(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 711**

(51) Int. CI.:
G06F 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03026014 .5**
(96) Fecha de presentación: **11.11.2003**
(97) Número de publicación de la solicitud: **1426846**
(97) Fecha de publicación de la solicitud: **09.06.2004**

(54) Título: **INICIO DE SESIÓN EN APLICACIONES DE SOPORTE LÓGICO QUE TIENEN CARACTERÍSTICAS DE SUGURIDAD.**

(30) Prioridad:
04.12.2002 US 309650

(45) Fecha de publicación de la mención BOPI:
05.03.2012

(45) Fecha de la publicación del folleto de la patente:
05.03.2012

(73) Titular/es:
MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WASHINGTON 98052, US

(72) Inventor/es:
Saunders, Stillman T.;
Coloma, Ignacio Ariel y
Gupta, Vishal

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Inicio de sesión en aplicaciones de soporte lógico que tienen características de seguridad

La presente invención versa en general acerca de sistemas de ordenadores que autentican la identidad de los usuarios o de dispositivos informáticos. Más específicamente, la presente invención versa acerca de operaciones de ordenador de inicio de sesión en aplicaciones de soporte lógico que tienen características de seguridad.

Las aplicaciones de soporte lógico actuales son fabricadas con una capacidad de servicios de red que requiere que los usuarios y los ordenadores verifiquen su identidad registrándose para acceder a características de seguridad dentro de las aplicaciones de soporte lógico y, por ello, conectarse a servicios de autenticación.

Los servicios de autenticación como PASSPORT.NET, disponible en MICROSOFT CORPORATION, de Redmond, Washington, se están convirtiendo en parte integral de las aplicaciones de soporte lógico que precisan autenticar a los usuarios para acceder a las características de seguridad. Estos servicios de autenticación controlan el acceso a características de seguridad dentro de las aplicaciones de soporte lógico y proporcionan servicios de identidad y autenticación para los usuarios de la red. Por ejemplo, un servicio de seguridad de fax en red usado desde dentro de una aplicación de tratamiento de texto requeriría la introducción de un nombre de usuario y una contraseña para autenticar la identidad del usuario y autorizar el uso del servicio de fax en red. Una vez que se autentica la identidad, la operación de autenticación actúa como una pasarela de autenticación, permitiendo que los usuarios accedan de forma segura a los servicios de red dentro de la aplicación de tratamiento de texto sin introducir un nombre de usuario y una contraseña en cada servicio de red o en cada sitio web al que accedan durante la sesión registrada.

Sin embargo, los usuarios deben aún introducir un nombre de usuario y una contraseña o hacer clic en un botón de inicio de sesión para acceder inicialmente características de seguridad dentro de una aplicación de soporte lógico. Una deficiencia de las operaciones actuales de inicio de sesión es su omnipresencia, requiriendo la intervención del usuario con una interfaz de inicio de sesión de forma repetitiva en características de soporte lógico de seguridad. Esto debe hacerse cada vez que un usuario se registra después de cerrar una aplicación de soporte lógico con características de seguridad. Por ejemplo, si un usuario que usar una característica de seguridad dentro de una aplicación de soporte lógico, el usuario debe arrancar la aplicación y o bien mecanografiar un nombre de usuario y una contraseña o bien hacer clic en un botón de la interfaz para introducir una contraseña guardada. Si el usuario cambia de ordenador, se pierde el beneficio de una contraseña guardada y vuelve a pedírsele que introduzca un nombre de usuario y una contraseña. Estas deficiencias tienen un efecto molesto en los usuarios que acceden a características de seguridad de forma regular.

Además, algunas operaciones de cookies basadas en páginas electrónicas guardan contraseñas y nombres de usuario, pero siguen teniendo varias deficiencias. En primer lugar, todos los sistemas basados en páginas electrónicas siguen requiriendo indicaciones al usuario y su intervención con visualizaciones de la contraseña guardada. En segundo lugar, la funcionalidad “guardar la contraseña” se pierde si el usuario cambia de ordenador. Por último, las operaciones de inicio de sesión no son controlables por una directriz administrativa de red y no son adaptables a las preferencias de red.

El documento US 2002/095571 A1 da a conocer un sistema de ordenador que proporciona una seguridad global de aplicaciones de ordenador usando identificadores basados en roles. Los identificadores jerárquicos se agrupan colectivamente en conjuntos de privilegios. Los conjuntos de privilegios y otros identificadores jerárquicos se agrupan colectivamente en funciones de tareas, que, a su vez, son agrupadas en subconjuntos mayores denominados roles. Estos roles de usuario están almacenados en un almacén de datos. Se crean identificadores de usuario. Cada identificador de usuario está enlazado con un role de usuario del almacén de datos. A un usuario se le da permiso para acceder a funciones de seguridad dentro de una aplicación recuperando del almacén de datos un identificador subrogado que comparte el mismo rol de usuario que el usuario. Los derechos de acceso se determinan usando el identificador subrogado para validar los permisos en un proveedor de seguridad. Cuando un usuario enciende un ordenador, el ordenador ejecuta su secuencia normal de arranque. Suponiendo que el ordenador esté conectado a una red, el usuario entra en la red a través de la secuencia normal de comienzo de sesión. Un proveedor de autenticaciones es el proveedor se seguridad del sistema que contiene la información de la cuenta del usuario y, por lo tanto, puede determinar si la ID y la contraseña del usuario son válidas. Cuando un coordinador de plataforma recibe una solicitud de autorización, lleva a cabo dos comprobaciones contra su memoria intermedia antes del envío de la solicitud al agente de seguridad. En primer lugar, el coordinador de plataforma comprueba su memoria intermedia en busca de un testigo de autenticación válido. En segundo lugar, el coordinador de plataforma comprueba su memoria intermedia en busca del recurso de seguridad solicitado. Si se encuentra una entrada coincidente y si la entrada no ha caducado, los permisos contenidos en la memoria intermedia son devueltos al componente integrado y no se realiza llamada alguna al agente de seguridad. Se ajusta para soportar simultáneamente definiciones de control de acceso “basadas en directrices” y “basadas en roles”.

Es el objeto de la presente invención proporcionar un procedimiento mejorado para el inicio de sesión en una aplicación de soporte lógico, así como un producto y un sistema correspondientes de un programa de ordenador que permite un inicio de sesión automático de un usuario sin indicaciones de la interfaz de usuario ni intervención manual cuando un usuario arranca una aplicación de soporte lógico que tiene características de seguridad.

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

Las reivindicaciones dependientes definen realizaciones preferentes.

La presente invención se ha realizado con respecto a estas y otras consideraciones.

Según la presente invención, los problemas anteriores y otros se resuelven mediante un inicio de sesión automático para acceder a características de seguridad dentro de aplicaciones de soporte lógico. La presente invención registra automáticamente a un usuario sin indicaciones de la interfaz de usuario ni intervención manual cuando un usuario arranca una aplicación de soporte lógico que tiene características de seguridad. Cuando arranca una aplicación de soporte lógico y está habilitada la condición de inicio de sesión automático, la aplicación de soporte lógico pasa a un estado registrado con la condición de que se satisfagan los criterios de seguridad. La transición a un estado registrado tiene lugar sin indicación de que un usuario introduzca una credencial (por ejemplo, un nombre de usuario y una contraseña). En consecuencia, se evitan etapas innecesarias y repetitivas cuando se realiza el inicio de sesión y los impertinentes diálogos emergentes de inicio de sesión son mucho menos probables mientras se usa la aplicación de soporte lógico.

Otra característica de la presente invención es que la condición de inicio de sesión automático se inicia de varias maneras. Una condición de inicio de sesión automático puede ser iniciada a través de la configuración inicial del sistema, desde una indicación de que se introduzca una credencial o a través de un menú de opciones de servicio. Esta característica permite que las aplicaciones de soporte lógico en un conjunto tengan cada una una condición habilitada de inicio de sesión automático. Esto mejora la capacidad de las aplicaciones de soporte lógico de trabajar bien conjuntamente.

En otra característica de la presente invención, la información de credenciales se almacena con un formato cifrado como una credencial de dominio. Además, se establece una clave de registro del sistema, habilitando con ello una condición de inicio de sesión automático. Esto ofrece ventajas de seguridad adicional y prestaciones de itinerancia.

La invención puede ser implementada como un procedimiento de ordenador, un sistema informático o como un artículo de fabricación como un producto de un programa de ordenador o medios legibles por ordenador. El producto de programa de ordenador puede ser un medio de almacenamiento de ordenador legible por un sistema de ordenador y codificar un programa de ordenador de instrucciones para la ejecución de un procedimiento de ordenador. El producto de programa de ordenador puede ser también una señal propagada en una portadora, legible por un sistema de ordenador, y codificar un programa de ordenador de instrucciones para ejecutar un procedimiento de ordenador.

Una ventaja de la presente invención es que mejora la eficiencia de la red, porque las transmisiones de la red se ejecutan solo cuando se necesitan. Aunque la aplicación de soporte lógico esté en un estado registrado, se reduce el tráfico de la red realizando transmisiones de red únicamente cuando se solicitan características de seguridad.

Otra ventaja de la presente invención es que la condición de inicio de sesión automático es capaz de itinerar a otros ordenadores dentro de una red, siguiendo por ello a usuarios móviles. Una ventaja adicional de la presente invención es que la condición de inicio de sesión automático es controlable por medio de una directriz administrativa de red, dado a los administradores de la red la capacidad de inhabilitar su funcionalidad cuando se desee.

La gran utilidad de la invención es que, después del arranque de la aplicación de soporte lógico, los usuarios se registran automáticamente para acceder a características de seguridad dentro de la aplicación de soporte lógico sin utilizar indicaciones al usuario para la introducción de credenciales y requerir la intervención manual.

Estas y diversas características adicionales, así como ventajas, que caracterizan a la presente invención serán evidentes con una lectura de la siguiente descripción detallada y un repaso de los dibujos asociados.

Breve descripción de los dibujos

La FIGURA 1 es un diagrama que ilustra la arquitectura de sistema utilizada en una realización real de la presente invención;

la FIGURA 2 ilustra un entorno informático en el que puede implementarse la invención;

las FIGURAS 3 y 4 son diagramas de pantalla que muestran visualizaciones ilustrativas de ordenador proporcionadas por una realización real de la presente invención;

la FIGURA 5 ilustra un flujo de operaciones para llevar a cabo el inicio de sesión en una aplicación de soporte lógico que tiene características de seguridad en una realización de la presente invención;

la FIGURA 6 ilustra una realización de la presente invención en la que se habilita una condición de inicio de sesión automático a partir de una indicación de solicitud de credenciales presentada después de una solicitud de inicio de sesión;

las FIGURAS 7A-B ilustran otra realización de la presente invención en la que una aplicación de soporte lógico que tiene características de seguridad pasa a un estado registrado en base a que se satisfagan criterios y condiciones de seguridad específicos.

Descripción detallada de la invención

Con referencia a la FIGURA 1, se describirá un diagrama ilustrativo que muestra una arquitectura 10 de sistema utilizada en una realización real de la presente invención. Tal como se muestra en la FIGURA 1, se proporciona un ordenador cliente 20 que se conecta a un servidor 60 de autenticación a través de una red 40. Según una realización real descrita en el presente documento, el ordenador cliente 20 comprende un ordenador personal estándar que se conecta a una red 40, como Internet, a través de una conexión, como una Línea Digital de Abonado o un módem de cable. Sin embargo, debería apreciarse que el ordenador cliente 20 puede comprender otro tipo de dispositivo informático, como una agenda electrónica, y puede estar conectado a la red 40 a través de otro tipo de conexión, como una conexión de marcado o por satélite.

El ordenador cliente 20 es capaz de ejecutar un programa de aplicación estándar de navegador web, como INTERNET EXPLORER, de MICROSOFT CORPORATION, de Redmond, Washington. El programa de aplicación estándar de navegador web puede ser utilizado para acceder a sitios y servicios 80 de seguridad de red si el ordenador cliente 20 tiene una credencial autenticada. Una credencial es autenticada después de que el ordenador cliente 20 transmite la credencial al servidor 60 de autenticación a través de la red 40. El servidor 60 de autenticación autentica la identidad de los usuarios antes de conceder a un usuario acceso a servicios o sitios web 80 de seguridad. Por ejemplo, antes de que un usuario del ordenador cliente 20 pueda acceder a un servicio de seguridad de fax o impresión dentro de una aplicación de soporte lógico de tratamiento de texto equipada con características de seguridad de fax e impresión, el usuario debe presentar una credencial (por ejemplo, un nombre de usuario y una contraseña) al servidor 60 de autenticación a través de la red 40.

El ordenador cliente 20 indica al usuario que inicie una sesión o un registro cronológico para acceder a características de seguridad dentro de la aplicación de soporte lógico con una credencial siempre que se solicite una característica de seguridad dentro de la aplicación de soporte lógico. Sin embargo, cuando una condición de inicio de sesión automático está habilitada en el ordenador cliente 20, se elimina la necesidad de intervención del usuario y la aplicación de soporte lógico pasa a un estado registrado sin pedir acción por parte del usuario. Si la condición de inicio de sesión automático está habilitada y se satisfacen los criterios de seguridad, se logra un estado registrado cuando se lanza la aplicación de soporte lógico que tiene características de seguridad.

Una vez que se valida la credencial, el servidor 60 de autenticación devuelve una cookie cifrada al ordenador cliente 20. La cookie cifrada da al ordenador cliente 20 acceso a servicios y sitios web de seguridad. Una vez que la memoria para la aplicación de soporte lógico recibe la cookie cifrada, el ordenador cliente 20 puede acceder a sitios y servicios de seguridad por medio de la aplicación de soporte lógico a través de la red 40 sin autenticar de nuevo la credencial durante una sesión registrada. Sin embargo, si el usuario sale de la aplicación de soporte lógico e inicia de nuevo las características de seguridad dentro una aplicación de soporte lógico, se pedirá al usuario que introduzca una credencial, a no ser que el inicio de sesión automático está habilitado dentro de la aplicación de soporte lógico en el ordenador cliente 20.

La FIGURA 2 ilustra un entorno informático adecuado en el que pueden implementarse realizaciones de la invención. Se describirá una realización de la invención en el contexto general de instrucciones ejecutables por ordenador que se ejecutan en un ordenador personal. Los expertos en la técnica apreciarán que la invención puede ser puesta en práctica con otras configuraciones de sistemas de ordenador, incluyendo dispositivos de mano, sistemas multiprocesador, dispositivos electrónicos de consumo basados en microprocesador o programables, ordenadores personales de red, miniordenadores, ordenadores centrales y similares. La invención puede también ser puesta en práctica en entornos informáticos distribuidos en los que las tareas son efectuadas por dispositivos remotos de proceso que están enlazados a través de la red de comunicaciones.

Con referencia a la FIG. 2, un sistema ejemplar para implementar la invención incluye un dispositivo informático de uso general en forma de un ordenador cliente convencional 20, que incluye una unidad 204 de proceso, una memoria 206 de sistema y un bus 212 de sistema que acopla diversos componentes de sistema que incluyen la memoria de sistema a la unidad 204 de proceso. El bus 212 de sistema puede ser cualquier de varios tipos de estructuras de bus, incluyendo un bus de memoria o un controlador de memoria, un bus de periféricos y un bus local que use cualquiera de una variedad de arquitecturas de bus. La memoria del sistema incluye memoria de solo lectura (ROM) 210 y memoria de acceso aleatorio (RAM) 208. En la ROM 210 está almacenado un sistema básico 222 de entrada/salida (BIOS) que contiene la rutina básica que contribuye a transferir información entre elementos dentro del ordenador cliente 20, como durante el arranque.

El ordenador cliente 20 incluye, además, un dispositivo 214 de almacenamiento para almacenar un sistema operativo 216, los programas de aplicación de soporte lógico con características 230 de seguridad, como OFFICE, de MICROSOFT CORPORATION, de Redmond, Washington, otros programas 235 de aplicación, un programa de aplicación estándar de navegador web, como INTERNET EXPLORER, de MICROSOFT CORPORATION, de Redmond, Washington, e información de registro del sistema en el que se escribe una credencial cifrada y se

registra un mecanismo de habilitación del inicio de sesión automático. El sistema operativo 216 trabaja en conjunción con un gestor 232 de credenciales, que es un mecanismo usado para almacenar de forma segura credenciales en el ordenador cliente 20. Además, el sistema operativo 216 trabaja en conjunción con una cookie cifrada 228 que es enviada desde el servidor 60 de autenticación. La cookie cifrada 228 da al ordenador cliente 20 acceso a servicios y sitios de seguridad que se ejecutan en la red 40.

Puede obtenerse una cookie cifrada 228 después de que el usuario arranque una de las aplicaciones de soporte lógico que tiene características 230 de seguridad y se registre en ella introduciendo una credencial cuando se le pida. Si está habilitado un inicio de sesión automático cuando el usuario arranca una de las aplicaciones 230 de soporte lógico, se evita la indicación de registro o inicio de sesión y el ordenador cliente 20 se registra en la aplicación de soporte lógico sin intervención del usuario. Cuando está habilitada una condición de registro o de inicio de sesión automáticos, está activa una clave 234 de registro del sistema de registro o de inicio de sesión automáticos y se almacena una credencial autenticada en el gestor 232 de credenciales. La clave 234 del registro del sistema escrita en la HKEY inicial del usuario actual (hkcu) tiene características de itinerancia que pueden seguir un perfil de usuario a ordenadores clientes, permitiendo, por lo tanto, las características de itinerancia de la condición de registro o inicio de sesión automáticos.

El dispositivo 214 de almacenamiento se conecta a la CPU 204 a través de un controlador de almacenamiento (no mostrado) conectado al bus 212. El dispositivo 214 de almacenamiento y sus medios asociados legibles por ordenador proporcionan un almacenamiento no volátil al ordenador cliente 20. Aunque la descripción de medios legibles por ordenador contenida en el presente documento se refiere a un dispositivo de almacenamiento como un disco duro o una unidad de CD-ROM, los expertos en la técnica deberían apreciar que los medios legibles por ordenador pueden ser cualesquiera medios disponibles que puedan ser objeto de acceso por el ordenador personal 20.

A título de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender medios de almacenamiento de ordenador y medios de comunicaciones. Los medios de almacenamiento de ordenador incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier procedimiento o tecnología para el almacenamiento de información, como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenamiento de ordenador incluyen, sin limitación, RAM, ROM, EPROM, EEPROM, memoria flash u otra tecnología de memoria de estado sólido, CD-ROM, DVD u otro almacenamiento óptico, casetes magnéticas, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda ser usado para almacenar la información deseada y que pueda ser objeto de acceso por el ordenador.

Típicamente, los medios de comunicaciones implementan instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal modulada de datos, como una onda portadora u otro mecanismo de transporte e incluyen cualquier información de medios de distribución. La expresión “señal modulada de datos” significa una señal una o más de cuyas características han sido establecidas o cambiadas de tal manera que se codifica la información de la señal. A título de ejemplo, y no de limitación, los medios de comunicaciones incluyen los medios cableados, como una red cableada o una conexión cableada directa y medios inalámbricos, como medios acústicos, de RF, infrarrojos y otros medios inalámbricos. Las combinaciones de cualquiera de los medios anteriores también deberían estar incluidas dentro del alcance de los medios legibles por ordenador. Los medios legibles por ordenador también pueden ser denominados producto de programa de ordenador.

Según diversas realizaciones de la invención, el ordenador cliente 20 puede operar en un entorno de red usando conexiones lógicas a ordenadores remotos a través de una red 40 como Internet. El ordenador cliente 20 puede conectarse a la red 40 a través de una unidad 220 de interfaz de red conectada al bus 212. Debería apreciarse que la unidad 220 de interfaz de red también puede ser utilizada para conectarse a otros tipos de red y sistemas de ordenadores remotos. El ordenador cliente 220 también puede incluir un controlador 222 de entrada/salida para recibir y procesar una entrada de varios dispositivos, incluyendo un teclado, un ratón o un estilete electrónico (no mostrados en la FIGURA 2). De modo similar, un controlador 222 de entrada/salida puede proporcionar salida a una pantalla de visualización, una impresora u otro tipo de dispositivo de salida.

Tal como se ha mencionado brevemente en lo que antecede, pueden almacenarse varios módulos de programa y ficheros de datos en el dispositivo 214 de almacenamiento y la RAM 208 del ordenador cliente 20, incluyendo un sistema operativo 216 adecuado para controlar la operación de un ordenador personal de red, como el sistema operativo WINDOWS XP, de MICROSOFT CORPORATION, de Redmond, Washington. El dispositivo 214 de almacenamiento y la RAM 208 puede también almacenar uno o más ficheros de datos. En particular, el dispositivo 214 de almacenamiento y la RAM 208 pueden almacenar la credencial que se escribe en el gestor 232 de credenciales y datos de registro del sistema escritos en el registro 233 del sistema. A continuación se describirán con mayor detalle detalles adicionales relativos a la operación de la operatoria de registro o inicio de sesión automáticos.

Con referencia ahora a la FIGURA 3, se describirá un diagrama de pantalla que muestra una visualización de ordenador ilustrativa proporcionada por una realización real de la presente invención. La FIGURA 3 muestra una

interfaz 30 de usuario que se presenta cuando se solicita una credencial para acceder a características de seguridad dentro de una aplicación de soporte lógico. Después de que se reciben un nombre 32 de usuario y una contraseña 34, se presenta una opción o casilla de control para permitir una condición de registro o inicio de sesión automáticos como casilla 36 de control. Si se afirma o se hace clic en la casilla 36 de control, se inicia una operación para permitir una condición de registro o inicio de sesión automáticos.

Pasando a la FIGURA 4, se describirá un diagrama de pantalla que muestra una visualización de ordenador ilustrativa proporcionada por una realización real de la presente invención. La FIGURA 4 muestra una interfaz 40 de usuario que se presenta en respuesta a la selección por parte de un usuario de un menú de opciones de servicio para revisar o modificar preferencias de un ordenador cliente 20 para interactuar con servicios y sitios de red. Alternativamente, puede iniciarse una condición de inicio de sesión automático a partir de la interfaz 40 de usuario. Si no se ha habilitado una condición de inicio de sesión automático, se presentan un nombre 42 de usuario, una opción para guardar la contraseña y la opción 48 de inicio de sesión automático con campos en blanco. Para iniciar la operación para habilitar la condición de inicio de sesión automático, se cumplimentan y se afirman o activan los campos nombre 42 de usuario, guardar 46 la contraseña y inicio de sesión automático. El nombre de usuario se cumplimenta haciendo clic en el botón 44 de inicio de sesión que muestra la interfaz 30 de usuario, permitiendo que un usuario introduzca un nombre de usuario y una contraseña.

Si se afirma la opción 46 de guardar la contraseña sin que se haya afirmado el inicio de sesión automático 48, la operación de registro o de inicio de sesión seguirá presentando una indicación de solicitud de intervención del usuario. Por ejemplo, puede pedirse al usuario que haga clic en un botón de “Inicio de sesión” en la interfaz de usuario. Además, la opción 48 de inicio de sesión automático se muestra en gris como inactiva hasta que se afirme la opción 46 para guardar la contraseña. Si el usuario selecciona Inicio de sesión 44, se presentará una interfaz 30 de usuario para introducir una credencial. En lo que sigue se proporcionarán detalles adicionales relativos a la habilitación de una condición de registro o inicio de sesión automáticos y de inicio de sesión sin la intervención del usuario.

Las operaciones lógicas de las diversas realizaciones de la presente invención se implementan (1) como una secuencia de acciones o módulos de programa implementados por ordenador que se ejecutan en un sistema informático y/o (2) como circuitos lógicos de máquina interconectados o módulos de programa dentro del sistema informático. La implementación es una cuestión de elección dependiente de los requisitos de rendimiento del sistema informático que implementa la invención. En consecuencia, las operaciones lógicas que componen las realizaciones de la presente invención descritas en el presente documento son denominadas de forma diversa como operaciones, dispositivos estructurales, acciones o módulos. Un experto en la técnica reconocerá que estas operaciones, estos dispositivos estructurales, acciones y módulos pueden ser implementados en soporte lógico, soporte lógico inalterable, en lógica digital de uso especial y cualquier combinación de los mismos sin apartarse del espíritu y el alcance de la presente invención según se enumera dentro de las reivindicaciones adjuntas al presente documento.

La FIGURA 5 ilustra un flujo operativo 500 ejecutado o efectuado de inicio de sesión automáticamente o iniciar sesión en una aplicación de soporte lógico que tiene características de seguridad sin pedir la intervención del usuario. El flujo operativo 500 se inicia con una operación 502 de habilitación por medio del cual se registra una condición de inicio de sesión automático. Con referencia a la FIGURA 6, un flujo 600 de operación ilustra una realización de la presente invención en la operación 502 de habilitación en la que una condición de inicio de sesión automático o de inicio de sesión es habilitada a partir de una indicación 30 de solicitud de credenciales mostrada en una operación 604 de visualización después de una solicitud de inicio de sesión de acceso a características de seguridad en la operación 602 de recepción. La habilitación de una condición de inicio de sesión automático puede llevarse a cabo mostrando una solicitud 30 de registro o inicio de sesión para acceder a la aplicación de seguridad de soporte lógico, recibiendo una credencial 32 y 34 para el registro de inicio de sesión en una aplicación de soporte lógico que tiene características de seguridad en una operación 606 de recepción, y la recepción de una solicitud 36 para registrarse o iniciar sesión automáticamente en lo sucesivo en aplicaciones de soporte lógico que tienen características de seguridad en la operación 608 de recepción. La recepción de una solicitud puede lograrla un usuario haciendo clic en una casilla de control “registrarme automáticamente”.

A continuación, la condición de inicio de sesión automático es habilitada adicionalmente autenticando la credencial en la operación 610 de autenticación y detectando si la credencial es válida en la operación 612 de detección. Aquí la credencial cifrada es transmitida al servidor 60 de autenticación, en el que se efectúa una determinación de si la credencial es válida. Si la credencial no es válida, el flujo operativo 600 se bifurca volviendo a la operación 604 de visualización. Sin embargo, si la credencial es válida, el flujo 600 de la operación procede a almacenar la credencial 32 y 34 en un gestor 232 de credenciales y a activar la clave 233 del registro del sistema en la operación 614 de escritura. En este punto se habilita la condición de inicio de sesión automático. El control de la operación vuelve a las otras rutinas en el conector 620.

Volviendo a la FIGURA 5, después de que la condición de inicio de sesión automático haya sido habilitada en la operación 502 de habilitación, la aplicación de soporte lógico es iniciada o lanzada en la operación 504 mientras esté en la condición de inicio de sesión automático. La operación 506 de detección determina entonces si se satisfacen

los criterios de seguridad. Los criterios de seguridad pueden comprender que se detecte una conexión de red, que se almacene una credencial válida, que esté activa la clave del registro del sistema, que se use un bloqueo y más. Si la operación 506 de detección detecta que no se satisfacen los criterios de seguridad, el flujo operativo 500 sale en la operación 508.

Si la operación 506 de detección detecta que se satisfacen los criterios de seguridad, la aplicación de soporte lógico pasa al estado registrado en la operación 510 de transición, concediendo con ello acceso a las características de seguridad sin pedir la intervención manual para introducir una credencial o hacer clic en un botón de inicio de sesión. El control de la operación vuelve a otras rutinas en el conector 512.

Las FIGURAS 7A-B ilustran otra realización de la presente invención en la que una aplicación de soporte lógico que tiene características de seguridad pasa a un estado registrado o de inicio de sesión en un flujo operativo 700 basado en el arranque de la aplicación de soporte lógico con la operación 722 de inicio y satisfaciéndose criterios y condiciones específicos de seguridad o de inicio de sesión automático. Después del arranque, la operación 723 de detección de la aplicación de soporte lógico determina si existe una conexión de red. Si la conexión de red no está presente, la condición de inicio de sesión automático se ve estorbada y el control vuelve a otras rutinas en el conector 738.

Si está presente la conexión de red, el flujo operativo 700 avanza entonces a la operación 724 de detección, en la que se realiza una determinación de si una o más aplicaciones de soporte lógico adicionales que tienen características de seguridad están en estado de ejecución o abierto en ese momento. Si una o más aplicaciones adicionales están en estado de ejecución o abierto, el flujo operativo 700 devuelve el control a otras rutinas en el conector 738. Si otras aplicaciones no están en estado de ejecución o abierto, la operación 726 de detección determina si se está usando en ese momento un bloqueo para registrar o iniciar sesión con otra aplicación de soporte lógico. Si el bloqueo no se está usando, la operación 728 de bloqueo adquiere el bloqueo para que la detección de criterios pueda proseguir sin interrupción de otras aplicaciones que se registren.

El flujo operativo 700 continúa con la operación 730 de detección que determina si una directriz administrativa ha habilitado una condición de registro o inicio de sesión automáticos. Un administrador de red puede deshabilitar la funcionalidad de registro o inicio de sesión automáticos al poner una clave del registro del sistema en la sección del registro del sistema del ordenador cliente bajo el control del administrador. Esta característica puede ser usada fundamentalmente para ordenadores públicos de redes privadas o KIOSK que tienen múltiples usuarios. La configuración por defecto para esta clave habilita la funcionalidad. Si la condición de registro o inicio de sesión automáticos está habilitada en la operación 730 de detección, la operación 730 de detección determina si la versión del sistema operativo soporta la condición de inicio de sesión automático. Las versiones del sistema operativo debería estar equipadas para soportar una condición de registro o inicio de sesión automáticos.

Si la versión del sistema operativo soporta la condición de registro o inicio de sesión automáticos, el flujo operativo 700 continúa con que la operación 734 de detección determine si la clave 230 del registro del sistema está activa. Si la clave 230 del registro del sistema está activa, la operación 740 de detección determina si una credencial está almacenada en el gestor de credenciales. Estando presente la credencial, la operación 742 de autenticación procede a autenticar la credencial. Aquí, la credencial es transmitida al servidor 60 de autenticación, en el que la operación 743 de detección determina si la credencial es válida. Si la credencial no es válida, se muestra un error y el flujo operativo 700 se bifurca al conector 752, en el que el control de la operación es devuelto a las otras rutinas. Si la credencial es válida, se transmite una cookie cifrada desde el servidor 60 de autenticación al ordenador cliente 20 y la aplicación de soporte lógico pasa a un estado registrado en la operación 746 de transición.

El flujo operativo 700 prosigue entonces desde la operación 746 de transición a la operación 748 de mensajería, en la que cambia la interfaz de usuario, indicando un estado registrado o de inicio de sesión para que la aplicación de soporte lógico y otras aplicaciones reciban aviso de que ha ocurrido un registro o un inicio de sesión automáticos. Una vez que las otras aplicaciones de soporte lógico han sido notificadas, la operación 750 de bloqueo quita el bloqueo. Acto seguido, el control de la operación es devuelto a otras rutinas en el conector 752.

Aunque la invención ha sido mostrada y descrita en particular con referencia a realizaciones de la misma, los expertos en la técnica entenderán que pueden realizarse en la misma diversos cambios adicionales en la forma y los detalles sin apartarse del alcance de la invención.

REIVINDICACIONES

1. Un procedimiento de inicio de sesión en una aplicación de soporte lógico, en el que la aplicación de soporte lógico tiene una o más características de seguridad, que comprende:

habilitar (502) una condición de inicio de sesión automático, habilitándose dicha condición de inicio de sesión automático recibiendo (606) una credencial, autenticando (610) dicha credencial y transmitiendo dicha credencial a un servidor (60) de autenticación para determinar si dicha credencial es válida y, si dicha credencial es válida, almacenando (614) dicha credencial en un gestor (232) de credenciales y activando una clave (230) del registro del sistema, siendo dicha credencial almacenada para el inicio de sesión para acceder a las características de seguridad después de que arranque la aplicación de soporte lógico;

arrancar (504) la aplicación de soporte lógico cuando está en la condición de inicio de sesión automático;

detectar (506) si se satisfacen los criterios de seguridad cuando está en la condición de inicio de sesión automático, en el que los criterios de seguridad comprenden:

que se detecte una conexión de red,

que no se use un bloqueo en la actualidad para el inicio de sesión de otra aplicación de soporte lógico,

que esté habilitada la condición de inicio de sesión automático por una directriz administrativa del sistema,

que la clave del registro del sistema esté activa;

que la credencial esté almacenada en dicho gestor de credenciales para el inicio de sesión para el acceso a las características de seguridad de la aplicación de soporte lógico, en el que, si está almacenada la credencial almacenada, dicha credencial almacenada es autenticada (742) y transmitida a dicho servidor de autenticación para validar (743) la credencial transmitida, satisfaciéndose el criterio de seguridad, si la credencial está almacenada en el gestor de credenciales, de que la credencial es autenticada y es válida; y

en respuesta a que se satisfagan la totalidad de dichos criterios de seguridad, pasando (510; 746) la aplicación de soporte lógico a un estado registrado dentro de la aplicación de soporte lógico con acceso a las características de seguridad.

2. El procedimiento de la reivindicación 1 que, además, comprende:

la recepción de una solicitud de acceso a las características de seguridad dentro de la aplicación de soporte lógico;

en respuesta a la solicitud, la transmisión de la información de autenticación y el acceso a las características de seguridad.

3. El procedimiento de la reivindicación 2 en el que la información de autenticación comprende una cookie cifrada recibida de un servidor (60) de autenticación.

4. El procedimiento de la reivindicación 1 en el que la habilitación de una condición de inicio de sesión automático comprende, además, las operaciones de:

recibir (602) una solicitud de acceso a las características de seguridad dentro de la aplicación de soporte lógico;

mostrar (604) una solicitud de una credencial; y

recibir (608) una solicitud de inicio de sesión automáticamente en lo sucesivo para el acceso a una o más características de seguridad dentro de una o más aplicaciones de soporte lógico que tienen características de seguridad.

5. El procedimiento de la reivindicación 4 en el que la credencial es almacenada en un formato cifrado.

6. El procedimiento de la reivindicación 4 en el que la solicitud de inicio de sesión automáticamente en lo sucesivo comprende que un usuario haga clic en una casilla (48) de control “registrarme automáticamente” para efectuar la solicitud.

7. El procedimiento de la reivindicación 1 en el que la habilitación de una condición de inicio de sesión automático comprende, además:

recibir una solicitud para mostrar un menú (40) de opciones de servicio;

mostrar el menú de opciones de servicio;

recibir (604) una solicitud de inicio de sesión automáticamente en lo sucesivo para el acceso a una o más características de seguridad dentro de una o más aplicaciones de soporte lógico; y

mostrar (604) una solicitud de una credencial.

8. El procedimiento de la reivindicación 7 en el que la solicitud de inicio de sesión automáticamente en lo sucesivo comprende una opción activa (46) “guardar la contraseña” y una opción activa “inicio de sesión automático” afirmadas por un usuario dentro del menú (40) de opciones de servicio.

9. El procedimiento de la reivindicación 1 en el que la aplicación de soporte lógico forma parte de una serie de dos o más aplicaciones de soporte lógico que tienen características de seguridad, en el que un sistema operativo soporta la condición de inicio de sesión automático, y en el que los criterios de seguridad comprenden, además, que una o más aplicaciones adicionales de soporte lógico no estén en un estado de ejecución cuando arranca la aplicación de soporte lógico.

10. El procedimiento de la reivindicación 9 que, además, comprende:

activar una interfaz de la aplicación de soporte lógico para indicar el estado registrado;

enviar uno o más mensajes que indiquen que ha ocurrido un inicio de sesión automático; y

liberar el uso del bloqueo.

11. El procedimiento de la reivindicación 1 en el que la credencial comprende un nombre de usuario y una contraseña.

12. El procedimiento de la reivindicación 1 en el que la condición de inicio de sesión automático puede ser deshabilitada por una directriz administrativa del sistema.

13. El procedimiento de la reivindicación 1 en el que las características de seguridad comprenden uno o más sitios web anfitriones y uno o más servicios anfitriones.

14. Un producto de programa de ordenador legible por un sistema informático e instrucciones de codificación para ejecutar un procedimiento de ordenador de inicio de sesión en una aplicación de soporte lógico, en el que la aplicación de soporte lógico tiene una o más características de seguridad, comprendiendo dicho procedimiento de ordenador:

habilitar (502) una condición de inicio de sesión automático, habilitándose dicha condición de inicio de sesión automático recibiendo (606) una credencial, autenticando (610) dicha credencial y transmitiendo dicha credencial a un servidor (60) de autenticación para determinar si dicha credencial es válida y, si dicha credencial es válida, almacenando (614) dicha credencial en un gestor (232) de credenciales y activando una clave (230) del registro del sistema, siendo dicha credencial almacenada para el inicio de sesión para acceder a las características de seguridad después de que arranque la aplicación de soporte lógico;

arrancar (504) la aplicación de soporte lógico cuando está en la condición de inicio de sesión automático;

determinar (506) si se satisfacen los criterios de seguridad cuando está en la condición de inicio de sesión automático, en el que los criterios de seguridad comprenden:

que se detecte una conexión de red,

que no se use un bloqueo en la actualidad para el inicio de sesión de otra aplicación de soporte lógico,

que esté habilitada la condición de inicio de sesión automático por una directriz administrativa del sistema,

que la clave del registro del sistema esté activa;

que la credencial esté almacenada en dicho gestor de credenciales para el inicio de sesión para el acceso a las características de seguridad de la aplicación de soporte lógico, en el que, si está almacenada la credencial almacenada, dicha credencial almacenada es autenticada (742) y transmitida a dicho servidor de autenticación para validar (743) la credencial transmitida, satisfaciéndose el criterio de seguridad, si la credencial está almacenada en el gestor de credenciales, de que la credencial es autenticada y es válida; y

en respuesta a que se satisfagan la totalidad de dichos criterios de seguridad, pasando (510; 746) la aplicación de soporte lógico a un estado registrado dentro de la aplicación de soporte lógico con acceso a las características de seguridad.

15. El producto de programa de ordenador de la reivindicación 14 en el que el procedimiento de ordenador, además, comprende:

la recepción de una solicitud de acceso a las características de seguridad dentro de la aplicación de soporte lógico;

en respuesta a la solicitud, la transmisión de la información de autenticación y el acceso a las características de seguridad.

16. El producto de programa de ordenador de la reivindicación 14 en el que la habilitación de una condición de inicio de sesión automático comprende, además:

recibir (602) una solicitud de acceso a las características de seguridad dentro de la aplicación de soporte lógico;

mostrar (604) una solicitud de una credencial; y

recibir (608) una solicitud de inicio de sesión automáticamente en lo sucesivo para acceder a una o más características de seguridad de una o más aplicaciones de soporte lógico lanzando las aplicaciones soporte lógico.

17. El producto de programa de ordenador de la reivindicación 16 en el que la credencial es almacenada en un formato cifrado.

18. El producto de programa de ordenador de la reivindicación 16 en el que la solicitud de inicio de sesión automáticamente en lo sucesivo comprende que un usuario haga clic en una casilla (48) de control “registrarme automáticamente” para efectuar la solicitud.

19. El producto de programa de ordenador de la reivindicación 16 en el que la solicitud de inicio de sesión automáticamente en lo sucesivo comprende una opción activa (46) “guardar la contraseña” y una opción activa (48) “inicio de sesión automático” activadas por un usuario dentro del menú de opciones de servicio.

20. El producto de programa de ordenador de la reivindicación 14 en el que la aplicación de soporte lógico forma parte de una serie de dos o más aplicaciones de soporte lógico que tienen características de seguridad, en el que un sistema operativo soporta la condición de inicio de sesión automático, y en el que los criterios de seguridad comprenden, además, que una o más aplicaciones adicionales de soporte lógico no estén en un estado abierto cuando arranca la aplicación de soporte lógico.

21. El producto de programa de ordenador de la reivindicación 14 en el que la credencial comprende un nombre de usuario y una contraseña.

22. El producto de programa de ordenador de la reivindicación 14 que, además, comprende:

cambiar una interfaz de la aplicación de soporte lógico para indicar el estado registrado;

enviar uno o más mensajes que indiquen que ha ocurrido un inicio de sesión automático; y

liberar el uso del bloqueo.

23. El producto de programa de ordenador de la reivindicación 14 en el que la condición de inicio de sesión automático puede ser deshabilitada por una directriz administrativa del sistema.

24. Un sistema (10; 20) de inicio de sesión en una aplicación de soporte lógico en el que la aplicación de soporte lógico tiene uno o más criterios de seguridad y una o más características de seguridad que comprende:

una unidad de memoria adaptada para almacenar una condición de inicio de sesión automático; y

una unidad de proceso adaptada para:

habilitar (502) una condición de inicio de sesión automático, habilitándose dicha condición de inicio de sesión automático recibiendo (606) una credencial, autenticando (610) dicha credencial y transmitiendo dicha credencial a un servidor (60) de autenticación para determinar si dicha credencial es válida y, si dicha credencial es válida, almacenando (614) dicha credencial en un gestor (232) de credenciales y

activando una clave (230) del registro del sistema, siendo dicha credencial almacenada para el inicio de sesión para acceder a las características de seguridad después de que arranque la aplicación de soporte lógico;

arrancar la aplicación de soporte lógico cuando está en la condición de inicio de sesión automático;

detectar si se satisfacen todos los criterios de seguridad, en respuesta a que se satisfagan la totalidad de dichos criterios de seguridad, pasando la aplicación de soporte lógico a un estado registrado dentro de la aplicación de soporte lógico con acceso a las características de seguridad, en el que la pluralidad de criterios de seguridad comprende:

que se detecte una conexión de red,

que no se use un bloqueo en la actualidad para el inicio de sesión de otra aplicación de soporte lógico,

que esté habilitada la condición de inicio de sesión automático por una directriz administrativa del sistema,

que la clave del registro del sistema esté activa;

que la credencial esté almacenada en dicho gestor de credenciales para el inicio de sesión para el acceso a las características de seguridad de la aplicación de soporte lógico, en el que, si está almacenada la credencial almacenada, dicha credencial almacenada es autenticada (742) y transmitida a dicho servidor de autenticación para validar (743) la credencial transmitida, satisfaciéndose el criterio de seguridad, si la credencial está almacenada en el gestor de credenciales, de que la credencial es autenticada y es válida.

25. El sistema de la reivindicación 24 que, además, comprende:

una unidad de visualización para indicar un estado registrado y la actividad de la red.

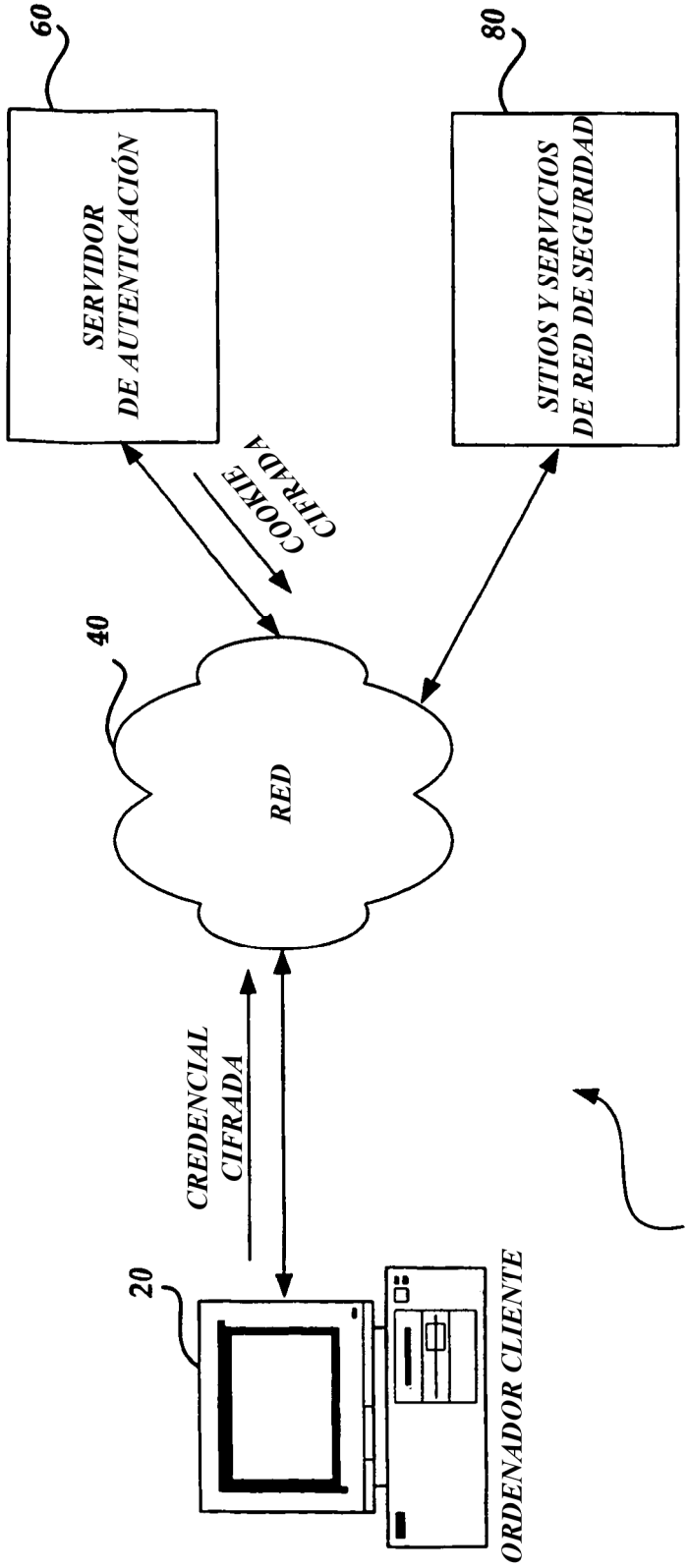
60
SERVIDOR
DE AUTENTICACIÓN
80
SITIOS Y SERVICIOS
DE RED DE SEGURIDAD
COOKIE
CIFRADA
40
RED
CREDENCIAL
CIFRADA
20
ORDENADOR CLIENTE
10

Fig. 1

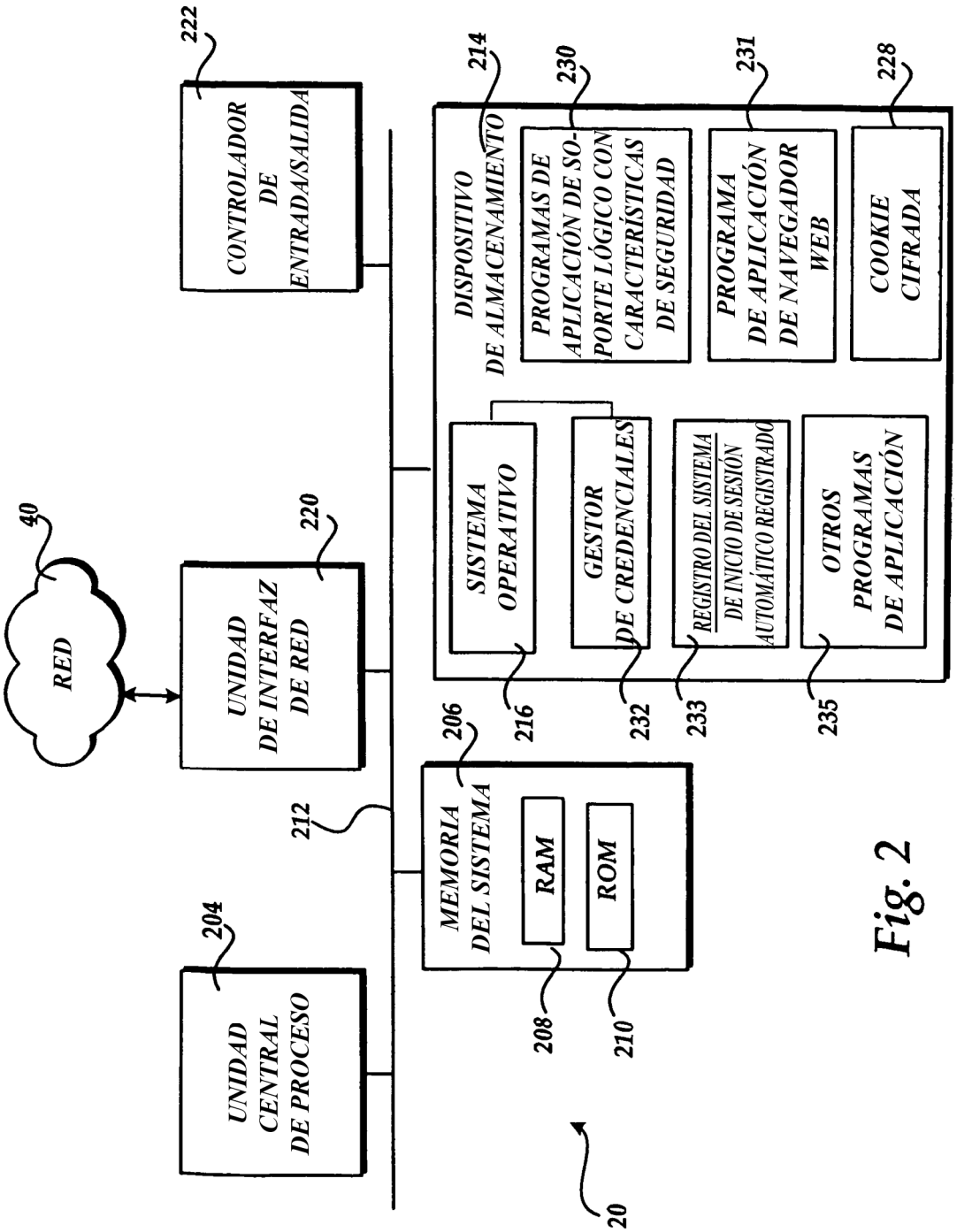
RED
40
UNIDAD DE INTERFAZ DE RED
220
CONTROLADOR DE ENTRADA/SALIDA
222
UNIDAD CENTRAL DE PROCESO
204
MEMORIA DEL SISTEMA
206
RAM
208
ROM
210
212
20
DISPOSITIVO DE ALMACENAMIENTO
214
SISTEMA OPERATIVO
216
GESTOR DE CREDENCIALES
232
REGISTRO DEL SISTEMA DE INICIO DE SESIÓN AUTOMÁTICO REGISTRADO
233
OTROS PROGRAMAS DE APLICACIÓN
235
PROGRAMAS DE APLICACIÓN DE SOPORTE LÓGICO CON CARACTERÍSTICAS DE SEGURIDAD
230
PROGRAMA DE APLICACIÓN DE NAVEGADOR WEB
231
COOKIE CIFRADA
228

Fig. 2

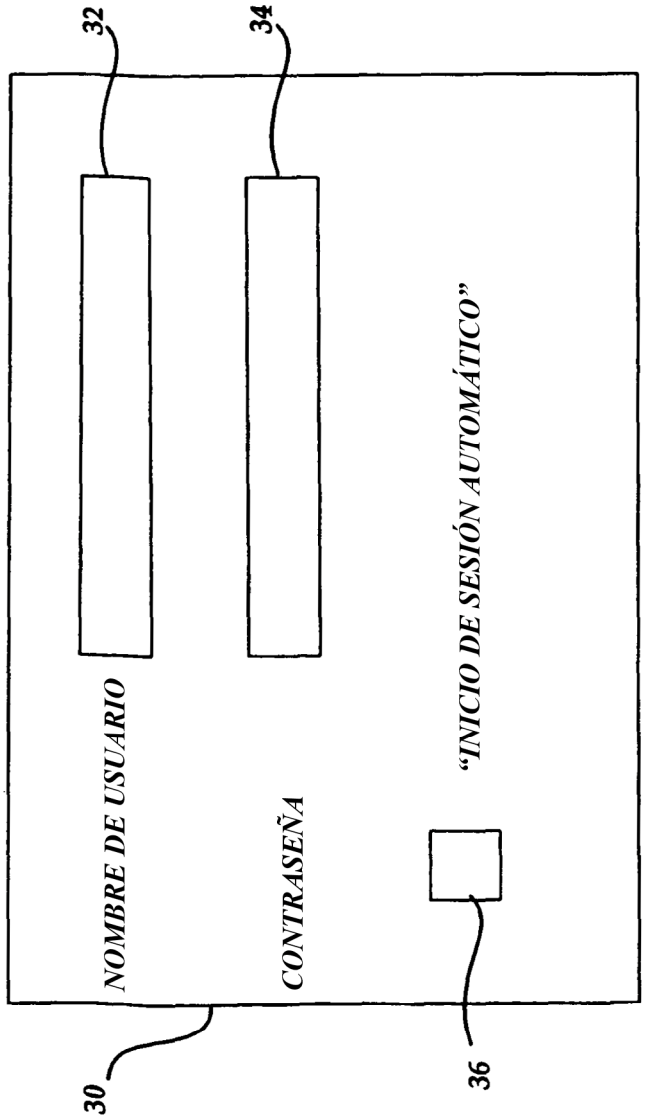
32
34
NOMBRE DE USUARIO
CONTRASEÑA
"INICIO DE SESIÓN AUTOMÁTICO"
30
36

Fig. 3

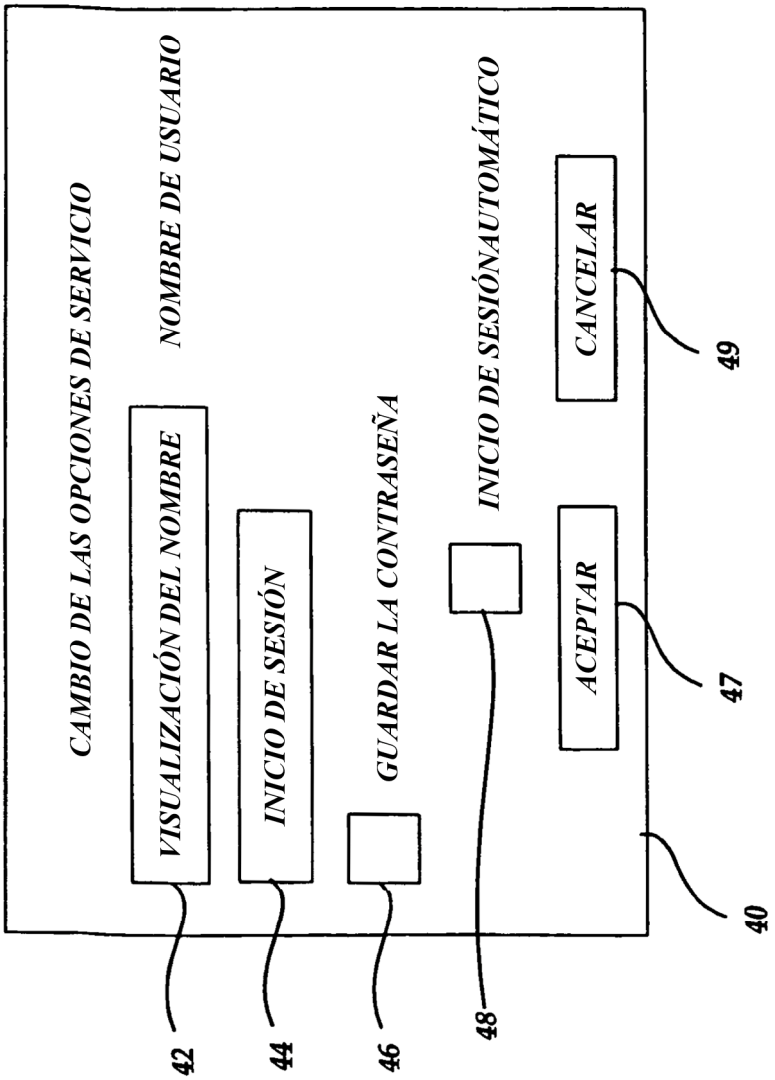
CAMBIO DE LAS OPCIONES DE SERVICIO
NOMBRE DE USUARIO
VISUALIZACIÓN DEL NOMBRE
INICIO DE SESIÓN
GUARDAR LA CONTRASEÑA
INICIO DE SESIÓNAUTOMÁTICO
ACEPTAR
CANCELAR
42
44
46
48
47
49
40

Fig. 4

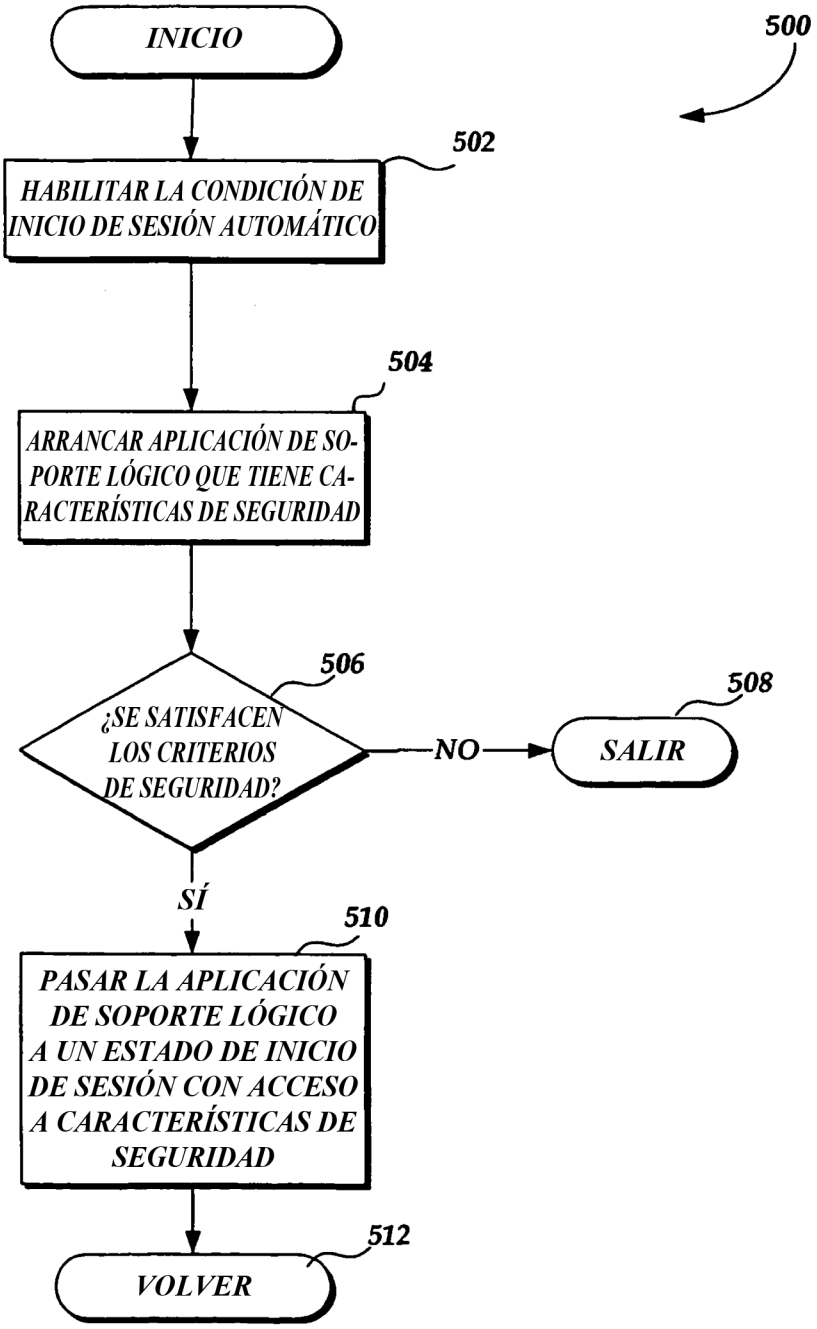
INICIO
500
502
HABILITAR LA CONDICIÓN DE INICIO DE SESIÓN AUTOMÁTICO
504
ARRANCAR APLICACIÓN DE SOPORTE LÓGICO QUE TIENE CARACTERÍSTICAS DE SEGURIDAD
506
¿SE SATISFACEN LOS CRITERIOS DE SEGURIDAD?
NO
508
SALIR
SÍ
510
PASAR LA APLICACIÓN DE SOPORTE LÓGICO A UN ESTADO DE INICIO DE SESIÓN CON ACCESO A CARACTERÍSTICAS DE SEGURIDAD
512
VOLVER

Fig. 5

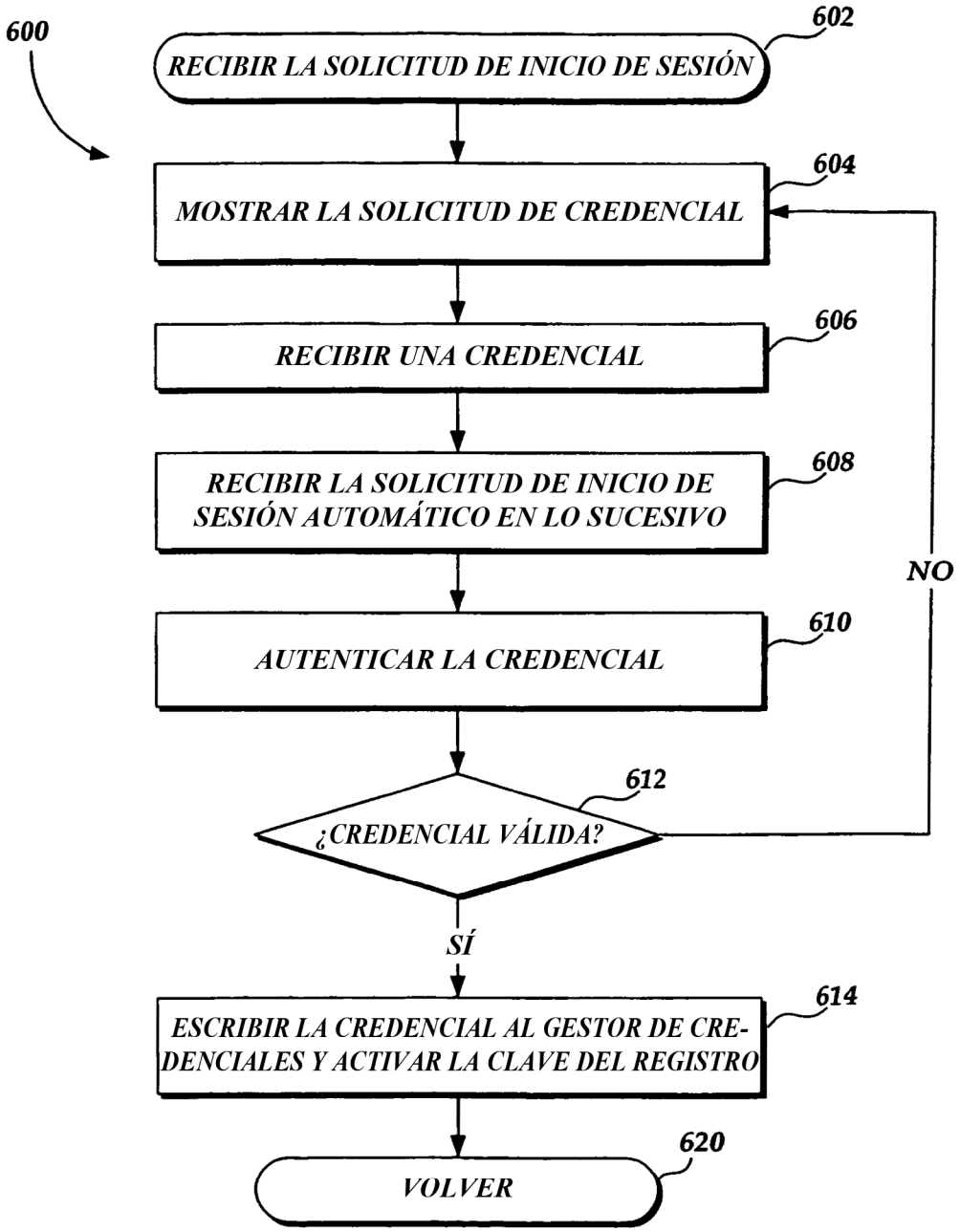
600
602
RECIBIR LA SOLICITUD DE INICIO DE SESIÓN
604
MOSTRAR LA SOLICITUD DE CREDENCIAL
606
RECIBIR UNA CREDENCIAL
608
RECIBIR LA SOLICITUD DE INICIO DE SESIÓN AUTOMÁTICO EN LO SUCESIVO
610
AUTENTICAR LA CREDENCIAL
612
¿CREDENCIAL VÁLIDA?
NO
SÍ
614
ESCRIBIR LA CREDENCIAL AL GESTOR DE CREDENCIALES Y ACTIVAR LA CLAVE DEL REGISTRO
620
VOLVER

Fig. 6

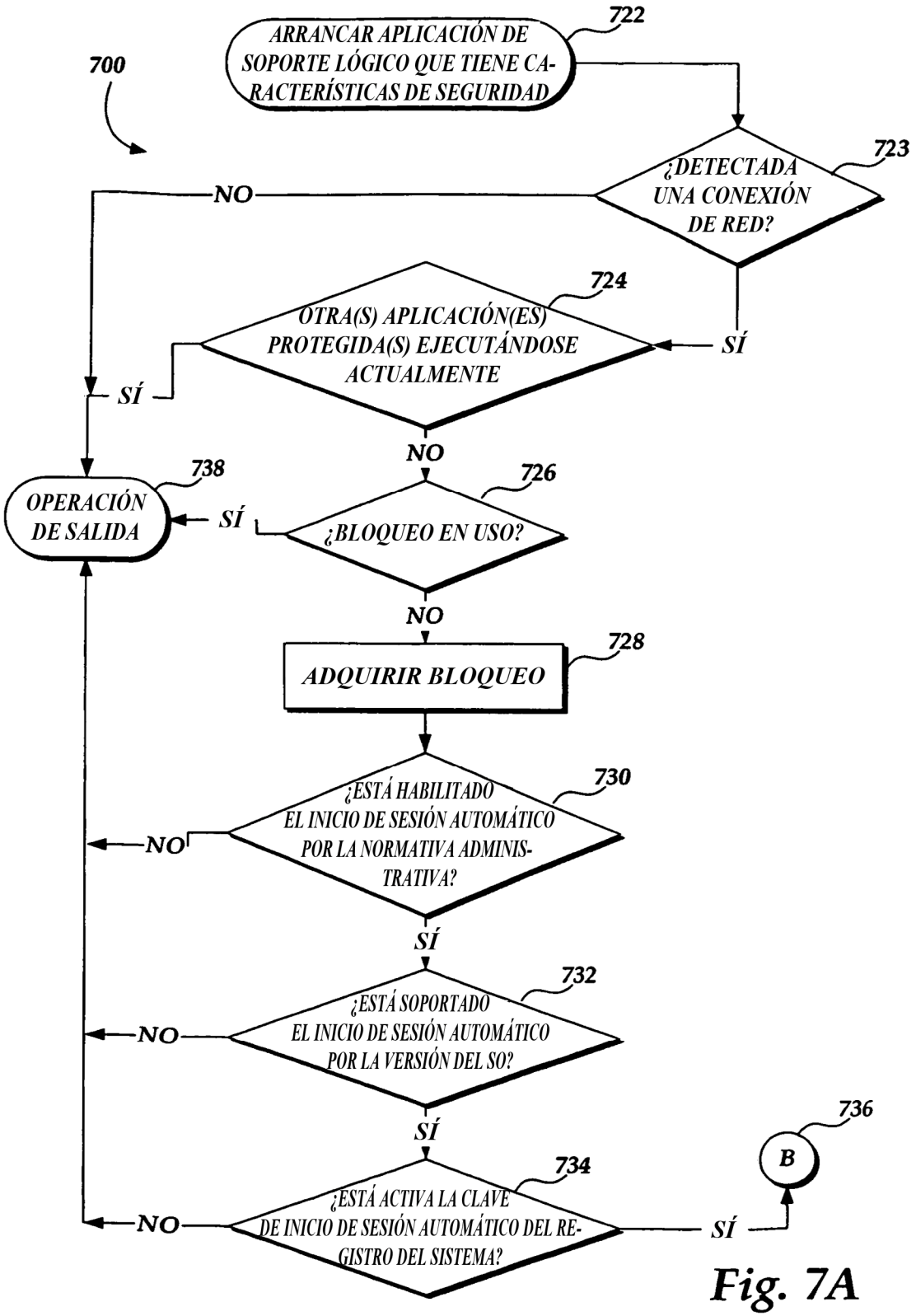
700
ARRANCAR APLICACIÓN DE SOPORTE LÓGICO QUE TIENE CARACTERÍSTICAS DE SEGURIDAD
722
¿DETECTADA UNA CONEXIÓN DE RED?
723
NO
SÍ
OTRA(S) APLICACIÓN(ES) PROTEGIDA(S) EJECUTÁNDOSE ACTUALMENTE
724
SÍ
NO
OPERACIÓN DE SALIDA
738
SÍ
¿BLOQUEO EN USO?
726
NO
ADQUIRIR BLOQUEO
728
¿ESTÁ HABILITADO EL INICIO DE SESIÓN AUTOMÁTICO POR LA NORMATIVA ADMINISTRATIVA?
730
NO
SÍ
¿ESTÁ SOPORTADO EL INICIO DE SESIÓN AUTOMÁTICO POR LA VERSIÓN DEL SO?
732
NO
SÍ
¿ESTÁ ACTIVA LA CLAVE DE INICIO DE SESIÓN AUTOMÁTICO DEL REGISTRO DEL SISTEMA?
734
NO
SÍ
B
736

Fig. 7A

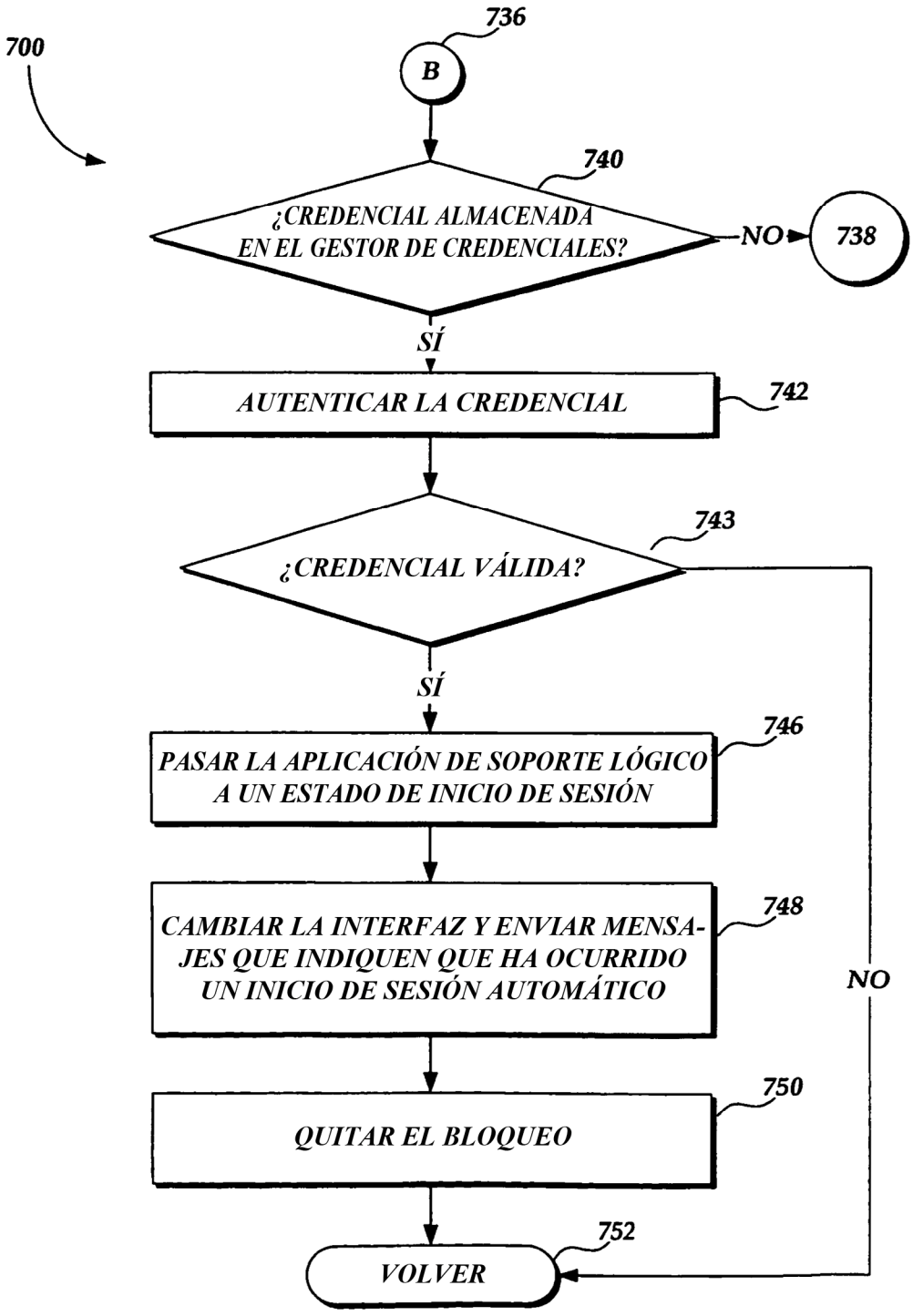
700
736
B
740
¿CREDENCIAL ALMACENADA EN EL GESTOR DE CREDENCIALES?
NO
738
SÍ
AUTENTICAR LA CREDENCIAL
742
743
¿CREDENCIAL VÁLIDA?
SÍ
746
PASAR LA APLICACIÓN DE SOPORTE LÓGICO A UN ESTADO DE INICIO DE SESIÓN
748
CAMBIAR LA INTERFAZ Y ENVIAR MENSAJES QUE INDIQUEN QUE HA OCURRIDO UN INICIO DE SESIÓN AUTOMÁTICO
NO
750
QUITAR EL BLOQUEO
752
VOLVER

Fig. 7B