(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 660 541**

(51) Int. CI.:

G06F 15/16 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.09.2010 PCT/US2010/050729**

(87) Fecha y número de publicación internacional: **07.04.2011 WO11041419**

(96) Fecha de presentación y número de la solicitud europea: **29.09.2010 E 10821173 (1)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2018 EP 2483791**

(54) Título: **Marco de autenticación de dispositivo modular**

(30) Prioridad:

30.09.2009 US 570416

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.03.2018

(73) Titular/es:

AMAZON TECHNOLOGIES, INC. (100.0%)
P.O. Box 8102
Reno, NV 89507, US

(72) Inventor/es:

HEGG, JOEL, C.;
SRIRAM, SIDDHARTH y
TALREJA, KAMLESH, T.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Marco de autenticación de dispositivo modular

Antecedentes

Entidades en línea ofrecen una amplia variedad de servicios a una diversidad de diferentes dispositivos cliente, incluyendo ordenadores personales (PC), asistentes digitales personales (PDA), teléfonos móviles, PC de bolsillo, teléfonos inteligentes, decodificadores de salón, grabadores de video digital (DVR) y consolas de juegos, entre otras posibilidades. Estos dispositivos cliente a menudo acceden a diversos servicios web, tales como almacenamientos online u otros proveedores de contenido de audio/visual, programas de software, libros digitales u otro contenido electrónico. En muchos casos, deben autenticarse peticiones de diferentes dispositivos cliente para un servicio web particular antes de que el servicio web acepte la petición. El documento US 2007/0094714 divulga un servidor de selección de autenticación automática.

Diferentes dispositivos cliente a menudo soportan diferentes mecanismos de autenticación que proporcionan acceso a los servicios web. Por ejemplo, algunos tipos de dispositivo pueden usar mecanismos de autenticación propietarios que son únicos para la marca particular del dispositivo. Otros tipos de dispositivo pueden usar mecanismos de autenticación de una aplicación más general, tales como Capa de Conexiones Seguras ("SSL"). En algunos casos, este problema se aborda proporcionando servicios web separados por cada tipo de dispositivo, de tal forma que cada servicio web implementa un mecanismo de autenticación particular. Sin embargo, cuando se proporcionan servicios web separados de esta manera, puede existir una duplicidad sustancial de esfuerzo entre los diversos servicios web, porque entidades deben implementar cada esquema de autenticación como un servicio web separado que se diseña para un tipo de dispositivo particular. Adicionalmente, proveedores pueden usar diferentes direcciones para cada servicio web, tales como Localizadores de Recursos Uniformes ("URL"). Esto puede provocar algo de confusión a usuarios con múltiples tipos de dispositivo. Por ejemplo, un usuario puede no darse cuenta que un único proveedor tiene múltiples sitios web y correspondientes URL para cada uno de los dispositivos del usuario. Por lo tanto, el usuario puede usar una URL incorrecta tratando de acceder a un servicio web con un dispositivo, incluso aunque el URL puede trabajar apropiadamente para otro dispositivo. Aunque mecanismos existentes pueden evitar este problema, por ejemplo, redirigiendo un dispositivo a un URL correcto, estos mecanismos son ad hoc y puede que no todos los tipos de dispositivo los soporten. Por lo tanto, se necesitan sistemas y métodos para superar estas limitaciones de mecanismos de dispositivo de autenticación tradicionales.

Breve descripción de los dibujos

Los dibujos adjuntos, que se incorporan a y constituyen una parte de esta divulgación, ilustran diversas realizaciones divulgadas. En los dibujos:

la Figura 1 es un diagrama de un ejemplo de un sistema para proporcionar acceso a un servicio;
la Figura 2 es un diagrama de un ejemplo de una arquitectura de un servidor;
la Figura 3 es un diagrama de un ejemplo de una arquitectura para un módulo de autenticación;
la Figura 4 es un diagrama de un ejemplo de una arquitectura para otro módulo de autenticación;
la Figura 5 es un diagrama de flujo de un ejemplo de una rutina para proporcionar acceso a un servicio;
la Figura 6 es un diagrama de flujo de un ejemplo de una rutina para autenticar una petición de dispositivo; y
la Figura 7 es un diagrama de flujo de un ejemplo de otra rutina para autenticar una petición de dispositivo.

Descripción detallada

La siguiente descripción detallada se refiere a los dibujos adjuntos. Siempre que sea posible, se usan los mismos números de referencia en los dibujos y la siguiente descripción para referirse a las mismas o similares partes. Mientras varias realizaciones ilustrativas se describen en este documento, son posibles modificaciones, adaptaciones y otras implementaciones. Por ejemplo, pueden hacerse sustituciones, adiciones o modificaciones a los componentes ilustrados en los dibujos y los métodos ilustrativos descritos en este documento pueden modificarse sustituyendo, reordenando o añadiendo etapas a los métodos divulgados. Por consiguiente, la siguiente descripción detallada no limita las realizaciones divulgadas. En su lugar, el alcance apropiado se define mediante las reivindicaciones adjuntas.

Realizaciones divulgadas proporcionan sistemas y métodos para proporcionar acceso a un servicio, tales como un servicio web. Los sistemas y métodos pueden permitir que un número de diferentes tipos de dispositivo accedan a un único servicio web, incluso cuando los tipos de dispositivo implementan diferentes esquemas de autenticación. Por ejemplo, un servidor que proporciona el servicio web puede almacenar varios módulos de autenticación específicos para tipo de dispositivo. Cuando un dispositivo particular solicita acceso al servicio web, el servidor puede extraer un identificador de tipo de dispositivo de la petición. El servidor puede a continuación seleccionar el módulo de autenticación apropiado para autenticar el dispositivo solicitante.

Consistente con una realización divulgada, un método implementado por ordenador proporciona acceso a un servicio. De acuerdo con el método, módulos de autenticación se almacenan para autenticar dispositivos que solicitan acceso al servicio. Los dispositivos incluyen al menos una primera pluralidad de dispositivos que tienen un primer tipo de dispositivo y una segunda pluralidad de dispositivos que tienen un segundo tipo de dispositivo. Uno primero de los módulos de autenticación se configura para realizar autenticación de la primera pluralidad de dispositivos usando un esquema de autenticación específico para el primer tipo de dispositivo. Un segundo de los módulos de autenticación se configura para realizar autenticación de la segunda pluralidad de dispositivos usando un esquema de autenticación específico para el segundo tipo de dispositivo. Un servidor recibe una petición para acceder al servicio y la petición incluye un identificador de tipo de dispositivo de un dispositivo que solicita el servicio.

El identificador de tipo de dispositivo se extrae de la petición y el método determina si identificador de tipo de dispositivo corresponde al primer tipo de dispositivo o al segundo tipo de dispositivo. El primer módulo de autenticación se selecciona cuando el identificador de tipo de dispositivo corresponde al primer tipo de dispositivo y se selecciona el segundo módulo de autenticación cuando el identificador de tipo de dispositivo corresponde al segundo tipo de dispositivo. La petición se autentica usando el módulo de autenticación seleccionado para determinar si se permite que el dispositivo solicitante acceda al servicio, realizando de este modo autenticación del dispositivo solicitante usando el esquema de autenticación específico para el dispositivo solicitante. Si el módulo de autenticación seleccionado determina que el dispositivo solicitante está autorizado para acceder al servicio, se proporciona acceso al servicio. Si el módulo de autenticación seleccionado determina que el dispositivo solicitante no está autorizado para acceder al servicio, se evita el acceso al servicio.

Consistente con otra realización divulgada, un método implementado por ordenador proporciona acceso a un servicio. De acuerdo con el método, se recibe una petición para acceder al servicio y la petición incluye un identificador de tipo de dispositivo de un dispositivo que solicita acceso al servicio. El identificador de tipo de dispositivo se extrae de la petición y se determina un tipo de dispositivo correspondiente para el dispositivo solicitante. Un módulo de autenticación se selecciona de una pluralidad de módulos de autenticación basándose en el identificador de tipo de dispositivo y el módulo de autenticación seleccionado implementa un esquema de autenticación para el tipo de dispositivo del dispositivo solicitante. La petición se autentica usando el módulo de autenticación seleccionado para determinar si se permite que el dispositivo solicitante acceda al servicio. Se proporciona acceso al servicio basándose en al menos una determinación de que el dispositivo solicitante está autorizado para acceder al servicio.

Consistente con otra realización divulgada, un servidor proporciona acceso a un servicio. El servidor incluye un procesador para ejecutar instrucciones de programa y un medio legible por ordenador que almacena las instrucciones de programa. Realizando las instrucciones de programa, cuando se ejecutan por el procesador, un proceso para recibir una petición de acceso a servicio. La petición incluye un identificador de tipo de dispositivo de un dispositivo que solicita acceso al servicio. Las instrucciones de programa extraen el identificador de tipo de dispositivo de la petición y determinan un tipo de dispositivo correspondiente para el dispositivo solicitante. Las instrucciones de programa seleccionan un módulo de autenticación de una pluralidad de módulos de autenticación basándose en el identificador de tipo de dispositivo y el módulo de autenticación seleccionado implementa un esquema de autenticación para el tipo de dispositivo del dispositivo solicitante. Las instrucciones de programa autentican la petición usando el módulo de autenticación seleccionado para determinar si se permite que el dispositivo solicitante acceda al servicio y proporcionan acceso al servicio basándose en al menos una determinación de que el dispositivo solicitante está autorizado para acceder al servicio.

La Figura 1 es un ejemplo de un sistema 100 para proporcionar acceso a un servicio, consistente con realizaciones divulgadas. El sistema 100 puede proporcionar funcionalidad para uno o más dispositivos cliente para acceder a un servicio (por ejemplo, un servicio web) que se ejecuta en un servidor. Como se muestra en el sistema 100, clientes 110, 120 y 130, servidor 140, autoridad de certificado 150, dispositivo de cliente no fiable 170, servidor asociado de confianza 180 y dispositivo heredado 190 se conectan a una red 160. Un experto en la materia apreciará que, aunque un número particular de componentes se representa en la Figura 1, puede proporcionarse cualquier número de estos componentes. Un experto en la materia también reconocerá que funciones proporcionadas por uno o más componentes del sistema 100 pueden combinarse en un componente o distribuirse por una pluralidad de componentes. Por ejemplo, el servidor 140 puede implementarse usando un parque de servidores que incluye varios servidores principales, así como varios servidores de respaldo. Además, el servidor 140 puede implementarse distribuyendo diversas etapas de procesamiento analizadas en este documento a través de múltiples servidores. La red 160 proporciona comunicaciones entre los diversos componentes en el sistema 100, tales como dispositivos cliente 110, 120 y 130, servidor 140, autoridad de certificado 150, dispositivo de cliente no fiable 170, servidor asociado de confianza 180 y dispositivo heredado 190. La red 160 puede ser una red compartida, pública o privada, puede incluir un área extensa o local y puede implementarse a través de cualquier combinación adecuada de redes de comunicación por cable y/o inalámbricas. Adicionalmente, la red 160 puede comprender una intranet o la Internet.

El servidor 140 puede comprender un ordenador de fin general (por ejemplo, un ordenador personal, ordenador de red, servidor u ordenador central) que tienen uno o más procesadores 145 que pueden activarse selectivamente o reconfigurarse mediante un programa informático. El procesador 145 puede realizar etapas o métodos consistentes con realizaciones divulgadas leyendo instrucciones de procesamiento de la memoria 146 y ejecutando las

instrucciones. En particular, el servicio web 141 y servicio web 142 pueden implementarse como instrucciones almacenadas en la memoria 146, adecuadas para su ejecución mediante el procesador 145.

La memoria 146 puede ser una o más memorias o dispositivos de almacenamiento que almacenan datos, así como software. La memoria 146 también puede comprender, por ejemplo, uno o más de RAM, ROM, almacenamiento magnético o almacenamiento óptico. Adicionalmente, la memoria 146 puede almacenar módulos de programa que, cuando se ejecutan mediante el procesador 140, realizan una o más etapas analizadas a continuación.

En otras realizaciones, el servidor 140 puede construirse específicamente para llevar a cabo métodos consistentes con realizaciones divulgadas. Por ejemplo, una o más de las etapas de procesamiento divulgadas en este documento pueden implementarse en un campo de matriz de puertas programables ("FPGA"), circuito integrado específico de aplicación ("ASIC") o conjunto de chips adecuado. Etapas de cifrado y descifrado analizadas en este documento pueden ser particularmente adecuadas para implementación en tales dispositivos de hardware. El servidor 140 puede proporcionar acceso a diversos servicios, tales como el servicio web 141 y servicio web 142. El servidor 140 también puede proporcionar funcionalidad para autenticar los dispositivos cliente 110, 120 y 130 y/o usuarios que operan tales dispositivos cliente. Por ejemplo, una entidad que proporciona contenido de audio/visual o software a través de la red 150 puede proporcionar tal contenido usando servicios web 141 y 142.

Ya que los dispositivos cliente 110, 120 y 130 pueden usar diferentes protocolos de comunicación o formatos de datos, el servidor 140 también puede incluir una capa de compatibilidad de dispositivos 143, que se analiza en más detalle en la Solicitud de Estados Unidos N.º 12/165,188, titulada "Client-to-Service Compatibility Framework," presentada el 30 de junio de 2008. Por ejemplo, la capa de compatibilidad de dispositivos 143 puede traducir comunicaciones de dispositivos cliente 110, 120 y 130 en una forma compatible con servicios web 141 y 142. El servidor 140 también puede incluir una capa de autenticación de dispositivo 144 para autenticar dispositivos web 110, 120 y 130, como se analiza en más detalle a continuación.

La autoridad de certificado 150 puede comprender un ordenador de fin general (por ejemplo, un ordenador personal, ordenador de red, servidor u ordenador central) que tienen uno o más procesadores (no mostrados) que pueden activarse selectivamente o reconfigurarse mediante un programa informático. Adicionalmente, la autoridad de certificado 150 puede comunicarse a través de la red 160 con el servidor 140 así como dispositivos cliente 110, 120 y 130. La autoridad de certificado 150 puede implementarse usando parques de servidores, tecnologías distribuidas y diversas combinaciones de software y hardware de una manera análoga a la descripción anterior con respecto a un servidor 140. La autoridad de certificado 150 puede incluir un codificador 151 para generar firmas digitales que se incluyen con certificados digitales, como se analiza en más detalle a continuación.

Los dispositivos cliente 110, 120 y 130 pueden ser cualquier tipo de dispositivo para comunicar con el servidor 140 y autoridad de certificado 150. Por ejemplo, los dispositivos cliente 110, 120 y 130 pueden ser ordenadores personales, dispositivos portátiles (por ejemplo, PDA, teléfonos celulares tales como teléfonos inteligentes, etc.), televisiones, reproductores de música digitales, decodificadores de salón, grabadores de video digital (DVR) o consolas de juegos o cualquier otra plataforma informática o dispositivo apropiado capaz de intercambiar datos con la red 160. Cada uno de los dispositivos cliente 110, 120 y 130 puede incluir, por ejemplo, uno o más procesadores y una o más memorias (no mostrados). Usuarios pueden acceder a los servicios web 141 y 142 en el servidor 140 a través de la red 160 a través de lógica de aplicación adecuada implementada en los dispositivos cliente 111, 121 y 131, tales como un explorador web. Por ejemplo, el servidor 140 puede transmitir un documento (por ejemplo, una página web) que se procesa mediante lógica de aplicación en los dispositivos cliente 111, 121 y 131 y se muestra a un usuario. El documento puede incluir opciones para que un usuario se registre en uno o más servicios seguros proporcionados por el servidor 140, tales como el servicio web 141 y servicio web 142. Por ejemplo, usuarios pueden registrarse en los servicios web 141 y 142 para acceder a contenido digital para usar en los dispositivos cliente 110, 120 y 130, suministrando credenciales, tales como un nombre de usuario (por ejemplo, una dirección de correo electrónico) y una contraseña.

El dispositivo de cliente no fiable 170 puede ser similar a los dispositivos cliente 110, 120 y 130, como se ha analizado anteriormente. Sin embargo, el dispositivo de cliente no fiable 170 puede ser un tipo de dispositivo que no soporta mecanismos de autenticación que están disponibles en el servidor 140. El servidor asociado de confianza 180 puede ser similar al servidor 140, como se ha analizado anteriormente. El servidor asociado de confianza 180 puede proporcionar acceso a un servicio web 181, que puede ser similar a los servicios web 141 y 142. El dispositivo de cliente no fiable 170 puede comunicarse con el servidor asociado de confianza 180 para acceder a los servicios web 141 y 142. Por ejemplo, el dispositivo de cliente no fiable 170 puede autenticar con el servidor asociado de confianza 180 y el servidor asociado de confianza 180 puede proporcionar un testigo seguro al dispositivo de cliente no fiable 170. El dispositivo de cliente no fiable 170 puede a continuación usar el testigo seguro para acceder al servicio web 141.

El servidor 140 puede recibir peticiones de los dispositivos cliente 110-130, dispositivo de cliente no fiable 170 y dispositivo heredado 190 para acceder a los servicios web 141 y 142. El servidor 140 puede a continuación seleccionar un módulo de autenticación apropiado para autenticar cada petición. El módulo de autenticación seleccionado puede depender del dispositivo que emitió la petición. De esta manera, el servidor 140 puede

proporcionar esquemas de autenticación específicos de tipo de dispositivo a través del módulo de autenticación seleccionados.

La Figura 2 muestra un diagrama de un ejemplo de una arquitectura del servidor 140, consistentes con realizaciones divulgadas. Como se ha analizado anteriormente, el servidor 140 puede incluir la capa de compatibilidad de dispositivos 143 para traducir comunicaciones desde los dispositivos cliente 110, 120 y 130 en una forma compatible con los servicios web 141 y 142. El servidor 140 también puede incluir una capa de autenticación de dispositivo 144 para autenticar los dispositivos cliente 110, 120 y 130 usando módulos de autenticación 221-225. El servidor 140 también puede incluir un filtro de autenticación 226 y un selector de módulos 227, que colectivamente sirven para encaminar peticiones desde los dispositivos cliente 110, 120 y 130 hasta uno apropiado de los módulos de autenticación 221-225, como se analiza en más detalle a continuación.

Después de que las peticiones de cliente se autentican mediante uno de los módulos de autenticación 221-225, las peticiones se pasan a un servicio apropiado, tales como el servicio web 141 o servicio web 142. Como alternativa, si las peticiones no se autentican, el módulo de autenticación apropiado puede no encaminar la petición a un servicio. El servicio web 141 puede ser un servicio web "por defecto" o "estándar", al que se encaminan la mayoría de peticiones después de la autenticación. El servicio web 142 puede ser un servicio web heredado con un mecanismo de autenticación incorporado y puede ser específico para un tipo de dispositivo heredado particular tales como el dispositivo heredado 190. Como se analiza a continuación, ya que módulos de autenticación 221-225 autentican diversas peticiones de los dispositivos cliente 110, 120 y 130, las peticiones autenticadas se pasan al servicio web apropiado. Aunque la Figura 2 ilustra un cierto número y disposiciones de componentes, puede usarse cualquier número o disposición de módulos de autenticación u otros componentes en el servidor 140.

La Figura 3 ilustra un diagrama de bloques ilustrativo de una arquitectura del módulo de autenticación 221, consistente con realizaciones divulgadas. El módulo de autenticación 221 puede implementar un esquema de autenticación que se soporta mediante un número de diferentes tipos de dispositivo. Por ejemplo, para propósitos de la siguiente descripción, los dispositivos cliente 110 y 130 son de dos diferentes tipos de dispositivo. Los dispositivos cliente 110 y 130 pueden ambos implementar SSL (Capa de Conexiones Seguras), un protocolo de seguridad que permite comunicaciones seguras a través de una red. El módulo de autenticación 221 puede implementar SSL en el servidor 140 para comunicar de forma segura con y autenticar los dispositivos cliente 110 y 130. En algunas realizaciones, el módulo de autenticación 221 puede implementar el protocolo TLS (Seguridad de Capa de Transporte), una versión mejorada de SSL.

Para implementar procesamiento SSL/TSL, el módulo de autenticación 221 puede almacenar un certificado de servidor 301. El certificado de servidor 301 puede usarse para autenticar el servidor 140 a uno o más dispositivos cliente, como se analiza en más detalle a continuación. El módulo de autenticación 221 también puede almacenar una clave de sesión 302 para cifrar comunicaciones durante una sesión particular de SSL/TSL con uno o más dispositivos cliente. El servidor 140 puede usar el codificador 303 para crear firmas digitales y el servidor 140 puede usar el decodificador 304 para verificar firmas digitales, como se analiza en más detalle a continuación. Dispositivos cliente pueden usar estas sesiones de SSL/TSL para descargar contenido electrónico del servicio web 141.

La Figura 4 ilustra un diagrama de bloques ilustrativo de una arquitectura del módulo de autenticación 222, consistente con realizaciones divulgadas. El módulo de autenticación 222 puede implementar un esquema de autenticación propietario, soportado por uno o más tipos de dispositivo asociados con un fabricante de dispositivo particular. Además, el dispositivo cliente 120 puede ser un dispositivo que usa el esquema de autenticación propietario.

El módulo de autenticación 222 puede implementar el esquema de autenticación propietario en el servidor 140 para comunicarse de forma segura con y autenticar el dispositivo 120. En algunas realizaciones, el módulo de autenticación 222 se proporciona por el fabricante de dispositivo asociado con el esquema de autenticación propietario. El módulo de autenticación 222 puede almacenar un secreto compartido 401, que también se almacena en el dispositivo cliente 120. El módulo de autenticación 222 también puede incluir un verificador de firma 402, que se usa para verificar firmas de peticiones para acceder a servicios web que se envían mediante el dispositivo cliente 120. Los módulos de autenticación 223, 224 y 225 pueden implementar diversos otros esquemas de autenticación. Por ejemplo, el módulo de autenticación 223 puede ser un módulo de "no operación" que simplemente permite que pasen datos a través sin autenticación. El módulo de autenticación 223 puede usarse tanto para propósitos de desarrollo, así como para acceder al servicio web 142. Permitir que la petición pase a través del módulo de autenticación 223 sin autenticar la petición no pone en riesgo la seguridad, porque el servicio web 142 tiene un esquema de autenticación interno.

El módulo de autenticación 224 puede implementar un esquema de "Autenticación de Sesión" con lo que el dispositivo de cliente no fiable 170 puede acceder al servicio web 141. Para hacer esto, el dispositivo de cliente no fiable 170 puede cooperar con el servidor asociado de confianza 180. El servidor asociado de confianza 180 puede acceder al servicio web 141 usando el módulo de autenticación 221 y adquirir un testigo seguro del servidor 140. El servidor 140 puede almacenar una clave criptográfica secreta que se usa para crear el testigo seguro. Como alternativa, el servidor asociado de confianza 180 también puede almacenar una copia de la clave criptográfica. En

tales realizaciones, el servidor asociado de confianza 180 puede crear el testigo seguro. En cualquier caso, el testigo seguro puede comprender datos cifrados, tales como un identificador del dispositivo de cliente no fiable 170.

Una vez que el servidor asociado de confianza 180 ha creado el testigo seguro u obtenido el testigo seguro del servidor 140, el servidor asociado de confianza 180 puede a continuación proporcionar el testigo seguro al dispositivo de cliente no fiable 170. El dispositivo de cliente no fiable 170 puede enviar el testigo con una petición para el servicio web 141 al servidor 140 y el módulo de autenticación 225 puede autenticar la petición validando el testigo. Por ejemplo, el módulo de autenticación 225 puede autenticar el testigo seguro descifrando el testigo con la clave criptográfica y verificar el identificador del dispositivo de cliente no fiable 170.

En algunas realizaciones, el testigo seguro se crea mediante el servidor 140 o el servidor asociado de confianza 180 usando una clave privada de un par de claves asimétricas. En tales realizaciones, puede usarse una clave pública correspondiente para descifrar el testigo seguro para determinar si el testigo seguro es auténtico. El módulo de autenticación 225 puede implementar un esquema de autenticación de lista blanca de IP que almacena una lista de direcciones IP registradas. El módulo de autenticación 225 puede únicamente permitir que peticiones de direcciones IP registradas pasen a través al servicio web 141. Para hacer esto, el módulo de autenticación 225 puede determinar una dirección IP asociada con una petición, comparar la dirección IP con una lista blanca de direcciones IP permitidas y proporcionar acceso al servicio web 141 si la dirección IP asociada con la petición está en la lista blanca.

El módulo de autenticación 225 puede ser particularmente útil cuando se integran nuevos tipos de dispositivo para acceder al servicio web 141. Por ejemplo, un nuevo tipo de dispositivo puede finalmente tener por objeto soportar el esquema de autenticación del módulo de autenticación 221. Sin embargo, cuando se desarrolla e integra el nuevo tipo de dispositivo para acceder al servicio web 141, puede ser más eficiente renunciar a usar el módulo de autenticación 221. Usando la lista blanca de IP para limitar los dispositivos que pueden solicitar el servicio web 141, la integración de dispositivo puede transcurrir más rápidamente. Durante el proceso de integración de dispositivo, el nuevo tipo de dispositivo puede transferirse para usar el módulo de autenticación 221 una vez que se ha probado la funcionalidad principal.

La Figura 5 es un diagrama de flujo de un ejemplo de una rutina 500 para proporcionar acceso a un servicio, consistente con realizaciones divulgadas. La rutina 500 puede implementar procesos de acuerdo con uno o más de módulos de programa almacenados en la memoria 146.

En el inicio de la rutina 500, en el bloque 501, el servidor 140 puede almacenar los módulos de autenticación 221-225 para autenticar los dispositivos cliente 110, 120 y 130, así como el dispositivo de cliente no fiable 170. Como se ha analizado anteriormente, los dispositivos cliente 110, 120 y 130 pueden ser de diversos tipos de dispositivo que usan diferentes esquemas de autenticación. En algunas realizaciones, los módulos de autenticación 221-225 pueden comprender una o más clases implementando cada una una interfaz común. Como se entenderá por los expertos en la materia, una interfaz puede definir un conjunto de los métodos que deben soportar cada clase que implementa la interfaz. Por lo tanto, cada uno de los módulos de autenticación 221-225 puede comprender una clase que suporta un conjunto común de métodos de autenticación definidos por la interfaz.

En el bloque 502, el servidor 140 puede configurar módulos de autenticación 221-225 para implementar los esquemas de autenticación específicos analizados anteriormente. Por ejemplo, un administrador puede interactuar con el servidor 140 para configurar el módulo de aplicación 221 para implementar el protocolo SSL soportado por los dispositivos cliente 110 y 130. El administrador también puede configurar el módulo de aplicación 222 para implementar el protocolo propietario soportado por el dispositivo cliente 120. Análogamente, el administrador también puede configurar los módulos de aplicación 223, 224 y 225 para implementar los esquemas de autenticación de no operación, lista blanca y sesión analizados anteriormente.

Desde la perspectiva de software de aplicación externo en el servidor 140, por ejemplo, puede recurrirse a los servicios web 141 y 142, la capa de compatibilidad de dispositivos 210, filtro de autenticación 226 y selector de módulos 227, los esquemas de autenticación usando uno o más de los métodos definidos por la interfaz común. Por lo tanto, los detalles de los esquemas de autenticación subyacentes pueden extraerse usando la interfaz y software externo puede recurrir a los métodos comunes usando el módulo de autenticación apropiado.

A continuación, en el bloque 503, el servidor 140 puede recibir una petición para acceder al servicio web 141 o servicio web 142. Como se ha analizado anteriormente, el servicio web 141 puede ser un servicio web por defecto, mientras que el servicio web 142 puede ser un servicio web habitualmente accedido por ciertos tipos de dispositivo heredados. Como se analiza en más detalle a continuación, el servidor 140 puede encaminar las peticiones a módulos de autenticación apropiados para autenticar las peticiones, antes de permitir que las peticiones alcancen los servicios web 141 y 142.

A continuación, en el bloque 504, el filtro de autenticación 226 puede extraer un identificador de tipo de dispositivo de la petición para determinar qué tipo de dispositivo está solicitando el servicio web 141. En algunas realizaciones, el filtro de autenticación 226 es un filtro J2EE que busca un encabezamiento de petición o lista de parámetros en la

petición para el identificador de tipo de dispositivo. En algunas realizaciones, pueden usarse otros mecanismos para determinar el tipo de dispositivo, tales como correlacionar un número de serie de dispositivo o ID de MAC con una tabla que almacena tipos de dispositivo correspondientes.

En el bloque 505, el dispositivo el filtro de autenticación 226 puede proporcionar el identificador de tipo de dispositivo extraído al selector de módulos 227. El selector de módulos 227 puede determinar el módulo autenticador apropiado 221-225 para autenticar la petición, basándose en el identificador de tipo de dispositivo extraído. En algunas realizaciones, el selector de módulos 227 es una vaina de java que se configura con una tabla de identificadores de tipo de dispositivo, cada uno de los que se correlaciona a uno en particular de los módulos de autenticación 221-225.

A continuación, en el bloque de decisión 506, el módulo de autenticación que se seleccionó en el bloque 505 puede determinar si autenticar la petición. Como se analiza en más detalle a continuación, cada uno de los módulos de autenticación 221-225 puede implementar diferentes esquemas de autenticación para autenticar las peticiones. Sin embargo, independientemente de qué módulo de autenticación autentica la petición en el bloque de decisión 506, pueden aplicarse técnicas de seguridad adicionales además de las implementadas por el módulo de autenticación seleccionado. Por ejemplo, usuarios de los dispositivos de cliente pueden autenticarse proporcionando un nombre de usuario y contraseña, además de la autenticación requerida por el módulo de autenticación seleccionado. Además, en algunas realizaciones, múltiples módulos de autenticación pueden autenticar colectivamente ciertas peticiones.

Como se muestra en la Figura 5, si el módulo(s) de autenticación seleccionado autentica la petición, la rutina 500 se mueve al bloque 507. En el bloque 507, el servidor 140 proporciona acceso al servicio solicitado, por ejemplo, el servicio web 141/142. Por lo tanto, el dispositivo solicitante puede acceder a contenido electrónico que está disponible desde el servicio web 141/142. Sin embargo, si el módulo(s) de autenticación seleccionado no autentica la petición, la rutina 500 se mueve al bloque 508 y el servidor 140 evita acceso al servicio web 141/142 solicitado. En algunas realizaciones, puede permitirse al dispositivo solicitante un número ilimitado de intentos de autenticación. En otras realizaciones, pueden bloquearse peticiones posteriores desde un dispositivo solicitante después de un cierto número de intentos.

Como se ha analizado anteriormente, en el bloque 505 de la rutina 500, el servidor 140 puede seleccionar un módulo de autenticación para autenticar una petición que se recibe desde un dispositivo. Dependiendo del tipo de dispositivo del dispositivo que envía la petición, se seleccionan diferentes módulos de autenticación en el bloque 505. Por ejemplo, puede seleccionarse uno cualquiera de los módulos de autenticación 221-225. La siguiente descripción proporciona una vista general de procesamiento para seleccionar uno de los módulos de autenticación 221-225.

El módulo de autenticación 221 puede usarse para autenticar tanto el dispositivo cliente 110 como el dispositivo cliente 130. Los dispositivos cliente 110 y 130 pueden ser de diferentes tipos de dispositivo que ambos se correlacionan con el módulo de autenticación 221. Cuando cualquiera del dispositivo cliente 110 o dispositivo cliente 130 envía una petición para el servicio web 141, el selector de módulos 227 selecciona el módulo de autenticación 221. El módulo de autenticación 221 puede a continuación autenticar la petición usando SSL, como se muestra en más detalle a continuación con respecto a la Figura 6. Aunque los dispositivos cliente 110 y 130 pueden ser dispositivos de diferentes tipos que usan diferentes identificadores de tipo de dispositivo, ambos tipos de dispositivo pueden correlacionarse con el módulo de autenticación 221.

El módulo de autenticación 222 puede usarse para autenticar tipos de dispositivo, tales como el dispositivo cliente 120. Por consiguiente, basándose en el identificador de tipo de dispositivo extraído para el dispositivo cliente 120, el selector de módulos 227 puede seleccionar el módulo de autenticación 222. Como se ha analizado anteriormente, el módulo de autenticación 222 implementa un esquema de autenticación propietario, que se soporta mediante el fabricante de ciertos tipos de dispositivo, tales como el dispositivo cliente 120. El módulo de autenticación 222 puede autenticar la petición usando el esquema de autenticación propietario, como se analiza en más detalle a continuación con respecto a la Figura 7. El módulo de autenticación 223 puede usarse para autenticar tipos de dispositivo heredados, tales como el dispositivo heredado 190. Como se ha analizado, el dispositivo heredado 190 usa el servicio web 142, un servicio web heredado con un esquema de autenticación incorporado. Basándose en el identificador de tipo de dispositivo extraído de peticiones del dispositivo heredado 190, el selector de módulos 227 puede seleccionar el módulo de autenticación 223. Como se ha analizado, el módulo de autenticación 223 puede implementar un esquema de autenticación de no operación, porque se permite que peticiones pasen directamente a través del módulo de autenticación 223 al servicio web 142. Sin embargo, puede mantenerse la seguridad porque el servicio web 142 implementa mecanismos de autenticación heredados incorporados para autenticar la petición. En algunas realizaciones, puede accederse a peticiones para el servicio web 142 en un URL distinto de peticiones para acceder al servicio web 141.

El módulo de autenticación 224 puede usarse para autenticar dispositivos, tales como el dispositivo de cliente no fiable 170. El dispositivo de cliente no fiable 170 puede usar un identificador de tipo de dispositivo que el selector de módulos 227 no reconoce. Cuando un identificador de tipo de dispositivo no es de un dispositivo fiable, el selector de módulos 227 puede seleccionar el módulo de autenticación 224 para autenticar la petición a través del servidor

asociado de confianza 180. Para hacer esto, el dispositivo de cliente no fiable 170 puede incluir un identificador del servidor asociado de confianza 180 con la petición. El módulo de autenticación 224 puede crear un testigo seguro y transmitir el testigo seguro al servidor asociado de confianza 180. Como alternativa, el servidor asociado de confianza 180 puede crear el testigo seguro. El testigo seguro puede crearse cifrando datos, tales como un identificador del dispositivo de cliente no fiable 170, con una clave criptográfica.

El dispositivo de cliente no fiable 170 puede realizar etapas para autenticar con el servidor asociado de confianza 180, en lugar de autenticarse directamente con el servidor 140. Por ejemplo, el dispositivo de cliente no fiable 170 puede autenticar con el servidor asociado de confianza 180 usando un nombre de usuario y contraseña. Una vez que el servidor asociado de confianza 180 ha autenticado la petición, el servidor asociado de confianza 180 puede transmitir el testigo seguro al dispositivo de cliente no fiable 170.

El dispositivo de cliente no fiable 170 puede acceder al servicio web 141 incluyendo el testigo seguro en comunicaciones posteriores con el servidor 140. Por ejemplo, el módulo de autenticación 224 puede autenticar el testigo seguro descifrando el testigo seguro con la clave criptográfica. En algunas realizaciones, el testigo seguro puede expirar después de una duración preestablecida. El servidor 140 puede no permitir acceso al servicio web 141 usando testigos expirados.

El módulo de autenticación 225 puede implementar un esquema de autenticación de lista blanca de IP. Ya que esta técnica puede implementarse fácilmente sin ningún soporte correspondiente por o modificaciones a dispositivos cliente, el módulo de autenticación 225 puede usarse en prácticamente cualquier petición para el servicio web 141 o 142. Por ejemplo, el módulo de autenticación 225 puede usarse para autenticar cualquier petición desde los dispositivos cliente 110 y 130. En tales realizaciones, el módulo de autenticación 225 puede comprobar la dirección IP del dispositivo que envío la petición. Si la dirección IP está en la lista blanca, el módulo de autenticación 225 podría a continuación proporcionar la petición al módulo de autenticación 221 para posterior procesamiento. El módulo de autenticación 225 puede usarse de manera similar en conjunto con los módulos de autenticación 222, 223 y 224. Además, como se ha analizado anteriormente, en algunas realizaciones, el módulo de autenticación 225 puede usarse para autenticación independiente de peticiones. Por ejemplo, el módulo de autenticación 225 puede usarse durante una fase de integración de dispositivo cuando el servicio web 141 se está probando para soportar un nuevo tipo de dispositivo.

En algunas realizaciones, uno o más de los módulos de autenticación 221-225 pueden proporcionar acceso limitado al servicio web 141, incluso si el dispositivo solicitante no se autentica. Por ejemplo, el servicio web 141 puede proporcionar una pluralidad de métodos, algunos de los cuales se usan para acceder a contenido electrónico, y otros que se usan para explorar diversas características del servicio web 141. En tales realizaciones, uno o más de los módulos de autenticación 221-225 pueden proporcionar acceso al servicio web 141 cuando el dispositivo solicitante está accediendo a métodos usados para explorar el servicio web 141, pero pueden requerir autenticación antes de permitir que el dispositivo solicitante acceda a métodos para descargar contenido electrónico.

Autenticación SSL/TSL

Como se ha analizado anteriormente, el módulo de autenticación 221 puede usar SSL o TSL para realizar autenticación de peticiones para el servicio web 141. La Figura 6 ilustra una rutina ilustrativa 600 usada por el módulo de autenticación 221 para implementar el bloque 506 de la rutina 500. La siguiente descripción supone que el dispositivo cliente 110 está solicitando acceso al servicio web 141. Sin embargo, como ya se ha analizado, los dispositivos cliente 110 y 130 pueden ambos soportar autenticación SSL/TSL. Como se analiza a continuación, tanto el dispositivo cliente 110 como el servidor 140 pueden realizar etapas para autenticarse entre sí usando la rutina 600.

En el bloque 601, el módulo de autenticación 221 puede recibir una petición para el servicio web 141 desde el dispositivo cliente 110. Como se ha analizado, la petición puede ser para acceder a cualquier tipo de datos seguros, tal como contenido electrónico disponible en el servicio web 141. Además, como se ha analizado, la petición puede pasarse al módulo de autenticación 221 desde el selector de módulos 227.
A continuación, en el bloque 602, el módulo de autenticación 221 en el servidor 140 puede enviar el certificado de servidor 301 almacenado al dispositivo cliente 110. El certificado de servidor 301 puede incluir un identificador para el servidor 140, un identificador de autoridad de certificado 150 y una clave de encriptación pública única al servidor 140. El certificado de servidor 301 también puede incluir una firma digital generada por la autoridad de certificado 150.

Después de que el dispositivo cliente 110 recibe el certificado de servidor 301, en el bloque 603, el dispositivo cliente 110 autentica el servidor 140 usando el certificado de servidor 301. Por ejemplo, el dispositivo cliente 110 puede verificar primero la firma digital para garantizar que el certificado de servidor 301 se creó por la autoridad de certificado 150. A continuación, el dispositivo cliente 110 puede extraer la clave de encriptación pública del certificado de servidor 301 y usar la clave de encriptación pública para autenticar comunicaciones desde el servidor 140. A continuación, en el bloque 604, el dispositivo cliente 110 puede enviar un certificado cliente al servidor 140. El certificado cliente puede incluir un identificador del dispositivo cliente 110, un identificador de autoridad de certificado

150 y una clave pública única al dispositivo cliente 110. El certificado cliente también puede incluir una firma digital que se generó por la autoridad de certificado 150 usando el codificador 151. Por ejemplo, antes de la rutina 600, la autoridad de certificado 150 puede haber generado el certificado cliente, transmitido el certificado al dispositivo cliente 110 y almacenado el certificado cliente en el dispositivo cliente 110.

A continuación, en el bloque 605, el servidor 140 autentica el dispositivo cliente 110 usando el certificado cliente. Por ejemplo, el servidor 140 puede verificar primero la firma digital en el certificado cliente para garantizar que el certificado de servidor 301 se creó por la autoridad de certificado 150. A continuación, el servidor 140 puede extraer la clave de encriptación pública del certificado cliente y usar la clave de encriptación pública para verificar comunicaciones desde el dispositivo cliente 110, usando el decodificador 304. A continuación, la rutina 600 se mueve al bloque 608. En el bloque 606, el dispositivo cliente 110 y el servidor 140 pueden establecer mutuamente una clave privada usada para cifrar comunicaciones entre ellos. Esta clave privada se muestra en la Figura 3 como la clave de sesión 302. En el bloque 609, el dispositivo cliente 110 puede acceder al servicio web 141 usando comunicaciones cifradas mediante la clave de sesión 302. En algunas realizaciones, la clave de sesión 302 es una clave de encriptación simétrica, que permite un procesamiento de encriptación más eficiente por el servidor 140 y el dispositivo cliente 110.

En algunas realizaciones, el dispositivo cliente 110 puede autenticar comunicaciones del servidor 140 en el bloque 603 verificando firmas digitales que el servidor 140 adjunta a las comunicaciones. En tales realizaciones, el servidor 140 puede generar las firmas digitales usando el codificador 303 con una clave de encriptación privada única que se proporcionó al servidor 140 antes de la rutina 600 por la autoridad de certificado 150. Esta clave privada única puede ser una clave de un par de claves asimétricas que también incluye la clave pública única asignada al servidor 140.

De manera similar, en algunas realizaciones, el servidor 140 puede autenticar comunicaciones del dispositivo cliente 110 en el bloque 605 verificando firmas digitales que el dispositivo cliente 110 adjunta a las comunicaciones. En tales realizaciones, el dispositivo cliente 110 puede generar las firmas digitales usando una clave de encriptación privada única proporcionada al dispositivo cliente 110 antes de la rutina 600 por la autoridad de certificado 150. Esta clave privada única puede ser una clave de un par de claves asimétricas que también incluye la clave pública única asignada al dispositivo cliente 110.

En otras realizaciones más, el módulo de autenticación 221 puede no realizar todos los bloques de la rutina 600. Por ejemplo, puede proporcionarse un módulo de equilibrio de carga separado (no mostrado) en el servidor 140. El módulo de equilibrio de carga puede ser responsable de la distribución de cargas de trabajo a través de una pluralidad de servidores y también puede implementar procesamiento SSL/TSL. En tales realizaciones, el módulo de equilibrio de carga implementa la rutina 600 y proporciona un resultado al módulo de autenticación 221 indicando si el certificado cliente se determina como válido en el bloque 605. Si es así, el módulo de autenticación 221 permite acceso al servicio web 141. De otra manera, el módulo de autenticación 221 evita el acceso al servicio web 141.

Autenticación propietaria

Como se ha analizado anteriormente, el dispositivo cliente 120 puede soportar un esquema de autenticación propietario y el módulo de autenticación 222 puede implementar el esquema de autenticación propietario en el servidor 140. La Figura 7 es un diagrama de flujo de un ejemplo de una rutina 700 para implementar un esquema de autenticación de este tipo. La rutina 700 puede implementar procesos de acuerdo con uno o más de módulos de programa almacenados en la memoria 146.

En el bloque 701, el secreto compartido puede almacenarse en el dispositivo cliente 120. En algunas realizaciones, el secreto compartido 401 es una clave de encriptación simétrica. Como alternativa, puede usarse un par de claves asimétricas para el secreto compartido 401. En realizaciones donde el secreto compartido 401 es un par de claves asimétricas, el dispositivo cliente 120 puede almacenar una de las claves del par y el módulo de autenticación 222 puede almacenar la otra clave del par.

En el bloque 702, secreto compartido 401 se almacena en el módulo de autenticación 222, mostrado en la Figura 4 como el secreto compartido 401. Esto puede requerir alguna coordinación entre el fabricante del dispositivo cliente 120 y el operador del servicio web 141. Por ejemplo, el fabricante puede embeber el secreto compartido en una memoria a prueba de manipulación en el dispositivo cliente 120 y proporcionar el secreto compartido 401 a través de canales seguros al operador del servicio web 141.

En el bloque 703, el dispositivo cliente 120 puede preparar una petición para el servicio web 141. La petición puede ser un bloque de datos no cifrados que identifican el contenido electrónico particular que se solicita desde el servicio web 141. La petición también puede incluir información que identifica el dispositivo cliente 120 al módulo de autenticación 222.

A continuación, en el bloque 704, el dispositivo cliente 120 puede firmar la petición para el servicio web 121 usando el secreto compartido 401. Por ejemplo, el dispositivo cliente 120 puede calcular un troceo como una función de la

petición más el secreto compartido 401. El dispositivo cliente 120 puede adjuntar el troceo a la petición como una firma. En algunas realizaciones, el dispositivo cliente 120 también puede cifrar la petición firmada.

En el bloque 705, el dispositivo cliente 120 puede enviar la petición firmada al servidor 140. A continuación, en el bloque 706, el módulo de autenticación 222 puede verificar la forma en la petición usando el verificador de firma 402. Por ejemplo, el verificador de firma 402 puede calcular la función de troceo de la petición más el secreto compartido y comparar el valor de troceo con la firma adjuntada. Si los valores coinciden, el módulo de autenticación 222 considera la petición intacta, por ejemplo, ningún atacante ha manipulado la petición. En el bloque 707, se permite que el dispositivo cliente 120 acceda al servicio web 141 si se verifica la firma en la petición. De otra manera, en el bloque 708, se evita acceso al servicio web 141.

Como un experto en la materia apreciará, uno o más de los bloques 501-508, 601-609 y 701-708 pueden ser opcionales y pueden omitirse de implementaciones en ciertas realizaciones. Adicionalmente, en algunas implementaciones, los bloques 501-508, 601-607 y 701-708 pueden reordenarse, incluir etapas sustitutas y/o incluir etapas adicionales.

Uso adicional de testigos

Como se ha analizado, el módulo de autenticación 224 puede usar un testigo seguro para autenticar comunicaciones con el dispositivo de cliente no fiable 170. En la implementación analizada, el servidor asociado de confianza 180 puede realizar procesamiento de autenticación con el dispositivo de cliente no fiable 170 y el servidor asociado de confianza 180 puede transmitir un testigo seguro al dispositivo de cliente no fiable 170. Sin embargo, una implementación de testigo seguro no se limita al uso con cualquier módulo de autenticación particular. En su lugar, pueden implementarse testigos seguros además de cualquiera de los módulos de autenticación 221-225.

En algunas realizaciones, un testigo seguro puede basarse en una clave criptográfica simétrica. La clave simétrica puede compartirse de alguna manera segura entre el servidor 140 y un dispositivo cliente particular. En algunas realizaciones, dispositivos cliente se llenan previamente con un testigo basándose en la clave simétrica. Por ejemplo, antes de que el dispositivo cliente 110 se distribuyan un usuario, una función de troceo de la ID de MAC, número de serie o combinación de las dos puede calcularse usando la clave simétrica como una entrada a la función de troceo. En algunas realizaciones, la clave simétrica puede generarse junto con el testigo correspondiente en el momento que un usuario recibe el dispositivo cliente 110 (por ejemplo, cuando un usuario compra el dispositivo de un vendedor tal como una tienda online). En otras realizaciones, el servidor 140 puede crear el testigo usando un par de claves asimétricas. Una clave privada del par puede usarse para cifrar el testigo seguro antes de proporcionar el testigo seguro al dispositivo cliente 110.

Una vez que el dispositivo cliente 110 se llena con el testigo seguro, el testigo seguro puede usarse para seguridad adicional. Por ejemplo, si el testigo seguro se usa en conjunto con el módulo de autenticación 221, el usuario puede no necesitar autenticarse usando un nombre de usuario y contraseña Una vez que la sesión SSL/TSL se establece entre el servidor 140 y el dispositivo cliente 110. En su lugar, el dispositivo cliente 110 puede transmitir el testigo seguro al servidor 140. El servidor 140 puede descifrar el testigo usando la clave simétrica o, si se usa encriptación asimétrica, la clave pública del par de claves. Esta implementación ahorra al usuario algunos inconvenientes al tener que remitir su nombre de usuario y contraseña cada vez que quieren acceder al servicio web 141, porque el testigo puede usarse como un sustituto para el nombre de usuario y contraseña.

La descripción anterior se ha presentado para propósitos de ilustración. No es exhaustiva y no se limita a las formas o realizaciones precisas divulgadas. Modificaciones y adaptaciones serán evidentes para expertos en la materia a partir de la consideración de la memoria descriptiva y practica de las realizaciones divulgadas. Por ejemplo, las implementaciones descritas incluyen software, pero sistemas y métodos consistentes con las realizaciones divulgadas pueden implementarse como una combinación de hardware y software o solo en hardware. Ejemplos de hardware incluyen sistemas de cálculo o procesamiento, incluyendo ordenadores personales, servidores, portátiles, grandes ordenadores, microprocesadores y similares. Adicionalmente, aunque aspectos de las realizaciones divulgadas se describen como que se almacenan en memoria, un experto en la materia apreciará que estos aspectos también pueden almacenarse en otros tipos de medio legible por ordenador, tales como dispositivos de almacenamiento secundarios, por ejemplo, discos duros, discos flexibles o CDROM u otras formas de RAM o ROM, medios USB, DVD u otros medios de disco óptico.

Programas informáticos basándose en la descripción escrita y métodos divulgados están dentro de los conocimientos de un desarrollador experimentado. Los diversos programas o módulos de programa pueden crearse usando cualquiera de las técnicas conocidas para un experto en la materia o pueden diseñarse en conexión con software existente. Por ejemplo, secciones de programa o módulos de programa pueden diseñarse en o por medio de .Net Framework, .Net Compact Framework (y lenguajes relacionados, tales como Visual Basic, C, etc.), Java, C++, HTML, combinaciones de HTML/AJAX, XML o HTML con mini-aplicaciones Java incluidas. Uno o más de tales secciones de software o módulos pueden integrarse en un sistema informático o software existente de correo electrónico o navegación.

Además, mientras realizaciones ilustrativas se han descrito en este documento, el alcance de cualquiera y todas las realizaciones que tienen elementos equivalentes, modificaciones, omisiones, combinaciones (por ejemplo, de aspectos a través de diversas realizaciones), adaptaciones y/o alteraciones como se reconocerían por los expertos en la técnica basándose en la presente divulgación. Las limitaciones en las reivindicaciones se deben interpretar ampliamente basándose en el lenguaje empleado en las reivindicaciones y no limitarse a ejemplos descritos en la presente memoria descriptiva o durante el procesamiento de la aplicación, cuyos ejemplos deben interpretarse como no exclusivos. Además, los bloques de las rutinas divulgadas pueden modificarse de cualquier manera, incluyendo reordenar bloques y/o insertar o eliminar bloques. Se concibe, por lo tanto, que la memoria descriptiva y ejemplos se consideran únicamente como ilustrativos, siendo un alcance verdadero indicado mediante las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método implementado por ordenador (500) para proporcionar acceso a un servicio, que comprende:

recibir (503) una petición de acceso a servicio, incluyendo la petición un identificador de tipo de dispositivo de un dispositivo que solicita acceso al servicio;
extraer (504) el identificador de tipo de dispositivo de la petición;
determinar un tipo de dispositivo correspondiente para el dispositivo solicitante;
seleccionar (505) un módulo de autenticación de una pluralidad de módulos de autenticación basándose en el identificador de tipo de dispositivo, en el que uno de la pluralidad de módulos de autenticación se selecciona basándose en que el dispositivo solicitante es un dispositivo no fiable que tiene un identificador de tipo de dispositivo no reconocido, implementando el módulo de autenticación seleccionado un esquema de autenticación para el tipo de dispositivo del dispositivo solicitante;
autenticar (506) la petición usando el módulo de autenticación seleccionado para determinar si se permite que el dispositivo solicitante acceda al servicio, en el que la autenticación incluye autenticar una petición que corresponde a un dispositivo no fiable a través de un servidor asociado de confianza;
proporcionar (507) acceso al servicio basándose en al menos una determinación de que el dispositivo solicitante está autorizado para acceder al servicio; y
evitar (508) acceso al servicio basándose en al menos una determinación de que el dispositivo solicitante no está autorizado para acceder al servicio.

2. El método implementado por ordenador de acuerdo con la reivindicación 1, en el que el módulo de autenticación seleccionado comparte datos secretos con el dispositivo solicitante para determinar si el dispositivo solicitante está autorizado para acceder al servicio.

3. El método implementado por ordenador de acuerdo con la reivindicación 1, en el que el módulo de autenticación seleccionado proporciona acceso a una pluralidad de métodos y un subconjunto de los métodos están accesibles a dispositivos no autenticados.

4. El método implementado por ordenador de acuerdo con la reivindicación 1, en el que una pluralidad de dispositivos que tienen una pluralidad de tipos de dispositivo acceden al servicio a través del módulo de autenticación seleccionado.

5. El método implementado por ordenador de acuerdo con la reivindicación 1, en el que al menos se accede a dos de los módulos de autenticación usando una URL común.

6. El método implementado por ordenador de acuerdo con la reivindicación 1, en el que el servidor asociado de confianza proporciona un testigo al dispositivo solicitante, comprendiendo el método además:

recibir una copia del testigo desde el dispositivo solicitante; y
proporcionar acceso al servicio basándose en una determinación de que la copia del testigo es auténtica.

7. El método implementado por ordenador de acuerdo con la reivindicación 6, en el que el testigo está cifrado con una clave privada que corresponde a una clave pública de un par de claves privada/pública, comprendiendo el método además:

descifrar el testigo con la clave pública correspondiente para determinar si el testigo es auténtico.

8. El método implementado por ordenador de acuerdo con la reivindicación 6, en el que se proporciona el testigo al dispositivo solicitante mediante el servidor asociado de confianza después de que el servidor asociado de confianza verifica una combinación de nombre de usuario y contraseña recibida desde el dispositivo solicitante.

9. El método implementado por ordenador de acuerdo con la reivindicación 1, que comprende adicionalmente:

prealmacenar un testigo en el dispositivo solicitante antes de recibir la petición desde el dispositivo solicitante; y
autenticar la petición usando el módulo de autenticación seleccionado verificando que la petición está acompañada por el testigo prealmacenado.

10. Un servidor (140) para proporcionar acceso a un servicio (141, 142), comprendiendo el servidor:

un procesador (145) para ejecutar instrucciones de programa; y
un medio legible por ordenador (146) que almacena las instrucciones de programa, realizando las instrucciones de programa, cuando se ejecutan por el procesador, un proceso para realizar el método de una cualquiera de las reivindicaciones anteriores.

11. Un medio legible por ordenador que almacena instrucciones de programa para realizar un método ejecutado por un procesador, comprendiendo el método el método de una cualquiera de las reivindicaciones 1-9.

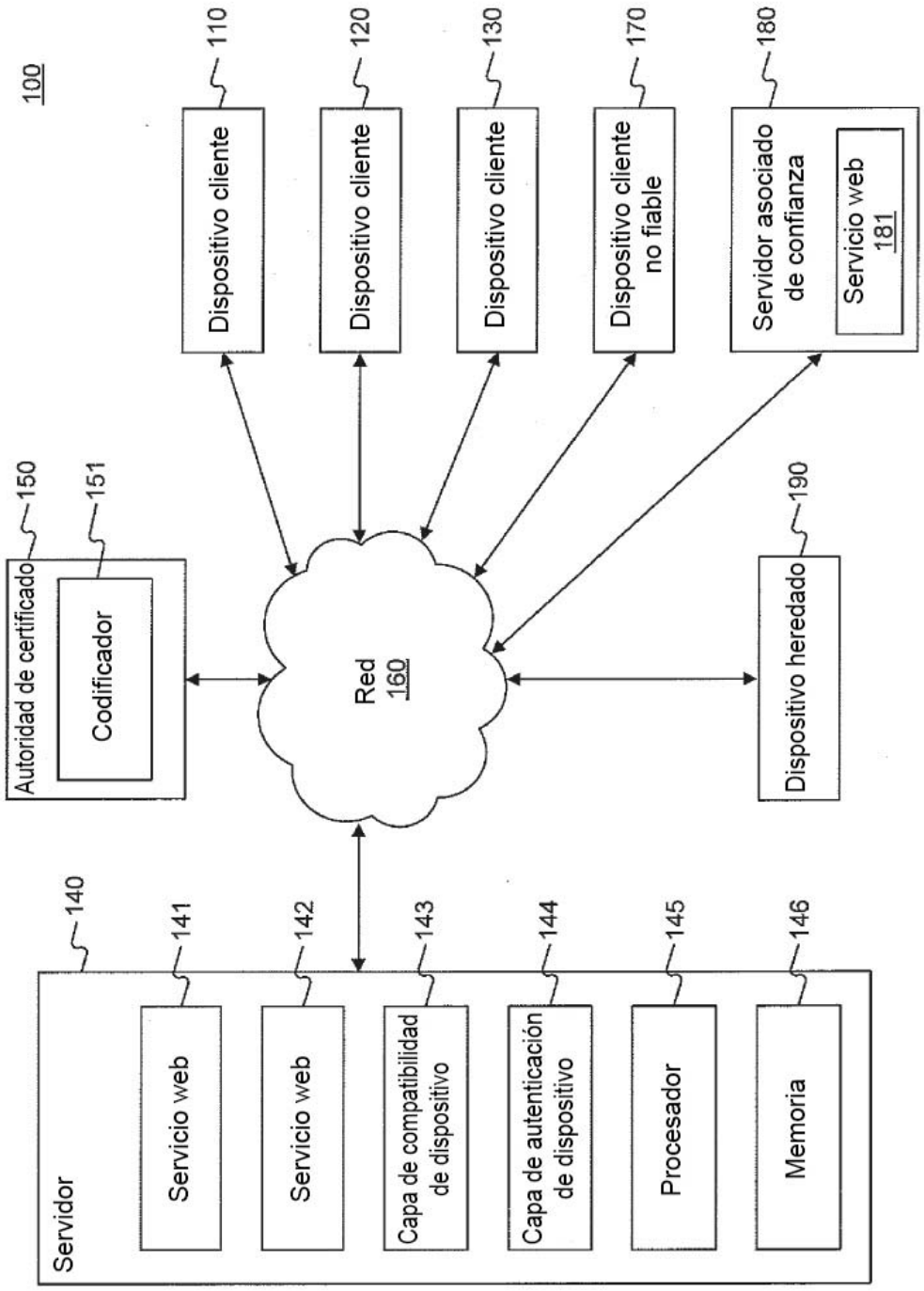
100
Dispositivo cliente
110
Dispositivo cliente
120
Dispositivo cliente
130
Dispositivo cliente no fiable
170
Servidor asociado de confianza
180
Servicio web
181
Autoridad de certificado
150
Codificador
151
Red
160
Dispositivo heredado
190
Servidor
140
Servicio web
141
Servicio web
142
Capa de compatibilidad de dispositivo
143
Capa de autenticación de dispositivo
144
Procesador
145
Memoria
146

FIG. 1

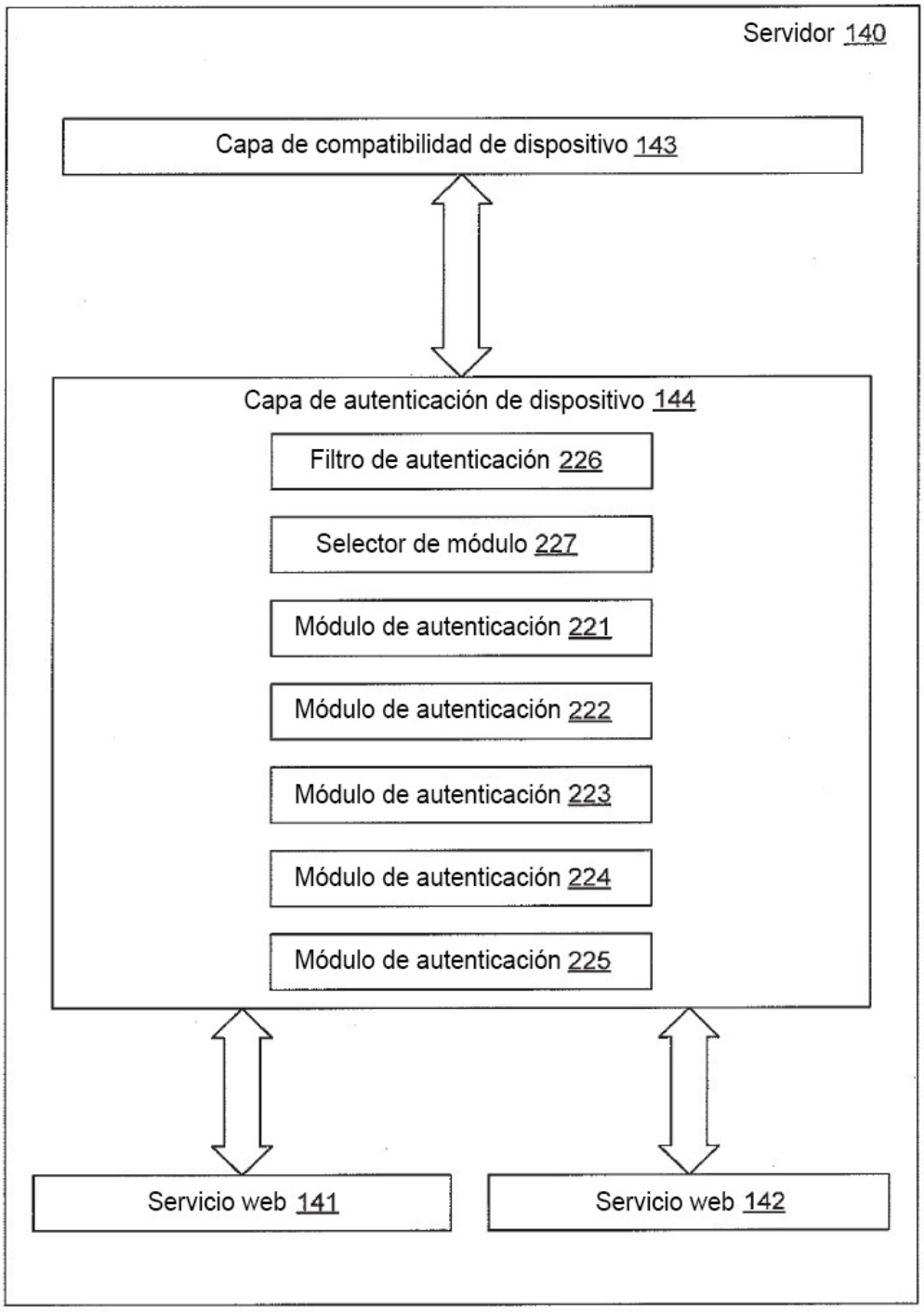
Servidor 140
Capa de compatibilidad de dispositivo 143
Capa de autenticación de dispositivo 144
Filtro de autenticación 226
Selector de módulo 227
Módulo de autenticación 221
Módulo de autenticación 222
Módulo de autenticación 223
Módulo de autenticación 224
Módulo de autenticación 225
Servicio web 141
Servicio web 142

FIG. 2

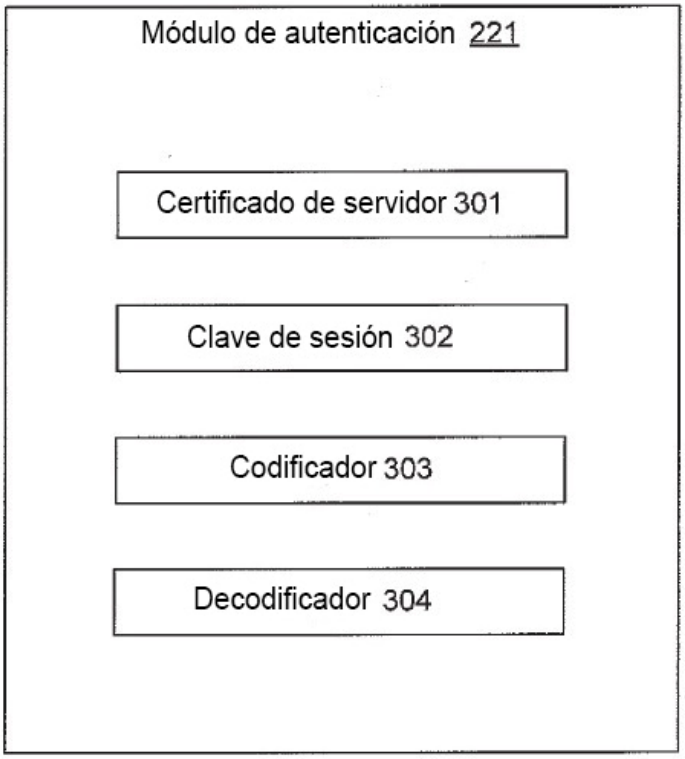
Módulo de autenticación 221
Certificado de servidor 301
Clave de sesión 302
Codificador 303
Decodificador 304

FIG. 3

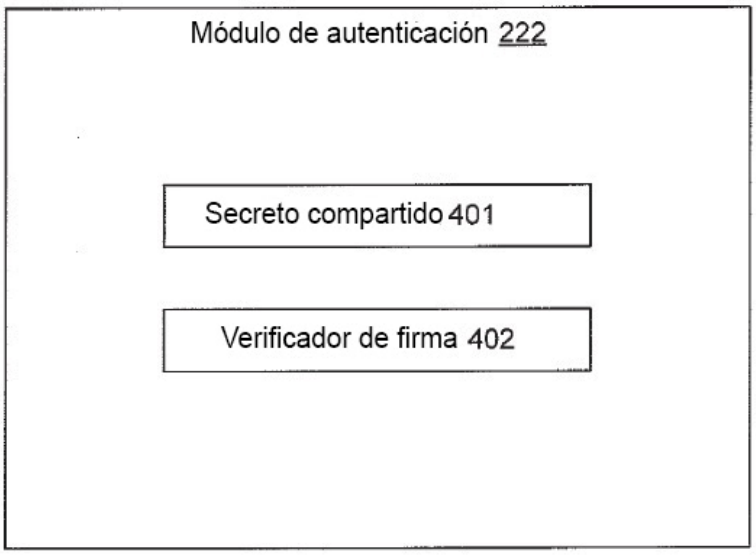
Módulo de autenticación 222
Secreto compartido 401
Verificador de firma 402

FIG. 4

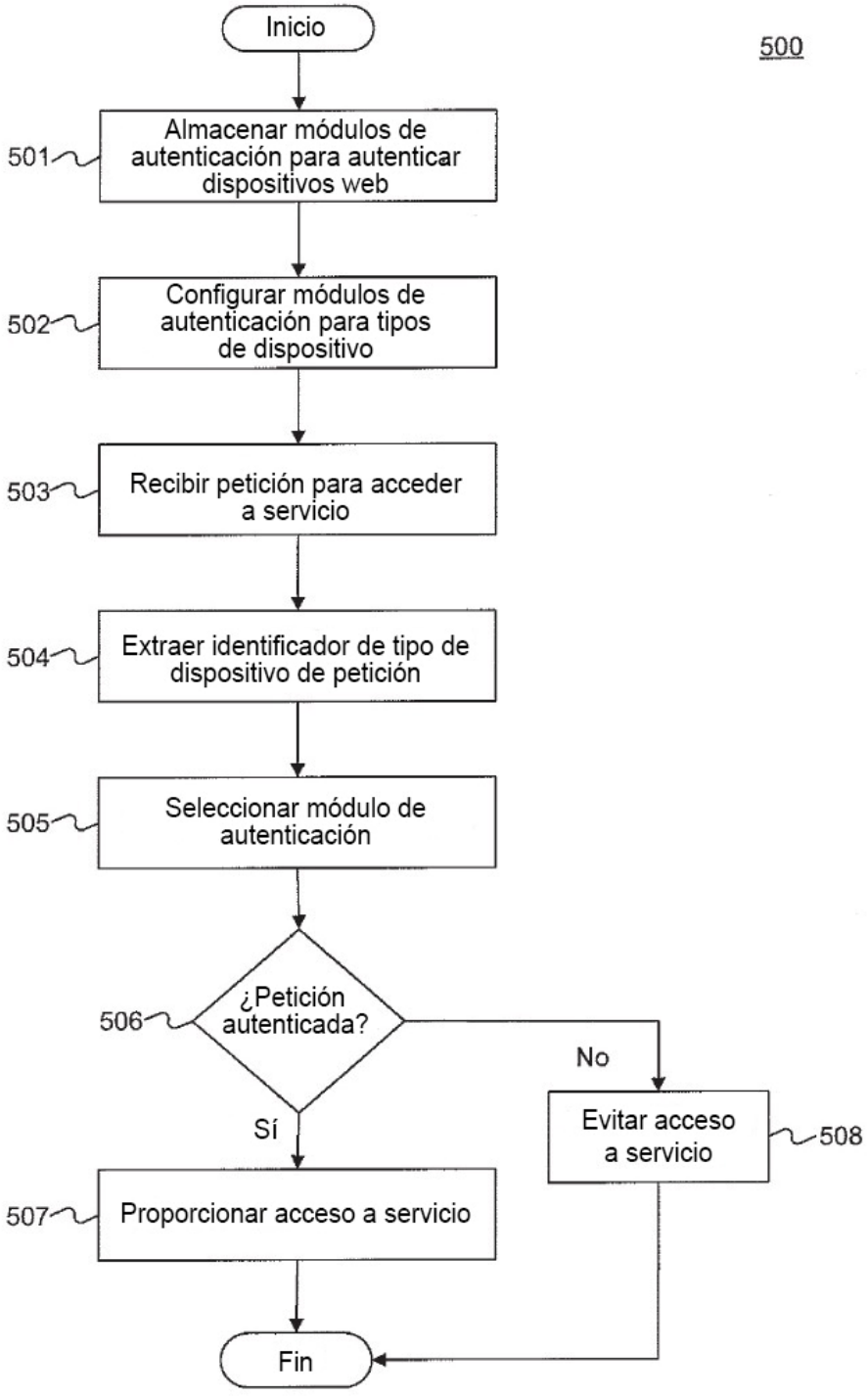
Inicio
500
Almacenar módulos de autenticación para autenticar dispositivos web
501
Configurar módulos de autenticación para tipos de dispositivo
502
Recibir petición para acceder a servicio
503
Extraer identificador de tipo de dispositivo de petición
504
Seleccionar módulo de autenticación
505
¿Petición autenticada?
506
No
Sí
Evitar acceso a servicio
508
Proporcionar acceso a servicio
507
Fin

FIG. 5

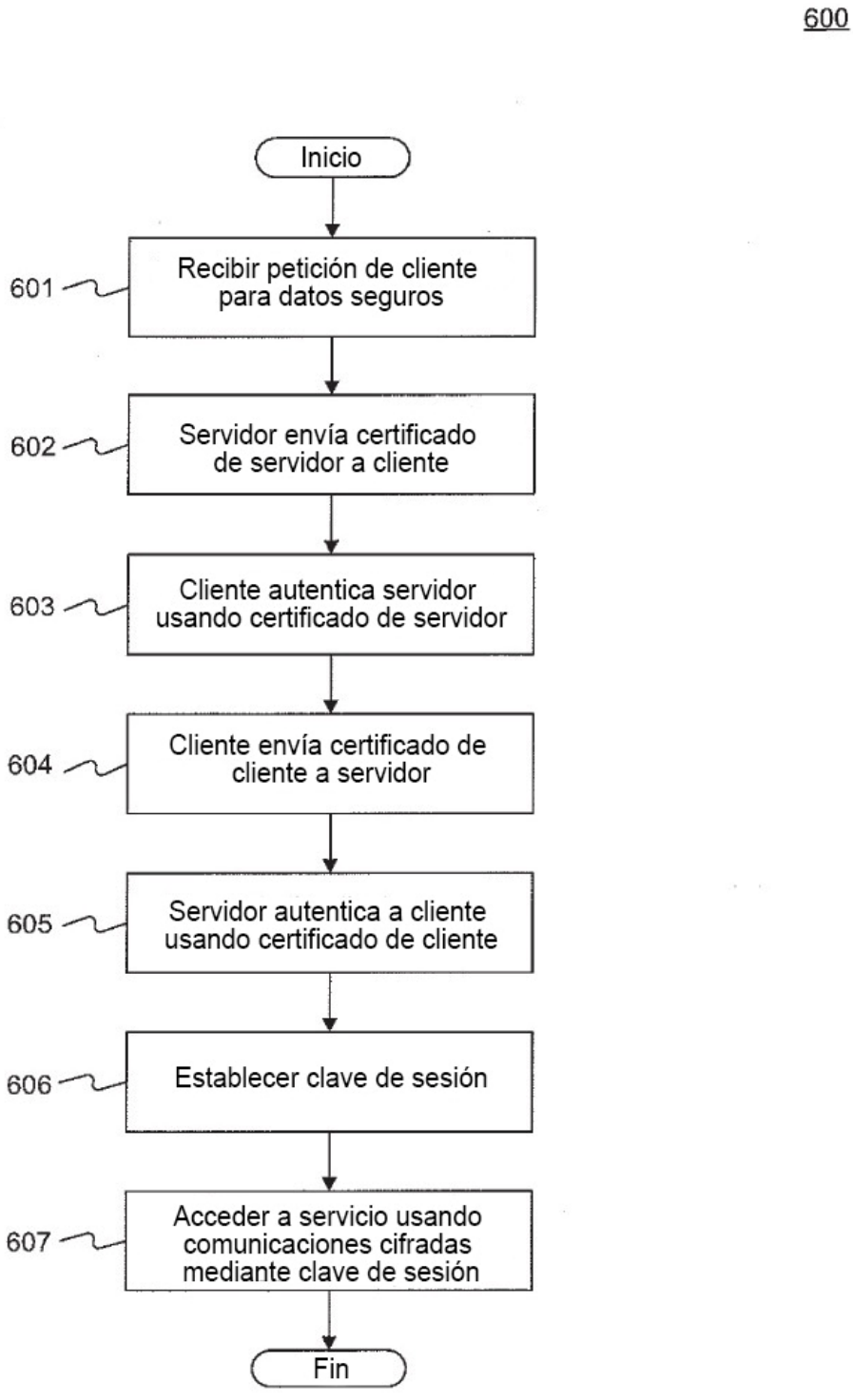
600
Inicio
601
Recibir petición de cliente para datos seguros
602
Servidor envía certificado de servidor a cliente
603
Cliente autentica servidor usando certificado de servidor
604
Cliente envía certificado de cliente a servidor
605
Servidor autentica a cliente usando certificado de cliente
606
Establecer clave de sesión
607
Acceder a servicio usando comunicaciones cifradas mediante clave de sesión
Fin

FIG. 6

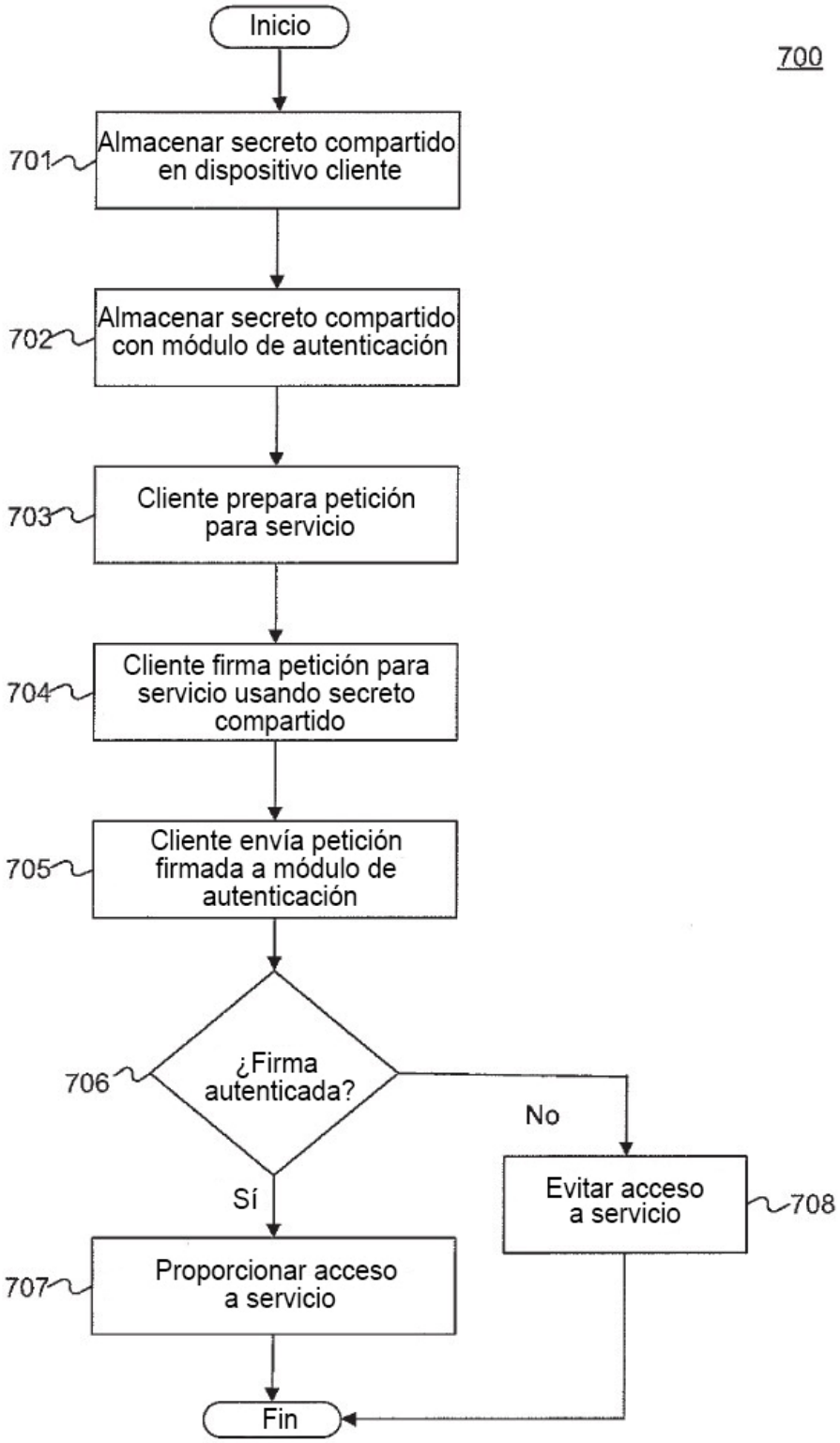
Inicio
700
701
Almacenar secreto compartido en dispositivo cliente
702
Almacenar secreto compartido con módulo de autenticación
703
Cliente prepara petición para servicio
704
Cliente firma petición para servicio usando secreto compartido
705
Cliente envía petición firmada a módulo de autenticación
706
¿Firma autenticada?
No
Sí
708
Evitar acceso a servicio
707
Proporcionar acceso a servicio
Fin

FIG. 7