(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 864 074**

(51) Int. CI.:

H04W 12/06 (2011.01)
H04W 12/08 (2011.01)
H04L 29/06 (2006.01)
H04W 4/18 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.02.2011 PCT/FI2011/050092**

(87) Fecha y número de publicación internacional: **25.08.2011 WO11101533**

(96) Fecha de presentación y número de la solicitud europea: **03.02.2011 E 11744313 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.03.2021 EP 2537316**

(54) Título: **Procedimiento y aparato para proporcionar el intercambio de sesiones de autenticación**

(30) Prioridad:

18.02.2010 US 707941

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.10.2021

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

OTRANEN, JARI y
KARHINEN, ANSSI

(74) Agente/Representante:

ISERN JARA, Jorge

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y aparato para proporcionar el intercambio de sesiones de autenticación

Antecedentes

Los proveedores de servicios de red y los fabricantes de dispositivos se enfrentan continuamente al desafío de suministrar valor, conveniencia y seguridad a los consumidores, por ejemplo, al brindar servicios de red atractivos. Cabe señalar que el número y la variedad de aplicaciones que se proporcionan en los dispositivos de los usuarios crece continuamente. Por ejemplo, los dispositivos de usuario modernos pueden incluir varias aplicaciones (por ejemplo, navegadores, aplicaciones cliente, etc.) que permiten al usuario acceder a los servicios de red que se proporcionan por diferentes servidores de aplicaciones. La conveniencia y la seguridad del acceso a estos servidores son desafíos importantes a los que se enfrentan los proveedores de servicios todos los días. En consecuencia, en una realización, pueden usarse servidores de autenticación para proporcionar seguridad para que tales aplicaciones accedan a los servidores de aplicaciones. Tradicionalmente, la información de autenticación entre las aplicaciones del navegador y las diferentes aplicaciones cliente no se comparten, por lo tanto, los recursos de red pueden desecharse y la experiencia del usuario puede disminuirse cuando se repite un proceso de autenticación para diferentes aplicaciones a las que se accede desde el mismo dispositivo.

El documento US2008/0046983 se refiere a un sistema de inicio de sesión de servicios web multiusuario en el que se usa una interfaz de autenticación para proporcionar acceso a una pluralidad de aplicaciones cliente a información de usuario personalizada y datos de autenticación. La información de usuario y los datos de autenticación se refieren a una pluralidad de cuentas y/o usuarios de cuentas en un dispositivo cliente. El documento US2008/0046983 enseña que un estado de autenticación puede transferirse entre una primera aplicación cliente y una segunda aplicación cliente, por ejemplo, entre una aplicación de navegador web y una aplicación de mensajería instantánea.

El documento US7509672 se refiere al campo del intercambio de datos que se basa en autenticación y, más específicamente, con el intercambio de datos a través de un sistema informático que se distribuye en base a un inicio de sesión inicial (vea la columna 1, líneas 7 a 9). El documento US7509672 enseña un sistema en el que las aplicaciones que se alojan en diferentes máquinas que se ejecutan en diferentes plataformas puedan acceder a los datos que se almacenan en un registro de datos. El registro de datos puede almacenar información de autenticación tal como identificaciones de usuario y contraseñas a las que se puede acceder para permitir que un usuario inicie sesión automáticamente en las aplicaciones después de un inicio de sesión global inicial (vea la columna 2, línea 65 a la columna 3, línea 4).

Algunas realizaciones ilustrativas

La presente invención es la que se expone en las reivindicaciones independientes. Cualquiera de los ejemplos y las características que se describen en esta memoria descriptiva que no caen dentro del ámbito de las reivindicaciones independientes deben interpretarse como ejemplos útiles para comprender varias realizaciones de la invención.

Por lo tanto, existe la necesidad de un enfoque para proporcionar el intercambio de sesiones de autenticación entre diferentes aplicaciones (tales como, pero no se limitan a, navegadores y entornos de tiempo de ejecución).

De acuerdo con un ejemplo de la divulgación, un procedimiento comprende recibir, en una interfaz, un contexto de autenticación que se asocia con un primer servicio. El procedimiento comprende además, provocar, al menos en parte, el almacenamiento del contexto de autenticación en una primera memoria caché que se asocia con la interfaz. El procedimiento comprende además, provocar, al menos en parte, el llenado del contexto de autenticación en una segunda memoria caché. La segunda memoria caché se asocia con un segundo servicio y la segunda memoria caché no se enlaza directamente a la interfaz. El contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio.

De acuerdo con otro ejemplo de la divulgación, un aparato que comprende al menos un procesador, y al menos una memoria que incluye un código de programa informático, la al menos una memoria y el código de programa informático que se configura para, con el al menos un procesador, para provocar, al menos en parte, que el aparato reciba un contexto de autenticación que se asocia con un primer servicio. El aparato se provoca además, para provocar, al menos en parte, el almacenamiento del contexto de autenticación en una primera memoria caché que se asocia con el aparato. El aparato se provoca además, para provocar, al menos en parte, el llenado del contexto de autenticación en una segunda memoria caché. La segunda memoria caché se asocia con un segundo servicio y la segunda memoria caché no se enlaza directamente al aparato. El contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio.

De acuerdo con otro ejemplo de la divulgación, un medio de almacenamiento legible por ordenador que lleva una o más secuencias de una o más instrucciones que, cuando se ejecutan por uno o más procesadores, provocan, al menos en parte, que un aparato reciba un contexto de autenticación que se asocia con un primer servicio. El aparato se provoca además, para provocar, al menos en parte, el almacenamiento del contexto de autenticación en una

primera memoria caché que se asocia con el aparato. El aparato se provoca además, para provocar, al menos en parte, el llenado del contexto de autenticación en una segunda memoria caché. La segunda memoria caché se asocia con un segundo servicio y la segunda memoria caché no se enlaza directamente al aparato. El contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio.

De acuerdo con otro ejemplo de la divulgación, un aparato comprende medios para un contexto de autenticación que se asocia con un primer servicio. El aparato comprende además, medios para provocar, al menos en parte, el almacenamiento del contexto de autenticación en una primera memoria caché que se asocia con el aparato. El aparato comprende además, medios para provocar, al menos en parte, el llenado del contexto de autenticación para una segunda memoria caché. La segunda memoria caché se asocia con un segundo servicio y la segunda memoria caché no se enlaza directamente al aparato. El contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio.

Para varios ejemplos de la divulgación de la invención, se puede aplicar lo siguiente: Un procedimiento que comprende: facilitar un procedimiento de y/o proceso: (1) datos y/o (2) información y/o (3) al menos una señal; los (1) datos y/o (2) información y/o (3) al menos una señal que se basa al menos en parte en (o que se derivan al menos en parte de) cualquiera o cualquier combinación de procedimiento (o procesos) que se divulgan en la presente solicitud como relevante para cualquier realización de la invención.

Para varios ejemplos de la divulgación de la invención, se puede aplicar lo siguiente: Un procedimiento que comprende facilitar el acceso a al menos una interfaz que se configura para permitir el acceso a al menos un servicio, el al menos un servicio que se configura para realizar una o cualquier combinación de procedimiento (o procesos) de red o de proveedor de servicios que se divulga en la presente solicitud.

Para varios ejemplos de la divulgación de la invención, se puede aplicar lo siguiente: Un procedimiento que comprende facilitar la creación y/o facilitar la modificación: (1) al menos un elemento de interfaz de usuario de dispositivo y/o (2) al menos una funcionalidad de interfaz de usuario de dispositivo; el (1) al menos un elemento de interfaz de usuario del dispositivo y/o (2) al menos una funcionalidad de interfaz de usuario del dispositivo; que se basa, al menos en parte, en lo siguiente: datos y/o información resultante de una o cualquier combinación de procedimientos o procesos que se divulgan en la presente solicitud como relevante para cualquier realización de la invención y/o al menos una señal resultante de una o cualquier combinación de procedimiento (o procesos) que se divulgan en la presente solicitud como relevante para cualquier realización de la invención.

Para varios ejemplos de la divulgación de la invención, se puede aplicar lo siguiente: Un procedimiento que comprende crear y/o modificar: (1) al menos un elemento de interfaz de usuario de dispositivo y/o (2) al menos una funcionalidad de interfaz de usuario de dispositivo; el (1) al menos un elemento de interfaz de usuario del dispositivo y/o (2) al menos una funcionalidad de interfaz de usuario del dispositivo; el (1) al menos un elemento de interfaz de usuario del dispositivo y/o (2) al menos una funcionalidad de interfaz de usuario del dispositivo que se basa al menos en parte, en lo siguiente: datos y/o información resultante de una o cualquier combinación de procedimientos (o procesos) que se divulgan en la presente solicitud como relevante para cualquier realización de la invención y/o al menos una señal resultante de una o cualquier combinación de procedimiento (o procesos) que se divulgan en la presente solicitud como relevante para cualquier realización de la invención.

En varias realizaciones de ejemplo, los procedimientos (o procesos) pueden realizarse en el lado del proveedor de servicios o en el lado del dispositivo móvil o de cualquier forma que se compartan entre el proveedor de servicios y el dispositivo móvil con acciones que se realizan en ambos lados.

Aún otros aspectos, características y ventajas de la invención son fácilmente evidentes a partir de la siguiente descripción que se detalla, simplemente mediante la ilustración de un número de realizaciones e implementaciones particulares, que incluyen el mejor modo que se contempla para llevar a cabo la invención. La invención es capaz, además de otras y diferentes realizaciones, y sus diversos detalles, de poder modificarse en varios aspectos obvios. En consecuencia, los dibujos y la descripción deben considerarse de naturaleza ilustrativa y no restrictiva.

Breve descripción de las figuras

Las realizaciones de la invención se ilustran a modo de ejemplo y no a modo de limitación en las figuras de los dibujos que la acompañan:

La Figura 1 es un diagrama de un sistema capaz de proporcionar una plataforma para compartir información de sesión de autenticación, de acuerdo con una realización;

La Figura 2 es un diagrama de los componentes de un habilitador de dispositivo, de acuerdo con una realización;

La Figura 3 es un diagrama de flujo de un proceso para intercambiar información de sesión de autenticación, tal como contexto de autenticación, entre diferentes aplicaciones, de acuerdo con una realización;

Las Figuras 4A y 4B son diagramas de secuencia de tiempo que ilustran una secuencia de mensajes y procesos para proporcionar una plataforma para compartir información de sesión de autenticación, de acuerdo con varias realizaciones;

La Figura 5 es un diagrama de un ejemplo de una interfaz de usuario para proporcionar datos que se refieren a las credenciales de autenticación, de acuerdo con una realización;

La Figura 6 es un diagrama de hardware que puede usarse para implementar una realización de la invención;

La Figura 7 es un diagrama de un conjunto de chips que pueden usarse para implementar una realización de la invención; y

La Figura 8 es un diagrama de un terminal móvil (por ejemplo, un teléfono) que puede usarse para implementar una realización de la invención.

Descripción de algunas realizaciones

Se divulgan ejemplos de un procedimiento, aparato y programa informático para proporcionar un intercambio de sesiones de autenticación entre navegadores y entornos de tiempo de ejecución. En la siguiente descripción, para los propósitos de la explicación, se exponen numerosos detalles específicos con el fin de proporcionar un entendimiento completo de las realizaciones de la invención. Sin embargo, es evidente para un experto en la técnica que las realizaciones de la invención se pueden poner en práctica sin estos detalles específicos o con una disposición equivalente. En otros casos, se muestran estructuras y dispositivos bien conocidos, en forma de diagrama de bloques con el fin de evitar oscurecer innecesariamente las realizaciones de la invención.

Como se usa en la presente memoria, el término *recurso de red* se refiere a cualquier servicio o estructura de datos o enlace de comunicación disponible a través de la conexión a una red. Un proceso de *inicio de sesión única* (SSO) se refiere a cualquier proceso de un solo proveedor, que permite a un usuario, durante una sesión que se conecta a la red, acceder a una pluralidad de recursos de red de ese proveedor sin entrada redundante por parte del usuario de información de autenticación o identificación del usuario. Un solo proveedor a menudo se identifica por un solo nombre de dominio de red en el sistema de nombres de identificación de recursos uniforme (URI), como se usa, por ejemplo, con un sistema de nombres de localizador de recursos uniforme (URL). Sin embargo, se contempla además, que el proceso SSO puede extenderse a los servicios que son proporcionados en múltiples dominios de red. Un ejemplo de proceso de inicio de sesión única son los procesos de inicio de sesión única para el sistema OVI™ de NOKIA CORPORATION™ de Espoo, Finlandia. Un *proveedor de acceso* es un proveedor de servicios de red que otorga acceso al equipo de usuario (por ejemplo, UE 101, que se describe más abajo) para acceder a una red (por ejemplo, la red de comunicación 105, que se describe más abajo).

La Figura 1 es un diagrama de un sistema capaz de proporcionar un intercambio de sesiones de autenticación, de acuerdo con una realización. Las aplicaciones (tales como, pero no se limitan a, las aplicaciones que se ejecutan en entornos de tiempo de ejecución (por ejemplo, Java runtime, Web runtime, etc.), navegadores, etc.) se pueden ejecutar en los dispositivos del usuario para permitir el acceso a los servicios que se proporcionan por los servidores de aplicaciones. Como se señaló anteriormente, el número y la variedad de estas aplicaciones cliente aumentan continuamente; y la seguridad y la conveniencia del acceso a los servidores de aplicaciones a través de las aplicaciones cliente son desafíos importantes que enfrentan los proveedores de servicios. Tradicionalmente, para que cada aplicación cliente (por ejemplo, un navegador o aplicación cliente) acceda a un servidor de aplicaciones, la aplicación cliente (y/o un usuario de la aplicación cliente) necesita autenticarse en un servidor de autenticación para recibir un contexto de autenticación. El contexto de autenticación se usa además, por la aplicación cliente para acceder a la aplicación del servidor. Sin embargo, este contexto de autenticación no se comparte tradicionalmente entre diferentes tipos de aplicaciones cliente. Por lo tanto, cada tipo de aplicación cliente realiza su propio proceso de autenticación para acceder a los servidores de aplicaciones, por ejemplo, incluso cuando accede a los mismos servidores o cuando los servidores de aplicaciones proporcionan servicios que se relacionan. Esto puede desperdiciar recursos de red al provocar cargas de tráfico potencialmente altas en los servidores de aplicaciones y servidores de autenticación participantes, lo que disminuye la experiencia del usuario. Por ejemplo, un contexto de autenticación históricamente no se comparte entre una aplicación que se ejecuta en un entorno de tiempo de ejecución y una aplicación cliente tal como un navegador. Por lo tanto, incluso si una aplicación cliente en tiempo de ejecución se ha autenticado y existe un contexto de autenticación, cuando un usuario usa un navegador para acceder al mismo servidor de aplicaciones o al servidor que se relaciona (tal como un servidor web), el usuario y/o el navegador realiza otro proceso de autenticación para obtener un contexto de autenticación específico para el navegador. Esta autenticación que se repite puede resultar en cargas de tráfico potencialmente altas en el servidor de autenticación participante.

Para abordar estos problemas, un sistema 100 de la Figura 1 puede proporcionar ventajosamente una plataforma para compartir información de sesión de autenticación, tal como el contexto de autenticación, entre diferentes aplicaciones, tal como aplicaciones cliente que se ejecutan en entornos de tiempo de ejecución y aplicaciones cliente como navegadores. Como se usa en la presente memoria, el término "contexto de autenticación" puede

incluir: (1) información respecto a los mecanismos de identificación inicial de un usuario, cliente, consumidor, etc.; (2) información respecto al mecanismo o procedimiento de autenticación (por ejemplo, contraseñas, contraseña de un solo uso, una cookie, una clave de uso limitado, una clave secreta, una clave de consumidor, un token de acceso, etc.); (3) información respecto al almacenamiento y la protección de credenciales (por ejemplo, reglas de contraseñas, carritos inteligentes, etc.); y similares.

De acuerdo con una realización de la Figura 1, un equipo de usuario (UE) 101 puede comunicarse con múltiples recursos de red, que incluye los servidores de aplicaciones 103a-130n (que se referencian colectivamente de ahora en adelante como servidores de aplicaciones 103), a través de, por ejemplo, la red de comunicación 105. En un ejemplo, el servidor de autenticación 107 puede usarse para identificar, autenticar y/o verificar el UE 101, un usuario del UE 101, aplicaciones cliente, navegadores, etc., que se asocian con el UE 101, para acceder a los servidores de aplicaciones 103. El UE 101 puede incluir una interfaz, tal como el habilitador de dispositivos (DE) 109, que puede proporcionar una plataforma para compartir información de sesión de autenticación, tal como el contexto de autenticación, entre, por ejemplo, aplicaciones cliente 111a-111m (que se referencian colectivamente de ahora en adelante como aplicaciones cliente 111) y el navegador 113. De acuerdo con una realización, cuando una de las aplicaciones cliente 111 se autentica con el servidor de autenticación 107 a través del DE 109, se puede recibir un contexto de autenticación, por ejemplo, en el DE 109 y el contexto de autenticación se puede almacenar en memoria caché y/o almacenar en, por ejemplo, una memoria caché y/o una base de datos de autenticación 117 que se asocia con el DE 109. El DE 109 puede provocar ventajosamente el llenado del contexto de autenticación desde, por ejemplo, la memoria caché y/o la base de datos de autenticación 117 que se asocia con el DE 109 a otra memoria caché y/o base de datos, tal como la base de datos 115, que no se enlaza directamente al DE 109. De acuerdo con una realización, este procedimiento puede ser un procedimiento de empuje en el que el contexto de autenticación de la base de datos de autenticación 117 se transmite o provoca que se transmita a la base de datos 115 sin una solicitud específica de la base de datos 115 o aplicación que se asocia con la base de datos 115 (por ejemplo, el navegador 113). En este ejemplo, el navegador 113 puede usar el contexto de autenticación rellenado de la memoria caché y/o la base de datos 115 para acceder a los servidores de aplicaciones 103 sin necesidad de autenticación adicional.

De acuerdo con determinadas realizaciones, una de las aplicaciones cliente 111, por ejemplo, la aplicación cliente 111a, desea acceder a los servidores de aplicaciones 103. Una interfaz, tal como el módulo DE 109, que puede implementarse como un conjunto de chips como se muestra en la Figura 7 y que se describen más abajo, con o sin una o más instrucciones del programa informático, pueden recibir una solicitud de autenticación de la aplicación cliente 111a. La solicitud de autenticación puede usarse para autenticar la aplicación cliente 111a, un usuario de la aplicación cliente 111a o una combinación de los mismos. En un ejemplo, el DE 109 determina si la aplicación cliente 111a, un usuario de la aplicación cliente 111a, o una combinación de las mismas, ya se ha autenticado para acceder al servidor de aplicaciones 103 que se solicita en una sesión actual a través de la red de comunicación 105. Si el DE 109 determina que es necesaria una autenticación (por ejemplo, si el usuario aún no se ha autenticado), se genera una interfaz de usuario (UI) y se solicita a un usuario de la aplicación cliente 111a las entradas que se emplean para identificar y autenticar al usuario. En una realización, la determinación de que una autenticación es necesaria puede basarse en la falta de un contexto de autenticación para la aplicación cliente 111a y/o un usuario de la aplicación cliente 111a, un contexto de autenticación desactualizado, etc. En un ejemplo, el DE 109 puede iniciar la interfaz de usuario para solicitar al usuario la autenticación de usuario y/o las entradas de identificación. Alternativa o adicionalmente, el servidor de autenticación 107 puede iniciar la UI.

La entrada de usuario, que puede incluir, pero no se limita a, credenciales de usuario, que se reciben por la interfaz DE 109. Las credenciales de usuario pueden incluir nombre de usuario, contraseña, datos biométricos, contraseña de un solo uso, filtrado de direcciones de red, etc. Sin embargo, se contempla que se puedan usar otros esquemas de autenticación y/o identificación. El DE 109 genera una solicitud de autenticación para la aplicación cliente 111a y/o un usuario de la aplicación cliente 111a y transmite la solicitud de autenticación al servidor de autenticación 107. El servidor de autenticación 107 determina si la aplicación cliente 111a y/o un usuario de la aplicación cliente 111a puede autenticarse basándose, al menos en parte, en las entradas del usuario, tales como las credenciales de usuario. Si la autenticación falla, el servidor de autenticación 107 informa al DE 109 de la autenticación fallida y el DE 109 devuelve el resultado de la autenticación a la aplicación cliente 111a. Sin embargo, si la autenticación es exitosa (por ejemplo, las credenciales de usuario son válidas), el servidor de autenticación 107 genera y devuelve un contexto de autenticación válido al DE 109. En un ejemplo, el éxito de la autenticación se determina por el servidor de autenticación 107 al comparar las credenciales de usuario que se reciben con las credenciales de usuario que se almacenan en una base de datos (que no se muestra) que se asocia con el servidor de autenticación 107. Sin embargo, se contempla que se pueden usar otros esquemas y protocolos de autenticación para autenticar las aplicaciones cliente 111 y/o el (los) usuario (s) de las aplicaciones cliente.

Cuando el DE 109 recibe el contexto de autenticación válido, en caso de una autenticación exitosa, el DE 109 informa a la aplicación cliente 111a que la autenticación ha sido exitosa. Además, el DE 109 puede almacenar en memoria caché y/o almacenar el contexto de autenticación que se recibe en una memoria caché y/o base de datos, tal como la base de datos de autenticación 117 que se asocia con el DE 109. Por lo tanto, si otras aplicaciones cliente que ese asocian con el DE 109 (tales como las aplicaciones cliente 111) solicitan autenticación del DE 109, el

DE 109 puede verificar la existencia y validez del contexto de autenticación que se almacena y enviar una respuesta de autenticación a la aplicación cliente solicitante sin contactar además, con el servidor de autenticación 107.

Además, el DE 109 puede provocar ventajosamente el llenado del contexto de autenticación que se almacena en memoria caché y/o se almacena en la base de datos de autenticación 117 en otra memoria caché y/o base de datos, que no se enlaza directamente con y/o que utiliza el DE 109 (tal como la base de datos 115). En un ejemplo, este llenado del contexto de autenticación proporciona la plataforma para compartir información de sesión de autenticación entre aplicaciones que utilizan el DE 109 y aplicaciones que no usan el DE 109 (tal como el navegador 113). Por lo tanto, si el navegador 113 desea acceder al servidor de aplicaciones 103, el navegador 113 puede utilizar el contexto de autenticación rellenado en, por ejemplo, la base de datos 115 para autenticarse (y/o su usuario) en los servidores de aplicaciones 103. A modo de ejemplo, la base de datos 115 puede ser un almacén de cookies que se puede acceder por el navegador 113. De esta manera, el navegador 113 no necesita realizar una autenticación adicional porque el contexto de autenticación ya estaría disponible en el almacén de cookies (por ejemplo, la base de datos 115). Por otra parte, el navegador 113 (u otra aplicación cliente similar) no necesita ser consciente de la transferencia o llenado del contexto de autenticación desde el DE 109. En cambio, el navegador 113 solo necesita comprobar la presencia del contexto de autenticación en el almacén de cookies o memoria caché donde normalmente almacena tales contextos de autenticación.

En un ejemplo, rellenar el contexto de autenticación entre las bases de datos 115 y 117 puede incluir copiar el contexto de autenticación de la base de datos de autenticación 117 a la base de datos 115. Adicional o alternativamente, rellenar el contexto de autenticación puede incluir convertir el contexto de autenticación que se recibe para la aplicación cliente 111a en otro contexto de autenticación que se basa, al menos en parte, en un protocolo de autenticación que se asocia con, por ejemplo, el navegador 113 y el almacenamiento en memoria caché y/o almacenamiento el contexto de autenticación que se convierte en la memoria caché y/o la base de datos 115. En un ejemplo, el contexto de autenticación que se recibe para la aplicación cliente 111a puede incluir un token y rellenar el contexto de autenticación en la memoria caché y/o la base de datos 115 puede incluir convertir el contexto de autenticación en una cookie cifrada que se asocia al navegador 113. Una cookie (por ejemplo, una cookie de navegador o una cookie de Protocolo de Transporte de Hipertexto (HTTP)) es generalmente una pequeña porción de texto que se almacena en el dispositivo de un usuario por, por ejemplo, un navegador web u otra aplicación. Una cookie consta de uno o más pares de nombre-valor que contienen bits limitados de información, tales como las preferencias del usuario, el contenido del carrito de compras, un identificador para una sesión basada en servidor u otros datos que se usan por los sitios web y los servidores de aplicaciones 103.

En una realización, las aplicaciones cliente 111 pueden incluir aplicaciones que se ejecutan en entornos de tiempo de ejecución, tales como Java Runtime, Web Runtime (WRT), etc. Además, aunque se explican varias realizaciones con respecto al navegador 113 como una aplicación cliente que no se enlaza directamente al DE 109, se contempla que se puedan usar otras aplicaciones cliente que no utilicen directamente el DE 109 (por ejemplo, otras aplicaciones cliente nativas).

Además, a modo de ejemplo, el servidor de autenticación 107 puede incluir un servidor de autenticación de inicio único de sesión (SSO). El inicio de sesión única es un proceso de autenticación que permite a un usuario (por ejemplo, un dispositivo de usuario, una aplicación cliente, un usuario de un dispositivo de usuario, etc.) autenticarse una vez y obtener acceso a recursos de múltiples softwares, aplicaciones, servidores, etc., sin que se le solicite que vuelva a autenticarse en cada uno de los recursos. Por lo tanto, cuando una aplicación cliente (como una de las aplicaciones cliente 111 y/o el navegador 113) y/o un usuario de la aplicación cliente se autentica con el servidor de autenticación 107, por ejemplo, como se discutió anteriormente, para acceder a uno de los servidores de aplicaciones 103, la aplicación cliente (y/o el usuario) puede acceder a otros servidores de aplicaciones (que son compatibles con el esquema de inicio de sesión única) durante una sesión que se conecta a la red, sin entrada redundante por, por ejemplo, el usuario de la información de autenticación o identificación del usuario. De acuerdo con este ejemplo, la interfaz DE 109 se puede implementar como un habilitador de autenticación SSO para compartir ventajosamente información de sesión de autenticación entre diferentes aplicaciones cliente (por ejemplo, aplicaciones cliente 111 y/o navegador 113) del UE 101.

Como se discutió anteriormente, cuando la interfaz DE 109 recibe una solicitud de autenticación de una de las aplicaciones cliente 111, tal como la aplicación cliente 111b, la DE 109 determina si ya se ha realizado un proceso de autenticación para las aplicaciones cliente 111. Por ejemplo, el DE 109 determina si el contexto de autenticación ya existe, no ha expirado o es válido de otro modo para la autenticación de otras aplicaciones cliente 111. Si el DE 109 determina que el proceso de autenticación ya se ha realizado, el DE 109 informa a la aplicación cliente 111b del resultado del proceso de autenticación. Por ejemplo, el DE 109 genera e inicia la transmisión de un mensaje a la aplicación cliente 111b para informar a la aplicación cliente 111b de un intento de autenticación exitoso o fallido. Si el DE 109 determina que el contexto de autenticación existe (y, por ejemplo, no está desactualizado), el contexto de autenticación se recupera de, por ejemplo, la memoria caché y/o la base de datos de autenticación 117 y se devuelve a la aplicación cliente 111b. Por lo tanto, la interfaz DE 109 implementa la funcionalidad de inicio de sesión única al almacenar en memoria caché y/o al almacenar el contexto de autenticación y recuperándolo para las aplicaciones cliente solicitantes. La aplicación cliente 111b puede usar el contexto de autenticación recuperada para conectarse, por ejemplo, al servidor de aplicaciones 103a. En un ejemplo, la solicitud de conexión de la aplicación

cliente 111b al servidor de aplicaciones 103a puede incluir el contexto de autenticación recuperada. El servidor de aplicaciones 103a puede utilizar el servidor de autenticación 107 para verificar el contexto de autenticación y permitir el acceso de la aplicación cliente 111b si se verifica el contexto de autenticación. En una realización, la verificación del contexto de autenticación puede incluir un mensaje de verificación (que por ejemplo incluye el contexto de autenticación) desde el servidor de aplicaciones 103a al servidor de autenticación 107, la verificación del contexto de autenticación en el servidor de autenticación 107 (por ejemplo, por comparar el contexto de autenticación que se recibe con los contextos de autenticación que se almacenan), y un mensaje de verificación del servidor de autenticación 107 al servidor de aplicaciones 103a que indica el resultado de la verificación.

En una realización, después de que se haya autenticado una aplicación cliente 111 (por ejemplo, al recibir un contexto de autenticación válido), el contexto de autenticación que se recibe se puede almacenar en memoria caché, por ejemplo, en la base de datos 117 que tiene un enlace directo al DE 109. El DE 109 puede entonces rellenar el contexto de autenticación en la base de datos 115 que se puede acceder directamente por el navegador 113. Este llenado del contexto de autenticación desde la base de datos 117 a la base de datos 115 permite ventajosamente que el DE 109 comparta un contexto de autenticación (por ejemplo, un contexto de autenticación SSO) con otra aplicación, tal como el navegador 113, que de otro modo no tendría un enlace directo con el contexto de autenticación a través del DE 109. De esta manera, el sistema 100 reduce ventajosamente además, el uso de recursos informáticos, recursos de red (por ejemplo, ancho de banda), recursos de potencia, etc. del UE 101 y/o la red de comunicación 105 al permitir compartir un contexto de autenticación entre diferentes aplicaciones cliente 111 para acceder previamente a servidores autenticados (por ejemplo, los servidores de aplicaciones 103).

Por ejemplo, el navegador 113 puede desear acceder a uno o más de los servidores de aplicaciones 103 (por ejemplo, el servidor de aplicaciones 103a). En este ejemplo, el navegador 113 genera e inicia la transmisión de una solicitud de acceso al servidor de aplicaciones 103a. Dado que las aplicaciones cliente 111 se han autenticado, un contexto de autenticación se ha recibido y se almacena en memoria caché y/o se almacena, y existe un contexto de autenticación rellenado para el navegador 113 en, por ejemplo, memoria caché y/o base de datos 115, la solicitud de acceso puede incluir el contexto de autenticación rellenado. Por lo tanto, la información de sesión de autenticación se puede compartir entre diferentes aplicaciones cliente y no es necesaria ninguna entrada adicional de, por ejemplo, credenciales de usuario para una autenticación adicional. Como se mencionó, el contexto de autenticación rellenado puede ser una copia del contexto de autenticación, una versión que se convierte del contexto de autenticación, etc.

A modo de ejemplo, el servidor de aplicaciones 103a que recibe la solicitud de acceso, puede generar e iniciar además, la transmisión de una solicitud de verificación para verificar el contexto de autenticación rellenado que se recibe. La solicitud de verificación se envía al servidor de autenticación 107. El servidor de autenticación 107 verifica la validez del contexto de autenticación, por ejemplo, comparándolo con el contexto de autenticación que se almacena. El servidor de autenticación 107 genera e inicia la transmisión de una respuesta de verificación que se basa, al menos en parte, en la verificación del contexto de autenticación rellenado. Si el contexto de autenticación es válido, se concede la solicitud de acceso.

De acuerdo con ciertas realizaciones, el DE 109 puede además, determinar si un contexto de autenticación se almacena o dispone de otro modo en una memoria caché y/o base de datos (tal como la base de datos 115) que se asocia con el navegador 113. Si la autenticación se dispone en la base de datos 115, el DE 109 puede recuperar el contexto de autenticación para rellenar el contexto de autenticación en la memoria caché y/o la base de datos (tal como la base de datos de autenticación 117) que se asocia con las aplicaciones cliente 111. En una realización, este proceso puede denominarse procedimiento de extracción para rellenar el contexto de autenticación en la base de datos 117.

En otro ejemplo, el navegador 113 puede desear acceder a uno o más de los servidores de aplicaciones 103 (por ejemplo, el servidor de aplicaciones 103a). Si el navegador 113, un usuario del navegador 113, el UE 101, un usuario de UE 101, o una combinación de los mismos, aún no se ha autenticado para acceder al servidor de aplicaciones 103a (por ejemplo, no se almacena ningún contexto de autenticación válido en la base de datos 115 que se asocia con el navegador 113), el navegador 113 puede dirigirse al servidor de autenticación 107 para la autenticación. En una realización, el navegador 113 recibe una solicitud de credenciales de usuario, por ejemplo, desde el servidor de autenticación 107 y, en respuesta, envía las credenciales de usuario al servidor de autenticación 107. En este ejemplo, el servidor de autenticación 107 puede determinar la validez de las credenciales de usuario mediante, por ejemplo, una comparación de las credenciales que se presentan con las credenciales que se almacenan. Se contempla que se pueda implementar cualquier otro mecanismo de autenticación para asegurar que solo los usuarios que se autorizan puedan acceder a los servidores de aplicaciones 103. Si el navegador 113, un usuario del navegador 113, el UE 101, un usuario de UE 101, o una combinación de los mismos se autentica, el servidor de autenticación 107 puede generar y transmitir un contexto de autenticación al navegador 113. El navegador 113 puede entonces almacenar el contexto de autenticación que se recibe en la base de datos 115 del navegador 113. Otras solicitudes de acceso a los servidores de aplicaciones 103 por el navegador 113 pueden autenticarse al usar el contexto de autenticación que se almacena en memoria caché.

En ciertas realizaciones, el DE 109 puede rellenar además, el contexto de autenticación que se almacena en la base de datos 115 que se puede acceder directamente por el navegador 113 a una memoria caché y/o base de datos (por ejemplo, base de datos 117) que se asocia con las aplicaciones cliente 111. En una realización, el DE 109 puede determinar que un contexto de autenticación que se asocia al navegador 113 está disponible y puede rellenar el contexto de autenticación en la base de datos de autenticación 117 para que se use por las aplicaciones cliente 111. Más específicamente, la autenticación del navegador 113, un usuario del navegador 113, el UE 101, un usuario del UE 101, o una combinación de los mismos puede ser a través del DE 109, por lo tanto, el DE 109 puede determinar la existencia del contexto de autenticación para el navegador 113. Este llenado del contexto de autenticación desde la base de datos 115 a la base de datos 117 permite ventajosamente que el DE 109 comparta un contexto de autenticación (por ejemplo, un contexto de autenticación SSO) con otras aplicaciones tales como las aplicaciones cliente 111 que de otro modo no tendrían un enlace directo a la base de datos 115.

Como se discutió, en un ejemplo, rellenar el contexto de autenticación entre las bases de datos 115 y 117 puede incluir copiar el contexto de autenticación de la base de datos de autenticación 115 a la base de datos 117. Adicional o alternativamente, rellenar el contexto de autenticación puede incluir convertir el contexto de autenticación que se recibe por el navegador 113 a otro contexto de autenticación que se basa, al menos en parte, en un protocolo de autenticación que se asocia con, por ejemplo, las aplicaciones cliente 111 y el almacenamiento en memoria caché y/o almacenamiento el contexto de autenticación que se convierte en la memoria caché de autenticación y/o la base de datos 117. En una realización, el contexto de autenticación que se generó para el navegador 113 puede ser un contexto de autenticación que se basa en cookies (por ejemplo, pero no se limita a, una cookie cifrada). En un ejemplo, rellenar el contexto de autenticación de la base de datos 115 a la base de datos de autenticación 117 puede incluir convertir el contexto de autenticación que se basa en cookies en un contexto de autenticación que se basa en token.

Como se discutió anteriormente, implementar una plataforma para compartir el contexto de autenticación entre, por ejemplo, las aplicaciones cliente 111 y el navegador 113 puede reducir ventajosamente la carga de comunicación en el servidor de autenticación 107 al reducir el número de solicitudes de autenticación que se generan por las aplicaciones cliente 111 y el navegador 113 que se destina al servidor de autenticación 107.

A modo de ejemplo, la red de comunicación 105 del sistema 100 incluye una o más redes tales como una red de datos (que no se muestra), una red inalámbrica (que no se muestra), una red de telefonía (que no se muestra) o cualquier combinación de las mismas. Se contempla que la red de datos puede ser cualquier red de área local (LAN), red de área metropolitana (MAN), red de área amplia (WAN), una red de datos pública (por ejemplo, Internet), red inalámbrica de corto alcance o cualquier otra red de conmutación de paquetes adecuada, tal como una red de conmutación de paquetes propietaria de propiedad comercial, por ejemplo, una red de cable o fibra óptica propietaria y similares, o cualquier combinación de los mismos. Además, la red inalámbrica puede ser, por ejemplo, una red celular y puede emplear varias tecnologías que incluyen velocidades de datos mejoradas para la evolución global (EDGE), servicio general de radio por paquetes (GPRS), sistema global para comunicaciones móviles (GSM), subsistema multimedia con protocolo de Internet (IMS), sistema universal de telecomunicaciones móviles (UMTS), etc., así como cualquier otro medio inalámbrico adecuado, por ejemplo, interoperabilidad mundial para acceso por microondas (WiMAX), redes de evolución a largo plazo (LTE), acceso múltiple por división de código (CDMA), acceso múltiple por división de código de banda ancha (WCDMA), fidelidad inalámbrica (Wi-Fi), LAN inalámbrica (WLAN), Bluetooth®, transmisión de datos de protocolo de Internet (IP), satélite, red móvil ad-hoc (MANET) y similares, o cualquier combinación de los mismos.

El UE 101 es cualquier tipo de terminal móvil, terminal fijo, o terminal portátil, que incluye un teléfono móvil, estación, unidad, dispositivo, ordenador multimedia, tableta multimedia, nodo de Internet, comunicador, ordenador de escritorio, ordenador portátil, asistentes digitales personales (PDA), reproductor de audio/video, cámara/videocámara digital, dispositivo de posicionamiento, receptor de televisión, receptor de radio difusión, dispositivo de libro electrónico, dispositivo de juego o cualquier combinación de los mismos. Se contempla además, que el UE 101 pueda admitir cualquier tipo de interfaz para el usuario (tal como circuitos "portátiles", etc.).

A modo de ejemplo, el UE 101, los servidores de aplicaciones 103a-103n y el servidor de autenticación 107 se comunican entre sí y con otros componentes de la red de comunicación 105 al usar protocolos bien conocidos, nuevos o aún en desarrollo. En este contexto, un protocolo incluye un conjunto de reglas que definen cómo los nodos de red dentro de la red de comunicación 105 interactúan entre sí en base a la información enviada a través de los vínculos de comunicación. Los protocolos son efectivos en diferentes capas de operación dentro de cada nodo, desde generar y recibir señales físicas de varios tipos, hasta seleccionar un enlace para transferir esas señales, al formato de información que se indica por esas señales, para identificar qué aplicación de software que se ejecuta en un sistema informático envía o recibe la información. Las diferentes capas conceptuales de los protocolos para el intercambio de información en una red se describen en el Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI).

Las comunicaciones entre los nodos de la red se efectúan típicamente mediante el intercambio de paquetes de datos discretos. Cada paquete típicamente comprende (1) información de encabezado que se asocia con un protocolo en particular, y (2) información de carga útil que sigue a la información de encabezado y contiene

información que puede procesarse independientemente de ese protocolo en particular. En algunos protocolos, el paquete incluye (3) información de cola que sigue a la carga útil e indica el final de la información de la carga útil. El encabezado incluye información tales como la fuente del paquete, su destino, la longitud de la carga útil y otras propiedades que se usan por el protocolo. A menudo, los datos en la carga útil para el protocolo en particular incluyen un encabezado y una carga útil para un protocolo diferente que se asocia con una capa superior diferente del modelo de referencia OSI. El encabezado de un protocolo en particular típicamente indica un tipo para el siguiente protocolo que se contiene en su carga útil. Se dice que el protocolo de capa superior se encapsula en el protocolo de capa inferior. Los encabezados que se incluyen en un paquete que atraviesa múltiples redes heterogéneas, tal como Internet, típicamente incluyen un encabezado físico (capa 1), un encabezado de enlace de datos (capa 2), un encabezado entre redes (capa 3) y un encabezado de transporte (capa 4) y varios encabezados de aplicación (capa 5, capa 6 y capa 7) como se define por el modelo de referencia OSI.

Cabe señalar que, aunque la Figura 1 ilustra los servidores de aplicaciones 103 y el servidor de autenticación 107 como entidades separadas, se contempla que cualquier combinación de estos servidores puede implementarse de manera que las funciones de estos componentes puedan combinarse en uno o más componentes o ser realizadas por otros componentes de funcionalidad equivalente. Además, se contempla que las aplicaciones cliente 111, el navegador 113 y el DE 109 se puedan distribuir en diferentes dispositivos y/o equipos y el contexto de autenticación se pueda compartir al usar una red de comunicación.

En una realización, las aplicaciones cliente 111 y el navegador 113 interactúan con los servidores de aplicaciones 103 de acuerdo con un modelo cliente-servidor. Cabe señalar que el modelo cliente-servidor de interacción de procesos informáticos se conoce y se usa ampliamente. De acuerdo con el modelo cliente-servidor, un proceso cliente envía un mensaje que incluye una solicitud a un proceso servidor, y el proceso servidor responde al proporcionar un servicio. El proceso servidor puede devolver además, un mensaje con una respuesta al proceso cliente. A menudo, el proceso cliente y el proceso servidor se ejecutan en diferentes dispositivos informáticos, que se denominan anfitriones, y se comunican a través de una red en la que usan uno o más protocolos para las comunicaciones de red. El término "servidor" se usa convencionalmente para referirse al proceso que proporciona el servicio, o el ordenador principal en el que opera el proceso. De manera similar, el término "cliente" se usa convencionalmente para referirse al proceso que realiza la solicitud, o el ordenador principal en el que opera el proceso. Como se usa en la presente memoria, los términos "cliente" y "servidor" se refieren a los procesos, en lugar de a los ordenadores principales, a menos que se aclare de otro modo en el contexto. Además, el proceso que se realiza por un servidor puede dividirse para ejecutarse como múltiples procesos en múltiples hosts (que a veces se denominan niveles) por razones que incluyen confiabilidad, escalabilidad y redundancia, entre otras.

La Figura 2 es un diagrama de los componentes de un habilitador de dispositivo, de acuerdo con una realización. A modo de ejemplo, el habilitador de dispositivos (DE) 109 puede incluir uno o más componentes para proporcionar una plataforma para compartir información de sesión de autenticación, tal como el contexto de autenticación, entre diferentes aplicaciones, tales como aplicaciones cliente que se ejecutan en entornos de tiempo de ejecución y aplicaciones cliente tales como navegadores. Se contempla que las funciones de estos componentes puedan combinarse en uno o más componentes o ser realizadas por otros componentes de funcionalidad equivalente. En esta realización, el DE 109 puede incluir un procesador 201 u otra lógica para ejecutar al menos un algoritmo para realizar las funciones del DE 109. Por ejemplo, cuando se accede al DE 109 mediante una de las aplicaciones cliente 111 de la Figura 1 para la autenticación, el procesador 201 en comunicación con el módulo de recuperación 203, determina si ya se ha procesado un procedimiento de autenticación para la aplicación cliente (y/o aplicaciones cliente que se relacionan). Por ejemplo, el módulo de recuperación 203 puede determinar si existe un contexto de autenticación para la aplicación cliente que solicita autenticación. En un ejemplo, el módulo de recuperación 203 puede consultar la base de datos de autenticación 117 para determinar si el contexto de autenticación está disponible. Adicionalmente, el módulo de recuperación 203 puede determinar además, si el contexto de autenticación aún es válido, por ejemplo, si no ha expirado.

Si el procesador 201 en comunicación con el módulo de recuperación 203 determina que un contexto de autenticación válido está disponible para la aplicación cliente solicitante, el módulo de recuperación 203 recupera el contexto de autenticación de una memoria caché y/o una base de datos tal como la base de datos de autenticación 117 e inicia la transmisión del contexto de autenticación a la aplicación cliente 111 que solicita autenticación. Sin embargo, si el módulo de recuperación 203 determina que el DE 109 ya ha procesado un procedimiento de autenticación para la aplicación cliente, que resultó en una autenticación fallida, el resultado de la autenticación fallida se proporciona además a la aplicación cliente.

Alternativamente, de acuerdo con ciertas realizaciones, si el módulo de recuperación 203 determina que no existe un contexto de autenticación válido para la aplicación cliente que solicitó autenticación, se invoca el módulo de interfaz de usuario 205 para iniciar una interfaz de usuario (UI) para solicitar al usuario de la aplicación cliente 111 para proporcionar información de autenticación y/o identificación, como credenciales de usuario. El módulo de recopilación de datos 207 puede recopilar la información de autenticación del usuario y preparar un mensaje de solicitud de autenticación para enviarlo a un servidor de autenticación, tal como el servidor de autenticación 107 de la Figura 1. El servidor de autenticación 107 puede verificar la información de autenticación del usuario y generar un contexto de autenticación si el usuario y/o la aplicación cliente está autorizado o validado de otro modo. En un

ejemplo, la información de usuario puede incluir credenciales de usuario tales como nombre de usuario y contraseña y el servidor de autenticación 107 puede comparar las credenciales de usuario con credenciales que se almacenan para autenticar al usuario y/o la aplicación cliente. El módulo de recopilación de datos 207 puede recibir el contexto de autenticación desde el servidor de autenticación 107.

Además, el módulo de recopilación de datos 207 puede recibir un mensaje de autenticación fallida del servidor de autenticación 107 si la información del usuario no es válida. El resultado de la solicitud de autenticación (contexto de autenticación o mensaje de autenticación fallido) se transmite a la aplicación cliente.

De acuerdo con ciertas realizaciones, si la autenticación es exitosa y el contexto de autenticación se recibe por, por ejemplo, el módulo de recopilación de datos 207, el módulo de almacenamiento en memoria caché/almacenamiento/llenado 209 puede almacenar en memoria caché y/o almacenar el contexto de autenticación en, por ejemplo, la base de datos de autenticación 117. Por lo tanto, el contexto de autenticación puede usarse, por ejemplo, por el módulo de recuperación 203 para autenticar solicitudes posteriores de la misma y/u otras aplicaciones cliente que se asocian con el DE 109. Además, el módulo de almacenamiento en memoria caché/almacenamiento/llenado 209 puede iniciar ventajosamente el llenado del contexto de autenticación en otra memoria caché y/o base de datos que no se enlaza directamente con y/o que utiliza el DE 109. Por ejemplo, el módulo de almacenamiento en memoria caché/almacenamiento/llenado 209 puede rellenar el contexto de autenticación que se recibe en la base de datos 115 de la Figura 1 que se asocia con el navegador 113 de la Figura 1. Por tanto, el navegador 113 de la Figura 1 puede usar el contexto de autenticación rellenado para acceder a los servidores de aplicaciones 103 de la Figura 1 sin necesidad de autenticarse primero con el servidor de autenticación 107. Como se mencionó, el módulo de almacenamiento en memoria caché/almacenamiento/llenado 209 puede rellenar el contexto de autenticación copiándolo, convirtiéndolo en base, al menos en parte, a un esquema de autenticación que se soporta, por ejemplo, por el navegador 113 de la Figura 1, etc.

La Figura 3 es un diagrama de flujo de un proceso para compartir información de sesión de autenticación, tal como el contexto de autenticación, entre diferentes aplicaciones (tales como aplicaciones cliente que se ejecutan en entornos de tiempo de ejecución y aplicaciones cliente tales como navegadores), de acuerdo con una realización. En una realización, el habilitador de dispositivo (DE) 109 de la Figura 1 realiza el proceso 300 y se implementa, por ejemplo, en un conjunto de chips que incluye un procesador y una memoria como se muestra en la Figura 7.

En el paso 301, se recibe una solicitud de autenticación. En una realización, la solicitud de autenticación se recibe de una aplicación cliente (tales como las aplicaciones cliente 111a-111m de la Figura 1) que se enlaza directamente con y/o que utiliza el DE 109. La solicitud de autenticación puede incluir información que se asocia con la aplicación cliente, un usuario de la aplicación cliente, etc. En el paso 303, se hace una determinación respecto a si ya existe un contexto de autenticación para la aplicación cliente que solicita la autenticación. En un ejemplo, la determinación puede basarse en la generación de una consulta a una base de datos, tal como la base de datos de autenticación 117, para determinar si un contexto de autenticación que se asocia con la aplicación cliente se recibió y almacenó previamente en la base de datos 117. Además, de acuerdo con ciertas realizaciones, si existe el contexto de autenticación, en el paso 303 se puede determinar si la autenticación es válida, por ejemplo, si no ha expirado. Si está disponible un contexto de autenticación (válido), en el paso 305 el contexto de autenticación se recupera de, por ejemplo, una memoria caché y/o una base de datos, tal como la base de datos de autenticación 117 de la Figura 1. En el paso 307, el contexto de autenticación recuperada se transmite a la aplicación cliente que solicita la autenticación. La aplicación cliente puede usar el contexto de autenticación para acceder a servicios de red tales como los servidores de aplicaciones 103 de la Figura 1.

Sin embargo, si en el paso 303 se determina que no está disponible un contexto de autenticación válido, en el paso 309 se genera una solicitud para recibir credenciales de autenticación que se asocian con un usuario de la aplicación cliente, que solicita la autenticación. En un ejemplo, se inicia una interfaz de usuario para solicitar al usuario credenciales de autenticación, tales como nombre de usuario, contraseña, contraseña de un solo uso, datos biométricos, etc. En el paso 311, las credenciales de autenticación se reciben de la aplicación cliente que se basan, al menos en parte, en la solicitud.

En el paso 313, se genera un mensaje de autenticación que se basa, al menos en parte, en las credenciales de autenticación que se reciben y el mensaje de autenticación se transmite a un servidor de autenticación, tal como el servidor de autenticación 107 de la Figura. 1. El servidor de autenticación valida las credenciales de autenticación (por ejemplo, comparándolas con las credenciales que se almacenan) para determinar si el usuario y/o la aplicación cliente están autorizados. En el paso 315, se recibe el resultado de la autenticación del usuario y/o cliente. Más específicamente, si el usuario y/o la aplicación cliente están autorizados, en el paso 315, se recibe un contexto de autenticación. En el paso 317, el contexto de autenticación se almacena en memoria caché y/o se almacena en una memoria caché y/o una base de datos que se asocia con el DE 109, tal como la base de datos 117 de autenticación de la Figura 1. El contexto de autenticación que se almacena en memoria caché y/o que se almacena puede ser usado adicionalmente por otras aplicaciones cliente, que, por ejemplo, se enlazan directamente con y/o que utilizan el DE 109.

En el paso 319, el contexto de autenticación se rellena además, en una segunda memoria caché y/o base de datos, que no se enlaza directamente con y/o que utiliza el DE 109, por ejemplo, la base de datos 115 de la Figura 1. En un ejemplo, la base de datos 115 puede ser un almacén de cookies que se asocia con el navegador 113 de la Figura 1. Como se mencionó, en una realización, en el paso 319, el llenado del contexto de autenticación puede incluir convertir el contexto de autenticación que se basa, al menos en parte, en un esquema de autenticación que se asocia con la aplicación cliente que se asocia con la segunda memoria caché y/o base de datos. Por ejemplo, el contexto de autenticación puede incluir un token y en el paso 319 el contexto de autenticación se convierte en un contexto de autenticación convertido que incluye una cookie cifrada que usa el nombre de usuario y la contraseña del usuario.

Las Figuras 4A y 4B son diagramas de secuencia de tiempo que ilustran una secuencia de mensajes y procesos para proporcionar una plataforma para compartir información de sesión de autenticación, de acuerdo con varias realizaciones. Un proceso de red se representa mediante una línea vertical. Un mensaje que se pasa de un proceso a otro se representa mediante flechas horizontales. El texto indica un paso se realiza por un proceso. Los procesos que se representan en las Figuras 4A y 4B son los servidores de aplicaciones 103, el servidor de autenticación 107, el habilitador de dispositivos (DE) 109, las aplicaciones cliente 111, el navegador 113, la base de datos 115 y la base de datos de autenticación 117. El ejemplo de la Figura 4A analiza el proceso 400 de autenticar una aplicación cliente y/o un usuario de la aplicación cliente, que recibe el contexto de autenticación, almacena el contexto de autenticación en una primera memoria caché y/o base de datos y rellena el contexto de autenticación en una segunda memoria caché y/o base de datos. Además, el ejemplo de la Figura 4B analiza el proceso 420 de solicitar autenticación por parte de una aplicación cliente y acceder a un servidor de aplicaciones mediante el navegador.

En el paso 401 del proceso 400, una de las aplicaciones cliente 111 de la Figura 1, como la aplicación cliente 111a, inicia una solicitud de autenticación al habilitador de dispositivo (DE) 109. En un ejemplo, la solicitud de autenticación puede incluir información que se asocia a la aplicación cliente 111a, un usuario de la aplicación cliente, un servidor de aplicaciones al que la aplicación cliente 111a desea acceder, etc. En el paso 403, el habilitador de dispositivo 109 inicia un diálogo, tal como una interfaz de usuario (UI), para solicitar al usuario credenciales de autenticación, si el DE 109 determina que la aplicación cliente 111a aún no se ha autenticado. En un ejemplo, la determinación se basa, al menos en parte, en una búsqueda en una memoria caché y/o una base de datos que se asocia con el DE 109 (tal como la base de datos de autenticación 117) para determinar si un contexto de autenticación que se asocia con la aplicación cliente 111a existe. Durante el diálogo 403, el DE 109 puede recopilar credenciales de autenticación de, por ejemplo, un usuario de la aplicación cliente 111a (y/o un usuario del UE 101).

En el paso 405, el DE 109 genera y transmite una solicitud de autenticación al servidor de autenticación 107 para validar las credenciales de autenticación que se recopilan por el DE 109. En un ejemplo, la solicitud de autenticación puede incluir las credenciales de autenticación y/o información que se asocia a las credenciales. A modo de ejemplo, las credenciales pueden incluir nombre de usuario, contraseña, contraseña de un solo uso, clave de consumidor, clave secreta, datos biométricos, etc. En el paso 407, el servidor de autenticación 107 verifica las credenciales de autenticación para determinar si la aplicación cliente y/o el usuario están autorizados. En un ejemplo, las credenciales de autenticación que se reciben (o la información que se asocia a ellas) se comparan con las credenciales que se almacenan. Si está autorizado, en el paso 409, se transmite un contexto de autenticación al DE 109. De acuerdo con una realización, el contexto de autenticación puede incluir una cookie o un token.

El DE 109, en el paso 411, inicia el almacenamiento en memoria caché y/o el almacenamiento del contexto de autenticación en una memoria caché y/o una base de datos que se enlaza directamente y o que utiliza el DE 109, tal como la base de datos de autenticación 117. El contexto de autenticación que se almacena en memoria caché/se almacena puede usarse adicionalmente por aplicaciones cliente que se enlazan directamente y/o que utilizan la base de datos de autenticación 117 y/o el DE 109. En el paso 413, el DE 109 transmite el contexto de autenticación que se recibe desde el servidor de autenticación 107 a la aplicación cliente 111a que solicitó la autenticación. Además, en el paso 415, el contexto de autenticación se rellena en una memoria caché y/o una base de datos que no se enlaza directamente con y/o que utiliza el DE 109. En un ejemplo, el contexto de autenticación se rellena desde la base de datos de autenticación 117 a la base de datos 115. Como se mencionó, de acuerdo con ciertas realizaciones, en el paso 415, el contexto de autenticación se convierte basándose, al menos en parte, en un protocolo de autenticación que se asocia con la aplicación cliente (tal como el navegador 113) que utiliza la base de datos 115. Se contempla que los mensajes y/o procesos que se ilustran puedan combinarse en uno o más mensajes y/o procesos o realizarse en otras secuencias.

La Figura 4B ilustra procesos ejemplares de una aplicación cliente (tal como la aplicación cliente 111b) que solicita autenticación y un navegador que solicita acceso a un servidor de aplicaciones. En el paso 421, la aplicación cliente 111b envía una solicitud de autenticación al DE 109. En un ejemplo, la solicitud de autenticación puede incluir información que se asocia con la aplicación cliente 111b, un usuario de la aplicación cliente 111b, etc. En el paso 423, se recupera el contexto de autenticación que se asocia con la aplicación cliente 111b y en el paso 425 el contexto de autenticación recuperada se transmite a la aplicación cliente 425. De acuerdo con determinadas realizaciones, en el paso 423, el DE 109 determina si ya se ha realizado un proceso de autenticación para la aplicación cliente 111b y/o aplicaciones cliente (tales como aplicaciones cliente 111) que se relacionan con la aplicación cliente 111b. En un ejemplo, la determinación puede basarse, al menos en parte, en una consulta a la

base de datos de autenticación 117 de la Figura 1 para determinar si un contexto de autenticación válido está disponible. Si no está disponible un contexto de autenticación válido, el proceso 400 de la Figura 4A se puede realizar. Si el contexto de autenticación válido está disponible, se recupera y se transmite a la aplicación cliente 111b. La aplicación cliente 111b puede usar el contexto de autenticación para, por ejemplo, acceder a los servidores de aplicaciones 103 de la Figura 1.

La Figura 4B ilustra además, los pasos del 427 al 435 que describen un proceso ejemplar del navegador 113 que accede al servidor de aplicaciones 103 que usa el contexto de autenticación rellenado en el paso 415 de la Figura 4A. En el paso 427, el navegador 113 envía una solicitud de datos al servidor de aplicaciones 103. La solicitud de datos puede incluir información que se refiere al navegador 113, el servidor de aplicaciones 103, el contexto de autenticación rellenado, etc. En una realización, el contexto de autenticación se ha rellenado, por ejemplo, en una memoria caché y/o base de datos que se asocia con el navegador 113 en un proceso tal como el proceso 400 de la Figura 4A. En un ejemplo, el contexto de autenticación rellenado puede ser una cookie que se almacena en un almacén de cookies del navegador. El navegador 113 puede acceder al almacén de cookies del navegador para recuperar la cookie e incluirla en la solicitud de datos 427.

En los pasos del 429 al 433, el servidor de aplicaciones 103 con el servidor de autenticación 107 verifica la validez del contexto de autenticación rellenado. En el paso 429, el servidor de aplicaciones 103 genera un mensaje de verificación de autenticación y transmite el mensaje al servidor de autenticación 107. El mensaje de verificación de autenticación puede incluir el contexto de autenticación rellenado y/o la información que se asocia con él. En el paso 431, el servidor de autenticación 107 verifica si el contexto de autenticación rellenado es válido. En un ejemplo, el contexto de autenticación 431 compara el contexto de autenticación (y/o la información que se asocia con él) con el contexto de autenticación (información que se asocia con él y/o credenciales de autenticación de un usuario o aplicación cliente) que se generó, por ejemplo, en el paso 407 del proceso 400 de la Figura 4A. En el paso 433, el servidor de autenticación 107 envía una respuesta de verificación al servidor de aplicaciones 103 que se basa, al menos en parte, en el paso 431. Si el contexto de autenticación rellenado es válido, en el paso 435, el servidor de aplicaciones 103 devuelve los datos solicitados al navegador 113.

Aunque las realizaciones que se discuten se refieren a procesos en los que el contexto de autenticación se genera primero para aplicaciones cliente que se ejecutan en un entorno de tiempo de ejecución y se rellena para otras aplicaciones, tales como navegadores (por ejemplo, a través de un método de empuje para intercambiar contextos de autenticación), sin embargo, se contempla que el proceso inverso (por ejemplo, a través de un procedimiento de extracción para intercambiar contextos de autenticación) pueden implementarse además. Por ejemplo, una aplicación cliente, tal como un navegador, puede autenticarse frente a un servidor de autenticación (tal como el servidor de autenticación 107 de la Figura 1), un contexto de autenticación puede generarse y almacenarse en memoria caché y/o almacenarse en una primera memoria caché y/o base de datos que se asocia con la aplicación cliente, y el contexto de autenticación se puede rellenar adicionalmente en una segunda memoria caché y/o base de datos para otras aplicaciones cliente que no se enlazan directamente con y/o que utilizan la primera memoria caché y/o base de datos.

La Figura 5 es un diagrama de un ejemplo de una interfaz de usuario para proporcionar datos que se refieren a las credenciales de autenticación, de acuerdo con una realización. Como se describió anteriormente, cuando el DE 109 de la Figura 1 recibe una solicitud de autenticación de una de las aplicaciones cliente 111 y determina que el contexto de autenticación válido no está disponible, el DE puede iniciar una interfaz de usuario (UI) para solicitar al usuario de la aplicación cliente las credenciales de autenticación. La Figura 5 es un ejemplo de interfaz de usuario 500 que solicita dicha información. En este ejemplo, el usuario y/o el UE 101 pueden ingresar el ID de usuario y la contraseña para propósitos de autenticación. Se contempla que el DE 109 pueda solicitar cualquier información para asegurar que solo los usuarios que se autorizan puedan acceder a los servicios y/o información que se solicitan.

Los procesos descritos en la presente memoria para proporcionar una plataforma para compartir información de sesión de autenticación, tal como el contexto de autenticación, entre diferentes aplicaciones se pueden implementar ventajosamente a través de software, hardware (por ejemplo, procesador general, chip de procesamiento de señal digital (DSP), un circuito integrado específico de la aplicación (ASIC), matrices de puertas programables en campo (FPGA), etc.), microprograma o una combinación de los mismos. Tal hardware ejemplar para realizar las funciones que se describen, se detalla más abajo.

La Figura 6 ilustra un sistema informático 600 en el que se puede implementar una realización de la invención. Aunque el sistema informático 600 se representa con respecto a un dispositivo o equipo en particular, se contempla que otros dispositivos o equipos (por ejemplo, elementos de red, servidores, etc.) dentro de la Figura 6 puedan desplegar el hardware y los componentes que se ilustran del sistema 600. El sistema informático 600 está programado (por ejemplo, a través de un código de programa informático o instrucciones) para proporcionar el intercambio de sesiones de autenticación como se describe en la presente memoria e incluir un mecanismo de comunicación tal como un bus 610 para pasar información entre otros componentes internos y externos del sistema informático 600. La información (que se denomina además, datos) se representa como una expresión física de un fenómeno medible, típicamente voltajes eléctricos, pero que incluye, en otras realizaciones, fenómenos tales como interacciones magnéticas, electromagnéticas, de presión, químicas, biológicas, moleculares, atómicas, subatómicas

y cuánticas. Por ejemplo, los campos magnéticos norte y sur, o un voltaje eléctrico cero y distinto de cero, representan dos estados (0, 1) de un dígito binario (bit). Otros fenómenos pueden representar dígitos de una base superior. Una superposición de múltiples estados cuánticos simultáneos antes de la medición representa un bit cuántico (qubit). Una secuencia de uno o más dígitos constituye datos digitales que se usan para representar un número o código para un carácter. En algunas realizaciones, la información que ese denomina datos analógicos se representa por un continuo aproximado de valores medibles dentro de un rango en particular. El sistema informático 600, o una porción del mismo, constituye un medio para realizar uno o más pasos para proporcionar un intercambio de sesiones de autenticación.

Un bus 610 incluye uno o más conductores paralelos de información de modo que la información se transfiera rápidamente entre los dispositivos que se acoplan al bus 610. Uno o más procesadores 602 para procesar información se acoplan con el bus 610.

Un procesador 602 realiza un conjunto de operaciones en la información como se especifica por el código del programa informático que se refiere al intercambio de sesiones de autenticación. El código del programa informático es un conjunto de instrucciones o declaraciones que proporcionan instrucciones para la operación del procesador y/o el sistema informático para realizar funciones específicas. El código, por ejemplo, puede estar escrito en un lenguaje de programación informático que se compila en un conjunto de instrucciones nativas del procesador. El código puede además, escribirse directamente al usar el conjunto de instrucciones nativas (por ejemplo, lenguaje de máquina). El conjunto de operaciones incluye traer información desde el bus 610 y colocar información en el bus 610. El conjunto de operaciones suele incluir además, comparar dos o más unidades de información, cambiar posiciones de unidades de información y combinar dos o más unidades de información, tal como por suma o multiplicación u operaciones lógicas como OR, OR exclusivo (XOR) y AND. Cada operación del conjunto de operaciones que puede realizase por el procesador se representa al procesador mediante información que se denominan instrucciones, tal como un código de operación de uno o más dígitos. Una secuencia de operaciones a ejecutar por el procesador 602, tal como una secuencia de códigos de operación, constituyen instrucciones del procesador, que se denominan además, instrucciones del sistema informático o, simplemente, instrucciones informáticas. Los procesadores pueden implementarse como componentes mecánicos, eléctricos, magnéticos, ópticos, químicos o cuánticos, entre otros, solos o en combinación.

El sistema informático 600 incluye además, una memoria 604 que se acopla al bus 610. La memoria 604, tal como una memoria de acceso aleatorio (RAM) u otro dispositivo de almacenamiento dinámico, almacena información que incluye instrucciones del procesador para proporcionar el intercambio de sesiones de autenticación. La memoria dinámica permite que la información que se almacena en ella se cambie por el sistema informático 600. La RAM permite que una unidad de información que se almacena en una ubicación que se denomina dirección de memoria se almacene y recupere independientemente de la información en direcciones vecinas. La memoria 604 se usa además, por el procesador 602 para almacenar valores temporales durante la ejecución de las instrucciones del procesador. El sistema informático 600 incluye además, una memoria de sólo lectura (ROM) 606 u otro dispositivo de almacenamiento estático que se acopla al bus 610 para almacenar información estática, incluidas instrucciones, que el sistema informático 600 no cambia. Algunas memorias se componen de almacenamiento volátil que pierde la información que se almacena en el mismo cuando se pierde la potencia. Un dispositivo de almacenamiento no volátil (persistente) 608 se acopla además, al bus 610, tales como un disco magnético, un disco óptico o una tarjeta flash, para almacenar información, que incluye las instrucciones, que persiste incluso cuando el sistema informático 600 se apaga o de otro modo se pierde la potencia.

La información, que incluye las instrucciones para proporcionar el intercambio de sesiones de autenticación, se proporciona al bus 610 para su uso por el procesador desde un dispositivo de entrada externo 612, tal como un teclado que contiene teclas alfanuméricas que se operan por un usuario humano, o un sensor. Un sensor detecta condiciones en su vecindad y transforma esas detecciones en expresión física compatible con el fenómeno medible que se usa para representar información en el sistema informático 600. Otros dispositivos externos que se acoplan al bus 610, que se usan principalmente para interactuar con humanos, incluyen un dispositivo de visualización 614, tal como un tubo de rayos catódicos (CRT) o una pantalla de cristal líquido (LCD), o una pantalla de plasma o una impresora para presentar texto o imágenes, y un dispositivo señalador 616, tal como un ratón o una bola de seguimiento o teclas de dirección del cursor, o un sensor de movimiento, para controlar una posición de una pequeña imagen de cursor que se presenta en la pantalla 614 y emitir comandos que se asocian con elementos gráficos presentes en la pantalla 614. En algunas realizaciones, por ejemplo, en las realizaciones en las que el sistema informático 600 realiza todas las funciones automáticamente sin intervención humana, se omite uno o más del dispositivo de entrada externo 612, el dispositivo de visualización 614 y el dispositivo señalador 616.

En la realización ilustrada, el hardware de propósito especial, tal como un circuito integrado de aplicaciones específicas (ASIC) 620, se acopla al bus 610. El hardware de propósito especial se configura para realizar operaciones que no se realizan por el procesador 602 lo suficientemente rápido para propósitos especiales. Algunos ejemplos de circuitos integrados específicos de aplicaciones incluyen tarjetas aceleradoras de gráficos para generar imágenes para la pantalla 614, placas criptográficas para cifrar y descifrar mensajes enviados a través de una red, reconocimiento de voz, e interfaces para dispositivos externos especiales, tales como brazos robóticos y equipos de

escaneo médico que realizan repetidamente algunas secuencias complejas de operaciones que se implementan más eficientemente en hardware.

El sistema informático 600 incluye además, una o más instancias de una interfaz de comunicaciones 670 que se acopla al bus 610. La interfaz de comunicación 670 proporciona un acoplamiento de comunicación unidireccional o bidireccional a una variedad de dispositivos externos que operan con sus propios procesadores, tales como impresoras, escáneres y discos externos. En general, el acoplamiento es con un enlace de red 678 que se conecta a una red local 680 a la que se conectan una variedad de dispositivos externos con sus propios procesadores. Por ejemplo, la interfaz de comunicación 670 puede ser un puerto paralelo o un puerto serie o un puerto de bus serie universal (USB) en un ordenador personal. En algunas realizaciones, la interfaz de comunicaciones 670 es una tarjeta de red digital de servicios integrados (ISDN) o una tarjeta de línea de abonado digital (DSL) o un módem telefónico que proporciona una conexión de comunicación de información a un tipo correspondiente de línea telefónica. En algunas realizaciones, una interfaz de comunicación 670 es un módem de cable que convierte señales en el bus 610 en señales para una conexión de comunicación a través de un cable coaxial o en señales ópticas para una conexión de comunicación a través de un cable de fibra óptica. Como otro ejemplo, la interfaz de comunicaciones 670 puede ser una tarjeta de red de área local (LAN) para proporcionar una conexión de comunicación de datos a una LAN compatible, tal como Ethernet. Se pueden implementar además, enlaces inalámbricos. Para enlaces inalámbricos, la interfaz de comunicaciones 670 envía o recibe o ambos envía y recibe señales eléctricas, acústicas o electromagnéticas, que incluyen señales ópticas e infrarrojas, que llevan flujos de información, tales como datos digitales. Por ejemplo, en dispositivos portátiles inalámbricos, tales como teléfonos móviles como celulares, la interfaz de comunicaciones 670 incluye un transmisor y receptor electromagnético de banda de radio que se denomina un transceptor de radio. En determinadas realizaciones, la interfaz de comunicaciones 670 permite la conexión a la red de comunicaciones 105 para proporcionar el intercambio de sesiones de autenticación al UE 101.

El término "medio legible por ordenador" como se usa en la presente memoria para referirse a cualquier medio que participa en proporcionar información al procesador 602, que incluye instrucciones para la ejecución. Tal medio puede tomar muchas formas, que incluyen, pero que no se limita a un medio de almacenamiento legible por ordenador (por ejemplo, medios no volátiles, medios volátiles), y medios de transmisión. Los medios no transitorios, tales como los medios no volátiles, incluyen, por ejemplo, discos ópticos o magnéticos, tal como el dispositivo de almacenamiento 608. Los medios volátiles incluyen, por ejemplo, la memoria dinámica 604. Los medios de transmisión incluyen, por ejemplo, cables coaxiales, alambre de cobre, cables de fibra óptica y ondas portadoras que viajan a través del espacio sin alambres ni cables, tales como ondas acústicas y ondas electromagnéticas, incluidas ondas de radio, ópticas e infrarrojas. Las señales incluyen variaciones transitorias provocadas por el hombre en amplitud, frecuencia, fase, polarización u otras propiedades físicas transmitidas a través de los medios de transmisión. Las formas comunes de medio legible por ordenador incluyen, por ejemplo, un disquete, un disco flexible, un disco duro, una cinta magnética, cualquier otro medio magnético, un CD-ROM, un CDRW, un DVD, cualquier otro medio óptico, tarjetas perforadas, cinta de papel, hojas de marcas ópticas, cualquier otro medio físico con patrones de agujeros u otros indicios ópticamente reconocibles, una RAM, una PROM, una EPROM, una FLASH-EPROM, cualquier otro chip o cartucho de memoria, una onda portadora o cualquier otro medio del que pueda leer un ordenador. El término medio de almacenamiento legible por ordenador se usa en la presente memoria para referirse a cualquier medio legible por ordenador, excepto los medios de transmisión.

La lógica que se codifica en uno o más medios tangibles incluye una o ambas instrucciones del procesador en un medio de almacenamiento legible por ordenador y hardware de propósito especial, tal como el ASIC 620.

El enlace de red 678 típicamente proporciona comunicación de información al usar medios de transmisión a través de una o más redes a otros dispositivos que usan o procesan la información. Por ejemplo, el enlace de red 678 puede proporcionar una conexión a través de la red local 680 a un ordenador principal 682 o a un equipo 684 que se opera por un proveedor de servicios de Internet (ISP). El equipo ISP 684 proporciona a su vez, servicios de comunicación de datos a través de la red pública de comunicación de conmutación de paquetes a nivel mundial de redes que ahora se refieren comúnmente como Internet 690.

Un ordenador que se denomina servidor host 692 que se conecta a Internet aloja un proceso que proporciona un servicio en respuesta a la información que se recibe a través de Internet. Por ejemplo, el servidor host 692 aloja un proceso que proporciona información que representa datos de vídeo para su presentación en la pantalla 614. Se contempla que los componentes del sistema 600 se puedan implementar en varias configuraciones dentro de otros sistemas informáticos, por ejemplo, el host 682 y el servidor 692.

Al menos algunas realizaciones de la invención se refieren al uso del sistema informático 600 para implementar algunas o todas las técnicas que se describen en la presente memoria. De acuerdo con una realización de la invención, esas técnicas se realizan por el sistema informático 600 en respuesta al procesador 602 que ejecuta una o más secuencias de una o más instrucciones del procesador que se contienen en la memoria 604. Tales instrucciones, que se denominan además, instrucciones informáticas, software y código de programa, pueden leerse en la memoria 604 desde otro medio legible por ordenador tal como el dispositivo de almacenamiento 608 o el enlace de red 678. La ejecución de las secuencias de instrucciones que se contienen en la memoria 604 provoca

que el procesador 602 realice uno o más de los pasos del procedimiento que se describen en la presente memoria. En realizaciones alternativas, se puede usar hardware, tal como el ASIC 620, en lugar de o en combinación con software para implementar la invención. Así, las realizaciones de la invención no se limitan a ninguna combinación específica de hardware y software, a menos que se indique explícitamente de otro modo en la presente memoria.

Las señales que se transmiten a través del enlace de red 678 y otras redes a través de la interfaz de comunicaciones 670, llevan información hacia y desde el sistema informático 600. El sistema informático 600 puede enviar y recibir información, que incluye el código de programa, a través de las redes 680, 690, entre otras, a través del enlace de red 678 y la interfaz de comunicaciones 670. En un ejemplo que usa Internet 690, un servidor host 692 transmite código de programa para una aplicación en particular, que se solicita por un mensaje que se envía desde el ordenador 600, a través de Internet 690, el equipo ISP 684, la red local 680 y la interfaz de comunicaciones 670. El código que se recibe puede ejecutarse por el procesador 602 a medida que se recibe, o puede almacenarse en la memoria 604, o en el dispositivo de almacenamiento 608 u otro almacenamiento no volátil para su posterior ejecución, o ambos. De esta manera, el sistema informático 600 puede obtener un código de programa de aplicación en forma de señales en una onda portadora.

Varias de estas formas de medios legibles por ordenador pueden involucrarse en llevar una o más secuencias de instrucciones o de datos, o ambas, a un procesador 602 para su ejecución. Por ejemplo, las instrucciones y los datos pueden llevarse inicialmente en un disco magnético de un ordenador remota como el host 682. El ordenador remoto carga las instrucciones y los datos en su memoria dinámica y envía las instrucciones y los datos a través de una línea telefónica que usa un módem. Un módem local del sistema informático 600 recibe las instrucciones y los datos en una línea telefónica y usa un transmisor de infrarrojos para convertir las instrucciones y los datos a una señal en una onda portadora de infrarrojos que sirve como el enlace de red 678. Un detector de infrarrojos que sirve como interfaz de comunicaciones 670 recibe las instrucciones y los datos que se llevan en la señal de infrarrojos y coloca la información que representa las instrucciones y los datos en el bus 610. El bus 610 lleva la información a la memoria 604 desde la que el procesador 602 recupera y ejecuta las instrucciones al usar algunos de los datos que se envían con las instrucciones. Las instrucciones y los datos que se reciben en la memoria 604 pueden almacenarse opcionalmente en el dispositivo de almacenamiento 608 ya sea antes o después de la ejecución por el procesador 602.

La Figura 7 ilustra un conjunto de chips 700 en el que se puede implementar una realización de la invención. El conjunto de chips 700 se programa para proporcionar el intercambio de sesiones de autenticación como se describe en la presente memoria e incluye, por ejemplo, el procesador y los componentes de memoria que se describen con respecto a la Figura 6 que se incorporan en uno o más envases físicos (por ejemplo, chips). A modo de ejemplo, un envase físico incluye una disposición de uno o más materiales, componentes y/o cables en un conjunto estructural (por ejemplo, una placa base) para proporcionar una o más características tales como resistencia física, conservación de tamaño y/o limitación de la interacción eléctrica. Se contempla que, en determinadas realizaciones, el conjunto de chips se pueda implementar en un solo chip. El conjunto de chips 700, o una porción del mismo, constituye un medio para realizar uno o más pasos para proporcionar el intercambio de sesiones de autenticación.

En una realización, el conjunto de chips 700 incluye un mecanismo de comunicación tal como un bus 701 para pasar información entre los componentes del conjunto de chips 700. Un procesador 703 tiene conectividad con el bus 701 para ejecutar instrucciones y procesar información que se almacena, por ejemplo, en una memoria 705. El procesador 703 puede incluir uno o más núcleos de procesamiento con cada núcleo que se configura para funcionar de forma independiente. Un procesador de múltiples núcleos permite el multiprocesamiento dentro de un solo envase físico. Los ejemplos de un procesador de múltiples núcleos incluyen dos, cuatro, ocho o un número mayor de núcleos de procesamiento. Alternativamente o además, el procesador 703 puede incluir uno o más microprocesadores que se configuran en tándem a través del bus 701 para permitir la ejecución independiente de instrucciones, canalización y subprocesos múltiples. El procesador 703 puede ir acompañado además, de uno o más componentes especializados para realizar determinadas funciones y tareas de procesamiento tales como uno o más procesadores de señales digitales (DSP) 707, o uno o más circuitos integrados de aplicación específica (ASIC) 709. Un DSP 707 típicamente se configura para procesar señales del mundo real (por ejemplo, sonido) en tiempo real independientemente del procesador 703. De manera similar, un ASIC 709 se puede configurar para realizar funciones especializadas que no se realizan fácilmente por un procesador de propósito general. Otros componentes especializados para ayudar a realizar las funciones inventivas que se describen en la presente memoria incluyen una o más matrices de puertas programables en campo (FPGA) (que no se muestran), uno o más controladores (que no se muestran), o uno o más de otros chips informáticos de propósito especial.

El procesador 703 y los componentes que lo acompañan tienen conectividad con la memoria 705 a través del bus 701. La memoria 705 incluye tanto una memoria dinámica (por ejemplo, RAM, disco magnético, disco óptico grabable, etc.) como una memoria estática (por ejemplo, ROM, CD-ROM, etc.) para almacenar instrucciones ejecutables que, cuando se ejecutan, realizan los pasos inventivos que se describen en la presente memoria para proporcionar el intercambio de sesiones de autenticación. La memoria 705 almacena además, los datos que se asocian con o se generan por la ejecución de las etapas inventivas.

La Figura 8 es un diagrama de componentes ejemplares de una terminal móvil (por ejemplo, auricular) para comunicaciones, que es capaz de operar en el sistema de la Figura 1, de acuerdo con una realización. En algunas realizaciones, la terminal móvil 800 o una porción del mismo, constituye un medio para realizar una o más etapas para proporcionar el intercambio de sesiones de autenticación. Generalmente, un receptor de radio a menudo se define en términos de características de front-end y back-end. El front-end del receptor abarca todos los circuitos de radiofrecuencia (RF), mientras que el back-end abarca todos los circuitos de procesamiento de banda base. Como se usa en la presente solicitud, el término "circuito" se refiere a ambos: (1) a implementaciones de solo hardware (tales como implementaciones en circuitos solo analógicos y/o digitales), y (2) a combinaciones de circuitos y software (y/o microprograma) (tal como, si es aplicable al contexto en particular, a una combinación de procesador (es), que incluye procesador (es) de señal digital, software y memoria (s) que trabajan juntas para provocar que un aparato, tal como un teléfono móvil o un servidor, realice varias funciones). Esta definición de "circuito(s)" se aplica a todos los usos de este término en la presente solicitud, incluso en cualquiera de las reivindicaciones. Como un ejemplo, además, como se usa en la presente solicitud y es aplicable al contexto en particular, el término "circuito" cubriría además, una implementación de un simple procesador (o múltiples procesadores) y su (o sus) software/o microprograma que lo acompañan. El término "circuito" cubriría además, si es aplicable al contexto en particular, por ejemplo, un circuito integrado de banda base o un circuito integrado de procesador de aplicaciones en un teléfono móvil o un circuito integrado similar en un dispositivo de red celular u otro dispositivo de red.

Los componentes internos pertinentes del teléfono incluyen una Unidad de Control Principal (MCU) 803, un Procesador de Señal Digital (DSP) 805 y una unidad de receptor/transmisor que incluye una unidad de control de ganancia de micrófono y una unidad de control de ganancia de altavoz. Una unidad de visualización principal 807 proporciona una pantalla al usuario en apoyo de varias aplicaciones y funciones de terminal móvil que realizan o apoyan las etapas de proporcionar el intercambio de sesiones de autenticación. La pantalla 807 incluye circuitos de pantalla que se configuran para mostrar al menos una porción de una interfaz de usuario del terminal móvil (por ejemplo, teléfono móvil). Además, la pantalla 807 y los circuitos de pantalla se configuran para facilitar el control del usuario de al menos algunas funciones del terminal móvil. Un circuito de función de audio 809 incluye un micrófono 811 y un amplificador de micrófono que amplifica la salida de la señal de voz del micrófono 811. La salida de la señal de voz amplificada del micrófono 811 alimenta a un codificador/descodificador (CODEC) 813.

Una sección de radio 815 amplifica la potencia y convierte la frecuencia con el fin de comunicarse con una estación base, que se incluye en un sistema de comunicación móvil, a través de la antena 817. El amplificador de potencia (PA) 819 y el circuito transmisor/modulación responden operativamente al MCU 803, con una salida del PA 819 que se acopla al duplexor 821 o al circulador o conmutador de antena, como se conoce en la técnica. El PA 819 se acopla además, a una interfaz de batería y una unidad de control de potencia 820.

En uso, un usuario del terminal móvil 801 habla por el micrófono 811 y su voz junto con cualquier ruido de fondo que se detecta se convierte en un voltaje analógico. Luego, el voltaje analógico se convierte en una señal digital a través del Convertidor Analógico a Digital (ADC) 823. La unidad de control 803 enruta la señal digital al DSP 805 para su procesamiento en el mismo, tal como codificación de voz, codificación de canal, encriptación e intercalación. En una realización, las señales de voz que se procesan se codifican, por unidades que no se muestran por separado, que usan un protocolo de transmisión celular tal como evolución global (EDGE), servicio general de radio por paquetes (GPRS), sistema global para comunicaciones móviles (GSM), subsistema multimedia con protocolo de Internet (IMS), sistema universal de telecomunicaciones móviles (UMTS), etc., así como cualquier otro medio inalámbrico adecuado, por ejemplo, acceso por microondas (WiMAX), redes de evolución a largo plazo (LTE), acceso múltiple por división de código (CDMA), acceso múltiple por división de código de banda ancha (WCDMA), fidelidad inalámbrica (WiFi), satélite y similares.

Las señales codificadas se enrutan luego a un ecualizador 825 para la compensación de cualquier deterioro dependiente de la frecuencia que se produzca durante la transmisión a través del aire, tal como la distorsión de fase y amplitud. Después de ecualizar la cadena de bits, el modulador 827 combina la señal con una señal de RF que se genera en la interfaz de RF 829. El modulador 827 genera una onda sinusoidal a modo de modulación de frecuencia o fase. Con el fin de preparar la señal para la transmisión, un convertidor ascendente 831 combina la salida de onda sinusoidal del modulador 827 con otra onda sinusoidal que se genera por un sintetizador 833 para lograr la frecuencia de transmisión que se desea. Luego, la señal se envía a través de un PA 819 para aumentar la señal a un nivel de potencia apropiado. En sistemas prácticos, el PA 819 actúa como un amplificador de ganancia variable cuya ganancia se controla por el DSP 805 a partir de la información que se recibe de una estación base de red. Luego, la señal se filtra dentro del duplexor 821 y opcionalmente se envía a un acoplador de antena 835 para igualar las impedancias para proporcionar la máxima transferencia de potencia. Finalmente, la señal se transmite a través de la antena 817 a una estación base local. Se puede suministrar un control de ganancia automático (AGC) para controlar la ganancia de las etapas finales del receptor. Las señales pueden ser enviadas desde allí a un teléfono remoto que puede ser otro teléfono celular, otro teléfono móvil o una línea terrestre que se conecta a una Red Telefónica Pública Conmutada (PSTN) u otras redes telefónicas.

Las señales de voz que se trasmiten al terminal móvil 801 se reciben a través de la antena 817 y se amplifican inmediatamente por un amplificador de bajo ruido (LNA) 837. Un convertidor descendente 839 reduce la frecuencia portadora mientras que el demodulador 841 se desprende de la RF dejando solo una cadena de bits digital. Luego,

la señal pasa a través del ecualizador 825 y se procesa por el DSP 805. Un Convertidor Digital a Analógico (DAC) 843 convierte la señal y la salida resultante se transmite al usuario a través del altavoz 845, todo bajo el control de una Unidad de Control Principal (MCU) 803, que se puede implementar como una Unidad Central de Procesamiento (CPU) (que no se muestra).

El MCU 803 recibe varias señales, que incluyen las señales de entrada del teclado 847. El teclado 847 y/o la MCU 803 en combinación con otros componentes de entrada de usuario (por ejemplo, el micrófono 811) comprenden un circuito de interfaz de usuario para gestionar la entrada de usuario. La MCU 803 ejecuta un software de interfaz de usuario para facilitar el control del usuario de al menos algunas funciones del terminal móvil 801 para proporcionar el intercambio de sesiones de autenticación. La MCU 803 envía además, un comando de visualización y un comando de conmutación a la pantalla 807 y al controlador de conmutación de salida de voz, respectivamente. Además, el MCU 803 intercambia información con el DSP 805 y puede acceder a una tarjeta SIM 849 incorporada opcionalmente y a una memoria 851. Además, el MCU 803 ejecuta varias funciones de control que se requieren del terminal. El DSP 805 puede, en dependencia de la implementación, realizar cualquiera de una variedad de funciones de procesamiento digital convencionales en las señales de voz. Además, el DSP 805 determina el nivel de ruido de fondo del entorno local a partir de las señales que se detectan por el micrófono 811 y establece la ganancia del micrófono 811 en un nivel que se selecciona para compensar la tendencia natural del usuario del terminal móvil 801.

El CODEC 813 incluye el ADC 823 y el DAC 843. La memoria 851 almacena varios datos, que incluyen los datos de tono de llamada entrante y es capaz de almacenar otros datos, que incluyen los datos de música que se reciben a través de, por ejemplo, Internet global. El módulo de software podría residir en la memoria RAM, memoria flash, registros o cualquier otra forma de medio de almacenamiento grabable conocido en la técnica. El dispositivo de memoria 851 puede ser, pero no se limita a, una única memoria, CD, DVD, ROM, RAM, EEPROM, almacenamiento óptico o cualquier otro medio de almacenamiento no volátil capaz de almacenar datos digitales.

Una tarjeta SIM 849 que se incorpora opcionalmente lleva, por ejemplo, información importante, tal como el número de teléfono celular, el servicio de suministro del operador, detalles de suscripción e información de seguridad. La tarjeta SIM 849 sirve principalmente para identificar el terminal móvil 801 en una red de radio. La tarjeta 849 contiene además, una memoria para almacenar un registro de número de teléfono personal, mensajes de texto y configuraciones de terminal móvil específicas del usuario.

Si bien la invención se ha descrito en conexión con una serie de realizaciones e implementaciones, la invención no se limita tanto, sino que abarca varias modificaciones obvias y disposiciones equivalentes, que caen dentro del alcance de las reivindicaciones adjuntas. Aunque las características de la invención se expresan en ciertas combinaciones entre las reivindicaciones, se contempla que estas características puedan disponerse en cualquier combinación y orden.

REIVINDICACIONES

1. Un procedimiento, que comprende:

recibir (315), en una interfaz, un contexto de autenticación que se asocia con un primer servicio;
provocar (317), al menos en parte, el almacenamiento del contexto de autenticación en una primera memoria caché que se asocia con la interfaz; y
provocar (319), al menos en parte, el llenado del contexto de autenticación en una segunda memoria caché que se asocia con un segundo servicio, la segunda memoria caché no se enlaza directamente a la interfaz,
en el que el contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio; y
en el que el llenado del contexto de autenticación en la segunda memoria caché comprende:

convertir el contexto de autenticación que se basa, al menos en parte, en un protocolo de autenticación que se asocia con el segundo servicio,
en el que el contexto de autenticación en la segunda memoria caché es el contexto de autenticación convertido.

2. Un procedimiento de la reivindicación 1, en el que cuando el contexto de autenticación se basa en cookies,

el contexto de autenticación convertido se basa en token, y cuando el contexto de autenticación se basa en token, el contexto de autenticación convertido se basa en cookies.

3. Un procedimiento de cualquiera de las reivindicaciones 1-2, en el que la interfaz realiza además:

recibir (301), desde el primer servicio, una solicitud para autenticar a un usuario;
solicitar (309) credenciales de autenticación que se asocian con el usuario;
recibir (311) las credenciales de autenticación en base a la solicitud;
provocar (313), al menos en parte, la transmisión de las credenciales de autenticación a un servidor de autenticación,
en el que el contexto de autenticación se recibe desde el servidor de autenticación que se basa, al menos en parte, en las credenciales de autenticación.

4. Un procedimiento de cualquiera de las reivindicaciones 1-3, en el que el contexto de autenticación es un contexto de autenticación de inicio único de sesión que se puede aplicar tanto al primer servicio como al segundo servicio.

5. Un procedimiento de cualquiera de las reivindicaciones 1-4, en el que el primer servicio y el segundo servicio son aplicaciones de tiempo de ejecución que se ejecutan en un dispositivo común.

6. Un procedimiento de cualquiera de las reivindicaciones 1-5, en el que al menos uno del primer servicio y el segundo servicio incluyen al menos uno de una aplicación, una sesión de navegador.

7. Un producto de programa informático que incluye una o más secuencias de una o más instrucciones que, cuando se ejecutan por uno o más procesadores, provocan que un aparato:

reciba (315), en una interfaz, un contexto de autenticación que se asocia con un primer servicio;
provoca (317), al menos en parte, el almacenamiento del contexto de autenticación en una primera memoria caché que se asocia con la interfaz; y
provoca (319), al menos en parte, el llenado del contexto de autenticación en una segunda memoria caché que se asocia con un segundo servicio, la segunda memoria caché no se enlaza directamente a la interfaz,
en el que el contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio; y
en el que el llenado del contexto de autenticación en la segunda memoria caché comprende:

convertir el contexto de autenticación que se basa, al menos en parte, en un protocolo de autenticación que se asocia con el segundo servicio,
en el que el contexto de autenticación en la segunda memoria caché es el contexto de autenticación convertido.

8. El producto de programa informático de la reivindicación 7, en el que cuando el contexto de autenticación se basa en cookies, el contexto de autenticación convertido se basa en token, y cuando el contexto de autenticación se basa en token, el contexto de autenticación convertido se basa en cookies.

9. Un producto de programa informático que incluye una o más secuencias de una o más instrucciones que, cuando se ejecutan por uno o más procesadores, provocan que un aparato realice al menos el procedimiento de una de las reivindicaciones 3-6.

10. Un aparato que comprende medios para realizar:

recibir (315), en una interfaz, un contexto de autenticación que se asocia con un primer servicio;
provocar (317), al menos en parte, el almacenamiento del contexto de autenticación en una primera memoria caché que se asocia con la interfaz; y
provocar (319), al menos en parte, el llenado del contexto de autenticación en una segunda memoria caché que se asocia con un segundo servicio, la segunda memoria caché no se enlaza directamente a la interfaz,
en el que el contexto de autenticación en la segunda memoria caché autentica el acceso al segundo servicio; y
en el que el llenado del contexto de autenticación en la segunda memoria caché comprende:

convertir el contexto de autenticación que se basa, al menos en parte, en un protocolo de autenticación que se asocia con el segundo servicio,
en el que el contexto de autenticación en la segunda memoria caché es el contexto de autenticación convertido.

11. El aparato de la reivindicación 10, en el que cuando el contexto de autenticación se basa en cookies, el contexto de autenticación convertido se basa en token, y cuando el contexto de autenticación se basa en token, el contexto de autenticación convertido se basa en cookies.

12. El aparato de cualquiera de las reivindicaciones 10-11, en el que la interfaz comprende además, medios para realizar:

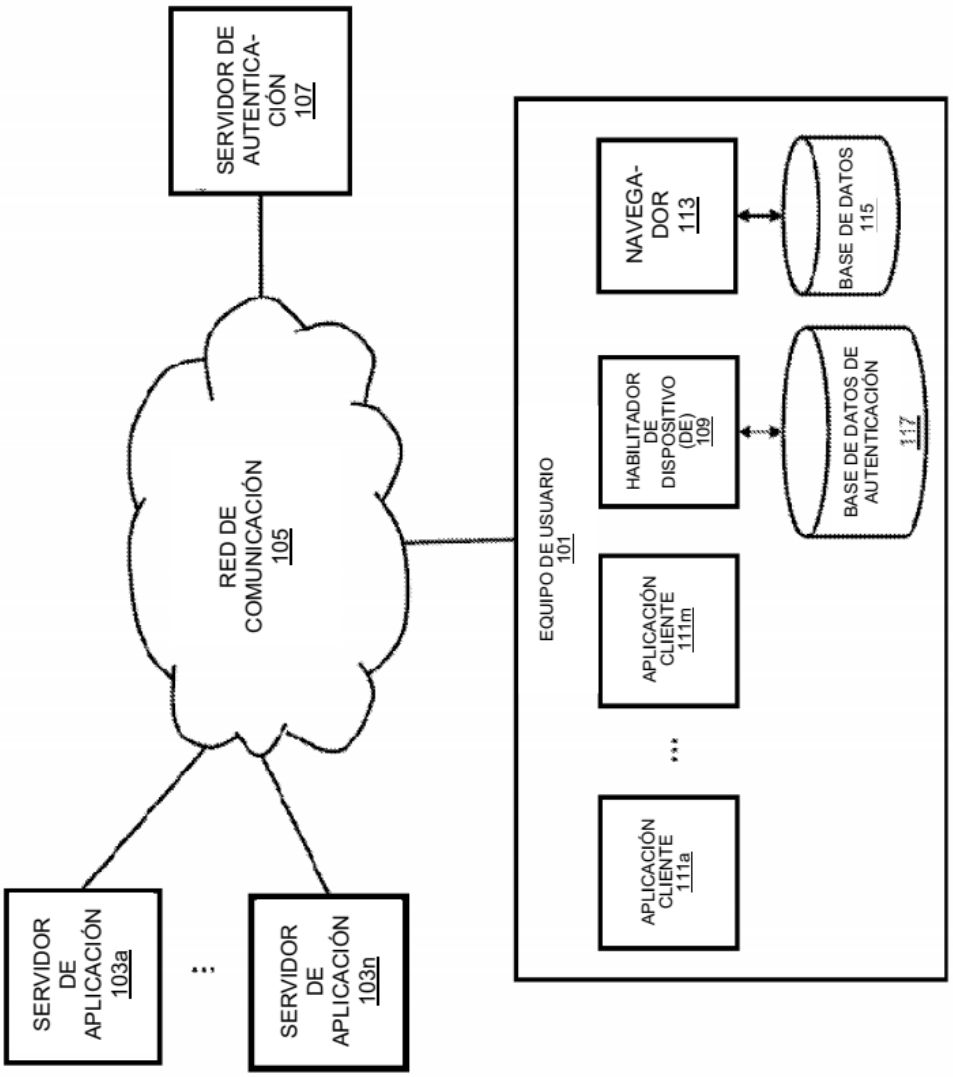
recibir (301), desde el primer servicio, una solicitud para autenticar a un usuario;
solicitar (309) credenciales de autenticación que se asocian con el usuario;
recibir (311) las credenciales de autenticación en base a la solicitud;
provocar (313), al menos en parte, la transmisión de las credenciales de autenticación a un servidor de autenticación,
en el que el contexto de autenticación se recibe desde el servidor de autenticación que se basa, al menos en parte, en las credenciales de autenticación.

13. El aparato de cualquiera de las reivindicaciones 10-12, en el que el contexto de autenticación es un contexto de autenticación de inicio único de sesión que se puede aplicar tanto al primer servicio como al segundo servicio.

14. El aparato de cualquiera de las reivindicaciones 10-13, en el que el primer servicio y el segundo servicio son aplicaciones de tiempo de ejecución que se ejecutan en un dispositivo común.

15. El aparato de cualquiera de las reivindicaciones 10-14, en el que al menos uno del primer servicio y el segundo servicio incluyen al menos uno de una aplicación, una sesión de navegador.

Figura 1


100
SERVIDOR DE AUTENTICA-CIÓN 107
RED DE COMUNICACIÓN 105
SERVIDOR DE APLICACIÓN 103a
SERVIDOR DE APLICACIÓN 103n
EQUIPO DE USUARIO 101
APLICACIÓN CLIENTE 111a
APLICACIÓN CLIENTE 111m
HABILITADOR DE DISPOSITIVO (DE) 109
NAVEGA-DOR 113
BASE DE DATOS DE AUTENTICACIÓN 117
BASE DE DATOS 115

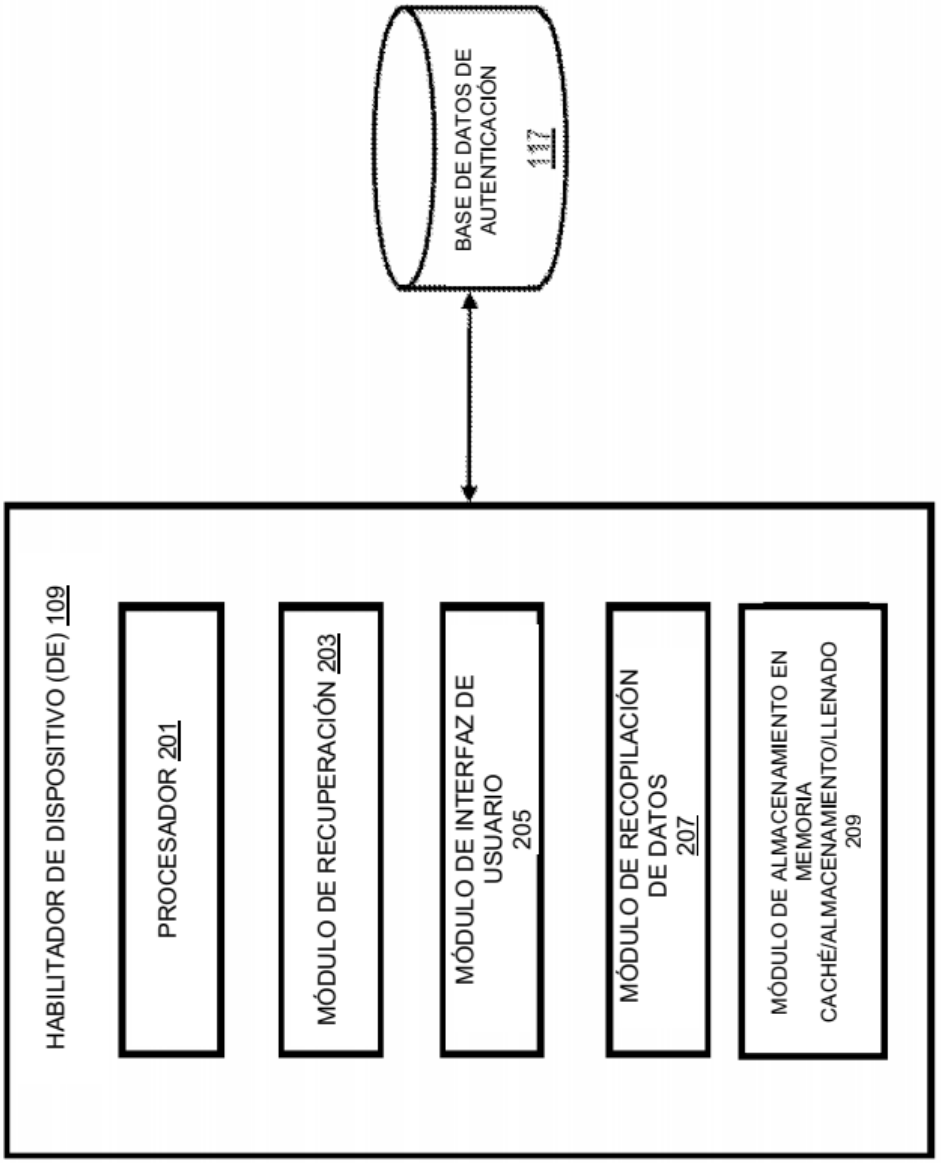
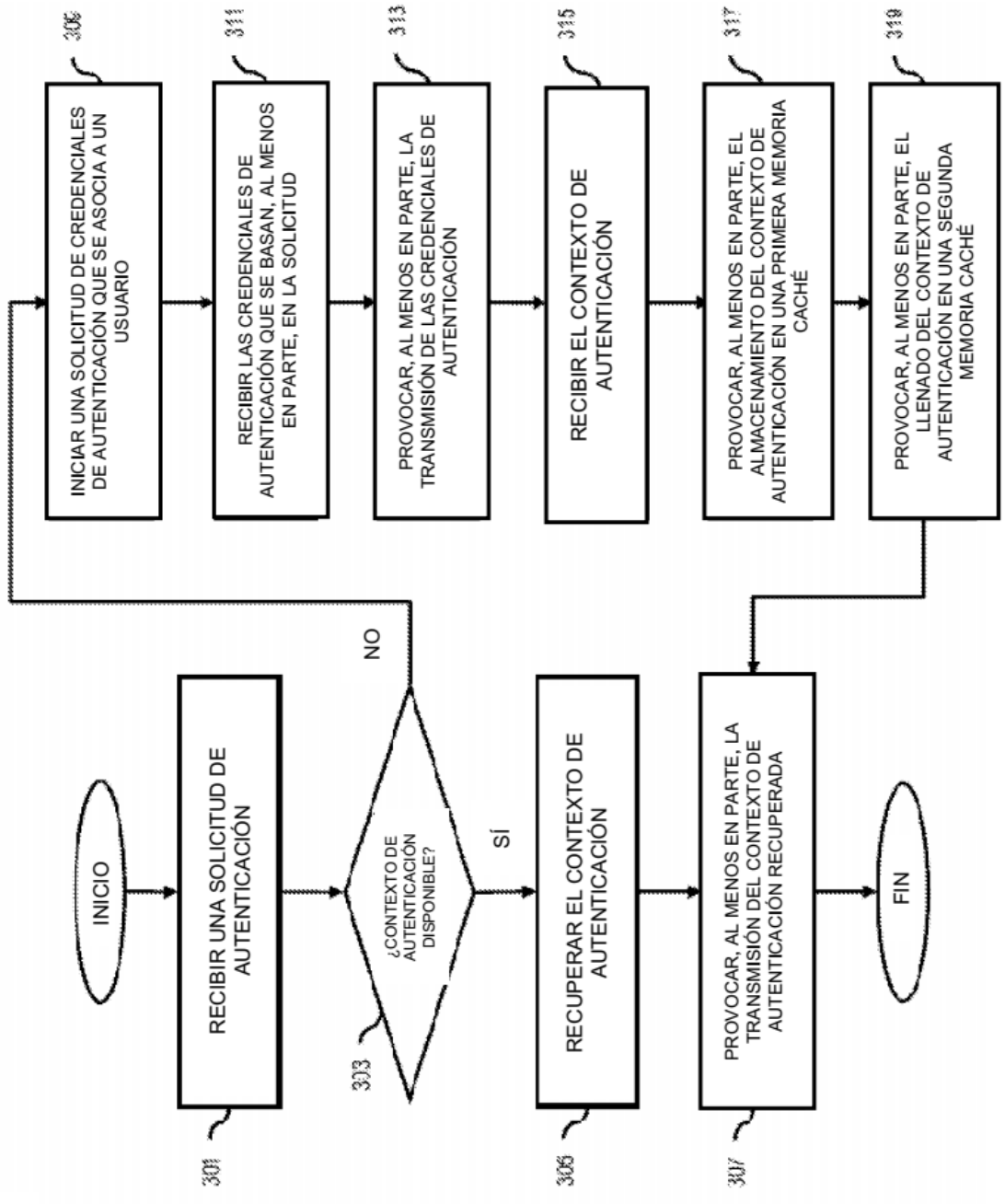

BASE DE DATOS DE AUTENTICACIÓN 117
HABILITADOR DE DISPOSITIVO (DE) 109
PROCESADOR 201
MÓDULO DE RECUPERACIÓN 203
MÓDULO DE INTERFAZ DE USUARIO 205
MÓDULO DE RECOPILACIÓN DE DATOS 207
MÓDULO DE ALMACENAMIENTO EN MEMORIA CACHÉ/ALMACENAMIENTO/LLENADO 209

Figura 2

Figura 3


300
INICIO
RECIBIR UNA SOLICITUD DE AUTENTICACIÓN
301
¿CONTEXTO DE AUTENTICACIÓN DISPONIBLE?
303
NO
SÍ
INICIAR UNA SOLICITUD DE CREDENCIALES DE AUTENTICACIÓN QUE SE ASOCIA A UN USUARIO
306
RECIBIR LAS CREDENCIALES DE AUTENTICACIÓN QUE SE BASAN, AL MENOS EN PARTE, EN LA SOLICITUD
311
PROVOCAR, AL MENOS EN PARTE, LA TRANSMISIÓN DE LAS CREDENCIALES DE AUTENTICACIÓN
313
RECIBIR EL CONTEXTO DE AUTENTICACIÓN
315
PROVOCAR, AL MENOS EN PARTE, EL ALMACENAMIENTO DEL CONTEXTO DE AUTENTICACIÓN EN UNA PRIMERA MEMORIA CACHÉ
317
PROVOCAR, AL MENOS EN PARTE, EL LLENADO DEL CONTEXTO DE AUTENTICACIÓN EN UNA SEGUNDA MEMORIA CACHÉ
319
RECUPERAR EL CONTEXTO DE AUTENTICACIÓN
305
PROVOCAR, AL MENOS EN PARTE, LA TRANSMISIÓN DEL CONTEXTO DE AUTENTICACIÓN RECUPERADA
307
FIN

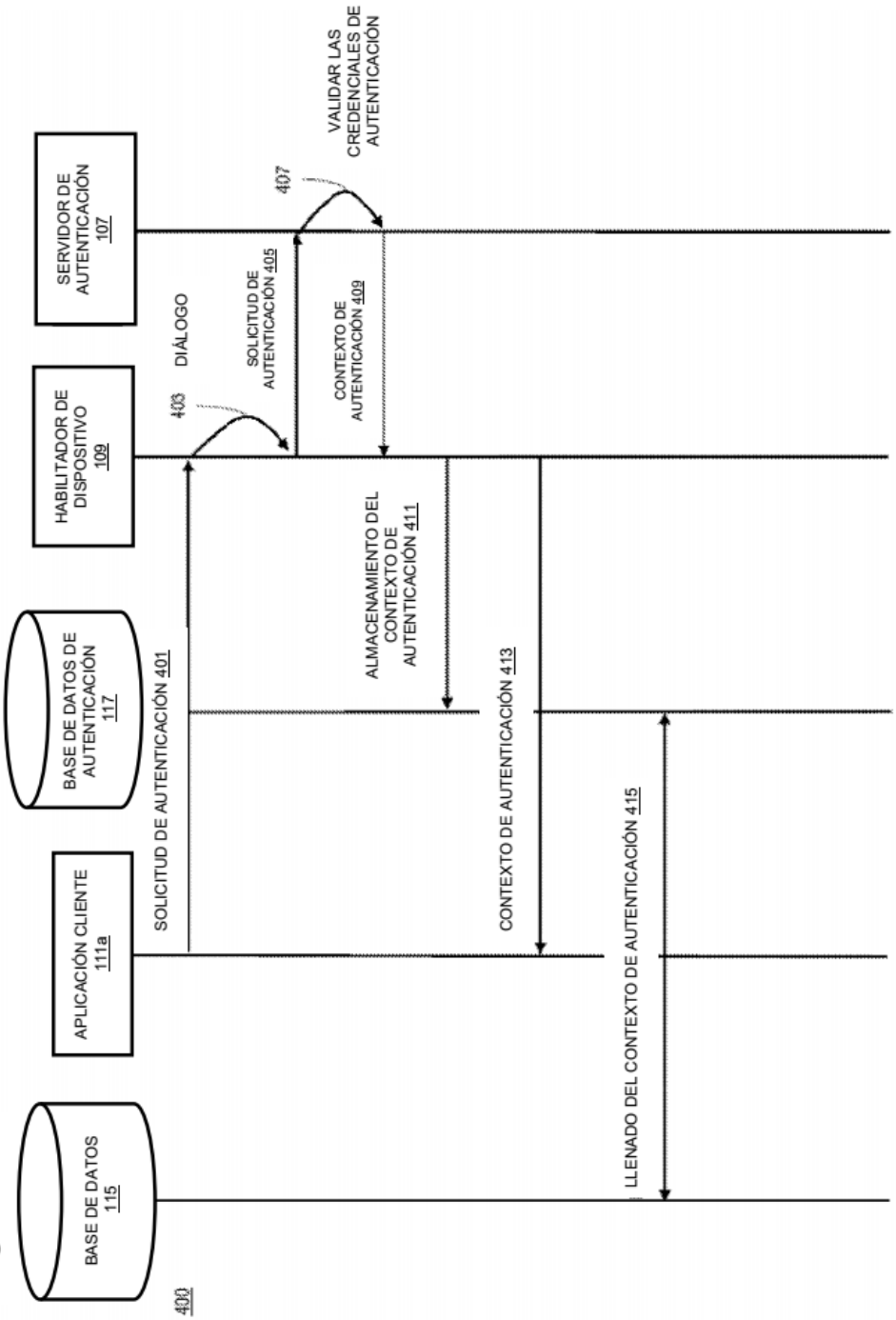

SERVIDOR DE AUTENTICACIÓN 107
HABILITADOR DE DISPOSITIVO 109
BASE DE DATOS DE AUTENTICACIÓN 117
APLICACIÓN CLIENTE 111a
BASE DE DATOS 115
400
403
DIÁLOGO
405
SOLICITUD DE AUTENTICACIÓN 405
407
VALIDAR LAS CREDENCIALES DE AUTENTICACIÓN
409
CONTEXTO DE AUTENTICACIÓN 409
411
ALMACENAMIENTO DEL CONTEXTO DE AUTENTICACIÓN 411
401
SOLICITUD DE AUTENTICACIÓN 401
413
CONTEXTO DE AUTENTICACIÓN 413
415
LLENADO DEL CONTEXTO DE AUTENTICACIÓN 415

Figura 4A

Figura 4B

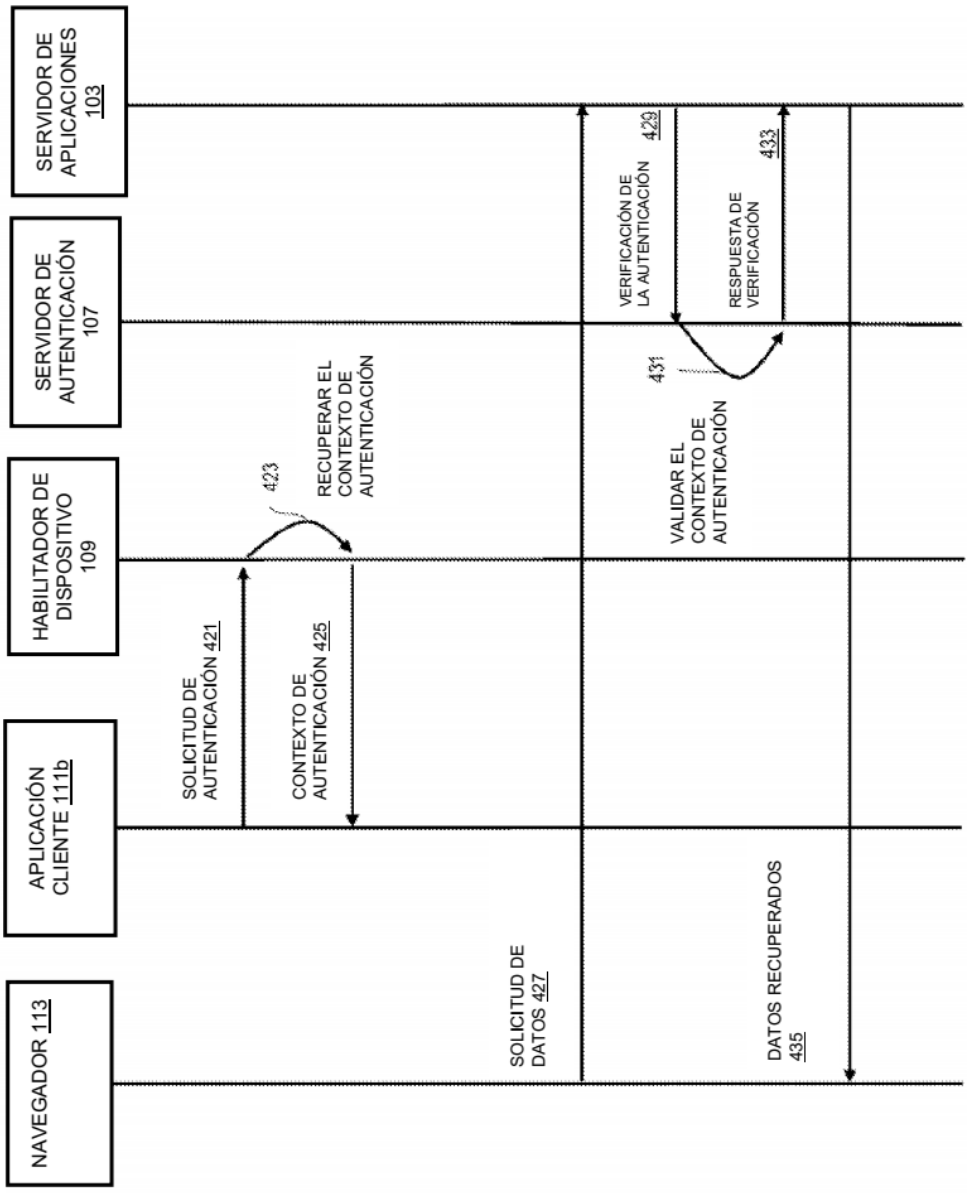
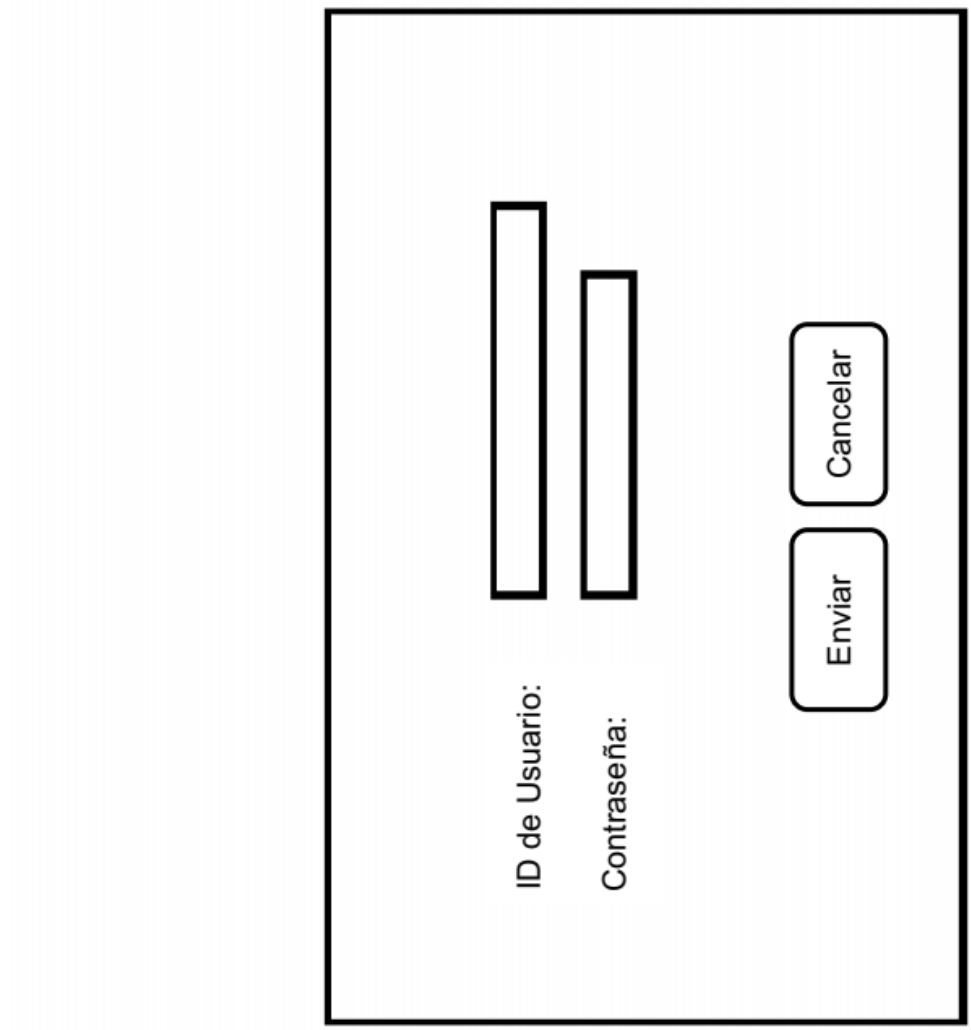

420
NAVEGADOR 113
APLICACIÓN CLIENTE 111b
HABILITADOR DE DISPOSITIVO 109
SERVIDOR DE AUTENTICACIÓN 107
SERVIDOR DE APLICACIONES 103
SOLICITUD DE AUTENTICACIÓN 421
423
RECUPERAR EL CONTEXTO DE AUTENTICACIÓN
CONTEXTO DE AUTENTICACIÓN 425
SOLICITUD DE DATOS 427
VERIFICACIÓN DE LA AUTENTICACIÓN 429
431
VALIDAR EL CONTEXTO DE AUTENTICACIÓN
RESPUESTA DE VERIFICACIÓN 433
DATOS RECUPERADOS 435

Figura 5



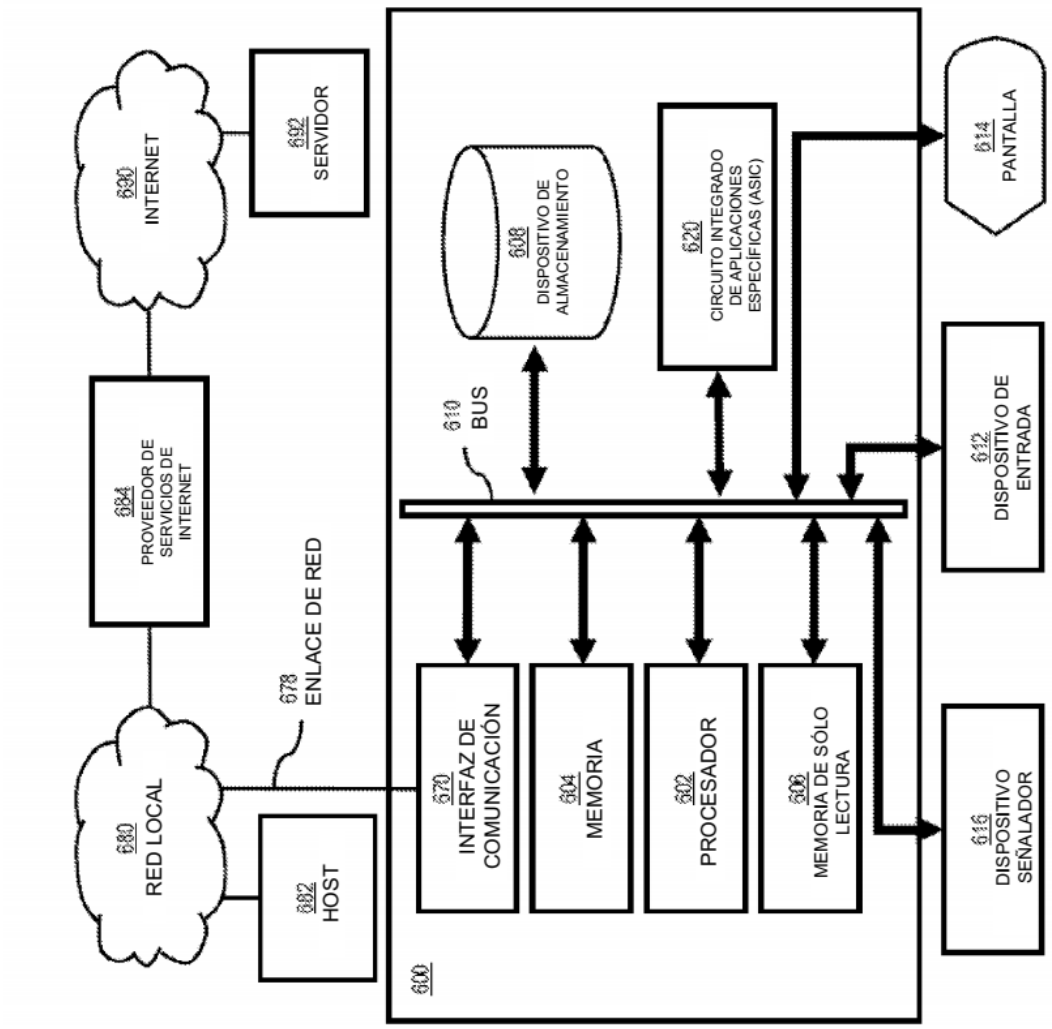

690 INTERNET
692 SERVIDOR
684 PROVEEDOR DE SERVICIOS DE INTERNET
678 ENLACE DE RED
680 RED LOCAL
682 HOST
600
670 INTERFAZ DE COMUNICACIÓN
604 MEMORIA
602 PROCESADOR
606 MEMORIA DE SÓLO LECTURA
610 BUS
608 DISPOSITIVO DE ALMACENAMIENTO
620 CIRCUITO INTEGRADO DE APLICACIONES ESPECÍFICAS (ASIC)
614 PANTALLA
612 DISPOSITIVO DE ENTRADA
616 DISPOSITIVO SEÑALADOR

Figura 6

Figura 7

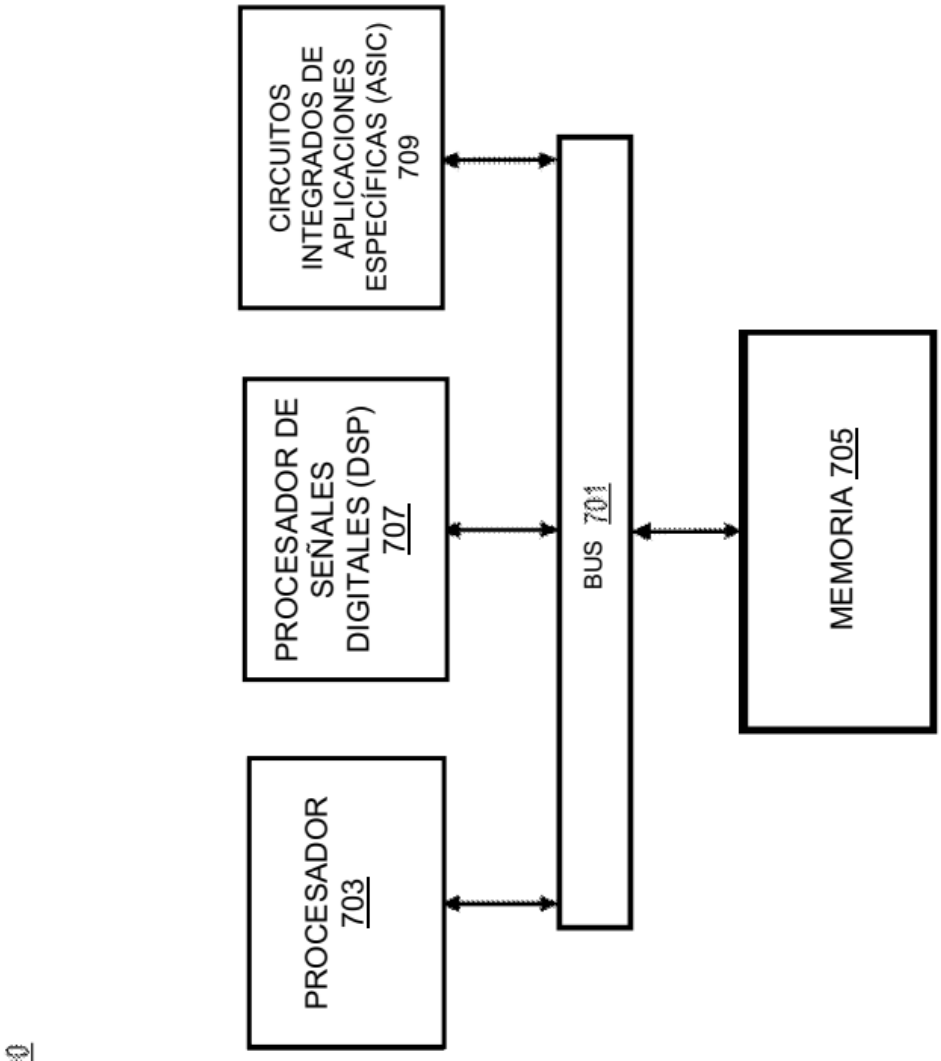
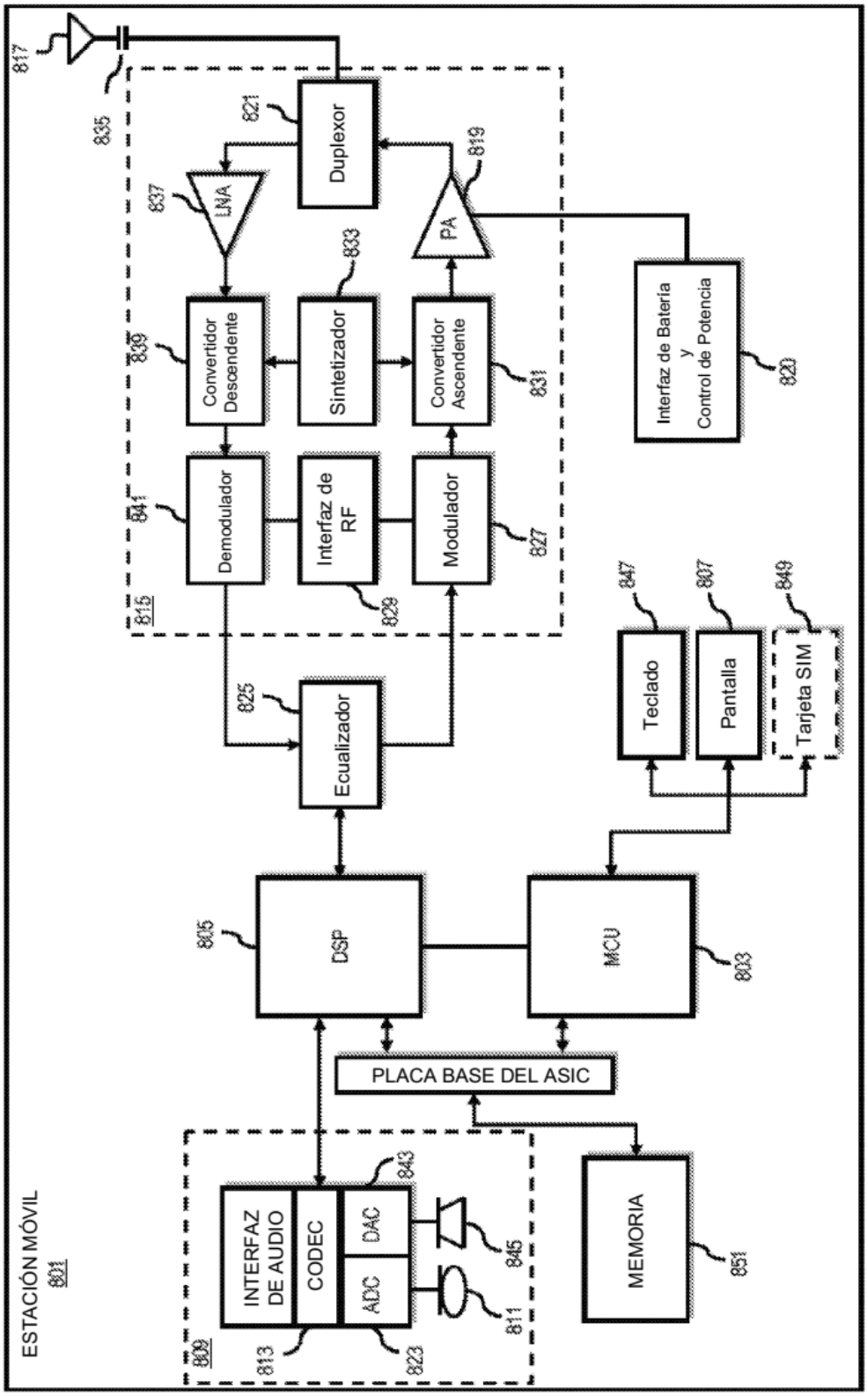

700
PROCESADOR 703
PROCESADOR DE SEÑALES DIGITALES (DSP) 707
CIRCUITOS INTEGRADOS DE APLICACIONES ESPECÍFICAS (ASIC) 709
BUS 701
MEMORIA 705

Figura 8


ESTACIÓN MÓVIL
801
817
835
Duplexor
821
819
LNA
837
PA
833
Convertidor Descendente
839
Sintetizador
Convertidor Ascendente
831
Interfaz de Batería y Control de Potencia
820
Demodulador
841
Interfaz de RF
828
Modulador
827
815
825
Ecualizador
847
Teclado
807
Pantalla
849
Tarjeta SIM
805
DSP
MCU
803
PLACA BASE DEL ASIC
INTERFAZ DE AUDIO
CODEC
DAC
ADC
843
845
811
813
823
809
MEMORIA
851