(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 581 911**

(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 14157508 (4)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2016 EP 2916509**

(54) Título: **Método de autentificación en red para verificación segura de identidades de usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.09.2016

(73) Titular/es:

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

(72) Inventor/es:

LIN, MAW-TSONG y
SKYGEBJERG, PER

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Método de autentificación en red para verificación segura de identidades de usuario.

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

En la actualidad, se están popularizando de manera creciente diversos servicios web, tales como los servicios en la nube. Para proteger los servicios web, es absolutamente necesaria una verificación de las identidades de usuario.

No obstante, debido al número creciente de usuarios y delitos en internet, y a la evolución continua de las técnicas delictivas, por ejemplo, es necesario que los proveedores de contenidos de Internet (ICP) proporcionen a cada usuario un dispositivo de verificación de identidad, por ejemplo, un dispositivo USB cargado con un certificado de infraestructura de clave pública (PKI), una tarjeta electrónica de circuito integrado (IC) o un *token* dinámico. Así, el coste del servicio de cliente por la personalización, la distribución y la resolución de problemas es considerable. Además, la necesidad del usuario de recordar la ID de usuario y la contraseña para cada uno de los diferentes ICPs y tener que disponer de diferentes dispositivos de verificación de identidad para los diferentes ICPs resulta bastante incómoda. Por otra parte, para los diferentes ICP, puede producirse una duplicación de la inversión en la autentificación de las identidades de usuario.

El documento EP 2 355 443, 10 de agosto de 2011 (10-8-2011), da a conocer un método de autentificación en red que se implementa utilizando un dispositivo de autentificación en red y un extremo de usuario para autentificar el extremo de usuario. El extremo de usuario almacena un programa de terminal e incluye una pluralidad de componentes de hardware cada uno de los cuales tiene un código de identificación exclusivo.

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

De acuerdo con la presente invención, se proporciona un método de autentificación en red para su implementación utilizando un terminal de usuario, una unidad de descarga, un servidor de proveedor de contenidos y una pluralidad de servidores de verificación de identidad para la verificación segura de la identidad de un usuario del terminal de usuario. El método de autentificación en red de esta invención comprende las siguientes etapas:

a) el terminal de usuario descarga un programa de exploración ("scan") y una clave pública asimétrica desde la unidad de descarga;

b) cada uno de los servidores de verificación de identidad descarga de la unidad de descarga un conjunto respectivo de información cifrada que está firmado con una clave privada asimétrica y que incluye una dirección web cifrada del servidor de verificación de identidades, y almacena datos de exploración de hardware de referencia que están asociados al terminal de usuario y que se corresponden de manera exclusiva con un identificador de usuario del usuario mencionado;

c) como respuesta a una solicitud de inicio de sesión de usuario desde el terminal de usuario para acceder al servidor de proveedor de contenidos a través de un primer enlace de comunicaciones, el servidor de proveedor de contenidos transmite a uno de los servidores de verificación de identidades una notificación de verificación de que es necesario verificar la identidad del usuario, y redirecciona el terminal de usuario para su conexión con el mencionado de los servidores de verificación de identidades a través de un segundo enlace de comunicaciones;

d) dicho servidor de entre los servidores de verificación de identidades transmite al terminal de usuario el conjunto respectivo de información cifrada descargada en la etapa b) a través del segundo enlace de comunicaciones;

e) el usuario, basándose en el conjunto respectivo de información cifrada transmitida en la etapa d) y la clave pública asimétrica descargada en la etapa a), determina si dicho servidor de entre los servidores de verificación de identidades es actualmente válido para llevar a cabo una verificación de identidad;

f) tras determinar que dicho servidor de entre los servidores de verificación de identidades es actualmente válido para llevar a cabo una verificación de identidad, el terminal de usuario ejecuta el programa de exploración descargado en la etapa a) para obtener datos de exploración de hardware asociados al terminal de usuario, y transmite los datos de exploración de hardware así obtenidos hacia dicho servidor de entre los servidores de verificación de identidades a través del segundo enlace de comunicaciones; y

g) dicho servidor de entre los servidores de verificación de identidades verifica la identidad del usuario basándose en la relación entre los datos de exploración de hardware recibidos desde el terminal de usuario en la etapa f) y los datos de exploración de hardware de referencia almacenados en la etapa b), y notifica al servidor de proveedor de contenidos un resultado de verificación.

Se pondrán de manifiesto otras características y ventajas de la presente invención en la siguiente descripción detallada de la forma de realización preferida haciendo referencia a los dibujos adjuntos, en los cuales:

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

la figura 2 es un diagrama de flujo que ilustra un procedimiento de registro del método de autentificación en red de la forma de realización preferida;

la figura 3 es un diagrama de flujo que ilustra un procedimiento de inicio de sesión del método de autentificación en red de la forma de realización preferida;

la figura 4 es un diagrama de flujo de un procedimiento que ilustra cómo se determina uno de los servidores de verificación de identidades para llevar a cabo una verificación de identidad en la forma de realización preferida; y

la figura 5 es un diagrama de flujo de un procedimiento que ilustra cómo un terminal de usuario determina si dicho servidor de entre los servidores de verificación de identidad es actualmente válido para llevar a cabo una verificación de identidad en la forma de realización preferida.

Haciendo referencia a la figura 1, un sistema de autentificación en red se usa para implementar un método de autentificación en red para una verificación segura de la identidad de un usuario 5 de acuerdo con la forma de realización preferida de la presente invención. El sistema de autentificación en red incluye una unidad de descarga 1, un terminal de usuario 2 cuyo propietario es el usuario 5, un servidor de proveedor de contenidos 3 (por ejemplo, un proveedor de contenidos de internet o ICP), y una pluralidad de servidores de verificación de identidades 4. Con fines ilustrativos, el propietario del terminal de usuario 2 es el usuario 5, y el primero puede ser un dispositivo electrónico con capacidad de navegación por Internet o de comunicación de datos, tal como un ordenador portátil de tipo *notebook*, un teléfono inteligente, un asistente personal digital, etcétera. El terminal de usuario 2 incluye una pluralidad de componentes de hardware (no mostrados), tales como una unidad de procesado central, una unidad de sistema básico de entrada/salida (BIOS), un dispositivo de almacenamiento, una interfaz de red, una placa madre, etcétera, cada uno de los cuales tiene un código de identificación exclusivo. El servidor de proveedor de contenidos 3 puede ser, aunque sin carácter limitativo, un servidor de banco por internet, un servidor de juegos en línea, o cualquier otro servidor que proporcione un servicio de red que requiera verificación de la identidad, tal como un portal web. Los servidores de verificación de identidad 4 están autorizados idealmente por la unidad de descarga 1 a llevar a cabo una verificación de identidades de terceros, y pueden ser, aunque sin carácter limitativo, sitios web de redes sociales, tales como Google, Yahoo, Facebook, etcétera. La unidad de descarga 1 incluye una unidad de base de datos (no representada) para almacenar por lo menos un programa de exploración, al menos un par de claves pública y privada asimétricas, y una pluralidad de conjuntos de información cifrada correspondiente respetivamente a los servidores de verificación de identidades 4. Cada conjunto de información cifrada se firma con la clave privada asimétrica, e incluye una dirección web cifrada de uno respectivo de los servidores de verificación de identidades 4. En particular, cada conjunto de información cifrada se ha procesado con la clave privada asimétrica para crear una firma digital, y la clave pública asimétrica se utiliza para verificar la firma digital. La unidad de descarga 1, el terminal de usuario 2, el servidor de proveedor de contenidos 3 y los servidores de verificación de identidades 4 están conectados a una red de comunicaciones 100.

Haciendo referencia a las figuras 1 y 2, la unidad de descarga 1 coopera con el terminal de usuario 2 y con el servidor de proveedor de contenidos 3 para implementar un procedimiento de registro del método de autentificación en red de la forma de realización preferida de acuerdo con la presente invención. El procedimiento de registro del método de autentificación en red de la forma de realización preferida incluye las siguientes etapas. Se observa que, antes del procedimiento de registro, cada uno de los servidores de verificación de identidades 4 se conecta a la unidad de descarga 1 a través de la red de comunicaciones 100 para descargar un conjunto respectivo de información cifrada desde la unidad de descarga 1.

En la etapa S21, el usuario 5 introduce una identificación de usuario (ID) que actúa como identificador de usuario, y una contraseña utilizando una interfaz de entrada de usuario (no representada) del terminal de usuario 2 en un sitio web proporcionado por el servidor de proveedor de contenidos 3. La ID de usuario y la contraseña se transmiten a continuación desde el terminal de usuario 2 al servidor de proveedor de contenidos 3 por medio de la red de comunicaciones 100.

En la etapa S22, como respuesta a la recepción de la ID de usuario y de la contraseña, el servidor de proveedor de contenidos 3 se puede hacer funcionar para comprobar si la ID de usuario y la contraseña con correctas. Si el resultado es afirmativo, el flujo prosigue hacia la etapa S23. En caso contrario, el servidor de proveedor de contenidos 3 se puede hacer funcionar para enviar un mensaje de error al terminal de usuario 2 con el fin de visualizarlo en un dispositivo de visualización (no representado) del terminal de usuario 2 (etapa S20).

En la etapa S23, el servidor de proveedor de contenidos 3 se puede hacer funcionar para redireccionar el terminal de usuario 2 para su conexión con la unidad de descarga 1.

En la etapa S24, la unidad de descarga 1 se puede hacer funcionar para posibilitar que el terminal de usuario 2 descargue el programa de exploración y la clave pública asimétrica desde el mismo.

En la etapa S25, después de que el terminal de usuario 2 almacene el programa de exploración y la clave pública asimétrica, el terminal de usuario 2 se puede hacer funcionar para ejecutar el programa de exploración con el fin de explorar los componentes de hardware del terminal de usuario 2 para obtener los códigos de identificación de los componentes de hardware, y para establecer datos de exploración de hardware de referencia de acuerdo con los códigos de identificación de los componentes de hardware así obtenidos. Los datos de exploración de hardware de referencia están asociados al terminal de usuario 2, y se corresponden de manera exclusiva con el identificador de usuario correspondiente al usuario 5.

En la etapa S26, el terminal de usuario 2 se puede hacer funcionar para transmitir los datos de exploración de hardware de referencia a cada uno de los servidores de verificación de identidades 4 por medio de la red de comunicaciones 100, de manera que cada uno de los servidores de verificación de identidades 4 almacena los datos de exploración de hardware de referencia recibidos desde el terminal de usuario 2.

Haciendo referencia a las figuras 1 y 3, el sistema de autentificación en red implementa un procedimiento de inicio de sesión del método de autentificación en red de la forma de realización preferida. El procedimiento de inicio de sesión del método de autentificación en red de la forma de realización preferida incluye las siguientes etapas.

En la etapa S31, el usuario 5 introduce la ID de usuario y la contraseña utilizando la interfaz de entrada de usuario del terminal de usuario 2 en el sitio web de servicio proporcionado por el servidor de proveedor de contenidos 3, y el terminal de usuario 2 se puede hacer funcionar para transmitir la ID de usuario y la contraseña al servidor de proveedor de contenidos 3 a través de un primer enlace de comunicaciones sobre la red de comunicaciones 100.

En la etapa S32, como respuesta a la recepción de la ID de usuario y de la contraseña desde el terminal de usuario 2, el servidor de proveedor de contenidos 3 se puede hacer funcionar para comprobar si la ID de usuario y la contraseña son correctas. Si el resultado es afirmativo, el flujo prosigue hacia la etapa S33. En caso contrario, el servidor de proveedor de contenidos 3 se puede hacer funcionar para enviar un mensaje de error al terminal de usuario 2 con el fin de visualizarlo en el dispositivo de visualización del terminal de usuario 2 (etapa S30).

En la etapa S33, el servidor de proveedor de contenidos 3 se puede hacer funcionar para transmitir a uno de los servidores de verificación de identidades 4 una notificación de verificación de que es necesario verificar la identidad del usuario 5. El servidor de proveedor de contenidos 3 se puede hacer funcionar además para redireccionar el terminal de usuario 2 con el fin de conectarse con dicho servidor de entre los servidores de verificación de identidades 4 a través de un segundo enlace de comunicaciones que es independiente con respecto al primer enlace de comunicaciones. En una forma de realización, se observa que dicho servidor de entre los servidores de verificación de identidades 4 es determinado por el servidor de proveedor de contenidos 3. En otra forma de realización, dicho servidor de entre los servidores de verificación de identidades 4 lo puede determinar el usuario 5. Haciendo referencia adicionalmente a la figura 4, se muestra un procedimiento para ilustrar cómo el usuario 5 determina uno de los servidores de verificación de identidades 4 para llevar a cabo una verificación de identidad. En la subetapa S41, el servidor de proveedor de contenidos 3 se puede hacer funcionar para enviar al terminal de usuario 2 una solicitud de selección que incluye una lista de elementos de opción, que representan respectivamente los servidores de verificación de identidades 4. Como respuesta a la solicitud de selección del servidor de proveedor de contenidos 3, el terminal de usuario 2 se puede hacer funcionar para enviar al servidor de proveedor de contenidos 3 una respuesta de selección que indica uno deseado de los elementos de opción que representa una correspondiente de los servidores de verificación de identidades 4 (sub-etapa S42). Por lo tanto, el servidor de proveedor de contenidos 3 se puede hacer funcionar para determinar el correspondiente de los servidores de verificación de identidades 4 con el fin de llevar a cabo la verificación de identidad de acuerdo con la respuesta de selección (sub-etapa S43).

En la etapa S34, como respuesta a la recepción de la notificación de verificación desde el servidor de proveedor de contenidos 3, dicho servidor de entre los servidores de verificación de identidades 4 se puede hacer funcionar para transmitir el conjunto respectivo de información cifrada almacenada en el mismo al terminal de usuario 2 a través del segundo enlace de comunicaciones.

En la etapa S35, tras recibir el conjunto respectivo de información cifrada desde dicho servidor de entre los servidores de verificación de identidades 4, el terminal de usuario 2 se puede hacer funcionar para determinar, basándose en el conjunto respectivo de información cifrada y en la clave pública asimétrica almacenada en la etapa S24 del procedimiento de registro, si dicho servidor de entre los servidores de verificación de identidades 4 es actualmente válido para llevar a cabo una verificación de identidad.

En una forma de realización, el terminal de usuario 2 se puede hacer funcionar para descifrar la dirección web cifrada del conjunto respectivo de información cifrada utilizando la clave pública asimétrica. Tras un descifrado exitoso de la dirección web cifrada, el terminal de usuario 2 determina que dicho servidor de entre los servidores de verificación de identidades 4 es actualmente válido para llevar a cabo una verificación de identidad. A continuación, el flujo prosigue hacia la etapa S36. Por otro lado, tras un descifrado fallido de la dirección web cifrada de la información cifrada, el terminal de usuario 2 determina que dicho servidor de entre los servidores de verificación de identidades 4 no es actualmente válido para llevar a cabo una verificación de identidad. A continuación, el terminal de usuario 2 se puede hacer funcionar para enviar al servidor de proveedor de contenidos 3 una notificación de no validez según la cual dicho servidor de entre los servidores de verificación de identidades 4 no es válido para llevar a cabo una verificación de identidad (etapa S40).

En otra forma de realización, cada conjunto de información cifrada, que está almacenado en la unidad de base de datos de la unidad de descarga 1 y se corresponde con uno de los servidores de verificación de identidades 4, incluye además un periodo de autorización cifrado asociado al servidor de verificación de identidades 4. Haciendo referencia adicionalmente a la figura 5, se muestra un procedimiento para ilustrar cómo el terminal de usuario 2 determina, en la etapa S35, si dicho servidor de entre los servidores de verificación de identidades 4 es actualmente válido para llevar a cabo una verificación de identidad. En la subetapa S51, el terminal de usuario 2 se puede hacer funcionar para determinar si la dirección web cifrada y el periodo de autorización cifrado (es decir, el conjunto de información cifrada) de dicho servidor de entre los servidores de verificación de identidades 4 se descifran de manera exitosa utilizando la clave pública asimétrica. Si el resultado es negativo, el flujo pasa a la etapa S40 de la figura 3. Por otro lado, tras un descifrado exitoso de la dirección web cifrada y del periodo de autorización cifrado asociado a dicho servidor de entre los servidores de verificación de identidades 4, el terminal de usuario 2 se puede hacer funcionar para determinar si la fecha actual se encuentra dentro del periodo de autorización descifrado asociado a dicho servidor de entre los servidores de verificación de identidades 4 (sub-etapa S52). Si el resultado es afirmativo, el terminal de usuario 2 determina que dicho servidor de entre los servidores de verificación de identidades 4 es actualmente válido para llevar a cabo una verificación de identidad (etapa S53). A continuación, el flujo pasa a la etapa 36 de la figura 3. Por otro lado, cuando el terminal de usuario 2 determina que la fecha actual no se encuentra dentro del periodo de autorización descifrado asociado a dicho servidor de entre los servidores de verificación de identidades 4, el terminal de usuario 2 se puede hacer funcionar para enviar a la unidad de descarga 1 una notificación de expiración según la cual se ha producido la expiración del periodo de autorización asociado a dicho servidor de entre los servidores de verificación de identidades 4 (etapa S54). A continuación, el flujo pasa a la etapa S40 de la figura 3.

En la etapa S36, el terminal de usuario 2 se puede hacer funcionar para ejecutar el programa de exploración con el fin de explorar los componentes de hardware del terminal de usuario 2 para obtener los códigos de identificación de los componentes de hardware que sirven como datos de exploración de hardware asociados al terminal de usuario 2, y para transmitir los datos de exploración de hardware así obtenidos a dicho servidor de entre los servidores de verificación de identidades 4.

En la etapa S37, tras la recepción de los datos de exploración de hardware desde el terminal de usuario 2, dicho servidor de entre los servidores de verificación de identidades 4 se puede hacer funcionar para comparar los datos de exploración de hardware con los datos de exploración de hardware de referencia almacenados en el mismo durante el procedimiento de registro del usuario 5 con el fin de verificar la identidad del usuario 5 asociado al terminal de usuario 2, y para enviar un resultado de la verificación al servidor de proveedor de contenidos 3. Cuando los datos de exploración de hardware obtenidos en la etapa S36 no concuerdan con los datos de exploración de hardware de referencia almacenados en dicho servidor de entre los servidores de verificación de identidades 4, el resultado de la verificación indica que la verificación de la identidad del usuario 5 ha fallado. Por otro lado, cuando los datos de exploración de hardware obtenidos en la etapa S36 concuerdan con los datos de exploración de hardware de referencia almacenados en dicho servidor de entre los servidores de verificación de identidades 4, el resultado de la verificación indica que la verificación de la identidad del usuario 5 ha sido exitosa.

En la etapa S38, el servidor de proveedor de contenidos 3 se puede hacer funcionar para determinar, sobre la base del resultado de la verificación de dicho servidor de entre los servidores de verificación de identidades 4, si la identidad del usuario 5 está autentificada. Cuando el resultado de la verificación indica que la verificación de la identidad del usuario 5 ha fallado, el servidor de proveedor de contenidos 3 determina que la identidad del usuario 5 no se ha autentificado. Por lo tanto, el flujo pasa a la etapa S30. En este caso, al terminal de usuario 2 se le deniega acceso al sitio web de servicio proporcionado por el servidor de proveedor de contenidos 3. Por otro lado, cuando el resultado de la verificación indica que la verificación de la identidad del usuario 5 ha sido exitosa, el servidor de proveedor de contenidos 3 determina que la identidad del usuario 5 se ha autentificado. A continuación, el servidor de proveedor de contenidos 3 se puede hacer funcionar para redireccionar el terminal de usuario 2 con el fin de conectarse con el sitio web de servicio proporcionado por el servidor de proveedor de contenidos 3 (etapa S39). Por lo tanto, al terminal de usuario 2 se le autoriza el acceso al sitio web de servicio.

En resumen, el método de autentificación en red de acuerdo con esta invención presenta las siguientes ventajas:

1. Debido a que al terminal de usuario 2 se le dirige dinámicamente a uno de los servidores de verificación de identidades 4 para una posterior verificación de la identidad (es decir, al terminal de usuario 2 se le puede dirigir a un servidor de verificación de identidades 4 diferente cada vez), y puesto que el conjunto respectivo de información cifrada almacenada en cada servidor de verificación de identidades 4 y la clave pública asimétrica almacenada en el terminal de usuario 2 se pueden actualizar aleatoriamente como respuesta a una notificación desde la unidad de descarga 1 según se requiera, se puede obtener una multi-autenticación para la identidad del usuario utilizando la unidad de descarga 1 que proporciona el conjunto respectivo de información cifrada a cada servidor de verificación de identidades 4, y la clave pública asimétrica y el programa de exploración al terminal de usuario 2.

2. Cada vez que el terminal de usuario 2 implementa la etapa S36 del procedimiento de inicio de sesión del método de autentificación en red, el terminal de usuario 2 puede ejecutar el programa de exploración para explorar los componentes de hardware del terminal de usuario 2 con el fin de obtener los datos de exploración de hardware de acuerdo con los códigos de identificación de los componentes de hardware, y los datos de exploración de hardware así obtenidos para su uso posterior en la autentificación de la identidad del usuario por parte de dicho servidor de entre los servidores de verificación de identidades 4 son datos dinámicos. Por lo tanto, no es necesario que el proveedor de contenidos en red compre equipos adicionales para la autentificación de la identidad, y no es necesario que proporcione al usuario un *token* dinámico, una tarjeta electrónica de IC, o un dispositivo USB con un certificado de PKI. Además, no es necesario que el usuario 5 disponga de dispositivos de autentificación adicionales para diferentes sitios web de servicio.

3. Puesto que el terminal de usuario 2 se conecta al servidor de proveedor de contenidos 3 a través del primer enlace de comunicaciones y se conecta a dicho servidor de entre los servidores de verificación de identidades 4 a través del segundo enlace de comunicaciones, resulta relativamente difícil atacar de manera simultánea el primer y el segundo enlaces de comunicaciones para robar y/o manipular indebidamente los datos enviados por el terminal de usuario 2.

REIVINDICACIONES

1. Método de autentificación en red para su implementación utilizando un terminal de usuario (2), una unidad de descarga (1), un servidor de proveedor de contenidos (3) y una pluralidad de servidores de verificación de identidades (4) para la verificación segura de la identidad de un usuario (5) del terminal de usuario (2), estando caracterizado dicho método de autentificación en red por que presenta las etapas siguientes:

a) el terminal de usuario (2) descarga un programa de exploración y una clave pública asimétrica desde la unidad de descarga (1);

b) cada uno de los servidores de verificación de identidades (4) descarga de la unidad de descarga (1) un conjunto respectivo de información cifrada que está firmado con una clave privada asimétrica y que incluye una dirección web cifrada del servidor de verificación de identidades (4), y almacena unos datos de exploración de hardware de referencia que están asociados al terminal de usuario (2) y que se corresponden de manera única con un identificador de usuario del usuario (5);

c) en respuesta a una solicitud de inicio de sesión de usuario desde el terminal de usuario (2) para acceder al servidor de proveedor de contenidos (3) a través de un primer enlace de comunicaciones, el servidor de proveedor de contenidos (3) transmite a uno de los servidores de verificación de identidades (4) una notificación de verificación de que resulta necesario verificar la identidad del usuario (5), y redirecciona el terminal de usuario (2) para conectar con dicho uno de los servidores de verificación de identidades (4) a través de un segundo enlace de comunicaciones;

d) dicho uno de los servidores de verificación de identidades (4) transmite al terminal de usuario (2) el conjunto respectivo de información cifrada descargada en la etapa b) a través del segundo enlace de comunicaciones;

e) el terminal de usuario (2) determina, basándose en por lo menos el conjunto respectivo de información cifrada transmitido en la etapa d) y la clave pública asimétrica descargada en la etapa a), si dicho uno de los servidores de verificación de identidades (4) es actualmente válido para llevar a cabo una verificación de identidad;

f) tras determinar que dicho uno de los servidores de verificación de identidades (4) es actualmente válido para llevar a cabo una verificación de identidad, el terminal de usuario (2) ejecuta el programa de exploración descargado en la etapa a) para obtener unos datos de exploración de hardware asociados al terminal de usuario (2), y transmite los datos de exploración de hardware así obtenidos a dicho uno de los servidores de verificación de identidades (4) a través del segundo enlace de comunicaciones; y

g) dicho uno de los servidores de verificación de identidades (4) verifica la identidad del usuario (5) basándose en la relación entre los datos de exploración de hardware recibidos desde el terminal de usuario (2) en la etapa f) y los datos de exploración de hardware de referencia almacenados en la etapa b), y notifica al servidor de proveedor de contenidos (3) un resultado de verificación.

2. Método de autentificación en red según la reivindicación 1, incluyendo el terminal de usuario (2) una pluralidad de componentes de hardware, presentando cada uno de los cuales un código de identificación único, estando caracterizado además dicho método de autentificación en red, entre las etapas a) y b), por que presenta la etapa siguiente:

el terminal de usuario (2) ejecuta el programa de exploración para explorar los componentes de hardware del mismo para obtener los códigos de identificación de los componentes de hardware respectivamente que sirven como datos de exploración de hardware de referencia, y transmite los datos de exploración de hardware de referencia a cada uno de los servidores de autentificación de identidades para su almacenamiento en la etapa b).

3. Método de autentificación en red según la reivindicación 2, caracterizado por que, durante el registro del terminal de usuario (2) en el servidor de proveedor de contenidos (3), el terminal de usuario (2) descarga el programa de exploración y la clave pública asimétrica desde la unidad de descarga (1) en la etapa a), y cada uno de los servidores de verificación de identidades (4) descarga la información cifrada respectiva desde la unidad de descarga (1) y almacena los datos de exploración de hardware de referencia en la etapa b).

4. Método de autentificación en red según cualquiera de las reivindicaciones 1 a 3, caracterizado por que, en la etapa c), dicho uno de los servidores de verificación de identidades (4) es determinado por el servidor de proveedor de contenidos (3).

5. Método de autentificación en red según cualquiera de las reivindicaciones 1 a 3, caracterizado por que, en la etapa c), dicho uno de los servidores de verificación de identidades (4) es determinado por el terminal de usuario (2).

6. Método de autentificación en red según la reivindicación 5, caracterizado por que la etapa c) incluye las subetapas siguientes:

c1) en respuesta a la solicitud de inicio de sesión del terminal de usuario (2), el servidor de proveedor de contenidos (3) envía al terminal de usuario (2) una solicitud de selección que incluye una lista de elementos de opción, que representan respectivamente los servidores de verificación de identidades (4);

c2) el servidor de proveedor de contenidos (3) recibe una respuesta de selección desde el terminal de usuario (2) que indica uno deseado de los elementos de opción que representa dicho uno de los servidores de verificación de identidades (4); y

c3) el servidor de proveedor de contenidos (3) redirecciona el terminal de usuario (2) para conectar con dicho uno de los servidores de verificación de identidades (4) de acuerdo con la respuesta de selección del terminal de usuario (2).

7. Método de autentificación en red según cualquiera de las reivindicaciones 1 a 6, caracterizado por que, en la etapa e):

el terminal de usuario (2) se puede hacer funcionar para descifrar la dirección web cifrada utilizando la clave pública asimétrica; y

tras un descifrado exitoso de la dirección web cifrada, el terminal de usuario (2) determina que dicho uno de los servidores de verificación de identidades (4) es válido actualmente para llevar a cabo una verificación de identidad.

8. Método de autentificación en red según cualquiera de las reivindicaciones 1 a 7, caracterizado por que:

en la etapa b), el conjunto respectivo de información cifrada descargado por cada uno de los servidores de verificación de identidades (4) incluye además un periodo de autorización cifrado asociado al servidor de verificación de identidades; y

la etapa e) incluye las subetapas siguientes

e1) el terminal de usuario (2) determina si la dirección web cifrada y el periodo de autorización cifrado asociado a dicho uno de los servidores de verificación de identidades (4) se descifran de manera exitosa utilizando la clave pública asimétrica,

e2) tras un descifrado exitoso de la dirección web cifrada y del periodo de autorización cifrado, el terminal de usuario (2) determina si la fecha actual se encuentra dentro del periodo de autorización descifrado asociado a dicho uno de los servidores de verificación de identidades (4), y

e3) tras determinar que la fecha actual se encuentra dentro del periodo de autorización descifrado asociado a dicho uno de los servidores de verificación de identidades (4), el terminal de usuario (2) determina que dicho uno de los servidores de verificación de identidades (4) es actualmente válido para llevar a cabo una verificación de identidad.

9. Método de autentificación en red según la reivindicación 8, caracterizado por que la etapa e) incluye además la subetapa siguiente:

e4) cuando la fecha actual no se encuentra dentro del periodo de autorización descifrado asociado a dicho uno de los servidores de verificación de identidades (4), el terminal de usuario (2) envía a la unidad de descarga (1) una notificación de expiración de que ha expirado el periodo de autorización asociado a dicho uno de los servidores de verificación de identidades (4).

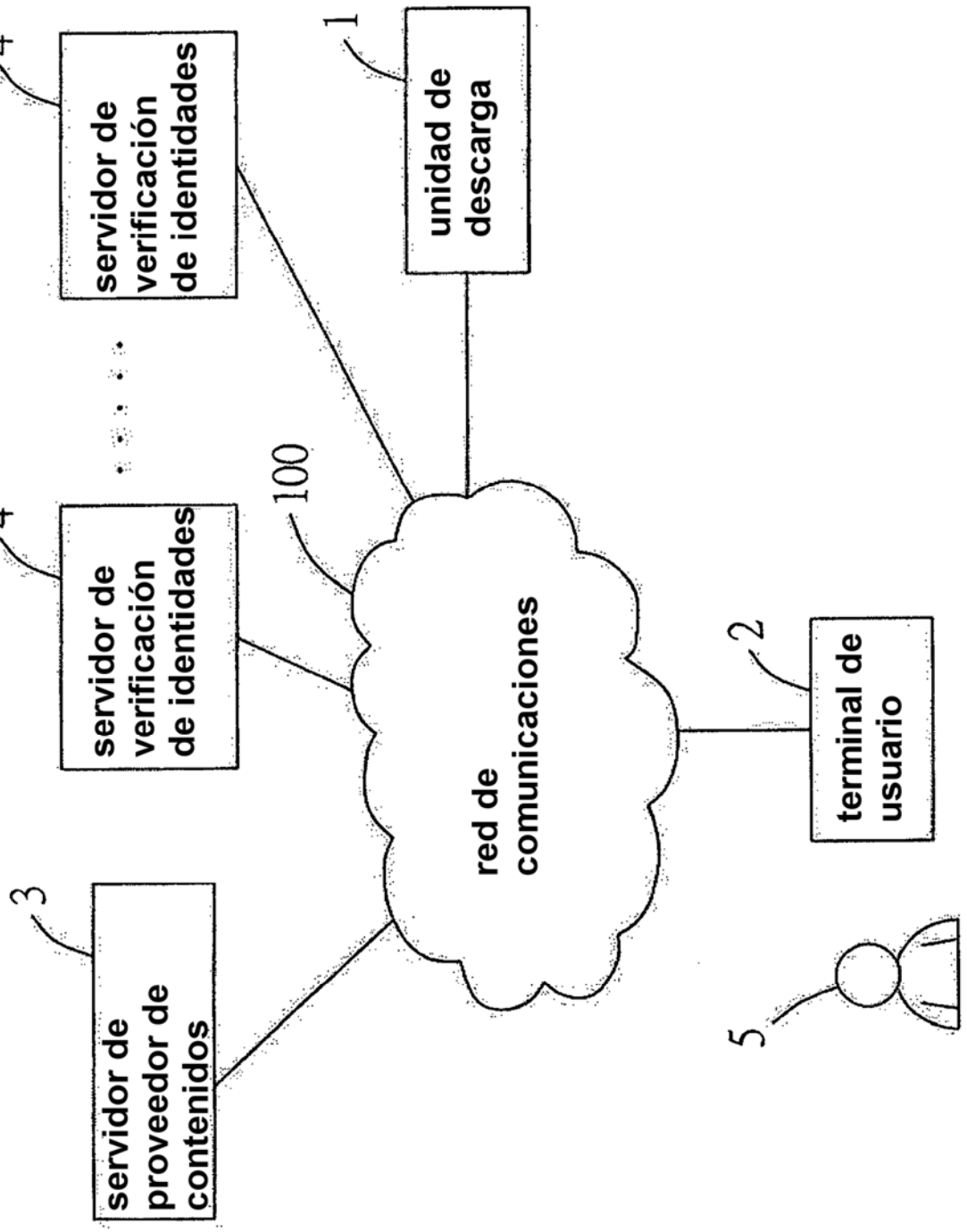
4
servidor de verificación de identidades
4
servidor de verificación de identidades
3
servidor de proveedor de contenidos
100
red de comunicaciones
1
unidad de descarga
2
terminal de usuario
5

FIG.1

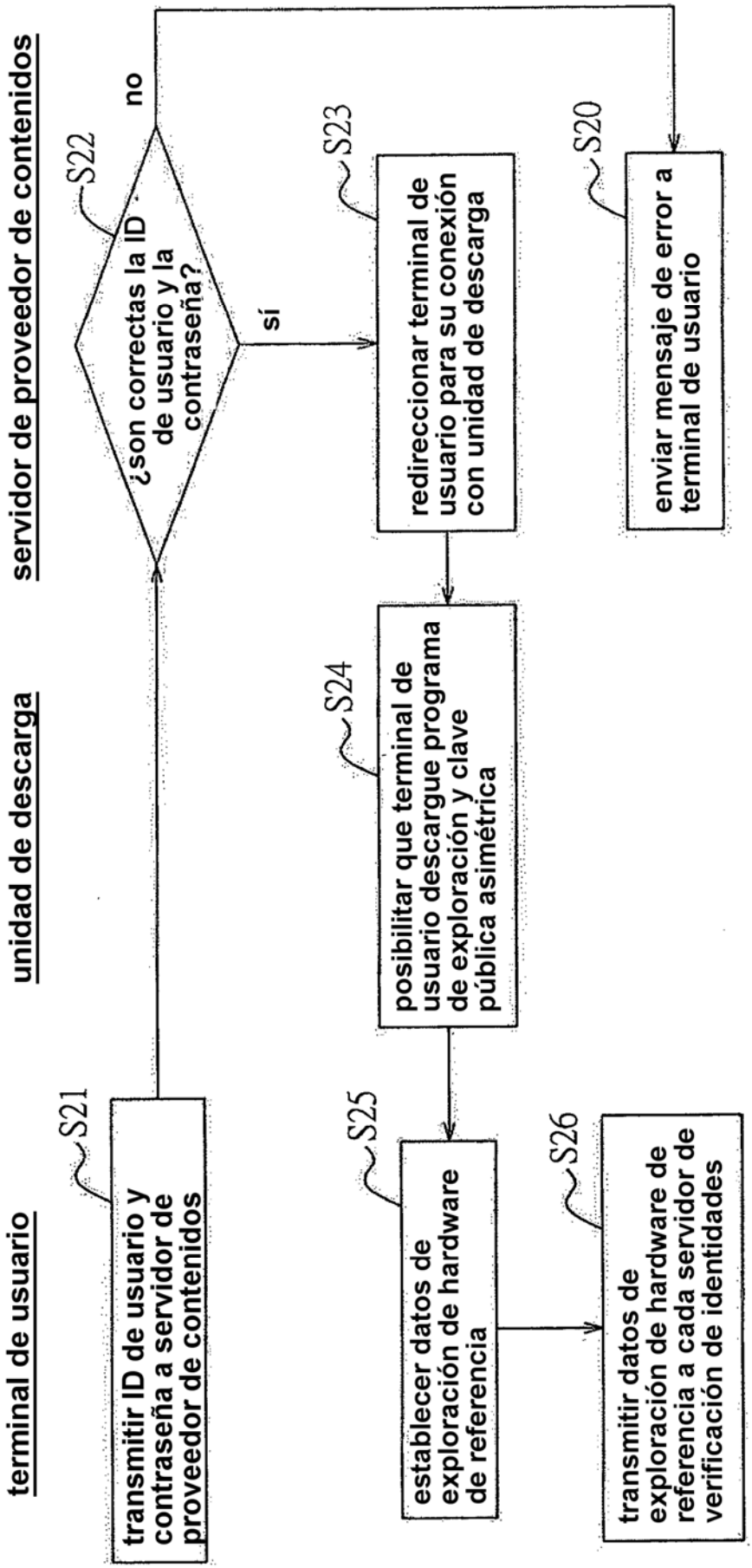
terminal de usuario
unidad de descarga
servidor de proveedor de contenidos
S21
transmitir ID de usuario y contraseña a servidor de proveedor de contenidos
S22
¿son correctas la ID de usuario y la contraseña?
no
sí
S20
enviar mensaje de error a terminal de usuario
S23
redireccionar terminal de usuario para su conexión con unidad de descarga
S24
posibilitar que terminal de usuario descargue programa de exploración y clave pública asimétrica
S25
establecer datos de exploración de hardware de referencia
S26
transmitir datos de exploración de hardware de referencia a cada servidor de verificación de identidades

FIG.2

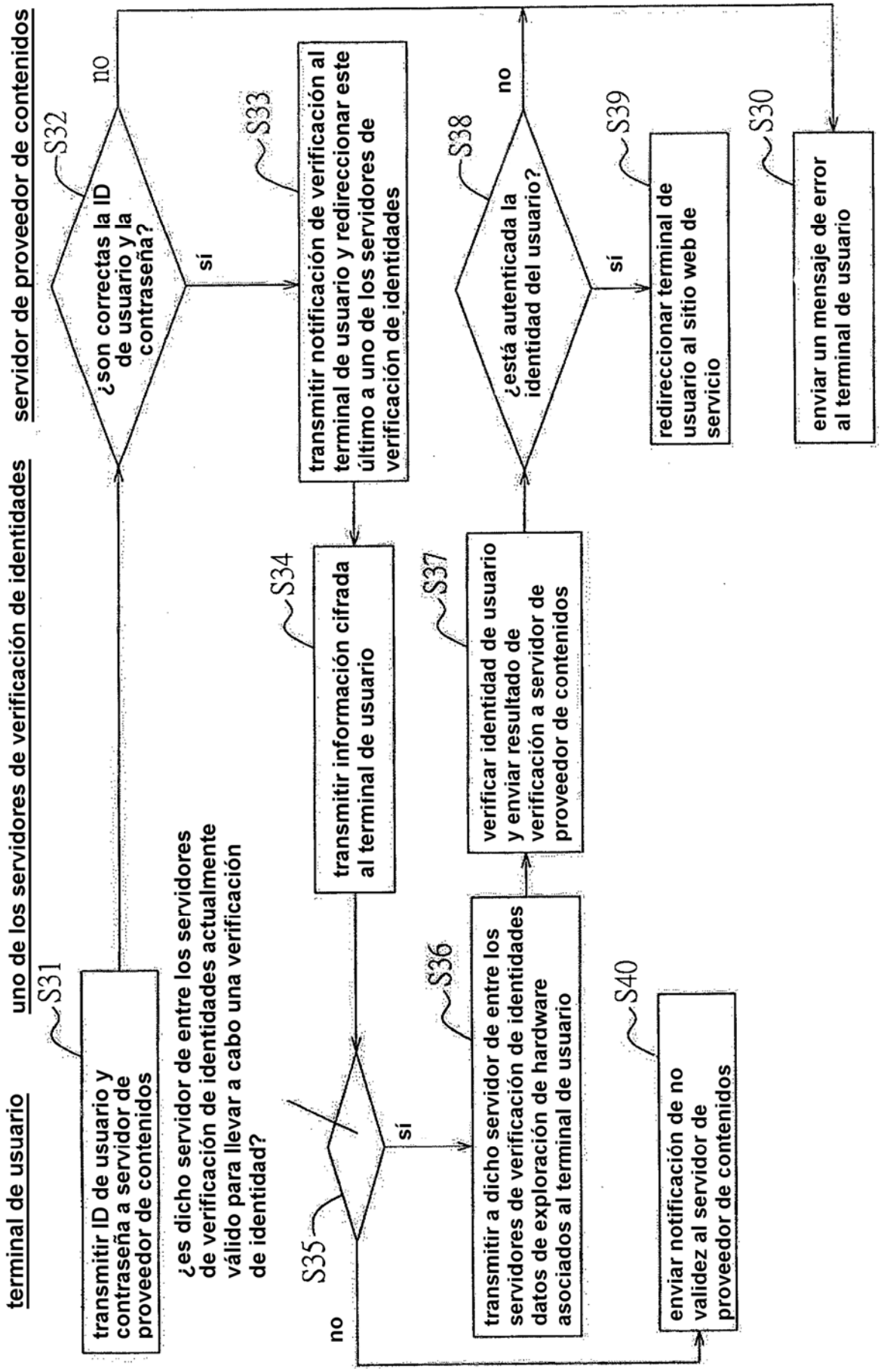
terminal de usuario
uno de los servidores de verificación de identidades
servidor de proveedor de contenidos
S31
transmitir ID de usuario y contraseña a servidor de proveedor de contenidos
S32
¿son correctas la ID de usuario y la contraseña?
no
sí
S33
transmitir notificación de verificación al terminal de usuario y redireccionar este último a uno de los servidores de verificación de identidades
S34
transmitir información cifrada al terminal de usuario
¿es dicho servidor de entre los servidores de verificación de identidades actualmente válido para llevar a cabo una verificación de identidad?
S35
no
sí
S36
transmitir a dicho servidor de entre los servidores de verificación de identidades datos de exploración de hardware asociados al terminal de usuario
S37
verificar identidad de usuario y enviar resultado de verificación a servidor de proveedor de contenidos
S38
¿está autenticada la identidad del usuario?
no
sí
S39
redireccionar terminal de usuario al sitio web de servicio
S30
enviar un mensaje de error al terminal de usuario
S40
enviar notificación de no validez al servidor de proveedor de contenidos

FIG.3

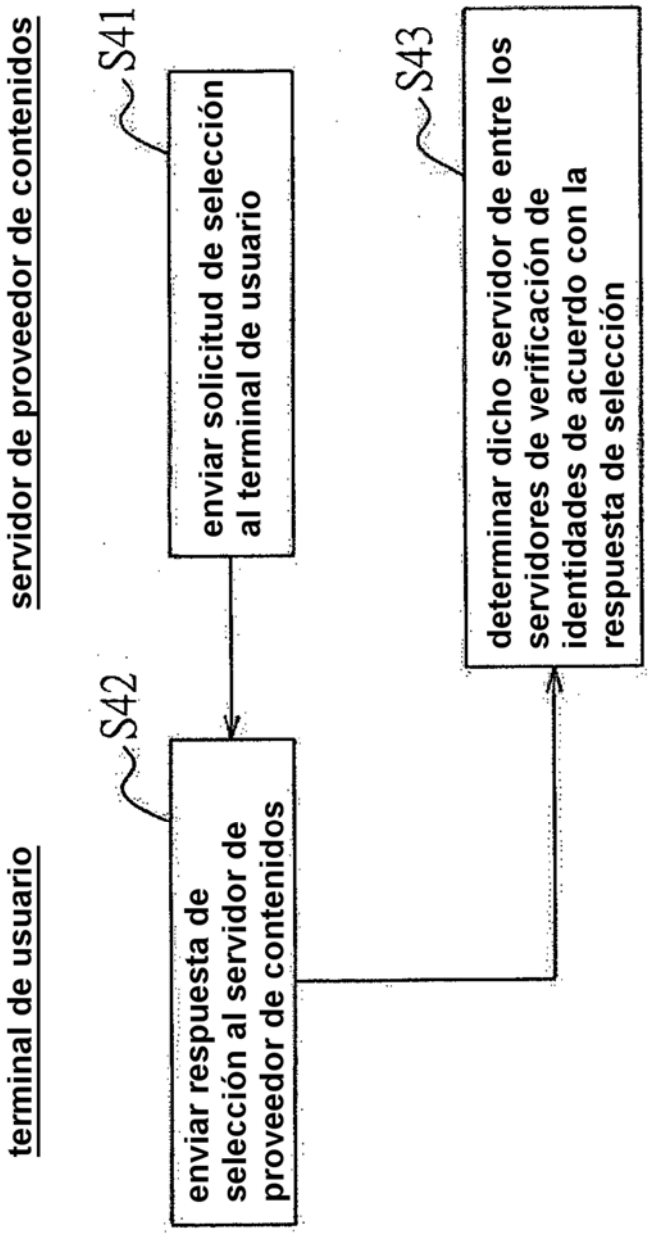
terminal de usuario
servidor de proveedor de contenidos
S41
enviar solicitud de selección al terminal de usuario
S42
enviar respuesta de selección al servidor de proveedor de contenidos
S43
determinar dicho servidor de entre los servidores de verificación de identidades de acuerdo con la respuesta de selección

FIG.4

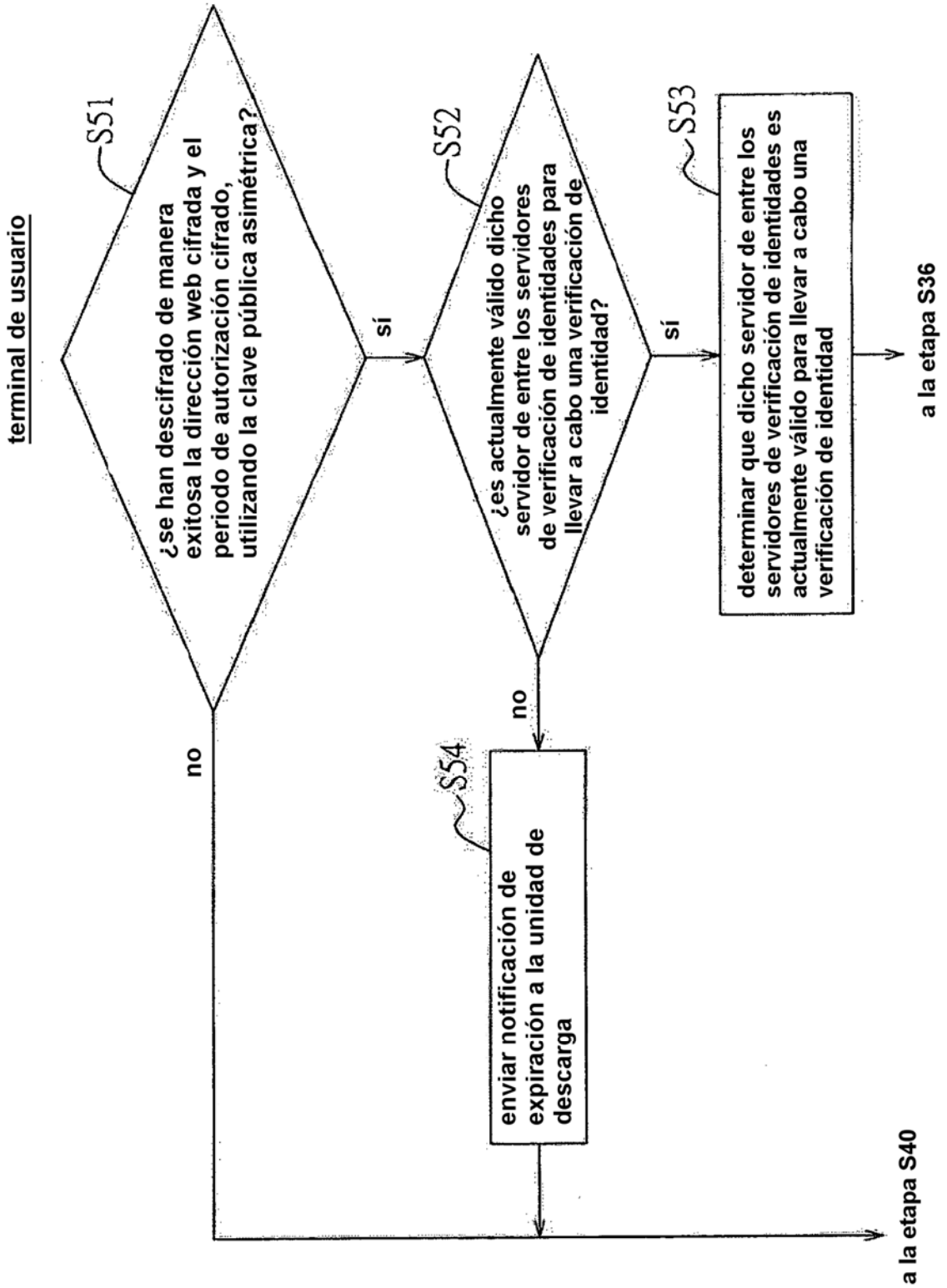
terminal de usuario
S51
¿se han descifrado de manera exitosa la dirección web cifrada y el periodo de autorización cifrado, utilizando la clave pública asimétrica?
sí
no
S52
¿es actualmente válido dicho servidor de entre los servidores de verificación de identidades para llevar a cabo una verificación de identidad?
sí
no
S53
determinar que dicho servidor de entre los servidores de verificación de identidades es actualmente válido para llevar a cabo una verificación de identidad
a la etapa S36
S54
enviar notificación de expiración a la unidad de descarga
a la etapa S40

FIG.5