(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 614 164**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.09.2010 PCT/US2010/049611**

(87) Fecha y número de publicación internacional: **24.03.2011 WO11035287**

(96) Fecha de presentación y número de la solicitud europea: **21.09.2010 E 10818010 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.11.2016 EP 2481185**

(54) Título: **Objeto de relé de túnel de control de acceso de identidad múltiple**

(30) Prioridad:

21.09.2009 US 244148 P
20.09.2010 US 886184

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.05.2017

(73) Titular/es:

RAM INTERNATIONAL CORPORATION (100.0%)
5465 Desert Point Drive
Las Vegas, NV 89118, US

(72) Inventor/es:

JOHNSTON, RICHARD, FENDALL;
PIERCE, DEAN, EDWARD y
STRAUSS, WILLIAM, JONATHAN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Objeto de relé de túnel de control de acceso de identidad múltiple

Campo

Las presentes enseñanzas se refieren a comunicaciones seguras en Internet.

Antecedentes

Las afirmaciones en esta sección proporcionan simplemente información de contexto relacionada con la presente divulgación y no pueden constituir la técnica anterior. Normalmente, los sistemas de control de acceso basado en roles actuales (RBAC) utilizan mecanismos de tunelización basados en capa de puertos seguros (SSL) para autentificar una única identidad. Generalmente, esta identidad se autoriza para llevar a cabo un cierto conjunto de acciones sobre un sistema definido para el cual se asocian los roles a esa identidad. Tal tunelización SSL y autentificación de identidad única ofrece solo una única capa de cifrado y es inadecuada para ciertas tareas y/o conjuntos de acciones en las que es importante un nivel superior de seguridad.

Diversos documentos de la técnica anterior, tal como el documento US 2002/0199007 y US 2007/0300057 describen la configuración y el proceso de autentificación para la comunicación segura sobre una red. Estos dos documentos se centran en reubicar lo que antes era un software cliente sobre un servidor, que evita la necesidad de una instalación personalizada en un dispositivo cliente. En el documento US 2002/0199007 el software cliente se distribuye a los usuarios, según sea necesario, cuando acceden a una red privada virtual y/o hacen uso de la comunicación de datos de proxy. El documento US 2007/0300057 está relacionado con la autorización basada en servidor de usuarios de una aplicación basada en la web a través de un dispositivo o autentificador de confianza de cliente.

El documento EP 1.349.032 y el documento US 2009/0193514 describen mejoras en los métodos de autentificación de usuario. El documento 1.349.032 emplea un par de claves de autentificación, que se adhieren a una tarjeta inteligente y a un lector en el establecimiento de un canal de comunicación seguro sobre una red. El documento US 2009/0193514 describe la permisión de acceso a un dispositivo informático, particularmente un dispositivo móvil, mediante la selección de una pluralidad de autentificadores desde su memoria.

Sumario

Generalmente, la presente divulgación proporciona un sistema y un método para establecer un túnel seguro entre un dispositivo cliente y un servidor remoto que utiliza múltiples identidades de usuario, y en algunas realizaciones, una identidad de dispositivo de cliente, para autentificar el acceso al servidor.

Más específicamente, la presente invención proporciona un método para establecer un túnel seguro entre un dispositivo cliente y un servidor remoto que utiliza múltiples identidades para autentificar el acceso al servidor remoto, comprendiendo dicho método:

ejecutar un programa de relé en un servidor remoto y descargar un programa conector desde el servidor remoto hasta el dispositivo cliente al ejecutar el programa de relé;
escanear el dispositivo cliente para uno o más dispositivos de autenticación que al menos uno se conecta de manera que se puede retirar a y se fija integrado al dispositivo cliente, mediante la ejecución del programa conector, habiendo almacenado cada dispositivo de autenticación en él una o más identidades;
seleccionar múltiples identidades desde las identidades almacenadas en el uno o más dispositivos de autenticación, pasar las identidades seleccionadas al servidor remoto, y validar las identidades pasadas, mediante una autenticación de pregunta-respuesta llevada a cabo por el programa de relé;
establecer un canal de comunicaciones de alto nivel de seguridad y gestionar una sesión de proxy cifrada entre un proxy del lado del servidor remoto, corroborada mediante la ejecución del relé, y un proxy del lado del cliente, corroborado mediante la ejecución del programa conector, y
proporcionar acceso por el dispositivo cliente a un primer objeto contenido en el servidor mediante una sesión de proxy cifrada sobre el canal de comunicaciones de alto nivel de seguridad.

Se harán evidentes las áreas de aplicabilidad adicionales de las presentes enseñanzas a partir de la descripción proporcionada en el presente documento. Debería entenderse que la descripción y los ejemplos específicos sirven para fines de ilustración solo y no se dirigen a limitar el ámbito de las presentes enseñanzas.

Dibujos

Los dibujos descritos en el presente documento son para fines ilustrativos solo y no se dirigen a limitar el ámbito de las presentes enseñanzas de ninguna manera,

La figura 1 es un diagrama de bloques de un sistema a modo de ejemplo para establecer un túnel seguro entre un dispositivo cliente y un servidor remoto utilizando múltiples identidades de usuario, de acuerdo con diversas realizaciones de la presente divulgación.

La figura 2 es un diagrama de bloques que ilustra diversos componentes del dispositivo cliente y del servidor remoto mostrado en la figura 1, de acuerdo con diversas realizaciones de la presente divulgación.

La figura 3 es un diagrama de flujo a modo de ejemplo de un método, implementable mediante el sistema mostrado en la figura 1, para establecer un túnel seguro entre un dispositivo cliente y el servidor remoto utilizando múltiples identidades de usuario, de acuerdo con diversas realizaciones de la presente divulgación.

Las referencias numéricas correspondientes indican las partes correspondientes a lo largo de varias vistas de los dibujos.

Descripción detallada

La siguiente descripción es meramente a modo de ejemplo en naturaleza y de ninguna manera se dirige a limitar las presentes enseñanzas, aplicación, o usos. A lo largo de esta memoria descriptiva, se usarán referencias numéricas similares para referirse a elementos similares.

La figura 1 es un diagrama de bloques de un sistema o red 10 informático a modo de ejemplo, tal como una Red de Área Local (LAN) o Red de Área Extendida (WAN), para establecer un túnel seguro entre al menos un dispositivo cliente 14 y un servidor remoto 18 utilizando múltiples identidades de usuario, y en algunas realizaciones, una identidad de dispositivo cliente, para autenticar el acceso al servidor 18. En diversas realizaciones, el sistema puede incluir al menos un dispositivo cliente 14 que se estructura para estar conectable operativamente con el servidor remoto 18, a través de un router 22 de comunicación, por ejemplo, Internet, para comunicar datos entre el dispositivo cliente 14 y el servidor 18.

Aunque el sistema 10 puede incluir una pluralidad de dispositivos clientes 14 operativamente conectables al servidor 18, para simplicidad y claridad, el sistema 10 se describirá en el presente documento con referencia a un único dispositivo cliente 14. Sin embargo, debería entenderse que las disposiciones de la presente divulgación son igualmente aplicables a las realizaciones que incluyen una pluralidad de dispositivos cliente 14, configurado cada uno para operar sustancialmente igual que el dispositivo cliente 14 descrito a continuación, y tales realizaciones permanecen dentro del ámbito de la presente divulgación.

Como se describe adicionalmente a continuación, el sistema 10 es operable de tal manera que el dispositivo cliente 14 y el servidor remoto 18 se comunican entre sí a través de un primer canal de comunicaciones inseguro 26 y un segundo canal de comunicaciones de bajo nivel de seguridad 30 para establecer un tercer canal de comunicaciones de alto nivel de seguridad 34 sobre el cual pueden pasar los datos cifrados.

En referencia ahora a la figura 2, en diversas implementaciones, el dispositivo cliente 14 puede ser un ordenador que incluye un procesador 38 adecuado para ejecutar todas las funciones y programas del dispositivo cliente 14. El dispositivo cliente 14 adicionalmente puede incluir al menos un dispositivo de almacenamiento 42 electrónico que comprende un medio legible informático, tal como un disco duro o cualquier otro dispositivo de almacenamiento de datos electrónico para almacenar tales cosas como paquetes o programas de software, algoritmos e información digital, datos, tablas de búsqueda, hojas de cálculo y bases de datos electrónicas, etc. El dispositivo cliente 14 puede incluir además una pantalla 46 para mostrar tales cosas como información, datos y/o representaciones gráficas, y una pluralidad de dispositivos 50 de interfaz de usuario, por ejemplo, un primer dispositivo de interfaz de usuario y un segundo dispositivo de interfaz de usuario. Cada dispositivo de interfaz de usuario 50 puede ser cualquier dispositivo de interfaz de usuario adecuado tal como un teclado, ratón, bolígrafo, micrófono, escáner y/o una pantalla táctil en la pantalla, y el dispositivo cliente 14 puede incluir cualquier combinación de dos o más de los dispositivos de interfaz de usuario 50.

En diversas realizaciones, el dispositivo cliente 14 puede aún incluir adicionalmente un lector de medios 54 retirable desde el que leer la información y los datos, y/o en el que escribir información y datos, medios de almacenamiento electrónico retirables tales como disquetes, discos compactos, discos DVD, discos zip, o cualquier otro medio de almacenamiento electrónico portátil y retirable legible por un ordenador. Alternativamente, el lector de medios retirable puede ser un puerto I/O utilizado para comunicarse con dispositivos de memoria externa o periférica tales como dispositivos de memoria, pinchos/tarjetas de memoria o discos duros externos. Aun adicionalmente, el dispositivo cliente 14 puede incluir un dispositivo de interfaz de router 58, tal como un módem de marcación, un módem por cable, una comunicación por satélite, una conexión DSL (Digital Subscriber Line), un puerto Ethernet, o similares.

Las realizaciones alternativas del dispositivo cliente 14 pueden incluir cualquier dispositivo eléctrico o electrónico capaz de comunicarse con el servidor remoto 18 a través del router de comunicaciones 22, tal como un asistente digital personal (PDA), teléfono móvil, un teléfono que opera con un sistema de voz interactivo, o una televisión que opera con un cable o un sistema interactivo de televisión por satélite.

De manera similar, en diversas realizaciones, el servidor remoto 18 puede ser un ordenador que incluye un procesador 40 adecuado para ejecutar todas las funciones y programas del servidor remoto 18. El servidor remoto 18 puede incluir adicionalmente al menos un dispositivo de almacenamiento 44, por ejemplo, un dispositivo de almacenamiento masivo, que comprende un medio legible por ordenador, tal como un disco duro o cualquier otro dispositivo de almacenamiento de datos electrónico para almacenar tales cosas como paquetes o programas de software, algoritmos e información digital, datos, tablas de búsqueda, hojas de cálculo electrónicas y, particularmente al menos una base de datos 48. Asimismo, en diversas realizaciones, el servidor remoto 18 aún incluye adicionalmente un dispositivo 60 de interfaz de router, tal como un módem por cable, una conexión por satélite, una conexión DSL (Digital Suscriber Line), un puerto Ethernet, o similares.

Aunque, como se describió anteriormente, en diversas realizaciones, el sistema 10 puede ser una red informática, tal como una LAN o una WAN, para simplicidad y claridad, el sistema se describirá a continuación con respecto a diversas realizaciones WAN. Sin embargo, debe entenderse que las disposiciones de la presente divulgación se aplican igualmente a cualquier otra red informática donde se desea la comunicación segura entre el dispositivo cliente 14 y el servidor 18, y que tales realizaciones permanecen dentro del ámbito de la presente divulgación.

En diversas realizaciones, el procesador 38 del dispositivo cliente es capaz de ejecutar un programa de interfaz de router 62, tal como un programa de navegador web y en adelante referido alternativamente como el navegador web, para comunicarse con el servidor 18, un servidor web a modo de ejemplo y alternativamente denominado en el presente documento como el servidor web 18, a través del router 22 de comunicaciones, Internet a modo de ejemplo y alternativamente denominado en el presente documento como Internet 22. Generalmente, en tales realizaciones, un usuario puede interactuar con el dispositivo cliente 14 viendo datos, a través de la pantalla 46, e introducir datos, a través de los dispositivos de interfaz de usuario 50. El navegador web 62 permite al usuario introducir direcciones, a las que se hace referencia como Localizadores de Recursos Uniformes, o URLs, u objetos contenidos de servidor web específicos para recuperar o acceder, por ejemplo, a una página web o base de datos remota. Los objetos contenidos de servidor web pueden contener diversos tipos de contenido desde información en texto sin formato hasta contenido multimedia e interactivo más complejo, tal como programas software, gráficos, señales de audio, vídeos, y demás.

En tales realizaciones, en las que el objeto contenido en el servidor comprende una página web, una configuración de páginas web interconectadas, que incluye normalmente una página de inicio, que se gestiona sobre el servidor web 18 como una recopilación se denomina de manera colectiva como la página web. El contenido y la operación de tales páginas web se gestionan mediante el servidor web 18. Más particularmente, como se describe a continuación, el servidor web 18 ejecuta e implementa un programa de relé 66 para establecer el tercer canal de comunicaciones de alto nivel de seguridad 34 entre el dispositivo cliente 14 y el servidor web 18, proporcionando así comunicaciones seguras entre el dispositivo cliente 14 y el servidor web 18.

El primer canal de comunicaciones inseguro 26 puede implementar cualquier protocolo de comunicaciones, tal como el Protocolo de Transferencia de Hipertexto (HTTP) para comunicar datos entre el dispositivo cliente 14 y el servidor web 18. Adicionalmente, como se describió anteriormente, el router 22 de comunicaciones puede ser cualquier red de intercambio de datos que implementa un protocolo de comunicaciones adecuado respectivo, tal como FTP (Protocolo de Transferencia de Archivo), TELNET (Red de Teletipo), y similares para comunicar sobre el generalmente primer canal de comunicaciones 26.

En referencia ahora a las figuras 1, 2 y 3, la operación del sistema 10 para establecer un túnel seguro entre el dispositivo cliente 14 y el servidor remoto 18 utilizando múltiples identidades se describirá ahora, de acuerdo con diversas realizaciones. Inicialmente, un usuario ejecutará el programa 62 de interfaz de router en el dispositivo cliente 14, por ejemplo, un programa de navegador web, mediante uno o más de los dispositivos de interfaz de usuario 50. A continuación, usando uno o más de los dispositivos de interfaz de usuario 50, el usuario establecerá el primer canal de comunicaciones generalmente inseguro 26 con el servidor remoto 18. Por ejemplo, el usuario introducirá la URL del servidor 18 en la línea de dirección de un navegador web 62. En respuesta, el servidor 18 inicia la ejecución del programa de relé 66 y vuelve a la página de inicio de la página web anfitriona dirigida por la URL, en la que la página de inicio incluye un "Botón de Inicio de Sesión". El usuario seguidamente selecciona el "Botón de Inicio de Sesión" en el punto en el que la página web anfitriona puede o no solicitar al usuario introducir la información de inicio de sesión tal como un nombre de usuario y una contraseña, como se indicó en 104 del diagrama de flujo 100 ilustrado en la figura 3. Posteriormente, el programa de relé 66 descargará un programa conector 70, por ejemplo, mediante JAVA Webstart, en el dispositivo cliente 14 e indicará al dispositivo cliente 14 que ejecute el programa conector 70, como se indicó en 108.

Al ejecutar el programa conector 70, el segundo canal de comunicaciones de bajo nivel de seguridad 30, es decir, un canal SSL, se establece entre el programa conector 70 del lado del cliente y el programa de relé 66 del lado del servidor.

Posteriormente, la ejecución del programa conector 70 proporciona una interfaz de usuario gráfica (GUI) sobre la pantalla 46 del dispositivo cliente y escanea el dispositivo cliente en busca de dispositivos de autentificación 74 conectados o integrados, como se indicó en 112 y 114. En diversas realizaciones, los dispositivos de autentificación

74 pueden incluir cualquier dispositivo de almacenamiento que se pueda conectar a un puerto I/O de datos, por ejemplo, un puerto USB, un puerto en serie, etc., o leer mediante un lector de medios de dispositivo de cliente, o conectarse a la placa base del dispositivo cliente 14. Por ejemplo, los dispositivos de autentificación 74 pueden incluir, dispositivos de memoria, pinchos/tarjetas de memoria, discos duros externos, disquetes, discos compactos, discos DVD, discos zip, teléfonos móviles, cualquier otro medio de almacenamiento electrónico portátil, o módulos de plataforma de confiable (TPM) conectados sobre la placa base del dispositivo cliente, o un dispositivo de entrada de datos periférico, tal como un lector de huellas dactilares. Se puede conectar uno o más dispositivos de autentificación 74 a uno o más puertos I/O del dispositivo cliente y/o integrar la placa base del dispositivo cliente.

Cada dispositivo de autentificación 74 tiene almacenado en sí mismo una o más identidades de usuario, o en diversas realizaciones, datos de identidad de lectura y entrada tales como huellas dactilares. Las identidades de usuario proporcionan tales cosas como credenciales, derechos o niveles de autentificación de usuario, y comprenden tales cosas como secuencias de autentificación alfanuméricas o numéricas, o certificados de seguridad. Generalmente, como se describe a continuación, se usan diversas combinaciones de identidades almacenadas en los dispositivos de autentificación 74 para identificar y autentificar el dispositivo cliente 14 y/o determinar a qué tipo de privilegios del usuario del dispositivo cliente 14 se deberían permitir acceder en el objeto contenido en el servidor, por ejemplo, una página web ejecutándose en un servidor 18.

Se presenta entonces una lista de dispositivos de autentificación 74 disponibles que se encuentran presentes y una lista de diversas identidades almacenadas en la misma o la entrada de datos correspondiente necesaria, por ejemplo, datos de huella dactilar, dentro de la interfaz de usuario gráfica en la pantalla 46 del dispositivo cliente, como se indicó en 120 y 124. En diversas realizaciones, puede que se requiera adicionalmente un nombre de usuario y una contraseña para acceder a la lista de identidades en uno o más dispositivos de autentificación 74 presentes.

Como se describe a continuación, en diversas realizaciones, uno de los dispositivos de autentificación puede comprender un módulo de plataforma confiable (TPM) dispuesto dentro del dispositivo cliente 14, en el que el sistema y los métodos descritos en el presente documento pueden aprovechar el TPM en el dispositivo cliente 14 de tal manera que no solo se puede identificar al usuario mediante diversos dispositivos de autentificación 14, sino también de tal manera que el dispositivo cliente 14 puede identificarse y autentificarse. Así, el dispositivo cliente 14 puede ser un sistema informático en cuarentena que se autentifica particularmente para su uso para acceder al objeto contenido en el servidor solicitado, por ejemplo, una página web. Por lo tanto, en diversas realizaciones, la identificación y la autentificación del dispositivo cliente 14 pueden requerirse en combinación con una o más de las identidades del usuario para acceder al objeto contenido en el servidor solicitado.

Seguidamente, basándose en el objeto contenido en el servidor solicitado, el usuario selecciona una o más identidades desde las que aparecen en la lista que son necesarias para obtener acceso al objeto contenido en el servidor solicitado, como se indicó en 128. Las identidades seleccionadas pasan seguidamente al servidor 18, a través del segundo canal de comunicaciones de bajo nivel de seguridad 30, donde se interpretan y se verifican, es decir, se validan, por el programa de relé 66, a través de una autentificación de pregunta-respuesta, como se indicó en 132.

Al validar las identidades seleccionadas, el programa de relé 66 gestiona entonces una sesión de proxy cifrada entre el servidor 18 y el dispositivo cliente 14, como se indicó en 136. Particularmente, el programa de relé 66 corrobora un proxy 78 del lado del servidor y se comunica con el programa conector 70 del dispositivo cliente, a través del segundo canal de comunicación 30, por el que el programa conector 70 corrobora un proxy 82 del lado del cliente. Una vez que se ha establecido el proxy 82 del lado del cliente, el programa de relé 66 establece el tercer canal de comunicaciones de alto nivel de seguridad 34 y la sesión de proxy cifrada entre el proxy 82 del lado del cliente y el proxy 78 del lado del servidor a través del tercer canal de comunicaciones de alto nivel de seguridad 34.

Por lo tanto, se puede aplicar una configuración de reglas de control de acceso en múltiples niveles a cualquier objeto contenido en el servidor basado en varias configuraciones de identidades por dispositivo de autentificación 74. Las identidades dentro de cada dispositivo de autentificación 74 no solo determinan el usuario que será un usuario autorizado, sino que puede también identificar el dispositivo cliente 14 actual que se está usando para un acceso autorizado de mayor seguridad. Identificando el dispositivo cliente 14 que se está utilizando para acceder con autorización a un estado de cuarentena se puede implementar desde el lado del servidor, asegurando adicionalmente la seguridad de la sesión de proxy cifrada establecida en última instancia.

Una vez que la sesión de proxy cifrada sobre el tercer canal 34 de comunicaciones se establece, la interfaz 58 del router del dispositivo cliente, por ejemplo, un navegador web, se conecta a un cargador de cookies del programa conector 70 y almacena un identificador de sesión para la sesión de proxy cifrada en memoria de acceso aleatorio del dispositivo cliente 14, como se indicó en 140. El cargador de cookies adicionalmente redirige la interfaz 62 del router cliente a través del proxy 82 del lado del cliente de tal manera que todo el contenido protegido pasa entre el servidor 18 y el dispositivo cliente 14 a través de la sesión de proxy cifrada sobre el tercer canal 34 de comunicaciones, como se indicó en 144 y 148.

En diversas realizaciones, el objeto contenido en el servidor puede incluir un programa de seguimiento que se ejecuta una vez que se establece la sesión de proxy cifrada sobre el tercer canal 34 de comunicaciones como se describió anteriormente, como se indicó en 152. El programa de seguimiento rastrea y mantiene la validez de la sesión de proxy cifrada.

Además, la sesión de proxy cifrada puede finalizar de diversas maneras desde tanto el lado del cliente o del lado del servidor, como se indicó en 156. Por ejemplo, la sesión de proxy cifrada se puede finalizar por el usuario al cerrar sesión o al cerrar el programa 62 de interfaz del router cliente. O, la sesión de proxy cifrada puede destruirse por el programa 62 del router del lado del cliente, informando al programa conector 70 de comportamiento malicioso o el objeto contenido del servidor del lado del servidor informando al relé 66 de comportamiento malicioso. Por ejemplo, la sesión se puede destruir después de que transcurra un tiempo de espera predeterminado, o si el usuario intenta acceder a la información o a un objeto contenido en el servidor para el cuál el usuario no tiene las identidades adecuadas. Al finalizar la sesión de proxy cifrada, de cualquier manera, el tercer canal de comunicaciones de alto nivel de seguridad 34 se destruye.

Alternativamente, la sesión de proxy cifrada puede finalizarse y el tercer canal de comunicaciones de alto nivel de seguridad 34 destruirse eliminando el(los) dispositivo(s) de autentificación 74 desde el dispositivo cliente 14.

En diversas realizaciones, una vez que el usuario ha establecido una sesión de proxy cifrada y el tercer canal de comunicaciones de alto nivel de seguridad 34, y obtenido acceso a un objeto contenido en el servidor primario, el usuario puede desear acceder a un objeto contenido en el servidor secundario o a información particular dentro del objeto accedido actualmente. En tales casos, pueden requerirse identidades adicionales. Tales identidades adicionales pueden requerirse desde los usuarios originales seleccionando identidades adicionales desde los dispositivos de autentificación 74 ya ubicadas por el programa conector 70, en cuyo caso el usuario podría simplemente seleccionar la identidad o identidades adicionales desde la lista mostrada previamente.

O, en otras realizaciones, las identidades adicionales pueden almacenarse en un dispositivo de autentificación 74 secundario, es decir, un segundo, un tercero, un cuarto, etc., dispositivo de autentificación 74. En tales casos, el acceso al objeto contenido en el servidor secundario o información solicitada puede requerir que el dispositivo de autentificación 74 secundario esté conectado al dispositivo cliente 14, en cuyo punto, el programa conector 70 podría ubicar el dispositivo de autentificación 74 secundario y la lista de identidades almacenadas en el mismo. El usuario podría entonces seleccionar las identidades necesarias desde la lista secundaria de identidades para obtener acceso al objeto contenido en el servidor o información secundaria.

En diversas otras realizaciones, puede añadirse un nivel adicional de seguridad imponiendo una "Regla en Pareja" para obtener acceso al objeto contenido en el servidor primario, o a un objeto contenido en el servidor o información secundaria. En tales realizaciones, el dispositivo de autentificación 74 secundario y las correspondientes identidades requeridas pueden ser accesibles solo por un segundo usuario, es decir, alguien diferente al primer usuario que originalmente inició la sesión de proxy cifrada como se describió anteriormente. Tales realizaciones requerirían que el segundo usuario esté presente para conectar el(los) dispositivo(s) de autentificación 74 secundario(s) al dispositivo cliente 14, además de cualquier dispositivo de autentificación 74 conectado actualmente proporcionado por el primer usuario, e introducir un nombre de usuario y/o una contraseña solo conocida por el segundo usuario para obtener acceso a una lista de las identidades almacenadas en el(los) dispositivo(s) de autentificación 74 secundario(s). Una o más identidades desde el(los) segundo(s) dispositivo(s) secundario(s) del usuario 74 podría entonces seleccionarse y autentificarse mediante el programa de relé 66 del lado del servidor para obtener acceso al objeto contenido en el servidor o información solicitada.

Por ejemplo, si un primer usuario ha proporcionado las identidades apropiadas para establecer la sesión de proxy cifrada y el correspondiente tercer canal de comunicaciones de alto nivel de seguridad 34, y obtenido acceso al objeto contenido en el servidor solicitado, por ejemplo, una cuenta bancaria conjunta. El primer usuario debe tener acceso solo a ciertos privilegios dentro de una tal cuenta bancaria. Por ejemplo, el primer usuario puede estar limitado en la cantidad de dinero que puede transferir desde la cuenta. Transferir dinero en una cantidad superior a este límite puede requerir la implementación de una "Regla en Pareja". En tales casos, se podría requerir a un segundo usuario proporcionar uno o más dispositivos de autentificación 74 secundarios y las identidades necesarias correspondientes, como se describió en el presente documento, con el fin de transferir la mayor suma de dinero.

Alternativamente, en diversas otras realizaciones, la "Regla en Pareja" puede requerir que el segundo usuario use un segundo dispositivo cliente 14 para establecer una segunda sesión de proxy cifrada y el correspondiente segundo tercer canal de comunicaciones de alto nivel de seguridad 34 entre el servidor 18 y el segundo dispositivo cliente 14, de la misma manera que la sesión de proxy cifrada primaria y el correspondiente tercer canal de comunicaciones de alto nivel de seguridad 34 descritos anteriormente. En tales realizaciones, se puede requerir que el segundo usuario proporcione el(los) dispositivo(s) de autentificación 74 secundario(s) adecuado(s) y las identidades con el fin de que el primer usuario (y el segundo usuario) accedan al objeto contenido en el servidor o información solicitada.

Adicionalmente, en diversas realizaciones, la "Regla en Pareja" puede implementarse de tal manera que se requiera que un tercer, cuarto, quinto, etc., usuario proporcione el correspondiente tercer, cuarto, quinto, etc., dispositivo de

autentificación 74 y las identidades para acceder al objeto contenido en el servidor o información solicitada, de la misma manera en la que se describió anteriormente con respecto a un segundo usuario y a el(los) dispositivo(s) de autentificación 74 secundario(s).

De manera similar, una vez que el acceso al objeto contenido en el servidor o información se ha establecido, como se describió anteriormente, el acceso a otro objeto contenido en el servidor y otra información puede no requerir los múltiples dispositivos de autentificación y/o las múltiples identidades. En tal caso, los dispositivos de autentificación 74 no necesarios y/o las múltiples identidades se pueden eliminar o finalizar.

En diversas otras realizaciones, el programa de relé 66 puede instalarse sobre una pluralidad de servidores remotos 18 con el fin de ofrecer acceso a la pluralidad de diferentes servidores 18. En tales realizaciones, un servidor 18 y el correspondiente programa de relé 66 actuarían como un "servidor concentrador" y un programa de relé 66 con los que los otros servidores 18 y los programas de relé 66 se comunican de vuelta. El "servidor concentrador" y el correspondiente programa de relé 66 se comunicaría entonces con el dispositivo cliente 14 a través de la sesión de proxy cifrada y el tercer canal de comunicaciones de alto nivel de seguridad 34 establecidos entre el dispositivo cliente 14 y el "servidor concentrador" 18, como se describió anteriormente. Adicionalmente, en diversas implementaciones, un tercer canal de comunicaciones de alto nivel de seguridad 34 se puede establecer entre el "servidor concentrador" 18 y uno o más otros servidores remotos 18 de la misma manera en la que se describió anteriormente.

Por lo tanto, el protocolo de objeto de relé del túnel de control de acceso de identidad múltiple descrito en el presente documento ofrece seguridad mejorada a los sistemas de información computarizados de varias maneras. Puede ser un reemplazo directo para mecanismos de tunelización basados en SSL exclusivamente. El protocolo de objeto de relé del túnel de control de acceso de identidad múltiple descrito en el presente documento ofrece el beneficio de identidad basada en una autentificación basada en pregunta y respuesta y una capa adicional de cifrado. Además de estos nuevos beneficios, el protocolo de objeto de relé del túnel de control de acceso de identidad múltiple descrito en el presente documento ofrece la capacidad para requerir múltiples credenciales desde uno o más usuarios para acceder a conjuntos extendidos de privilegios o documentos secretos u objetos contenidos en un sistema de información computarizada de alta seguridad.

El acceso basado en credenciales múltiples puede mejorar el nivel de responsabilidad del (de los) usuario(s) y hacer el robo de credenciales mucho más difícil y, por lo tanto, proteger adicionalmente la integridad del sistema de información informático y sus contenidos y acceso a otros sistemas que están conectados en la misma red de circuito cerrado. Además, el protocolo de objeto de relé del túnel de control de acceso de identidad múltiple descrito en el presente documento ofrece la capacidad de autentificar el dispositivo cliente 14 que se está usando para acceder al servidor remoto 18. Una identidad para un dispositivo cliente 14 específico ofrece una nueva capa de inicio de sesión de acceso y auditoría.

Una serie de requisitos pueden aplicarse a un dispositivo cliente 14 que será confiable, tal como la ubicación del dispositivo cliente 14, el tipo de red a la que el dispositivo 14 se conecta, con qué frecuencia se inspecciona y mantiene el dispositivo cliente 14, cuántos usuarios diferentes tienen permitido acceder al dispositivo cliente 14, quién tiene permitido acceder al dispositivo cliente 14, así como qué credenciales son necesarios para permitir acceder al servidor remoto 18. Todos estos proporcionan la capacidad de rastrear el acceso y crear pistas de auditoría basadas en fichas de hardware y en criptografía real en oposición a la autentificación basada en el secreto (contraseña) y protocolos de baja seguridad tal como SSL y TLS.

Con el protocolo de objeto de relé del túnel de control de acceso de identidad múltiple descrito en el presente documento, se usan múltiples identidades para autentificar una única sesión. Esto permite escenarios donde una organización que ejecuta un servicio seguro (servidor remoto) 18 quiere garantizar que no solo es el usuario del servicio alguien de confianza, sino también que el dispositivo cliente 14 que está accediendo al servicio es de confianza. También, con la utilización del protocolo de objeto de relé del túnel de control de acceso de identidad múltiple descrito en el presente documento, ciertas operaciones pueden permitirse solo con múltiples usuarios presentes y las identidades se pueden añadir y retirar de la sesión en tiempo real, permitiendo una escala flexible de confianza/autentificación.

La descripción en el presente documento es simplemente a modo de ejemplo en naturaleza y, por lo tanto, las variaciones que no salen del fundamento de lo que se describe se pretende que estén dentro del ámbito de la invención, como se definió en las reivindicaciones.

REIVINDICACIONES

1. Un método para establecer un túnel seguro entre un dispositivo cliente (14) y un servidor remoto (18) utilizando múltiples identidades (74) para autentificar el acceso al servidor remoto (18), comprendiendo dicho método:

ejecutar un programa de relé (66) en el servidor remoto (18) y descargar un programa conector (70) desde el servidor remoto (18) hasta el dispositivo cliente (14) al ejecutar el programa de relé (66);
escanear el dispositivo cliente (14) para uno o más dispositivos de autentificación (74) de los que al menos uno está conectado de manera que se puede retirar y/o está integrado de manera fija al dispositivo cliente (14), mediante la ejecución del programa conector (70), habiendo almacenado cada dispositivo de autentificación (74) allí una o más identidades;
seleccionar múltiples identidades desde las identidades almacenadas en uno o más dispositivos de autentificación (74), pasar las identidades seleccionadas al servidor remoto (18) y validar las identidades pasadas mediante una autentificación pregunta-respuesta llevada a cabo por el programa de relé (66);
establecer un canal de comunicaciones de alto nivel de seguridad (34) y gestionar una sesión de proxy cifrada entre un proxy (78) del lado del servidor remoto, corroborado mediante la ejecución del relé, y un proxy (82) del lado del cliente, corroborado mediante la ejecución del programa conector (70), y
proporcionar acceso por el dispositivo cliente (14) a un primer objeto contenido en el servidor mediante la sesión de proxy cifrada (78) sobre el canal de comunicaciones de alto nivel de seguridad (34).

2. El método de la Reivindicación 1, en el que ejecutar el programa de relé (66) comprende establecer un primer canal de comunicaciones sustancialmente inseguro (26) entre el dispositivo cliente (14) y el servidor remoto (18), a través del cual el programa conector (70) se descarga desde el servidor remoto (18) hasta el dispositivo cliente (14).

3. El método de la Reivindicación 2 que comprende además ejecutar el programa conector (70) en el dispositivo cliente (14) para establecer un segundo canal de comunicaciones de bajo nivel de seguridad (30) entre el programa conector (70) y el programa de relé (66).

4. El método de la Reivindicación 3, en el que seleccionar múltiples identidades (74) y pasar las identidades seleccionadas al servidor remoto (18) comprende pasar las múltiples identidades (74) seleccionadas al servidor remoto (18) a través del segundo canal de comunicaciones de bajo nivel de seguridad (30).

5. El método de las Reivindicaciones 1 o 4, en el que seleccionar múltiples identidades comprende seleccionar al menos una identidad desde un dispositivo de autentificación fijo (74) que está conectado integralmente al dispositivo cliente (14), integrado en el mismo, y seleccionar al menos una identidad desde un dispositivo de autentificación (74) conectado de manera que se puede retirar que proporciona el usuario y que se puede conectar, de manera que se puede retirar, al dispositivo cliente (14).

6. El método de la Reivindicación 5, en el que seleccionar la al menos una identidad desde el dispositivo de autentificación fijo (74) comprende seleccionar al menos una identidad que identifica al dispositivo cliente.

7. El método de las Reivindicaciones 1 o 4 que comprende además seleccionar identidades adicionales desde uno o más dispositivos de autentificación (74) para acceder a un segundo objeto contenido en el servidor o datos particulares dentro del primer objeto contenido en el servidor.

8. El método de las Reivindicaciones 1 o 4 que comprende además conectar de manera que se puede retirar uno o más dispositivos de autentificación (74) adicionales al dispositivo cliente (14) para proporcionar identidades requeridas para acceder a un segundo objeto (48) contenido en el servidor o datos particulares dentro del primer objeto (48) contenido en el servidor.

9. El método de la Reivindicación 8, que comprende requerir a un segundo usuario proporcionar uno o más dispositivos de autentificación (74) adicionales.

10. El método de la Reivindicación 1 en el que la etapa de escanear el dispositivo cliente (14) para uno o más dispositivos de autentificación (74) implica escanear para un primer dispositivo de autentificación (74) integralmente conectado al dispositivo cliente, integrado en el mismo, y al menos un segundo dispositivo de autentificación (74) conectado de manera que se puede retirar al dispositivo cliente, habiendo almacenado allí el primer dispositivo de autentificación una identidad de dispositivo cliente y habiendo almacenado allí el segundo dispositivo de autentificación una o más identidades de usuario; y
la etapa de seleccionar múltiples identidades implica seleccionar la identidad del dispositivo cliente y al menos una identidad de usuario desde el primer y el segundo dispositivos de autentificación.

11. El método de la Reivindicación 10, en el que ejecutar el programa de relé (66) comprende establecer un primer canal de comunicaciones sustancialmente inseguro (26) entre el dispositivo cliente (14) y el servidor remoto (18), a través del cual el programa conector (70) se descarga desde el servidor remoto (18) hasta el dispositivo cliente (14).

12. El método de la Reivindicación 11, que comprende, además:

ejecutar el programa conector (70) en el dispositivo cliente (14) para establecer un segundo canal de comunicaciones de bajo nivel de seguridad (30) entre el programa conector (70) y el programa de relé (66); y
pasar las identidades (74) seleccionadas al servidor remoto (18) a través del segundo canal de comunicaciones de bajo nivel de seguridad (30).

13. El método de la Reivindicación 10 que comprende además seleccionar identidades adicionales desde al menos uno entre el primer y el segundo dispositivos de autentificación (74) para acceder a un segundo objeto (48) contenido en el servidor o datos particulares dentro del primer objeto (48) contenido en el servidor.

14. El método de la Reivindicación 1 que comprende además conectar de manera que se puede retirar uno o más dispositivos de autentificación (74) adicionales al dispositivo cliente (14) para proporcionar identidades requeridas para acceder a un segundo objeto (48) contenido en el servidor o datos particulares dentro del primer objeto (48) contenido en el servidor, en donde se requiere que un segundo usuario proporcione uno o más dispositivos de autentificación (74) adicionales.

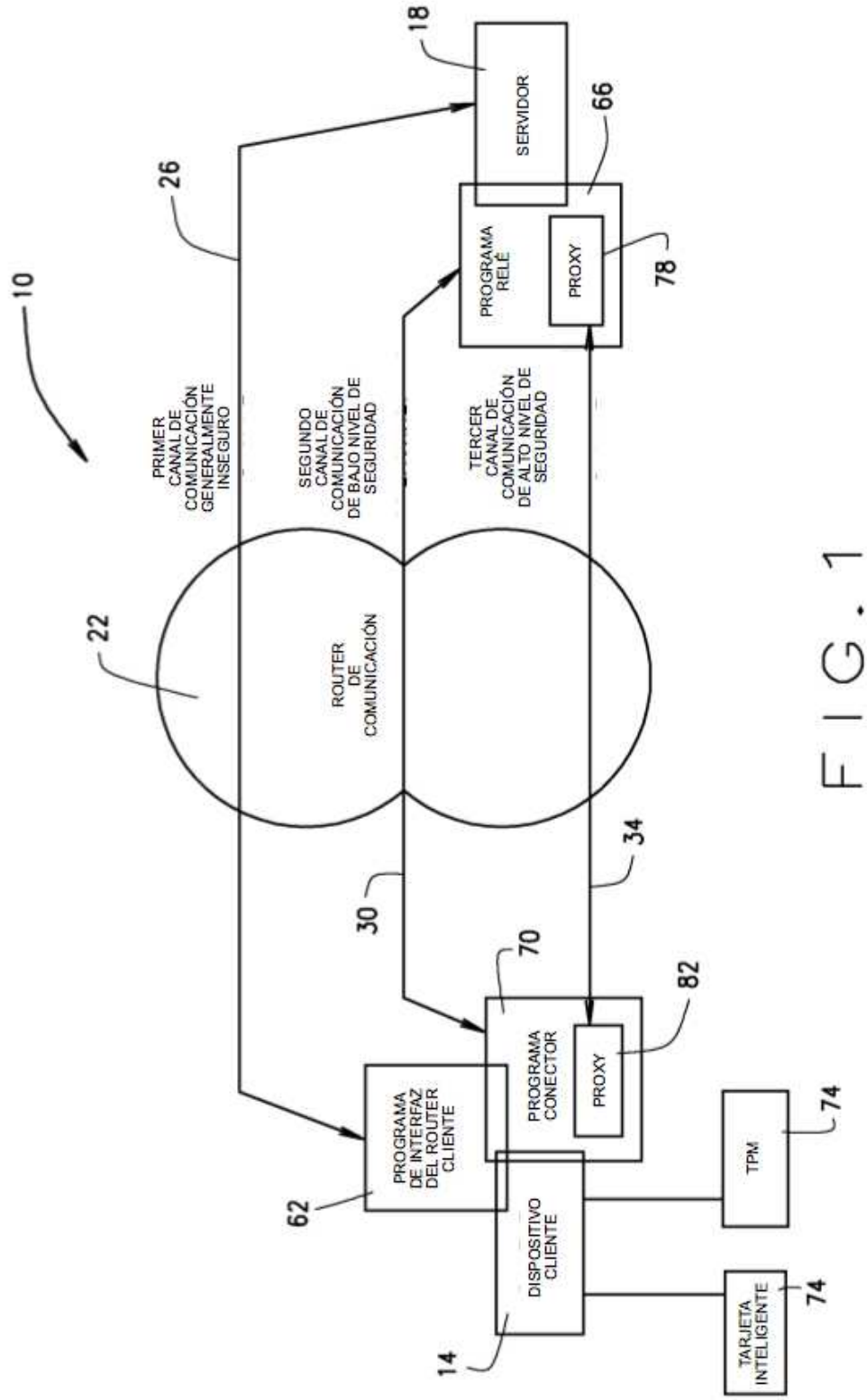
10
18
SERVIDOR
66
26
PROGRAMA RELÉ
PROXY
78
PRIMER CANAL DE COMUNICACIÓN GENERALMENTE INSEGURO
SEGUNDO CANAL DE COMUNICACIÓN DE BAJO NIVEL DE SEGURIDAD
TERCER CANAL DE COMUNICACIÓN DE ALTO NIVEL DE SEGURIDAD
22
ROUTER DE COMUNICACIÓN
34
30
70
82
PROGRAMA CONECTOR
PROXY
PROGRAMA DE INTERFAZ DEL ROUTER CLIENTE
62
TPM
74
DISPOSITIVO CLIENTE
14
TARJETA INTELIGENTE
74

FIG. 1

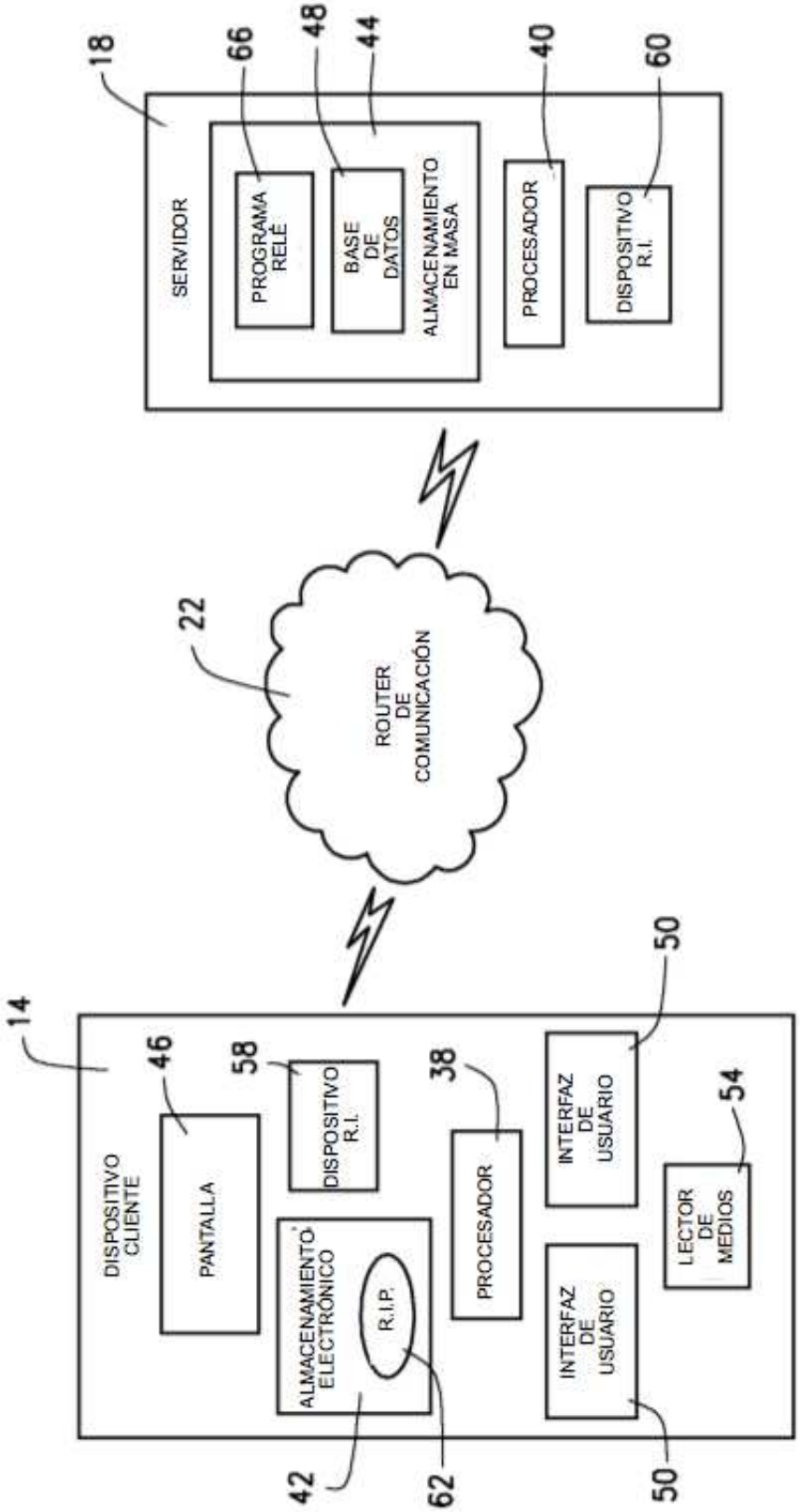
18
66
48
44
40
60
SERVIDOR
PROGRAMA RELÉ
BASE DE DATOS
ALMACENAMIENTO EN MASA
PROCESADOR
DISPOSITIVO R.I.
22
ROUTER DE COMUNICACIÓN
14
50
46
58
38
54
DISPOSITIVO CLIENTE
PANTALLA
DISPOSITIVO R.I.
INTERFAZ DE USUARIO
PROCESADOR
LECTOR DE MEDIOS
ALMACENAMIENTO ELECTRÓNICO
R.I.P.
INTERFAZ DE USUARIO
42
62
50

FIG. 2

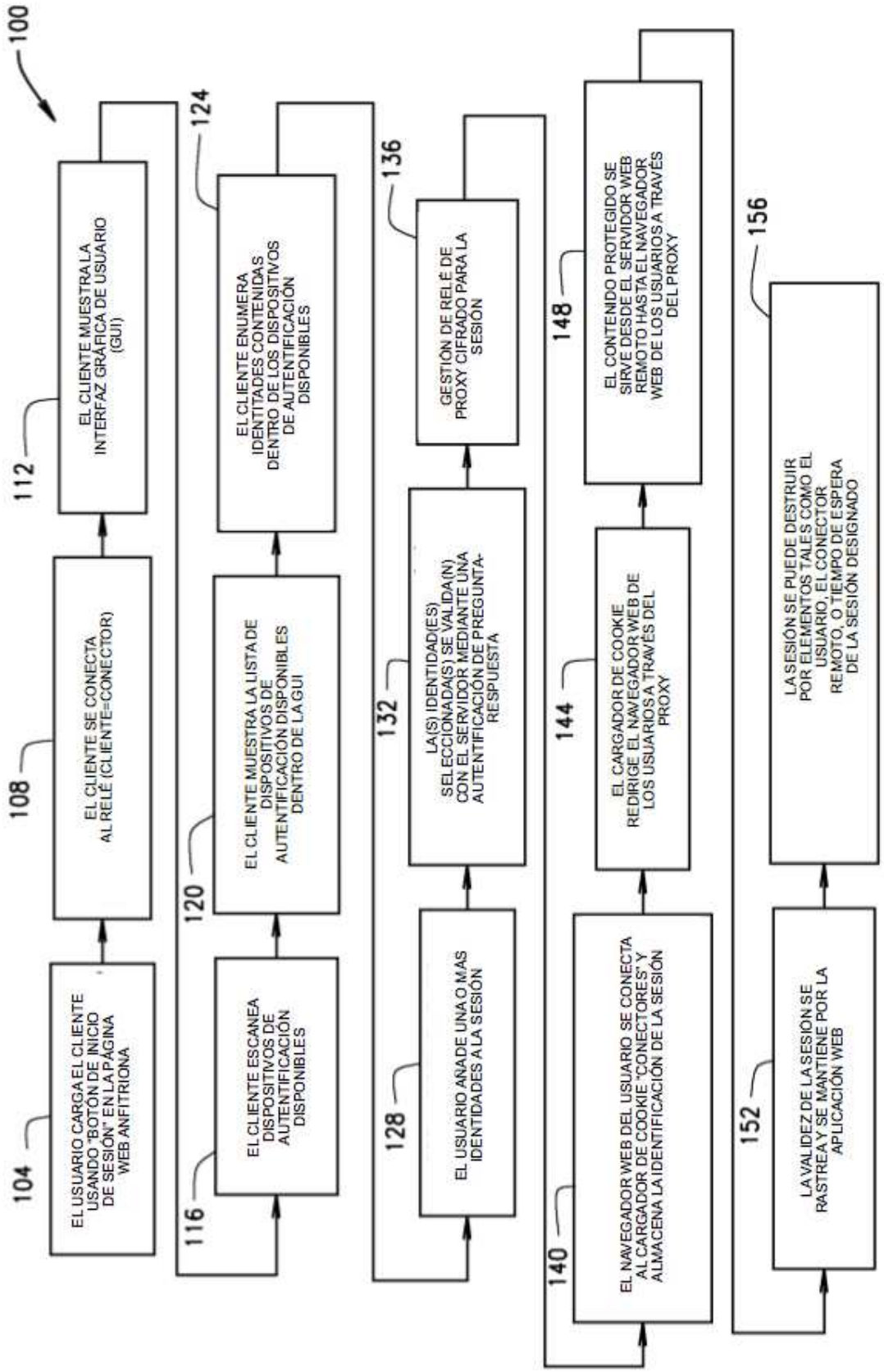
100
104
EL USUARIO CARGA EL CLIENTE USANDO "BOTÓN DE INICIO DE SESIÓN" EN LA PÁGINA WEB ANFITRIONA
108
EL CLIENTE SE CONECTA AL RELÉ (CLIENTE=CONECTOR)
112
EL CLIENTE MUESTRA LA INTERFAZ GRÁFICA DE USUARIO (GUI)
116
EL CLIENTE ESCANEA DISPOSITIVOS DE AUTENTIFICACIÓN DISPONIBLES
120
EL CLIENTE MUESTRA LA LISTA DE DISPOSITIVOS DE AUTENTIFICACIÓN DISPONIBLES DENTRO DE LA GUI
124
EL CLIENTE ENUMERA IDENTITADES CONTENIDAS DENTRO DE LOS DISPOSITIVOS DE AUTENTIFICACIÓN DISPONIBLES
128
EL USUARIO AÑADE UNA O MÁS IDENTIDADES A LA SESIÓN
132
LA(S) IDENTIDAD(ES) SELECCIONADA(S) SE VALIDA(N) CON EL SERVIDOR MEDIANTE UNA AUTENTIFICACIÓN DE PREGUNTA-RESPUESTA
136
GESTIÓN DE RELÉ DE PROXY CIFRADO PARA LA SESIÓN
140
EL NAVEGADOR WEB DEL USUARIO SE CONECTA AL CARGADOR DE COOKIE "CONECTORES" Y ALMACENA LA IDENTIFICACIÓN DE LA SESIÓN
144
EL CARGADOR DE COOKIE REDIRIGE EL NAVEGADOR WEB DE LOS USUARIOS A TRAVÉS DEL PROXY
148
EL CONTENIDO PROTEGIDO SE SIRVE DESDE EL SERVIDOR WEB REMOTO HASTA EL NAVEGADOR WEB DE LOS USUARIOS A TRAVÉS DEL PROXY
152
LA VALIDEZ DE LA SESIÓN SE RASTREA Y SE MANTIENE POR LA APLICACIÓN WEB
156
LA SESIÓN SE PUEDE DESTRUIR POR ELEMENTOS TALES COMO EL USUARIO, EL CONECTOR REMOTO, O TIEMPO DE ESPERA DE LA SESIÓN DESIGNADO

FIG. 3