(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 714 377**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.06.2005 PCT/US2005/021034**

(87) Fecha y número de publicación internacional: **29.12.2005 WO05125073**

(96) Fecha de presentación y número de la solicitud europea: **14.06.2005 E 05758533 (3)**

(97) Fecha y número de publicación de la concesión europea: **10.10.2018 EP 1756994**

(54) Título: **Procedimiento de seguridad en la red y de detección de fraude**

(30) Prioridad:

14.06.2004 US 867871

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.05.2019

(73) Titular/es:

IOVATION, INC. (100.0%)
111 SW Fifth Avenue, Suite 3200
Portland, OR 97204, US

(72) Inventor/es:

PIERSON, GREG y
DEHAAN, JASON

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento de seguridad en la red y de detección de fraude

Campo de la invención

La presente invención se refiere, en general, al campo de la seguridad en la red, incluidas la detección y prevención de transacciones fraudulentas y la usurpación de identidad. Al compartir información acerca de asociaciones entre usuarios finales y dispositivos de red específicos, la presente invención tiene otros usos potenciales que incluyen, pero no se limitan a, la distribución de contenido, la autenticación de hardware, la protección contra la piratería de software y otros medios electrónicos, vigilar el comportamiento del consumidor, la segmentación del mercado y la gestión de relaciones con consumidores.

Antecedentes de la invención

El continuo crecimiento de la infraestructura de las telecomunicaciones y la proliferación de dispositivos de red, proveedores de servicios, tecnología inalámbrica y productos de software relacionados han transformado Internet en una herramienta de uso diario. Las empresas utilizan cada vez más Internet como un procedimiento de comunicación con los consumidores, proveedores, empleados y accionistas, y de realización de transacciones comerciales. En teoría, la realización de negocios en Internet es a menudo eficaz y rentable, sobre todo cuando los productos y servicios pueden distribuirse de forma electrónica. En la práctica, los daños causados por los piratas informáticos, la usurpación de identidad, las tarjetas de crédito robadas y otras actividades fraudulentas puede ser enormemente costoso y difícil de manejar. Como mínimo, estas realidades aumentan significativamente los riesgos y costes asociados a la realización de negocios a través de Internet específicamente y, en general, a través de cualquier tipo de red.

Aunque varios procedimientos se utilizan comúnmente para hacer más seguro el uso de Internet y facilitar las transacciones de comunicación y de negocios, todos ellos tienen debilidades inherentes y explotables. Los nombres de usuario y las contraseñas son una de las formas de seguridad básica en la red más ampliamente utilizadas y aceptadas, donde el acceso está limitado a una coincidencia exacta de una combinación de nombre de usuario y contraseña. La identificación de nombres de usuario válidos es a menudo trivial, sobre todo en redes en las que los nombres de usuario son visibles para los observadores y en organizaciones en las que los usuarios tienen un formato de nombre de usuario común, tal como "*primeraInicial_apellido*". Dado que los usuarios finales suelen utilizar contraseñas comunes, simples y por defecto, comparten contraseñas y anotan las contraseñas más complicadas, y las contraseñas se pueden adivinar, solicitar u observar. Por lo tanto, la combinación del nombre de usuario y la contraseña solo proporciona un nivel básico de seguridad del que no se debe confiar exclusivamente, sobre todo para proteger redes accesibles a través de Internet.

Un sistema de autenticación de usuario secundaria va un paso más allá en la fiabilidad con un solo nombre de usuario y contraseña y puede aumentar en gran medida la seguridad. La autenticación secundaria se basa en algo que el usuario tiene en su poder, como por ejemplo un dispositivo de hardware de propósito especial. Por ejemplo, después de introducir un nombre de usuario y una contraseña válidos para acceder a una red, un usuario puede recibir un código como parte del proceso de inicio de sesión. El usuario introduce el código en un dispositivo dentro de una cantidad de tiempo especificada, y el dispositivo proporciona un código/contraseña secundarios que el usuario introducirá como parte del proceso de inicio de sesión. Aunque mucho más seguros, estos sistemas no son perfectos. Más importante aún, estos sistemas pueden ser poco prácticos en la protección de grandes redes accesibles por el público en general, y crean importantes barreras de entrada.

Una clave de hardware, denominada en ocasiones llave USB (*dongle*), que puede conectarse a un ordenador mediante un puerto USB, se utiliza en ocasiones para identificar usuarios finales que se conectan desde un dispositivo particular. Un número de serie de componente de sistema fijo y otros procedimientos de hardware utilizados para identificar de manera única un dispositivo de red específico también se usan para limitar el acceso a dispositivos 'conocidos'. Desafortunadamente, estos procedimientos se pueden copiar y simular en software. Estos sistemas también crean barreras y pueden ser poco prácticos en la protección de grandes redes accesibles por el público en general.

El uso de certificados digitales y de Autoridades de Certificación de Terceras Partes de Confianza son procedimientos cada vez más populares que garantizan que la parte que se conecta a una red es realmente quien dice ser. Desafortunadamente, los certificados se pueden copiar e incluso robar de forma remota. Además, debe confiarse en gran medida en grupos de verificación de terceras partes que no tengan un interés directo en las redes que confían en ellos. El requisito de que los usuarios de red utilicen certificados también puede crear una barrera importante, sobre todo para grandes redes accesibles por el público en general, y crear importantes barreras de entrada.

Una dirección de Protocolo de Internet (IP) y servicios de localización geográfica que dependen de la dirección IP se utilizan algunas veces para verificar los usuarios finales o, al menos, para cruzar una ubicación de referencia,

probablemente física, con información conocida acerca de un usuario. Estos procedimientos están limitados por el hecho de que muchos usuarios de Internet obtienen una nueva dirección IP temporal cada vez que se conectan a Internet. Además, el uso de direcciones IP para determinar la ubicación real de un dispositivo conectado es inherentemente deficiente por el modo en que se distribuyen bloques de números IP y la relativa facilidad de suplantación de direcciones IP, una técnica usada por intrusos de la red para que parezca que se están conectando desde una dirección IP de confianza u otra diferente.

Las bases de datos de tarjetas de crédito no válidas y las listas de identidades utilizadas en actividades fraudulentas son herramientas de verificación razonables y se deben utilizar en la medida en que sean rentables. Sin embargo, nunca se puede confiar exclusivamente en tales listas porque es prácticamente imposible que tales listas estén actualizadas y sean exhaustivas. Además, estas listas no ofrecen ninguna protección contra las denominadas 'devoluciones amistosas', pagos rechazados por los titulares de tarjetas de crédito que hacen compras utilizando su propia tarjeta de crédito válida y quienes, posteriormente, sostienen que no hicieron la compra.

Servicios de verificación, tales como RiskGardian proporcionado por TrustMarque, y otros servicios de evaluación de riesgos también son herramientas de verificación razonables y se deben utilizar en la medida en que sean rentables. Estos servicios utilizan poca información concreta acerca de un usuario o dispositivo específico y sólo asignan riesgos relativos asociados a una transacción particular basándose en la información general y en tendencias. Por último, tales servicios se basan exclusivamente en historiales de tendencias y son deficientes en la identificación de nuevos problemas y áreas de riesgo emergentes.

Las huellas digitales, el reconocimiento de voz, el escáner de retina, el reconocimiento facial, el ADN y otros procedimientos de identificación biométrica serán cada vez más comunes. En este momento, estos procedimientos de identificación de usuario tienen un precio muy elevado. Además, uno o más de estos procedimientos deben ser ampliamente distribuidos y generalmente aceptados por los usuarios finales para su consideración y su uso por la mayoría de las organizaciones que realizan negocios a través de Internet. Incluso si un procedimiento de este tipo estuviera disponible y fuese rentable, una vez que los identificadores biométricos únicos se conviertan en información electrónica, también pueden ser robados, copiados y verse comprometidos de otro modo.

Aunque todos estos procedimientos, y otros, tienen puntos débiles que pueden ser explotados, cada uno ocupa un lugar en la seguridad de las redes. Los tipos de acceso, el nivel de seguridad, la naturaleza de las poblaciones de usuarios y otros factores determinarán qué grupo de procedimientos servirá mejor a cada aplicación. La presente invención no pretende sustituir ninguno de estos medios de protección de redes y de descarte de usuarios no autorizados. Las organizaciones deben utilizar todo tipo de medios rentables a su disposición para regular el acceso a la red. La presente invención mejora la seguridad al proporcionar capacidades no ofrecidas por ninguno de los sistemas y procedimientos típicos anteriores. Por lo tanto, es deseable proporcionar un sistema y un procedimiento de seguridad en la red y de detección de fraudes, siendo éste el fin al que está dirigida la presente invención.
El documento US 2002/073046A1 da a conocer un sistema para permitir una transacción electrónica segura en una red, donde la red presenta un dispositivo de usuario que dispone de huella digital, un servidor y medios para proporcionar la identidad del usuario. El documento US 2003/005287A1 da a conocer un sistema y un procedimiento que proporcionan seguridad electrónica por medio de una red a través de un identificador de cliente positivo extensible, que funciona con un sistema de perfiles de información positiva, localizadores de recursos seudouniformes para ayudar a proporcionar integridad de datos, un sistema de publicación de páginas virtuales y un respondedor de seguridad activo. El documento US2002/035622A1 da a conocer un proceso de recopilación y archivo de datos de máquina en línea que genera un perfil de datos de máquina del ordenador de un consumidor que accede a un formulario de transacción de un sitio web comercial y que vincula el perfil de datos de máquina y un registro de transacción con información de identificación de consumidor usando una cadena de identificación de transacción única.

Resumen de la invención

Estos y otros objetos se consiguen mediante un procedimiento según la reivindicación 1 que permite identificar de manera única dispositivos de red que se conectan a una red, y correlacionar inicios de sesión con cada dispositivo de red utilizado.

Esta información puede utilizarse para observar un comportamiento de inicio de sesión, tales como cuentas que se conectan desde 'demasiados' dispositivos, o 'demasiadas' cuentas que se conectan desde el mismo dispositivo. Además, esta información puede utilizarse para una referencia cruzada entre dispositivos físicos utilizados por cuentas fraudulentas conocidas, y para una referencia cruzada con otras cuentas utilizadas por dispositivos específicos. Puede evitarse que dispositivos físicos implicados en una actividad sospechosa o fraudulenta, o que dispositivos asociados a cuentas implicadas en actividades sospechosas, se conecten a una red. Por último, esta información puede ser compartida con otras redes que utilizan el sistema. De esta manera, a los dispositivos físicos asociados con la actividad sospechosa o fraudulenta en una red se les puede denegar el acceso a otras redes, de acuerdo con las reglas de negocio y los parámetros de tolerancia al riesgo de cada red individual.

El procedimiento de la invención permite proporcionar una herramienta avanzada de prevención y detección de fraude que puede reducir significativamente el riesgo de fraude de identidad y de transacción en Internet al permitir que una empresa evite 'consumidores problemáticos' identificados por otras empresas participantes antes de que empiecen a crear problemas en ese negocio, y facilita el proceso de identificación de posibles reincidentes antes de que creen más problemas. Para lograr este objetivo, la herramienta prevención y detección de fraude identifica de manera única los clientes finales, así como su mutua asociación. Realiza un seguimiento de la conducta de consumidores finales en el tiempo, identifica un comportamiento 'sospechoso' basándose en parámetros establecidos por los proveedores de servicios de red, y mantiene el estado de las asociaciones entre dispositivos y usuarios finales. Esta información es compartida por todas las empresas participantes, de manera que una empresa puede tomar las decisiones más educadas acerca de nuevos y actuales consumidores en función de los dispositivos de red que utilizan y el historial de esos dispositivos con otras empresas. En una forma de realización, el procedimiento de la invención funciona con un sistema de prevención y de detección de fraude que comprende tres componentes principales en tiempo real que incluyen un servidor, un cliente y un conjunto de interfaces de programación de aplicaciones (API). El servidor contiene una base de datos centralizada del historial de fraude que se mantiene. El cliente es un pequeño programa ejecutable (que tiene una pluralidad de líneas de código) que 'registra' un dispositivo de red con el servidor. El cliente puede estar incluido dentro de un programa distribuido por un proveedor de servicios de red que debe utilizarse para conectarse a la red. El cliente también puede suministrarse a través de una aplicación independiente, integrada en un producto de software común, tal como un navegador web, o incluso integrada en el hardware o la memoria, siendo necesario que cualquiera de tales formas esté en ejecución cuando se autentica una conexión a una red mediante un proveedor de servicios de red protegido por este sistema. El cliente también podría suministrarse bajo demanda, a través de JavaScript, un control ActiveX u otra tecnología similar cuando un usuario se conecta a un proveedor de servicios de red a través de su navegador web favorito. Por ejemplo, un sitio de apuestas podría hacer que un nuevo usuario se descargue una aplicación de software que genere una lógica y una interfaz de usuario de mesa de póquer, y el cliente del sistema de prevención y detección de fraude es parte de esa aplicación de software descargada. La API ('ieSnAPi' en una forma de realización preferida) es un conjunto de herramientas que un sistema de procesamiento de un proveedor de servicios de red (que utiliza el sistema de prevención y de detección de fraude) utiliza para comunicarse con el sistema. Además de los tres componentes en tiempo real, el sistema comprende además dos componentes administrativos, incluidas páginas de administración de sitios web y un módulo de informes. Las páginas de administración de sitios web pueden permitir a un usuario del sistema ajustar sus niveles de tolerancia al fraude, inspeccionar y cambiar el estado de fraude de consumidores individuales y comprobar las relaciones de los consumidores entre sí. Los informes mantendrán un negocio al tanto de los consumidores existentes que realicen una nueva actividad fraudulenta, así como del uso del sistema.

De este modo, de acuerdo con los ejemplos dados a conocer en el presente documento, un sistema de prevención y detección de fraude y de seguridad en la red puede requerir que uno o más proveedores de servicios de red que proporcionan un servicio y que un dispositivo de red que se conecta a al menos uno de los proveedores de servicios de red a través de una red de comunicaciones utilicen el servicio prestado. Al menos uno de los proveedores de servicios de red tiene un detector de fraude que comprende un cliente que se descarga en el dispositivo de red cuando el dispositivo de red se conecta con el proveedor de servicios de red en el que el cliente recopila información acerca del dispositivo de red para generar una huella digital que identifica al dispositivo de red. El detector de fraude también tiene una base de datos y un módulo que recibe la huella digital, almacena la huella digital en la base de datos y asocia la huella digital con información de usuario. De acuerdo con la invención, la huella digital y la información de usuario se comparten entre el uno o más proveedores de servicios de red para detectar fraude usando el dispositivo de red a través de los proveedores de servicios de red. De acuerdo con otro aspecto de la invención se valida un identificador de dispositivo de red asignado al dispositivo de red y se valida la combinación del identificador de dispositivo de red y una huella digital de dispositivo de red para el dispositivo de red. Además, el estado del identificador de dispositivo de red y la huella digital de dispositivo de red para el dispositivo de red se verifican como aceptables para el proveedor de servicios de red en función de las reglas de estado del proveedor de servicios de red. A continuación, el estado del identificador de dispositivo de red y la huella digital de dispositivo de red para el dispositivo de red se verifican como aceptables para los proveedores de servicios de red asociados. De acuerdo con otro aspecto de la invención, se proporciona un procedimiento para detectar fraudes durante una conexión de un dispositivo de red desconocido con un proveedor de servicios de red. Utilizando el procedimiento, se activa una aplicación en un dispositivo de red, que a su vez activa un cliente de detección de fraude en el dispositivo de red. El cliente determina entonces que el dispositivo de red es un dispositivo de red no registrado y recibe un identificador de dispositivo de red solicitado desde un sistema de detección de fraude. El cliente genera entonces una huella digital basándose en características del dispositivo de red, la cual se reenvía al sistema de detección de fraude. El sistema de detección de fraude verifica entonces que la huella digital del dispositivo de red no esté duplicada y, a continuación, proporciona un cuadro de diálogo de inicio de sesión al dispositivo de red si la huella digital no está duplicada.

Breve descripción de las figuras

La Figura 1 es un diagrama que ilustra una red de transacciones electrónicas implementada por ordenador que tiene uno o más dispositivos de red que están conectados a uno o más proveedores de servicios de red que comparten información de fraude con un servidor de detección de fraude que es parte del sistema de detección de fraude según

la invención.

La Figura 2 es un diagrama que ilustra un ejemplo de un dispositivo de red según la invención.

La Figura 3 es un diagrama que ilustra un ejemplo de un proveedor de servicios de red según la invención.

La Figura 4 es un diagrama que ilustra un ejemplo del servidor de detección de fraude según la invención.

La Figura 5 ilustra ejemplos de una parte de una base de datos para cada proveedor de servicios de red.

La Figura 6 es un diagrama que ilustra un ejemplo de una base de datos de registro de dispositivo de red según la invención.

La Figura 7 es un procedimiento para etiquetar un dispositivo de red según la invención.

La Figura 8A es un diagrama que ilustra las tablas de una base de datos relacional de un ejemplo de una forma de realización preferida de un esquema de base de datos para un sistema de detección de fraude según la invención.

Las Figuras 8B a 8E son diagramas que ilustran detalles adicionales de las tablas de base de datos mostradas en la Figura 8A.

Las Figuras 9A y 9B son un diagrama de flujo que ilustra un procedimiento preferido para la validación de una cuenta usando el sistema de prevención y detección de fraude según la invención.

Las Figuras 9C y 9D son un diagrama de flujo que ilustra un procedimiento preferido para la validación de un nuevo usuario/dispositivo usando el sistema de prevención y detección de fraude según la invención.

Las Figuras 9E y 9F son un diagrama de flujo que ilustra un procedimiento preferido para la validación de un usuario/dispositivo existente.

Descripción detallada de una forma de realización preferida

La invención es particularmente aplicable a un sistema y procedimiento de detección de fraude de transacciones electrónicas y es en este contexto en que se describirá la invención. Se apreciará, sin embargo, que el sistema y procedimiento según la invención tiene una mayor utilidad, tal como en cualquier tipo de transacción en la que pueda ser deseable detectar fraude llevado a cabo por uno o más dispositivos de red y cuentas de usuario a través de una red de comunicaciones, o incluso detectar e impedir posibles fraudes o usurpaciones de identidad por personas que tratan de finalizar una transacción de forma remota por teléfono o correo, o incluso en persona. Un aspecto importante de este sistema y procedimiento consiste en asociar dos elementos de información acerca de una transacción, supervisar estas asociaciones para todos los consumidores y compartir información de estado acerca de estas asociaciones con otras empresas. A continuación se ilustra el uso de este sistema para correlacionar un dispositivo físico y un usuario. De acuerdo con la invención, el asociar cualquier combinación de identificador de consumidor, número de teléfono, número de permiso de conducir, número de la seguridad social, dirección postal, dirección de entrega, número de tarjeta de crédito, dirección de correo electrónico, dispositivo de red, ubicación de compra al por menor y cualquier otra información capturada como parte de una compra podría utilizarse para identificar y minimizar el fraude en una transacción y la usurpación de identidad. Uno de los aspectos más importantes de la invención es la creación de asociaciones, el seguimiento del comportamiento en el tiempo y el intercambio de información con múltiples redes o empresas que se benefician de compartir este tipo de información. De esta manera, una actividad fraudulenta puede ser identificada y detenida dentro de una red/empresa e impedirse en otras que compartan información a través de este sistema de prevención de fraude. Con fines ilustrativos se describirá un ejemplo específico del sistema de detección de fraude en el contexto de un sitio web de apuestas en línea. Según la invención, el sistema según la invención puede utilizar 1) tanto un identificador de dispositivo de red (NDI) como una huella digital de dispositivo de red (NDF) para identificar un dispositivo de red; 2) sólo un NDI para identificar un dispositivo de red; 3) solamente una NDF para identificar un dispositivo de red; o 4) cualquier otro dato que pueda utilizarse para identificar de manera única un dispositivo de red. La información utilizada para identificar un dispositivo de red puede conocerse como identificador de dispositivo. En algunas situaciones, puede que sea imposible extraer datos de un dispositivo de red, de forma que sólo el NDI se utiliza para identificar el dispositivo de red. En otras situaciones, los demás datos que se utilizan para identificar el dispositivo de red pueden ser un número de teléfono de una persona que llama a un sistema de pedidos telefónico o un identificador de un teléfono celular. En el ejemplo descrito a continuación, un NDI y una NDF se utilizan conjuntamente para identificar un dispositivo de red.

La Figura 1 es un diagrama que ilustra una red de transacciones electrónicas 20 implementada por ordenador que tiene uno o más dispositivos de red (ND1,..., NDn) 22 que están conectados a uno o más proveedores de servicios de red (NSP1,..., NSPn) 24, también denominados ordenadores centrales, que comparten información de fraude con un servidor de detección de fraude 26 que es parte del sistema de detección de fraude según la invención. Como se

muestra en la Figura 1, el servidor de detección de fraude 26 puede estar interconectado con los proveedores de servicios de red a través de una red privada o puede estar interconectado con los proveedores de servicios de red a través de una red de comunicaciones 28, tal como Internet, o *World Wide Web*, o cualquier otra red que sea capaz de comunicar datos digitales, tal como una red inalámbrica o celular. Si el servidor de detección de fraude 26 está conectado a la red de comunicaciones 28, entonces los datos entre los proveedores de servicios de red 24 y el servidor de detección de fraude 26 pueden cifrarse o transmitirse a través de una red privada virtual para garantizar la privacidad y la seguridad. Como se muestra en la Figura 1, cada dispositivo de red puede conectarse a cualquier proveedor de servicios de red 24 a través de la red de comunicaciones 28 utilizando protocolos de datos ampliamente conocidos, tales como HTTP, HTTPS y similares. En el sistema mostrado en la Figura 1, cada proveedor de servicios de red puede proporcionar un servicio a cada dispositivo de red conectado al mismo y puede llevar a cabo una transacción electrónica con cada dispositivo de red, tal como una apuesta en juegos de azar o la compra de un producto. Según la invención, cada transacción electrónica es susceptible de fraude y cada dispositivo de red y su usuario deben ser identificados de manera única para reducir el riesgo de fraude. Por lo tanto, el servidor de detección de fraude 26 puede recibir información única de identificación de usuario desde cada proveedor de servicios de red, así como generar un identificador único de dispositivo de red que identifica de manera única cada dispositivo de red. Usando la información única de identificación de usuario y la huella digital única de dispositivo de red según la invención, el servidor de detección de fraude 26 es capaz de detectar actividades fraudulentas a través de la red de transacciones electrónicas 20. En particular, el servidor de fraude 26 puede proporcionar un servicio centralizado que utiliza esta invención para identificar de manera única dispositivos físicos, registrar dispositivos únicos, realizar un seguimiento de inicios de sesión de usuario final, asociar una cuenta de usuario final con uno o más dispositivos específicos, asociar un dispositivo con una o más cuentas de usuario final, y compartir esta información con cada proveedor de servicios de red. El servidor de detección de fraude 26 puede incluir una base de datos de registro de dispositivos de red (NDRD) 30 centralizada. Más detalles del servidor de detección de fraude y del sistema de detección de fraude según la invención se describirán posteriormente con referencia a las Figuras 4 a 7.

El dispositivo de red 22, por ejemplo, puede ser un ordenador personal, un ordenador de tipo servidor, un ordenador portátil, un asistente personal digital (PDA), tal como un dispositivo basado en Palm o un dispositivo CE de Windows, un teléfono celular, un dispositivo inalámbrico, tal como un dispositivo inalámbrico de correo electrónico u otro dispositivo capaz de comunicarse de forma inalámbrica con una red de ordenadores o cualquier otro recurso informático que tenga un procesador, memoria y capacidades de entrada/salida para poder comunicarse con una red de ordenadores y manejar transacciones electrónicas. El dispositivo de red puede ser también un teléfono de un usuario utilizado, por ejemplo, para encargar artículos de un catálogo de venta por correo. En funcionamiento, un dispositivo de red, tal como ND1, puede solicitar acceso a la red de transacciones electrónicas 20 y a un proveedor de servicios de red particular, tal como NSP1 en este ejemplo. Para obtener acceso al NSP, completar una transacción o acceder a una parte en particular de la red, un usuario debe iniciar sesión a través de un dispositivo de red. El NSP puede pasar entonces un identificador de cuenta de usuario final (EAI) al servidor de detección de fraude 26. Un programa cliente en el dispositivo de red puede generar una huella digital de dispositivo de red (NDF) para el dispositivo de red (a menos que una huella digital ya se haya asignado a ese dispositivo de red) y envía esa NDF al servidor de detección de fraude. El servidor de detección de fraude almacena el EAI y la NDF en la NDRD 30. En función del EAI y la NDF, como se describe posteriormente con más detalle, se determina la probabilidad de que el usuario final particular cometa fraude con el dispositivo de red ND1, y se lleva a cabo una acción apropiada. Suponiendo que el dispositivo de red ND1 obtiene acceso a la red 20, el dispositivo de red realiza su transacción electrónica. Si se produce una actividad fraudulenta durante esa transacción electrónica, esa información también se almacena en la NDRD 30. De esta manera, el uno o más proveedores de servicios de red 24 comparten información de fraude entre sí de forma selectiva (como se describe posteriormente con más detalle) de manera que un fraude cometido contra un proveedor de servicios de red se registra en y es rastreado por el sistema de detección de fraude según la invención. Por lo tanto, se hace un seguimiento de un dispositivo de usuario o de red que haya cometido actividades fraudulentas, incluso cuando el dispositivo de usuario o de red se conecta a un proveedor de servicios de red diferente. Por lo tanto, se realiza un seguimiento de las actividades fraudulentas de un dispositivo de usuario o de red en todo el sistema de transacciones electrónicas 20. A continuación se describirá cada dispositivo de red con mayor detalle.

La Figura 2 es un diagrama que ilustra un ejemplo de un dispositivo de red 22 según la invención. En este ejemplo, el dispositivo de red es un ordenador personal. En este ejemplo, el dispositivo de red tiene un dispositivo de visualización 32, tal como una pantalla de tubo de rayos catódicos o de cristal líquido, para mostrar información y (opcionalmente imágenes) al usuario del dispositivo de red, un chasis 34 y uno o más dispositivos de entrada/salida para permitir al usuario comunicarse con el dispositivo de red y permitir que el dispositivo de red se comunique con el mundo exterior, tales como un teclado 36, un ratón 38 y un dispositivo 40 para la conexión y comunicación con una red de comunicaciones, tal como una tarjeta de interfaz de red, un módem por cable, un módem DSL, un módem inalámbrico, un módem de línea telefónica, etc. El dispositivo de red 22 comprende además uno o más procesadores 42, un dispositivo de almacenamiento persistente 44, tal como una unidad de cinta óptica, una unidad óptica, una unidad de disco duro, memoria flash, etc., que almacena datos incluso cuando el sistema informático está apagado, y una memoria 46, tal como SRAM, DRAM, SDRAM, etc., que almacena temporalmente datos que están siendo ejecutados por el procesador y que, por lo general, pierden los datos cuando el sistema informático se apaga. Normalmente, cuando el procesador está ejecutando las instrucciones de un programa de ordenador o

procesando datos en base a dichas instrucciones, las instrucciones y los datos se cargan en la memoria 46. De este modo, cuando el dispositivo de red está comunicándose con el sistema de transacciones electrónicas 20, la memoria puede almacenar un sistema operativo (OS) 48, una aplicación de navegador 50 y un paquete de software descargado 52, donde cada uno de estos son un programa de software que tiene una pluralidad de líneas de instrucciones que hacen que el dispositivo de red lleve a cabo una función particular. Por ejemplo, el sistema operativo 48, tal como Windows 2000, puede funcionar para mostrar al usuario una interfaz gráfica de usuario y permitir al usuario ejecutar otros programas de ordenador, tales como la aplicación de navegador 50 y uno o más paquetes de software descargados 52. La aplicación de navegador, tal como Netscape Navigator o Microsoft Internet Explorer, cuando es ejecutada por el procesador, permite al usuario acceder a la *World Wide Web* como es bien sabido. En este ejemplo, el dispositivo de red 22 puede conectarse a los proveedores de servicios de red (también conocidos como ordenadores centrales) utilizando la aplicación descargable 52 distribuida por cada ordenador central. Por ejemplo, para conectarse al ordenador central 1, los usuarios deben iniciar sesión a través del paquete de software de cliente 1, y para conectarse al ordenador central 2, los usuarios deben iniciar sesión a través del paquete de cliente de software 2, etc. Según la invención, cada paquete de software descargado puede incluir un pequeño programa cliente 54 que se ejecuta en el dispositivo de red y que, entre otras cosas, realiza algunas funciones de prevención y de detección de fraude y genera la huella digital de dispositivo de red según la invención como se describe posteriormente.

Según la invención, cada paquete de software de cliente incluye un pequeño elemento de software que realiza una parte de un procedimiento de registro de dispositivo red (NDRM) común que se describe con mayor detalle posteriormente con referencia a la Figura 7. En el ejemplo mostrado en la Figura 1, cada ordenador central representa un entorno de red privada diferente utilizado por organizaciones independientes que no comparten identidades de usuario final. También en este ejemplo, la NDRD centralizada 30 utilizada por cada ordenador central está ubicada de forma remota en el servidor de detección de fraude 26 y es un servicio proporcionado por un tercero. Los expertos en la técnica apreciarán que el NDRM puede implementarse de varias maneras diferentes que están dentro del alcance de esta invención. Por ejemplo, el NDRM puede estar distribuido a través de una pluralidad de dispositivos informáticos (sin ningún servidor central de detección de fraude 26 y ninguna NDRD central), donde cada dispositivo informático, tales como una combinación de los dispositivos de red y de proveedores de servicios de red, realiza parte de las funciones del sistema de prevención y de detección de fraude según la invención. Como alternativa, el NDRM puede estar incluido en una aplicación personalizada, integrado en la aplicación del navegador u otra aplicación/aplicaciones común(es) o en el firmware. Además, el NDRM puede ser una aplicación independiente o ejecutarse de forma remota, y todos estos ejemplos del NDRM están dentro del alcance de la invención. Además, el NDRM puede ejecutarse antes, después y/o durante la conexión a una red o a intervalos periódicos, donde todas las combinaciones de esto están dentro del alcance de la invención.

El NDRM según la invención puede personalizarse para diferentes tipos de dispositivos de red. Por ejemplo, con un ordenador personal que se conecta a un NSP, el NDRM puede utilizar el NDI y la NDF para identificar el dispositivo de red. Con un teléfono celular, normalmente es posible extraer datos del teléfono celular, tal como su número de serie, de modo que una NDF sólo puede utilizarse para identificar el dispositivo de red de telefonía celular. En cuanto a un dispositivo de red de tipo asistente personal digital (PDA), normalmente es posible introducir datos/información en el PDA solamente para que el NDI pueda utilizarse para identificar el PDA. Como otro ejemplo, un PC que utiliza Linux necesitará un cliente diferente al de un PC basado en Windows. Según la invención, el NDRM también se puede llevar a la práctica en una situación en la que puede usarse un dispositivo de hardware, tal como una tarjeta inteligente o una tarjeta PCMCIA, con un módulo cliente contra el fraude precargado en la tarjeta, donde la tarjeta tiene su propio identificador único que puede utilizarse para identificar de manera única la tarjeta. Por lo tanto, el NDRM según la invención puede implementarse de varias maneras diferentes. A continuación se describirán más detalles de un proveedor de servicios de red (NSP) a modo de ejemplo.

La Figura 3 es un diagrama que ilustra un ejemplo de un proveedor de servicios de red 24 según la invención. En este ejemplo, el proveedor de servicios de red puede ser uno o más ordenadores de tipo servidor basado en web, tal como un servidor web, un servidor de aplicaciones, un servidor de base de datos, etc., que son capaces de comunicarse con un dispositivo de red a través una red de comunicaciones, tales como Internet o una red inalámbrica, y son capaces de descargar páginas web o una aplicación de software en el dispositivo de red. El proveedor de servicios de red 24 comprende en este ejemplo uno o más procesadores 60, uno o más dispositivos de almacenamiento persistente 62, tales como los descritos anteriormente, y una memoria 64, tal como se describió anteriormente. Para que el proveedor de servicios de red 24 proporcione los servicios a los dispositivos de red, la memoria puede almacenar (y el/los procesador(es) puede(n) ejecutar) un sistema operativo de servidor 64 y un sistema de software de procesamiento de transacciones 68 para facilitar una transacción electrónica entre el proveedor de servicios de red 24 y uno o más dispositivos de red. Por ejemplo, el procesador de transacciones puede procesar apuestas en un sitio de juegos de azar o compras en un sitio de comercio electrónico. El proveedor de servicios de red 24 puede comprender además un paquete de software cliente 70 que se almacena en el proveedor de servicios de red y que después se descarga en cada dispositivo de red que quiera llevar a cabo una transacción con el proveedor de servicios de red particular. Por ejemplo, el paquete de software cliente puede ser un juego de mesa virtual de póquer, un juego de blackjack virtual, una máquina tragaperras virtual, una interfaz de usuario de comercio electrónico, etc. Según la invención, cada paquete de software cliente puede incluir un módulo cliente de detección de fraude 72 (que puede ser, preferiblemente, una pluralidad de líneas de código y datos) que

es ejecutado por cada dispositivo de red para implementar el sistema de prevención y de detección de fraude en este ejemplo. Cada proveedor de servicios de red 24 puede comprender además una base de datos 74, tal como un servidor de base de datos o una estructura de datos almacenada en la memoria del proveedor de servicios de red, que almacena los datos de transacciones electrónicas ampliamente conocidos para el proveedor de servicios de red. En una forma de realización utilizada como ejemplo, el sistema utiliza un cliente de detección de fraude 72 integrado. En una implementación del sistema, el cliente está integrado en una aplicación de software propietaria, por ejemplo para que el cliente pueda estar incluido dentro de un programa distribuido por un proveedor de servicios de red que se debe utilizar para conectarse a la red. En otra forma de realización, el cliente también puede suministrarse a través de una aplicación independiente, estar integrado en un producto de software común, tal como un navegador web, o incluso estar integrado en hardware o memoria, siendo necesario que, de cualquiera de las maneras, esté en ejecución cuando se autentica una conexión a una red mediante un proveedor de servicios de red protegido por este sistema. En otra forma de realización, el cliente también podría suministrarse bajo demanda, a través de JavaScript, un control ActiveX u otra tecnología similar cuando un usuario se conecta a un proveedor de servicios de red a través de su navegador web favorito. Según la invención, el sistema puede implementarse sin ningún cliente en el dispositivo de red. Por ejemplo, en un sistema de pedidos telefónico o por correo, el sistema puede establecer un identificador único del usuario en base a un número de teléfono mediante el cual el operador de venta por correo puede llamar al usuario para verificar ese número de teléfono y luego usar ese número de teléfono como identificador único del usuario. En este caso, el sistema utiliza una NDF (el número de teléfono). Después, según la invención, el número de teléfono puede almacenarse en la base de datos y después usarse como se describe posteriormente.

Por tanto, según la invención, el cliente 72, para el dispositivo en el que está instalado, determina el estado del dispositivo (puesto que ya tiene un identificador único, o no) y controla la conexión del dispositivo al proveedor de servicios de red. El proveedor de servicios de red controla cada dispositivo y/o el acceso de cada usuario a los recursos del proveedor de servicios de red, por ejemplo denegando el acceso a un usuario o dispositivo, tal como se describe posteriormente. Por lo tanto, el proveedor de servicios de red utiliza el estado de dispositivo/usuario proporcionado por el cliente con el fin de controlar eficazmente la seguridad de la red y evitar el fraude. A continuación se describirá un ejemplo del servidor de detección de fraude.

La Figura 4 es un diagrama que ilustra un ejemplo del servidor de detección de fraude 26 según la invención. En este ejemplo, el servidor de detección de fraude 26 es un recurso informático independiente, tal como un ordenador de tipo servidor, con la NDRD 30, aunque las funciones del servidor de detección de fraude 26 y la NDRD 30 pueden estar distribuidas, como se ha descrito anteriormente. El servidor de detección de fraude 26 puede incluir uno o más procesadores 80, uno o más dispositivos de almacenamiento persistente 82, como los descritos anteriormente, y una memoria 84, como se describió anteriormente. El servidor de detección de fraude puede incluir además un servidor/gestor de base de datos 86 que almacena la NDRD 30 según la invención. La estructura y el funcionamiento del procesador, del dispositivo de almacenamiento persistente y de la memoria se han descrito anteriormente. La memoria puede almacenar un sistema operativo de servidor 88, un módulo de software de administración 90, un módulo de software de detección de fraude 92, un módulo de software de informes 94 y un módulo de software de etiquetado 96, donde cada módulo comprende una pluralidad de instrucciones (y datos asociados) que son ejecutados por el procesador para implementar el sistema de prevención y detección de fraude. Según la invención, el cliente 72 descargado en el dispositivo puede realizar el "etiquetado" de cada dispositivo, donde el cliente puede determinar si el dispositivo ya tiene un identificador único del servidor 26 o si solicitará un nuevo identificador único. El sistema operativo del servidor es ampliamente conocido. El módulo de administración 90, en una forma de realización preferida, puede generar páginas web de administración que permiten al usuario del sistema de prevención y de detección de fraude interactuar con el sistema usando las páginas web y configurar el sistema. Por ejemplo, las páginas web de administración pueden permitir al usuario configurar elementos del sistema, ajustar elementos de consulta y actualizar elementos. En la configuración de los elementos del sistema, el usuario puede activar/desactivar la verificación maestra, donde el estado desactivo siempre aceptará que un nuevo dispositivo de usuario o de red acceda a la red. El usuario también puede configurar el número máximo de usuarios (nombres de usuario diferentes, distintos) que pueden compartir un determinado dispositivo de red/resultados y el número máximo de dispositivos de red que un solo usuario puede utilizar. Si se excede el umbral máximo antes establecido y la verificación maestra está activada, entonces el sistema de prevención y de detección de fraude puede restringir el acceso para el dispositivo de red o usuario que haya superado los valores umbral. El usuario también puede establecer si un estado de cada usuario de un proveedor de servicios de red particular puede influir en las operaciones de detección de fraude, tal como permitir la creación de cuentas, permitir el inicio de sesión, permitir un depósito en una cuenta o permitir abandonar una cuenta. El módulo de administración también permite al usuario configurar los elementos de consulta que extraen información de la base de datos del sistema de prevención y detección de fraude. Por ejemplo, el usuario puede generar una consulta de, dado un dispositivo de red particular, qué usuarios han usado ese dispositivo de red o una consulta que solicita, dado un usuario particular, qué dispositivos de red han sido utilizados por el usuario particular. El usuario también puede configurar una consulta que solicita, dado un dispositivo de red particular, qué otros proveedores de servicios de red configuraron este dispositivo de red para asociar usuarios/ordenadores a un número predeterminado de niveles de profundidad o, dado un usuario en particular, cuál es el estado actual de ese usuario en el sistema. El módulo de administración también permite la configuración de los elementos de actualización. Por ejemplo, el usuario puede establecer que siempre se acepte que un dispositivo de red particular acceda al sistema, establecer que un determinado dispositivo

de red sea aceptado en el sistema, establecer que un determinado dispositivo de red sea atrapado por el sistema (para determinar además las intenciones del dispositivo de red), establecer que un determinado dispositivo de red debe sea rechazado por el sistema o establecer que un usuario dado sea siempre aceptado por el sistema (por ejemplo, todos los dispositivos de red asociados al usuario siempre serán aceptados). El usuario también puede establecer que un usuario dado sea aceptado durante un intervalo predeterminado o un intento de acceso predeterminado (los dispositivos de red asociados al usuario son aceptados), establecer que un usuario dado (y todos los dispositivos de red asociados al usuario) sean atrapados o establecer que un usuario dado (y todos los dispositivos de red asociados al usuario) sean rechazados. Los ordenadores centrales pueden fijar cualquier número de niveles de estado de dispositivo y de usuario, y establecer cualquier número de patrones de comportamiento, cada uno de los cuales podría requerir una acción diferente, tales como notificar una dirección de correo electrónico particular, localizar un número particular, denegar el acceso a la red, permitir el acceso pero cambiar el estado del dispositivo, etc.

El módulo de software de informes 94 permite a un usuario configurar y generar informes acerca del sistema de prevención y de detección de fraude y su base de datos. Por ejemplo, el sistema puede generar un informe que muestra un informe de cambios diario (con una lista de los dispositivos de red cuyo estado ha cambiado), un informe de fraude de terceros que enumera los dispositivos de red que otros proveedores de servicios de red conocen y su estado, o un informe de ordenadores compartidos que enumera todos los dispositivos de red que tienen varias cuentas de usuario asociadas a los mismos. El módulo de informes también puede generar un informe de múltiples ordenadores que enumera los usuarios que han utilizado varios dispositivos de red y los dispositivos de red utilizados por cada usuario, y un informe de uso que enumera el número de consultas de administrador, actualizaciones de administrador, consultas de la API y el número de dispositivos de red que están siendo rastreados por el sistema de detección de fraude. El módulo de software de detección de fraude 92 contiene las instrucciones y la lógica, en base a los datos de los dispositivos de red y los usuarios, para determinar el estado apropiado de un dispositivo de usuario/red particular y su estado de acceso en el sistema de transacciones electrónicas. Según la invención, cada proveedor de servicios de red puede establecer sus propias reglas de estado. Por ejemplo, un proveedor de servicios de red particular puede establecer un "Sí" o un "No" para la conexión con el proveedor de servicios de red. Como otro ejemplo, un proveedor de servicios de red particular puede tener un estado "Sí para conectarse, pero generar una puntuación para el dispositivo de red particular", o un estado "Sí, pero capturar la información acerca del dispositivo de red". Posteriormente se describirá con más detalle la lógica de detección de fraude.

El módulo de software de etiquetado 96 contiene la variedad de software, lógica y datos para identificar de manera única cada dispositivo de red (generar el identificador para un dispositivo de red particular) que está estableciendo una conexión con el sistema de transacciones electrónicas. La conexión con el sistema puede incluir, pero sin limitarse a, una conexión inicial con la red, una configuración de cuenta, un inicio de sesión, un cambio en la información de cuenta, un depósito, un reintegro, una compra, una conexión totalmente aleatoria a la red, etc. Según la invención, el procedimiento real para el etiquetado de cada dispositivo de red puede variar, como se describe posteriormente. Según la invención, cada dispositivo de red se identifica de manera única de forma que se hace un seguimiento de cada dispositivo en el sistema, incluso cuando un usuario diferente inicia sesión en un ordenador central con el mismo dispositivo de red. El etiquetado de dispositivos de red individuales permite que el sistema de detección de fraude deniegue el acceso a un ordenador central a un usuario particular (independientemente del dispositivo de red que se utilice), a un dispositivo de red particular (independientemente del usuario que esté utilizando el dispositivo de red), a la combinación de un usuario particular con un dispositivo de red particular, o a cualquier combinación de usuarios y dispositivos. A continuación se describirán con más detalle ejemplos de la base de datos de usuario en cada proveedor de servicios de red y la base de datos de registro de dispositivos de red del sistema de detección de fraude.

La Figura 5 ilustra ejemplos de una parte de una base de datos 100_1, 100_2, 100_3, 100_4 para cada proveedor de servicios de red (NSP 1, NSP 2, NSP 3 y NSP 4) en un sistema de transacciones electrónicas que tiene cuatro proveedores de servicios de red. Según la invención, la información contenida en estas bases de datos se reenvía al sistema de detección de fraude para que el sistema de detección de fraude pueda distinguir los usuarios de cada proveedor de servicios de red con respecto a los usuarios de otros proveedores de servicios de red. Cada proveedor de servicios de red tiene un identificador de cuenta de usuario final (EAI), tales como EA_{11} - EAI_{n1}, EAI_{12} - EAI_{n2}, EAI_{13} - EAI_{n3} y EAI_{14} - EAI_{n4}. En este ejemplo, NSP 1, NSP 2 y NSP 3 usan un EAI individual que no proporciona ninguna información acerca de la cuenta del usuario, mientras que NSP 4 utiliza el ID de usuario real del usuario final ("Tim1" y "Smurf") como EAI. Todo lo que el sistema de fraude necesita es que cada ordenador central proporcione un EAI que tenga una relación directa con una cuenta única en ese ordenador central.

La Figura 6 es un diagrama que ilustra un ejemplo de una base de datos de registro de dispositivo de red rellenada 110. En este ejemplo, la base de datos es una tabla de base de datos que contiene la información pertinente. Sin embargo, los datos pueden almacenarse en diferentes bases de datos y diferentes estructuras de datos de base de datos que estén dentro del alcance de esta invención. En este ejemplo, la NDRD 110 puede incluir una columna de ordenador central 112, una columna de EAI 114 y una columna de identificador de dispositivo de red (NDI) 116 que permite al sistema de detección de fraude asociar un ordenador central particular a un usuario particular y a un dispositivo de red particular. Como se describió anteriormente, los EAI representan cuentas de usuario final que son

únicos para cada ordenador central. Los identificadores de dispositivo de red (NDI) representan dispositivos de red únicos que se han conectado a al menos un ordenador central. Las filas individuales de la tabla de base de datos representan combinaciones únicas de ordenador central, EAI y NDI. Por ejemplo, una primera fila 118 que representa un EAI_{11} para el ordenador $central_1$ a partir del NDI_1 representa una cuenta procedente de un dispositivo específico (NDI) y que intenta conectarse al ordenador central 1. Si esta misma cuenta se conectase al ordenador central 1 desde un dispositivo diferente, se creará una nueva fila 120, por ejemplo EAI_{11} para el ordenador $central_1$ a partir del NDI_2, de modo que el acceso por parte del mismo usuario a través de dos dispositivos de red diferentes es rastreado y registrado en el sistema. Si el usuario final representado por el EAI_{11} en el ordenador $central_1$ tiene una cuenta en el ordenador $central_2$ (mostrado como EAI_{12} ya que cada ordenador central tiene sus propios EAI únicos) y se conecta al ordenador $central_2$ a partir del NDI_2, se creará una nueva entrada 122, tal como el EAI_{12} para el ordenador $central_2$ con el NDI_2, de modo que el mismo usuario que se conecta a un proveedor de servicios de red diferente con el mismo dispositivo de red es rastreado y registrado en el sistema de fraude. Puede mantenerse una gran cantidad de información adicional, tal como la fecha y hora del último inicio de sesión con éxito, la fecha y hora del último inicio de sesión fallido, los inicios de sesión con éxito totales, los inicios de sesión fallidos totales, etc. A continuación se describe con mayor detalle un procedimiento para el registro de dispositivos de red según la invención.

La Figura 7 es un procedimiento 130 para etiquetar un dispositivo de red (procedimiento de registro de dispositivo de red) según la invención. El procedimiento logra el objetivo de identificar de manera única cada dispositivo de red que se conecta al sistema de transacciones electrónicas que el sistema de prevención y de detección de fraude está vigilando. Idealmente, este procedimiento se lleva a cabo cada vez que un dispositivo se conecta a un ordenador central protegido por este sistema, y también puede llevarse a cabo en varios puntos e intervalos a lo largo de una sesión. Por ejemplo, el sistema puede realizar periódicamente el procedimiento para comprobar periódicamente cada dispositivo conectado a la red. Por lo tanto, en la etapa 132, el procedimiento determina si el dispositivo de red es nuevo (por ejemplo, si el dispositivo de red ya está registrado en la NDRD y ya tiene asignado un identificador único). Si el dispositivo de red es nuevo y no tiene una huella digital única, entonces, en la etapa 134, el procedimiento genera una huella digital única (etiqueta) para el dispositivo de red. La huella digital única puede ser generada por el programa cliente 54 en cada dispositivo de red (en el ejemplo mostrado en la Figura 2) o por otros medios, tales como el servidor de detección de fraude 26 que genera una huella digital para cada dispositivo de red basándose en información recibida desde el dispositivo de red o cualquier combinación. La huella digital única se almacena después en la base de datos en la etapa 136 y el procedimiento se completa de modo que cada dispositivo de red único en el sistema es identificado de manera única.

Por lo tanto, cuando un dispositivo de red intenta conectarse a una red por primera vez, el procedimiento garantiza que el dispositivo está registrado (y por tanto, rastreado) al menos de dos maneras diferentes. En primer lugar, el procedimiento solicita un identificador de dispositivo de red (NDI) único a partir de la NDRD 30 a través del ordenador central. El procedimiento almacena de manera fehaciente el NDI cifrado en al menos dos elementos; por ejemplo, la parte A en el registro y la Parte B en un archivo. Los NDI son distribuidos por la NDRD y se garantiza que sean únicos. El procedimiento también genera una huella digital de dispositivo de red (NDF) para cada dispositivo recopilando discretamente información acerca del dispositivo, como los números de serie de hardware, los números de serie de software, fechas de instalación y otra información, y envía la NDF resultante a la NDRD a través del ordenador central (el proveedor de servicios de red). Aunque no se garantiza que los componentes individuales de una NDF sean únicos, el aumento del tamaño de la NDF o del número de elementos de información utilizados para crear la NDF aumenta la probabilidad de que la NDF resultante sea única y aumenta su valor para su identificación positiva. Según la invención, la combinación del NDI y la NDF es única y permite que cada dispositivo de red se identifique de manera única. Por lo tanto, el NDI mostrado en la Figura 6 incluye la NDF ya que la combinación identificará de manera única un dispositivo de red.

La metodología exacta para el registro de un dispositivo no es crítica, siempre que identifique de manera única los dispositivos con una probabilidad extremadamente alta. Por ejemplo, diversos procedimientos para identificar dispositivos de manera única pueden ser ligeramente diferentes para adaptar aspectos únicos de clientes ligeros, ordenadores de mano, teléfonos celulares, terminales de juego y otros tipos de dispositivos. Según la invención, el programa cliente 54 puede recopilar información para cada dispositivo de red con el fin de generar la NDF. Es muy probable que los ordenadores centrales que utilizan este sistema puedan distribuir un procedimiento de registro común de diferentes maneras, dependiendo de las características de usuario final y las plataformas típicas usadas para conectarse a su red, o incluso ejecutar el procedimiento de registro de forma remota.

Además de facilitar la comunicación entre el NDRM y la NDRD, el ordenador central de tipo proveedor de servicios de red también transmite un identificador de cuenta de usuario final (EAI) a la NDRD asociada a la cuenta específica de usuario final que está intentando acceder/conectarse al proveedor de servicios de red. Este identificador puede ser un número de cuenta de cliente u otro valor único asociado a una cuenta de usuario final específica que no se utiliza en el sistema de ordenador central para ningún otro propósito. Dependiendo de la relación comercial entre el ordenador central y el proveedor de servicios NDRM, la información real del consumidor puede registrarse o no. Sin embargo, el que se proporcione o no información real de un consumidor no cambia sustancialmente el proceso. Según la invención, la NDRD realiza un seguimiento de cada dispositivo de red (que tenga un NDI único) que trata de conectarse a un ordenador central, junto con su NDF correspondiente. La NDRD también mantiene una

asociación para cada EAI que se conecta desde cada dispositivo de red único. La NDRD también rastrea información tal como la primera conexión, la última conexión, las conexiones totales, la última conexión fallida, las conexiones totales fallidas, el estado de NDI por ordenador central y el estado de NDF por ordenador central. Según la invención, el sistema puede utilizar el NDI, la NDF, la combinación del NDI y la NDF u otra información con el fin de validar un usuario/dispositivo. Por ejemplo, la otra información puede ser un número de serie de un teléfono celular. A continuación se describirá con mayor detalle un ejemplo del esquema de base de datos preferido del sistema de detección de fraude.

La Figura 8A es un diagrama que ilustra las tablas de base de datos relacional para un ejemplo de una forma de realización preferida de un esquema de base de datos 140 (para el producto ieSnare de Iovation, inc.) para un sistema de detección de fraude según la invención, y las Figuras 8B a 8E son diagramas que ilustran detalles adicionales de las tablas de base de datos mostradas en la Figura 8A. Como se muestra en la Figura 8A, el esquema de base de datos 140 puede incluir una pluralidad de tablas de base de datos que incluye una tabla SNARE_USER_TOKEN_ACTIVITY 141, una tabla SNARE_USER_TOKEN 142, una tabla SNARE_USER 143, una tabla SNARE_AFFILIATE 144, una tabla SNARE_SOAPD_AUDIT 145, una tabla SNARE_ACTIVITY_TYPE 146, una tabla SNARE_TOKEN_ACTIVITY 147, una tabla SNARE_TOKEN 148, una tabla SNARE_TOKEN_NUID 149, una tabla SNARE_AFFIL_TOKEN 150 y una tabla SNARE_TOKEN_STATUS 151 que están vinculadas entre sí por al menos una clave primaria, tal como SNARE_USR_TKN_2_USR_TKN_ACT_FK, como se muestra. Las diversas claves primarias entre cada tabla en el esquema de base de datos no se describen aquí, pero aparecen en la figura 8A. En estas tablas de bases de datos, la variable TOKEN corresponde al NDI descrito en otra parte de este documento, y la variable NUID corresponde a la NDF descrita en otra parte de este documento.

La Figura 8B ilustra más detalles de la tabla SNARE_USER_TOKEN 142 y de la tabla SNARE_USER_TOKEN_ACTIVITY 141 junto con una tabla SNARE_TOKEN_NUID_HIST 152 y una tabla SNARE_AFFIL_TOKEN_HIST 153 que no se muestran en la Figura 8A. Como se muestra en la Figura 8B, se muestra cada campo de datos 154 de cada tabla, donde cada campo de datos contiene varias características, tales como el tipo de datos almacenados en el campo, etc. Según la invención, cada usuario del sistema puede tener una o más credenciales (identificadores) que se almacenan en la tabla SNARE_USER_TOKEN 142, y cualquier evento relacionado con una credencial particular de un usuario particular se almacena en la tabla SNARE_USER_TOKEN_ACTIVITY 141. Las tablas HIST 152, 153 contienen datos históricos acerca de las credenciales y las credenciales de afiliación. La Figura 8C ilustra más detalles de la tabla SNARE_USER 143 (que contiene datos sobre cada usuario del sistema), la tabla SNARE_SOAPD_AUDIT 145 (que contiene información de depuración del sistema) y la tabla SNARE_AFFIL_TOKEN 150 que contiene la una o más credenciales (identificadores) para cada afiliado del sistema, donde el afiliado es un proveedor de servicios de red particular. La Figura 8D ilustra más detalles de la tabla SNARE_AFFILIATE 144 (que contiene datos acerca de cada afiliado asociado al sistema), la tabla SNARE_TOKEN_ACTIVITY 147 (que contiene datos acerca de cualquier evento relacionado con una credencial particular) y la tabla SNARE_TOKEN_NUID 149, que contiene datos acerca de la huella digital para un dispositivo de red para un dispositivo con una credencial / un NDI particular. Finalmente, la Figura 8E ilustra más detalles de la tabla SNARE_ACTIVITY_TYPE 146 (que contiene datos acerca de cada actividad rastreable única/distinta que se produce en el sistema), la tabla SNARE_TOKEN 148 (que contiene datos acerca de cada credencial almacenada en el sistema) y la tabla SNARE_TOKEN_STATUS 151, que contiene estados únicos/distintos para cada credencial en el sistema.

Las Figuras 9A y 9B son un diagrama de flujo que ilustra un procedimiento preferido 200 para la validación de un dispositivo y una correlación dispositivo/cuenta, donde un ordenador central está usando el sistema de prevención y detección de fraude según la invención. Las Figuras 9C a 9F ilustran procedimientos para la validación de un nuevo usuario/dispositivo y de un usuario/dispositivo existente según la invención. Las etapas descritas posteriormente pueden implementarse mediante instrucciones de ordenador en un módulo de software ejecutado por un ordenador central particular de un proveedor de servicios de red o mediante instrucciones de ordenador en un módulo de software ejecutado por el servidor de detección de fraude. La invención no está limitada a ninguna ubicación particular de las instrucciones de ordenador que implementan el procedimiento de validación. En funcionamiento, antes de que una cuenta (un dispositivo de red particular con un identificador de cuenta de usuario final particular) esté autorizada por un ordenador central particular (proveedor de servicios de red), una serie de etapas de validación se producen cada vez. Si el dispositivo de red particular o la correlación dispositivo/cuenta que está probándose no satisface ninguna de las etapas de validación descritas a continuación, la validación se aborta y se impide que el dispositivo/cuenta acceda al ordenador central particular. Las etapas de validación pueden ser iniciadas por ordenadores centrales en cualquier número de puntos de interacción con el consumidor, incluyendo, pero sin limitarse a, una conexión inicial con la red, una configuración de cuenta, un inicio de sesión, un cambio en la información de cuenta, un depósito, un reintegro, una compra, una conexión totalmente aleatoria con la red, etc. En más detalle, en la etapa 202, se determina si el identificador de dispositivo de red (NDI) es válido. Con más detalle, el NDI no debe aparecer modificado, con el valor emitido originalmente por la NDRD, y no parecer que ha iniciado sesión actualmente en el mismo ordenador central. A un NDI no válido no se le permitirá conectarse al ordenador central, como se muestra en la etapa 203. Si el NDI es válido, entonces, en la etapa 204, se determina si el par NDI / huella digital de dispositivo de red (NDF) coinciden. En particular, la NDF proporcionada en el inicio de sesión debe coincidir con el valor de NDF asociado originalmente con el NDI del dispositivo de red que trata de conectarse al ordenador central. Sin embargo, se permite un cierto cambio en la NDF. Por ejemplo, una 'variación de NDF' debe

considerarse como elementos individuales que se utilizan para calcular una NDF que puede cambiar con el tiempo. Generalmente, elementos adicionales no presentes en la NDF original, tales como un nuevo elemento de software o hardware que se ha instalado, no son preocupantes. En estos casos, la NDF se actualiza y los cambios se anotan. Sin embargo, cambios en los valores de NDF individuales existentes son más preocupantes. Según la invención, cada ordenador central puede establecer reglas para la variación del sistema y que uno o más elementos de la NDF perciben como críticas y, por lo tanto, no deben ser modificadas sin generar un mensaje de excepción/error. Por ejemplo, el número de serie de la unidad central de procesamiento puede ser considerado crítico y, por tanto, se generará un mensaje de error (un par NDI/NDF incompatible), mientras que un cambio en la cantidad de memoria en el dispositivo de red no puede causar por sí solo un par NDI/NDF incompatible. Como otro ejemplo, varios elementos no críticos del dispositivo de red pueden ser modificados, pero se seguirá considerando que el par NDF/NDI coincide. Así, dependiendo de las reglas establecidas y mantenidas por cada ordenador central, puede considerarse que un par NDI/NDF no coincide y no se le permite conectarse al ordenador central en la etapa 203.

En la etapa 206, si el par NDI/NDF coincide, se determina si el estado de NDI es aceptable para el ordenador central particular. En particular, un dispositivo de red individual puede conectarse a varias redes protegidas por este sistema y, por lo tanto, el NDI particular puede estar asociado a varios ordenadores centrales. Según la invención, cada NDI tiene un estado para cada ordenador central que usa la NDRD, y cada ordenador central define cualquier número de estados para los NDI. Cuando un dispositivo de red está intentando conectarse al ordenador central 1, la NDRD sigue cualquier regla asociada al estado de NDI para el ordenador central 1. Por ejemplo, el ordenador central 1 puede establecer solamente dos niveles de estado, uno para permitir el acceso y uno para denegar el acceso. El ordenador central 2 puede establecer un único conjunto de varios niveles de estado, donde cada estado tiene un conjunto diferente de criterios y donde cada estado determina a qué área de su red puede acceder un dispositivo/una cuenta. El ordenador central 3 puede tener varios conjuntos de estados, donde el conjunto 1 se aplica a la conexión con la red, el conjunto 2 se aplica para acceder a diversas áreas de la red, y el conjunto 3 se aplica a diversas actividades en la red (tal como establecer una nueva cuenta, cambiar la información de una cuenta, compras, etc.) y donde cada estado tiene un único criterio establecido y mantenido por el ordenador central 3. Si el estado de NDI no es aceptable para el ordenador central particular, el procedimiento se interrumpe en la etapa 203 y se deniega el acceso. En la etapa 208, si el estado de NDI es aceptable para el ordenador central, se determina si el estado de NDF para el dispositivo de red particular es aceptable para el ordenador central particular. En particular, cada NDF tiene también un estado para cada ordenador central que usa la NDRD, y cada ordenador central define cualquier número de estados para las NDF. Cuando un dispositivo de red está intentando conectarse al ordenador central 1, la NDRD sigue cualquier regla asociada al estado de NDF para el ordenador central 1. Al igual que con los niveles de estado y las reglas asociadas de los NDI, los ordenadores centrales pueden establecer cualquier número de niveles de estado para NDF apropiadas a su fin. Si el estado de NDF no es aceptable para el ordenador central particular, el procedimiento se interrumpe en la etapa 203 y se deniega el acceso. Estas dos etapas (206, 208) son una línea de defensa contra los piratas informáticos que eliminan todo rastro de los NDI e intentan conectarse a una red protegida. En casos extremos, un nuevo NDI podría ser emitido a un dispositivo de red, pero el acceso a la red podría aún denegarse en función del estado de la NDF controlada por cada ordenador central, tanto de forma manual como por las reglas establecidas con la NDRD.

En la etapa 210, si el estado de NDF para el dispositivo de red es aceptable para el ordenador central particular, se determina si el estado de NDI para el dispositivo de red particular es aceptable para cualquier otro ordenador central identificado como de confianza por el ordenador central particular. En particular, dispositivos de red individuales pueden conectarse a varias redes protegidas por este sistema y, por lo tanto, el NDI puede estar asociado a varios ordenadores centrales. Al tratar de conectarse al ordenador central 1, el estado de NDI del ordenador central 1 puede ser válido, mientras que el estado de NDI para otros ordenadores centrales está marcado como 'malo'. Según la invención, cada ordenador central puede identificar otros ordenadores centrales que son 'de confianza', por lo que si el estado de NDI es 'malo' para cualquier otro ordenador central de confianza, el acceso a la red se denegará independientemente del estado de NDI para el ordenador central 1. Esta etapa evita el fraude por un usuario que pueda tener un estado malo en un primer proveedor de servicios de red, pero no en un segundo proveedor de servicios de red y, por lo tanto, comparte información acerca de un dispositivo de red "malo" identificado por un NDI particular. Si el estado de NDI no es aceptable para ningún ordenador central de confianza, el procedimiento se interrumpe en la etapa 203 y se deniega el acceso.

En la etapa 212, si el NDI es aceptable para todos los ordenadores centrales de confianza, se determina si el estado de NDF es aceptable para cualquier otro ordenador central considerado como "de confianza" por el ordenador central particular. En particular, dispositivos de red individuales pueden conectarse a varias redes protegidas por este sistema y, por lo tanto, una NDF particular puede estar asociada a varios ordenadores centrales. Al tratar de conectarse al ordenador central 1, el estado de NDF del ordenador central 1 puede ser válido, mientras que el estado de NDF para otros ordenadores centrales está marcado como 'malo'. Cada ordenador central puede identificar otros ordenadores centrales que son 'de confianza', por lo que si el estado de NDF es 'malo' para cualquier otro ordenador central de confianza, el acceso a la red se denegará independientemente del estado de NDI para el ordenador central 1. Esta etapa comparte información acerca de los estados de NDF de dispositivos de red a través del sistema de transacciones electrónicas. Si la NDF del dispositivo de red particular no es aceptable para un ordenador central de confianza, a la cuenta con la NDF se le niega el acceso. En la etapa 214, si la NDF es aceptable para todos los ordenadores centrales de confianza, entonces se determina si el número de identificadores

de cuenta de usuario final (EAI) por NDI está dentro del intervalo aceptable para el ordenador central particular. En particular, cada ordenador central establece reglas para la pluralidad de EAI permitidos por NDI o, dicho de otro modo, la pluralidad de usuarios que pueden utilizar un dispositivo de red individual. Por ejemplo, el ordenador central 1 puede no estar preocupado por 3, o menos, cuentas procedentes de un PC individual, puede que quiera ser advertido acerca de 4-6 cuentas procedentes de un PC, y puede desear denegar el acceso a red a cualquier intento de inicio de sesión en el que 7 o más cuentas procedan del mismo PC. Para cada conjunto de reglas pueden introducirse diferentes niveles de preocupación y diferentes remedios (ninguna acción, advertencia o denegación de acceso), y los niveles particulares de preocupación y remedios pueden ajustarse por cada ordenador central según la invención. Como otro ejemplo, otro ordenador central puede permitir solamente una cuenta por dispositivo de red y denegar el acceso a cualquier intento de inicio de sesión en el que más de una cuenta haya tratado de conectarse desde el mismo dispositivo de red.

En la etapa 216 se determina si el número de NDI por cada EAI está dentro del intervalo aceptable para el ordenador central particular. En particular, cada ordenador central también establece reglas para la pluralidad de NDI a partir de los cuales cada EAI está autorizado a conectarse o, dicho de otro modo, la pluralidad de dispositivos de red diferentes a partir de los cuales una cuenta individual está autorizada a conectarse. Por ejemplo, el ordenador central 1 puede no estar preocupado por una cuenta que procede de 5, o menos, PC, puede que quiera ser avisado de una cuenta que utiliza entre 6 y 10 PC, y puede desear denegar el acceso a red a cualquier inicio de sesión que haya intentado conectarse desde 11 o más PC. Otro ordenador central puede permitir solamente una cuenta por PC y denegar el acceso a cualquier intento de inicio de sesión procedente de un segundo dispositivo de red. Por lo tanto, estos niveles de preocupación y remedios pueden ajustarse por cada ordenador central según la invención. En la etapa 218, la cuenta identificada por el par de NDI y EAI particular (que ha superado todas las pruebas descritas anteriormente) puede acceder al sistema del proveedor de servicios de red particular, y los datos acerca de la transacción/conexión se introducen en la NDRD.

Las Figuras 9C y 9D son un diagrama de flujo que ilustra un procedimiento preferido 220 para la validación de un nuevo usuario/dispositivo usando el sistema de prevención y detección de fraude según la invención. Las etapas descritas posteriormente pueden implementarse mediante instrucciones de ordenador en un módulo de software ejecutado por un ordenador central particular de un proveedor de servicios de red o mediante instrucciones de ordenador en un módulo de software ejecutado por el servidor de detección de fraude. La invención no está limitada a ninguna ubicación particular de las instrucciones de ordenador que implementan el procedimiento de validación. En la etapa 222, un usuario inicia una aplicación (después de descargar la aplicación desde el proveedor de servicios de red en la forma de realización en la que el cliente está integrado en una aplicación) y la aplicación inicia automáticamente el cliente. En la etapa 224, el cliente determina si el dispositivo está registrado con el sistema de detección de fraude. Si el dispositivo ya está registrado, entonces el procedimiento finaliza y el procedimiento para la validación de un usuario existente se describe en las Figuras 9E y 9F. Si el cliente no detecta que el dispositivo ya está registrado, entonces, en la etapa 226, el cliente solicita un nuevo NDI (identificador/credencial/número de serie) desde el proveedor de servicios de red, que reenvía la solicitud al servidor de detección de fraude 26. El servidor genera un NDI único y lo pasa al proveedor de servicios de red que, posteriormente, reenvía el NDI al cliente. Después, el cliente almacena el NDI en su disco y en su registro. En la etapa 228, el cliente recopila datos del dispositivo, genera una NDF y reenvía esa NDF al proveedor de servicios de red. En la etapa 230, el proveedor de servicios de red reenvía la NDF al servidor que almacena la NDF y comprueba la NDF con datos de NDF existentes para el estado de la NDF particular.

En la etapa 232, el servidor determina si la NDF está duplicada, tal como si un pirata informático hubiera eliminado el NDI anterior en el dispositivo, pero la NDF era idéntica a una NDF existente. Si hay una NDF duplicada, entonces el proveedor de servicios de red es notificado en la etapa 234 y la sesión de usuario finaliza. En la etapa 236, si la NDF no está duplicada (lo que indica un nuevo dispositivo), el servidor devuelve un mensaje de acuse de recibo de proceso de validación al proveedor de servicios de red. En la etapa 238, el proveedor de servicios de red presenta al usuario un cuadro de diálogo de inicio de sesión. En la etapa 240, el proveedor de servicios de red determina si se proporcionan un nombre de usuario y una contraseña válidos. Si se proporciona un nombre de usuario o una contraseña no válidos, la sesión de usuario finaliza en la etapa 242. En la etapa 244, si se proporcionan un nombre de usuario y una contraseña válidos, el proveedor de servicios de red envía el NDI del dispositivo y la información de cuenta de usuario final (EAI) generada por el proveedor de servicios de red al servidor. En la etapa 246, el servidor registra la asociación de NDI y EAI en su base de datos y actualiza diversa información para el dispositivo, tal como la fecha/hora del último inicio de sesión con éxito, los inicios de sesión totales y otros datos sobre el dispositivo. En la etapa 250, el servidor comprueba el estado de NDI y EAI con los parámetros del proveedor de servicios de red. En la etapa 252, basándose en las reglas del proveedor de servicios de red, el servidor envía el estado de NDI/EAI al proveedor de servicios de red. En la etapa 254, el proveedor de servicios de red termina/continúa la sesión del usuario en función del estado de NDI/EAI devuelto por el servidor. A continuación se describirá con mayor detalle un procedimiento para la validación de un usuario/dispositivo existente.

Las Figuras 9E y 9F son un diagrama de flujo que ilustra un procedimiento preferido 260 para la validación de un usuario/dispositivo existente usando el sistema de prevención y detección de fraude según la invención. Las etapas descritas posteriormente pueden implementarse mediante instrucciones de ordenador en un módulo de software ejecutado por un ordenador central particular de un proveedor de servicios de red o mediante instrucciones de

ordenador en un módulo de software ejecutado por el servidor de detección de fraude. La invención no está limitada a ninguna ubicación particular de las instrucciones de ordenador que implementan el procedimiento de validación. En la etapa 262, un usuario inicia una aplicación (después de descargar la aplicación desde el proveedor de servicios de red en la forma de realización en la que el cliente está integrado en una aplicación) y la aplicación inicia automáticamente el cliente. En la etapa 264, el cliente determina si el dispositivo está registrado con el sistema de detección de fraude. Si el dispositivo no está registrado aún, entonces el procedimiento finaliza y el procedimiento para la validación de un nuevo usuario se describe en las Figuras 9C y 9D. Si el dispositivo ya está registrado, entonces, en la etapa 266, el cliente recopila datos del dispositivo, genera una NDF y reenvía esa NDF y el NDI ya asignado al proveedor de servicios de red. El proveedor de servicios de red reenvía entonces la NDF y el NDI al servidor, que almacena la NDF y comprueba la NDF con datos de NDF existentes para el estado de la NDF particular.

En la etapa 268, el servidor determina si existe el par NDF/NDI en la base de datos. Si no hay ninguna coincidencia en la base de datos, entonces el proveedor de servicios de red es notificado en la etapa 270 y la sesión de usuario finaliza. En la etapa 272, el servidor determina si el estado de NDI o NDF es malo y, si el estado de alguno de ellos es malo, el proveedor de servicios de red es notificado y la sesión de usuario finaliza en la etapa 274. Si los estados del NDI y la NDF son buenos, entonces, en la etapa 276, el proveedor de servicios de red presenta al usuario un cuadro de diálogo de inicio de sesión. Según la invención, el cliente y/o el sistema de validación también puede presentar el inicio de sesión al usuario y realizar el proceso de inicio de sesión de usuario, además de los procesos de validación. En la etapa 278, el proveedor de servicios de red determina si se proporcionan un nombre de usuario y una contraseña válidos. Si se proporciona un nombre de usuario o una contraseña no válidos, la sesión de usuario finaliza en la etapa 280. En la etapa 282, si se proporcionan un nombre de usuario y una contraseña válidos, el proveedor de servicios de red envía el NDI del dispositivo y el EAI al servidor. En la etapa 284, el servidor registra la asociación de NDI y EAI en su base de datos y actualiza diversa información para el dispositivo, tal como la fecha/hora del último inicio de sesión con éxito, los inicios de sesión totales y otros datos sobre el dispositivo. En la etapa 286, el servidor comprueba el estado de NDI y EAI con los parámetros del proveedor de servicios de red. En la etapa 288, basándose en las reglas del proveedor de servicios de red, el servidor envía el estado de NDI/EAI al proveedor de servicios de red. En la etapa 290, el proveedor de servicios de red termina/continúa la sesión de usuario en función del estado de NDI/EAI devuelto por el servidor.

A continuación se proporcionan varios ejemplos del funcionamiento del procedimiento anterior. Como se ha descrito anteriormente, cada ordenador central establecerá sus propias reglas personalizadas para cada aspecto del presente procedimiento de validación. Debido a esto, las mismas circunstancias que dan lugar a la negación del acceso a un usuario final en un ordenador central pueden no dar como resultado un acceso denegado en otro ordenador central. Por lo tanto, los siguientes ejemplos están destinados simplemente a ilustrar algunas de las maneras en las que podría utilizarse la presente invención.

El ordenador central 1 identifica un problema con una cuenta identificada por un EAI de EAI2004. Después de cerrar la cuenta en el sistema del ordenador central 1, un administrador del ordenador central 1 inicia sesión en la NDRD y busca en la NDRD utilizando una interfaz de usuario para identificar cuatro NDI adicionales utilizados por EAI2004, y cambia el estado de cada NDI de tal forma que jamás se les permitirá conectarse con el ordenador central 1. Además, el administrador identifica otros dos EAI que han utilizado estos NDI para conectarse al ordenador central 1. Después de investigar las cuentas recién identificadas, se determina que son potencialmente fraudulentas y también se cierran. De este modo, el usuario es capaz de identificar una cuenta, sus dispositivos de red asociados y otros EAI asociados a los dispositivos de red identificados a los que se les niega el acceso al sistema. En un primer ejemplo, un usuario final intenta conectarse al ordenador central 1 desde un NDI que ha sido identificado por el ordenador central 1 como que se ha utilizado en una transacción fraudulenta. Basándose en el estado establecido por el ordenador central 1, el usuario no podrá acceder a la red. En un segundo ejemplo, un usuario final intenta conectarse al ordenador central 1 a partir de un NDI que ha sido identificado por el ordenador central 1 como que se ha utilizado de manera sospechosa. Basándose en el estado establecido por el ordenador central 1, al usuario se le permite el acceso a la red, pero por cada combinación de nombre de usuario y contraseña válidos proporcionada por el usuario final, esa cuenta se desactiva automáticamente en el sistema del ordenador central 1 y se pide al usuario que introduzca un nombre de usuario y contraseña diferentes.

En un tercer ejemplo, un usuario final intenta conectarse al ordenador central 1 a partir de un NDI que ha sido identificado por el ordenador central 2 como que se ha utilizado en una transacción fraudulenta. Basándose en el estado de NDI establecido por el ordenador central 2 y por el hecho de que el ordenador central 1 ha identificado el ordenador central 2 como de confianza, el usuario no podrá acceder a la red. Además, el estado de NDI para el ordenador central 1 se cambia a 'malo' y la cuenta del usuario final se cierra en el sistema del ordenador central 1. En un cuarto ejemplo, un usuario final intenta conectarse al ordenador central 1 a partir de un NDI que ha sido identificado por el ordenador central 3 como que se ha utilizado en una transacción fraudulenta. Puesto que el ordenador central 3 no ha sido identificado como de confianza por el ordenador central 1, esta condición se ignora y se permite al usuario que acceda a la red.

En otro ejemplo, periódicamente, un administrador del ordenador central 1 recibe un informe desde la NDRD referente a todos los NDI identificados por los ordenadores centrales de confianza como 'malos' que tienen un

estado para el ordenador central 1 de 'bueno', incluyendo todos los EAI para el ordenador central 1 asociado a estos NDI. El administrador investiga estas cuentas para determinar la medida apropiada. El administrador puede entonces, por ejemplo, cambiar el estado de los NDI y los EAI a "malo" e investigar cuentas de usuario asociadas dentro de su sistema para identificar posibles cuentas fraudulentas.

En otro ejemplo, el ordenador central 1 verifica de manera proactiva información de cuenta para todas las cuentas identificadas a través de la NDRD como que comparten el mismo NDI, y cuentas sospechosos son identificadas para su posterior investigación. Por ejemplo, tres cuentas con direcciones indicadas en tres países diferentes que han iniciado sesión desde el mismo dispositivo de red serían identificadas como sospechosas. Como alternativa, el sistema de prevención de fraude puede generar de forma automática y periódica información a partir de la NDRD basándose en las solicitudes de un ordenador central particular. A continuación se proporcionará un ejemplo del funcionamiento de una implementación del sistema de detección de fraude según la invención.

Una vez que un proveedor de servicios de red particular (NSP1) ha integrado el cliente y el sistema de detección de fraude en su sistema, el sistema de proveedor de servicios de red puede solicitar automáticamente información, etc. desde el sistema de detección de fraude. La solicitud de información puede ocurrir por varias razones, tales como una nueva instalación del consumidor, un inicio de sesión del consumidor, un intento de compra/depósito del consumidor y un intento reembolso/reintegro del consumidor. En cada situación, el software de cliente del proveedor de servicios de red puede invocar al cliente de detección de fraude, que puede devolver un conjunto de información que el software cliente pasará a un sistema de procesamiento. En una implementación del sistema, el sistema de procesamiento del proveedor de servicios de red puede pasar 1) un identificador único (que será proporcionado al proveedor de servicios de red que se registra para el servicio) que identifica de forma única al proveedor de servicios de red particular al sistema de detección de fraude y permite que la NDRD almacene datos de acuerdo con el proveedor de servicios de red particular; 2) un único "identificador de sesión" para identificar la sesión de acceso de usuario particular al proveedor de servicios de red particular; 3) un identificador de consumidor único para el consumidor específico (si está disponible, el cual debería estarlo en todos los casos excepto en una nueva instalación del consumidor), tal como el EAI; 4) un "código de acción" que identifica el tipo de cuenta de usuario (ver más abajo); y 5) la información que el cliente proporcionó a través de la API al servidor. El servidor puede entonces responder a través de la API con una "respuesta de acción" que indica una medida sugerida para la cuenta particular, la información que desea pasar a través del cliente, tal como el cliente ieSnare en una forma de realización preferida de la invención, o ambas cosas. A continuación se describirá con mayor detalle un ejemplo de la API para el sistema de detección de fraude.

En una forma de realización preferida, la API utiliza lenguaje de marcado extensible ("XML") para pasar información entre el sistema de procesamiento del proveedor de servicios de red y el servidor de detección de fraude. La API es una manera simple pero potente de automatizar consultas comunes e interpretar sus respuestas.

Las solicitudes de la API tienen normalmente el siguiente formato:

```
<ieRequest>
<SnareID>NúmeroConsumidorSnare</SnareID>
<SessionID> Número de sesión </SessionID>
<CustomerID>  Su identificador de consumidor único (si no estuviera disponible, dejar en blanco) </CustomerID>
<Action>Número de código de acción</Action>
<Data> Información de cliente ieSnare proporcionada </Data>
</ieRequest>
```

Las respuestas de la API tienen normalmente el siguiente formato:

```
<ieResponse>
<SnareID>NúmeroConsumidorSnare</SnareID>
<SessionID> Número de sesión </SessionID>
<CustomerID>Su identificador de consumidor único (o en blanco si no aplicable)</CustomerID>
<ComputerID>  Su identificador de ordenador único  </ComputerID>
<Response>Número de código de respuesta</Response>
<Reason>Número de código de motivo</Reason>
<PassData>  Información que transmitir al cliente ieSnare (opcional)  </PassData>
</ieResponse>
```

donde los números de código de acción actualmente admitidos son:

1000 - creación de cuenta nueva
2000 - intento de inicio de sesión
3000 - intento de compra/depósito
4000 - intento de reembolso/reintegro

y los números de código de respuesta actualmente admitidos son:

0 - ACEPTAR
1 - ATRAPAR
2 - RECHAZAR

y los números de código de motivo actualmente admitidos son:

0 - reglas estándar
1 - ajustar manualmente a siempre para este usuario/ordenador
2 - asociación con otro usuario/ordenador
3 - número de otros usuarios que comparten ordenador
4 - número de ordenadores que está usando este usuario

Aunque lo anterior se ha descrito con referencia a una forma de realización particular de la invención, los expertos en la técnica apreciarán que pueden realizarse cambios en esta forma de realización sin apartarse de la invención, cuyo alcance está definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento implementado por ordenador (220) para detectar fraude durante una conexión de un dispositivo de red no registrado (22) a un proveedor de servicios de red (24), en el que un cliente de software (54) se ejecuta (222) en el dispositivo de red (22), comprendiendo el procedimiento:

determinar (224), mediante el cliente de software, que el dispositivo de red no está registrado con un sistema de detección de fraude (26);
asignar, mediante el sistema de detección de fraude (26), un identificador de dispositivo de red único al dispositivo de red no registrado (22) y enviar (226) el identificador de dispositivo de red al dispositivo de red (22);
generar (228), mediante el cliente de software (54) que se ejecuta en el dispositivo de red (22), una huella digital de dispositivo de red para el dispositivo de red (22) en función de una o más características de dispositivo;
reenviar (230), mediante el cliente de software (54), la huella digital de dispositivo de red al sistema de detección de fraude (26);
comparar (230), mediante el sistema de detección de fraude (26), la huella digital de dispositivo de red con una base de datos (30) de dispositivos de red registrados; y
verificar (232, 236), mediante el sistema de detección de fraude (26), que la huella digital de dispositivo de red no está duplicada con el fin de impedir un fraude.

2. El procedimiento según la reivindicación 1, que comprende además asociar (246) el identificador de dispositivo de red con información de cuenta de usuario final.

3. El procedimiento según la reivindicación 1, que comprende además:

verificar (202) que el identificador de dispositivo de red es válido;
verificar (206 - 208) que un estado de dispositivo de red del identificador de dispositivo de red y la huella digital de dispositivo de red es aceptable para el sistema de detección de fraude (26) de acuerdo con un conjunto de reglas de estado; y
verificar (210 - 212) que el estado de dispositivo de red del identificador de dispositivo de red y la huella digital de dispositivo de red es aceptable para ordenadores centrales de confianza.

4. El procedimiento según la reivindicación 1, en el que el dispositivo de red (22) está conectado al proveedor de servicios de red (24), y el procedimiento comprende además:

verificar (214) que una pluralidad de cuentas de usuario por identificador de dispositivo de red es aceptable para el proveedor de servicios de red (24), y
verificar (216) que una pluralidad de identificadores de dispositivo de red por cuenta de usuario es aceptable para el proveedor de servicios de red (24).

5. El procedimiento según la reivindicación 1, en el que el dispositivo de red está conectado al proveedor de servicios de red, y el procedimiento comprende además al menos una de las siguientes etapas:

proporcionar (238) un cuadro de diálogo de inicio de sesión al dispositivo de red (22); y
verificar (240, 244) que un nombre de usuario y una contraseña proporcionados por un usuario del dispositivo de red (22) son válidos, proporcionando (244) el identificador de dispositivo de red y un identificador de usuario final al sistema de detección de fraude desde el proveedor de servicios de red (24), y
comprobar (250) un estado del identificador de dispositivo de red y el identificador de usuario final en función de un conjunto de reglas del proveedor de servicios de red (24).

6. El procedimiento según la reivindicación 1, que comprende además proporcionar (238) un cuadro de diálogo de inicio de sesión al dispositivo de red.

7. El procedimiento según la reivindicación 1, en el que el dispositivo de red (22) está conectado al proveedor de servicios de red (24), y el procedimiento comprende además:

verificar (240, 244) que un nombre de usuario y una contraseña proporcionados por un usuario del dispositivo de red (22) son válidos,
proporcionar (244) el identificador de dispositivo de red y un identificador de usuario final al sistema de detección de fraude (26) desde el proveedor de servicios de red (24), y
comprobar (250) un estado del identificador de dispositivo de red y el identificador de usuario final en función de un conjunto de reglas del proveedor de servicios de red (24).

8. El procedimiento según la reivindicación 1, en el que el sistema de detección de fraude (26) comprende el cliente de software (54), la base de datos (30) y un módulo de software (96),

el cliente de software (54) se descarga automáticamente en el dispositivo de red (22) y recopila automáticamente información de identificación de dispositivo desde y acerca del dispositivo de red (22) para generar la huella digital de dispositivo de red,
el módulo de software (96) recibe la huella digital de dispositivo de red, almacena la huella digital de dispositivo de red en la base de datos (30) y asocia la huella digital de dispositivo de red con información de cuenta de usuario final proporcionada por el proveedor de servicios de red (24), y
la huella digital de dispositivo de red y la información de cuenta de usuario final son compartidas entre un grupo selecto de proveedores de servicios de red participantes (24) para realizar un seguimiento del comportamiento sospechoso y de este modo detectar y evitar un fraude cometido usando el dispositivo de red (22).

9. El procedimiento según la reivindicación 8, en el que la base de datos (30) comprende además una pluralidad de registros (118 - 122), donde cada registro comprende además:

un campo de ordenador central (112) que contiene un identificador de un proveedor de servicios de red particular (24),
un campo de información de cuenta de usuario (114) que contiene información del proveedor de servicios de red particular (24) que identifica un usuario particular, y
el identificador de dispositivo de red (116).

10. El procedimiento según la reivindicación 8, en el que el sistema de detección de fraude (26):

valida cada dispositivo de red (22) de manera aleatoria y periódica, o
valida cada dispositivo de red (22) después de la conexión del dispositivo de red con el proveedor de servicios de red (24), o
valida cada dispositivo de red (22) cuando el dispositivo de red inicia sesión en el proveedor de servicios de red (24), o
valida cada dispositivo de red (22) cuando el dispositivo de red realiza una transacción con el proveedor de servicios de red (24), o
valida cada dispositivo de red (22) cada vez que el dispositivo de red vuelve a conectarse con el proveedor de servicios de red (24).

11. El procedimiento según la reivindicación 8, en el que el cliente de software (54):

está integrado en una aplicación de software que se descarga en el dispositivo de red (22) desde el proveedor de servicios de red (24), o
es una aplicación de software independiente que se descarga en el dispositivo de red (22) desde el proveedor de servicios de red (24), o
es un elemento de código que se descarga automáticamente en el dispositivo de red (22) desde el proveedor de servicios de red (24), o
se descarga en el dispositivo de red (22) cuando el dispositivo de red se conecta al proveedor de servicios de red (24).

12. El procedimiento según la reivindicación 8, en el que el proveedor de servicios de red (24) comprende el sistema de detección de fraude (26).

13. El procedimiento según la reivindicación 1, en el que el dispositivo de red (22) comprende un teléfono celular, un asistente personal digital, un ordenador portátil, un ordenador personal o un teléfono.

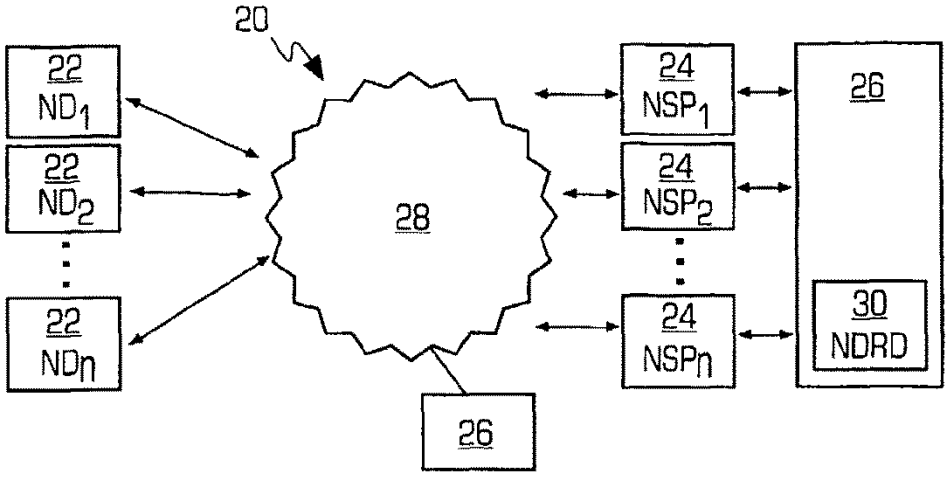

FIG. 1

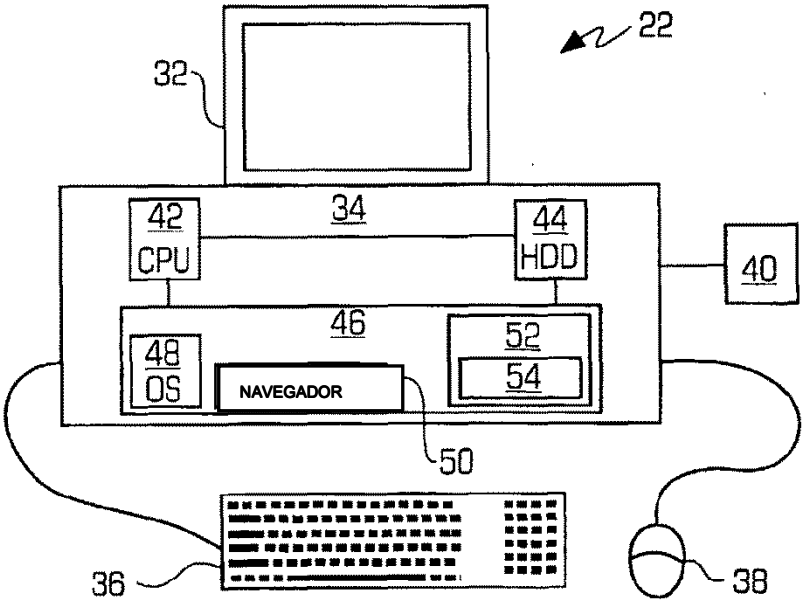

FIG. 2

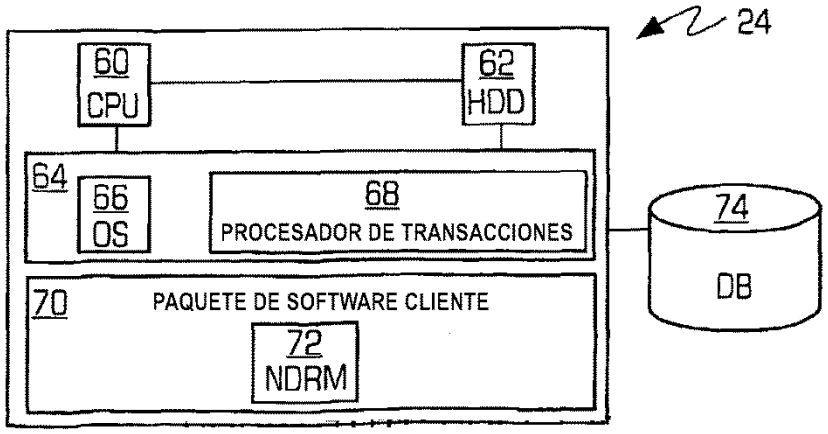

FIG. 3

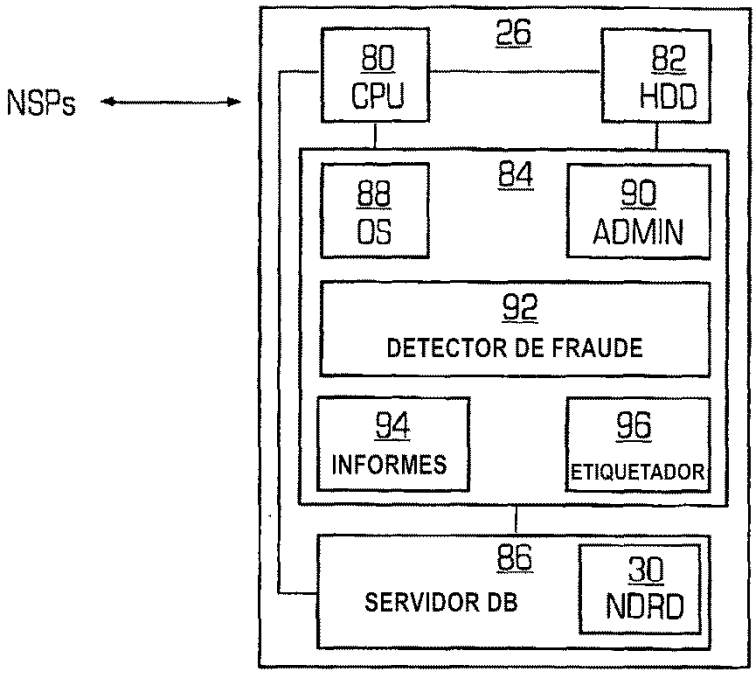

FIG. 4

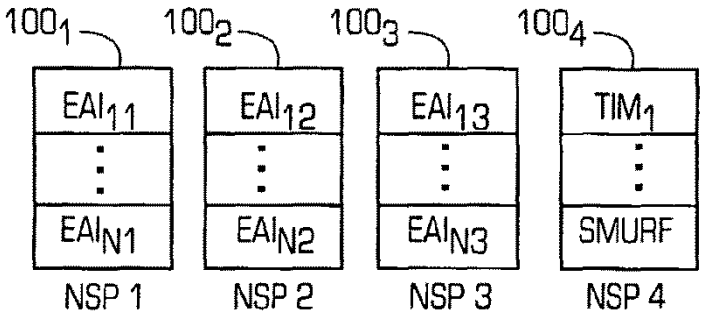

FIG. 5

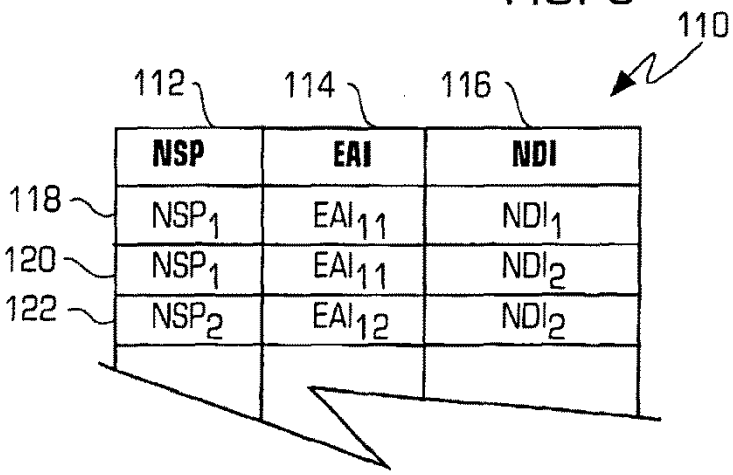

FIG. 6

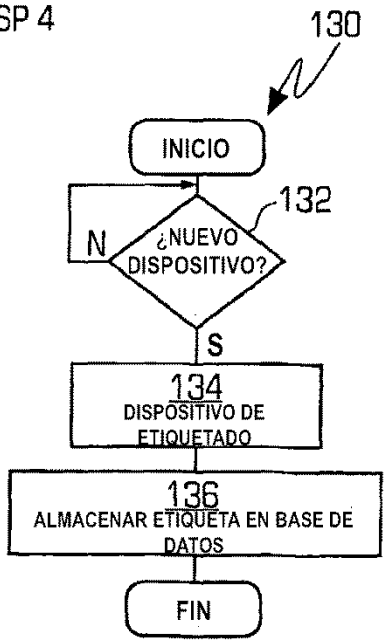

FIG. 7

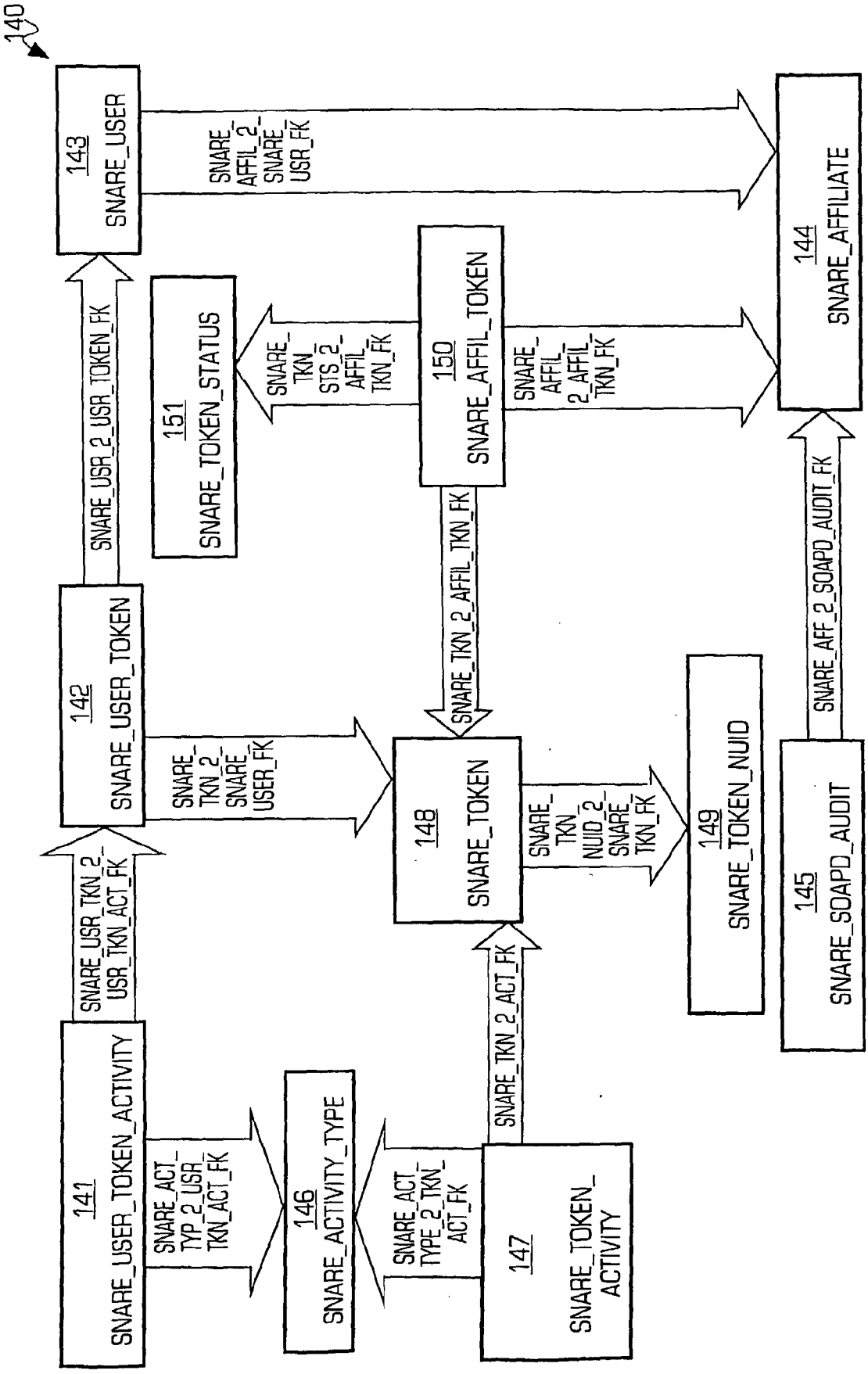
140
143
SNARE_USER
SNARE_AFFIL_2_SNARE_USR_FK
144
SNARE_AFFILIATE
SNARE_USR_2_USR_TOKEN_FK
151
SNARE_TOKEN_STATUS
SNARE_TKN_STS_2_AFFIL_TKN_FK
150
SNARE_AFFIL_TOKEN
SNARE_AFFIL_2_AFFIL_TKN_FK
142
SNARE_USER_TOKEN
SNARE_TKN_2_AFFIL_TKN_FK
SNARE_AFF_2_SOAPD_AUDIT_FK
SNARE_TKN_2_SNARE_USER_FK
148
SNARE_TOKEN
SNARE_TKN_NUID_2_SNARE_TKN_FK
149
SNARE_TOKEN_NUID
145
SNARE_SOAPD_AUDIT
SNARE_USR_TKN_2_USR_TKN_ACT_FK
SNARE_TKN_2_ACT_FK
141
SNARE_USER_TOKEN_ACTIVITY
SNARE_ACT_TYP_2_USR_TKN_ACT_FK
146
SNARE_ACTIVITY_TYPE
SNARE_ACT_TYPE_2_TKN_ACT_FK
147
SNARE_TOKEN_ACTIVITY

FIG. 8A

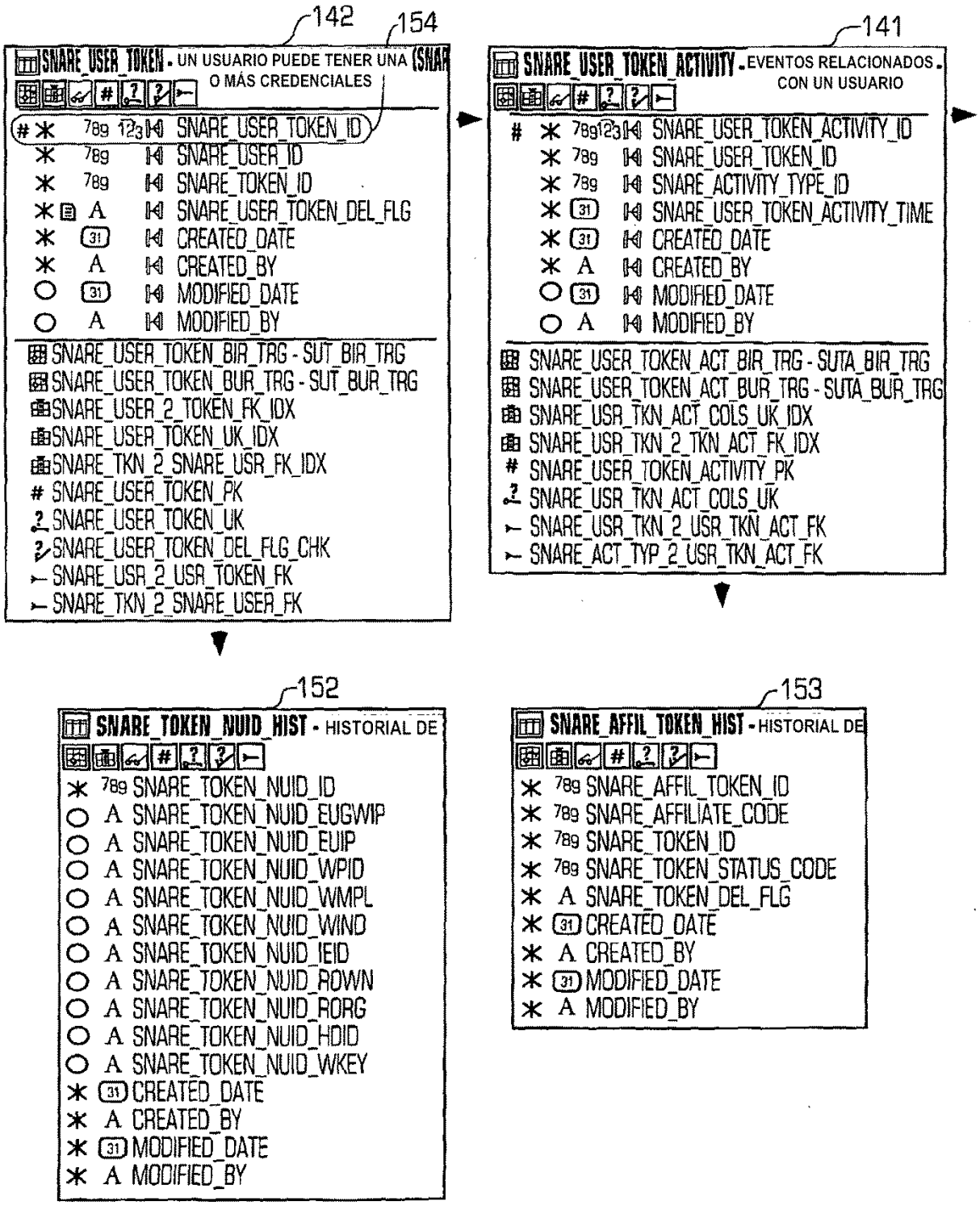
142
154
SNARE_USER_TOKEN - UN USUARIO PUEDE TENER UNA O MÁS CREDENCIALES (SNAR
SNARE_USER_TOKEN_ID
SNARE_USER_ID
SNARE_TOKEN_ID
SNARE_USER_TOKEN_DEL_FLG
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_USER_TOKEN_BIR_TRG - SUT_BIR_TRG
SNARE_USER_TOKEN_BUR_TRG - SUT_BUR_TRG
SNARE_USER_2_TOKEN_FK_IDX
SNARE_USER_TOKEN_UK_IDX
SNARE_TKN_2_SNARE_USR_FK_IDX
SNARE_USER_TOKEN_PK
SNARE_USER_TOKEN_UK
SNARE_USER_TOKEN_DEL_FLG_CHK
SNARE_USR_2_USR_TOKEN_FK
SNARE_TKN_2_SNARE_USER_FK
141
SNARE_USER_TOKEN_ACTIVITY - EVENTOS RELACIONADOS CON UN USUARIO
SNARE_USER_TOKEN_ACTIVITY_ID
SNARE_USER_TOKEN_ID
SNARE_ACTIVITY_TYPE_ID
SNARE_USER_TOKEN_ACTIVITY_TIME
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_USER_TOKEN_ACT_BIR_TRG - SUTA_BIR_TRG
SNARE_USER_TOKEN_ACT_BUR_TRG - SUTA_BUR_TRG
SNARE_USR_TKN_ACT_COLS_UK_IDX
SNARE_USR_TKN_2_TKN_ACT_FK_IDX
SNARE_USER_TOKEN_ACTIVITY_PK
SNARE_USR_TKN_ACT_COLS_UK
SNARE_USR_TKN_2_USR_TKN_ACT_FK
SNARE_ACT_TYP_2_USR_TKN_ACT_FK
152
SNARE_TOKEN_NUID_HIST - HISTORIAL DE
SNARE_TOKEN_NUID_ID
SNARE_TOKEN_NUID_EUGWIP
SNARE_TOKEN_NUID_EUIP
SNARE_TOKEN_NUID_WPID
SNARE_TOKEN_NUID_WMPL
SNARE_TOKEN_NUID_WIND
SNARE_TOKEN_NUID_IEID
SNARE_TOKEN_NUID_ROWN
SNARE_TOKEN_NUID_RORG
SNARE_TOKEN_NUID_HDID
SNARE_TOKEN_NUID_WKEY
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
153
SNARE_AFFIL_TOKEN_HIST - HISTORIAL DE
SNARE_AFFIL_TOKEN_ID
SNARE_AFFILIATE_CODE
SNARE_TOKEN_ID
SNARE_TOKEN_STATUS_CODE
SNARE_TOKEN_DEL_FLG
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY

FIG. 8B

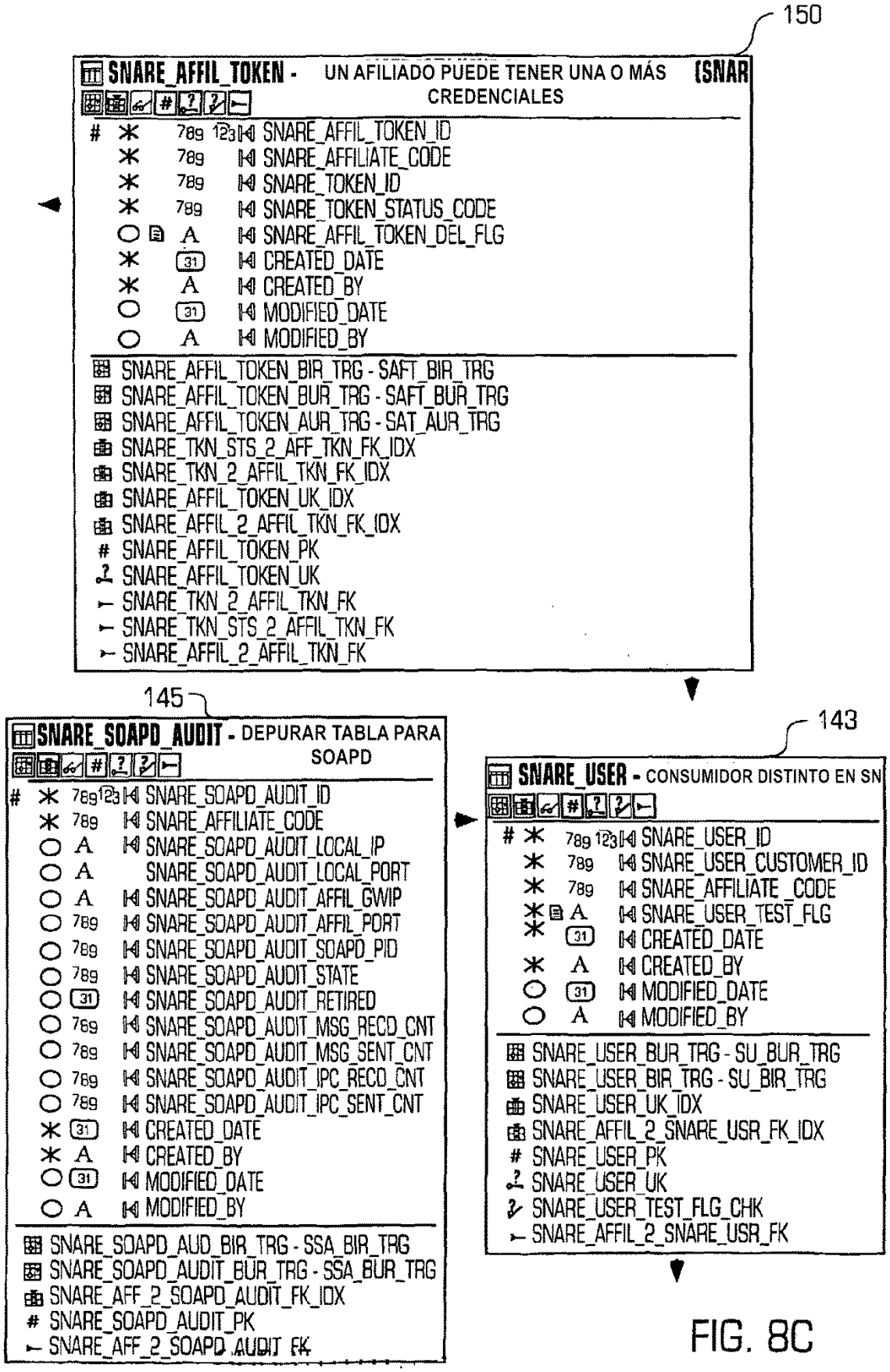
150
SNARE_AFFIL_TOKEN - UN AFILIADO PUEDE TENER UNA O MÁS CREDENCIALES (SNAR
SNARE_AFFIL_TOKEN_ID
SNARE_AFFILIATE_CODE
SNARE_TOKEN_ID
SNARE_TOKEN_STATUS_CODE
SNARE_AFFIL_TOKEN_DEL_FLG
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_AFFIL_TOKEN_BIR_TRG - SAFT_BIR_TRG
SNARE_AFFIL_TOKEN_BUR_TRG - SAFT_BUR_TRG
SNARE_AFFIL_TOKEN_AUR_TRG - SAT_AUR_TRG
SNARE_TKN_STS_2_AFF_TKN_FK_IDX
SNARE_TKN_2_AFFIL_TKN_FK_IDX
SNARE_AFFIL_TOKEN_UK_IDX
SNARE_AFFIL_2_AFFIL_TKN_FK_IDX
SNARE_AFFIL_TOKEN_PK
SNARE_AFFIL_TOKEN_UK
SNARE_TKN_2_AFFIL_TKN_FK
SNARE_TKN_STS_2_AFFIL_TKN_FK
SNARE_AFFIL_2_AFFIL_TKN_FK
145
SNARE_SOAPD_AUDIT - DEPURAR TABLA PARA SOAPD
SNARE_SOAPD_AUDIT_ID
SNARE_AFFILIATE_CODE
SNARE_SOAPD_AUDIT_LOCAL_IP
SNARE_SOAPD_AUDIT_LOCAL_PORT
SNARE_SOAPD_AUDIT_AFFIL_GWIP
SNARE_SOAPD_AUDIT_AFFIL_PORT
SNARE_SOAPD_AUDIT_SOAPD_PID
SNARE_SOAPD_AUDIT_STATE
SNARE_SOAPD_AUDIT_RETIRED
SNARE_SOAPD_AUDIT_MSG_RECD_CNT
SNARE_SOAPD_AUDIT_MSG_SENT_CNT
SNARE_SOAPD_AUDIT_IPC_RECD_CNT
SNARE_SOAPD_AUDIT_IPC_SENT_CNT
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_SOAPD_AUD_BIR_TRG - SSA_BIR_TRG
SNARE_SOAPD_AUDIT_BUR_TRG - SSA_BUR_TRG
SNARE_AFF_2_SOAPD_AUDIT_FK_IDX
SNARE_SOAPD_AUDIT_PK
SNARE_AFF_2_SOAPD_AUDIT_FK
143
SNARE_USER - CONSUMIDOR DISTINTO EN SN
SNARE_USER_ID
SNARE_USER_CUSTOMER_ID
SNARE_AFFILIATE_CODE
SNARE_USER_TEST_FLG
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_USER_BUR_TRG - SU_BUR_TRG
SNARE_USER_BIR_TRG - SU_BIR_TRG
SNARE_USER_UK_IDX
SNARE_AFFIL_2_SNARE_USR_FK_IDX
SNARE_USER_PK
SNARE_USER_UK
SNARE_USER_TEST_FLG_CHK
SNARE_AFFIL_2_SNARE_USR_FK

FIG. 8C

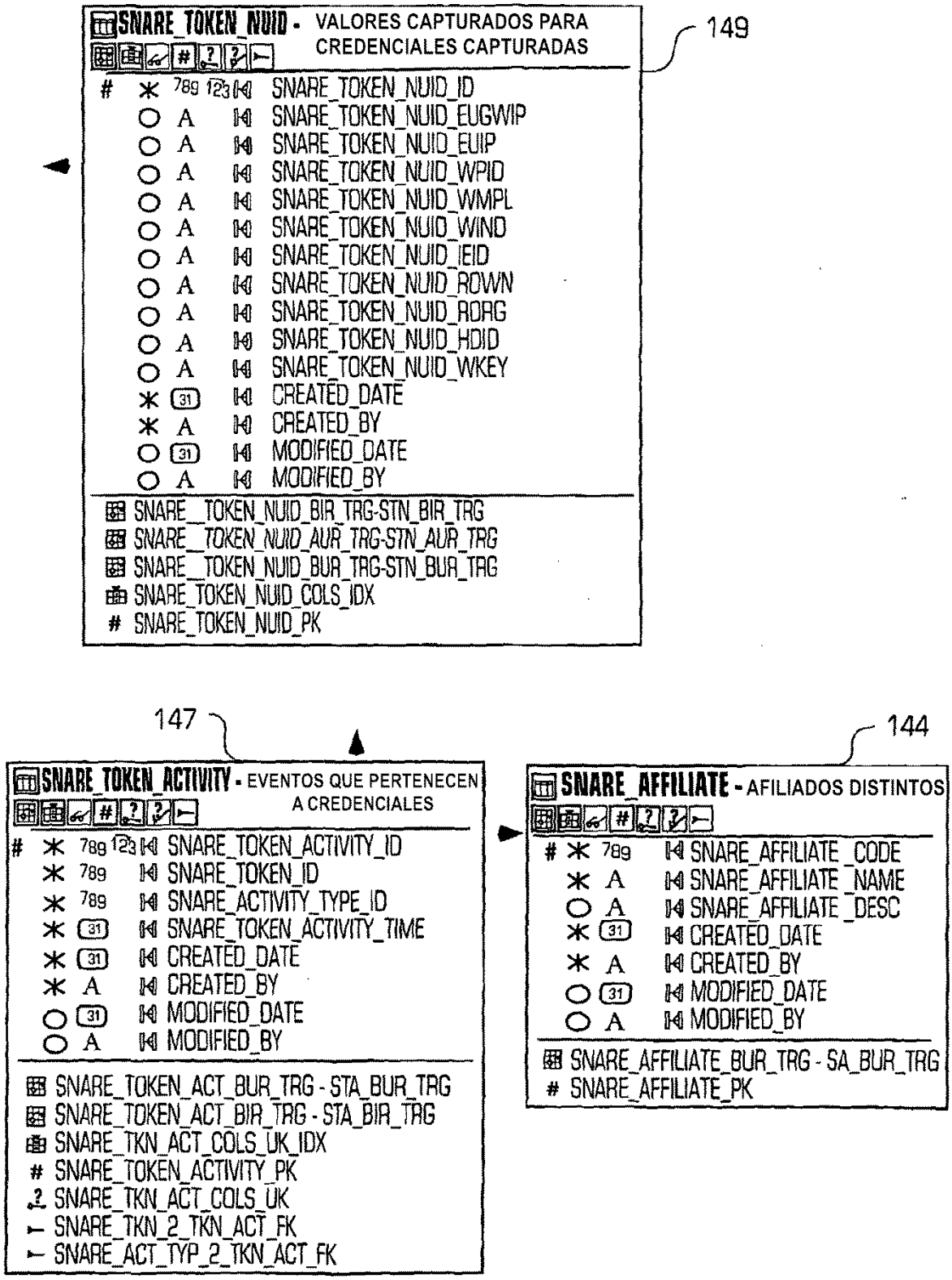
SNARE_TOKEN_NUID - VALORES CAPTURADOS PARA CREDENCIALES CAPTURADAS
149
SNARE_TOKEN_NUID_ID
SNARE_TOKEN_NUID_EUGWIP
SNARE_TOKEN_NUID_EUIP
SNARE_TOKEN_NUID_WPID
SNARE_TOKEN_NUID_WMPL
SNARE_TOKEN_NUID_WIND
SNARE_TOKEN_NUID_IEID
SNARE_TOKEN_NUID_ROWN
SNARE_TOKEN_NUID_RORG
SNARE_TOKEN_NUID_HDID
SNARE_TOKEN_NUID_WKEY
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_TOKEN_NUID_BIR_TRG-STN_BIR_TRG
SNARE_TOKEN_NUID_AUR_TRG-STN_AUR_TRG
SNARE_TOKEN_NUID_BUR_TRG-STN_BUR_TRG
SNARE_TOKEN_NUID_COLS_IDX
SNARE_TOKEN_NUID_PK
147
SNARE_TOKEN_ACTIVITY - EVENTOS QUE PERTENECEN A CREDENCIALES
SNARE_TOKEN_ACTIVITY_ID
SNARE_TOKEN_ID
SNARE_ACTIVITY_TYPE_ID
SNARE_TOKEN_ACTIVITY_TIME
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_TOKEN_ACT_BUR_TRG - STA_BUR_TRG
SNARE_TOKEN_ACT_BIR_TRG - STA_BIR_TRG
SNARE_TKN_ACT_COLS_UK_IDX
SNARE_TOKEN_ACTIVITY_PK
SNARE_TKN_ACT_COLS_UK
SNARE_TKN_2_TKN_ACT_FK
SNARE_ACT_TYP_2_TKN_ACT_FK
144
SNARE_AFFILIATE - AFILIADOS DISTINTOS
SNARE_AFFILIATE_CODE
SNARE_AFFILIATE_NAME
SNARE_AFFILIATE_DESC
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_AFFILIATE_BUR_TRG - SA_BUR_TRG
SNARE_AFFILIATE_PK

FIG. 8D

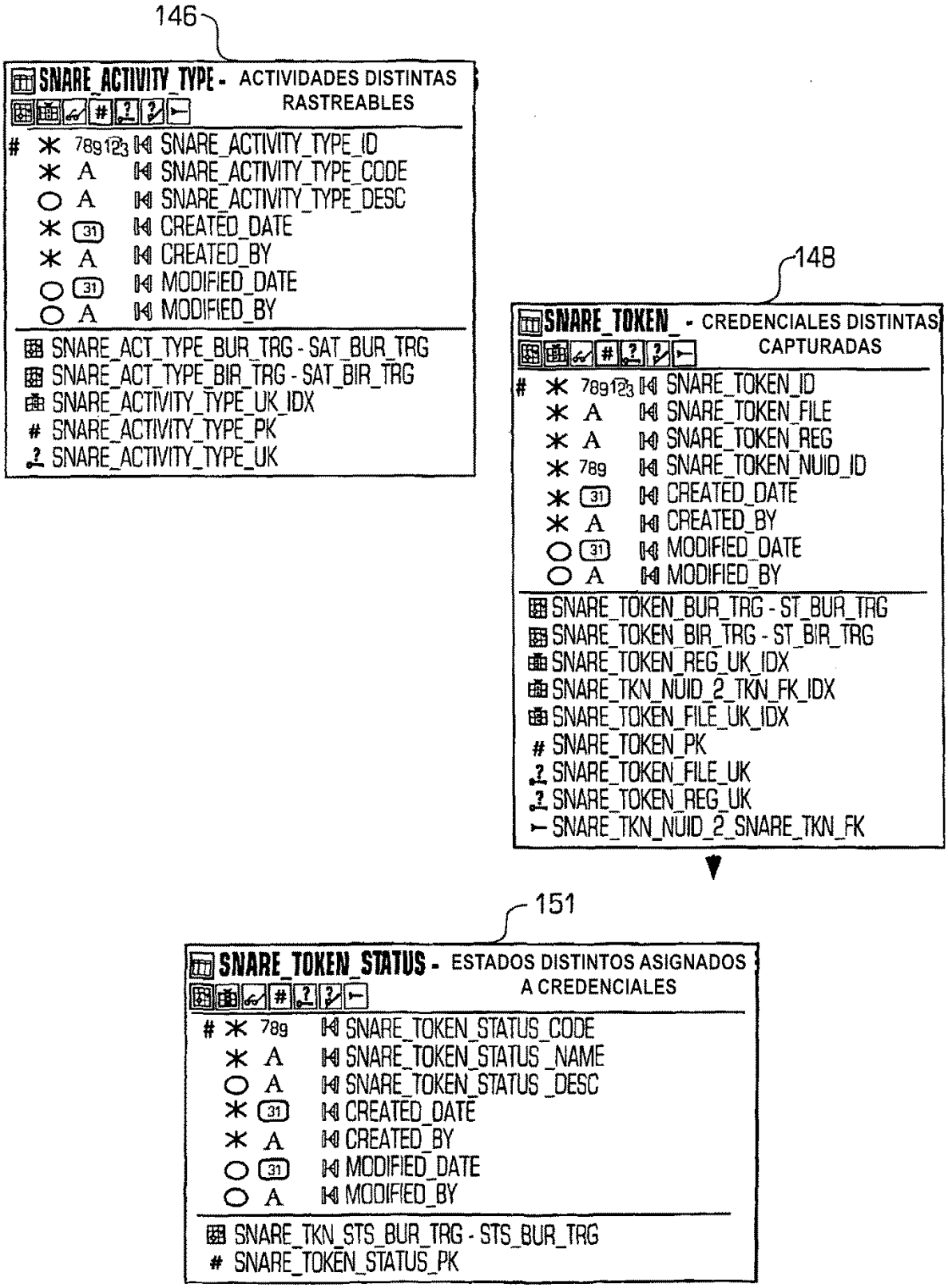
146
SNARE_ACTIVITY_TYPE - ACTIVIDADES DISTINTAS RASTREABLES
SNARE_ACTIVITY_TYPE_ID
SNARE_ACTIVITY_TYPE_CODE
SNARE_ACTIVITY_TYPE_DESC
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_ACT_TYPE_BUR_TRG - SAT_BUR_TRG
SNARE_ACT_TYPE_BIR_TRG - SAT_BIR_TRG
SNARE_ACTIVITY_TYPE_UK_IDX
SNARE_ACTIVITY_TYPE_PK
SNARE_ACTIVITY_TYPE_UK
148
SNARE_TOKEN_ - CREDENCIALES DISTINTAS CAPTURADAS
SNARE_TOKEN_ID
SNARE_TOKEN_FILE
SNARE_TOKEN_REG
SNARE_TOKEN_NUID_ID
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_TOKEN_BUR_TRG - ST_BUR_TRG
SNARE_TOKEN_BIR_TRG - ST_BIR_TRG
SNARE_TOKEN_REG_UK_IDX
SNARE_TKN_NUID_2_TKN_FK_IDX
SNARE_TOKEN_FILE_UK_IDX
SNARE_TOKEN_PK
SNARE_TOKEN_FILE_UK
SNARE_TOKEN_REG_UK
SNARE_TKN_NUID_2_SNARE_TKN_FK
151
SNARE_TOKEN_STATUS - ESTADOS DISTINTOS ASIGNADOS A CREDENCIALES
SNARE_TOKEN_STATUS_CODE
SNARE_TOKEN_STATUS _NAME
SNARE_TOKEN_STATUS _DESC
CREATED_DATE
CREATED_BY
MODIFIED_DATE
MODIFIED_BY
SNARE_TKN_STS_BUR_TRG - STS_BUR_TRG
SNARE_TOKEN_STATUS_PK

FIG. 8E

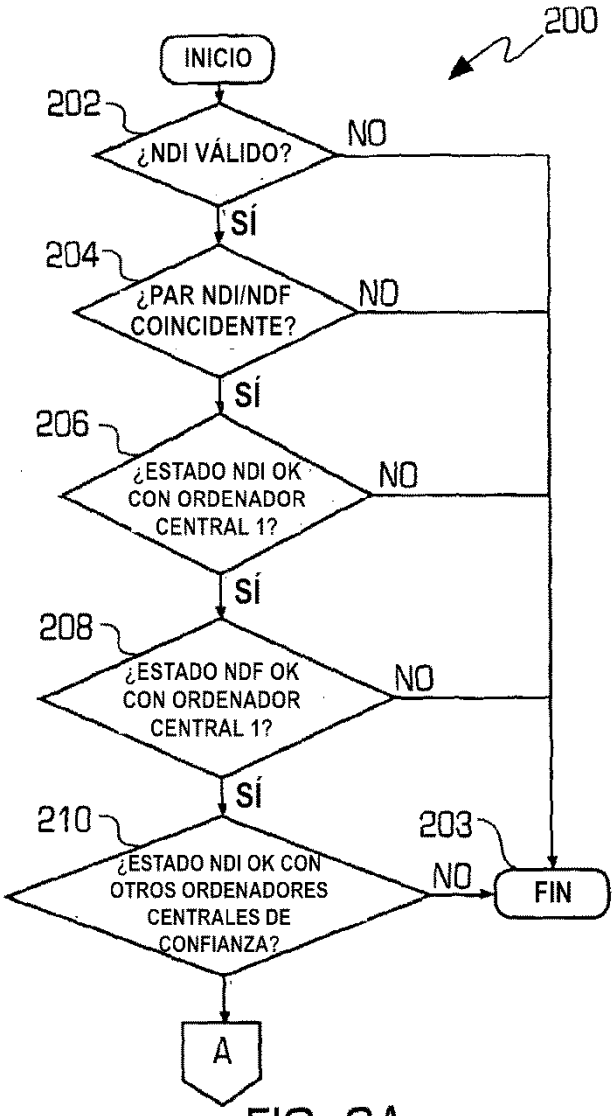
200
INICIO
202
¿NDI VÁLIDO?
NO
SÍ
204
¿PAR NDI/NDF COINCIDENTE?
NO
SÍ
206
¿ESTADO NDI OK CON ORDENADOR CENTRAL 1?
NO
SÍ
208
¿ESTADO NDF OK CON ORDENADOR CENTRAL 1?
NO
SÍ
210
¿ESTADO NDI OK CON OTROS ORDENADORES CENTRALES DE CONFIANZA?
NO
203
FIN
A

FIG. 9A

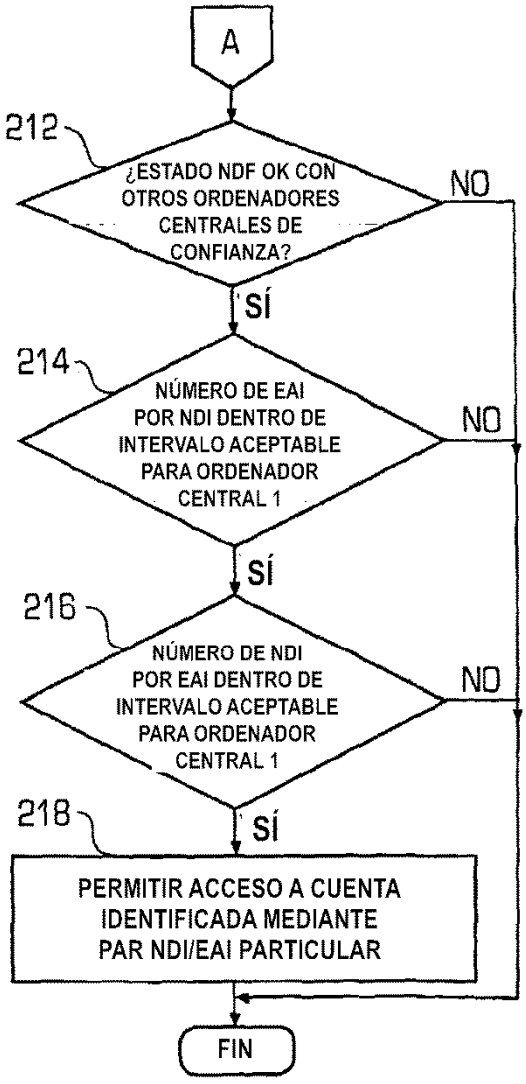
A
212
¿ESTADO NDF OK CON OTROS ORDENADORES CENTRALES DE CONFIANZA?
NO
SÍ
214
NÚMERO DE EAI POR NDI DENTRO DE INTERVALO ACEPTABLE PARA ORDENADOR CENTRAL 1
NO
SÍ
216
NÚMERO DE NDI POR EAI DENTRO DE INTERVALO ACEPTABLE PARA ORDENADOR CENTRAL 1
NO
SÍ
218
PERMITIR ACCESO A CUENTA IDENTIFICADA MEDIANTE PAR NDI/EAI PARTICULAR
FIN

FIG. 9B

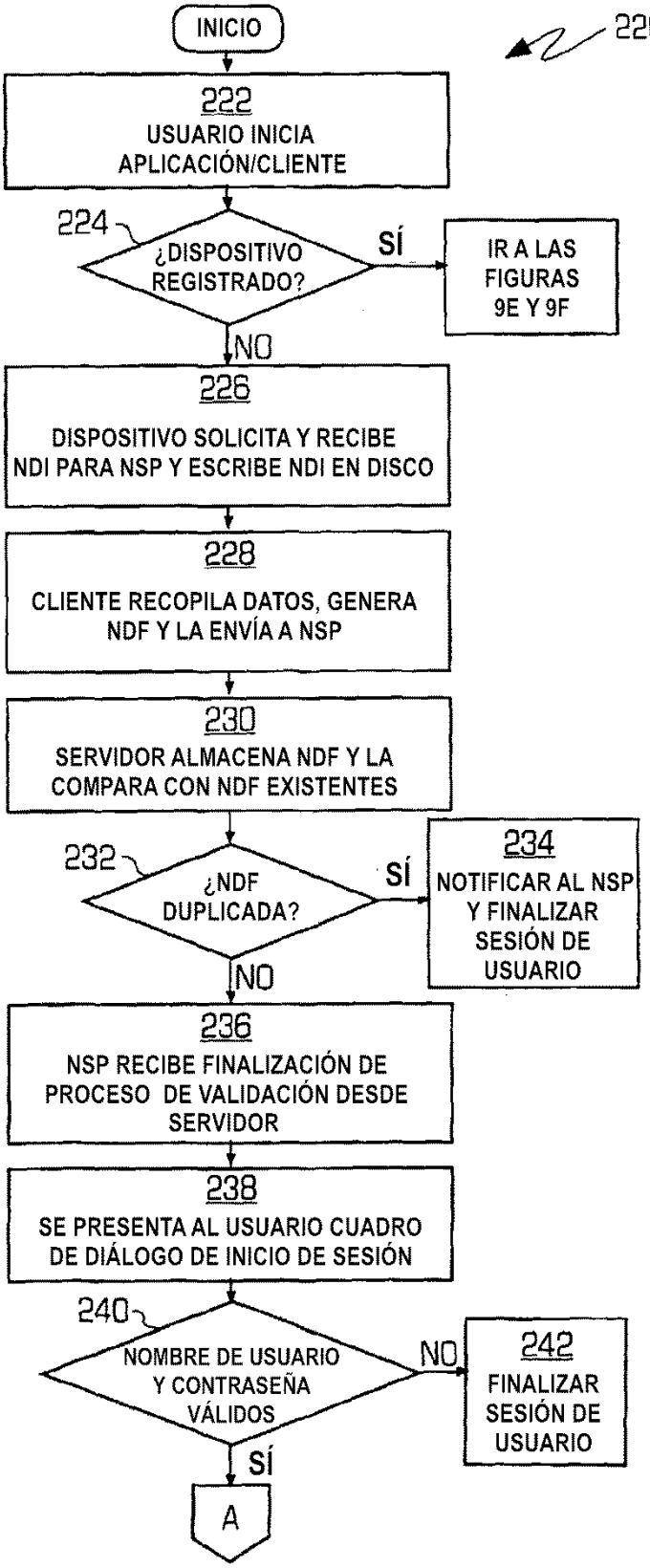
INICIO
220
222
USUARIO INICIA APLICACIÓN/CLIENTE
224
¿DISPOSITIVO REGISTRADO?
SÍ
IR A LAS FIGURAS 9E Y 9F
NO
226
DISPOSITIVO SOLICITA Y RECIBE NDI PARA NSP Y ESCRIBE NDI EN DISCO
228
CLIENTE RECOPILA DATOS, GENERA NDF Y LA ENVÍA A NSP
230
SERVIDOR ALMACENA NDF Y LA COMPARA CON NDF EXISTENTES
232
¿NDF DUPLICADA?
SÍ
234
NOTIFICAR AL NSP Y FINALIZAR SESIÓN DE USUARIO
NO
236
NSP RECIBE FINALIZACIÓN DE PROCESO DE VALIDACIÓN DESDE SERVIDOR
238
SE PRESENTA AL USUARIO CUADRO DE DIÁLOGO DE INICIO DE SESIÓN
240
NOMBRE DE USUARIO Y CONTRASEÑA VÁLIDOS
NO
242
FINALIZAR SESIÓN DE USUARIO
SÍ
A

FIG 9C

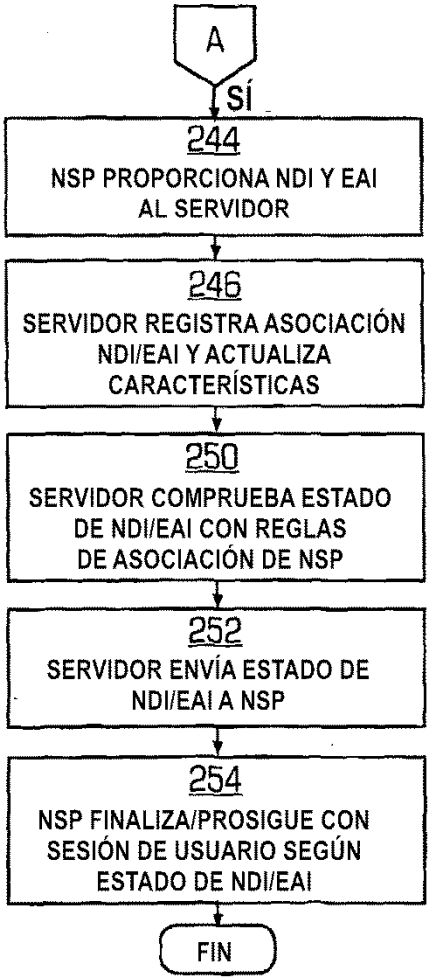
A
SÍ
244
NSP PROPORCIONA NDI Y EAI AL SERVIDOR
246
SERVIDOR REGISTRA ASOCIACIÓN NDI/EAI Y ACTUALIZA CARACTERÍSTICAS
250
SERVIDOR COMPRUEBA ESTADO DE NDI/EAI CON REGLAS DE ASOCIACIÓN DE NSP
252
SERVIDOR ENVÍA ESTADO DE NDI/EAI A NSP
254
NSP FINALIZA/PROSIGUE CON SESIÓN DE USUARIO SEGÚN ESTADO DE NDI/EAI
FIN

FIG. 9D

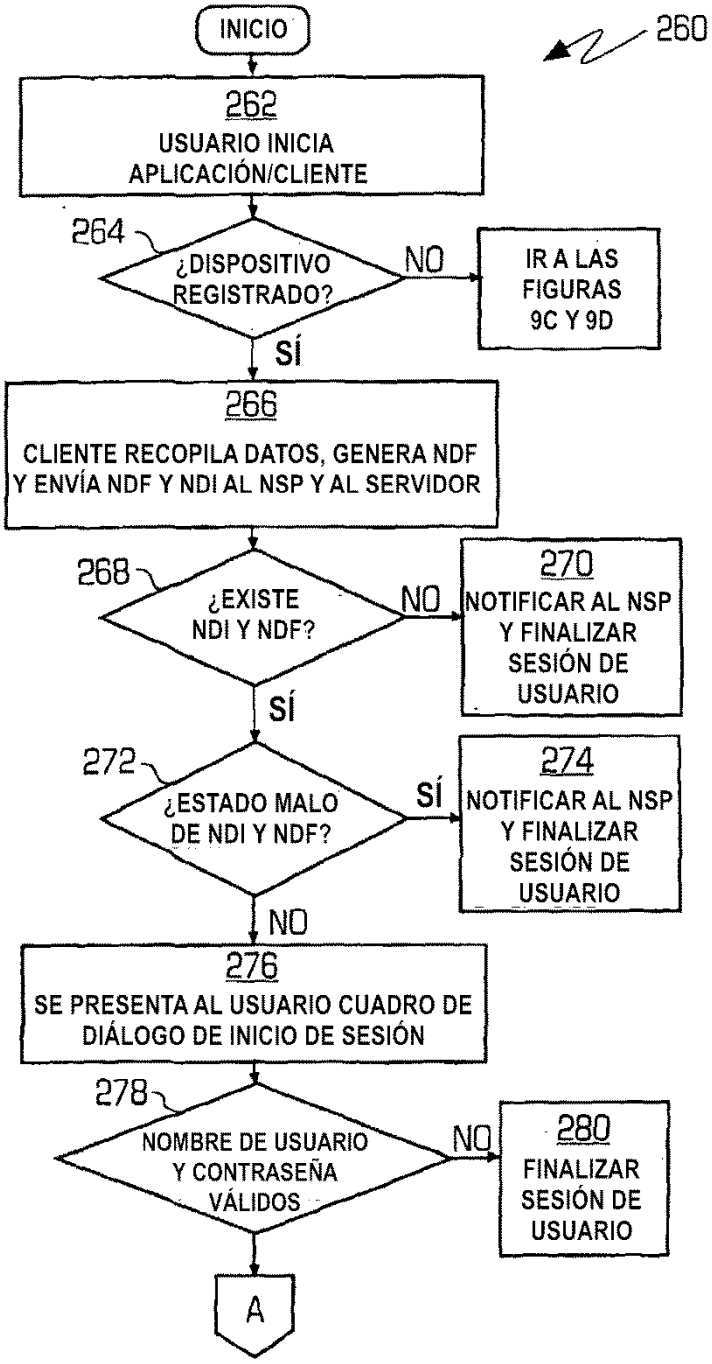
INICIO
260
262
USUARIO INICIA APLICACIÓN/CLIENTE
264
¿DISPOSITIVO REGISTRADO?
NO
IR A LAS FIGURAS 9C Y 9D
SÍ
266
CLIENTE RECOPILA DATOS, GENERA NDF Y ENVÍA NDF Y NDI AL NSP Y AL SERVIDOR
268
¿EXISTE NDI Y NDF?
NO
270
NOTIFICAR AL NSP Y FINALIZAR SESIÓN DE USUARIO
SÍ
272
¿ESTADO MALO DE NDI Y NDF?
SÍ
274
NOTIFICAR AL NSP Y FINALIZAR SESIÓN DE USUARIO
NO
276
SE PRESENTA AL USUARIO CUADRO DE DIÁLOGO DE INICIO DE SESIÓN
278
NOMBRE DE USUARIO Y CONTRASEÑA VÁLIDOS
NO
280
FINALIZAR SESIÓN DE USUARIO
SÍ
A

FIG. 9E


A
SÍ
282
NSP PROPORCIONA NDI Y EAI AL SERVIDOR
284
SERVIDOR REGISTRA ASOCIACIÓN NDI/EAI Y ACTUALIZA CARACTERÍSTICAS
286
SERVIDOR COMPRUEBA ESTADO NDI/EAI CON REGLAS DE ASOCIACIÓN DE NSP
288
SERVIDOR ENVÍA ESTADO DE NDI/EAI AL NSP
290
NSP FINALIZA/PROSIGUE CON SESIÓN DE USUARIO SEGÚN ESTADO DE NDI/EAI
FIN

FIG. 9F