(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 955 941**

(51) Int. CI.:

G06F 21/33 (2013.01)
G06F 21/40 (2013.01)
H04L 9/40 (2012.01)
G06F 21/32 (2013.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.03.2008 PCT/US2008/057375**

(87) Fecha y número de publicación internacional: **30.10.2008 WO08130760**

(96) Fecha de presentación y número de la solicitud europea: **18.03.2008 E 08732419 (0)**

(97) Fecha y número de publicación de la concesión europea: **23.08.2023 EP 2149102**

(54) Título: **Autenticación específica de petición para acceder a recursos de servicio web**

(30) Prioridad:

20.04.2007 US 912986 P
01.02.2008 US 24901

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2023

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052-6399, US

(72) Inventor/es:

MCMURTRY, CRAIG;
WEINERT, ALEXANDER, T.;
MELESHUK, VADIM y
GABARRA, MARK, E.

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Autenticación específica de petición para acceder a recursos de servicio web

Antecedentes

Cuando un usuario intenta acceder a un recurso remoto protegido a través de una red, tal como Internet, el usuario típicamente se ajusta a las declaraciones de política emitidas por un servidor que controla ese recurso. Las declaraciones de política proporcionan un conjunto de reglas de autenticación y de autorización requeridas para iniciar la comunicación con un recurso. Por ejemplo, la declaración de política puede requerir que un usuario proporcione una contraseña antes de acceder a un recurso. Si el usuario proporciona la contraseña correcta, se autentica la identidad del usuario y se permite el acceso al recurso.

Si bien el método de autenticación de declaración de política funciona bien en situaciones en las que basta una manera de autenticación para iniciar la comunicación con un recurso protegido, las declaraciones de política no funcionan bien en entornos dinámicos. En un entorno dinámico, una única instancia de autenticación al inicio de las comunicaciones entre un cliente y un recurso protegido puede no ser suficiente. Por ejemplo, cuando un usuario intenta acceder a un sitio web con recursos protegidos, puede ser inicialmente suficiente que el usuario proporcione autenticación introduciendo una contraseña. Sin embargo, una vez que el usuario ha accedido al sitio web puede intentar cambiar su contraseña, actualizar un directorio, acceder a un recurso altamente protegido o pedir los privilegios de un grupo de acceso elevado, tal como el grupo de administradores de sistema. En tal caso, el usuario pide hacer algo más que simplemente ver información. Estas acciones tienen el potencial de causar un daño tremendo al recurso protegido.

Algunos métodos de autenticación requieren autenticación antes de permitir la comunicación con un recurso. Sin embargo, en un entorno dinámico es difícil determinar qué reglas de autenticación y de autorización aplicar hasta que se reciba una petición real pidiendo acceso a un recurso protegido.

El documento WO 01/11451 A1 describe un servicio de inicio de sesión que proporciona un cambio de nivel de credencial sin pérdida de continuidad de sesión. En particular, se describe una arquitectura de seguridad en la que se proporciona un inicio de registro único desde múltiples recursos de información. La arquitectura de seguridad asocia requisitos de nivel de confianza con recursos de información. Se emplean esquemas de autenticación (por ejemplo, aquellos basados en contraseñas, certificados, técnicas biométricas, tarjetas inteligentes, etc.) dependiendo de los requisitos de nivel de confianza de los recursos de información a los que se accede. Una vez que se han obtenido las credenciales para una entidad y la entidad ha sido autenticada a un nivel de confianza dado, se concede acceso, sin necesidad de credenciales ni autenticación adicionales, a los recursos de información para los cuales es suficiente el nivel de confianza autenticado. La arquitectura de seguridad permite actualizar las credenciales para una sesión determinada. Una aplicación de cliente actuada por un usuario interactúa con la arquitectura de seguridad mediante un componente de control de acceso y de controlador de entrada y un componente de inicio de sesión. Los componentes de controlador de acceso y de controlador de entrada proporcionan un punto de entrada para aplicaciones de cliente externas que piden acceso a aplicaciones y/o a recursos de empresa.

El objeto de la presente invención es proporcionar un esquema de autenticación mejorado para acceder a recursos de servicios web.

Este objeto se consigue mediante el objeto de las reivindicaciones independientes.

Las realizaciones están definidas por las reivindicaciones dependientes.

Sumario

Las realizaciones de la presente divulgación se refieren a sistemas, métodos y estructuras de datos para la autenticación específica de mensajes. Un aspecto es un sistema informático para controlar el acceso a un recurso de servicio web protegido. El sistema informático incluye un dispositivo de comunicación, un procesador y memoria. El dispositivo de comunicación se comunica a través de una red de comunicación. El procesador está conectado comunicativamente con el dispositivo de comunicación. La memoria almacena instrucciones de programa que, cuando las ejecuta el procesador, hacen que el sistema informático realice un método para controlar el acceso a un recurso de servicio web protegido. El método incluye recibir una primera petición de un cliente para acceder a un recurso de servicio web protegido desde la red de comunicación; determinar que el cliente ha sido autenticado de acuerdo con un primer factor; conceder la primera petición para acceder al recurso de servicio web protegido en base a la autenticación de acuerdo con el primer factor; recibir una segunda petición de un cliente para acceder a un recurso de servicio web protegido desde la red de comunicación; denegar la segunda petición para acceder al recurso de servicio web protegido en base a que la autenticación de acuerdo con el primer factor es insuficiente para conceder la segunda petición, determinar que el cliente ha sido autenticado de acuerdo con un segundo factor y conceder la segunda petición para acceder al recurso protegido de servicio web en base a la autenticación de

acuerdo con el segundo factor.

Otro aspecto es un método para autenticar a un cliente para acceder a un recurso de servicio web. El método incluye: (i) recibir una petición de un cliente para ser autenticado; (ii) enviar un mensaje de desafío al cliente; (iii) recibir una respuesta de confirmación al mensaje de desafío del cliente; (iv) determinar que la respuesta de confirmación cumple con un criterio predeterminado; (v) determinar que la petición de autenticar requiere autenticación adicional; (iv) repetir (ii) a (iv) con un segundo mensaje de desafío, una segunda respuesta de confirmación y un segundo criterio predeterminado; y (v) enviar un mensaje de autenticación al cliente.

Un aspecto adicional se refiere a un medio legible por ordenador que contiene instrucciones ejecutables por ordenador, las cuales, cuando son ejecutadas por un ordenador, realizan un método para controlar el acceso a un recurso protegido, comprendiendo el método: recibir una petición de un cliente que identifica el recurso protegido de un servicio web; enviar una respuesta al cliente pidiendo autenticación desde un servicio de autenticación; recibir un testigo (o token) de autenticación del cliente después de ser autenticado desde el servicio de autenticación; determinar si el testigo de autenticación es suficiente para conceder la petición; conceder la petición si el testigo de autenticación es suficiente; y denegar la petición si el testigo de autenticación no es suficiente para conceder la petición.

Las realizaciones pueden implantarse como un proceso informático, como un sistema informático o como un artículo de fabricación tal como un producto de programa informático o un medio legible por ordenador. El producto del programa informático puede ser un medio de almacenamiento informático legible por un sistema informático y que codifica un programa informático de instrucciones para ejecutar un proceso informático. El producto de programa informático puede también ser una señal propagada en un soporte legible por un sistema informático y que codifica un programa informático de instrucciones para ejecutar un proceso informático.

Este sumario se proporciona para presentar una selección de conceptos de una manera simplificada y que se describe con más detalle a continuación en la descripción detallada. Este sumario no pretende identificar características clave o esenciales del objeto reivindicado, ni tampoco pretende ser utilizado de ninguna manera para limitar el alcance del objeto reivindicado.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques de un sistema de ejemplo configurado para realizar autenticación dinámica.

La figura 2 es un diagrama de flujo que ilustra un método de ejemplo para determinar dinámicamente si se requiere autenticación.

La figura 3 es un diagrama de flujo que ilustra un método de ejemplo para autenticar a un cliente.

La figura 4 es un diagrama de flujo que ilustra un método de ejemplo para controlar dinámicamente el acceso a un recurso protegido.

La figura 5 es un diagrama de flujo que ilustra un método de ejemplo para controlar el acceso a un recurso protegido.

La figura 6 es un diagrama de bloques de un sistema informático ejemplar para implantar aspectos de la presente divulgación.

Descripción detallada

Esta divulgación describirá ahora con más detalle realizaciones ejemplares con referencia a los dibujos que se acompañan, en los que se muestran realizaciones específicas. Sin embargo, pueden incorporarse otros aspectos de muchas maneras diferentes, y la inclusión de realizaciones específicas en la divulgación no debe interpretarse como una limitación de tales aspectos a las realizaciones establecidas en el presente documento. Más bien, se incluyen las realizaciones representadas en los dibujos para proporcionar una divulgación que sea minuciosa y completa y que transmita plenamente su pretendido alcance al experto en la técnica. Cuando se hace referencia a las figuras, las estructuras y elementos similares mostrados en todas partes se indican con números de referencia similares.

Algunas realizaciones de la presente divulgación se relacionan con sistemas y métodos para autenticación específica de mensajes. Un aspecto es un método para determinar si se necesita autenticación antes de que a un cliente se le permita acceder a un recurso protegido.

En general, la autenticación es un proceso de verificación de la veracidad de reclamaciones de identidad realizadas por algo, tal como un sistema informático, un cliente, un sistema o una persona. Autenticar un sistema informático típicamente incluye confirmar su origen o fuente. La confirmación del origen o fuente se lleva a cabo habitualmente comparando información sobre el sistema informático que reclama una identidad específica, tal como lugar y hora de

fabricación, ubicación en una red, ubicación física, número de identificación y similares, para conocer información sobre esa identidad específica.

Sin embargo, el acto de autentificar a una persona implica, por ejemplo, confirmar la identidad de la persona. Hay muchas características de identificación diferentes que se pueden utilizar para la autenticación. Un método para identificar a una persona implica detectar identificadores biométricos. Este método de autenticación requiere que la persona que reclama una identidad proporcione verificación en forma de características únicas de la persona que reclama la identidad, tales como ADN, patrones de huellas dactilares, patrones de retina, etc. Otra manera de verificar la identidad de una persona es mediante algo que la persona sepa. Este método de autenticación requiere que la persona que reclama una identidad proporcione verificación en forma de información personal tal como una contraseña, un número PIN, etc. Otra manera más de verificar la identidad de una persona es mediante algo que tenga. Este método de autenticación requiere que la persona que reclama una identidad proporcione verificación en forma de un objeto, tal como una clave, una tarjeta de seguridad, un testigo de seguridad, una tarjeta de crédito, etc. Estos métodos de autenticación pueden usarse individualmente o juntos en un proceso conocido como autenticación de múltiples factores.

Generalmente, al autenticar a un cliente, el proceso incluye autenticar a un cliente o autenticar la identidad de la persona que utiliza el cliente. En una realización, el cliente puede ser un navegador web. En otra realización, el cliente puede ser un programa configurado para realizar llamadas a procedimientos remotos, o cualquier otra aplicación u otro programa que se comunique con un recurso protegido.

En un entorno dinámico, los tipos de autenticación y las reglas para autenticar a un cliente varían dependiendo de los tipos de peticiones realizadas para acceder a un recurso protegido. Por ejemplo, un mensaje que pide ver un recurso protegido puede requerir una autenticación menos exigente que un mensaje que pide modificar el recurso protegido. En una realización, un recurso protegido es un sitio web privado al que sólo tienen acceso usuarios específicos. En otra realización, un recurso protegido puede ser un grupo de correo electrónico privado, datos protegidos, métodos protegidos, procedimientos protegidos, actuaciones protegidas, o cualquier otro tipo de información o funcionalidad protegida que deba limitarse a usuarios o clientes específicos.

La figura 1 es un diagrama de bloques de un sistema 100 de ejemplo configurado para realizar autenticación dinámica específica de petición. En la realización ilustrada, el sistema 100 incluye el cliente 102, el servicio web 104 y el servicio 108 de autenticación. El servicio web 104 incluye el recurso protegido 106. En esta realización, el cliente 102 desea obtener acceso al recurso protegido 106. Sin embargo, el recurso protegido 106 está protegido contra el acceso de clientes no autenticados. El cliente 102, el servicio web 104 y el servicio 108 de autenticación están configurados para comunicarse a través de la red 110. La red 110 es una ruta de comunicación de datos. En una realización, la red 110 es Internet. En otras realizaciones, la red 110 es una red de área local, Intranet, red inalámbrica, o cualquier otra ruta de comunicación configurada para comunicar datos desde un sistema informático a otro sistema informático.

En una realización, el cliente 102 es un sistema informático. En otras realizaciones, el cliente 102 es cualquier sistema informático configurado para comunicar datos a través de la red 110. Un ejemplo de cliente 102 es el sistema informático 600, mostrado en la figura 6. El cliente 102 está conectado comunicativamente con el servicio web 104 y con el servicio 108 de autenticación a través de la red 110. En algunas realizaciones, el cliente 102 puede acceder al recurso protegido 106 enviando mensajes al servicio web 104. En otra realización, el cliente 102 envía mensajes directamente al recurso protegido 106.

En una realización, el servicio web 104 es un sistema informático (por ejemplo, el sistema informático 600, mostrado en la figura 6), tal como un servidor web, que actúa un servicio web. En general, el servicio web 104 proporciona una funcionalidad útil a la que se puede acceder a través de la red 110, usando un protocolo de comunicación de datos. Los servicios web se pueden utilizar para proporcionar una variedad infinita de funciones útiles. En una realización, el servicio web 104 es un servidor. En otra realización, el servicio web 104 es una aplicación de sistema informático que actúa en un sistema informático conectado comunicativamente a la red 110. En algunas realizaciones, el servicio web 104 es una entidad, procesador o recurso de referencia al que se pueden dirigir mensajes de servicio web.

Generalmente, algunas realizaciones del servicio web 104 monitorizan la red 110 en busca de mensajes enviados desde el cliente 102 relacionados con el recurso protegido 106. Cuando se recibe un mensaje, el servicio web 104 determina si el mensaje contiene una petición que requiera la autenticación del cliente 102. La autenticación del cliente 102 es a veces necesaria antes de permitir que el cliente 102 acceda al recurso protegido 106, para controlar el acceso al recurso protegido 106. Si el servicio web 104 determina que se necesita autenticación, el servicio web 104 dirige al cliente 102 al servicio 108 de autenticación.

En la realización ilustrada, el servicio web 104 incluye el recurso protegido 106. Los recursos protegidos incluyen, por ejemplo, funciones realizadas por un servicio web 104 y datos almacenados por el servicio web 104 a los que sólo puede acceder, utilizar o modificar un cliente autenticado. Por ejemplo, si el servicio web 104 proporciona el servicio de mantener una lista de distribución de grupo, la lista de distribución de grupo es un recurso protegido al

que sólo puede acceder, utilizar o modificar un cliente autenticado. Como otro ejemplo, el recurso protegido 106 es una entrada en un directorio. En otra realización, el recurso protegido 106 es un registro en una base de datos. En otra realización, el recurso protegido 106 es un archivo o parte de un archivo almacenado en un dispositivo de almacenamiento de memoria. Otras realizaciones utilizan otras formas de recursos protegidos 106.

En una realización, el servicio 108 de autenticación es un sistema informático (por ejemplo, el sistema informático 600, mostrado en la figura 6), tal como un servidor conectado comunicativamente a la red 110. En otra realización, el servicio 108 de autenticación es un sistema informático que ejecuta una aplicación de software ubicada en una red. El servicio 108 de autenticación está configurado para autenticar al cliente 102. Un ejemplo de servicio 108 de autenticación es un punto final de servicio de testigo de seguridad. Aunque la realización ilustrada muestra un ejemplo de servicio 108 de autenticación separado y distinto del servicio web 104, en otras realizaciones, el servicio 108 de autenticación y el servicio web 104 actúan en el mismo servidor.

Si el cliente 102 se autentica para realizar la petición contenida en su mensaje en el recurso protegido 106, el servicio web 104 comunica los resultados de la actuación pedida al cliente 102. Sin embargo, en otras realizaciones posibles, el servicio 108 de autenticación se comunica directamente con el servicio web 104, a través de la red 110, tal como para recibir una petición de autenticación del servicio web 104, o para enviar una prueba de autenticación al servicio web 104.

Además de la autenticación, a veces es recomendable controlar el acceso a recursos protegidos exigiendo que el cliente no sólo esté autenticado, sino también autorizado. La autorización se describe en la solicitud de patente de EE.UU. núm. 12/024.896, titulada “Authorization for Access to Web Service Resources”, presentada el 1 de febrero de 2008 por Craig V. McMurtry, Alexander T. Weinert, Vadim Meleshuk y Mark E. Gabarra, incorporándose la totalidad de esta divulgación al presente documento por referencia.

La figura 2 es un diagrama de flujo que ilustra un método de ejemplo 200 para determinar dinámicamente si se requiere autenticación. El método 200 incluye las actuaciones 202, 204, 206, 208 y 210. El método 200 comienza con la actuación 202 durante la cual se realiza una petición de recurso. En una realización, la actuación 202 implica comunicar un mensaje desde el cliente 102 al servicio web 104 que incluye una petición para acceder al recurso protegido 106. En algunas realizaciones, el mensaje es una llamada a procedimiento remoto. En otra realización, la petición puede tomar la forma de un correo electrónico o de cualquier otro tipo de comunicación eléctrica entre el cliente y un recurso. En otra realización, la actuación 202 implica que el cliente 102 envíe la petición de crear, obtener, poner, eliminar o enumerar al servicio web 104, tal como se usa comúnmente en las comunicaciones de servicios web.

Después de que se ha realizado la petición de recursos, se realiza la actuación 204 para evaluar la petición y determinar si la autenticación es necesaria. En una realización, el servicio web analiza el mensaje enviado desde el cliente al recurso protegido para determinar si el mensaje contiene una petición que requiere que el cliente proporcione autenticación. En una realización, un cliente que intente acceder a un recurso protegido no tendrá que proporcionar autenticación si el cliente ha proporcionado previamente la autenticación requerida para la petición. En otra realización, el cliente no tendrá que proporcionar autenticación si el recurso es un recurso público que está disponible para cualquiera que lo pida. En otra realización, aunque un recurso pueda estar protegido, no se requiere autenticación si el mensaje contiene una petición que no requiere autenticación, tal como si el mensaje es de un tipo que no puede dañar el recurso protegido. Si el servicio web 104 determina en la actuación 204 que no se requiere autenticación, se realiza entonces la actuación 206. Si se requiere autenticación, se realiza entonces la actuación 208.

En un ejemplo, el servicio web 104 determina si se requiere autenticación evaluando una serie de consideraciones. Estas consideraciones incluyen el medio por el cual se transmite la petición (tal como una red de área local en contraposición con un acceso remoto), el tipo de objeto al que pertenece la petición, las propiedades del objeto al que pertenece la petición y la calidad de las credenciales ya incluidas con la petición. En cuanto a la calidad de las credenciales, por ejemplo, si las credenciales son para un usuario de otra organización, entonces, dependiendo del recurso al que el usuario está intentado acceder, es posible que se requieran credenciales adicionales.

Si no se requiere autenticación, se realiza la actuación 206 para conceder acceso al recurso pedido. El servicio web concede acceso al recurso protegido, por ejemplo, enviando una representación del recurso al cliente, realizando la actuación pedida en el recurso protegido o enviando el resultado de la actuación pedida al cliente.

Sin embargo, si se requiere autenticación, se realiza la actuación 208 para realizar la autenticación. La autenticación del cliente se analizará más detalladamente en relación con la figura 3. Los ejemplos de situaciones que requieren que el cliente proporcione autenticación incluyen casos en los que el cliente intenta acceder o modificar sitios web privados, grupos de correo electrónico privados, datos protegidos, métodos protegidos, procedimientos protegidos, actuaciones protegidas o cualquier otro tipo de información o funcionalidad protegida. En algunas realizaciones, el servicio web 104 desafía al cliente 102 a proporcionar autenticación. Alternativamente, el servicio web 104 dirige al cliente a un servicio de autenticación (tal como el servicio 108 de autenticación). El servicio 108 de autenticación puede estar ubicado en el servicio web 104, ubicado en otro lugar del servicio web, o en ambos, como en el caso de

una red distribuida. Se ilustra y describe un método de ejemplo de autenticación de un cliente con referencia a la figura 3.

Después de autenticar al cliente, se realiza la actuación 206 para conceder al cliente acceso al recurso protegido del servicio web. En una realización, el acceso se concede después de que el cliente proporcione un testigo de autenticación desde el servicio de autenticación al servicio web. El servicio web concede acceso al recurso protegido, por ejemplo, enviando el recurso al cliente, realizando una actuación pedida en el recurso protegido, indicando al recurso protegido que realice una actuación pedida o enviando el resultado de una actuación pedida al cliente.

Si se determina que el cliente no debe autenticarse, se realiza la actuación 210, durante la cual se deniega el acceso al recurso protegido. En un ejemplo, se deniega el acceso porque el servicio 108 de autenticación no proporciona el testigo de autenticación necesario con el fin de obtener acceso al recurso protegido.

La figura 3 es un diagrama de flujo que ilustra un método 300 de ejemplo para autenticar a un cliente. En una realización, el método 300 se corresponde con la actuación 208 mostrada en la figura 2. El método 300 comienza con la actuación 302, durante la cual se realiza una petición de autenticación. En una realización, la actuación 302 implica que se envíe un mensaje desde el cliente 102 al servicio 108 de autenticación, y que el servicio 108 de autenticación reciba la petición de autenticación.

En la realización ilustrada, después de recibir la petición de autenticación, se realiza la actuación 304 para comunicar un desafío de autenticación. En una realización, el servicio 108 de autenticación comunica un desafío al cliente 102 para probar la veracidad de la identidad del cliente o usuario. En algunas realizaciones, el desafío toma la forma de pedir una contraseña, de pedir una respuesta a una pregunta de seguridad, de pedir una muestra de ADN, de patrones de huellas dactilares, de patrones de retina, de otras formas de identificadores biométricos, de otros identificadores únicos de la persona que utilice el cliente, de pedir verificación en la forma de un objeto tal como una clave, una tarjeta de seguridad, un testigo de seguridad, una tarjeta de crédito o algún otro objeto exclusivo de la persona que utilice el cliente, de pedir información específica del cliente tal como lugar y hora de fabricación, ubicación en una red, ubicación física, número de identificación, o de pedir cualquier otro tipo de información que pueda ser utilizada con fines de autenticación.

En la realización ilustrada, una vez que se ha comunicado el desafío, se realiza la actuación 306 para recibir una respuesta de confirmación al desafío. La actuación 306 implica proporcionar la información, la muestra, el identificador, o similar, que se pidió en la actuación 304, y comunicarla al servicio 108 de autenticación. En una realización, un dispositivo de entrada (por ejemplo, el dispositivo de entrada 614, mostrado en la figura 6) es utilizado por el usuario de cliente 102 para proporcionar la información de identificación al cliente 102, que luego comunica la información al servicio 108 de autenticación. En algunas realizaciones, se usa un sensor (que también es una forma de dispositivo de entrada). Por ejemplo, un usuario coloca un dedo sobre un escáner de huellas dactilares, que escanea la huella dactilar. Los datos de huellas dactilares se transmiten luego al servicio 108 de autenticación. Se pueden usar diversos tipos de dispositivos de entrada, incluyendo un teclado, un ratón, un panel táctil, un micrófono, un bolígrafo, un sensor biométrico, un escáner, un lector de tarjetas, un detector químico, y similares. En otras realizaciones, se introducen los datos en el cliente 102, que los comunica luego al servicio 108 de autenticación.

En la realización ilustrada, una vez que se ha comunicado la confirmación, se realiza la actuación 308 para verificar la respuesta de confirmación. En una realización, el servicio de autenticación compara la respuesta de confirmación que recibió del cliente 102 con información conocida sobre la identidad reclamada. Por ejemplo, el servicio 108 de autenticación recupera datos almacenados en una base de datos y los compara con los datos de respuesta de confirmación. El servicio 108 de autenticación determina entonces si la respuesta de confirmación coincide con los datos previamente almacenados. Si es así, se verifica la respuesta de confirmación y se realiza la actuación 312. En caso contrario, no se verifica la respuesta de confirmación y se realiza la actuación 310.

Si la respuesta de confirmación recibida no coincide con la información conocida, se realiza la actuación 310 en la que se deniega el acceso al recurso pedido. En otra realización, el servicio 108 de autenticación vuelve a la actuación 304 para volver a intentar la autenticación. En tal realización, se pueden permitir múltiples reintentos, tal como tres reintentos. Si los reintentos no tienen éxito, se realiza la actuación 310 para denegar el acceso al recurso protegido.

Si la respuesta de confirmación recibida coincide con la información conocida, se realiza entonces la actuación 312 para determinar si es necesaria una autenticación adicional. En una realización, el servicio 108 de autenticación determina si se requieren formas de autenticación más sólidas, es decir, una autenticación de múltiples factores que requiera que el cliente proporcione múltiples formas de autenticación. Si es necesaria la autenticación de múltiples factores, el método 300 vuelve a la actuación 304 para comunicar un segundo desafío. A continuación se repiten las actuaciones 304, 306, 308 y 310 ó 312 tantas veces como se desee. Sin embargo, cuando se repita, el desafío de autenticación tomará una forma diferente al desafío emitido anteriormente por el servicio de autenticación. Por ejemplo, si el servicio de autenticación originalmente requirió que el cliente proporcionara una contraseña, puede

requerir que el cliente use una tarjeta inteligente o un escáner biométrico durante la segunda o siguientes rondas de verificación. En algunas realizaciones, se puede utilizar cualquier manera de autenticación siempre que la manera de autenticación difiera de algún modo de la forma utilizada anteriormente, de tal manera que el servicio 108 de autenticación no pida la misma información una y otra vez simplemente. En la mayoría de las situaciones, pedir repetidamente la misma información no proporcionaría ningún valor de autenticación adicional. Sin embargo, en algunas situaciones, se pueden utilizar peticiones repetidas, tal como si ha pasado una cantidad significativa de tiempo desde el desafío anterior.

Si no se requiere autenticación adicional, se realiza entonces la actuación 314 para emitir un testigo de autenticación. El servicio 108 de autenticación devuelve un testigo de seguridad al cliente, que el cliente utiliza como prueba de que ha sido autenticado. El testigo de autenticación se envía desde el cliente 102 al servicio web 104, y el servicio web 104 concede entonces al cliente 102 acceso al recurso protegido pedido originalmente.

La figura 4 es un diagrama de flujo que ilustra un método de ejemplo 400 para controlar dinámicamente el acceso a un recurso protegido. En una realización, el método 400 lo realiza el servicio web 104, en respuesta a mensajes recibidos del cliente 102, tal como en un intento de obtener acceso al recurso protegido 106. El método 400 comienza con la actuación 404, durante la cual se recibe un mensaje de petición. En una realización, el servicio web 104 recibe una petición del cliente 102 relacionada con el recurso protegido 106. Como algunos ejemplos, la petición es una petición para ver el recurso protegido, para obtener acceso al recurso protegido o para modificar el recurso protegido.

En la realización ilustrada, se realiza luego la actuación 406 para determinar si el mensaje de petición contiene una petición que requiera autenticación. En una realización, el servicio web 104 analiza la petición para determinar si la petición contenida en la petición requiere autenticación del cliente. En algunas realizaciones, un cliente que intenta acceder a un recurso protegido no tendrá que proporcionar autenticación, por ejemplo, si el cliente ha proporcionado previamente la autenticación requerida para la petición, si el recurso es público y está disponible para todos, si el tipo de petición es uno que contiene una petición que no requiere autenticación, o si el tipo de petición y su petición asociada no pueden dañar el recurso protegido. Si no se requiere autenticación, se realiza entonces la actuación 414 para realizar la actuación pedida.

En la realización ilustrada, si la petición contenida en el mensaje requiere autenticación, se realiza entonces la actuación 408 para comunicar que se requiere autenticación. En una realización, la actuación 408 implica enviar un mensaje desde el servicio web 104 al cliente 102 informando al cliente 102 que se requiere autenticación para realizar la actuación pedida. En una realización, el servicio web 104 dirige al cliente 102 al servicio 108 de autenticación para su autenticación, tal como se describe con referencia a la figura 3. Por ejemplo, el mensaje contiene una dirección de un proveedor de autenticación. El cliente utiliza la dirección para localizar al proveedor de autenticación e intentar recibir la autenticación. En otra realización, el método 300 lo realiza el servicio web 104, de tal modo que el mensaje contiene un desafío al cliente 102 pidiendo que el cliente 102 proporcione información de autenticación.

En la realización ilustrada, si el cliente se autentica exitosamente, se realiza entonces la actuación 410, en la que se recibe el testigo de autenticación. Como se describe con referencia a la figura 3, el resultado de una autenticación exitosa es la recepción de un testigo de autenticación. Ese testigo se pasa al servicio web 104 para proporcionar la prueba de la autenticación. El servicio web 104 evalúa el testigo y verifica que el testigo sea válido.

En algunas realizaciones, la evaluación del testigo implica dos pasos. El primer paso implica la criptografía de clave pública. Si el servicio web 104 puede descifrar el testigo utilizando la clave pública del servicio 108 de autenticación, entonces el servicio web 104 determina que el testigo debe haber sido emitido por el servicio 108 de autenticación. El segundo paso incluye decidir si las reclamaciones realizadas por el servicio 108 de autenticación, sobre el cliente 102, satisfacen una o más condiciones de acceso.

Por ejemplo, para poder acceder a un recurso protegido particular 106, el servicio web 104 podría requerir que se realizaran tres procesos de autenticación particulares para autenticar al cliente 102 en el servicio 108 de autenticación. Como resultado, el servicio web 104 evaluaría el testigo recibido del cliente 102 para verificar que contiene las tres reclamaciones provenientes del servicio 108 de autenticación, afirmando que el cliente 102 ha completado los tres procesos de autenticación. En otras realizaciones, se requiere cualquier número de procesos de autenticación. En algunas realizaciones, el número y el tipo de procesos de autenticación requeridos están relacionados con el tipo de petición que se realiza. Por ejemplo, las peticiones que impliquen un riesgo más alto a menudo requerirán procesos de autenticación más estrictos.

En algunas realizaciones, una serie de procesos de autenticación que se completan con éxito se denominan niveles de autenticación. En algunas realizaciones, una actuación de bajo riesgo que involucra al recurso protegido 106 requiere sólo un nivel de autenticación bajo, tal como uno o dos niveles de autenticación. En algunas realizaciones, una actuación de alto riesgo requiere un alto nivel de autenticación, tal como entre tres y cinco niveles de autenticación. Un único recurso protegido puede asociarse con diversos niveles de autenticación, de acuerdo con la petición que se realice. Por ejemplo, una petición para recuperar información de un recurso protegido puede requerir

sólo un nivel de autenticación bajo en algunas situaciones, mientras que una petición para eliminar información de un recurso protegido puede requerir un nivel de autenticación moderado o alto. En otras situaciones, una petición para recuperar información de un recurso protegido podría requerir un alto nivel de autenticación si la información fuera sensible o confidencial.

En la realización ilustrada, si no se proporciona una prueba válida de autenticación, o si la autenticación proporcionada se evalúa y se determina que es insuficiente, se realiza la actuación 411 para denegar el acceso al recurso protegido. En algunas realizaciones, se envía un mensaje al cliente 102 para informar al cliente 102 de la denegación. En algunas realizaciones, el mensaje también incluye información sobre cómo obtener la autenticación adecuada, tal como dirigir al cliente 102 al servicio 108 de autenticación.

En la realización ilustrada, si se proporciona la prueba de autenticación y se verifica como válida, la actuación pedida se realiza en la actuación 412. En otras palabras, se concede acceso al recurso protegido. En algunas realizaciones, se realiza luego la actuación 414 para informar al pedidor que la petición fue procesada. Por ejemplo, el servicio web 104 envía un mensaje informando al cliente 102 que la petición fue procesada en relación con el recurso protegido. En otros ejemplos, el servicio web 104 concede acceso al recurso protegido enviando una representación del recurso 106 al cliente 102, realizando una actuación pedida en el recurso protegido 106, o enviando el resultado de una actuación pedida al cliente 102.

En la realización ilustrada, se realiza luego la actuación 416 para monitorizar la recepción de mensajes adicionales. Por ejemplo, el servicio web 104 supervisa comunicaciones adicionales del cliente 102 relacionadas con el recurso 106. Si el cliente 102 envía mensajes adicionales al recurso 106, el método 400 vuelve a la actuación 404 para evaluar si el nuevo mensaje requiere autenticación adicional a través de las actuaciones 404, 406, y 408. Aunque es posible que el cliente ya se haya autenticado en este punto propiamente, en un entorno dinámico es posible que el cliente tenga que proporcionar formas más sólidas de autenticación, es decir, una autenticación de múltiples factores, dependiendo de los tipos de mensajes y de peticiones que envíe. Si no se reciben más mensajes, entonces finaliza el método 400.

La figura 5 es un diagrama de flujo que ilustra un método 500 de ejemplo para controlar el acceso a un recurso protegido. El método 500 implica al cliente 102, al servicio web 104, al servicio 108 de autenticación y al recurso protegido 106. Aunque el servicio 108 de autenticación se ilustra como una entidad separada y distinta del servicio web 104, en algunas realizaciones el servicio 108 de autenticación y el servicio web 104 actúan en el mismo sistema informático. En una realización, el recurso protegido 106 está ubicado en el servicio web 104. En otra realización más, el recurso protegido 106 está ubicado en otro servicio web, servidor, ordenador u otro sistema informático. En la comunicación 512, el cliente 102 envía una petición de recurso protegido 106. El servicio web 104 recibe esta petición. En la comunicación 514, el servicio web 104 determina que la autenticación es necesaria y responde con un fallo, que indica que se debe completar al menos un proceso de autenticación para que se procese la petición. En posibles realizaciones, el fallo puede tomar la forma de un fallo del protocolo simple de acceso a objetos (SOAP), como se define en la especificación SOAP 1.2. En otras realizaciones, el fallo puede adoptar la forma de cualquier otro tipo de protocolo de comunicación de datos. En realizaciones adicionales, el fallo del servicio web 104 contendrá una dirección a un servicio 108 de autenticación, tal como un punto final de servicio de testigo de seguridad.

En la comunicación 516, el cliente 102 envía una petición de un testigo de seguridad al servicio 108 de autenticación, reclamando que se han completado los procesos de autenticación necesarios. En una realización, esta petición toma la forma de un mensaje de respuesta de testigo de seguridad de petición de confianza de servicios web (WS-Trust) tal como se define en la especificación de WS-Trust. En otras realizaciones, la petición puede tomar la forma de otros protocolos. En la comunicación 518, el servicio 108 de autenticación responde al cliente 102 con un desafío para la confirmación de identidad. En algunas realizaciones, el desafío toma la forma de los desafíos descritos con respecto a la figura 3. En la comunicación 520, el cliente 102 responde con una confirmación de identidad. En algunas realizaciones, la confirmación de identidad toma la forma de la confirmación descrita con respecto a la figura 3. En la comunicación 522, el servicio 108 de autenticación responde al cliente 102 con un desafío adicional para la confirmación de identidad. En una realización, este desafío es en respuesta a una confirmación fallida de identidad. En otra realización más, este desafío es necesario para realizar la autenticación de múltiples factores. En la comunicación 524, el cliente 102 responde al servicio 108 de autenticación con una confirmación adicional de identidad. Este proceso puede repetirse una vez más con un desafío en la comunicación 526 y la confirmación del desafío 528. Aunque se ilustra que el conjunto de desafíos y confirmaciones se realiza tres veces, en otras realizaciones tales comunicaciones de desafío y respuesta se repiten cualquier número de veces. Después de que el servicio 108 de autenticación confirme la identidad del cliente 102, el servicio 108 de autenticación emite el testigo de seguridad pedido al cliente 102 en la comunicación 530.

En la comunicación 532, el cliente 102 vuelve a enviar la petición original de un recurso protegido junto con el testigo de seguridad. El servicio web 104 examina la petición para asegurarse de que sea la misma que la petición original y valida el testigo de seguridad para asegurarse de que sea válido. En la comunicación 534, el servicio web 104 procesa la petición realizada por el cliente 102. En algunas realizaciones, este procesamiento implica buscar y/o actualizar el recurso protegido 106. En la comunicación 536, se devuelve el resultado de la búsqueda y/o

actualización del recurso protegido 106. al servicio web 104. En la comunicación 538, el servicio web 104 responde a la petición realizada por el cliente 102.

Con referencia ahora a la Tabla 1: Esquema de desafío de autenticación, se proporciona una estructura de datos para indicar que se requiere un proceso de autenticación específico de mensaje para procesar una petición. En algunas realizaciones, las comunicaciones descritas en relación con la figura 5 se comunican en la forma de la estructura de datos definida en la Tabla 1, tal como cuando un servicio web, tal como el servicio web 104, determina que se requiere un proceso específico de mensaje para autenticar al usuario que inició una petición. En una realización, el servicio devolverá un fallo SOAP, según se define en la especificación SOAP 1.2. En algunas realizaciones, a diferencia de los fallos SOAP tradicionales, el fallo SOAP utilizado para indicar que se requiere un protocolo de autenticación específico de mensaje contendrá un encabezado de contexto que contiene un identificador mediante el cual se muestran los detalles de la petición original, y cualquier proceso de autenticación que se haya encontrado asociado con la petición puede ser recuperado por el servicio web. En otra realización, el fallo SOAP devuelto contendrá también un elemento de Detalle que indicará la identidad del usuario en nombre del cual se realiza la petición. Esta es la identidad que será autenticada adicionalmente. En aún otra realización, el elemento de Detalle también proporcionará o lo hará alternativamente la dirección de un servicio de autenticación, tal como el servicio 108 de autenticación, que pueda emitir un testigo de seguridad al usuario confirmando que el usuario ha completado con éxito cada uno de los procesos de autenticación asociados con la petición. En algunas realizaciones, la dirección del servicio de autenticación es la misma que la dirección del servicio web. En otras realizaciones, la dirección del servicio de autenticación es diferente de la dirección del servicio web.

Tabla 1: Esquema de desafío de autenticación

```
<?xml version=‘ 1.0’ encoding=’utf-8’?>
<xs:schema
 elementFormDefault=’qualified’
targetN amespace=’http://schemas.microsoft.com/2006/11/IdentityManagem
ent’
 xmlns:xs=’http://www.w3 .org/200 1/XMLSchema’
 xmlns:wsa=http://schemas.xmlsoap.org/ws/2004/08/addressing
 xmlns:idm=‘http://schemas.microsoft.com/2006/1 1/IdentityManagement’>
 <xs:import
  namespace=’http://schemas .xmlsoap.org/ws/2004/08/ addressing’ />
 <xs:complexType name=’AuthenticationChallengeType’>
  <xs:sequence>
   <xs: element
   name=’ Challenge’
   nillable=’true’
   minOccurs=’0’>
    <xs:complexType>
      <xs:sequence>
       <xs:any
        minOccurs=’0’
        processContents=’lax’ />
      </xs:sequence>
    </xs:complexType>
   </xs:element>
  </xs:sequence>
 </xs:complexType>
 <xs:element
  name=’AuthenticationChallenge’
  nillable=’true’
  type=‘idm:AuthenticationChallengeType’ />
</xs:schema>
```

El esquema mostrado en la Tabla 1 incluye un elemento Challenge (desafío) y un elemento AuthenticationChallenge (desafío de autenticación). El elemento Challenge se utiliza para transferir al cliente la información necesaria para desafiar al usuario a proporcionar los datos de autenticación requeridos. En algunas realizaciones, el cliente puede ser un navegador web que mostrará los datos de desafío al usuario, para impulsarle a que proporcione datos en respuesta al desafío. Por ejemplo, el elemento de desafío puede indicarle al cliente 102 que represente visualmente un cuadro de texto impulsando al usuario a que introduzca una contraseña. Otras realizaciones impulsarán al usuario a que proporcione autenticación pidiendo una respuesta a una pregunta de seguridad, pidiendo una muestra de ADN, patrones de huellas dactilares, patrones de retina o algún otro identificador único de la persona que utiliza el cliente, pidiendo verificación en forma de un objeto tal como una clave, tarjeta de seguridad, testigo de seguridad, tarjeta de crédito o algún otro objeto exclusivo de la persona que utiliza el cliente, según se describe con referencia a

la figura 3. En posibles realizaciones, el esquema de desafío de autenticación incluirá un elemento AuthenticationChallenge que sirva como envoltorio para el esquema.

Con referencia ahora a la Tabla 2: Esquema de respuesta al desafío de autenticación, se proporciona una estructura de datos para responder a un desafío de autenticación. El servicio de autenticación, tal como el servicio 108 de autenticación, emite desafíos al usuario para autenticar información. En algunas realizaciones, los desafíos se realizan de acuerdo con el marco de desafío definido en la sección 10 de la especificación WS-Trust. Si el servicio de autenticación requiere información adicional para autenticar la identidad de un usuario, responderá a una petición de un mensaje de testigo de seguridad con una respuesta definida por la especificación WS-Trust.

Tabla 2: Esquema de respuesta al desafío de autenticación

```
<?xml version=‘ 1.0’ encoding=’utf-8’?>
<xs:schema
 elementFormDefault=’qualified’
targetN amespace=’http://schemas.microsoft.com/2006/11/IdentityManagem
ent’
 xmlns:xs=’http://www.w3 .org/200 1/XMLSchema’
 xmlns:wsa=http://schemas.xmlsoap.org/ws/2004/08/addressing
 xmlns:idm=‘http://schemas.microsoft.com/2006/1 1/IdentityManagement’>
 <xs:import
  namespace=‘http://schemas.xmlsoap.org/ws/2004/08/addressing’/>
 <xs:complexType name=‘AuthenticationChallengeResponseType’>
  <xs:sequence>
   <xs: element
   name=’Response’
   nillable=’true’
   minOccurs=’0’>
    <xs:complexType>
      <xs:sequence>
       <xs:any
        minOccurs=’0’
        processContents=’lax’ />
      </xs:sequence>
    </xs:complexType>
   </xs:element>
  </xs:sequence>
 </xs:complexType>
 <xs:element
  name=’ AuthenticationChallengeResponse’
  nillable=’true’
  type=‘idm:AuthenticationChallengeResponseType’ />
</xs:schema>
```

El esquema de respuesta al desafío de autenticación incluye un elemento de respuesta y un elemento AuthenticationChallengeResponse. El elemento de respuesta identifica para el servicio de autenticación la información de autenticación que se requiere del cliente. El servicio de autenticación utiliza esta información, por ejemplo, para determinar qué desafíos deben enviarse al cliente para autenticarlo. El elemento AuthenticationChallengeResponse sirve como envoltorio para el esquema.

La figura 6 es un diagrama de bloques de un sistema informático ejemplar 600 para implantar aspectos de la presente divulgación. En una realización, el sistema informático 600 es el cliente 102. En otra realización, el sistema informático 600 es el servicio web 104. En otra realización posible, el sistema informático 600 es el servicio 108 de autenticación. En su configuración más básica, el sistema informático 600 incluye típicamente al menos una unidad 602 de procesamiento y memoria 604. Dependiendo de la configuración exacta y del tipo de sistema informático, la memoria 604 puede ser volátil (tal como RAM), no volátil (tal como ROM, memoria flash, etc.) o alguna combinación de ambas. Esta configuración más básica se ilustra en la figura 6 con la línea discontinua 606. Además, el sistema informático 600 puede tener también características/funcionalidades adicionales. Por ejemplo, el sistema informático 600 puede incluir también almacenamiento adicional (extraíble y/o no extraíble) que incluye, entre otros, discos o cintas magnéticos u ópticos. Tal almacenamiento adicional se ilustra en la figura 6 con el almacenamiento extraíble 608 y el almacenamiento no extraíble 610. Los medios de almacenamiento informático incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implantados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. La memoria 604, el almacenamiento extraíble 608 y el almacenamiento no extraíble 610 son todos ejemplos de medios de almacenamiento informático. Los medios de almacenamiento informático incluyen, sin limitarse a,

RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en discos magnéticos, u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y al que pueda acceder el sistema informático 600. Cualquiera de tales medios de almacenamiento informático puede ser parte del sistema informático 600.

El sistema informático 600 también puede contener conexión o conexiones 612 de comunicaciones que permita/n que el sistema informático se comunique con otros dispositivos. La conexión o las conexiones 612 de comunicaciones son un ejemplo de medios de comunicación. Los medios de comunicación incorporan típicamente instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada tal como una onda portadora u otro mecanismo de transporte, e incluyen cualquier medio de entrega de información. El término "señal de datos modulada" significa que una señal tiene una o más de sus características establecidas o cambiadas de tal manera que codifica información en la señal. A modo de ejemplo, y sin limitación, los medios de comunicación incluyen medios cableados, tales como una red cableada o una conexión cableada directa, y medios inalámbricos, tales como medios acústicos, RF, infrarrojos y otros medios inalámbricos. El término medios legibles por ordenador, tal como se utiliza en el presente documento, incluye tanto medios de almacenamiento como medios de comunicación.

El sistema informático 600 también puede tener uno o varios dispositivos 614 de entrada, tales como teclado, ratón, lápiz, dispositivo de entrada de voz, dispositivo de entrada táctil, etc. En algunas realizaciones, los dispositivos de entrada incluyen también (o alternativamente), por ejemplo, datos biométricos. identificadores, sensores, detectores, lectores de tarjetas y similares. También pueden incluirse dispositivos 616 de salida, tales como una pantalla, altavoces, impresora, etc. Todos estos dispositivos son bien conocidos en la técnica y no es necesario tratarlos en detalle aquí.

En algunas realizaciones, la memoria 604 incluye uno o más elementos de entre el sistema operativo 620, los programas 622 de aplicación, otros módulos 624 de programa y datos 626 de programa. En algunas realizaciones, los datos globales, los datos específicos del cliente y las reglas de transformación pueden ser cada uno de ellos almacenarse en la memoria 604, en el almacenamiento extraíble 608, en el almacenamiento no extraíble 610 o en cualquier otro medio de almacenamiento informático descrito en el presente documento.

Aunque las realizaciones se han descrito en un lenguaje específico de características estructurales, actos metodológicos y medios legibles por ordenador que contienen tales actos, se ha de entender que las posibles realizaciones, tal como se definen en las reivindicaciones adjuntas, no se limitan necesariamente a la estructura, los actos o los medios específicos descritos. El experto en la técnica reconocerá otras realizaciones o mejoras que están dentro del alcance de la presente divulgación. Por lo tanto, la estructura, los actos o los medios específicos se divulgan sólo como realizaciones ilustrativas.

REIVINDICACIONES

1. Un método para controlar el acceso a un recurso de servicio web protegido (106), que comprende:

(i) recibir una primera petición de un cliente (102) para acceder al recurso de servicio web protegido (106) desde una red (110) de comunicación;

(ii) recibir un primer testigo de autenticación del cliente después de que el cliente haya sido autenticado desde un servicio (108) de autenticación, y determinar, en base a la evaluación del primer testigo de autenticación, que el cliente ha sido autenticado de acuerdo con un primer factor;

(iii) conceder la primera petición para acceder al recurso de servicio web protegido (106) en base a la autenticación de acuerdo con el primer factor;

(iv) recibir una segunda petición del cliente (102) para acceder al recurso de servicio web protegido (106) desde la red (110) de comunicación;

(v) denegar la segunda petición para acceder al recurso de servicio web protegido (106) en base a que la autenticación de acuerdo con el primer factor es insuficiente para conceder la segunda petición, y enviar un mensaje al cliente dirigiendo al cliente al servicio de autenticación para que se autentique de acuerdo con un segundo factor;

(vi) recibir un segundo testigo de autenticación del cliente después de que el cliente haya sido autenticado por el servicio de autenticación de acuerdo con el segundo factor, y determinar, en base a la evaluación del segundo testigo de autenticación, que el cliente (102) ha sido autenticado de acuerdo con un segundo factor, y

(vii) conceder la segunda petición para acceder al recurso de servicio web protegido (106) en base a la autenticación de acuerdo con el segundo factor,

en el que el cliente (102) se conecta comunicativamente con el servicio web (104) y con el servicio de autenticación (108) a través de la red (110),

en el que los testigos primero y segundo de autenticación incluyen una reclamación del servicio de autenticación relacionada con un factor que se usó para autenticar al cliente y en el que el testigo de autenticación se cifra usando criptografía de clave pública,

en el que el primer factor se selecciona del grupo que comprende: una contraseña, una respuesta a una pregunta de seguridad, un identificador biométrico, un objeto, e información específica de cliente,

en el que el segundo factor es diferente del primer factor, y

en el que determinar, en base a un testigo de autenticación, que el cliente ha sido autenticado comprende:

descifrar el testigo de autenticación con una clave pública del servicio de autenticación; y

determinar que una reclamación realizada por el servicio de autenticación en el testigo de autenticación satisface una condición de acceso, que comprende evaluar el testigo de autenticación para verificar el número y el tipo de procesos de autenticación completados por el cliente en el servicio de autenticación.

2. El método de la reivindicación 1, en el que denegar la petición comprende

enviar un mensaje de fallo de acuerdo con un protocolo simple de acceso a objetos, y en el que recibir una autenticación comprende recibir un mensaje de respuesta de testigo de seguridad de petición de confianza de servicios web de acuerdo con una especificación de confianza de servicios web.

3. Un sistema informático (104, 108) que comprende:

un dispositivo (612) de comunicación para comunicarse a través de una red (110) de comunicación;

un procesador (602) conectado comunicativamente al dispositivo (612) de comunicación; y

memoria (604) que almacena instrucciones de programa, que cuando son ejecutadas por el procesador (602) hacen que el sistema informático (104) realice el método de la reivindicación 1 ó 2.

4. Un medio de almacenamiento legible por ordenador (608) que contiene instrucciones ejecutables por ordenador que, cuando se ejecutan por un ordenador (104), realizan el método de la reivindicación 1 ó 2.

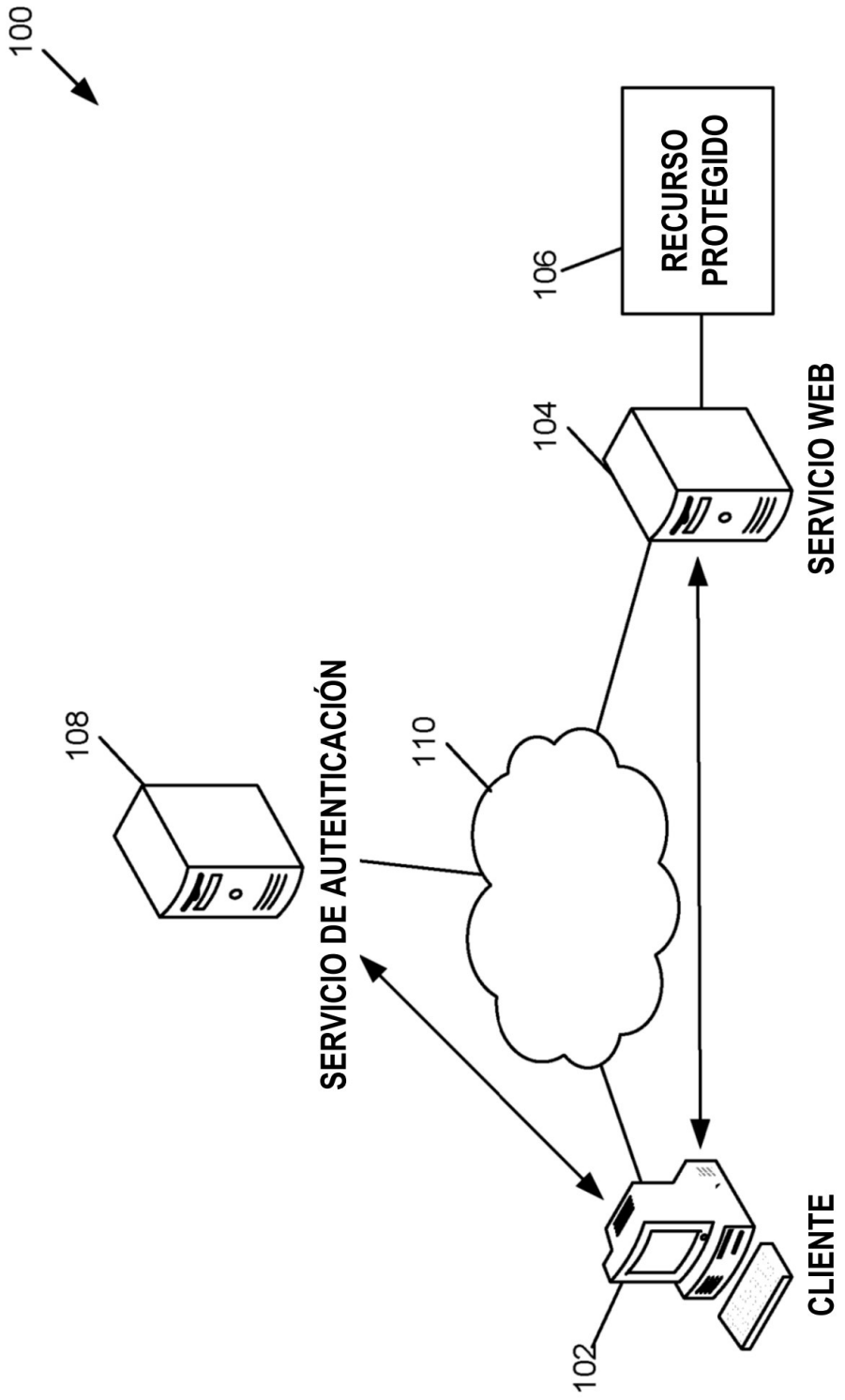
100
RECURSO PROTEGIDO
106
104
SERVICIO WEB
108
SERVICIO DE AUTENTICACIÓN
110
102
CLIENTE

FIG. 1

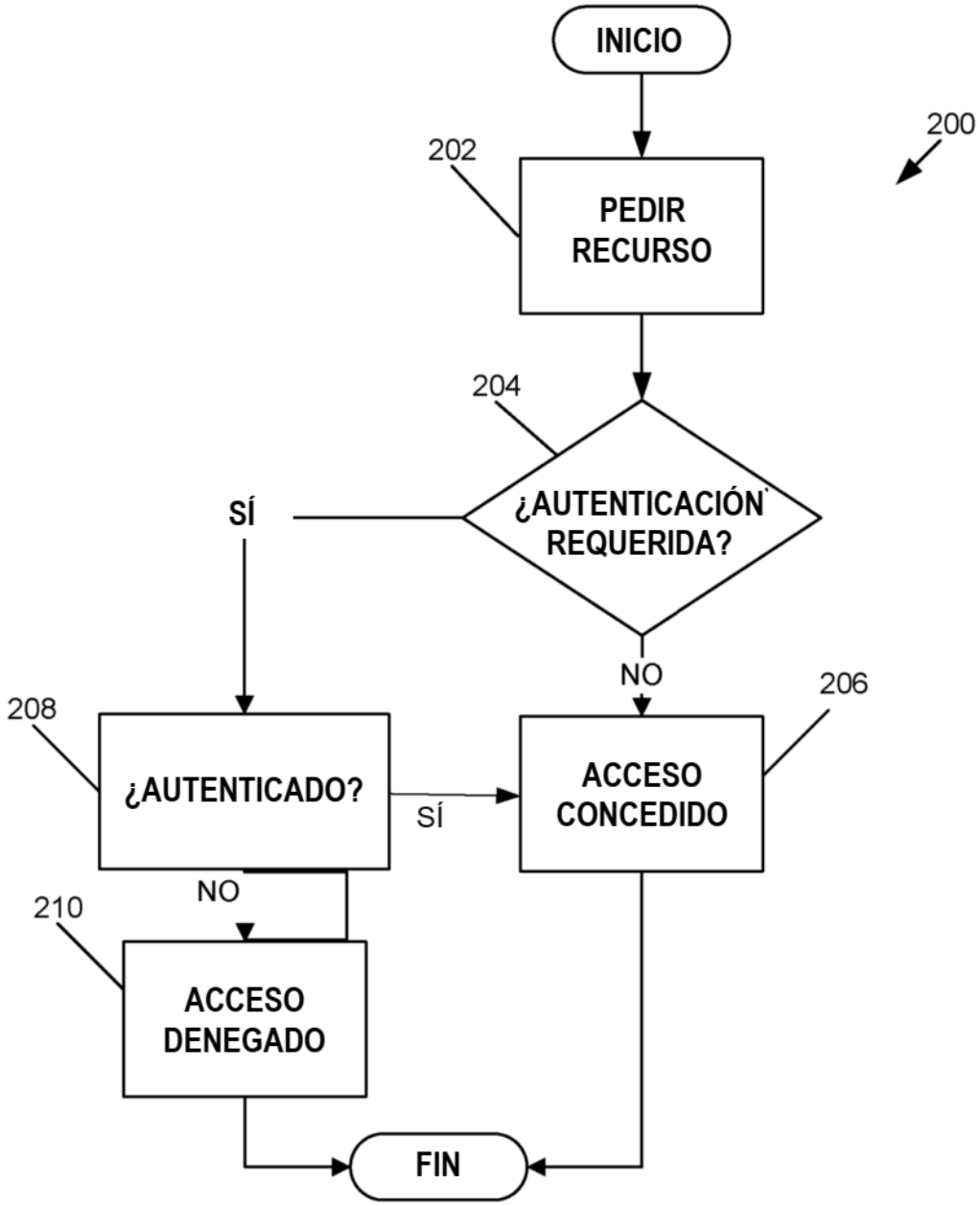
INICIO
200
202
PEDIR RECURSO
204
¿AUTENTICACIÓN REQUERIDA?
SÍ
NO
206
208
¿AUTENTICADO?
SÍ
ACCESO CONCEDIDO
NO
210
ACCESO DENEGADO
FIN

FIG. 2

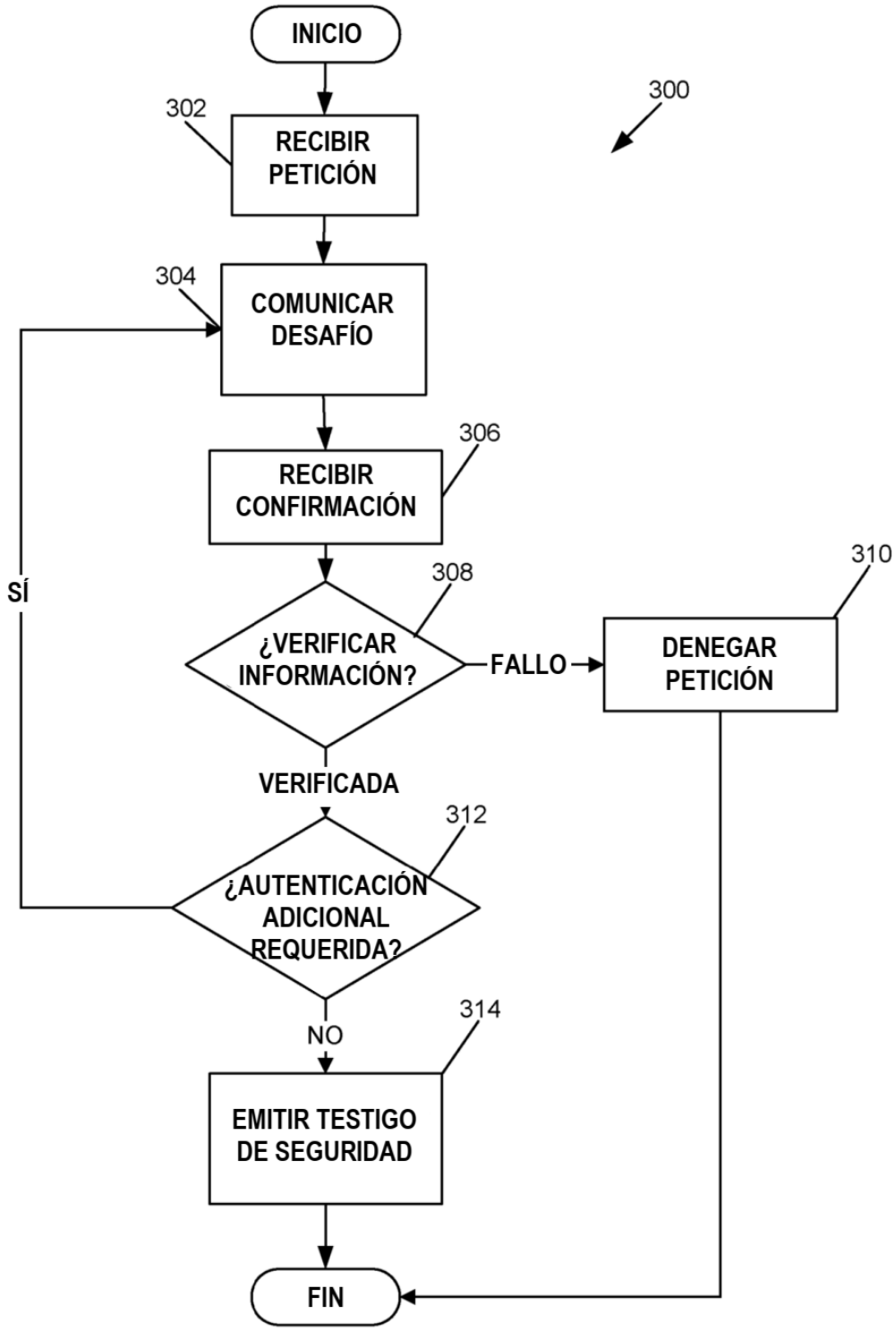
INICIO
300
302
RECIBIR PETICIÓN
304
COMUNICAR DESAFÍO
306
RECIBIR CONFIRMACIÓN
308
¿VERIFICAR INFORMACIÓN?
FALLO
310
DENEGAR PETICIÓN
SÍ
VERIFICADA
312
¿AUTENTICACIÓN ADICIONAL REQUERIDA?
NO
314
EMITIR TESTIGO DE SEGURIDAD
FIN

FIG. 3

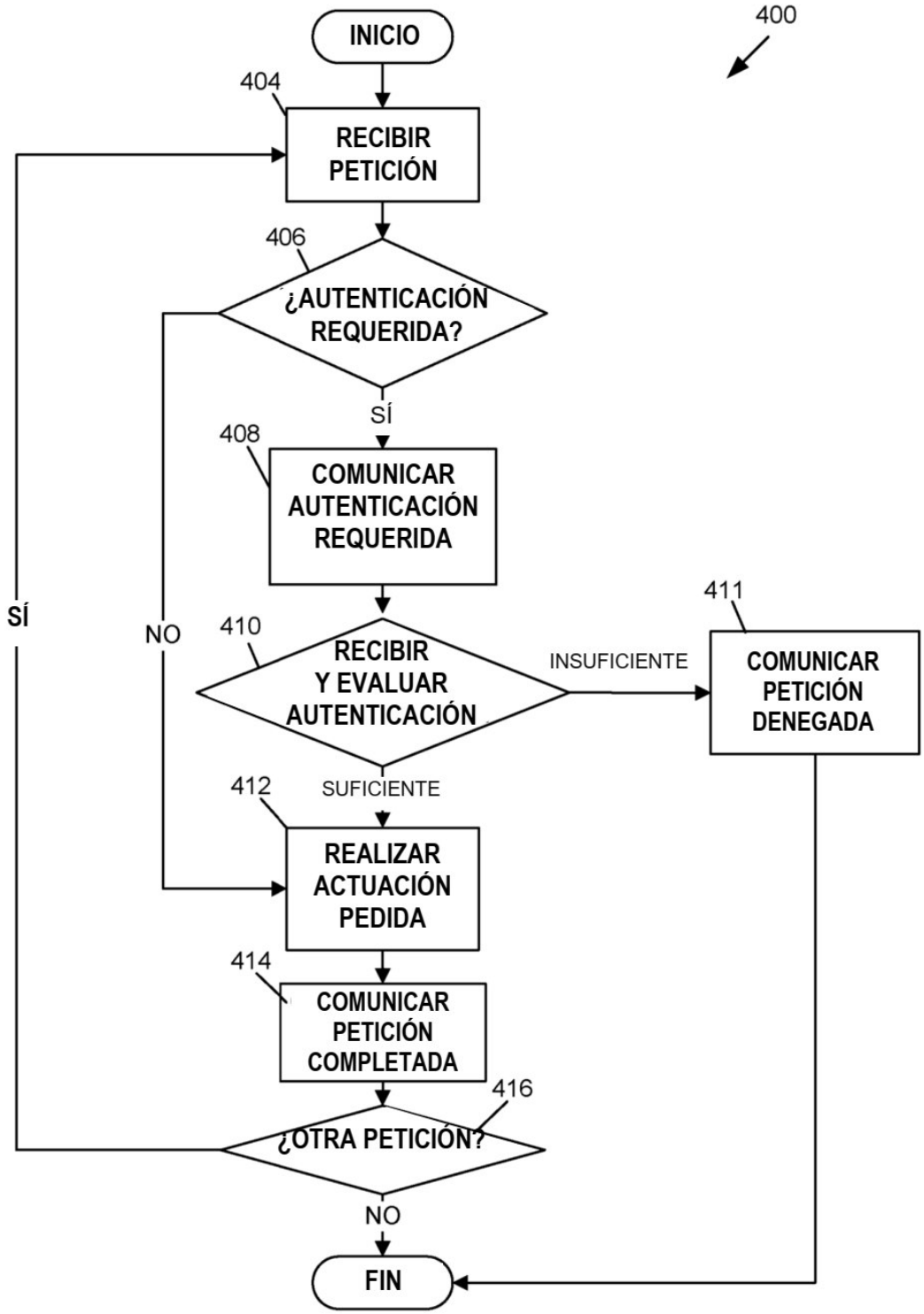
400
INICIO
404
RECIBIR PETICIÓN
406
¿AUTENTICACIÓN REQUERIDA?
SÍ
NO
408
COMUNICAR AUTENTICACIÓN REQUERIDA
410
RECIBIR Y EVALUAR AUTENTICACIÓN
INSUFICIENTE
411
COMUNICAR PETICIÓN DENEGADA
SUFICIENTE
412
REALIZAR ACTUACIÓN PEDIDA
414
COMUNICAR PETICIÓN COMPLETADA
416
¿OTRA PETICIÓN?
SÍ
NO
FIN

FIG. 4

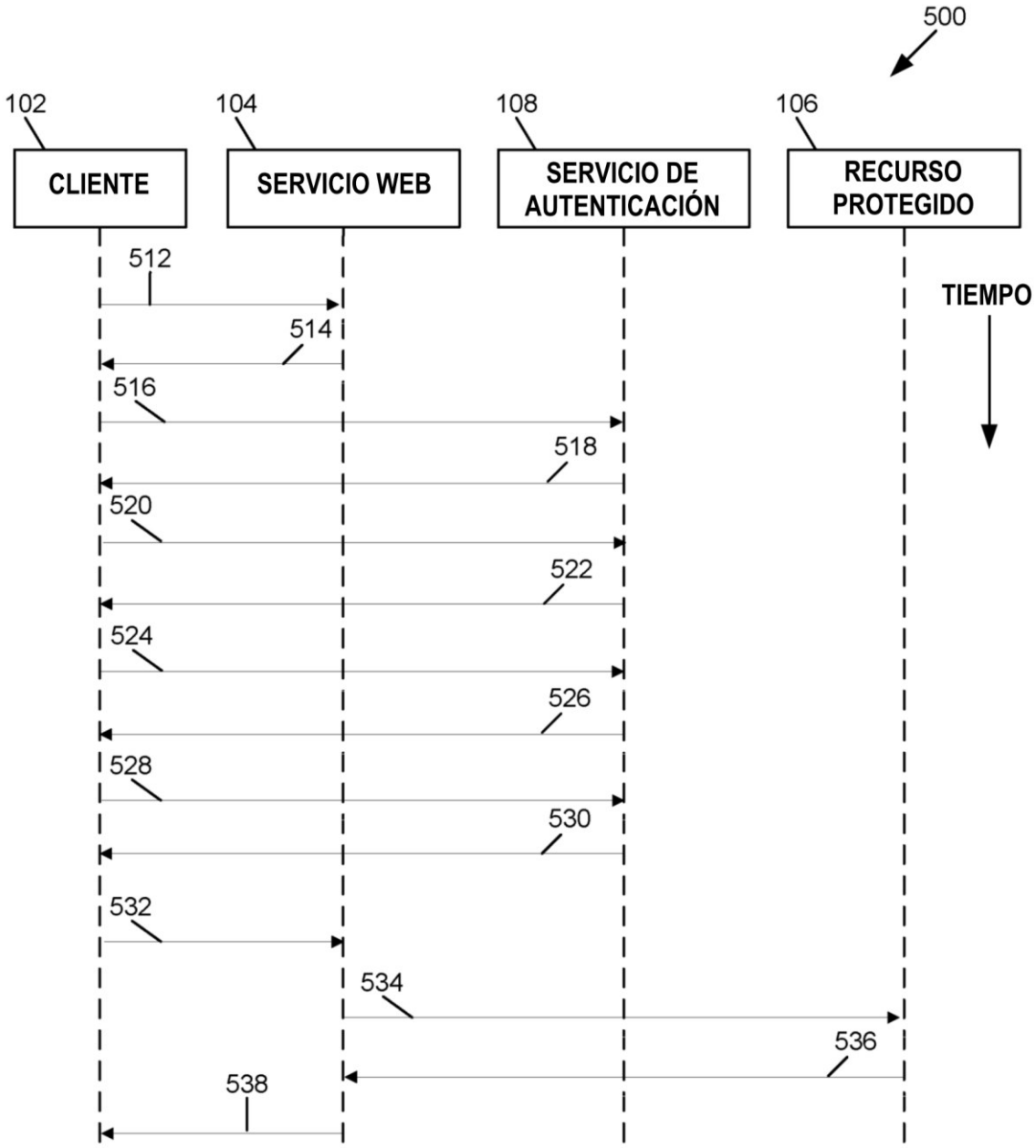
500
102
104
108
106
CLIENTE
SERVICIO WEB
SERVICIO DE AUTENTICACIÓN
RECURSO PROTEGIDO
TIEMPO
512
514
516
518
520
522
524
526
528
530
532
534
536
538

FIG. 5

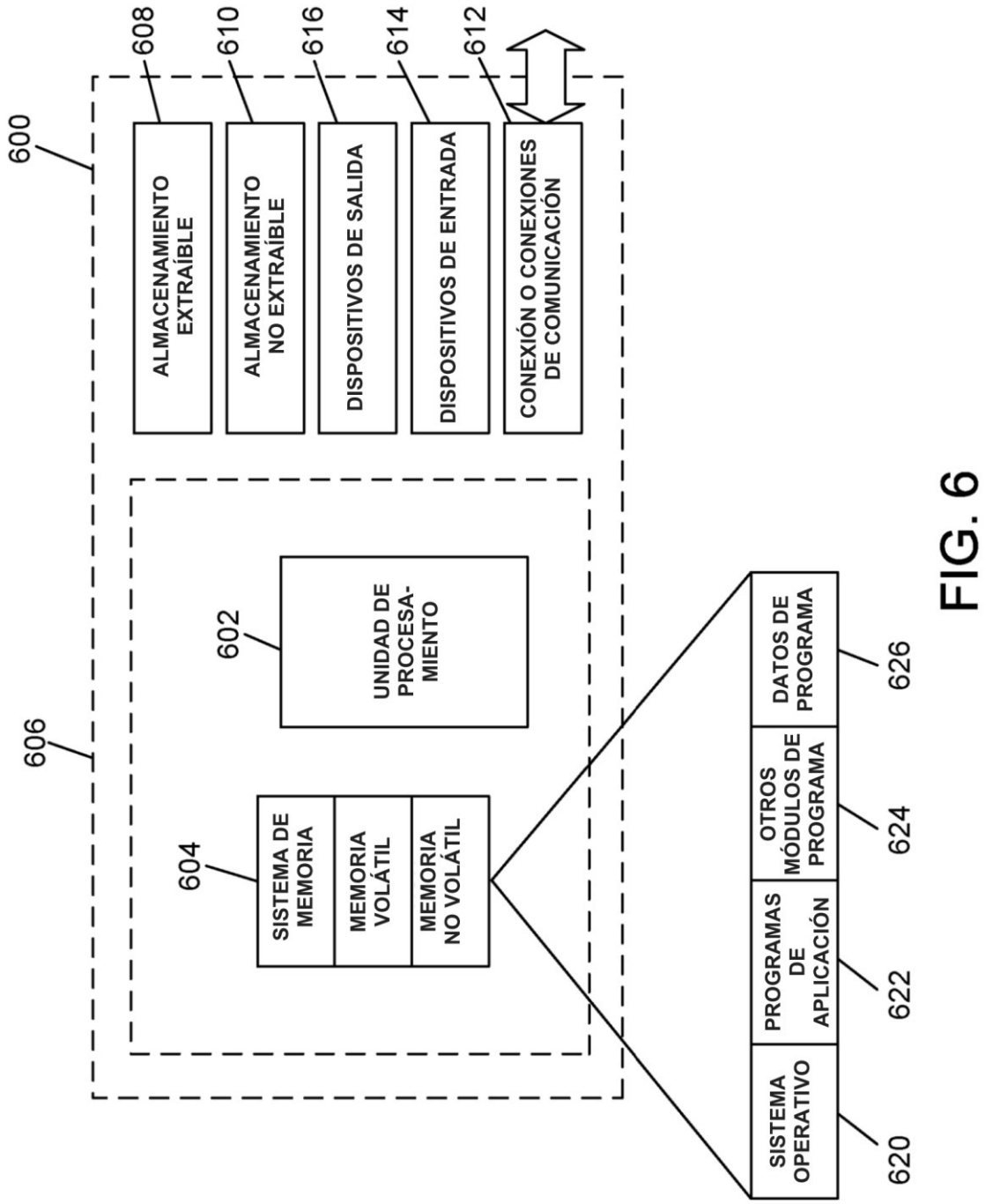
600
608
610
616
614
612
ALMACENAMIENTO EXTRAÍBLE
ALMACENAMIENTO NO EXTRAÍBLE
DISPOSITIVOS DE SALIDA
DISPOSITIVOS DE ENTRADA
CONEXIÓN O CONEXIONES DE COMUNICACIÓN
606
602
UNIDAD DE PROCESA-MIENTO
604
SISTEMA DE MEMORIA
MEMORIA VOLÁTIL
MEMORIA NO VOLÁTIL
DATOS DE PROGRAMA
626
OTROS MÓDULOS DE PROGRAMA
624
PROGRAMAS DE APLICACIÓN
622
SISTEMA OPERATIVO
620

FIG. 6