

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 817 936**

51 Int. Cl.:

H04M 3/42	(2006.01)
H04W 8/26	(2009.01)
H04W 4/16	(2009.01)
H04M 3/22	(2006.01)
H04W 12/08	(2009.01)
H04W 12/12	(2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **12.12.2015 PCT/SE2015/051330**

87 Fecha y número de publicación internacional: **29.09.2016 WO16153407**

96 Fecha de presentación y número de la solicitud europea: **12.12.2015 E 15886620 (2)**

97 Fecha y número de publicación de la concesión europea: **24.06.2020 EP 3275165**

54 Título: **Métodos y sistemas para verificar usuarios mediante números de teléfono**

30 Prioridad:

25.03.2015 US 201562138145 P

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

08.04.2021

73 Titular/es:

**SINCH MOBILE AB (100.0%)
Lindhagensgatan 74
112 18 Stockholm, SE**

72 Inventor/es:

**FORSMAN, DANIEL;
FRANSSON, BJÖRN y
RIKAKIS, MICHAEL**

74 Agente/Representante:

VIDAL GONZÁLEZ, Maria Ester

ES 2 817 936 T3

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

Métodos y sistemas para verificar usuarios mediante números de teléfono

5 Campo técnico

La presente invención se refiere a una técnica para verificar usuarios mediante números de teléfono.

Antecedentes

10

Muchos servicios proporcionados en el Internet requieren que los usuarios ingresen un número de teléfono cuando se registran para y/o usar el servicio. El número de teléfono puede usarse por el servicio, por ejemplo, para identificar al usuario de otros usuarios del servicio, o para garantizar que sólo se crea una cuenta de usuario para cada número de teléfono. Para tal servicio, es importante verificar que el usuario que se conecta al servicio es una persona real, lo que corresponde a verificar que el número de teléfono existe, está en uso y pertenece al usuario que se conecta al servicio.

15

20

Para verificar los números de teléfono, son comunes dos métodos. El primer método es la verificación basada en SMS, en la que un servicio envía un mensaje de texto (SMS) con un código PIN a un número de teléfono proporcionado por el usuario, y solicita que el usuario ingrese el código PIN en el servicio para verificar que de hecho el número de teléfono se conecta al usuario. La verificación basada en SMS tiene la desventaja de ser costosa, ya que enviar mensajes de texto se asocia con un costo. La verificación basada en SMS puede ser además indeseablemente lenta debido al tiempo que toma el SMS en alcanzar al usuario y/o al usuario reaccionar al SMS. El segundo método es la verificación basada en llamadas, en la que el servicio realiza una llamada automatizada mediante el uso de un sistema IVR (Respuesta de voz interactiva) a un número de teléfono proporcionado por el usuario. La llamada automatizada informa al usuario de un código PIN y solicita que el usuario ingrese el código PIN al servicio. En una variante, el servicio muestra el código PIN, realiza la llamada automatizada al número de teléfono y solicita que el usuario ingrese el PIN en el teléfono. En una variante adicional, por ejemplo, conocida por el documento US8964951, el servicio muestra un número de teléfono y solicita que el usuario llame a este número de teléfono desde el número de teléfono a verificarse, después de lo que el servicio verifica al usuario si el servicio encuentra que la llamada resultante se origina desde el número de teléfono a verificarse. Las técnicas de verificación basada en llamadas tienen la desventaja de costar dinero, ya que la interacción de la llamada telefónica con el usuario se asocia con un costo. Las técnicas de verificación basada en llamadas tienen la desventaja adicional de no ser automáticas ya que se requieren acciones del usuario.

25

30

35

Pueden encontrarse ejemplos de la técnica anterior en el documento US2010/135477 relacionado con un método para verificar la identidad de un usuario mediante el uso de un proceso de ID del llamante inverso, y en el documento US2011/246366 relacionado con un método para la autenticación mediante el uso de un dispositivo de telecomunicaciones.

40

Resumen

Es un objetivo de la invención superar al menos parcialmente una o más limitaciones de la técnica anterior.

45

En vista a lo anterior, un objetivo es proporcionar una técnica sencilla y simple de usar para verificar a un usuario mediante un número de teléfono.

Otro objetivo es permitir tal verificación del usuario con un mínimo de intervención del usuario.

50

Otro objetivo es permitir tal verificación del usuario a un bajo costo para tanto el usuario como el servicio.

Un objetivo más es proporcionar una técnica para la verificación del usuario que sea difícil engañar.

55

Uno o más de estos objetivos, y objetivos adicionales que pueden aparecer de la descripción más abajo, se logran al menos parcialmente por medio de métodos implementados por ordenador, un sistema de verificación implementado por ordenador en un dispositivo de comunicación, un sistema de servidor de verificación implementado por ordenador de acuerdo con a las reivindicaciones independientes, y un método para verificar un usuario, modalidades de los mismos que se definen por las reivindicaciones dependientes.

60

Un primer aspecto de la invención es un método implementado por ordenador realizado por un dispositivo de comunicación controlado por software asociado con un número de teléfono de suscripción en una red de telefonía. El método comprende: operar un proceso de monitoreo para detectar una llamada de verificación entrante y determinar un número de teléfono de origen o identificador de la llamada de verificación entrante, dicha llamada de verificación entrante que se inicia en un sistema de servidor para verificar un número de teléfono no confirmado al realizar la llamada de verificación al número de teléfono no confirmado desde un número de teléfono que llama; y transmitir, cuando el proceso de monitoreo detecta la llamada de verificación entrante, una solicitud de verificación al

65

sistema de servidor, la solicitud de verificación que incluye el número de teléfono de origen de la llamada de verificación entrante, o el identificador lo que permite de esta manera que el sistema de servidor verifique que el número de teléfono no confirmado es un número de teléfono de suscripción asignado al dispositivo de comunicación al comparar el número de teléfono de origen con el número de teléfono que llama o validar el identificador.

5 Un segundo aspecto de la invención es un medio legible por ordenador que comprende instrucciones de programa que, cuando se ejecutan por un procesador en un dispositivo de comunicación asociado con un número de teléfono de suscripción en una red de telefonía, realiza el método del primer aspecto.

10 Un tercer aspecto de la invención es un sistema de verificación implementado por ordenador en un dispositivo de comunicación que se asocia con un número de teléfono de suscripción en una red de telefonía. El sistema de verificación comprende: un detector de llamada de verificación configurado para monitorear una interfaz de llamada de voz en el dispositivo de comunicación para la detección de una llamada de verificación entrante y determinar un número de teléfono de origen o un identificador de la llamada de verificación entrante, dicha llamada de verificación entrante que se inicia en un sistema de servidor para verificar un número de teléfono no confirmado al realizar la llamada de verificación al número de teléfono no confirmado desde un número de teléfono que llama; y un gestor de solicitud configurado para generar, cuando se detecta la llamada de verificación entrante, una solicitud de verificación que incluye el número de teléfono de origen o el identificador de la llamada de verificación entrante, y transmitir la solicitud de verificación al sistema de servidor, lo que permite de esta manera que el sistema de servidor verifique que el número de teléfono no confirmado es un número de teléfono de suscripción asignado al dispositivo de comunicación al comparar el número de teléfono de origen con el número de teléfono que llama o validar el identificador.

25 Una modalidad adicional se refiere a un método para verificar un usuario. El método comprende: permitir que el usuario inicie una solicitud para la verificación de un número de teléfono no confirmado en un sistema de servidor, para provocar que el sistema de servidor inicie una llamada de verificación desde una red de telefonía al número de teléfono no confirmado desde un número de teléfono que llama; y proporcionar, al usuario, un programa informático para la instalación en un dispositivo de comunicación, dicho programa informático que es operable para: detectar una llamada de verificación entrante y determinar un número de teléfono de origen de la llamada de verificación entrante; y transmitir, cuando el proceso de monitoreo detecta la llamada de verificación entrante, una solicitud de verificación al sistema de servidor, la solicitud de verificación que incluye el número de teléfono de origen de la llamada de verificación entrante, lo que permite de esta manera que el sistema de servidor verifique que el número de teléfono no confirmado es un número de teléfono de suscripción asignado al dispositivo de comunicación al comparar el número de teléfono de origen con el número de teléfono que llama.

35 Aún otros objetivos, características, aspectos y ventajas de la presente invención aparecerán de la siguiente descripción detallada, de las reivindicaciones adjuntas, así como también de los dibujos. El alcance de la invención se define por las reivindicaciones adjuntas.

40 Breve descripción de los dibujos

Las modalidades de la invención se describirán ahora en la presente descripción sólo a modo de ejemplo, con referencia a los dibujos esquemáticos acompañantes.

45 La Figura 1 es un diagrama de bloques de un entorno de red que implica un número de terminales móviles y sistemas de servidor.

La Figura 2 es un diagrama de secuencia de nodos para un proceso de verificación ejecutado en el entorno de red de la Figura 1.

50 La Figura 3 es un diagrama de flujo de un proceso de verificación del lado del terminal ejecutado por uno de los terminales en la Figura 1.

La Figura 4 es un diagrama de flujo de un proceso de verificación del lado del servidor ejecutado por un servidor de verificación en la Figura 1.

Las Figuras 5A-5D son diagramas de secuencia de nodos para modalidades alternativas del proceso de verificación de la Figura 2.

55 La Figura 6 es un diagrama de bloques de bloques funcionales de un terminal para la implementación del proceso de verificación de la Figura 3.

La Figura 7 es un diagrama de bloques de bloques funcionales de un sistema de servidor para la implementación del proceso de verificación de la Figura 4.

Las Figuras 8A-8B son diagramas de secuencia de nodos para modalidades adicionales del proceso de verificación de la Figura 2.

60 La Figura 9 es un diagrama de flujo de etapas realizadas por un proveedor de verificación en relación con un usuario. La Figura 10 es un diagrama de bloques de una arquitectura ilustrativa para el terminal respectivo en la Figura 1.

Descripción detallada de las modalidades ilustrativas

65 Se describirán modalidades de la invención con referencia al entorno de red ilustrativo mostrado en la Figura 1. Una pluralidad de terminales 10 se configuran para la conexión a una red de telefonía 12A. El terminal 10 puede ser

5 cualquier tipo de dispositivo de comunicación de red que se asocia con un número de teléfono de suscripción en la red de telefonía 12A. Este tipo de terminal incluye dispositivos móviles tales como teléfonos móviles y tabletas de ordenador, así como también ordenadores que comprenden equipos tales como un módem para acceder a la red de telefonía 12A. Los terminales 10 acceden además a una red de datos 12B a través de su conexión a la red de telefonía 12A. Como se muestra en la Figura 1, los terminales 10 pueden conectarse además directamente a la red de datos 12B, en lugar de o en adición a, la red de telefonía 12A.

10 La red de datos 12B puede ser cualquier tipo de red que permite que el terminal 10 se comunice con uno o más servidores o sistemas de servidor 14, 16, ubicados típicamente en una red de área amplia (WAN) tal como el Internet. Sin embargo, es concebible además que uno o más de los servidores 14, 16 se ubique en una red de área privada (PAN) o una red de área local (LAN). Cada servidor 14, 16 es una instancia en ejecución de una aplicación (software) capaz de aceptar solicitudes de un cliente y dar respuestas en consecuencia. Cada servidor 14, 16 puede ejecutarse en cualquier ordenador o combinación de ordenadores y proporcionar uno o más servicios.

15 Los terminales 10 pueden conectarse de manera inalámbrica a la red de telefonía 12A, por ejemplo, por enlace de radio a una estación base o pasarela de una red celular. Del mismo modo, los terminales 10 pueden conectarse de manera inalámbrica a la red de datos 12B, por ejemplo, por enlace de radio a un punto de acceso inalámbrico, tal como un dispositivo de acceso IEEE 802.11. Alternativamente, los terminales 10 pueden conectarse por cable a la red respectiva 12A, 12B.

20 Los terminales 10 para su uso en redes de telefonía celular almacenan de manera segura una identidad de abonado móvil internacional (IMSI) que se usa para identificar el usuario y se asocia directamente o indirectamente con un número de teléfono de suscripción en la red de telefonía 12A. IMSI se almacena como un campo de 64 bits y puede enviarse por el terminal 10 a la red 12A. Para redes GSM, UMTS y LTE, IMSI se proporciona en un Módulo de identidad de abonado (SIM) que se instala en el terminal. Para las redes CDMA2000, IMSI se proporciona directamente en el terminal o en un Módulo de identidad de usuario extraíble (R-UIM), que es análogo a una SIM. El módulo que almacena la IMSI puede denominarse además Tarjeta de circuito integrado universal (UICC) o Módulo de identidad de abonado CDMA (CSIM). Por razones de seguridad, la IMSI se envía con la menor frecuencia posible y en su lugar se envía una Identidad de abonado móvil temporal (TMSI) generada aleatoriamente. TMSI se asigna aleatoriamente por la red a cada dispositivo móvil en el momento en que se enciende. Independientemente de la red de telefonía 12A, cada terminal 10 se asocia de forma única con un número de teléfono de suscripción en la red de telefonía 12A. La red de telefonía 12A se refiere comúnmente como la red de telefonía pública conmutada (PSTN), que representa el conjunto de las redes de telefonía del mundo que son operadas por operadores telefónicos nacionales, regionales, o locales, que proporcionan infraestructura y servicios para las telecomunicaciones públicas, incluidos tanto redes de telefonía fija como redes de telefonía celular.

35 Los terminales 10 pueden ser capaces de conectarse a una o ambas redes 12A, 12B para establecer comunicaciones de voz y datos. Las comunicaciones de datos pueden relacionarse con servicios de comunicación tales como mensajería de texto (por ejemplo, SMS), mensajería de correo electrónico, mensajería en tiempo real, mensajería de voz, VoIP (voz sobre IP) etc, así como también la recuperación de documentos y/o transmisiones electrónicas, tales como páginas web, fotografías, videos etc.

40 En la Figura 1, la red de telefonía 12A incluye al menos un servidor de PSTN 18 que es operable para realizar una llamada de voz a un número de teléfono de suscripción especificado a través de la red de telefonía pública conmutada 12A. Puede ordenarse al servidor de PSTN 18 que realice una llamada de voz al número de suscripción especificado desde un número del llamante especificado ("número de teléfono que llama") a través de una API estandarizada. La operación del servidor de PSTN 18 se conoce bien por el experto y no se describirá con más detalle.

50 Los terminales 10 son capaces de ejecutar programas de software, que pueden preinstalarse en el terminal 10 o instalarse por el usuario del terminal, por ejemplo, descargados desde un servidor en la red. En la siguiente, estos programas de software se denotan "programas de aplicación". Al menos uno de estos programas de aplicación implementa un proceso de verificación y se denota "solicitud de verificación" en la siguiente.

55 La aplicación de verificación puede ser un programa de verificación genérico, que se ejecuta en el terminal 10 para verificar genéricamente a un usuario del terminal 10 a una pluralidad de servicios en la red 12B, y en particular para verificar que un número de teléfono particular de hecho se asocia con el usuario del terminal 10. Tal aplicación de verificación genérica puede ser una aplicación confiable en el terminal 10 que verifica el número de teléfono con otros programas de aplicación en el terminal 10. Por ejemplo, la aplicación de verificación genérica puede ejecutarse por comando por otros programas de aplicación en el terminal 10 para verificar el número de teléfono. Alternativamente, la aplicación de verificación puede diseñarse para permitir el acceso desde el terminal 10 a un servicio específico o grupo de servicios proporcionado por un servidor en la red 12B, por ejemplo, como parte de un procedimiento de registro o inicio de sesión entre el terminal 10 y el servidor.

65 El proceso de verificación en el terminal 10 se ejecuta en comunicación con un servidor de verificación, designado por 14 en la Figura 1. Como se entiende de lo anterior, el servidor de verificación 14 puede configurarse

exclusivamente para proporcionar un servicio de verificación que verifica el número de teléfono. Alternativamente, el servidor de verificación 14 puede ejecutar el servicio de verificación como parte de o junto con otro servicio.

5 Típicamente, el terminal 10 se comunica directamente con el servidor de verificación 14 mediante el uso de un protocolo común. Específicamente, la comunicación entre el terminal 10 y el servidor de verificación 14 puede implicar transmitir llamadas remotas o "solicitudes" que se interpretan en el receptor. Las solicitudes pueden transmitir un valor de un cierto parámetro o iniciar una acción en el receptor.

10 La Figura 2 muestra una modalidad de un proceso de verificación ejecutado en el entorno de red de la Figura 1 para verificar que un número de teléfono no confirmado, que se ingresa a través del terminal 10, corresponde a un número de teléfono de suscripción real y que este número de teléfono de suscripción se asocia con el terminal 10. Como se explicó en lo anterior, el proceso de verificación se realiza por una aplicación de verificación ejecutada en el terminal 10 y un servicio de verificación ejecutado en el servidor de verificación 14. Básicamente, el proceso de verificación implica establecer una única llamada desde un servidor de PSTN 18 al número de teléfono no confirmado, y verificar si la llamada se recibe por el terminal 10. Si se recibe la llamada, el servidor de verificación 14 concluye que el número de teléfono no confirmado es un número de teléfono de suscripción asociado con el terminal 10. El proceso de verificación es particularmente, pero no exclusivamente, útil para verificar números de teléfonos móviles.

20 En el ejemplo de la Figura 2, el terminal 10 envía una solicitud de verificación primera o inicial VR1 al servidor de verificación 14 (etapa 20). La solicitud VR1 incluye un número de teléfono no confirmado, designado por MI#. Al recibir VR1, el servidor de verificación 14 envía una solicitud de llamada CR al servidor de PSTN 18 (etapa 21). La solicitud de llamada CR incluye MI# y un número de teléfono que llama seleccionado, designado por #DE LLAMANTE. El #DE LLAMANTE se selecciona por el servidor 14. La solicitud de llamada CR provoca que el servidor de PSTN 18 realice una llamada de verificación a MI# desde el #DE LLAMANTE (etapa 22). El terminal 10 cancela la llamada de verificación después de haber determinado el número de teléfono de origen de la llamada entrante, designado por #DE ORIGEN (etapa 23). El terminal 10 envía entonces una segunda solicitud de verificación VR2 al servidor 14. La solicitud VR2 incluye MI# y #DE ORIGEN (etapa 24). El servidor 14 compara #DE ORIGEN con #DE LLAMANTE. Si coinciden, la verificación se considera exitosa, de lo contrario se considera que la verificación falla. El servidor 14 puede enviar además un mensaje de confirmación CONF al terminal 10 que indica si la verificación fue exitosa o no (etapa 25).

35 El proceso de verificación puede proporcionar acceso a un servicio de diferentes modos. En una variante, el servidor 14 da a la aplicación de verificación en el terminal 10 acceso a otro servicio en el servidor 14 o en otro servidor conectado a la red 12B, cuando el servidor encuentra que #DE ORIGEN coincide con #DE LLAMANTE. En otra variante, la aplicación de verificación en el terminal 10 da a otro programa de aplicación en el terminal 10 acceso a un servicio en el servidor 14 o en otro servidor conectado a la red 12B, cuando la aplicación de verificación recibe el mensaje de confirmación CONF.

40 El proceso de verificación en la Figura 2 puede realizarse automáticamente, sin requerir ninguna intervención del usuario a través del terminal 10. Puede ocultarse además para el usuario, es decir las etapas 20-25 pueden ejecutarse sin que se informe al usuario sobre las etapas respectivas o la llamada de verificación. Además, el proceso de verificación puede realizarse sin incurrir en ningún costo para el usuario o el proveedor del servicio de verificación, por ejemplo, al terminar la llamada de verificación sin responder. Todavía más, es difícil para el usuario engañar al proceso de verificación, ya que la verificación real se hace a distancia desde el terminal 10, en el lado del servidor. El usuario no puede manipular la llamada de verificación, que se genera bajo el control del servidor 14 y se realiza desde el servidor de PSTN 18. Pueden tomarse medidas convencionales para evitar que el usuario acceda a la aplicación de verificación en el terminal 10, que ejecuta el proceso de verificación en el lado del terminal.

50 El proceso de verificación puede usarse siempre que hay una necesidad de verificar un número de teléfono, y para verificar de esta manera indirectamente un usuario a un servicio. Algunos ejemplos se dan más abajo.

55 Muchos proveedores de programas de aplicación y servicios asociados tienen un incentivo para adquirir una gran base de usuarios. Para atraer nuevos usuarios, el proveedor puede ofrecer artículos gratuitos a cambio de un registro de usuario. Por ejemplo, un proveedor de un servicio de VoIP puede darle al usuario llamadas gratuitas, créditos de tiempo de llamada gratuitas, mensajes de texto gratuitos, un mes de uso gratuito, etc. Esto puede proporcionar un incentivo para que un usuario se registre múltiples veces con el mismo servicio, para obtener acceso a más artículos gratuitos. Para evitar esto, el proveedor puede implementar el proceso de verificación inventivo como parte del procedimiento de registro y requerir que el usuario ingrese un número de teléfono de suscripción. El usuario sólo garantiza acceso al servicio, y a los artículos gratuitos, si el número de teléfono de suscripción ingresado se verifica por el proceso de verificación.

65 Un servicio que permite que un usuario haga una llamada telefónica saliente o envíe un mensaje de texto a través de un programa de aplicación o una página web en el terminal 10 puede necesitar presentar al llamante/remitente al destinatario de la llamada/mensaje de texto. En la ausencia de verificación, un usuario puede ingresar un número de teléfono incorrecto como llamante/remitente. El proveedor de servicios puede implementar el proceso de verificación

inventivo como parte de un procedimiento de registro, un procedimiento de inicio de sesión, o siempre que un usuario desee hacer una llamada saliente o enviar un mensaje de texto a través del servicio, para garantizar que el número de teléfono ingresado por el usuario se asocia de manera válida con el usuario.

5 Muchos servicios usan un número de teléfono de un usuario para encontrar otros usuarios. Uno de tales ejemplo es Viber, que es un programa de aplicación de mensajería instantánea y VoIP. Tras la instalación en el terminal, el programa de aplicación de VoIP crea una cuenta de usuario con un número de teléfono como nombre de usuario. El servicio se sincroniza con la libreta de direcciones en el terminal. Ya que todos los usuarios se registran por su número de teléfono, el servicio vuelve a la información del terminal sobre todos los usuarios de Viber entre los
10 contactos de la libreta de direcciones. En tal servicio, puede ser vital que se verifiquen los números de teléfono proporcionados al servicio. El proceso de verificación inventivo puede implementarse como parte del proceso de instalación para garantizar que el número de teléfono ingresado se asocie de manera válida con el usuario.

15 Como otro ejemplo, un servicio de citas puede requerir que sus usuarios ingresen un número de teléfono cuando se registran para el servicio. Para evitar que un usuario registre un número de teléfono falso para el anonimato total, el servicio de citas puede implementar el proceso de verificación inventivo como parte del procedimiento de registro, o en una etapa posterior, para verificar que el número de teléfono ingresado por el usuario es un número de teléfono de suscripción asociado de manera válida con el usuario.

20 La Figura 3 es un diagrama de flujo que ilustra una modalidad del lado del terminal del proceso de verificación en la Figura 2. En la etapa 30, el proceso de verificación se inicia, por ejemplo, por un usuario del terminal 10, por otro programa de aplicación en el terminal, o por un servicio en un servidor al que el terminal 10 se ha conectado. Por lo tanto, el proceso de verificación puede iniciarse a solicitud por el usuario o automáticamente. En la etapa 31, se obtiene un número de teléfono no confirmado (MI#). El número de teléfono no confirmado puede ingresarse
25 manualmente por el usuario, recuperarse desde una agenda telefónica en el terminal 10, proporcionarse para la verificación por otro programa de aplicación en el terminal 10 o por un servicio a través de una página web en el terminal 10. En la etapa 32 (correspondiente a la etapa 20 en la Figura 2), la primera solicitud de verificación (VR1) con el número de teléfono no confirmado se transmite al servidor de verificación 14. Al mismo tiempo, el proceso puede garantizar que el bloqueo CID (identificación de llamadas) se desactive en el terminal 10. Entonces, en las etapas 33-34, el proceso espera por la llamada de verificación. La etapa 33 puede iniciar un proceso de monitoreo en el terminal, si aún no se ha iniciado, para monitorear o interceptar todas las llamadas entrantes. Este proceso de monitoreo puede implementarse por un software de interceptación dedicado incluido en o usado por la aplicación de verificación en el terminal 10. La llamada de verificación puede identificarse por el proceso de monitoreo de diferentes modos. En una alternativa, la primera llamada entrante después de la etapa 32 se identifica como la llamada de verificación. En otra alternativa, si se conoce que la llamada de verificación pertenece a un cierto grupo de números de teléfono, la etapa 33 identificará la llamada de verificación como la primera llamada entrante que se origina desde un número de teléfono que coincide con este grupo de números de teléfono. El grupo de números de teléfono puede, por ejemplo, almacenarse en cualquier formato en la memoria del terminal 10. Si no se recibe ninguna llamada de verificación dentro de un límite de tiempo dado (etapa 34), se transmite un mensaje de error al servidor 14 para indicar que la verificación falló (etapa 35). Si se recibe la llamada de verificación (correspondiente a la etapa 22 en la Figura 2), se determina el número de teléfono de origen (#DE ORIGEN) de la llamada de verificación (etapa 36), si no se ha determinado ya durante las etapas 33-34. El número de teléfono de origen puede obtenerse como el CID para la llamada entrante. El CID representa el número del llamante y se transmite durante la señal de llamada, o cuando se configura la llamada, pero antes que se responda la llamada. Por lo tanto, el número de teléfono de origen para una llamada puede recuperarse sin responder la llamada. Después de recuperar el número de teléfono de origen, la llamada de verificación se cancela, por ejemplo, al terminar la llamada o al presentar una señal de ocupado al llamante. En la etapa 37 (correspondiente a la etapa 24 en la Figura 2), la segunda solicitud de verificación (VR2) se transmite al servidor 14 con el número de teléfono no confirmado y el número de teléfono de origen. Si el terminal 10 recibe una confirmación desde el servidor 14 que indica que la verificación ha tenido éxito (etapa 38), el terminal 10 puede, por ejemplo, proceder a acceder al servicio particular (etapa 39).

La Figura 4 es un diagrama de flujo que ilustra una modalidad del lado del servidor del proceso de verificación en la Figura 2. En la etapa 40 (correspondiente a la etapa 20 en la Figura 2), se recibe la primera solicitud de verificación (VR1), lo que provoca que el servidor 14 asigne un número que llama (#DE LLAMANTE) para la llamada de verificación (etapa 41). El número que llama se selecciona típicamente de un grupo de números de teléfono que se han adquirido para su uso por el servicio de verificación. La información sobre los números que llaman disponibles puede almacenarse en una memoria del servidor 14. En la etapa 42, se almacena en la memoria una asociación entre el número que llama y el terminal (por ejemplo, el número de teléfono no confirmado). En la etapa 43 (correspondiente a la etapa 21 en la Figura 2), la llamada de verificación se inicia al transmitir la solicitud de llamada (CR) al servidor de PSTN 18. Entonces, en las etapas 44-45 (correspondientes a la etapa 24 en la Figura 2), el proceso espera la segunda solicitud de verificación (VR2). Si la segunda solicitud de verificación no se recibe dentro de un límite de tiempo dado (etapa 45), se considera que la verificación falla y se transmite una confirmación correspondiente (CONF) al terminal (etapa 46). Si se recibe la segunda solicitud de verificación, el terminal se identifica (etapa 47), por ejemplo, por el número de teléfono no confirmado (MI#) incluido en la segunda solicitud de verificación, y el número que llama correspondiente al terminal se recupera desde la memoria del servidor (etapa 48).

En la etapa 49, el número de teléfono de origen (#DE ORIGEN) incluido en la segunda solicitud de verificación se compara con el número que llama recuperado en la etapa 48. Si coinciden, la verificación se considera exitosa, de lo contrario se considera que la verificación falla (etapa 50). Se transmite una confirmación (CONF) correspondiente al terminal (etapa 46).

5 El proceso de verificación en la Figura 2 puede modificarse de muchos modos diferentes sin apartarse del concepto subyacente de la presente invención. Se discutirán brevemente unas cuantas modalidades alternativas con referencia a las Figuras 5A-5D, con el enfoque en las diferencias en comparación con la Figura 2.

10 En la Figura 5A, la etapa 20 se modifica para incluir un identificador ID de terminal único en la primera solicitud de verificación VR1. El identificador de terminal puede predefinirse y almacenarse en una memoria del terminal 10, o puede asignarse dinámicamente por o para el terminal 10 antes de generar la primera solicitud de verificación VR1. El identificador de terminal se usa por el servidor de verificación 14 en la etapa 21 para asociar el número que llama #DE LLAMANTE con el terminal 10. En consecuencia, la etapa 24 se modifica además al incluir el identificador ID de terminal en la segunda solicitud de verificación VR2 en lugar del número de teléfono no confirmado MI#.

15 En la Figura 5B, el lado del terminal es idéntico a la Figura 2 mientras que el lado del servidor difiere en que el servidor de verificación 14 ha delegado la generación de la solicitud de llamada CR a otro servidor 16. No obstante, la llamada de verificación se inicia por el servidor de verificación 14 en la etapa 20'. En la etapa 20', el servidor de verificación 14 transmite una solicitud específica (que incluye el número de teléfono no confirmado MI#) al servidor 16 que provoca que el servidor 16 asigne independientemente un número que llama #DE LLAMANTE y genere y transmita la solicitud de llamada CR. En la etapa 20'', el servidor 16 informa al servidor de verificación 14 sobre el número que llama #DE LLAMANTE asignado al número de teléfono no confirmado MI#.

20 En la Figura 5C, el lado del terminal es idéntico además a la Figura 2 mientras el lado del servidor difiere en que el servidor de verificación 14 ha delegado tanto la generación de la solicitud de llamada CR como la comparación del #DE LLAMANTE con el #DE ORIGEN a otro servidor 16. En la etapa 20', el servidor de verificación 14 transmite una solicitud específica (que incluye el número de teléfono no confirmado MI#) al servidor 16 que provoca que el servidor 16 asigne independientemente un número que llama #DE LLAMANTE y genere y transmita la solicitud de llamada CR. En contraste con la Figura 5B, el servidor 16 no devuelve el #DE LLAMANTE al servidor de verificación 14, pero almacena una asociación MI#: #DE LLAMANTE. En la etapa 24', cuando el servidor de verificación 14 ha recibido la segunda solicitud de verificación VR2 desde el terminal 10, el servidor de verificación 14 envía una solicitud específica (que incluye MI# y #DE ORIGEN) al servidor 16 que provoca que el servidor 16 recupere el #DE LLAMANTE asociado con MI# y compare el #DE ORIGEN con el #DE LLAMANTE recuperado. En la etapa 24'', el servidor 16 devuelve una confirmación CONF al servidor de verificación que indica si hay una coincidencia o no. Se entiende que el servidor de verificación 14, mediante la etapa 24', controla el proceso en el servidor 16 y por lo tanto realiza indirectamente la etapa para comparar #DE ORIGEN con #DE LLAMANTE.

25 La Figura 5D ilustra una generalización del proceso de verificación en la Figura 2, que no requiere que el servidor de verificación 14 base la verificación en una comparación de #DE LLAMANTE y #DE ORIGEN. En su lugar, en la etapa 21, el servidor de verificación 14 inicia/genera la solicitud de llamada CR para incluir el número de teléfono no confirmado MI# y un identificador ID1. El identificador se genera por o para el servidor de verificación 14 y se asocia con el terminal 10 (por ejemplo, por MI#). Si se requiere el servidor de PSTN 18, la solicitud de llamada CR puede incluir además un número que llama #DE LLAMANTE. Sin embargo, en contraste con el proceso en la Figura 2, el #DE LLAMANTE no necesita ser único. La solicitud de llamada CR provoca que el servidor de PSTN 18 incluya la ID1 en la llamada de verificación a MI#. En las redes de PSTN actuales, no es posible incluir un identificador arbitrario en una llamada de voz de manera que el identificador pueda interceptarse sin responder la llamada de voz. En una modalidad, la solicitud de llamada CR se configura por lo tanto para provocar que el servidor de PSTN 18 codifique el primer identificador ID1 como señales (sonidos) transmitidas por la llamada de voz, por ejemplo, mediante el uso de DTMF (señalización de multifrecuencia de tono dual). Cuando la llamada de verificación se intercepta por el proceso del lado del terminal, en la etapa 22, se responde la llamada de verificación y las señales codificadas se decodifican en un valor de identificador recibido, designado por ID2 en la Figura 5D. La llamada de verificación se cancela entonces en la etapa 23, después de lo que el valor de identificador ID2 se envía al servidor de verificación 14 junto con MI# en la segunda solicitud de verificación VR2 (etapa 24). El servidor de verificación 14 verifica entonces el usuario al validar el valor de identificador ID2 recibido, por ejemplo, al recuperar el primer identificador ID1 (en base a MI#) y comparar ID2 con ID1. Como todos los otros procesos de verificación descritos en la presente descripción, el proceso del lado del terminal en la Figura 5D puede realizarse automáticamente y ocultarse al usuario del terminal 10.

30 Debería entenderse que los diagramas de flujo en las Figuras 3-4 son relevantes además para las modalidades en las Figuras 5A-5D y las Figuras 8A-8B (ver más abajo) con modificaciones que deberían ser evidentes para el experto en base a las enseñanzas presentadas en la presente descripción y no se discutirán con más detalle.

35 La Figura 6 es un diagrama de bloques del terminal 10 que ilustra bloques funcionales que se usan o instancian durante la ejecución del proceso de verificación como se presenta en las Figuras 2-4. Debe entenderse que el bloque respectivo puede implementarse por hardware y/o software. Por ejemplo, los bloques 60A, 60B y 64 pueden

implementarse por software, por ejemplo, un programa de aplicación, y los bloques 62 y 66 pueden existir en el terminal 10 independientemente del programa de aplicación y pueden implementarse por hardware y/o software.

En la Figura 6, el terminal 10 incluye un primer gestor de solicitud 60A que implementa las etapas 30-32 en la Figura 3. El gestor 60A es operable para conectarse a una interfaz de comunicación de datos 62 para la transmisión de la primera solicitud de verificación VR1 al servidor (no mostrado). Un detector de llamada de verificación o módulo de interceptación 64 implementa las etapas 33-36 en la Figura 3. El detector 64 es operable para conectarse a una interfaz de llamada de voz 66 para la interceptación y detección de la llamada de verificación. Como se indica por una flecha discontinua, el gestor 60A es operable para iniciar directamente o indirectamente el detector 64 para iniciar el monitoreo de las llamadas entrantes en la interfaz 66. El terminal 10 incluye además un segundo gestor de solicitud 60B que implementa las etapas 37-38 en la Figura 3. El gestor 60B es por lo tanto operable para obtener el número de teléfono de origen #DE ORIGEN determinado por el detector 64. El gestor 60B puede operarse además para conectarse a la interfaz 62 para la transmisión de la segunda solicitud de verificación VR2 al servidor (no mostrado).

La Figura 7 es un diagrama de bloques del servidor de verificación 14 que ilustra bloques funcionales que se usan o instancian durante la ejecución del proceso de verificación como se presenta en las Figuras 2-4. Como en la Figura 6, el bloque respectivo puede implementarse por hardware y/o software. Por ejemplo, los bloques 70A, 70B y 74 pueden implementarse por software, por ejemplo, un programa de servidor, y los bloques 72 y 76 pueden existir en el servidor 14 independientemente del programa de servidor y pueden implementarse por hardware y/o software.

En la Figura 7, el servidor 14 incluye un primer gestor de solicitud 70A que implementa la etapa 40 en la Figura 4. El gestor 70A es operable para conectarse a una interfaz de comunicación de datos 72 para recibir la primera solicitud de verificación VR1 desde el terminal (no mostrado). Un módulo de iniciación de llamadas 74 implementa las etapas 41-43 en la Figura 4. El módulo 74 es operable para recibir el número de teléfono no confirmado MI# determinado por el gestor 70A. El módulo 74 es operable además para conectarse a la interfaz 72 para el inicio de la llamada de verificación, por ejemplo, al transmitir la solicitud de llamada CR al servidor de PSTN 18. El módulo 74 es operable además para conectarse a una memoria 76 para el almacenamiento del número que llama #DE LLAMANTE, por ejemplo, en asociación con MI#. El servidor 14 incluye además un segundo gestor de solicitud 70B que implementa las etapas 44-51 en la Figura 4. Por lo tanto el gestor 70B es operable para conectarse a la interfaz 72 para recibir la segunda solicitud de verificación VR2 desde el terminal (no mostrado). El gestor 70B es operable además para conectarse a la memoria 76 para recuperar el número de teléfono de origen #DE ORIGEN, por ejemplo, en base a MI# incluido en VR2, y para comparar el #DE LLAMANTE en VR2 con el #DE ORIGEN para la verificación.

Debería entenderse que los diagramas de bloques en las Figuras 6-7 son relevantes además para las modalidades en las Figuras 5A-5D y las Figuras 8A-8B (ver más abajo) con modificaciones que deberían ser evidentes para el experto en base a las enseñanzas presentadas en la presente descripción y no se discutirán con más detalle.

Al volver a la modalidad en las Figuras 2-3, debería notarse que el proceso de verificación no necesita iniciarse (etapa 30) a través del terminal 10 que se asocia con el número de teléfono no confirmado. Del mismo modo, la primera solicitud de verificación VR1 no necesita generarse y transmitirse desde este terminal 10 (etapas 31-32). De hecho, las etapas 30-32 pueden ejecutarse por cualquier dispositivo de comunicación que sea capaz de conectarse a la red de telefonía o datos 12A, 12B (Figura 1), como se ejemplifica además más abajo con referencia a las Figuras 8A-8B.

En la modalidad de la Figura 8A, la solicitud VR1 se genera por y transmite al servidor 14 desde un dispositivo de comunicación 10' además del terminal 10 (etapa 20). El dispositivo 10' puede ser un ordenador, un servidor, un terminal móvil, etc. Por ejemplo, la solicitud VR1 puede generarse y transmitirse cuando un usuario accede a un servicio de red, por ejemplo, a través de un navegador web en un ordenador/terminal. La solicitud VR1 puede generarse por y transmitirse al servidor 14 desde el ordenador/terminal que se opera por el usuario para acceder al servicio de red, o desde el propio servicio de red. Por lo tanto, la solicitud VR1 puede de hecho proporcionarse como un comando interno en el servidor 14, por ejemplo, si el servicio de red al que accede el usuario es el propio servicio de verificación. Debería notarse que la solicitud VR1, en todas las modalidades y variantes descritas en la presente descripción, puede ser ya sea explícita o implícita. Tal solicitud VR1 explícita puede contener el número de teléfono no confirmado MI# para verificarse, mientras que una solicitud VR1 implícita no puede ni formarse como una solicitud o comando, ni incluir MI#. Por ejemplo, la solicitud VR1 implícita puede ser una simple señal de activación que el servidor 14 es capaz de asociar con un número de teléfono específico para verificarse. El lado del servidor en la Figura 8A es idéntico a la Figura 2 y no se describirá, además. En el ejemplo de la Figura 8A, el servidor 14 envía el mensaje de confirmación CONF al dispositivo 10', aunque CONF puede enviarse al terminal 10 o a cualquier otro dispositivo, por ejemplo, el servicio de red al que se accede por el usuario. Aunque no se muestra en la Figura 8A, el servidor 14 puede configurarse, como parte de la etapa 21, para transmitir un mensaje al dispositivo 10' o al terminal 10 que solicita que el usuario inicie el proceso de verificación en el terminal 10, por ejemplo, al activar la aplicación de verificación en el terminal 10.

En comparación con la Figura 8A, la modalidad en la Figura 8B implica aún otro dispositivo de comunicación 10'', que puede ser un ordenador, un servidor, un terminal móvil, etc. El dispositivo 10'' se usa en la etapa 20A para proporcionar el número de teléfono no confirmado MI# al servidor 14, junto con los datos de identificación del usuario

(UID). El UID identifica al usuario y se asocia con MI# en el servidor 14. La etapa 20A puede realizarse por ejemplo, cuando el usuario se registra para un servicio, y el UID puede incluir uno o más de un nombre, una dirección postal, una dirección de correo electrónico, una fecha de nacimiento, etc. En la etapa 20, se genera y transmite la solicitud VR1 desde el dispositivo de comunicación 10', por ejemplo, como se describe en relación con la Figura 8A. Sin embargo, en el ejemplo ilustrado, la solicitud VR1 no incluye MI# sino UID. Tras la recepción de VR1, el servidor 14 identifica MI# en base a UID e incluye MI# en la solicitud de llamada CR al servidor de PSTN 18. Las etapas posteriores 22-25 son idénticas a la Figura 2 y no se repetirán.

La Figura 9 es un diagrama de flujo de etapas realizado por un proveedor de verificación en relación con un usuario. En la etapa 90, el proveedor de verificación suministra una aplicación de verificación para la instalación en el terminal 10, la aplicación de verificación que se configura para implementar el proceso de verificación en el lado del terminal. La aplicación de verificación puede suministrarse como parte del sistema operativo en el terminal 10, o como un programa de software para la instalación selectiva en el terminal 10, por ejemplo, mediante descarga. En la etapa 91, el proveedor permite que el usuario inicie una solicitud para la verificación en el servicio de verificación. Esto puede hacerse por ejemplo, a través de la aplicación de verificación en el terminal 10 o al proporcionar una página web para acceder por el usuario a través del terminal 10 u otro dispositivo de comunicación 10'. El usuario puede ordenar explícitamente la verificación, o la verificación puede proceder automáticamente en base a alguna actividad del usuario. Al suministrar la aplicación de verificación para la instalación en el terminal 10, puede verse que el proveedor permite que los terminales 10 realicen el proceso de verificación, que implica esperar por y detectar la llamada de verificación desde el servicio de verificación (etapa 92) y enviar la segunda solicitud de verificación VR2 al servicio de verificación (etapa 93). En la etapa 94, la verificación del usuario se completa por el servicio de verificación en el servidor 14.

La Figura 10 es un diagrama de bloques de una arquitectura ilustrativa 100 de los terminales 10 en la Figura 1. El terminal 10 puede incluir una interfaz de memoria 102, uno o más procesadores 104 tales como procesadores de datos, procesadores de imágenes y/o unidades de procesamiento central, y una interfaz de periféricos 106. La interfaz de memoria 102, uno o más procesadores 104 y/o la interfaz de periféricos 106 pueden ser componentes separados o integrados en uno o más circuitos integrados. Los diversos componentes en el terminal 10 pueden acoplarse por uno o más buses de comunicación o líneas de señal. Los sensores, dispositivos, y subsistemas pueden acoplarse a la interfaz de periféricos 106 para facilitar múltiples funcionalidades.

Las funciones de comunicación pueden facilitarse a través de uno o más subsistemas de comunicación inalámbrica 110, que pueden incluir receptores y transmisores de radiofrecuencia y/o receptores y transmisores ópticos (por ejemplo, infrarrojos). El diseño e implementación específicos del subsistema de comunicación 110 pueden depender de la(s) red(es) de comunicación sobre las que se pretende que opere el terminal 10. Por ejemplo, el terminal 10 puede incluir subsistemas de comunicación 110 diseñados para operar sobre redes de acuerdo con cualquier protocolo de red celular, tal como GSM, GPRS, EDGE, UMTS, CDM y LTE, así como también otras redes tales como WiFi, WiMax y Bluetooth™.

Un subsistema de audio 112 puede acoplarse al(a los) componente(s) de hardware de audio 114, tales como un altavoz y un micrófono, para facilitar las funciones habilitadas por voz, tales como reconocimiento de voz, replicación de voz, grabación digital, y funciones de telefonía, así como también para permitir la presentación de archivos de audio grabados.

Un subsistema de E/S 116 puede incluir uno o más controladores de entrada/salida acoplados al(a los) componente(s) de hardware de entrada/salida 118, que incluyen, pero no limitados a uno o más de una pantalla táctil, un visor, un teclado, un panel táctil, uno o más botones, interruptores, una ruedecilla, un puerto de infrarrojos, un puerto USB, y un dispositivo de puntero tal como un lápiz óptico.

En el ejemplo específico de la Figura 8, un subsistema de cámara 120 con una cámara 122 se conecta a la interfaz de periféricos 106 para facilitar las funciones de la cámara, tales como grabar fotografías y videoclips. Además, uno o más sensores auxiliares 124 tales como un sensor de movimiento, sensor de orientación, sensor de proximidad, sistema de posicionamiento (por ejemplo, receptor GPS), sensor de temperatura, sensor biométrico, magnetómetro, etc., se acoplan a la interfaz de periféricos 106 para facilitar las funcionalidades relacionadas.

La interfaz de memoria 102 puede acoplarse a una memoria 108. La memoria 108 puede incluir una memoria de acceso aleatorio de alta velocidad y/o una memoria no volátil, tal como uno o más dispositivos de almacenamiento de disco magnético, uno o más dispositivos de almacenamiento óptico, y/o memoria flash (por ejemplo, NAND, NOR). La memoria 108 puede almacenar un sistema operativo, tal como Android, OS X, Windows Mobile, Darwin, RTXC, LINUX, UNIX, o un sistema operativo integrado tal como VxWorks. El sistema operativo puede incluir instrucciones para manejar los servicios del sistema básicos y para realizar tareas dependientes del hardware. En algunas implementaciones, el sistema operativo puede incluir instrucciones para realizar una verificación en relación con un sistema de servidor que proporciona un servicio en la red de datos. Por ejemplo, el sistema operativo puede implementar el proceso de verificación del lado del terminal como se describe con referencia a las Figuras 1-9.

La memoria 108 puede almacenar además instrucciones de comunicación para facilitar la comunicación con uno o más dispositivos adicionales, uno o más ordenadores y/o uno o más servidores. La memoria 108 puede incluir instrucciones de interfaz gráfica de usuario para facilitar el procesamiento de la interfaz gráfica de usuario; instrucciones de procesamiento del sensor para facilitar el procesamiento y las funciones relacionados con el sensor; instrucciones telefónicas para facilitar los procesos y funciones relacionados con el teléfono; instrucciones de mensajería electrónica para facilitar los procesos y funciones relacionados con la mensajería electrónica; instrucciones de navegación web para facilitar los procesos y funciones relacionados con la navegación web; instrucciones de procesamiento de medios para facilitar los procesos y funciones relacionados con el procesamiento de medios; instrucciones de navegación/GPS para facilitar los procesos e instrucciones relacionados con el GPS y la navegación; e instrucciones de la cámara para facilitar los procesos y funciones relacionados con la cámara. En algunas modalidades, la memoria 108 puede almacenar además información sobre los contactos de un usuario (nombres, direcciones, números de teléfono, etc.), citas y eventos programados, notas, activos multimedia tales como audio, video, imágenes fijas, o similares, que pueden reproducirse por el terminal 10, junto con los metadatos que describen los activos multimedia (por ejemplo, nombre del activo, artista, título, género, etc.), listas de reproducción (listas de activos que pueden reproducirse secuencialmente o en orden aleatorio), y similares.

La memoria 108 puede almacenar además programas de aplicación (referidos además en la presente descripción como "aplicaciones") que incluyen cualquier programa ejecutable por el(los) procesador(es) 104. Por ejemplo, en un conjunto de modalidades, una aplicación puede ser un programa que incluye una interfaz de usuario para permitir la interacción con un usuario. En otras modalidades, una aplicación puede ser un proceso que se ejecuta en el segundo plano, tal como un demonio. En algunas modalidades, ciertas aplicaciones pueden instalarse en el terminal 10 por su fabricante, mientras otras aplicaciones pueden instalarse por un usuario. Los ejemplos de programas de aplicación pueden incluir programas de videojuegos, programas de gestión de información personal, programas para reproducir activos multimedia y/o navegar por la base de datos de activos multimedia, programas para controlar una interfaz de telefonía para realizar y/o recibir llamadas, y así sucesivamente. Como se indica en lo anterior y se muestra en la Figura 10, un programa de aplicación 126 puede incluir instrucciones para realizar una verificación en relación con un sistema de servidor que proporciona un servicio de verificación. Por ejemplo, el programa de aplicación 126 puede implementar el proceso de verificación del lado del terminal como se describe con referencia a las Figuras 1-9.

Las modalidades descritas y otras y las operaciones funcionales descritas en esta descripción pueden implementarse en circuitos electrónicos digitales, o en software, firmware, o hardware, de ordenador que incluye las estructuras descritas en esta descripción y sus equivalentes estructurales, o en combinaciones de una o más de ellos. Las modalidades descritas y otras pueden implementarse como uno o más productos de programas informáticos, es decir, uno o más módulos de instrucciones de programas informáticos codificados en un medio legible por ordenador para su ejecución por, o para controlar la operación de, un aparato de procesamiento de datos. El medio legible por ordenador puede ser un dispositivo de almacenamiento legible por máquina, un sustrato de almacenamiento legible por máquina, un dispositivo de memoria, una composición de materia que efectúa una señal propagada legible por máquina, o cualquier combinación de los mismos. El término "aparato de procesamiento de datos" abarca todos los aparatos, dispositivos, y máquinas para procesar datos, que incluyen a modo de ejemplo un procesador programable, un ordenador, o múltiples procesadores u ordenadores. El aparato puede incluir, en adición al hardware, el código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, el código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo, o una combinación de uno o más de ellos. Una señal propagada es una señal generada artificialmente, por ejemplo, una señal eléctrica, óptica, o electromagnética generada por máquina, que se genera para codificar información para la transmisión al aparato receptor adecuado.

Un programa informático (conocido además como un programa, software, aplicación de software, script, o código) puede escribirse en cualquier forma de lenguaje de programación, que incluye los lenguajes compilados o interpretados, y puede implementarse en cualquier forma, que incluye como un programa independiente o como un módulo, componente, subrutina, u otra unidad adecuada para su uso en un entorno informático. Un programa informático no se corresponde necesariamente con un archivo en un sistema de archivos. Un programa puede almacenarse en una porción de un archivo que contiene otros programas o datos (por ejemplo, uno o más scripts almacenados en un documento de lenguaje de marcado), en un único archivo dedicado al programa en cuestión, o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas, o porciones de código). Un programa informático puede implementarse para ejecutarse en un ordenador o en múltiples ordenadores que se ubican en un sitio o distribuyen a través de múltiples sitios y se interconectan por una red de comunicación.

Los procesos y flujos lógicos descritos en esta descripción pueden realizarse por uno o más procesadores programables que ejecutan uno o más programas informáticos para realizar funciones al operar sobre datos de entrada y generar salida. Los procesos y flujos lógicos pueden realizarse además por, y el aparato puede implementarse además como, el circuito lógico de propósito especial, por ejemplo, una FPGA (matriz de puerta programable en campo) o un ASIC (circuito integrado específico de aplicación).

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, tanto microprocesadores de propósito general como especial, y uno cualquiera o más procesadores de cualquier tipo de ordenador digital. Generalmente, un procesador recibirá instrucciones y datos desde una memoria de sólo lectura o una memoria de acceso aleatorio o ambas.

5 Aunque esta descripción contiene muchos detalles, estos no deberían interpretarse como limitaciones en el alcance de lo que se reivindica o de los que puede reivindicarse, sino más bien como descripciones de características específicas a modalidades particulares. Ciertas características que se describen en esta descripción en el contexto de modalidades separadas pueden implementarse además en combinación en una única modalidad. A la inversa, 10 diversas características que se describen en el contexto de una única modalidad que pueden implementarse además en múltiples modalidades de manera separada o en cualquier subcombinación adecuada. Además, aunque las características pueden describirse anteriormente como que actúan en ciertas combinaciones e incluso reivindicarse inicialmente como tal, una o más características de una combinación reivindicada pueden en algunos casos eliminarse de la combinación, y la combinación reivindicada puede dirigirse a una subcombinación o variación 15 de una subcombinación.

De manera similar, aunque las operaciones se representan en los dibujos en un orden particular, esto no debería entenderse como que requiere que tales operaciones se realicen en el orden particular mostrado o en orden secuencial, o que todas las operaciones ilustradas se realicen, para lograr resultados deseables. En ciertas 20 circunstancias, la multitarea y el procesamiento en paralelo pueden ser ventajosos. Además, la separación de diversos componentes del sistema en las modalidades descritas anteriormente no debería entenderse como que requiere tal separación en todas las modalidades, y debería entenderse que los componentes y sistemas del programa descritos pueden integrarse generalmente juntos en un único producto de software o empaquetarse en múltiples productos de software.

REIVINDICACIONES

1. Un método implementado por ordenador realizado por un dispositivo de comunicación controlado por software (10) asociado con un número de teléfono de suscripción en una red de telefonía (12A), dicho método que comprende:
 - operar un proceso de monitoreo para detectar una llamada de verificación entrante y determinar un número de teléfono de origen (#DE ORIGEN) de la llamada de verificación entrante, o un identificador (ID2) transmitido por la llamada de verificación entrante, al identificar la llamada de verificación entrante como la primera llamada entrante que se origina desde un número de teléfono que coincide con un grupo de números de teléfono conocidos por dicho dispositivo de comunicación, dicha llamada de verificación entrante que se inicia en un sistema de servidor (14) para verificar un número de teléfono no confirmado (MI#) al realizar, en respuesta a una solicitud de verificación inicial (VR1) que incluye el número de teléfono no confirmado, la llamada de verificación al número de teléfono no confirmado (MI#) desde un número de teléfono que llama (#DE LLAMANTE); y
 - transmitir, cuando el proceso de monitoreo detecta la llamada de verificación entrante, una segunda solicitud de verificación (VR2) al sistema de servidor (14), la segunda solicitud de verificación (VR2) que incluye el número de teléfono de origen (#DE ORIGEN) de la llamada de verificación entrante o el identificador (ID2), lo que permite de esta manera que el sistema de servidor (14) verifique que el número de teléfono no confirmado (MI#) es un número de teléfono de suscripción asignado al dispositivo de comunicación (10) al comparar el número de teléfono de origen (#DE ORIGEN) con el número de teléfono que llama (#DE LLAMANTE) o al validar el identificador (ID2).
2. El método de acuerdo con la reivindicación 1, en donde la llamada de verificación entrante se termina en el dispositivo de comunicación (10) sin responderse.
3. El método de acuerdo con la reivindicación 1 o 2, en donde el proceso de monitoreo opera para detectar la llamada de verificación entrante como la primera llamada entrante recibida por el dispositivo de comunicación (10) dentro de un período de tiempo predefinido.
4. El método de acuerdo con una cualquiera de las reivindicaciones 1-3, en donde el proceso de monitoreo intercepta la llamada de verificación entrante sin notificar al usuario del dispositivo de comunicación (10).
5. El método de acuerdo con una cualquiera de las reivindicaciones 1-4, en donde la llamada de verificación entrante se oculta del usuario.
6. El método de acuerdo con una cualquiera de las reivindicaciones 1-5, en donde la solicitud de verificación (VR2) incluye además el número de teléfono no confirmado (MI#).
7. El método de acuerdo con una cualquiera de las reivindicaciones 1-6, que comprende además, si el proceso de monitoreo falla al detectar la llamada de verificación entrante dentro de un periodo de tiempo máximo, enviar un mensaje de error al sistema de servidor (14).
8. El método de acuerdo con una cualquiera de las reivindicaciones 1-7, que comprende además: recibir un mensaje de estado (CONF) desde el sistema de servidor (14) que indica que la verificación por el sistema de servidor (14) ha tenido éxito o ha fallado.
9. El método de acuerdo con una cualquiera de las reivindicaciones 1-8, que comprende además: recibir una solicitud para la verificación en relación con dicho sistema de servidor (14); obtener el número de teléfono no confirmado (MI#); y transmitir dicha solicitud inicial (VR1) para la verificación desde el dispositivo de comunicación (10) hacia el sistema de servidor (14), la solicitud inicial (VR1) que incluye el número de teléfono no confirmado (MI#) y que se configura para provocar que el sistema de servidor (14) inicie la llamada de verificación desde la red de telefonía (12A) hacia el número de teléfono no confirmado (MI#) desde el número de teléfono que llama (#DE LLAMANTE).
10. El método de acuerdo con la reivindicación 9, en donde el proceso de monitoreo opera para detectar la llamada de verificación entrante como la primera llamada entrante recibida por el dispositivo de comunicación (10) dentro de un período de tiempo predefinido desde la transmisión de la solicitud inicial (VR1).
11. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en donde el grupo de números de teléfono se almacena en cualquier formato en una memoria del dispositivo de comunicación.
12. Un medio legible por ordenador que comprende instrucciones de programa que, cuando se ejecutan por un procesador (104) en un dispositivo de comunicación (10) asociado con un número de teléfono de suscripción en una red de telefonía (12A), realiza el método de una cualquiera de las reivindicaciones 1-11.

13. Un sistema de verificación implementado por ordenador en un dispositivo de comunicación (10) que se asocia con un número de teléfono de suscripción en una red de telefonía (12A), dicho sistema de verificación que comprende:
- 5 un detector de llamada de verificación (64) configurado para monitorear una interfaz de llamada de voz (66; 110) en el dispositivo de comunicación (10) para la detección de una llamada de verificación entrante y determinar un número de teléfono de origen (#DE ORIGEN) de la llamada de verificación entrante, o un identificador (ID2) transmitido por la llamada de verificación entrante, al identificar la llamada de verificación entrante como la primera llamada entrante que se origina desde un número de teléfono que coincide con un grupo de números de teléfono conocidos por el dispositivo de comunicación (10), dicha llamada de verificación entrante que se inicia en un sistema de servidor (14) para verificar un número de teléfono no confirmado (MI#) al realizar, en respuesta a una solicitud de verificación inicial (VR1) que incluye el número de teléfono no confirmado, la llamada de verificación al número de teléfono no confirmado (MI#) desde un número de teléfono que llama (#DE LLAMANTE); y
- 10 un gestor de solicitud (60B) configurado para generar, cuando se detecta la llamada de verificación entrante, una segunda solicitud de verificación (VR2) que incluye el número de teléfono de origen (#DE ORIGEN) de la llamada de verificación entrante, o el identificador (ID2), y transmitir la segunda solicitud de verificación (VR2) al sistema de servidor (14), lo que permite de esta manera que el sistema de servidor (14) verifique que el número de teléfono no confirmado (MI#) es un número de teléfono de suscripción asignado al dispositivo de comunicación (10) al comparar el número de teléfono de origen (#DE ORIGEN) con el número de teléfono que llama (#DE LLAMANTE) o al validar el identificador (ID2).
- 15
14. El sistema de verificación implementado por ordenador de acuerdo con la reivindicación 13, que comprende además un gestor de solicitud inicial (60A) configurado para generar una solicitud inicial (VR1) para la verificación, que incluye el número de teléfono no confirmado (MI#) y se configura para provocar que el sistema de servidor (14) inicie la llamada de verificación al número de teléfono no confirmado (MI#) desde el número de teléfono que llama (#DE LLAMANTE), y transmitir la solicitud inicial (VR1) al sistema de servidor (14) a través de una interfaz de comunicación de datos (62; 110) en el dispositivo de comunicación (10).
- 20
15. Un método para permitir la verificación de un usuario, que comprende:
- 25 permitir que el usuario inicie una solicitud (VR1) para la verificación de un número de teléfono no confirmado (MI#) en un sistema de servidor (14), para provocar que el sistema de servidor (14) inicie una llamada de verificación desde una red de telefonía (12A) hacia el número de teléfono no confirmado (MI#) desde un número de teléfono que llama (#DE LLAMANTE); y
- 30 proporcionar, al usuario, un programa informático (126) para la instalación en un dispositivo de comunicación (10), dicho programa informático (126) que es operable para realizar el método descrito en una cualquiera de las reivindicaciones 1-11.
- 35

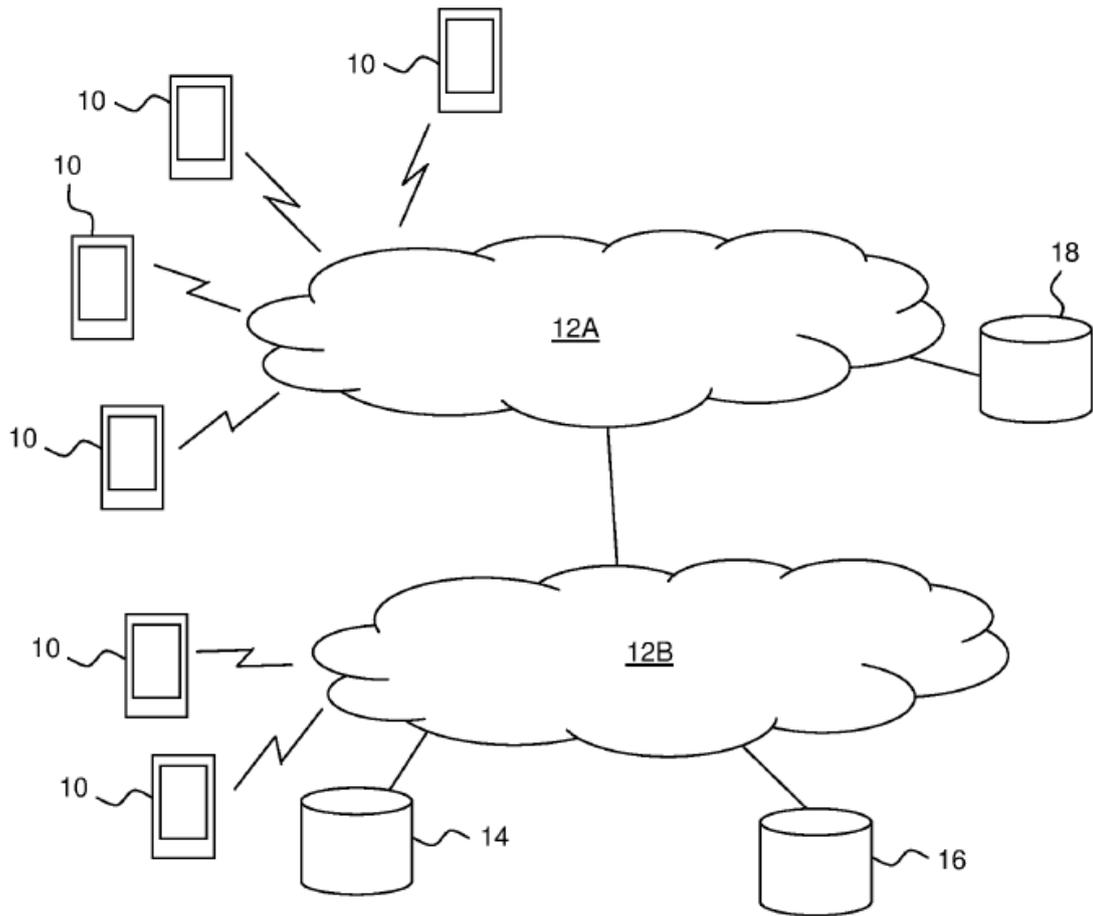


Figura 1

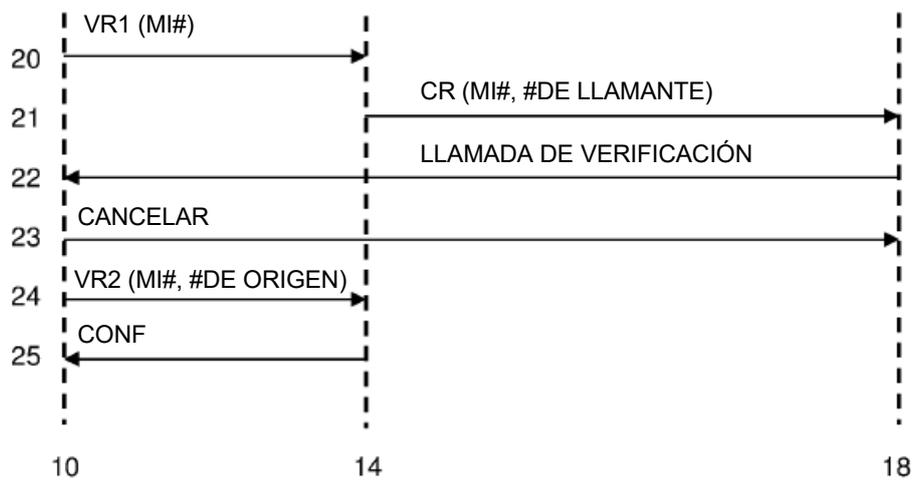


Figura 2

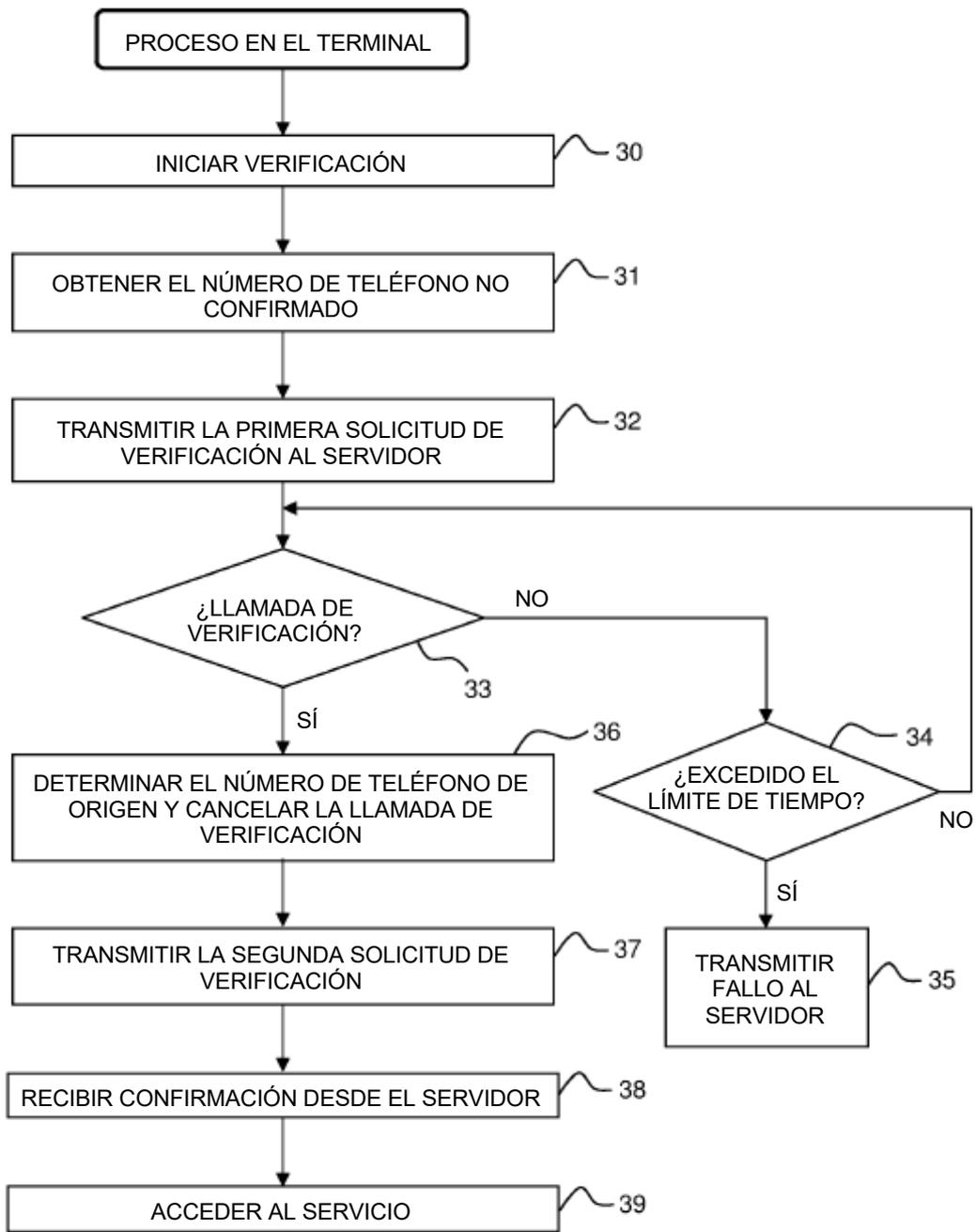


Figura 3

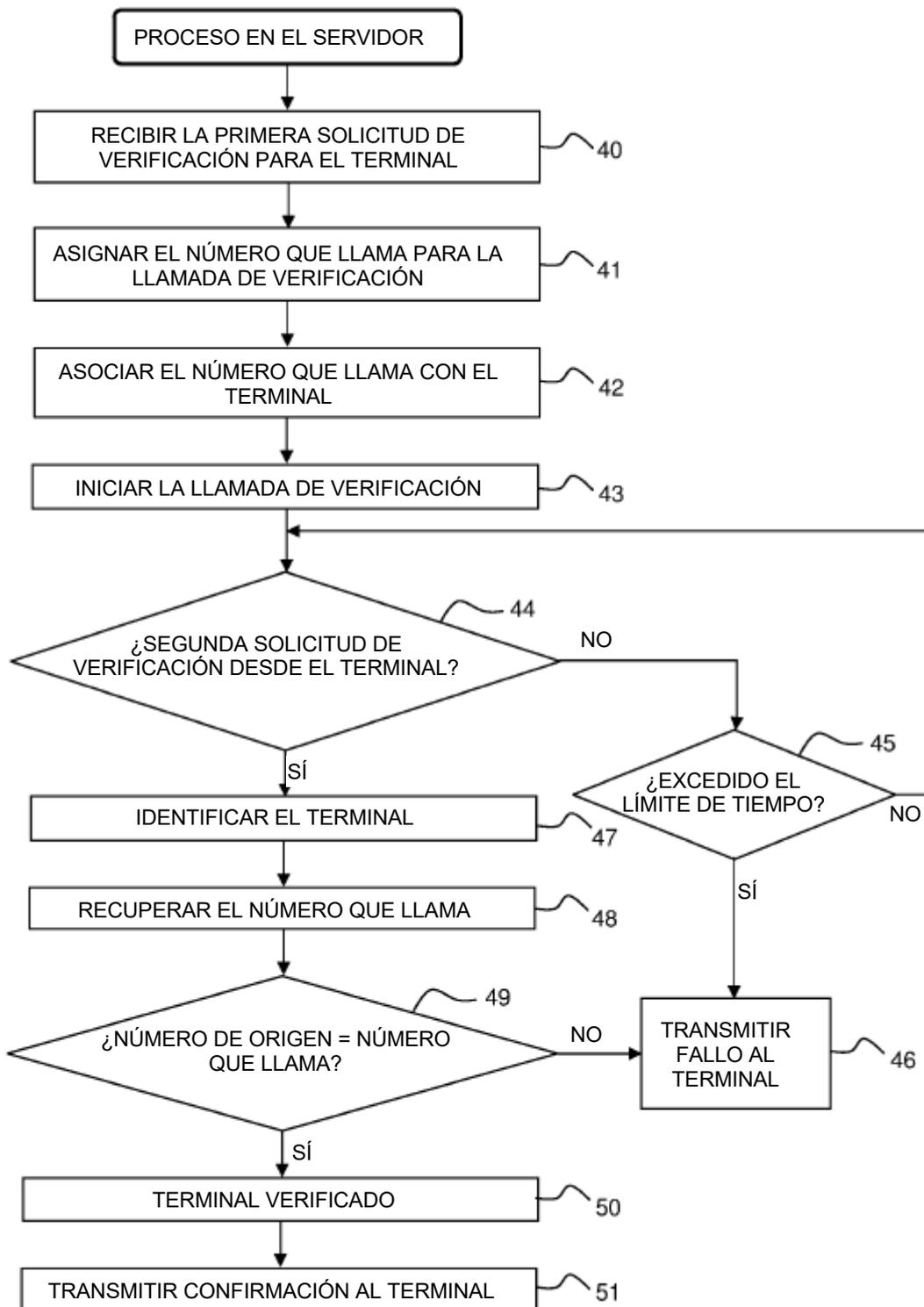


Figura 4

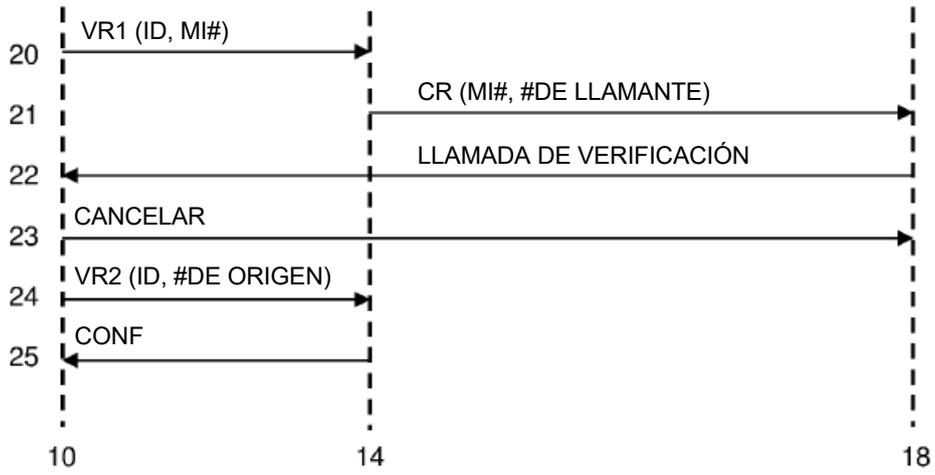


Figura 5A

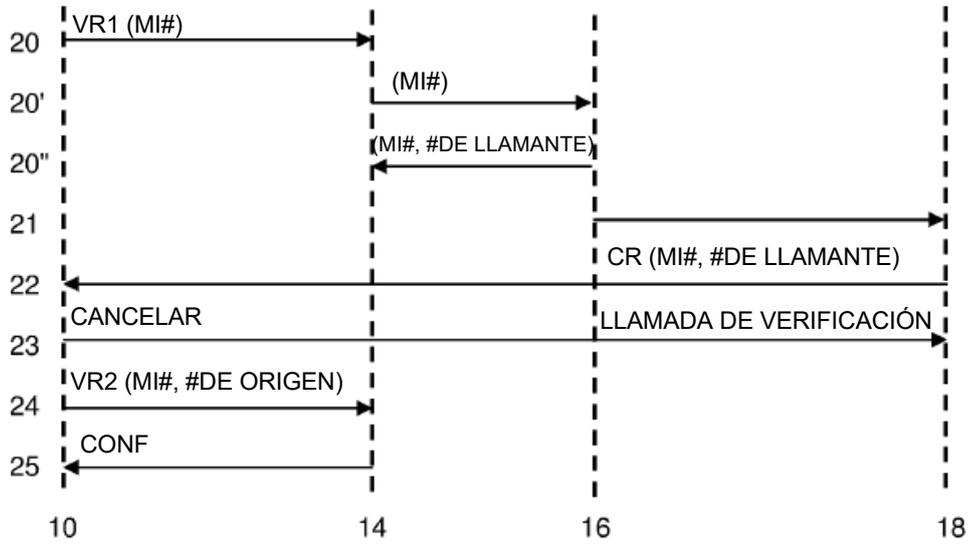


Figura 5B

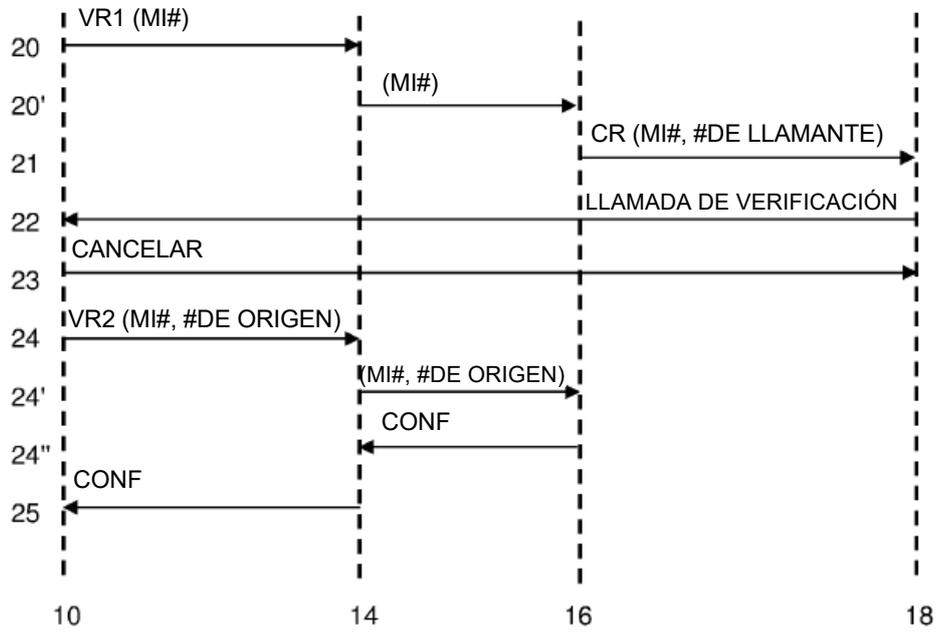


Figura 5C

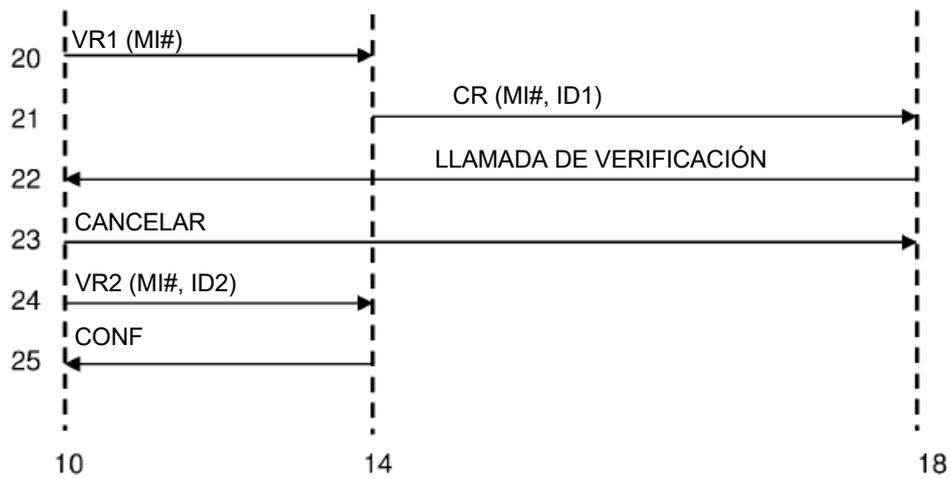


Figura 5D

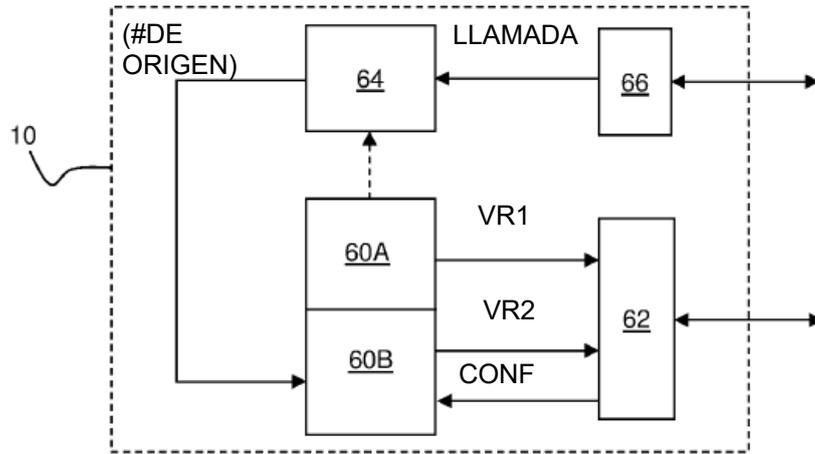


Figura 6

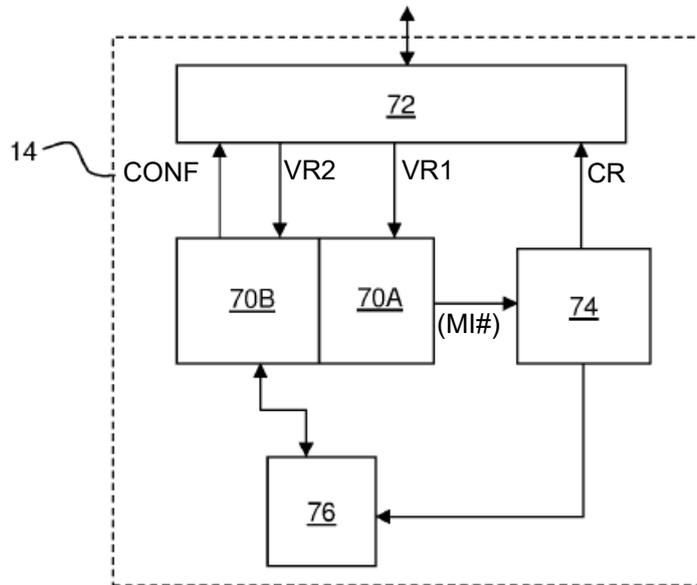


Figura 7

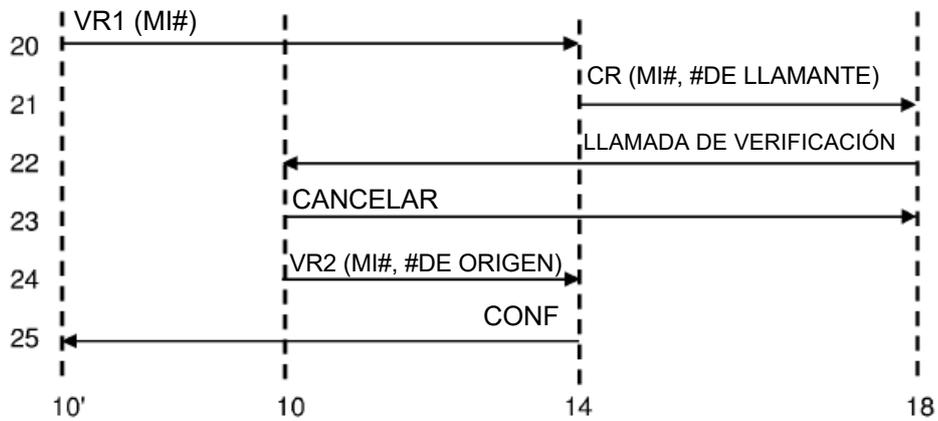


Figura 8A

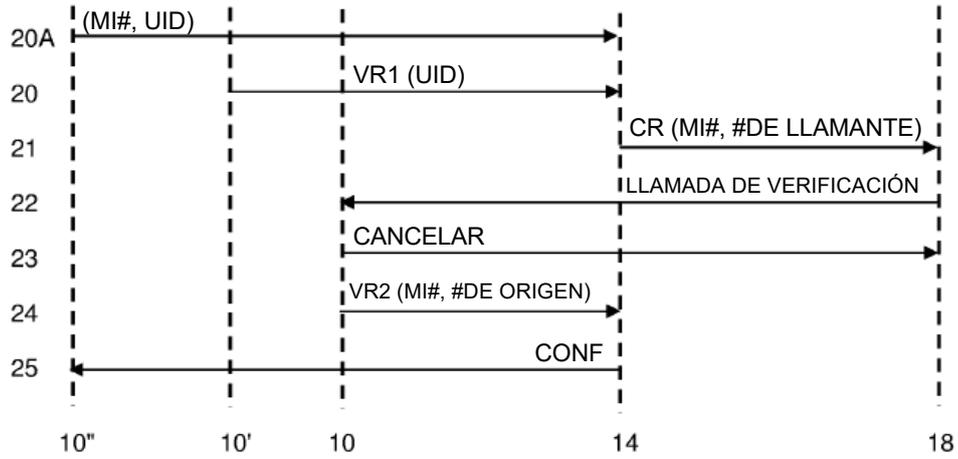


Figura 8B

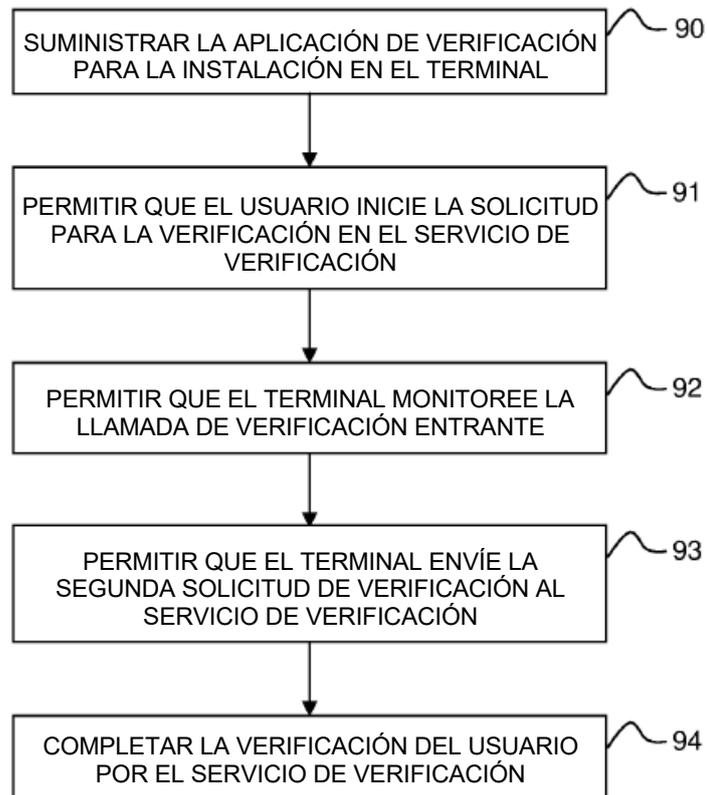


Figura 9

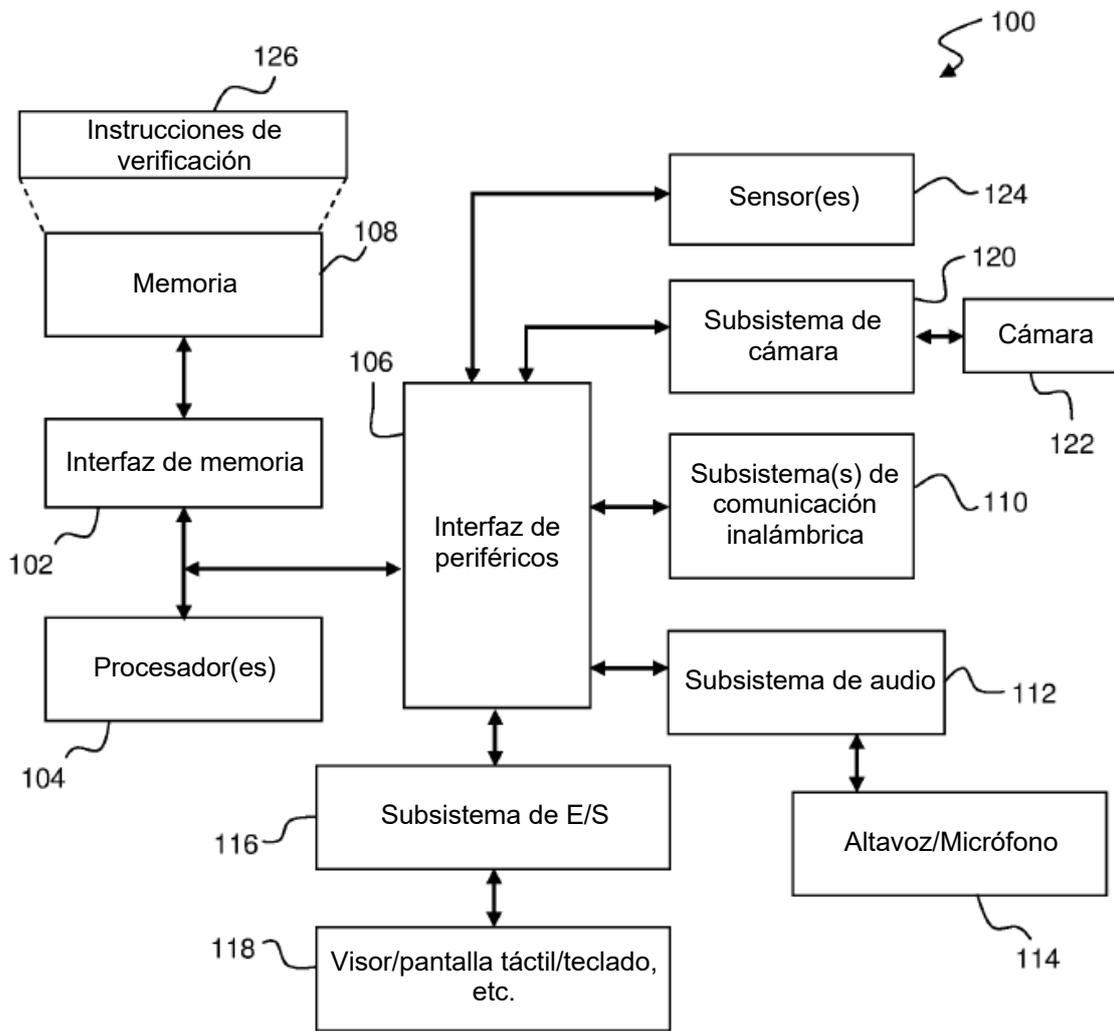


Figura 10