(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 367**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/33 (2013.01)
G06Q 20/34 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/10 (2006.01)
H04L 29/06 (2006.01)
G06Q 30/06 (2012.01)
G06F 21/40 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.05.1999 PCT/US1999/11196**

(87) Fecha y número de publicación internacional: **25.11.1999 WO99060483**

(96) Fecha de presentación y número de la solicitud europea: **20.05.1999 E 99924403 (1)**

(97) Fecha y número de publicación de la concesión europea: **18.01.2017 EP 1080415**

(54) Título: **Sistema y método para la autentificación de usuarios de red**

(30) Prioridad:

21.05.1998 US 86258 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

EQUIFAX INC. (100.0%)
1600 PEACHTREE STREET, N.W.
ATLANTA, GA 30309, US

(72) Inventor/es:

FRENCH, JENNIFER y
WILDER, JONE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y método para la autentificación de usuarios de red

La invención se refiere a las comunicaciones electrónicas, y más particularmente a la autentificación de la identidad de los usuarios de red.

Una variedad de redes se usan hoy en día. Las redes de ordenadores incluyen redes de área local (LAN), redes de área metropolitana (MAN), redes de área extensa (WAN), intranets, Internet y otros tipos de redes. Las redes de comunicación incluyen aquellas para el servicio de telefonía convencional, las redes móviles de diferentes variedades, los servicios de mensajería mediante busca y otras. Las redes se usan para muchos propósitos, incluyendo para comunicar, para acceder a los datos y para ejecutar transacciones. Por muchas razones, incluyendo la seguridad, a menudo es necesario confirmar o autentificar la identidad de un usuario antes de permitir el acceso a los datos o una transacción a ocurrir en la red.

Un enfoque conocido a la autentificación de la red informática es el uso de contraseñas específicas de usuario. Las contraseñas proporcionan algún nivel de protección, pero no son a prueba de fallos. Una razón por la que las contraseñas son vulnerables es que los usuarios a menudo las comparten. Incluso si se mantienen privadas, alguien que quiera obtener una contraseña con suficiente vehemencia a menudo puede, usando generadores aleatorios, monitores de teclados u otras técnicas. Además, cuando se trata con usuarios desconocidos tales como personas que quieren llevar a cabo una transacción electrónica a través de Internet, las contraseñas ad hoc no son prácticas.

Existen varios esquemas sin contraseña que realizan algún nivel de autentificación antes de autorizar transacciones o permitir el acceso a los datos. Estos sistemas generalmente requieren que un usuario proporcione una muestra de información de identificación básica tal como el nombre, la fecha de nacimiento, el número de la seguridad social, la dirección, el número de teléfono y la información del carnet de conducir. Este tipo de información, a veces conocida como información de tipo cartera, se compara con datos conocidos tales como el archivo de crédito para determinar como de bien la entrada del usuario coincide con esa fuente.

Por varias razones, los esquemas de autentificación de un nivel no son totalmente fiables. En algunos casos, un usuario que proporciona una información de identificación precisa puede no ser autentificado. Esto puede ocurrir, por ejemplo, porque el usuario introduce un apodo o una contracción en lugar de un nombre propio, y el proceso de autentificación no comprueba por un apodo u otra variación. Como resultado, un usuario que debería ser autorizado para acceder a la información o realizar una transacción no puede. Otras inconsistencias pueden desencadenar un falso negativo, y a menudo el falso negativo terminará la transacción sin más procesamiento o consulta correctiva.

En otros casos, un usuario que suministra información fraudulenta puede ser autentificado. Esto puede ocurrir cuando información de tipo cartera perdida o robada es introducida por un usuario no autorizado. Otras situaciones pueden llevar también a un resultado de falso positivo.

Tanto los falsos positivos como los falsos negativos son indeseables.

Existen otras razones para el rechazo injustificado del compendio, y otros inconvenientes.

El documento US 5,712,914 describe un método y aparato para comunicar información que comprende proporcionar un dato que incluye un certificado digital que contiene los datos.

El documento US 5,436,972 describe una autentificación multi factor haciendo preguntas conocidas por el usuario. Un objetivo de una realización de la invención es superar estos y otros inconvenientes de los sistemas y métodos de autentificación existentes.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que realice un primer nivel de autentificación basándose en un primer tipo de información y que, basándose en los resultados del primer nivel de autentificación, determine si realizar al menos un segundo nivel de autentificación usando otro tipo de información.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que determine si realizar al menos un segundo nivel de autentificación dependiendo en la información disponible y el nivel de certeza deseado.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que incluye una característica de consulta interactiva automática.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que procese previamente la información suministrada por el usuario para comprobar, por ejemplo, la estandarización, el formato, la validez y consistencia interna de esa información antes de compararla con los datos conocidos.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que sea personalizable.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que acceda a la información desde una variedad de fuentes de datos.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que permita la selección de las fuentes de datos usadas para la comparación, y las circunstancias bajo las cuales se hacen esas comparaciones.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación que genere una puntuación que indica el nivel de confianza o certeza de la autentificación.

Otro objetivo de una realización de la invención es proporcionar un sistema y un método de autentificación en el cual se debe establecer una puntuación o requisito mínimos para los campos de datos o fuentes particulares.

La invención se define en las reivindicaciones.

En una realización ilustrativa de la invención, un usuario que desea solicitar una transacción en línea accede a una red cliente/servidor a través de un terminal de cliente. El lado del servidor de la red incluye un servidor de aplicación que se comunica con un servidor de autentificación. Cuando el usuario desea iniciar la transacción o en otro momento, el servidor de autentificación determina si la identidad del usuario puede ser confirmada, y el nivel de autentificación que se puede acordar a la identidad del usuario basándose en las reglas específicas al proveedor que acepta la transacción.

La transacción que el usuario está solicitando, tal como un comercio de intermediación electrónico, es bien llevado a cabo o no llevado a cabo o es tomada otra acción dependiendo de los resultados de la autentificación. La extensión del procesamiento de la autentificación realizado depende de la naturaleza de la transacción y de los requisitos específicos del proveedor. Una vez que el proceso de autentificación ha sido satisfecho, la invención puede generar un certificado digital registrando los niveles de autentificación y otra información relacionada con el usuario. El certificado digital puede entonces ser presentado en futuras transacciones para evitar la necesidad de volver a autentificar al usuario para cada nuevo evento de la transacción.

Por ejemplo, en el contexto del comercio electrónico, las transacciones de menor riesgo tales como compras relativamente pequeñas puede no requerir un proceso de autentificación extenso. Por otro lado, las transacciones más sensibles o de mayor riesgo tales como grandes compras o datos de acceso sensibles pueden requerir un proceso de autentificación más exhaustivo y un mayor nivel de certeza. Un mayor nivel de seguridad podría ser obtenido posiblemente mediante la realización automática de un proceso de autentificación exhaustivo para cada transacción. Sin embargo, este enfoque incurre en costes o recursos innecesarios en los casos donde sólo se necesita un menor nivel de certeza.

La invención evita estos inconvenientes permitiendo que sean realizados diferentes niveles de autentificación basándose en el nivel de seguridad deseado, reduciendo los costes y el uso innecesario de los recursos del sistema.

Generalmente en la invención, el usuario se autentifica según su habilidad para responder a sucesivas consultas de información personal y el nivel de coincidencia alcanzado al comparar la información que ellos proporcionan con las fuentes de datos fiables. Inicialmente se solicita al usuario proporcionar un primer tipo de información de identificación. El primer tipo de información es preferiblemente información de tipo cartera, esto es, información tal como el nombre, la dirección, el carnet de conducir u otra información que pueda ser comúnmente llevada en la persona. Esta información se transmite al servidor de autentificación que lleva a cabo un proceso de autentificación de primer nivel sobre esa información.

Ese proceso de autentificación de primer nivel compara el grado de coincidencia entre la información de primer tipo suministrada por el usuario y los datos conocidos sobre el usuario de otras fuentes. En la finalización de este proceso de autentificación de primer nivel, el servidor de autentificación puede permitir el acceso solicitado, permitir el acceso solicitado con restricciones, rechazar el acceso o proceder a otro nivel de autentificación.

Preferiblemente, el segundo y cualquier nivel adicional de autentificación solicita una segunda información del usuario, diferente al de tipo cartera. El segundo tipo de información se basa preferiblemente en información relativamente privada que sólo el usuario conocería. Por ejemplo, el segundo tipo de información puede incluir el préstamo hipotecario u otra información obtenida de un informe de crédito u otra fuente. Tal información no es típicamente portada por una persona, y por lo tanto se reducen las posibilidades de fraude por alguien que obtiene información perdida o robada e intenta ejecutar una transacción.

Los datos financieros privados u otros datos obtenidos en el proceso de autentificación de segundo nivel pueden ser solicitados usando una consulta interactiva. La consulta interactiva puede incluir preguntas de selección múltiple que se generan automáticamente sobre la información disponible en las fuentes de datos conocidos. Por ejemplo, el servidor de autentificación puede acceder a un archivo de crédito para identificar los préstamos del usuario que estén aún en estado de amortización. Se pueden seleccionar uno o más préstamos y el nombre del prestamista y la correspondiente cantidad de pago mensual recuperada del archivo de crédito.

La consulta interactiva puede preguntar al usuario por el nombre del prestamista o la cantidad de pago en el préstamo identificado y ofrecer un número de opciones para cada uno de los nombres de prestamistas y de la correcta cantidad de pago, siendo correcta sólo una de ellas.

Dependiendo de las respuestas, la identidad del usuario puede ser totalmente autentificada, o con un mayor o menor grado de certeza comparada con la basada solamente en el proceso de autentificación de primer nivel.

La invención puede incluir una etapa de procesamiento previo ejecutada antes que la autentificación de primer o segundo nivel. La etapa de procesamiento previo filtra o corrige errores relativamente menores en el formato y la consistencia de las respuestas del usuario, preservando la transacción para el procesamiento adicional y evitando la terminación innecesaria antes de que se alcancen las etapas superiores.

Según la invención, se proporciona un método y un sistema como se define en las reivindicaciones.

La invención será ahora descrita por medio de un ejemplo no limitativo con referencia a los dibujos adjuntos, en los cuales:

La Fig. 1 es un diagrama de flujo de un proceso general para autentificar usuarios según la invención.

La Fig. 2 es un diagrama de flujo de un flujo de procesamiento general para autentificar usuarios según la invención en otro aspecto.

La Fig. 3 es un diagrama de flujo de ciertos aspectos de la autentificación de segundo nivel según la invención.

La Fig. 4 es un diagrama de flujo de un proceso de procesamiento previo según la invención.

La Fig. 5 es un diagrama de flujo que representa un proceso de verificación de formato según la invención.

La Fig. 6 es un diagrama de flujo que representa un proceso de estandarización según la invención.

La Fig. 7 es un diagrama de flujo que representa un proceso de verificación de validez según la invención.

La Fig. 8 es un diagrama de flujo que representa un proceso de verificación de consistencia según la invención.

La Fig. 9 ilustra un ejemplo de una matriz de verificación usada en la invención.

La Fig. 10 ilustra un ejemplo de códigos de error que se pueden generar según la invención.

La Fig. 11 ilustra un ejemplo de una matriz de procesamiento previo usada en la invención.

La Fig. 12 ilustra un diagrama de bloques de un sistema general según la invención.

Las Figs. 13 – 16 ilustran un registro de transacción generado según la invención.

Las Figs. 17 y 18 ilustran criterios de reconocimiento de patrones usados por la invención para detectar irregularidades.

La Fig. 19 ilustra la acción potencial tomada por la invención tras la detección de los criterios de reconocimiento de patrones.

La Fig. 20 ilustra una matriz de puntuación para los diferentes tipos de cuentas en la autentificación de segundo nivel según la invención.

La Fig. 21 ilustra una ponderación relativa de los diferentes tipos de consultas usadas en la autentificación de segundo nivel según la invención.

La Fig. 22 ilustra una graduación de las puntuaciones de certeza en un conjunto de categorías según la invención.

Las Figs. 23 – 28 ilustran una asignación de puntuaciones de certeza generales de los resultados de las autentificaciones de primer y segundo nivel según la invención, de mayor al menor.

La Fig. 29 ilustra una graduación de los resultados de las autentificaciones para los diferentes tipos de cuentas de origen según la invención.

La Fig. 30 ilustra los umbrales de acción para un conjunto de acciones diferentes según la invención.

Las Figs. 31 – 33 ilustran el procesamiento previo y las consultas de la autentificación de primer nivel en una sesión de autentificación ejemplar según la invención.

Las Figs. 34 – 36 ilustran las consultas de la autentificación de segundo nivel en una sesión de autentificación ejemplar según la invención.

Las Figs. 37 – 40 ilustran las consultas usadas para emitir un certificado digital según la invención.

La Fig. 41 ilustra un certificado digital generado según la invención.

La Fig. 42 ilustra un sistema de autentificación remoto según la invención en el cual la autentificación se realiza de un modo fuera de línea.

La Fig. 43 ilustra la realización de la autentificación remota fuera de línea de la invención que opera cuando se suministra un campo de datos del número de la seguridad social.

La Fig. 44 ilustra la realización de la autentificación remota fuera de línea de la invención que opera cuando no se suministra un campo de la seguridad social.

La Fig. 45 ilustra un diagrama de bloques de un sistema general según la invención, en otro aspecto.

La invención en general opera en un entorno de red y proporciona un sistema y un método para autentificar una identidad de un usuario de la red usando una jerarquía de consultas de información. La invención puede recurrir a información de una o más fuentes de datos para ejecutar la jerarquía de etapas de autentificación, dependiendo de la transacción o la sensibilidad de los datos. La invención puede ajustar dinámicamente la extensión de la autentificación necesaria, basándose en umbrales preestablecidos o en pruebas de validez de la entrada según el usuario suministra esa información.

Una interfaz de etapa de procesamiento previo puede servir para filtrar o corregir información errónea tal como un código postal equivocado, dígitos olvidados u otras cuestiones de forma para que se pueda preservar la transacción sin una terminación innecesaria antes de la autentificación de primer o segundo nivel. En la conclusión del proceso de autentificación, la invención puede emitir un certificado digital a la máquina del usuario para registrar la información de autentificación, para presentarla para transacciones posteriores o para actualizarla. Una ilustración de la arquitectura general de la invención está en la Fig. 45, y los diagramas de flujo del flujo de procesamiento general se muestran en las Figs. 1 y 2.

En términos del entorno de red de la invención, en una realización ilustrada en la Fig.12, el cliente 110 se comunica con el servidor 120 de aplicación sobre un enlace 150 de transmisión físico o inalámbrico. El enlace 150 de transmisión puede ser una conexión a Internet directa o incluir Internet como un segmento intermedio. El enlace 150 de transmisión puede incluir una conexión a Internet telefónica, un acceso a un servidor por marcación, una conexión a una intranet, una línea digital T1 o T3, una línea digital ISDN, una conexión LAN, una red de área extensa, Ethernet, una conexión DSL u otra conexión por cable o inalámbrica.

En un contexto de Internet, el servidor 130 de aplicación preferiblemente contiene software de servidor de Internet (tal como el paquete Apache disponible públicamente u otros) que se comunica con una aplicación del navegador residente en un cliente 110, que puede ser un ordenador personal o una estación de trabajo ejecutando los sistemas operativos Microsoft Windows™ 95 o 98, un dispositivo de acceso a Internet como una unidad WebTV™, u otro hardware o software.

El sistema incluye un servidor 120 de autentificación en el cual el proceso 10 de autentificación de la invención es residente y se ejecuta. El proceso 10 de autentificación se puede implementar por ejemplo en instrucciones de máquina programadas, tales como en C, C++, Java u otro lenguaje de programación informático compilado, interpretado u otro. En una realización alternativa, el proceso 10 de autentificación puede ser corresidente en un servidor 130 de aplicación, obviando la necesidad del servidor 120 de autentificación. El servidor 120 de autentificación y el servidor 130 de aplicación puede ser cada uno una estación de trabajo o un ordenador personal, por ejemplo ejecutando los sistemas operativos Unix, Linux o Microsoft Windows™ NT™ u otro hardware o software, y cada uno puede comunicarse con varias bases de datos para obtener la información de identificación de usuario para la autentificación de primer y segundo nivel.

Como se ilustra en la Fig. 12, tales bases de datos pueden incluir una base de datos 160 de crédito, una base de datos 170 de correo, una base de datos 180 de teléfono y una o más otras bases de datos 190 que pueden ser directa o indirectamente accesibles o por residentes en el servidor 120 de autentificación o por el servidor 130 de aplicación. Además, la base de datos 152 de autorización se asocia y comunica con el servidor 120 de autentificación. El proceso 10 de autentificación preferiblemente recibe y almacena los datos en y desde la base de datos 152 de autorización, que incluye un registro 112 de transacción (ilustrado en las Figs. 13 – 16) que registra las entradas de usuario, consultas y otra información como un registro temporal o permanente.

La Fig. 12 también muestra uno o más recursos 140 que son accesibles para el servidor 130 de aplicación. Estos pueden incluir, por ejemplo, las bases de datos, otros ordenadores, memorias electrónicas, CD ROMs, almacenamiento RAID, cinta u otro almacenamiento de archivo, enrutadores, terminales, y otros periféricos y recursos.

Según la invención, se solicita a un usuario que quiere acceder a la información o procesar una transacción sobre una red que envíe información al proceso 10 de autentificación a través del cliente 110. El proceso 10 de

autentificación invoca el paso 26 de procesamiento previo, en el cual se solicita al usuario que suministre una información de identificación de usuario de primer tipo. La información de identificación de usuario de primer tipo comprende preferiblemente información de tipo cartera tal como el nombre, la dirección, el número de teléfono, el número de la seguridad social, el número del carnet de conducir y otra información personal común.

Esta información se suministra al proceso 10 de autentificación a través de un servidor 130 de aplicación, en un formato de aplicación estándar, por el cliente 110. En un aspecto de la invención, el servidor 130 de aplicaciones se puede operar por un proveedor en línea, tal como una firma de corredores, un minorista de mercancías u otro (véase por ejemplo la Fig. 45) y sirve como un conducto entre el cliente 110 y el servidor 120 de autentificación una vez que se invoca el proceso 10 de autentificación. Sin embargo es posible para el cliente 110 y el servidor 120 de autentificación comunicar los datos solicitados directamente sin pasar a través del servidor 130 de aplicación.

El usuario introduce la información de primer tipo solicitada en el cliente 110. Los datos del usuario se pueden consultar a través de preguntas textuales, interfaces de usuario gráficas (GUI), formularios de marcas de hipertexto (HTML) o cualquier otro mecanismo adecuado, bien en un entorno interactivo en tiempo real o a través de un envío por lotes. La selección del modo de entrada puede depender de varios factores tales como la carga y disponibilidad de recursos, el modelo de negocio, el tráfico de usuario y de sistema y la criticidad de la transacción.

Tras la inicialización del registro 112 de transacción, se puede ejecutar el control 24 de asociación. Antes de entrar en el paso 26 de procesamiento previo, el proceso de autentificación puede invocar el control 24 de asociación para evaluar si la solicitud bajo consideración se asocia con otras solicitudes o intentos, si recientes, concurrentes o lo contrario. El propósito de los controles de asociación es filtrar las solicitudes sospechosas de ser fraudulentas o parte de un ataque de algún tipo. El reconocimiento de patrones (ilustrado en las Figs. 17 y 18) se puede usar para identificar solicitudes que deberían ser identificadas como que tienen un defecto fatal o potencial para el fraude, requiriendo el rechazo inmediato de la solicitud.

En una realización preferida, el proceso 10 de autentificación almacena la información recibida a través de todas las solicitudes en la base de datos 152 de autorización, que almacena el registro 112 de transacción que registra todas las entradas recibidas del usuario. Usando esta información, se facilitan los controles de asociación basados en los datos disponibles. Por ejemplo, si un intento de acceso incluye un nombre y un número de la seguridad social asociado, se puede denegar una solicitud concurrente o posterior con el mismo nombre pero un número de la seguridad social diferente o marcar para una autentificación adicional.

En cambio, si la solicitud posterior incluye un nombre diferente al número de la seguridad social previamente enviado, la solicitud se puede denegar también o marcar para una autentificación adicional. Los controles de asociación pueden examinar cualquier dato proporcionado por el usuario antes o durante el paso 26 de procesamiento previo.

Tras el control 24 de asociación, el paso de procesamiento previo puede ocurrir en uno o más de entre el cliente 110 de autentificación, el servidor 120 de autentificación y el servidor 130 de aplicación. El paso 26 de procesamiento previo en el cliente 110 se puede efectuar a través del uso de, por ejemplo, la transmisión de los applets de Java al cliente 110 o a través de otro software residente o que se ejecuta en el cliente 110. Así, aunque el proceso 10 de autentificación se muestra en la Fig. 12 como residente en el servidor 120 de autentificación, partes o todo el proceso 10 de autentificación se puede distribuir en otro lugar.

Una ventaja del paso 26 de procesamiento previo es que procesa tantos datos solicitados como sea posible antes de recuperar los datos desde las fuentes de datos almacenados por separado tales como los archivos de crédito, que pueden ser caros en términos de recursos de procesamiento, tiempo y coste. Estos archivos de datos separados pueden ser accesibles a través de Internet u otras redes, pueden ser propiedad de entidades separadas y pueden implicar un cargo por acceso. El paso 26 de procesamiento previo implica en un sentido asegurar que el formato de los datos es coherente entre la información suministrada por el usuario y lo que se espera en las bases de datos.

El paso 26 de procesamiento previo así ayuda a asegurar que los datos suministrados son tan precisos como sea posible para aumentar la probabilidad de generar una coincidencia cuando la identidad del usuario es genuina. Esto reduce los falsos negativos debidos a las inconsistencias tales como el suministro de apodos en lugar de un primer nombre completo, las contracciones, títulos que faltan, o formatos incompatibles de números de la seguridad social aplicados contra las fuentes de datos conocidas.

Si se determina que los datos suministrados por el usuario no son factibles, son incorrectos, u otra cosa claramente deficiente antes de solicitar los datos de las fuentes de datos separadas, es aún posible proceder a aquellas otras fuentes de datos después de que la entrada del usuario ha sido revisada para encontrar los mínimos requerimientos sin interrumpir la transacción general.

Si el usuario no responde a una solicitud para un punto de información obligatorio (por ejemplo, el nombre) es preferible volver a solicitar al usuario ese campo antes de incurrir en cualquier cargo de base de datos o gastar recursos de procesamiento adicionales. Otro ejemplo donde la intercepción en esta manera es beneficiosa es cuando un usuario suministra un número de la seguridad social de seis dígitos. En este caso está claro que la

respuesta es deficiente y no es posible ninguna coincidencia en las bases de datos del número de la seguridad social, así que esas bases de datos no deberían ser accedidas innecesariamente.

En una realización preferida, el paso 26 de procesamiento previo puede realizar una o más de los siguientes controles de validación.

1) Controles de Campo Estándar. Para determinar si todos los campos de información requeridos están presentes y en el formato apropiado y si no, volver a solicitarlos o reformatearlos como sea necesario a la forma adecuada.

2) Control de Seguridad Social. El número de la seguridad social introducido se compara con una o más tablas de números de la seguridad social publicadas o se procesa usando uno o más algoritmos para determinar su validez. Estas tablas pueden incluir información tal como números reportados como fallecidos o fraudulentos.

3) Controles de Dirección y Teléfono. La dirección y el número telefónico proporcionados se verifican por consistencia (esto es, la ciudad, el estado, y el código postal concuerdan; el código de área concuerda con el estado) y se estandariza la dirección del usuario. La estandarización permite una coincidencia más exacta con otras bases de datos en etapas posteriores del proceso 10 de autentificación. Durante el paso 26 de procesamiento previo, el rechazo o marcado para una autentificación adicional puede ocurrir como resultado de las discordancias.

4) Control de Validación del Carnet de Conducir. La entrada del número del carnet de conducir se procesa para verificar que el número es válido para el estado de emisión. Estos algoritmos se pueden obtener a través de los departamentos de vehículos de motor o de otra manera.

La siguiente información se solicita preferiblemente (R que es requerido, O que es opcional) por el proceso 10 de autentificación durante el paso 26 de procesamiento previo y es suministrada por el usuario:

Tabla 1

DESCRIPCIÓN	REQ/OPC
Apellido	R
Nombre de Pila	R
Inicial del segundo nombre	O
Sufijo	O
Nombre de Soltera, si aplica	O
Dirección Actual (CA)	R
en CA Indicador de < 2 Años (S/N)	R
Dirección Anterior	R sólo si en CA Indicador < de 2 Años es S, de lo contrario Opcional
Número de Teléfono de Casa	R
Indicador de Cambio de Código de Área (S/N)	R
Indicador de Teléfono de Casa Publicado (S/N)	R
Número de Teléfono de Trabajo	O
Género	R
Fecha de Nacimiento	R
Número de la Seguridad Social	R
Indicador de Carnet de Conducir (S/N)	R
Número de Carnet de Conducir (DL)	R sólo si el Indicador DL se establece a S, de lo contrario Opcional
Estado de Emisión del Carnet de Conducir	R sólo si el indicador DL se establece a S, de lo contrario Opcional

DESCRIPCIÓN	REQ/OPC
Nombre de Soltera de la Madre	O
Año de Graduación de la Escuela Secundaria	O
Número de Hermanos	O, incluye medio hermanos y hermanastros
Dirección de Email	O

Otra, información diferente al de tipo cartera, que se usa para posteriores niveles de autentificación, se puede recoger durante el paso 26 de procesamiento previo o se puede diferir hasta una fase posterior del proceso 10 de autentificación. A un usuario que falla al suministrar esta información durante el paso 26 de procesamiento previo se le puede volver a solicitar, y el procesamiento puede o no continuar en el caso de que el usuario nunca suministre la información designada como requerida. Esta información preferiblemente incluye:

Tabla 2

DESCRIPCIÓN	REQ/OPC
Nombre del Prestamista	R, sólo si se usa Autentificación de Segundo Nivel
Número de Cuenta del Préstamo	O
Indicador de Tipo de Préstamo	R, sólo si se usa Autentificación de Segundo Nivel
Cantidad de Pago Mensual	R, sólo si se usa Autentificación de Segundo Nivel

El paso 26 de procesamiento previo puede así incluir un conjunto de controles de validación que incluye controles de campo estándar, validación de número de seguridad social, validación de dirección, validación de código de área, y validación de carnet de conducir y la verificación de otros datos preliminares. Es preferible que el procesamiento previo ocurra en el orden presentado, en parte debido a las dependencias de los datos de los controles posteriores en los previos. Sin embargo, se entenderá que el orden pueda ser reorganizado, y que se puedan emplear diferentes controles de procesamiento previo. Los controles de validación enumerados se discuten en más detalles en orden a continuación.

Primero, los controles de campo estándar preferiblemente ocurren en el cliente 110, donde y cuando los datos solicitados se recopilan, para asegurar que todos los datos requeridos están presentes y todos los datos proporcionados están en el formato apropiado y cumplen con los requisitos mínimos. Completar este procesamiento en el cliente 110 minimiza el número de solicitudes que deben ser terminadas en este temprano punto en el proceso de autentificación debido a datos formalmente incorrectos. Esto es particularmente importante cuando el usuario no está presente en el momento de la autentificación, tal como cuando las solicitudes se envían en forma de lotes en lugar de interactivamente. En general, los controles de campos estándar se aseguran de que un intervalo o un formato de caracteres esperado sean introducidos por el usuario, apropiados a las solicitudes individuales y a los tipos de datos.

Lo siguiente se realiza preferiblemente durante los controles de campos estándar:

1) Todos los campos requeridos deben estar presentes.

2) Todos los campos proporcionados deben estar en el formato apropiado.

- El nombre de pila debe contener al menos una letra.
- Los números de teléfono deben tener 10 dígitos.
- El número de la seguridad social deben tener 9 dígitos.
- El número de la seguridad social no deben tener todos los 9 dígitos iguales.
- Los 3 primeros dígitos del número de la seguridad social no deben ser igual a 000.
- Los 4º y 5º dígitos del número de la seguridad social no deben ser iguales a 00.
- Los últimos 4 dígitos del número de la seguridad social no deben ser iguales a 0000.

3) Los campos especificados deben cumplir requisitos adicionales.

- La edad, derivada de la fecha de nacimiento, debe ser de 18 años o mayor. (Sin embargo, un número de teléfono y un carnet de conducir pueden aún ser verificados, incluso si un archivo de crédito no está disponible)

- La dirección de correo electrónico debe contener un signo @ y un ".com" u otro dominio.

Al usuario se le conceden preferiblemente hasta dos intentos adicionales para corregir cualquier campo que no cumpla los requisitos de control de campo estándar. Si algún campo no se puede corregir después de un total de tres intentos, el proceso 10 de autentificación es preferiblemente abortado. Si la solicitud se ha completado con éxito como se determina por la parte de control de campo estándar del paso 26 de procesamiento previo, la solicitud puede continuar al siguiente control de procesamiento previo.

En la siguiente etapa de controles de campo estándar, el número de la seguridad social se puede ser comprobado para alguno o todos de los siguientes:

- El número de la seguridad social contiene 9 dígitos

- El número de la seguridad social ≠ 000000000, 111111111, ..., 999999999.

- Los primeros 3 dígitos del número de la seguridad social ≠ 000

- Los dígitos 4º y 5º del número de la seguridad social ≠ 00

- Los últimos 4 dígitos del número de la seguridad social ≠ 0000

- El número de la seguridad social no coincide con ningún número de la seguridad social encontrado en la tabla de fraude de números de la seguridad Social.

- El número de la seguridad social está en el intervalo emitido como se determina mediante una búsqueda en la tabla de intervalos de números de la seguridad social.

- La fecha de nacimiento concuerda con las fechas de emisión del número de la seguridad social.

El control contra la tabla de fraude de números de la seguridad social publicada se usa para asegurar que el número de la seguridad social suministrado no está listado como fraudulento. Dicha tabla se puede obtener de varias fuentes que incluyen, por ejemplo compañías que reportan el crédito o de las agencias de la ley. La tabla de intervalos de números de la seguridad social se usa para asegurar que el número de la seguridad social suministrado no es un número inválido. Dicha tabla se puede obtener de varias fuentes que incluyen, por ejemplo, agencias gubernamentales.

Una vez que se ha determinado que el número de la seguridad social ha sido emitido, y que se conoce un intervalo de fechas de emisión, la fecha de nacimiento proporcionada en la solicitud se puede comparar con el intervalo de fechas por coherencia. Así es posible realizar otro control para asegurar que el número de la seguridad social es válido basándose en la información de la fecha de nacimiento.

Al usuario se le da preferiblemente sólo un intento adicional para corregir la información del número de la seguridad social que ha sido rechazado por la comprobación de la validación del número de la seguridad social. Si el número de la seguridad social no se puede aceptar después de un total de dos intentos, el proceso 10 de autentificación es preferiblemente abortado.

A continuación, la validez de la información de dirección se confirma, preferiblemente usando un paquete de corrección y estandarización de la dirección (tal como el paquete PostalSoft disponible de la First Logic Corp.). Para la dirección actual, y la dirección anterior si se proporciona, el paquete puede:

- Verificar que la ciudad, estado y código postal concuerdan. Si sólo se proporcionan una ciudad y un estado, el paquete puede ser capaz de añadir el código postal. Si sólo se proporciona el código postal, el paquete generalmente puede añadir la ciudad y el estado.

- Estandarizar la línea de dirección. El paquete puede corregir nombres de calles mal escritos, completar información que falta y eliminar signos de puntuación y espacios innecesarios.

- Identificar direcciones no entregables (esto es, terrenos desocupados, edificios condenados, etc.).

- Crear un código de estado que diga cómo una dirección de entrada tenía que ser corregida.

- Crear un código de error que diga porqué una dirección de entrada podría no ser coincidente, o asignada.

Las respuestas, o las acciones, para cada uno de los posibles códigos de estado o códigos de error relacionados con la dirección en la matriz 156 de códigos de error (ilustrada en las Figs. 9-11) se proporcionan como salida durante el paso 26 de procesamiento previo. Al usuario se le da preferiblemente solo un intento adicional para corregir cada dirección que haya sido rechazada por la validación de la dirección. Si la dirección no se puede corregir después de un total de dos intentos, la solicitud procede como designada en la matriz 154 de respuestas ilustrada en las Figs. 9-11. La matriz 154 de respuestas se puede ubicar en el servidor 120 de autentificación, en la base de datos 152 de autorización o en otro lugar y servir para asociar los mensajes con los resultados de las pruebas y los registros de las transacciones durante la parte de dirección del paso 26 de procesamiento previo, simultáneamente con el procesamiento general de la aplicación.

En otras palabras, la matriz 154 de respuestas envía mensajes al cliente 110 basados en las pruebas de verificación específicas o basados en el estado actual del registro 112 de transacción. Por ejemplo, el mensaje puede solicitar al usuario que verifique que los datos que se introdujeron son correctos o un mensaje para dirigir al usuario a llamar a una atención al cliente para una intervención manual. La matriz 154 de respuestas es preferiblemente parametrizada, de forma que los mensajes apropiados puedan ser asociados con eventos particulares.

El código de área para el número de teléfono de casa se comprueba preferiblemente para determinar si es válido para el estado suministrado en la dirección actual, en el paso 26 de procesamiento previo. El código de área y el estado proporcionados en conexión con la solicitud se comparan con una entrada para el código de área en una tabla de códigos de área, disponible de una base de datos y otras fuentes. La tabla de códigos de área contiene información de códigos de área para cada una de las ubicaciones de código de área en el área geográfica que se sirve.

La base de datos para el código de área y la información asociada se puede implementar preferiblemente, por ejemplo, usando el paquete MetroNet disponible comercialmente. La información de la base de datos de números de teléfono se puede almacenar en bases de datos 180 de teléfono conectadas a un servidor 120 de autentificación, o de otro modo. La consistencia del código de área con el estado de residencia puede, por ejemplo, ser comprobada.

Al usuario preferiblemente se le da solo un intento adicional para corregir la información del número de teléfono de casa que ha sido rechazada por el control de la validación del código de área. Después de que el número de teléfono de casa ha sido aceptado o después de un total de dos intentos, el proceso indica el resultado, válido o no válido, en el registro 112 de transacción y procede.

A continuación, el número del carnet de conducir se comprueba para asegurar que el formato del número es coherente con el formato para el estado de emisión. Un algoritmo puede buscar el estado de emisión y comparar el número del carnet de conducir proporcionado en la solicitud con el formato aceptado en el estado. Al usuario preferiblemente se le da solo un intento adicional para corregir la información del número del carnet de conducir que ha sido rechazada por el control del carnet de conducir (o se puede terminar inmediatamente, según las preferencias del proveedor). Después de que el número del carnet de conducir haya sido aceptado o después de un total de dos intentos, el proceso 10 de autentificación indica el resultado, válido o no válido, en el registro 112 de transacción y procede.

En el caso de que el usuario estuviera pagando por un producto o servicio con una tarjeta de crédito, el proceso 10 de autentificación puede invocar la verificación de la tarjeta de crédito en este punto. En este caso, los controles se pueden ejecutar contra una base de datos de tarjetas de crédito. Estos controles pueden incluir garantizar que la línea de crédito disponible es suficiente para hacer la compra, asegurando que la dirección de facturación de la tarjeta de crédito en la base de datos coincide con la dirección presentada, y asegurando que la tarjeta de crédito no es robada. Las bases de datos que presentan este tipo de información están disponibles comercialmente.

El paso 26 de procesamiento previo puede así incluir correcciones internas así como comparaciones de datos suministrados por el usuario con los datos conocidos que se pueden obtener de fuentes separadas. Estas fuentes pueden ser bases de datos de terceros tales como base de datos comerciales o gubernamentales, o bases de datos internas. Preferiblemente, sin embargo, el paso 26 de procesamiento previo se limita a comprobar los datos suministrados por el usuario contra los datos de tipo cartera que son accedidos relativamente convenientemente, y locamente. El paso 26 de procesamiento previo por consiguiente ofrece una certeza de autentificación aumentada mediante el uso de bases de datos adicionales y la necesidad de coherencia interna como un predicado para la autentificación de primer y segundo nivel.

En conjunción con los controles llevados a cabo por el paso 26 de procesamiento previo, la base de datos 160 de crédito puede ser cualquier base de datos adecuada de historial de crédito del consumidor disponible a partir de varias fuentes incluyendo las empresas de informes de crédito tales como Equifax™. La base de datos 170 de correo y la base de datos 180 de teléfono puede ser cualquier base de datos adecuada que proporciona información de dirección y teléfono para el área geográfica pertinente (por ejemplo, MetroMail que es un compendio de información suministrada por la compañía operadora regional de Bell). Otras bases de datos 190 pueden incluir, por ejemplo, una base de datos de carnets de conducir de servicios de control que proporciona información sobre la validez del control. Cualquier base de datos disponible comercialmente o interna u otra se puede emplear en el procesamiento de los subpasos de verificación del paso 26 de procesamiento previo.

Además, los controles del paso 26 de procesamiento previo pueden incluir el uso de un modelo de fraude de aplicación de tarjeta de crédito, o algún otro modelo que analice estadísticamente los datos de respuesta. Por ejemplo, los datos suministrados por el usuario se pueden modelar y puntuar según el nivel de confianza basándose en modelos empíricos suministrados por terceros proveedores o disponibles internamente. Una ilustración de los criterios de reconocimiento de patrones que se puede emplear por la invención a este respecto se ilustra en las Figs. 17 y 18. Como se ilustra en esas figuras, en general la invención monitoriza la entrada del usuario registrada en el registro 112 de transacción o de otra manera para los intentos repetitivos de autentificación, los cuales pueden representar intentos de fraude o algún tipo de ataque de red.

En tales casos, y como se ilustra en la matriz 904 de criterios de reconocimiento de patrones mostrada en la Fig. 17, la entrada puede incluir partes válidas de información tales como un número de la seguridad social pero varios intentos infructuosos de encontrar entradas válidas para otros campos. En cualquier momento durante el proceso 10 de autentificación, la invención puede evitar el evento de autentificación y terminar la sesión cuando el reconocimiento de patrones detecta una significativa probabilidad de irregularidad. Las diferentes respuestas a los diferentes tipos de transacciones fraudulentas potenciales detectadas se muestran en la matriz 912 de acción de coincidencia de reconocimiento de patrones de la Fig. 19. Como se ilustra en la figura, diferentes tipos de inconsistencias pueden resultar en acciones diferentes, incluyendo el bloqueo del acceso a entradas fraudulentas sospechosas para tales patrones como el mismo nombre bajo direcciones de correo electrónico. Otras inconsistencias pueden derivar en el inicio del proceso 10 de autentificación de nuevo (entradas QILT) a petición del usuario.

En una realización preferida de la invención, los datos suministrados por el usuario deben coincidir con un registro a partir de al menos dos fuentes de datos para graduarse del paso 26 de procesamiento previo. Esto aumenta el nivel de certeza de que la identidad del usuario es genuina antes de graduarse de esa etapa. La coincidencia de rutinas, implementadas para cada fuente de datos y tipo de control, compara los datos de consulta con los datos de fuentes conocidas y asigna preferiblemente un valor a cada caso de coincidencia. Este valor puede denominado una puntuación de certeza de autenticidad. Una puntuación de certeza de autenticidad se puede acumular basada en los valores colectivos asignados para cada caso de coincidencia del paso 26 de procesamiento previo. La puntuación de certeza de autenticidad se puede emplear y comparar contra umbrales predeterminados para determinar la siguiente acción para la solicitud (esto es, aprobarla, aprobarla con restricciones, denegarla, ir al procesamiento previo de primer u otros niveles).

Si los datos proporcionados por el usuario no cumplen los requisitos de algunos o todos los controles del paso 26 de procesamiento previo, se puede devolver un mensaje al usuario a través del enlace 150 solicitando que se corrijan los datos en cuestión y se reenvíen. Tras el reenvío, los datos de entrada serán analizados de nuevo, Alternativamente, el proceso 10 de autentificación se puede configurar con antelación para rechazar inmediatamente una solicitud basándose en un fallo de satisfacer un nivel mínimo durante el paso 26 de procesamiento previo.

Si la solicitud se identifica como resultado del control 24 de asociación u otro análisis como posiblemente fraudulento usando el control de asociación u otra cosa, se puede devolver un mensaje al cliente 110 indicando que la solicitud no se puede procesar automáticamente y que es necesario un procesamiento manual tal como llamar al servicio de atención al cliente.

Los datos biométricos se pueden emplear bien solos o en combinación con el procesamiento previo anterior así como los niveles posteriores de autentificación para asegurar la identidad de un usuario. Esos datos biométricos pueden incluir, por ejemplo, información de huella dactilar del usuario, capturada de manera analógica o digital, por ejemplo, a través de un periférico de huellas conectado al cliente 110. Los datos biométricos pueden también incluir infrarrojos u otras exploraciones de retina o iris, o la coincidencia de la geometría del dedo o de la mano. Asimismo, los datos biométricos usados por la invención pueden incluir también reconocimiento de escritura, reconocimiento de voz usando muestreo digitalizado u otros medios o entradas de reconocimiento facial de video u otros dispositivos.

Los datos biométricos pueden también incluir coincidencias de bases de datos de ADN. En general, cualquier tecnología biométrica existente ahora o desarrollada en el futuro se puede incorporar a la invención. Los datos biométricos se pueden usar como campos o registro de entrada en el procesamiento previo, en las etapas de primero o segundo nivel de autentificación. Alternativamente, los datos biométricos se pueden usar como una llave para desbloquear y liberar un certificado 902 digital emitido al usuario, para ser almacenado en el cliente 110 o de otra manera.

La Fig. 1 es un diagrama de flujo que ilustra el proceso general de autentificación según la invención. El proceso 10 de autentificación comienza en el paso 12. El proceso 10 de autentificación solicita a un usuario el primer nivel de información en el paso 14. De nuevo, el primer tipo de información es preferiblemente información de tipo cartera, esto es, información tal como el nombre, la dirección, el carnet de conducir u otra información comúnmente llevada en la persona. El usuario introduce esa información de primer nivel a través de un teclado, un ratón, un digitalizador de voz u otro mecanismo de entrada adecuado en el paso 16. El paso 18 identifica que el usuario ha completado la introducción de la información de primer nivel. El paso 20 transmite los datos introducidos. El registro 112 de transacción se inicializa en el paso 22.

El paso 24 realiza un control de asociación en la información introducida por el usuario. El proceso 10 de autentificación puede entonces invocar el paso 26 de procesamiento previo discutido anteriormente. Si se incluye el paso 26 de procesamiento previo, se puede proporcionar también el paso 28, que determina si el paso 26 de procesamiento previo está completo. Si el paso 26 de procesamiento previo no está completo, el proceso 10 de autentificación puede volver al paso 14 para solicitar al usuario información omitida, corregida o adicional, volver al paso 16 para permitir al usuario introducir la información, o finalizar el proceso de autentificación en el paso 30. Si el paso 26 de procesamiento previo está completo, el proceso 10 de autentificación procede al paso 32 de autentificación de primer nivel.

El proceso 10 de autentificación hace corresponder, en el paso 32, la información de primer tipo introducida por el usuario con la información recibida de una o más fuentes de datos separadas. Basándose en esa comparación, el proceso 10 de autentificación determina si la autentificación de primer nivel está completa en el paso 34. Si el primer nivel de autentificación no está completo, el proceso 10 de autentificación puede volver al paso 14 para solicitar al usuario información omitida, corregida o adicional, volver al paso 16 para permitir al usuario introducir la información, o finalizar el proceso de autentificación en el paso 36.

Si el primer nivel de autentificación está completo, el proceso 10 de autentificación determina en el paso 38 si el usuario debería ser autentificado. Si el usuario no ha sido rechazado totalmente pero aún no ha autentificado, el proceso 10 de autentificación procede al paso 40, autentificación de segundo nivel. El paso 40 solicita y prueba la entrada del usuario de un segundo tipo de información, que preferiblemente es información diferente al de tipo cartera.

El proceso 10 de autentificación determina si una solicitud de información se ha repetido más que un número predeterminado de veces en el paso 42. Si los intentos exceden el límite predeterminado, el proceso 10 de autentificación finaliza en el paso 44. SI los intentos no exceden el límite predeterminado, el proceso 10 de autentificación determina si el paso 40 está completo en el paso 46. Si el paso 40 está completo, el proceso 10 de autentificación interpreta una decisión de autentificación en el paso 48, luego finaliza en el paso 50. Si el paso 40 no está completo, el proceso de autentificación puede volver al paso 38 o finalizar en el paso 47.

La Fig. 2 es un diagrama de flujo que ilustra el proceso del paso 32 de autentificación de primer nivel en más detalle. El proceso 32 de autentificación de primer nivel se inicia en un paso 52 de comparación de primer nivel. El paso 52 de comparación de primer nivel compara la información introducida por el usuario con la información sobre el usuario recuperada de una o más fuentes de datos conocidas. El usuario puede ser consultado en el paso 32 de autentificación de primer nivel por información similar a la aceptada durante el paso 26 de procesamiento previo, o por información refinada o adicional. Durante el procesamiento de cualquier información de número de teléfono introducida por el usuario en el paso 32 de autentificación de primer nivel tras el paso 26 de procesamiento previo (pero preferiblemente no en el mismo paso 26 de procesamiento previo), si el usuario indica que han estado en el número de teléfono de casa por menos de cuatro meses, el número de teléfono de casa y la información de origen relacionada puede ser preferiblemente comprobada en más profundidad contra una fuente de ayuda de directorio electrónico, para una mejor actualidad en comparación con una base de datos fuera de línea. Durante el procesamiento de cualquier información del carnet de conducir introducida por el usuario en el paso 32 de autentificación de primer nivel (pero preferiblemente no en el paso 26 de procesamiento previo), cualquier control adicional contra la base de datos de carnets de conducir se puede implementar preferiblemente, por ejemplo, usando la base de datos de carnets de conducir ChoicePoint disponible comercialmente. La información de esa base de datos externa se deriva generalmente de un departamento oficial de registros de vehículos a motor o de información de reclamaciones de seguros, el contenido de la cual puede variar según el estado de emisión. El paso 54 asigna valores y prioridades a cada respuesta introducida por el usuario. A la información que es de mayor importancia se puede asignar a mayor valor o prioridad.

El registro 112 de transacción (ilustrado en las Figs. 13 - 16) inicializado en el paso 22 se usa a través del proceso 10 de autentificación para mantener un registro de la entrada de usuario y los resultados de autentificación. Después de que las consultas apropiadas hayan sido procesadas y todos los resultados hayan sido almacenados en el registro 112 de transacción, el registro 112 de transacción se usa para determinar una puntuación de autentificación con respecto a la solicitud. El paso 56 calcula la puntuación de autentificación total, y opcionalmente, una puntuación para cada fuente de datos, campo de datos, etc. Los resultados se categorizan como un gran éxito (B), un éxito normal (R), un posible éxito (P), o un fallo (N) dependiendo de los resultados. Estos resultados se pueden combinar después con los resultados del proceso 40 de autentificación de segundo nivel para determinar una puntuación general de certeza de autenticidad, como se ilustra en las Figs. 23 – 28 y se discute más adelante.

El proceso 10 de autentificación determina si una o más de las puntuaciones de autentificación son mayores o iguales que un valor o umbral de autentificación predeterminado en el paso 58. Si las puntuaciones de autentificación son mayores o iguales que el valor de autentificación predeterminado, el proceso 10 de autentificación interpreta una decisión de autentificación en el paso 60 y después finaliza en el paso 62.

Si una o más de las puntuaciones son menores que su valor de autentificación predeterminado correspondiente, el proceso 10 de autentificación determina si el nivel de certeza cumple un nivel predeterminado de certeza en el paso 64. Si el nivel de certeza está por debajo del nivel predeterminado de certeza, el proceso 10 de autentificación

finaliza en el paso 66. De lo contrario, el proceso 10 de autentificación determina si es necesaria información de primer tipo corregida o adicional en el paso 68. Si no es necesaria otra información, la autentificación procede al paso 40, autentificación de segundo nivel. Si la información de entrada del usuario necesita ser revisada, el proceso 10 de autentificación puede volver al paso 14 o al paso 16.

Las Figs. 31 – 33 ilustran un conjunto de consultas asociadas con el paso 26 de procesamiento previo y la autentificación 32 de primer nivel en una sesión de autentificación ejemplar según la invención. Como se puede ver en las figuras, estas fases de la invención consultan y procesan información de tipo cartera para alcanzar un primer nivel de confianza sobre la autenticidad de la identidad del usuario.

La Fig.3 es un diagrama de flujo que ilustra el proceso 40 de autentificación de segundo nivel en más detalle. El proceso 40 de autentificación de segundo nivel comienza con el paso 310. El paso 310 accede a la información de segundo tipo disponible a partir de fuentes de datos, tales como un archivo de crédito. El paso 312 solicita al usuario información de segundo tipo desde aquella determinada como disponible en el paso 310. El paso 314 determina si la entrada de usuario coincide con la información accedida.

En la ejecución del proceso 40 de autentificación de segundo nivel, el servidor 120 de autentificación puede acceder a la base de datos 160 de crédito. La base de datos 160 de crédito se puede implementar preferiblemente, por ejemplo, usando un archivo de crédito del consumidor Equifax™ disponible comercialmente, en el formato de archivo ACRO.

Las consultas se pueden transmitir hacia adelante y hacia atrás entre el servidor 130 de aplicación y el servidor 120 de autentificación durante el proceso de autentificación de segundo nivel, usando el formato de consulta Sistema-a-Sistema (STS) para estos tipos de archivos de datos, como se apreciará por las personas expertas en la técnica. La información de línea de crédito devuelta de la base de datos 160 de crédito puede estar en formato fijo de archivo (FFF) Sistema-a-Sistema, consistente con la configuración de archivo ACRO. El proceso 40 de autentificación de segundo nivel ejecuta la búsqueda contra la base de datos 160 de crédito para hacer corresponder la información introducida por el usuario contra los datos en ese archivo.

La búsqueda se puede llevar a cabo según el formato de búsqueda ACRO L90, con resultados de nuevo categorizados como un gran éxito (B), un éxito normal (R), un posible éxito (P), o un fallo (N) dependiendo de los resultados, los cuales en una realización se devuelven al servidor 120 de autentificación comenzando en la posición 285 del segmento de cabecera ACRO en un segmento de 13 bytes. Las coincidencias o no coincidencias se devuelven como banderas lógicas dentro de ese segmento de cabecera.

Si la información coincide, el proceso 10 de autentificación bien proporciona un mayor grado de autentificación en el paso 316 o emite otro grado de autentificación en el paso 318. Si la información no coincide, el proceso 10 de autentificación puede emitir una autentificación de menor grado, volver al paso 312 o finalizar en el paso 324.

Un ejemplo de puntuación usado un una autentificación de segundo nivel según la invención se ilustra en las Figs. 20 y 31. La matriz 906 de puntuación de la Fig. 20 incluye un conjunto de valores de puntos para valores de puntos relacionados con cuentas de línea de comercio que el usuario puede tener, en escala móvil según el grado relativo de importancia de varias cuentas. En general, y como se indica en la matriz de pesos relativos de la Fig. 21, a la identificación apropiada de un nombre de prestamista se le da un mayor peso comparado a la cantidad de pago mensual o los términos de los datos de la cuenta.

En la Fig. 22, las puntuaciones de certeza resultantes se clasifican según cuatro categorías de gran éxito (B), éxito normal (R), éxito probable (P), y fallo (N). Las diferentes combinaciones de cuentas pueden llevar a diferentes puntuaciones máximas, según la fiabilidad o importancia de las cuentas disponibles para el paso 40 de autentificación de segundo nivel.

Tras la finalización de tanto el paso 32 de autentificación de primer nivel como el paso 40 de autentificación de segundo nivel, los resultados de todas las comprobaciones se pueden agrupar para determinar una puntuación general de certeza de autenticidad, valores que se ilustran en la matriz 918 de puntuación general de certeza de las Figs. 23 – 28. En general en estas figuras, los grandes éxitos en los controles al archivo de crédito (autentificación de segundo nivel) contribuyen a una puntuación general de certeza mayor, que se normaliza de 0 a 100. Sin embargo, preferiblemente ningún control único califica o descalifica a un usuario de la autentificación.

Más bien, según la invención la ponderación agregada de todas las respuestas del usuario se tiene en cuenta en una variedad de posibles intervalos de puntuación, dependiendo de cómo de altamente la información que suministraron correlaciona con toda la colección de fuentes de datos usadas por la invención. Los niveles de puntuación se pueden agregar como se muestra en la matriz 920 de asignación de la Fig. 29 para desarrollar una categorización escalonada (B, R, P, N) para todos los nivele de autentificación, y generar respuestas según la tabla 922 de umbrales como se ilustra en la Fig. 30. Mientras los niveles numéricos particulares se muestran en esas matrices, se apreciará que las diferentes puntuaciones y niveles son seleccionables o escalables según las necesidades de la aplicación, en la invención.

Las Figs. 34 – 36 ilustran un conjunto de consultas en forma de una captura de pantalla asociadas con el paso 40 de autentificación de segundo nivel en una sesión de autentificación ejemplar según la invención. En general, en esta etapa el proceso 10 de autentificación identifica y accede a la información de línea de comercio (crédito) para consultar datos de una naturaleza específica y privada, los cuales mejoran el perfil de seguridad del usuario. En el ejemplo mostrado, se consultan tanto el crédito como el comerciante o las cuentas de línea comercio por la identidad del prestamista y las cantidades. La identificación precisa resulta en una autentificación, seguida por la emisión de un certificado 902 digital como se desee.

El sistema y el método de la invención son personalizables para permitir a un proveedor operar un servidor 120 de autentificación para establecer varios parámetros, incluyendo los umbrales o niveles predeterminados en diferentes puntos del proceso 10 de autentificación. Si la autentificación predeterminada o cierto nivel no se ha alcanza para una fuente de datos o campo de datos particulares, el usuario puede no ser elegible para la autentificación, o para un mayor grado de autentificación.

Si un usuario completa con éxito el procesamiento previo, la primera y segunda autentificación, en una realización la invención puede emitir un certificado 902 digital al usuario, como se ilustra en las Figs. 37 – 41. Como se ilustra en las Figs. 37 – 40, tras una indicación de autentificación con éxito el usuario es dirigido a introducir la identificación y la información de reto o contraseña para generar y almacenar el certificado 902 digital. El certificado 902 digital contiene un conjunto de campos que incluyen la identificación de usuario, un número de serie del certificado digital, un periodo de expiración, así como información relacionada con el emisor del certificado digital y los datos de la huella dactilar para el certificado digital.

El certificado 902 digital se puede almacenar preferiblemente de forma segura en el cliente 110, esto es, protegido por la identificación de usuario y la consulta del reto o contraseña antes de que el destinatario pueda liberar el certificado 902 digital para otras transacciones, como se ilustra en las Figs. 37 y 38. El certificado digital 902 puede ser un archivo de datos almacenado en un formato común legible por una máquina que cuando se libera adecuadamente por el usuario se puede presentar a otros servidores de autentificación para transacciones posteriores, como evidencia de identidad y evitando la necesidad de volver a autentificar al usuario para eventos posteriores. Como se ilustra, el certificado 902 digital contiene un campo de expiración, pero el certificado se puede generar para persistir indefinidamente.

El certificado 902 digital se puede actualizar usando un proceso 10 de autentificación completo o abreviado según la invención, según el grado de seguridad requerido para transacciones particulares futuras. Por ejemplo, un certificado 902 digital se puede emitir registrando un grado medio de confianza en la identidad del usuario, pero para ejecutar una transacción sensible, el usuario puede necesitar actualizar y mejorar el certificado 902 digital para realizar esa transacción posterior.

Aunque se ilustra con dos niveles de procesamiento de autentificación, se entenderá que la invención contempla tres o más niveles de autentificación que realizan controles adicionales que usan bases de datos adicionales o que solicitan al usuario más información, cuando sea apropiado para los requisitos de las transacciones. Cualquiera de los niveles del proceso 10 de autentificación se puede implementar a través de un formato de consulta interactivo, por ejemplo, usando una casilla de verificación de elección múltiple. En ningún momento durante la presentación de la consulta interactiva se presenta al usuario con respuestas potenciales que revelan sólo la información correcta, para que la información de identificación no pueda capturarse simplemente entrando en el proceso 10 de autentificación. Además, en la implementación de la invención es posible seguir el proceso 10 de autentificación completo con un paso de caracterización del consumidor, en el cual la identidad del usuario ahora autentificado se asocia con información de compras, viajes, geográfica y otra para permitir un mayor marketing orientado o actividad de transacciones.

En general, en la ejecución del proceso 10 de autentificación de la invención, a las respuestas a las preguntas de consulta interactivas se les da la mayor ponderación relativa, seguidas por los controles de autentificación contra un archivo de crédito del usuario, seguidos por la información del teléfono y luego por la información del carnet de conducir.

Como se muestra en la Fig. 4 y se describió anteriormente, el paso 26 de procesamiento previo se puede realizar antes de la jerarquía de niveles de autentificación e incluir varios procedimientos preliminares, principalmente diseñados para asegurar la coherencia en el formato. La discusión volverá al paso 26 de procesamiento previo para describir la etapa de procesamiento previo en más detalle en conjunción con las Figs. 5-8. Se entenderá que varias combinaciones de la estandarización 400, de la verificación 410 de formato, de la verificación 420 de la coherencia, y de la verificación de la validez 430 de los datos se pueden incorporar en el paso 26 de procesamiento previo. Como se ilustra en la Fig. 1, después de que el paso 26 de procesamiento previo se ejecuta se toma una decisión 218 de si la autentificación debería proceder. La decisión 28 puede resultar en una vuelta al paso 14 inicial o en un final del proceso 10 de autentificación automatizado en el paso 30.

Si el paso 26 de procesamiento previo incluye una verificación 410 de formato, se puede seguir el proceso siguiente. La entrada de usuario se comprueba en el paso 500 para determinar que está en el formato apropiado. Por ejemplo, los datos se pueden comprobar para verificar que los campos requeridos se han introducido (por ejemplo, el nombre

de usuario) o que se ha introducido el número apropiado de caracteres (por ejemplo, nueve dígitos para un número de la seguridad social). Si el resultado del paso 500 de decisión es que los datos no están en la forma apropiada, se toma una determinación en el paso 510 si al usuario se le ha solicitado esta información previamente.

El proceso 10 de autentificación de puede configurar para permitir un número predeterminado de oportunidades al usuario para introducir los datos en el formato correcto. Si el número de intentos excede el número predeterminado, el proceso puede terminar en el paso 520. Si el número predeterminado de oportunidades no se ha excedido, se le puede solicitar al usuario introducir los datos en el formato correcto en el paso 530. Si los datos están en el formato correcto, el proceso procede al paso 540.

La Fig.6 representa el proceso para la estandarización 400 de los datos. En el paso 600 se toma una determinación si los datos están en la forma estándar apropiada. Por ejemplo, se puede verificar la dirección postal del usuario por nombres de calles mal escritos, o signos de puntuación innecesarios. Si la determinación 600 encuentra que los datos no son estándar, se toma una determinación 610 si los datos no estándar pueden ser corregidos. Si los datos pueden ser corregidos, se puede realizar en el paso 620 por procesos internos u otros. Si los datos no pueden ser corregidos, se toma una determinación en el paso 630 si el usuario se le ha solicitado previamente esta información.

El proceso de autentificación se puede configurar para permitir al usuario un número predeterminado de oportunidades para introducir los datos en el formato correcto. Si el número de intentos excede el número predeterminado, el proceso puede terminar en el paso 640. Si el número predeterminado de oportunidades no se ha excedido, se le puede solicitar al usuario introducir los datos estándar en el paso 650. Si los datos están en forma estándar, el proceso procede al paso 660.

La Fig.7 representa el proceso para determinar la validez 430 de los datos. Por ejemplo, la validez se puede verificar mediante la determinación en el paso 700 si los datos son válidos (por ejemplo, el número de la seguridad social coincide con algún número de la seguridad social encontrado en la tabla publicada de fallecidos o fraudulentos). Si se toma la determinación de que los datos son inválidos, se toma una determinación 710 en el paso 710 si al usuario se le ha sido solicitado previamente esta información. Si el número de intentos excede el número predeterminado, el proceso puede actualizar el registro de transacción en el paso 720 para reflejar la presencia de los datos inválidos.

Después de que el registro 112 se actualiza en el paso 720, se toma una determinación adicional en el paso 730 de si el proceso puede proceder con estos datos inválidos. Si no, el proceso puede terminar en el paso 740. Si puede, el proceso puede proceder al paso 750. Si el número predeterminado de oportunidades no se ha excedido, se le puede solicitar al usuario introducir datos válidos en el paso 760. Si los datos son válidos, el proceso procede al paso 750.

Un proceso similar se puede seguir para determinar si los datos son consistentes en el paso 420, como se ilustra en la Fig.8. En el paso 760, se toma la determinación si los datos de entradas de campo separadas son consistentes. Por ejemplo, los datos se pueden comprobar para verificar que el código de área introducido coincide con el código postal introducido. Si se toma la determinación de que los datos introducidos por el usuario no son consistentes, se toma una determinación en el paso 770 si al usuario se le ha solicitado previamente esta información. Si el número de intentos excede el número predeterminado, el proceso puede actualizar el registro 112 de transacción en el paso 780 para reflejar la presencia de los datos inconsistentes.

Después de que el registro 112 se actualiza 780, se toma una determinación adicional en el paso 790 de si el proceso puede proceder con estos datos inconsistentes. Si no, el proceso puede terminar en el paso 800. Si puede, el proceso puede proceder al paso 810. Si el número predeterminado de oportunidades no se ha excedido, se le puede solicitar al usuario introducir datos válidos en el paso 820. Si los datos son válidos, el proceso procede al paso 810 y al siguiente control de procesamiento previo.

Las Figs. 9 – 11 muestran un ejemplo del uso de una matriz para verificar la información de dirección de la validez 430 o coherencia 420 de procesamiento. Como se muestra, el proceso de verificación, que se puede implementar usando PostalSoft comercialmente disponible, genera una matriz de valores de direcciones para determinar cierta información de dirección. La Fig. 10 muestra un ejemplo de ciertos códigos de error que se puede generar para solicitar al usuario respuestas según el formato PostalSoft cuando los valores introducidos, tales como el código postal, no están en el formato apropiado. La Fig. 11 muestra un ejemplo de ciertas acciones y mensajes según otros tipos de datos introducidos durante el procesamiento de la coherencia 420.

Generalmente hablando, hay varias maneras de administrar las consultas en los distintos niveles de autentificación de la invención, dependiendo de los requisitos de la transacción. Si el usuario está disponible en el momento de solicitar un diálogo interactivo (por ejemplo, solicitud de Internet), se crea un cuestionario de opción múltiple preferiblemente dinámico por el proceso 10 de autentificación y se presenta al usuario, a través del cliente 110, para su finalización.

Se seleccionan preferiblemente alternativas de elección múltiple para cada pregunta basándose en los sesgos regionales del usuario, si son aplicables, y se diseñan para hacer difícil para una solicitud fraudulenta adivinar correctamente las respuestas. Esto es, las selecciones potenciales para varias líneas de crédito o proveedores de cuentas comerciales se proporcionan en la misma región geográfica general de la dirección de casa del usuario,

para que los proveedores de cuentas de líneas de crédito no estén obviamente equivocados basándose en la localización. Los puntos de usuario y los clics en sus selecciones, o las respuestas proporcionadas de alguna otra manera adecuada. Las respuestas suministradas por el usuario se devuelven entonces al proceso 10 de autentificación por el cliente 110 para la evaluación automatizada.

Si el usuario no está presente en el momento de la solicitud (por ejemplo, envío por lotes), la información requerida para administrar la validación se proporciona en la solicitud inicial. Si el usuario suministra los números de cuenta, el paso 40 de autentificación de segundo nivel intentará hacer las comparaciones automáticamente. Sin embargo, si las comparaciones no se pueden hacer automáticamente o los números de cuenta no se han proporcionado, las comparaciones se pueden realizar manualmente a través de la intervención humana. Los resultados se devuelven al paso 40 de autentificación de segundo nivel para la evaluación final.

La Fig. 18 ilustra una autentificación ejemplar llevada a cabo según el proceso 10 de autentificación de la invención. En general, como se ilustra en esa figura, el usuario presenta el nombre, el número de la seguridad social, la fecha de nacimiento, el correo electrónico y la información de dirección postal, seguida por el número de teléfono de casa y los datos del carnet de conducir. Esa información se acepta y procesa a través del paso 26 de procesamiento previo y el paso 32 de autentificación de primer nivel, después del cual se determina que los datos son coherentes y merecen proceder al paso 40 de autentificación de segundo nivel.

En el paso 40 de autentificación de segundo nivel, una secuencia de preguntas se presenta en una consulta interactiva dirigida a la información de cuenta hipotecaria, solicitando información del prestamista y cantidad seguida de otra información de cuenta comercial. Siguiendo la autentificación exitosa, se pregunta al usuario si desearían generar un certificado 902 digital, el cual se genera registrando la autentificación exitosa y protegiendo el certificado 902 digital mediante los datos de identificación y la consulta de reto.

Cualquiera o todos los pasos de procesamiento descritos anteriormente se pueden invocar selectivamente o reorganizar para constituir un proceso 10 de autentificación completo. Los requisitos de la transacción determinarán qué procesos combinar para las necesidades de autentificación particulares. Es posible configurar varias implementaciones diferentes como ofertas estándar. La parte que emplea el sistema de autentificación (proveedor) puede bien usar estas ofertas estándar, o personalizar una configuración a sus necesidades. Con cualquier implementación, la invención permite flexibilidad en la determinación de la certeza de autenticidad, bien a través del proceso de configuración o estableciendo umbrales de certeza.

En la práctica de la invención, en el caso de interrupción temporal u otra indisponibilidad de cualquiera de las fuentes de datos usadas para la comparación, la invención puede volver a una fuente de respaldo para ese tipo particular de información (la cual puede ser generalmente coherente pero no como la actual), sustituir otra fuente de datos, o tomar otras acciones.

La Fig. 42 ilustra una realización de autentificación remota fuera de línea de la invención, en la cual algún procesamiento incluyendo la entrega de un ID validado se realiza usando el correo ordinario. Como se ilustra en la Fig. 42, en esta realización, un sistema 1002 de autentificación remota controla dos objetos de procesamiento, un objeto de autentificación remoto con un campo 1004 del número de la seguridad social, y un objeto de autentificación remoto sin un campo 1006 del número de la seguridad social. El sistema 1002 de autentificación remoto invoca el objeto 1004 de autentificación remoto cuando un usuario ha presentado un número de la seguridad social, en una solicitud en línea para un crédito u otra transacción. El objeto 1004 de autentificación remoto puede invocar el paso 26 de procesamiento previo, para procesar los controles de campo estándar como en las otras realizaciones anteriores. En esta realización, en parte por los requisitos para la entrega del correo, fallar uno o más campos de datos para la estandarización de la dirección, tales como los errores en el código postal, los campos en blanco, las direcciones extranjeras, y los no entregables puede resultar en un estado 1018 de fallo. El estado 1018 de fallo se puede alcanzar también cuando la edad es menor que un nivel predeterminado, o como se describió anteriormente los controles de la seguridad social estándar no se cumplen. Otros factores que pueden resultar en un estado 1018 de fallo incluyen mezclar coincidencias relativas a los números de teléfono, los números de la seguridad social y los indicadores de víctimas de fraudes presentes en un archivo de crédito.

Si el objeto 1004 de autentificación remoto determina que el usuario ha alcanzado una puntuación suficiente durante el paso 26 de procesamiento previo y cualquier paso de procesamiento posterior, se puede alcanzar el estado 1008 de paso. Puede resultar la emisión en línea de un certificado 902 digital u otra autentificación. Sin embargo, si el objeto 1004 de autentificación remota determina que la puntuación del usuario está entre aquellas designadas para un estado 1008 de paso y un estado 1018 de fallo, el objeto de autentificación remoto puede ofrecer un estado 1010 de autentificación fuera de línea, en el cual se transmite la verificación usando correo regular.

En esta condición, el estado 1010 de autentificación fuera de línea invoca el filtro 1012 de capacidad de envío por correo, que prueba por coincidencias en la primera inicial, apellido, un número de casa y un código postal de al menos una base de datos de direcciones, así como la coherencia de la edad y la fecha de nacimiento y un número de la seguridad social que es bien válido o no muestra más que un pequeño número de transposiciones de dígitos. Otros criterios pueden ser aplicados. Si se alcanza una puntuación suficiente en el procesamiento del filtro 1012 de capacidad de envío por correo, se alcanza un estado 1014 de correo en el cual la información de direccionamiento

introducida se usa para transmitir un PIN u otra información de identificación al usuario a través del correo regular. Si no se alcanza una puntuación suficiente en el filtro 1012 de capacidad de envío por correo, se alcanza un estado 1016 de fallo, no se manda ninguna verificación por correo y el procesamiento termina.

Si un usuario falla al suministrar un número de la seguridad social, como se ilustra en la Fig. 42 el control se pasa al objeto 1006 de autentificación remoto, que puede aplicar el paso 26 de procesamiento previo y pasos adicionales para probar la información de usuario introducida. Si la información de usuario introducida no alcanza un umbral predeterminado, el control pasa a un estado 1022 de fallo. Si se alcanza una puntuación de autentificación suficiente, el procesamiento procede al objeto 1020 de autentificación fuera de línea. El objeto 1020 de autentificación fuera de línea invoca el filtro 1024 de capacidad de envío por correo que procesa la información introducida por el usuario sin un número de la seguridad social para determinar si la estandarización de la dirección, lo relacionado con la edad, lo relacionado con la dirección, o las banderas de fraude están presentes. Si se alcanza una puntuación de autentificación suficiente en el filtro 1024 de capacidad de envío por correo, el control pasa al estado 1026 de correo, en el cual se transmite un PIN de identificación válido a un usuario en la dirección introducida usando el correo regular. A la inversa, si el filtro 1024 de capacidad de envío por correo no se satisface, se alcanza un estado 1028 de fallo en el que ningún material se envía por correo y el procesamiento termina.

Una realización del sistema 1002 de autentificación remoto se ilustra en más detalle en la Fig. 43, en la cual un objeto 1030 suministrador de la seguridad social prueba si el usuario es capaz de proporcionar un campo número de la seguridad social. Si el usuario es capaz de proporcionar un campo número de la seguridad social, el control procede al módulo 1032 de prueba de paso, el cual puede realizar el paso 26 de procesamiento previo, el paso 32 de autentificación de primer nivel, el paso 40 de autentificación de segundo nivel u otros procesamientos. Si el usuario pasa esos niveles de autentificación con una puntuación suficiente, el control pasa a un estado 1034 de icono ganado, que provee al usuario de un icono de autentificación fuera de línea, un certificado 902 digital u otra verificación emitida.

Si el módulo 1032 de prueba de paso no se pasa, un objeto 1036 de error fatal puede probar por errores fatales en los campos de seguridad social, dirección, relacionados con la edad u otros de datos deseados. Si el objeto 1036 de error fatal no detecta un error fatal, el control pasa a un filtro 1038 de capacidad de envío por correo que prueba la capacidad de envío por correo usando el código postal y el estado, el nombre, la entregabilidad y otros controles de campo, tras los cuales se entra en un estado 1040 de correo si el usuario ha establecido con éxito la información fiable. Después de que se entre en el estado 1040 de correo, se puede enviar por correo regular tanto el PIN como un icono de usuario emitido en el estado 1042 de icono ganado. A la inversa, si bien el objeto 1036 de error fatal o el filtro 1038 de capacidad de envío por correo no son satisfechos con la información que el usuario ha introducido, se entra en un estado 1044 de fallo, y el procesamiento finaliza sin transmitir un ID a través del correo o sin emitir un icono.

Como se ilustra en la Fig. 44, alternativamente si el usuario no es capaz de suministrar un número de la seguridad social al objeto 1030 de prueba de la seguridad social, entonces el control pasa al objeto 1046 de error fatal. Si no es detectado ningún error fatal por el objeto 1046 de error fatal, el control se pasa al filtro 1048 de capacidad de envío por correo, el cual prueba la información de correo entregable, como anteriormente. Si se satisface el filtro 1048 de capacidad de envío por correo, se alcanza el estado 1050 de correo en el cual una identificación de PIN regular se envía a través del correo al usuario, tras lo cual se alcanza un estado 1052 de icono ganado, emitiendo al usuario una identificación de icono en línea. A la inversa, si bien el objeto 1046 de error fatal o el filtro 1048 de capacidad de envío por correo no se satisfacen, se alcanza un estado 1054 de fallo y el procesamiento finaliza.

La descripción anterior del sistema y el método de autentificación de la invención es ilustrativa, y variaciones en la construcción e implementación se les ocurrirán a personas expertas en la técnica. Por ejemplo, mientras que la invención se ha descrito generalmente como que implica a un usuario único que suministra la información de autentificación en una sesión interactiva única o alternativamente en modo por lotes, tanto las consultas como la información introducida por el usuario se pueden proporcionar en diferentes momentos usando diferentes modos de entrada, cuando la transacción lo permita. Este puede ser el caso para el ejemplo de cuando la transacción implique la configuración de una suscripción en línea a publicaciones o servicios.

Para más ejemplo, mientras la invención se ha descrito en un entorno cliente/servidor en el cual un usuario inicia una transacción usando un ordenador personal u otro dispositivo sobre una red informática, el usuario podría iniciar la transacción sobre otras redes. El usuario por ejemplo podría realizar una transacción usando un teléfono móvil equipado con una pantalla alfanumérica que permite al usuario teclear los datos a través de la red celular móvil.

Para aún más ejemplo, mientras la invención se ha ilustrado en términos de un consumidor individual que inicia una transacción de red, la invención puede también verificar la identidad de otras entidades tales como corporaciones, escuelas, unidades gubernamentales y otros que buscan llevar a cabo negocios a través de una red. Estas entidades pueden ser internacionales por naturaleza. El alcance de la invención está orientado consecuentemente a ser limitado sólo por las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método (10) de autentificación de un usuario en una red, comprendiendo dicho método:

realizar un primer paso (32) de autentificación basado en un primer tipo de información;

realizar al menos un segundo paso (40) de autentificación basado en un segundo tipo de información aparte del primer tipo de información, siendo dicho método caracterizado por:

almacenar un registro (22) de transacción del primer paso (32) de autentificación;

en donde al menos uno del primer paso (32) de autentificación y del segundo paso (40) de autentificación comprende generar una consulta interactiva, comprendiendo la consulta interactiva al menos una pregunta que tiene respuestas de opción múltiple , en donde no todas las respuestas son respuestas correctas.

2. El método (10) de la reivindicación 1, en donde la red comprende Internet.

3. El método (10) de la reivindicación 1, en donde la primera información comprende al menos una entre la información del nombre, la información de la dirección, la información del número de la seguridad social, la información del número de teléfono, y la información del carnet de conducir.

4. El método (10) de la reivindicación 1, en donde la segunda información comprende al menos una entre la información de la tarjeta de crédito, la información de la hipoteca, la información de otros préstamos, y la información del pago mensual.

5. El método (10) de la reivindicación 1, en donde la consulta interactiva comprende una pregunta que pide al usuario un nombre de prestamista y una cantidad de pago correcta, en donde hay respuestas de opción múltiple para cada uno de los nombres de prestamistas y de las cantidades de pago correctas, sólo una de las cuales es correcta.

6. El método (10) de la reivindicación 1, en donde el segundo tipo de información comprende la información correspondiente a las cuentas de crédito de las cuales el usuario es una parte, la información correspondiente a las cuentas de crédito comprende la información del préstamo hipotecario, en donde se solicita al usuario identificar al menos una de:

i. la información del prestamista hipotecario; y

ii. la información de la cantidad del préstamo hipotecario.

7. El método (10) de la reivindicación 1, en donde la realización del primer paso de autentificación además comprende:

i. obtener (14, 16) el primer tipo de información del usuario;

ii. recuperar (24) la información de identificación del usuario de una fuente de datos;

iii. comparar (52) el primer tipo de información suministrada por el usuario con la información de identificación de usuario recuperada de la fuente de datos; y

iv. determinar (56) un nivel de correspondencia entre el primer tipo de información suministrada por el usuario y la información de identificación de usuario recuperada de la fuente de datos; y

en donde la fuente de datos para el primer tipo de información se usa para identificar la disponibilidad del segundo tipo de información para el usuario.

8. El método (10) de la reivindicación 1, comprendiendo además:

ejecutar un proceso de reconocimiento de patrones para detectar irregularidades potenciales en al menos uno entre el primer tipo de información y el segundo tipo de información.

9. El método (10) de la reivindicación 1, comprendiendo además:

realizar un paso (1004) de autentificación remoto basado en al menos uno entre el primer tipo de información y el segundo tipo de información.

10. El método (10) de la reivindicación 1 o 9, comprendiendo además:

realizar una autentificación (1010) fuera de línea basada en al menos uno entre el primer tipo de información y el segundo tipo de información.

11. El método (10) de la reivindicación 1, en donde el paso (1010) de realización de la autentificación fuera de línea comprende filtrar a través de filtro (1012) de capacidad de envío por correo al menos uno entre el primer tipo de información y el segundo tipo de información.

12. Un sistema (110, 120, 130, 152) para autentificar un usuario en una red, comprendiendo dicho sistema:

una interfaz (110) de entrada para recibir la información introducida por el usuario; y

un procesador (120, 152), conectado a la interfaz de entrada (110) y configurado para;

realizar un primer paso (32) de autentificación basado en un primer tipo de información; y

realizar al menos un segundo paso (40) de autentificación basado en un segundo tipo de información aparte del primer tipo de información, caracterizada en que:

el procesador (120, 152) se configura para almacenar un registro (112) de transacción del primer paso (32) de autentificación;

en donde el procesador genera una consulta interactiva, comprendiendo la consulta interactiva al menos una pregunta que tenga respuestas de opción múltiple en donde no todas las respuestas son respuestas correctas.

13. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde la red comprende Internet.

14. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde la primera información comprende al menos una entre la información del nombre, la información de la dirección, la información del número de la seguridad social, la información del número de teléfono, y la información del carnet de conducir.

15. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde la segunda información comprende al menos una entre la información de la tarjeta de crédito, la información de la hipoteca, la información de otros préstamos, y la información del pago mensual.

16. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde la consulta interactiva comprende una pregunta que pide al usuario un nombre de prestamista y una cantidad de pago correcta, en donde hay respuestas de opción múltiple para cada uno de los nombres de prestamistas y de las cantidades de pago correctas, sólo una de las cuales es correcta.

17. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde el primer tipo de información comprende información de tipo cartera y el segundo tipo de información comprende información de tipo diferente a cartera correspondiente a las cuentas de crédito de las cuales el usuario es parte.

18. El sistema (110, 120, 130, 152) de la reivindicación 17, en donde el segundo tipo de información además comprende información de préstamo hipotecario; y

en donde el segundo paso de autentificación además comprende una solicitud para el usuario para identificar al menos uno entre:

la información del prestamista hipotecario; y

la información de la cantidad del préstamo hipotecario.

19. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde el primer paso de autentificación además comprende:

i. obtener (14, 16) el primer tipo de información del usuario;

ii. recuperar (24) la información de identificación de usuario de una fuente de datos;

iii. comparar (52) el primer tipo de información suministrada por el usuario con la información de identificación de usuario recuperada de una fuente de datos; y

iv. determinar (52) un nivel de correspondencia entre el primer tipo de información suministrado por el usuario y la información de usuario recuperada de una fuente de datos; y

en donde la información de identificación de usuario recuperada de la fuente de datos se usa para identificar la disponibilidad del segundo tipo de información para el usuario.

20. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde el procesador ejecuta un proceso de reconocimiento de patrones para detectar irregularidades potenciales en la entrada suministrada por el usuario.

21. El sistema (110, 120, 130, 152) de la reivindicación 12, en donde el procesador realiza un paso de autentificación remota basado en al menos uno entre el primer tipo de información y el segundo tipo de información.

22. El sistema (110, 120, 130, 152) de la reivindicación 12 ó 21 en donde el procesador realiza una autentificación fuera de línea basada en al menos uno entre el primer tipo de información y el segundo tipo de información.

23. El sistema (110, 120, 130, 152) de la reivindicación 22 en donde la autentificación fuera de línea comprende aplicar un filtro (1012) de capacidad de envío por correo a al menos uno entre el primer tipo de información y el segundo tipo de información.

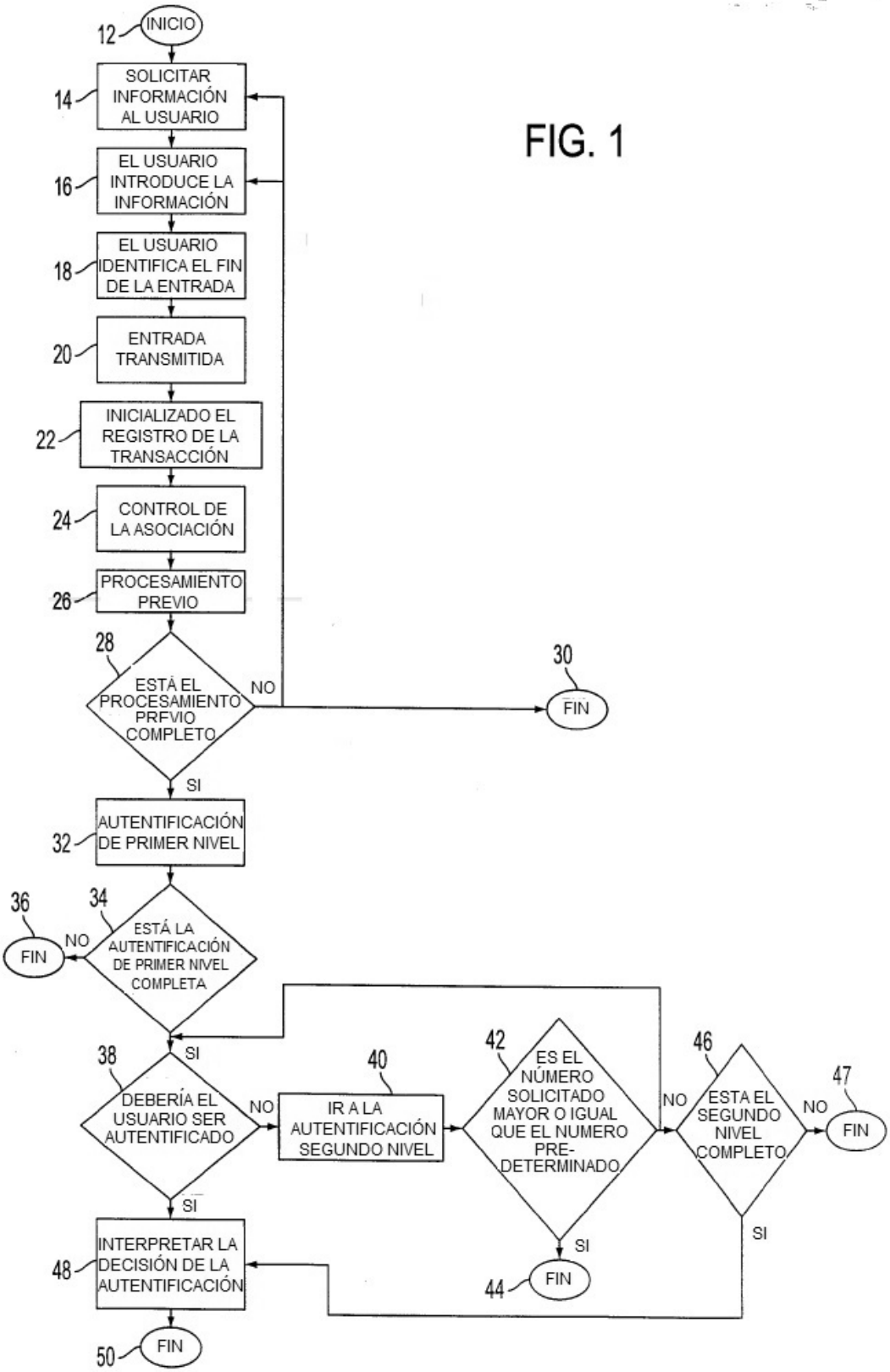

12
INICIO
14
SOLICITAR INFORMACIÓN AL USUARIO
16
EL USUARIO INTRODUCE LA INFORMACIÓN
18
EL USUARIO IDENTIFICA EL FIN DE LA ENTRADA
20
ENTRADA TRANSMITIDA
22
INICIALIZADO EL REGISTRO DE LA TRANSACCIÓN
24
CONTROL DE LA ASOCIACIÓN
26
PROCESAMIENTO PREVIO
28
ESTÁ EL PROCESAMIENTO PREVIO COMPLETO
NO
30
FIN
SI
32
AUTENTIFICACIÓN DE PRIMER NIVEL
34
ESTÁ LA AUTENTIFICACIÓN DE PRIMER NIVEL COMPLETA
36
FIN
NO
SI
38
DEBERÍA EL USUARIO SER AUTENTIFICADO
NO
40
IR A LA AUTENTIFICACIÓN SEGUNDO NIVEL
42
ES EL NÚMERO SOLICITADO MAYOR O IGUAL QUE EL NUMERO PRE-DETERMINADO
NO
46
ESTA EL SEGUNDO NIVEL COMPLETO
NO
47
FIN
SI
SI
44
FIN
SI
48
INTERPRETAR LA DECISIÓN DE LA AUTENTIFICACIÓN
50
FIN

FIG. 1

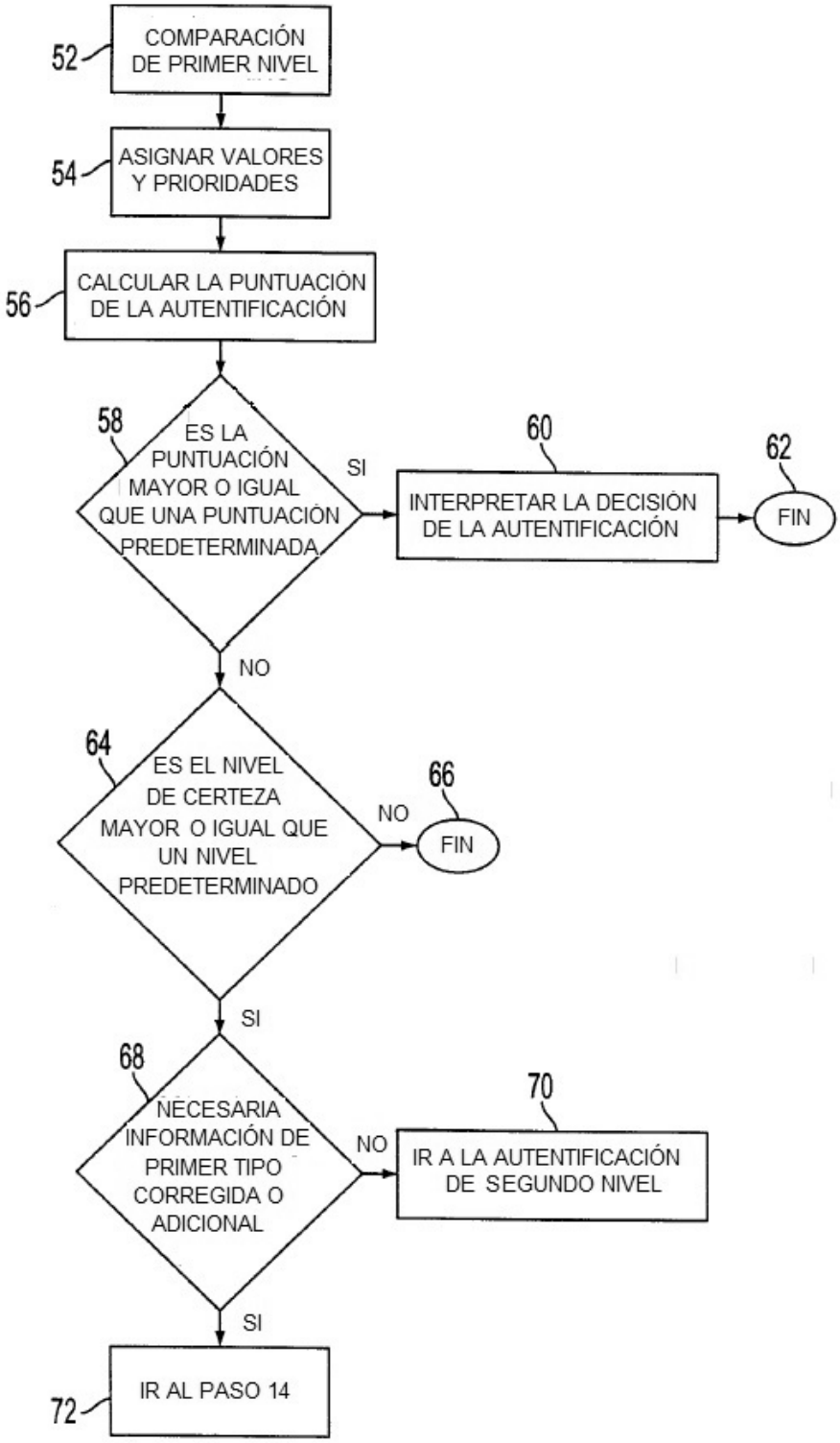

52
COMPARACIÓN DE PRIMER NIVEL
54
ASIGNAR VALORES Y PRIORIDADES
56
CALCULAR LA PUNTUACIÓN DE LA AUTENTIFICACIÓN
58
ES LA PUNTUACIÓN MAYOR O IGUAL QUE UNA PUNTUACIÓN PREDETERMINADA
SI
60
INTERPRETAR LA DECISIÓN DE LA AUTENTIFICACIÓN
62
FIN
NO
64
ES EL NIVEL DE CERTEZA MAYOR O IGUAL QUE UN NIVEL PREDETERMINADO
NO
66
FIN
SI
68
NECESARIA INFORMACIÓN DE PRIMER TIPO CORREGIDA O ADICIONAL
NO
70
IR A LA AUTENTIFICACIÓN DE SEGUNDO NIVEL
SI
72
IR AL PASO 14

FIG. 2

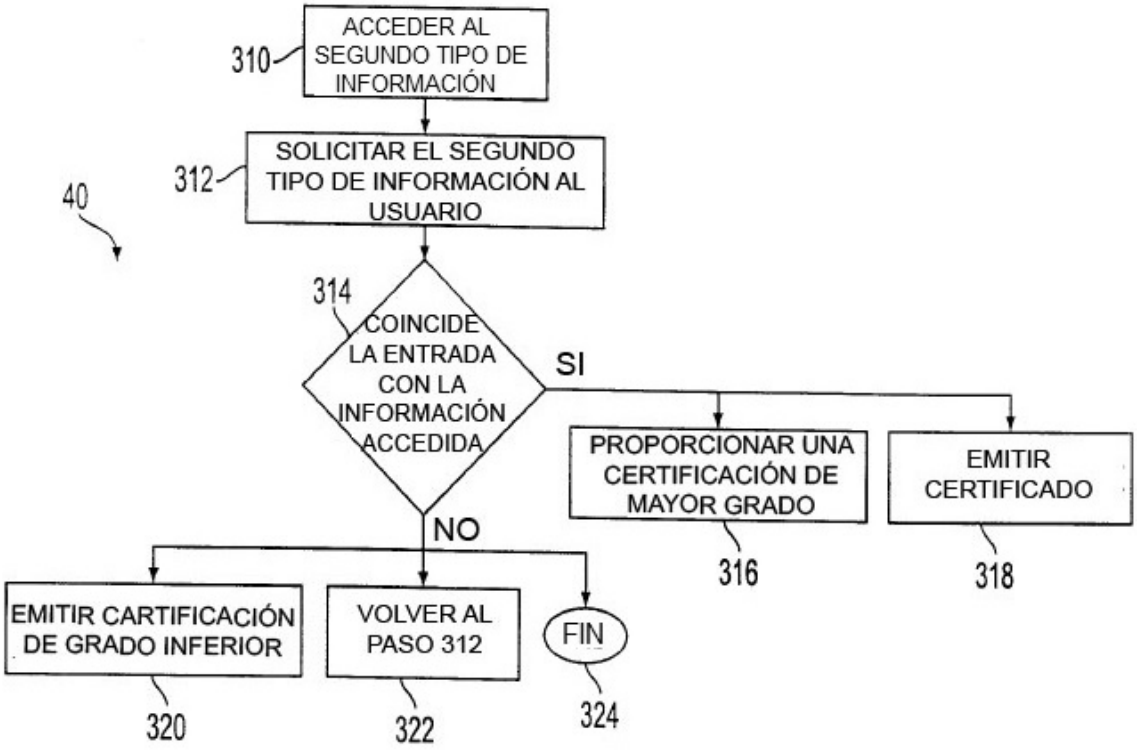

ACCEDER AL SEGUNDO TIPO DE INFORMACIÓN
310
SOLICITAR EL SEGUNDO TIPO DE INFORMACIÓN AL USUARIO
312
40
314
COINCIDE LA ENTRADA CON LA INFORMACIÓN ACCEDIDA
SI
NO
PROPORCIONAR UNA CERTIFICACIÓN DE MAYOR GRADO
316
EMITIR CERTIFICADO
318
EMITIR CARTIFICACIÓN DE GRADO INFERIOR
320
VOLVER AL PASO 312
322
FIN
324

FIG. 3

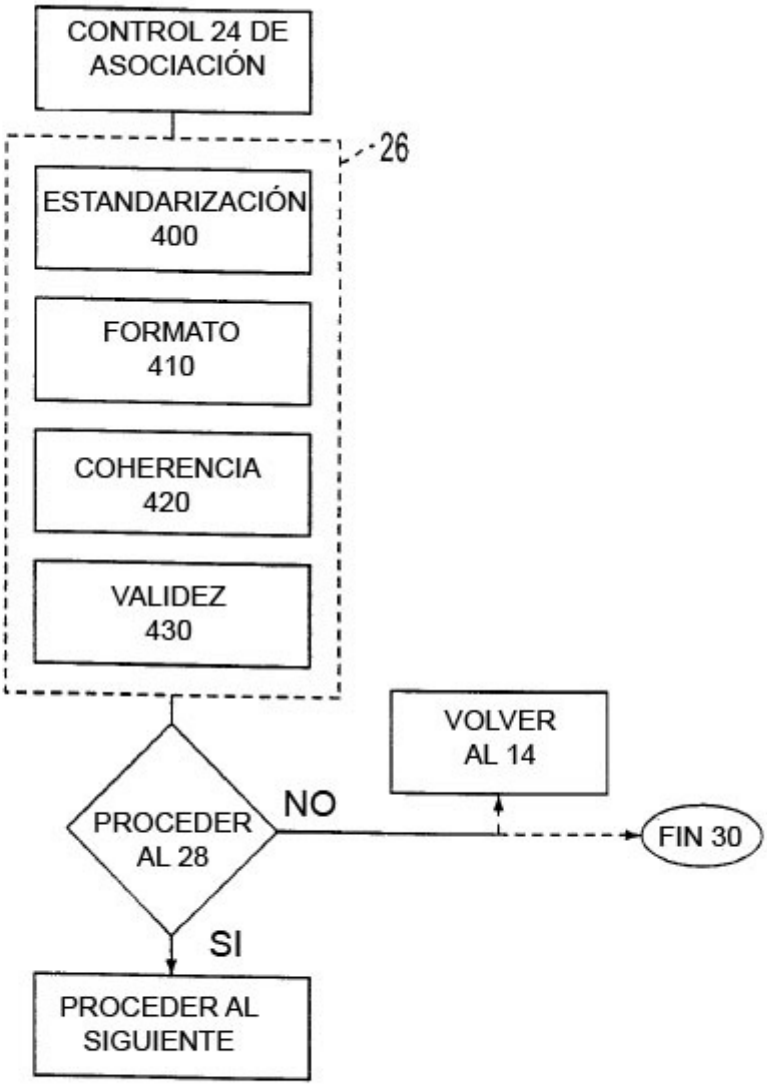

CONTROL 24 DE ASOCIACIÓN
26
ESTANDARIZACIÓN 400
FORMATO 410
COHERENCIA 420
VALIDEZ 430
VOLVER AL 14
PROCEDER AL 28
NO
FIN 30
SI
PROCEDER AL SIGUIENTE

FIG. 4

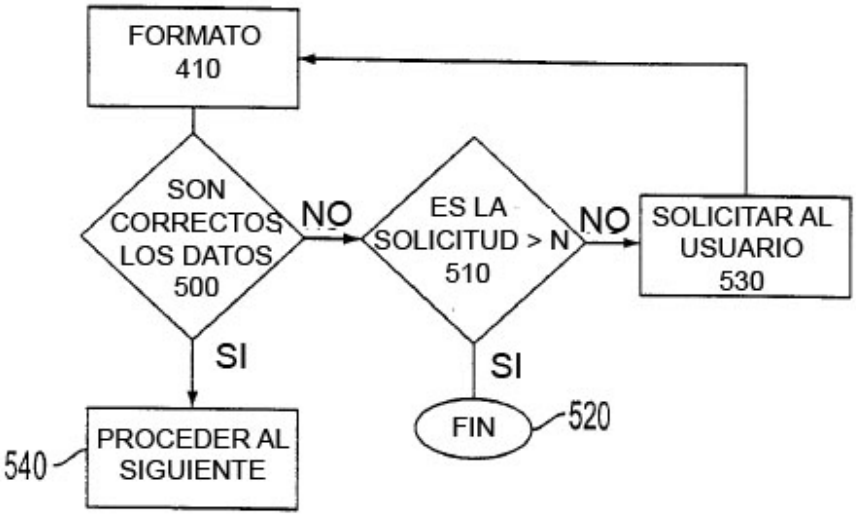

FORMATO
410
SON CORRECTOS LOS DATOS
500
NO
ES LA SOLICITUD > N
510
NO
SOLICITAR AL USUARIO
530
SI
SI
FIN
520
PROCEDER AL SIGUIENTE
540

FIG. 5

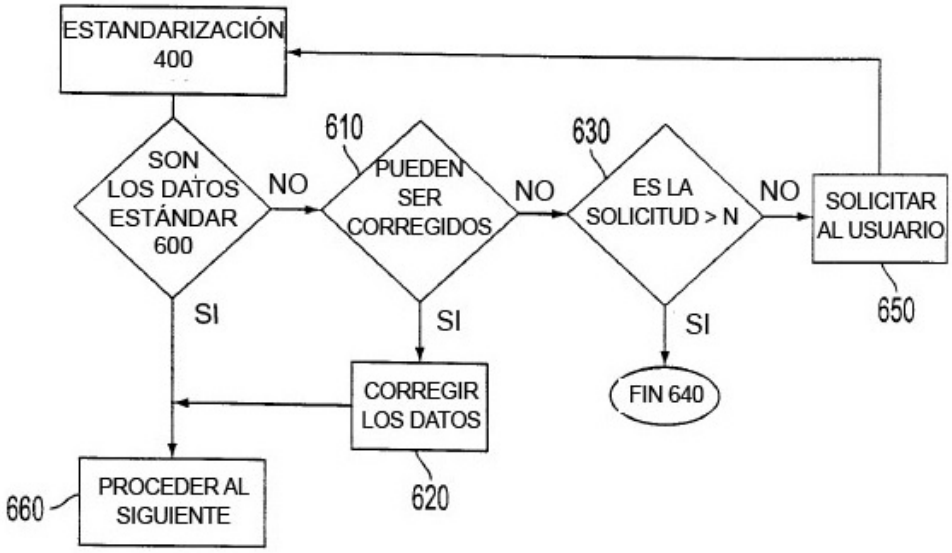

ESTANDARIZACIÓN
400
SON LOS DATOS ESTÁNDAR
600
NO
610
PUEDEN SER CORREGIDOS
NO
630
ES LA SOLICITUD > N
NO
SOLICITAR AL USUARIO
650
SI
SI
SI
FIN 640
CORREGIR LOS DATOS
620
PROCEDER AL SIGUIENTE
660

FIG. 6

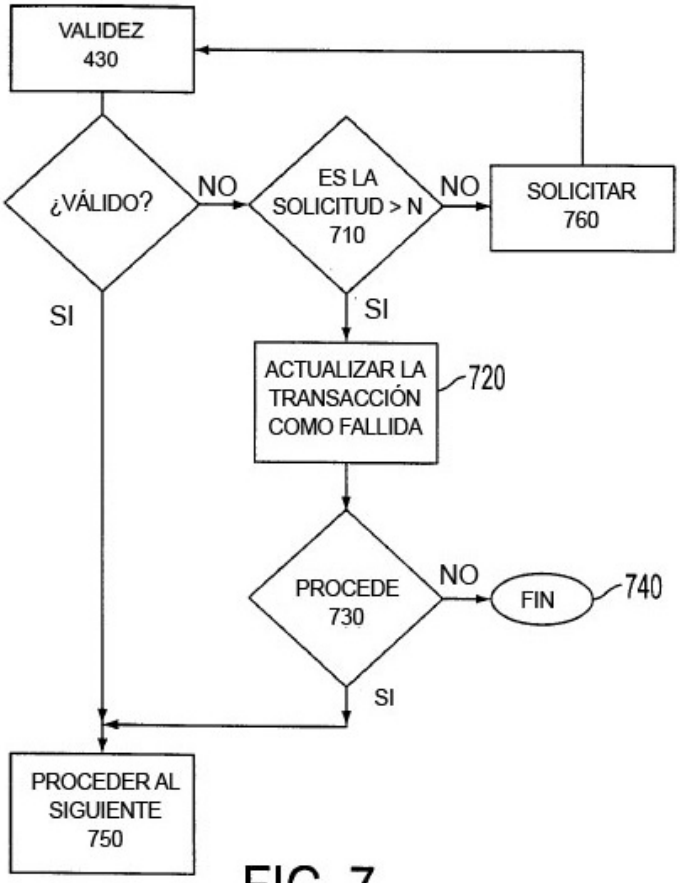

VALIDEZ
430
¿VÁLIDO?
NO
ES LA SOLICITUD > N
710
NO
SOLICITAR
760
SI
SI
ACTUALIZAR LA TRANSACCIÓN COMO FALLIDA
720
PROCEDE
730
NO
FIN
740
SI
PROCEDER AL SIGUIENTE
750

FIG. 7

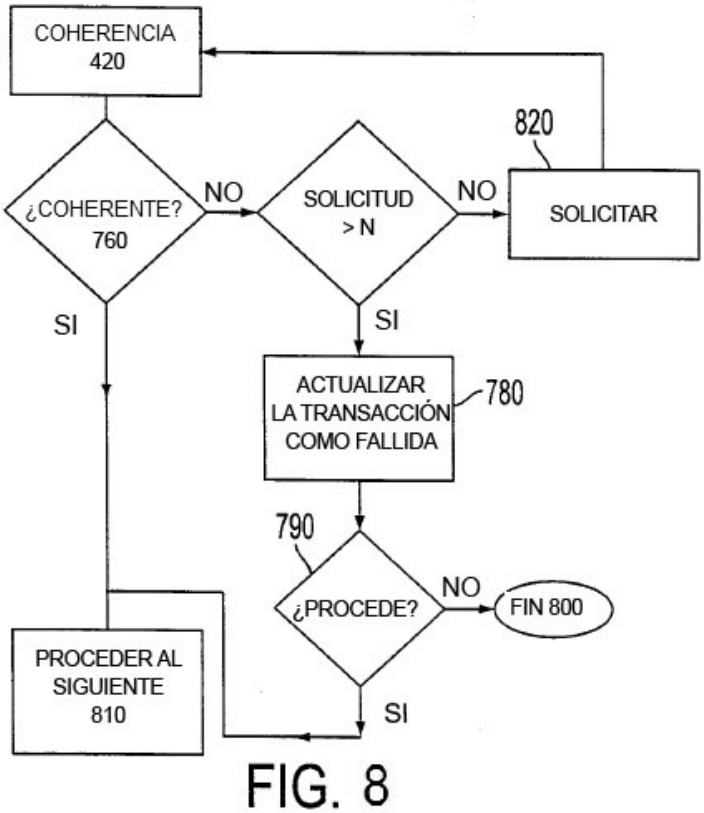

COHERENCIA
420
820
¿COHERENTE?
760
NO
SOLICITUD > N
NO
SOLICITAR
SI
SI
ACTUALIZAR LA TRANSACCIÓN COMO FALLIDA
780
790
¿PROCEDE?
NO
FIN 800
PROCEDER AL SIGUIENTE
810
SI

FIG. 8

	MATRIZ DE ACCIÓN DE CÓDIGOS DE ESTADO POSTALES SUAVES (EJEMPLO)															
	DÍGITO 3															
DÍGITO 2	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
1	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
2	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
3	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
4	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
5	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
6	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
7	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
8	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
9	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
A	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
B	P	P	P	P	P	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP
C	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
D	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
E	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP
F	P	P	P	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP	VP

154

DEFINICIONES DE CÓDIGOS DE ACCIÓN

P PROCEDER A LA VALIDACIÓN DEL CÓDIGO DE ÁREA

VP PRESENTAR ESTE MENSAJE EN EL PRIMER INTENTO: "POR FAVOR VERIFIQUE QUE LA DIRECCIÓN QUE HA INTRODUCIDO ES LA CORRECTA Y REENVÍE." EN EL SEGUNDO Y ÚLTIMO INTENTO, REGISTRAR LOS RESULTADOS DE LA TRANSACCIÓN Y PROCEDER A LA VALIDACIÓN DEL CÓDIGO DE ÁREA.

FIG. 9

ES 2 619 367 T3

MATRIZ DE ACCIÓN DE CÓDIGOS DE ERROR POSTALES SUAVES (EJEMPLO)		
	ACCIÓN	
CÓDIGO DE ERROR	INTENTO 1	INTENTO 2
E101	V	M
E212	V	M
E213	V	M
E214	V	M
E216	V	P
E302	V	P
E412	V	P
E413	V	P
E420	V	P
E421	V	P
E422	V	P
E423	V	P
E425	V	P
E427	V	P
E428	V	P
E429	V	P
E430	V	P
E431	V	P
E500	V	P
E501	M	-
E502	V	M
E503	V	P
E504	V	P
E600	V	M

156

DEFINICIONES DE CÓDIGOS DE ACCIÓN

V PRESENTA ESTE MENSAJE:"POR FAVOR VERIFIQUE QUE LA DIRECCIÓN QUE HA INTRODUCIDO ES CORRECTA Y REENVÍE."

M REGISTRA LOS RESULTADOS DE LA TRANSACCIÓN Y PRESENTA ESTE MENSAJE: "SOMOS INCAPACES DE AUTENTIFICAR INMEDIATAMENTE SU IDENTIDAD CON LA INFORMACIÓN QUE HA PROPORCIONADO. ALGUIEN DE SU DEPARTAMENTO DE ATENCIÓN AL CLIENTE LE CONTACTARÁ EN LAS PRÓXIMAS 24 HORAS. SI NECESITA HABLAR CON ALGUIEN INMEDIATAMENTE, POR FAVOR LLAME A ATENCIÓN AL CLIENTE AL 1-800-999-9999."

P REGISTRA LOS RESULTADOS DE LA TRANSACCIÓN Y PROCEDE A LA VALIDACIÓN DEL CÓDIGO DE ÁREA

FIG. 10

MATRIZ DE ACCIONES DE VERIFICACIÓN DE LA SOLICITUD (EJEMPLO)			
	PROCESO Y RESULTADO	ACCIÓN	MENSAJE
X	VALIDACIÓN NSS		
	PASAR	IR A LA VALIDACIÓN DE LA DIRECCIÓN	
	PRIMER RECHAZO	PRESENTAR MENSAJE	POR FAVOR VERIFIQUE QUE EL NÚMERO DE LA SEGURIDAD SOCIAL QUE HA INTRODUCIDO ES CORRECTO Y REEMVÍE
	SEGUNDO RECHAZO	REGISTRAR TODOS LOS DATOS Y RESULTADOS DE LA SOLICITUD DE VALIDACIÓN NSS. PRESENTAR EL MENSAJE Y ENVIAR LA SOLICITUD A ATENCIÓN AL CLIENTE PARA SU EVALUACIÓN MANUAL	SOMOS INCAPACES DE AUTENTIFICAR INMEDIATAMENTE SU IDENTIDAD CON LA INFORMACIÓN QUE HA PROPORCIONADO. ALGUIEN DE SU DEPARTAMENTO DE ATENCIÓN AL CLIENTE LE CONTACTARÁ EN LAS PRÓXIMAS 24 HORAS. SI NECESITA HABLAR CON ALGUIEN INMEDIATAMENTE, POR FAVOR, LLAME A ATENCIÓN AL CLIENTE AL 1-800-999-9999.
X	VALIDACIÓN DE LA DIRECCIÓN	VER MATRICES DE ACCIÓN POSTAL SUAVE	VER MATRICES DE ACCIÓN POSTAL SUAVE
X	VALIDACIÓN DEL CÓDIGO DE ÁREA		
	PASAR	IR A LA VALIDACIÓN DEL CARNET DE CONDUCIR	
	PRIMER RECHAZO	PRESENTAR MENSAJE	POR FAVOR VERIFIQUE QUE EL NÚMERO DE TELÉFONO DE CASA QUE HA INTRODUCIDO ES CORRECTO Y REENVÍE
	SEGUNDO RECHAZO	REGISTRAR LOS RESULTADOS Y PROCEDER AL SIGUIENTE PROCESO	
X	VALIDACION DEL CARNET DE CONDUCIR		
	PASAR	IR A LA IDENTIFICACIÓN DE LA DECISIÓN	
	PRIMER RECHAZO	PRESENTAR MENSAJE	POR FAVOR VERIFIQUE QUE EL NÚMERO DEL CARNET DE CONDUCIR QUE HA INTRODUCIDO ES CORRECTO Y REENVÍO
	SEGUNDO RECHAZO	REGISTRAR LOS RESULTADOS Y PROCEDER AL SIGUIENTE PROCESO	

158

FIG. 11

ES 2 619 367 T3

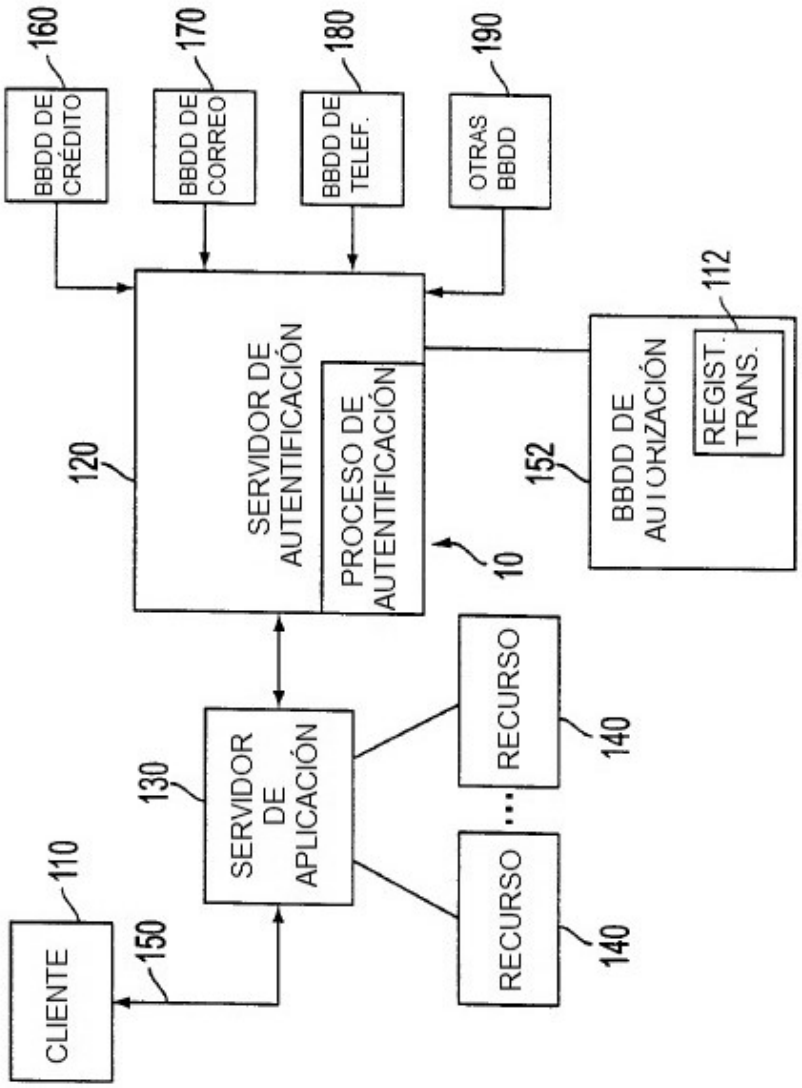

160
BBDD DE CRÉDITO
170
BBDD DE CORREO
180
BBDD DE TELEF.
190
OTRAS BBDD
120
SERVIDOR DE AUTENTIFICACIÓN
PROCESO DE AUTENTIFICACIÓN
10
152
BBDD DE AUTORIZACIÓN
112
REGIST. TRANS.
130
SERVIDOR DE APLICACIÓN
RECURSO
140
RECURSO
140
110
CLIENTE
150

FIG. 12

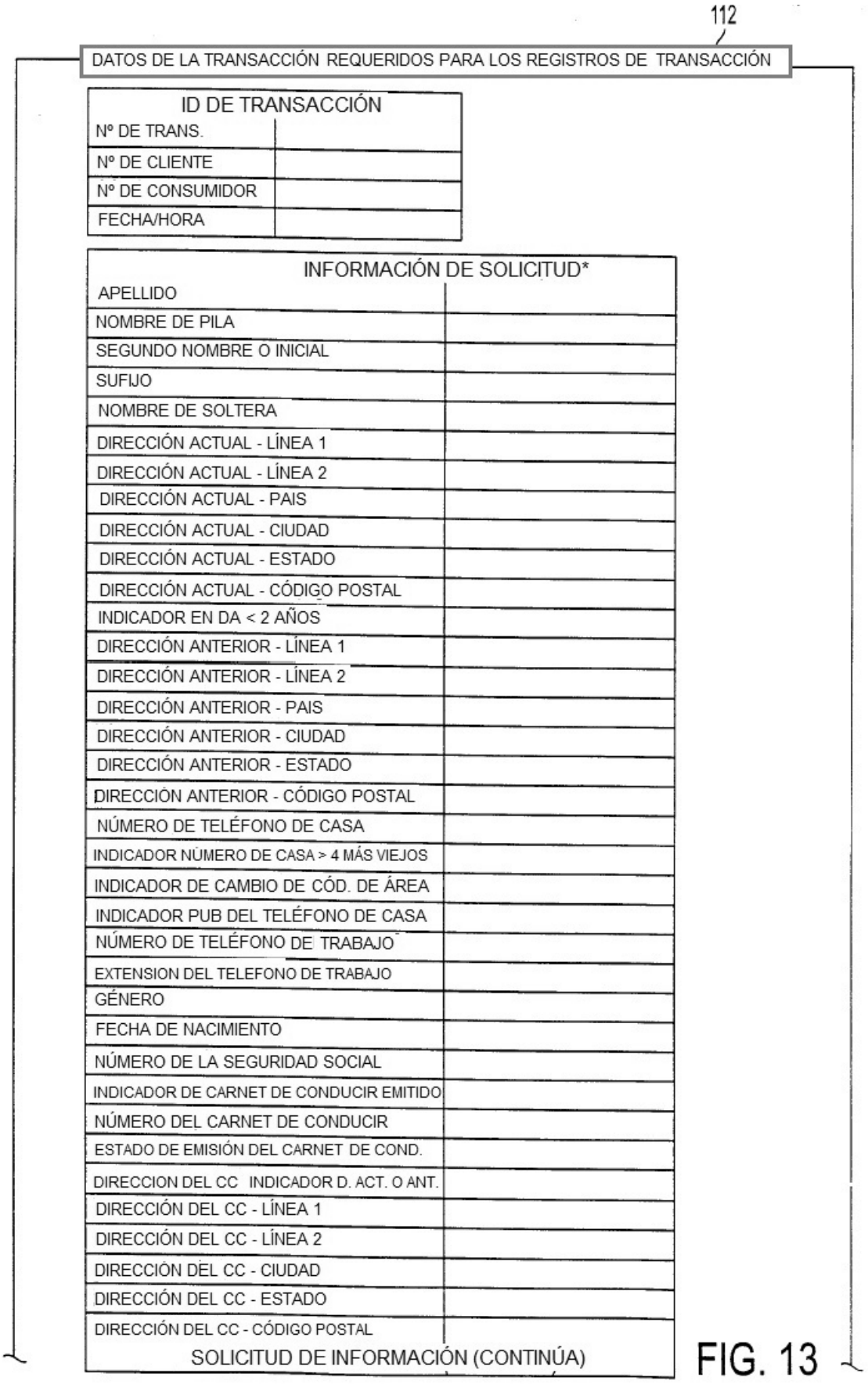

112
DATOS DE LA TRANSACCIÓN REQUERIDOS PARA LOS REGISTROS DE TRANSACCIÓN
ID DE TRANSACCIÓN
Nº DE TRANS.
Nº DE CLIENTE
Nº DE CONSUMIDOR
FECHA/HORA
INFORMACIÓN DE SOLICITUD*
APELLIDO
NOMBRE DE PILA
SEGUNDO NOMBRE O INICIAL
SUFIJO
NOMBRE DE SOLTERA
DIRECCIÓN ACTUAL - LÍNEA 1
DIRECCIÓN ACTUAL - LÍNEA 2
DIRECCIÓN ACTUAL - PAIS
DIRECCIÓN ACTUAL - CIUDAD
DIRECCIÓN ACTUAL - ESTADO
DIRECCIÓN ACTUAL - CÓDIGO POSTAL
INDICADOR EN DA < 2 AÑOS
DIRECCIÓN ANTERIOR - LÍNEA 1
DIRECCIÓN ANTERIOR - LÍNEA 2
DIRECCIÓN ANTERIOR - PAIS
DIRECCIÓN ANTERIOR - CIUDAD
DIRECCIÓN ANTERIOR - ESTADO
DIRECCIÓN ANTERIOR - CÓDIGO POSTAL
NÚMERO DE TELÉFONO DE CASA
INDICADOR NÚMERO DE CASA > 4 MÁS VIEJOS
INDICADOR DE CAMBIO DE CÓD. DE ÁREA
INDICADOR PUB DEL TELÉFONO DE CASA
NÚMERO DE TELÉFONO DE TRABAJO
EXTENSION DEL TELEFONO DE TRABAJO
GÉNERO
FECHA DE NACIMIENTO
NÚMERO DE LA SEGURIDAD SOCIAL
INDICADOR DE CARNET DE CONDUCIR EMITIDO
NÚMERO DEL CARNET DE CONDUCIR
ESTADO DE EMISIÓN DEL CARNET DE COND.
DIRECCION DEL CC INDICADOR D. ACT. O ANT.
DIRECCIÓN DEL CC - LÍNEA 1
DIRECCIÓN DEL CC - LÍNEA 2
DIRECCIÓN DEL CC - CIUDAD
DIRECCIÓN DEL CC - ESTADO
DIRECCIÓN DEL CC - CÓDIGO POSTAL
SOLICITUD DE INFORMACIÓN (CONTINÚA)

FIG. 13

NOMBRE DE SOLTERA DE LA MADRE	
AÑO DE GRADUACIÓN EN LA ESCUELA SECUND.	
NÚMERO DE HERMANOS	
DIRECCIÓN DE CORREO ELECTRÓNICO	

112

*LA INFORMACIÓN RECIBIDA EN LA SOLICITUD,SERÁ ALMACENADA EXACTAMENTE COMO SE HAYA PROPORCIONADO POR EL CONSUMIDOR EN EL FORMULARIO DE LA SOLICITUD

RESULTADOS DEL PROCESAMIENTO	
COMPONENTE DEL PROCESO	
CÓDIGO DE ESTADO DEL PROCESO	
PUNTUACIÓN DEL PROCESO	
FECHA/HORA	

COMPONENTES DEL PROCESO VÁLIDOS	PUNTUACIONES DEL PROCESO VÁLIDAS
VALIDACIÓN DEL NSS	PASA, FALLA
VALIDACIÓN DE LA DIRECCIÓN	P, F
VALIDACIÓN DEL CÓDIGO DE ÁREA	P, F
VALIDACIÓN DEL FORMATO DEL CARNET DE CONDUCIR	P, F
COMPARAR ID ACRO	GRAN, NORMAL, POSIBLE, FALLO
COMPARAR ID CORREO	B, R, P, N
COMPARAR ID DEL CARNET DE CONDUCIR	B, R, P, N
COMPARAR ID LISTA DE CLIENTES	B, R, P, N
PRUEBA DE LÍNEA COMERCIAL	B, R, P, N
EVALUACIÓN MANUAL	B, R, P, N
ID DE DECISIÓN	B, R, P, N

CÓDIGOS DEL ESTADO DEL PROCESO VÁLIDOS	
CÓDIGO DE ESTADO	DESCRIPCIÓN
NO ASIGNADO	PROCESO COMPLETO
NO ASIGNADO	PROCESO COMPLETO - MARCADO PARA MANUAL
NO ASIGNADO	ABORTADO - COM. ERROR
NO ASIGNADO	ABORTADO - ERROR DE SISTEMA
NO ASIGNADO	ABORTADO - ENVIADO A MANUAL

DATOS DE VALIDACIÓN DEL NSS	
CONTROLES PARA EDITAR EL NSS	PASA. FALLA. NO INVOCADO
COMPROBAR NSS FRAUDULENTO	P, F, N
NSS FALLECIDO	P, F, N
NSS FRAUDULENTO	P, F, N
Nº DE VERSIÓN DE TABLA	

FIG. 14

SALIDA POSTALSOFT	
DIRECCIÓN DE SALIDA	
CÓDIGO DE ERROR	
TIPO DE REGISTRO	
VERSIÓN DE DIRECTORIO	
VERSIÓN DE PROGRAMA	

COMPARAR DATOS ID ACRO	
ARCHIVOS DEVUELTOS	0, 1, 2, 3
VÍCTIMA DE FRAUDE	S, N
CÓDIGO DE ESCANEO SEGURO	
PUNTUACIÓN DE BÚSQUEDA L90	

COMPARAR DATOS ID CHOICEPOINT DEL CARNET DE CONDUCIR	
CP # DE CANDIDATOS DEVUELTOS	
CP CLASIFICACIÓN P151	RS = REPORTAR SUJETO
CP NOMBRE - APELLIDO	
CP NOMBRE - DE PILA	
CP NOMBRE - SEGUNDO	
CP NOMBRE - SUFIJO	
CP FECHA DE NACIMIENTO	
CP GÉNERO	
CP NSS	
CP FSI - NOMBRE - APELLIDO	COINCIDENCIA, DISCREPANCIA, BLANCO
CP FSI - NOMBRE - DE PILA	C , D, BLANCO
CP FSI - NOMBRE - SEGUNDO	C , D, BLANCO
CP FSI - NOMBRE - SUFIJO	C , D, BLANCO
CP FSI - FECHA DE NACIMIENTO	C , D, BLANCO
CP FSI - GÉNERO	C , D, BLANCO
CP FSI - NSS	C , D, BLANCO
CP CLASIFICACIÓN DL51	CP = ACTUAL PERSONAL CL = ACTUAL PERMISO DE PRINCIPIANTE CC = ACTUAL COMERCIAL PP = ANTERIOR PERSONAL PC = ANTERIOR COMERCIAL
CP NÚMERO DEL CARNET DE CONDUCIR	
CP ESTADO DEL CARNET DE CONDUCIR	
CP FSI - NBR DEL CARNET DE CONDUCIR	C , D, BLANCO
CP FSI - ESTADO DEL CARNET DE CONDUCIR	C , D, BLANCO
CP FECHA DE VENCIMIENTO DEL CARNET DE CONDUCIR	POSIBLE FUTURA MEJORA
CP FECHA DE EMISIÓN DEL CARNET DE CONDUCIR	POSIBLE FUTURA MEJORA
CP CLASIFICACIÓN AL51	DR = DIRECCIÓN DE RESIDENCIA DA = DIRECCIÓN ANTERIOR
CP DIRECCIÓN - NÚMERO DE CASA	

COMPARAR DATOS ID CHOICEPOINT DEL CARNET DE CONDUCIR (CONT)

112

FIG. 15

CP DIRECCION - NOMBRE DE LA CALLE	
CP DIRECCION - NUMERO DEL APARTAMENTO	
CP DIRECCIÓN - CIUDAD	
CP DIRECCIÓN - ESTADO	
CP DIRECCION - CÓDIGO POSTAL	
CP DIRECCIÓN - CÓDIGO POSTAL + 4	
CP FSI DIRECCIÓN - NÚMERO DE LA CASA	C, D, BLANCO
CP FSI DIRECCIÓN - NOMBRE DE LA CALLE	C, D, BLANCO
CP FSI DIRECCIÓN - NÚMERO DE APT.	C, D, BLANCO
CP FSI DIRECCION - CIUDAD	C, D, BLANCO
CP FSI DIRECCIÓN - ESTADO	C, D, BLANCO
CP FSI DIRECCIÓN - CÓDIGO POSTAL	C, D, BLANCO
CP FSI DIRECCIÓN - CÓDIGO POSTAL +4	C, D, BLANCO

*CP = CHOICEPOINT

112

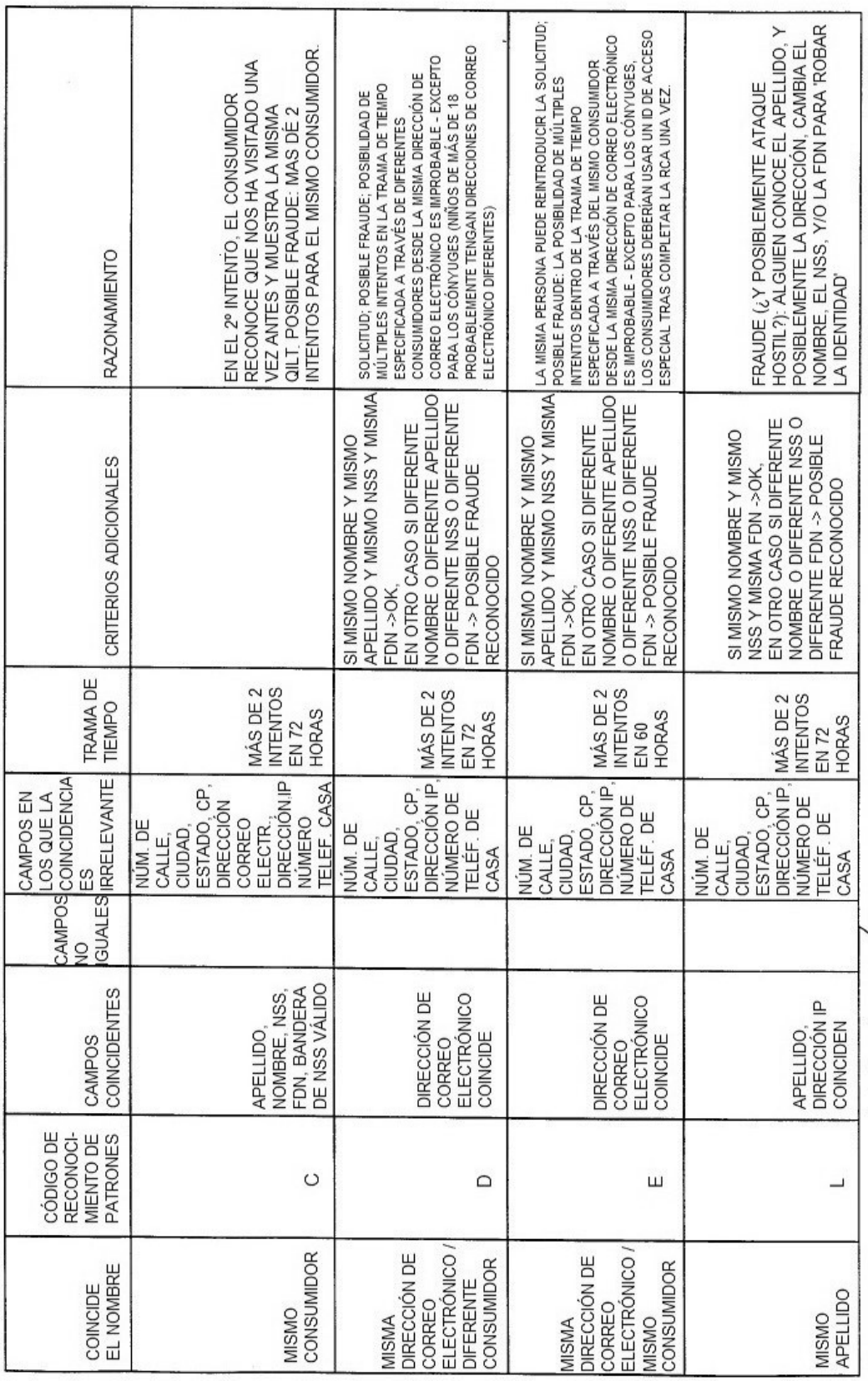
COMPARAR DATOS ID METRONET	
MN NOMBRE	
MN DIRECCIÓN	
MN NÚMERO DE TELÉFONO	
MN CÓDIGO DE RESPUESTA PRIMARIA	
MN NM/ADD VERIFICACIÓN DE CÓDIGO DE RESPUESTA	
MN CÓDIGO DE RESPUESTA DE VERIFICACIÓN DE TELÉFONO	
MN SOLICITUD EDA	S, N
MN SOLICITUD EDA DE CÓDIGO DE CONFIANZA	NULO, SI CONTROL EDA = 'N'

*MN = METRONET

DATOS DE PRUEBA DE LA LÍNEA COMERCIAL	
TIPO DE COMERCIO	M, A, P, S, G
FECHA ABIERTA	
NOMBRE DEL PRESTAMISTA	
PRESTAMISTA - OPCIONES DE ELECCIÓN MÚLTIPLE*	
PRESTAMISTA - RESPUESTA DEL CONSUMIDOR	
TÉRMINOS O PAGO MENSUAL	
TÉRMINOS O PAGO MENSUAL - OPCIONES DE EM*	
TÉRMINOS O PAGO MENSUAL - RESP. DEL CONSUM.	

*LAS OPCIONES DE SELECCIÓN MÚLTIPLE DEBERÍAN SER ALMACENADAS EN EL ORDEN PRESENTADO AL CONSUMIDOR Y CON LA RESPUESTA CORRECTA INCLUIDA.

FIG. 16



COINCIDE EL NOMBRE	CÓDIGO DE RECONOCI-MIENTO DE PATRONES	CAMPOS COINCIDENTES	CAMPOS NO IGUALES	CAMPOS EN LOS QUE LA COINCIDENCIA ES IRRELEVANTE	TRAMA DE TIEMPO	CRITERIOS ADICIONALES	RAZONAMIENTO
MISMO CONSUMIDOR	C	APELLIDO, NOMBRE, NSS, FDN, BANDERA DE NSS VÁLIDO		NÚM. DE CALLE, CIUDAD, ESTADO, CP, DIRECCIÓN CORREO ELECTR., DIRECCIÓN.IP NÚMERO TELÉF. CASA	MÁS DE 2 INTENTOS EN 72 HORAS		EN EL 2º INTENTO, EL CONSUMIDOR RECONOCE QUE NOS HA VISITADO UNA VEZ ANTES Y MUESTRA LA MISMA QILT. POSIBLE FRAUDE: MAS DE 2 INTENTOS PARA EL MISMO CONSUMIDOR.
MISMA DIRECCIÓN DE CORREO ELECTRÓNICO / DIFERENTE CONSUMIDOR	D	DIRECCIÓN DE CORREO ELECTRÓNICO COINCIDE		NÚM. DE CALLE, CIUDAD, ESTADO, CP, DIRECCIÓN IP, NÚMERO DE TELÉF. DE CASA	MÁS DE 2 INTENTOS EN 72 HORAS	SI MISMO NOMBRE Y MISMO APELLIDO Y MISMO NSS Y MISMA FDN ->OK, EN OTRO CASO SI DIFERENTE NOMBRE O DIFERENTE APELLIDO O DIFERENTE NSS O DIFERENTE FDN -> POSIBLE FRAUDE RECONOCIDO	SOLICITUD; POSIBLE FRAUDE; POSIBILIDAD DE MÚLTIPLES INTENTOS EN LA TRAMA DE TIEMPO ESPECIFICADA A TRAVÉS DE DIFERENTES CONSUMIDORES DESDE LA MISMA DIRECCIÓN DE CORREO ELECTRÓNICO ES IMPROBABLE - EXCEPTO PARA LOS CÓNYUGES (NIÑOS DE MÁS DE 18 PROBABLEMENTE TENGAN DIRECCIONES DE CORREO ELECTRÓNICO DIFERENTES)
MISMA DIRECCIÓN DE CORREO ELECTRÓNICO / MISMO CONSUMIDOR	E	DIRECCIÓN DE CORREO ELECTRÓNICO COINCIDE		NÚM. DE CALLE, CIUDAD, ESTADO, CP, DIRECCIÓN IP, NÚMERO DE TELÉF. DE CASA	MÁS DE 2 INTENTOS EN 60 HORAS	SI MISMO NOMBRE Y MISMO APELLIDO Y MISMO NSS Y MISMA FDN ->OK, EN OTRO CASO SI DIFERENTE NOMBRE O DIFERENTE APELLIDO O DIFERENTE NSS O DIFERENTE FDN -> POSIBLE FRAUDE RECONOCIDO	LA MISMA PERSONA PUEDE REINTRODUCIR LA SOLICITUD; POSIBLE FRAUDE; LA POSIBILIDAD DE MÚLTIPLES INTENTOS DENTRO DE LA TRAMA DE TIEMPO ESPECIFICADA A TRAVÉS DEL MISMO CONSUMIDOR DESDE LA MISMA DIRECCIÓN DE CORREO ELECTRÓNICO ES IMPROBABLE - EXCEPTO PARA LOS CÓNYUGES; LOS CONSUMIDORES DEBERÍAN USAR UN ID DE ACCESO ESPECIAL TRAS COMPLETAR LA RCA UNA VEZ.
MISMO APELLIDO	L	APELLIDO, DIRECCIÓN IP COINCIDEN		NÚM. DE CALLE, CIUDAD, ESTADO, CP, DIRECCIÓN IP, NÚMERO DE TELÉF. DE CASA	MÁS DE 2 INTENTOS EN 72 HORAS	SI MISMO NOMBRE Y MISMO NSS Y MISMA FDN ->OK, EN OTRO CASO SI DIFERENTE NOMBRE O DIFERENTE NSS O DIFERENTE FDN -> POSIBLE FRAUDE RECONOCIDO	FRAUDE (¿Y POSIBLEMENTE ATAQUE HOSTIL?): ALGUIEN CONOCE EL APELLIDO, Y POSIBLEMENTE LA DIRECCIÓN, CAMBIA EL NOMBRE, EL NSS, Y/O LA FDN PARA 'ROBAR LA IDENTIDAD'

FIG. 17 904

MISMA DIRECCIÓN & NSS	S	NÚMERO DE CALLE, CIUDAD, ESTADO, CP, NSS, BANDERA DE NSS VÁLIDO TODOS COINCIDEN	APELL.	NOMBRE, FDN NÚMERO DE TELÉFONO DE CASA	MÁS DE 2 INTENTOS EN 72 HORAS		FRAUDE: ALGUIEN ROBANDO INFORMACIÓN SOBRE OTRO, PERO USANDO SU PROPIA DIRECCIÓN PARA PROPÓSITOS DE ENVIO POR CORREO, INTENTANDO VARIOS APELLIDOS
MISMA DIRECCIÓN & APELLIDO	N	NÚMERO DE CALLE, CIUDAD, ESTADO, CP, APELLIDO, BANDERA DE NSS VÁLIDO TODOS COINCIDEN	NSS		MÁS DE 2 INTENTOS EN 72 HORAS		FRAUDE: ALGUIEN ROBANDO INFORMACIÓN SOBRE OTRO, PERO USANDO SU PROPIA DIRECCIÓN PARA PROPÓSITOS DE ENVIO POR CORREO, INTENTANDO VARIOS NSSs
6 PARA 6	X	APELLIDO, NOMBRE, DIRECCIÓN IP, NSS, FDNM CORREO ELECTRÓNICO, ESTADO, CP TODOS COINCIDEN			MÁS DE 2 INTENTOS EN 72 HORAS		EN EL 2º INTENTO, RECONOCE QUE EL CONSUMIDOR NOS HA VISITADO UNA VEZ ANTES Y MUESTRA LA MISMA CALIDAD. POSIBLE FRAUDE: MÁS DE 2 INTENTOS PARA EL MISMO CONSUMIDOR
MISMA SOLICITUD	A	DIRECCION IP, NOMBRE, SEGUNDO NOMBRE, APELLIDO, SUFIJO DIRECCIÓN DE CORREO ELECTRÓNICO, NÚMERO DE CALLE, TIPO DE CALLE, CIUDAD, ESTADO, CP, NSS, TELÉFONO DE CASA, FDN, BANDERA DE NSS VÁLIDO TODOS COINCIDEN	APELL.		MÁS DE 2 INTENTOS EN 24 HORAS		POSIBLE ATAQUE HOSTIL - ALGUIEN QUE VARÍA UNA PARTE DE LA SOLICITUD DE INFORMACIÓN - SIMILAR A LOS INTENTOS PARA ARCHIVOS ACRO (POR JIM DIFFENBAUGH)

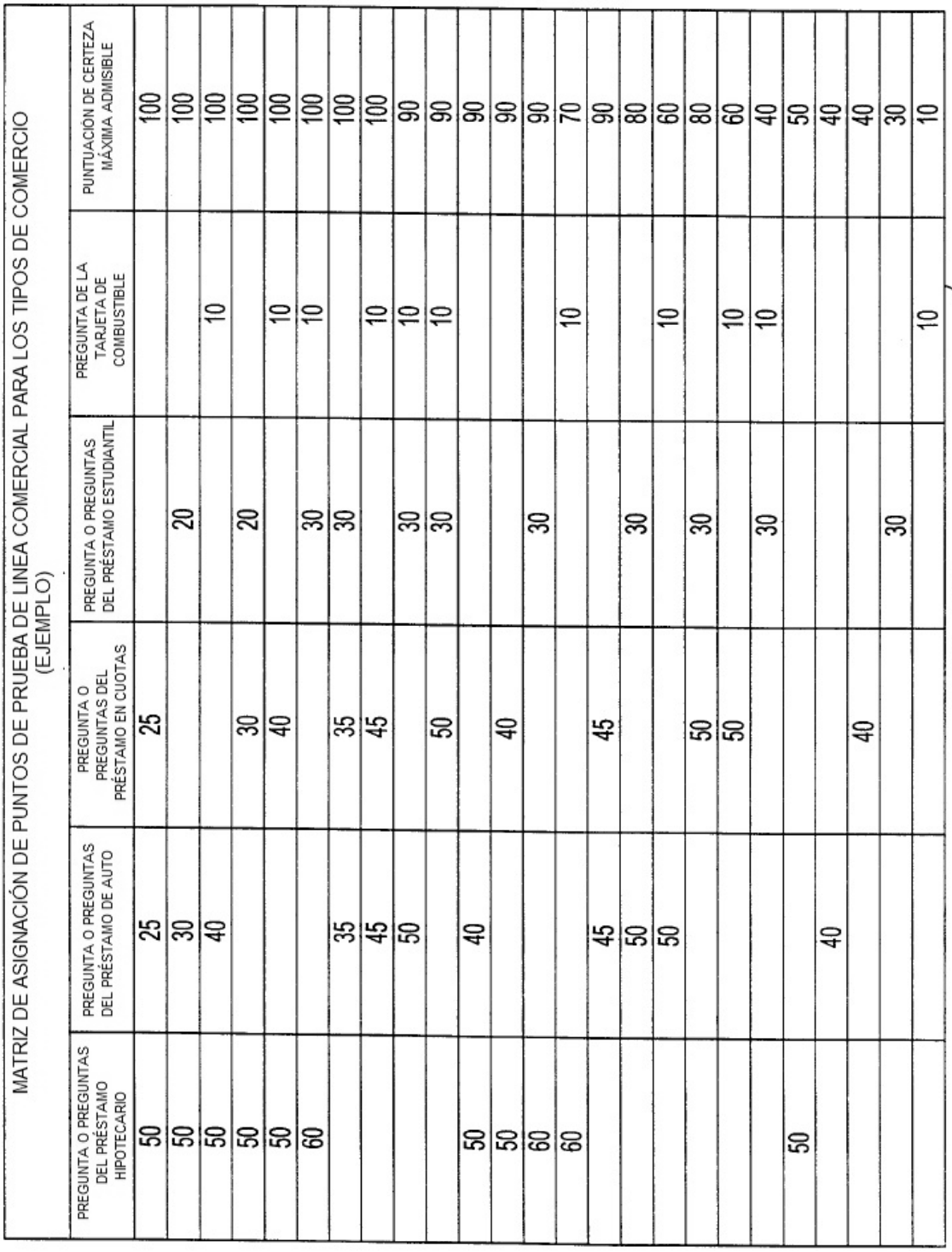
FIG. 18

904

NOMBRE COINCIDENTE	NÚMERO DE SESIONES (DEVUELTAS DEL RECONOCIMIENTO DE PATRONES)	ACCIÓN
MISMO CONSUMIDOR	0	NUEVA QUILT
MISMO CONSUMIDOR	1	QILT ANTERIOR
MISMO CONSUMIDOR	>1	SOSPECHA DE FRAUDE: BLOQUEO
MISMO CORREO ELECTRÓNICO/DIFERENTE CLIENTE/DIFERENTE CONSUMIDOR	0	NUEVA QUILT
MISMO CORREO ELECTRÓNICO/DIFERENTE CLIENTE/DIFERENTE CONSUMIDOR	1	NUEVA QUILT
MISMO CORREO ELECTRÓNICO/DIFERENTE CLIENTE/DIFERENTE CONSUMIDOR	>1	SOSPECHA DE FRAUDE: BLOQUEO
MISMO CORREO ELECTRÓNICO/MISMO CLIENTE/DIFERENTE CONSUMIDOR	0	NUEVA QUILT
MISMO CORREO ELECTRÓNICO/MISMO CLIENTE/DIFERENTE CONSUMIDOR	1	NUEVA QUILT
MISMO CORREO ELECTRÓNICO/MISMO CLIENTE/DIFERENTE CONSUMIDOR	>1	SOSPECHA DE FRAUDE: BLOQUEO
MISMO APELLIDO/MISMA DIRECCIÓN IP	0	NUEVA QUILT
MISMO APELLIDO/MISMA DIRECCIÓN IP	1	NUEVA QUILT
MISMO APELLIDO/MISMA DIRECCIÓN IP	>1	SOSPECHA DE FRAUDE: BLOQUEO
MISMA DIRECCIÓN/MISMO NSS/DIFERENTE APELLIDO	0	NUEVA QUILT
MISMA DIRECCIÓN/MISMO NSS/DIFERENTE APELLIDO	1	NUEVA QUILT
MISMA DIRECCIÓN/MISMO NSS/DIFERENTE APELLIDO	>1	SOSPECHA DE FRAUDE: BLOQUEO
MISMA DIRECCIÓN/DIFERENTE NSS/MISMO APELLIDO	0	NUEVA QUILT
MISMA DIRECCIÓN/DIFERENTE NSS/MISMO APELLIDO	1	NUEVA QUILT
MISMA DIRECCIÓN/DIFERENTE NSS/MISMO APELLIDO	>1	SOSPECHA DE FRAUDE: BLOQUEO
6 PARA 6	0	NUEVA QUILT
6 PARA 6	1	NUEVA QUILT
6 PARA 6	>1	SOSPECHA DE FRAUDE: BLOQUEO
MISMA SOLICITUD	0	NUEVA QUILT
MISMA SOLICITUD	1	NUEVA QUILT
MISMA SOLICITUD	>1	SOSPECHA DE FRAUDE: BLOQUEO

912

FIG. 19



MATRIZ DE ASIGNACIÓN DE PUNTOS DE PRUEBA DE LINEA COMERCIAL PARA LOS TIPOS DE COMERCIO (EJEMPLO)

PREGUNTA O PREGUNTAS DEL PRÉSTAMO HIPOTECARIO	PREGUNTA O PREGUNTAS DEL PRÉSTAMO DE AUTO	PREGUNTA O PREGUNTAS DEL PRÉSTAMO EN CUOTAS	PREGUNTA O PREGUNTAS DEL PRÉSTAMO ESTUDIANTIL	PREGUNTA DE LA TARJETA DE COMBUSTIBLE	PUNTUACION DE CERTEZA MÁXIMA ADMISIBLE
50	25	25			100
50	30		20		100
50	40			10	100
50		30	20		100
50		40		10	100
60			30	10	100
	35	35	30		100
	45	45		10	100
	50		30	10	90
		50	30	10	90
50	40				90
50		40			90
60			30		90
60				10	70
	45	45			90
	50		30		80
	50			10	60
		50	30		80
		50		10	60
			30	10	40
50					50
	40				40
		40			40
			30		30
				10	10

906

FIG. 20

MATRIZ DE ASIGNACIÓN DE PESOS DE PRUEBAS DE LÍNEA COMERCIAL PARA LOS TIPOS DE PREGUNTAS (EJEMPLO) (%)

PREG. DEL NOMBREDEL PRESTAMISTA	PREGUNTA DEL PAGO MENSUAL	PREG. DE LOS TÉRMINOS	NINGUNA SEGUNDA PREGUNTA
75	25		
80		20	
80			0
*100	0		
*100		0	

*ESTAS ENTRADAS APLICAN SÓLO AL TIPO COMERCIAL DE TARJETA DE COMBUSTIBLE. NUNCA SE PRESENTARÁ UNA SEGUNDA PREGUNTA PARA LOS TIPOS COMERCIALES DE TARJETA DE COMBUSTIBLE, POR LO TANTO TODOS LOS PUNTOS DISPONIBLES PARA ESTE TIPO COMERCIAL DEBERÍAN SER APLICADOS A LA PREGUNTA DEL PROVEEDOR DE CRÉDITO. 908

FIG. 21

MATRIZ DE CALIDAD DE COINCIDENCIA PARA LA PRUEBA DE LÍNEA COMERCIAL (EJEMPLO)

PUNTUACIÓN DE CERTEZA	CLASIFICACIÓN DEL CLIENTE
85 - 100	B
40 - 84	R
10 - 39	P
0 - 9	N

910

FIG. 22

PUNTUACIONES DE CERTEZA POR ID DE DECISIÓN - ORDENADAS POR PUNTUACIÓN DE CERTEZA					
RESULTADOS DEL PROCESO				PUNTUACIÓN DE CERTEZA	
ACRO	METRONET	CHOICEPOINT	PRUEBA LÍNEA COMERCIAL	ESTÁNDAR	PERSONALIZADA
B	B	B	B	100	
B	B	R	B	95	
B	R	B	B	95	
R	B	B	B	95	
B	B	P	B	91	
B	B	N	B	90	
B	R	R	B	90	
R	B	R	B	90	
R	R	B	B	90	
B	R	P	B	86	
R	B	P	B	86	
B	R	N	B	85	
B	P	B	B	85	
R	B	N	B	85	
R	R	R	B	85	
P	B	B	B	85	
R	R	P	B	81	
B	B	B	R	80	
B	P	R	B	80	
B	N	B	B	80	
R	R	N	B	80	
R	P	B	B	80	
P	B	R	B	80	
P	R	B	B	80	
B	P	P	B	76	
P	B	P	B	76	
B	B	R	R	75	
B	R	B	R	75	
B	P	N	B	75	
B	N	R	B	75	
R	B	B	R	75	
R	P	R	B	75	
R	N	B	B	75	
P	B	N	B	75	
P	R	R	B	75	
B	B	P	R	71	
B	N	P	B	71	
R	P	P	B	71	
P	R	P	B	71	
B	B	N	R	70	
B	R	R	R	70	
B	N	N	B	70	
R	B	R	R	70	
R	R	B	R	70	
R	P	N	B	70	
R	N	R	B	70	
P	R	N	B	70	
P	P	B	B	70	
B	R	P	R	66	

918

FIG. 23

PUNTUACIONES DE CERTEZA PARA LA DECISIÓN DE LA ID					
RESULTADOS DEL PROCESO				PUNTUACIÓN DE CERTEZA	
ACRO	METRONET	CHOICEPOINT	PRUEBA LÍNEA COMERCIAL	ESTÁNDAR	PERSONALIZADA
R	B	P	R	66	
R	N	P	B	66	
B	R	N	R	65	
B	P	B	R	65	
R	B	N	R	65	
R	R	R	R	65	
R	N	N	B	65	
P	B	B	R	65	
P	P	R	B	65	
P	N	B	B	65	
R	R	P	R	61	
P	P	P	B	61	
B	P	R	R	60	
B	N	B	R	60	
R	R	N	R	60	
R	P	B	R	60	
P	B	R	R	60	
P	R	B	R	60	
P	P	N	B	60	
P	N	R	B	60	
B	P	P	R	56	
P	B	P	R	56	
P	N	P	B	56	
B	B	B	P	55	
B	P	N	R	55	
B	N	R	R	55	
R	P	R	R	55	
R	N	B	R	55	
P	B	N	R	55	
P	R	R	R	55	
P	N	N	B	55	
B	N	P	R	51	
R	P	P	R	51	
P	R	P	R	51	
B	B	B	N	50	
B	B	R	P	50	
B	R	B	P	50	
B	N	N	R	50	
R	B	B	P	50	
R	P	N	R	50	
R	N	R	R	50	
P	R	N	R	50	
P	P	B	R	50	
B	B	P	P	46	
R	N	P	R	46	
B	B	R	N	45	
B	B	N	P	45	
B	R	B	N	45	
B	R	R	P	45	

918

FIG. 24

PUNTUACIONES DE CERTEZA PARA LA DECISIÓN DE LA ID					
RESULTADOS DEL PROCESO				PUNTUACIÓN DE CERTEZA	
ACRO	METRONET	CHOICEPOINT	PRUEBA LÍNEA COMERCIAL	ESTÁNDAR	PERSONALIZADA
R	B	B	N	45	
R	B	R	P	45	
R	R	B	P	45	
R	N	N	R	45	
P	P	R	R	45	
P	N	B	R	45	
B	B	P	N	41	
B	R	P	P	41	
R	B	P	P	41	
P	P	P	R	41	
B	B	N	N	40	
B	R	R	N	40	
B	R	N	P	40	
B	P	B	P	40	
R	B	R	N	40	
R	B	N	P	40	
R	R	B	N	40	
R	R	R	P	40	
P	B	B	P	40	
P	P	N	R	40	
P	N	R	R	40	
B	R	P	N	36	
R	B	P	N	36	
R	R	P	P	36	
P	N	P	R	36	
B	R	N	N	35	
B	P	B	N	35	
B	P	R	P	35	
B	N	B	P	35	
R	B	N	N	35	
R	R	R	N	35	
R	R	N	P	35	
R	P	B	P	35	
P	B	B	N	35	
P	B	R	P	35	
P	R	B	P	35	
P	N	N	R	35	
B	P	P	P	31	
R	R	P	N	31	
P	B	P	P	31	
B	P	R	N	30	
B	P	N	P	30	
B	N	B	N	30	
B	N	R	P	30	
R	R	N	N	30	
R	P	B	N	30	
R	P	R	P	30	
R	N	B	P	30	
P	B	R	N	30	

918

FIG. 25

PUNTUACIONES DE CERTEZA PARA LA DECISIÓN DE LA ID					
RESULTADOS DEL PROCESO				PUNTUACIÓN DE CERTEZA	
ACRO	METRONET	CHOICEPOINT	PRUEBA LÍNEA COMERCIAL	ESTÁNDAR	PERSONALIZADA
P	B	N	P	30	
P	R	B	N	30	
P	R	R	P	30	
N	B	B	N	30	
N	B	B	N	30	
N	B	B	N	30	
N	B	B	N	30	
B	P	P	N	26	
B	N	P	P	26	
R	P	P	P	26	
P	B	P	N	26	
P	R	P	P	26	
B	P	N	N	25	
B	N	R	N	25	
B	N	N	P	25	
R	P	R	N	25	
R	P	N	P	25	
R	N	B	N	25	
R	N	R	P	25	
P	B	N	N	25	
P	R	R	N	25	
P	R	N	P	25	
P	P	B	P	25	
N	B	R	N	25	
N	B	R	N	25	
N	B	R	N	25	
N	B	R	N	25	
N	R	B	N	25	
N	R	B	N	25	
N	R	B	N	25	
B	N	P	N	21	
R	P	P	N	21	
R	N	P	P	21	
P	R	P	N	21	
N	B	P	N	21	
N	B	P	N	21	
N	B	P	N	21	
N	B	P	N	21	
B	N	N	N	20	
R	P	N	N	20	
R	N	R	N	20	
R	N	N	P	20	
P	R	N	N	20	
P	P	B	N	20	
P	P	R	P	20	
P	N	B	P	20	
N	B	N	N	20	
N	B	N	N	20	

918

FIG. 26

PUNTUACIONES DE CERTEZA PARA LA DECISIÓN DE LA ID					
RESULTADOS DEL PROCESO				PUNTUACIÓN DE CERTEZA	
ACRO	METRONET	CHOICEPOINT	PRUEBA LÍNEA COMERCIAL	ESTÁNDAR	PERSONALIZADA
N	B	N	N	20	
N	B	N	N	20	
N	R	R	N	20	
N	R	R	N	20	
N	R	R	N	20	
N	R	R	N	20	
R	N	P	N	16	
P	P	P	P	16	
N	R	P	N	16	
N	R	P	N	16	
N	R	P	N	16	
N	R	P	N	16	
R	N	N	N	15	
P	P	R	N	15	
P	P	N	P	15	
P	N	B	N	15	
P	N	R	P	15	
N	R	N	N	15	
N	R	N	N	15	
N	R	N	N	15	
N	R	N	N	15	
N	P	B	N	15	
N	P	B	N	15	
N	P	B	N	15	
N	P	B	N	15	
P	P	P	N	11	
P	N	P	P	11	
P	P	N	N	10	
P	N	R	N	10	
P	N	N	P	10	
N	P	R	N	10	
N	P	R	N	10	
N	P	R	N	10	
N	P	R	N	10	
N	N	B	N	10	
N	N	B	N	10	
N	N	B	N	10	
N	N	B	N	10	
P	N	P	N	6	
N	P	P	N	6	
N	P	P	N	6	
N	P	P	N	6	
N	P	P	N	6	
P	N	N	N	5	
N	P	N	N	5	
N	P	N	N	5	
N	P	N	N	5	
N	P	N	N	5	
N	N	R	N	5	

918

FIG. 27

PUNTUACIONES DE CERTEZA PARA LA DECISIÓN DE LA ID					
RESULTADOS DEL PROCESO				PUNTUACIÓN DE CERTEZA	
ACRO	METRONET	CHOICEPOINT	PRUEBA LÍNEA COMERCIAL	ESTÁNDAR	PERSONALIZADA
N	N	R	N	5	
N	N	R	N	5	
N	N	R	N	5	
N	N	P	N	1	
N	N	P	N	1	
N	N	P	N	1	
N	N	P	N	1	
N	N	N	N	0	
N	N	N	N	0	
N	N	N	N	0	
N	N	N	N	0	

918

FIG. 28

TABLA DE ASIGNACIÓN DE VALORES

EVENTO	MÁXIMA PUNTUACIÓN		ACRO		METRONET		CHOICEPOINT		PRUEBA DE LÍNEA COMERCIAL	
	ESTÁNDAR	PERSONALIZADA	ESTÁNDAR	PERSONALIZADA	ESTÁNDAR	PERSONALIZADA	ESTÁNDAR	PERSONALIZADA	ESTÁNDAR	PERSONALIZADA
GRAN ÉXITO	100		20		20		10		50	
ÉXITO NORMAL	70		15		15		5		30	
POSIBLE ÉXITO	36		5		5		1		5	
FALLO	0		0		0		0		0	

920

FIG. 29

TABLA DE UMBRALES DE PUNTUACIÓN DE CERTEZA

PUNTUACIÓN DE CERTEZA	ACCIÓN
80 - 100	ACCIÓN A
60 - 79	ACCIÓN B
40 - 59	ACCIÓN C
0 - 39	ACCIÓN D

922

FIG. 30

ES 2 619 367 T3

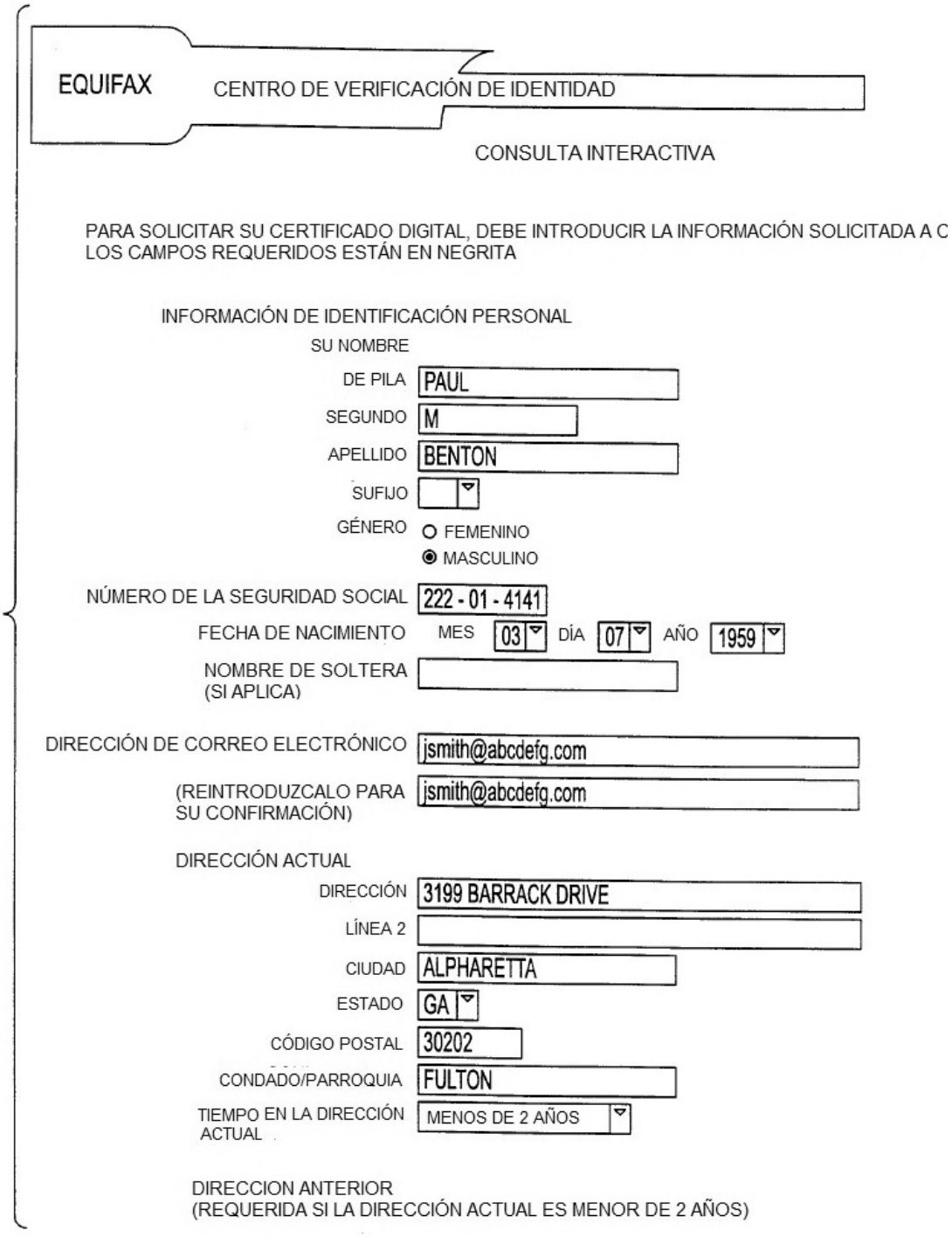

EQUIFAX
CENTRO DE VERIFICACIÓN DE IDENTIDAD
CONSULTA INTERACTIVA
PARA SOLICITAR SU CERTIFICADO DIGITAL, DEBE INTRODUCIR LA INFORMACIÓN SOLICITADA A C
LOS CAMPOS REQUERIDOS ESTÁN EN NEGRITA
INFORMACIÓN DE IDENTIFICACIÓN PERSONAL
SU NOMBRE
DE PILA
PAUL
SEGUNDO
M
APELLIDO
BENTON
SUFIJO
GÉNERO
FEMENINO
MASCULINO
NÚMERO DE LA SEGURIDAD SOCIAL
222 - 01 - 4141
FECHA DE NACIMIENTO
MES
03
DÍA
07
AÑO
1959
NOMBRE DE SOLTERA
(SI APLICA)
DIRECCIÓN DE CORREO ELECTRÓNICO
jsmith@abcdefg.com
(REINTRODUZCALO PARA
SU CONFIRMACIÓN)
jsmith@abcdefg.com
DIRECCIÓN ACTUAL
DIRECCIÓN
3199 BARRACK DRIVE
LÍNEA 2
CIUDAD
ALPHARETTA
ESTADO
GA
CÓDIGO POSTAL
30202
CONDADO/PARROQUIA
FULTON
TIEMPO EN LA DIRECCIÓN
ACTUAL
MENOS DE 2 AÑOS
DIRECCION ANTERIOR
(REQUERIDA SI LA DIRECCIÓN ACTUAL ES MENOR DE 2 AÑOS)

FIG. 31

DIRECCIÓN 8544 FULTON INDUSTRIAL BLVD

LÍNEA 2

CIUDAD ATLANTA

ESTADO GA

CÓDIGO POSTAL 30396

CONDADO/PARROQUIA FULTON

INFORMACIÓN DEL NÚMERO DE TELÉFONO

LOS NÚMEROS DE TELÉFONO PUEDEN TENER EL FORMATO (nnn) nnn - nnnn, o nnn . nnn - nnnn, O n

NÚMERO DE TELÉFONO DE CASA (770) 592 - 3673

¿HA CAMBIADO EL CÓDIGO DE ÁREA DE SU NÚMERO DE TELÉFONO DE CASA EN LOS ÚLTIMOS 6 MESES? NO

¿HA TENIDO SU NÚMERO DE TELÉFONO DE CASA ACTUAL POR MÁS DE 4 MESES? SI

¿ESTÁ PUBLICADO SU NÚMERO DE TELÉFONO DE CASA? SI

NÚMERO DE TELÉFONO DE TRABAJO

EXTENSIÓN

INFORMACIÓN DEL CARNET DE CONDUCIR

¿TIENE O HA TENIDO ALGUNA VEZ UN CARNET DE CONDUCIR (REQUERIDOS NÚMERO Y ESTADO EN CASO AFIRMATIVO) O SI O NO

NÚMERO DEL CARNET DE CONDUCIR B36492014

ESTADO DE EMISIÓN GA

DIRECCIÓN DEL CARNET DE CONDUCIR (DIRECCIÓN REQUERIDA SI ES DIFERENTE) O MISMA QUE LA DIRECCIÓN ACTUAL O MISMA QUE DIRECCIÓN ANTERIOR O DIRECCIÓN DIFERENTE

DIRECCIÓN

LÍNEA 2

CIUDAD

ESTADO

CÓDIGO POSTAL

POR FAVOR INTRODUZCA LA SIGUIENTE INFORMACIÓN.
SE USARÁ PARA SEGURIDAD ADICIONAL

FIG. 32

NOMBRE DE SOLTERA DE LA MADRE

AÑO DE GRADUACIÓN DE LA ESCUELA SECUNDARIA (AAAA)

NÚMERO DE HERMANOS (INCLUYENDO MEDIO HERMANOS Y HERMANASTROS)

ENVIAR SOLICITUD CANCELAR SOLICITUD

FIG 33

EQUIFAX

CENTRO DE VERIFICACIÓN DE IDENTIDAD

CONSULTA INTERACTIVA

1. SU ARCHIVO DE CRÉDITO INDICA QUE PUEDE TENER UN PRÉSTAMO HIPOTECARIO, EN O ALREDEDOR DE AGOSTO DE 1998. POR FAVOR ELIJA EL PROVEEDOR DE CRÉDITO PARA LAS SIGUIENTES OPCIONES:

- ○ BANK OF AMERICA, FSB
- ○ DARBY BANK & TRUST CO.
- ◉ HEALTH CARE CREDIT UNION
- ○ IBEW FEDERAL CREDIT UNION
- ○ **NINGUNA DE LAS ANTERIORES**

2. POR FAVOR ELIJA EL INTERVALO DENTRO DEL CUAL ESTÁ SU PAGO MENSUAL PARA LA CUENTA ANTERIORMENTE REFERENCIADA. SI HACE PAGO BISEMANALES MULTIPLIQUE EL PAGO POR 2.17 PARA CACULAR EL PAGO MENSUAL.

- ○ $575 - $674
- ○ $675 - $774
- ◉ $775 - $874
- ○ $875 - $974
- ○ **NINGUNA DE LAS ANTERIORES**

3. SU ARCHIVO DE CRÉDITO INDICA QUE USTED PUEDE TENER UNA CUENTA A PLAZOS TAL COMO UN PRÉSTAMO BANCARIO, CUENTAS DE DISPOSITIVOS ELECTRÓNICOS, CUENTAS DE JOYEROS, PRESTAMOS AUTOMOVILÍSTICOS ABIERTOS EN O SOBRE NOVIEMBRE DE 1994. POR FAVOR ELIJA EL ACREEDOR DE LAS SIGUIENTES OPCIONES:

- ◉ EXCEL FEDERAL CREDTI UNION
- ○ HALLMARK FINANCE CO.
- ○ INDEPENDENT BANK
- ○ JOE COOPER'S FINANCE CORP.
- ○ **NINGUNA DE LAS ANTERIORES**

FIG. 34

4. POR FAVOR ELIJA EL INTERVALO DENTRO DEL CUAL ESTÁ SU PAGO MENSUAL PARA LA CUENTA REFERENCIADA ANTERIORMENTE. SI USTED HACE PAGOS BISEMANALES MULTIPLIQUE EL PAGO POR 2.17 PARA CALCULAR EL PAGO MENSUAL

- ○ $375 - $424
- ◉ $425 - $474
- ○ $475 - $524
- ○ $525 - 4574
- ○ **NINGUNA DE LAS ANTERIORES**

ENVIAR SOLICITUD | CANCELAR SOLICITUD

FIG. 35


EQUIFAX
CENTRO DE VERIFICACIÓN DE IDENTIDAD
CONSULTA INTERACTIVA
USTED HA SIDO AUTENTIFICADO CON ÉXITO.
PARA CONSEGUIR SU CERTIFICADO DIGITAL, HAGA CLIC EN EL BOTÓN CONTINUAR.
CONTINUAR

FIG. 36

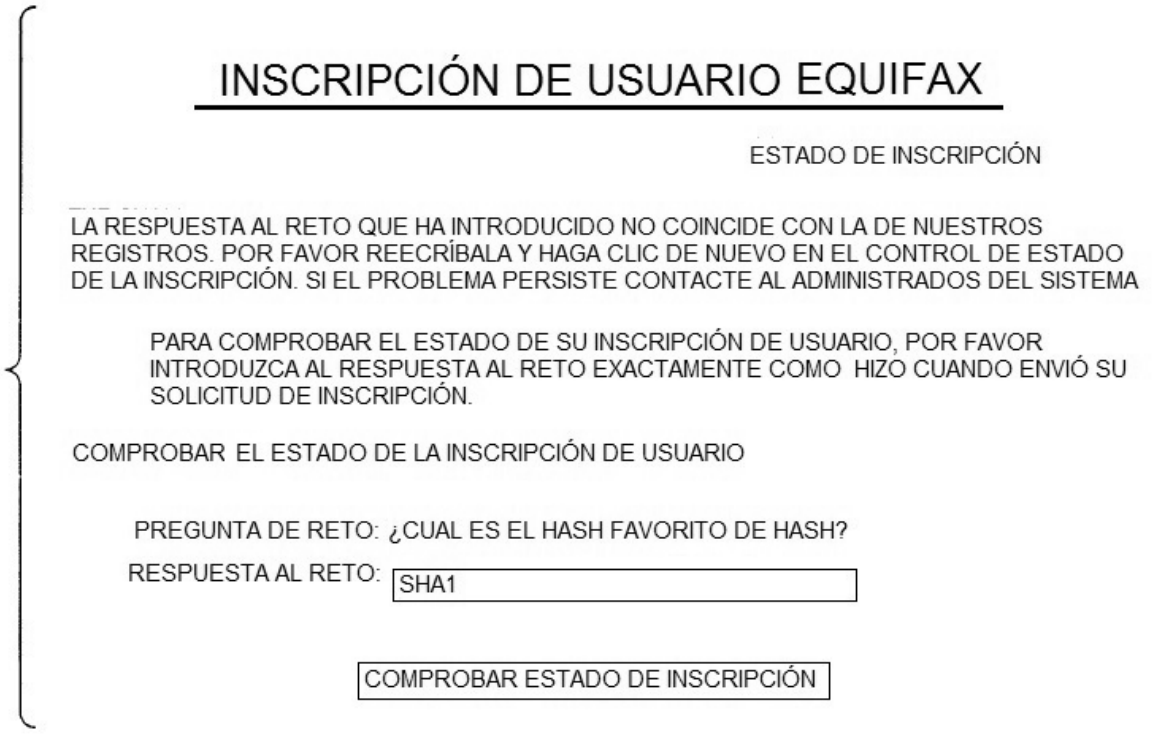

INSCRIPCIÓN DE USUARIO EQUIFAX
ESTADO DE INSCRIPCIÓN
LA RESPUESTA AL RETO QUE HA INTRODUCIDO NO COINCIDE CON LA DE NUESTROS REGISTROS. POR FAVOR REECRÍBALA Y HAGA CLIC DE NUEVO EN EL CONTROL DE ESTADO DE LA INSCRIPCIÓN. SI EL PROBLEMA PERSISTE CONTACTE AL ADMINISTRADOS DEL SISTEMA
PARA COMPROBAR EL ESTADO DE SU INSCRIPCIÓN DE USUARIO, POR FAVOR INTRODUZCA AL RESPUESTA AL RETO EXACTAMENTE COMO HIZO CUANDO ENVIÓ SU SOLICITUD DE INSCRIPCIÓN.
COMPROBAR EL ESTADO DE LA INSCRIPCIÓN DE USUARIO
PREGUNTA DE RETO: ¿CUAL ES EL HASH FAVORITO DE HASH?
RESPUESTA AL RETO: SHA1
COMPROBAR ESTADO DE INSCRIPCIÓN

FIG. 37

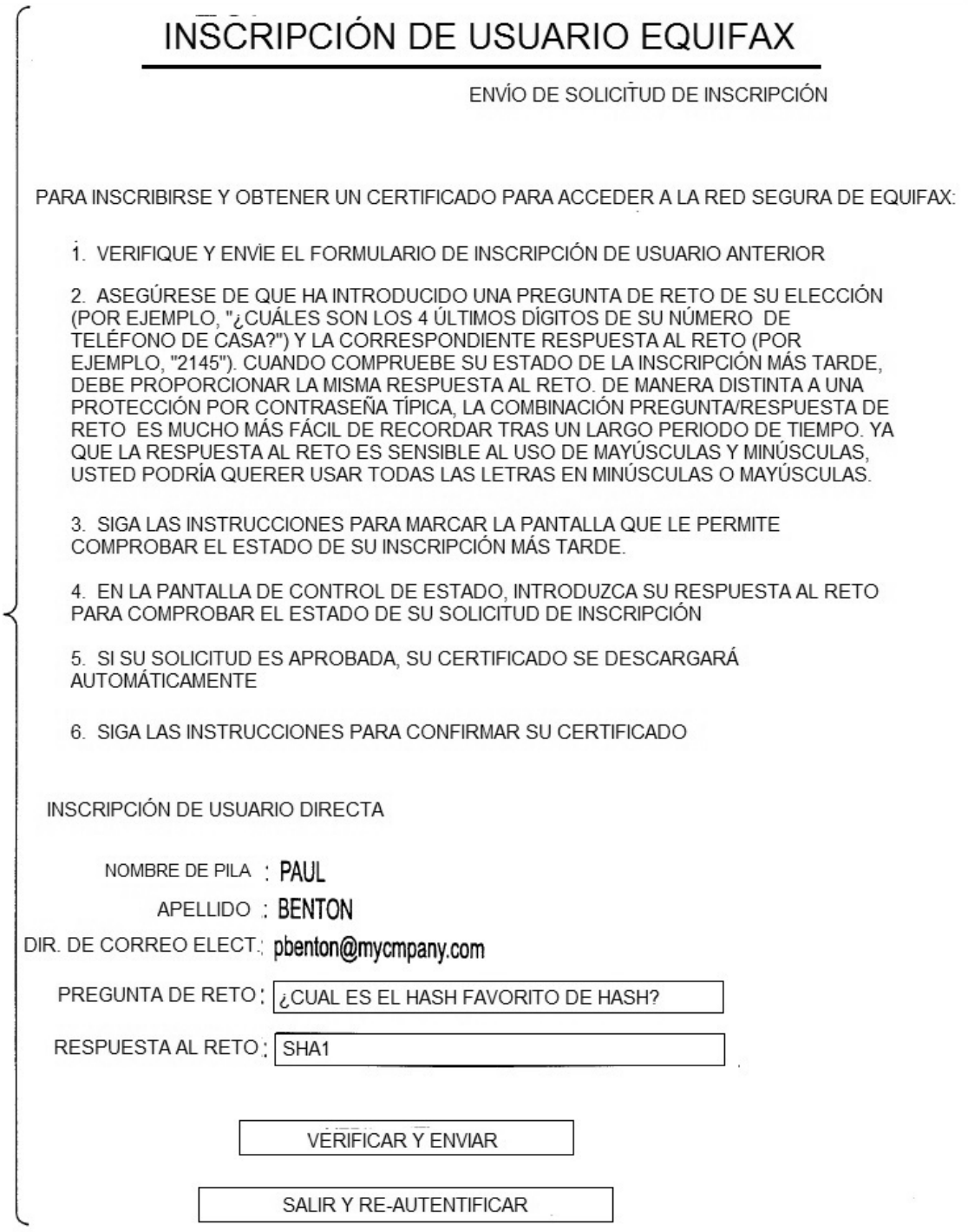

INSCRIPCIÓN DE USUARIO EQUIFAX
ENVÍO DE SOLICITUD DE INSCRIPCIÓN
PARA INSCRIBIRSE Y OBTENER UN CERTIFICADO PARA ACCEDER A LA RED SEGURA DE EQUIFAX:
1. VERIFIQUE Y ENVÍE EL FORMULARIO DE INSCRIPCIÓN DE USUARIO ANTERIOR
2. ASEGÚRESE DE QUE HA INTRODUCIDO UNA PREGUNTA DE RETO DE SU ELECCIÓN (POR EJEMPLO, "¿CUÁLES SON LOS 4 ÚLTIMOS DÍGITOS DE SU NÚMERO DE TELÉFONO DE CASA?") Y LA CORRESPONDIENTE RESPUESTA AL RETO (POR EJEMPLO, "2145"). CUANDO COMPRUEBE SU ESTADO DE LA INSCRIPCIÓN MÁS TARDE, DEBE PROPORCIONAR LA MISMA RESPUESTA AL RETO. DE MANERA DISTINTA A UNA PROTECCIÓN POR CONTRASEÑA TÍPICA, LA COMBINACIÓN PREGUNTA/RESPUESTA DE RETO ES MUCHO MÁS FÁCIL DE RECORDAR TRAS UN LARGO PERIODO DE TIEMPO. YA QUE LA RESPUESTA AL RETO ES SENSIBLE AL USO DE MAYÚSCULAS Y MINÚSCULAS, USTED PODRÍA QUERER USAR TODAS LAS LETRAS EN MINÚSCULAS O MAYÚSCULAS.
3. SIGA LAS INSTRUCCIONES PARA MARCAR LA PANTALLA QUE LE PERMITE COMPROBAR EL ESTADO DE SU INSCRIPCIÓN MÁS TARDE.
4. EN LA PANTALLA DE CONTROL DE ESTADO, INTRODUZCA SU RESPUESTA AL RETO PARA COMPROBAR EL ESTADO DE SU SOLICITUD DE INSCRIPCIÓN
5. SI SU SOLICITUD ES APROBADA, SU CERTIFICADO SE DESCARGARÁ AUTOMÁTICAMENTE
6. SIGA LAS INSTRUCCIONES PARA CONFIRMAR SU CERTIFICADO
INSCRIPCIÓN DE USUARIO DIRECTA
NOMBRE DE PILA : PAUL
APELLIDO : BENTON
DIR. DE CORREO ELECT.: pbenton@mycmpany.com
PREGUNTA DE RETO : ¿CUAL ES EL HASH FAVORITO DE HASH?
RESPUESTA AL RETO : SHA1
VERIFICAR Y ENVIAR
SALIR Y RE-AUTENTIFICAR

FIG. 38

EQUIFAX

CERTIFICADO CENTRAL

EL CERTIFICADO CENTRAL ES EL PUNTO DE INICIO PARA LA EMISIÓN DEL CERTIFICADO ACTUAL.

SI TIENE PREGUNTAS SOBRE LA INSCRIPCIÓN DEL CERTIFICADO, POR FAVOR LEA LAS PREGUNTAS FRECUENTEMENTE HECHAS PARA LA INSCRIPCIÓN DE UN CERTIFICADO EQUIFAX Y SUS RESPUESTAS PARA MAYOR INFORMACIÓN

¿QUE NAVEGADORES SON SOPORTADOS PARA LA INSCRIPCION DEL CERTIFICADO?

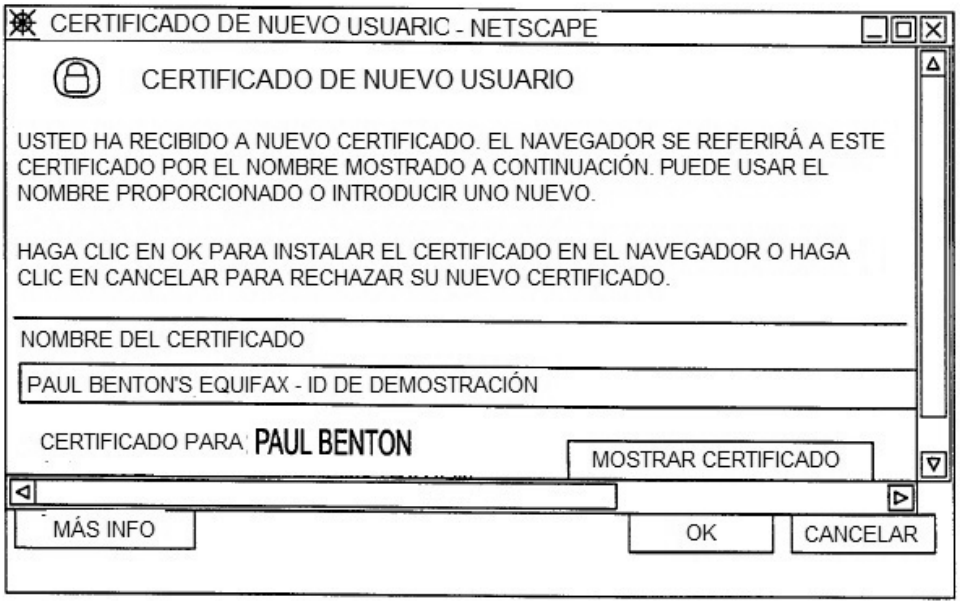
LA INSCRIPCIÓN DEL CERTIFICADO SOPORTA EL NETSCAPE NAVIGATOR 3.x, NAVIGATOR AND COMUNICATOR 4.x, Y MICROSOFT INTERNET EXPLORER 4.X CON JAVASCRIPT HABILITADO.

INCRIPCIÓN DEL CERTIFICADO EQUIFAX

SR. BENTON, PARA SOLICITAR SU CERTIFIADO BASÁNDOSE EN SU EXITOSA AUTENTIFICACIÓN , PULSE EL BOTÓN IR.

IR.

FIG. 39



FIN

FIG. 40

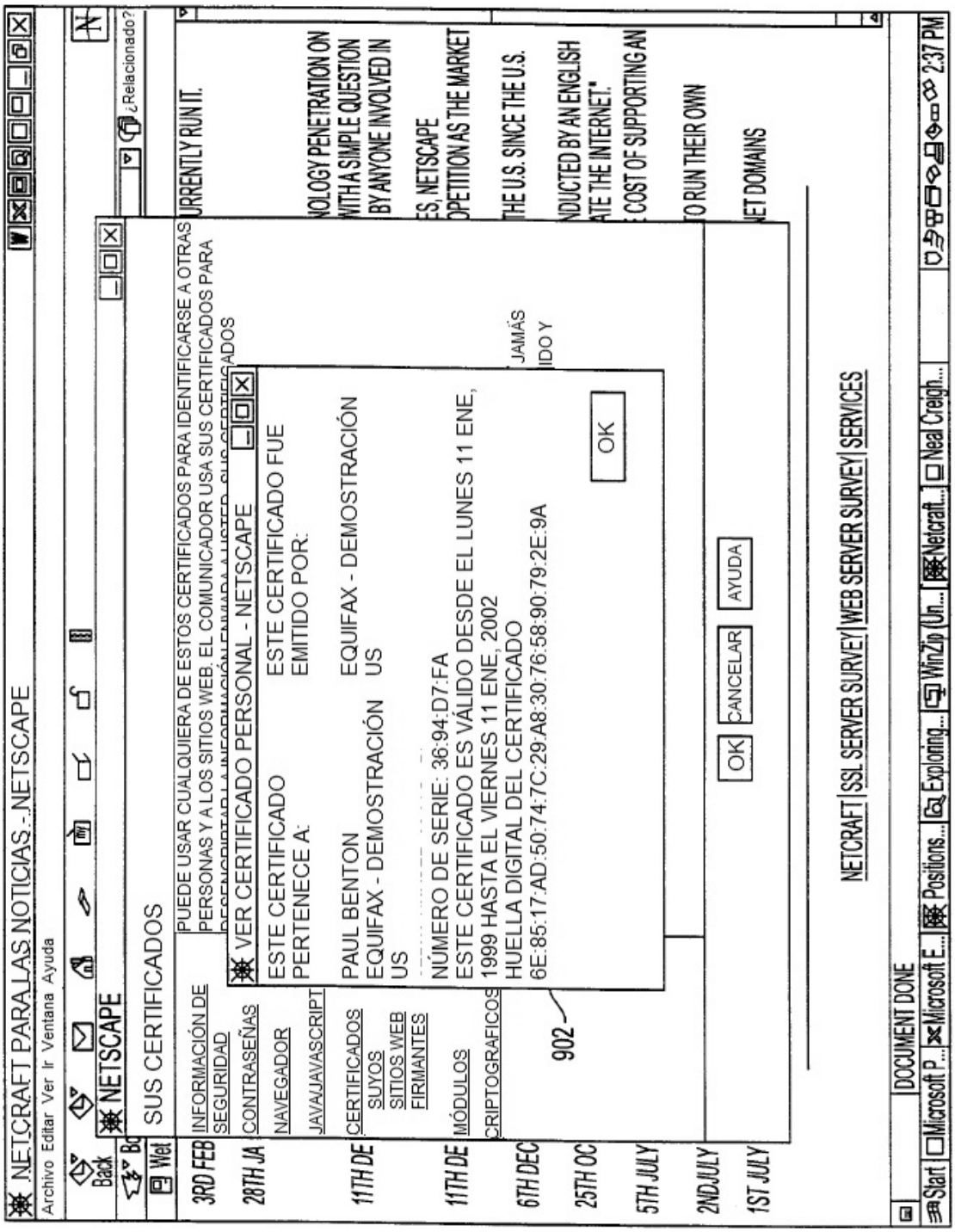

NETCRAFT PARA LAS NOTICIAS - NETSCAPE
Archivo Editar Ver Ir Ventana Ayuda
Back
NETSCAPE
¿Relacionado?
SUS CERTIFICADOS
INFORMACIÓN DE SEGURIDAD
CONTRASEÑAS
NAVEGADOR
JAVA/JAVASCRIPT
CERTIFICADOS
SUYOS
SITIOS WEB
FIRMANTES
MÓDULOS
CRIPTOGRAFICOS
PUEDE USAR CUALQUIERA DE ESTOS CERTIFICADOS PARA IDENTIFICARSE A OTRAS PERSONAS Y A LOS SITIOS WEB. EL COMUNICADOR USA SUS CERTIFICADOS PARA
VER CERTIFICADO PERSONAL - NETSCAPE
ESTE CERTIFICADO PERTENECE A:
PAUL BENTON
EQUIFAX - DEMOSTRACIÓN
US
NÚMERO DE SERIE: 36:94:D7:FA
ESTE CERTIFICADO ES VÁLIDO DESDE EL LUNES 11 ENE, 1999 HASTA EL VIERNES 11 ENE, 2002
HUELLA DIGITAL DEL CERTIFICADO
6E:85:17:AD:50:74:7C:29:A8:30:76:58:90:79:2E:9A
ESTE CERTIFICADO FUE EMITIDO POR:
EQUIFAX - DEMOSTRACIÓN
US
OK
902
OK
CANCELAR
AYUDA
URRENTLY RUN IT.
NOLOGY PENETRATION ON
WITH A SIMPLE QUESTION
BY ANYONE INVOLVED IN
ES, NETSCAPE
OPETITION AS THE MARKET
THE U.S. SINCE THE U.S.
NDUCTED BY AN ENGLISH
ATE THE INTERNET."
COST OF SUPPORTING AN
TO RUN THEIR OWN
NET DOMAINS
JAMÁS
IDO Y
3RD FEB
28TH JA
11TH DE
11TH DE
6TH DEC
25TH OC
5TH JULY
2NDJULY
1ST JULY
NETCRAFT | SSL SERVER SURVEY | WEB SERVER SURVEY | SERVICES
DOCUMENT DONE
Start
Microsoft P...
Microsoft E...
Positions...
Exploring...
WinZip (Un...
Netcraft...
Neal Creigh...
2:37 PM

FIG. 41

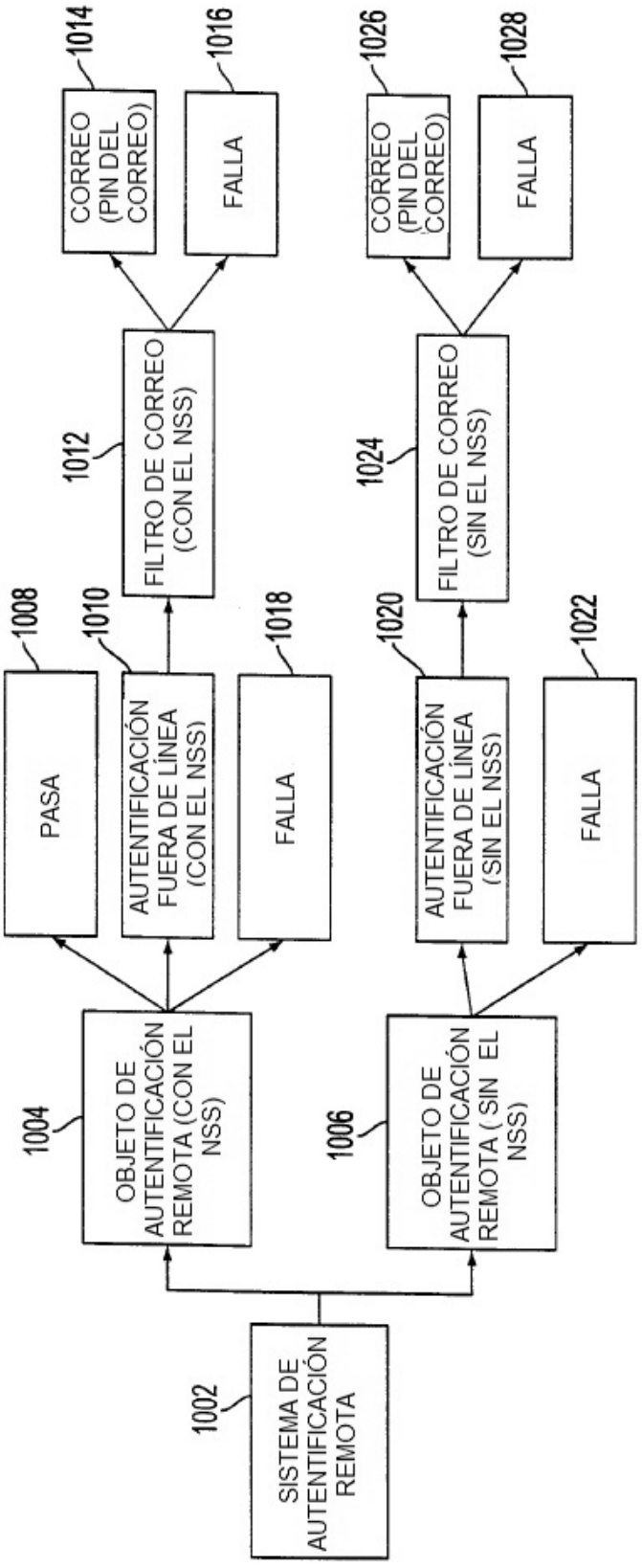

1002
SISTEMA DE AUTENTIFICACIÓN REMOTA
1004
OBJETO DE AUTENTIFICACIÓN REMOTA (CON EL NSS)
1006
OBJETO DE AUTENTIFICACIÓN REMOTA (SIN EL NSS)
1008
PASA
1010
AUTENTIFICACIÓN FUERA DE LÍNEA (CON EL NSS)
1012
FILTRO DE CORREO (CON EL NSS)
1014
CORREO (PIN DEL CORREO)
1016
FALLA
1018
FALLA
1020
AUTENTIFICACIÓN FUERA DE LÍNEA (SIN EL NSS)
1022
FALLA
1024
FILTRO DE CORREO (SIN EL NSS)
1026
CORREO (PIN DEL CORREO)
1028
FALLA

FIG. 42

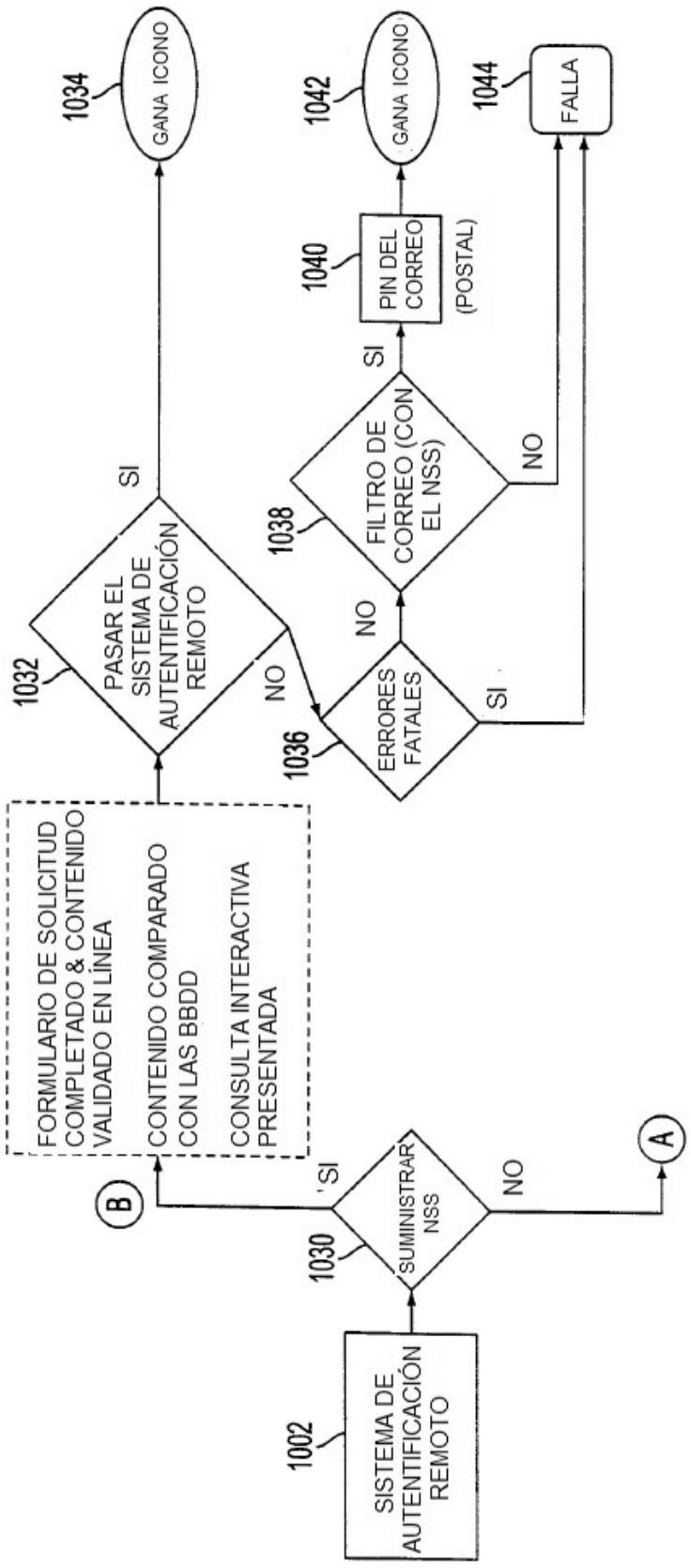

1002
SISTEMA DE AUTENTIFICACIÓN REMOTO
1030
SUMINISTRAR NSS
SI
NO
A
B
FORMULARIO DE SOLICITUD COMPLETADO & CONTENIDO VALIDADO EN LÍNEA
CONTENIDO COMPARADO CON LAS BBDD
CONSULTA INTERACTIVA PRESENTADA
1032
PASAR EL SISTEMA DE AUTENTIFICACIÓN REMOTO
SI
NO
1034
GANA ICONO
1036
ERRORES FATALES
SI
NO
1038
FILTRO DE CORREO (CON EL NSS)
SI
NO
1040
PIN DEL CORREO (POSTAL)
1042
GANA ICONO
1044
FALLA

FIG. 43

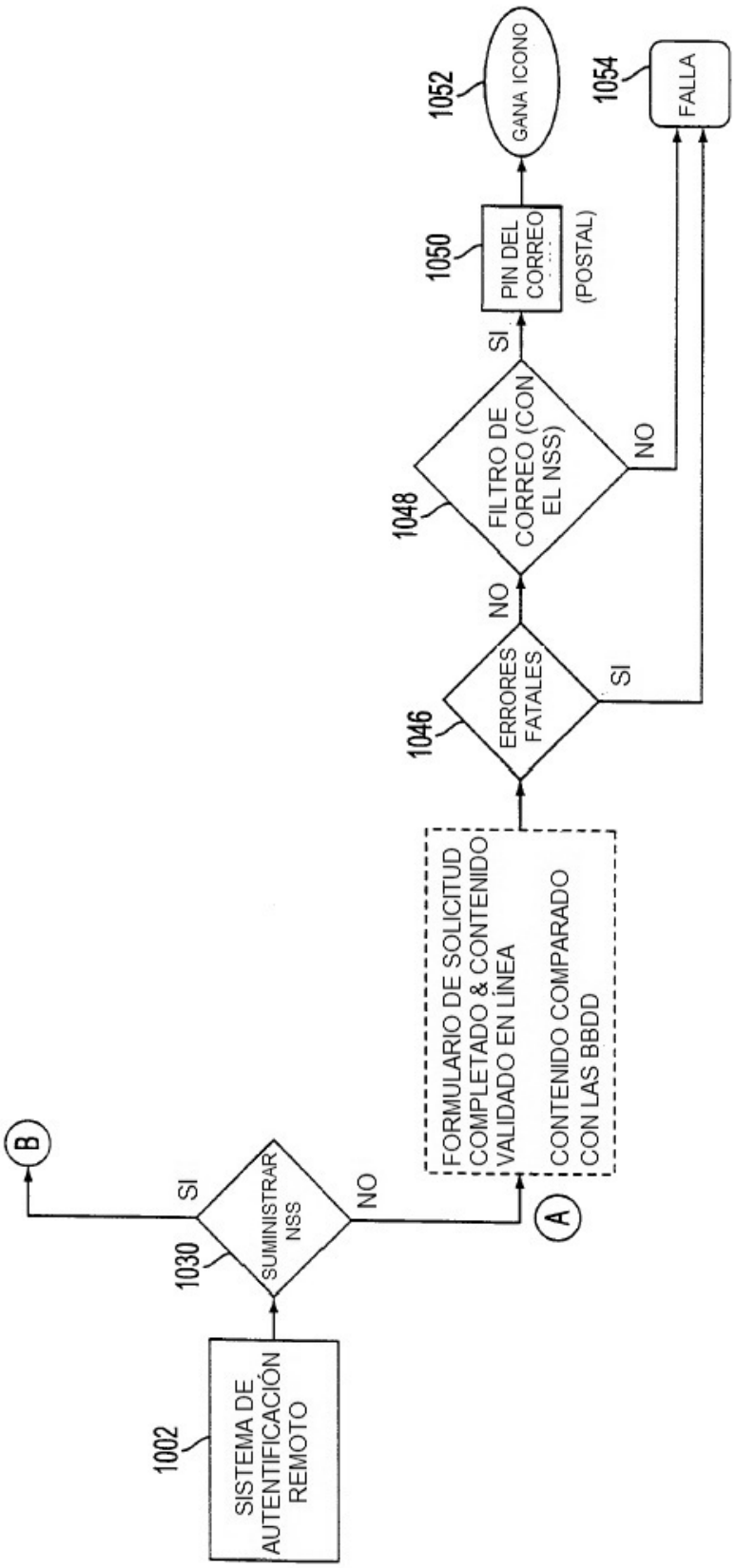

1002
SISTEMA DE AUTENTIFICACIÓN REMOTO
1030
SUMINISTRAR NSS
SI
NO
B
A
FORMULARIO DE SOLICITUD COMPLETADO & CONTENIDO VALIDADO EN LÍNEA
CONTENIDO COMPARADO CON LAS BBDD
1046
ERRORES FATALES
SI
NO
1048
FILTRO DE CORREO (CON EL NSS)
NO
SI
1050
PIN DEL CORREO
(POSTAL)
1052
GANA ICONO
1054
FALLA

FIG. 44

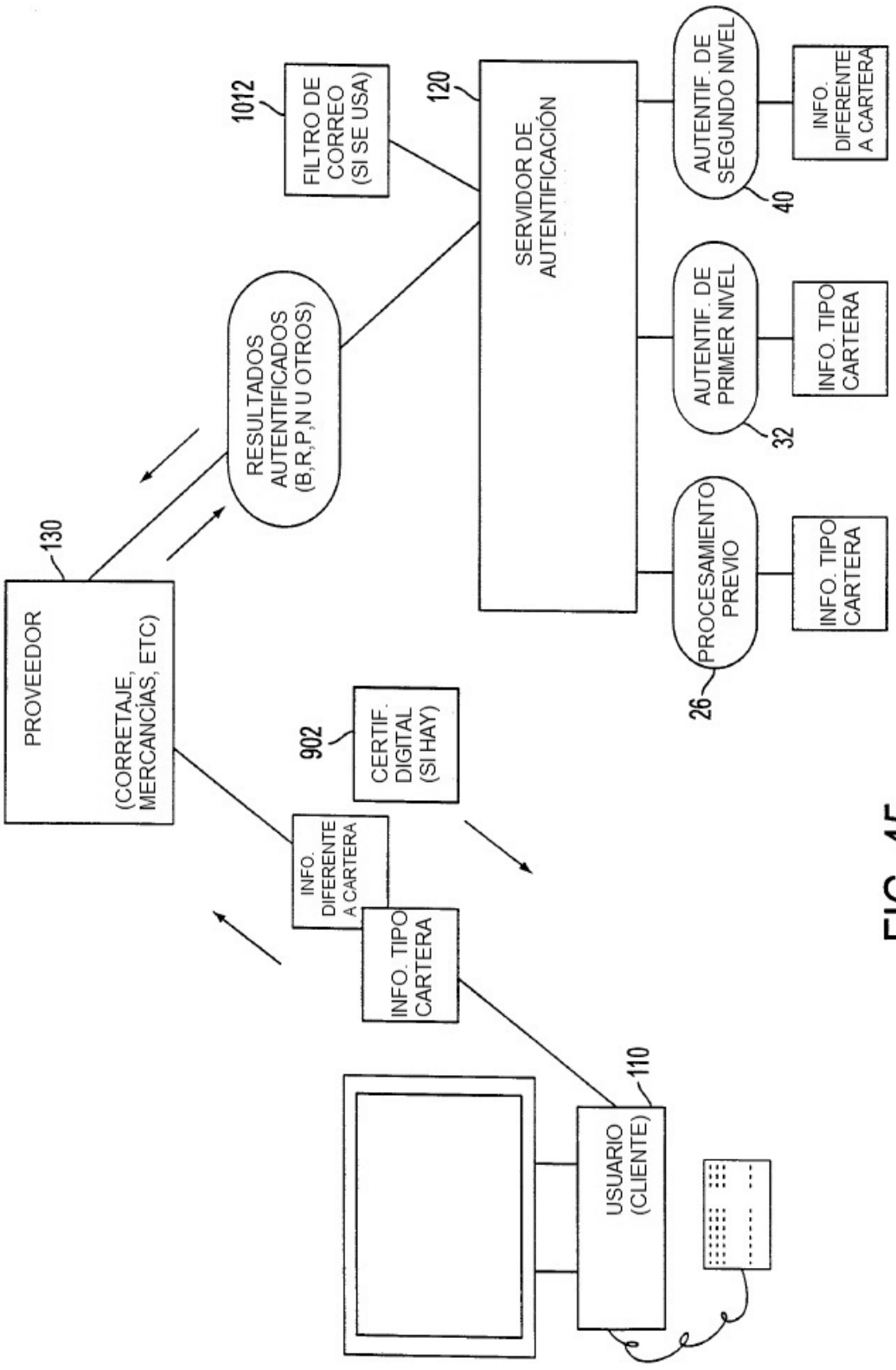

PROVEEDOR
(CORRETAJE, MERCANCÍAS, ETC)
130
RESULTADOS AUTENTIFICADOS (B,R,P,N U OTROS)
1012
FILTRO DE CORREO (SI SE USA)
120
SERVIDOR DE AUTENTIFICACIÓN
AUTENTIF. DE SEGUNDO NIVEL
40
INFO. DIFERENTE A CARTERA
AUTENTIF. DE PRIMER NIVEL
32
INFO. TIPO CARTERA
PROCESAMIENTO PREVIO
26
INFO. TIPO CARTERA
902
CERTIF. DIGITAL (SI HAY)
INFO. DIFERENTE A CARTERA
INFO. TIPO CARTERA
USUARIO (CLIENTE)
110

FIG. 45