de respuesta (DataStringResponse) signado recibido y del paquete de datos (DataString) reenviado, con la ayuda de una clave privada y, una vez realizada la verificación, el envío (s21) del comando de ejecución al aparato (1) que ha de ser controlado; y
- la ejecución del comando de control y el envío (s22) al servidor de administración de aparatos (6) de una información de estado sobre el enlace de datos BLE entre el terminal móvil (4) y el aparato (1) que ha de ser controlado, a través del módulo BLE (3), el terminal móvil (4) y un enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6), y si se pueden generar varios comandos de control, el procedimiento comprende los siguientes pasos:
- el inicio (s1) por parte del usuario (8) de un software en el terminal móvil (4);
- la realización (s2) de un registro o un alta del usuario (8) por medio de un enlace entre el terminal móvil (4) y el servidor de autenticación (5), y tras la realización (s3) del alta o del registro es enviada por el servidor de autenticación (5) al terminal móvil (4) una ID de sesión de usuario;
- la selección (s4.1) de un aparato (1) que ha de ser controlado, por el usuario (8) a través del terminal móvil (4), y mediante una interacción BLE entre el terminal móvil (4) y un módulo BLE (3) del aparato (1) que ha de ser controlado es enviada (s4.2) por el módulo BLE (3) al terminal móvil (4) una señal de difusión que contiene la ID

de hardware del aparato (1) que ha de ser controlado ;

- el establecimiento (s5) de un enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6), siendo consultado el estado del aparato (1) que ha de ser controlado, que puede identificarse con la ayuda de la ID de hardware, y el envío (s6) por el servidor de administración de aparatos (6) al terminal móvil (4) de una señal que indica la aptitud para ser controlado del aparato (1) que ha de ser controlado a través del terminal móvil (4), y adicionalmente los comandos de control posibles (lista de comandos),
- la selección (s4.3) por parte del usuario (8) del comando de control deseado que ha de ser generado, de entre una pluralidad de comandos de control posibles, a través del terminal móvil (4), siendo enviada (s5') esta información por el terminal móvil (4) al servidor de administración de aparatos (6) que en un paso siguiente (s6') confirma la selección;
- el almacenamiento (s7') del comando de control seleccionado en el servidor de administración de aparatos (6) y la asignación del comando de control seleccionado a la ID de hardware del aparato 1;
- el establecimiento (s7) de un enlace de datos BLE entre el terminal móvil (4) y el aparato (1) que ha de ser controlado través del módulo BLE (3) y de un microcontrolador (2) del aparato (1) que ha de ser controlado, y en un siguiente paso (s8), el microcontrolador (2) signa un paquete de datos (DataString) con una clave pública del servidor de administración de aparatos (6) y lo envía (s9) al terminal móvil (4);
- el envío (s10) al servidor de administración de aparatos (6) del paquete de datos (DataString) signado, junto a la ID de sesión de usuario y la ID de hardware del aparato (1) que ha de ser controlado, solicitando el comando de control;
- la verificación (s11, s12) de la ID de sesión de usuario por el servidor de administración de aparatos (6) mediante una interacción con el servidor de autenticación (5), y en caso de una ID de sesión de usuario (s12) válida, la solicitud (s13) de un paquete de datos de respuesta (DataStringResponse) por el módulo de codificación (7), conteniendo o correspondiendo dicho paquete de datos de respuesta (DataStringResponse) al comando de control seleccionado deseado;
- la verificación (s14) por el módulo de codificación (7) del paquete de datos (DataString) signado por el microcontrolador (2) mediante una clave privada del servidor de administración de aparatos (6) y la generación (s15) de un paquete de datos de respuesta (DataStringResponse) que contiene el comando de control y que, junto al paquete de datos (DataString) contenido, es signado (s16) por el módulo de codificación (7) con una clave pública del microcontrolador (2);
- la transmisión (s17) al servidor de administración de aparatos (6) del paquete de datos de respuesta (DataStringResponse) signado se transmite, junto al paquete de datos (DataString) signado contenido, y a continuación, en el paso (s18), el paquete de datos de respuesta (DataStringResponse) signado se conduce, junto al paquete de datos (DataString) signado contenido, al microcontrolador (2) a través de un enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6), el terminal móvil (4) y el enlace de datos BLE entre el terminal móvil (4) y el microcontrolador (2), sin almacenarse en el terminal móvil (4);
- la verificación (s19, s20) por el microcontrolador (2) del paquete de datos de respuesta (DataStringResponse) signado recibido y del paquete de datos (DataString) reenviado, con la ayuda de una clave privada y, una vez realizada la verificación, el envío (s21) del comando de ejecución al aparato (1) que ha de ser controlado; y
- la ejecución del comando de control y el envío (s22) al servidor de administración de aparatos (6) de una información de estado sobre el enlace de datos BLE entre el terminal móvil (4) y el aparato (1) que ha de ser controlado, a través del módulo BLE (3), el terminal móvil (4) y un enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6).

2. Procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato (1) a través de un terminal móvil (4), por medio de un enlace de datos local entre el terminal móvil (4) y el aparato (1) que ha de ser controlado, según la reivindicación 1, **caracterizado por que** el enlace entre el terminal móvil (4) y el servidor de administración de aparatos (6) es un enlace basado en Internet.

3. Procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato (1) a través de un terminal móvil (4), por medio de un enlace de datos local entre el terminal móvil (4) y el aparato (1) que ha de ser controlado, según la reivindicación 1 o 2, **caracterizado por que** el aparato (1) que ha de ser controlado es un dispositivo de cierre para una puerta, un depósito de bicicletas, una consigna automática, un armario, una cerradura de esquí o una taquilla, o bien, un dispositivo de control de acceso de personas o una máquina automática para dispensar productos predeterminados.

4. Procedimiento para el control, que requiere autorizaciones referidas al usuario, de un aparato (1) a través de un terminal móvil (4), por medio de un enlace de datos local entre el terminal móvil (4) y el aparato (1) que ha de ser controlado, según las reivindicaciones 1, 2 o 3, **caracterizado por que** en lugar de un enlace de datos local, establecido a través de un estándar Bluetooth-Low-Energy (BLE), entre el terminal móvil (4) y el aparato (1) que ha de ser controlado se usa otro estándar para la comunicación de datos inalámbrica o por cable, y cuando no está disponible ninguna señal de difusión, la ID de hardware del aparato (1) que ha de ser controlado es consultada de forma activa por el terminal móvil (4).

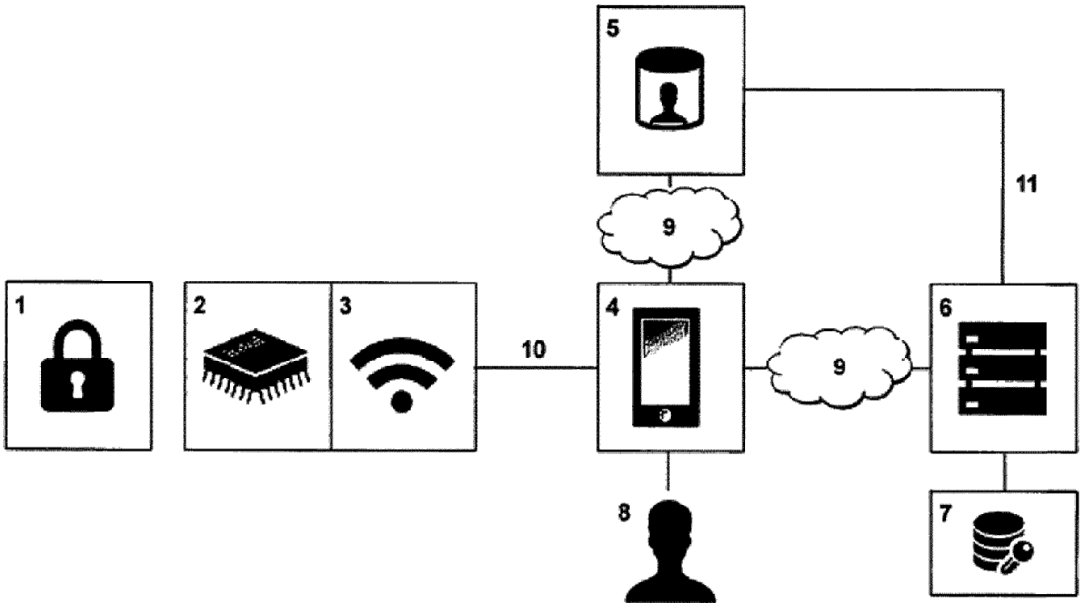

FIG. 1

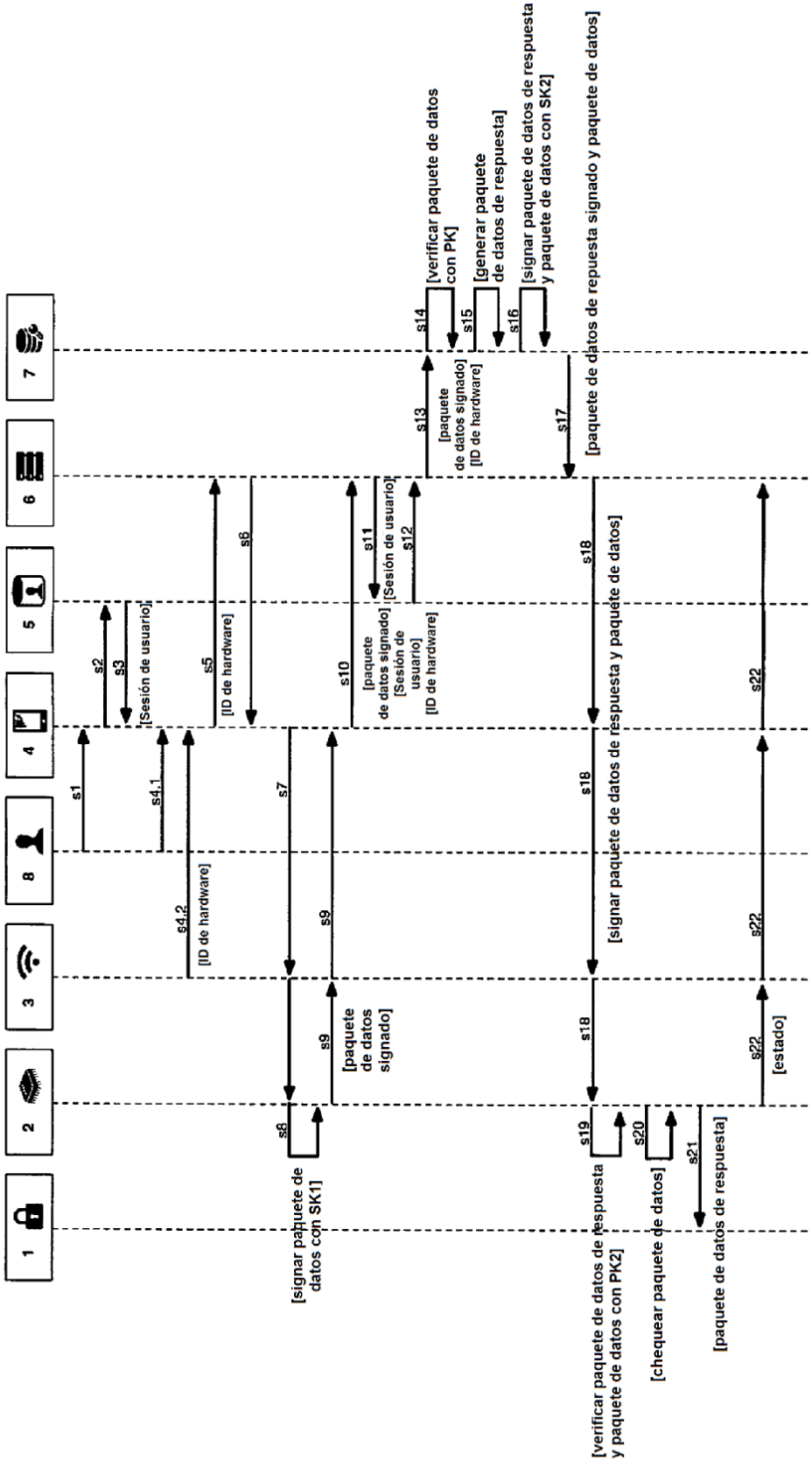
1
2
3
8
4
5
6
7
s1
s2
s3
[Sesión de usuario]
s4.1
s4.2
[ID de hardware]
s5
[ID de hardware]
s6
s7
s8
[signar paquete de datos con SK1]
s9
[paquete de datos signado]
s9
s10
[paquete de datos signado] [Sesión de usuario] [ID de hardware]
s11
[Sesión de usuario]
s12
s13
[paquete de datos signado] [ID de hardware]
s14
[verificar paquete de datos con PK]
s15
[generar paquete de datos de respuesta]
s16
[signar paquete de datos de respuesta y paquete de datos con SK2]
s17
[paquete de datos de repuesta signado y paquete de datos]
s18
[signar paquete de datos de respuesta y paquete de datos]
s18
s18
s19
[verificar paquete de datos de respuesta y paquete de datos con PK2]
s20
[chequear paquete de datos]
s21
[paquete de datos de respuesta]
s22
s22
s22
[estado]

FIG. 2

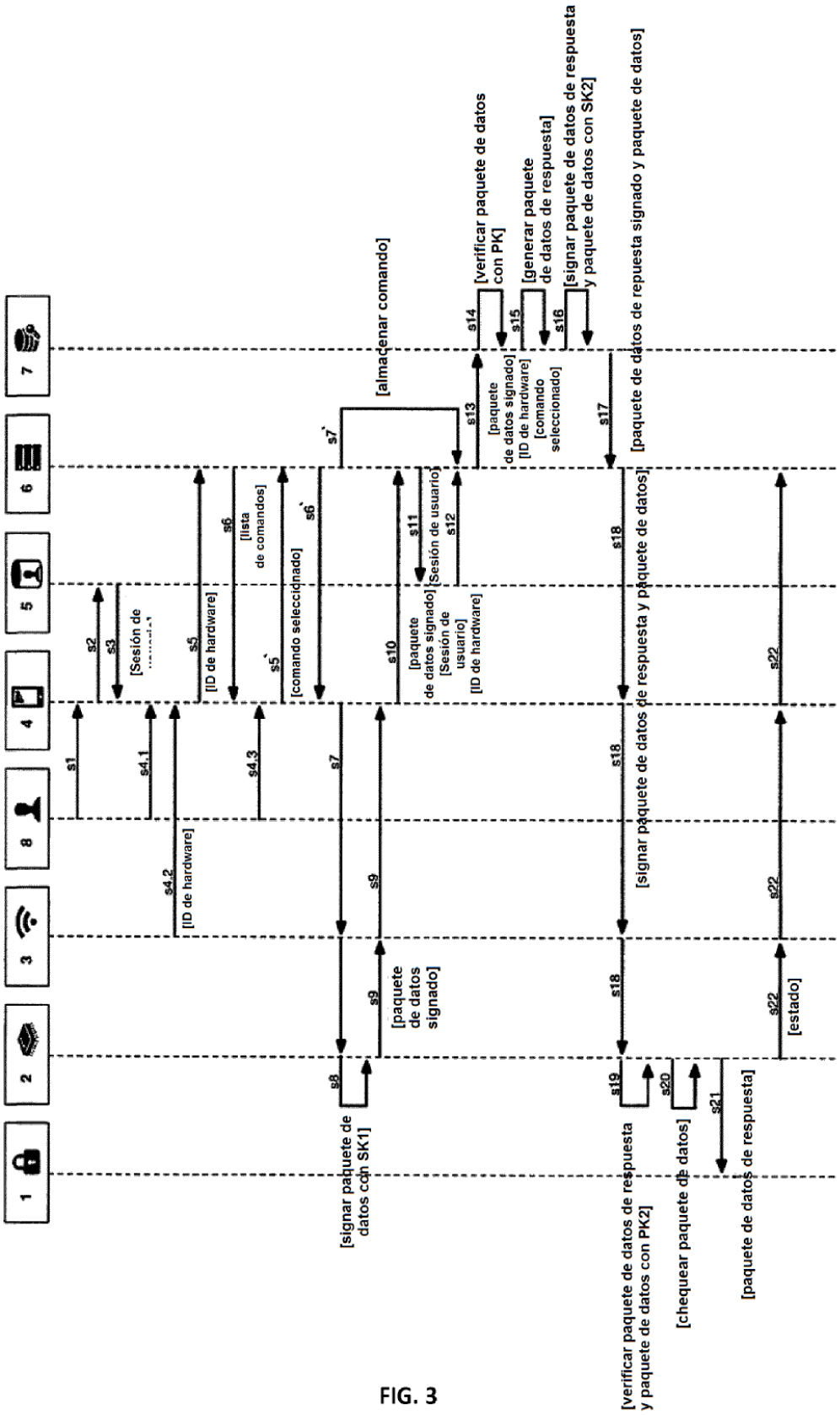
1
2
3
8
4
5
6
7
s1
s2
s3
[Sesión de
s4.1
s4.2
[ID de hardware]
s4.3
s5
[ID de hardware]
s6
[lista
de comandos]
s5`
[comando seleccionado]
s6`
s7
s7`
[almacenar comando]
s8
[signar paquete de
datos con SK1]
s9
[paquete
de datos
signado]
s9
s10
[paquete
de datos signado]
[Sesión de
usuario]
[ID de hardware]
s11
[Sesión de usuario]
s12
s13
[paquete
de datos signado]
[ID de hardware]
[comando
seleccionado]
s14
[verificar paquete de datos
con PK]
s15
[generar paquete
de datos de respuesta]
s16
[signar paquete de datos de respuesta
y paquete de datos con SK2]
s17
[paquete de datos de repuesta signado y paquete de datos]
s18
[signar paquete de datos de respuesta y paquete de datos]
s18
s18
s19
[verificar paquete de datos de respuesta
y paquete de datos con PK2]
s20
[chequear paquete de datos]
s21
[paquete de datos de respuesta]
s22
s22
[estado]
s22

FIG. 3