(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 665 553**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.03.2014 E 14157510 (0)**

(97) Fecha y número de publicación de la concesión europea: **31.01.2018 EP 2916510**

(54) Título: **Método de autenticación en red para una verificación segura de identidades de usuario utilizando información de posicionamiento de usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.04.2018

(73) Titular/es:

KEYPASCO AB (100.0%)
Magasinsgatan 24
41118 Gothenburg, SE

(72) Inventor/es:

SKYGEBJERG, PER

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Método de autenticación en red para una verificación segura de identidades de usuario utilizando información de posicionamiento de usuario.

La invención se refiere a la autenticación de identidades en redes, y, más particularmente, a un método de autenticación en red para una verificación segura de la identidad de un usuario.

En la actualidad, se han popularizado de manera creciente diversas transacciones web. Para proteger las transacciones web, es absolutamente necesaria una autenticación de las identidades de los usuarios. No obstante, debido al creciente número de los usuarios de la web y de los delitos en la misma, y, por ejemplo, al avance continuo de las técnicas delictivas, es necesario que los proveedores de contenido de internet (ICP) proporcionen un dispositivo de verificación de identidad para cada usuario. De este modo, los costes del servicio de atención al cliente para la personalización, la distribución y la resolución de problemas es considerable. Además, la necesidad de que el usuario disponga de diferentes dispositivos de verificación de identidad para diferentes ICPs es bastante incómoda. Por otra parte, además de interceptar y robar IDs y contraseñas de usuario, los piratas informáticos también intentan manipular datos de transacciones. Por tanto, los ICP se ven con frecuencia obligados a cambiar de equipos de hardware, generando así costes adicionales.

Por ello, es un objetivo de la presente invención proporcionar un método de autenticación en red para una verificación segura de la identidad de un usuario y que pueda superar los inconvenientes previamente mencionados de la técnica anterior.

El documento US 2004/250074 A1 da a conocer un método para proporcionar un acceso seguro a un servicio de aplicación, en el cual un *token* de seguridad y un *token de proximidad* comprueban que sus ubicaciones están próximas entre sí antes de iniciar un procesado criptográfico entre el *token* de seguridad y el servicio de aplicación. El documento GB 2 492 614 A da a conocer otro método de autenticación relacionado que se lleva a cabo en un terminal cuando el mismo está a menos de una distancia predefinida con respecto a un dispositivo móvil. El documento EP 2 506 525 A1 da a conocer un método de autorización relacionado que se lleva a cabo entre un dispositivo de cliente y un dispositivo de servidor.

Según un aspecto de la presente invención, se proporciona un método de autenticación en red de acuerdo con la reivindicación independiente 1.

Según otro aspecto de la presente invención, se proporciona un método de autenticación en red de acuerdo con la reivindicación independiente 11.

Otras características y ventajas de la presente invención se pondrán de manifiesto en la siguiente descripción detallada de las formas de realización preferidas, en referencia a los dibujos adjuntos, en los cuales:

la Figura 1 es un diagrama de bloques esquemático que ilustra un sistema de autenticación en red que está configurado para implementar la primera forma de realización preferida de un método de autenticación en red de acuerdo con la presente invención;

la Figura 2 es un diagrama de flujo que ilustra la primera forma de realización preferida;

la Figura 3 es un diagrama de flujo de un primer procedimiento entre las etapas S23 y S24 de la primera forma de realización preferida;

la Figura 4 es un diagrama de flujo de un segundo procedimiento entre las etapas S23 y S24 de la primera forma de realización preferida;

la Figura 5 es un diagrama de flujo de un tercer procedimiento entre las etapas S23 y S24 de la primera forma de realización preferida;

la Figura 6 es un diagrama de bloques esquemático que ilustra una primera variante del sistema de autenticación en red;

la Figura 7 es un diagrama de flujo de un cuarto procedimiento entre las etapas S23 y S24 de la primera forma de realización preferida, para su implementación por medio de la primera variante del sistema de autenticación en red de la Figura 6;

la Figura 8 es un diagrama de bloques esquemático que ilustra una segunda variante del sistema de autenticación en red;

la Figura 9 es un diagrama de flujo de un quinto procedimiento entre las etapas S23 y S24 de la primera forma de realización preferida, para su implementación por medio de la segunda variante del sistema de autenticación en red de la Figura 8;

la Figura 10 es un diagrama de bloques esquemático que ilustra otro sistema de autenticación en red que está configurado para implementar la segunda forma de realización preferida de un método de autenticación en red de acuerdo con la presente invención; y

la Figura 11 es un diagrama de flujo que ilustra la segunda forma de realización preferida.

Antes de describir de forma más detallada la presente invención, debe indicarse que los elementos equivalentes se indican con los mismos numerales de referencia en toda la exposición.

En referencia a la Figura 1, se usa un sistema de autenticación en red para implementar la primera forma de realización preferida de un método de autenticación en red para la identificación segura de la identidad de un usuario 5, de acuerdo con la presente invención. El sistema de autenticación en red incluye un terminal de usuario 1, tal como un ordenador personal o un ordenador de tipo *notebook*, manejado por el usuario 5, un servidor de proveedor de contenido 2, tal como el servidor de un proveedor de contenido de Internet (ICP), un servidor de verificación 3, y un dispositivo electrónico personal portátil 4 llevado por el usuario 5. El terminal de usuario 1, el servidor de proveedor de contenido 2 y el servidor de verificación 3 están conectados a una red de comunicaciones 100, tal como Internet. El dispositivo electrónico personal portátil 4 tiene la capacidad de conectarse con la red de comunicaciones 100 y/o de conectarse a corta distancia con el terminal de usuario 1 (véase, por ejemplo, la Figura 6). En esta forma de realización, si se autentica satisfactoriamente la identidad del usuario 5 por medio del sistema de autenticación en red, se permite que el usuario 5 acceda a datos en el servidor de proveedor de contenido 2 utilizando el terminal de usuario 1.

La Figura 2 es un diagrama de flujo de la primera forma de realización preferida del método de autenticación en red, que ilustra cómo se verifica la identidad del usuario 5. La primera forma de realización preferida del método de autenticación en red incluye las siguientes etapas.

En la etapa S21, el usuario 5 introduce datos de inicio de sesión de usuario usando una interfaz de entrada de usuario (no mostrada) del terminal de usuario 1, en un sitio web proporcionado por el servidor de proveedor de contenido 2. A continuación, los datos de inicio de sesión de usuario se transmiten desde el terminal de usuario 1 al servidor de proveedor de contenido 2 por medio de la red de comunicaciones 100. En esta forma de realización, los datos de inicio de sesión de usuario incluyen una identificación de usuario (ID) que sirve como identificador de usuario, y una contraseña.

En la etapa S22, tras la recepción de los datos de inicio de sesión de usuario desde el terminal de usuario 1, el servidor de proveedor de contenido 2 comprueba si los datos de inicio de sesión de usuario son correctos. Si el resultado es afirmativo, el flujo prosigue hacia la etapa S23. En caso contrario, el servidor de proveedor de contenido 2 envía un mensaje de error al terminal de usuario 1 para su visualización en un dispositivo de visualización (no mostrado) del terminal de usuario 1 (etapa S20).

En la etapa S23, el servidor de proveedor de contenido 2 transmite una solicitud de verificación, que incluye el identificador de usuario, al servidor de verificación 3 por medio de la red de comunicaciones 100. En esta forma de realización, el servidor de verificación 3 puede considerarse como un tercero designado por el servidor de proveedor de contenido 2 para llevar a cabo la autenticación de identidades.

En la etapa S24, después de la recepción de la solicitud de verificación desde el servidor de proveedor de contenido 2, el servidor de verificación 3 recibe además datos de identificación de hardware e información de posicionamiento que están asociados al terminal de usuario 1 y al dispositivo electrónico personal portátil 4. Por ejemplo, tal como se muestra en la Figura 1, el terminal de usuario 1 incluye un módulo de sistema de posicionamiento global (GPS) 11, y tiene prealmacenado un primer programa de exploración 12. El dispositivo electrónico personal portátil 4 puede ser, aunque sin carácter limitativo, un teléfono inteligente o un ordenador de tipo tableta, incluye un módulo de GPS 41, y tiene prealmacenado un segundo programa de exploración 42. En este ejemplo, se asignan dos direcciones de red diferentes, por ejemplo, direcciones IP, respectivamente al terminal de usuario 1 y al dispositivo electrónico personal portátil 4. La Figura 3 muestra un primer procedimiento para ser llevado a cabo entre las etapas S23 y S24, y que ilustra cómo se proporcionan los datos de identificación de hardware y la información de posicionamiento al servidor de verificación 3. El primer procedimiento incluye las siguientes etapas. En la etapa S31, después de transmitir la solicitud de verificación al servidor de verificación 3, el servidor de proveedor de contenido 2 transmite además una primera y una segunda solicitudes de datos, respectivamente, al terminal de usuario 1 y al dispositivo electrónico personal portátil 4, por medio de la red de comunicaciones 100. En la etapa S32, como respuesta a la primera solicitud de datos del servidor de proveedor de contenido 2, el terminal de usuario 1 lleva a cabo un posicionamiento de GPS usando el módulo de GPS 11, para obtener unos primeros datos de posicionamiento que se corresponden con una ubicación geográfica del terminal de usuario 1, ejecuta el primer programa de exploración 12 para obtener una

primera combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del terminal de usuario 1, y transmite los primeros datos de posicionamiento y la primera combinación de los códigos de identificación al servidor de verificación 3 por medio de la red de comunicaciones 100. Debe indicarse que, puesto que la generación de la primera combinación de los códigos de identificación usando la ejecución del primer programa de exploración 12 es conocida para aquellos versados en la materia, en la presente se omiten detalles de la misma por motivos de brevedad. En la etapa S33, como respuesta a la segunda solicitud de datos del servidor de proveedor de contenido 2, el dispositivo electrónico personal portátil 4 lleva a cabo un posicionamiento de GPS usando el módulo de GPS 41 para obtener unos segundos datos de posicionamiento que se corresponden con una ubicación geográfica actual del dispositivo electrónico personal portátil 4, ejecuta el segundo programa de exploración 42 para obtener una segunda combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del dispositivo electrónico personal portátil 4, y transmite los segundos datos de posicionamiento y la segunda combinación de los códigos de identificación al servidor de verificación 3 por medio de la red de comunicaciones 100. De este modo, la primera combinación de los códigos de identificación del terminal de usuario 1 y la segunda combinación de los códigos de identificación del dispositivo electrónico personal portátil 4 constituyen, cooperativamente, los datos de identificación de hardware recibidos por el servidor de verificación 3 en la etapa S24. Los primeros datos de posicionamiento del terminal de usuario 1 y los segundos datos de posicionamiento del dispositivo electrónico personal portátil 4 constituyen, cooperativamente, la información de posicionamiento recibida por el servidor de verificación 3 en la etapa S24.

La Figura 4 muestra un segundo procedimiento que se efectuará entre la etapa S23 y la etapa S24, y que ilustra cómo se proporcionan los datos de identificación de hardware y la información de posicionamiento al servidor de verificación 3. El segundo procedimiento incluye las siguientes etapas. En la etapa S41, el servidor de proveedor de contenido 2 transmite una primera solicitud de datos al terminal de usuario 1 por medio de la red de comunicaciones 100. En la etapa S42, como respuesta a la recepción de la solicitud de verificación del servidor de proveedor de contenido 2, el servidor de verificación 3 transmite una segunda solicitud de datos al dispositivo electrónico personal portátil 4 por medio de la red de comunicaciones 100. En la etapa S43, de manera similar a la etapa S32 de la Figura 3, la primera combinación de los códigos de identificación, y los primeros datos de posicionado generados, ambos, por el terminal de usuario 1, se transmiten desde el terminal de usuario 1 al servidor de verificación 3 por medio de la red de comunicaciones 100. En la etapa S44, de manera similar a la etapa S33 de la Figura 3, la segunda combinación de los códigos de identificación, y los segundos datos de posicionamiento, generados ambos por el dispositivo electrónico personal portátil 4, se transmiten desde el dispositivo electrónico personal portátil 4 al servidor de verificación 3 por medio de la red de comunicaciones 100.

La Figura 5 muestra un tercer procedimiento que se llevará a cabo entre la etapa S23 y la etapa S24, y que ilustra cómo se proporcionan los datos de identificación de hardware y la información de posicionamiento al servidor de verificación 3. El tercer procedimiento incluye las siguientes etapas. En la etapa S51, de manera similar a la etapa S41 de la Figura 4, se transmite la primera solicitud de datos desde el servidor de proveedor de contenido 2 al terminal de usuario 1. En la etapa S52, de manera similar a la etapa S43 de la Figura 4, la primera combinación de los códigos de identificación, y los primeros datos de posicionamiento, generados ambos por el terminal de usuario 1, se transmiten desde el terminal de usuario 1 al servidor de verificación 3 por medio de la red de comunicaciones 100. No obstante, a diferencia del primer y del segundo procedimientos, el dispositivo electrónico personal portátil 4 se puede hacer funcionar para llevar a cabo un posicionamiento de GPS con el fin de obtener los segundos datos de posicionamiento de una manera periódica, para ejecutar automáticamente el segundo programa de exploración 42 con el fin de obtener la segunda combinación de los códigos de identificación, y para transmitir los segundos datos de posicionamiento y la segunda combinación de los códigos de identificación al servidor de verificación 3 de una manera periódica. Por lo tanto, la etapa S53 del tercer procedimiento conlleva esencialmente la generación y la transmisión periódicas de los segundos datos de posicionamiento y de la segunda combinación de los códigos de identificación al servidor de verificación 3 por parte del dispositivo electrónico personal portátil 4. En este caso, la primera combinación de los códigos de identificación del terminal de usuario 1, y la segunda combinación de los códigos de identificación, que es la recibida más recientemente por el servidor de verificación 3 en la etapa S24 después de que el servidor de verificación 3 haya recibido la solicitud de verificación, constituyen, cooperativamente, los datos de identificación de hardware. Los primeros datos de posicionamiento del terminal de usuario 1, y los segundos datos de posicionamiento, que son los recibidos más recientemente por el servidor de verificación 3 en la etapa S24, constituyen, cooperativamente, la información de posicionamiento.

En referencia a la Figura 6, se muestra una primera variante del sistema de autenticación en red. A diferencia del sistema de autenticación en red de la Figura 1, el terminal de usuario 1 incluye una interfaz de comunicación inalámbrica de corta distancia 13, y tiene prealmacenado el primer programa de exploración 12. El dispositivo electrónico personal portátil 4 no puede conectarse con la red de comunicaciones 100, incluye una interfaz de comunicaciones inalámbrica de corta distancia 43, y tiene prealmacenado el segundo programa de exploración 42. Las interfaces de comunicación inalámbrica de corta distancia 13, 43 pueden usar tecnología de comunicación de campo cercano (NFC), Bluetooth o fidelidad inalámbrica (Wi-Fi). La Figura 7 muestra un cuarto procedimiento a realizar entre la etapa S23 y la etapa S24 por el sistema de autenticación en red de la Figura 6, y que ilustra cómo se proporcionan los datos de identificación de hardware y la información de posicionamiento al

servidor de verificación 3. El cuarto procedimiento incluye las siguientes etapas. En la etapa S71, de manera similar a la etapa S41 de la Figura 4, la primera solicitud de datos se transmite desde el servidor de proveedor de contenido 2 al terminal de usuario 1. En la etapa S72, como respuesta a la primera solicitud de datos del servidor de proveedor de contenido 2, el terminal de usuario 1 ejecuta el primer programa de exploración 12 para obtener la primera combinación de los códigos de identificación. Cuando el dispositivo electrónico personal portátil 4 está muy próximo al terminal de usuario 1 para es tablecer con el mismo un enlace de comunicación inalámbrica de corta distancia usando las interfaces de comunicación inalámbrica de corta distancia 13, 43, y el terminal de usuario 1 transmite la segunda solicitud de datos al dispositivo electrónico personal portátil 4 a través del enlace de comunicación inalámbrica de corta distancia. En la etapa S73, como respuesta a la segunda solicitud de datos del terminal de usuario 1, el dispositivo electrónico personal portátil 4 ejecuta el segundo programa de exploración 42 para obtener la segunda combinación de los códigos de identificación, y transmite la segunda combinación de los códigos de identificación al terminal de usuario 1 a través del enlace de comunicación inalámbrica de corta distancia. En este caso, la segunda combinación de los códigos de identificación sirve como datos de identificación asociados al dispositivo electrónico personal portátil 4. En la etapa S74, el terminal de usuario 1 transmite, al servidor de verificación 3 por medio de la red de comunicaciones 100, los datos de identificación de hardware, que consisten en la primera combinación de los códigos de identificación y de la segunda combinación de los códigos de identificación, es decir, los datos de identificación, así como la información de posicionamiento, que indica que el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 comparten la misma dirección de red, es decir, la dirección de red asignada al terminal de usuario 1. De este modo, el servidor de verificación 3 obtiene los datos de identificación de hardware y la información de posicionamiento.

En referencia a la Figura 8, se muestra una segunda variante del sistema de autenticación en red. A diferencia del sistema de autenticación en red de la Figura 6, el dispositivo electrónico personal portátil 4 puede ser una tarjeta electrónica, y tiene prealmacenado un código de identificación, el cual se corresponde de manera exclusiva con el dispositivo electrónico personal portátil 4 (la tarjeta electrónica). Además, las interfaces de comunicación inalámbrica de corta distancia 13, 43 pueden usar la tecnología de identificación por radiofrecuencia (RFID). La Figura 9 muestra un quinto procedimiento a realizar entre la etapa S23 y la etapa S24 por el sistema de autenticación en red de la Figura 8, y que ilustra cómo se proporcionan los datos de identificación de hardware y la información de posicionamiento al servidor de verificación 3. El quinto procedimiento incluye las siguientes etapas. En la etapa S91, de manera similar a la etapa S71 de la Figura 7, se transmite la primera solicitud de datos desde el servidor de proveedor de contenido 2 al terminal de usuario 1. En la etapa S92, de manera similar a la etapa S72 de la Figura 7, el terminal de usuario 1 genera la primera combinación de los códigos de identificación, y se transmite la segunda solicitud de datos desde el terminal de usuario 1 al dispositivo electrónico personal portátil 4 usando una comunicación inalámbrica de corta distancia. En la etapa S93, como respuesta a la segunda solicitud de datos del terminal de usuario 1, el dispositivo electrónico personal portátil 4 transmite el código de identificación, que sirve como datos de identificación, al terminal de usuario 1 usando una comunicación inalámbrica de corta distancia. En la etapa S94, el terminal de usuario 1 transmite los datos de identificación de hardware, que consisten en la primera combinación de los códigos de identificación y el código de identificación, es decir, los datos de identificación, y la información de posicionamiento, que indica que el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 están muy próximos entre sí, por medio de la red de comunicaciones 100. De este modo, el servidor de verificación 3 obtiene los datos de identificación de hardware y la información de posicionamiento.

En referencia de nuevo a las Figuras 1 y 2, después de la etapa S24, el método prosigue a la etapa S25, donde, como respuesta a la solicitud de verificación, el servidor de verificación 3 determina si los datos de identificación de hardware obtenidos según el modo mencionado coinciden con los datos de identificación de hardware de referencia 31, los cuales están prealmacenados en el mismo y se corresponden con el identificador de usuario, es decir, la ID de usuario. Si se determina que los datos de identificación de hardware son un subconjunto de los datos de identificación de hardware de referencia 31, el flujo prosigue a la etapa S26. En caso contrario, el flujo se dirige a la etapa S28.

Debe indicarse que, durante un procedimiento de registro previo a la autenticación, el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 aportados por el mismo propietario se registran en el servidor de proveedor de contenido 2, y, en los mismos se cargan, respectivamente, el primer programa de exploración 12, y el segundo programa de exploración 42 (Figuras 1 y 6) o el código de identificación (Figura 8). Después de esto, el primer y el segundo programas de exploración 12, 42 son ejecutados, respectivamente, por el terminal de usuario 1 y el dispositivo electrónico personal portátil 4, para obtener los códigos de identificación de los componentes de hardware del terminal de usuario 1, y los códigos de identificación de los componentes de hardware del dispositivo electrónico personal portátil 4 que constituyen, cooperativamente, los datos de identificación de hardware de referencia 31 correspondientes al identificador de usuario del propietario. En una alternativa, el primer y el segundo programas de exploración 12, 42 pueden obtener los códigos de identificación de ciertos componentes de entre los componentes de hardware de terminal de usuario 1, y los códigos de identificación de ciertos componentes de entre los componentes de hardware del dispositivo electrónico personal portátil 4 para constituir, cooperativamente, los datos de identificación de hardware de referencia 31. Alternativamente, los códigos de identificación obtenidos usando la ejecución del primer programa de exploración

12 y asociados al terminal de usuario 1, el código de identificación cargado en el dispositivo electrónico personal portátil 4 constituyen, cooperativamente, los datos de identificación de hardware de referencia 31 correspondientes al identificador de usuario del propietario. A continuación, los datos de identificación de hardware de referencia 31 se almacenan en el servidor de verificación 3 con fines relativos a la autenticación. Por lo tanto, si se determina que los datos de identificación de hardware son un subconjunto de los datos de identificación de hardware de referencia 31 (o una coincidencia total en el caso alternativo), en la etapa S25, el terminal de usuario 1 manejado por el usuario 5 y el dispositivo electrónico personal portátil 4 llevado por el usuario 5 pertenecen al mismo propietario.

En la etapa S26, el servidor de verificación 3, basándose en la información de posicionamiento, determina si el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 están muy próximos entre sí. Por ejemplo, cuando los primeros datos de posicionamiento generados en las subetapas S32, S43 y S52 de las Figuras 3, 4 y 5, son idénticos a los segundos datos de posicionamiento generados en las subetapas S33, S44 y S53 de las Figuras 3, 4 y 5, cuando la información de posicionamiento transmitida en la subetapa S74 de la Figura 7 indica que el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 comparten la misma dirección de red, o cuando la información de posicionamiento transmitida en la subetapa S94 de la Figura 9 indica que el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 están muy próximos entre sí, el servidor de verificación 4 determina que el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 están muy próximos entre sí, y, a continuación, el flujo prosigue a la etapa S27. En caso contrario, el flujo se dirige a la etapa S28.

Debe indicarse que, cuando el terminal de usuario 1 y el dispositivo electrónico personal portátil 4 están muy próximos entre sí (etapa S26) mientras, en la etapa S25, se resuelve una determinación afirmativa, el usuario 5 se verifica como propietario del terminal de usuario 1 y del dispositivo electrónico personal portátil 4.

En la etapa S27, el servidor de verificación 3 transmite una respuesta de verificación que indica una autenticación satisfactoria de la identidad del usuario 5, al servidor de proveedor de contenido 2, por medio de la red de comunicaciones 100. De este modo, se permite al usuario 5 acceder a datos en el servidor de proveedor de contenido 2.

En la etapa S28, el servidor de verificación 3 transmite una respuesta de verificación que indica una autenticación fallida de la identidad del usuario 5 al servidor de proveedor de contenido 2, por medio de la red de comunicaciones. De este modo, se le deniega al usuario 5 acceso a datos en el servidor de proveedor de contenido 2.

En referencia a la Figura 10, se usa otro sistema de autenticación en red, el cual es una modificación del sistema de autenticación en red de la Figura 1, para implementar la segunda forma de realización preferida de un método de autenticación en red para la identificación segura de la identidad de un usuario 5 de acuerdo con la presente invención. A diferencia del sistema de autenticación en red de la Figura 1, el terminal de usuario 1' del sistema de autenticación en red de la Figura 10 puede ser, aunque sin carácter limitativo, un terminal de punto de venta (POS) o un cajero automático (ATM), y tiene prealmacenados unos primeros datos de posicionamiento 14 correspondientes a una ubicación geográfica del terminal de usuario 1'. Además, el dispositivo electrónico personal portátil 4' es un dispositivo de comunicación personal portátil 4', el cual puede ser, aunque sin carácter limitativo, un teléfono inteligente o un ordenador de tipo tableta. El dispositivo de comunicación personal portátil, 4' incluye un módulo de GPS 41, y tiene prealmacenado un programa de exploración 42'. En esta forma de realización, si el sistema de autenticación en red de la Figura 10 autentica satisfactoriamente la identidad del usuario 5, se permite al usuario 5 acceder a datos en el servidor de proveedor de contenido 2.

La Figura 11 es un diagrama de flujo de la segunda forma de realización preferida del método de autenticación en red que ilustra cómo se verifica la identidad del usuario 5. La segunda forma de realización preferida del método de autenticación en red incluye las siguientes etapas.

En la etapa S10, el usuario 5 introduce datos de inicio de sesión de usuario usando una interfaz de entrada de usuario (no mostrada) del terminal de usuario 1', en un sitio web proporcionado por el servidor de proveedor de contenido 2. A continuación, el terminal de usuario 1' transmite los datos de inicio de sesión de usuario y los primeros datos de posicionamiento al servidor de proveedor de contenido 2, por medio de la red de comunicaciones 100. En esta forma de realización, los datos de inicio de sesión de usuario incluyen una identificación de usuario (ID) que sirve como identificador de usuario, y una contraseña.

En la etapa S11, tras la recepción de los datos de inicio de sesión de usuario y de los primeros datos de posicionamiento del terminal de usuario 1', el servidor de proveedor de contenido 2 comprueba si los datos de inicio de sesión de usuario son correctos. Si el resultado es afirmativo, el flujo prosigue a la etapa S12. En caso contrario, el servidor de proveedor de contenido 2 envía un mensaje de error al terminal de usuario 1' para su visualización en un dispositivo de visualización (no mostrado) del terminal de usuario 1' (etapa S9).

En la etapa S12, el servidor de proveedor de contenido 2 transmite una primera solicitud, que incluye el identificador de usuario, al servidor de verificación 3, por medio de la red de comunicaciones 100. En esta forma

de realización, el servidor de verificación 3 puede considerarse como un tercero designado por el servidor de proveedor de contenido 2 para realizar una autenticación de identificación del hardware.

En la etapa S13, después de la recepción de la primera solicitud del servidor de proveedor de contenido 2, el servidor de verificación 3 recibe además datos de identificación de hardware e información de posicionamiento que están asociados al dispositivo de comunicación personal portátil, 4', desde el dispositivo de comunicación personal portátil, 4', por medio de la red de comunicaciones 100. En un ejemplo, como respuesta a la primera solicitud del servidor de proveedor de contenido 2, el servidor de verificación 3 transmite una segunda solicitud de los datos de identificación de hardware y de los segundos datos de posicionamiento, al dispositivo de comunicación personal portátil, 4', por medio de la red de comunicaciones 100. De este modo, como respuesta a la segunda solicitud del servidor de verificación 3, el dispositivo de comunicación personal portátil, 4', lleva a cabo un posicionamiento de GPS para generar los segundos datos de posicionamiento que se corresponden con una ubicación geográfica actual del dispositivo de comunicación personal portátil, 4', ejecuta el programa de exploración 42' para obtener una combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware (no mostrados) del dispositivo de comunicación personal portátil, 4', que sirve como datos de identificación de hardware, y transmite los segundos datos de posicionamiento y los datos de identificación de hardware al servidor de verificación 3, por medio de la red de comunicaciones 100. En otro ejemplo, el dispositivo de comunicación personal portátil, 4', se puede hacer funcionar para llevar a cabo un posicionamiento de GPS con el fin de obtener los segundos datos de posicionamiento de una manera periódica, para ejecutar el programa de exploración 42' con el fin de obtener la combinación de los códigos de identificación que sirve como datos de identificación de hardware automáticamente, y para transmitir los segundos datos de posicionamiento y los datos de identificación de hardware al servidor de verificación, por medio de la red de comunicaciones 100, de una manera periódica. De este modo, el servidor de verificación 3 recibe los datos de identificación de hardware y los segundos datos de posicionamiento periódicamente.

En la etapa S14, el servidor de verificación 3 determina si los datos de identificación de hardware obtenidos según el modo mencionado son un subconjunto de los datos de identificación de hardware de referencia 31, que están prealmacenados en el servidor de verificación 3 y que se corresponden con el identificador de usuario. Si el resultado de la determinación es afirmativo, el flujo prosigue hacia la etapa S15. En caso contrario, el flujo se dirige a la etapa S18.

En la etapa S15, el servidor de verificación 3 transmite los segundos datos de posicionamiento al servidor de proveedor de contenido 2. Debe indicarse que, cuando el dispositivo de comunicación personal portátil, 4', transmite periódicamente los datos de identificación de hardware y los segundos datos de posicionamiento, los segundos datos de posicionamiento, que son los recibidos más recientemente por el servidor de verificación 3 en la etapa S13 después de la recepción de la primera solicitud del servidor de proveedor de contenido 2, se transmiten al servidor de proveedor de contenido 2.

En la etapa S16, el servidor de proveedor de contenido 2 determina, basándose en los primeros datos de posicionamiento y los segundos datos de posicionamiento, si el terminal de usuario 1' y el dispositivo de comunicación personal portátil, 4' están muy próximos entre sí. Cuando el servidor de proveedor de contenido 2 detecta que los primeros datos de posicionamiento son idénticos a los segundos datos de posicionamiento, el servidor de proveedor de contenido 2 determina que el terminal de usuario 1' y el dispositivo de comunicación personal portátil, 4' están muy próximos entre sí. A continuación, el servidor de proveedor de contenido 2 considera que la identidad del usuario 5 se ha autenticado satisfactoriamente (etapa S17). De este modo, se permite al usuario 5 acceder a datos en el servidor de proveedor de contenido 2 usando el terminal de usuario 1'. En caso contrario, el flujo se dirige a la etapa S19.

En la etapa S18, cuando no se resuelve que los datos de identificación de hardware son un subconjunto de los datos de identificación de hardware de referencia 31, el servidor de verificación 3 transmite una respuesta de verificación fallida al servidor de proveedor de contenido 2.

En la etapa S19, como contestación a la respuesta de verificación fallida del servidor de verificación 3 en la etapa S18, o cuando se determina que el terminal de usuario 1' no está muy próximo al dispositivo de comunicación personal portátil, 4', en la etapa S16, el servidor de proveedor de contenido 2 considera que la autenticación de la identidad del usuario 5 ha fallado. De este modo, se deniega al usuario 5 acceso a datos en el servidor de proveedor de contenido 2.

En resumen, el método de autenticación en red de esta invención utiliza una verificación de identificación de hardware y una verificación de posicionamiento para el terminal de usuario 1, 1' y el dispositivo electrónico personal portátil, 4, 4'. Por consiguiente, resulta relativamente difícil para los piratas informáticos robar simultáneamente información de hardware y de posicionamiento asociada al terminal de usuario 1, 1' y al dispositivo electrónico personal portátil, 4, 4', garantizándose así una verificación segura de la identidad del usuario 5. Además, el propio teléfono inteligente u ordenador de tipo tableta del usuario se utiliza como dispositivo electrónico personal portátil, 4, 4', sin necesidad de dispositivos de verificación de identidad

adicionales. Por lo tanto, se minimizan los costes de autenticación de identidad para el servidor de proveedor de contenido 2.

REIVINDICACIONES

1. Método de autenticación en red para su implementación por medio de un sistema de autenticación en red para la verificación segura de la identidad de un usuario (5), incluyendo el sistema de autenticación en red un terminal de usuario (1) manejado por el usuario (5), un servidor de proveedor de contenido (2), un servidor de verificación (3), y un dispositivo electrónico personal portátil (4) llevado por el usuario (5), estando el terminal de usuario (1), el servidor de proveedor de contenido (2) y el servidor de verificación (3) conectados a una red de comunicaciones (100), teniendo el dispositivo electrónico personal portátil (4) la capacidad de conectarse con la red de comunicaciones (100) y/o de comunicarse inalámbricamente a corta distancia con el terminal de usuario (1), estando dicho método de autenticación en red caracterizado por que comprende las etapas siguientes:

a) tras la recepción de unos datos de inicio de sesión de usuario correctos, que incluyen un identificador de usuario, desde el terminal de usuario (1) por medio de la red de comunicaciones (100), el servidor de proveedor de contenido (2) transmite una solicitud de verificación, que incluye el identificador de usuario, al servidor de verificación (3) por medio de la red de comunicaciones (100);

b) después de la recepción de la solicitud de verificación desde el servidor de proveedor de contenido (2), el servidor de verificación (3) además recibe datos de identificación de hardware e información de posicionamiento que están asociados al terminal de usuario (1) y al dispositivo electrónico personal portátil, (4), por medio de la red de comunicaciones (100);

c) como respuesta a la solicitud de verificación, el servidor de verificación (3) determina si los datos de identificación de hardware obtenidos en la etapa b) coinciden con o son un subconjunto de datos de identificación de hardware de referencia (31), que están prealmacenados en el servidor de verificación (3) y que se corresponden con el identificador de usuario, y resuelve, basándose en la información de posicionamiento, si el terminal de usuario (1) y el dispositivo electrónico personal portátil, (4) están muy próximos entre sí; y

d) tras la detección de la existencia de una coincidencia o de que los datos de identificación de hardware son un subconjunto de los datos de identificación de hardware de referencia (31) y la resolución de que el terminal de usuario (1) y el dispositivo electrónico personal portátil, (4) están muy próximos entre sí, el servidor de verificación (3) transmite una respuesta de verificación que indica una autenticación satisfactoria de la identidad del usuario (5), al servidor de proveedor de contenido (2) por medio de la red de comunicaciones (100).

2. Método de autenticación en red según la reivindicación 1, estando el dispositivo electrónico personal portátil, (4) conectado a la red de comunicaciones (100), siendo dos direcciones de red diferentes, respectivamente, asignadas al terminal de usuario (1) y al dispositivo electrónico personal portátil (4), estando además el método de autenticación en red caracterizado por que comprende, entre las etapas a) y b), las etapas siguientes:

e) el servidor de proveedor de contenido (2) transmite una primera solicitud de datos al terminal de usuario (1) por medio de la red de comunicaciones (100);

f) como respuesta a la primera solicitud de datos del servidor de proveedor de contenido (2), el terminal de usuario (1) lleva a cabo un posicionamiento por el sistema de posicionamiento global (GPS) para obtener unos primeros datos de posicionamiento correspondientes a una ubicación geográfica del terminal de usuario (1), ejecuta un primer programa de exploración (12) preinstalado en el mismo, para obtener una primera combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del terminal de usuario (1), y transmite los primeros datos de posicionamiento y la primera combinación de los códigos de identificación al servidor de verificación (3) por medio de la red de comunicaciones (100); y

g) el dispositivo electrónico personal portátil (4) lleva a cabo un posicionamiento de GPS para obtener unos segundos datos de posicionamiento correspondientes a una ubicación geográfica actual del dispositivo electrónico personal portátil (4), ejecuta un segundo programa de exploración (42) preinstalado en el mismo, para obtener una segunda combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del dispositivo electrónico personal portátil (4), y transmite los segundos datos de posicionamiento y la segunda combinación de los códigos de identificación al servidor de verificación (3) por medio de la red de comunicaciones (100); y

caracterizado por que la primera combinación de los códigos de identificación transmitida en la etapa f) y la segunda combinación de los códigos de identificación transmitida en la etapa g), constituyen cooperativamente los datos de identificación de hardware recibidos por el servidor de verificación (3) en la etapa b), y los primeros datos de posicionamiento transmitidos en la etapa f) y los segundos datos de posicionamiento transmitidos en la etapa g) constituyen cooperativamente la información de posicionamiento recibida por el servidor de verificación (3) en la etapa b).

3. Método de autenticación en red según la reivindicación 2, caracterizado por que:

en la etapa e), el servidor de proveedor de contenido (2) además transmite una segunda solicitud de datos al dispositivo electrónico personal portátil (4) por medio de la red de comunicaciones (100); y

en la etapa g), el dispositivo electrónico personal portátil (100) lleva a cabo un posicionamiento de GPS y ejecuta el segundo programa de exploración (42) como respuesta a la recepción de la segunda solicitud de datos desde el servidor de proveedor de contenido (2).

4. Método de autenticación en red según la reivindicación 2, caracterizado por que además, antes de la etapa g), comprende la etapa siguiente:

f') como respuesta a la recepción de la solicitud de verificación desde el servidor de proveedor de contenido (2), el servidor de verificación (3) transmite una segunda solicitud de datos al dispositivo electrónico personal portátil (4) por medio de la red de comunicaciones (100); y

caracterizado por que, en la etapa g), el dispositivo electrónico personal portátil (4) lleva a cabo un posicionamiento de GPS y ejecuta el segundo programa de exploración (42) como respuesta a la recepción de la segunda solicitud de datos desde el servidor de verificación (3).

5. Método de autenticación en red según la reivindicación 2, caracterizado por que:

en la etapa g), el dispositivo electrónico personal portátil (4) lleva a cabo un posicionamiento de GPS para obtener los segundos datos de posicionamiento de una manera periódica, ejecuta automáticamente el segundo programa de exploración (42) para obtener la segunda combinación de los códigos de identificación, y transmite los segundos datos de posicionamiento y la segunda combinación de los códigos de identificación al servidor de verificación (3) de una manera periódica; y

la primera combinación de los códigos de identificación transmitida en la etapa f), y la segunda combinación de los códigos de identificación, que es la transmitida más recientemente al servidor de verificación (3) en la etapa g) después de que el servidor de verificación (3) haya recibido la solicitud de verificación constituyen cooperativamente los datos de identificación de hardware, y los primeros datos de posicionamiento transmitidos en la etapa f), y los segundos datos de posicionamiento, que son los transmitidos más recientemente al servidor de verificación (3) en la etapa g) después de que el servidor de verificación (3) haya recibido la solicitud de verificación constituyen cooperativamente la información de posicionamiento.

6. Método de autenticación en red según la reivindicación 2, caracterizado por que, en la etapa c), el servidor de verificación (3) determina que el terminal de usuario (1) y el dispositivo electrónico personal portátil (4) están muy próximos entre sí cuando los primeros datos de posicionamiento son idénticos a los segundos datos de posición.

7. Método de autenticación en red según la reivindicación 1, teniendo el dispositivo electrónico personal portátil (4) la capacidad de comunicarse inalámbricamente a corta distancia con el terminal de usuario (1), estando además el método de autenticación en red caracterizado, entre las etapas (a) y (b) por que comprende las siguientes etapas:

h) el servidor de proveedor de contenido (2) transmite una primera solicitud de datos al terminal de usuario (1) por medio de la red de comunicaciones (100);

i) como respuesta a la primera solicitud de datos del servidor de proveedor de contenido (2), el terminal de usuario (1) ejecuta un primer programa de exploración (12) preinstalado en el mismo, para obtener una primera combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del terminal de usuario (1), y, tras el establecimiento de un enlace de comunicación inalámbrica de corta distancia con el dispositivo electrónico personal portátil (4), transmite una segunda solicitud de datos al dispositivo electrónico personal portátil (4) a través del enlace de comunicación inalámbrica de corta distancia;

j) como respuesta a la segunda solicitud de datos del terminal de usuario (1), el dispositivo electrónico personal portátil (4) transmite datos de identificación asociados al mismo al terminal de usuario (1) a través del enlace de comunicación inalámbrica de corta distancia; y

k) el terminal de usuario (1) transmite los datos de identificación de hardware, que consisten en la primera combinación de los códigos de identificación y los datos de identificación, y la información de posicionamiento al servidor de verificación (3) por medio de la red de comunicaciones (100).

8. Método de autenticación en red según la reivindicación 7, caracterizado por que, en la etapa j), el dispositivo electrónico personal portátil (4) ejecuta un segundo programa de exploración (42) preinstalado en el mismo para obtener una segunda combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del dispositivo electrónico personal portátil (4), sirviendo la segunda combinación de los códigos de identificación como datos de identificación.

9. Método de autenticación en red según la reivindicación 8, caracterizado por que, en la etapa c), el servidor de verificación (3) determina que el terminal de usuario (1) y el dispositivo electrónico personal portátil (4) están muy próximos entre sí cuando la información de posicionamiento indica que el terminal de usuario (1) y el dispositivo electrónico personal portátil (4) comparten la misma dirección de red.

10. Método de autenticación en red según la reivindicación 7, siendo el dispositivo electrónico personal portátil (4) una tarjeta electrónica, caracterizado por que:

en la etapa j), los datos de identificación son un código de identificación, que está prealmacenado en la tarjeta electrónica y que se corresponde de manera exclusiva con esta última; y

en la etapa k), la información de posicionamiento indica que el terminal de usuario (1) y el dispositivo electrónico personal portátil (4) están muy próximos entre sí.

11. Método de autenticación en red para su implementación por medio de un sistema de autenticación en red para la verificación segura de la identidad de un usuario (5), incluyendo el sistema de autenticación en red un terminal de usuario (1) manejado por el usuario (5), un servidor de proveedor de contenido (2), un servidor de verificación (3), y un dispositivo de comunicación personal portátil (4') llevado por el usuario (5), estando el terminal de usuario (1), el servidor de proveedor de contenido (2), el servidor de verificación (3) y el dispositivo de comunicación personal portátil (4') conectados a una red de comunicaciones (100), estando dicho método de autenticación en red caracterizado por que comprende las etapas siguientes:

a) tras la recepción de unos datos de inicio de sesión de usuario correctos que incluyen un identificador de usuario, y de unos primeros datos de posicionamiento correspondientes a una ubicación geográfica del terminal de usuario (1) desde el terminal de usuario (1) por medio de la red de comunicaciones (100), el servidor de proveedor de contenido (2) transmite al servidor de verificación (3) una primera solicitud, que incluye el identificador de usuario, de unos segundos datos de posicionamiento correspondientes a una ubicación geográfica actual del dispositivo de comunicación personal portátil (4'), por medio de la red de comunicaciones;

b) tras la recepción de la primera solicitud desde el servidor de proveedor de contenido (2), el servidor de verificación (3) además recibe unos datos de identificación de hardware y segundos datos de posicionamiento que están asociados al dispositivo de comunicación personal portátil (4') desde el dispositivo de comunicación personal portátil (4'), por medio de la red de comunicaciones (100);

c) el servidor de verificación (3) determina si los datos de identificación de hardware obtenidos en la etapa b) coinciden con o son un subconjunto de datos de identificación de hardware de referencia (31), que están prealmacenados en el servidor de verificación (3) y que se corresponden con el identificador de usuario, y transmite los segundos datos de posicionamiento al servidor de proveedor de contenido (2) si existe una coincidencia o si los datos de identificación de hardware son un subconjunto de los datos de identificación de hardware de referencia (31); y

d) tras la recepción de los segundos datos de posicionamiento desde el servidor de verificación (3), el servidor de proveedor de contenido (2), basándose en los primeros datos de posicionamiento recibidos por el mismo en la etapa a) y en los segundos datos de posicionamiento transmitidos al mismo en la etapa c), resuelve si el terminal de usuario (1) y el dispositivo de comunicación personal portátil (4') están muy próximos entre sí, y resuelve una autenticación satisfactoria de la identidad del usuario (5) tras resolver que el terminal de usuario (1) y el dispositivo de comunicación personal portátil (4') están muy próximos entre sí.

12. Método de autenticación en red según la reivindicación 11, estando además caracterizado, entre las etapas a) y b), por que comprende las etapas siguientes:

e) como respuesta a la primera solicitud del servidor de proveedor de contenido (2), el servidor de verificación (3) transmite una segunda solicitud de los datos de identificación de hardware y los segundos datos de posicionamiento al dispositivo de comunicación personal portátil (4') por medio de la red de comunicaciones (100); y

f) como respuesta a la segunda solicitud del servidor de verificación (3), el dispositivo de comunicación personal portátil (4') lleva a cabo una posicionamiento de GPS para generar los segundos datos de posicionamiento que se corresponden con una ubicación geográfica actual del dispositivo de comunicación

personal portátil (4'), ejecuta un programa de exploración (42') preinstalado en el mismo para obtener una combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del dispositivo de comunicación personal portátil (4'), que sirve como datos de identificación de hardware, y transmite los segundos datos de posicionamiento y los datos de identificación de hardware al servidor de verificación (3) por medio de la red de comunicaciones (100).

13. Método de autenticación en red según la reivindicación 11, caracterizado por que además comprende la etapa siguiente:

g) el dispositivo de comunicación personal portátil (4') lleva a cabo un posicionamiento de GPS para generar los segundos datos de posicionamiento de una manera periódica, y ejecuta un programa de exploración (42') preinstalado en el mismo para obtener una combinación de códigos de identificación de ciertos componentes de entre una pluralidad de componentes de hardware del dispositivo de comunicación personal portátil (4'), que sirve como datos de identificación de hardware automáticamente, y transmite los segundos datos de posicionamiento y los datos de identificación de hardware al servidor de verificación (3) por medio de la red de comunicaciones (100) de una manera periódica; y

caracterizado por que, en la etapa c), los segundos datos de posicionamiento, que son los recibidos más recientemente por el servidor de verificación (3) en la etapa b) después de la recepción de la primera solicitud desde el servidor de proveedor de contenido (2), se transmiten al servidor de proveedor de contenido (2).

14. Método de autenticación en red según la reivindicación 11, caracterizado por que, en la etapa d), el servidor de proveedor de contenido (2) resuelve que el terminal de usuario y el dispositivo de comunicación personal portátil (4') están muy próximos entre sí cuando los primeros datos de posicionamiento son idénticos a los segundos datos de posicionamiento.

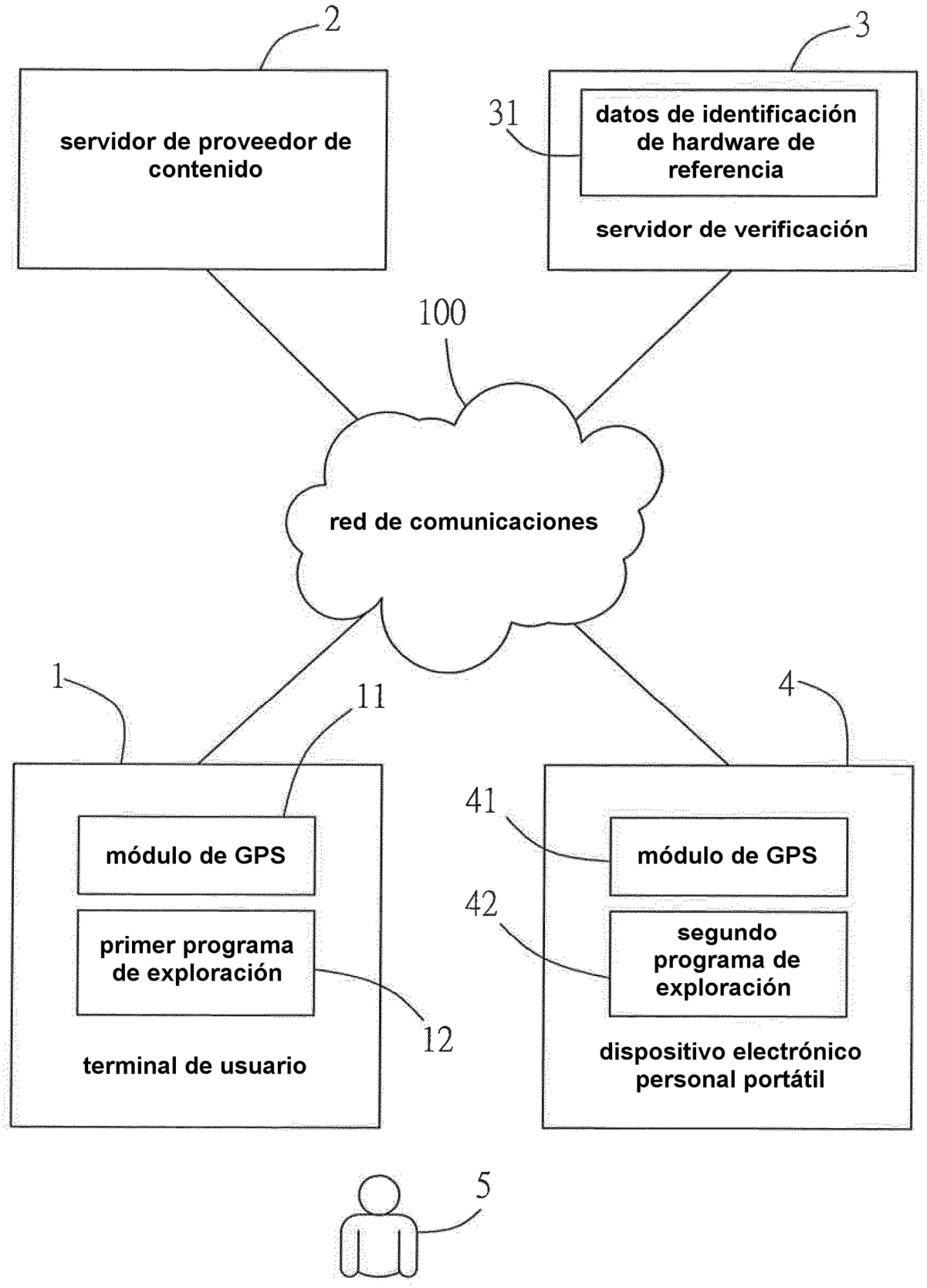
2
servidor de proveedor de contenido
3
31
datos de identificación de hardware de referencia
servidor de verificación
100
red de comunicaciones
1
11
módulo de GPS
primer programa de exploración
12
terminal de usuario
4
41
módulo de GPS
42
segundo programa de exploración
dispositivo electrónico personal portátil
5

FIG. 1

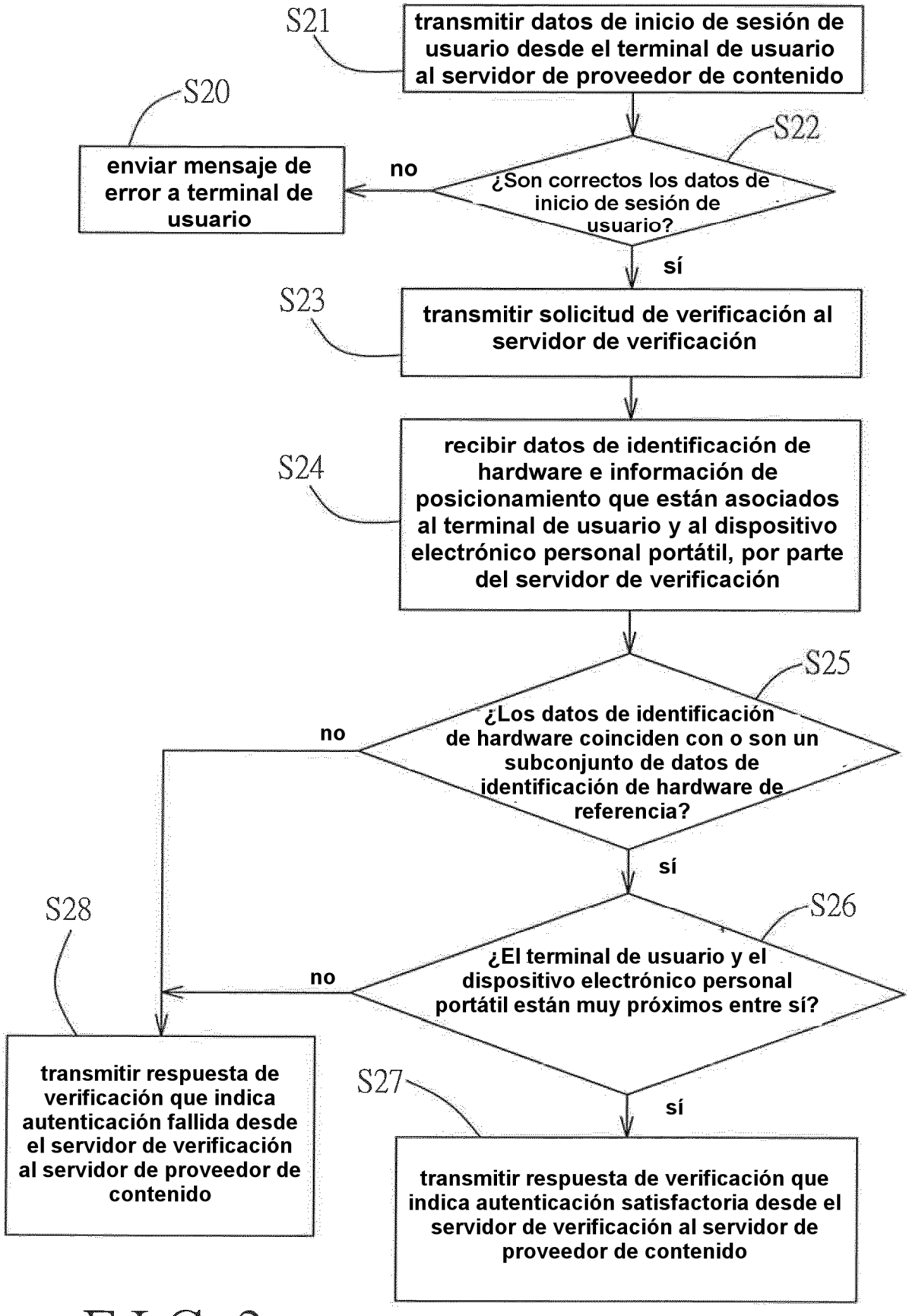
S21
transmitir datos de inicio de sesión de usuario desde el terminal de usuario al servidor de proveedor de contenido
S22
¿Son correctos los datos de inicio de sesión de usuario?
no
S20
enviar mensaje de error a terminal de usuario
sí
S23
transmitir solicitud de verificación al servidor de verificación
S24
recibir datos de identificación de hardware e información de posicionamiento que están asociados al terminal de usuario y al dispositivo electrónico personal portátil, por parte del servidor de verificación
S25
¿Los datos de identificación de hardware coinciden con o son un subconjunto de datos de identificación de hardware de referencia?
no
sí
S26
¿El terminal de usuario y el dispositivo electrónico personal portátil están muy próximos entre sí?
no
S28
transmitir respuesta de verificación que indica autenticación fallida desde el servidor de verificación al servidor de proveedor de contenido
sí
S27
transmitir respuesta de verificación que indica autenticación satisfactoria desde el servidor de verificación al servidor de proveedor de contenido

FIG. 2

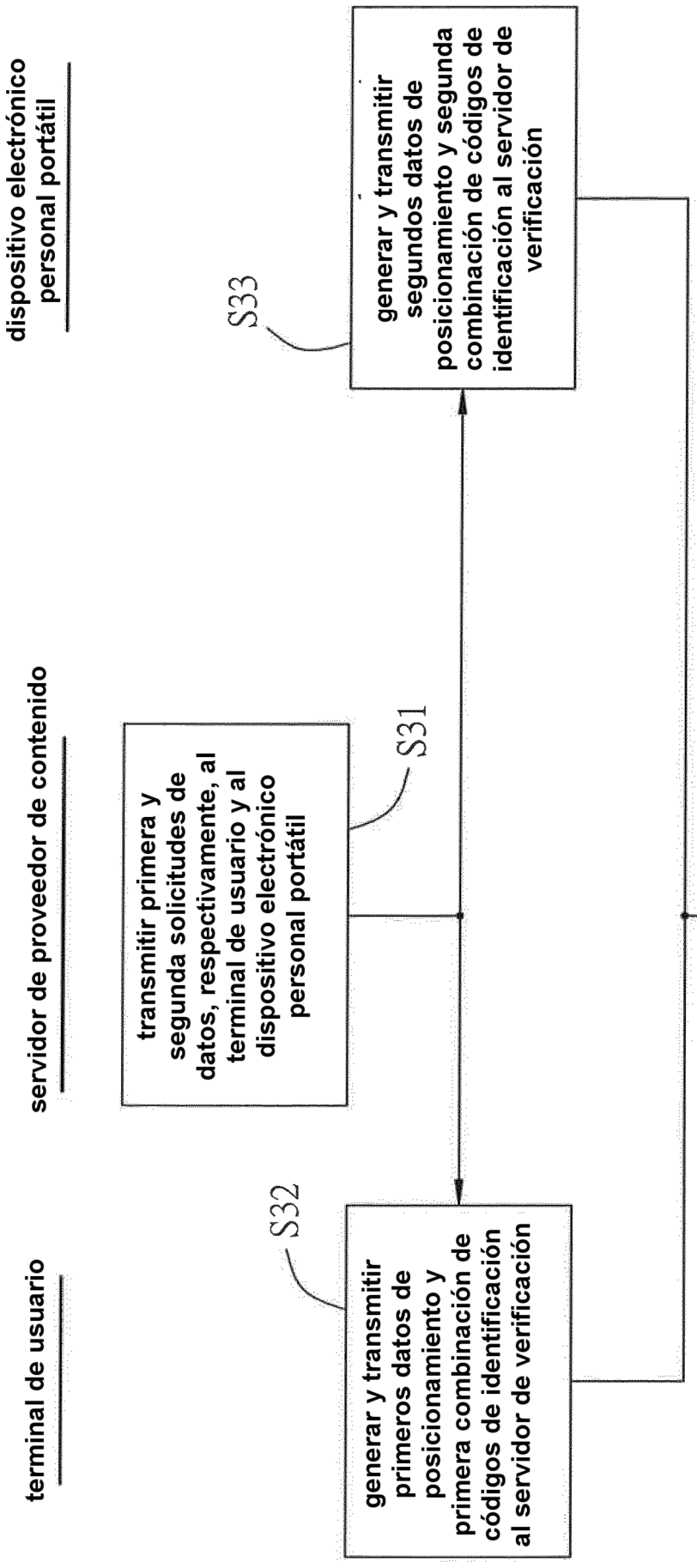
terminal de usuario
servidor de proveedor de contenido
dispositivo electrónico personal portátil
generar y transmitir primeros datos de posicionamiento y primera combinación de códigos de identificación al servidor de verificación
S32
transmitir primera y segunda solicitudes de datos, respectivamente, al terminal de usuario y al dispositivo electrónico personal portátil
S31
generar y transmitir segundos datos de posicionamiento y segunda combinación de códigos de identificación al servidor de verificación
S33
a S25

FIG. 3

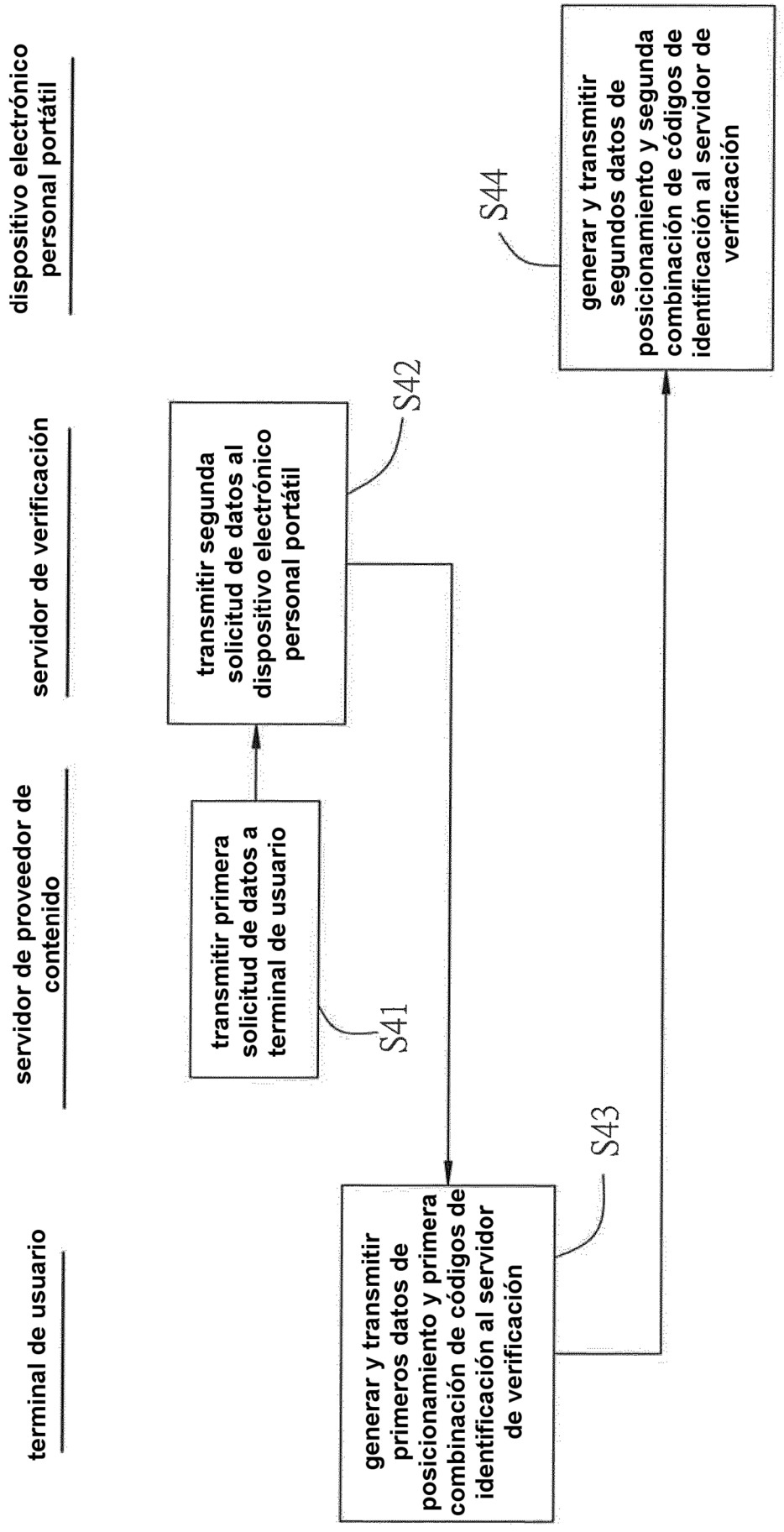
terminal de usuario
servidor de proveedor de contenido
servidor de verificación
dispositivo electrónico personal portátil
transmitir primera solicitud de datos a terminal de usuario
S41
transmitir segunda solicitud de datos al dispositivo electrónico personal portátil
S42
generar y transmitir primeros datos de posicionamiento y primera combinación de códigos de identificación al servidor de verificación
S43
generar y transmitir segundos datos de posicionamiento y segunda combinación de códigos de identificación al servidor de verificación
S44

FIG. 4

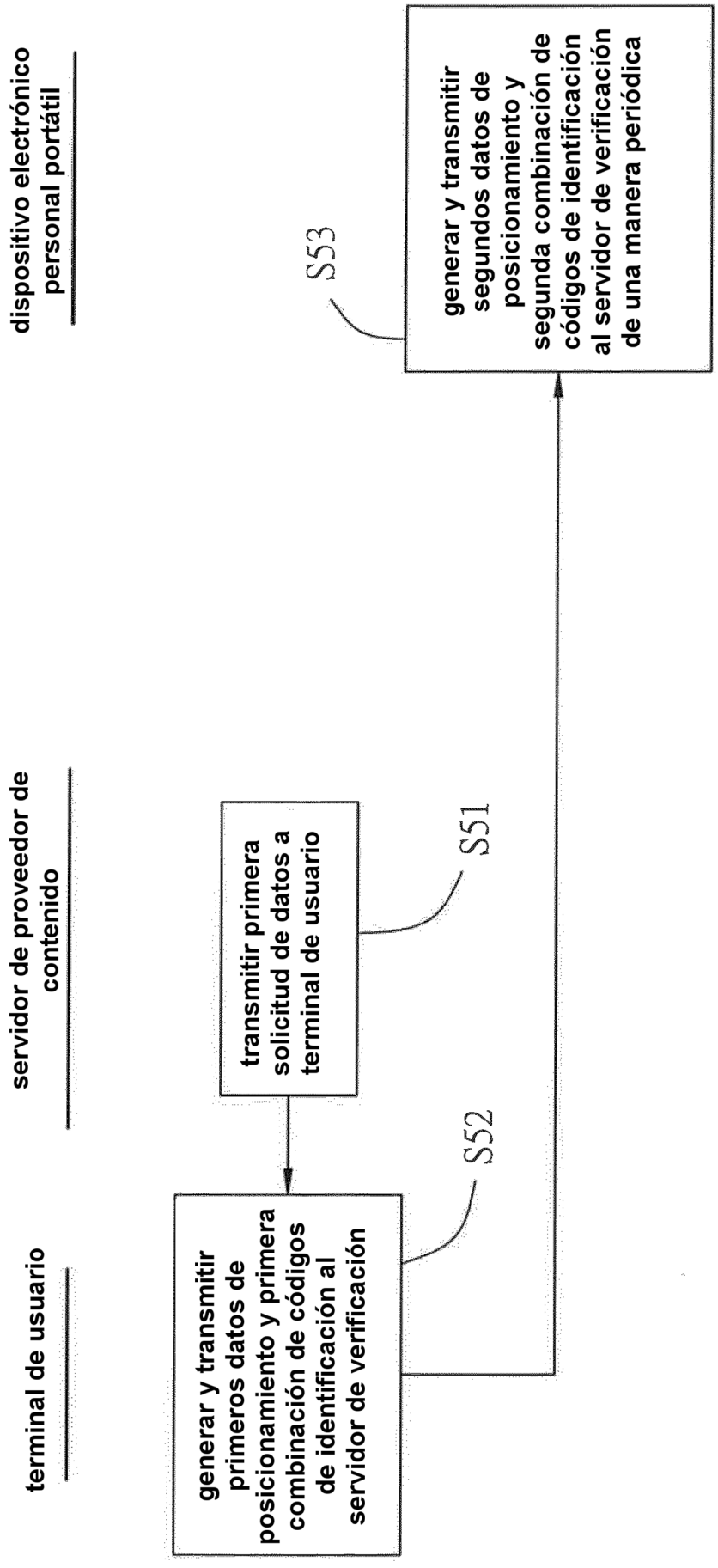
terminal de usuario
servidor de proveedor de contenido
dispositivo electrónico personal portátil
generar y transmitir primeros datos de posicionamiento y primera combinación de códigos de identificación al servidor de verificación
S52
transmitir primera solicitud de datos a terminal de usuario
S51
generar y transmitir segundos datos de posicionamiento y segunda combinación de códigos de identificación al servidor de verificación de una manera periódica
S53

FIG. 5

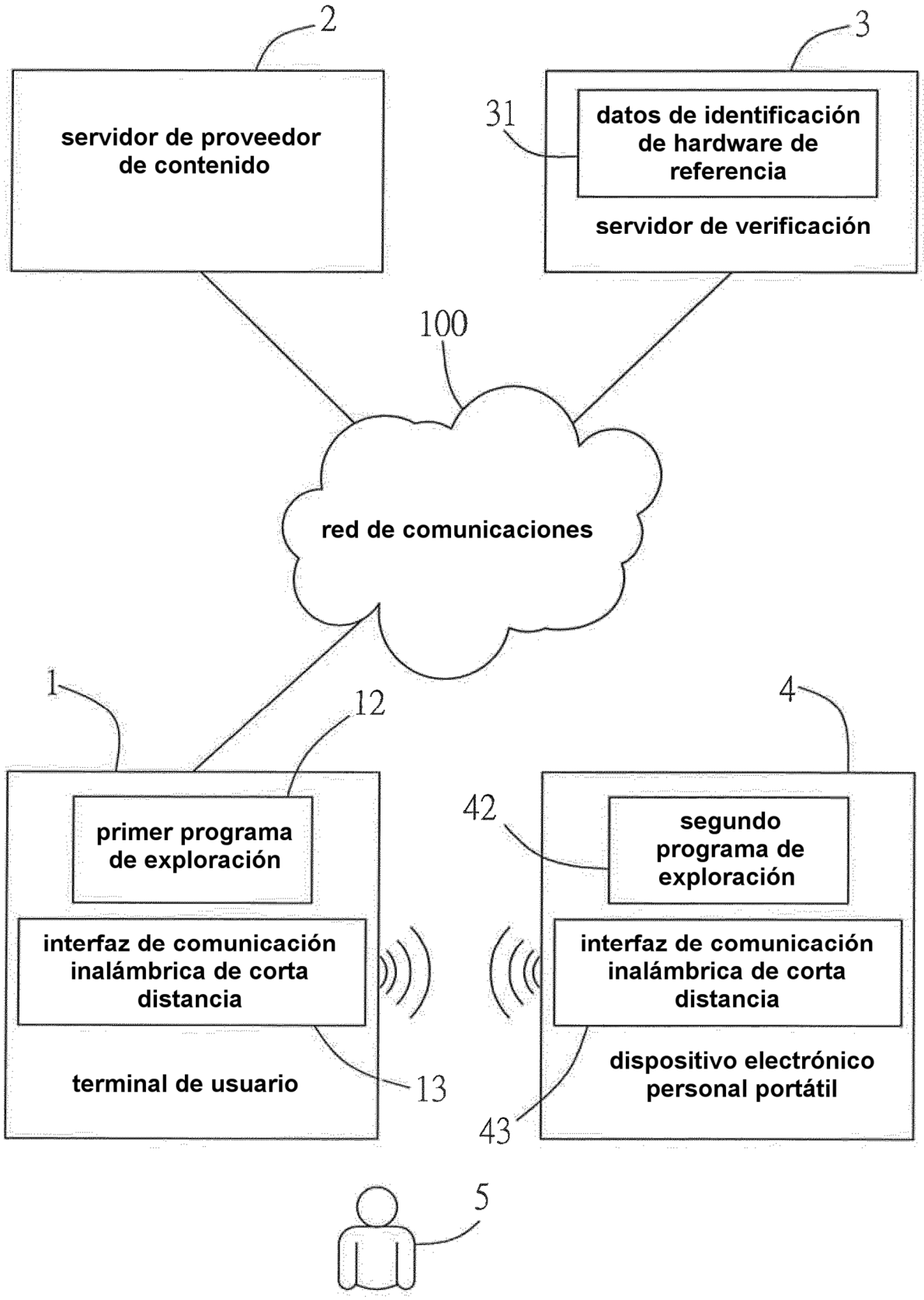
2
servidor de proveedor de contenido
3
31
datos de identificación de hardware de referencia
servidor de verificación
100
red de comunicaciones
1
12
primer programa de exploración
interfaz de comunicación inalámbrica de corta distancia
terminal de usuario
13
4
42
segundo programa de exploración
interfaz de comunicación inalámbrica de corta distancia
dispositivo electrónico personal portátil
43
5

FIG. 6

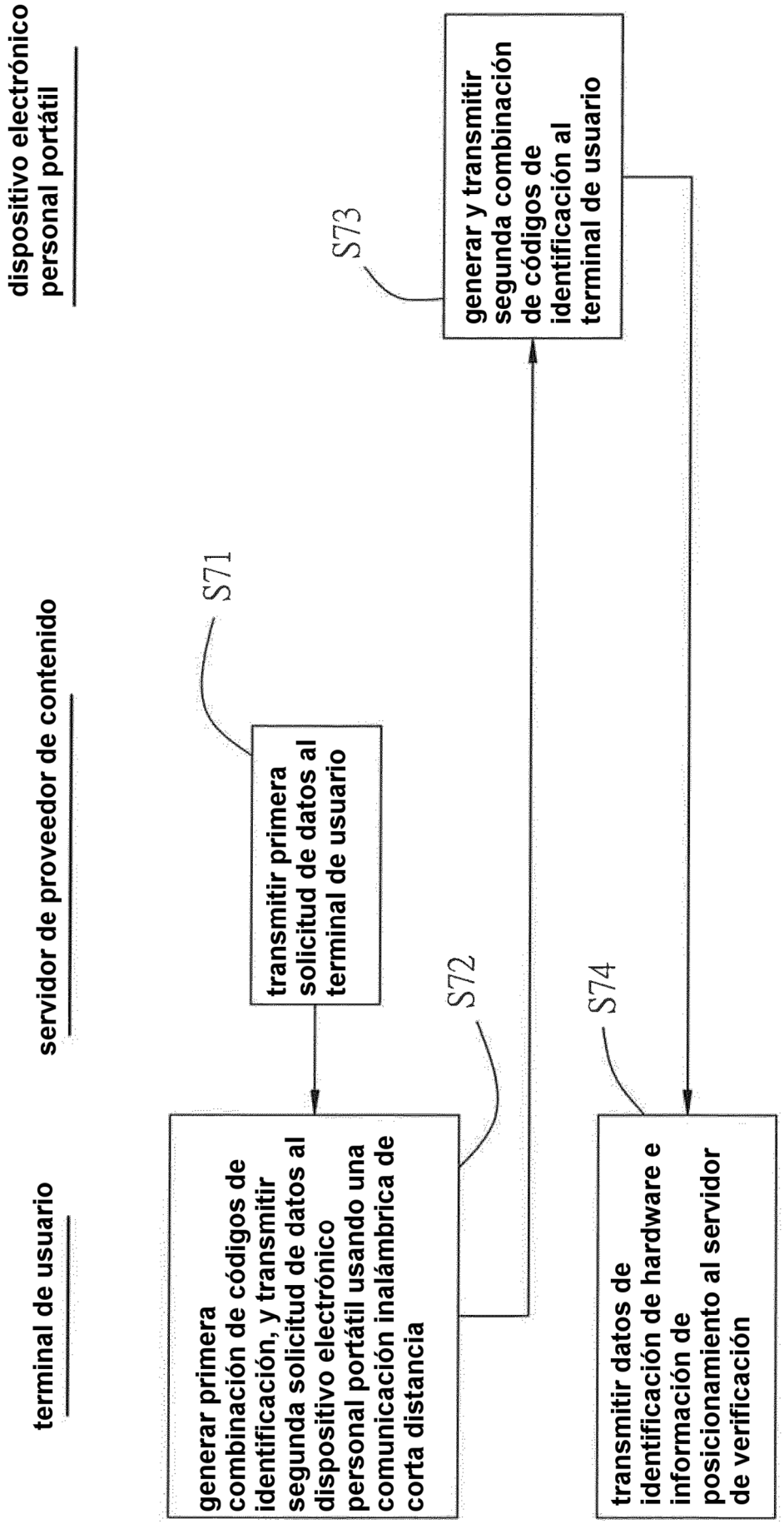
dispositivo electrónico personal portátil
servidor de proveedor de contenido
terminal de usuario
S71
transmitir primera solicitud de datos al terminal de usuario
S72
generar primera combinación de códigos de identificación, y transmitir segunda solicitud de datos al dispositivo electrónico personal portátil usando una comunicación inalámbrica de corta distancia
S73
generar y transmitir segunda combinación de códigos de identificación al terminal de usuario
S74
transmitir datos de identificación de hardware e información de posicionamiento al servidor de verificación

FIG. 7

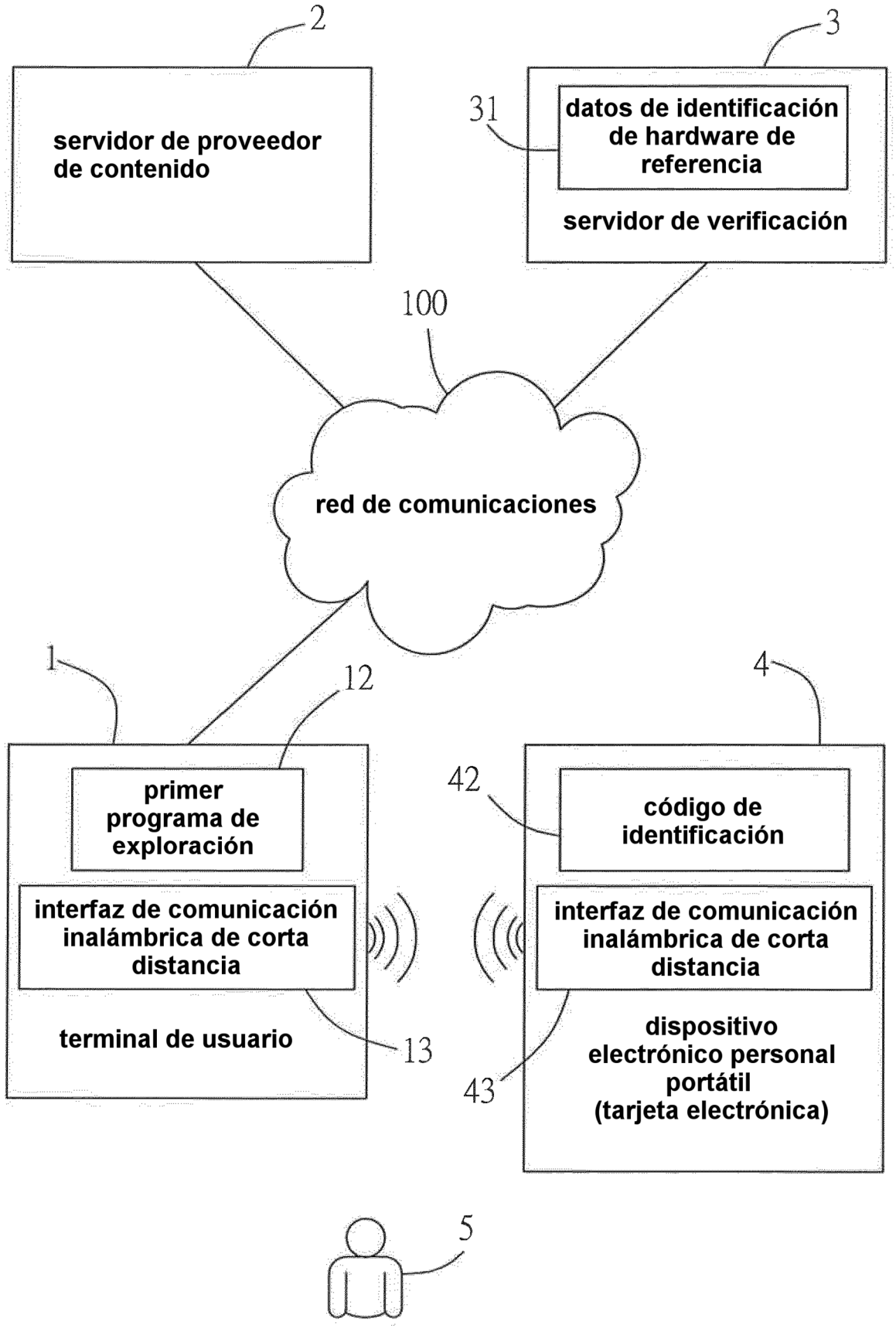
2
servidor de proveedor de contenido
3
31
datos de identificación de hardware de referencia
servidor de verificación
100
red de comunicaciones
1
12
primer programa de exploración
interfaz de comunicación inalámbrica de corta distancia
terminal de usuario
13
4
42
código de identificación
interfaz de comunicación inalámbrica de corta distancia
dispositivo electrónico personal portátil (tarjeta electrónica)
43
5

FIG. 8

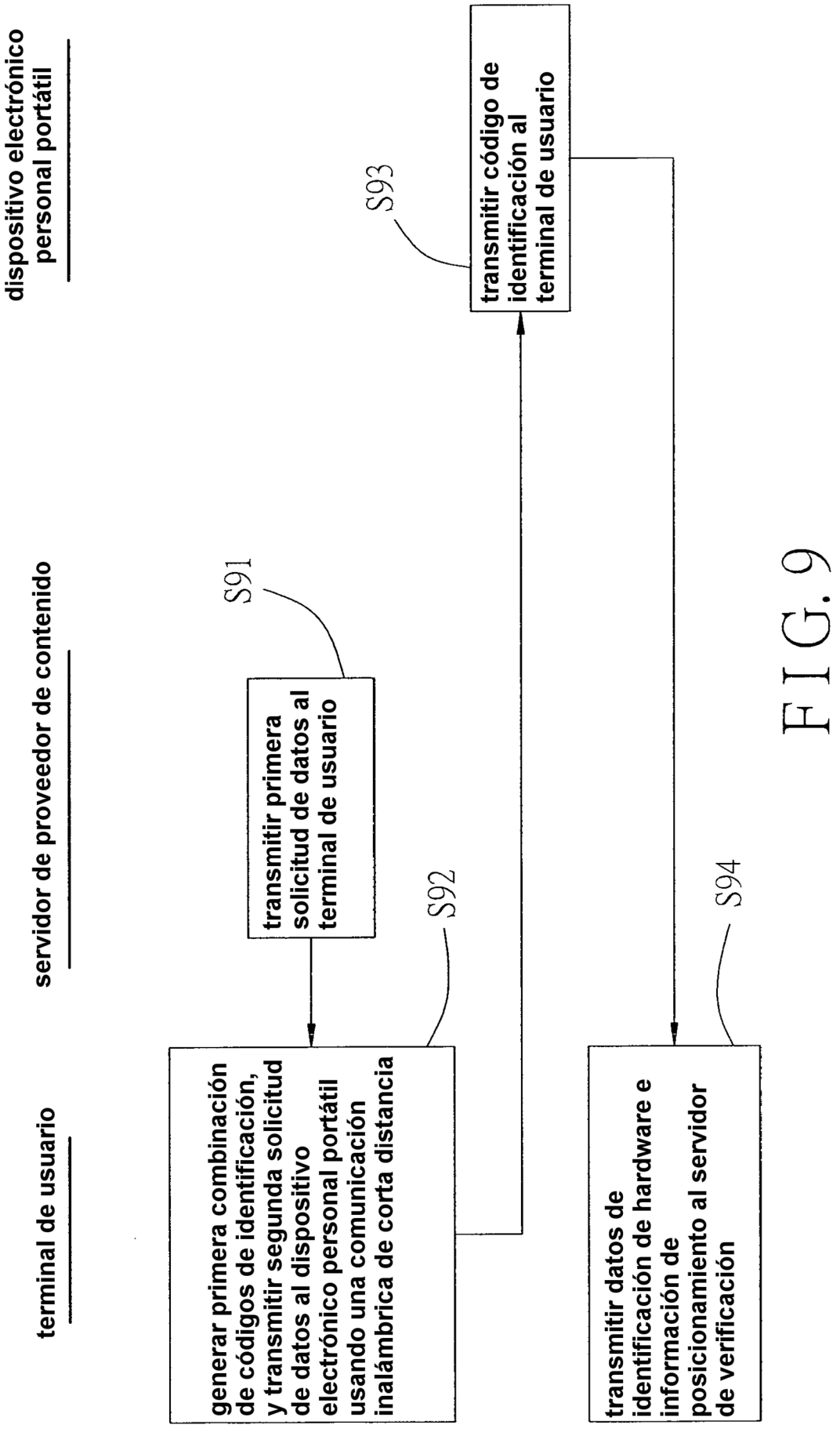
terminal de usuario
servidor de proveedor de contenido
dispositivo electrónico personal portátil
generar primera combinación de códigos de identificación, y transmitir segunda solicitud de datos al dispositivo electrónico personal portátil usando una comunicación inalámbrica de corta distancia
S91
transmitir primera solicitud de datos al terminal de usuario
S92
S93
transmitir código de identificación al terminal de usuario
S94
transmitir datos de identificación de hardware e información de posicionamiento al servidor de verificación

FIG. 9

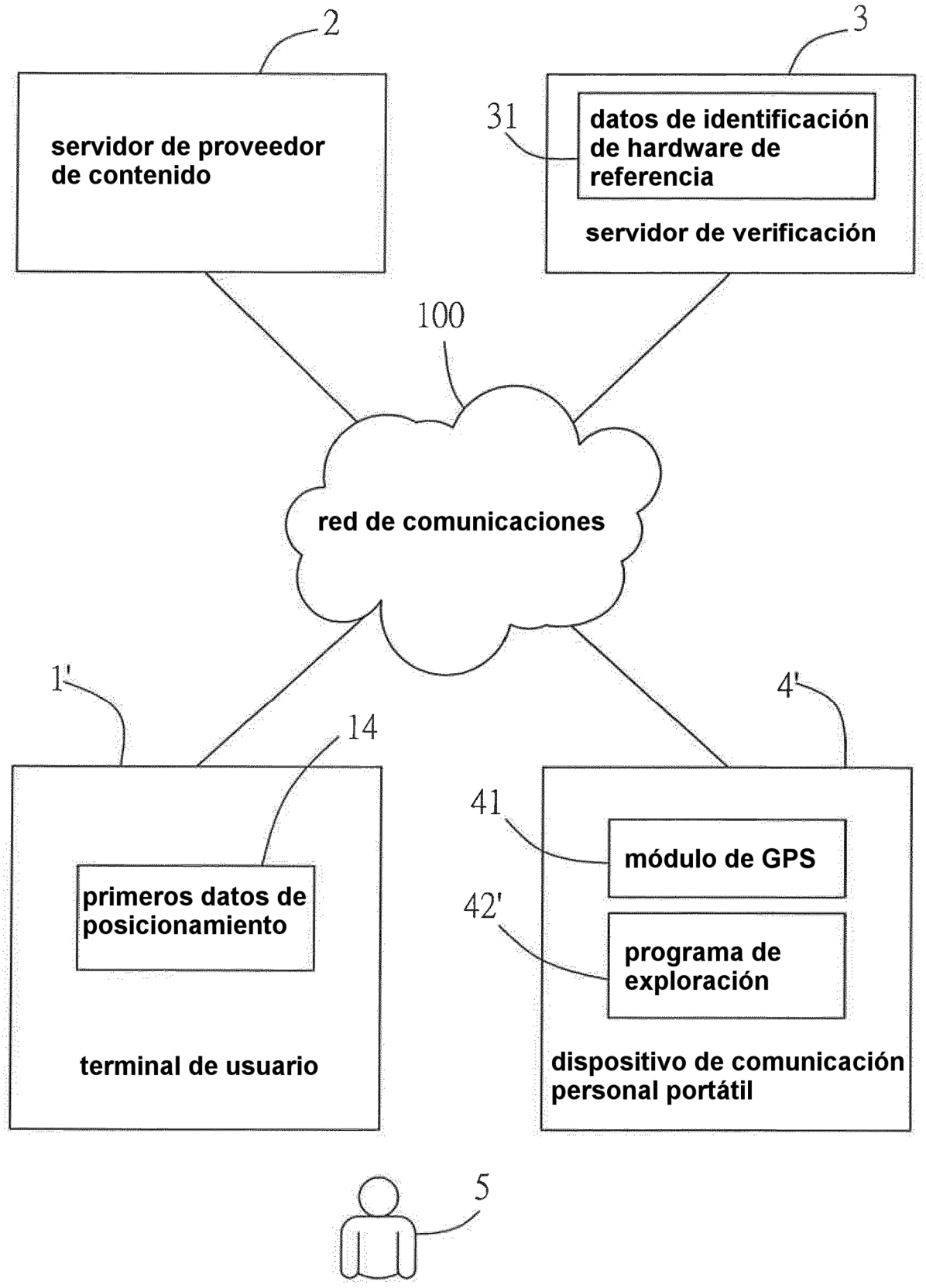
2
servidor de proveedor de contenido
3
31
datos de identificación de hardware de referencia
servidor de verificación
100
red de comunicaciones
1'
14
primeros datos de posicionamiento
terminal de usuario
4'
41
módulo de GPS
42'
programa de exploración
dispositivo de comunicación personal portátil
5

FIG. 10

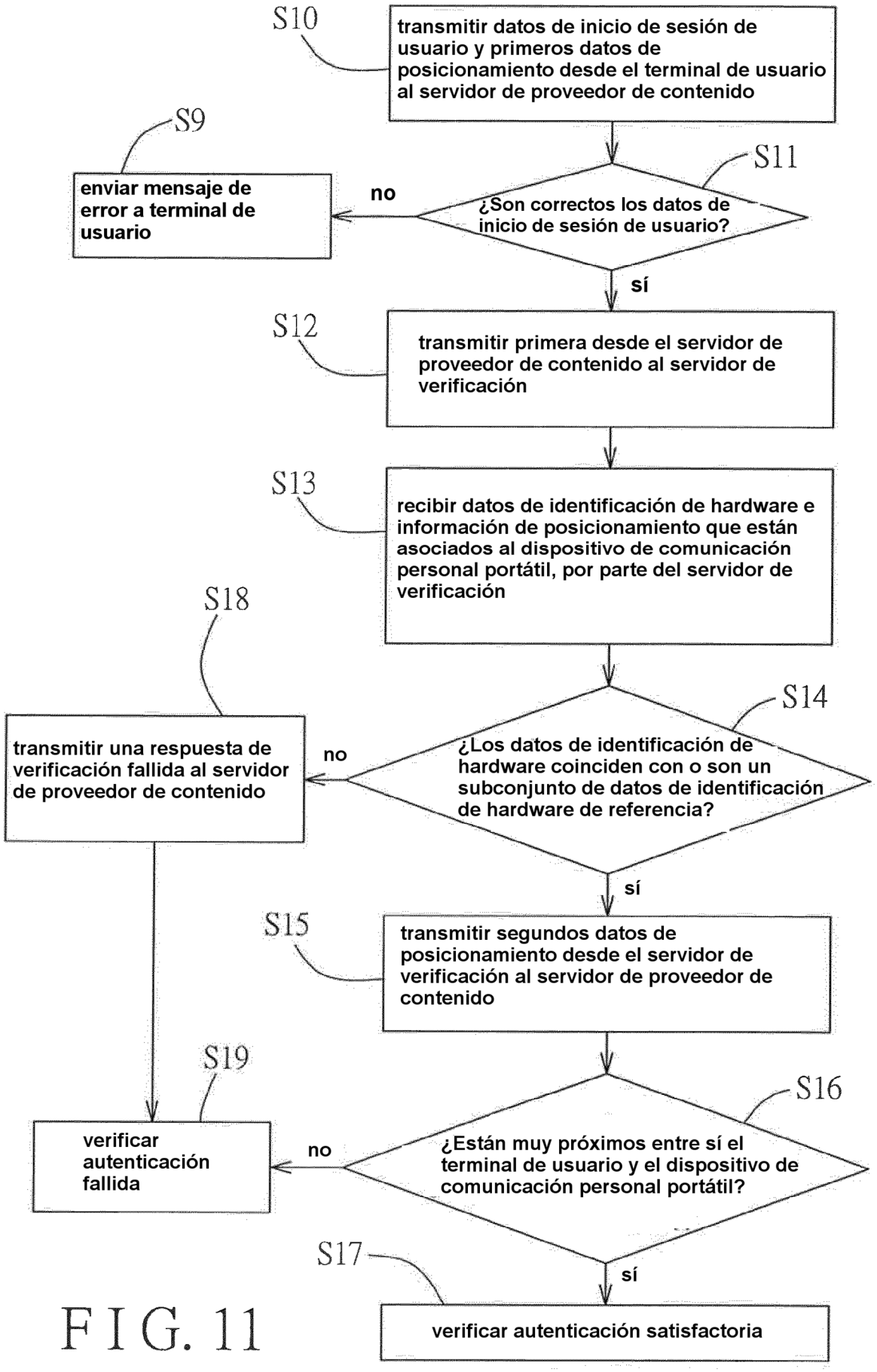
S10
transmitir datos de inicio de sesión de usuario y primeros datos de posicionamiento desde el terminal de usuario al servidor de proveedor de contenido
S11
¿Son correctos los datos de inicio de sesión de usuario?
no
S9
enviar mensaje de error a terminal de usuario
sí
S12
transmitir primera desde el servidor de proveedor de contenido al servidor de verificación
S13
recibir datos de identificación de hardware e información de posicionamiento que están asociados al dispositivo de comunicación personal portátil, por parte del servidor de verificación
S14
¿Los datos de identificación de hardware coinciden con o son un subconjunto de datos de identificación de hardware de referencia?
no
S18
transmitir una respuesta de verificación fallida al servidor de proveedor de contenido
sí
S15
transmitir segundos datos de posicionamiento desde el servidor de verificación al servidor de proveedor de contenido
S16
¿Están muy próximos entre sí el terminal de usuario y el dispositivo de comunicación personal portátil?
no
S19
verificar autenticación fallida
sí
S17
verificar autenticación satisfactoria

FIG. 11