(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 423 824**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.11.2003 E 03026812 (2)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2013 EP 1422907**

(54) Título: **Procesamiento con seguridad de credenciales de cliente usadas para el acceso a recursos basado en la Red**

(30) Prioridad:

20.11.2002 US 428152 P
12.06.2003 US 459863

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.09.2013

(73) Titular/es:

MICROSOFT CORPORATION (100.0%)
ONE MICROSOFT WAY
REDMOND, WA 98052, US

(72) Inventor/es:

BRACEWELL, SHAWN DEREK;
WARD, RICHARD B.;
SIMPSON, RUSSELL LEE, JR. y
BATTHISH, KARIM MICHEL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procesamiento con seguridad de credenciales de cliente usadas para el acceso a recursos basado en la Red

Antecedentes de la invención

2. El campo de la invención

La presente invención se refiere a redes de ordenadores y, más específicamente, al procesamiento con seguridad de credenciales de cliente usadas para el acceso a recursos basado en la Red.

3. Antecedentes y técnica relevante

Los sistemas de ordenadores y la tecnología relacionada afectan a muchos aspectos de la sociedad. De hecho, la capacidad de un sistema de ordenador para procesar información ha transformado la manera en que vivimos y trabajamos. Los sistemas de ordenadores en la actualidad realizan usualmente una multitud de tareas (p. ej., procesamiento de la palabra, planificación y gestión de bases de datos) que antes del advenimiento del sistema de ordenador se realizaban manualmente. Más recientemente, los sistemas de ordenadores han sido acoplados entre sí para formar redes de ordenadores, tanto cableadas como inalámbricas, por las cuales los sistemas de ordenadores pueden comunicarse electrónicamente para compartir datos. Como resultado, muchas tareas realizadas en un sistema de ordenador (p. ej., la comunicación de la voz, el acceso al correo electrónico, la conferencias electrónicas, la exploración de la Red) incluyen la comunicación electrónica con uno o más sistemas de ordenadores mediante redes de ordenadores, cableadas y / o inalámbricas.

En particular, el correo electrónico se ha convertido en un procedimiento importante para la comunicación. Los sistemas de correo electrónico habitualmente incluyen un componente cliente del correo electrónico y un componente servidor de correo electrónico. Estos componentes son habitualmente aplicaciones de software que están configuradas para ejecutarse en sistemas de ordenadores (p. ej., servidores, ordenadores personales, portátiles y agendas electrónicas). Un componente cliente del correo electrónico y un componente servidor de correo electrónico están habitualmente diseñados y configurados para operación específica entre sí. El componente cliente del correo electrónico y el componente servidor de correo electrónico se comunican generalmente entre sí usando un protocolo de propiedad industrial, tal como las Llamadas a Procedimientos Remotos (“RPC”), que permite, por ejemplo, que un programa de aplicación en un sistema de ordenador cliente ejecute un programa en un sistema de ordenador servidor. Por ejemplo, un componente cliente del correo electrónico puede enviar un mensaje a un componente servidor de correo electrónico con los argumentos adecuados, y el componente servidor de correo electrónico devuelve un mensaje de correo electrónico.

Algunos tipos de servidores de correo electrónico están configurados para permitir el acceso al correo electrónico mediante un cliente de “contacto cero”, tal como, por ejemplo, un sistema de ordenador cliente con un explorador de la Red, en lugar de un cliente dedicado del correo electrónico. En estos tipos de servidores de correo electrónico, el explorador de la Red interactúa con el servidor de correo electrónico, y toda función requerida para su realización en el sistema cliente es realizada a través del explorador de la Red. Por ejemplo, un sistema de ordenador cliente puede descargar instrucciones y guiones del Lenguaje de Marcado de HiperTexto (“HTML”) (generados dinámicamente por una tecnología tal como las Páginas Activas Servidoras) que permiten a un explorador de la Red interactuar adecuadamente con el servidor de correo electrónico. De tal modo, un cliente basado en un explorador, de contacto cero, permite a un usuario acceder a su correo electrónico y a otra información relacionada con el correo (p. ej., el calendario y las carpetas compartidas) desde cualquier sistema de ordenador servidor que esté conectado con una red común (p. ej., la Malla Máxima Mundial (“WWW”)) con el cliente basado en un explorador, de contacto cero. En consecuencia, los protocolos tales como, por ejemplo, el Protocolo de Transferencia de HiperTexto (“HTTP”), usados para acceder a otro contenido basado en la Red en la WWW también pueden ser usados para acceder al correo electrónico y a otra información relacionada con el correo.

Sin embargo, la accesibilidad, basada en un explorador, al correo electrónico y a otra información relacionada con el correo también da como resultado cuestiones potenciales de seguridad, estando algunas cuestiones de seguridad referidas al almacenamiento en memoria caché de credenciales de usuario en la memoria del explorador de la Red. En un entorno de la Red, el contenido, y las solicitudes de contenido, son generalmente transportados usando el HTTP. Por ejemplo, una solicitud del HTTP para acceder a contenidos se origina en un usuario en un cliente basado en un explorador, y luego es transferida desde el cliente basado en un explorador, a través de una red. La solicitud es luego recibida en un servidor de la Red, en un sistema de ordenador servidor que procesa la solicitud para determinar si el usuario del cliente basado en un explorador está autorizado para acceder al contenido solicitado. Si el usuario está autorizado para acceder al contenido solicitado, el servidor de la Red transportará el contenido de vuelta al cliente basado en un explorador, en un mensaje del HTTP.

Algunas versiones del HTTP (p. ej., el HTTP/1.0) carecen de estado. Es decir, la comunicación mediante el HTTP (p. ej., una solicitud de un mensaje de correo electrónico) es realizada sin conocimiento de ninguna comunicación previa por

parte del servidor (p. ej., otras solicitudes previas de mensajes de correo electrónico). Así pues, estas versiones del HTTP no prestan soporte al concepto de una "sesión" donde un usuario se "conectaría" o "desconectaría". Otras versiones del HTTP (p. ej., el HTTP/1.1) prestan soporte a mensajes de "supervivencia" que son enviados entre un cliente y un servidor para intentar mantener viva una conexión del HTTP. Sin embargo, el uso de mensajes de supervivencia no es muy fiable e, incluso cuando se usan mensajes de supervivencia, no hay ninguna garantía de que una conexión del HTTP puede ser mantenida en actividad. Además, dado que las solicitudes de clientes son frecuentemente canalizadas a través de servidores agentes intermedios que comparten enlaces de supervivencia entre un cierto número de usuarios, puede no haber ninguna manera para que un servidor determine si una solicitud recibida fue enviada por un cliente previamente autenticado. En consecuencia, ya sea que la comunicación del HTTP carezca de estado o que use mensajes de supervivencia, cada solicitud para acceder a contenidos que sea transportada mediante el HTTP (llamada en lo sucesivo en la presente memoria "una solicitud del HTTP") debe incluir información adecuada de autenticación del HTTP.

En consecuencia, la información de autenticación del HTTP puede ser incluida en solicitudes del HTTP mediante una cabecera especial llamada la cabecera de Autorización-del-WWW y que tiene el formato: "Autorización-del-WWW: [Tipo-de-Autenticación] [Credenciales]". La primera vez que un explorador de la Red intenta acceder a contenido que requiere autenticación (p. ej., las credenciales de presentación ingresadas por el usuario), un servidor de la Red habitualmente rehusará proporcionar el contenido solicitado y, en cambio, devolverá un mensaje del HTTP con código de estado 401 No autorizado. El mensaje de respuesta del HTTP incluye una cabecera con el formato: "Autenticación-del-WWW:[Procedimiento de autenticación][reino=valor de reino][Información optativa]".

Cuando es recibido de vuelta en el explorador de la Red, el mensaje de respuesta del HTTP hace que el explorador de la Red presente un cuadro de diálogo que solicita credenciales, tales como, por ejemplo, un nombre de usuario y una contraseña. Después de que un usuario ingresa las credenciales, el explorador de la Red retransmite la solicitud original del HTTP junto con una cabecera de Autorización-del-WWW del HTTP que incluye las credenciales ingresadas. Si el servidor de la Red acepta las credenciales ingresadas por el usuario y devuelve el contenido solicitado (p. ej., un mensaje de correo electrónico), el explorador de la Red almacena en memoria caché las credenciales ingresadas por el usuario, en la memoria del explorador. Así, en solicitudes posteriores al mismo Localizador Uniforme de Recursos ("URL"), o a correspondientes URL relativas derivadas, asociadas al mismo contenido, las credenciales en memoria caché son extraídas de la memoria del explorador e incluidas en las correspondientes cabeceras de la Autorización-del-WWW del HTTP. En consecuencia, incluso aunque el HTTP carezca de estado, se libera al usuario de tener que reingresar las credenciales para cada solicitud al mismo URL, o a los correspondientes URL relativos derivados.

Desafortunadamente, los exploradores de la Red mantienen usualmente credenciales almacenadas en memoria caché del explorador, de manera esencialmente indefinida, hasta que se haga cerrar un explorador de la Red (saliendo del programa explorador de la Red, o rebotando o apagando el sistema de ordenador o el dispositivo cliente). De tal modo, las credenciales de un usuario privilegiado que accedió a contenido protegido pueden estar almacenadas en memoria caché del explorador después de que el usuario no esté ya usando el explorador de la Red. Si el usuario privilegiado se aleja luego del sistema de ordenador, otro usuario no privilegiado puede llegar y usar el botón de retroceso del explorador, o la característica de historia reciente, para intentar acceder al contenido protegido. Dado que las credenciales del usuario privilegiado están aún almacenadas en la memoria caché del explorador, el explorador de la Red extraerá las credenciales almacenadas en memoria caché y las presentará junto con la solicitud del usuario no privilegiado para acceder al contenido protegido. De tal modo, puede darse al usuario no privilegiado acceso al contenido protegido sin tener que ingresar las credenciales adecuadas en el explorador de la Red.

Las credenciales en memoria caché pueden ser especialmente problemáticas en ubicaciones que tienen ordenadores públicos y / o en sistemas de ordenadores que no permiten que se cierre un explorador de la Red. Un ejemplo de un sistema de ordenador de ese tipo es un Kiosco de Internet. Los Kioscos de Internet están a menudo situados en lugares públicos, tales como, por ejemplo, bibliotecas, cibercafés y centros de conferencias, para brindar al público acceso a Internet. Los Kioscos de Internet están diseñados para permitir a cualquiera que se acerque al kiosco poder acceder rápidamente a Internet sin tener primero que hallar y lanzar un explorador de la Red. Así, muchos Kioscos de Internet están configurados de modo que un explorador de la Red esté siempre activo y no pueda ser cerrado.

Si bien esto brinda un acceso eficaz a Internet, también da como resultado potencial que las credenciales en memoria caché permanezcan en la memoria del explorador de manera esencialmente indefinida. Por ejemplo, cuando un usuario privilegiado ingresa credenciales (p. ej., para acceder a contenido protegido) en un Kiosco de Internet, las credenciales del usuario privilegiado son almacenadas en la memoria caché del explorador. Dado que el explorador de la Red no puede ser cerrado, no hay esencialmente ninguna manera para eliminar las credenciales en memoria caché sin quitar la energía al Kiosco público. Así, incluso si el usuario privilegiado tiene el conocimiento práctico para borrar credenciales en memoria caché (p. ej., cerrando el explorador de la Red), el usuario privilegiado puede estar impedido para hacerlo.

El uso de credenciales almacenadas en memoria caché para acceder a contenido protegido tiene interés específico para las aplicaciones de correo electrónico basadas en un explorador. Por ejemplo, un usuario no privilegiado puede ser capaz de retroceder por las páginas para ganar acceso a mensajes de correo electrónico de un usuario privilegiado, que también

podrían contener datos privados. Además de acceder al correo electrónico del usuario privilegiado, las credenciales en memoria caché también pueden permitir que el usuario no privilegiado finja ser el usuario privilegiado. Por ejemplo, el no privilegiado puede ser capaz de enviar mensajes de correo electrónico desde una cuenta asociada a un usuario privilegiado.

Una posible solución a este problema es forzar a los usuarios a reautenticarse cada vez que se solicita contenido. Sin embargo, esto requeriría que los usuarios reingresaran manualmente información de autenticación para cada solicitud del HTTP, a fin de acceder al contenido. Como una interacción típica con una sede de la Red puede consistir en decenas o incluso cientos de solicitudes del HTTP, esto daría como resultado que un usuario tuviera que reingresar credenciales decenas o cientos de veces. De tal modo, el reingreso de credenciales para cada solicitud del HTTP aumentaría significativamente la cantidad de tiempo y de ingreso de datos necesarios para acceder al contenido. Esta solución es demasiado engorrosa para la mayoría de los usuarios, que preferirían ingresar sus credenciales solamente una vez por sesión. Por lo tanto, serían ventajosos los sistemas, procedimientos y productos de programa de ordenador para procesar con seguridad las credenciales de clientes usadas para acceder a recursos basados en la Red.

El documento WO 00 / 79367 A1 se refiere a un procedimiento y un sistema para transacciones garantizadas seguras por una red de ordenadores. Esta solicitud de patente revela el uso de señuelos para almacenar credenciales del usuario. Los señuelos son firmados y cifrados digitalmente.

El documento US 2002 / 010776 A1 se refiere a un procedimiento y aparato para integrar un sistema distribuido de servicios compartidos. Según esta solicitud de patente, los contenidos de los señuelos son cifrados usando un esquema de rotación de claves.

El documento de Park, J. S. et al.: “Señuelos seguros en la Red”, Informática en Internet del IEEE, julio de 2000, páginas 36 a 44, se refiere a señuelos seguros en la Red.

El documento US 6 041 357 A se refiere a un sistema y protocolo de testigos comunes de sesiones.

Breve resumen de la invención

Es el objeto de la presente invención proporcionar procedimientos, sistemas, productos de programa de ordenador y estructuras de datos para determinar la validez de credenciales de usuario usadas para el acceso a recursos basado en la Red.

Este objeto es resuelto por la materia en cuestión de las reivindicaciones independientes.

Las realizaciones se dan en las reivindicaciones dependientes.

Un sistema de ordenador cliente (denominado en adelante en la presente memoria el “cliente”) y un sistema de ordenador servidor (denominado en adelante en la presente memoria el “servidor”) están conectados con una red común, tal como, por ejemplo, Internet. El servidor está configurado para permitir el acceso a recursos basado en la Red, tales como, por ejemplo, los mensajes de correo electrónico y los datos de correo asociados. El cliente está configurado con un explorador que puede solicitar acceso a recursos basados en la Red y presentar recursos basados en la Red a un usuario en el cliente.

El cliente envía una primera solicitud para acceder a un recurso en el servidor. Por ejemplo, el cliente puede enviar una solicitud para acceder a un mensaje de correo electrónico almacenado en el servidor. El servidor recibe la primera solicitud y, dado que el cliente no está autenticado, el servidor redirige al cliente a una página de conexión en respuesta a la recepción de la primera solicitud. La redirección del cliente puede incluir el envío por el servidor al cliente de una respuesta que incluye un indicador de redirección (p. ej., un Mensaje del Protocolo de Transferencia de HiperTexto (“HTTP”) con un código de estado 302 Temporalmente Desplazado) junto con un Identificador Uniforme de Recurso (“URI”) de la página de conexión. La página de conexión puede ser una página de las Páginas Activas de Servidor (“ASP”) que proporciona una interfaz para un usuario en un cliente, para ingresar credenciales de usuario. El cliente accede a la página de conexión y utiliza la página de conexión para presentar credenciales de usuario al servidor. Un cliente puede presentar credenciales, por ejemplo, usando la Capa de Receptáculos Seguros (“SSL”), para asegurar un puesto del HTTP.

El servidor recibe las credenciales presentadas. El servidor envía información cifrada que representa a las credenciales del usuario y una firma digital dependiente del tiempo. Puede ser que el servidor envíe información cifrada después de delegar la autenticación de las credenciales presentadas a una autoridad fiable para realizar la autenticación. El servidor genera los datos cifrados usando una clave proveniente de un almacén de claves rotativas. Cada clave en el almacén de claves rotativas caduca automáticamente después de un intervalo temporal especificado (p. ej., diez minutos). Después del intervalo temporal especificado, el servidor puede hacer rotar una nueva clave al almacén de claves rotativas y eliminar por rotación una clave caducada del almacén de claves rotativas. El número de claves mantenidas en un

almacén de claves rotativas, y el intervalo temporal especificado, pueden ser configurados por un administrador.

Cuando se reciben credenciales de usuario, el servidor asocia las credenciales de usuario a un identificador único (p. ej., un Identificador Globalmente Único ("GUID")). El servidor obtiene una clave de firma, que puede ser usada para firmar digitalmente los datos, troceando (p. ej., usando el algoritmo de troceo SHA-1 o MD-5) una combinación de la clave más actual en el almacén de claves rotativas, el identificador único y una primera cadena constante. El servidor usa luego la clave de firma para obtener una firma digital (p. ej., un Código de Autenticación de Mensaje con rutinas de autentificación ("HMAC")) de una combinación del identificador único y de las credenciales del usuario.

El servidor también obtiene una clave de cifrado, que puede ser usada para cifrar datos, troceando una combinación de la clave más actual en el almacén de claves rotativas, el identificador único y una segunda cadena constante. El servidor usa luego la clave de cifrado para cifrar una combinación de la firma digital y las credenciales del usuario en información cifrada. El servidor envía el identificador único y la información cifrada al cliente. El cliente recibe el identificador único y la información cifrada y almacena el identificador único y la información cifrada (p. ej., en correspondientes señuelos).

El cliente envía una segunda solicitud, que incluye el identificador único y la información cifrada, para acceder al recurso en el servidor. El servidor recibe la segunda solicitud e intenta validar las credenciales del usuario usando la clave más actual en el almacén de claves rotativas. El servidor obtiene una clave de descifrado, que puede ser usada para descifrar datos, troceando una combinación de la clave más actual en el almacén de claves rotativas, el identificador único y la segunda cadena constante. El servidor usa la clave de descifrado para descifrar la información cifrada, revelando por ello la firma digital y las credenciales de usuario. El servidor obtiene una clave de validación, que puede ser usada para autenticar datos, troceando una combinación de la clave más actual en el almacén de claves rotativas, el identificador único y la primera cadena constante. El servidor usa la clave de firma de validación para obtener una firma digital de validación a partir de una combinación del identificador único y las credenciales del usuario.

El servidor compara la firma digital de validación con la firma digital. Cuando la firma digital de validación y la firma digital coinciden, las credenciales del usuario son validadas. Por otra parte, cuando la firma digital de validación y la firma digital no coinciden, las credenciales no son validadas. Cuando las credenciales de usuario no son validadas usando la clave más actual en el almacén de claves rotativas, se usa la siguiente clave más actual en el almacén de claves rotativas para intentar validar las credenciales del usuario (p. ej., usando la siguiente clave más actual para generar una clave de descifrado y una firma digital de validación). El servidor puede intentar validar las credenciales del usuario usando cada clave en el almacén de claves rotativas. Las credenciales de usuario validadas son remitidas a un módulo (p. ej., un servidor de correo electrónico) que controla el acceso al recurso solicitado (p. ej., un mensaje de correo electrónico).

Cuando las credenciales del usuario son validadas con una clave del almacén de claves rotativas que no es la clave más actual, el servidor determina que ha de obtenerse información cifrada refrescada. El servidor usa la clave más actual en el almacén de claves rotativas para obtener la información cifrada refrescada (p. ej., obteniendo una firma digital refrescada y una clave de cifrado refrescada a partir de la clave más actual). Cuando las credenciales de usuario validadas son las adecuadas, el recurso solicitado y, cuando corresponda, también la información cifrada refrescada son devueltos al cliente. El cliente recibe el recurso y cualquier información cifrada refrescada. El cliente almacena toda información cifrada refrescada, sobrescribiendo la información cifrada anterior correspondiente al identificador único. Cuando las credenciales de usuario no pueden ser validadas usando ninguna clave rotativa en el almacén de claves rotativas, el cliente es redirigido a la página de conexión, donde pueden ser ingresadas nuevas credenciales de usuario.

En algunas realizaciones, una página de conexión incluye una interfaz para seleccionar propiedades de comunicación (p. ej., soporte para la compresión por gzip, el sistema de ordenador cliente es un cliente privado o no fiable, el cliente es un cliente avanzado que preferiría contenido simplificado) que pueden alterar cómo son procesados los mensajes del HTTP. Las propiedades de comunicación son seleccionadas en la página de conexión y enviadas a un filtro de comunicación para indicar al filtro de comunicación cómo ha de ser procesada la comunicación del HTTP con el cliente. Las propiedades de comunicación seleccionadas son recibidas en el servidor.

El servidor interroga al cliente para determinar si las propiedades de comunicación seleccionadas disponen de soporte por parte del cliente, así como para identificar otras propiedades de comunicación relevantes. El servidor configura el filtro de comunicación para procesar la comunicación del HTTP con el cliente, de acuerdo a toda propiedad de comunicación seleccionada, y otras propiedades relevantes de comunicación identificadas que disponen de soporte por parte del cliente. En base a estar un cliente en una ubicación no segura, el servidor puede utilizar un almacén distinto de claves rotativas que tenga un intervalo de rotación más breve y que mantenga un número reducido de claves.

Las características y ventajas adicionales de la invención se estipularán en la descripción que sigue, y en parte serán obvias a partir de la descripción, o bien pueden ser aprendidas con la práctica de la invención. Las características y ventajas de la invención pueden ser realizadas y obtenidas por medio de los instrumentos y combinaciones específicamente señalados en las reivindicaciones adjuntas. Estas y otras características de la presente invención devendrán más completamente evidentes a partir de la siguiente descripción y reivindicaciones adjuntas, o bien pueden

ser aprendidas por la práctica de la invención, según se estipula a continuación en la presente memoria.

Breve descripción de los dibujos

A fin de describir la manera en que pueden ser obtenidas las ventajas y características expuestas anteriormente, y otras, de la invención, se representará una descripción más específica de la invención brevemente descrita en lo anterior, por referencia a realizaciones específicas de la misma que están ilustradas en los dibujos adjuntos. Entendiéndose que estos dibujos ilustran solamente realizaciones típicas de la invención y, por lo tanto, no han de considerarse como limitadores de su alcance, la invención será descrita y explicada con especificidad y detalle adicionales, mediante el uso de los dibujos adjuntos, en los cuales:

la Figura 1 ilustra un entorno operativo adecuado para los principios de la presente invención.

La Figura 2A ilustra un ejemplo de una arquitectura de red que facilita asegurar credenciales de parte del cliente cuando un cliente solicita acceso a un recurso en un servidor, de acuerdo a la presente invención.

La Figura 2B ilustra un ejemplo de una arquitectura de red que facilita utilizar credenciales aseguradas de parte del cliente para acceder a un recurso en un servidor, de acuerdo a la presente invención.

La Figura 3 ilustra un diagrama ejemplar de flujo de un procedimiento para asegurar credenciales de parte del cliente cuando un cliente solicita acceso a un recurso en un servidor, de acurdo a la presente invención.

La Figura 4 ilustra un diagrama ejemplar de flujo de un procedimiento para utilizar credenciales aseguradas de parte del cliente para acceder a un recurso en un servidor, de acuerdo a la presente invención.

La Figura 5 ilustra un diagrama ejemplar de flujo de un procedimiento para determinar propiedades de comunicación asociadas a un cliente, de acuerdo a los principios de la presente invención.

La Figura 6 ilustra una página ejemplar de conexión que puede aceptar credenciales y selecciones de propiedades de comunicación, de acuerdo a los principios de la presente invención.

Descripción detallada de las realizaciones preferidas

Los principios de la presente invención admiten procesar con seguridad credenciales de cliente usadas para el acceso basado en la Red a los recursos. Un servidor mantiene al menos un almacén de claves rotativas, de una o más claves. Cada clave en un almacén de claves rotativas caduca automáticamente después de un intervalo temporal especificado (p. ej., diez minutos). Después del intervalo temporal especificado, el servidor rota una nueva clave hacia el almacén de claves rotativas y elimina por rotación una clave caducada del almacén de claves rotativas. El número de claves mantenidas en el almacén de claves rotativas y el intervalo temporal especificado pueden ser configurados por un administrador (p. ej., mantener tres claves y rotar las claves cada cinco minutos). El servidor asegura las credenciales de usuario generando firmas digitales para credenciales de usuario y cifrando credenciales de usuario en base a claves en el almacén de claves rotativas.

Una página de conexión, con una interfaz para ingresar credenciales de usuario, es presentada a un cliente. Las credenciales de usuario ingresadas en el cliente son enviadas al servidor. En respuesta a la recepción de credenciales de usuario, el servidor generar un único identificador de sesión para el cliente. El servidor obtiene una firma digital para las credenciales de usuario en base a la clave más actual en un almacén de claves rotativas y al identificador único de sesión. El servidor cifra luego la firma digital y las credenciales de usuario en base a una clave de cifrado deducida de la clave más actual en un almacén de claves rotativas y al identificador único de sesión. Cuando las credenciales cifradas son recibidas de vuelta en el cliente, las claves del almacén de claves rotativas son usadas para intentar validar las credenciales. Si la clave del almacén de claves rotativas, originalmente usada para cifrar las credenciales de usuario, ha sido eliminada por rotación del almacén de claves rotativas, el cliente es redirigido a la página de conexión para ingresar nuevas credenciales.

Las realizaciones dentro del alcance de la presente invención incluyen medios legibles por ordenador para llevar o tener instrucciones ejecutables por ordenador, o estructuras de datos almacenadas en los mismos. Tales medios legibles por ordenador pueden ser medios disponibles cualesquiera, que sean accesibles por un sistema de ordenador de propósito general o de propósito especial. A modo de ejemplo, y no de limitación, tales medios legibles por ordenador pueden comprender medios de almacenamiento físico tales como RAM, ROM, EPROM, CD-ROM u otros dispositivos de almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, u otros medios cualesquiera que puedan ser usados para llevar o almacenar medios deseados de código de programa, en forma de instrucciones ejecutables por ordenador, instrucciones legibles por ordenador o estructuras de datos, y a las que pueda acceder un sistema de ordenador de propósito general o de propósito especial.

En esta descripción y en las siguientes reivindicaciones, una “red” está definida como uno o más enlaces de datos que

permiten el transporte de datos electrónicos entre sistemas de ordenadores y / o módulos. Cuando la información es transferida o proporcionada por una red u otra conexión de comunicaciones (ya sea cableada, inalámbrica, o una combinación de cableada o inalámbrica) a un sistema de ordenador, la conexión es debidamente vista como un medio legible por ordenador. De tal modo, cualquier conexión de ese tipo es correctamente denominada un medio legible por ordenador. Las combinaciones de lo que antecede también deberían ser incluidas dentro del alcance de los medios legibles por ordenador. Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que hacen que un sistema de ordenador de propósito general, o un sistema de ordenador de propósito especial, realicen una cierta función o grupo de funciones. Las instrucciones ejecutables por ordenador pueden ser, por ejemplo, datos binarios, instrucciones de formato intermedio tales como código de lenguaje ensamblador, o incluso código fuente.

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

Los expertos en la técnica apreciarán que la invención puede ser puesta en práctica en entornos informáticos en red, con muchos tipos de configuraciones de sistemas de ordenadores, que incluyen ordenadores personales, ordenadores portátiles, dispositivos de mano, sistemas multiprocesadores, electrónica de consumo basada en microprocesadores, o programable, ordenadores personales en red, miniordenadores, ordenadores centrales, teléfonos móviles, agendas electrónicas, buscapersonas y similares. La invención también puede ser puesta en práctica en entornos de sistemas distribuidos, donde realizan tareas sistemas de ordenadores tanto locales como remotos, que están enlazados (ya sea por enlaces de datos cableados, enlaces de datos inalámbricos, o por una combinación de enlaces de datos cableados e inalámbricos) a través de una red. En un entorno de sistemas distribuidos, los módulos de programa pueden ser ubicados en dispositivos de almacenamiento de memoria tanto local como remota.

La Figura 1 y la siguiente exposición están concebidas para proporcionar una breve descripción general de un entorno informático adecuado en el cual pueda ser implementada la invención. Aunque no se requiere, la invención será descrita en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutados por sistemas de ordenador. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos y similares, que realizan tareas específicas o implementan tipos específicos de datos abstractos. Las instrucciones ejecutables por ordenador, las estructuras de datos asociadas y los módulos de programa representan ejemplos de los medios de código de programa para ejecutar actos de los procedimientos revelados en la presente memoria.

Con referencia a la Figura 1, un sistema ejemplar para implementar la invención incluye un dispositivo informático de propósito general, en forma del sistema 120 de ordenador, que incluye una unidad 121 de procesamiento, una memoria 122 del sistema y un bus 123 del sistema que acopla diversos componentes del sistema, incluyendo la memoria 122 del sistema con la unidad 121 de procesamiento. La unidad 121 de procesamiento puede ejecutar instrucciones ejecutables por ordenador diseñadas para implementar características del sistema 120 de ordenador, incluyendo características de la presente invención. El bus 123 del sistema puede ser cualquiera entre diversos tipos de estructuras de bus, que incluyen un bus de memoria o controlador de memoria, un bus periférico y un bus local, usando cualquiera entre una amplia variedad de arquitecturas de bus. La memoria del sistema incluye la memoria de sólo lectura (“ROM”) 124 y la memoria de acceso aleatorio (“RAM”) 125. Un sistema básico de entrada / salida (“BIOS”) 126, que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del sistema 120 de ordenador, tal como durante el arranque, puede ser almacenado en la ROM 124.

El sistema 120 de ordenador también puede incluir el controlador 127 de disco rígido magnético, para leer de, y escribir en, el disco rígido magnético 139, el controlador 128 de disco magnético para leer de, o escribir en, el disco magnético extraíble 129, y el controlador 130 de disco óptico para leer de, o escribir en, el disco óptico extraíble 131, tal como, por ejemplo, un CD-ROM u otros medios ópticos. El controlador 127 de disco rígido magnético, el controlador 128 de disco magnético y el controlador 130 de disco óptico están conectados con el bus 123 del sistema por la interfaz 132 de controlador de disco rígido, la interfaz 133 de controlador de disco magnético y la interfaz 134 de controlador óptico, respectivamente. Los controladores y sus medios asociados legibles por ordenador proporcionan el almacenamiento no volátil de instrucciones ejecutables por ordenador, estructuras de datos, módulos de programa y otros datos para el sistema 120 de ordenador. Aunque el entorno ejemplar descrito en la presente memoria emplea el disco rígido magnético 139, el disco magnético extraíble 129 y el disco óptico extraíble 131, pueden ser usados otros tipos de medios legibles por ordenador para almacenar datos, incluyendo los casetes magnéticos, las tarjetas de memoria flash, los discos versátiles digitales, los cartuchos de Bernoulli, las memorias RAM, las memorias ROM y similares.

Los medios de código de programa que comprendan uno o más módulos de programa pueden ser almacenados en el disco rígido 139, el disco magnético 129, el disco óptico 131, la ROM 124 o la RAM 125, incluso un sistema operativo 135, uno o más programas 136 de aplicación, otros módulos 137 de programa y los datos 138 de programa. Un usuario puede ingresar comandos e información en el sistema 120 de ordenador a través del teclado 140, el dispositivo puntero 142 u otros dispositivos de entrada (no mostrados) tales como, por ejemplo, un micrófono, una palanca de juegos, un panel de juegos, un escáner o similares. Estos y otros dispositivos de entrada pueden ser conectados con la unidad 121 de procesamiento a través de la interfaz 146 de entrada / salida, acoplada al bus 123 del sistema. La interfaz 146 de entrada / salida representa lógicamente a cualquiera entre una amplia variedad de distintas interfaces, tales como, por ejemplo, una interfaz de puerto en serie, una interfaz PS/2, una interfaz de puerto paralelo, una interfaz del Bus Universal en Serie ("USB") o una interfaz 1394 del Instituto de Ingenieros Eléctricos y Electrónicos ("IEEE") (es decir, una interfaz FireWire); o incluso puede representar lógicamente a una combinación de distintas interfaces.

Un monitor 147, u otro dispositivo visor, también está conectado con el bus 123 del sistema mediante el adaptador 148 de vídeo. Los altavoces 169, u otro dispositivo de salida de audio, también están conectados con el bus 123 del sistema mediante la interfaz 149 de audio. Otros dispositivos periféricos de salida (no mostrados) tales como, por ejemplo, impresoras, también pueden estar conectados con el sistema 120 de ordenador. El sistema 120 de ordenador es conectable con redes tales como, por ejemplo, una red de ordenadores de ámbito de oficina o de ámbito de empresa, una red casera, una intranet y / o Internet. El sistema 120 de ordenador puede intercambiar datos con fuentes externas tales como, por ejemplo, sistemas de ordenadores remotos, aplicaciones remotas y / o bases de datos remotas, por dichas redes.

El sistema 120 de ordenador incluye la interfaz 153 de red, a través de la cual el sistema 120 de ordenador recibe datos desde fuentes externas y / o transmite datos a fuentes externas. Según se ilustra en la Figura 1, la interfaz 153 de red facilita el intercambio de datos con el sistema 183 de ordenador remoto, mediante el enlace 151. La interfaz 153 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 la correspondiente pila de la Especificación de Interfaz de Controlador de Red ("NDIS"). El enlace 151 representa una parte de una red (p. ej., un segmento de Ethernet) y el sistema 183 de ordenador remoto representa un nodo de la red. Por ejemplo, el sistema 183 de ordenador remoto puede ser el sistema de ordenador servidor que proporciona al sistema 120 de ordenador acceso basado en la Red a los recursos (p. ej., mensajes de correo electrónico). Por otra parte, el sistema 183 de ordenador remoto puede ser un sistema de ordenador cliente que usa el acceso basado en la Red para acceder a recursos desde el sistema 120 de ordenador.

Análogamente, el sistema 120 de ordenador incluye la interfaz 146 de entrada / salida, a través de la cual el sistema 120 de ordenador recibe datos desde fuentes externas y / o transmite datos a fuentes externas. La interfaz 146 de entrada / salida está acoplada con el módem 154 (p. ej., un módem estándar, un módem de cable, o un módem de línea digital de abonado ("DSL")) mediante el enlace 159, a través del cual el sistema 120 de ordenador recibe datos desde, y / o transmite datos a, fuentes externas. Según lo ilustrado en la Figura 1, la interfaz 146 de entrada / salida y el módem 154 facilitan el intercambio de datos con el sistema 193 de ordenador remoto, mediante el enlace 152. El enlace 152 representa una parte de una red y el sistema 193 de ordenador remoto representa un nodo de la red. Por ejemplo, el sistema 193 de ordenador remoto puede ser un sistema de ordenador servidor que proporciona al sistema 120 de ordenador acceso basado en la Red a los recursos (p. ej., mensajes de correo electrónico). Por otra parte, el sistema 193 de ordenador remoto puede ser un sistema de ordenador cliente que usa el acceso basado en la Red para acceder a recursos desde el sistema 120 de ordenador.

Si bien la Figura 1 representa un entorno operativo adecuado para la presente invención, los principios de la presente invención pueden ser empleados en cualquier sistema que sea capaz, con la modificación adecuada, si es necesario, de implementar los principios de la presente invención. El entorno ilustrado en la Figura 1 es ilustrativo solamente y en modo alguno representa siquiera una pequeña parte de la amplia variedad de entornos en los cuales pueden ser implementados los principios de la presente invención.

Los módulos de la presente invención, así como los datos de programa asociados, pueden ser almacenados y admiten acceso desde cualquiera de los medios legibles por ordenador asociados al sistema 120 de ordenador. Por ejemplo, partes de tales módulos y partes de los datos de programa asociados pueden estar incluidos en el sistema operativo 135, los programas 136 de aplicación, los módulos 137 de programa y / o los datos 138 de programa, para su almacenamiento en la memoria 122 del sistema. Cuando un dispositivo de almacenamiento masivo, tal como, por ejemplo, el disco rígido magnético 139, está acoplado con el sistema 120 de ordenador, tales módulos y datos de programa asociados pueden también ser almacenados en el dispositivo de almacenamiento masivo. En un entorno en red, los módulos de programa ilustrados con respecto al sistema 120 de ordenador, o partes de los mismos, pueden ser almacenados en dispositivos remotos de almacenamiento de memoria, tales como la memoria del sistema y / o los dispositivos de almacenamiento masivo asociados al sistema 183 de ordenador remoto y / o al sistema 193 de ordenador remoto. La ejecución de tales módulos puede ser realizada en un entorno distribuido, según lo descrito anteriormente.

La Figura 2 ilustra un ejemplo de arquitectura 200 de red que facilita asegurar las credenciales de parte del cliente cuando

un cliente solicita acceso a un recurso en un servidor. El sistema 201 de ordenador cliente y el sistema 211 de ordenador servidor pueden estar conectados con una red común, tal como, por ejemplo, una Red de Área Local ("LAN"), una Red de Área Amplia ("WAN") o incluso Internet. El sistema 201 de ordenador cliente incluye el explorador 202, que puede ser usado para solicitar el acceso basado en la Red a recursos y presentar los recursos recibidos en el sistema 201 de ordenador cliente. Los señuelos 203 pueden incluir uno o más señuelos que almacenan partes de datos previamente recibidos desde sistemas de ordenadores servidores. Los datos en los señuelos 203 pueden ser enviados a un correspondiente sistema de ordenador servidor para indicar información o preferencias personalizadas al sistema de ordenador servidor y / o para liberar a un usuario de tener que ingresar manualmente una parte de información almacenada.

El sistema 211 de ordenador servidor incluye el servidor 212 de correo electrónico, que brinda acceso a recursos del correo electrónico tales como, por ejemplo, mensajes de correo electrónico, información de la libreta de direcciones e información de calendario. Para ser autorizado a acceder a recursos del correo electrónico, puede requerirse a un usuario suministrar credenciales al servidor 212 de correo electrónico, para autenticarse en el servidor 212 de correo electrónico. El servidor 212 de correo electrónico puede comparar las credenciales recibidas con las credenciales autorizadas en la base 213 de datos de credenciales, para determinar si ha de concederse una solicitud para acceder a recursos del correo electrónico. Cuando un usuario es autorizado, el servidor 212 de correo electrónico puede devolver recursos solicitados del correo electrónico a un sistema de ordenador cliente solicitante. Cuando un usuario no es autorizado, el servidor 212 de correo electrónico puede devolver un mensaje de desautorización (p. ej., un mensaje del Protocolo de Transferencia de HiperTexto ("HTTP") con código de estado 401 No autorizado) a un sistema de ordenador cliente solicitante.

El sistema 211 de ordenador servidor también incluye el módulo 214 de generación de claves. El módulo 214 de generación de claves puede generar y rotar nuevas claves como claves rotativas 220 y puede eliminar por rotación las claves caducadas de las claves rotativas 220. El módulo 214 de generación de claves puede ser configurado para mantener uno o más almacenes de claves rotativas. Por ejemplo, en la arquitectura 200 de red, el módulo 214 de generación de claves mantiene el almacén 221 de claves rotativas no fiables y el almacén 231 de claves rotativas privadas.

El intervalo temporal especificado en que se rotan las claves es configurable. Es decir, el módulo 214 de generación de claves puede ser configurado para rotar las claves recientemente generadas hacia, y eliminar las claves caducadas de, un almacén de claves rotativas, a intervalos especificados. Por ejemplo, el módulo 214 de generación de claves puede insertar una nueva clave en, y eliminar una clave caducada de, el almacén 231 de claves rotativas privadas cada 10 minutos. El número de claves mantenidas en un almacén de claves rotativas también es configurable. Es decir, el módulo 214 de generación de claves también puede ser configurado para mantener un número especificado de claves en un almacén de claves rotativas. Por ejemplo, el módulo 214 de generación de claves puede ser configurado para mantener 3 claves en el almacén 221 de claves rotativas no fiables.

El número de claves mantenidas y de intervalos especificados puede diferir entre los almacenes de claves rotativas. Por ejemplo, el módulo 214 de generación de claves puede mantener 3 claves con un intervalo de rotación especificado de cinco minutos en el almacén 221 de claves no fiables y cuatro claves con un intervalo de rotación especificado de una hora en el almacén 231 de claves privadas. Según las propiedades asociadas a un sistema de ordenador cliente, pueden ser utilizados distintos almacenes de claves para implementar los principios de la presente invención. Las flechas ilustradas debajo de las claves en los almacenes de claves rotativas indican que las claves rotan hacia abajo cuando se añade una nueva clave, hasta que las claves caducadas sean eventualmente eliminadas por rotación del almacén de claves rotativas. Por ejemplo, cuando se añade una nueva clave al almacén 231 de claves rotativas privadas, la clave 232 rotará hacia la posición de la clave 233.

El sistema 211 de ordenador servidor también incluye la página 217 de conexión. La página 217 de conexión puede ser una página de la Red (p. ej., una página de las Páginas Activas de Servidor ("ASP")) que proporciona una interfaz para presentar credenciales de usuario y seleccionar propiedades de comunicación asociadas a un sistema de ordenador cliente. En respuesta a un sistema de ordenador cliente que accede a un Identificador Uniforme de Recursos ("URI") correspondiente a la página 217 de conexión, el sistema 211 de ordenador servidor puede enviar la página 217 de conexión al sistema de ordenador cliente. Un explorador en el lado del cliente puede presentar la página 217 de conexión en un sistema de ordenador cliente. Las credenciales de usuario y las selecciones de propiedades de comunicación presentadas en la página 217 de conexión pueden ser enviadas al sistema 211 de ordenador servidor.

El sistema de ordenador servidor también incluye el filtro 243 de comunicación. El filtro 243 de comunicación puede interceptar la comunicación del HTTP, tal como, por ejemplo, solicitudes, respuestas y mensajes que son transferidos hacia y desde el sistema 211 de ordenador servidor. El filtro 243 de comunicación puede referirse a información de estado de cliente incluida en señuelos cifrados para determinar si la comunicación del HTTP entre el sistema 211 de ordenador servidor y un sistema de ordenador cliente debería ser alterada (p. ej., modificando las cabeceras del HTTP). El filtro 243 de comunicación también puede implementar algoritmos criptográficos (utilizando claves de un almacén de claves rotativas) para descifrar y validar credenciales de usuario.

El sistema 211 de ordenador servidor también incluye el validador 216 de elementos de conexión. El validador 216 de elementos de conexión puede recibir credenciales de usuario presentadas, ingresadas en la página 217 de conexión, e implementar algoritmos criptográficos (utilizando claves de un almacén de claves rotativas) para rubricar digitalmente y cifrar las credenciales de usuario presentadas. El validador 216 de elementos de conexión también puede generar identificadores únicos de sesión (p. ej., Identificadores Globalmente Únicos ("GUID")) para sistemas de ordenador cliente que solicitan acceso basado en la Red a recursos del sistema 211 de ordenador servidor. El validador 216 de elementos de conexión puede enviar identificadores únicos de sesión e información cifrada, incluso credenciales de usuario y firmas digitales dependientes del tiempo, a sistemas de ordenadores clientes. Por ejemplo, el validador 216 de elementos de conexión puede enviar identificadores únicos de sesión y credenciales de usuario cifradas al sistema 201 de ordenador cliente, para su almacenamiento en los señuelos 203.

La Figura 3 ilustra un diagrama ejemplar de flujo de un procedimiento 300 para asegurar las credenciales de parte del cliente cuando un cliente solicita acceso a un recurso en un servidor. El procedimiento 300 será descrito con respecto al sistema de ordenador cliente y al sistema de ordenador servidor ilustrados en la Figura 2A. El procedimiento 300 incluye un acto de enviar una primera solicitud a un servidor (acto 301). El acto 301 puede incluir un sistema de ordenador cliente que envía una primera solicitud para el acceso basado en la Red a un recurso (p. ej., un mensaje de correo electrónico) en el servidor.

Por ejemplo, el sistema 201 de ordenador cliente puede enviar la solicitud 251, que incluye el URI 267 del servidor de correo, al sistema 211 de ordenador servidor. El URI 267 del servidor de correo puede ser un URI que corresponde al servidor 212 de correo electrónico. Es decir, los usuarios que desean acceder a recursos del correo electrónico mantenidos por el servidor de correo electrónico pueden intentar el acceso basado en la Red a los recursos del correo electrónico, accediendo al URI 267 del servidor de correo. En consecuencia, puede ser que un usuario en el sistema 201 de ordenador cliente ingrese comandos en el explorador 202 para hacer que el sistema 201 de ordenador cliente envíe la solicitud 251.

El procedimiento 300 incluye un acto de recibir una primera solicitud desde un cliente (acto 306). El acto 306 puede incluir un sistema de ordenador servidor que recibe una primera solicitud de acceso basado en la Red a un recurso (p. ej., el mensaje de correo electrónico) en el servidor. Por ejemplo, el sistema 211 de ordenador servidor puede recibir la solicitud 251, que incluye el URI 267 del servidor de correo, desde el sistema 201 de ordenador cliente. Según lo indicado por la línea discontinua a través del filtro 243 de comunicación, el filtro 243 de comunicación puede ser configurado para permitir que la solicitud 251 pase, sin alterar la solicitud 251. En consecuencia, la solicitud 251 puede ser remitida al servidor 212 de correo electrónico sin modificación.

El procedimiento 300 incluye una etapa funcional orientada a resultados para asegurar las credenciales de parte del cliente (etapa 311). La etapa 311 puede incluir cualquier acto correspondiente para asegurar las credenciales de parte del cliente. Sin embargo, en el ejemplo ilustrado de la Figura 3, la etapa 311 incluye un acto correspondiente de redirección del cliente a una página de conexión, en respuesta a la primera solicitud (acto 307). El acto 307 puede incluir que el sistema de ordenador servidor redirija el sistema de ordenador cliente a una página de conexión, en respuesta a la primera solicitud.

En respuesta a la solicitud 251, el servidor 212 de correo electrónico puede enviar la respuesta 252, que incluye el indicador 272 de desautorización. La respuesta 252 puede ser un mensaje del HTTP con el código de estado 401 No autorizado, devuelto como resultado de no incluir la solicitud 251 las credenciales del usuario. El filtro 243 de comunicación puede ser configurado para interceptar mensajes que incluyen indicadores de desautorización. En consecuencia, el filtro 243 de comunicación puede interceptar la respuesta 252.

El filtro 243 de comunicación puede modificar el contenido de la respuesta 252 (p. ej., cambiando las cabeceras del HTTP) para hacer que el sistema 201 de ordenador cliente sea redirigido a una página de conexión que proporciona una interfaz para ingresar credenciales de usuario. Por ejemplo, el filtro 243 de comunicación puede eliminar el indicador 272 de desautorización de la respuesta 252 e insertar el URI 263 de la página de conexión y el indicador 271 de redirección en la respuesta 252, dando como resultado la respuesta 252A. La respuesta 252A puede ser un mensaje del HTTP con código de estado 302 Hallado. El URI 263 de la página de conexión puede ser un URI usado para acceder a la página 217 de conexión. En consecuencia, la respuesta 252A puede indicar al sistema 201 de ordenador cliente que el recurso solicitado (p. ej., el mensaje de correo electrónico) es, en cambio, el acceso en el URI 263 de la página de conexión.

El procedimiento 300 incluye un acto para ser redirigido a una página de conexión (acto 302). El acto 302 puede incluir que un sistema de ordenador cliente sea redirigido a una página de conexión que proporciona una interfaz para aceptar credenciales de usuario. Por ejemplo, el sistema 201 de ordenador cliente puede ser redirigido a la página 217 de conexión. En respuesta a la recepción de la respuesta 252A, el sistema 201 de ordenador cliente puede enviar la solicitud 257, que incluye el URI 263 de la página de conexión, al sistema 211 de ordenador servidor. En respuesta a la solicitud 257, el sistema 211 de ordenador servidor puede enviar la respuesta 258, que incluye la página 217 de conexión, al sistema 201 de ordenador cliente. Una página de conexión puede ser una página de la Red, tal como, por ejemplo, una

página de las Páginas Activas de Servidor (“ASP”).

El explorador 202 puede presentar la página 217 de conexión en el sistema 201 de ordenador cliente. Avanzando desde la Figura 3 y con referencia ahora a la Figura 6, la Figura 6 ilustra una página 600 ejemplar de conexión que puede aceptar credenciales de usuario y selecciones de propiedades de comunicación, de acuerdo a los principios de la presente invención. La página 217 de conexión puede ser similar a la página 600 de conexión. La página 600 de conexión incluye el campo 606, que puede aceptar un identificador de usuario, y el campo 607, que puede aceptar una correspondiente contraseña.

El botón 601 de radio puede ser usado para aceptar una selección de propiedades de comunicación que indica que un explorador del lado del cliente es un “Cliente Avanzado”. El botón 602 de radio puede ser usado para aceptar una selección de propiedades de comunicación que indica que un explorador del lado del cliente es un “Cliente de Nivel Bajo”. Un Cliente Avanzado puede incluir la funcionalidad para realizar un procesamiento más avanzado, tal como, por ejemplo, la ejecución de guiones o la presentación de salidas de multimedios. Por otra parte, un Cliente de Nivel Bajo no puede incluir la funcionalidad para realizar el procesamiento avanzado. En consecuencia, la riqueza del contenido devuelto desde un servidor puede ser ajustado adecuadamente, según las capacidades de un explorador del lado del cliente. Cuando un Cliente Avanzado está conectado con un servidor por una conexión de ancho de banda reducido y / o de alta latencia (p. ej., una conexión por discado telefónico), una selección de Cliente de Nivel Bajo puede reducir la magnitud del contenido devuelto desde el servidor.

El botón 603 de radio puede ser usado para aceptar una selección de propiedades de comunicación que indica que un explorador del lado del cliente está en un “Sistema de Ordenador Cliente No Fiable”. El botón 604 de radio puede ser usado para aceptar una selección de propiedades de comunicación que indica que un explorador del lado del cliente está en un “Sistema Privado de Ordenador Cliente”. Un Sistema Privado de Ordenador Cliente puede ser un sistema de ordenador cliente de un hogar, o una corporación, que tiene acceso público limitado (o incluso ninguno). Un “Sistema de Ordenador Cliente No Fiable” puede ser un sistema de ordenador cliente que tiene acceso público aumentado, tal como, por ejemplo, un kiosco de Internet en un hotel o aeropuerto. En consecuencia, la seguridad asociada al contenido devuelto desde un servidor puede ser adecuadamente ajustado, según la fiabilidad de un sistema de ordenador cliente. El botón 608 puede ser seleccionado para enviar las credenciales de usuario ingresadas y las propiedades de comunicación seleccionadas a un sistema de ordenador servidor.

Avanzando desde la Figura 6 y con referencia ahora a la Figura 5, la Figura 5 ilustra un diagrama ejemplar de flujo de un procedimiento 500 para determinar las propiedades de comunicación asociadas a un cliente, de acuerdo a los principios de la presente invención. El procedimiento 500 será descrito con respecto al sistema de ordenador cliente y el sistema de ordenador servidor, ilustrados en la arquitectura 200 de red. El procedimiento 500 incluye un acto de enviar una página de conexión a un cliente (acto 501). El acto 501 puede incluir un sistema de ordenador servidor que envía una página de conexión que incluye una interfaz para seleccionar una o más propiedades de comunicación que pueden alterar cómo han de procesarse los mensajes del HTTP. Por ejemplo, el sistema 211 de ordenador servidor puede enviar la página 600 de conexión (o una página de conexión similar) al sistema 201 de ordenador cliente.

El procedimiento 500 incluye un acto de recibir una página de conexión desde un servidor (acto 505). El acto 505 puede incluir un sistema de ordenador cliente que recibe una página de conexión que incluye una interfaz para seleccionar una o más propiedades de comunicación que pueden alterar cómo el servidor procesa los mensajes del HTTP. Por ejemplo, el sistema 201 de ordenador cliente puede recibir la página 600 de conexión (o una página de conexión similar). El procedimiento 500 incluye un acto de presentación de la página de conexión al cliente (acto 506). El acto 506 puede incluir un explorador en un sistema de ordenador cliente, que presenta la página de conexión en el sistema de ordenador cliente. Por ejemplo, el explorador 202 puede presentar la página 600 de conexión (una página de conexión similar) en el sistema 201 de ordenador cliente.

El procedimiento 500 incluye un acto de recepción de selecciones de al menos una entre una o más propiedades de comunicación (acto 507). El acto 507 puede incluir un sistema de ordenador cliente que recibe selecciones de al menos una entre una o más propiedades de comunicación en la página de conexión. Por ejemplo, un usuario en el sistema 201 de ordenador cliente puede manipular un dispositivo de entrada (p. ej., un teclado y / o ratón) para ingresar selecciones de propiedades de comunicación en la página 600 de conexión. La página 600 de conexión puede recibir selecciones ingresadas por el usuario. Por ejemplo, la página 600 de conexión puede recibir selecciones ingresadas por el usuario, bien del botón 601 de radio o bien del botón 602 de radio, y selecciones ingresadas por el usuario, bien del botón 603 de radio o bien del botón 604 de radio (potencialmente, junto con la recepción de credenciales ingresadas por el usuario en los campos 606 y 607).

El procedimiento 500 incluye un acto de enviar las selecciones de propiedades de comunicación a un filtro de comunicación en el servidor (acto 508). El acto 508 puede incluir un sistema de ordenador cliente que envía las selecciones de propiedades de comunicación a un filtro de comunicación en el sistema de ordenador servidor. Por ejemplo, el sistema 201 de ordenador cliente puede enviar selecciones de propiedades de comunicación (p. ej., junto con

las credenciales ingresadas por el usuario) al sistema 211 de ordenador servidor. El procedimiento 500 incluye un acto de recepción de al menos una selección de propiedades de comunicación desde el cliente (acto 502). El acto 502 puede incluir que el sistema de ordenador servidor reciba selecciones de al menos una entre una o más propiedades de comunicación seleccionables en la página de conexión. Por ejemplo, el filtro 243 de comunicación puede recibir una o más selecciones de propiedades de comunicación (p. ej., seleccionadas en la página 600 de conexión) desde el sistema 201 de ordenador cliente.

El procedimiento 500 incluye un acto de interrogación del cliente para determinar si las al menos una selecciones de propiedades de comunicación recibidas disponen de soporte, así como para identificar otras propiedades de comunicación relevantes con soporte por parte del cliente (acto 503). El acto 503 puede incluir un sistema de ordenador servidor que interroga a un sistema de ordenador cliente para determinar si las selecciones de propiedades de comunicación recibidas disponen de soporte, y para identificar otras propiedades de comunicación relevantes con soporte por parte del cliente. Por ejemplo, un sistema de ordenador servidor puede determinar las capacidades del sistema de ordenador cliente usando una cabecera del HTTP de Usuario-Agente y el conocimiento previo del sistema de ordenador cliente. Las capacidades adicionales de un sistema de ordenador cliente pueden ser determinadas a través de una página de conexión y a partir de guiones (p. ej., guiones de JavaScript) que se ejecutan dentro de la página de conexión en el sistema de ordenador cliente.

Alternativamente, la interrogación de un sistema de ordenador cliente puede incluir enviar solicitudes al sistema de ordenador cliente que hacen que el sistema de ordenador cliente revele información de configuración a un sistema de ordenador servidor. Por ejemplo, el sistema 211 de ordenador servidor puede enviar solicitudes al sistema 201 de ordenador cliente, solicitando la configuración del explorador 202. En respuesta, el explorador 202 puede indicar información de configuración tal como, por ejemplo, un número de versión, y si el explorador 202 presta o no soporte a la compresión del HTTP, tal como la compresión gzip. En base a un número de versión, el sistema 211 de ordenador servidor puede determinar si una selección de “Cliente Avanzado” en la página 600 de conexión fue o no adecuada. Por ejemplo, el sistema de ordenador servidor puede ser capaz de determinar que la versión del explorador de 202 no da soporte a guiones. Así, incluso si fuera seleccionado el “Cliente Avanzado”, el sistema de ordenador servidor puede proporcionar contenido simplificado al sistema 201 de ordenador cliente.

La simplificación del contenido puede incluir reducir la cantidad de contenido que es entregada a un sistema de ordenador cliente. Por ejemplo, en respuesta a una solicitud, de cliente de nivel bajo, de información de ayuda, un sistema de ordenador servidor puede devolver información de ayuda reducida (menos locuaz). Por otra parte, en respuesta a la solicitud, de un cliente avanzado, de información de ayuda, un sistema de ordenador servidor puede devolver información de ayuda aumentada, por ejemplo, incluir guiones de búsqueda y otra funcionalidad avanzada. Un sistema de ordenador servidor también puede variar el contenido entregado en base a la fiabilidad de un sistema de ordenador cliente. Por ejemplo, un sistema de ordenador servidor puede proporcionar información de ayuda, acerca de cómo acceder a datos corporativos sensibles, a un sistema privado de ordenador cliente, pero puede no proporcionar la misma información a un sistema de ordenador de cliente no fiable.

Puede ser que el sistema 211 de ordenador servidor pruebe el explorador 202 para verificar que las características publicitadas están adecuadamente dotadas de soporte. Por ejemplo, cuando el explorador 202 indica soporte para la compresión gzip, el sistema 211 de ordenador servidor puede enviar un contenido comprimido por gzip al sistema 201 de ordenador cliente, para determinar si el explorador 202 procesa adecuadamente el contenido comprimido por gzip. Puede ser que el sistema 201 de ordenador cliente configure una cabecera de solicitud adecuada, que indique el soporte para la compresión por gzip. El sistema 201 de ordenador cliente puede incluir la cabecera de solicitud adecuada en una solicitud del cliente que es enviada a, y recibida en, el sistema 211 de ordenador servidor. En respuesta, el sistema 211 de ordenador servidor puede interrogar el sistema 201 de ordenador cliente para determinar si el sistema 201 de ordenador cliente almacena adecuadamente en memoria caché el contenido comprimido por gzip y si procesa el contenido comprimido por gzip de una manera que no afecte, por detrimento, la seguridad e integridad de una aplicación basada en la Red.

El procedimiento 500 incluye un acto de configuración del filtro de comunicación, de acuerdo a las propiedades de comunicación seleccionadas e identificadas (acto 504). El acto 504 puede incluir un sistema de ordenador servidor que configura el filtro de comunicación para procesar la comunicación del HTTP con el cliente, de acuerdo a propiedades de comunicación seleccionadas cualesquiera, y a otras propiedades relevantes identificadas que disponen de soporte por parte del cliente. Por ejemplo, el sistema 211 de ordenador servidor puede configurar el filtro 243 de comunicación para procesar la comunicación del HTTP con el sistema 201 de ordenador cliente, de acuerdo a las selecciones de propiedades de comunicación (p. ej., un sistema de ordenador de Cliente Avanzado o de Cliente No Fiable) y a otras propiedades de comunicación relevantes identificadas (p. ej., el soporte para la compresión del HTTP) del explorador 202.

Cuando un mensaje del HTTP ha de ser enviado desde el sistema 211 de ordenador servidor al sistema 201 de ordenador cliente, el filtro 243 de comunicación puede alterar las cabeceras de mensajes del HTTP y el contenido del mensaje del HTTP, para hacer que el contenido sea conforme a las propiedades de comunicación para el sistema 201 de ordenador

cliente. Por ejemplo, si el servidor 212 de correo electrónico envía un mensaje con información de correo electrónico no comprimida al sistema 201 de ordenador cliente, el filtro 243 de comunicación puede interceptar el mensaje, comprimir por gzip el contenido y alterar las cabeceras del mensaje para indicar que la información de correo electrónico está comprimida por gzip. Alternativamente, otros módulos del sistema de ordenador servidor tales como, por ejemplo, módulos de un Servidor de Información de Internet ("IIS"), pueden implementar la compresión por gzip. En consecuencia, el contenido puede ser presentado a un sistema de ordenador cliente de una manera que utilice óptimamente las capacidades del sistema de ordenador cliente, y según los deseos de un usuario.

Cuando el sistema 211 de ordenador servidor recibe una selección que india que un explorador del lado del cliente está en un "Sistema Privado de Ordenador Cliente", un almacén privado de claves rotativas tal como, por ejemplo, el almacén 231 de claves privadas, puede ser utilizado para asegurar credenciales de usuario. Por otra parte, cuando el sistema 211 de ordenador servidor recibe una selección que indica que un explorador del lado del cliente es un "Sistema de Ordenador Cliente No Fiable", un almacén no fiable de claves rotativas, tal como el almacén 221 no fiable de claves, puede ser utilizado para asegurar credenciales de usuario.

Así, hay una realización en un sistema de ordenador servidor que incluye un filtro de comunicación, donde el filtro de comunicación es capaz de alterar cabeceras de mensajes, y un procedimiento para determinar propiedades de comunicación asociadas a un sistema de ordenador cliente comprende: un acto de envío de una página de conexión al sistema de ordenador cliente, incluyendo la página de conexión una interfaz para seleccionar una o más propiedades de comunicación seleccionables que puedan alterar cómo han de ser procesados los mensajes del HTTP; un acto de recepción de selecciones de al menos una de dichas una o más propiedades de comunicación seleccionables desde la página de conexión, indicando las propiedades de comunicación seleccionadas al filtro de comunicación cómo ha de ser procesada la comunicación del HTTP con el sistema de ordenador cliente; un acto de interrogación del sistema de ordenador cliente para determinar si dichas al menos una selecciones de propiedades de comunicación recibidas disponen de soporte, así como para identificar otras propiedades de comunicación relevantes con soporte por parte del sistema de ordenador cliente; y un acto de configuración del filtro de comunicación para procesar la comunicación del HTTP con el cliente, de acuerdo a cualquier propiedad de comunicación seleccionada y otras propiedades de comunicación relevantes identificadas que disponen de soporte por parte del cliente.

En el procedimiento, el acto de recepción de selecciones de al menos una entre dichas una o más propiedades de comunicación seleccionables desde la página de conexión puede comprender un acto de recepción de una selección de propiedades de comunicación que indica la fiabilidad del sistema de ordenador cliente.

En el procedimiento, el acto de recepción de selecciones de al menos una entre dichas una o más propiedades de comunicación seleccionables desde la página de conexión puede comprender un acto de recepción de una selección de propiedades de comunicación que indica las capacidades de procesamiento de contenido y / o el nivel deseado de funcionalidad del sistema de ordenador cliente.

En el procedimiento, un acto de interrogación del sistema de ordenador cliente puede comprender el acto de determinar que el sistema de ordenador cliente presta soporte a la compresión del HTTP.

Además, puede proporcionarse un procedimiento en un sistema de ordenador cliente. El procedimiento es para indicar las propiedades de comunicación deseadas a un sistema de ordenador servidor. El procedimiento comprende: un acto de recepción de una página de conexión desde el sistema de ordenador servidor, incluyendo la página de conexión una interfaz para seleccionar una o más propiedades de comunicación seleccionables, que pueden alterar cómo el servidor procesa los mensajes del HTTP; un acto de presentación de la página de conexión en el cliente; un acto de recepción de selecciones de al menos una entre dichas una o más propiedades de comunicación en la página de conexión; y un acto de envío de las selecciones de propiedades de comunicación a un filtro de comunicación en el sistema de ordenador servidor, indicando las selecciones de propiedades de comunicación al filtro de comunicación cómo ha de ser procesada la comunicación del HTTP con el sistema de ordenador cliente.

En el procedimiento, el acto de recepción de selecciones de al menos una entre dichas una o más propiedades de comunicación en la página de conexión puede comprender el acto de recibir una selección que indica la fiabilidad del sistema de ordenador cliente.

En el procedimiento, el acto de recepción de selecciones de al menos una entre dichas una o más propiedades de comunicación en la página de conexión puede comprender un acto de recibir una selección que indica las capacidades de procesamiento de contenido y / o el nivel deseado de funcionalidad del sistema de ordenador cliente.

En el procedimiento, el acto del envío de las selecciones de propiedades de comunicación a un filtro de comunicación en el sistema de ordenador servidor puede comprender un acto de envío de las selecciones de propiedades de comunicación junto con las credenciales de usuario.

Con referencia ahora de nuevo a la Figura 3, el procedimiento 300 incluye un acto de utilización de la página de conexión

para presentar credenciales al servidor (acto 303). El acto 303 puede incluir el sistema de ordenador cliente, utilizando la página de conexión para presentar credenciales al sistema de ordenador servidor. Por ejemplo, el sistema 201 de ordenador cliente puede utilizar la página 217 de conexión para presentar credenciales (en potencia, junto con selecciones de propiedades de comunicación) al sistema 211 de ordenador servidor. Las credenciales de usuario y las selecciones de propiedades de comunicación pueden ser incluidas como elementos de conexión en un mensaje de correo que es presentado a un validador del formato de elementos de conexión. Por ejemplo, el sistema 201 de ordenador cliente puede enviar el mensaje 254 de correo, que incluye elementos 273 de conexión, al sistema de ordenador servidor.

El procedimiento 300 incluye un acto de recepción de credenciales de usuario que fueron presentadas en la página de conexión (acto 308). El acto 308 puede incluir un sistema de ordenador servidor que recibe credenciales de usuario que fueron presentadas en la página de conexión. Por ejemplo, el sistema 211 de ordenador servidor puede recibir credenciales de usuario (en potencia, junto con las selecciones de propiedades de comunicación) desde el sistema 201 de ordenador cliente. Las credenciales y las selecciones de propiedades de comunicación pueden ser recibidas como elementos de conexión en un mensaje de correo. Por ejemplo, el sistema 211 de ordenador servidor puede recibir el mensaje 254 de correo, que incluye los elementos 273 de conexión, desde el sistema 201 de ordenador cliente. Según lo indicado por la línea discontinua a través del filtro 243 de comunicación, el filtro 243 de comunicación puede ser configurado para permitir que el mensaje 254 de correo pase sin alterar el mensaje 254 de correo. En consecuencia, el mensaje 254 de correo puede ser remitido al validador 216 de elementos de conexión sin modificación. Cuando corresponda, una conexión mutuamente autenticada, por ejemplo, usando la Seguridad de la Capa de Transporte ("TLS") o la Capa de Receptáculos Seguros ("SSL"), puede ser establecida entre un sistema de ordenador cliente y un sistema de ordenador servidor, para reducir la probabilidad de procesos maliciosos, o de usuarios "olfateando" paquetes, y para reducir la probabilidad de ataques de intermediarios.

El validador 216 de elementos de conexión también puede generar un identificador único, tal como, por ejemplo, un Identificador Globalmente Único ("GUID") para el sistema 201 de ordenador cliente. El validador 216 de elementos de conexión puede usar la firma digital y algoritmos de cifrado para asegurar las credenciales de usuario recibidas (p. ej., las incluidas en los elementos 273 de conexión). Por ejemplo, el validador 216 de elementos de conexión puede generar una firma digital usada para validar posteriormente credenciales de usuario recibidas. El validador 216 de elementos de conexión puede obtener una clave de firma, que puede ser usada para rubricar datos digitalmente, por troceo (p. ej., usando los algoritmos de troceo SHA1 o MD-5) de una combinación de una clave más actual en un almacén de claves rotativas, el identificador único generado y una primera cadena constante. En algunas realizaciones, una firma digital es representada como un Código de Autenticación de Mensaje Con rutinas de autentificación. En consecuencia, una clave de firma puede ser deducida según la Fórmula 1:

$$\mathbf{K_{SIG} = SHA\text{-}1\ (K_{ROTATIVA\ MÁS\ ACTUAL},\ GUID,\ HMACCadenaClave)}$$

FÓRMULA 1

En la Fórmula 1, $K_{ROTATIVA\ MÁS\ ACTUAL}$ representa la clave más actual en el almacén adecuado de claves rotativas. Por ejemplo, cuando el explorador 202 está en un "Sistema Privado de Ordenador Cliente" (p. ej., según lo indicado por una selección de propiedades de comunicación), $K_{ROTATIVA}$ MÁS ACTUAL representa la clave más actual en el almacén privado 231 de claves rotativas (p. ej., la clave 232). GUID representa un identificador único correspondiente al sistema 201 de ordenador cliente. HMACCadenaClave representa una cadena constante de texto. A partir de K_{SIG} puede generarse un Código de Autenticación de Mensaje Con rutinas de autentificación según la Fórmula 2:

$$\mathbf{Firma\ Digital = HMAC\ (K_{SIG},\ (GUID,\ \{nombre\ de\ usuario:\ contraseña\},\ Indicadores)\}}$$

FÓRMULA 2

En la Fórmula 2, HMAC representa un algoritmo de Código de Autenticación de Mensaje Con rutinas de autentificación tal como, por ejemplo, el descrito en la Solicitud de Comentarios ("RFC") 2104. La parte de (GUID, {nombre de usuario: contraseña}, Indicadores) de la Fórmula 2 representa que el GUID, las credenciales de usuario y los indicadores que representan selecciones de propiedades de comunicación están incluidos como texto ingresado al algoritmo del Código de Autenticación de Mensaje Con rutinas de autentificación. Cuando corresponda, las credenciales de usuario pueden ser convertidas al formato de texto (p. ej., por codificación, por base64, de las credenciales de usuario) para su compatibilidad con un algoritmo del Código de Autenticación de Mensaje Con rutinas de autentificación. Aunque se describe en términos de un algoritmo del Código de Autenticación de Mensaje Con rutinas de autentificación, el algoritmo usado para generar una firma digital no es importante, y puede usarse prácticamente cualquier algoritmo de firma digital, digesto o código de autenticación.

El validador 216 de elementos de conexión también puede obtener una clave de cifrado, que puede ser usada para cifrar datos, troceando una combinación de una clave más actual en un almacén de claves rotativas, el identificador único y una

segunda cadena constante. En consecuencia, puede deducirse una clave de cifrado según la Fórmula 3:

$$K_{ENC} = \text{SHA-1}\ (K_{\text{ROTATIVA MÁS ACTUAL}}, \text{GUID, CifradoClaveCadena})$$

FÓRMULA 3

En la Fórmula 3, $K_{\text{ROTATIVA MÁS ACTUAL}}$ representa la clave más actual proveniente de un almacén de claves rotativas que fue usada en la generación de la clave de firma. De tal modo, si la clave 232 fue usada para generar K_{SIG}, la clave 232 también puede ser usada para generar K_{ENC}. GUID representa el identificador único correspondiente al sistema 201 de ordenador cliente. CifradoClaveCadena representa una cadena constante de texto que difiere de HMACClaveCadena. En consecuencia, la información cifrada puede ser generada según la Ecuación 4:

$$\text{Información Cifrada} = K_{ENC}\ [\text{Firma Digital}, \{\text{nombre de usuario: contraseña}\}, \text{Indicadores}]$$

FÓRMULA 4

En la Fórmula 4, la Firma Digital representa la Firma Digital generada por la Fórmula 2, {nombre de usuario: contraseña} representa las credenciales de usuario e Indicadores representa las selecciones de propiedades de comunicación.

La etapa 311 incluye un acto correspondiente de envío de información cifrada que representa al menos una parte de las credenciales de usuario y una firma dependiente del tiempo (acto 309). El acto 309 puede incluir el envío por el sistema de ordenador servidor de información cifrada que representa al menos una parte de las credenciales de usuario y una firma dependiente del tiempo al sistema de ordenador cliente. Por ejemplo, el validador 216 de elementos de conexión puede enviar el mensaje 255, que incluye el GUID 274 y las credenciales cifradas 275, al sistema 201 de ordenador cliente. Según lo indicado por la línea discontinua a través del filtro 243 de comunicación, el filtro 243 de comunicación puede ser configurado para permitir que el mensaje 255 pase sin alterar el mensaje 255. En consecuencia, el mensaje 255 puede ser remitido al sistema 201 de ordenador cliente sin modificación.

El procedimiento 300 incluye un acto de recepción de información cifrada que representa al menos una parte de las credenciales de usuario y una firma dependiente del tiempo (acto 304). El acto 304 puede incluir la recepción por el sistema de ordenador cliente de información cifrada que representa al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, desde el sistema de ordenador servidor. Por ejemplo, el sistema 201 de ordenador cliente puede recibir el mensaje 255, que incluye el GUID 274 y las credenciales cifradas 275, desde el sistema 211 de ordenador servidor. El mensaje 255 puede ser configurado para hacer que el sistema 201 de ordenador cliente almacene el GUID 274 y las credenciales cifradas 275 en los señuelos 203. Por ejemplo, el mensaje 255 puede ser configurado de la siguiente manera:

Fijar-Señuelo:idsesión={GUID};trayecto=/

Fijar-Señuelo:datoscred={Información Cifrada};trayecto=/

El procedimiento 300 incluye un acto de envío de una segunda solicitud que incluye la información cifrada (acto 305). El acto 305 puede incluir el envío por el sistema de ordenador cliente de una segunda solicitud de acceso basado en la Red al recurso (p. ej., el mensaje de correo electrónico solicitado en la primera solicitud). Por ejemplo, el sistema 201 de ordenador cliente puede enviar la solicitud 256, que incluye el URI 267 del servidor de correo, el GUID 274 y las credenciales cifradas 275, al sistema 211 de ordenador servidor. El procedimiento 300 incluye un acto de recepción de una segunda solicitud que incluye la información cifrada (acto 310). El acto 310 puede incluir la recepción por el sistema de ordenador servidor de una segunda solicitud para el acceso basado en la Red al recurso (p. ej., el mensaje de correo electrónico solicitado en la primera solicitud). Por ejemplo, el sistema 211 de ordenador servidor puede recibir la solicitud 256, que incluye el URI 267 del servidor de correo, el GUID 274 y las credenciales cifradas 275, desde el sistema 201 de ordenador cliente.

En algunas realizaciones, un sistema de ordenador cliente ya almacena los señuelos correspondientes con un GUID e información cifrada en la memoria del explorador. El GUID almacenado y la información cifrada pueden ser usados al solicitar acceso basado en la Red a un recurso (p. ej., datos de correo electrónico) en un servidor. La Figura 2B ilustra un ejemplo de arquitectura 200 de red que facilita la utilización de credenciales aseguradas del lado del cliente para acceder a un recurso en un servidor, de acuerdo a la presente invención. La Figura 4 ilustra un diagrama ejemplar de flujo de un procedimiento 400 para utilizar credenciales aseguradas del lado del cliente para acceder a un recurso en un servidor, de acuerdo a la presente invención. El procedimiento 400 será descrito con respecto al sistema de ordenador cliente y al sistema de ordenador servidor ilustrados en la Figura 2B.

El procedimiento 400 incluye un acto de envío de una solicitud, que incluye un identificador de sesión y credenciales de usuario cifradas, para el acceso basado en la Red a un recurso en un servidor (acto 401). El acto 401 puede incluir el envío por un sistema de ordenador cliente de una solicitud de acceso basado en la Red a un recurso en un sistema de ordenador servidor. Por ejemplo, el sistema 201 de ordenador cliente puede enviar la solicitud 291, que incluye el URI 267

del servidor de correo, el GUID 274 y las credenciales cifradas 275, al sistema 211 de ordenador servidor. El URI 267 del servidor de correo representa un URI que proporciona acceso a recursos de correo electrónico controlados por el servidor 212 de correo electrónico. El GUID 274 representa un identificador único de sesión que fue previamente enviado desde el sistema 211 de ordenador servidor al sistema 201 de ordenador cliente. Las credenciales cifradas 275 representan credenciales de usuario cifradas y una firma dependiente del tiempo, que fueron previamente enviadas desde el sistema 211 de ordenador servidor al sistema 201 de ordenador cliente. Las credenciales cifradas 275 pueden haber sido generadas a partir de una clave en un almacén adecuado de claves rotativas.

El procedimiento 400 incluye un acto de recepción de una solicitud, que incluye un identificador de sesión y credenciales de usuario cifradas, para el acceso basado en la Red a un recurso en el servidor (acto 404). El acto 404 puede incluir la recepción por el sistema de ordenador servidor de una solicitud para el acceso basado en la Red a un recurso en el sistema de ordenador servidor. Por ejemplo, el sistema 211 de ordenador servidor puede recibir la solicitud 291, que incluye el URI 267 del servidor de correo, el GUID 274 y las credenciales cifradas 275, desde el sistema 201 de ordenador cliente.

El procedimiento 400 incluye un acto de intento de validar las credenciales de usuario cifradas, usando la clave más actual en un almacén de claves rotativas (acto 405). El acto 405 puede incluir el intento por el sistema de ordenador servidor de validar al menos una parte de las credenciales de usuario, usando la clave más actual en un almacén de claves rotativas. Por ejemplo, cuando se indica que el explorador 202 está en un sistema privado de ordenador cliente, el sistema de ordenador servidor puede intentar validar las credenciales cifradas 275 usando la clave 232. Por otra parte, cuando se indica que el explorador 202 está en un sistema no fiable de ordenador cliente, el sistema de ordenador servidor puede intentar validar las credenciales cifradas 275 usando la clave 222. El validador 237 de credenciales puede obtener una clave de descifrado, que puede ser usada para descifrar datos, troceando una combinación de la clave más actual proveniente de un almacén adecuado de claves rotativas, el identificador único de sesión y la segunda cadena constante (usada al obtener la clave de cifrado). En consecuencia, una clave de descifrado puede ser deducida según la Fórmula 5:

$$\mathbf{K_{DCR} = SHA\text{-}1\ (K_{ROTATIVA\ MÁS\ ACTUAL},\ GUID,\ CifradoClaveCadena)}$$

FÓRMULA 5

En la Fórmula 5, $\mathbf{K_{ROTATIVA\ MÁS\ ACTUAL}}$ representa la clave más actual en un almacén adecuado de claves rotativas (p. ej., la clave 232 o la clave 222). GUID representa el identificador único correspondiente al sistema 201 de ordenador cliente. CifradoClaveCadena representa la cadena constante usada durante la obtención de K_{ENC}. En consecuencia, el validador 237 de credenciales puede descifrar la información cifrada para revelar una Firma Digital, Credenciales de Usuario e Indicadores que representan selecciones de propiedades de comunicación, según la Fórmula 6:

$$\mathbf{Firma\ Digital,\ \{nombre\ de\ usuario{:}contraseña\},\ Indicadores = K_{DCR}\ [Información\ Cifrada]}$$

FÓRMULA 6

El validador 237 de credenciales puede obtener una clave de validación, que puede ser usada para generar una firma digital de validación, troceando una combinación de la clave más actual en un almacén adecuado de claves rotativas, el identificador único y una primera cadena constante. En algunas realizaciones, una firma digital de validación es representada como un Código de Autenticación de Mensaje Con rutinas de autentificación. En consecuencia, una clave de validación puede ser deducida según la Fórmula 7:

$$\mathbf{K_{VAL} = SHA\text{-}1\ (K_{ROTATIVA\ MÁS\ ACTUAL},\ GUID,\ HMACClaveCadena)}$$

FÓRMULA 7

En la Fórmula 7, $K_{ROTATIVA\ MÁS\ ACTUAL}$ representa la clave más actual en un almacén adecuado de claves rotativas. GUID representa el identificador único correspondiente al sistema 201 de ordenador cliente. HMACClaveCadena representa la cadena constante de texto usada al obtener la clave de firma. A partir de K_{VAL}, y usando las credenciales de usuario reveladas y los Indicadores de la Fórmula 6, puede generarse un Código de Autenticación de Mensaje Con rutinas de autentificación según la Fórmula 8:

$$\mathbf{Firma\ Digital\ de\ Validación = HMAC\ (K_{VAL},\ (GUID,\ \{nombre\ de\ usuario{:}\ contraseña\},\ Indicadores)\}}$$

FÓRMULA 8

En la Fórmula 8, HMAC representa un algoritmo del Código de Autenticación de Mensaje Con rutinas de autentificación. La parte de (GUID, {nombre de usuario:contraseña}, Indicadores) de la Fórmula 8 representa que el GUID, las credenciales de usuario y los indicadores que representan selecciones de propiedades de comunicación están incluidos como texto introducido en el algoritmo del Código de Autenticación de Mensaje Con rutinas de autentificación. Aunque

está descrito en términos de un algoritmo del Código de Autenticación de Mensaje Con rutinas de autentificación, el algoritmo usado para generar una firma digital de validación no es importante, y puede usarse prácticamente cualquier algoritmo de firma digital, digesto o código de autenticación.

Cuando la firma digital de validación es igual a la firma digital, las credenciales de usuario representadas en las credenciales cifradas 275 son validadas. En consecuencia, el filtro 243 de comunicación construye una cabecera de autorización (p. ej., una cabecera de autorización del HTTP) que incluye las credenciales de usuario validadas. El filtro 243 de comunicación puede insertar la cabecera de autorización en la solicitud de acceso basado en la Red a un recurso. Por ejemplo, el filtro 243 de comunicación puede eliminar las credenciales cifradas 275 de la solicitud 291 e insertar las credenciales 289 en la solicitud 291, dando como resultado la solicitud 291A.

Cuando la firma digital de validación no es igual a la firma digital, las credenciales de usuario no son validadas. En consecuencia, el validador 237 de credenciales repite la funcionalidad de las Fórmulas 5, 6, 7 y 8 en base a la siguiente clave más actual en el almacén adecuado de claves rotativas. Por ejemplo, para un explorador del lado del cliente en un sistema privado de ordenador cliente, el validador 237 de credenciales puede usar la clave 233. Por otra parte, para un explorador del lado del cliente en un cliente no fiable, el validador 237 de credenciales puede usar la clave 223. El validador de credenciales puede intentar validar credenciales de usuario usando cada clave en un almacén adecuado de claves rotativas. Las credenciales de usuario validadas pueden ser incluidas en una cabecera de autorización adecuada.

En algunas realizaciones, se incluye un índice junto con las credenciales cifradas, para indicar la clave rotativa que ha de ser usada para intentar validar las credenciales cifradas (p. ej., la clave rotativa previamente usada para cifrar las credenciales). Por ejemplo, el sistema 201 de ordenador cliente puede incluir un índice, que identifica una clave rotativa en un almacén 221 no fiable de claves rotativas, o en un almacén 231 privado de claves rotativas, en la solicitud 291. Un índice puede ser un valor numérico (p. ej., 0, 1, 2, etc.) que identifica la generación de una clave rotativa que ha de ser usada. Por ejemplo, cuando el sistema 201 de ordenador cliente es un sistema privado de ordenador cliente, un índice 0 puede identificar la clave 232. De manera similar, cuando el sistema 201 de ordenador cliente es un sistema no fiable de ordenador cliente, un índice 2 puede identificar la clave 224. En consecuencia, el uso de un índice puede aumentar la eficacia del proceso de validación. Cuando las credenciales no son validadas con una clave rotativa identificada en un índice, entonces pueden ser usadas otras claves en un almacén correspondiente de claves rotativas para intentar validar las credenciales.

El procedimiento 400 incluye un acto de remisión de la solicitud a un módulo que controla el acceso basado en la Red al recurso solicitado (acto 406). El acto 406 puede incluir la remisión por el sistema de ordenador servidor de la solicitud a un módulo que controla el acceso basado en la Red al recurso. Por ejemplo, el filtro 243 de comunicación puede remitir la solicitud 291A, que incluye el URI 267 del servidor de correo y las credenciales 289 (según lo revelado a partir de las credenciales cifradas 275), al servidor 212 de correo electrónico. El servidor 212 de correo electrónico puede ser un módulo que controla el acceso basado en la Red a recursos de correo electrónico. El servidor 212 de correo electrónico puede comparar las credenciales 289 con la base 213 de datos de credenciales, para determinar si está autorizado el acceso basado en la Red a un recurso solicitado del correo electrónico.

El procedimiento 400 incluye un acto de determinación de si deberían obtenerse credenciales de usuario cifradas refrescadas a partir de la clave más actual en el almacén de claves rotativas (acto 407). El acto 407 puede incluir la determinación por el sistema de ordenador servidor de si debería obtenerse información cifrada refrescada que represente las credenciales de usuario y una firma dependiente del tiempo, a partir de la clave más actual en el almacén de claves rotativas. Cuando las credenciales de usuario son validadas con una clave proveniente de un almacén de claves rotativas, distinta a la clave más actual proveniente del almacén de claves rotativas, el servidor determina que ha de obtenerse información cifrada refrescada. Por ejemplo, si el validador 237 de credenciales valida las credenciales cifradas con la clave 224, el filtro 243 de comunicación puede determinar que han de obtenerse credenciales cifradas refrescadas para las credenciales de usuario representadas en las credenciales cifradas.

En consecuencia, según lo representado por la flecha de línea discontinua, el filtro 243 de comunicación puede enviar optativamente la solicitud 294 de refresco de señuelo al validador 216 de elementos de conexión. El validador 216 de elementos de conexión puede usar la clave rotativa más actual en un almacén adecuado de claves rotativas para obtener la información cifrada refrescada (p. ej., obteniendo una firma digital refrescada y una clave de cifrado refrescada a partir de la clave más actual). El validador 216 de elementos de conexión puede devolver un GUID actualizado y credenciales cifradas refrescadas al filtro 243 de comunicación. Por ejemplo, según lo representado por la flecha de línea discontinua, el validador 216 de elementos de conexión devuelve el mensaje 295, que incluye el GUID 296 actualizado y las credenciales 297 cifradas refrescadas, al filtro 243 de comunicación.

Cuando las credenciales 289 son las adecuadas para el acceso basado en la Red a recursos de correo electrónico en el servidor 212 de correo electrónico, el servidor 212 de correo electrónico puede devolver un recurso de correo electrónico en respuesta a la solicitud 291 A. Por ejemplo, el servidor 212 de correo electrónico puede devolver la respuesta 292, que incluye el recurso 293 (p. ej., un mensaje de correo electrónico), al filtro 243 de comunicación. Por otra parte, cuando las

credenciales 289 no son adecuadas para el acceso basado en la Red a recursos de correo electrónico en el servidor 212 de correo electrónico, el servidor 212 de correo electrónico puede devolver una indicación de desautorización en respuesta a la solicitud 291 A. Por ejemplo, según lo representado por la flecha de línea discontinua, el servidor 212 de correo electrónico puede devolver la respuesta 294, que incluye el indicador 272 de desautorización, al filtro 243 de comunicación, Cuando el filtro 243 de comunicación recibe un indicador de desautorización, el filtro 243 de comunicación puede redirigir el sistema 201 de ordenador cliente a la página 217 de conexión.

Cuando las credenciales de usuario validadas son las adecuadas, el filtro 243 de comunicación puede enviar un recurso solicitado al sistema 201 de ordenador cliente. Por ejemplo, cuando las credenciales cifradas 275 son validadas con la clave más actual de un almacén adecuado de claves rotativas, la respuesta 292, que incluye el recurso 293, es recibida en el filtro 243 de comunicación. El filtro 243 de comunicación puede remitir la respuesta 292 al sistema 201 de ordenador cliente. En consecuencia, el recurso 293 puede ser presentado en el explorador 202.

Cuando las credenciales de usuario validadas son las adecuadas, el filtro 243 de comunicación también puede enviar credenciales cifradas refrescadas y un GUID actualizado, junto con un recurso, al sistema 201 de ordenador cliente. Por ejemplo, cuando las credenciales cifradas 275 son validadas con una clave del almacén de claves rotativas que no es la clave más actual en el almacén de claves rotativas, el recurso 293, el GUID 296 actualizado y las credenciales 297 cifradas refrescadas pueden ser recibidas en el filtro 243 de comunicación. Según lo representado por la flecha de línea discontinua, el módulo 243 de comunicación puede entonces enviar la respuesta 276, que incluye el recurso 293, el GUID 296 actualizado y las credenciales 297 cifradas refrescadas, al sistema 201 de ordenador cliente.

El procedimiento 400 incluye un acto de recepción del recurso junto con un identificador de sesión actualizado y credenciales de usuario cifradas refrescadas en un explorador del lado del cliente (acto 402). El acto 402 puede incluir la recepción por el sistema de ordenador cliente de lo solicitado, junto con un identificador de sesión actualizado e información cifrada refrescada que representa al menos la parte de las credenciales de usuario y una firma refrescada dependiente del tiempo. Por ejemplo, el sistema 201 de ordenador cliente puede recibir la respuesta 276, que incluye el recurso 293, el GUID 296 actualizado y las credenciales 297 cifradas refrescadas, desde el sistema 201 de ordenador servidor.

El procedimiento 400 incluye un acto de almacenamiento del identificador de sesión actualizado y las credenciales de usuario cifradas refrescadas en los correspondientes señuelos (acto 403). El acto 403 puede incluir el almacenamiento por el sistema de ordenador cliente del identificador de sesión actualizado y la información cifrada refrescada, en señuelos correspondientes en el sistema de ordenador cliente. Por ejemplo, el GUID 296 actualizado y las credenciales 297 cifradas refrescadas pueden ser almacenadas en correspondientes señuelos, en los señuelos 203, sobrescribiendo el GUID 274 y las credenciales cifradas 275. El recurso 293 puede ser presentado en el explorador 202.

Según una realización adicional, en un sistema de ordenador servidor que recibe solicitudes desde sistemas de ordenador cliente, solicitudes que solicitan acceso basado en la Red a recursos en el sistema de ordenador servidor, puede proporcionarse un procedimiento para asegurar las credenciales del lado del cliente que han de ser usadas para ser autorizado a acceder a recursos. El procedimiento comprende: un acto de recepción, por el servidor, de una primera solicitud de acceso basado en la Red a un recurso, siendo enviada la primera solicitud por el sistema de ordenador cliente; una etapa para usar una clave de un almacén de claves rotativas, para asegurar credenciales del lado del cliente, a fin de reducir la posibilidad de que las credenciales del lado del cliente proporcionen a un usuario malicioso acceso no autorizado a un recurso; y un acto de recepción, por el sistema de ordenador servidor, de una segunda solicitud de acceso basado en la Red al recurso, siendo la segunda solicitud enviada desde el sistema de ordenador cliente, e incluyendo información cifrada.

Según otra realización, en un sistema de ordenador servidor que incluye un filtro de comunicación, siendo el filtro de comunicación capaz de alterar cabeceras de mensajes, puede ser proporcionado un procedimiento para determinar propiedades de comunicación asociadas a un sistema de ordenador cliente. El procedimiento comprende: enviar una página de conexión al sistema de ordenador cliente, incluyendo la página de conexión una interfaz para seleccionar una o más propiedades de comunicación seleccionables, que puedan alterar cómo han de ser procesados los mensajes del HTTP; recibir selecciones de al menos una entre dichas una o más propiedades de comunicación seleccionables a partir de la página de conexión, indicando las propiedades de comunicación seleccionadas al filtro de comunicación cómo ha de ser procesada la comunicación del HTTP con el sistema de ordenador cliente; interrogar al sistema de ordenador cliente para determinar si dicha al menos una selección de propiedades de comunicación recibida dispone de soporte, así como para identificar otras propiedades de comunicación relevantes con soporte por parte del sistema de ordenador cliente; y configurar el filtro de comunicación para procesar la comunicación del HTTP con el cliente, de acuerdo a cualquier propiedad de comunicación seleccionada, y otras propiedades de comunicación relevantes identificadas que disponen de soporte por parte del cliente.

La presente invención puede ser realizada en otras formas específicas sin apartarse de su espíritu o características esenciales. Las realizaciones descritas han de ser consideradas, en todos los aspectos, solamente como ilustrativas y no

restrictivas. El alcance de la invención, por lo tanto, está indicado por las reivindicaciones adjuntas, en vez de la descripción precedente. Todos los cambios que queden dentro del significado y la gama de equivalencia de las reivindicaciones han de estar comprendidas dentro de su alcance.

REIVINDICACIONES

1. Un procedimiento en un sistema (211) de ordenador servidor para determinar la validez de credenciales de usuario usadas para el acceso basado en la Red a recursos en el sistema de ordenador servidor, comprendiendo el procedimiento:

un acto de recepción (404), por el sistema de ordenador servidor, de una solicitud para el acceso basado en la Red a un recurso en el servidor, incluyendo la solicitud un identificador único de sesión e información cifrada que representa al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, siendo deducida la firma dependiente del tiempo de al menos una parte de las credenciales de usuario y de una clave de firma dependiente del tiempo, estando cifrada la información cifrada usando una clave de cifrado dependiente del tiempo, siendo deducidas, tanto la clave de firma dependiente del tiempo como la clave de cifrado dependiente del tiempo, a partir de una clave en un almacén (220) de claves rotativas;

un acto de intento (405), por el sistema de ordenador servidor, de validar al menos una parte de las credenciales de usuario, usando la clave más actual en un almacén de claves rotativas;

un acto de remisión (406), por el sistema de ordenador servidor, de la solicitud a un módulo que controla el acceso basado en la Red al recurso solicitado; y

un acto de determinación (407), por el sistema de ordenador servidor, de si la información cifrada refrescada que representa dicha al menos una parte de las credenciales de usuario, y una firma dependiente del tiempo, han de ser deducidas de la clave más activa en el almacén de claves rotativas.

2. El procedimiento según la reivindicación 1, en el cual el acto de intentar validar al menos una parte de las credenciales de usuario, usando la clave más actual en un almacén de claves rotativas, comprende un acto de determinación de que, en base a la clave más actual en el almacén de claves rotativas, dicha al menos una parte de las credenciales de usuario es válida.

3. El procedimiento según la reivindicación 1, en el cual el acto de intentar validar al menos una parte de las credenciales de usuario, usando la clave más actual en un almacén de claves rotativas, comprende un acto de determinación de que, en base a la clave más actual en el almacén de claves rotativas, dicha al menos una parte de las credenciales de usuario no es válida.

4. El procedimiento según la reivindicación 1, que comprende adicionalmente:

un acto de determinación, por el sistema de ordenador servidor, de que, en base a una clave previamente generada en el almacén de claves rotativas, dicha al menos una parte de las credenciales de usuario es válida, siendo insertada la clave previamente generada en el almacén de claves rotativas, antes de la clave más actual.

5. El procedimiento según la reivindicación 1, en el cual el acto de determinación, por el sistema de ordenador servidor, de si debería ser deducida información cifrada refrescada, que representa dicha al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, a partir de la clave más actual en el almacén de claves rotativas, comprende un acto de determinación de si debería ser deducida información cifrada refrescada, que representa dicha al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, a partir de la clave más actual en el almacén de claves rotativas.

6. El procedimiento según la reivindicación 5, en el cual el acto de determinación de si debería ser deducida información cifrada refrescada, que representa dicha al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, a partir de la clave más actual en el almacén de claves rotativas, comprende un acto de determinación de que el sistema de ordenador servidor validó dicha al menos una parte de las credenciales de usuario en base a una clave previamente generada en el almacén de claves rotativas, siendo insertada la clave previamente generada en el almacén de claves rotativas antes de la clave más actual.

7. El procedimiento según la reivindicación 5, en el cual el acto de determinación de si debería ser deducida información cifrada refrescada, que representa dicha al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, a partir de la clave más actual en el almacén de claves rotativas, comprende un acto de determinar que el sistema de ordenador servidor no pudo validar dicha al menos una parte de las credenciales de usuario con ninguna clave en el almacén de claves rotativas.

8. El procedimiento según la reivindicación 7, que comprende adicionalmente:

un acto de redirección, por el sistema de ordenador servidor, del sistema ordenador cliente a una página de conexión que proporciona una interfaz para recibir credenciales de usuario.

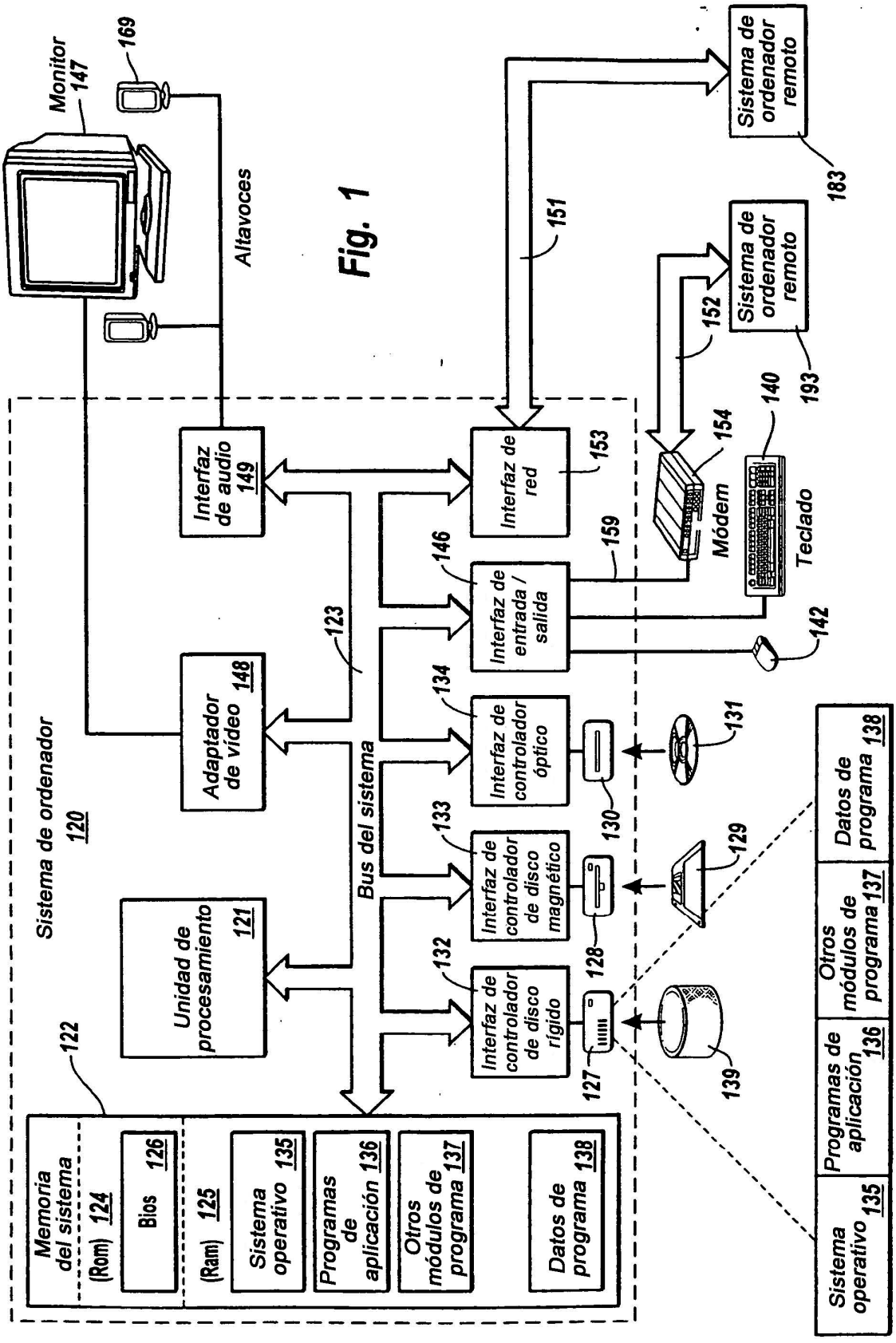
9. El procedimiento según la reivindicación 1, en el cual el acto de determinar, por el sistema de ordenador servidor, si ha de obtenerse información cifrada refrescada, que representa dicha al menos una parte de las credenciales de usuario y una firma dependiente del tiempo, a partir de la clave más actual en el almacén de claves rotativas, comprende un acto de obtener información cifrada refrescada y una firma dependiente del tiempo a partir de la clave más actual en el almacén de claves rotativas.

10. El procedimiento según la reivindicación 9, que comprende adicionalmente:

un acto de envío, por el sistema de ordenador servidor, del recurso solicitado, el identificador único de sesión actualizado e información cifrada refrescada al sistema de ordenador cliente.

11. Un producto de programa de ordenador, para su uso en un sistema de ordenador servidor, siendo el producto de programa de ordenador para implementar un procedimiento para determinar la validez de credenciales de usuario usadas para el acceso en base a la Red a recursos en el sistema de ordenador servidor, comprendiendo el producto de programa de ordenador uno o más medios legibles por ordenador que tienen almacenadas en los mismos instrucciones ejecutables que, cuando son ejecutadas por un procesador, hacen que el sistema de ordenador servidor realice el procedimiento de una de las reivindicaciones 1 a 10.

12. Un sistema informático que comprende medios adaptados para realizar el procedimiento de una de las reivindicaciones 1 a 10.


Monitor 147
169
Altavoces
Fig. 1
Sistema de ordenador 120
Interfaz de audio 149
Interfaz de red 153
Sistema de ordenador remoto 183
151
152
Sistema de ordenador remoto 193
140
154
Módem
Teclado
142
159
146
Interfaz de entrada / salida
123
Adaptador de vídeo 148
134
Interfaz de controlador óptico
131
Bus del sistema
133
Interfaz de controlador de disco magnético
130
129
132
Interfaz de controlador de disco rígido
128
127
139
Unidad de procesamiento 121
122
Memoria del sistema
(Rom) 124
Bios 126
(Ram) 125
Sistema operativo 135
Programas de aplicación 136
Otros módulos de programa 137
Datos de programa 138
Sistema operativo 135
Programas de aplicación 136
Otros módulos de programa 137
Datos de programa 138

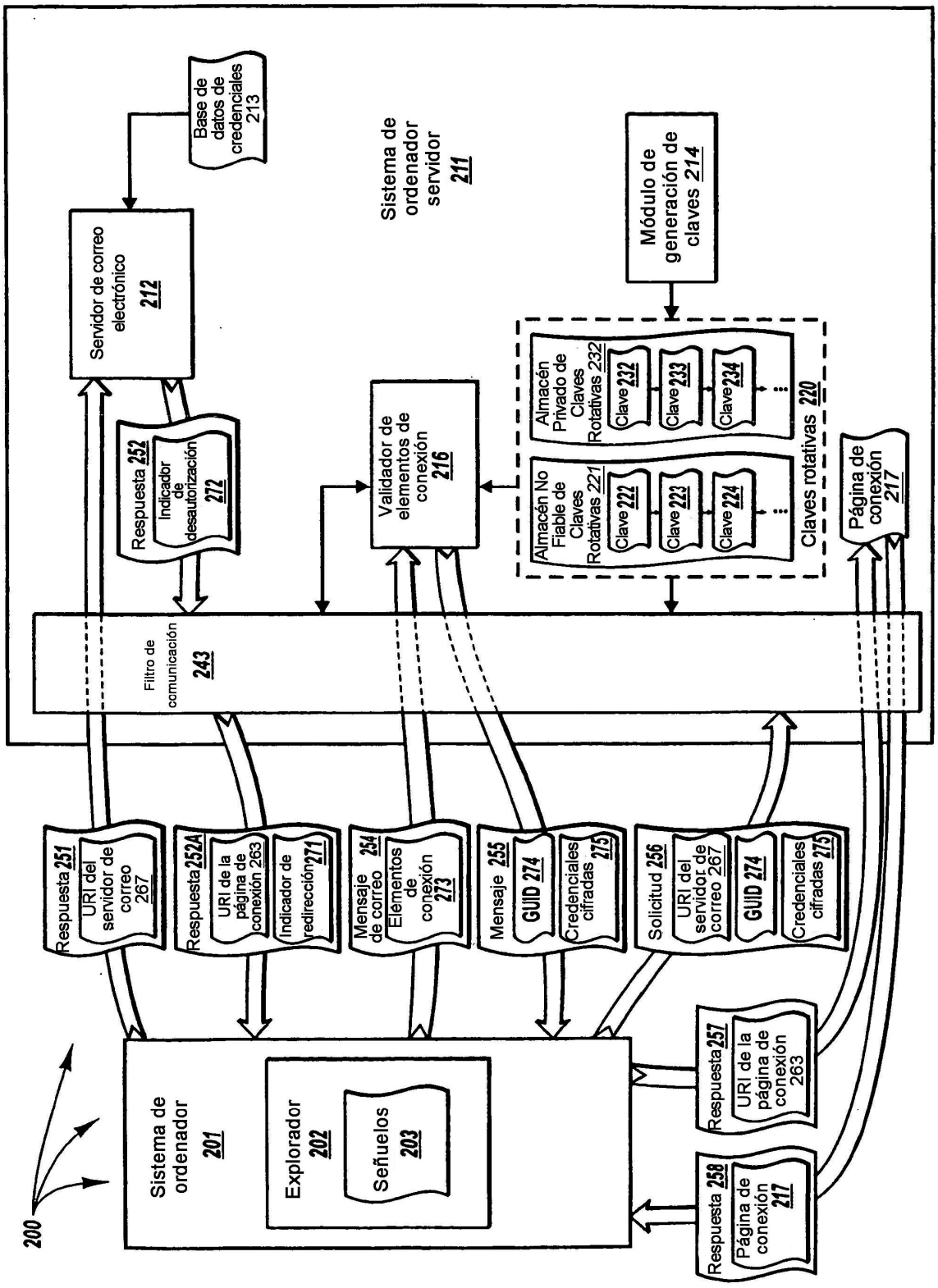

Sistema de ordenador servidor 211
Base de datos de credenciales 213
Servidor de correo electrónico 212
Módulo de generación de claves 214
Respuesta 252
Indicador de desautorización 272
Validador de elementos de conexión 216
Almacén Privado de Claves Rotativas 232
Clave 232
Clave 233
Clave 234
Almacén No Fiable de Claves Rotativas 221
Clave 222
Clave 223
Clave 224
Claves rotativas 220
Página de conexión 217
Filtro de comunicación 243
Respuesta 251
URI del servidor de correo 267
Respuesta 252A
URI de la página de conexión 263
Indicador de redirección 271
Mensaje de correo
Elementos de conexión 273
Mensaje 255
GUID 274
Credenciales cifradas 275
Solicitud 256
URI del servidor de correo 267
GUID 274
Credenciales cifradas 275
Sistema de ordenador 201
Explorador 202
Señuelos 203
Respuesta 257
URI de la página de conexión 263
Respuesta 258
Página de conexión 217
200

Fig. 2A

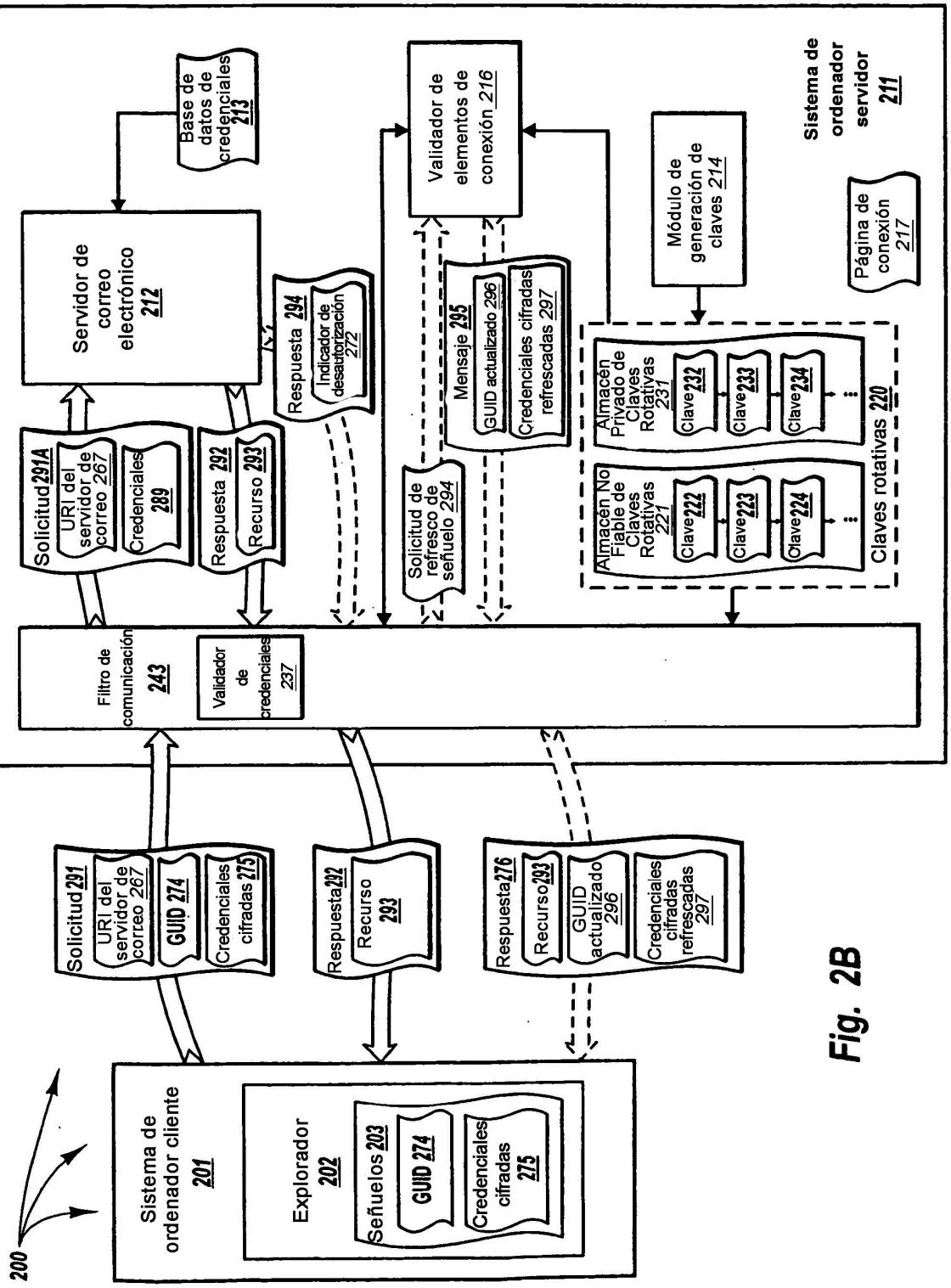

200
Sistema de ordenador cliente 201
Explorador 202
Señuelos 203
GUID 274
Credenciales cifradas 275
Solicitud 291
URI del servidor de correo 267
GUID 274
Credenciales cifradas 275
Respuesta 292
Recurso 293
Respuesta 276
Recurso 293
GUID actualizado 296
Credenciales cifradas refrescadas 297
Filtro de comunicación 243
Validador de credenciales 237
Solicitud 291A
URI del servidor de correo 267
Credenciales 289
Respuesta 292
Recurso 293
Respuesta 294
Indicador de desautorización 272
Solicitud de refresco de señuelo 294
Mensaje 295
GUID actualizado 296
Credenciales cifradas refrescadas 297
Servidor de correo electrónico 212
Base de datos de credenciales 213
Validador de elementos de conexión 216
Módulo de generación de claves 214
Sistema de ordenador servidor 211
Página de conexión 217
Claves rotativas 220
Almacén Privado de Claves Rotativas 231
Clave 232
Clave 233
Clave 234
Almacén No Fiable de Claves Rotativas 221
Clave 222
Clave 223
Clave 224

Fig. 2B

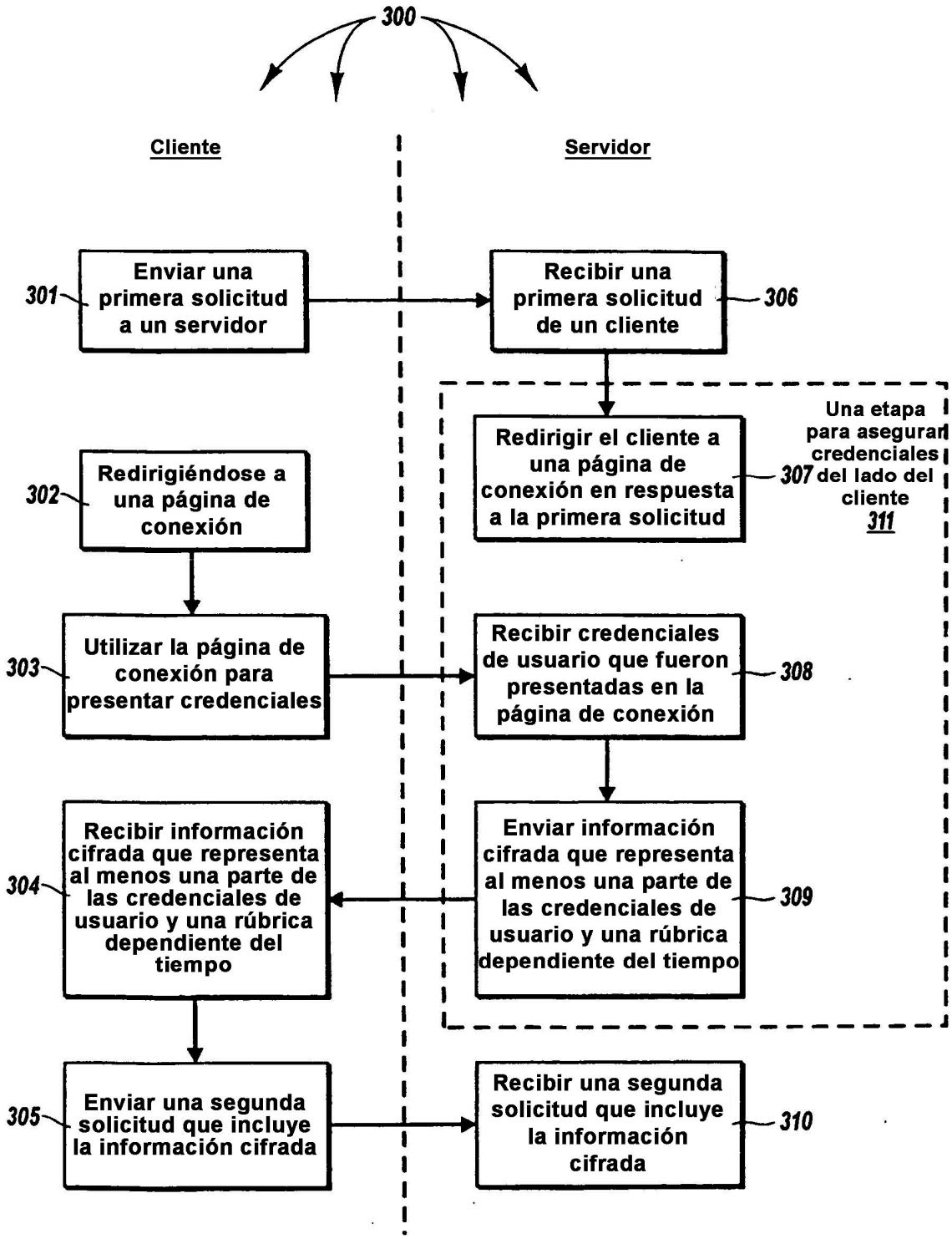

300
Cliente
Servidor
Enviar una primera solicitud a un servidor
301
Recibir una primera solicitud de un cliente
306
Redirigir el cliente a una página de conexión en respuesta a la primera solicitud
307
Una etapa para asegurar credenciales del lado del cliente
311
Redirigiéndose a una página de conexión
302
Utilizar la página de conexión para presentar credenciales
303
Recibir credenciales de usuario que fueron presentadas en la página de conexión
308
Enviar información cifrada que representa al menos una parte de las credenciales de usuario y una rúbrica dependiente del tiempo
309
Recibir información cifrada que representa al menos una parte de las credenciales de usuario y una rúbrica dependiente del tiempo
304
Enviar una segunda solicitud que incluye la información cifrada
305
Recibir una segunda solicitud que incluye la información cifrada
310

Fig. 3

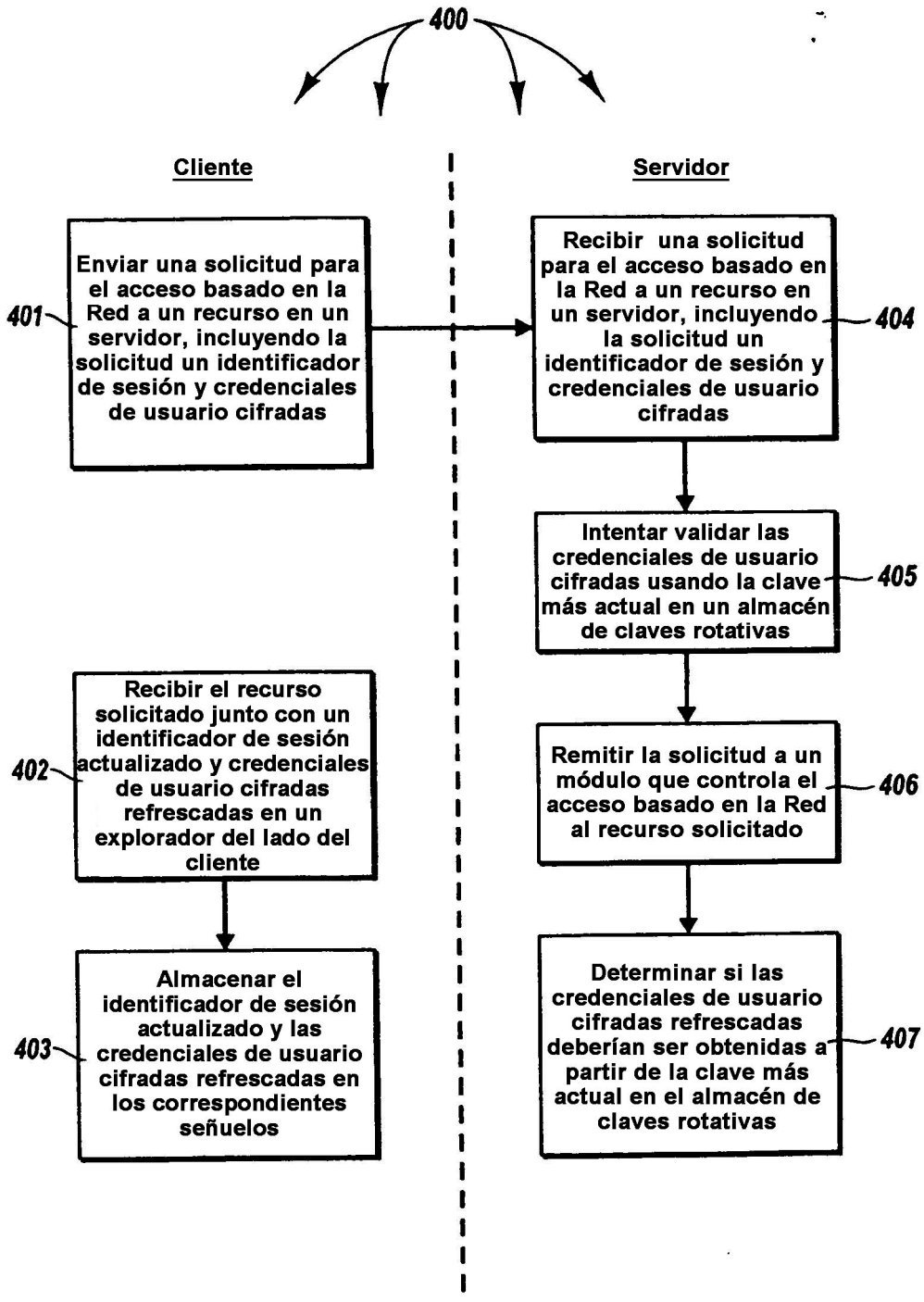

400
Cliente
Servidor
Enviar una solicitud para el acceso basado en la Red a un recurso en un servidor, incluyendo la solicitud un identificador de sesión y credenciales de usuario cifradas
401
Recibir una solicitud para el acceso basado en la Red a un recurso en un servidor, incluyendo la solicitud un identificador de sesión y credenciales de usuario cifradas
404
Intentar validar las credenciales de usuario cifradas usando la clave más actual en un almacén de claves rotativas
405
Recibir el recurso solicitado junto con un identificador de sesión actualizado y credenciales de usuario cifradas refrescadas en un explorador del lado del cliente
402
Remitir la solicitud a un módulo que controla el acceso basado en la Red al recurso solicitado
406
Almacenar el identificador de sesión actualizado y las credenciales de usuario cifradas refrescadas en los correspondientes señuelos
403
Determinar si las credenciales de usuario cifradas refrescadas deberían ser obtenidas a partir de la clave más actual en el almacén de claves rotativas
407

Fig. 4

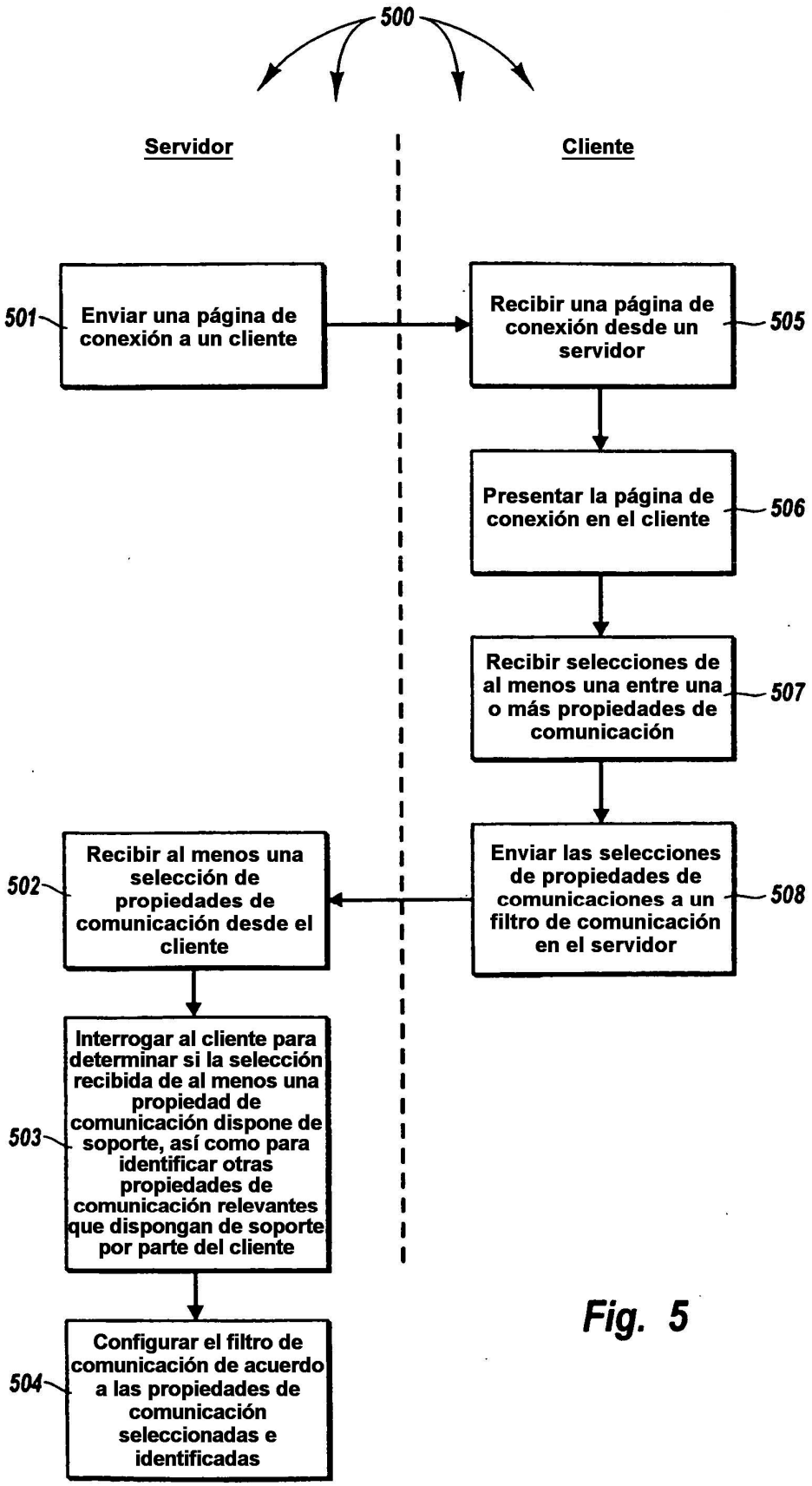

500
Servidor
Cliente
501
Enviar una página de conexión a un cliente
Recibir una página de conexión desde un servidor
505
Presentar la página de conexión en el cliente
506
Recibir selecciones de al menos una entre una o más propiedades de comunicación
507
Enviar las selecciones de propiedades de comunicaciones a un filtro de comunicación en el servidor
508
502
Recibir al menos una selección de propiedades de comunicación desde el cliente
503
Interrogar al cliente para determinar si la selección recibida de al menos una propiedad de comunicación dispone de soporte, así como para identificar otras propiedades de comunicación relevantes que dispongan de soporte por parte del cliente
504
Configurar el filtro de comunicación de acuerdo a las propiedades de comunicación seleccionadas e identificadas

Fig. 5

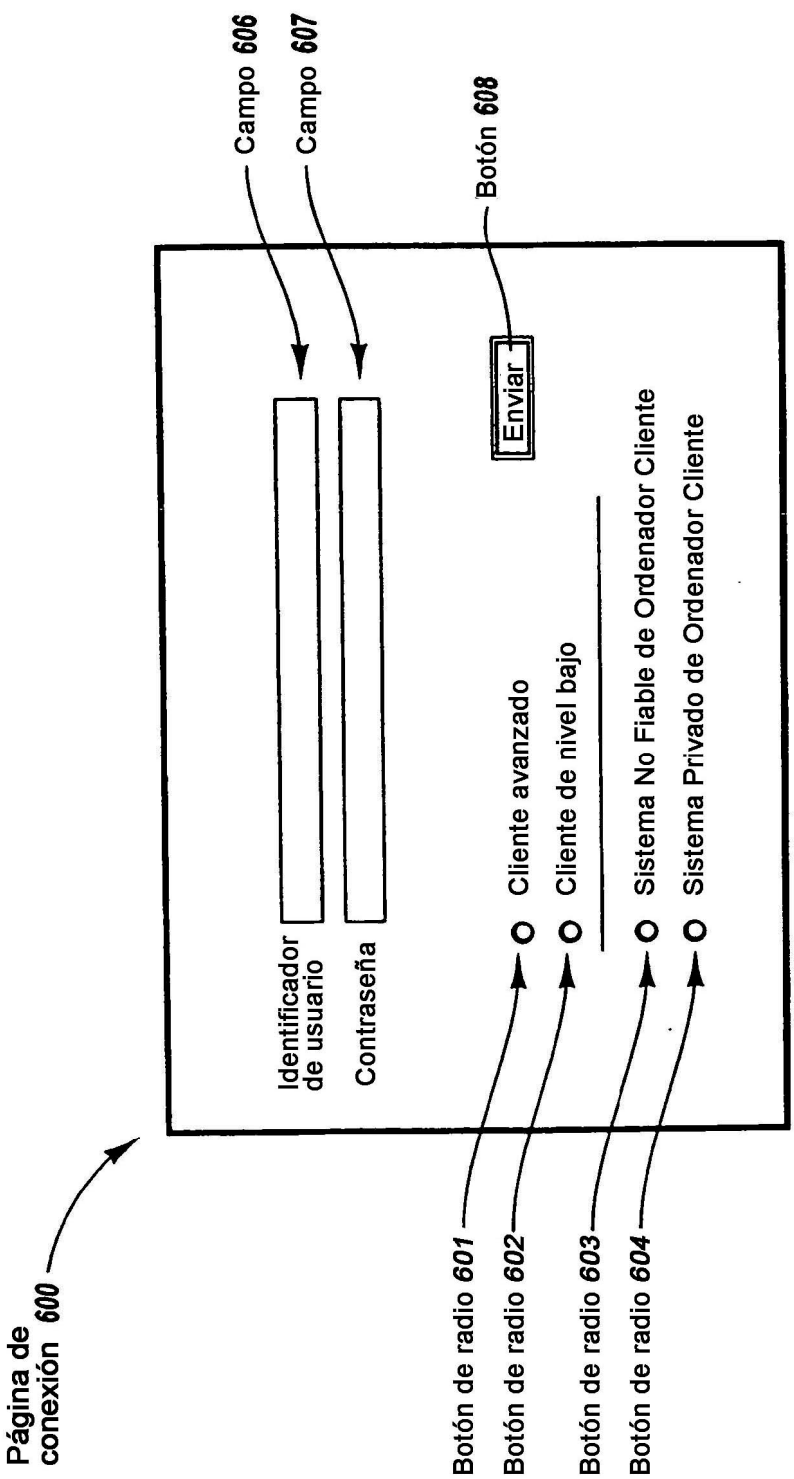

Página de conexión 600
Campo 606
Campo 607
Botón 608
Identificador de usuario
Contraseña
Enviar
Cliente avanzado
Cliente de nivel bajo
Sistema No Fiable de Ordenador Cliente
Sistema Privado de Ordenador Cliente
Botón de radio 601
Botón de radio 602
Botón de radio 603
Botón de radio 604

Fig. 6