(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 666**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.04.2007 PCT/US2007/066344**

(87) Fecha y número de publicación internacional: **25.10.2007 WO07121190**

(96) Fecha de presentación y número de la solicitud europea: **10.04.2007 E 07760412 (2)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2018 EP 2005706**

(54) Título: **Procedimiento y aparato para unir múltiples autentificaciones**

(30) Prioridad:

11.04.2006 US 791321 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.04.2019

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
INTERNATIONAL IP ADMINISTRATION 5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

DONDETI, LAKSHMINATH REDDY y
NARAYANAN, VIDYA

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Procedimiento y aparato para unir múltiples autentificaciones

ANTECEDENTES

Campo

[0001] La presente divulgación se refiere, en general, a la comunicación, y más específicamente a técnicas para unir autentificaciones.

Antecedentes

[0002] La autentificación se usa ampliamente para determinar la verdadera identidad de una entidad determinada, para determinar si la entidad tiene derecho a recibir un servicio en particular y/o para otros fines. Por ejemplo, un terminal puede intentar establecer comunicación con una red de comunicación inalámbrica para obtener un servicio de datos, por ejemplo, un Protocolo de Voz sobre Internet (VoIP). La identidad del terminal puede ser autentificada por un servidor de autentificación de la red inalámbrica para asegurar que el terminal pueda comunicarse con la red. El terminal también puede ser autentificado por el mismo o diferente servidor de autentificación para asegurar que el terminal tenga la suscripción adecuada y pueda recibir el servicio de datos solicitado.

[0003] La autentificación puede realizarse enviando información segura de una entidad y verificando esta información mediante otra entidad. Para evitar ataques fraudulentos, la información segura se puede generar basándose en información secreta (por ejemplo, una clave criptográfica) que solo conocen estas dos entidades. La información segura puede ser datos cifrados, un código de autentificación de mensaje u otra información generada basándose en una técnica criptográfica que utiliza la información secreta.

[0004] El terminal puede realizar múltiples autentificaciones secuencialmente o en paralelo. El terminal puede realizar una autentificación para el acceso al sistema y otra autentificación para la petición de servicio. El terminal también puede realizar la autentificación de dispositivo para la petición de servicio. El terminal también puede realizar la autentificación del dispositivo para verificar el terminal y la autentificación del usuario para verificar un usuario del terminal. Es deseable realizar las múltiples autentificaciones de manera tal que estas autentificaciones puedan estar unidas, si es apropiado.

[0005] Se presta mayor atención al documento US 2005/0015490 A1 en el que se describe un adaptador de inicio de sesión único (adaptador SSO) que implementa uno o más mecanismos de autentificación que pueden ser utilizados por el middleware del Portal en nombre de un usuario del portal. Un usuario que busca acceder a un servidor de recursos a través de un servidor de portal realiza un inicio de sesión único con el servidor de portal al comienzo de una sesión. Cuando solicita un recurso del servidor de recursos que requiere autentificación, el servidor de portal maneja la autentificación sin requerir una respuesta de autentificación del usuario. El servidor del portal puede usar credenciales de usuario almacenadas, un servicio de autentificación compartido basado en token o una autentificación proxy para obtener acceso al servidor de recursos en nombre del usuario del portal.

[0006] El documento WILLIAM JOSEPHSON ET AL: " Peer-to-Peer Authentication with a Distributed Single Sign-On Service [Autentificación de igual a igual con un servicio de inicio de sesión único distribuido"] EL TALLER INTERNACIONAL SOBRE SISTEMAS DE IGUAL A IGUAL, 26 de febrero de 2004, describe un principio de igual a igual en el diseño de un servicio de autentificación en toda la red.

SUMARIO

[0007] De acuerdo con la presente invención, se proporciona un aparato como se expone en la reivindicación 1, un procedimiento como se expone en la reivindicación 10, un aparato como se expone en la reivindicación 11 y un procedimiento como se expone en la reivindicación 12. Modos de realización adicionales de la invención se reivindican en las reivindicaciones dependientes.

[0008] Las técnicas para unir múltiples autentificaciones para un igual [peer] se describen en el presente documento. El igual puede realizar múltiples autentificaciones con uno o más servidores de autentificación, que pueden enviar los resultados de las autentificaciones a uno o más autentificadores. Un autentificador es una entidad que inicia y/o facilita la autentificación y típicamente se encuentra en el borde de una red de comunicación. Un igual es una entidad que responde a un autentificador. Un servidor de autentificación es una entidad que proporciona un servicio de autentificación a un autentificador.

[0009] En un diseño, se pueden unir varias autentificaciones para el igual basándose en un identificador único (UID) para el igual. El identificador único puede ser un número pseudoaleatorio y puede intercambiarse de forma segura entre el igual, un servidor de autentificación y un autentificador para evitar un ataque de hombre en el medio (MiTM).

Los datos de todas las autentificaciones unidas por el identificador único pueden intercambiarse de forma segura basándose en una o más claves criptográficas generadas por todas o un subconjunto de estas autentificaciones.

[0010] De acuerdo con un aspecto, un aparato para un igual obtiene un identificador único para el igual y realiza múltiples autentificaciones con al menos un servidor de autentificación. El identificador único se utiliza para unir las múltiples autentificaciones al igual.

[0011] De acuerdo con otro aspecto, un aparato para un servidor de autentificación obtiene un identificador único para un igual, realiza la autentificación con el igual, y asocia el identificador único con el igual.

[0012] De acuerdo con todavía otro aspecto, un aparato para un autentificador recibe resultados de al menos una autentificación entre al menos un servidor de autentificación y un igual. El aparato une la al menos una autentificación al igual basándose en un identificador único.

[0013] En otro diseño, se pueden usar múltiples niveles de seguridad (o seguridad agrupada) para múltiples autentificaciones para un igual. El igual puede realizar una primera autentificación con un primer servidor de autentificación y obtener una primera clave criptográfica. El igual también puede realizar una segunda autentificación con un segundo servidor de autentificación y obtener una segunda clave criptográfica. A continuación, el igual puede intercambiar datos de manera segura usando las dos claves.

[0014] De acuerdo con todavía otro aspecto, se describe un aparato que genera un primer paquete para datos de acuerdo con la primera información de seguridad obtenida a partir de una primera autentificación, genera un segundo paquete que lleva el primer paquete de acuerdo con la segunda información de seguridad obtenida a partir de una segunda autentificación, y envía el segundo paquete.

[0015] A continuación, se describen en más detalle diversos diseños, aspectos y características de la divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0016]

La FIG. 1 muestra una arquitectura para múltiples autentificaciones.

La FIG. 2 muestra un proceso para realizar autentificación.

La FIG. 3 muestra dos autentificaciones para un igual con un ataque MiTM.

La FIG. 4 muestra un proceso para múltiples autentificaciones con un identificador único.

Las FIGs. 5, 6 y 7 muestran los procesos realizados por un igual, un servidor de autentificación y un autentificador, respectivamente, para múltiples autentificaciones con un identificador único.

La FIG. 8 muestra seguridad agrupada para dos autentificaciones.

La FIG. 9 muestra un proceso para múltiples autentificaciones con seguridad agrupada.

La FIG. 10 muestra un diagrama de bloques de diversas entidades en la FIG. 1.

DESCRIPCIÓN DETALLADA

[0017] Las técnicas descritas en el presente documento se pueden usar para varias redes de comunicación tales como redes de área amplia (WAN), redes de área local (LAN), WAN inalámbricas (WWAN), LAN inalámbricas (WLAN), etc. Los términos "redes" y "sistemas" a menudo se usan indistintamente. Las WWAN pueden ser redes de Acceso Múltiple por División de Código (CDMA), redes de Acceso Múltiple por División de Tiempo (TDMA), redes de Acceso Múltiple por División de Frecuencia (FDMA), redes FDMA Ortogonales (OFDMA), redes FDMA de Portadora Única (SC-FDMA), etc. Una red CDMA puede implementar una tecnología de radio como CDMA de banda ancha (W-CDMA), cdma2000, etc. cdma2000 cubre los estándares IS-2000, IS-95 e IS-856. Una red TDMA puede implementar una tecnología de radio tal como el Sistema Global de Comunicaciones Móviles (GSM). Las WLAN pueden implementar IEEE 802.11, Hiperlan, etc. Estas diversas tecnologías y estándares de radio son conocidos en la técnica. Para mayor claridad, ciertos aspectos de las técnicas se describen utilizando la terminología definida en RFC 3748, titulada "Protocolo de autentificación extensible (EAP)", junio de 2004, que está disponible públicamente.

[0018] **La FIG. 1** muestra un despliegue 100 en el que un igual 110 puede realizar múltiples autentificaciones. Para simplificar, solo las entidades lógicas relacionadas con la autentificación se muestran en la FIG. 1. Un despliegue puede incluir otras entidades de red que no se muestran en la FIG. 1.

[0019] El igual 110 puede ser cualquier dispositivo como un teléfono celular, un asistente digital personal (PDA), un dispositivo de comunicación inalámbrica, un dispositivo de mano, un módem inalámbrico, un ordenador portátil, un teléfono inalámbrico, etc. El igual 110 también se puede denominar una estación móvil, una estación, un equipo de usuario, una terminal, una terminal de acceso, una unidad de abonado, un equipo móvil, etc.

[0020] En el ejemplo mostrado en la FIG. 1, el lado de la red incluye L puntos de aplicación 120a a 1201, M autentificadores 130a a 130m y N servidores de autentificación 140a a 140n para N proveedores 150a a 150n, donde en general $L \geq 1$, $M \geq 1$ y $N \geq 1$. El igual 110 puede comunicarse con el punto de aplicación 122a. Cada punto de aplicación 120 puede comunicarse con uno o más puntos de aplicación diferentes 120 y/o con uno o más autentificadores 130. Cada autentificador 130 puede comunicarse con uno o más puntos de aplicación 120, uno o más autentificadores diferentes 130, y/o uno o más servidores de autentificación 140. La FIG. 1 muestra una conexión de ejemplo entre las entidades en el despliegue 100. Estas entidades también se pueden conectar de otras maneras, por ejemplo, se pueden omitir las conexiones discontinuas. Un punto de aplicación es una entidad que hace cumplir o aplica cualquier autentificación que un igual haya completado en los datos de entrada y salida para el igual. Los puntos de aplicación, los autentificadores y los servidores de autentificación son entidades lógicas, y una o más de estas entidades pueden ubicarse dentro de una entidad de red física. Los puntos de aplicación y los autentificadores pueden ser entidades de red separadas, como se muestra en la FIG. 1. Una sola entidad de red también puede realizar las funciones de diferentes entidades lógicas, como un punto de aplicación y un autentificador. Las diversas entidades lógicas en la FIG. 1 se describen en RFC 3748.

[0021] Los puntos de aplicación 120 y los autentificadores 130 pueden ser implementados por diferentes entidades de red en diferentes redes de comunicación. En una WLAN, un punto de aplicación puede ser implementado por un punto de acceso, y un autentificador puede ser implementado por un conmutador de WLAN. En una red celular, un punto de aplicación puede ser implementado por una estación base, y un autentificador puede ser implementado por un controlador de red de radio (RNC). Un servidor de autentificación puede ser implementado por un servidor de Autentificación, Autorización y Contabilidad (AAA) tanto en una WLAN como en una red celular.

[0022] **La FIG. 2** muestra un flujo de mensajes para un proceso de autentificación 200. El igual 110 puede enviar inicialmente una petición de acceso al punto de aplicación 120a, que puede reenviar la petición al autentificador 130a (paso 210). Para el proceso de autentificación, el punto de aplicación 120a puede simplemente reenviar mensajes entre el igual 110 y el autentificador 130a y no se muestra en la FIG. 2 para mayor claridad. El igual 110 puede enviar la petición de acceso, así como otros mensajes, al autentificador 130a utilizando un identificador de capa inferior LID_{peer} asignado al igual 110. Un identificador de capa inferior puede ser una dirección de Control de Acceso al Medio (MAC) o algún otro identificador de capa inferior utilizado entre un igual y un punto de autentificador/aplicación. El autentificador 130a puede recibir la petición de acceso, determinar que no tiene registro para el igual 110 y enviar una petición de autentificación al igual 110 (paso 212).

[0023] El igual 110 puede responder a la petición de autentificación mediante el envío de una respuesta de autentificación que puede incluir una dirección o identidad de un servidor de autentificación que se utilizará para la autentificación del igual 110, un identificador de acceso a la red NAI_{peer} asignado al igual 110, etc. (paso 216). En este ejemplo, el servidor de autentificación 140a es seleccionado por el igual 110, y la respuesta de autentificación puede incluir la dirección del servidor de autentificación 140a (servidor a). El NAI_{peer} puede ser cualquier identificador utilizado entre el igual 110 y el servidor de autentificación 140a y puede que no sea necesario que el autentificador 130a lo conozca. Por lo tanto, el igual 110 puede enviar una respuesta de autentificación anónima y omitir el NAI_{peer}. El autentificador 130a puede recibir la respuesta de autentificación del igual 110 y enviar una petición de autentificación del igual al servidor de autentificación 140a, que se identifica mediante la respuesta de autentificación (paso 218). El servidor de autentificación 140a puede entonces intercambiar mensajes con el igual 110 para la autentificación del igual 110 o para la autentificación mutua (paso 220). El servidor de autentificación 140a puede tener credenciales (por ejemplo, un nombre de usuario y una contraseña) para el igual 110 y puede autentificar el igual 110 basándose en las credenciales. De manera similar, el igual 110 puede tener información almacenada para el servidor de autentificación 140a y puede autentificar el servidor basándose en la información almacenada. La autentificación en el paso 220 se puede realizar basándose en cualquier esquema de autentificación tal como autentificación y acuerdo de clave (AKA), seguridad de la capa de transporte (TLS), TLS tunelizado (TTLS), etc., que se conocen en la técnica.

[0024] Una vez completada la autentificación, el servidor de autentificación 140a puede enviar un mensaje autentificado por el igual al autentificador 130a (paso 222). Este mensaje puede incluir información pertinente como, por ejemplo, una clave criptográfica KEY_1 para usar para la comunicación con el igual 110, una ID de clave para KEY_1 (ID de Key1), etc. Una clave criptográfica también se conoce simplemente como una clave. El autentificador 130a puede enviar la información pertinente al punto de aplicación 120a (no mostrado en la FIG. 2). El punto de aplicación 120a puede usar la KEY_1 o una clave derivada generada a partir de la KEY_1 para el cifrado y/o la protección de la integridad de los datos intercambiados entre el punto de aplicación 120a y el igual 110. Cifrado se refiere a un proceso de aleatorización de datos con una clave de tal manera que los datos originales no son reconocibles y los datos cifrados se pueden recuperar con la misma clave o una clave complementaria dependiendo el tipo de criptografía. La protección de integridad se refiere al proceso de generar un código de autentificación de mensaje para datos con una clave y enviar este código junto con los datos. El código de autentificación del mensaje puede ser utilizado por una entidad receptora para verificar que la entidad emisora utilizó la clave correcta para generar el código y que los datos

no se han alterado. Los datos para la autentificación, que son datos que pueden ser enviados por la autentificación, pueden intercambiarse de manera segura utilizando la clave generada por la autentificación.

[0025] La FIG. 2 muestra un flujo de mensajes de ejemplo en el que el autentificador 130a inicia la autentificación. El igual 110 también puede iniciar la autentificación. En tal caso, puede invertirse la dirección de los mensajes de petición/respuesta de autentificación. En general, se pueden usar menos pasos adicionales y/o diferentes para un flujo de mensajes para la autentificación. Cada paso en el flujo de mensajes puede representar uno o más mensajes enviados por una entidad o múltiples mensajes intercambiados entre diferentes entidades.

[0026] La FIG. 2 muestra una autentificación entre el igual 110 y el servidor de autentificación 140a. El igual 110 puede realizar múltiples autentificaciones con uno o más servidores de autentificación, por ejemplo, para autentificaciones de acceso y servicio, para autentificaciones de dispositivo y usuario, para autentificaciones de proveedor de acceso a la red (NAP) y proveedor de servicios de Internet (ISP), etc. Las múltiples autentificaciones pueden realizarse (i) secuencialmente para que una autentificación se complete antes de que se inicie la siguiente autentificación, (ii) en paralelo para que más de una autentificación pueda estar pendiente en un momento dado, o (iii) una combinación de ambos. Las múltiples autentificaciones pueden ser a través de autentificadores iguales o diferentes. Por ejemplo, se pueden usar diferentes autentificadores para (i) diferentes tipos de autentificación en algunas arquitecturas, (ii) para las autentificaciones de acceso y servicio cuando los proveedores de acceso y servicio son diferentes, etc. Las múltiples autentificaciones también pueden ser iguales o diferentes. servidores de autentificación. Las múltiples autentificaciones pueden ser especialmente aplicables cuando diferentes servidores de autentificación necesitan autentificar el igual 110 por diferentes razones, por ejemplo, cuando los proveedores de acceso y servicio son diferentes.

[0027] En general, una autentificación puede o no dar como resultado que una clave se genere y se pase a un autentificador. Cuando se realizan múltiples autentificaciones, cada autentificación puede generar una clave diferente, un subconjunto de las autentificaciones puede generar claves, o ninguna de las autentificaciones puede generar una clave. Cuando al menos una autentificación no genera claves, puede ser posible un ataque de hombre en el medio.

[0028] **La FIG. 3** muestra dos autentificaciones para el igual 110 con un ataque de hombre en el medio (MiTM). El igual 110 puede realizar una primera autentificación con el servidor de autentificación 140a a través del autentificador 130a utilizando el LID_{peer} y el NAI_{peer} del igual 110, por ejemplo, como se describió anteriormente para la FIG. 2. El igual 110 puede ser autentificado por el servidor de autentificación 140a basado en las credenciales válidas almacenadas en el servidor 140a para el igual 110.

[0029] Un atacante MiTM 112 también puede realizar una autentificación con el servidor de autentificación 140a a través del autentificador 130a utilizando un identificador de capa inferior LID_{MiTM} y un identificador de acceso a la red NAI_{MiTM} asignado al atacante MiTM 112. El atacante MiTM 112 puede ser autentificado por el servidor de autentificación 140a con base en las credenciales válidas almacenadas en el servidor 140a para el atacante MiTM 112.

[0030] El igual 110 puede intentar una segunda autentificación con el servidor de autentificación 140a a través del autentificador 130a utilizando el LID_{peer} y el NAI_{peer} del igual 110. El atacante MiTM 112 puede interceptar la respuesta de autentificación del igual 110 para la segunda autentificación, reemplazar el LID_{peer} del igual 110 con el LID_{MiTM} del atacante 112 y reenviar la respuesta de autentificación manipulada al autentificador 130a. El autentificador 130a puede no tener manera de detectar que la respuesta de autentificación del atacante MiTM 112 ha sido manipulada y puede llevar a cabo la autentificación de la manera habitual. El atacante MiTM 112 puede ser autentificado por el servidor de autentificación 140a y puede obtener el servicio utilizando su LID_{MiTM} y el NAI_{peer} del igual 110. Las facturas relacionadas con la segunda autentificación se pueden redirigir al igual 110, al que se asigna el NAI_{peer}.

[0031] En la FIG. 3, la primera autentificación para el igual 110 puede generar una clave, y esta clave se puede usar para autentificar los datos del igual 110. La primera y la segunda autentificaciones para el igual 110 pueden ocurrir secuencialmente o en paralelo. La segunda autentificación para el igual 110 puede no ser generadora de clave o generar clave, pero no se utiliza ninguna clave para autentificar los datos del igual 110.

[0032] En un aspecto, las múltiples autentificaciones para un igual pueden estar unidas basándose en un identificador único para el igual. El identificador único se puede intercambiar de forma segura entre el igual, un servidor de autentificación y un autentificador para evitar un ataque de MiTM. Los datos de todas las autentificaciones unidas por el identificador único pueden intercambiarse de forma segura basándose en una o más claves generadas por todas o un subconjunto de estas autentificaciones.

[0033] **La FIG. 4** muestra un flujo de mensajes para un proceso 400 para unir varias autentificaciones con un identificador único. El igual 110 puede enviar inicialmente una petición de acceso al autentificador 130a utilizando el LID_{peer} del igual 110 (paso 410). El autentificador 130a puede responder enviando una petición de autentificación al igual 110 (paso 412).

[0034] Para la primera autentificación, el igual 110 puede obtener un identificador único UID_{peer} para sí mismo, como se describe a continuación (paso 414). A continuación, el igual 110 puede enviar una respuesta de autentificación que puede incluir la dirección del servidor de autentificación 140a que se utilizará para la primera autentificación, el NAI_{peer} y el UID_{peer} del igual 110, etc. (paso 416). El UID_{peer} puede enviarse de manera segura (por ejemplo, utilizando cifrado y/o protección de integridad) basándose en una clave compartida entre el igual 110 y el servidor de autentificación 140a. El UID_{peer} puede ser transportado desde el igual 110 al servidor de autentificación 140a, por ejemplo, a través de un procedimiento EAP descrito en RFC 3748 o algún otro procedimiento seguro. La otra información (por ejemplo, el NAI_{peer}) puede o no enviarse de manera segura junto con el UID_{peer}. El autentificador 130a puede recibir la respuesta de autentificación del igual 110 y enviar una petición de autentificación del igual al servidor de autentificación 140a (paso 418).

[0035] El servidor de autentificación 140a puede entonces intercambiar mensajes con el igual 110 para la autentificación del igual 110 o para la autentificación mutua (paso 420). Una vez completada la autentificación, el servidor de autentificación 140a puede enviar un mensaje autentificado por el igual al autentificador 130a (paso 422). Este mensaje puede incluir información pertinente como, por ejemplo, una clave KEY_1 que se usará para la comunicación con el igual 110, una ID de clave para la KEY_1, el UID_{peer} del igual 110, etc. El UID_{peer} se puede enviar de forma segura (p. ej., usando cifrado y/o protección de integridad) basándose en una clave compartida entre el servidor de autentificación 140a y el autentificador 130a. El autentificador 130a puede registrar el UID_{peer} del igual 110 y puede unir la primera autentificación así como la KEY_1 generada por esta autentificación a este UID_{peer} (paso 424). El autentificador 130a también puede unir el UID_{peer} del igual 110 al UID_{peer}. La unión se refiere a asociar diferentes elementos (por ejemplo, una autentificación, una clave, un UID, una LID, etc.) y/o diferentes instancias de un elemento determinado (por ejemplo, múltiples autentificaciones, múltiples claves, etc.) juntas. Unión, asociación y asignación son términos sinónimos que se pueden usar indistintamente.

[0036] Después de completar la primera autentificación, o en paralelo con la primera autentificación, el igual 110 puede enviar una petición de servicio al autentificador 130a utilizando el LID_{peer} del igual 110 (paso 430). El autentificador 130a puede responder enviando una petición de autentificación al igual 110 (paso 432). En general, la segunda autentificación puede ser activada por el igual 110 (por ejemplo, si el igual 110 sabe que se deben realizar múltiples autentificaciones, por ejemplo, para las autentificaciones de dispositivos y usuarios) o por un autentificador.

[0037] Para la segunda autentificación, el igual 110 puede usar el mismo UID_{peer} obtenido anteriormente para la primera autentificación. El igual 110 puede enviar una respuesta de autentificación que puede incluir la dirección del servidor de autentificación 140a que se usará para la segunda autentificación, el NAI_{peer} y el UID_{peer} del igual 110, etc. (paso 436). Nuevamente, el UID_{peer} puede enviarse de manera segura. El autentificador 130a puede recibir la respuesta de autentificación del igual 110 y puede enviar una petición de autentificación del igual al servidor de autentificación 140a (paso 438).

[0038] El servidor de autentificación 140a puede entonces intercambiar mensajes con el igual 110 para la autentificación (paso 440). Una vez completada la autentificación, el servidor de autentificación 140a puede enviar un mensaje autentificado por el igual al autentificador 130a (paso 442). Este mensaje puede incluir información pertinente como, por ejemplo, una clave KEY_2 para usar para la comunicación con el igual 110, una ID de clave para el KEY_2, el UID_{peer} del igual 110, etc. En general, el KEY_2 puede o no generarse mediante la segunda autentificación. El autentificador 130a puede recibir el mensaje autentificado por el igual, extraer el UID_{peer} del mensaje y reconocer que este UID_{peer} ya está almacenado en el autentificador 130a. A continuación, el autentificador 130a puede determinar que esta autentificación es para el mismo igual 110 basándose en el UID_{peer} coincidente. El autentificador 130a puede unir la segunda autentificación, así como la KEY_2 (si es generada por la segunda autentificación) al UID_{peer} (paso 444). El autentificador 130a esencialmente une las autentificaciones primera y segunda para el igual 110 al mismo UID_{peer}.

[0039] En el ejemplo mostrado en la FIG. 4, el igual 110 puede enviar una petición de acceso para una red diferente al autentificador 130a usando el LID_{peer} del igual 110 (paso 450). El autentificador 130a puede responder enviando una petición de autentificación al igual 110 (paso 452). En general, la tercera autentificación puede ser activada por un igual 110 o un autentificador y puede ser por cualquier motivo.

[0040] Para la tercera autentificación, el igual 110 puede usar el mismo UID_{peer} obtenido anteriormente para la primera autentificación. El igual 110 puede enviar una respuesta de autentificación que puede incluir la dirección del servidor de autentificación 140n (Servidor n) que se usará para la tercera autentificación, el NAI_{peer} y el UID_{peer} del igual 110, etc. (paso 456). Nuevamente, el UID_{peer} puede enviarse de manera segura. El autentificador 130a puede recibir la respuesta de autentificación del igual 110 y puede enviar una petición de autentificación del igual al servidor de autentificación 140n, que es seleccionado por el igual 110 (paso 458).

[0041] El servidor de autentificación 140n puede intercambiar mensajes con el igual 110 para la autentificación (paso 460). Una vez completada la autentificación, el servidor de autentificación 140n puede enviar al autentificador 130a un mensaje autentificado por un igual que puede incluir información pertinente como, por ejemplo, una clave KEY_3 para usar para la comunicación con el igual 110, una ID de clave para el KEY_3, el UID_{peer} del igual 110, etc. (paso 442). En general, la KEY_3 puede o no ser generada por la tercera autentificación. El autentificador 130a puede recibir el mensaje autentificado por el igual, reconocer que este UID_{peer} ya está almacenado en el autentificador 130a y unir la tercera

autentificación, así como la KEY_3 (si se generó) al UID_{peer} (paso 464). El autentificador 130a esencialmente une las autentificaciones primera, segunda y tercera para el igual 110 al mismo UID_{peer}, aunque estas autentificaciones se realizaron a través de diferentes servidores de autentificación 140a y 140n.

[0042] En general, el igual 110 puede realizar cualquier número de autentificaciones con cualquier número de servidores de autentificación. Estas múltiples autentificaciones pueden realizarse secuencialmente (como se muestra en la FIG. 4), o en paralelo (no se muestra en la FIG. 4), o una combinación de ambos. Cada autentificación puede autentificarse mutuamente para que el igual 110 se autentifique en un servidor de autentificación y el servidor de autentificación también se autentifique en el igual 110. Cada autentificación puede o no generar una clave. El autentificador 130a puede unir todas las autentificaciones y todas las claves con el mismo UID_{peer} al igual 110. Solo una autentificación puede generar una clave, y todas las autentificaciones unidas con esta autentificación pueden intercambiar datos de forma segura basándose en la clave de esta autentificación.

[0043] El UID_{peer} puede intercambiarse de manera segura entre el igual 110 y cada servidor de autentificación, por ejemplo, utilizando cifrado y/o protección de integridad basada en las credenciales conocidas por el igual 110 y el servidor de autentificación. En este caso, un atacante MiTM no podría interceptar al UID_{peer} y secuestrar el intercambio de autentificación.

[0044] En el diseño mostrado en la FIG. 4, el igual 110 envía el UID_{peer} en la respuesta de autentificación al autentificador 140a en los pasos 416, 436 y 456, y el autentificador 140a reenvía el UID_{peer} a los servidores de autentificación 140a y 140n. El igual 110 también puede enviar el UID_{peer} en otros momentos, por ejemplo, en los pasos 420, 440, 460, etc.

[0045] En general, un UID se puede obtener de varias maneras. En un diseño, el igual 110 genera un número pseudoaleatorio (PRN) y utiliza este PRN como el UID. Diferentes iguales pueden generar independientemente diferentes PRNs. La probabilidad de que dos iguales generen el mismo PRN, que se conoce como colisión, depende de la longitud del PRN. Por ejemplo, si el PRN tiene una longitud de 32 bits, entonces la probabilidad de colisión puede ser $1/2^{32}$. En general, el PRN puede tener cualquier longitud, por ejemplo, 32 bits, 48 bits, 64 bits, etc. El PRN puede definirse como suficientemente largo para lograr la probabilidad deseada de colisión. Se pueden usar PRN de la misma longitud para todas las autentificaciones. De forma alternativa, los PRN de diferentes longitudes pueden ser para diferentes autentificaciones, donde la longitud de PRN para cada autentificación puede depender de los requisitos de seguridad y/o de otros factores.

[0046] En otro diseño, una ID asignada al igual 110 o una pseudo versión de esta ID puede usarse como el UID. Por ejemplo, el UID puede ser un número de serie electrónico (ESN), un identificador de equipo móvil (MEID), una identidad de abonado móvil internacional (IMSI), un número de identificación móvil (MIN), un pseudo-ESN, un IMSI temporal, o alguna otra ID verdadera o pseudo asignada al igual 110. En otro diseño más, una dirección asignada al igual 110 puede usarse como el UID. Por ejemplo, el UID puede ser una dirección MAC, una dirección IP, etc. En general, un ID o dirección de cualquier tipo que sea único para un igual (o que tenga una probabilidad de colisión suficientemente baja) puede usarse como el UID para unir autentificaciones para el igual.

[0047] Se puede usar un solo UID para todas las autentificaciones para el igual 110. Todas estas autentificaciones pueden estar unidas a este UID único. Las autentificaciones para el igual 110 también se pueden dividir en varios grupos, y cada grupo incluye una o más autentificaciones. Se puede usar un UID diferente para cada grupo. Todas las autentificaciones de cada grupo pueden estar unidas por el UID para ese grupo. En general, se puede usar un UID para que todas las autentificaciones se unan. Un UID dado puede usarse para una o más autentificaciones.

[0048] En el diseño mostrado en la FIG. 4, el igual 110 puede obtener un UID y enviar este UID de forma segura a cada servidor de autentificación. Un UID también puede ser generado por una entidad que no sea el igual 110. En otro diseño, un servidor de autentificación puede generar un UID y proporcionar este UID a ambos iguales 110 y un autentificador. El igual 110 puede informar al servidor de autentificación para la primera autentificación (por ejemplo, durante el paso 420) que no se ha generado un UID para el igual 110. En respuesta, el servidor de autentificación puede generar un UID para el igual 110. El igual 110 puede usar este UID para cada autentificación subsiguiente para unirse con la primera autentificación. En otro diseño más, un autentificador puede generar un UID para el igual 110.

[0049] En el ejemplo mostrado en la FIG. 4, el igual 110 realiza múltiples autentificaciones a través de un único autentificador 140a, que une todas las autentificaciones y claves al UID_{peer} del igual 110. El igual 110 también puede realizar múltiples autentificaciones a través de múltiples autentificadores, por ejemplo, utilizando el mismo UID_{peer}. En este caso, el UID_{peer} puede ser transmitido de manera segura a todos los autentificadores para sincronizar estos autentificadores.

[0050] Las múltiples autentificaciones para el igual 110 se pueden aplicar en uno o más puntos de aplicación. Si todas las autentificaciones son aplicadas por un solo punto de aplicación, entonces todos los autentificadores utilizados para las múltiples autentificaciones pueden pasar información de seguridad (por ejemplo, claves) para el igual 110 y posiblemente el UID_{peer} a este punto de aplicación. De forma alternativa, un autentificador puede pasar el UID_{peer} del igual 110 y la información de seguridad al punto de aplicación, y los autentificadores restantes solo pueden pasar el

UID_{peer} del igual 110. Si las múltiples autentificaciones son aplicadas por múltiples puntos de aplicación, entonces cada punto de aplicación puede recibir el UID_{peer} del igual 110 y cualquier información de seguridad asociada para que la(s) autentificación(ones) sea(n) aplicada(s) por ese punto de aplicación. En general, cada punto de aplicación puede aplicar todas las autentificaciones responsables de ese punto de aplicación basándose en la información de seguridad asociada con las autentificaciones que se aplican.

[0051] La unión de varias autentificaciones a través de un único UID permite que una clave generada por una autentificación se utilice para intercambios de datos para otra autentificación. De hecho, una sola clave generada por una única autentificación puede usarse para todas las autentificaciones. Los datos para una autentificación que no es de generación de claves pueden enviarse de manera segura utilizando una clave de otra autentificación que sea de generación de claves. Esto es posible ya que las dos autentificaciones están unidas al mismo UID y, por lo tanto, al mismo igual.

[0052] Las múltiples autentificaciones pueden generar múltiples claves. En este caso, los intercambios de datos seguros para las múltiples autentificaciones se pueden lograr de varias maneras. En un diseño, se puede seleccionar una sola clave de entre las múltiples claves y utilizarla para enviar datos de manera segura para todas las autentificaciones. En otro diseño, las múltiples claves pueden usarse para generar una clave compuesta, que luego puede usarse para enviar datos de manera segura para todas las autentificaciones. En otro diseño más, los datos para cada autentificación generadora de clave pueden enviarse de manera segura utilizando la clave generada por esa autentificación. Los datos para cada autentificación no generadora de clave pueden enviarse de forma segura utilizando una clave de una autentificación generadora de clave o una clave compuesta. Los datos de las múltiples autentificaciones también pueden enviarse de forma segura de otras maneras.

[0053] La **FIG. 5** muestra un diseño de un proceso 500 realizado por un igual para múltiples autentificaciones con un identificador único. Se puede obtener un identificador único para el igual (bloque 512). Se pueden realizar múltiples autentificaciones con al menos un servidor de autentificación, con el identificador único que se utiliza para unir las múltiples autentificaciones al igual (bloque 514). El igual puede obtener el identificador único basándose en un número pseudoaleatorio, un identificador o una dirección asignada al igual, etc. El igual puede enviar de forma segura el identificador único a cada servidor de autentificación utilizando el cifrado y/o la protección de integridad. El igual también puede obtener el identificador único de un servidor de autentificación o un autentificador. Las múltiples autentificaciones se pueden realizar secuencialmente y/o en paralelo y pueden ser para autentificación de acceso, autentificación de servicio, autentificación de dispositivo, autentificación de usuario, autentificación de NAP, autentificación de ISP, etc.

[0054] Al menos una clave criptográfica se puede obtener de las múltiples autentificaciones (bloque 516). Los datos para las múltiples autentificaciones se pueden intercambiar de forma segura basándose en la al menos una clave criptográfica (bloque 518). Por ejemplo, se puede obtener una clave criptográfica a partir de una primera autentificación y utilizarla para intercambiar datos de manera segura para una segunda autentificación.

[0055] La **FIG. 6** muestra un diseño de un proceso 600 realizado por un servidor de autentificación. Se puede obtener un identificador único para un igual, por ejemplo, recibido de forma segura del igual o un autentificador, o generado por el servidor de autentificación (bloque 612). La autentificación puede realizarse con el igual (bloque 614). El identificador único puede estar asociado con el igual (bloque 616). Se puede enviar a un autentificador una indicación del igual autentificado, el identificador único y, posiblemente, la información de seguridad (por ejemplo, una clave criptográfica), que puede usar el identificador único para unir la autentificación al igual (bloque 616).

[0056] La **FIG. 7** muestra un diseño de un proceso 700 realizado por un autentificador. Se pueden recibir los resultados de al menos una autentificación entre al menos un servidor de autentificación y un igual (bloque 712). La al menos una autentificación puede estar unida a un igual basándose en un identificador único (bloque 714). Se puede obtener al menos una clave criptográfica a partir de los resultados de la al menos una autentificación (bloque 716). Ya sea la al menos una clave criptográfica o al menos una clave derivada (que puede generarse basándose en la al menos una clave criptográfica) y posiblemente el identificador único puede reenviarse a un punto de aplicación para la al menos una autentificación (bloque 718). El autentificador también puede aplicar la al menos una autentificación basada en la al menos una clave criptográfica. Los resultados de una o más autentificaciones diferentes para el igual y el identificador único también pueden recibirse de otro autentificador. La al menos una autentificación y las una o más autentificaciones diferentes para el igual pueden unirse basándose en el identificador único.

[0057] En otro aspecto, se pueden usar múltiples niveles de seguridad (o seguridad agrupada) para múltiples autentificaciones para un igual. Por ejemplo, el igual 110 puede realizar una primera autentificación (por ejemplo, autentificación de acceso o dispositivo) con un primer servidor de autentificación y obtener una primera clave KEY_1. El igual 110 también puede realizar una segunda autentificación (por ejemplo, autentificación de servicio o usuario) con un segundo servidor de autentificación y obtener una segunda clave KEY_2. A continuación, los datos para el servicio deseado pueden intercambiarse de manera segura usando las dos claves KEY_1 y KEY_2.

[0058] En general, el igual 110 puede realizar cualquier número de autentificaciones con cualquier número de servidores de autentificación. Cada autentificación puede o no ser generadora de clave. Una clave generada por una autentificación dada puede usarse para intercambiar datos de forma segura para esa autentificación.

[0059] Para la seguridad agrupada, las múltiples autentificaciones se pueden realizar a través de uno o más autentificadores y se pueden hacer cumplir por uno o más puntos de aplicación. Cada autentificador puede obtener una o más claves para una o más autentificaciones y puede unir todas las claves con el igual, por ejemplo, basándose en la LID o alguna otra identificación del igual. Cada punto de aplicación puede recibir una o más claves para una o más autentificaciones de uno o más autentificadores. Cada punto de aplicación puede intercambiar datos de forma segura con el igual utilizando una o más claves recibidas por ese punto de aplicación.

[0060] **La FIG. 8** muestra seguridad agrupada para dos autentificaciones. La autentificación 1 puede ser para la autentificación del servicio, y la autentificación 2 puede ser la autentificación de acceso. Los datos para la autentificación 1 pueden intercambiarse entre el igual 110 y un punto de aplicación para un proveedor de servicios. Los datos para la autentificación 2 pueden intercambiarse entre el igual 110 y un punto de acceso en una red de acceso. Se pueden usar los mismos o diferentes puntos de aplicación para las autentificaciones 1 y 2.

[0061] El paquete 1 para la autentificación 1 puede incluir una cabecera, una carga útil y un extremo. La carga útil puede transportar datos, que pueden estar cifrados y/o protegidos por integridad con una clave generada por la autentificación 1. La cabecera puede llevar un ID de clave de la clave generada por la autentificación 1 y utilizada para los datos enviados en la carga útil. El extremo puede llevar un código de autentificación de mensaje (MAC1), que puede generarse basándose en los datos enviados en la carga útil con la clave generada por la autentificación 1. El destinatario del paquete puede utilizar el código de autentificación del mensaje para verificar la integridad de los datos enviados en la carga útil, así como la prueba de propiedad de la clave utilizada por un remitente del paquete.

[0062] De manera similar, el paquete 2 para la autentificación 2 puede incluir una cabecera, una carga útil y un extremo. La carga útil para el paquete 2 puede llevar todo el paquete 1, que puede estar cifrado y/o protegido por integridad con una clave generada por la autentificación 2. La cabecera puede llevar un ID de clave de la clave generada por la autentificación 2. El extremo puede llevar un código de autentificación de mensaje (MAC2) generado basándose en los datos en la carga útil del paquete 2 y con la clave generada por la autentificación 2.

[0063] El igual 110 puede realizar el procesamiento agrupado que se muestra en la FIG. 8 para enviar datos para autentificaciones 1 y 2. Si se usa un solo punto de aplicación para las autentificaciones 1 y 2, entonces este punto de aplicación puede extraer (por ejemplo, descifrar y/o verificar) datos de ambas cargas útiles en los paquetes 1 y 2. Si se usan diferentes puntos de aplicación para las autentificaciones 1 y 2, entonces el punto de aplicación para la autentificación 2 puede extraer los datos de la carga útil del paquete 2, y el punto de aplicación para la autentificación 1 puede extraer los datos de la carga útil del paquete 1.

[0064] En otro diseño, los datos se procesan de forma segura (por ejemplo, cifrados y/o protegidos por integridad) con las claves generadas por las autentificaciones 1 y 2 para obtener un paquete de datos. Por ejemplo, los datos pueden procesarse de manera segura con la clave generada por la autentificación 1 para obtener los primeros datos procesados, que pueden además procesarse de manera más segura con la clave generada por la autentificación 2 para obtener segundos datos procesados, que pueden enviarse en la carga útil del paquete de datos. El paquete de datos puede incluir una única cabecera, que puede contener los ID de clave de ambas claves. El paquete de datos puede incluir además un solo extremo que puede incluir MAC1 y/o MAC2.

[0065] La **FIG. 9** muestra un diseño de un proceso 900 realizado por un igual para múltiples autentificaciones con seguridad agrupada. La primera y segunda autentificaciones se pueden realizar con al menos un servidor de autentificación (bloque 912). La primera autentificación se puede realizar con un primer servidor de autentificación, y la segunda autentificación se puede realizar con el primer servidor de autentificación o un segundo servidor de autentificación. La primera y la segunda información de seguridad, por ejemplo, la primera y la segunda claves criptográficas, se pueden obtener para la primera y la segunda autentificación, respectivamente (bloque 914). Posteriormente, se puede generar un paquete de datos con la primera y la segunda información de seguridad obtenidas a partir de la primera y la segunda autentificación (bloque 916).

[0066] En un diseño, los datos pueden procesarse de forma segura (por ejemplo, cifrados y/o protegidos por integridad) basándose en la primera información de seguridad (por ejemplo, la primera clave criptográfica) para obtener un paquete inicial. El paquete inicial puede procesarse de forma segura basándose en la segunda información de seguridad (por ejemplo, la segunda clave criptográfica) para obtener el paquete de datos. En otro diseño, los datos pueden procesarse de manera segura con la primera y la segunda información de seguridad para obtener el paquete de datos. Se puede realizar el mismo procesamiento seguro (por ejemplo, cifrado y/o protección de integridad) con cada una de la primera y la segunda información de seguridad. De forma alternativa, un tipo de procesamiento seguro (por ejemplo, cifrado) puede realizarse con la primera información de seguridad, y otro tipo de procesamiento seguro (por ejemplo, protección de integridad) puede realizarse con la segunda información de seguridad.

[0067] En otro aspecto más, la seguridad secuencial puede usarse para múltiples autentificaciones para un igual. Por ejemplo, el igual 110 puede realizar la primera autentificación con un primer servidor de autentificación y obtener una primera clave KEY_1. Después de completar la primera autentificación, se puede usar la KEY_1 para el procesamiento seguro de cada autentificación posterior. Las autentificaciones subsiguientes pueden realizarse secuencialmente o en paralelo después de la primera autentificación.

[0068] **La FIG. 10** muestra un diagrama de bloques del igual 110, el punto de aplicación 120a, el autentificador 130a y el servidor de autentificación 140a en la FIG. 1. El igual 110 puede ser un terminal, etc. El punto de aplicación 120a puede ser una estación base, un punto de acceso, etc. El autentificador 130a puede ser un conmutador WLAN, un RNC, etc. El servidor de autentificación 140a puede ser un servidor AAA, etc. Por simplicidad, La FIG. 10 muestra (a) un controlador/procesador 1010, una memoria 1012 y un transceptor 1016 para el igual 110, (b) un controlador/procesador 1020, una memoria 1022, una unidad de comunicación (Comm) 1024 y un transceptor 1026 para el punto de aplicación 120a, (c) un controlador/procesador 1030, una memoria 1032 y una unidad de comunicación 1034 para el autentificador 130a, y (d) un controlador/procesador 1040, una memoria 1042 y una unidad de comunicación 1044 para el servidor de autentificación 140a. En general, cada entidad puede incluir cualquier número de controladores, procesadores, memorias, transceptores, unidades de comunicación, etc.

[0069] El igual 110 puede enviar datos al punto de aplicación 120a. Los datos pueden ser procesados por el procesador 1010 y acondicionados por el transceptor 1016 para generar una señal modulada, que puede ser transmitida por una antena. En el punto de aplicación 120a, la señal del igual 110 puede ser recibida y acondicionada por el transceptor 1026 y procesada por el procesador 1020 para recuperar los datos enviados por el igual 110. El punto de aplicación 120a también puede enviar datos al igual 110. Los datos pueden ser procesados por el procesador 1020 y acondicionados por el transceptor 1026 para generar una señal modulada, que puede ser transmitida al igual 110. En el igual 110, la señal del punto de aplicación 120a puede ser recibida y acondicionada por el transceptor 1016 y procesada por el procesador 1010 para recuperar los datos enviados por el punto de aplicación 120a.

[0070] El procesador 1010 puede realizar el procesamiento para el igual 110 para autentificación, intercambio de datos, etc. El procesador 1010 puede realizar el proceso 500 en la FIG. 5, proceso 900 en la FIG. 9, y/u otros procesos de autentificación e intercambio de datos. Las memorias 1012 y 1022 pueden almacenar códigos y datos de programa para el igual 110 y el punto de aplicación 120a, respectivamente. El punto de aplicación 120a puede comunicarse con otras entidades, como el autentificador 130a, a través de la unidad de comunicación 1024.

[0071] Dentro del autentificador 130a, el procesador 1030 puede realizar el procesamiento para el autentificador 130a y dirigir el funcionamiento de varias unidades dentro del autentificador. La memoria 1032 puede almacenar datos y códigos de programa para el autentificador 130a. El procesador 1030 puede implementar el proceso 700 en la FIG. 7 y/u otros procesos para la autentificación de iguales. La unidad de comunicación 1034 puede soportar la comunicación entre el autentificador 130a y otras entidades como el punto de aplicación 120a y el servidor de autentificación 140a.

[0072] Dentro del servidor de autentificación 140a, el procesador 1040 puede realizar el procesamiento del servidor de autentificación 140a y dirigir la operación de varias unidades dentro del servidor de autentificación. El procesador 1040 puede implementar el proceso 600 en la FIG. 6 y/u otros procesos para la autentificación de iguales. La memoria 1042 puede almacenar códigos de programa y datos para el servidor de autentificación 140a. La unidad de comunicación 1044 puede soportar la comunicación entre el servidor de autentificación 140a y otras entidades tales como el autentificador 130a.

[0073] Los expertos en la materia entenderán que la información y las señales pueden representarse usando cualquiera entre una diversidad de tecnologías y técnicas diferentes. Por ejemplo, los datos, las instrucciones, los comandos, la información, las señales, los bits, los símbolos y los chips que puedan haberse mencionado a lo largo de la descripción anterior pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos o cualquier combinación de los mismos.

[0074] Los expertos en la técnica apreciarán, además, que los diversos bloques lógicos, módulos, circuitos y pasos de algoritmo ilustrativos, descritos en relación con la divulgación en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito, en general, diversos componentes, bloques, módulos, circuitos y pasos ilustrativos en términos de su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de la aplicación particular y de las restricciones de diseño impuestas en el sistema global. Los expertos en la materia pueden implementar la funcionalidad descrita de distintas maneras para cada aplicación particular, pero no se debería interpretar que dichas decisiones de implementación suponen apartarse del alcance de la presente divulgación.

[0075] Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con la divulgación en el presente documento pueden implementarse o realizarse con un procesador de uso general, con un procesador de señales digitales (DSP), con un circuito integrado específico de la aplicación (ASIC), con una formación de puertas programables in situ (FPGA) o con otro dispositivo de lógica programable, con lógica de puertas discretas o

transistores, con componentes de hardware discretos o con cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de uso general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estados convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ejemplo, una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo.

[0076] Los pasos de un procedimiento o algoritmo descrito en relación con la divulgación en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo de software puede residir en una memoria RAM, en una memoria flash, en una memoria ROM, en una memoria EPROM, en una memoria EEPROM, en registros, en un disco duro, en un disco extraíble, en un CD-ROM o en cualquier otra forma de medio de almacenamiento conocido en la técnica. Un medio de almacenamiento a modo de ejemplo está acoplado al procesador de modo que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

[0077] La descripción anterior de la divulgación se da a conocer para permitir que cualquier experto en la materia realice o use la divulgación. Diversas modificaciones de la divulgación resultarán fácilmente evidentes para los expertos en la técnica, y los principios genéricos definidos en el presente documento pueden aplicarse a otras variantes sin apartarse de la divulgación. Por lo tanto, la divulgación no pretende limitarse a los ejemplos descritos en el presente documento, sino que se le concede el alcance más amplio compatible con los principios y características novedosas divulgados en el presente documento.

[0078] La invención se divulga mediante las reivindicaciones independientes. Se definen modos de realización adicionales mediante las reivindicaciones dependientes.

REIVINDICACIONES

1. Un aparato que comprende:

medios para obtener un solo identificador único para un igual; y

medios para realizar múltiples autentificaciones con al menos un servidor de autentificación;

medios para unir las múltiples autentificaciones a través del solo identificador único; y

medios para obtener una única clave criptográfica, a partir de al menos un servidor de autentificación, en el que dicha única clave criptográfica se genera basándose en una única de las múltiples autentificaciones, y en el que dicha única clave criptográfica se usa para todas las otras autentificaciones de las múltiples autentificaciones.

2. El aparato según la reivindicación 1, en el que los medios para obtener y realizar son un procesador que genera un número pseudoaleatorio y usa el número pseudoaleatorio como el identificador único para el igual.

3. El aparato según la reivindicación 1, en el que el procesador usa un identificador o una dirección asignada al igual como el identificador único para el igual.

4. El aparato según la reivindicación 1, en el que el procesador recibe el identificador único de un servidor de autentificación o un autentificador.

5. El aparato según la reivindicación 1, en el que para una de las múltiples autentificaciones, el procesador recibe una petición de autentificación de un autentificador, envía una respuesta de autentificación con el identificador único, siendo el identificador único reenviado por el autentificador al servidor de autentificación, y realiza la autentificación mutua con el servidor de autentificación.

6. El aparato según la reivindicación 1, en el que el procesador envía de forma segura el identificador único a un servidor de autentificación para una primera autentificación, y envía de forma segura el identificador único al servidor de autentificación para una segunda autentificación.

7. El aparato según la reivindicación 1, en el que las múltiples autentificaciones comprenden autentificación de acceso y autentificación de servicio.

8. El aparato según la reivindicación 1, en el que las múltiples autentificaciones comprenden la autentificación del dispositivo y la autentificación del usuario.

9. El aparato según la reivindicación 1, en el que las múltiples autentificaciones comprenden una primera autentificación para un proveedor de acceso a la red, NAP, y una segunda autentificación para un proveedor de servicios de Internet, ISP.

10. Un procedimiento que comprende:

obtener un solo identificador único para un igual; y

realizar múltiples autentificaciones con al menos un servidor de autentificación;

unir las múltiples autentificaciones a través del solo identificador único; y

obtener una única clave criptográfica, de al menos un servidor de autentificación, en el que dicha única clave criptográfica se genera basándose en una única de las múltiples autentificaciones, y en el que dicha única clave criptográfica se usa para todas las otras autentificaciones de las múltiples autentificaciones.

11. Un aparato para un servidor de autentificación, que comprende:

un procesador para obtener un solo identificador único para un igual, para realizar múltiples autentificaciones con el igual, para asociar el solo identificador único y al menos una clave criptográfica con el igual y para generar una única clave criptográfica basada en una única de las múltiples autentificaciones, y en el que dicha única clave criptográfica se usa para todas las demás autentificaciones de las múltiples autentificaciones; y

una memoria acoplada con el procesador.

12. Un procedimiento que comprende:

obtener un solo identificador único para un igual;

realizar múltiples autentificaciones con el igual;

asociar el solo identificador único y al menos una clave criptográfica con el igual; y

generar una única clave criptográfica basada en una única de las múltiples autentificaciones, y en la que dicha clave criptográfica única se utiliza para todas las demás autentificaciones de las múltiples autentificaciones.

13. Un medio legible por procesador que comprende instrucciones almacenadas en el mismo que, cuando son ejecutadas por un procesador, llevan a cabo los pasos de procedimiento de cualquiera de las reivindicaciones 10 o 12.

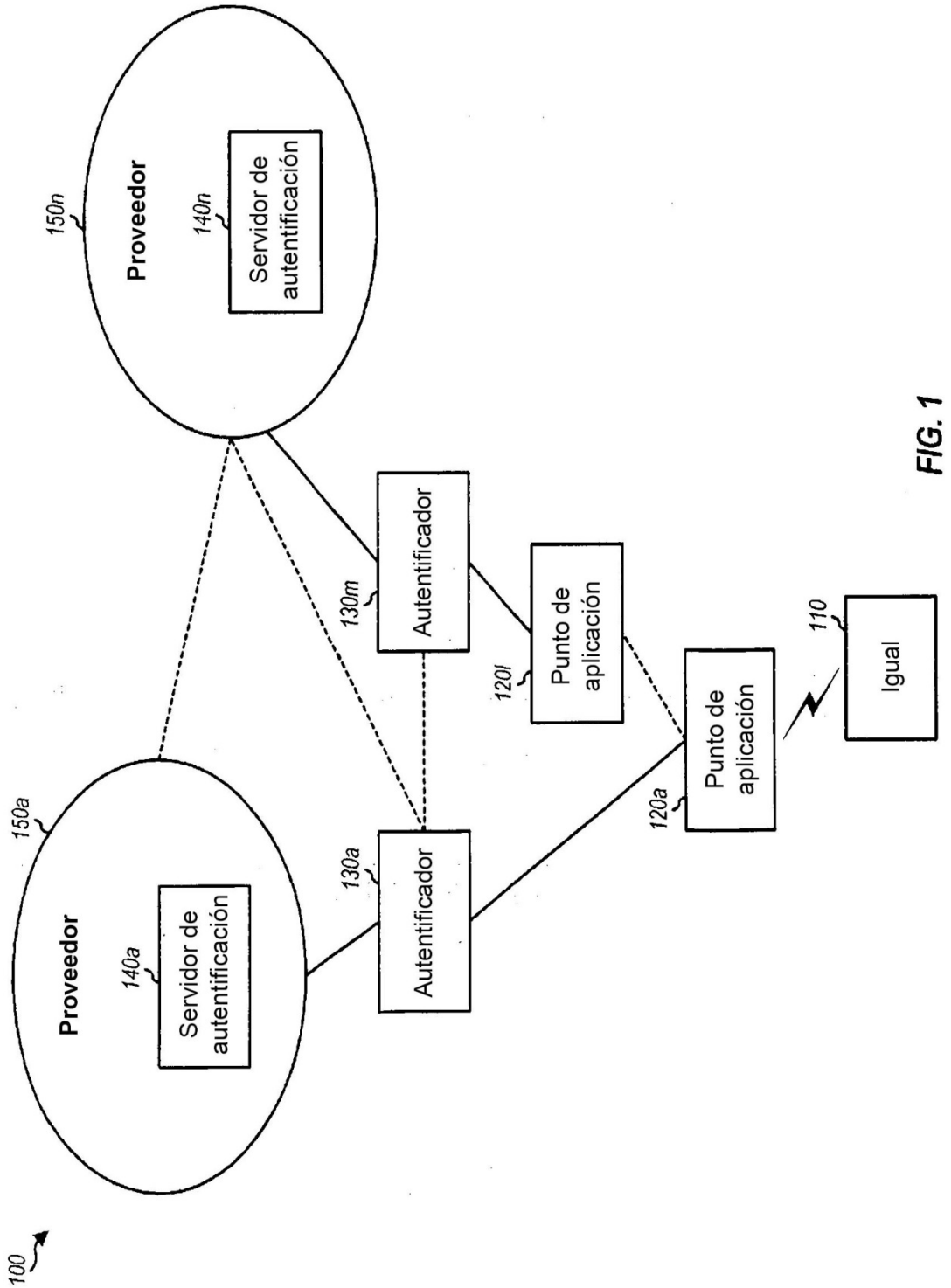
100
150a
Proveedor
140a
Servidor de autentificación
150n
Proveedor
140n
Servidor de autentificación
130a
Autentificador
130m
Autentificador
120a
Punto de aplicación
120l
Punto de aplicación
110
Igual

FIG. 1

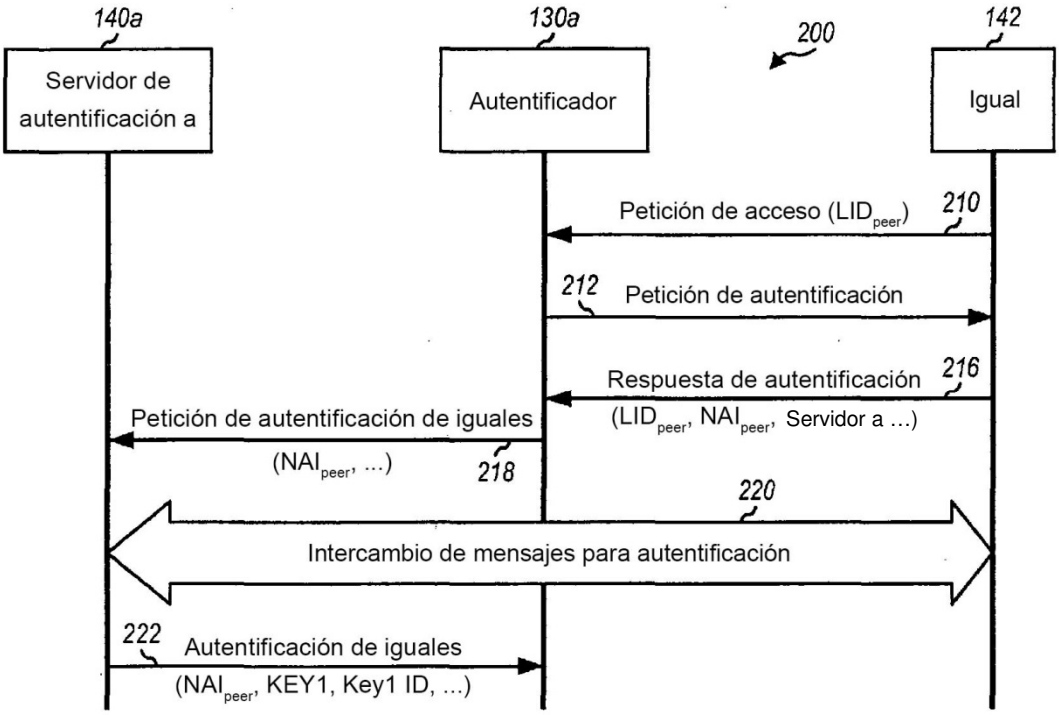
140a
Servidor de autentificación a
130a
Autentificador
200
142
Igual
Petición de acceso (LID$_{peer}$)
210
212
Petición de autentificación
Respuesta de autentificación
216
(LID$_{peer}$, NAI$_{peer}$, Servidor a ...)
Petición de autentificación de iguales
(NAI$_{peer}$, ...)
218
220
Intercambio de mensajes para autentificación
222
Autentificación de iguales
(NAI$_{peer}$, KEY1, Key1 ID, ...)

FIG. 2

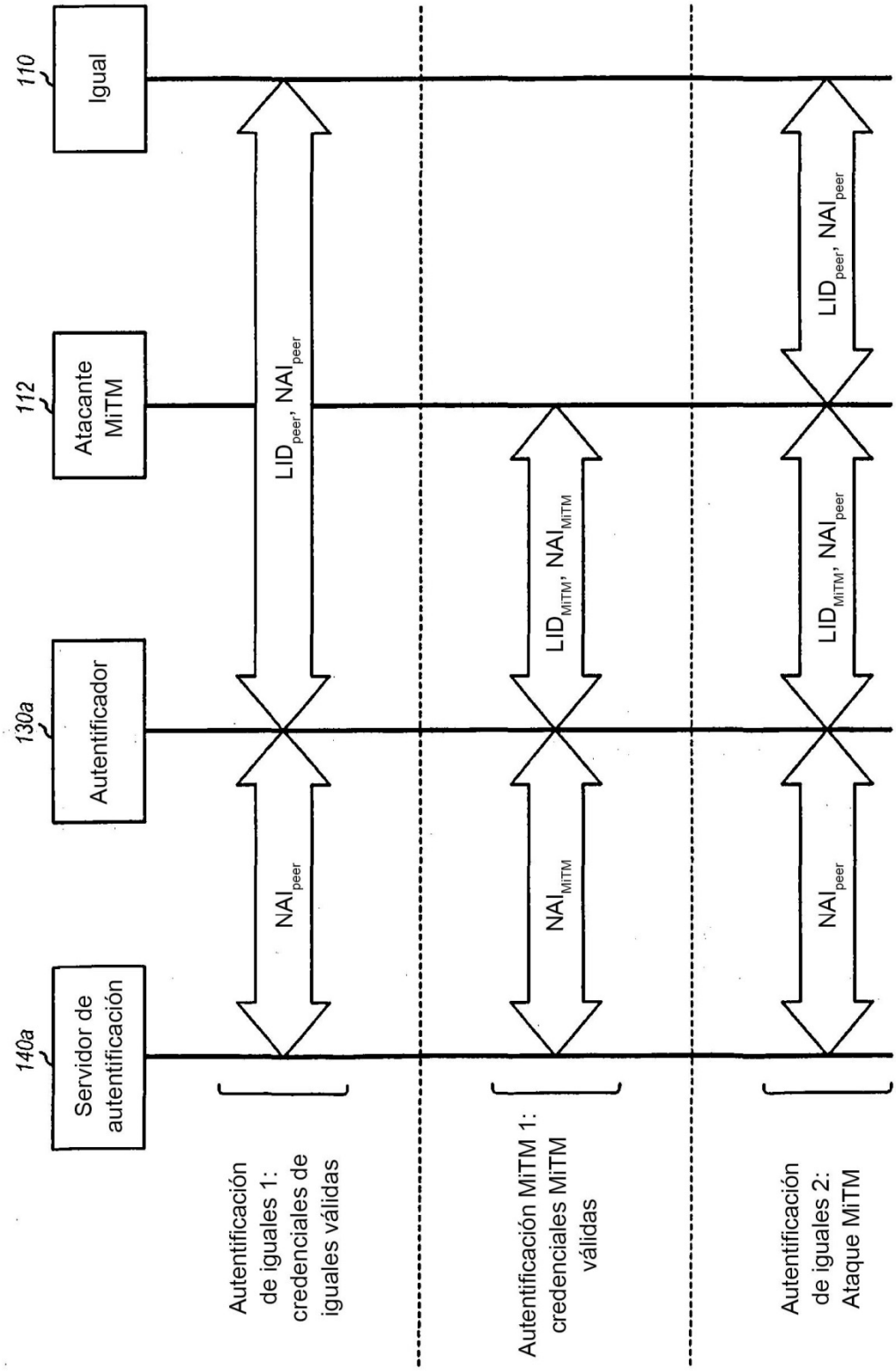
110
Igual
112
Atacante MiTM
130a
Autentificador
140a
Servidor de autentificación
LID_peer, NAI_peer
NAI_peer
LID_MiTM, NAI_MiTM
NAI_MiTM
LID_MiTM, NAI_peer
LID_peer, NAI_peer
NAI_peer
Autentificación de iguales 1: credenciales de iguales válidas
Autentificación MiTM 1: credenciales MiTM válidas
Autentificación de iguales 2: Ataque MiTM

FIG. 3

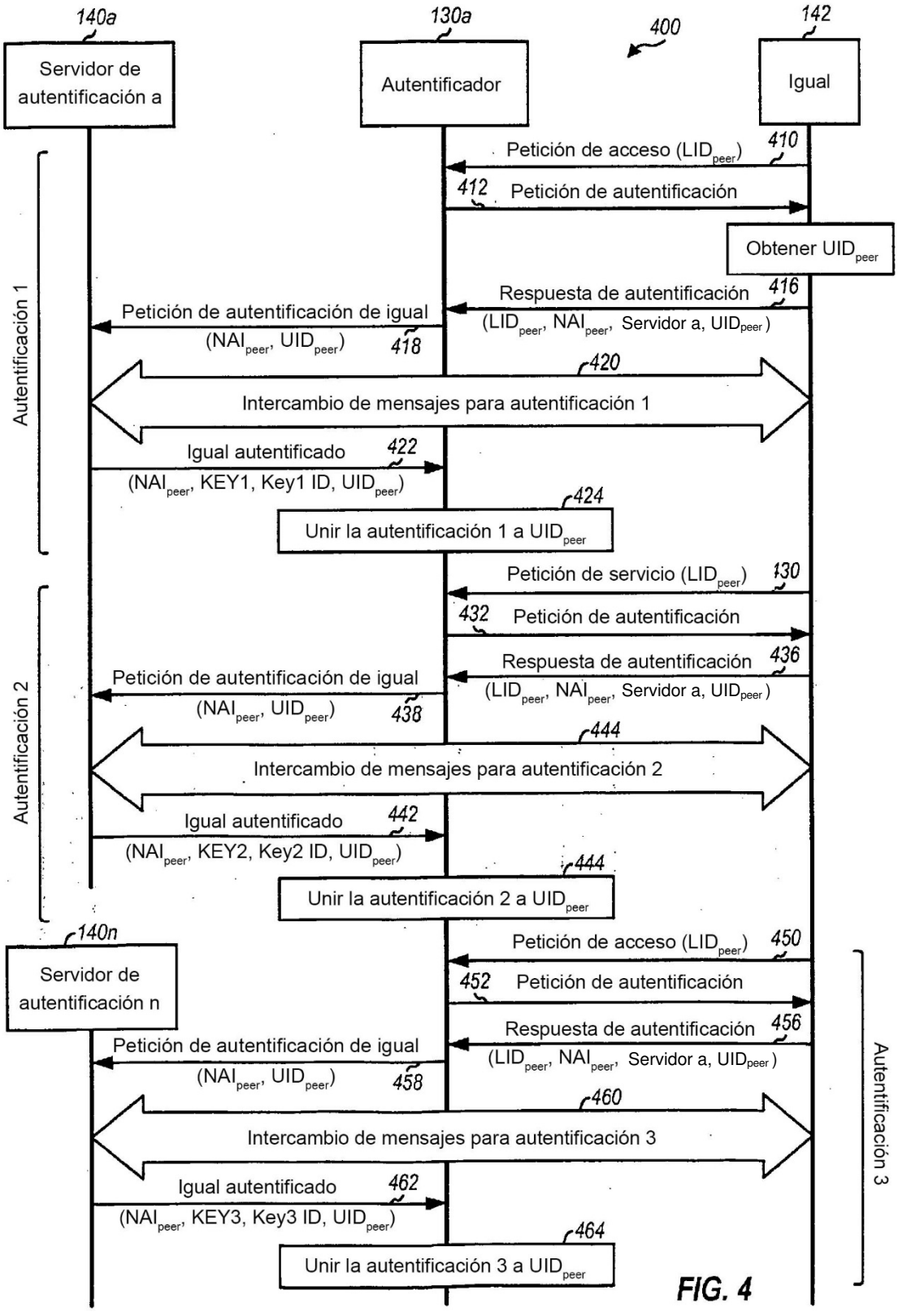
140a
Servidor de autentificación a
130a
Autentificador
400
142
Igual
Petición de acceso (LID_peer)
410
412
Petición de autentificación
Obtener UID_peer
Respuesta de autentificación
416
(LID_peer, NAI_peer, Servidor a, UID_peer)
Petición de autentificación de igual
(NAI_peer, UID_peer)
418
420
Intercambio de mensajes para autentificación 1
Igual autentificado
422
(NAI_peer, KEY1, Key1 ID, UID_peer)
424
Unir la autentificación 1 a UID_peer
Autentificación 1
Petición de servicio (LID_peer)
130
432
Petición de autentificación
Respuesta de autentificación
436
(LID_peer, NAI_peer, Servidor a, UID_peer)
Petición de autentificación de igual
(NAI_peer, UID_peer)
438
444
Intercambio de mensajes para autentificación 2
Igual autentificado
442
(NAI_peer, KEY2, Key2 ID, UID_peer)
444
Unir la autentificación 2 a UID_peer
Autentificación 2
140n
Servidor de autentificación n
Petición de acceso (LID_peer)
450
452
Petición de autentificación
Respuesta de autentificación
456
(LID_peer, NAI_peer, Servidor a, UID_peer)
Petición de autentificación de igual
(NAI_peer, UID_peer)
458
460
Intercambio de mensajes para autentificación 3
Igual autentificado
462
(NAI_peer, KEY3, Key3 ID, UID_peer)
464
Unir la autentificación 3 a UID_peer
Autentificación 3

FIG. 4

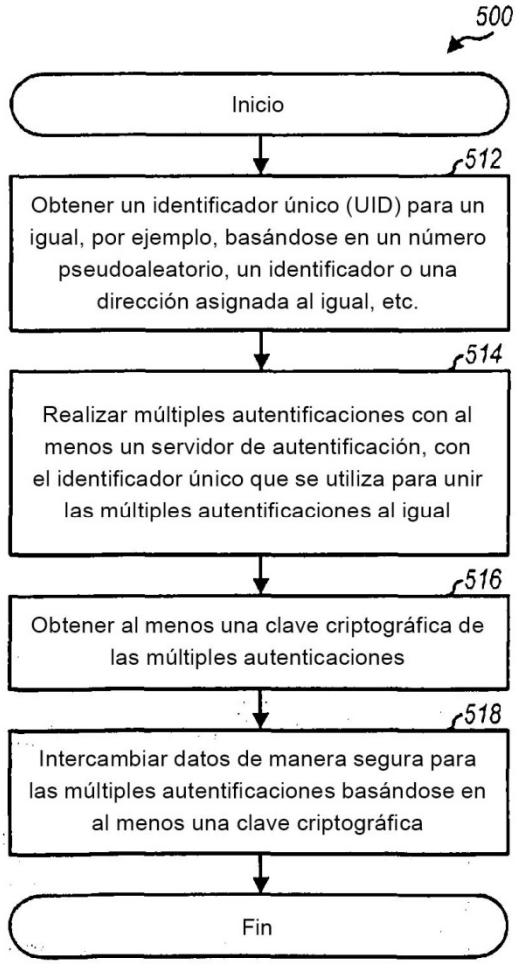
500
Inicio
512
Obtener un identificador único (UID) para un igual, por ejemplo, basándose en un número pseudoaleatorio, un identificador o una dirección asignada al igual, etc.
514
Realizar múltiples autentificaciones con al menos un servidor de autentificación, con el identificador único que se utiliza para unir las múltiples autentificaciones al igual
516
Obtener al menos una clave criptográfica de las múltiples autenticaciones
518
Intercambiar datos de manera segura para las múltiples autentificaciones basándose en al menos una clave criptográfica
Fin

FIG. 5

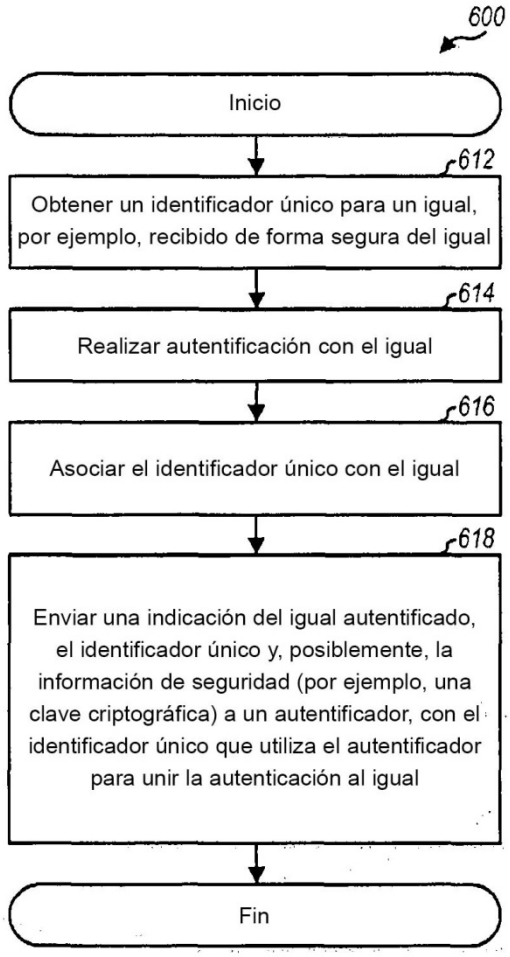
600
Inicio
612
Obtener un identificador único para un igual, por ejemplo, recibido de forma segura del igual
614
Realizar autentificación con el igual
616
Asociar el identificador único con el igual
618
Enviar una indicación del igual autentificado, el identificador único y, posiblemente, la información de seguridad (por ejemplo, una clave criptográfica) a un autentificador, con el identificador único que utiliza el autentificador para unir la autenticación al igual
Fin

FIG. 6

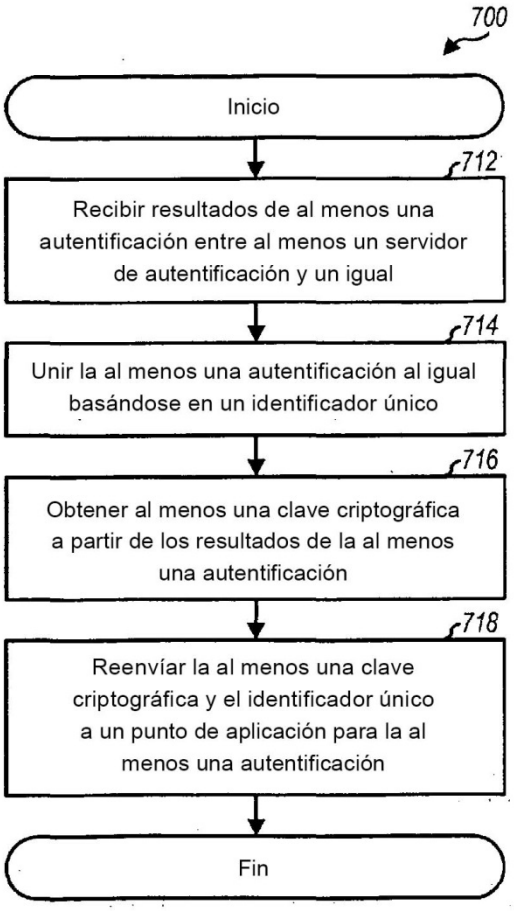

FIG. 7

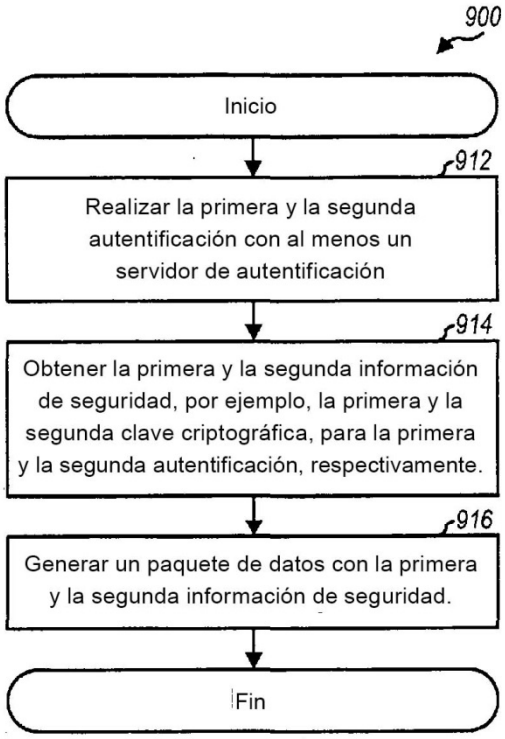

FIG. 9

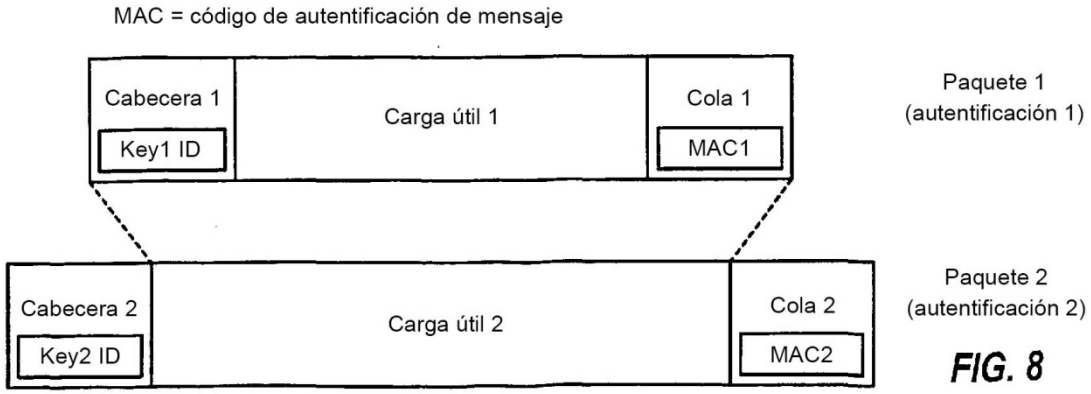

FIG. 8

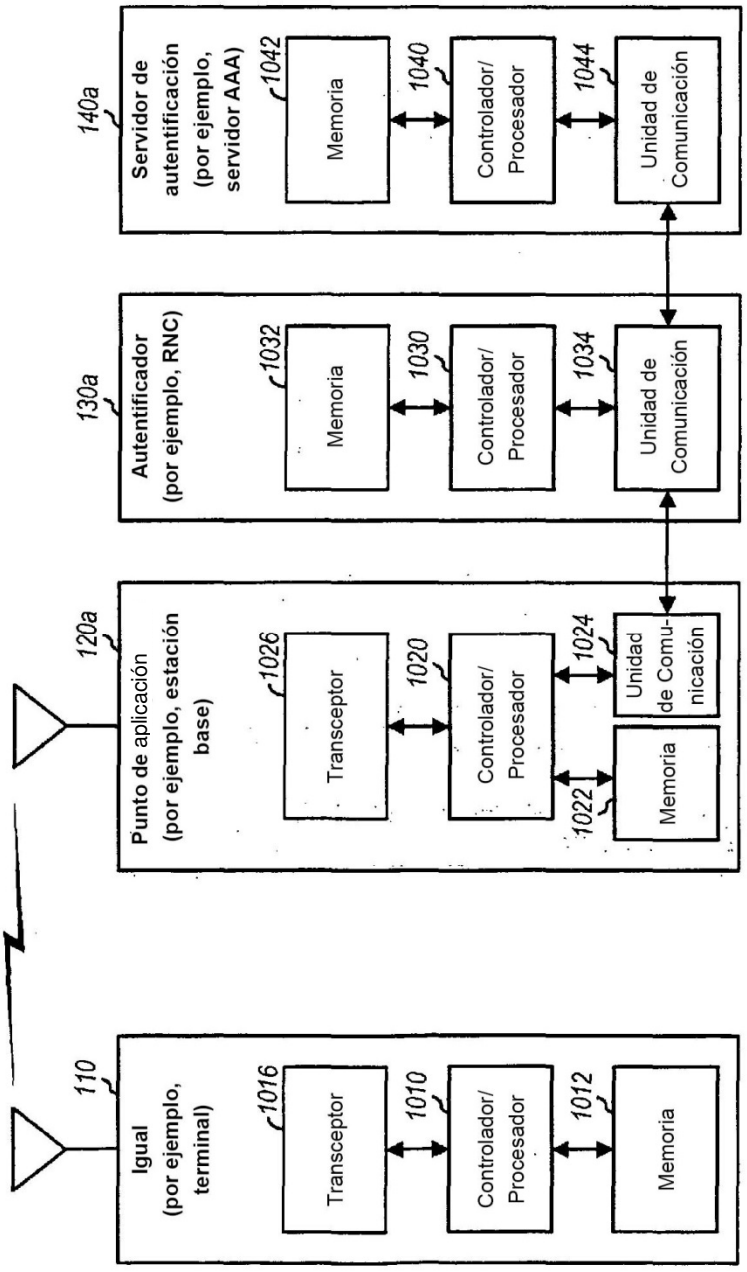
Igual (por ejemplo, terminal)
110
Transceptor
1016
Controlador/ Procesador
1010
Memoria
1012
Punto de aplicación (por ejemplo, estación base)
120a
Transceptor
1026
Controlador/ Procesador
1020
Memoria
1022
Unidad de Comu-nicación
1024
Autentificador (por ejemplo, RNC)
130a
Memoria
1032
Controlador/ Procesador
1030
Unidad de Comunicación
1034
Servidor de autentificación (por ejemplo, servidor AAA)
140a
Memoria
1042
Controlador/ Procesador
1040
Unidad de Comunicación
1044

FIG. 10