(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 701 873**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/33 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.08.2006 PCT/US2006/032156**

(87) Fecha y número de publicación internacional: **01.03.2007 WO07024626**

(96) Fecha de presentación y número de la solicitud europea: **16.08.2006 E 06813502 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 1917603**

(54) Título: **Servicio de inicio de sesión único distribuido**

(30) Prioridad:

22.08.2005 US 208509

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.02.2019

(73) Titular/es:

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

(72) Inventor/es:

ZHU, BIN;
CHEN, TIERUI y
LI, SHIPENG

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

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

Servicio de inicio de sesión único distribuido

Antecedentes

Los usuarios en línea suelen ser necesarios para mantener un conjunto de credenciales de autenticación (por ejemplo, un nombre de usuario y contraseña) para cada proveedor de servicios al que él o ella tiene derecho a acceder. Estos usuarios a menudo se enfrentan al dilema de usar diferentes credenciales de autenticación para cada proveedor de servicios individual a fin de mantener un alto nivel de seguridad, o usar las mismas credenciales de autenticación para los diversos proveedores de servicios, lo que resulta en un nivel de seguridad disminuido. Con frecuencia, este último es elegido sobre el primero, ya que es difícil memorizar y mantener numerosas credenciales de autenticación. Además, aparte de las implicaciones de seguridad, exigir a los usuarios que ingresen credenciales de autenticación cada vez que sea necesario el acceso a un proveedor de servicios es un procedimiento generalmente incómodo y lento.

Se han propuesto varias tecnologías convencionales para aliviar o eliminar la necesidad de mantener varios conjuntos de credenciales de autenticación que permiten acceder a diversos servicios en línea. Una de estas tecnologías utiliza una gestión de credenciales centralizada que proporciona servicios de autenticación para los proveedores de servicios participantes. Después de que un usuario establece inicialmente una relación y se autentica con la administración centralizada de credenciales, la administración centralizada de credenciales administra el proceso de autenticación cuando el usuario posteriormente solicita acceso a cualquiera de los proveedores de servicios participantes. Esta tecnología reduce significativamente la complejidad de tener que solicitar el acceso de numerosos proveedores de servicios. La administración de credenciales centralizada maneja de manera transparente los detalles de la autenticación con varios proveedores de servicios participantes, mientras se mantiene un alto nivel de seguridad del usuario.

Las actuales tecnologías de administración de credenciales centralizadas convencionales no son adecuadas para todos los entornos en línea. Una tecnología de administración de credenciales centralizada convencional requiere que un usuario se autentique con un servidor de autenticación. Después de la autenticación, el servidor de autenticación emite un ticket de autenticación al usuario. El usuario utiliza el ticket de autenticación para obtener acceso a un servidor que emite tickets de acceso al servicio. El servidor emitirá un ticket de acceso de servicio al usuario si el ticket de autenticación es válido. El usuario puede usar el ticket de acceso al servicio para obtener acceso a un proveedor de servicios.

La tecnología de gestión de credencial centralizada convencional descrita proporciona la funcionalidad de acceso seguro si los proveedores de servicios se mantienen de forma centralizada. Sin embargo, el acceso seguro a los proveedores de servicios se ve comprometido si los proveedores de servicios forman parte de una red que tiene numerosos usuarios/entidades dispares, como Internet.

Otra tecnología de autenticación convencional utiliza una base de datos centralizada que contiene usuarios registrados y sus credenciales de autenticación asociados. Cada uno de los usuarios registrados tiene un número de identificación único de 64 bits. Esta tecnología de autenticación convencional también asigna a cada proveedor de servicios participante una ID única. Estas ID únicas también se guardan en una base de datos centralizada. Los proveedores de servicios participantes acuerdan implementar un componente de servidor que facilite la comunicación segura con una entidad que administra las bases de datos centralizadas. Cuando un usuario registrado intenta autenticarse con un proveedor de servicios participante, el usuario se redirige de forma transparente a la entidad administradora para facilitar la autenticación. La ruta de comunicación segura implementada entre el proveedor de servicios participante y la entidad administradora ayuda a garantizar la solicitud de autenticación concedida.

La tecnología de autenticación que se discutió anteriormente proporciona autenticación segura basada en la Web. Sin embargo, la tecnología de Internet no ha sido ampliamente adoptada. Esto se debe principalmente a la característica de diseño de base de datos centralizada de la tecnología. Algunos proveedores de servicios no aprueban la tecnología porque se utilizan bases de datos centrales. En particular, un proveedor de servicios debe confiar en una entidad que administra las bases de datos centralizadas para garantizar la autenticación exitosa del usuario. Si la entidad experimenta dificultades técnicas, la autenticación del usuario puede verse interrumpida. Esta posibilidad de interrupción, que no es controlable por el proveedor de servicios, puede ser un riesgo que el proveedor de servicios no está dispuesto a asumir. Además, el uso de bases de datos centralizadas hace que la tecnología de autenticación sea especialmente propensa a los ataques de hackers y malware.

WILLIAM JOSEPHSON ET AL: "Autenticación de igual a igual con un servicio de inicio de sesión único distribuido", TALLER INTERNACIONAL SOBRE SISTEMAS DE PEER-A-PEER, XX, XX, 26 de febrero de 2004 (2004-02-26), páginas 1-6, XP002425458 revela un procedimiento para la autenticación de igual a igual con un servicio de inicio de sesión único distribuido. Los servidores de aplicaciones delegan la verificación de la identificación del cliente a combinaciones de servidores de autenticación. El servidor de aplicaciones *S*, a través de su política de autenticación, especifica qué subconjuntos de los servidores de autenticación deben trabajar juntos para verificar la

identidad de un usuario para que S confíe en el resultado. Los servidores de autenticación crean firmas parciales que, solo cuando *t* se combinan utilizando criptografía de umbral, producen una declaración firmada por k_i. Además, esa firma es verificada por el servidor de aplicaciones *S*, porque la K_i pública correspondiente se envía a *S*.

Por lo tanto, el objetivo de la presente invención es proporcionar un procedimiento mejorado para otorgar comunicaciones autenticadas y los artículos de fabricación correspondientes para el proveedor de servicios y el servidor de autenticación, y un dispositivo informático correspondiente para el proveedor de servicios.

Este objeto es resuelto por el tema de las reivindicaciones independientes.

Las realizaciones de la invención se definen en las reivindicaciones dependientes.

Sumario

Las implementaciones descritas en este documento se refieren al establecimiento de una comunicación autenticada entre un dispositivo informático cliente y un proveedor de servicios. La comunicación es posible sin el uso de una autoridad confiable que guarda secretos de un dispositivo informático cliente y un proveedor de servicios.

Después de un proceso de registro, un dispositivo informático cliente utiliza los servidores de autenticación para solicitar la comunicación autenticada con un proveedor de servicios. El dispositivo informático del cliente puede usar cualquier conjunto de una pluralidad de servidores de autenticación con los que está registrado, donde el número de servidores en el conjunto es grande o igual a un valor umbral, para solicitar una comunicación autenticada con un proveedor de servicios. El proveedor de servicios también debe estar registrado con los servidores de autenticación que el dispositivo informático del cliente puede usar para establecer una comunicación autenticada.

Un cliente de dispositivo informático puede enviar un proveedor de servicios una solicitud de autenticación que incluye su identificador ID único y un testigo de autenticación cifrado que incluye la ID de identificador único, una dirección de red como la dirección IP del dispositivo y un nonce (clave de un solo uso). El testigo de autenticación cifrado se recibió en una comunicación anterior con los servidores de autenticación. Cada servidor de autenticación usó una clave dividida, obtenida del proveedor de servicios con el que el dispositivo informático del cliente está deseando una comunicación autenticada, para cifrar y generar un testigo de autenticación parcial. El proveedor de servicios utiliza una clave secreta no revelada para descifrar el testigo de autenticación, exponiendo así la información de autenticación cifrada. Esta información, junto con la ID de identificador único enviado, es utilizada por el proveedor del servicio para decidir si se autorizará la comunicación autenticada.

Este sumario se proporciona para introducir una selección de conceptos en una forma simplificada que se describen más adelante en la descripción detallada. Este sumario no tiene la intención de identificar características clave o características esenciales de la materia reclamada, ni pretende ser utilizado como una ayuda para determinar el alcance de la materia reclamada.

Breve descripción de los dibujos

Se describen realizaciones no limitantes y no exhaustivas con referencia a las siguientes figuras, en las que números de referencia se refieren a partes similares en todas las diversas vistas a menos que se especifique lo contrario.

La figura 1 ilustra una implementación ejemplar de un entorno de red informática que incluye varios dispositivos informáticos del cliente que pueden comunicarse con uno o más proveedores de servicios.
La figura 2 ilustra una implementación ejemplar en la que un dispositivo cliente solicita una comunicación autenticada con un proveedor de servicios utilizando un procedimiento de acceso de proveedores de servicios de dispositivos cliente.
La figura 3 ilustra una implementación ejemplar en la que un proveedor de servicios se registra con un servidor de autenticación utilizando un procedimiento de registro de proveedor de servicios.
La figura 4 ilustra una implementación ejemplar en la que un dispositivo informático cliente se registra con un servidor de autenticación utilizando un procedimiento de registro de dispositivo cliente.
La figura 5 ilustra una implementación ejemplar en la que un dispositivo informático cliente se autentica con el servidor de autenticación utilizando un procedimiento de registro de dispositivo informático cliente.
La figura 6 es un dispositivo informático ilustrativo que se puede usar para implementar un proveedor de servicios.
La figura 7 es un dispositivo informático ilustrativo que se puede usar para implementar un dispositivo informático cliente.
La figura 8 es un dispositivo informático ilustrativo que se puede usar para implementar un servidor de autenticación.

Descripción detallada

Visión de conjunto

Se describen los sistemas y procedimientos para la autenticación con un proveedor de servicios. A continuación, se proporciona una amplia discusión de los procedimientos utilizados entre el cliente, el proveedor de servicios y los dispositivos de autenticación para establecer una comunicación autenticada entre un dispositivo informático del cliente y un dispositivo proveedor de servicios. Esta discusión hará uso de un entorno ejemplar ilustrado en la figura 1. Implementaciones ejemplares de diversos procedimientos utilizados entre varios dispositivos se describen a continuación con más detalle. En particular, se proporciona una explicación detallada de un procedimiento utilizado por un dispositivo informático cliente para obtener acceso autenticado a un proveedor de servicios junto con la figura 2; junto con la figura 3, se proporciona una discusión detallada de un procedimiento de registro del proveedor de servicios con un servidor de autenticación; junto con la figura 4 se proporciona una discusión detallada de un procedimiento de registro de dispositivo informático del cliente con un servidor de autenticación; y una discusión detallada de un procedimiento de autenticación del dispositivo informático del cliente con un servidor de autenticación se proporciona junto con la figura 5. Finalmente, las implementaciones ejemplares de un proveedor de servicios, dispositivo informático cliente y servidor de autenticación se discuten en conjunto con las figuras 6 - 8, respectivamente.

Entorno ejemplar

La figura 1 ilustra una implementación ejemplar de un entorno de red informática 100 que incluye varios dispositivos 102(1) - 102(n) informáticos cliente que pueden comunicarse con uno o más proveedores de servicios 104(1) - 104(n). La comunicación bidireccional entre los dispositivos 102(1) - 102(n) informáticos cliente y los proveedores 104(1) - 104(n) de servicios se facilita con una red 120 (por ejemplo, Internet). Los servidores 106(1) - 106(n) de autenticación también están interconectados con la red 120. Uno o más servidores 106 de autenticación trabajan juntos para proporcionar servicios de autenticación a los dispositivos 102(1) - 102(n) informáticos cliente y a los proveedores 104(1) - 104(n) de servicios. Cada servidor de autenticación tiene generalmente la misma funcionalidad que otro servidor de autenticación.

En cualquier momento dado, uno de los varios dispositivos 102(1) - 102(n) informáticos cliente, tales como el dispositivo 102(1) informático cliente, puede requerir los servicios proporcionados por uno de los proveedores 104(1) - 104(n) de servicios, como el proveedor 104(1) de servicios. Un subconjunto de los servidores 106(1) - 106(n) de autenticación proporciona tecnología que permite que el dispositivo 102(1) informático cliente se autentique correctamente con el proveedor 104(1) de servicios. El proveedor 104(1) de servicios generalmente no proporcionará servicios a ninguno de los dispositivos 102(1) - 102(n) informáticos cliente hasta que se logre la autenticación adecuada.

El proveedor 104(1) de servicios y el dispositivo 102(1) informático cliente, cada una a establecer una relación con los servidores 106(1) - 106(n) de autenticación antes de solicitar los servicios de autenticación de los servidores 106(1) - 106(n). Después de que el proveedor 104(1) de servicios establece contacto inicial con los servidores 106(1) -106(n) de autenticación, se proporciona un módulo 130 de servidor al proveedor 104(1) de servicios. Este módulo 130 de servidor proporciona los parámetros operativos que el proveedor 104(1) de servicios necesitará durante una fase de registro de la relación. El módulo 130 de servidor puede almacenarse directamente en una memoria, volátil o no volátil, del proveedor 104(1) de servicios. Si el proveedor 104(1) de servicios comprende varios servidores (por ejemplo, una comunidad de servidores), el módulo 130 de servidor puede almacenarse en uno de esos servidores múltiples.

Después de obtener el módulo 130 de servidor, el proveedor 104(1) de servicios crea una clave de cifrado secreta y una clave de descifrado secreta correspondiente. La clave de cifrado secreta se divide para crear claves adicionales. En una implementación, la clave secreta se divide utilizando un esquema de umbral. Sin embargo, también se pueden usar otros esquemas de división. Una clave dividida se envía de forma segura a cada servidor de autenticación, tal como 106(1) con una ID única que identifica al proveedor 104(1) de servicios. El servidor 106(1) de autenticación envía una respuesta exitosa al proveedor 104(1) de servicios después de recibir la clave dividida y la ID exclusiva del proveedor de servicios. La clave de descifrado secreta permanece en el proveedor 104(1) de servicios y nunca se hace pública a ninguna otra entidad, como el servidor 106(1) de autenticación. El módulo 130 de servidor proporciona las rutinas para crear las claves secretas y dividir la clave de cifrado secreta.

El dispositivo 102(1) informático cliente recibe un módulo 140 cliente. El módulo 140 cliente puede ser un módulo de complemento de navegador web que se integra con un navegador web del dispositivo 102(1) informático cliente. El módulo 140 cliente proporciona los parámetros operativos requeridos durante un procedimiento de registro de relaciones realizado entre el dispositivo 102(1) informático cliente y cada servidor 106(i) de autenticación. El módulo 140 cliente puede almacenarse directamente en una memoria, volátil o no volátil, del dispositivo 102(1) informático cliente.

Después de obtener el módulo 140 cliente, el dispositivo 102(1) informático cliente puede proceder a registrarse con cada servidor 106(i) de autenticación. Esto se debe hacer antes de que el módulo 140 cliente solicite servicios de uno o más de los proveedores 104(1) - 104(n) de servicios. El proceso de registro entre el módulo 140 cliente y un servidor 106(i) de autenticación implica el uso del módulo 140 cliente. Un usuario del dispositivo 102(1) informático cliente utiliza el módulo 140 cliente, a través de una interfaz de usuario como un navegador web asociado, para ingresar un nombre de usuario única y una contraseña. El módulo 140 cliente genera un identificador de cliente

único a partir del nombre de usuario única. El módulo 140 cliente también genera una clave de autenticación de cliente para que el cliente se autentique en un servidor 106(i) de autenticación a partir del nombre de usuario única, la contraseña y una identificación del servidor de autenticación que se recibió con el módulo 140 cliente. Se puede usar una función de dispersión para crear la clave de autenticación del cliente. El módulo 140 cliente envía la clave de autenticación del cliente y el identificador del cliente de forma segura a un servidor 106(i) de autenticación. Después de recibir y conservar el identificador del cliente y la clave de autenticación del cliente, el servidor 106(i) enviará un mensaje de éxito al dispositivo 102(1) informático cliente.

Después de registrarse con cada servidor 106(i) de autenticación, el dispositivo 102(1) informático cliente puede usar un subconjunto de los servidores 106(1) - 106(n) de autenticación de establecer comunicación autenticada con uno de los proveedores 104(1) - 104(n) de servicios que ya ha establecido una relación con los servidores 106(1) - 106(n) de autenticación.

Antes de solicitar la comunicación autenticada con uno de los proveedores de servicios 104(1) - 104(n), el dispositivo 102(1) informático cliente autenticará con un subconjunto de los servidores 106(1) - 106(n) de autenticación, que proporcionará servicios de autenticación al dispositivo informático del cliente. Este procedimiento de autenticación establece las claves de sesión utilizadas por el dispositivo 102(1) informático cliente y el subconjunto del servidor 106(1) - 106(n) de autenticación para comunicaciones confidenciales posteriores.

Para autenticar, a un usuario del dispositivo 102(1) informático cliente envía cada servidor 106(i) de autenticación en el subconjunto una solicitud de autenticación. La solicitud de autenticación y el establecimiento de una clave de sesión se facilitan utilizando el módulo 140 del cliente. Cada servidor 106(i) de autenticación responde a una solicitud de autenticación enviando un nonce al dispositivo 102(1) informático cliente. El dispositivo 102(1) informático cliente, en respuesta, envía al servidor 106(i) de autenticación el identificador del cliente y el nonce recibidos cifrado mediante la clave de autenticación del cliente al servidor 106(i) de autenticación. El cifrado también incluye un número aleatorio de dispositivo de cliente y un nonce de dispositivo de cliente. El módulo 140 del cliente genera el número aleatorio del dispositivo cliente y el dispositivo cliente. El identificador del cliente y la clave de autenticación del cliente se crearon durante el proceso de registro descrito anteriormente.

El servidor 106(i) de autenticación utiliza el identificador de cliente para recuperar la clave de autenticación de cliente que se creó durante el proceso de registro. La clave de autenticación del cliente recuperada se utiliza para descifrar el nonce del servidor de autenticación cifrado, el número aleatorio del dispositivo del cliente y el nonce del dispositivo del cliente. Si el descifrado es exitoso y el nonce del servidor de autenticación descifrado coincide con el nonce enviado al cliente por el servidor de autenticación en un proceso anterior, el servidor 106(i) de autenticación envía al cliente 102(1) un cifrado que incluye un servidor de autenticación que genera un número aleatorio en el servidor 106, el nonce y el nonce del dispositivo del cliente. En este punto, tanto el servidor 106 como el cliente 102(1) poseen los dos números aleatorios. El servidor 106(i) y el cliente 102(1) utilizan una función de dispersión en los dos números aleatorios para crear una clave de sesión en ambos extremos. Esta clave de sesión se utiliza para establecer un enlace seguro entre el dispositivo 102(1) informático cliente y el servidor 106(i) de autenticación cuando el dispositivo 102(1) informático cliente utiliza el servidor 106(i) de autenticación en el subconjunto de la autenticación elegida servidores para establecer comunicación autenticada con uno de los proveedores 104(1) - 104(n) de servicios.

Después de obtener una clave de sesión desde el servidor 106(i) de autenticación, el dispositivo 102(1) cliente está listo para solicitar la comunicación autenticada con un proveedor de servicios ya registrado con los servidores 106(1) - 106(n) de autenticación (por ejemplo, el proveedor 104(1) de servicios). Esta solicitud comienza en el punto en que el dispositivo 102(1) informático cliente envía una solicitud de acceso al proveedor 104(1) de servicios. El proveedor 104(1) de servicios responde enviando su ID única y un desafío (por ejemplo, un nonce del proveedor de servicios) al dispositivo 102(1) informático cliente. Opcionalmente, el proveedor 104(1) de servicios puede enviar una lista de servidores de autenticación con los que ya se ha registrado en el dispositivo 102(1) informático cliente para que el cliente pueda solicitar servicios de autenticación de esos servidores. Si el cliente no se ha autenticado con los servidores de autenticación en la lista, el cliente se autentica con los servidores de autenticación en la lista y establece una clave de sesión para la posterior comunicación confidencial con cada uno de esos servidores de autenticación.

El dispositivo 102(1) informático cliente ya está listo para ponerse en contacto con cada uno de los servidores de autenticación en el subconjunto de servidores de autenticación, por ejemplo, la autenticación del servidor 106(i), para establecer la comunicación autenticada con el proveedor 104(1) de servicios. El dispositivo 102(1) informático cliente envía a cada servidor 106(i) de autenticación la ID única del proveedor de servicios y el nonce del proveedor de servicios. Opcionalmente, el dispositivo 102(1) informático cliente también puede enviar su propio identificador de cliente al proveedor 104(1) de servicio de autenticación. El servidor 106(i) de autenticación también debe tener el identificador del cliente del dispositivo 102(1) informático cliente y la clave de sesión guardada en la memoria de comunicaciones anteriores entre los dos dispositivos.

El servidor 106(i) de autenticación encripta el identificador de cliente, una dirección de red tal como una dirección IP del dispositivo 102(1) informático cliente, y el nonce del proveedor de servicios utilizando la clave de división recibida previamente del proveedor 104(1) de servicios. Este proceso crea un testigo de autenticación parcial que se pasa al

dispositivo 102(1) informático cliente. El dispositivo 102(1) informático cliente crea un testigo de autenticación a partir de los testigos de autenticación parciales recibidos y empaqueta el testigo de autenticación con su propio identificador de cliente y envía el paquete al proveedor 104(1) de servicios. El proveedor 104(1) de servicios intentará descifrar el testigo de autenticación cifrado utilizando su clave de descifrado secreta. Si el descifrado es exitoso y el nonce descifrado coincide con el nonce enviado al cliente en una comunicación autenticada anterior, la comunicación autenticada es exitosa y se otorga acceso al servicio del proveedor del servicio. El proveedor 104(1) de servicios notifica al dispositivo 102(1) informático cliente si se otorga la comunicación autenticada.

Las ventajas del procedimiento de autenticación discutido son al menos las siguientes. Las claves secretas de un proveedor de servicios solo son conocidas por el proveedor. Ciertamente, los servidores de autenticación no conocen las claves secretas y obtener la clave secreta de un proveedor de servicios generalmente solo es posible si ocurriera una colusión significativa entre varios servidores de autenticación. En el lado del dispositivo informático del cliente, la contraseña de un usuario nunca se usa directamente durante el proceso de autenticación. De hecho, cada entidad en el proceso de autenticación, los dispositivos informáticos del cliente y los proveedores de servicios controlan sus propios secretos. Esto hace que el procedimiento de autenticación descrito aquí sea muy atractivo, ya que no se requiere la existencia de una autoridad confiable. Las autoridades confiables se utilizan con muchas otras tecnologías de encriptación/autenticación (por ejemplo, PKI).

Acceso del dispositivo cliente al procedimiento del proveedor de servicios

La figura 2 ilustra una implementación ejemplar en la que el dispositivo 102(1) cliente solicita una comunicación autenticada con el proveedor 104(1) de servicios utilizando un procedimiento 200 de acceso al proveedor de servicios del dispositivo cliente. La comunicación autenticada se facilita utilizando un subconjunto de los servidores 106(1) - 106 (n) de autenticación. Una tabla I proporciona detalles relacionados con las notaciones utilizadas en el texto que sigue.

Tabla I

S	Un proveedor de servicios participante.
U	Un dispositivo cliente participante.
A_i	El i-ésimo servidor de autenticación.
UID	Una ID de cliente única para un U participante.
SID	Una ID de proveedor de servicios única para un proveedor de servicios participante S.
AID_i	Una ID única para el i-ésimo servidor de autenticación A_i.
K_S	Una clave de cifrado secreta generada por y conocida solo por S.
K_S^{-1}	Una clave de descifrado secreta correspondiente a K_S y conocida solo por S.
K_S^i	La i-ésima parte parcial de K_S generada por un esquema de umbral.
K_U^i	Una clave de cliente secreta para que U se autentique en el i-ésimo servidor de autenticación A_i.
p_1, p_2	Dos enteros primos correctamente seleccionados, $p_2 > p_1$.
g	Un generador en $Z_{p_1}^*$, $2 \le g \le p_1 - 2$.
$SK_{U, Ai}$	Una clave de sesión entre un usuario U y el i-ésimo servidor de autenticación A_i.
$<m>_k$	Un mensaje m cifrado por un cifrado simétrico con una clave k.
$<m>^{k,p}$	Significa $m^k \bmod p$ donde $m \in Z_p$.

n_X nonce generado por la entidad *X*.

r_X Un número aleatorio generado por la entidad *X*.

[*x*] *x* es opcional en la descripción de un protocolo. Los corchetes indican parámetros opcionales a lo largo de la descripción.

El procedimiento comienza cuando el dispositivo 102(1) informático cliente envía el proveedor 104(1) de servicios una solicitud de acceso en una comunicación 201. El proveedor 104(1) de servicios responde en una comunicación 202 con *SID,* n_S, [$< g >^{r_S, p1}$], [una lista de *t* servidores de autenticación {A_{df}, $1 \leq f \leq t$}], donde *t* es el umbral para la cantidad de servidores de autenticación necesarios para proporcionar servicios de autenticación. Una vez que se recibe la comunicación 202, el dispositivo 102(1) informático cliente envía *SID,* n_S, [$< g >^{r_U, p1}$], [*UID*] al servidor 106 de autenticación en una comunicación 204. El servidor 106 de autentificación responde enviando $< UID, U, n_S, [< g >^{r_U, p_1}] >^{K_S^d, p_2}$ en una comunicación 206, donde *U* es el identificador de red del dispositivo 102(1) informático cliente, como la dirección IP del cliente (*Dirección IP*). El contenido de la comunicación 206 define un testigo de autenticación parcial. El dispositivo 102(1) informático cliente utiliza los testigos de autenticación parcial recibidos en la comunicación 206 con los servidores de autenticación para crear un testigo de autenticación < *UID, U,* n_S, [$< g >^{r_U, p1}$]> $^{K_S, p2}$ que se empaqueta junto con *UID* y [$< n_S >_k$] y se envía al proveedor de servicios 104(1), donde $k = < g >^{r_S \cdot r_U, p1}$. El proveedor 104(1) de servicios utiliza su clave de descifrado secreta K_S^{-1} para descifrar el testigo de autenticación cifrado, donde

$$((UID, U, n_S, [< g >^{r_U, p_1}])^{K_S})^{K_S^{-1}} = (UID, U, n_S, [< g >^{r_U, p_1}]) \bmod p_2 .$$

De acuerdo con el descifrado anterior y la información adicional recibida con el testigo de autenticación, el proveedor 104(1) de servicios enviará una respuesta de acceso al dispositivo 102(1) informático cliente en una comunicación 210 indicando si se otorga el acceso autenticado. El uso opcional de un generador (g) en $Z_{p_1}^*$ durante la comunicación autenticada proporciona una manera de generar una clave de sesión que se utiliza para la comunicación segura posterior entre el dispositivo 102(1) informático cliente y el proveedor 104(1) de servicios después de que se establece la sesión autenticada.

Las comunicaciones 204 y 206 son seguras usando una clave de sesión establecida entre el dispositivo 102(1) informático cliente y un servidor 106(i) de autenticación. El dispositivo 102(1) informático cliente y el servidor 106(i) de autenticación están en posesión de la clave de sesión. Los detalles de la creación de dicha clave de sesión se describen más adelante.

Las diversas comunicaciones discutidas se facilitan utilizando los módulos 140 y 130 de cliente y de servidor. Sin embargo, las diversas comunicaciones e instrucciones pueden llevarse a cabo por cualquier dispositivo habilitado para llevar a cabo dichas comunicaciones e instrucciones, proporcionando así el acceso del dispositivo cliente descrito al procedimiento del proveedor de servicios.

Procedimiento de registro del proveedor de servicios

La figura 3 ilustra una implementación ejemplar en la que el proveedor 104(1) de servicios se registra en el servidor 106(i) de autenticación utilizando un procedimiento 300 de registro de proveedores de servicios. El procedimiento 300 de registro del proveedor de servicios se lleva a cabo antes de que un proveedor de servicios pueda beneficiarse de los servicios de autenticación ofrecidos por un servidor de autenticación. La tabla I anterior proporciona detalles relacionados con las notaciones utilizadas en el texto que sigue.

Antes de que el procedimiento se inicie, el proveedor 104(1) de servicio descarga e instala un módulo 130 de servidor. El módulo 130 de servidor en esta implementación proporciona la funcionalidad que permite al proveedor 104(1) de servicios procesar solicitudes y comunicaciones relacionadas con la autenticación hacia y desde el servidor 106(i) de autenticación. El procedimiento comienza cuando el proveedor 104(1) de servicios envía al servidor 106(i) de autenticación una comunicación 302 que solicita el registro del proveedor de servicios. El servidor 106(i) de autenticación responde con una comunicación 304 que informa al proveedor 104(1) de servicios que está listo para aceptar el registro.

El proveedor 104(1) de servicios utiliza el módulo 130 de servidor para completar el procedimiento de registro proveedor de servicio se ilustra en la figura 3. El proveedor de servicios 104(1) genera una clave secreta K_S, $1 \leq K_S \leq p_2 - 2$, y calcula K_S^{-1} de tal manera que $K_S^{-1} K_S = K_S K_S^{-1} = 1 \bmod (p_2 - 1)$. A continuación, el proveedor 104(1) de servicios utiliza un esquema de umbral (*t, n*) para dividir K_S en *n* acciones de clave dividida K_S^i, $1 \leq i \leq n$. Una de

estas claves divididas $\{K_S^i\}$ y el *SID* se envía en una comunicación 306 segura a cada servidor 106(i) de autenticación. El servidor 106(i) de autenticación almacena la clave dividida K_S^i y el *SID* para usar durante el procedimiento 200 de acceso al proveedor de servicios del dispositivo cliente discutido en conexión con la figura 2.

Habiendo recibido y almacenado la clave dividida K_S^i y el *SID,* el servidor 106(i) de autenticación envía al proveedor 104(1) de servicios una respuesta correcta en una comunicación 308.

Varias comunicaciones discutidas son facilitadas mediante el módulo 130 servidor. Sin embargo, las diversas comunicaciones e instrucciones pueden llevarse a cabo por cualquier dispositivo habilitado para llevar a cabo dichas comunicaciones e instrucciones, proporcionando así el procedimiento de registro del proveedor de servicios descrito.

Procedimiento de registro del dispositivo del cliente

La figura 4 ilustra una implementación ejemplar en la que el dispositivo 102(1) informático cliente se registra con cada servidor 106(i) de autenticación utilizando un procedimiento 400 de registro del dispositivo del cliente. El procedimiento 400 de registro del dispositivo cliente se lleva a cabo antes de que un dispositivo informático cliente pueda beneficiarse de los servicios de autenticación ofrecidos por un servidor de autenticación. La tabla I anterior proporciona detalles relacionados con las notaciones utilizadas en el texto que sigue.

Antes de que el procedimiento se inicia, el dispositivo 102(1) informático cliente descarga e instala un módulo 140 cliente. El módulo 140 cliente en esta implementación proporciona la funcionalidad que permite al dispositivo 102(1) informático cliente procesar las comunicaciones hacia y desde cada servidor 106(i) de autenticación. El procedimiento comienza cuando el dispositivo 102(1) informático cliente envía al servidor 106(i) de autenticación una comunicación 402 que solicita el registro del dispositivo informático cliente. El servidor 106(i) de autenticación responde con una comunicación 404 que informa al dispositivo 102(1) informático cliente que está listo para aceptar el registro.

El dispositivo 102(1) informático cliente utiliza el módulo 140 cliente para crear un *UID* ID de cliente único desde una entrada de nombre de usuario por un usuario del dispositivo 102(1) informático cliente. El *UID* se puede crear mediante la dispersión del nombre de usuario, o dispersión partes del nombre de usuario. También se puede usar otro proceso que crea un *UID* de ID de cliente único a partir del nombre de usuario. El dispositivo 102(1) informático cliente utiliza el módulo 140 cliente para crear una clave de cliente K^i_U = *dispersión (NombreUsuario, Contraseña, AID$_i$),* $1 \le i \le n$ que se utilizará en el procedimiento de autenticación del dispositivo informático del cliente 500 con el servidor 106(i) de autenticación que se muestra en la figura5. La clave del cliente puede crearse usando el nombre de usuario también. El *AID$_i$* identifica un *i*-ésimo servidor de autenticación, en este caso el servidor 106(i) de autenticación.

El dispositivo 102(1) informático cliente envía *UID,* K_U^i, A_i, $1 \le i \le n$, al servidor 106(i) de autenticación por medio de una comunicación 406 segura. El servidor 106 de autenticación conserva la ID de usuario única *UID* y la clave del cliente K_U^i para su uso posterior. En particular, el servidor de autenticación utiliza la ID de usuario única *UID* y la clave del cliente K_U^i cuando el dispositivo 102(1) informático cliente realiza una solicitud de comunicación de autenticación con un proveedor de servicios. El proceso de autenticación con un proveedor de servicios generalmente requerirá una comunicación segura entre el dispositivo 102(1) informático cliente y un servidor 106(i) de autenticación; la ID de usuario única *UID* y la clave de cliente K_U^i facilita la generación de una clave de sesión utilizada para este fin.

Varias comunicaciones discutidas se facilitan usando el módulo 140 cliente. Sin embargo, las diversas comunicaciones e instrucciones pueden llevarse a cabo por cualquier dispositivo habilitado para llevar a cabo dichas comunicaciones e instrucciones, proporcionando así el procedimiento de registro del dispositivo informático del cliente descrito.

Procedimiento de autenticación del dispositivo cliente

La figura 5 ilustra una implementación ejemplar en la que el dispositivo 102(1) informático cliente se autentica con un servidor 106(i) de autenticación utilizando un procedimiento 500 de autenticación del dispositivo informático del cliente. El procedimiento 500 de autenticación del dispositivo informático del cliente se lleva a cabo para autenticar un dispositivo 102(1) informático cliente con un servidor 106(i) de autenticación y para establecer una clave de sesión que sea utilizada por el dispositivo informático del cliente y el servidor de autenticación mientras que el dispositivo cliente está intentando establecer comunicaciones autenticadas con un proveedor de servicios. La tabla I anterior proporciona detalles relacionados con las notaciones utilizadas en el texto que sigue.

El procedimiento comienza cuando el dispositivo 102(1) informático cliente envía un servidor 106 (i) autenticación de una comunicación 502 que solicita la autenticación. El servidor 106(i) de autenticación responde con una comunicación 504 que incluye un nonce n_{Ai}. El dispositivo 102(1) informático cliente responde, ayudado por el

módulo 140 cliente, con una comunicación 506 que incluye la ID de usuario única *UID* y un cifrado $< r_U, n_U, n_{A_i} >_{K_U^i}$. El servidor 106(i) de autenticación usará la clave del cliente K_U^i recibido en una comunicación previa para intentar descifrar el cifrado $< r_U, n_U, n_{A_i} >_{K_U^i}$. Si el descifrado es exitoso y el nonce descifrado coincide con el nonce n_{Ai} enviado al cliente en un proceso anterior, el servidor 106(i) de autenticación envía al dispositivo 102(1) informático cliente una comunicación 508 que incluye $< r_{A_i}, n_{A_i}, n_U >_{K_U^i}$ o un mensaje de error.

En este punto, tanto el dispositivo 102(1) informático cliente y el servidor 106 de autenticación tienen los valores de número aleatorio r_U, r_{Ai}. Usando estos valores de números aleatorios, tanto el dispositivo 102(1) informático cliente como el servidor 106(i) de autenticación computan una clave de sesión $SK_{U,Ai}$ = *dispersión* (r_U, r_{Ai}). Esta clave de sesión se utiliza cuando el dispositivo 102(1) informático cliente se pone en contacto con el servidor 106(i) de autenticación para solicitar una comunicación autenticada con un proveedor de servicios. El uso de la clave de sesión junto con el establecimiento de una comunicación autenticada con un proveedor de servicios se explica en detalle anteriormente en este documento.

Varias comunicaciones discutidas se facilitan usando el módulo 140 cliente. Sin embargo, las diversas comunicaciones e instrucciones pueden llevarse a cabo por cualquier dispositivo habilitado para llevar a cabo dichas comunicaciones e instrucciones, proporcionando de este modo el procedimiento de autenticación informático del cliente descrito.

Dispositivos informáticos ejemplares

Las figuras 6-8 ilustran dispositivos informáticos ejemplares que pueden usarse para implementar los procedimientos descritos. La figura 6 ilustra una implementación ejemplar de un proveedor 104(1) de servicios; la figura 7 ilustra una implementación ejemplar de un dispositivo 102(1) informático cliente; y la figura 8 ilustra una implementación ejemplar de un dispositivo 800 informático. Un servidor de autenticación, como el servidor 106(i) de autenticación, puede emplear los elementos operativos descritos en conexión con el dispositivo 800 informático. Esto también es válido para los dispositivos informáticos del cliente y los proveedores de servicios descritos en este documento.

La figura 6 es un dispositivo informático ilustrativo que puede usarse para implementar un proveedor 104(1) de servicios. En una configuración muy básica, el dispositivo informático incluye al menos una unidad 604 de procesamiento y una memoria 606 del sistema. Dependiendo de la configuración exacta y el tipo de dispositivo 600 informático, la memoria 606 del sistema puede ser volátil (como RAM), no volátil (como ROM, memoria flash, etc.) o alguna combinación de los dos. La memoria 606 del sistema incluye típicamente un sistema 608 operativo, uno o más módulos 610 de programa, y puede incluir datos 612 de programa. Al menos uno de los módulos 610 de programa incluye un módulo 130 de servidor.

El dispositivo informático puede tener características o funcionalidad adicionales. Por ejemplo, el dispositivo informático también puede incluir dispositivos de almacenamiento de datos adicionales (extraíbles y/o no extraíbles) como, por ejemplo, discos magnéticos, discos ópticos o cintas. Los medios legibles por ordenador pueden implementarse en cualquier procedimiento o tecnología para el almacenamiento de información tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos. La memoria 606 del sistema es un ejemplo de medios de almacenamiento informáticos. Los medios de almacenamiento informáticos incluyen medios físicos (tangibles), tales como, entre otros, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CDROM, discos versátiles digitales (DVD) u otro almacenamiento de disco óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético que pueden almacenar los datos deseados y a los que se puede acceder desde el ordenador 512. Cualquiera de estos medios de almacenamiento informático puede ser parte del dispositivo. El dispositivo informático también puede tener dispositivo(s) de entrada, como teclado, ratón, lápiz, dispositivo de entrada de voz, dispositivo de entrada táctil, etc. También se pueden incluir dispositivos de salida como una pantalla, altavoces, impresora, etc. Estos dispositivos son bien conocidos en la técnica y no necesitan ser discutidos/ilustrados en detalle.

El dispositivo informático puede contener también una conexión de comunicación que permite que el dispositivo se comunique con otros dispositivos informáticos, tales como en una red. Dicha red se muestra como la red 120 de la figura 1. La(s) conexión(es) de comunicación es un ejemplo de medios de comunicación. Los medios de comunicación pueden estar representados típicamente por instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, como una onda portadora u otro mecanismo de transporte, e incluye cualquier medio de entrega de información. El término "señal de datos modulados" significa una señal que tiene una o más de sus características configuradas o modificadas de tal manera que codifican información en la señal. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios cableados, como una red cableada o conexión directa, y medios inalámbricos, como acústicos, RF, infrarrojos y otros medios inalámbricos. Los medios legibles por ordenador pueden ser cualquier medio disponible al que se pueda acceder desde un ordenador. A modo de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender "medios de almacenamiento informático" y "medios de comunicación".

Varios módulos y técnicas pueden ser descritos en este documento en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutados por uno o más ordenadores u otros dispositivos. Generalmente, los módulos de programa incluyen rutinas, programas, objetos, artefactos físicos, estructuras de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Estos módulos de programas y similares pueden ejecutarse como código nativo o pueden descargarse y ejecutarse, como en una máquina virtual u otro entorno de ejecución de compilación justo a tiempo. Típicamente, la funcionalidad de los módulos del programa puede combinarse o distribuirse según se desee en diversas realizaciones. Una implementación de estos módulos y técnicas puede almacenarse o transmitirse a través de algún tipo de medio legible por ordenador.

La figura 7 es un dispositivo informático ilustrativo que se puede usar para implementar un dispositivo 102(1) informático cliente. En una configuración muy básica, el dispositivo informático incluye al menos una unidad 704 de procesamiento y una memoria 706 del sistema. Dependiendo de la configuración exacta y el tipo de dispositivo 700 informático, la memoria 706 del sistema puede ser volátil (como RAM), no volátil (como ROM, memoria flash, etc.) o alguna combinación de los dos. La memoria 706 del sistema incluye típicamente un sistema 708 operativo, uno o más módulos 710 de programa, y puede incluir datos 712 de programa. Al menos uno de los módulos 710 de programa incluye un módulo 140 cliente.

El dispositivo informático puede tener características o funcionalidades adicionales. Por ejemplo, el dispositivo informático también puede incluir dispositivos de almacenamiento de datos adicionales (extraíbles y/o no extraíbles) como, por ejemplo, discos magnéticos, discos ópticos o cintas. Los medios legibles por ordenador pueden implementarse en cualquier procedimiento o tecnología para el almacenamiento de información tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos. La memoria 706 del sistema es un ejemplo de medios de almacenamiento informáticos. Los medios de almacenamiento informáticos incluyen medios físicos (tangibles), tales como, entre otros, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CDROM, discos versátiles digitales (DVD) u otro almacenamiento de disco óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético que pueden almacenar los datos deseados y a los que se puede acceder desde el ordenador 512. Cualquiera de estos medios de almacenamiento informático puede ser parte del dispositivo. El dispositivo informático también puede tener dispositivo(s) de entrada, como teclado, ratón, lápiz, dispositivo de entrada de voz, dispositivo de entrada táctil, etc. También se pueden incluir dispositivos de salida como una pantalla, altavoces, impresora, etc. Estos dispositivos son bien conocidos en la técnica y no necesitan ser discutidos/ilustrados en detalle.

El dispositivo informático puede contener también una conexión de comunicación que permite que el dispositivo se comunique con otros dispositivos informáticos, tales como en una red. Dicha red se muestra como la red 120 de la figura 1. La(s) conexión(es) de comunicación es un ejemplo de medios de comunicación. Los medios de comunicación pueden estar representados típicamente por instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, como una onda portadora u otro mecanismo de transporte, e incluye cualquier medio de entrega de información. El término "señal de datos modulados" significa una señal que tiene una o más de sus características configuradas o modificadas de tal manera que codifican información en la señal. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios cableados, como una red cableada o conexión directa, y medios inalámbricos, como acústicos, RF, infrarrojos y otros medios inalámbricos. Los medios legibles por ordenador pueden ser cualquier medio disponible al que se pueda acceder desde un ordenador. A modo de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender "medios de almacenamiento informático" y "medios de comunicación".

Varios módulos y técnicas pueden ser descritos en este documento en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutados por uno o más ordenadores u otros dispositivos. Generalmente, los módulos de programa incluyen rutinas, programas, objetos, artefactos físicos, estructuras de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Estos módulos de programas y similares pueden ejecutarse como código nativo o pueden descargarse y ejecutarse, como en una máquina virtual u otro entorno de ejecución de compilación justo a tiempo. Típicamente, la funcionalidad de los módulos del programa puede combinarse o distribuirse según se desee en diversas realizaciones. Una implementación de estos módulos y técnicas puede almacenarse o transmitirse a través de algún tipo de medio legible por ordenador.

La figura 8 es un dispositivo 800 informático ilustrativo que puede usarse para implementar un servidor de autenticación, o cualquier otro dispositivo informático descrito en el presente documento. En una configuración muy básica, el dispositivo 800 informático incluye al menos una unidad 804 de procesamiento y una memoria 806 del sistema. Dependiendo de la configuración exacta y el tipo de dispositivo 800 informático, la memoria 806 del sistema puede ser volátil (como RAM), no volátil (como ROM, memoria flash, etc.) o alguna combinación de los dos. La memoria 806 del sistema incluye típicamente un sistema 808 operativo, uno o más módulos 810 de programa, y puede incluir datos 812 de programa.

El dispositivo 800 informático puede tener características o funcionalidades adicionales. Por ejemplo, el dispositivo 800 informático también puede incluir dispositivos de almacenamiento de datos adicionales (extraíbles y/o no extraíbles) como, por ejemplo, discos magnéticos, discos ópticos o cintas. Dicho almacenamiento adicional se ilustra

en la figura 8 mediante un almacenamiento 820 extraíble y un almacenamiento 822 no extraíble. Los medios legibles por ordenador pueden implementarse en cualquier procedimiento o tecnología para el almacenamiento de información tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos. La memoria 806 del sistema, el almacenamiento 820 extraíble y el almacenamiento 822 no extraíble son ejemplos de medios de almacenamiento de ordenador. Los medios de almacenamiento en ordenador incluyen medios físicos (tangibles), tales como, entre otros, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CDROM, discos versátiles digitales (DVD) u otro almacenamiento de disco óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético que pueden almacenar los datos deseados y al que se puede acceder desde el ordenador 800. Cualquiera de tales medios de almacenamiento informático puede ser parte del dispositivo 800. El dispositivo 800 informático también puede tener un dispositivo (s) de entrada 824 tal como un teclado, ratón, lápiz, dispositivo de entrada de voz, dispositivo de entrada táctil, etc. Un dispositivo(s) de salida 826 tal como una pantalla, altavoces, impresora, etc. también puede ser incluido. Estos dispositivos son bien conocidos en la técnica y no necesitan ser discutidos extensamente.

El dispositivo 800 informático puede contener también una conexión 828 de comunicación que permiten que el dispositivo se comunique con otros dispositivos 830 informáticos, tal como en una red. Dicha red se muestra como la red 120 de la figura 1. Las conexiones 828 de comunicación son un ejemplo de medios de comunicación. Los medios de comunicación pueden estar representados típicamente por instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada, como una onda portadora u otro mecanismo de transporte, e incluye cualquier medio de entrega de información. El término "señal de datos modulados" significa una señal que tiene una o más de sus características configuradas o modificadas de tal manera que codifican información en la señal. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios cableados, como una red cableada o conexión directa, y medios inalámbricos, como acústicos, RF, infrarrojos y otros medios inalámbricos. Los medios legibles por ordenador pueden ser cualquier medio disponible al que se pueda acceder desde un ordenador. A modo de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender "medios de almacenamiento informático" y "medios de comunicación".

Varios módulos y técnicas pueden ser descritos en este documento en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutados por uno o más ordenadores u otros dispositivos. Generalmente, los módulos de programa incluyen rutinas, programas, objetos, artefactos físicos, estructuras de datos, etc. que realizan tareas particulares o implementan tipos de datos abstractos particulares. Estos módulos de programas y similares pueden ejecutarse como código nativo o pueden descargarse y ejecutarse, como en una máquina virtual u otro entorno de ejecución de compilación justo a tiempo. Típicamente, la funcionalidad de los módulos del programa puede combinarse o distribuirse según se desee en diversas realizaciones. Una implementación de estos módulos y técnicas puede almacenarse o transmitirse a través de algún tipo de medio legible por ordenador.

Mientras que las realizaciones de ejemplo se han ilustrado y descrito, debe entenderse que la invención no se limita a la configuración precisa y recursos descrito anteriormente. Se pueden realizar diversas modificaciones, cambios y variaciones evidentes para los expertos en la técnica en la disposición, operación y detalles de las realizaciones descritas en este documento sin apartarse del alcance de la invención reivindicada.

REIVINDICACIONES

1. Un procedimiento realizado por un proveedor (104(1) - 104(n)) de servicios, que comprende:

recibir una solicitud (208) de autenticación que incluya al menos un identificador de cliente y un testigo de autenticación encriptado derivado de una pluralidad de testigos de autenticación parcial,
en el que cada testigo de autenticación parcial se cifra con una clave dividida generada a partir de una clave secreta conocida solo por el proveedor del servicio, en el que cada testigo de autenticación parcial incluye el identificador del cliente, una dirección de red y un desafío/nonce del proveedor de servicios;
intentar descifrar el testigo de autenticación cifrado utilizando la clave secreta; y
otorgar comunicación autenticada si el descifrado es posible con la clave secreta y un contenido descifrado del testigo de autenticación cifrado es aceptable.

2. El procedimiento de acuerdo con la reivindicación 1, en el que el testigo de autenticación cifrado incluye un identificador de cliente y un desafío/nonce.

3. El procedimiento de acuerdo con la reivindicación 2, en el que el identificador del cliente identifica un dispositivo (102(1) - 102 (n)) cliente que desea una comunicación autenticada con el proveedor de servicios.

4. El procedimiento de acuerdo con la reivindicación 2, en el que el proveedor de servicios proporciona el desafío/nonce que intenta descifrar el testigo de autenticación cifrado.

5. El procedimiento de acuerdo con la reivindicación 1, en el que el testigo de autenticación cifrado incluye además una dirección de red de un dispositivo (102 (n)) cliente.

6. Un artículo de fabricación para su uso en la programación de un procesador (604), comprendiendo el artículo de fabricación al menos un dispositivo (606) de almacenamiento legible por ordenador que incluye al menos un programa (130) de ordenador incrustado en el mismo que hace que el procesador (604) realice el procedimiento de la reivindicación 1.

7. Un dispositivo informático que comprende:

un procesador (604); y
una memoria (606) que tiene al menos un componente (130) ejecutable por ordenador capaz de realizar el procedimiento de la reivindicación 1.

8. Un procedimiento realizado por un servidor (106 (1) - 106 (n)) de autenticación para proporcionar servicios de autenticación a un proveedor de servicios como se define en la reivindicación 1, que comprende:

establecer una sesión (508) segura con una clave de sesión si dicha sesión (508) segura no se estableció en un procedimiento anterior;
recibir un ID de proveedor de servicios y un desafío/nonce suministrado por un proveedor (104(1) - 104(n)) de servicios;
cifrar una ID única de un dispositivo (102(1) - 102 (n)) informático cliente, una dirección de red del dispositivo informático cliente y el desafío/nonce proporcionado por el proveedor de servicios utilizando una clave dividida derivada de una clave secreta desconocida para el servidor de autentificación y
ofrecer el cifrado al dispositivo informático del cliente, el cifrado utilizable al intentar obtener acceso al proveedor de servicios.

9. El procedimiento de acuerdo con la reivindicación 8, en el que la clave de sesión se genera a partir de una clave de autenticación, la clave de autenticación se deriva de las credenciales de inicio de sesión del dispositivo informático del cliente que desea la autenticación y una ID del servidor de autenticación.

10. El procedimiento de acuerdo con la reivindicación 9, en el que las credenciales de inicio de sesión incluyen una contraseña y un nombre de usuario.

11. El procedimiento de acuerdo con la reivindicación 8, en el que una ID única de una entidad que desea la autenticación se deriva de al menos el nombre de inicio de sesión de la entidad.

12. El procedimiento de acuerdo con la reivindicación 9, en el que la clave de autenticación y la ID única del dispositivo informático del cliente que desea la autenticación son generadas por un módulo (140) en el dispositivo informático del cliente que desea la autenticación durante un procedimiento de autenticación que establece una sesión segura, la clave de autenticación y la ID única que se conoce y almacena mediante una autenticación en un procedimiento anterior.

13. El procedimiento de acuerdo con la reivindicación 8, en el que el cifrado incluye además el cifrado de un elemento o la firma de un elemento, utilizándose el elemento para generar otra clave de sesión para posteriores comunicaciones seguras.

14. El procedimiento de acuerdo con la reivindicación 8, en el que recibir además incluye recibir un elemento, el elemento se usará para generar otra clave de sesión para comunicaciones posteriores seguras.

15. El procedimiento de acuerdo con la reivindicación 8, que además comprende:

recibir una solicitud de autenticación en una pluralidad de servidores (106 (1) - 106 (n)) de autenticación, la solicitud de autenticación solicita una comunicación autenticada con el proveedor de servicios; y
cada servidor (106 (i)) de autenticación proporciona un testigo de autenticación parcial, utilizándose la pluralidad de testigos de autenticación parcial juntos para generar un testigo de autenticación utilizado para lograr una comunicación autenticada con el proveedor de servicios.

16. El procedimiento de acuerdo con la reivindicación 15, en el que cada servidor (106 (i)) de autenticación cifra un testigo de autenticación parcial utilizando la clave dividida derivada de una clave secreta generada por el proveedor de servicios.

17. El procedimiento de acuerdo con la reivindicación 16, en el que se usa un esquema de umbral para generar claves divididas a partir de una clave secreta.

18. El procedimiento de acuerdo con la reivindicación 15, en el que la solicitud de autenticación incluye una ID de proveedor de servicios y un desafío/nonce proporcionado por el proveedor de servicios, estando asociada la ID de proveedor de servicios con el proveedor de servicios.

19. El procedimiento de acuerdo con la reivindicación 15, en el que cada testigo de autenticación parcial incluye una ID de un dispositivo (102(1) - 102(n) informático cliente que solicita comunicación autenticada con el proveedor de servicios, una dirección de red del dispositivo informático cliente y un desafío/nonce suministrado por el proveedor de servicios.

20. Un artículo de fabricación para su uso en la programación de un procesador (604, 704, 804), comprendiendo el artículo de fabricación al menos un dispositivo (606, 706, 806) de almacenamiento legible por ordenador que incluye al menos un programa (610, 710, 810) de ordenador incrustado en el mismo que hace que el procesador (604, 704, 804) realice el procedimiento de la reivindicación 8.

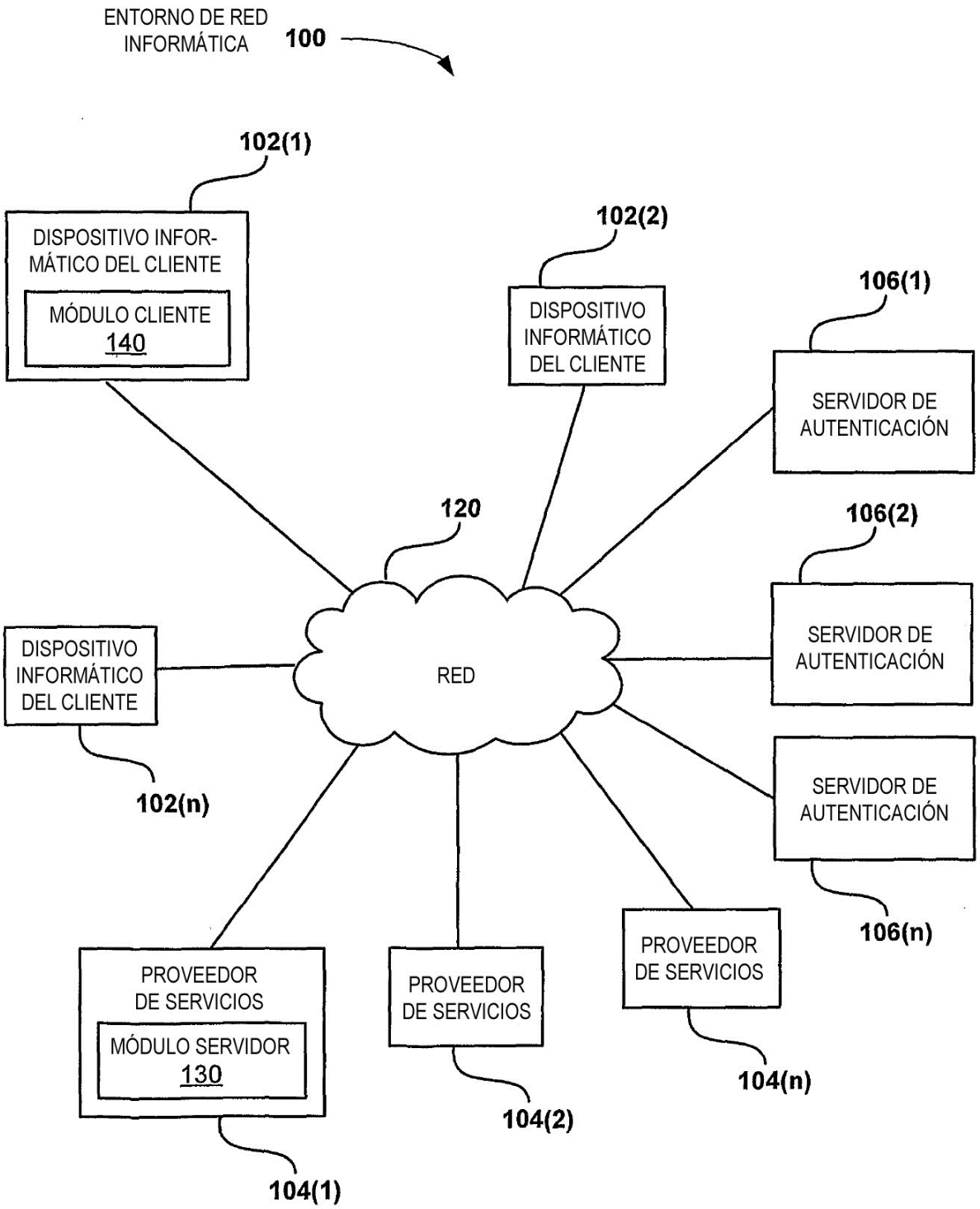
ENTORNO DE RED INFORMÁTICA
100
102(1)
DISPOSITIVO INFORMÁTICO DEL CLIENTE
MÓDULO CLIENTE
140
102(2)
DISPOSITIVO INFORMÁTICO DEL CLIENTE
106(1)
SERVIDOR DE AUTENTICACIÓN
120
RED
106(2)
SERVIDOR DE AUTENTICACIÓN
DISPOSITIVO INFORMÁTICO DEL CLIENTE
102(n)
SERVIDOR DE AUTENTICACIÓN
106(n)
PROVEEDOR DE SERVICIOS
MÓDULO SERVIDOR
130
104(1)
PROVEEDOR DE SERVICIOS
104(2)
PROVEEDOR DE SERVICIOS
104(n)

Fig. 1

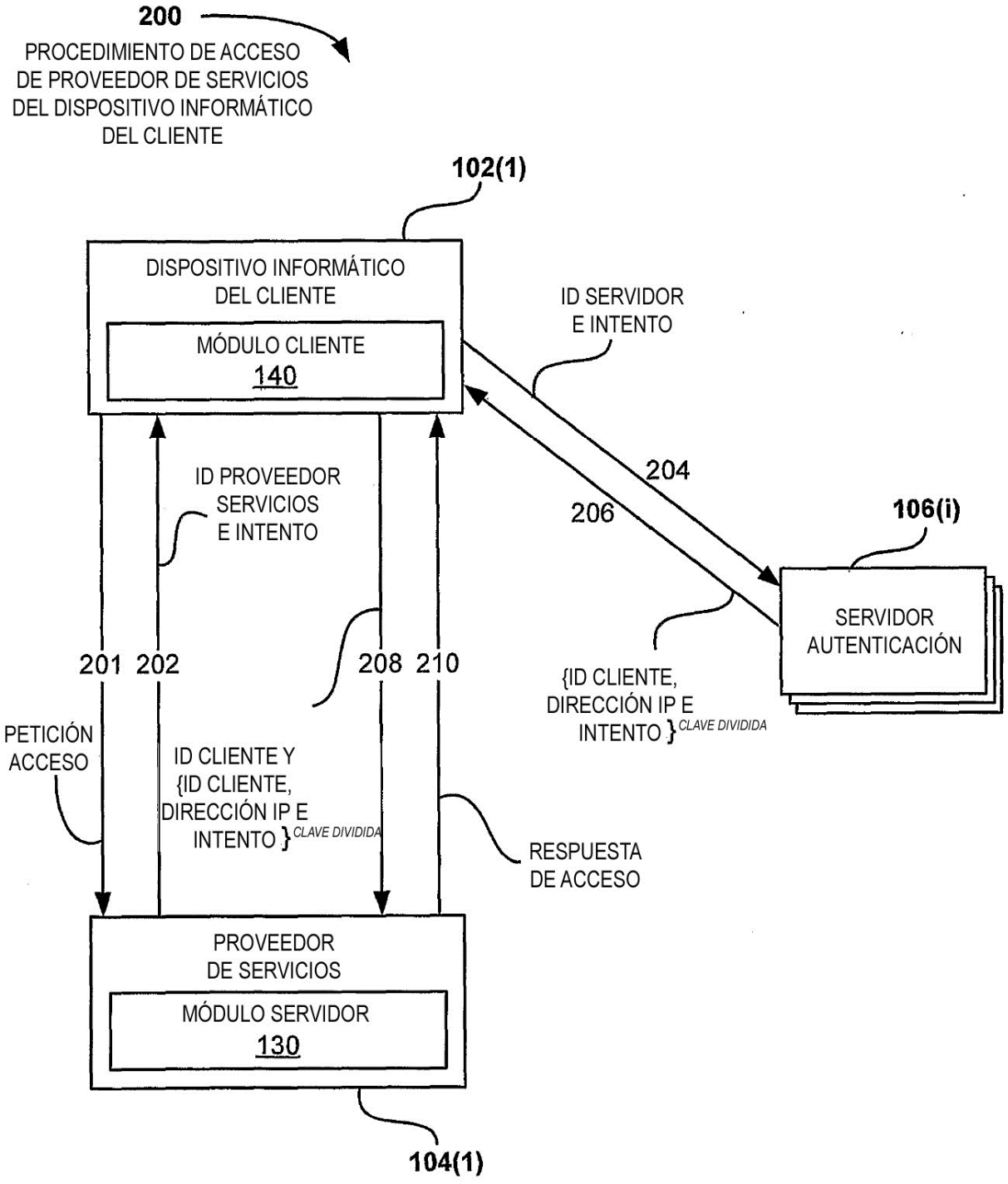
200
PROCEDIMIENTO DE ACCESO DE PROVEEDOR DE SERVICIOS DEL DISPOSITIVO INFORMÁTICO DEL CLIENTE
102(1)
DISPOSITIVO INFORMÁTICO DEL CLIENTE
MÓDULO CLIENTE
140
ID SERVIDOR E INTENTO
204
206
106(i)
SERVIDOR AUTENTICACIÓN
ID PROVEEDOR SERVICIOS E INTENTO
201 202
208 210
{ID CLIENTE, DIRECCIÓN IP E INTENTO } CLAVE DIVIDIDA
PETICIÓN ACCESO
ID CLIENTE Y {ID CLIENTE, DIRECCIÓN IP E INTENTO } CLAVE DIVIDIDA
RESPUESTA DE ACCESO
PROVEEDOR DE SERVICIOS
MÓDULO SERVIDOR
130
104(1)

Fig. 2

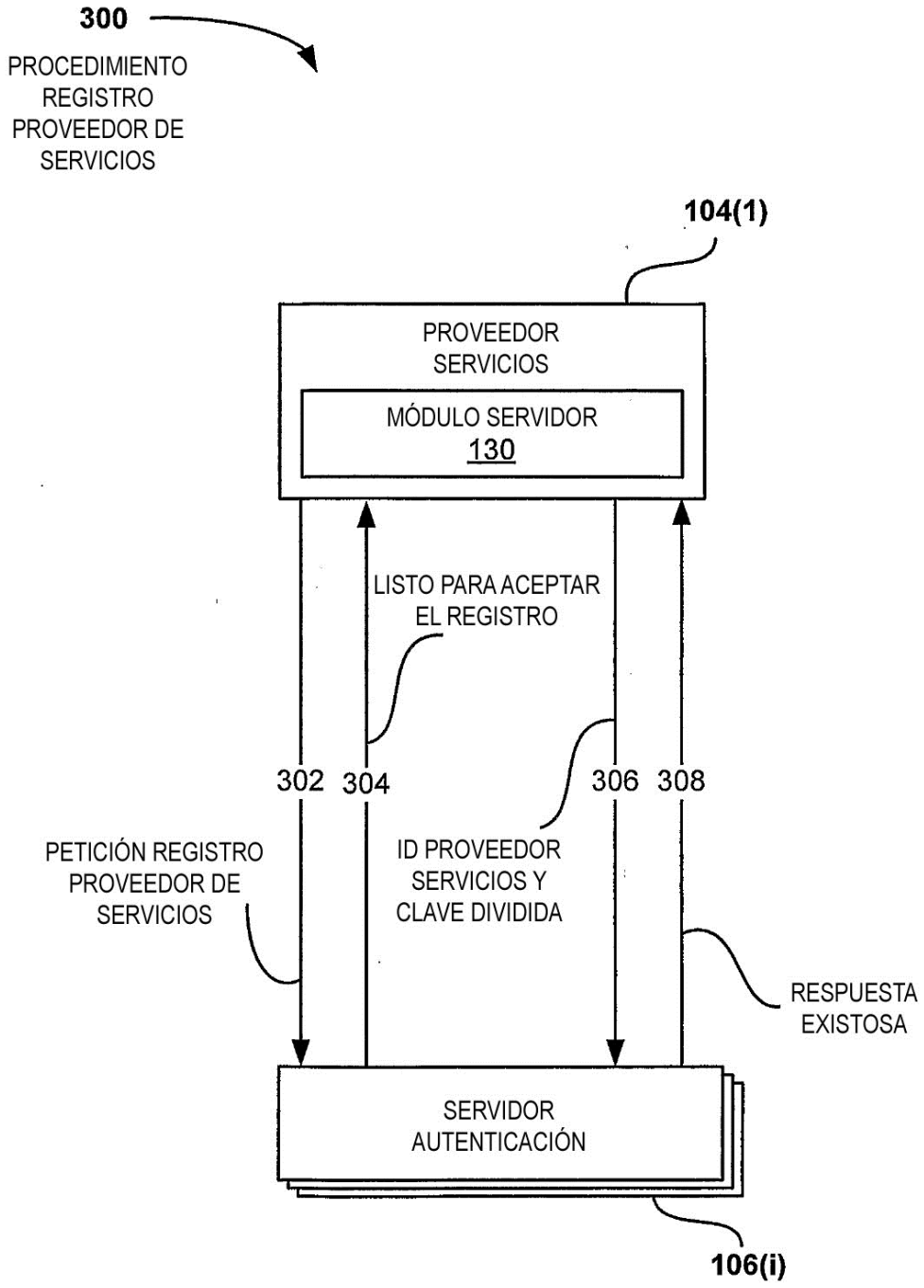
300
PROCEDIMIENTO REGISTRO PROVEEDOR DE SERVICIOS
104(1)
PROVEEDOR SERVICIOS
MÓDULO SERVIDOR 130
LISTO PARA ACEPTAR EL REGISTRO
302
304
306
308
PETICIÓN REGISTRO PROVEEDOR DE SERVICIOS
ID PROVEEDOR SERVICIOS Y CLAVE DIVIDIDA
RESPUESTA EXISTOSA
SERVIDOR AUTENTICACIÓN
106(i)

Fig. 3

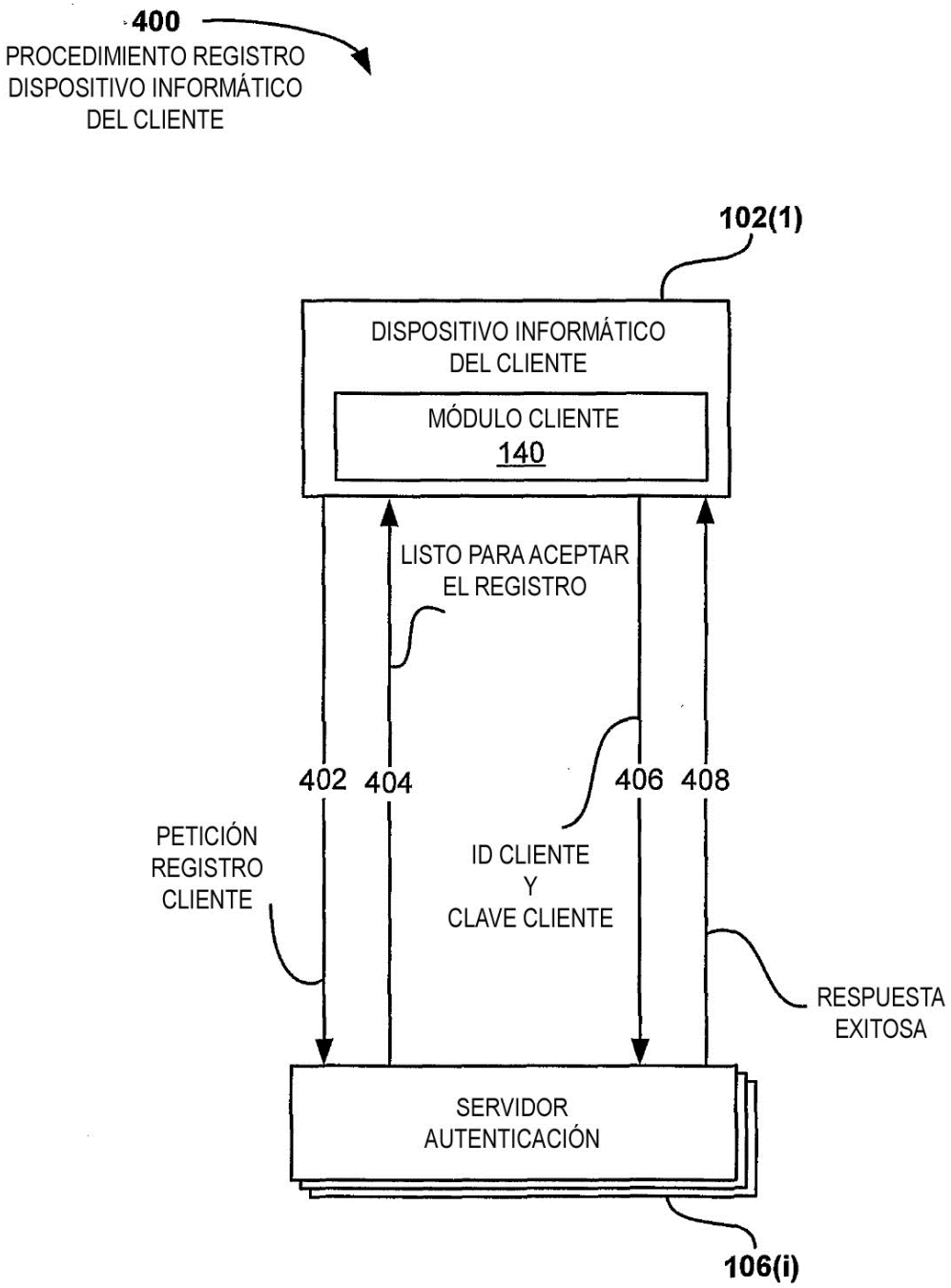
400
PROCEDIMIENTO REGISTRO DISPOSITIVO INFORMÁTICO DEL CLIENTE
102(1)
DISPOSITIVO INFORMÁTICO DEL CLIENTE
MÓDULO CLIENTE
140
LISTO PARA ACEPTAR EL REGISTRO
402
404
406
408
PETICIÓN REGISTRO CLIENTE
ID CLIENTE Y CLAVE CLIENTE
RESPUESTA EXITOSA
SERVIDOR AUTENTICACIÓN
106(i)

Fig. 4

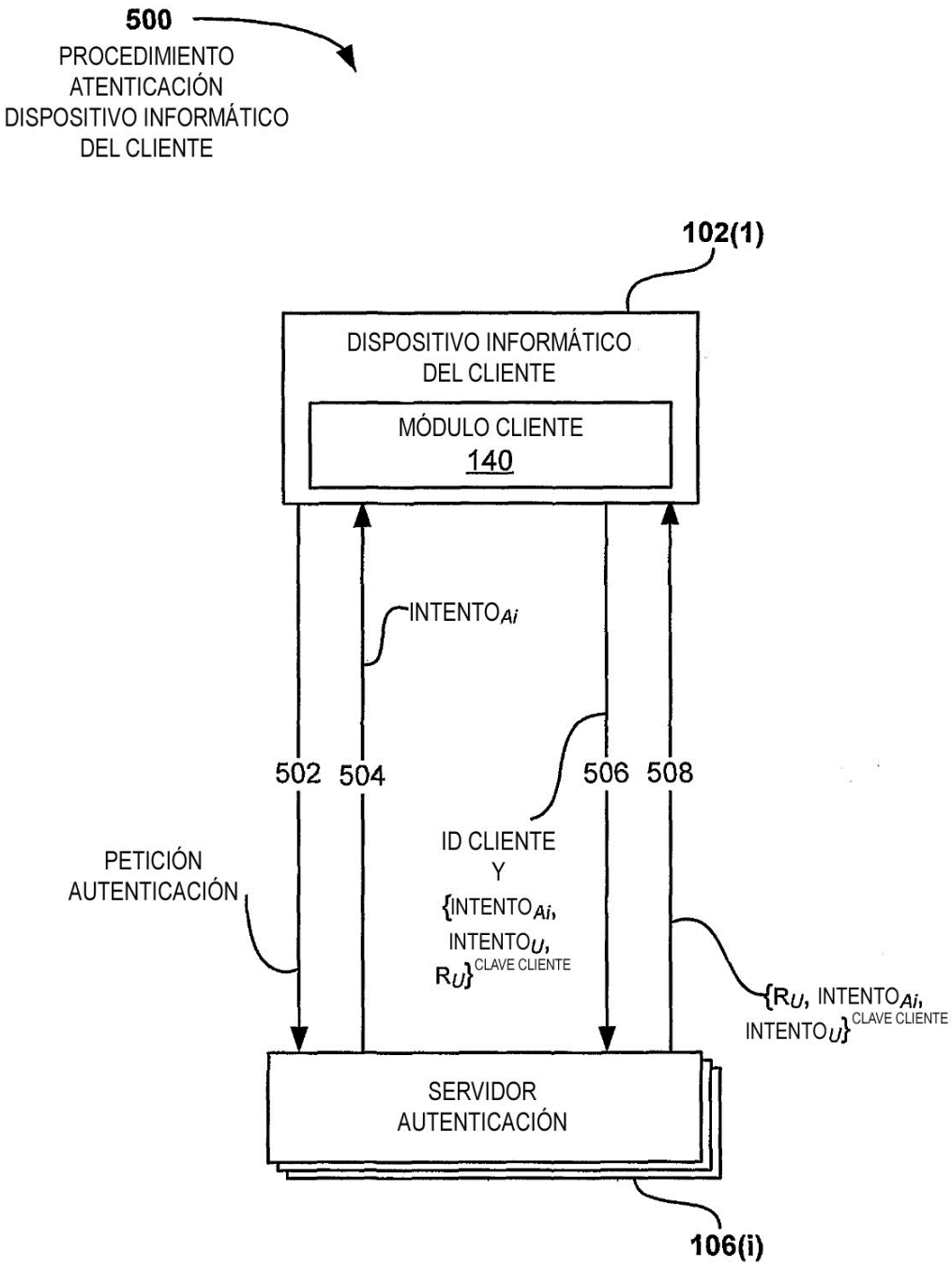
500
PROCEDIMIENTO ATENTICACIÓN DISPOSITIVO INFORMÁTICO DEL CLIENTE
102(1)
DISPOSITIVO INFORMÁTICO DEL CLIENTE
MÓDULO CLIENTE 140
INTENTO$_{Ai}$
502
504
506
508
ID CLIENTE Y {INTENTO$_{Ai}$, INTENTO$_U$, R$_U$}$^{CLAVE\ CLIENTE}$
PETICIÓN AUTENTICACIÓN
{R$_U$, INTENTO$_{Ai}$, INTENTO$_U$}$^{CLAVE\ CLIENTE}$
SERVIDOR AUTENTICACIÓN
106(i)

Fig. 5

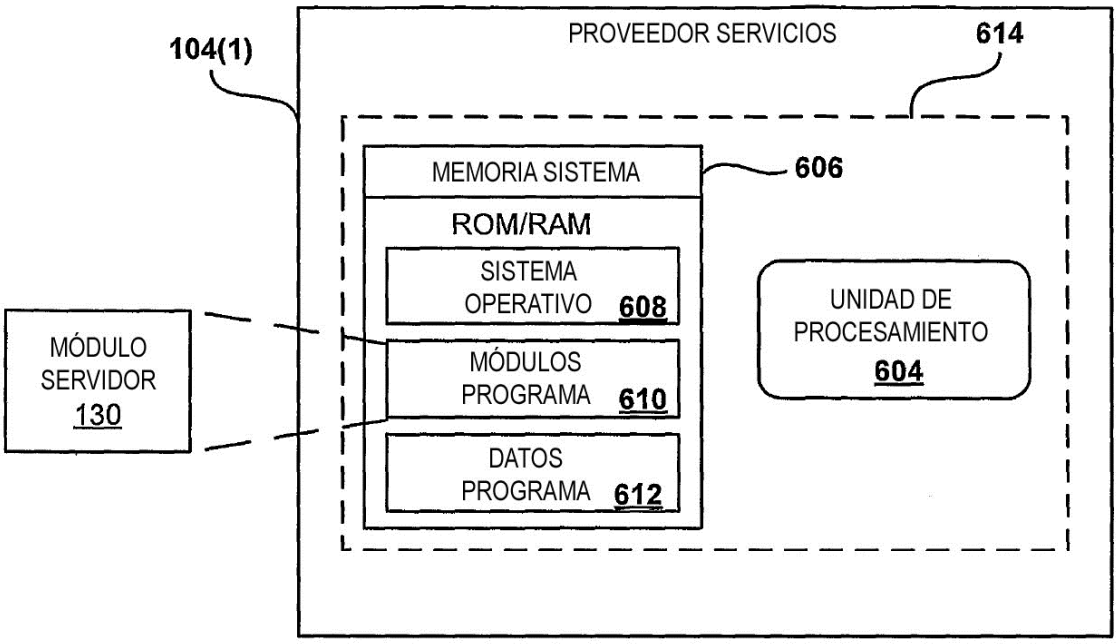
104(1)
PROVEEDOR SERVICIOS
614
MEMORIA SISTEMA
606
ROM/RAM
SISTEMA OPERATIVO 608
MÓDULOS PROGRAMA 610
DATOS PROGRAMA 612
UNIDAD DE PROCESAMIENTO 604
MÓDULO SERVIDOR 130

Fig. 6

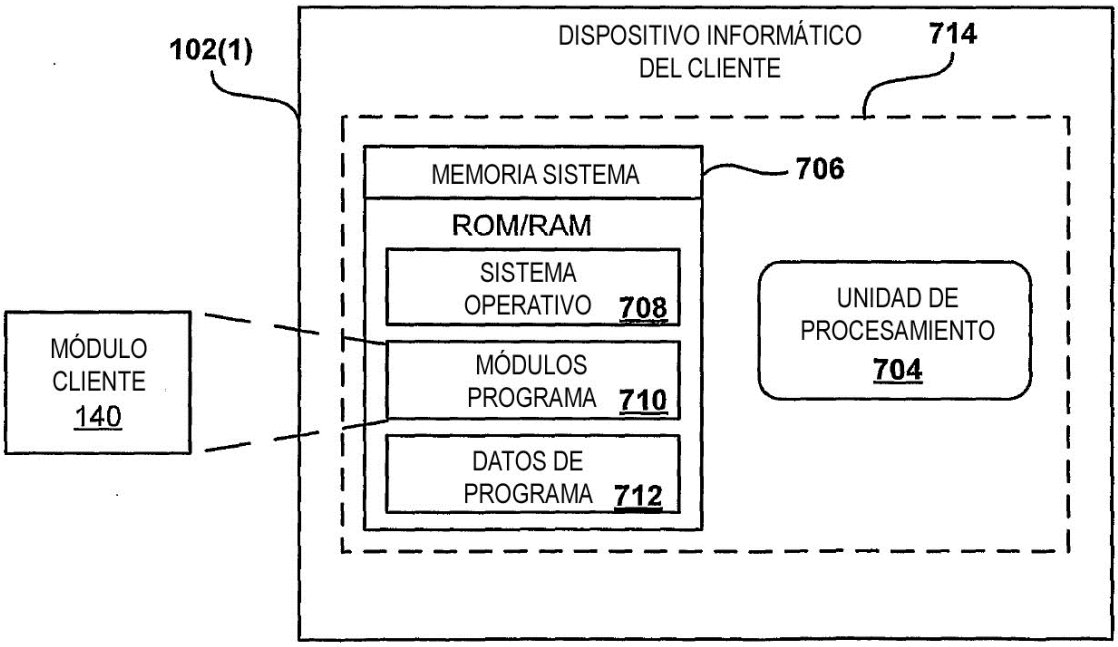
102(1)
DISPOSITIVO INFORMÁTICO DEL CLIENTE
714
MEMORIA SISTEMA
706
ROM/RAM
SISTEMA OPERATIVO 708
MÓDULOS PROGRAMA 710
DATOS DE PROGRAMA 712
UNIDAD DE PROCESAMIENTO 704
MÓDULO CLIENTE 140

Fig. 7

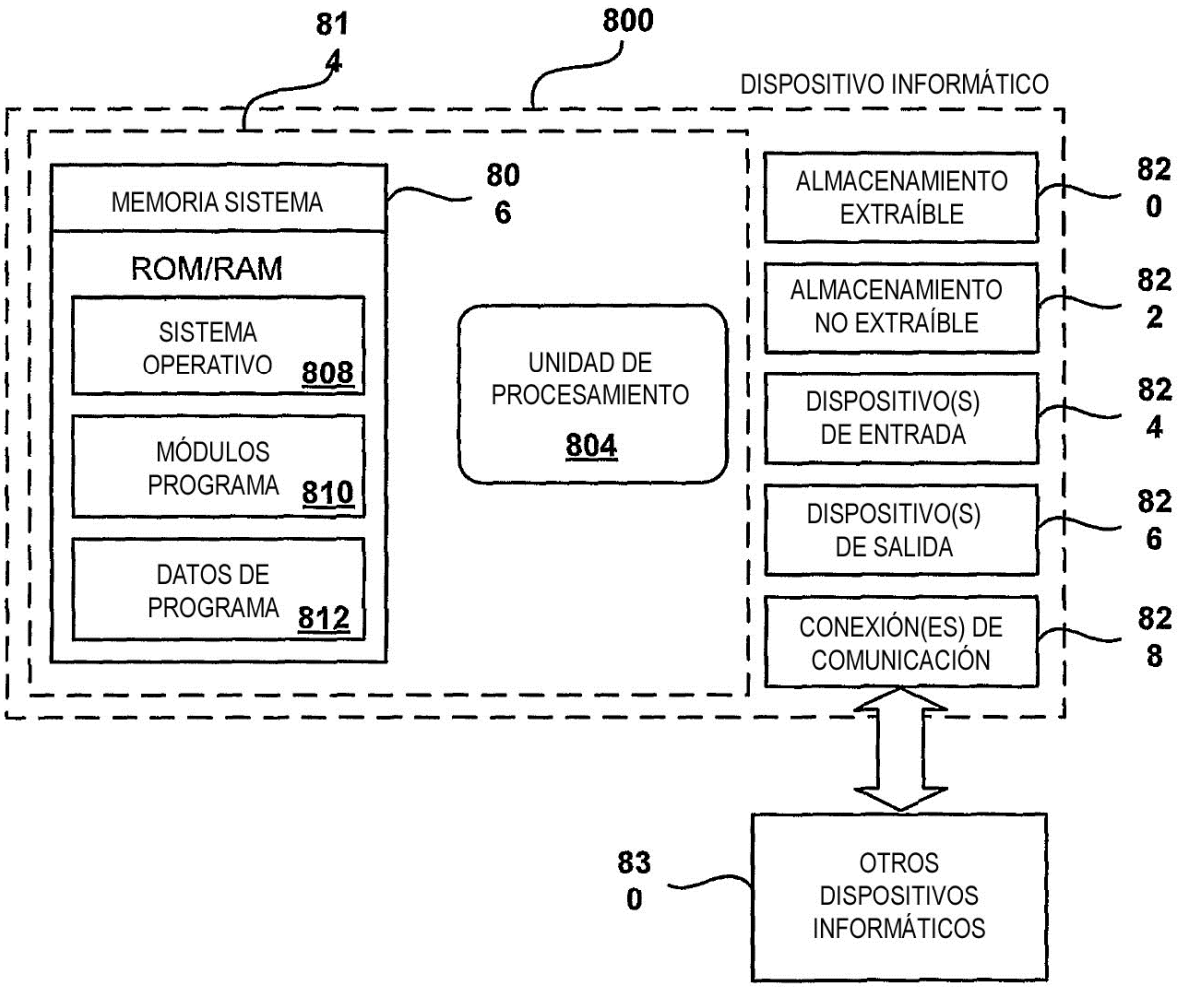
814
800
DISPOSITIVO INFORMÁTICO
MEMORIA SISTEMA
806
ROM/RAM
SISTEMA OPERATIVO 808
MÓDULOS PROGRAMA 810
DATOS DE PROGRAMA 812
UNIDAD DE PROCESAMIENTO 804
ALMACENAMIENTO EXTRAÍBLE
820
ALMACENAMIENTO NO EXTRAÍBLE
822
DISPOSITIVO(S) DE ENTRADA
824
DISPOSITIVO(S) DE SALIDA
826
CONEXIÓN(ES) DE COMUNICACIÓN
828
830
OTROS DISPOSITIVOS INFORMÁTICOS

Fig. 8