(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 776 129**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06Q 50/26 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.08.2010 PCT/US2010/044130**

(87) Fecha y número de publicación internacional: **03.02.2011 WO11014878**

(96) Fecha de presentación y número de la solicitud europea: **02.08.2010 E 10805176 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2019 EP 2460307**

(54) Título: **Sistema y método para una prueba de identidad remota fuerte**

(30) Prioridad:

31.07.2009 US 230389 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.07.2020

(73) Titular/es:

ANAKAM, INC. (100.0%)
9171 Town Centre Drive Suite 460
San Diego, CA 92122, US

(72) Inventor/es:

WILLIAMS, JEFFREY, B. y
CAMAISA, ALLAN

(74) Agente/Representante:

ELZABURU, S.L.P

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema y método para una prueba de identidad remota fuerte

Antecedentes

La presente invención se refiere en general a los sistemas y métodos utilizados para confirmar la identidad afirmada de un individuo con un alto nivel de confianza de forma remota a través de la Web. El mismo método también se puede utilizar en una transacción cara a cara cuando el individuo que afirma su identidad no tiene otra información de identificación.

La prueba de identidad se extiende a través de múltiples niveles de riesgo. La prueba de identidad suele ser la primera etapa en un proceso asociado con la emisión de credenciales a un individuo. La credencial se puede reutilizar una y otra vez como una afirmación de la prueba de identidad inicial. El proceso de utilizar la credencial para realizar una transacción es la autenticación. Además, el riesgo asociado con la prueba de identidad es independiente del riesgo asociado con la autenticación. Como ejemplo, hay algunas transacciones en las que el usuario puede ser anónimo, pero la información proporcionada debe permanecer confidencial y asociada solo con ese usuario único. En tal caso, la prueba de identidad puede ser débil o inexistente, mientras que la credencial y la autenticación son fuertes. Estas pruebas de identidad, credenciales y principios de autenticación se aplican tanto en contextos físicos como lógicos.

En el contexto lógico (y también en el físico), la prueba de identidad puede realizarse cara a cara, por referencia o por autoafirmación. Cada uno de estos tipos de pruebas de identidad puede aprovechar una serie de etapas para probar la identidad y las etapas implementadas definen el rigor y la fuerza de la prueba de identidad. Como ejemplo, la prueba de identidad cara a cara puede requerir una única identificación con foto emitida por el gobierno o podría requerir dos más una verificación de domicilio.

De acuerdo con la Publicación Especial NIST 800-63, la base de la prueba de identidad remota con una alta confianza de la identidad de los individuos se define como "Posesión de una identificación gubernamental válida (por ejemplo, una licencia de conducir o pasaporte) y un número de cuenta financiera (por ejemplo, cuenta corriente, cuenta de ahorro, préstamo o tarjeta de crédito) con confirmación mediante registros de ambos números ". Este documento continúa definiendo las acciones necesarias para lograr estas acciones. La publicación especial NIST 800-63 establece que la autoridad de registro (RA) primero "verifica la información proporcionada por el solicitante, incluido el número de identificación y el número de cuenta a través de verificaciones de registros, ya sea con la agencia o institución correspondiente o mediante agencias de crédito o bases de datos similares, y confirma que: nombre, [fecha de nacimiento], dirección y otra información personal en los registros son consistentes con la solicitud y suficientes para identificar a un individuo único ". La RA también debe proporcionar la confirmación de la dirección realizando cualquiera de estas acciones, "a) Emite credenciales de una manera que confirma la dirección de registro proporcionada por el Solicitante; o b) Emite credenciales de una manera que confirma la capacidad del Solicitante para recibir comunicaciones telefónicas en un número asociado con el Solicitante en los registros, mientras graba la voz del Solicitante o utiliza medios alternativos equivalentes para establecer el no rechazo ".

El documento WO01/44940 (Authentify Inc.) se refiere a un método para intentar verificar la identidad de un usuario de Internet mediante el uso de comunicaciones simultáneas o sustancialmente simultáneas en dos redes diferentes para verificar la identidad de un usuario. Cuando un usuario inicia sesión en un sitio, a través de Internet, se utiliza un número de teléfono, previamente almacenado u obtenido en tiempo real del visitante, donde se puede llamar al visitante esencialmente de inmediato, para configurar, a través de la red telefónica conmutada, otro enlace de comunicación. El documento US2004/254868 (Kirkland Dustin C et al) se refiere a un sistema y método para la detección temprana y la prevención del robo de identidad. Un usuario autorizado establece una identidad con el sistema informático de una organización y registra un dispositivo móvil y un dispositivo de notificación con el sistema informático de la organización. Cuando se intenta un uso de la identidad, se recupera un registro asociado con la identidad y se envía una solicitud al dispositivo móvil registrado para obtener información de ubicación. La ubicación actual del dispositivo móvil se compara con la ubicación de la fuente de la solicitud para la autorización. Si la ubicación actual del dispositivo móvil no se encuentra dentro del área de origen de la solicitud de autenticación, la información sobre el intento de uso se compara con los criterios de notificación registrados. Si las condiciones del intento de uso caen dentro de los criterios de notificación, se envía un mensaje de notificación al dispositivo de notificación. El documento EP0444351 (American Telephone & Telegraph) se refiere a un sistema de seguridad controlado por contraseña de voz. Después de completar con éxito el procedimiento de contraseña normal, el ordenador realiza una llamada de voz a un teléfono asociado con el usuario. El ordenador le pregunta al usuario que repita una serie de dígitos seleccionados al azar o una frase que consiste en un grupo de palabras. Luego, el ordenador compara la información de voz recibida a través de la línea de voz con la información de voz previamente almacenada asociada con el supuesto usuario. El ordenador permite el acceso a sus recursos si y solo si se produce una coincidencia de voz. Kevin Trilli et al ((Knowledge-Based Authentication. Challenge Response System) proporciona seguridad crítica e infraestructura de pago basada en VeriSign® Security. El documento WO2007/051090 (Daylife Inc.) se refiere a un artículo en línea que comprende instancias de creadores de noticias que es proporcionado por un servidor de noticias conectado a Internet o un servidor de agregador de noticias y los nombres de los creadores de noticias se identifican automáticamente mediante un módulo de verificación y comentarios de los creadores de noticias. El artículo se muestra a un lector en un ordenador cliente conectado a Internet. Las instancias de los creadores de noticias en el

artículo se enfatizan de tal manera que se destacan en el artículo. El lector inicia un proceso de verificación al indicar que es un periodista. El módulo de verificación y comentarios de los comunicadores de noticias está en comunicación con una base de datos de verificación y la identidad del lector se verifica como el creador de noticias a través de una serie de preguntas y respuestas. El documento WO 2008/002979 (Solidus Networks Inc et al) se refiere a un sistema y método para autorizar un pago por una transacción en el punto de venta mediante la autenticación del usuario de un dispositivo móvil, como un teléfono móvil.

Las instituciones buscan una capacidad para implementar los requisitos de los estándares NIST y, al mismo tiempo, permiten la prueba de identidad remota de un individuo a través de una transacción Web, de modo que no haya demora y el usuario pueda realizar inmediatamente transacciones con esa identidad. El proceso de confirmación de un número de cuenta o identidad emitida por el gobierno junto con una confirmación de dirección generalmente requiere una demora al realizar estas etapas del proceso. Esta realización describe un método y un proceso para realizar esta transacción descrita anteriormente de forma remota mientras lo hace de modo que la transacción pueda procesarse en tiempo real y permitir las transacciones posteriores si la transacción de prueba de identidad es exitosa.

Compendio de la invención

El objeto de la presente invención se resuelve mediante un método que tiene las características de la reivindicación 1 y mediante un aparato que tiene las características de la reivindicación 7. Realizaciones ventajosas de los mismos se definen en las respectivas reivindicaciones dependientes.

La presente invención proporciona sistemas y métodos para una prueba de identidad remota fuerte tal como se define en las reivindicaciones. Al confirmar con un alto nivel de confianza que la identidad electrónica afirmada es la del individuo real, el individuo que realiza la prueba de identidad electrónica deberá afirmar una identidad proporcionando los detalles biográficos de su identidad, incluidos, pero no limitados a, su nombre legal, fecha de nacimiento y dirección. El sistema consultará los repositorios de datos con los datos biográficos proporcionados. Estos repositorios de datos incluyen, pero no están limitados a, registros empresariales existentes, fuentes de datos públicos, proveedores que agregan datos públicos y agencias de crédito. Esta realización proporciona el método para cumplir con las tres etapas clave del proceso: 1) validar la identidad emitida por el gobierno, 2) validar el número de cuenta y 3) confirmar la dirección proporcionada en los registros en tiempo real. Además, esta realización proporciona preguntas adicionales basadas en el conocimiento del proceso de recopilación de datos que se van a presentar para confirmar aún más la identidad.

La presente realización recopila cantidades y cualidades variables de datos sobre el individuo. Una vez recopiladas, determina si es capaz de realizar la prueba de identidad en función de los datos disponibles. Si es así, combina un conjunto de interfaces gráficas de usuario, así como preguntas y respuestas para facilitar la implementación en tiempo real de este estándar.

Los métodos y sistemas descritos en este documento pueden utilizarse para cualquier prueba de identidad en la que se requiera una alta confianza de que la afirmada es la identidad real del usuario final. Esto incluye, pero no se limita a, transacciones electrónicas gubernamentales, de atención médica, bancarias y comerciales realizadas en una infraestructura de red, incluida la WWW. Los detalles de la presente invención, tanto en cuanto a su estructura como a su funcionamiento, pueden entenderse mejor en referencia a los dibujos adjuntos, en los que los números de referencia similares se refieren a partes similares, y en los que:

Breve descripción de los dibujos

La figura 1 muestra el flujo del proceso general completo para realizar pruebas de identidad de alta confianza remotas.

La figura 2 muestra y el detalle detrás del flujo del proceso del sistema de interfaz gráfica de usuario para el usuario.

Descripción detallada

A menos que se especifique lo contrario, todas las referencias de figuras en este documento se refieren a la figura 1. La presente invención proporciona un método de prueba de identidad remota en tiempo real a un usuario que utiliza un sistema de información como se define en las reivindicaciones. Un usuario (1) que utiliza un ordenador conectado a la Web (10) se conecta a un sistema a través de un servidor (11) Web que requiere prueba de identidad. El servidor (12) de prueba de identidad presenta una solicitud (100) al servidor Web para mostrar una página solicitando al usuario que proporcione las credenciales. El servidor Web muestra esta página en (101) [El detalle se puede encontrar en la secuencia de la figura 2 (901)]. El usuario (1) en (101) afirma su propia identidad al proporcionar información biográfica a un sistema que solicita dicha información al solicitante de registro. Esta información incluye mínimamente el nombre y la dirección legales como mínimo, pero opcionalmente puede requerir la fecha de nacimiento, el Número de Seguro Social o algún otro identificador específico de la empresa que admita la resolución de identidad. La información se transfiere del servidor Web al servidor de prueba de identidad en (102). El servidor (12) de prueba de identidad consulta (103) uno o más conjuntos de datos que intentan encontrar al individuo único asociado con la información biométrica y reúne toda la información de identidad emitida por el gobierno disponible, todos los números de cuentas financieras e instituciones (incluidos, pero no limitados a) tarjetas de crédito, hipotecas, préstamos, cuentas corrientes y de ahorros), y todos los números de teléfono asociados con el individuo. Si no hay suficientes datos disponibles, la

empresa puede tomar la decisión de proceder con la prueba de identidad, omitiendo las etapas que no son válidas ya que los datos no están disponibles o no son suficientes, o la empresa puede decidir remitir al individuo a un proceso alternativo que podría incluir detener la prueba de identidad remota y forzar una transacción cara a cara o demorada.

El servidor de prueba de identidad revisa los números de identificación emitidos por el gobierno que tiene registrados y presenta una interfaz gráfica de usuario a través del servidor Web en (201) y (202) que proporciona al usuario una selección de tipos de Identificaciones de Gobierno que puede validar para ese usuario en un botón de selección, una lista desplegable o un formato similar. Esta lista estaría compuesta por aquellos que tiene registrados y eliminaría como inválidos aquellas identificaciones o licencias que la empresa considere inapropiadas para este uso. Esta lista mostrará elementos como la licencia de conducir estatal, la tarjeta de identidad estatal, la tarjeta de identificación militar, la licencia de caza, la licencia de piloto, la licencia médica, etc., pero solo las que tiene sobre el individuo.

El usuario (1) seleccionaría una de las identificaciones para las cuales podría proporcionar un número, o seleccionaría que no tiene ninguna de las identidades en la lista. Luego, se le presentaría al usuario una pantalla en la que se le solicitaría que proporcionara el número de la identificación particular y el usuario escribirá esos datos en la pantalla y los enviará al servidor Web y luego al servidor de prueba de identidad mediante (203) y (204). [El flujo de la interfaz gráfica de usuario detallada para esto y el párrafo anterior se muestran en la figura 2 (902)]

El servidor de prueba de identidad revisa los números de cuenta financiera que tiene registrados y presenta una interfaz gráfica de usuario a través del servidor Web en (205) y (206) que proporciona al usuario una selección de tipos de cuentas financieras que puede validar para ese usuario en un botón de selección, lista desplegable o formato similar. Esta lista estaría compuesta por aquellas que tiene registradas y eliminaría como inválidas aquellas cuentas financieras que la empresa considere inapropiadas para este uso. Esta lista mostraría elementos como tarjeta de crédito, tarjeta de débito, hipoteca, cuenta corriente, cuenta de ahorro, préstamo de automóvil, línea de crédito, etc., pero solo aquellos que tiene sobre el individuo.

El usuario (1) seleccionaría uno de los tipos de cuenta para los cuales podría proporcionar un número, o seleccionaría que no tienen ninguna de las identidades en la lista. Luego, se le presentaría al usuario una pantalla en la que se le solicitaría que proporcionara el número de la cuenta en particular y el usuario escribirá esos datos en la pantalla y los devolverá al servidor Web y luego al servidor de prueba de identidad mediante (207) y (208). Es importante observar que un usuario podría tener tres tarjetas de crédito. Si existen varias cuentas y un tipo de cuenta, el usuario seleccionará el tipo de cuenta e ingresará las cuentas y el sistema se comparará con varios números, no solo con un número único. [El flujo de la interfaz gráfica de usuario detallada para esto y el párrafo anterior se muestran en la figura 2 (903)]

Si hay un error en el proceso de validación, el sistema y el método permiten a la empresa definir si al usuario se le presenta o no el manejo de errores después de cada envío (identificación emitida por el gobierno o cuenta bancaria) o después de ambas presentaciones (identificación emitida por el gobierno y cuenta bancaria).

El sistema y el método permiten opcionalmente la presentación de una serie de preguntas de seguridad secretas al usuario final utilizando la autenticación basada en el conocimiento en (300) y (301). La autenticación basada en el conocimiento puede ser un aumento o un reemplazo para la provisión de una identificación emitida por el gobierno y la provisión de un número de cuenta financiera. El formato de presentación (serie frente a paralelo), el número de preguntas, el balance de las fuentes de datos para esas preguntas, la existencia de respuestas ficticias ("ninguna de las anteriores") en el conjunto de datos y el tiempo permitido para completar las preguntas son completamente controlados por la empresa. El usuario final envía sus respuestas. La prueba se puntúa y la puntuación de la prueba se pondera en la evaluación del éxito completo de la prueba. [Un compendio de este flujo de interfaz gráfica de usuario para esto se muestra en la figura 2 (904)]

Para realizar la confirmación de la dirección y el no rechazo de la misma, el servidor de pruebas de identidad en (400) y (401) luego presenta al usuario uno o más números de teléfono parciales recopilados de la consulta externa y le pide al usuario que seleccione uno de los números de teléfono parciales como uno en el que puede recibir una llamada telefónica. Los números de teléfono parciales incluyen aquellos con dígitos menos significativos oscurecidos o reemplazados por símbolos para evitar que se les llame y aun así los identifiquen como únicos para el individuo. El número de teléfono puede ser teléfonos de casa, teléfonos de oficina o números de teléfonos móviles según la disponibilidad de datos en el individuo. Uno o más de los números de teléfono parciales en la lista pueden ser números ficticios que se sabe que no pertenecen al individuo. El usuario (1) selecciona el mejor número para comunicarse con su dispositivo telefónico (15) de voz y envía estos datos al servidor de prueba de identidad a través del servidor Web en (402) y (403).

El servidor de prueba de identidad en (404) realiza una llamada al individuo en el número que seleccionó. Al mismo tiempo, el servidor de prueba de identidad también presenta un número de transacción, número de sesión u otro número aleatorio a través del servidor Web en (405) y (406). Durante esta sesión de llamada en (404), se informa a la persona que contesta el teléfono que la llamada es parte de una llamada de prueba de identidad y que debe introducir el número de transacción de prueba de identidad provisto en (406). Este número puede introducirse por DTMF o por reconocimiento de voz del código hablado en el dispositivo (15) de teléfono de voz del usuario en (408). Luego se le pide al usuario que indique una frase que el usuario (1) repite en el teléfono en (408), se registra devolviéndola al

servidor de prueba de identidad en (404) y se almacena en un repositorio (14) de transacciones de prueba de identidad de tal manera que se puede utilizar luego para no rechazar la transacción de prueba de identidad. [El flujo de la interfaz gráfica de usuario detallada para esto y el párrafo anterior se muestran en la figura 2 (905)]

Si el usuario selecciona un número incorrecto, esto debería considerarse como parte del proceso de preguntas y respuestas de prueba de identidad como una respuesta falsa y se debe ponderar en consecuencia al evaluar el riesgo de que un impostor esté realizando la transacción. Si el usuario selecciona un número correcto pero falla al responder, se le puede ofrecer la posibilidad de volver a intentarlo con el mismo número o con un número alternativo.

El sistema de prueba de identidad luego presenta los resultados para puntuar respecto a las reglas de la empresa para determinar si se puede confiar en la identidad afirmada. Opcionalmente, la empresa puede variar el nivel de riesgo asociado con la identidad del usuario en función de su desempeño en el proceso de prueba de identidad. Esta identidad ahora comprobada se transfiere a la siguiente etapa en el proceso empresarial que puede incluir una transacción o registro para un sistema de credenciales y autenticación.

Mientras que los Sistemas y Métodos particulares para la Prueba de Identidad Remota Fuerte como se muestra aquí y se describe en detalle son completamente capaces de alcanzar los objetos de la invención descritos anteriormente, debe entenderse que es la realización actualmente preferida de la presente invención y es representativa, por lo tanto, de la materia que está ampliamente contemplada por la presente invención, que el alcance de la presente invención abarca completamente otras realizaciones que pueden resultar obvias para los expertos en la técnica, y que el alcance de la presente invención está por consiguiente limitado por nada más que las reivindicaciones adjuntas, en las cuales la referencia a un elemento en singular no pretende significar "uno y solo uno" a menos que se indique explícitamente, sino "uno o más". No es necesario que un dispositivo o método aborde todos y cada uno de los problemas que se pretenden resolver con la presente invención, para que se abarque en las presentes reivindicaciones. Además, ningún elemento, componente o etapa de método en la presente descripción está destinado a ser dedicado al público, independientemente de si el elemento, componente o etapa de método se menciona explícitamente en las reivindicaciones.

REIVINDICACIONES

1. Un método de prueba de identidad remota en tiempo real para un usuario que utiliza un sistema de información en una red electrónica, el sistema comprende:

i) un ordenador (10);

ii) un servidor (11) web;

iii) el ordenador (10) conectado a la red a través del servidor web;

iv) un servidor (12) de prueba de identidad conectado a la red;

v) conjuntos (13) de datos de datos (103) asociados con un individuo a prueba de identidad, conectado a la red, los datos incluyen:

a) datos asociados con tarjetas de identificación emitidas por el gobierno;

b) datos asociados con cuentas financieras;

c) datos asociados con los números de teléfono de la persona a prueba de identidad; y

vi) un teléfono (15) asociado con dicho individuo a prueba de identidad;

en donde el método comprende las etapas realizadas por el servidor de prueba de identidad de:

vii) pedir (100) al usuario (1) que use el ordenador (10) conectado al servidor (12) de prueba de identidad a través del servidor (11) web para proporcionar (101, 901) datos biográficos;

viii) en respuesta a la recepción de los datos biográficos del usuario, el servidor de prueba de identidad consulta los repositorios de datos que comprenden números de teléfono asociados con el usuario y le pide que seleccione de una lista de números de teléfono parcialmente ocultos (400,401, 402, 403, 905) presentados en una interfaz gráfica de usuario, al menos uno de los números de teléfono parcialmente ocultos que corresponde a un número de teléfono para comunicarse con un dispositivo telefónico de voz del usuario (15), y además le pide al usuario que envíe datos asociados con un número de teléfono parcialmente oculto al servidor de prueba de identidad a través del servidor web (203), mediante el cual los dígitos menos significativos de los números de teléfono parcialmente ocultos se oscurecen o reemplazan por símbolos para evitar que se les llame y en respuesta a la selección del tipo de números de teléfono parcialmente ocultados, se solicita al usuario que envíe los datos asociados con el número de teléfono parcialmente oculto seleccionado;

ix) realizar una llamada (404) al usuario en el número de teléfono correspondiente al número de teléfono parcialmente oculto seleccionado de los números de teléfono parcialmente ocultos;

x) presentar un número de transacción de prueba de identidad (405), número de sesión o número aleatorio por el servidor de prueba de identidad al usuario a través del servidor (11) web basándose en las selecciones de dicho usuario; y

xi) pedir al usuario que ingrese el número de transacción de prueba de identidad, número de sesión o número aleatorio (406) a través del teléfono, mediante el cual se introduce el número de transacción, número de sesión o número aleatorio por DTMF o por reconocimiento de voz del número de transacción hablado, número de sesión o número aleatorio en su dispositivo (15) de teléfono de voz,

caracterizado por que en respuesta a la recepción de los datos biográficos del usuario, el servidor (12) de prueba de identidad consulta además los repositorios de datos que comprenden uno o más conjuntos de datos con los datos biográficos proporcionados para datos relacionados con datos asociados con tarjetas de identificación del gobierno y datos asociados con números de cuenta; y en respuesta a la consulta de los repositorios de datos, comprende además las etapas realizadas por el servidor de prueba de identidad de:

a) pedir al usuario que seleccione entre varios tipos de tarjetas (201, 202) de identificación emitidas por el gobierno presentadas en la interfaz gráfica de usuario y en respuesta a la selección del tipo de tarjetas de identificación emitidas por el gobierno, se le solicita al usuario que envíe los datos asociados con las tarjetas (203, 204) de identificación emitidas por el gobierno seleccionadas;

b) pedir al usuario que seleccione entre varios tipos de cuentas (205, 206) financieras presentadas en la interfaz gráfica de usuario y en respuesta a la selección del tipo de cuentas financieras, se le solicita al usuario que envíe los datos asociados con la cuenta (207) 208) financiera seleccionada;

c) validar los datos asociados con las tarjetas de identificación emitidas por el gobierno y las cuentas financieras seleccionadas por el usuario con los datos en los repositorios de datos en tiempo real;

d) presentar los resultados de la selección de usuarios para puntuar respecto a las reglas de la empresa para determinar si se confiará en la identidad afirmada

en donde uno o más de los números de teléfono parcialmente ocultos en la lista son números ficticios que se sabe que no pertenecen al usuario de tal manera que la selección de un número de teléfono incorrecto es ponderada por el servidor de prueba de identidad al evaluar el riesgo de que un impostor esté realizando una transacción

2. El método de la reivindicación 1; donde:

i) los conjuntos (3) de datos del sistema para datos (103) incluyen segundos datos para autenticación basada en el conocimiento, dichos datos disponibles para dicha red; y,

ii) el método comprende la etapa adicional de pedirle al usuario (1) que realice una autenticación basada en el conocimiento.

3. El método de las reivindicaciones 1 o 2, en donde dicho número de transacción de prueba de identidad es una frase.

4. El método de cualquiera de las reivindicaciones 1 a 3, en el que el número de transacción de prueba de identidad se identifica por voz.

5. El método de cualquiera de las reivindicaciones 1 a 4, en donde dichos datos asociados con un individuo incluyen fecha de nacimiento, número de seguro social, nombre.

6. El método de cualquiera de las reivindicaciones 1 a 5, en donde dichos datos (103) asociados con tarjetas de identificación emitidas por el gobierno incluyen tarjetas de identificación militar, licencias médicas.

7. Aparato para prueba de identidad remota en tiempo real de un usuario que utiliza un sistema de información en una red electrónica, estando configurado el aparato para realizar las etapas del método en cualquiera de las reivindicaciones anteriores.

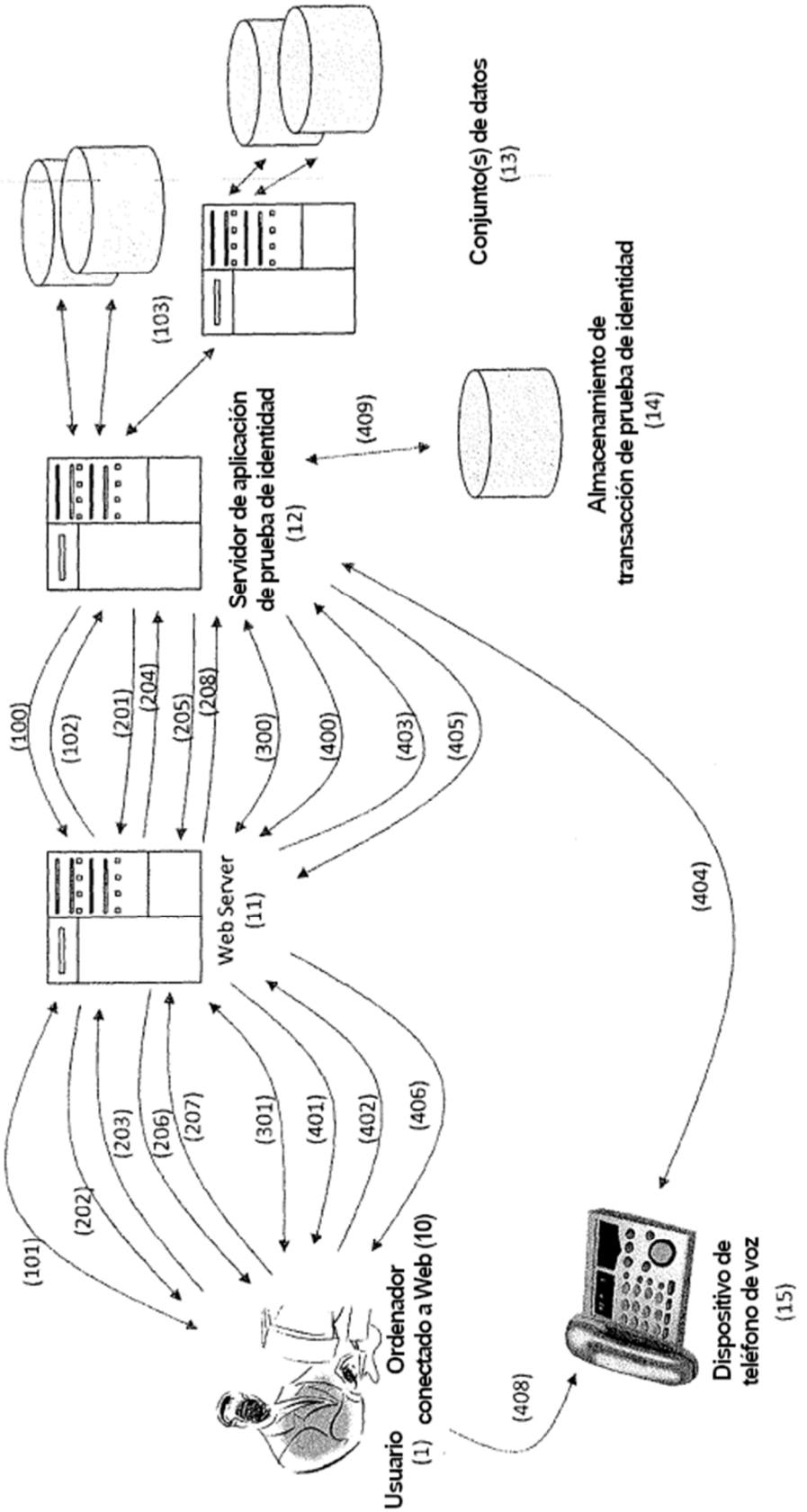

Figura 1 - Flujo de preceso completo de prueba de identidad remota de alta confianza

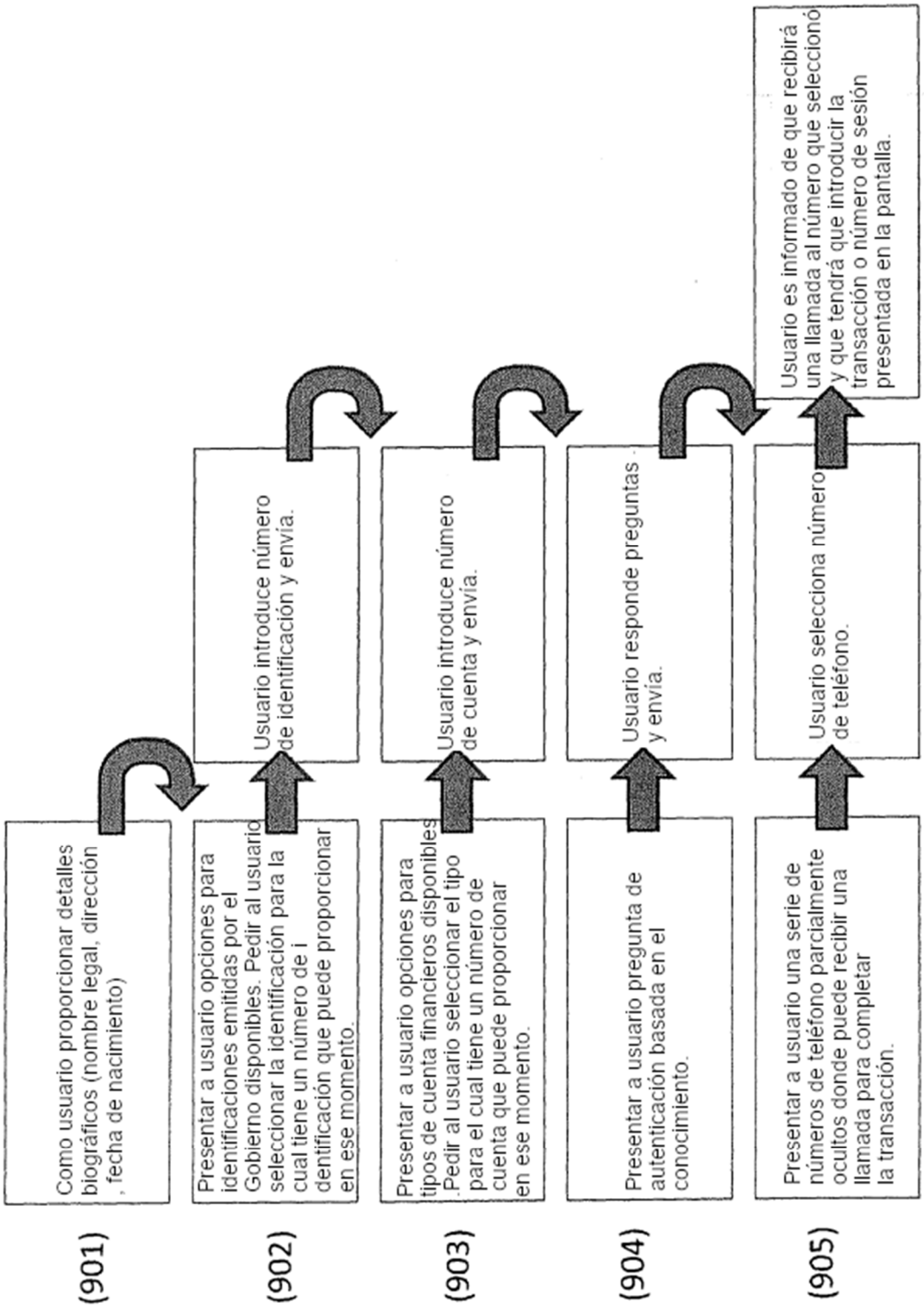

Figura 2 - flujo del proceso de interfaz gráfica de usuario