(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 534**

(51) Int. CI.:

H04L 12/46 (2006.01)
H04L 9/06 (2006.01)
H04W 12/02 (2009.01)
H04W 12/04 (2009.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)
H04W 4/02 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.04.2017 PCT/IB2017/052354**

(87) Fecha y número de publicación internacional: **02.11.2017 WO17187326**

(96) Fecha de presentación y número de la solicitud europea: **25.04.2017 E 17720888 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.06.2019 EP 3406067**

(54) Título: **Dispositivo electrónico para generar una señal de control de manera protegida, y procedimiento para generar dicha señal de control usando el dispositivo electrónico**

(30) Prioridad:

28.04.2016 EP 16167493

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.02.2020

(73) Titular/es:

ACCEDY SAGL (100.0%)
Via Serafino Balestra 33
6900 Lugano, CH

(72) Inventor/es:

COVAIN, SERGE

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Dispositivo electrónico para generar una señal de control de manera protegida, y procedimiento para generar dicha señal de control usando el dispositivo electrónico.

Campo

La presente exposición se refiere a un dispositivo electrónico configurado para generar una señal de control para controlar otro dispositivo de una manera protegida cuando se envía y recibe una señal de orden desde un dispositivo móvil. La presente exposición trata, además, sobre un procedimiento para generar la señal de control de manera protegida de acuerdo con la señal de orden usando el dispositivo electrónico.

Descripción de la técnica anterior

Durante los últimos años, la noción de los objetos inteligentes conectados, tales como sensores y accionadores, ha abierto la puerta a un sinfín de aplicaciones, tales como redes eléctricas inteligentes, vehículos conectados, ciudades inteligentes o atención sanitaria inteligente, por mencionar algunos. Con ese fin, se han propuesto varias "arquitecturas", que consisten, en general, o bien en conectar estos dispositivos a través de pasarelas multiprotocolo o bien en usar el Protocolo de Internet (IP) (por ejemplo, IPv6) de extremo-a-extremo, además de varias opciones mixtas.

No obstante, normalmente las comunicaciones que se usan para intercomunicarse con dicho objeto conectado no son excesivamente seguras, lo cual hace que aumente el riesgo de que un usuario no autorizado pueda tomar el control del objeto.

El documento US2016036594 divulga un sistema para la gestión inalámbrica de claves con vistas a su autenticación. La autenticación incluye transmitir una solicitud a un dispositivo de bloqueo, transmitir un desafío de seguridad al dispositivo móvil, y transmitir una respuesta al desafío y un perfil de usuario cifrado para el dispositivo de bloqueo. La respuesta incluye datos generados con una clave de acceso que es almacenada tanto por el dispositivo móvil como por el dispositivo de bloqueo. No obstante, el perfil de usuario se cifra por medio de un servidor usando una clave secreta que es almacenada por el servidor.

El producto Okidokeys fabricado por Openways permite el control de la cerradura de una puerta usando un dispositivo móvil, tal como un teléfono inteligente. La señal enviada por el teléfono inteligente para controlar la cerradura se cifra usando un cifrado AES de 256 bits. No obstante, la clave usada para el cifrado se almacena en un servidor remoto.

Por lo tanto, estas soluciones son subsidiarias de la seguridad ofrecida por el proveedor del servidor. Por otra parte, las soluciones anteriores proporcionan un grado bajo de seguridad debido a las posibilidades de interceptación, por ejemplo mediante un ataque del tipo hombre en el medio, de reproducción y de utilización de la clave entre el momento de emisión de la misma y el momento de su utilización.

El documento US2008271123 describe un sistema y un procedimiento domóticos para controlar por lo menos un dispositivo de una pluralidad de dispositivos en una red domótica. El sistema domótico incluye un receptor configurado para recibir una señal indicativa de la ubicación de un usuario. El usuario está situado más allá de las proximidades del hogar que está siendo automatizado por la red domótica. El sistema domótico incluye, también, un procesador adaptado para controlar el por lo menos un dispositivo de la pluralidad de dispositivos como respuesta a la señal indicativa recibida.

El documento WO15157720 se refiere a mecanismos para proteger un sistema de comunicaciones usando rellenos de un solo uso (*one-time pads*). Se pueden generar e intercambiar rellenos de un solo uso en persona usando mecanismos basados en proximidad que incluyen mecanismos de comunicación óptica en dispositivos móviles. En ejemplos particulares, un código de respuesta rápida en el dispositivo móvil de una de las partes es explorado por el dispositivo móvil de la otra parte para intercambiar de manera segura una clave simétrica generada aleatoriamente. La clave simétrica se usa para cifrar un relleno de un solo uso generado aleatoriamente, transmitido desde el dispositivo móvil de una de las partes al dispositivo móvil de la otra parte. El relleno de un solo uso se puede compartir de manera cifrada usando mecanismos basados en proximidad que incluyen Bluetooth, WiFi, etcétera.

Sumario

De acuerdo con un primer aspecto de la invención, se proporciona un dispositivo electrónico según la reivindicación 1. De acuerdo con un segundo aspecto de la invención, se proporciona un procedimiento según la reivindicación 6. En la descripción siguiente, los dibujos y las reivindicaciones dependientes se exponen otros aspectos de la invención.

Breve descripción de los dibujos

La invención se entenderá mejor con la ayuda de la descripción de una forma de realización que se ofrece a título de ejemplo y se ilustra con las figuras, en las cuales:

la figura 1 representa un dispositivo electrónico según una forma de realización;

la figura 2 muestra el dispositivo electrónico, según otra forma de realización; y

la figura 3 ilustra una pluralidad de los dispositivos electrónicos usados como dispositivo de mensajería privada, de acuerdo con una forma de realización.

Descripción detallada de posibles formas de realización

La figura 1 representa esquemáticamente un dispositivo electrónico 1, de acuerdo con una forma de realización. El dispositivo electrónico 1 está configurado para generar una señal de control para controlar otro dispositivo de una manera protegida cuando se recibe una señal de orden desde un móvil. El dispositivo electrónico 1 comprende un enlace de comunicaciones de corto alcance 2 configurado para establecer una comunicación de corto alcance entre el dispositivo electrónico 1 y un dispositivo móvil 3 dentro de un área de corto alcance 7. El dispositivo electrónico 1 comprende, además, un enlace de comunicaciones de largo alcance 4 configurado para establecer una comunicación de largo alcance entre el dispositivo electrónico 1 y el primer dispositivo móvil cuando el dispositivo móvil 3 es remoto, es decir, cuando el dispositivo móvil 3 está fuera del área de corto alcance 7.

En la presente exposición, la expresión “enlace de comunicaciones de corto alcance” significa un enlace de comunicaciones que se establece dentro de un área de corto alcance 7, tal como una vivienda, una escuela, un laboratorio o un edifico de oficinas. Un ejemplo de enlace de comunicaciones de corto alcance del tipo mencionado es una red de área local (LAN), preferentemente basada en tecnologías inalámbricas (WLAN). El enlace de comunicaciones de corto alcance 2 no requiere un punto de acceso inalámbrico. El término “remoto” significa que el dispositivo móvil 3 está fuera del área de cobertura 7 y que no podría comunicarse a través del enlace de comunicaciones de corto alcance 2 sino, solamente, a través del enlace de comunicaciones de largo alcance 4. La expresión “enlace de comunicaciones de largo alcance” significa que se establece un enlace de comunicaciones entre el dispositivo electrónico 1 y el dispositivo móvil 3, fuera del alcance del área de corto alcance 7. Puede que el enlace de comunicaciones de largo alcance 4 necesite un punto de acceso de tal manera que se pueda establecer una comunicación entre el dispositivo electrónico 1 y el dispositivo móvil remoto 3. Un ejemplo de enlace de comunicaciones de largo alcance del tipo mencionado es una red de área extensa (WAN), tal como Internet.

En la figura 1, el área de corto alcance se representa con la línea de trazos 7. El enlace de comunicaciones de corto alcance 2 está configurado para establecer una comunicación con el dispositivo móvil 3 dentro del área de corto alcance 7. El enlace de comunicaciones de corto alcance 2 puede comprender cualquier tecnología basada en redes de área local inalámbricas. La comunicación a través del enlace de comunicaciones de corto alcance se puede proteger por cifrado, tal como un cifrado asimétrico.

En una forma de realización, el dispositivo electrónico 1 está configurado para generar una señal de control para controlar un objeto que va a ser controlado. Por ejemplo, el dispositivo electrónico 1 se puede usar para dispositivos llevables inteligentes, hogares inteligentes, ciudades inteligentes, entornos inteligentes y empresas inteligentes. El dispositivo electrónico 1 se puede usar para captar y/o controlar objetos que están dentro del área de corto alcance 7, aunque también objetos remotos (fuera del área de corto alcance 7). Los objetos remotos se pueden captar y/o controlar usando el enlace de comunicaciones de corto alcance 4, por ejemplo a través de una infraestructura de red existente.

Los ejemplos de captación y control/accionamiento de objetos pueden incluir aplicaciones que hacen frente a la gestión de la calefacción, la electricidad y la energía, características de seguridad doméstica y domótica, control de dispositivos eléctricos instalados en una casa, y medición y control de la temperatura del agua de tal manera que el agua esté caliente en cuanto alguien se levante por la mañana con vistas a tomar una ducha. Otros ejemplos incluyen la gestión de equipos de fabricación, la gestión de activos y situaciones, o sistemas de control de procesos de fabricación, de monitorización sanitaria remota y de notificación de emergencias.

En una forma de realización, el dispositivo electrónico 1 está configurado para funcionar como un dispositivo inteligente de control doméstico, de tal manera que la señal de control está dispuesta para controlar un dispositivo relacionado con la casa. En el ejemplo de la figura 1, el dispositivo electrónico 1 se muestra en comunicación con un horno 11 y un sistema de iluminación 12. No obstante, el dispositivo electrónico 1 se puede usar para controlar cualquier tipo de dispositivo doméstico, tal como un dispositivo de calefacción, un sistema de ventilación, el aire acondicionado (HVAC), la cerradura de una puerta, un TV, una nevera, una lavadora, una secadora, y similares, un sistema de alarma contra incendios, un contador (por ejemplo, un contador eléctrico, un contador del suministro de gas y similares), un sistema de energía solar, un sistema de aspersores, un termostato, o un sistema de seguridad, etcétera.

El dispositivo móvil 3 puede ser cualquier dispositivo móvil adecuado, incluyendo un teléfono inteligente, un dispositivo informático de tipo tableta, un dispositivo ponible (por ejemplo, gafas inteligentes o un reloj inteligente), etc.

La señal de control para controlar el objeto que va a ser controlado se puede enviar a través de cualesquiera medios de comunicación por cable o inalámbricos 10 adecuados. Estos pueden incluir el mismo enlace de comunicaciones de corto alcance 2 u otros medios de comunicación de corto alcance.

El enlace de comunicaciones de corto alcance 2 y/o los medios de comunicación 10, cuando se usan dentro del área de corto alcance 7, pueden incluir un dispositivo de comunicaciones por ondas de radio u ópticas, en especial usando la comunicación de RFID y de campo cercano, el protocolo de transmisión Bluetooth®, el Bluetooth de Baja Energía (BLE), un protocolo de comunicaciones de campo cercano (NFC), una tarjeta de proximidad o una conexión directa WiFi, Zigbee, una comunicación por líneas eléctricas, transmisión infrarroja (IR), comunicación por ultrasonidos, un protocolo *Z-wave* o cualquier otro protocolo de comunicación domótica.

El enlace de comunicaciones de largo alcance 4 y/o los medios de comunicación 10, cuando se usan fuera del área de corto alcance 7, pueden comprender cualquier forma adecuada de telecomunicación por cable o inalámbrica, incluyendo redes, radiocomunicación, transmisión por microondas, fibra óptica y satélites de comunicaciones. El enlace de comunicaciones de largo alcance 4 puede comprender una red telefónica o una red informática que use el Protocolo de Internet.

Alternativamente, el enlace de comunicaciones de corto alcance 2 puede comprender una conexión por cable 9 entre el dispositivo electrónico 1 y el dispositivo móvil 3, tal como una conexión a través de un conector USB o cualquier otro conector apropiado.

El dispositivo electrónico 1 comprende, además, una unidad de procesado 6 configurada para generar y almacenar por lo menos un conjunto de claves que comprenden una pluralidad de claves de cifrado. El conjunto de claves se puede transmitir al dispositivo móvil 3 a través del enlace de comunicaciones de corto alcance 2 cuando el dispositivo móvil 3 está dentro del área de corto alcance 7.

Cuando el dispositivo móvil 3 está fuera del área de corto alcance 7, es decir, cuando el dispositivo móvil 3 es remoto con respecto al dispositivo electrónico 1, el enlace de comunicaciones de largo alcance 4 está configurado, además, para recibir una señal de orden enviada por el dispositivo móvil 3. La señal de orden se puede cifrar con una clave del conjunto de claves, usándose solo una vez cada clave del conjunto de claves.

El conjunto de claves puede comprender un número cualquiera de claves. Por ejemplo, el conjunto de claves puede comprender 10’000 contraseñas aleatorias generadas aleatoriamente.

La señal de orden cifrada se puede descifrar cuando se recibe en el dispositivo electrónico 1, por ejemplo en la unidad de procesado 6. A continuación, el dispositivo electrónico 1 genera una señal de control de acuerdo con la señal de orden recibida. Por ejemplo, la señal de orden puede estar destinada a controlar un dispositivo, y la señal de control generada está configurada para controlar el dispositivo de acuerdo con uno o más de diferentes protocolos, en función del dispositivo respectivo que va a ser controlado. El dispositivo controlado puede incluir un horno 11 o un sistema de iluminación 12. El dispositivo controlado puede incluir, además, un horno, una lavadora, una secadora, un sistema de alarma contra incendios, un contador eléctrico, un contador de gas, un sistema de aspersores, un termostato, etc.

De acuerdo con una forma de realización, un procedimiento para generar una señal de control para controlar otro dispositivo de una manera protegida en función de una señal de orden recibida desde un dispositivo móvil 3, comprende:

establecer un enlace de comunicaciones de corto alcance 2 entre el dispositivo electrónico 1 y el dispositivo móvil 3 cuando el dispositivo móvil 3 está dentro del área de corto alcance 7;

generar y almacenar el conjunto de claves en la unidad de procesado 6

transmitir el conjunto de claves al dispositivo móvil 3 por medio del enlace de comunicaciones de corto alcance 2;

recibir la señal de orden cifrada con una de las claves transferidas al dispositivo móvil y descifrar la señal de orden con la mencionada de las claves almacenadas en el dispositivo de procesado 6; y

generar la señal de control en función de la señal de orden.

El mismo conjunto de claves se almacena en la unidad de procesado 6 del dispositivo electrónico 1 y en el

dispositivo móvil 3, y la misma clave, seleccionada de entre el conjunto de claves, se usa para cifrar la señal de orden enviada por el dispositivo móvil 3 y para descifrar la señal de orden cifrada recibida por el dispositivo electrónico 1.

El procedimiento comprende, además, la etapa de destruir la clave usada para cifrar y descifrar la señal de orden.

De este modo, cuando una señal de orden adicional es enviada por el dispositivo móvil remoto 3 y recibida por el dispositivo electrónico 1, se usa otra clave de entre el conjunto de claves para cifrar y descifrar esta señal de orden adicional. Cada clave del conjunto de claves puede ser diferente con respecto a las otras, de tal manera que cada señal de orden recibida por el dispositivo electrónico 1 desde el dispositivo móvil remoto 3 se cifrará con una clave diferente. Cada clave usada para cifrar y descifrar cada información recibida se destruye después de la etapa de descifrado.

El conjunto de claves se almacena solamente en el dispositivo electrónico 1 y en el dispositivo móvil 3. Las claves usadas para cifrar y descifrar la información no son accesibles en un servidor o en la nube, y, por lo tanto, para un posible pirata informático.

El conjunto de claves se puede renovar cada vez que el dispositivo móvil 3 está dentro del área de corto alcance 7. El conjunto de claves se puede renovar automáticamente cuando el dispositivo móvil 3 está dentro del área de corto alcance 7. Con ese fin, pueden usarse medios de detección para detectar la presencia del dispositivo móvil 3 en el área de corto alcance 7.

De este modo, se transmite un conjunto nuevo de claves al dispositivo móvil 3 cada vez que el dispositivo móvil 3 está dentro del área de corto alcance 7 (en el hogar, la escuela, el laboratorio, el edificio de oficinas, etc., o conectado por cable al dispositivo electrónico 1 por ejemplo a través de un conector USB). Cada conjunto nuevo de claves comprende una pluralidad de claves que son diferentes con respecto a las claves comprendidas en el otro conjunto generado de claves.

Las claves pueden ser códigos o contraseñas generados de una manera aleatoria. La generación de claves puede usar un algoritmo de claves simétricas, tal como la norma de cifrado avanzado (AES 256) o cualquier otro algoritmo apropiado de claves simétricas. La generación de claves también puede usar un algoritmo de claves asimétricas, tal como el sistema asimétrico de clave pública-privada RSA o cualquier otro algoritmo apropiado de claves asimétricas.

En una forma de realización, las claves se generan usando un algoritmo de contraseña de un solo uso basada en el tiempo (TOTP), por ejemplo usando la norma RFC 6238. Una clave generada por TOPT combina una clave secreta (conjunto de claves) con un sello de tiempo actual usando una función *hash* criptográfica para generar una contraseña de un solo uso. Típicamente, el sello de tiempo se puede incrementar en intervalos de 30 segundos, por lo que las contraseñas generadas temporalmente cerca entre sí a partir de la misma clave secreta serán iguales. Cuando se usa un conjunto de claves generado por TOTP, el dispositivo electrónico 1 y el dispositivo móvil 3 necesitarán usar el mismo algoritmo al mismo tiempo para calcular la contraseña.

El conjunto de claves generado por TOTP es seguro contra un ataque del tipo “hombre en el medio”. De hecho, en el caso de que la señal de orden enviada por el dispositivo móvil 3 sea interceptada por un ataque de tipo hombre en el medio, el dispositivo electrónico 1 no recibirá nunca la señal de orden y, por lo tanto, no generará una señal de control. El ataque de tipo hombre en el medio puede enviar la señal de orden interceptada en un momento posterior de tal manera que el dispositivo electrónico 1 generará la señal de control en ese momento retardado. Por ejemplo, si la señal de orden está destinada al dispositivo electrónico 1 para que genere una señal de control con vistas a abrir una puerta de casa, el ataque de hombre en el medio puede usar la señal de orden interceptada para abrir la puerta en un instante de tiempo retardado adecuado (cuando no haya nadie más en casa). No obstante, cuando se usa el conjunto de claves generado por TOTP, el dispositivo electrónico 1 no podrá generar ninguna señal de control puesto que, en el instante de tiempo retardado, se habrá producido la expiración de la contraseña, a no ser que la señal de orden interceptada se envíe antes de un tiempo de retardo breve cuando la persona a la que iba destinada la señal de orden de apertura de la puerta esté todavía de pie delante de esta última.

La contraseña puede ser válida durante un periodo de tiempo limitado que se puede fijar a menos de una hora, menos de 30 minutos, menos de 5 minutos o menos de 30 segundos, un periodo de tiempo variable o cualquier periodo de tiempo adecuado.

En otra forma de realización, la señal de orden enviada por el dispositivo móvil remoto 3 y recibida por el dispositivo electrónico 1 se divide en una pluralidad de partes de señal de orden. Cada parte de señal de orden se cifra usando una de las claves.

En una forma de realización, el enlace de comunicaciones de largo alcance 4 se materializa a través de uno o una pluralidad de servidores remotos por medio de un protocolo de Internet (véase la figura 1). En una variante

preferida, el enlace de comunicaciones de largo alcance 4 se materializa usando un protocolo extensible de mensajería y presencia (XMPP). No obstante, también podría usarse otro protocolo, tal como el protocolo comunicación web en tiempo real (WebRTC).

En una forma de realización, la señal de orden comprende una pluralidad de partes de señal de orden, enviándose cada parte de señal de orden por separado a través del enlace de comunicaciones de largo alcance 4 y recibiéndose por separado en el dispositivo electrónico 1. Cada parte de señal de orden se puede cifrar usando una de las claves del conjunto de claves.

Cada parte de señal de orden puede ser enviada por (y, por lo tanto, recibida desde) un servidor diferente. En ese caso, cada parte de señal de orden puede tener un código de identificación diferente, por ejemplo que adopta la forma de una dirección de correo electrónico (tal como “código-identificación@nombre-servidor.xxx”) que se corresponde con un código de registro en cada uno de los servidores. En caso de que uno de los servidores no esté funcionando, puede usarse otro servidor de servicio para enviar la parte de señal de orden.

Más particularmente, cuando el dispositivo móvil 3 está dentro del área de corto alcance 7, la unidad de procesado 6 puede generar una pluralidad de clientes (por ejemplo, clientes XMPP) en una pluralidad de servidores (por ejemplo, servidores XMPP), y puede generar aleatoriamente una pluralidad de códigos de identificación (además de generar un conjunto nuevo de claves). La pluralidad de clientes se selecciona aleatoriamente de una lista de clientes disponibles. Preferentemente, los clientes seleccionados se protegen por SSL/TLS. A continuación, el dispositivo electrónico 1 almacena la pluralidad de códigos de identificación (y el conjunto de claves recién generado), y transmite al dispositivo móvil proximal 3 la pluralidad de códigos de identificación (junto con el conjunto de claves recién generado).

La siguiente vez que el dispositivo móvil 3 esté dentro del área de corto alcance 7, la pluralidad de clientes y la pluralidad de códigos de identificación previamente generadas se destruyen y la unidad de procesado 6 genera un nuevo conjunto de pluralidad de clientes y un nuevo conjunto de pluralidad de códigos de identificación (junto con un conjunto nuevo de claves). De este modo, los clientes seleccionados y los códigos de identificación generados tienen una duración limitada.

Puesto que los códigos de identificación (y las claves) se transfieren desde el dispositivo electrónico 1 al dispositivo móvil 3 a través del enlace de comunicaciones de corto alcance 2 y no transitan a través de ningún servidor. Por lo tanto, los códigos de identificación (y las claves) son conocidos únicamente para el dispositivo electrónico 1 y el dispositivo móvil 3, y se reduce fuertemente el riesgo de interceptación de cualquiera de los códigos de identificación (y claves) por parte de un tercero.

En una forma de realización, el dispositivo electrónico comprende un dispositivo de identificación de dispositivos móviles. El dispositivo de identificación de dispositivos móviles se puede usar en una etapa inicial de identificación del dispositivo móvil 3, cuando dicho dispositivo móvil 3 está dentro del área de corto alcance 7. La etapa inicial de identificación del dispositivo móvil 3 se puede llevar a cabo por medio de una conexión por cable del dispositivo móvil 3 con el dispositivo electrónico 1, por ejemplo, a través de un conector físico, tal como un conector USB 9 o cualquier otro conector apropiado.

El dispositivo móvil 3 se puede identificar registrando un código de identificación exclusivo representativo del *hardware* del dispositivo móvil 3, tal como la Identidad Internacional de Equipo de Estación Móvil (IMEI). En caso de que el dispositivo móvil tenga un chip a modo de circuito integrado de módulo de identificación de abonado (SIM), el número de serie SIM se puede registrar como código de identificación exclusivo. Alternativamente, como código de identificación exclusivo se puede registrar la dirección de control de acceso a los medios (dirección MAC).

El registro del código de identificación exclusivo se puede usar para garantizar que el conjunto de claves transmitido únicamente se puede usar en combinación con el dispositivo móvil 3 específico que se corresponde con el código de identificación exclusivo. Por lo tanto, el conjunto de claves no se puede ejecutar en ningún otro dispositivo móvil.

En otra forma de realización mostrada en la figura 2, el dispositivo electrónico 1 comprende un dispositivo de identificación de usuario 14. El procedimiento comprende, entonces, una etapa de identificación de usuarios en la que las características de un usuario 5 que es propietario del dispositivo móvil 3 se registran en el dispositivo electrónico 1 cuando el usuario y el dispositivo móvil 3 están dentro del área de corto alcance 7. El procedimiento puede comprender una etapa de emparejamiento del dispositivo móvil 3 identificado en el dispositivo electrónico 1 y su propietario también identificado en el dispositivo electrónico 1 durante la etapa de identificación de usuarios.

El dispositivo de identificación de usuarios puede comprender un dispositivo de reconocimiento facial 14. El sistema de reconocimiento facial puede ser un sistema de reconocimiento facial bidimensional, aunque, preferentemente, es un sistema de reconocimiento facial tridimensional. Un sistema de reconocimiento facial tridimensional del tipo mencionado puede comprender, ventajosamente, por lo menos dos cámaras de vídeo 15 y/o un sensor 3D (no mostrado).

Alternativamente, el dispositivo de reconocimiento facial puede comprender un dispositivo de formación térmica de imágenes por infrarrojos (IR). En ese caso, las cámaras 15 pueden ser cámaras de infrarrojos. El reconocimiento facial mediante el dispositivo de formación térmica de imágenes por IR se puede fusionar con el reconocimiento facial mediante un dispositivo de formación de imágenes visibles. En otra alternativa, el dispositivo de reconocimiento puede comprender un dispositivo de medición biométrica (no mostrado).

Las características del usuario registrado 5 se pueden asociar al conjunto de claves transmitido al dispositivo móvil 3 del cual es propietario el usuario 5. La etapa de identificación del dispositivo móvil se puede llevar a cabo en combinación con la etapa de identificación del usuario, tal que permita la transmisión del conjunto de claves al dispositivo móvil 3.

La etapa de identificación del usuario se puede usar para permitir la transmisión del conjunto de claves al dispositivo móvil 3 a través del enlace de comunicaciones de corto alcance 2. Cuando la etapa de identificación del dispositivo móvil se lleva a cabo en combinación con la etapa de identificación del usuario, la transmisión del conjunto de claves se produce únicamente cuando el usuario registrado 5 y el dispositivo móvil 3 están simultáneamente dentro del área de corto alcance 7. El conjunto de claves se puede transferir desde el dispositivo electrónico 1 al dispositivo móvil 3 únicamente cuando el dispositivo móvil 3 ha sido identificado en el dispositivo electrónico 1, por ejemplo registrando un código de identificación exclusivo del dispositivo móvil 3, y el usuario que es propietario del dispositivo móvil 3 ha sido identificado en el dispositivo electrónico 1 por el dispositivo de reconocimiento.

En otra forma de realización, el dispositivo electrónico 1 comprende un dispositivo sensor 16 configurado para detectar un rasgo característico dentro del área de corto alcance 7. Los ejemplos de un dispositivo sensor del tipo mencionado pueden incluir un detector de movimiento/presencia, un detector de humo, un detector de gas (o de cualquier otra sustancia química) o un sistema de videovigilancia. El dispositivo electrónico 1 está configurado, además, para enviar una señal al dispositivo móvil 3, a través del enlace de comunicaciones de largo alcance 4. La señal se puede usar en el dispositivo móvil 3 para avisar al propietario del dispositivo móvil 3 sobre el rasgo característico detectado por el dispositivo sensor (aparición de un intruso, un incendio, etc.). La señal enviada se puede cifrar con una de las claves del conjunto de claves en el dispositivo electrónico 1 y se puede descifrar con la clave correspondiente en el dispositivo móvil 3, según se ha descrito anteriormente. La clave usada para el cifrado y el descifrado se usa solamente una vez y, después de esto, se destruye.

Todavía en otra forma de realización ilustrada en la figura 3, el dispositivo electrónico 1 se usa como dispositivo de mensajería privada. En esta forma de realización, la señal de orden comprende un mensaje y la señal de control generada por el dispositivo electrónico 1 comprende, también, un mensaje. En este caso, el término “mensaje” puede comprender cualquier forma de información, tal como texto, imagen, vídeo, sonido y cualquier combinación de estas informaciones.

La figura 3 ilustra un ejemplo de un dispositivo de mensajería privada del tipo mencionado que usa el dispositivo electrónico 1. El dispositivo de mensajería privada comprende un primer dispositivo electrónico 1 de la invención, y una pluralidad de primeros dispositivos móviles 30, 30’, 30’’, 30’’’.

Cada uno de los primeros dispositivos móviles 30 a 30’’’ está destinado a situarse dentro del área de corto alcance 7 del primer dispositivo electrónico 1, de tal manera que un primer conjunto de claves se transfiera a cada uno de ellos a través del enlace de comunicaciones de corto alcance 2. El primer conjunto de claves transferidas a cada uno de los primeros dispositivos móviles 30 a 30’’’ pueden ser diferentes entre sí. La etapa de identificación del dispositivo móvil se puede llevar a cabo, además, para cada uno de los dispositivos móviles 30 a 30’’’, de tal manera que un código de identificación exclusivo representativo del *hardware* de cada uno de los primeros dispositivos móviles 30 a 30’’ se registra en el primer dispositivo electrónico 1, y de tal manera que el primer conjunto de claves se transfiere de forma válida únicamente para el primer dispositivo móvil registrado correspondiente 30 a 30’’’. La etapa de identificación del dispositivo móvil se puede llevar a cabo, además, en combinación con la etapa de identificación del usuario, de tal manera que el primer conjunto de claves se transfiere de forma válida únicamente para el primer dispositivo móvil registrado correspondiente 30 a 30’’’ y cuando el usuario respectivo está simultáneamente dentro del área de corto alcance 7.

En esta configuración, el primer dispositivo electrónico 1 puede recibir una señal de orden (mensaje) enviada desde uno de los primeros dispositivos móviles 30 a 30’’’ (emisor) cuando está dentro o fuera del área de corto alcance 7, a través de los medios de comunicación 10. El mensaje se cifrará con una clave del primer conjunto de claves que se transmitió sobre el primer dispositivo móvil emisor 30 a 30’’’ la última vez que el mismo se situó proximal con respecto al primer dispositivo electrónico 1.

Cuando el primer dispositivo electrónico 1 recibe el mensaje cifrado, el primer dispositivo electrónico 1 descifra el mensaje, descodifica el destinatario deseado, y a continuación el primer dispositivo electrónico 1 cifra el mensaje y envía este último al destinatario, es decir, aquel de los primeros dispositivos móviles 30 a 30’’’ al cual va destinado el mensaje, a través de los medios de comunicación 10.

El mensaje recibido descifrado en el dispositivo electrónico 1 puede comprender una etiqueta que indica que la información recibida es una orden (por ejemplo, en el caso de la internet de la aplicación de hogar inteligente) o si se trata de un mensaje (en el caso presente). En caso de que la información sea un mensaje, la etiqueta se puede usar, además, para identificar el destinatario. Por ejemplo, los primeros caracteres del mensaje cifrado se pueden usar para la etiqueta.

El primer dispositivo electrónico 1 puede generar, además, una lista de usuarios para los cuales se han registrado en el primer dispositivo electrónico 1 el código de identificación exclusivo de su dispositivo móvil 30 a 30''' y/o las características del usuario 5. A continuación, el primer dispositivo electrónico verificará si el código de identificación exclusivo y/o las características del usuario 5 se han registrado y enviará el mensaje al destinatario únicamente si el código de identificación exclusivo y/o las características del usuario 5 están en la lista generada.

El mensaje puede ser un mensaje instantáneo de tal manera que el dispositivo electrónico 1 se use como un dispositivo de mensajería privada instantánea.

Preferentemente, el mensaje se puede visionar durante un espacio de tiempo especificado por el usuario antes de que resulte inaccesible (por ejemplo, cuando se destruye el mensaje). Dicho espacio de tiempo especificado se puede fijar, por ejemplo, a entre 1 y 30 segundos, 5 minutos, 30 minutos, o cualquier periodo de tiempo adecuado.

Cuando el mensaje enviado por el primer dispositivo electrónico 1 llega al destinatario, el primer dispositivo electrónico 1 puede recibir un mensaje de acuse de recibo enviado por el dispositivo móvil 30 a 30''' que sea el destinatario. En caso de que el destinatario no recibiese el mensaje de acuse de recibo, por ejemplo porque el dispositivo móvil destinatario 30 a 30''' no estaba activo (el dispositivo móvil 30 a 30''' está apagado), el primer dispositivo electrónico 1 puede enviar un mensaje de tiempo límite al emisor.

El dispositivo de mensajería privada puede incluir, además, una pluralidad de dispositivos electrónicos 1, que cooperan, cada uno de ellos, con una pluralidad de dispositivos móviles 3 de tal manera que pueden transmitirse mensajes no solamente entre los dispositivos móviles 3 que cooperan con uno de los dispositivos electrónicos 1 sino también aquellos que cooperan con otros dispositivos electrónicos 1, tal como se ejemplificará posteriormente.

En la figura 3, el dispositivo de mensajería privada comprende un segundo dispositivo electrónico 1' de la invención y una pluralidad de segundos dispositivos móviles 31, 31', 31'', 31'''. Por ejemplo, el primer dispositivo electrónico 1 puede estar dentro de una primera área de corto alcance 7, tal como un primer hogar o primer edificio de oficinas, y el segundo dispositivo electrónico 1' puede estar en una segunda área de corto alcance 7', tal como un segundo hogar o segundo edificio de oficinas.

El segundo dispositivo electrónico 1' se puede usar como dispositivo de mensajería privada en combinación con la pluralidad de segundos dispositivos móviles 31 a 31''' según se ha descrito anteriormente para el primer dispositivo electrónico 1 y los primeros dispositivos móviles 30 a 30'''.

En una forma de realización, por lo menos uno de los segundos dispositivos móviles 31 a 31''' se puede llevar dentro de la primera área de corto alcance 7, y la etapa de identificación del dispositivo móvil se puede llevar a cabo para el segundo dispositivo móvil 31 a 31''' dentro de la primera área de corto alcance 7 tal que registre su código de identificación exclusivo en el primer dispositivo electrónico 1. Llamaremos dispositivo invitado 31* a este segundo dispositivo móvil 31 a 31''' (la figura 3 muestra un ejemplo de uno de los segundos dispositivos móviles 31 a 31''' que se usa como dispositivo invitado 31*).

La etapa de identificación del dispositivo móvil se puede llevar a cabo, además, en combinación con la etapa de identificación del usuario para el usuario que es propietario del dispositivo invitado 31* para el cual se ha registrado un código de identificación exclusivo en el primer dispositivo electrónico 1.

Cuando el dispositivo invitado 31* registrado en el primer dispositivo electrónico 1 está dentro de la primera área de corto alcance 7, el primer dispositivo electrónico 1 transmite al mismo un primer conjunto de claves.

Cuando el dispositivo invitado 31* está dentro de la segunda área de cobertura 7', el segundo dispositivo electrónico 1' transmite al mismo un segundo conjunto de claves (el segundo dispositivo móvil 31 a 31''' está registrado también en el segundo dispositivo electrónico 1'). Por otra parte, el segundo dispositivo electrónico 1' recibió el primer conjunto de claves del dispositivo invitado 31*.

En una forma de realización ejemplificativa, un mensaje es enviado por uno de los segundos dispositivos móviles 31 a 31''' (no necesariamente el dispositivo invitado 31*) a un destinatario que es uno de los primeros dispositivos móviles 30 a 30''' (llamaremos dispositivo destinatario 30* a este último). En tal caso, el segundo dispositivo electrónico 1' recibe un mensaje enviado por uno de los segundos dispositivos móviles 31 a 31''' (que no es necesariamente el dispositivo invitado 31*).

El segundo dispositivo electrónico 1' descifra el mensaje recibido usando una clave del segundo conjunto de claves y cifra el mensaje recibido usando una clave del primer conjunto de claves. El segundo dispositivo electrónico 1' envía, a continuación, el mensaje cifrado al primer dispositivo electrónico 1, por ejemplo a través del enlace de comunicaciones de largo alcance 4. El primer dispositivo electrónico 1 recibe el mensaje y lo descifra usando la misma clave mencionada del primer conjunto de claves. A continuación, el primer dispositivo electrónico 1 cifra el mensaje con otra clave del primer conjunto de claves, y lo envía al dispositivo destinatario 30*. La clave usada para el cifrado y el descifrado se destruye.

De este modo, es posible enviar un mensaje por medio de los dispositivos electrónicos 1, 1' entre uno de los dispositivos móviles registrados en uno de los dispositivos electrónicos 1, 1' y otro dispositivo móvil registrado en otro de los dispositivos electrónicos 1, 1', incluso cuando el dispositivo móvil que está registrado en los dos dispositivos electrónicos 1, 1' no está en funcionamiento (por ejemplo, está apagado). De hecho, los dos dispositivos electrónicos 1, 1' se pueden conectar a una red de Internet.

En una forma de realización, hay un soporte de ordenador que comprende partes de código de programa que serán ejecutadas por el dispositivo electrónico 1 de acuerdo con una de las reivindicaciones 1 a 10, con el fin de llevar a cabo el procedimiento divulgado en la presente memoria cuando dicho programa es ejecutado por dicho dispositivo electrónico 1.

El soporte de ordenador puede comprender, además, partes de código de programa que serán ejecutadas por el dispositivo móvil 3 con el fin de llevar a cabo el procedimiento cuando dicho programa es ejecutado por dicho dispositivo electrónico 1 y dicho dispositivo móvil 3.

Todavía en otra forma de realización, cualquiera de los primeros dispositivos móviles 30 a 30''' puede enviar un mensaje a cualquiera de los segundos dispositivos móviles 31 a 31''' a través del enlace de comunicaciones de largo alcance 4. El mensaje enviado por uno de los primeros dispositivos móviles 30 a 30''' se cifra con una clave del primer conjunto de claves. Cuando es recibido por uno de los segundos dispositivos móviles 31 a 31''', el mensaje se descifra usando una clave del segundo conjunto de claves. Cada clave usada para cifrar y descifrar cada mensaje se destruye después de la etapa de descifrado.

Números y símbolos de referencia

1	dispositivo electrónico, primer dispositivo electrónico
1'	segundo dispositivo electrónico
2	enlace de comunicaciones de corto alcance
3	dispositivo móvil
4	enlace de comunicaciones de largo alcance
5	usuario, propietario del dispositivo móvil
6	unidad de procesado
7	área de corto alcance, primera área de corto alcance
7'	segunda área de corto alcance
8	Internet
9	conexión por cable
10	medios de comunicación
11	horno
12	sistema de iluminación
14	sistema de reconocimiento facial
15	cámara
16	dispositivo sensor
30, 30', 30'', 30'''	primeros dispositivos móviles
30*	dispositivo destinatario
31, 31', 31'', 31'''	segundos dispositivos móviles
31*	dispositivo invitado

REIVINDICACIONES

1. Dispositivo electrónico (1) configurado para generar una señal de control para controlar otro dispositivo de una manera protegida cuando se recibe una señal de orden desde un dispositivo móvil (3), comprendiendo el dispositivo electrónico (1):

una unidad de procesado (6) configurada para generar y almacenar un conjunto de claves que comprende una pluralidad de claves de cifrado;

unos medios para establecer un enlace de comunicaciones de corto alcance (2) entre el dispositivo electrónico (1) y el dispositivo móvil (3) dentro de un área de corto alcance (7) y transmitir el conjunto de claves al dispositivo móvil (3), cuando el dispositivo móvil está dentro del área de corto alcance (7);

medios para establecer un enlace de comunicaciones de largo alcance (4) entre el dispositivo electrónico (1) y el dispositivo móvil (3) cuando el dispositivo móvil (3) está fuera del área de corto alcance (7);

estando configurado, además, dicho enlace de comunicaciones de largo alcance (4) para recibir una señal de orden enviada por el dispositivo móvil (3), cifrándose la señal de orden con una clave del conjunto de claves;

estando configurada, además, la unidad de procesado (6) para descifrar dicha señal de orden y generar la señal de control en función de la señal de orden recibida; utilizándose cada clave del conjunto de claves solamente una vez;

caracterizado por que,

el dispositivo electrónico comprende, además, un dispositivo de identificación de dispositivos móviles configurado para identificar el dispositivo móvil (3) cuando este último está dentro del área de corto alcance (7); y

un dispositivo de identificación de usuarios (14) configurado para registrar las características de un usuario (5) que es propietario del dispositivo móvil (3);

de tal manera que la transmisión del conjunto de claves se produce solamente cuando el usuario registrado (5) y el dispositivo móvil (3) están simultáneamente dentro del área de corto alcance (7).

2. Dispositivo electrónico según la reivindicación 1, en el que la señal de control está configurada para controlar un objeto que va a ser controlado dentro del área de corto alcance (7), tal como para objetos conectados y aplicaciones domóticas.

3. Dispositivo electrónico según la reivindicación 1, configurado para funcionar como dispositivo de mensajería privada en el que la señal de orden comprende un mensaje y la señal de control generada comprende el mensaje que se va a enviar a un destinatario.

4. Dispositivo electrónico según cualquiera de las reivindicaciones 1 a 3, en el que dicho enlace de comunicaciones de corto alcance (2) comprende un dispositivo de comunicaciones ópticas o por ondas de radio, que usa en especial una comunicación de RFID y de campo cercano, el protocolo de transmisión Bluetooth®, el Bluetooth de Baja Energía (BLE), un protocolo de comunicación de campo cercano (NFC), una tarjeta de proximidad o una conexión directa WiFi, el Zigbee, la comunicación por líneas eléctricas, una transmisión por infrarrojos (IR), un protocolo *Z-wave* o una comunicación por ultrasonidos.

5. Dispositivo electrónico según cualquiera de las reivindicaciones 1 a 4, en el que el dispositivo de identificación de usuarios (14) es un dispositivo de formación térmica de imágenes por infrarrojos y/o un dispositivo de formación de imágenes visibles.

6. Procedimiento para generar una señal de control para controlar otro dispositivo de una manera protegida, que comprende:

proporcionar un dispositivo electrónico (1) según cualquiera de las reivindicaciones 1 a 5;

establecer un enlace de comunicaciones de corto alcance (2) entre el dispositivo electrónico (1) y el dispositivo móvil (3) cuando el dispositivo móvil (3) está dentro del área de corto alcance (7);

establecer un enlace de comunicaciones de largo alcance entre el dispositivo electrónico (1) y el dispositivo móvil (3) cuando el dispositivo móvil (3) está fuera del área de corto alcance (7);

generar y almacenar el conjunto de claves en la unidad de procesado (6);

transmitir el conjunto de claves al dispositivo móvil (3) a través del enlace de comunicaciones de corto alcance (2);

recibir una señal de orden del dispositivo móvil (3), cifrándose la señal de orden con una de las claves transferidas al dispositivo móvil (3) a través del enlace de comunicaciones de largo alcance (4) y descifrar la señal de orden con la mencionada de las claves almacenadas en el dispositivo de procesado (6);

generar la señal de control en función de la señal de orden;

utilizándose cada clave del conjunto de claves solamente una vez;

caracterizado por que el procedimiento comprende, además, las etapas de:

identificar el dispositivo móvil (3) cuando este último está dentro del área de corto alcance (7) usando el dispositivo de identificación de dispositivos móviles; y

registrar las características de un usuario (5) que es propietario del dispositivo móvil (3) usando el dispositivo de identificación de usuarios (14);

de tal manera que la transmisión del conjunto de claves se produce solamente cuando el usuario registrado (5) y el dispositivo móvil (3) están simultáneamente dentro del área de corto alcance (7).

7. Procedimiento según la reivindicación 6, que comprende, además, una etapa de destruir la clave usada para cifrar y descifrar la señal de orden.

8. Procedimiento según la reivindicación 6 o 7, en el que la etapa de generar la señal de control comprende controlar un objeto que va a ser controlado dentro del área de corto alcance (7), tal como en el control de objetos conectados y/o aplicaciones domóticas.

9. Procedimiento según cualquiera de las reivindicaciones 6 a 8, en el que la señal de orden comprende un mensaje y en el que la generación de la señal de control comprende enviar el mensaje a un destinatario.

10. Procedimiento según cualquiera de las reivindicaciones 6 a 9, en el que el dispositivo móvil comprende una pluralidad de dispositivos móviles (30, 30', 30'', 30'''); y en el que la generación y el almacenamiento del conjunto de claves en la unidad de procesado (6) comprende generar y almacenar una pluralidad de conjuntos de claves, transfiriéndose un conjunto diferente de claves a cada uno de la pluralidad de dispositivos móviles (30 a 30''').

11. Procedimiento según cualquiera de las reivindicaciones 6 a 10, que comprende, además, asociar las características registradas de un usuario (5) al conjunto de claves transmitidas al dispositivo móvil (3) del que es propietario el usuario (5).

12. Procedimiento según cualquiera de las reivindicaciones 6 a 11, en el que cada clave de dicha pluralidad de conjuntos de claves se basa en un algoritmo de contraseña de un solo uso basada en tiempo.

13. Procedimiento según cualquiera de las reivindicaciones 6 a 12, en el que la señal de orden recibida es válida durante un periodo de tiempo limitado.

14. Procedimiento según cualquiera de las reivindicaciones 6 a 13,

en el que dicha señal de orden comprende una pluralidad de partes de señal de orden; y

en el que dicha recepción de una señal de orden comprende recibir las partes de señal de orden, cifrándose cada parte de señal de orden con el uso de dicha una clave.

15. Procedimiento según cualquiera de las reivindicaciones 6 a 14,

en el que el enlace de comunicaciones de largo alcance (4) se materializa a través de uno o una pluralidad de servidores remotos por medio de un protocolo de Internet; y

en el que el procedimiento comprende, además, generar una pluralidad de clientes en dicho uno o una pluralidad de servidores remotos, cuando el dispositivo móvil (3) está dentro del área de corto alcance (7).

16. Procedimiento según la reivindicación 15, que comprende, además:

generar aleatoriamente una pluralidad de códigos de identificación por parte del dispositivo electrónico (1);

almacenar dicha pluralidad de códigos de identificación en el dispositivo electrónico (1); y

transmitir la pluralidad almacenada de códigos de identificación al dispositivo móvil (3) proximal dentro del área de corto alcance (7).

17. Procedimiento según la reivindicación 16, que comprende, además, la siguiente vez que el dispositivo móvil (3) esté dentro del área de corto alcance (7), destruir la pluralidad transmitida de códigos de identificación y generar un conjunto nuevo de pluralidad de clientes y un conjunto nuevo de pluralidad de códigos de identificación.

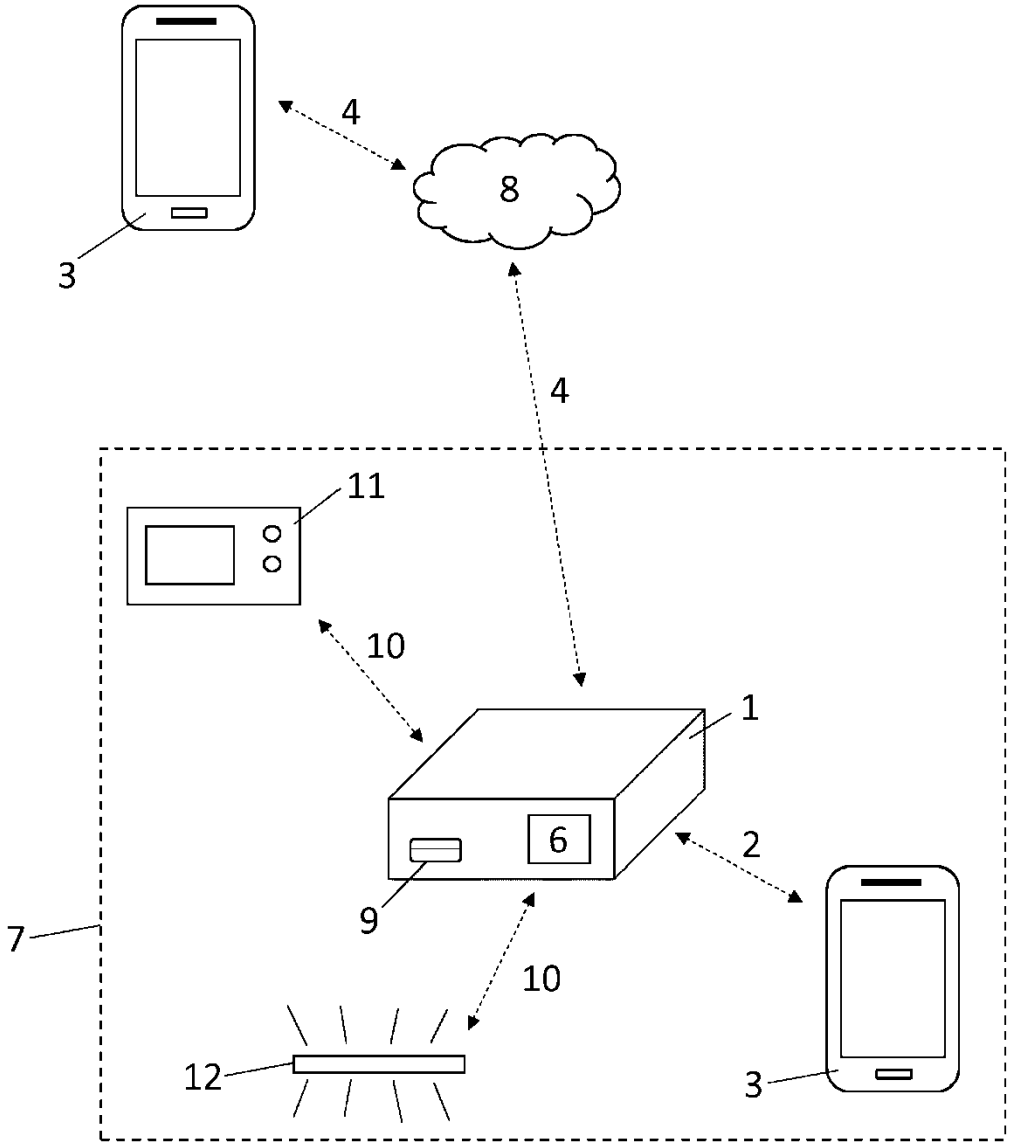

Fig. 1

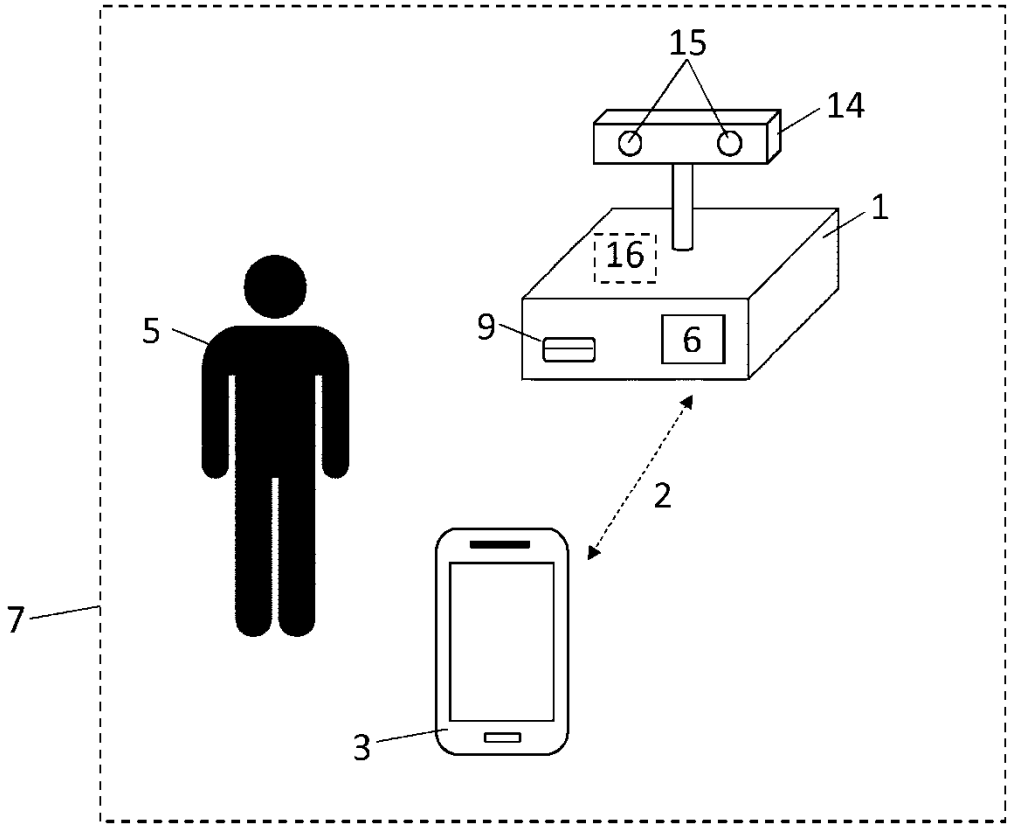

Fig. 2

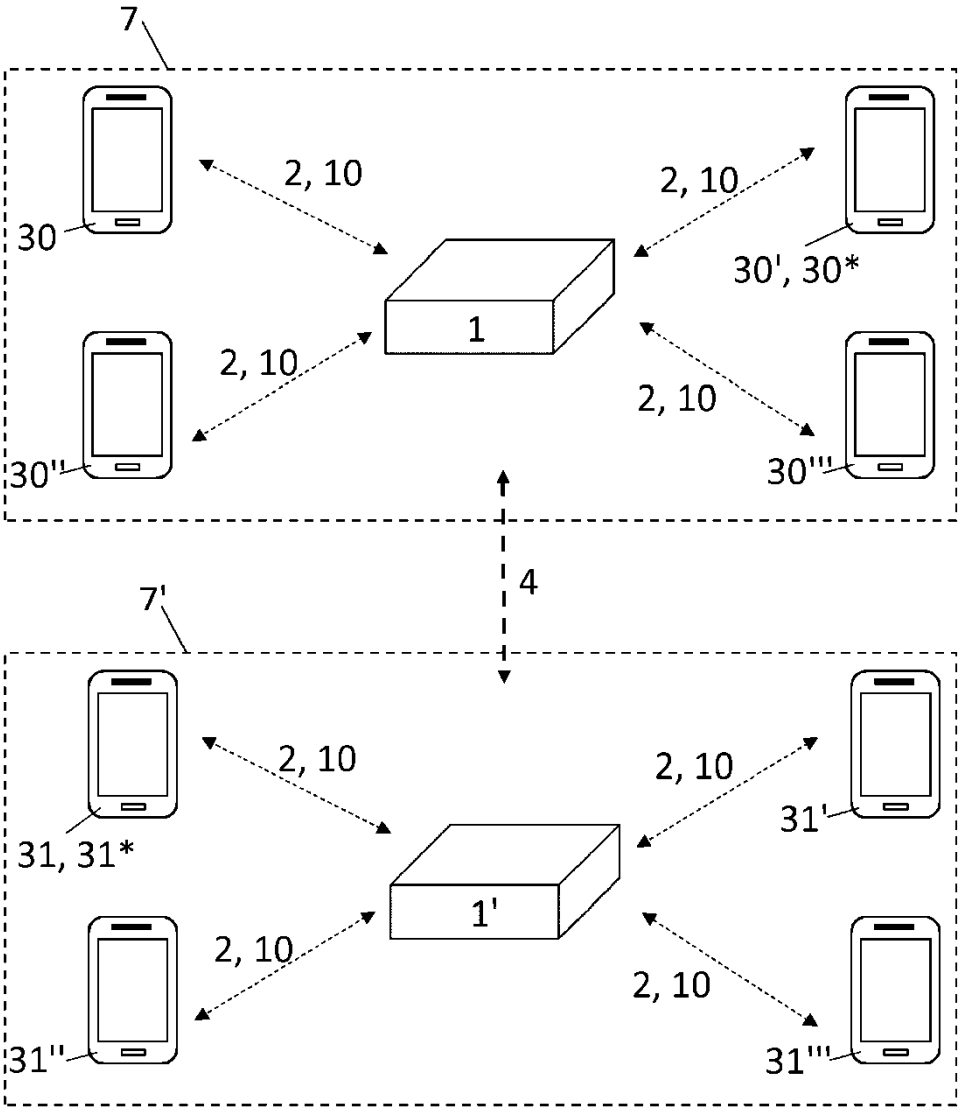

Fig. 3