(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 595 105**

(51) Int. CI.:

***G06F 21/31*** (2013.01)
***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.03.2005 E 09006596 (2)**

(97) Fecha y número de publicación de la concesión europea: **13.07.2016 EP 2105819**

(54) Título: **Autenticación eficaz y segura de sistemas informáticos**

(30) Prioridad:

**19.03.2004 US 804591**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**27.12.2016**

(73) Titular/es:

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

(72) Inventor/es:

**ADOBA, BERNARD, D.;**
**SIMON, DANIEL, R.;**
**MOORE, TIMOTHY, M. y**
**FREEMAN, TREVOR, WILLIAM**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

## DESCRIPCIÓN

Autenticación eficaz y segura de sistemas informáticos

La presente invención se refiere a aprovisionamiento de autenticación y credenciales extensible. Más específicamente, la presente invención se refiere a negociación automatizada de mecanismos de autenticación y credenciales de uso limitado que pueden usarse para aprovisionar credenciales adicionales.

Los sistemas informáticos y tecnología relacionada afectan a muchos aspectos de la sociedad. De hecho, la capacidad de los sistemas informáticos para procesar la información ha transformado la manera en que vivimos y trabajamos. Los sistemas informáticos ahora comúnmente realizan una multitud de tareas (por ejemplo, procesamiento de textos, planificación y gestión de bases de datos) que antes de la llegada de los sistemas informáticos se realizaban manualmente. Más recientemente, se han acoplado sistemas informáticos entre sí para formar redes informáticas a través de las que los sistemas informáticos pueden comunicar electrónicamente para compartir datos. Como resultado, muchas de las tareas realizadas en un sistema informático (por ejemplo, acceder a correo electrónico y exploración web) incluyen comunicación electrónica con uno u otros sistemas informáticos más mediante una red informática (por ejemplo, internet).

Para que un sistema informático comunique electrónicamente con otro sistema informático, el sistema informático, así como un usuario de sistema informático correspondiente, pueden necesitar autenticarse con (es decir, probar su identidad a) el otro sistema informático (o un sistema informático que autoriza acceso al otro sistema informático). Dependiendo del entorno, puede usarse cualquiera de una amplia diversidad de diferentes mecanismos de autenticación informatizados, tales como, por ejemplo, Kerberos, Capa de Conexiones Segura (“SSL”), Gestor de LAN de NT (“NTLM”), y/o autenticación resumida.

Algunos mecanismos autenticación incluyen un inicio de sesión interactivo. Por ejemplo, antes de que un sistema informático pueda comunicar electrónicamente en internet, se requiere a menudo que un usuario del sistema informático inicie sesión con un Proveedor de Servicio de Internet (en lo sucesivo denominado como un “ISP”) que puede autorizar acceso a internet. Iniciar sesión con un ISP típicamente incluye una presentación de credenciales de usuario (por ejemplo, un nombre de usuario y una contraseña) desde el sistema informático al ISP. Tras recibir los credenciales, el ISP compara los credenciales con una base de datos de credenciales y si los credenciales son apropiados el sistema informático está autorizado a comunicar con internet.

Desafortunadamente, existe siempre algún riesgo de que usuarios no autorizados obtengan unos credenciales de usuario autorizado y usen los credenciales para hacerse pasar por el usuario autorizado. Puesto que unos credenciales de usuario autorizado esencialmente permiten acceso total a todos los recursos de usuarios autorizados en un sistema particular (por ejemplo, ficheros, mensajes electrónicos, datos personales y financieros, etc.), cualquier compromiso en los credenciales puede proporcionar a un usuario no autorizado con la capacidad de copiar y destruir los recursos del usuario autorizado. En particular, las contraseñas son vulnerables a ataques por adivinanza, por ejemplo, desde programas que presentan secuencialmente cada palabra en un diccionario como una contraseña (denominado comúnmente como “ataques de diccionario”).

Otros mecanismos de autenticación no incluyen un inicio de sesión interactivo y por lo tanto no hay credenciales de usuario que puedan obtenerse. Por ejemplo, un servidor web puede probar su identidad a un cliente web usando SSL. Cuando el cliente web entra en contacto con una página web con seguridad en el servidor web (por ejemplo, una página que comienza con “https:”), el servidor web responde, enviando automáticamente un certificado digital que autentica el servidor web. El cliente web genera una clave de sesión única para encriptar toda la comunicación con el servidor web. El cliente web encripta la sesión con la clave pública del servidor web (por ejemplo, referenciada en el certificado) por lo que únicamente el servidor web puede leer la clave de sesión. Por lo tanto, se establece una sesión segura sin requerir ninguna acción del usuario.

Aunque se han descrito ejemplos de mecanismos de autenticación interactiva y autenticación no interactiva, debería entenderse que las implementaciones de autenticación interactiva y autenticación no interactiva pueden variar entre redes y sistemas informáticos. Por ejemplo, una red puede configurarse para usar autenticación Kerberos, mientas otra red está configurada para usar algún otro mecanismo de autenticación interactivo. Además, un mecanismo de autenticación particular puede tener diferentes opciones de configuración que provocan que el mecanismo de autenticación opere de manera diferente. Por ejemplo, algunas implementaciones de SSL permiten que se seleccionen diferentes algoritmos de encriptación cuando se establece una sesión segura.

Desafortunadamente, puede ser difícil o incluso imposible, determinar el mecanismo de autenticación y/o las opciones de configuración que ha desplegado un sistema o red informática. Por lo tanto, un sistema informático puede intentar autenticar con otro sistema informático usando un mecanismo de autenticación y/u opción de configuración que no se haya desplegado en el otro sistema informático. Como resultado, la autenticación puede fallar y evitar que los sistemas informáticos comuniquen.

El potencial para intentar autenticar usando un mecanismo de autenticación sin desplegar es especialmente alto en sistemas distribuidos. Los sistemas distribuidos a menudo incluyen un número de sistemas y redes informáticas interconectadas, donde diversas porciones del sistema distribuido están bajo el control de diferentes entidades.

Estas diferentes entidades pueden desplegar cada una diferentes mecanismos de autenticación y pueden no necesariamente anunciar o publicar una indicación de los mecanismos de autenticación que se despliegan. Por lo tanto, puede evitarse que un primer componente del sistema distribuido se autentique con un segundo componente del sistema distribuido puesto que el primer componente no conoce (y puede no tener manera para determinar) los mecanismos de autenticación desplegados en el segundo componente.

Pueden tener lugar otros problemas de comunicación en entornos inalámbricos. Por ejemplo, para que un dispositivo se autentique inalámbricamente con una red cableada/inalámbrica mixta, puede requerirse que el dispositivo tenga un certificado que corresponda con la red. Sin embargo, la red puede configurarse para permitir que únicamente dispositivos autenticados accedan al certificado. Por lo tanto, puede requerirse que el dispositivo se conecte inicialmente a la red mediante una conexión cableada. Requerir una conexión cableada para acceder a un certificado puede sobrecargar a un usuario (por ejemplo, un usuario puede necesitar localizar una toma de red) y en algunos entornos puede ser difícil (por ejemplo, las tomas de red pueden estar en localizaciones de acceso restringido) o incluso imposible (por ejemplo, algunos dispositivos no están configurados para acceso de red cableada). Por consiguiente, incluso puede evitarse que los usuarios autorizados accedan inalámbricamente a una red.

Por lo tanto, lo que sería ventajoso son mecanismos para negociar automáticamente procedimientos de autenticación y aprovisionamiento más seguro de credenciales.

El documento US 2001/009025 A1 se refiere a un procedimiento de comunicación seguro para permitir a un anfitrión móvil comunicar con un anfitrión correspondiente de una Red Privada Virtual. Se describe en primer lugar negociar una o más Asociaciones de Seguridad (SA) entre el anfitrión móvil y un correspondiente anfitrión de una Red Privada Virtual (VPN). Posteriormente, se inicia una comunicación entre el anfitrión móvil y una pasarela de seguridad (SG) de la VPN y se envía un certificado de autenticación a la SG, conteniendo el certificado al menos la identidad de una SA que se usará para comunicación posterior entre el anfitrión móvil y el anfitrión correspondiente. Se envían paquetes de datos desde el anfitrión móvil al anfitrión correspondiente usando la SA identificada, mediante la SG. Dichos paquetes de datos se reenvían mediante la SG al anfitrión correspondiente únicamente si están autenticados mediante la SG. Se establece que las realizaciones descritas reducen la cantidad de mensajería relacionada con seguridad durante los cambios de dirección IP al vuelo, ya que pre-existen las SA necesarias para proporcionar comunicación segura entre el anfitrión móvil y el correspondiente anfitrión. Se proporciona una descripción de una realización con respecto a los intercambios de mensajes durante las fases de negociación de SA de Asociación de Seguridad de Internet y Protocolo de Gestión de Clave (ISAKMP). Los tipos de mensaje intercambiados proporcionan negociación de algoritmo, generación de clave secreta y autenticación de pares. Se supone que se usa IKE para obtener material de codificación autenticado para uso con las asociaciones de seguridad ISAKMP e IPsec. Se describe establecer un intercambio de clave autenticada que genera material de codificación autenticado a partir de un intercambio Diffie-Hellman, creando el procedimiento un secreto compartido entre las partes de la comunicación. Los mensajes de intercambio Diffie-Hellman llevarán valores públicos Diffie-Hellman y datos auxiliares (por ejemplo números aleatorios usados solo una vez) necesarios para el intercambio.

El documento “RFC 2409 - The Internet Key Exchange” [en línea] noviembre de 1998 se refiere a asociación de seguridad de ISAKMP y a la negociación de un algoritmo de encriptación, algoritmo de troceo y procedimiento de autenticación e información acerca de un grupo a través del que hacer Diffie-Hellman.

El documento US 2002/194342 A1 se refiere a un conmutador de aplicación sensible a contenido que conmuta de manera inteligente paquetes de cliente a un servidor entre un grupo de servidores en una granja de servidores. Una ilustración esquemática desvela la información llevada en una etiqueta de paquete que comprende un campo de ID de paquete y un campo de ID de paquete anterior.

Andersson S. Josefsson RSA Security Glen Zorn Cisco Dan Simon Ashwin Palekar Microsoft H: “Protected EAP Protocol (PEAP); draft-josefsson-ppext-eap- 02.txt” IETF Standard-Working-Draft, Internet Engineering Task Force, IETF, CH, n.º 2, 23 de febrero de 2002 describe un protocolo de autenticación extensible protegida (PEAP), en el que EAP proporciona soporte de múltiples procedimientos de autenticación.

Es el objeto de la presente invención proporcionar un procedimiento mejorado y medio legible por ordenador correspondiente de negociación de autenticación entre un cliente y un sistema informático de servidor.

Este objeto se resuelve mediante la materia objeto de las reivindicaciones independientes.

Se definen realizaciones preferidas en las reivindicaciones dependientes.

Los problemas anteriores con el estado de la técnica anterior se superan mediante los principios de la presente invención, que se refieren a sistemas informáticos de autenticación más eficaz y más segura. En algunas realizaciones, un sistema informático de cliente recibe un credencial de uso limitado. El sistema informático de cliente y un sistema informático de servidor establecen un enlace seguro entre sí. El sistema informático de cliente presenta el credencial de uso limitado al sistema informático de servidor a través del enlace seguro establecido.

El sistema informático de servidor recibe el credencial de uso limitado desde el sistema informático de cliente a través del enlace seguro establecido. El sistema informático de servidor aprovisiona un credencial adicional para el sistema informático de cliente basándose en el credencial de usuario limitado recibido. El sistema informático de servidor envía el credencial adicional al sistema informático de cliente a través del enlace seguro establecido. El sistema informático de cliente recibe el credencial adicional desde el sistema informático de servidor. Opcionalmente, el sistema informático de cliente usa posteriormente el credencial adicional recibido para autenticar con el sistema informático de servidor.

En otras realizaciones, un servidor envía primeras peticiones que incluyen al menos los mecanismos de autenticación desplegados en el sistema informático de servidor. El cliente recibe la primera petición y envía una primera respuesta que incluye al menos los mecanismos de autenticación desplegados en el sistema informático de cliente. El cliente y el servidor identifican una clave de túnel que puede usarse para encriptar contenido transferido entre el sistema informático de cliente y el sistema informático de servidor.

El servidor envía una segunda petición que incluye contenido de autenticación encriptado (encriptado con la clave de túnel) que indica un mecanismo de autenticación mutuamente desplegado. El cliente recibe la segunda petición y desencripta el contenido de autenticación encriptado con la clave de túnel para revelar el contenido de autenticación desencriptado. Indicando el contenido de autenticación desencriptado el mecanismo de autenticación mutuamente desplegado. El cliente envía una segunda respuesta que incluye datos de respuesta encriptados que son la respuesta al contenido de autenticación desencriptado. Los datos de respuesta encriptados contienen información para autenticar con el servidor de acuerdo con el mecanismo de autenticación mutuamente desplegado. El servidor recibe la segunda respuesta que incluye los datos de respuesta encriptados que contienen información para autenticar con el servidor de acuerdo con el mecanismo de autenticación mutuamente desplegado.

Se expondrán características y ventajas adicionales de la invención en la descripción que sigue, y en parte serán evidentes a partir de la descripción, o pueden aprenderse mediante la puesta en práctica de la invención. Las características y ventajas de la invención pueden realizarse y obtenerse por medio de los instrumentos y combinaciones particularmente señaladas en las reivindicaciones adjuntas. Estas y otras características de la presente invención se harán más completamente evidentes a partir de la siguiente descripción y reivindicaciones adjuntas, o pueden aprenderse mediante la puesta en práctica de la invención como se expone en lo sucesivo.

**Breve descripción de los dibujos**

Para describir la manera en la que pueden obtenerse las ventajas y características anteriormente indicadas y otras de la invención, se presentará una descripción más particular de la invención descrita brevemente antes por referencia a las realizaciones específicas de la misma que se ilustran en los dibujos adjuntos. Entendiéndose que estos dibujos representan únicamente realizaciones típicas de la invención y no se consideran por lo tanto que son limitantes de su alcance, la invención se describirá y explicará con especificidad y detalle adicional a través del uso de los dibujos adjuntos en los que:

La Figura 1 ilustra la arquitectura informática de ejemplo que facilita autenticación más eficaz y segura de un sistema informático de acuerdo con la presente invención.

La Figura 2 ilustra un diagrama de flujo de un procedimiento de ejemplo para aprovisionar credenciales.

La Figura 3 ilustra un intercambio de mensaje para procedimientos de autenticación de negociación automáticamente.

La Figura 4 ilustra un entorno de operación adecuado para implementar los principios de la presente invención.

**Descripción detallada de las realizaciones preferidas**

Los principios de la presente invención se refieren a sistemas, procedimientos y productos de programa informático para sistemas informáticos de autenticación más eficaces y más seguros. Las realizaciones dentro del alcance de la presente invención incluyen medios legibles por ordenador para llevar a cabo o tener instrucciones ejecutables por ordenador o estructuras de datos almacenadas en los mismos. Tal medio legible por ordenador puede ser cualquier medio disponible, que sea accesible mediante un sistema informático de fin general o de fin especial. A modo de ejemplo, y no como limitación, tal medio legible por ordenador puede comprender medio de almacenamiento físico tal como RAM, ROM, EPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para llevar o almacenar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador, instrucciones legibles por ordenador, o estructuras de datos y que pueda accederse mediante un sistema informático de fin general o de fin especial.

En esta descripción y en las siguientes reivindicaciones, una “red” se define como uno o más enlaces de datos que posibilitan el transporte de datos electrónicos entre sistemas y/o módulos informáticos. Cuando se transfiere la información o se proporciona a través de una red u otra conexión de comunicaciones (ya sea de cableado permanente, inalámbrica o una combinación de cableado permanente o inalámbrica) a un sistema informático, la conexión se observa apropiadamente como un medio legible por ordenador. Por lo tanto, cualquier tal conexión se denomina apropiadamente un medio legible por ordenador. Combinaciones de lo anterior deberían incluirse también

dentro del alcance de medio legible por ordenador. Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que provocan que un sistema informático de fin general o sistema informático de fin especial realice una cierta función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, binarios, instrucciones de formato intermedio tal como lenguaje ensamblador o incluso código fuente.

En esta descripción y en las siguientes reivindicaciones, un “sistema informático” se define como uno o más módulos de software, uno o más módulos de hardware, o combinaciones de los mismos, que funcionan juntos para realizar operaciones en datos electrónicos. Por ejemplo, la definición de sistema informático incluye los componentes de hardware de un ordenador personal, así como módulos de software, tal como el sistema operativo del ordenador personal. La distribución física de los módulos no es importante. Un sistema informático puede incluir uno o más ordenadores acoplados mediante una red. Análogamente, un sistema informático puede incluir un único dispositivo físico (tal como un teléfono móvil o Asistente Digital Personal “PDA”) donde los módulos internos (tales como una memoria y procesador) funcionan juntos para realizar operaciones en datos electrónicos.

Como se usa en el presente documento, el término “módulo” o “componente” puede referirse a objetos de software o rutinas que se ejecutan en el sistema informático. Los diferentes componentes, módulos, motores, y servicios descritos en el presente documento pueden implementarse como objetos o procedimientos que se ejecutan en el sistema informático (por ejemplo, como hilos separados). Aunque el sistema y procedimientos descritos en el presente documento se implementan preferentemente en software, las implementaciones en software y hardware o hardware son también posibles y se contemplan.

Los expertos en la materia apreciarán que la invención puede ponerse en práctica en entornos informáticos de red con muchos tipos de configuraciones de sistemas informáticos, incluyendo, ordenadores personales, ordenadores portátiles, dispositivos portátiles, sistemas multiprocesador, electrónica de consumo programable o basada en microprocesador, PC de red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, y similares. La invención puede ponerse también en práctica en entornos de sistemas distribuidos donde sistemas informáticos locales y remotos, que están enlazados (mediante enlaces de datos de cableado permanente, enlaces de datos inalámbricos o mediante una combinación de enlaces de datos de cableado permanente e inalámbrico) a través de una red, ambos realizan tareas. En un entorno de sistema distribuido, los módulos de programa pueden localizarse tanto en dispositivos de almacenamiento de memoria locales como remotos.

La Figura 1 ilustra la arquitectura 100 informática de ejemplo que facilita autenticación más eficaz y segura de un sistema informático de acuerdo con la presente invención. Como se representa en la arquitectura 100 informática, el sistema 101 informático de cliente incluye el par 103 de claves. El par 103 de claves incluye la clave 104 pública y la correspondiente clave 106 privada, por ejemplo, un par de claves Diffie-Hellman. El sistema 111 informático de servidor incluye el módulo 112 de aprovisionamiento de credenciales y el par 113 de claves. El módulo 112 de aprovisionamiento de credenciales puede configurarse para recibir un primer tipo de credencial, tal como, por ejemplo, un credencial de uso limitado, y, basado en el primer tipo de credencial, aprovisionar un segundo tipo de credencial, tal como, por ejemplo, un credencial más permanente. De manera similar al par 103 de claves, el par 113 de claves incluye la clave 114 pública y la correspondiente clave 116 privada, por ejemplo, un par de claves Diffie-Hellman.

La Figura 2 ilustra un diagrama de flujo de un procedimiento 200 de ejemplo para aprovisionar credenciales. El procedimiento 200 se describirá con respecto a los sistemas informáticos y módulos en la arquitectura 100 informática. El procedimiento 200 incluye un acto de recibir un credencial de uso limitado (acto 201). Por ejemplo, el sistema 101 informático de cliente puede recibir el credencial 102 de uso limitado.

El uso de un credencial de uso limitado puede limitarse en cualquier número de maneras. Por ejemplo, el credencial de uso limitado puede ser válido durante un número de usos especificado, durante un periodo de tiempo especificado o hasta la aparición de un evento especificado. Un credencial de uso limitado puede limitarse a cualquier número de usos válidos (por ejemplo, tres usos), basándose en políticas de seguridad aplicables. Los credenciales de uso limitado que son válidos para autenticar únicamente una vez pueden denominarse como “credenciales de único uso”. Después de los números especificados de uso, el credencial de uso limitado ya no se acepta como un credencial válido.

Un credencial de uso limitado puede limitarse a cualquier periodo de tiempo especificado (por ejemplo, cinco minutos), basándose en políticas de seguridad aplicables. Después de que un periodo de tiempo especificado expira, el credencial de uso limitado ya no se acepta como un credencial válido. Cualquier evento especificado puede limitar el uso de un credencial de uso limitado, basándose en políticas de seguridad aplicables. Por ejemplo, un credencial de uso limitado puede rechazarse después de que no se aprovisionan más credenciales permanentes.

Un credencial de uso limitado puede recibirse mediante procedimientos de comunicación fuera de banda, tales como, por ejemplo, comunicación telefónica o correo. Como alternativa, pueden usarse también procedimientos de comunicación informatizados confiables para recibir un credencial de uso limitado (por ejemplo, encriptar el credencial de uso limitado en un mensaje de correo electrónico).

El procedimiento 200 incluye un acto de establecer un lado de cliente un enlace seguro (acto 202) y establecer un lado de servidor un enlace seguro (acto 205). Por ejemplo, el sistema 101 informático de cliente y el sistema 111 informático de servidor pueden establecer el enlace 122 seguro. El establecimiento de un enlace seguro puede incluir que el sistema 101 informático de cliente y el sistema 111 informático de servidor intercambien claves públicas para establecer una clave de sesión. Por ejemplo, la clave 104 pública y la clave 114 pública pueden intercambiarse para establecer la clave 131 de sesión. En algunas realizaciones, el establecimiento de una clave de sesión puede ser suficiente para autenticación posterior, tal como, por ejemplo, cuando el sistema 101 informático de cliente y el sistema 111 informático de servidor están configurados con claves de Diffie-Hellman estáticas.

Como alternativa, pueden obtenerse otras claves para proporcionar otra prueba. Por ejemplo, en respuesta a un desafío desde un sistema informático de servidor, un sistema informático de cliente puede encriptar una contraseña usando una clave de encriptación obtenida desde la clave de sesión Diffie-Hellman y la contraseña y enviar la clave de encriptación al sistema informático de servidor. Por consiguiente, cuando el sistema informático de servidor recibe la contraseña encriptada, el sistema informático de servidor puede desencriptar la contraseña y comparar la contraseña con una base de datos de credenciales para determinar si la contraseña es válida.

De manera similar, un sistema informático de cliente puede encriptar un ancla de confianza usando una clave de encriptación obtenida desde un secreto compartido y la clave de sesión Diffie-Hellman y enviar el ancla de confianza encriptada a un sistema informático de servidor. Por consiguiente, cuando el sistema informático de servidor recibe el ancla de confianza encriptada, el sistema informático de servidor puede desencriptar y validar el ancla de confianza. Un ancla de confianza incluye datos relacionados con la autenticación, tales como, por ejemplo, un certificado, (por ejemplo, un certificado X.509), un testigo de seguridad (por ejemplo, un testigo de seguridad WS), un troceo (por ejemplo, SHA-1) y el Identificador de Recursos Uniforme (“URI”) (por ejemplo, un Localizador de Recursos Uniforme (“URL”)) de un certificado, o un troceo y URI de un testigo de seguridad.

Análogamente, un sistema informático de cliente puede enviar una nueva ancla de confianza que está firmada con o incluye un resumen de un ancla de confianza previamente establecida. Por consiguiente, el sistema informático de servidor puede validar la nueva ancla de confianza basándose en la firma o troceo del ancla de confianza previamente establecida.

Haciendo referencia de nuevo a la Figura 2, el procedimiento 200 incluye un acto de presentar el credencial de uso limitado a través del enlace seguro establecido (acto 203). Por ejemplo, el sistema 101 informático de cliente puede presentar el credencial 102 de uso limitado al sistema 111 informático de servidor a través del enlace 122 seguro. Como se ha descrito anteriormente, una clave de encriptación obtenida desde la clave de sesión Diffie-Hellman y una contraseña pueden usarse para encriptar la contraseña. Por lo tanto, puede ser que el credencial 102 de uso limitado esté encriptado usando una clave de encriptación obtenida desde la clave 131 de sesión y el credencial 102 de uso limitado.

El procedimiento 200 incluye un acto de recibir un credencial de uso limitado a través del enlace seguro establecido (acto 206). Por ejemplo, el sistema 111 informático de servidor puede recibir el credencial 102 de uso limitado desde el sistema 101 informático de cliente a través del enlace 122 seguro. También, en respuesta a una petición anterior, el sistema 111 informático de servidor puede recibir una clave de encriptación (por ejemplo, usada para encriptar el credencial 102 de uso limitado) desde el sistema 101 informático de cliente.

El procedimiento 200 incluye un acto de aprovisionar un credencial adicional para el cliente basándose en el credencial de uso limitado recibido (acto 207). Por ejemplo, el módulo 112 de aprovisionamiento de credenciales puede aprovisionar un credencial (o credenciales) más permanente para el sistema 101 informático de cliente basándose en credencial 102 de uso limitado. Cuando sea apropiado, el sistema 111 informático de servidor puede desencriptar el credencial 102 de uso limitado usando una clave de encriptación previamente recibida.

El módulo 112 de aprovisionamiento de credenciales puede comparar el credencial 102 de uso limitado con una base de datos de credenciales para determinar si el credencial 102 de uso limitado es válido. Cuando el credencial 102 de uso limitado no es válido, el sistema 111 informático de servidor puede terminar el procesamiento del credencial 102 de uso limitado. Dependiendo de las políticas de seguridad, el sistema 111 informático de servidor puede o puede no notificar al sistema 101 informático de cliente que el procesamiento del credencial 102 de uso limitado terminó. Por otra parte, cuando el credencial 102 de uso limitado es válido, existe una fiabilidad aumentada en la identidad del sistema 101 informático de cliente. Por consiguiente, el sistema informático de servidor puede generar un credencial (o credenciales) más permanente para el sistema 101 informático de cliente. Por ejemplo, el módulo 112 de aprovisionamiento de credenciales puede generar el credencial 117 adicional.

El credencial 117 adicional puede ser el mismo tipo de credencial que el credencial 102 de uso limitado. Por ejemplo, en respuesta a recibir una contraseña de único uso apropiada, el sistema 111 informático de servidor puede expedir una contraseña más permanente. Como alternativa, el credencial 117 adicional puede ser un tipo diferente de credencial. Por ejemplo, en respuesta a recibir una contraseña de único uso apropiada, el sistema 111 informático de servidor puede expedir un certificado, un testigo (por ejemplo, un testigo de seguridad WS o testigo Kerberos), un troceo y URI de un certificado, o un troceo y URI de un testigo.

Otros datos de soporte de credenciales, tales como, cadenas de certificados, lista de revocación de certificados, respuestas de protocolo de estado de certificado en línea, testigos de seguridad WS y metadatos que se han de asociar con un intercambio, pueden identificarse también. Los metadatos identificados pueden incluir instrucciones del Lenguaje de Marcado Extensible ("XML").

El procedimiento 200 incluye un acto de enviar un credencial adicional (acto 208). Por ejemplo, el sistema 111 informático de servidor puede enviar un credencial 117 adicional al sistema 101 informático de cliente. El procedimiento 200 incluye un acto de recibir un credencial adicional (acto 204). Por ejemplo, el sistema 101 informático de cliente puede recibir el credencial 117 adicional desde el sistema 111 informático de servidor.

Por consiguiente, las realizaciones de la presente invención pueden facilitar el acceso a una red cuando el acceso puede evitarse de otra manera. Por ejemplo, un credencial de uso limitado (o único uso) puede usarse mediante un sistema informático inalámbrico para facilitar acceso a un certificado usado para acceder inalámbricamente a una red. Además, los credenciales de uso limitado pueden reducir la vulnerabilidad del sistema informático a ataques de diccionario. Por ejemplo, un credencial de uso limitado puede ya no ser válido en el momento que un usuario malicioso eventualmente rompa el credencial de uso limitado. En particular, puesto que un credencial de único uso se hace inválido después de que se usa la primera vez, los credenciales de único uso pueden reducir significativamente la vulnerabilidad a ataques de diccionario.

La Figura 3 ilustra un intercambio 300 de mensaje para mecanismos de autenticación de negociación. Debería entenderse que el intercambio 300 de mensaje puede tener lugar antes o después del intercambio de otros mensajes durante la autenticación. Por ejemplo, un sistema informático de cliente y sistema informático de servidor pueden intercambiar uno o más pares petición/respuesta del Protocolo de Autenticación Extensible ("EAP") que identifican preliminarmente el sistema informático de cliente y el sistema informático de servidor entre sí.

Las peticiones y respuestas representadas en el intercambio 300 de mensaje pueden ser mensajes de un protocolo de autenticación. Cada mensaje puede incluir el número de versión del protocolo de autenticación (por ejemplo, representando tipos de cabida útil soportados), un cuerpo de mensaje, y un Código de Autenticación de Mensaje Troceado ("HMAC") de una porción del cuerpo del mensaje. Un HMAC puede generarse usando cualquier función de troceo criptográfico, tal como, por ejemplo, MD5, SHA-1, etc. Los mensajes del protocolo de autenticación pueden embeberse con mensajes de EAP.

El lado 360 de servidor puede enviar la petición 301 de servidor al lado 305 del cliente. La petición 301 de servidor incluye el ID 302 de paquete anterior, número aleatorio usado solo una vez 303, y los procedimientos 304 de autenticación. El ID 302 de paquete anterior puede indicar el ID de paquete que corresponde al último paquete que se intercambió entre el lado 350 de cliente y el lado 360 de servidor (por ejemplo, el ID de paquete del paquete en un intercambio de petición/respuesta anterior). El número aleatorio usado solo una vez 303 puede ser datos aleatorios generados en el lado 360 de servidor. Los procedimientos 305 de autenticación pueden incluir los mecanismos de autenticación propuestos soportados en el lado 360 de servidor. Un lado de servidor puede soportar cualquier número de diferentes mecanismos de autenticación (por ejemplo, desafíos y respuestas como se ha descrito anteriormente, MS-CHAP v2, autenticación con MD5, autenticación con Tarjeta de Testigo Genérica, autenticación con Kerberos, autenticación con X.509, y autenticación con seguridad WS).

En respuesta a la petición 301 de servidor, el lado 350 de cliente puede enviar la respuesta 306 de cliente al lado 306 de servidor. La respuesta 306 de cliente puede incluir el ID 307 de paquete anterior, el número aleatorio usado solo una vez 308, asociación o asociaciones 309 de seguridad, clave o claves 311 públicas, y procedimientos 312 de autenticación. El ID 307 de paquete anterior puede indicar el ID de paquete que corresponde a la petición 301 de servidor. El número aleatorio usado solo una vez 308 puede ser datos aleatorios generados en el lado 360 de cliente. La asociación o asociaciones 309 de seguridad pueden incluir asociaciones de seguridad propuestas que se soportan en el lado 350 de cliente. La Tabla 1 indica alguna de las asociaciones de seguridad que pueden soportarse.

**Tabla 1**

| |
|---|
| Modo 128 bits AES CBC<br>Diffie-Hellman Grupo 2 (1024 bits)<br>SHA-1 + HMAC<br>Troceo SHA-1 |
| Modo 128 bits AES CBC<br>Diffie-Hellman Grupo 5 (1536 bits)<br>SHA-1 + HMAC<br>Troceo SHA-1 |
| Modo 128 bits AES CBC<br>Diffie-Hellman Grupo 14 (2048 bits)<br>SHA-1 + HMAC<br>Troceo SHA-1 |

(continuación)

| |
|---|
| Modo 128 bits AES CBC |
| ECC Diffie-Hellman Grupo 4 (185 bits) |
| SHA256 HMAC |
| Troceo SHA256 |

La clave o claves 311 públicas pueden incluir una o más claves públicas. La clave o claves 311 públicas pueden incluir una clave de una longitud apropiada (por ejemplo, 1024 bits, 2048 bits, etc.) para cada asociación de seguridad soportada. La clave o claves 311 públicas pueden ser una o más claves públicas Diffie-Hellman incluyendo, por ejemplo, la clave 104 pública. Los procedimientos 312 de autenticación pueden incluir mecanismos de autenticación soportados en el lado 350 de cliente y seleccionados de entre los mecanismos de autenticación incluidos en los procedimientos 304 de autenticación.

En respuesta a la respuesta 306 de cliente, el lado 360 de servidor puede enviar la petición 313 de servidor. La petición 313 de servidor puede incluir el ID 314 de paquete anterior, la asociación 316 de seguridad, la clave 317 pública, y otros datos de autenticación basándose en el procedimiento de autenticación. El ID 314 de paquete anterior puede indicar el ID de paquete que corresponde a la respuesta 306 de cliente. La asociación 316 de seguridad puede indicar una asociación de seguridad soportada en el lado 360 de servidor y seleccionada de entre los procedimientos de autenticación incluidos en la asociación o asociaciones 309 de seguridad. La clave 317 pública puede ser una clave de longitud apropiada para la asociación de seguridad indicada en la asociación 316 de seguridad. La clave 317 pública puede ser una clave pública Diffie-Hellman, tal como, por ejemplo, la clave 114 pública.

Por consiguiente, basándose en la clave de longitud apropiada desde la clave o claves 311 públicas y la clave 317 pública, puede establecerse un enlace seguro entre el lado 350 de cliente y el lado 360 de servidor.

En general, los datos encriptados enviados entre el lado 350 de cliente y el lado 360 de servidor se encriptan usando una clave de túnel. La clave de túnel puede obtenerse troceando la concatenación de un secreto compartido Diffie-Hellman (por ejemplo, la clave 131 de sesión) junto con los números aleatorios usados solo una vez de cliente y de servidor. Por ejemplo, puede obtenerse una clave de túnel de acuerdo con la siguiente fórmula:

$$\textbf{Clave de túnel} = \textbf{TROCEO}\ [DH_{SS} + N_c + N_s]$$

Una clave de túnel puede ser una clave simétrica. Es decir la clave de túnel puede usarse para desencriptar datos encriptados que se encriptaron usando la clave de túnel. Por consiguiente, el lado 350 de cliente puede encriptar datos que se han de enviar al lado 360 de servidor con la clave de túnel y puede desencriptar contenido recibido desde el lado 360 de servidor con la clave de túnel. De manera similar, el lado 360 de servidor puede encriptar datos que se han de enviar al lado 350 de cliente con la clave de túnel y puede desencriptar contenido recibido desde el lado 350 de cliente usando la clave de túnel.

Cuando el lado 350 de cliente y el lado 360 de servidor están realizando una negociación, la petición 313 de servidor puede incluir el contenido 318 encriptado de negociación. El contenido 318 encriptado de negociación puede incluir el desafío 319, el procedimiento 321 de autenticación, y el ancla 322 de confianza. El desafío 319 puede ser un HMAC del ID de paquete anterior (por ejemplo, el ID 314 de paquete anterior) que usa un secreto compartido (por ejemplo, la clave 131 de sesión). Por ejemplo, el desafío 319 puede configurarse de acuerdo con la siguiente fórmula:

$$\textbf{Desafío} = \textbf{HMAC}_{SS}\ [\textbf{PPid}]$$

El lado 360 de servidor puede mantener una respuesta apropiada al desafío. Por ejemplo, una respuesta apropiada puede ser el HMAC del desafío usando el secreto compartido. Una respuesta apropiada puede configurarse de acuerdo con la siguiente fórmula:

$$\textbf{Respuesta}_S = \textbf{HMAC}_{SS}\ [\textbf{Desafío}]$$

El procedimiento 321 de autenticación puede indicar un procedimiento de autenticación que se soporta mutuamente en el lado 350 de cliente y el lado 360 de servidor. El ancla 322 de confianza puede ser un ancla de confianza como se ha descrito anteriormente.

Cuando el lado 350 de cliente está volviéndose a autenticar con el lado 360 de servidor (por ejemplo, autenticando algún tiempo después de una negociación), la petición 313 de servidor puede incluir como alternativa la re-autenticación encriptada 328. El contenido encriptado de re-autenticación puede incluir la firma 329 de autenticación y el certificado 331 de identidad. La firma 329 de autenticación puede incluir un tipo de ID de firma (por ejemplo, SHA-1 (longitud de ID de clave = 20 octetos) o SHA256 (longitud de ID de clave = 32 octetos)), un ID de clave de firma y un tipo de firma (por ejemplo, HMAC, RSA PKCS N.º 1, RSA PSS, o DSA). El certificado 331 de identidad puede incluir, por ejemplo, un certificado X.509, un testigo Kerberos, un testigo de seguridad WS, una Clave Pública

en Bruto, un troceo y URL o un certificado X.509, un troceo y URL de un testigo de seguridad WS, un troceo y URL de una clave pública en bruto.

Debería entenderse que otros tipos de contenido de autenticación encriptado (en lugar del contenido 318 encriptado de negociación o el contenido 328 encriptado de re-autenticación) pueden incluirse como alternativa en la petición 313 de servidor. Por ejemplo, cuando se arranca un cliente usando un nombre de usuario y contraseña existentes, la petición 313 de servidor puede tener contenido encriptado que incluye una firma de autenticación, un certificado de identidad, y un procedimiento de autenticación.

Cuando se arranca un nuevo cliente con un certificado X.509, la petición 313 de servidor puede tener contenido encriptado que incluye un desafío, un ancla de confianza, un procedimiento de autenticación, y una petición de inscripción. Una petición de inscripción puede incluir un tipo de petición (por ejemplo, petición TGT de Kerberos, petición AS de Kerberos, petición PCKS N.º 10, o petición CMC), un tipo de clave (por ejemplo, firma RSA, DSA, ECDSA, o DH + ECDH), un sub-tipo de clave (por ejemplo, claves de firma PSA o claves DH + ECDH) y un tamaño de clave (por ejemplo, 1024 bits). Cuando se autentica con un certificado X.509, la petición 313 puede tener contenido encriptado que incluye una firma de autenticación, un certificado de identidad, y un procedimiento de autenticación.

Cuando se arranca un nuevo cliente con un tique de Kerberos, la petición 313 de servidor puede tener contenido encriptado que incluye un desafío y una petición de inscripción.

En respuesta a la petición 313 de servidor, el lado 350 de cliente puede enviar la respuesta 332 de cliente. La respuesta 332 de cliente puede incluir el ID 333 de paquete anterior y datos en respuesta a contenido encriptado incluido en la petición 313 de servidor. El ID 333 de paquete anterior puede indicar el ID de paquete que corresponde a la petición 313 de servidor. Cuando el lado 350 de cliente y el lado 360 de servidor están realizando una negociación, la respuesta 332 de cliente puede incluir la respuesta 334 encriptada (encriptada con la clave de túnel). La respuesta 334 encriptada puede ser una respuesta al desafío 319.

El lado 350 de cliente puede generar una respuesta apropiada al desafío 319. Por ejemplo, una respuesta apropiada puede ser el HMAC del desafío 119 usando un secreto compartido. Una respuesta apropiada puede configurarse de acuerdo con la siguiente fórmula:

$$\textbf{Respuesta}_{c} = \textbf{HMAC}_{SS}\ \textbf{[Desafío]}$$

Cuando el lado 350 de cliente se vuelve a autenticar con el lado 360 de servidor, la respuesta 332 de cliente puede incluir la firma 336 de autenticación.

Debería entenderse que otros tipos de datos en respuesta al contenido de autenticación encriptado (en lugar de la respuesta 334 encriptada o la firma 336 de autenticación) pueden incluirse como alternativa en la respuesta 332 de cliente. Por ejemplo, cuando se arranca un cliente usando un nombre de usuario y contraseña existentes, la respuesta 332 de cliente puede tener datos de respuesta encriptados que incluyen un desafío, una cabida útil de identidad de usuario final y una cabida útil de identidad de dominio. Las cabidas útiles de identidad de usuario final y cabidas útiles de identidad de dominio pueden incluir un tipo de nombre (por ejemplo, nombre de DNS completamente calificado, una dirección de correo electrónico, una dirección de IPv4, y la dirección de IPv6, un nombre distinguido X.500 codificado DER, o un nombre de ámbito).

Cuando se arranca un nuevo cliente con un certificado X.509, la respuesta 332 de cliente puede tener datos de respuesta encriptados que incluyen una respuesta y una petición de certificado. Cuando se autentica con un certificado X.509, la respuesta 332 de cliente puede tener datos de respuesta encriptados que incluyen una firma de autenticación y un certificado de identidad. Cuando se arranca un nuevo cliente con un tique de Kerberos, la respuesta 332 de cliente puede tener datos de respuesta encriptados que incluyen una respuesta y una petición de certificado.

Las realizaciones de la presente invención facilitan los mecanismos de autenticación de negociación de entre un número de diferentes mecanismos de autenticación. Los sistemas informáticos de cliente y los sistemas informáticos de servidor pueden identificar mecanismos de autenticación mutuamente soportados y usar mecanismos identificados para autenticación. La negociación automatizada aligera que un usuario tenga que tener conocimiento de los mecanismos de autenticación que pueden desplegarse para una red. Por consiguiente, la autenticación puede realizarse más eficazmente.

La Figura 4 y el siguiente análisis se pretenden para proporcionar una breve descripción general de un entorno informático adecuado en el que puede implementarse la invención. Aunque no se requiere, la invención se describirá en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, que se ejecutan mediante sistemas informáticos. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, y similares, que realizan tareas particulares o implementan tipos de datos abstractos particulares. Las instrucciones ejecutables por ordenador, estructuras de datos asociadas, y módulos de programa representan ejemplos de los medios de código de programa para ejecutar actos de los procedimientos desvelados en el presente documento.

Con referencia a la Figura 4, un sistema de ejemplo para implementar la invención incluye un dispositivo informático de fin general en forma del sistema 420 informático, que incluye una unidad 421 de procesamiento, una memoria 422 de sistema, y un bus 423 de sistema que acopla diversos componentes de sistema incluyendo la memoria 422 de sistema a la unidad 421 de procesamiento. La unidad 421 de procesamiento puede ejecutar instrucciones ejecutables por ordenador diseñadas para implementar características del sistema 420 informático, incluyendo las características de la presente invención. El bus 423 de sistema puede ser cualquiera de varios tipos de estructuras de bus incluyendo un bus de memoria o controlador de memoria, un bus periférico y un bus local que usa cualquiera de una diversidad de arquitecturas de bus. La memoria de sistema incluye memoria de solo lectura ("ROM") 424 y memoria de acceso aleatorio ("RAM") 425. Un sistema básico de entrada/salida ("BIOS") 426, que contiene las rutinas básicas que ayudan a transferir información entre elementos en el sistema 420 informático, tales como durante el arranque, puede almacenarse en la ROM 424.

El sistema 420 informático puede incluir también la unidad 427 de disco duro magnético para leer desde y escribir al disco 439 duro magnético, la unidad 428 de disco magnético para leer desde o escribir al disco 429 magnético extraíble, y la unidad 430 de disco óptico para leer desde o escribir en el disco 431 óptico extraíble, tal como, por ejemplo, un CD-ROM u otro medio óptico. La unidad 427 de disco duro magnético, la unidad 428 de disco magnético, y la unidad 430 de disco óptico están conectadas al bus 423 de sistema mediante la interfaz 432 de unidad de disco duro, la interfaz 433 de unidad de disco magnético, y la interfaz 434 de disco óptico, respectivamente. Las unidades y sus medios legibles por ordenador asociados proporcionan almacenamiento no volátil de instrucciones ejecutables por ordenador, estructuras de datos, módulos de programa, y otros datos para el sistema 420 informático. Aunque el entorno de ejemplo descrito en el presente documento emplea el disco 439 duro magnético, el disco 429 magnético extraíble y el disco 431 óptico extraíble, pueden usarse otros tipos de medios legibles por ordenador para almacenar datos, incluyendo cintas magnéticas, tarjetas de memoria flash, discos versátiles digitales, cartuchos Bernoulli, RAM, ROM, y similares. El almacenamiento 132 puede ser una porción de uno de los tipos descritos de medios legibles por ordenador.

Los medios de código de programa que comprenden uno o más módulos de programa pueden almacenarse en el disco 439 duro, disco 429 magnético, disco 431 óptico, ROM 424 o RAM 425, incluyendo un sistema 435 operativo, uno o más programas 436 de aplicación, otros módulos 437 de programa y datos 438 de programa. Un usuario puede introducir comandos e información en el sistema 420 informático a través del teclado 440, dispositivo apuntador 442, u otros dispositivos de entrada (no mostrados), tales como, por ejemplo, un micrófono, palanca de mandos, control de juegos, escáner, o similares. Estos y otros dispositivos de entrada pueden conectarse a la unidad 421 de procesamiento a través de la interfaz 446 de entrada/salida acoplada al bus 423 de sistema. La interfaz 446 de entrada/salida representa lógicamente cualquiera de una amplia diversidad de posibles interfaces, tales como, por ejemplo, una interfaz de puerto serie, una interfaz PS/2, una interfaz de puerto paralelo, una interfaz de Bus Serie Universal ("USB"), o una interfaz del Instituto de Ingenieros Eléctricos y Electrónicos ("IEEE") 1394 (es decir, una interfaz Firewire), o puede incluso representar lógicamente una combinación de diferentes interfaces.

Un monitor 447 u otro dispositivo de visualización está también conectado al bus 423 de sistema mediante la interfaz 448 de vídeo. El monitor 447 puede visualizar objetos gráficos monocromo y/o de color, incluyendo texto, generado mediante el sistema 420 informático. Otros dispositivos periféricos (no mostrados), tales como, por ejemplo, altavoces, impresoras y escáneres, pueden conectarse también al sistema 420 informático. Las impresoras conectadas al sistema 447 informático pueden imprimir objetos gráficos monocromo y/o de color, incluyendo texto, generados mediante el sistema 420 informático.

El sistema 420 informático es conectable a redes, tales como, por ejemplo, una red informática por toda la oficina o por toda la empresa, una red doméstica, una intranet, y/o internet. El sistema 420 informático puede intercambiar datos con fuentes externas, tales como, por ejemplo, sistemas informáticos remotos, aplicaciones remotas y/o bases de datos remotas a través de tales redes.

El sistema 420 informático incluye la interfaz 453 de red, a través de la que el sistema 420 informático recibe datos desde fuentes externas y/o transmite datos a fuentes externas. Como se representa en la Figura 4, la interfaz 453 de red facilita el intercambio de datos con el sistema 483 informático remoto mediante el enlace 451. La interfaz 453 de red puede representar lógicamente uno o más módulos de software y/o hardware, tales como, por ejemplo, una tarjeta de interfaz de red y correspondiente pila de Especificación de Interfaz de Controlador de Red ("NDIS"). El enlace 451 representa una porción de una red (por ejemplo, un segmento de Ethernet), y el sistema 483 informático remoto representa un nodo de la red.

Análogamente, el sistema 420 informático incluye la interfaz 446 de entrada/salida, a través de la que el sistema 420 informático recibe datos desde fuentes externas y/o transmite datos a fuentes externas. La interfaz 446 de entrada/salida está acoplada al módem 454 (por ejemplo, un módem convencional, un módem de cable, o un módem de línea de abonado digital ("DSL")), a través del cual el sistema 420 informático recibe datos desde y/o transmite datos a las fuentes externas. Como se representa en la Figura 4, la interfaz 446 de entrada/salida y el módem 454 facilitan el intercambio de datos con el sistema 493 informático remoto mediante el enlace 452. El enlace 452 representa una porción de una red y el sistema 493 informático remoto representa un nodo de la red.

Aunque la Figura 4 representa un entorno operativo adecuado para la presente invención, los principios de la presente invención pueden emplearse en cualquier sistema que sea capaz de, o con modificación adecuada si fuera necesario, implementar los principios de la presente invención. El entorno ilustrado en la Figura 4 es ilustrativo únicamente y por ningún medio representa incluso una pequeña porción de la amplia diversidad de entornos en los que pueden implementarse los principios de la presente invención.

De acuerdo con la presente invención, módulos, tales como, por ejemplo, el módulo 112 de aprovisionamiento de credenciales así como datos de programa asociados, tales como, por ejemplo, el credencial 102 de uso limitado, los pares 103 y 113 de claves, las peticiones 301 y 313 de servidor, y las respuestas 306 y 332 de cliente, pueden almacenarse y accederse desde cualquiera de los medios legibles por ordenador asociados con el sistema 420 informático. Por ejemplo, porciones de tales módulos y porciones de datos de programa asociados pueden incluirse en el sistema 435 operativo, programas 436 de aplicación, módulos 437 de programa y/o datos 438 de programa, para almacenamiento en la memoria 422 de sistema.

Cuando un dispositivo de almacenamiento masivo, tal como, por ejemplo, el disco 439 duro magnético, está acoplado al sistema 420 informático, tales módulos y datos de programa asociados pueden almacenarse también en el dispositivo de almacenamiento masivo. En un entorno en red, los módulos de programa representados con relación al sistema 420 informático, o porciones del mismo, pueden almacenarse en dispositivos de almacenamiento de memoria remotos, tales como, memoria de sistema y/o dispositivos de almacenamiento masivo asociados con el sistema 483 informático remoto y/o el sistema 493 informático remoto. La ejecución de tales módulos puede realizarse en un entorno distribuido.

**REIVINDICACIONES**

1. En un sistema (350) informático de cliente, un procedimiento para participar en autenticación con un sistema (360) informático de servidor, comprendiendo el procedimiento:

un acto de recibir una primera petición (301) de servidor que incluye los mecanismos (304) de autenticación desplegados en el sistema (360) informático de servidor y un número aleatorio usado solo una vez (303) de lado de servidor;
un acto de enviar una primera respuesta (306) que incluye los mecanismos (312) de autenticación desplegados en el sistema (350) informático de cliente y un número aleatorio usado solo una vez (308) de lado de cliente;
un acto de identificar una clave de túnel que puede usarse para encriptar contenido transferido entre el sistema informático de cliente y el sistema informático de servidor, que comprende obtener la clave de túnel basándose en un secreto compartido, el número aleatorio usado solo una vez del lado de cliente, y el número aleatorio usado solo una vez del lado de servidor;
un acto de recibir una segunda petición (313) de servidor que incluye contenido (318, 328) de autenticación encriptado, estando encriptado el contenido de autenticación encriptado con la clave de túnel e incluyendo contenido encriptado de negociación que incluye un desafío (319), un mecanismo (321) de autenticación mutuamente desplegado y un ancla (322) de confianza;
un acto de desencriptar el contenido (318, 328) de autenticación encriptado con la clave de túnel para revelar el contenido de autenticación desencriptado; y
un acto de enviar una segunda respuesta (332), incluyendo la segunda respuesta datos (334) de respuesta encriptados que están encriptados con la clave de túnel y que son en respuesta al contenido de autenticación encriptado, que incluyen una respuesta al desafío, los datos de respuesta encriptados para autenticar con el sistema informático de servidor de acuerdo con el mecanismo de autenticación mutuamente desplegado.

2. El procedimiento de acuerdo con la reivindicación 1, en el que la primera petición (301) de servidor incluye adicionalmente un ID (302) de paquete anterior.

3. El procedimiento de acuerdo con la reivindicación 1 o 2, en el que los mecanismos de autenticación desplegados en el sistema informático de servidor incluyen uno o más mecanismos de autenticación seleccionados de entre MS-CHAP v2, autenticación con MD5, autenticación con tarjeta de testigo genérica, autenticación con Kerberos, autenticación con X.509 y autenticación con seguridad WS y/o
en el que los mecanismos de autenticación desplegados en el sistema informático de cliente incluyen uno o más mecanismos de autenticación seleccionados de entre MS-CHAP v2, autenticación con MD5, autenticación con tarjeta de testigo genérica, autenticación con Kerberos, autenticación con X.509 y autenticación con seguridad WS.

4. El procedimiento de acuerdo con una de las reivindicaciones 1 a 3, en el que la primera respuesta incluye adicionalmente un ID (307) de paquete anterior, una o más asociaciones (309) de seguridad y una o más claves (311) públicas.

5. El procedimiento de acuerdo con una de las reivindicaciones 1 a 4,
en el que la segunda petición (313) de servidor incluye el contenido (318, 328) de autenticación encriptado, un ID (314) de paquete anterior, una asociación (316) de seguridad y una clave (317) pública.

6. El procedimiento de acuerdo con una de las reivindicaciones 1 a 5,
en el que la segunda respuesta (332) incluye datos (334) de respuesta encriptados y un ID (333) de paquete anterior.

7. En un sistema (360) informático de servidor, un procedimiento para participar en autenticación con un sistema (350) informático de cliente, comprendiendo el procedimiento:

un acto de enviar una primera petición (301) que incluye los mecanismos (304) de autenticación desplegados en el sistema (360) informático de servidor y un número aleatorio usado solo una vez (303) del lado de servidor;
un acto de recibir una primera respuesta (306) de cliente que incluye los mecanismos (312) de autenticación desplegados en el sistema (350) informático de cliente y un número aleatorio usado solo una vez (308) del lado de cliente;
un acto de identificar una clave de túnel que puede usarse para encriptar contenido transferido entre el sistema informático de cliente y el sistema informático de servidor, que comprende obtener la clave de túnel basándose en un secreto compartido, el número aleatorio usado solo una vez del lado de cliente, y el número aleatorio usado solo una vez del lado de servidor;
un acto de enviar una segunda petición (313) que incluye contenido (318, 328) de autenticación encriptado, estando encriptado el contenido de autenticación encriptado con la clave de túnel, incluyendo el contenido de autenticación encriptado contenido encriptado de negociación que incluye un desafío (319), un mecanismo (321) de autenticación mutuamente desplegado y un ancla (322) de confianza; y
un acto de recibir una segunda respuesta (332) de cliente, incluyendo la segunda respuesta de cliente los datos (334) de respuesta encriptados que están encriptados con la clave de túnel y que son en respuesta al contenido de autenticación encriptado, que incluye una respuesta al desafío, los datos de respuesta encriptados para

autenticar con el sistema informático de servidor de acuerdo con el mecanismo de autenticación mutuamente desplegado.

8. El procedimiento de acuerdo con la reivindicación 7, en el que la primera petición (301) incluye además un ID (302) de paquete anterior.

9. El procedimiento de acuerdo con la reivindicación 7 u 8, en el que los mecanismos de autenticación desplegados en el sistema informático de servidor incluyen uno o más mecanismos de autenticación seleccionados de entre MS-CHAP v2, autenticación con MD5, autenticación con tarjeta de testigo genérica, autenticación con Kerberos, autenticación con X.509 y autenticación con seguridad WS y/o
en el que los mecanismos de autenticación desplegados en el sistema informático de cliente incluyen uno o más mecanismos de autenticación seleccionados de entre MS-CHAP v2, autenticación con MD5, autenticación con tarjeta de testigo genérica, autenticación con Kerberos, autenticación con X.509 y autenticación con seguridad WS.

10. El procedimiento de acuerdo con una de las reivindicaciones 7 a 9, en el que la primera respuesta (306) de cliente incluye adicionalmente un ID (307) de paquete anterior, una o más asociaciones (309) de seguridad y una o más claves (311) públicas.

11. El procedimiento de acuerdo con una de las reivindicaciones 7 a 10,
en el que la segunda petición (313) incluye contenido (318, 328) de autenticación encriptado, un ID (314) de paquete anterior, una asociación (316) de seguridad y una clave (317) pública.

12. El procedimiento de acuerdo con una de las reivindicaciones 7 a 11,
en el que la segunda respuesta (332) de cliente incluye datos (334) de respuesta encriptados y un ID (333) de paquete anterior.

13. Un medio legible por ordenador que comprende instrucciones ejecutables por ordenador que, cuando se ejecutan, realizan el procedimiento de una de las reivindicaciones 1 a 12.

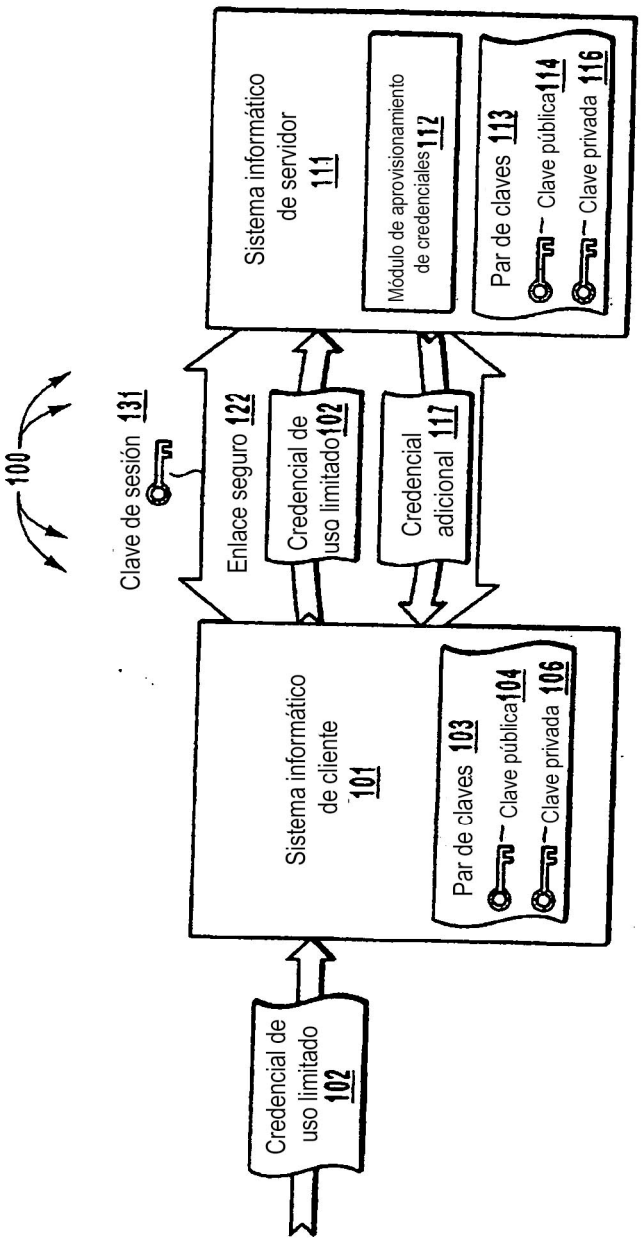
Credencial de uso limitado 102
Sistema informático de cliente 101
Par de claves 103
Clave pública 104
Clave privada 106
Enlace seguro 122
Credencial de uso limitado 102
Credencial adicional 117
Clave de sesión 131
100
Sistema informático de servidor 111
Módulo de aprovisionamiento de credenciales 112
Par de claves 113
Clave pública 114
Clave privada 116

Fig. 1

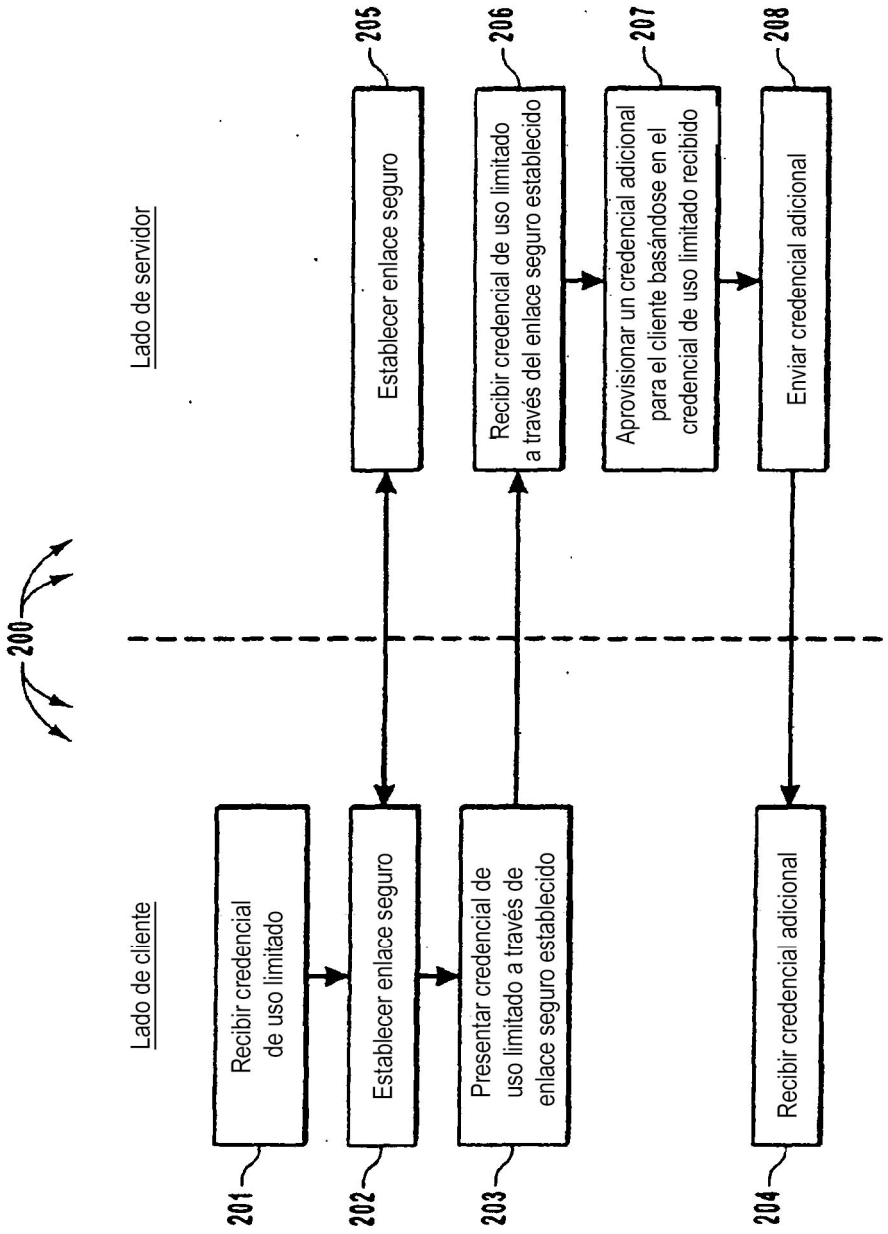
Lado de servidor
Lado de cliente
200
205
Establecer enlace seguro
206
Recibir credencial de uso limitado a través del enlace seguro establecido
207
Aprovisionar un credencial adicional para el cliente basándose en el credencial de uso limitado recibido
208
Enviar credencial adicional
201
Recibir credencial de uso limitado
202
Establecer enlace seguro
203
Presentar credencial de uso limitado a través de enlace seguro establecido
204
Recibir credencial adicional

Fig. 2

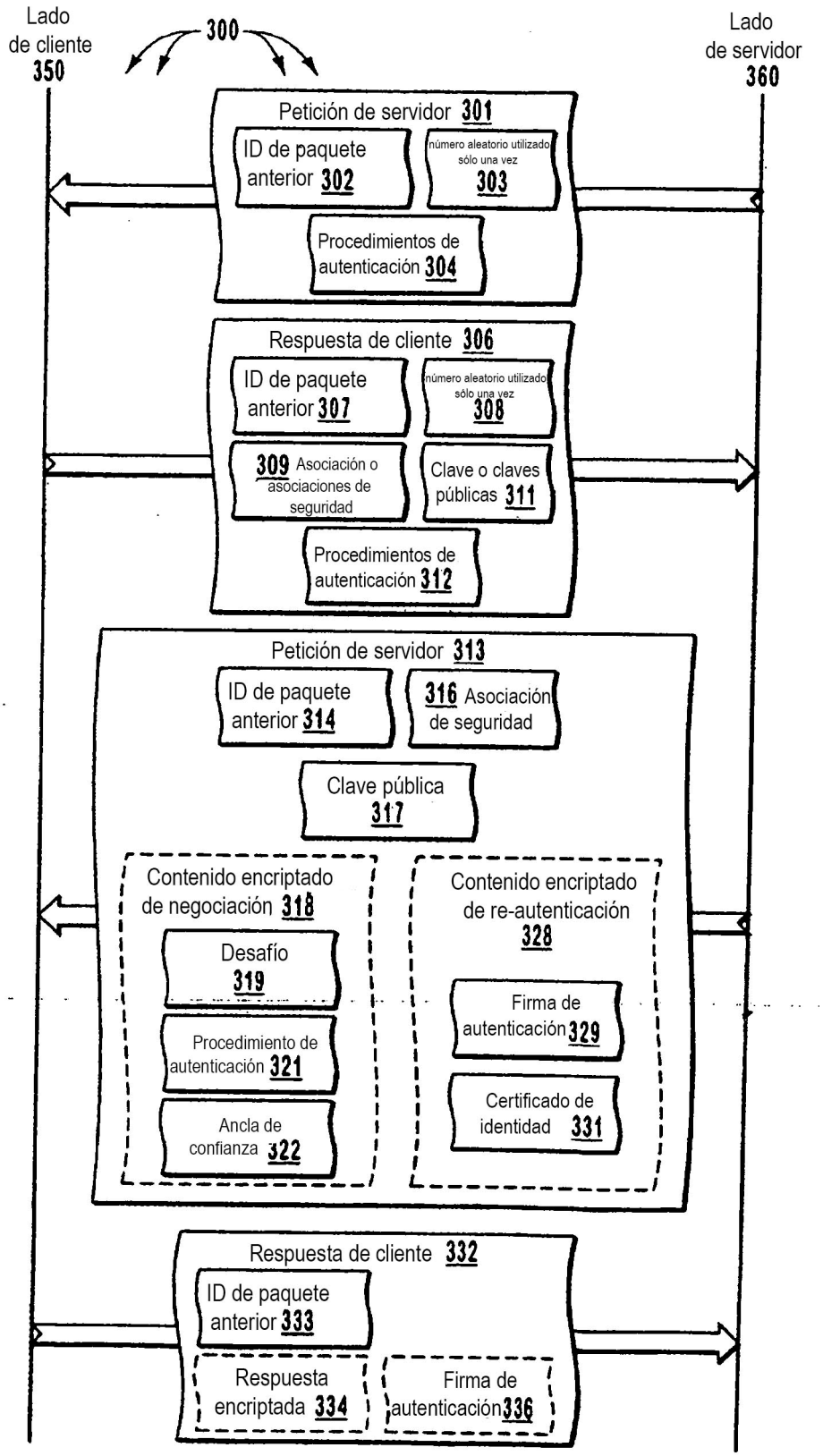
Lado de cliente 350
300
Lado de servidor 360
Petición de servidor 301
ID de paquete anterior 302
número aleatorio utilizado sólo una vez 303
Procedimientos de autenticación 304
Respuesta de cliente 306
ID de paquete anterior 307
número aleatorio utilizado sólo una vez 308
309 Asociación o asociaciones de seguridad
Clave o claves públicas 311
Procedimientos de autenticación 312
Petición de servidor 313
ID de paquete anterior 314
316 Asociación de seguridad
Clave pública 317
Contenido encriptado de negociación 318
Desafío 319
Procedimiento de autenticación 321
Ancla de confianza 322
Contenido encriptado de re-autenticación 328
Firma de autenticación 329
Certificado de identidad 331
Respuesta de cliente 332
ID de paquete anterior 333
Respuesta encriptada 334
Firma de autenticación 336

Fig. 3

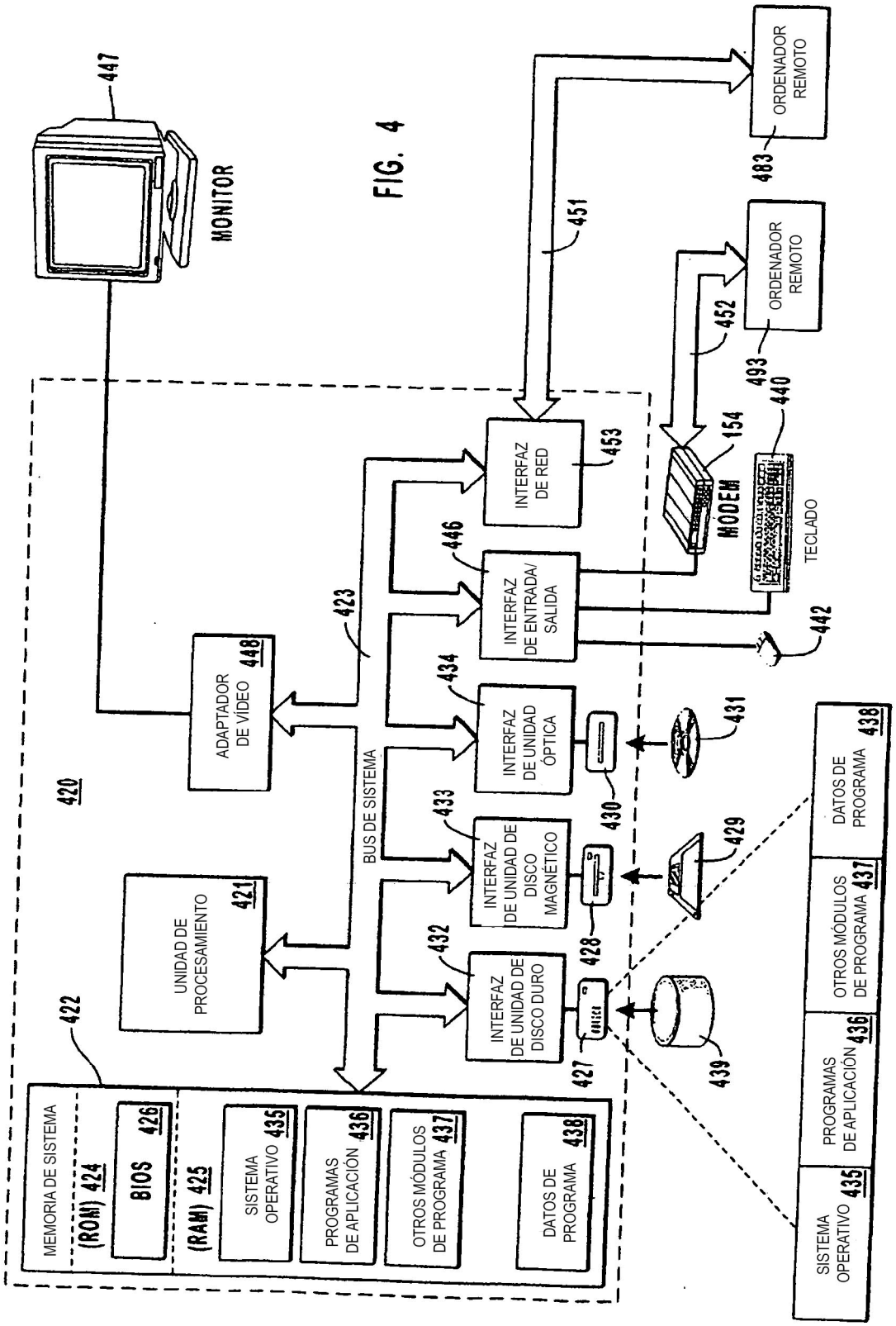
447
MONITOR
ORDENADOR REMOTO
483
451
ORDENADOR REMOTO
452
493
440
154
MÓDEM
TECLADO
INTERFAZ DE RED
453
446
INTERFAZ DE ENTRADA/ SALIDA
442
423
ADAPTADOR DE VÍDEO 448
434
INTERFAZ DE UNIDAD ÓPTICA
431
420
BUS DE SISTEMA
433
INTERFAZ DE UNIDAD DE DISCO MAGNÉTICO
430
429
UNIDAD DE PROCESAMIENTO 421
432
INTERFAZ DE UNIDAD DE DISCO DURO
428
422
MEMORIA DE SISTEMA
(ROM) 424
BIOS 426
(RAM) 425
SISTEMA OPERATIVO 435
PROGRAMAS DE APLICACIÓN 436
OTROS MÓDULOS DE PROGRAMA 437
DATOS DE PROGRAMA 438
427
439
DATOS DE PROGRAMA 438
OTROS MÓDULOS DE PROGRAMA 437
PROGRAMAS DE APLICACIÓN 436
SISTEMA OPERATIVO 435

FIG. 4