(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 431 625**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.10.2011 E 11183898 (3)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2013 EP 2439969**

(54) Título: **Autentificación de datos personales en sistemas de telecomunicaciones**

(30) Prioridad:

06.10.2010 FI 20106032

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2013

(73) Titular/es:

TELIASONERA AB (100.0%)
Stureplan 8
106 63 Stockholm, SE

(72) Inventor/es:

JUSSILA, OLLI

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Autentificación de datos personales en sistemas de telecomunicaciones

Campo

La invención se refiere al campo de las telecomunicaciones y, en particular, a proporcionar la autentificación de los datos personales en un sistema de telecomunicaciones de manera que una persona pueda verificar de una manera digna de confianza a otra persona que los datos personales dados por él/ella son correctos.

Antecedentes

La siguiente descripción de la técnica anterior puede incluir puntos de vista, descubrimientos, entendimientos o divulgaciones, o asociaciones junto con descripciones no conocidas en la técnica anterior relevante de la presente invención, pero proporcionada por la invención. Algunas de estas contribuciones de la invención pueden indicarse específicamente a continuación, mientras que otras de tales contribuciones de la invención serán evidentes a partir de su contexto.

El documento EP 1835688 divulga una solución en la que un abonado puede ser autentificado en una red local sin la participación de la red doméstica del abonado. En la solución, la red local comprende un servidor de autentificación de red y una entidad de autentificación local. Cuando la entidad de autentificación local desea autentificar a un abonado, envía una solicitud al servidor de autentificación de red, conteniendo la solicitud la identidad del terminal del usuario que el abonado está utilizando. El servidor de autentificación de red a continuación crea una clave de autentificación, la envía de forma segura al terminal del usuario y a la entidad de autentificación local, que almacenan la clave de autentificación recibida. La entidad de autentificación local entonces autentifica el terminal del usuario, y por lo tanto el abonado, mediante la verificación de la clave almacenada en el terminal del usuario con la clave almacenada en la entidad de autentificación local.

La cantidad de servicios basados en la web que requieren algún tipo de autentificación de usuarios se ha incrementado rápidamente en los últimos años, gracias a la evolución de los sistemas de identificación electrónica y las tecnologías de comunicaciones seguras. Ejemplos de este tipo de servicios basados en la web incluyen la banca en línea, diferentes servicios de pago, servicios en línea ofrecidos por las autoridades estatales, tales como solicitar una tarjeta de deducción de impuestos en línea, diferentes medios de comunicación social, etc. Normalmente, cada proveedor de servicios decide cómo se autentifica al usuario o se verificada su identificación para que el usuario esté autorizado para acceder al servicio.

Una de las últimas soluciones para la identificación segura y firmas digitales, destinada a diferentes servicios web, es un esquema de identificación móvil basado en SIM que utiliza la infraestructura de clave pública inalámbrica. En el esquema de identificación móvil, también llamado un sistema de certificados móviles, un par de claves criptográficas asimétricas se almacenan de forma segura con una aplicación de autentificación correspondiente en un módulo de identidad de abonado (SIM). Una persona que está en posesión del módulo de identidad del abonado puede identificarse a sí mismo/a en diferentes servicios web con la identificación móvil. En el esquema de identificación móvil, cuando un usuario inicia una sesión en un servicio, el usuario proporciona su número de teléfono móvil o un nombre de usuario, por medio de los cuales se puede resolver el número de móvil, y un servidor que proporciona el servicio envía una solicitud de autentificación a un proveedor de servicios de firma móvil (MSSP), que es el operador del usuario o un tercer proveedor de servicios de confianza y asocia el par de claves con los datos personales propios de la persona. El MSSP genera y envía un mensaje corto flash encriptado a la aplicación de autentificación del usuario en el SIM en el teléfono móvil, el mensaje corto flash que informa al usuario de que él/ella está tratando de entrar en el servicio y solicita al usuario que introduzca una contraseña que el usuario ha seleccionado para la autentificación de identificación móvil, si el usuario quiere ingresar en el servicio indicado en el mensaje corto flash. El mensaje corto flash se descifra mediante la aplicación de autentificación en el dispositivo móvil en el que está el módulo de identidad de abonado, y el contenido se muestra al usuario. El usuario introduce la contraseña a través de la interfaz de usuario, la aplicación de autentificación comprueba la contraseña, crea un mensaje que indica el resultado de la comprobación, cifra el mensaje (es decir, firma la solicitud recibida) y el dispositivo móvil envía el mensaje al MSSP. El MSSP descifra el mensaje verificando así al usuario y reenvía el resultado de la autentificación al servicio. Si el resultado es positivo, se abre el servicio para el usuario. En el proceso, el MSSP utiliza una clave pública y la aplicación de autentificación una clave privada correspondiente.

Un problema con la solución es que la identificación móvil sólo se puede utilizar para servicios web, ya sea para ingresar en el servicio para el uso del servicio o para la firma de los documentos; no existen mecanismos para utilizar el esquema de identificación móvil para verificar la identidad de un usuario a otro usuario (persona), por ejemplo. Un escenario de implementación sencillo sería que los dispositivos móviles contendrían un servicio de autentificación en el que otros usuarios puedan iniciar la sesión, realizando el servicio en el dispositivo móvil la funcionalidad descrita anteriormente del servidor y el envío después de un registro con éxito en algunas piezas de la información personal del usuario móvil del dispositivo de la persona que utiliza el otro dispositivo. Sin embargo, el registro en un servicio que se localiza en el dispositivo móvil de otra persona requiere información de la dirección del

servicio en el dispositivo móvil de la otra persona y una clave pública de la otra persona en el dispositivo móvil de un usuario que quiera obtener información personal de confianza en la otra persona. Esta es una solución bastante complicada y muy difícil de implementar.

Sumario

A continuación se presenta un resumen simplificado de la invención con el fin de proporcionar una comprensión básica de algunos aspectos de la invención. Este resumen no es una amplia descripción de la invención. No se pretende identificar elementos clave/críticos de la invención o delinear el alcance de la invención. Su único propósito es presentar algunos conceptos de la invención en una forma simplificada como un preludio de la descripción más detallada que se presenta más adelante.

La invención se basa en la utilización de la cooperación y la confianza entre los diferentes operadores (o proveedores) que venden suscripciones para los usuarios, y que proporciona a los suscriptores de los operadores en un sistema de comunicaciones un servicio común que permite que el sistema de identificación móvil descrito anteriormente se utilice para la autorización de persona a persona de los datos personales, tales como piezas de información de identidad personal.

Varios aspectos de la invención comprenden un procedimiento, un producto de programa de ordenador, un aparato y un sistema tal como se define en las reivindicaciones independientes. Otras realizaciones de la invención se describen en las reivindicaciones dependientes.

Breve descripción de los dibujos

A continuación, se describirán en mayor detalle diferentes realizaciones con referencia a los dibujos adjuntos, en los cuales

La figura 1 muestra una arquitectura simplificada de un sistema de ejemplo y diagramas esquemáticos de algunos dispositivos móviles;
La figura 2 es un diagrama esquemático de un aparato de servidor de acuerdo con una realización;
Las figuras 3 a 5 ilustran ejemplos de señalización; y
Las figuras 6 y 7 son diagramas de flujo que ilustran realizaciones de la invención.

Descripción detallada de algunas realizaciones

Ejemplos de realización de la presente invención se describirán ahora con más detalle con referencia a los dibujos adjuntos, en los cuales se muestran algunas, pero no todas las realizaciones de la invención. De hecho, la invención puede realizarse de muchas formas diferentes y no debe interpretarse como limitada a las realizaciones indicadas en este documento; más bien, estas realizaciones se proporcionan para que esta descripción satisfaga los requisitos legales aplicables. Aunque la memoria puede referirse a "un", "una", o "alguna" realización(es) en varios lugares, esto no significa necesariamente que cada una de tales referencias sea a la(s) misma(s) realización(es), o que la función se aplique sólo a una única realización. Características individuales de las diferentes realizaciones también pueden combinarse para proporcionar otras realizaciones.

Las realizaciones de la presente invención son aplicables a cualesquiera aparatos que proporcionen la funcionalidad de servidor y/o a cualquier sistema de comunicación o cualquier combinación de diferentes sistemas de comunicación que soporten el esquema de identificación móvil descrito anteriormente, o un esquema correspondiente que utilice una identidad electrónica segura asociada con medios digitales utilizados para identificar un abonado en un sistema de comunicaciones. El sistema de comunicación puede ser un sistema de comunicación inalámbrico o un sistema de comunicación que utiliza redes fijas y redes inalámbricas. Los protocolos utilizados y las especificaciones de los sistemas de comunicación, y de los aparatos, especialmente en la comunicación inalámbrica, se desarrollan rápidamente. Dicho desarrollo puede requerir cambios adicionales a una realización. Por lo tanto, todas las palabras y expresiones deberían ser interpretadas ampliamente y están destinadas a ilustrar, no a restringir, la realización.

Una arquitectura general de un sistema 100 que proporciona un servicio de identificación de persona a persona se ilustra en la figura 1. La figura 1 es una arquitectura simplificada que sólo muestra algunos aparatos, elementos y entidades funcionales, siendo todas unidades lógicas cuya implementación puede ser diferente a lo que se muestra.

Un dispositivo móvil 110, 110' se refiere a un dispositivo de computación que opera con un módulo de identificación de abonado (SIM), que incluye, pero no está limitado a, los siguientes tipos de dispositivos de comunicación inalámbricos móviles portátiles: teléfonos móviles, teléfonos inteligentes, asistentes digitales personales (PDA), auriculares, ordenadores portátiles, dispositivos de lectura electrónica portátiles, tabletas. El dispositivo móvil 110, 110' está configurado para realizar una o más funcionalidades de dispositivos móviles que se describen a continuación con una realización, y pueden configurarse para realizar funciones de diferentes realizaciones. Para este propósito, el dispositivo móvil comprende una identificación móvil 11, 11' de seguridad almacenada en el SIM

12. 12' para proporcionar la autentificación de los datos personales, como se describirá más adelante, y para el almacenamiento de algunas piezas de datos personales, al menos una contraseña (puede también llamarse número de identificación personal, PIN) para la identificación móvil. La identificación móvil comprende una aplicación de autentificación y un par de claves de una clave pública y una clave privada. La identificación móvil, o más precisamente la aplicación de autentificación, puede implementarse con un conjunto de herramientas de aplicación SIM. El conjunto de herramientas de aplicación SIM consiste en un conjunto de comandos programados en el SIM que definen cómo el SIM debe interactuar directamente con el mundo exterior e inicia comandos de forma independiente del dispositivo real en el que está el SIM y la red. Esto permite que la identificación móvil en el SIM cree un intercambio interactivo que termina en la obtención de los datos personales autentificados sobre otra persona, tal como se describirá a continuación. El conjunto de herramientas de aplicación SIM también da órdenes al dispositivo real, tales como menú de pantalla y pide la intervención del usuario. El par de claves se utiliza sólo para la aplicación de autentificación, almacenándose y utilizándose las claves o pares de claves para otros fines por separado.

Se debe apreciar que el SIM cubre aquí sus equivalentes y módulos correspondientes, como una tarjeta universal de circuito integrado, un módulo de identidad de usuario extraíble, una tarjeta de memoria flash extraíble, y un hardware informático seguro incrustado. Además, el dispositivo móvil comprende otras unidades y módulos que no se muestran, como una interfaz de red, la interfaz del SIM y una interfaz de usuario.

En el ejemplo ilustrado, hay un servidor separado 120 que contiene el servicio común de identificación móvil de persona a persona (modID P2P), que se describe en más detalle a continuación, y una entidad adquiriente separada (AE) 130. Sin embargo, pueden estar integrados juntos.

La entidad adquirente es un dispositivo informático que proporciona una interfaz para la autentificación y el servicio de proveedor de identidad. La entidad adquirente pertenece, en el ejemplo que se ilustra, a un sistema 300 de proveedor de servicio de firma móvil (MSSP), que es una malla asegurada 310 formada por diferentes proveedores de servicios de firma móvil 131, 131' que utilizan autoridades de emisión de certificados 132, 132'. La malla proporciona itinerancia por el servicio de identificación móvil. Un proveedor de servicios de firma móvil 131, 131' es un tercero de confianza que proporciona un nivel de confianza básica para un usuario proporcionado de identidad y genera pares de claves. Durante el registro de una persona al servicio de identificación móvil, una autoridad de emisión de certificados 132, 132' emite un certificado digital que comprende la clave pública y los datos personales básicos (información de identidad) mediante la solicitud de un proveedor de servicios de firma móvil de origen, es decir, el proveedor de servicios en el que se registra la persona. Típicamente, una persona se suscribe al servicio desde el operador de la persona que coopera con un proveedor de servicio de firma móvil, y el sistema 300 es un dominio de confianza de los operadores que prestan el servicio en cooperación. El certificado digital se almacena en un entorno seguro del proveedor de servicios de firma móvil y se asocia con la verdadera identidad de la persona y los datos personales 31, 31'. Los datos personales 31, 31' pueden incluir, además de la información de identidad certificada, información adicional proporcionada por la persona. Ejemplos de información adicional incluyen una dirección de correo electrónico y una foto. El par de claves se pueden almacenar en el SIM antes del suministro del SIM, o pueden utilizarse comandos aéreos para generar y almacenar el par de claves.

Sin embargo, se debe apreciar que los detalles de implementación del sistema de proveedor de servicio de firma móvil (MSSP), o un sistema correspondiente de autentificación de los datos personales de la persona, no soporta ningún significado para la invención y, por lo tanto, se pueden utilizar otras soluciones.

La(s) red(es) 200 en la(s) que los dispositivos móviles pueden comunicarse entre sí y/o con el servidor de identidad móvil de persona a persona puede(n) utilizar GSM/EDGE de tercera generación (3G), WiMax, una combinación de evolución a largo plazo (LTE) y una red de núcleo de paquetes evolucionado (EPC), una combinación de LTE avanzado y EPC, y otras tecnologías de redes celulares de cuarta generación (4G), o diferentes combinaciones de las mismas. Se debe apreciar que, aunque el sistema de proveedor de servicio de firma móvil se ha ilustrado por separado de la red 200, los aparatos y los dispositivos pueden utilizar la misma infraestructura de red con la entidad adquiriente y/o para el intercambio de información.

Aunque aparatos, tales como los dispositivos móviles, el servidor, y la entidad de autentificación se han representado en la figura 1 como una entidad, pueden implementarse en una o más entidades físicas o lógicas. Sus unidades y funciones pueden ser componentes de software y/o software-hardware y/o de firmware (grabadas indeleblemente en un medio como memoria de sólo lectura o incorporados en un circuito de ordenador cableado).

La figura 2 ilustra un diagrama de bloques de ejemplo de un aparato que proporciona el servicio de identificación móvil de persona a persona. En aras de la claridad del aparato, o un componente correspondiente, en este documento se le llama un servidor. El servidor 120 es un dispositivo informático configurado para realizar una o más funcionalidades de servidor que se describen a continuación con una realización, y puede configurarse para realizar funciones de diferentes realizaciones. Para este fin, el servidor de ejemplo ilustrado en la figura 2 comprende una unidad de gestión de casos (Caso M) 21, una unidad de obtención de datos (datos O) 22, una unidad de autentificación (aut) 23, y al menos una memoria 24 para almacenar información relacionada con el servicio al menos para la unidad de gestión de casos. En el ejemplo que se ilustra, la unidad de gestión de casos 21 está

configurada para gestionar diferentes solicitudes de servicio, incluyendo la detección de si el servicio es solicitado por el usuario o por un proveedor de servicios, la asignación de las solicitudes a las solicitudes pendientes, la solicitud a la unidad de autentificación para cuidarse de la autentificación, y la solicitud de datos a la unidad de obtención de datos solicitados cuando se recibe la autentificación, y cuidar de que la información entregada es lo que se pide, por ejemplo. La unidad de gestión de casos también puede configurarse para generar identificadores de sesión y/o detectar usuarios registrados y para proporcionar datos adicionales, tales como fotografías, o un enlace a la tarjeta de identificación almacenada en Internet (proporcionado como un enlace web de una sola vez que es válido sólo durante un corto período de tiempo), a los usuarios registrados sin una solicitud específica. La unidad de obtención de datos 22 está configurada para obtener datos de un almacenamiento que almacena datos personales. El almacenamiento puede ser en el SIM, o en una identificación móvil en el SIM, en un dispositivo móvil, en cuyo caso se puede obtener como se describe a continuación o se solicita separadamente de la identificación móvil/SIM después de una autentificación exitosa. El almacenamiento puede ser parte del servidor o un dispositivo de almacenamiento que contiene información separada almacenada por el operador como parte de una suscripción de identificación móvil y verificado cuando se solicita la suscripción, o la información puede estar obtenida en dos o más almacenamientos, por ejemplo, la edad del usuario a partir de la identificación móvil y una localización de un registro de la posición del abonado local del operador del usuario final, o de un GPS o aplicación de localización correspondiente en el dispositivo móvil, o solicitada al usuario, por ejemplo. La información puede ser almacenada por el operador específicamente en almacenamientos. No hay restricciones en cuanto a dónde y cómo se almacenan los datos personales, los medios de obtenerlos después de que el número móvil internacional de abonado del usuario, tales como MSISDN, se haya resuelto, es bien conocido por los expertos en la materia y no se describirán en detalle aquí. En función de una implementación, la unidad de autentificación 23 está configurada para realizar la autentificación, es decir, actúa como una entidad de autentificación, o solicita a la entidad de autentificación para la autentificación.

La memoria 24, o memorias, comprende al menos espacio para diferentes entradas de casos pendientes 241, de modo que la asignación se puede realizar sobre la base de un identificador de casos (id caso). En el ejemplo ilustrado, una entrada de caso también incluye para cada caso una indicación de la información que una de las partes (por ejemplo A) solicita de la otra parte (B), de manera que la información apropiada puede ser enviada en una respuesta. Se dan a continuación ejemplos de esto.

El servidor comprende diferentes unidades de interfaz 25, 25', 25", incluyendo una unidad de interfaz un transmisor y/o un receptor o un medio correspondiente para recibir y/o transmitir información, tales como datos, contenido, información de control, mensajes y realizan las funciones necesarias para que los datos del usuario, el contenido, la información de control, la señalización y/o los mensajes puedan ser recibidos y/o transmitidos. En el ejemplo ilustrado, hay al menos una interfaz para los proveedores de servicios, una interfaz para solicitudes/respuestas de servicio y una interfaz para la autentificación. Sin embargo, es suficiente que haya una interfaz que permita el intercambio de información.

Cada una de las unidades puede ser una unidad separada o integrada con otra unidad o las unidades podrán estar integradas entre sí. Se debe apreciar que el servidor puede comprender otras unidades utilizadas en o para el servicio de identificación móvil de persona a persona. Sin embargo, son irrelevantes para la invención actual y, por lo tanto, no necesitan ser descritas aquí con más detalle.

El servidor y los aparatos correspondientes que implementan la funcionalidad o parte de la funcionalidad de acuerdo con una realización pueden incluir generalmente un procesador (no mostrado en la figura 2), controlador, unidad de control, microcontrolador, o similar conectado a una memoria y para distintas interfaces del aparato. En general, el procesador es una unidad central de procesamiento, pero el procesador puede ser un procesador de operación adicional. La unidad de gestión de casos 21, y/o la unidad de obtención de datos 22 y/o la unidad de autentificación 23 pueden estar configuradas como un ordenador o un procesador, o un microprocesador, tal como un elemento informático de un solo chip, o como un conjunto de chips, incluyendo al menos una memoria para proporcionar un área de almacenamiento utilizada para una operación aritmética y un procesador de operación para la ejecución de la operación aritmética. La unidad de gestión de casos 21, y/o la unidad de obtención de datos 22 y/o la unidad de autentificación 23 pueden comprender uno o más procesadores de ordenador, circuitos integrados de aplicación específica (ASIC), procesadores de señales digitales (DSP), dispositivos de procesamiento de señales digitales (DSPD), dispositivos lógicos programables (PLD), matrices de puertas de campo programables (FPGA), y/u otros componentes de hardware que se han programado para realizar una o más funciones de una o más realizaciones.

El servidor puede generalmente incluir, además, una memoria volátil y/o no volátil y, típicamente, datos de almacenamiento, o similares. Por ejemplo, la memoria puede almacenar el código de programa de ordenador, tales como aplicaciones de software (por ejemplo, para la unidad de multiplexación de enlace ascendente o la unidad de asignación de recursos) o sistemas operativos, información, datos, contenidos, o similares para que el procesador realice las etapas asociadas con una operación del servidor de acuerdo con las realizaciones. La memoria puede ser, por ejemplo, memoria de acceso aleatorio, una unidad de disco duro, u otra memoria de datos fija o dispositivo de almacenamiento. Además, la memoria, o parte de ella, pueden ser una memoria extraíble conectada de manera amovible al aparato.

A continuación, diferentes realizaciones y ejemplos se describirán utilizando el servicio de identificación móvil descrito anteriormente utilizando una infraestructura de clave pública inalámbrica y mensajes cortos flash, sin embargo, sin la restricción de las realizaciones a este tipo de implementación del servicio de identificación móvil. Las ventajas proporcionadas por los mensajes cortos flash incluyen que no se almacenan en la memoria de mensajes de la tarjeta del usuario y que se presentan directamente al usuario. Los mensajes cortos flash son mensajes cortos preferentemente binarios. En lugar de un mensaje corto flash, se podría utilizar un mensaje corto convencional, un mensaje de inserción, tal como un mensaje de WAP (protocolo de acceso inalámbrico) o un mensaje de inserción de arquitectura de empuje genérica segura. Las solicitudes de servicio de identificación móvil de persona a persona también se pueden hacer a través de Internet (la persona utiliza una interfaz web para introducir la información requerida, como un número de teléfono) o mediante el uso de WAP.

En los siguientes ejemplos, se asume que todos los usuarios tienen una identificación móvil, y, para mayor claridad, no se ilustra ninguna verificación para el derecho del usuario a utilizar el servicio, aunque la comprobación se realiza en las implementaciones reales.

Además, en los ejemplos ilustrados en las figuras 3 a 5, el término "servidor" cubre un aparato que proporciona servicios de identificación móvil de persona a persona, funcionalidades de servicio correspondientes, autentificación de funcionalidades de entidades y funcionalidades de un MSSP local de persona, siendo el intercambio de información durante la fase de autentificación simplificando para realizarse entre el servidor y el UE, ya que no se requiere ninguna modificación en el intercambio de información y el esquema de descifrado-cifrado entre el dispositivo de enlace de dispositivo AE local y MSSP móvil. Además, el término "dispositivo móvil", o UE, abarca también el módulo de identidad de abonado que contiene la identificación móvil y las funcionalidades correspondientes, aunque no se menciona explícitamente cada vez por motivos de claridad.

La figura 3 es un gráfico simplificado que ilustra un ejemplo de señalización de acuerdo con una realización, donde los datos personales de los usuarios registrados se mantienen al menos en un servidor y donde un identificador de sesión acordado por los usuarios se utiliza como un identificador de casos. En este caso, un usuario registrado significa un usuario que registró específicamente al servicio de identificación móvil de persona a persona. El registro al servicio de identificación móvil de persona a persona no es necesario, pero servicios adicionales, como la revisión de los registros y el establecimiento de un sistema privado, se pueden proporcionar a los usuarios registrados. En el ejemplo ilustrado, se supone que Anna ha charlado en un servicio de citas por Internet con Bert y quieren encontrarse cara a cara por primera vez. Antes de tener una cita, Anna quiere saber si Bert es realmente Bert Smith, un hombre de 26 años de edad, y Bert quiere estar seguro de que Anna tiene más de 20 años. Por lo tanto, Bert sugiere, en el servicio de citas en Internet, utilizar un servicio de identificación móvil de persona a persona con un código de sesión aleatoria "dating11" para la verificación de la información personal. El código de sesión aleatoria incluye aquí códigos de sesiones realizadas por un usuario o de acuerdo con los usuarios. En lugar de un código de sesión aleatoria, se puede utilizar un código predefinido por el servicio y proporcionado a un usuario para este fin. Sin embargo, la información intercambiada en el servicio de citas no se ilustra en la figura 3. Otro supuesto es que Anna y Bert son usuarios registrados del servicio.

Tras ponerse de acuerdo (punto 3-0) para utilizar el servicio y en el identificador de sesión para el servicio, Anna crea un mensaje corto que contiene el identificador de sesión y los parámetros acordados (por ejemplo, atributos) que indica que Anna quiere saber el nombre y apellido de Bert, el género y la edad, y dirige el mensaje al servicio de identificación móvil de persona a persona. A continuación, el dispositivo móvil de Anna UE-A envía el mensaje 3-1 a un servidor que proporciona el servicio. Bert también crea un mensaje corto que contiene el identificador de sesión y los parámetros acordados que indican que Bert quiere saber la edad de Anna, y dirige el mensaje a la identificación móvil para el servicio P2P. El mensaje 3-2 se envía a continuación desde el terminal móvil de Bert UE-B.

Cuando el servidor recibe el mensaje 3-1, detecta que es de un usuario registrado y extrae, en el punto 3.3, el identificador de sesión de las solicitudes, las compara con las de las entradas de los casos de servicios pendientes, no encuentra ninguna coincidencia y, por lo tanto, detecta un nuevo caso de servicio. En respuesta al nuevo caso de servicio (es decir, una nueva sesión de servicio), el servidor crea una entrada correspondiente a la que se añade el MSISDN del número de móvil de Anna y los parámetros indicados en el mensaje 3-1, y comienza, en el punto 3-3, a esperar un mensaje corto que contenga el mismo identificador de sesión. Cuando el servidor recibe el mensaje 3-2, detecta que es de un usuario registrado y extrae, en el punto 3.3, el identificador de sesión de las solicitudes, las compara con las de las entradas de los casos de servicio abiertos, encuentra una coincidencia, por lo que desencadena, en el punto 3.3, el servicio de autentificación de identificación móvil. Como consecuencia, se crean dos mensajes cortos flash, el mensaje 3-4 al UE-A (o más precisamente, la identificación móvil en el SIM de Anna insertado en el UE-A), cifrándose el mensaje mediante la clave pública de Anna, y el mensaje 3 -5 al UE-B (o, más precisamente, a la identificación móvil del SIM de Bert insertado en el UE-B), cifrándose el mensaje mediante la clave pública de Bert, conteniendo ambos mensajes la siguiente pregunta: "¿Quieres intercambiar información de identificación móvil con su amigo: código de sesión dating11?”. Se debe apreciar que esto es sólo un ejemplo del contenido del mensaje, el mensaje también puede indicar la información solicitada más específicamente, por ejemplo.

En una implementación, el servidor está configurado para tener en cuenta el riesgo de que, además de Bert y Anna, otras personas puedan haber acordado utilizar el mismo identificador "dating11" para su servicio de identificación móvil de persona a persona. En la implementación, si los identificadores de sesión independientes (es decir, "dating11") coinciden en el punto 3-3, el servidor puede configurarse para añadir números de teléfono móvil a los mensajes 3-4 y 3-5 que se muestran a las personas (número de Anna a Bert y número de Bert a Anna, o los dos números para ambos), si los números de teléfonos móviles no están no listados (lo que significa que son secretos y no está permitido mostrarlos). Si al menos uno de los números que está en la lista, entonces puede que el servidor solicite al primer usuario (en este ejemplo Anna) proporcionar un identificador de sesión adicional, o el servidor puede generar un nuevo identificador de sesión y enviarlo al primer usuario, lo que provoca que el primer usuario pase la información al segundo usuario, y luego los dos usuarios pueden enviar otra solicitud que pueda contener el nuevo identificador de sesión generado por el servidor o los identificadores de sesión originales y otros o el identificador de sesión adicional para que el servidor pueda, mediante la asociación de números de teléfono móvil con los identificadores de sesión, asegurarse de que las partes adecuadas están conectados a la sesión. Alternativamente, el servidor puede proporcionar parámetros adicionales cuando el primer usuario está solicitando un servicio de identificación móvil de persona a persona.

En respuesta a la recepción de mensajes de 3-4, la identificación móvil en el UE-A descifra el mensaje mediante la clave privada de Anna, y muestra el contenido a través de la interfaz de usuario a Anna. Anna confirma su voluntad (es decir, proporciona un reconocimiento), introduciendo su contraseña de servicios de identificación móvil. A continuación, la identificación móvil en el UE-Un comprueba la contraseña, cifra el contenido que se muestra al usuario mediante el uso de la clave privada de Anna y envía el contenido cifrado en el mensaje 3-6 al servidor.

De la misma manera, en respuesta a la recepción del mensaje 3-5, la identificación móvil en el UE-B descifra el mensaje utilizando la clave privada de Bert, y muestra el contenido a través de la interfaz de usuario a Bert. Bert confirma su voluntad (es decir, proporciona un reconocimiento), introduciendo su contraseña de servicios de identificación móvil. A continuación, la identificación móvil en el UE-B comprueba la contraseña, cifra el contenido que se muestra al usuario mediante el uso de la clave privada de Bert y envía el contenido cifrado en el mensaje 3-7 al servidor.

El servidor detecta que se recibe una respuesta de ambos participantes del caso de servicio y comprueba, en el punto 3-8, el resultado de las autentificaciones. En este caso, el envío de la información permitida, y el servidor obtienen la información solicitada sobre Anna y Bert de la memoria del servidor. El servidor crea, en el punto 3-8, correspondientes mensajes cortos flash, es decir, mensajes 3-9 a Anna que contiene "Bert Smith, de 26 años, sexo masculino" y el mensaje 3-10 de Bert contiene "23". UE-A muestra (punto 3-11) el contenido del mensaje 3-9 a Anna y UE-B muestra (punto 3-12) el contenido del mensaje 3-10 de Bert. Entonces Anna y Bert podrán acordar cuándo y dónde reunirse. Como ambos eran usuarios registrados, alguna información adicional, como una foto, se puede agregar a los mensajes 3-9 y 3-10, en respuesta a los datos personales que indiquen que la persona quiere que se agregue una foto cuando se autentifica el nombre o la edad, por ejemplo.

En una implementación, los datos adicionales de una persona registrada, tal como un enlace a una tarjeta de identificación, podrán sustituir la información solicitada, como la edad y/o el nombre, que se muestra al usuario. En otras palabras, en los mensajes 3-9 y 3-10 Anna y Bert podrían recibir un enlace a cada uno de las demás tarjetas de identidad que se mantienen en Internet por parte de una persona de confianza.

En una realización, una identificación móvil de persona a persona se utiliza para un grupo. En la realización, el mensaje 3-1 contiene un número que indica el tamaño del grupo, los miembros del cual autentificarán parte de los datos personales entre sí, o al remitente del mensaje 3-1. En la realización, el servidor mantendría "peticiones de conteo", es decir, el mensaje 3-2 de diferentes personas y monitoriza que el número de peticiones no supere el tamaño del grupo. Dependiendo de la implementación, la autentificación puede ser activada cuando todos (excepto el remitente del mensaje 3-1) han enviado el mensaje 3-2 o cada vez que hay una coincidencia.

En otra realización, en lugar de un identificador de sesión acordado, se utiliza una combinación de números de teléfono móvil como identificador de caso. Para este fin, las personas intercambian sus números de teléfono móvil. Por ejemplo, Anna envía o le dice su MSISDN a Bert para añadirse a la solicitud en lugar del identificador de sesión, y Bert envía o dice su MSISDN a Anna para añadirse a la solicitud en lugar del identificador de sesión, para que el mensaje 3-1 contenga el MSISDN de Bert y el mensaje 3-2 el MSISDN de Anna. En la realización, el servidor asocia el MSISDN del remitente con el MSISDN en el mensaje y se utiliza la asociación como si fuera un identificador de sesión (dos mismos MSISDN asociados entre sí es una coincidencia de caso de servicio).

La figura 4 es un gráfico simplificado que ilustra la señalización de acuerdo con otra realización que difiere de la realización ilustrada en la figura 3, donde el propio servicio crea identificadores de sesión. Utilizando el mismo ejemplo, en la realización, Anna y Bert pueden o no estar de acuerdo de antemano sobre cómo utilizar el servicio de identificación móvil de persona a persona.

Anna quiere estar segura de que Bert es lo que dice ser y crea un mensaje corto que contiene los parámetros que indican que Anna quiere conocer primero el nombre de Bert y sus apellidos, sexo y edad. A continuación, el

dispositivo móvil de Anna UE-A envía el mensaje 4-1 a un servidor que proporciona el servicio, como se describió anteriormente con la figura 3.

Cuando el servidor recibe el mensaje 4-1, detecta, en el punto 4-2, que el mensaje es de un usuario registrado. Además, como el mensaje 4-1 no contiene ningún identificador de sesión, el servidor detecta, en el punto 4-2, un nuevo caso de servicio. En respuesta al nuevo caso de servicio, el servidor crea una entrada correspondiente a la que el servidor agrega el MSISDN de Anna y los parámetros indicados en el mensaje 4-1, y activa, en el punto 4-2, el servicio de autentificación de identificación móvil para Anna. Como consecuencia de ello, se crea un mensaje corto flash, mensaje 4-3, y se envía al UE-A, estando el mensaje cifrado con la clave pública de Anna y que contiene una siguiente pregunta: "¿Quieres intercambiar información de identificación móvil con tu amigo?", por ejemplo.

En respuesta a la recepción del mensaje 4-3, la identificación móvil en el UE-A descifra el mensaje mediante la clave privada de Anna y muestra el contenido a través de la interfaz de usuario a Anna. Anna confirma su voluntad (es decir, proporciona un reconocimiento), introduciendo su contraseña de servicios de identificación móvil. A continuación, la identificación móvil en el UE-Un comprueba la contraseña, crea un mensaje que indica el resultado de la comprobación, cifra el mensaje utilizando la clave privada de Anna y envía el mensaje 4-4 al servidor.

En respuesta a la recepción del mensaje 4-4, el servidor comprueba, en el punto 4-5, el resultado de la autentificación. En este caso, Anna permitió el envío de la información y el servidor genera, en el punto 4-5, un identificador de sesión, lo agrega a la entrada correspondiente, crea, en el punto 4-5, un mensaje flash que contiene la información siguiente "El identificador de sesión para utilizarse con esta solicitud es verify39", y envía el mensaje 4-6 a Anna. A continuación, se inicia el servidor, en el punto 4-5, para esperar una solicitud que contenga el identificador de sesión.

En respuesta a la recepción del mensaje 4-6, el dispositivo móvil muestra, en el punto 4-7, el contenido a través de la interfaz de usuario a Anna. Entonces Anna pide a Bert que autentifique su información usando el servicio con el identificador de sesión. La solicitud y el identificador de sesión pueden ser enviados a través del servicio de citas a Bert o mediante un mensaje corto flash, por ejemplo, mostrándose este intercambio de información 4-8 mediante una línea de trazos en la figura 4 entre los dispositivos móviles de Anna y Bert.

Cuando Bert recibe la solicitud y el identificador de sesión, crea un mensaje corto que contiene el identificador de sesión, y el dispositivo móvil de Bert UE-B envía el mensaje 4-9 al servidor.

Cuando el servidor recibe el mensaje 4-9, se detecta, en el punto 4-10, que el mensaje es de un usuario registrado. Además, el servidor detecta, en el punto 4-10, que el mensaje contiene un identificador de sesión, lo compara con los de las entradas de los casos de servicios pendientes, encuentra una coincidencia, y así activa, en el punto 4-10, un servicio de autentificación de identificación móvil para Bert. Para ello, el servidor crea un mensaje corto flash, mensaje 4-11, a UE-B, estando el mensaje cifrado con la clave pública de Bert y que contiene una siguiente pregunta: "¿Quieres intercambiar información de identificación móvil con su amigo, el identificador es verify39?", por ejemplo.

En respuesta a la recepción del mensaje 4-11, la identificación móvil en el UE-B descifra el mensaje utilizando la clave privada de Bert y muestra el contenido a través de la interfaz de usuario a Bert. Bert confirma su voluntad (es decir, proporciona un reconocimiento), introduciendo su contraseña de servicios de identificación móvil. A continuación, la identificación móvil en el UE-B comprueba la contraseña, crea un mensaje que indica el resultado de la comprobación, cifra el mensaje utilizando la clave privada de Bert y envía el mensaje 4-12 al servidor.

Cuando el servidor recibe el mensaje 4-12, comprueba, en el punto 4-13, el resultado de la autentificación. Como en este ejemplo ambos permitieron el envío de la información, el servidor obtiene la información solicitada sobre Anna y Bert de la memoria del servidor y crea correspondientes mensajes cortos flash, es decir, mensajes 4-14 a Anna que contiene "Bert Smith, 26 años, sexo masculino" y el mensaje 4-15 a Bert, que contiene de "Anna Johnson, 23 años, sexo femenino". Como se describió anteriormente, el UE-A muestra el contenido del mensaje 4-14 a Anna y el UE-B muestra el contenido del mensaje 4-15 a Bert. Entonces Anna y Bert podrán acordar cuándo y dónde reunirse.

En los ejemplos anteriores Anna y Bert permiten que parte de su información personal que muestre al otro. Dependiendo de la implementación, si Anna, por ejemplo, no permite y Bert sí lo hace, la información de Bert puede o no se puede obtener, enviar y mostrar a Anna. Sin embargo, la información de Anna no se obtiene, envía ni muestra.

En el ejemplo anterior se supone que Anna decide la parte de información que han de ser autentificada, y por lo tanto, Bert no necesita añadir parámetros a la solicitud 5-9. Si Bert añade parámetros, pueden ser ignorados. Sin embargo, en otro ejemplo Bert también tiene que añadir parámetros, y se comparan con los parámetros dados por Anna. Si los parámetros son diferentes, por ejemplo, Anna indica la edad y el género y Bert la edad y el nombre, el servicio puede terminarse. Otra posibilidad es que la información indicada por los parámetros en el mensaje 41 y en el mensaje 4-9, es decir, la edad en el ejemplo, se obtenga y se muestre a los dos usuarios.

Aunque se supone anteriormente que Anna y Bert utilizan el mismo procedimiento de autentificación, se debe apreciar que Anna podría utilizar un procedimiento diferente de Bert; basta que los datos personales se autentifiquen de una manera digna de confianza.

La figura 5 es un gráfico simplificado que ilustra la señalización de acuerdo con un ejemplo adicional. Supongamos que Anton va a encontrarse con sus amigos en un pub llamado Silvers. Desafortunadamente, Anton dejó su tarjeta de identificación impresa en casa. Anton se ve muy joven para su edad y, por lo tanto, el portero pregunta a Anton si se ha suscrito al servicio de identificación móvil. Como Anton dice que sí, el portero sugiere el uso de un servicio de identificación móvil de persona a persona.

Anton está de acuerdo y el portero envía el mensaje 5-1 al servicio utilizando un dispositivo móvil de Silver UE-S. El mensaje 5-1 contiene una solicitud de una identificación de sesión. Sin embargo, no se incluyen parámetros, ya que en el ejemplo se supone que los parámetros se almacenan como parte de la información de usuario registrado en el servicio de persona a persona.

En respuesta a la recepción del mensaje 5-1 de UE-S, el servidor detecta que Silver se ha registrado en el servicio como una autoridad y tiene una interfaz de proveedor de servicios para el servicio. Por lo tanto, el servidor obtiene, en el punto 5-2, las especificaciones de servicio de Silver, siendo las especificaciones de los servicios en el ejemplo que la edad debe ser autentificada, crea, en el punto 5-2, una entrada para la solicitud, genera, en el punto 5-2, un identificador de sesión, lo agrega a la entrada correspondiente, crea, en el punto 5-2, un mensaje flash 5-3 que contiene la siguiente información "El identificador de sesión que se utilizará con esta solicitud es Silver47", y envía el mensaje 5-3 al UE-S. Aunque se supone que en el ejemplo que el mensaje 5-3 no está cifrado, puede cifrarse mediante la clave pública de Silver antes de enviarse (y a continuación, el ID de móvil en UE-S se encarga de mostrar el contenido). Por ejemplo, en una realización de una interfaz de proveedor de servicios está siempre asociada a una clave pública correspondiente y, por lo tanto, está fácilmente disponible. A continuación, se inicia el servidor, en el punto 5-2, para esperar una solicitud que contenga el identificador de sesión.

En respuesta a la recepción del mensaje 5.3, el UE-S muestra, en el punto 4.5, el contenido a través de la interfaz de usuario para el portero. El portero a continuación muestra el identificador de sesión a Anton (que se muestra mediante la línea discontinua 5-5 en la figura 5), que a continuación crea un mensaje corto que contiene el identificador de sesión y envía el mensaje al servidor. A continuación, el dispositivo móvil de Anton UE-A envía el mensaje 5-6 al servidor.

Cuando el servidor recibe el mensaje 5-6, detecta, en el punto 5-7, el mensaje 5-6 que contiene un identificador de sesión, lo compara con los de los registros de casos de servicio abiertos, encuentra una coincidencia, activando así, en el punto 5-7, un servicio de autentificación de identificaicón móvil para Anton. Para ello, el servidor crea un mensaje corto flash, el mensaje 5-8, al UE-A, estando el mensaje cifrado mediante la clave pública de Anton y que contiene una indicación de una información solicitada (edad en este ejemplo) y la siguiente pregunta: "¿Desea mostrar su información de identificación móvil a su amigo, el identificador es Silver47?", por ejemplo. (Aunque Anton no se ha registrado en el servicio de identificación móvil de persona a persona, Anton se ha registrado con el servicio de identificación móvil y, por lo tanto, el MSSP local de Anton se puede encontrar sobre la base del número de teléfono móvil de Anton).

En respuesta a la recepción del mensaje 5-8, la identificación móvil en el UE-A descifra el mensaje mediante la clave privada de Anton, y muestra la cuestión a través de la interfaz de usuario de Anton. Anton confirma su voluntad (es decir, proporciona un reconocimiento), introduciendo su contraseña de servicios de identificación móvil. A continuación, la identificación móvil en el UE-Un comprueba la contraseña, crea un mensaje que indica el resultado de la comprobación y que contiene la parte de los datos personales de Anton solicitado, cifra el mensaje utilizando la clave privada de Anton y envía el mensaje 5-9 al servidor.

Cuando el servidor recibe el mensaje 5-9, comprueba, en el punto 5-10, el resultado de la autentificación. Como en este ejemplo Anton permite el envío de la información, el servidor extrae la información solicitada sobre Anton del mensaje 5-9, crea un mensaje corto flash, mensaje 5-11, para UE-S, conteniendo el mensaje "19 años", y envía el mensaje 5-11. Como se describió anteriormente, el UE-S muestra el contenido del mensaje 5-11 al portero.

Como puede verse en el ejemplo anterior, se proporciona identificación anónima (es decir, que muestra sólo la edad de Anton al portero) sin cambiar ningún dato personal mediante la realización.

La figura 6 es un diagrama de flujo que ilustra una funcionalidad del servidor en una realización en la que los identificadores de sesión son generados por el servidor en cada caso, el número al que el solicitante de servicio envía la solicitud indicando los datos personales solicitados, una solicitud de una sesión sin identificador que indica que no hay ningún caso y que espera una solicitud con un identificador de sesión que indique que la solicitud es la segunda solicitud y que es para un caso pendiente. En el ejemplo ilustrado en la figura 6, el remitente de la primera solicitud se indica mediante A y el solicitante posterior se indica mediante B. Además, aquí el término "autoridad" se refiere a los usuarios finales registrados como proveedores de servicios, incluidas las autoridades estatales, la administración pública y diferentes empresas. El término "usuario final" se refiere a una persona en calidad de

usuario final.

La figura 6 se inicia cuando se recibe una solicitud, en el ejemplo un mensaje corto, en la etapa 601, en el servidor, estando dirigido el mensaje corto a un servicio de "autentificación de edad" en el ejemplo. El servidor comprueba, en la etapa 602, si el mensaje contiene un identificador de sesión. Si no, el servidor comprueba, en el punto 603, si el remitente es un usuario final o una autoridad. La detección puede realizarse sobre la base de la interfaz a través de la que se recibió el mensaje corto, por ejemplo, sobre la base de la dirección (o número de teléfono) que se utiliza.

Si el remitente (A) es un usuario final, el servidor envía, en la etapa 604, una solicitud de autentificación a A, la solicitud de autentificación que indica que se solicita un servicio de edad y que incluye la identificación de sesión generada. A continuación, el servidor espera, en la etapa 605, durante un período de tiempo predeterminado si se recibe una respuesta de autentificación en el tiempo desde A. Si se recibe la respuesta de autentificación a tiempo y es una aceptación (etapa 606), el servidor genera, en la etapa 607, un identificador de sesión y lo envía a A en la etapa 608. A continuación, se inicia el servidor, en la etapa 609, para esperar durante un período de tiempo predeterminado, que puede ser diferente del periodo de tiempo de la etapa 605, una solicitud de servicio que contenga el identificador de sesión generado, es decir, la segunda solicitud de servicio en relación con el caso de servicio pendiente.

Si el remitente (A) es una autoridad (etapa 603), el servidor procede directamente a la etapa 607 y continúa con la generación de un identificador de sesión.

Si la solicitud de servicio contiene un identificador de sesión, es una segunda solicitud y el servidor asigna el identificador de sesión con los identificadores de sesión de los casos pendientes, es decir, comprueba, en el punto 620, si se encuentra un caso con un identificador de sesión correspondiente. En caso afirmativo, el servidor comprueba, en el punto 610, si la solicitud se recibe dentro del límite de tiempo predeterminado. En caso afirmativo, el servidor envía, en la etapa 611, una solicitud de autentificación a B, indicando la solicitud de autentificación que se solicita un servicio de edad y que incluye la identificación de sesión generada. A continuación, el servidor espera, en la etapa 612, durante un período de tiempo predeterminado, si se ha recibido una respuesta de autentificación desde B. Si se recibe la respuesta de autentificación a tiempo (etapa 612) y es una aceptación (etapa 613), y A es una autoridad (etapa 614), el servidor obtiene, en la etapa 615, la edad de B (o la fecha de nacimiento y calcula la edad), envía, en la etapa 616, la edad desde B a A, y se cierra el caso de servicio en la etapa 617. Si se recibe la respuesta de autentificación a tiempo (etapa 612) y es una aceptación (etapa 613) y A es un usuario final (etapa 614) el servidor obtiene, en la etapa 618, la edad X de A (o la fecha de nacimiento y calcula la edad) y la edad Y de B, se envía, en la etapa 619, la edad de A a B y la edad de B a A, y se cierra, en la etapa 617, el caso de servicio.

Si la asignación de la segunda solicitud falla (etapa 620), el usuario final B es informado sobre el fallo enviando, en la etapa 621, un mensaje de "no se ha encontrado ningún identificador de sesión correspondiente", por ejemplo.

Si la respuesta de autentificación desde A (etapa 605) o la segunda solicitud (etapa 610) o la respuesta de autentificación desde B (etapa 612) no se recibe a tiempo o no se aceptó (etapa 606 y etapa 613), el usuario final (o los usuarios finales) es informado, en la etapa 622, de que la solicitud de servicio se cancela, y el caso de servicio se cierra en la etapa 617.

La figura 7 ilustra una funcionalidad de un servidor de acuerdo con otro ejemplo. También en el ejemplo ilustrado en la figura 7, el remitente de la primera solicitud se indica mediante A y el solicitante posterior se indica mediante B.

La figura 7 se inicia cuando un mensaje corto, es decir, una solicitud de servicio, es recibido, en la etapa 701, desde un dispositivo móvil, siendo el número del teléfono móvil del remitente del mensaje corto MSISDN1, conteniendo el mensaje corto MSISDN2 y un parámetro "edad".

El servidor comprueba, en la etapa 702, si hay o no un caso de servicio pendiente que tenga la combinación de MSISDN1 y MSISDN2. Si no existe tal caso de servicio, el servidor crea, en la etapa 703, una entrada de caso correspondiente con el parámetro "edad" indicado, y empieza en la etapa 704, a esperar un tiempo predeterminado para una segunda solicitud en relación con el caso de servicio (es decir, una solicitud de otro usuario final que tenga MSISDN2) y se activa la autentificación. Si el tiempo expira antes de recibir la segunda solicitud y se activa la autentificación (etapa 704), A es informado, en la etapa 705, del fallo del servicio y el caso de servicio se cierra mediante la eliminación de la entrada correspondiente en la etapa 706.

Si una entrada correspondiente está aún pendiente (etapa 702), es decir, una entrada creada anteriormente en respuesta a un mensaje corto recibido desde MSISDN2, existe el mensaje corto que contiene MSISDN1 y uno o más parámetros, la solicitud recibida en la etapa 701 es la segunda solicitud recibida dentro del periodo de tiempo predeterminado. Por lo tanto, el servidor activa, en la etapa 707, una autentificación de A y B. La activación de la autentificación también cierra la monitorización de temporización (etapa 704) si una segunda solicitud se recibe a tiempo o no. Después de la activación de la autentificación, el servidor espera, en la etapa 708, durante un período predeterminado de tiempo si las respuestas de autentificación se reciben en el tiempo de A y B. Si se reciben las respuestas de autentificación a tiempo (etapa 708) y ambas incluyen una aceptación (etapa 709) para autentificar los

datos personales, el servidor obtiene, en la etapa 710, los datos personales de A y B en función de parámetros en las solicitudes de A y B, y envía, en la etapa 711, los datos personales de B obtenidos a A y los datos personales obtenidos de A a B. A continuación, el servidor borra, en la etapa 706, la entrada correspondiente.

Las etapas/puntos, mensajes y funciones relacionadas descritas anteriormente en las figuras 3 a 7 no están en ningún orden cronológico absoluto, y algunas de las etapas/puntos se pueden realizar y/o los mensajes se pueden enviar simultáneamente o en un orden que difiere al dado. Otras funciones también se pueden ejecutar entre los puntos o etapas o dentro de las etapas/puntos y otros mensajes enviados entre los mensajes ilustrados, como el envío de acuses de recibo, y comprobar si un usuario final ha suscrito al servicio o no. Algunas de las funciones o etapas/puntos o parte de las etapas/puntos también se pueden omitir o sustituir por una función o etapa/punto o parte de una etapa/punto. Además, las etapas/puntos y/o mensajes con las diferentes realizaciones descritas se pueden combinar para obtener otras realizaciones. Por ejemplo, las solicitudes de los usuarios finales pueden gestionarse como se describe en la figura 7 (es decir, con usuarios finales persona), y como se describe en la figura 6 (es decir, con usuarios finales autoridad). Las diferentes maneras descritas anteriormente para detectar que se solicitan parámetros se pueden utilizar en todas las realizaciones. Los mensajes son sólo a modo de ejemplo e incluso pueden comprender varios mensajes separados para transmitir la misma información. Además, los mensajes también pueden contener otra información. Dependiendo de las tecnologías de red implicadas, otras entidades distintas de las descritas anteriormente pueden participar en la señalización.

Como es evidente a partir de los ejemplos anteriores, el servicio de identificación móvil de persona a persona permite que un usuario final autentifique de una manera que se puede confiar partes de datos personales facilitados por otro usuario final, y viceversa, de forma remota o en una situación cara a cara, simplemente mediante el uso de sus teléfonos móviles. Además, se da ningún dato personal sobre un usuario a otro usuario sin el consentimiento explícito del primero.

Anteriormente, la edad, el nombre y el género han sido utilizados como ejemplos de datos personales, sin limitar los datos personales que deben autentificarse a los mismos. Otros ejemplos incluyen la posición, el número de teléfono móvil, el número de seguridad social y si una persona tiene una licencia de conducir válida.

Aunque anteriormente, se recibió el número de miembros del grupo como un parámetro, puede almacenarse durante el registro. Por ejemplo, en el ejemplo de la figura 5, la información de registro de Silver podría contener una indicación de que la sesión se puede utilizar para la autentificación de N personas.

Como se ha descrito anteriormente, la solicitud de servicio puede contener parámetros que indican qué información se solicita. Otras alternativas incluyen que la información de la dirección utilizada indica la información (por ejemplo, 17345 es para la edad, el 17367 es para el nombre, y 17656 es para la edad y el nombre) o el solicitante tiene predefinida en su suscripción al servicio la información que se solicita. Por lo tanto, los usuarios finales pueden obtener la autentificación de sólo algunas partes de los datos personales de otra persona, dependiendo de la necesidad.

Aunque diferentes realizaciones se han descrito anteriormente suponiendo que se utiliza una contraseña, se debe apreciar que las realizaciones pueden implementarse por otros medios de identificación personal, como por ejemplo por medio de identificadores biométricos.

Será obvio para una persona experta en la materia que, a medida que avanza la tecnología, el concepto inventivo puede implementarse de diversas maneras. La invención y sus realizaciones no se limitan a los ejemplos descritos anteriormente, sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento que comprende:

recibir, en un aparato (120), un primer mensaje de un primer dispositivo de usuario final (110, 110'), siendo el primer mensaje una solicitud que indica que una o más partes específicas autentificadas solicita los datos personales de un usuario que utiliza otro dispositivo de usuario final (110, 110'),
crear entre el primer dispositivo de usuario final y el aparato una sesión para la solicitud,
mantener en el aparato la información relacionada con la sesión de las sesiones que tiene el aparato,
recibir en el aparato un segundo mensaje desde un segundo dispositivo de usuario final,
detectar que el segundo mensaje contiene, al menos, información con la que el aparato es capaz de asignar el segundo mensaje respecto a la información relacionada con las sesiones;
comparar la información recibida con la información correspondiente en la información relacionada con la sesión mantenida para detectar una coincidencia si el resultado de la comparación es que la información recibida en el segundo mensaje y la información correspondiente son iguales;
si hay una coincidencia, realizar mediante el aparato, al menos, lo siguiente:

enviar una solicitud de autentificación al segundo dispositivo de usuario final para autentificar a un segundo usuario mediante el segundo dispositivo de usuario final mediante un esquema de identificación móvil que utiliza un subsistema de autentificación para la identificación móvil, comprendiendo el subsistema de autentificación claves públicas, cada una asociada con los datos personales de un usuario durante una emisión de un certificado móvil, y un módulo de identidad de abonado (12, 12') que comprende una aplicación de autentificación y un par de claves de una clave pública y una clave privada del subsistema de autentificación, estando el módulo de identidad de abonado en un dispositivo de usuario final cuando se ejecuta la aplicación de autentificación;
recibir una respuesta de autentificación desde el segundo dispositivo de usuario final; y
si la respuesta de autentificación indica que la autentificación tuvo éxito y el segundo usuario aceptó la entrega de los datos personales, obtener las partes especificadas de datos personales del segundo usuario a partir de una memoria donde se almacenan los datos personales de identificación móvil, y enviar las partes obtenidas de los datos personales del segundo usuario al primer dispositivo de usuario final.

2. Un procedimiento de acuerdo con la reivindicación 1, que también comprende:

generar, mediante el aparato, un identificador de sesión en respuesta a la primera solicitud,
enviar, mediante el aparato, el identificador de sesión al primer dispositivo de usuario final; y
si la segunda solicitud contiene el identificador de sesión generado, detectar mediante el aparato una coincidencia.

3. Un procedimiento de acuerdo con la reivindicación 2, que también comprende:

enviar, mediante el aparato, una solicitud de autentificación al primer dispositivo de usuario final para autentificar el primer usuario mediante el esquema de identificación móvil;
recibir, mediante el aparato, una respuesta de autentificación desde el primer dispositivo de usuario final; y
si las respuestas de autentificación indican que la autentificación del primer dispositivo de usuario final y el segundo dispositivo de usuario final tuvieron éxito y el primer usuario y el segundo usuario aceptan la entrega de los datos personales, obtener, mediante el aparato, las partes especificadas de los datos personales del segundo usuario y las partes especificadas de los datos personales del primer usuario de la memoria, enviando las partes obtenidas de los datos personales del segundo usuario al primer dispositivo de usuario final, y enviando las partes obtenidas de los datos personales del primer usuario al dispositivo del segundo usuario final.

4. Un procedimiento de acuerdo con la reivindicación 1, 2 o 3, que también comprende:

recibir, mediante el aparato, en la primera solicitud, un identificador de sesión; y
si la segunda solicitud contiene el mismo identificador de sesión, detectar, mediante el aparato, una coincidencia.

5. Un procedimiento de acuerdo con la reivindicación 1, 2, 3 o 4, que también comprende:

recibir, mediante el aparato, en la primera solicitud, un número de teléfono móvil del segundo usuario desde el primer dispositivo de usuario final usando un número de teléfono móvil del primer usuario;
si se recibe la segunda solicitud desde un dispositivo usando el número de teléfono móvil del segundo usuario, y la segunda solicitud contiene el número de teléfono móvil del primer usuario, detectar, mediante el aparato, una coincidencia.

6. Un producto de programa informático que comprende un código de programa informático configurado para realizar un procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 5 cuando se ejecuta en un aparato.

7. Un aparato que comprende medios para la implementación de un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 5.

8. Un aparato de acuerdo con la reivindicación 7, donde el aparato es un aparato configurado para proporcionar un servicio de identificación móvil de persona a persona.

9. Un sistema que comprende al menos
un subsistema de autentificación para identificación móvil, comprendiendo el subsistema de autentificación claves públicas, cada una asociada con los datos personales de una persona durante una emisión de certificados móviles;
un primer dispositivo de usuario final y un segundo dispositivo de usuario final (110, 110');
un módulo de identidad de abonado (12, 12') que comprende una aplicación de autentificación y un par de claves de una clave pública y clave privada para el subsistema de autentificación, insertándose el módulo de abonado en el dispositivo del segundo usuario final;
una memoria configurada para almacenar partes de datos personales de un usuario del módulo de identidad de abonado, estando al menos algunas de las partes de los datos personales insertados en la memoria durante la emisión de los certificados móviles y asociados con la clave pública correspondiente;
un servidor (120) que comprende medios para la implementación de un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 5 y configurado para utilizar el subsistema de autentificación para la autentificación.

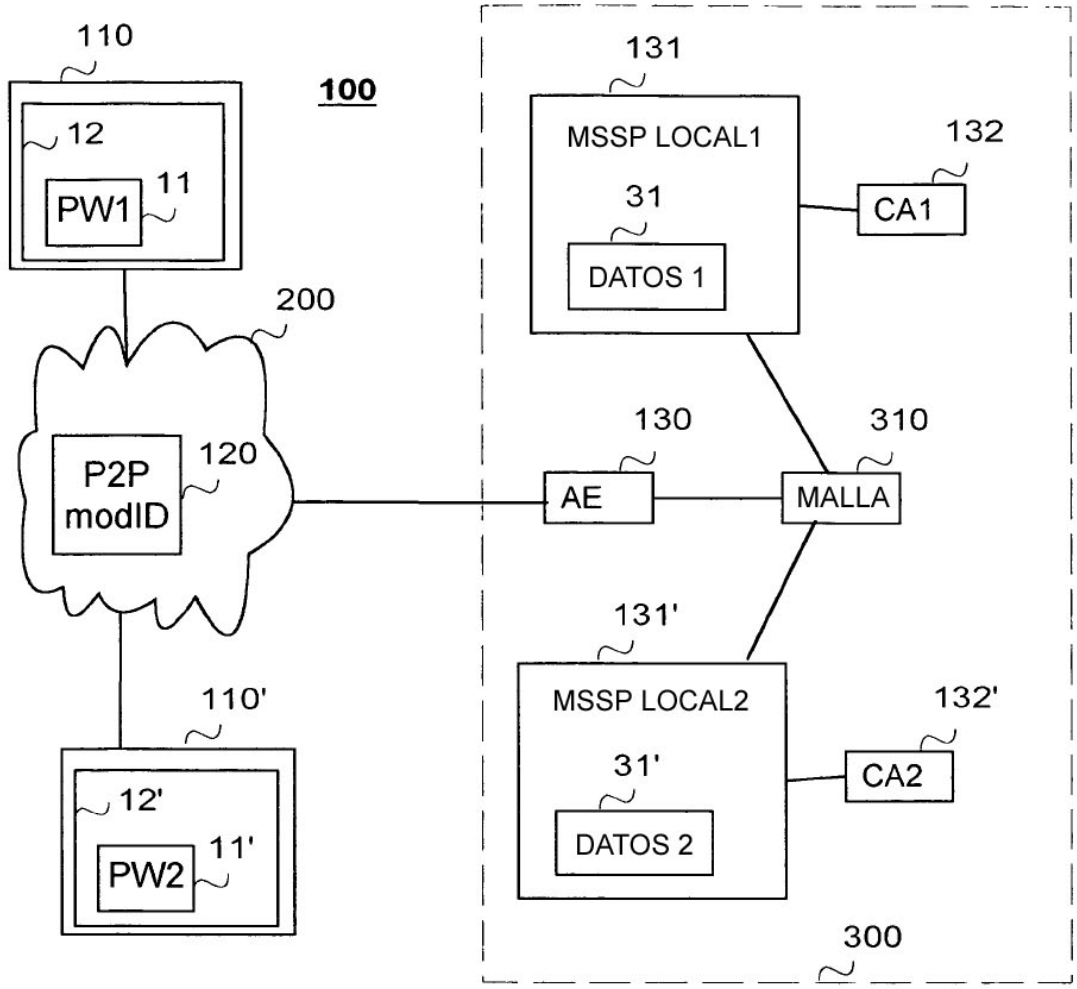
110
100
12
PW1
11
200
P2P
modID
120
131
MSSP LOCAL1
31
DATOS 1
132
CA1
130
AE
310
MALLA
131'
MSSP LOCAL2
31'
DATOS 2
132'
CA2
110'
12'
PW2
11'
300

FIG.1

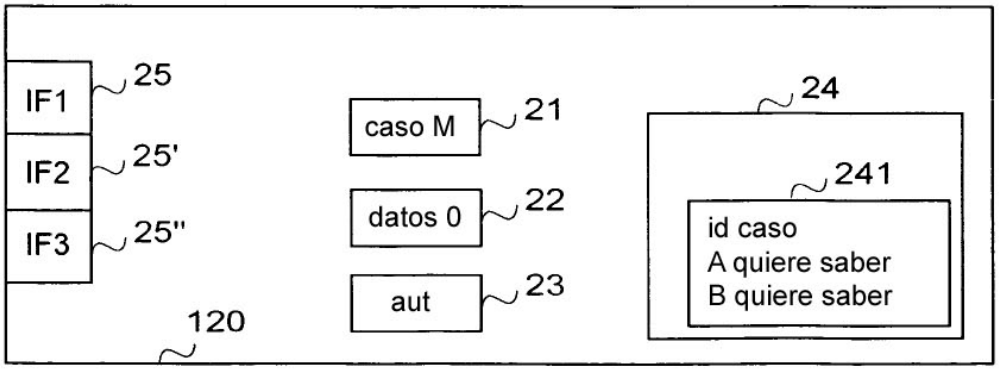
IF1
25
IF2
25'
IF3
25"
120
caso M
21
datos 0
22
aut
23
24
241
id caso
A quiere saber
B quiere saber

FIG.2

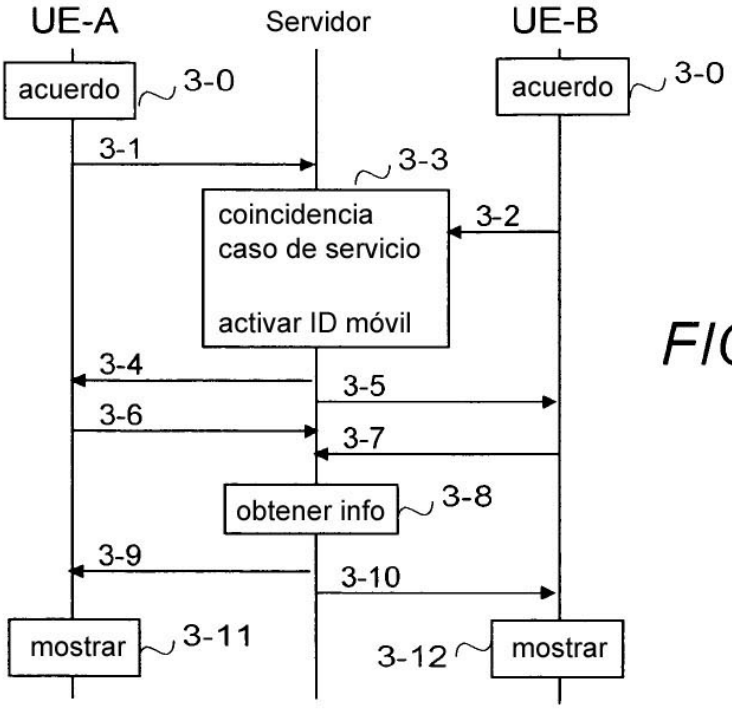
UE-A
Servidor
UE-B
acuerdo
3-0
acuerdo
3-0
3-1
3-3
coincidencia
caso de servicio
activar ID móvil
3-2
3-4
3-5
3-6
3-7
obtener info
3-8
3-9
3-10
mostrar
3-11
3-12
mostrar

FIG.3

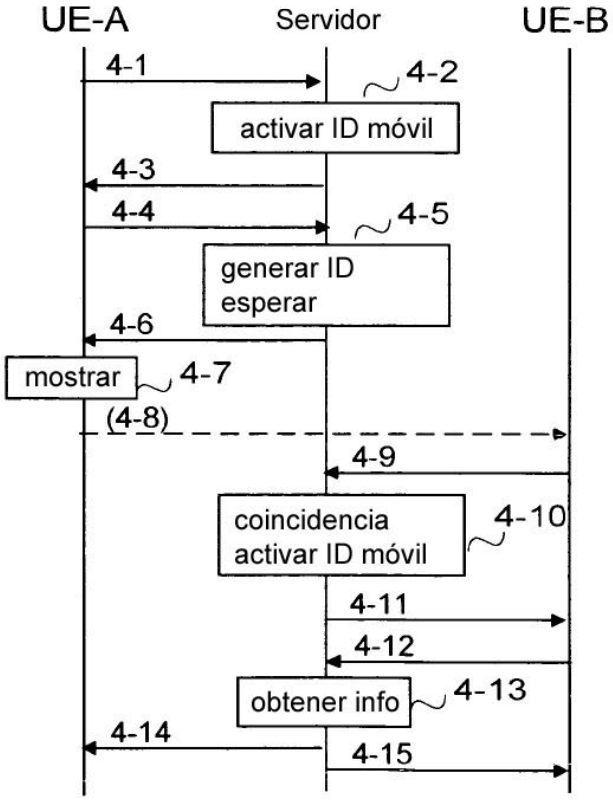
UE-A
Servidor
UE-B
4-1
4-2
activar ID móvil
4-3
4-4
4-5
generar ID
esperar
4-6
mostrar
4-7
(4-8)
4-9
coincidencia
activar ID móvil
4-10
4-11
4-12
obtener info
4-13
4-14
4-15

FIG.4

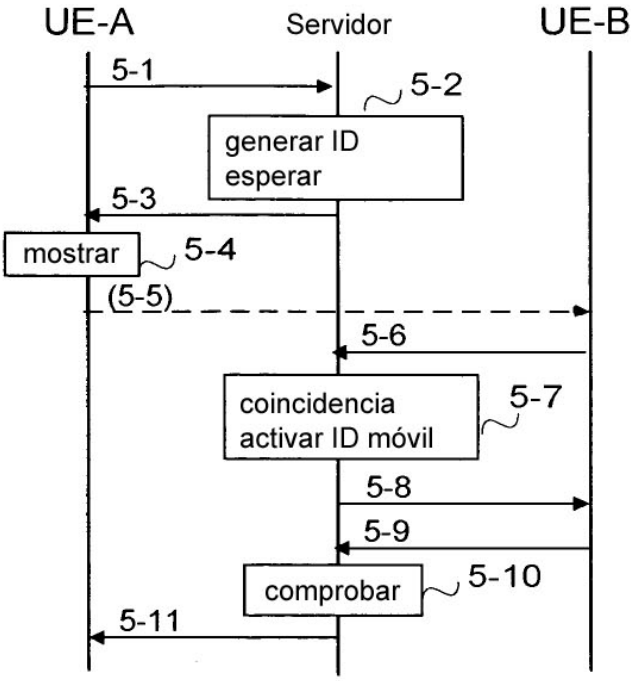
UE-A
Servidor
UE-B
5-1
5-2
generar ID
esperar
5-3
mostrar
5-4
(5-5)
5-6
coincidencia
activar ID móvil
5-7
5-8
5-9
comprobar
5-10
5-11

FIG.5

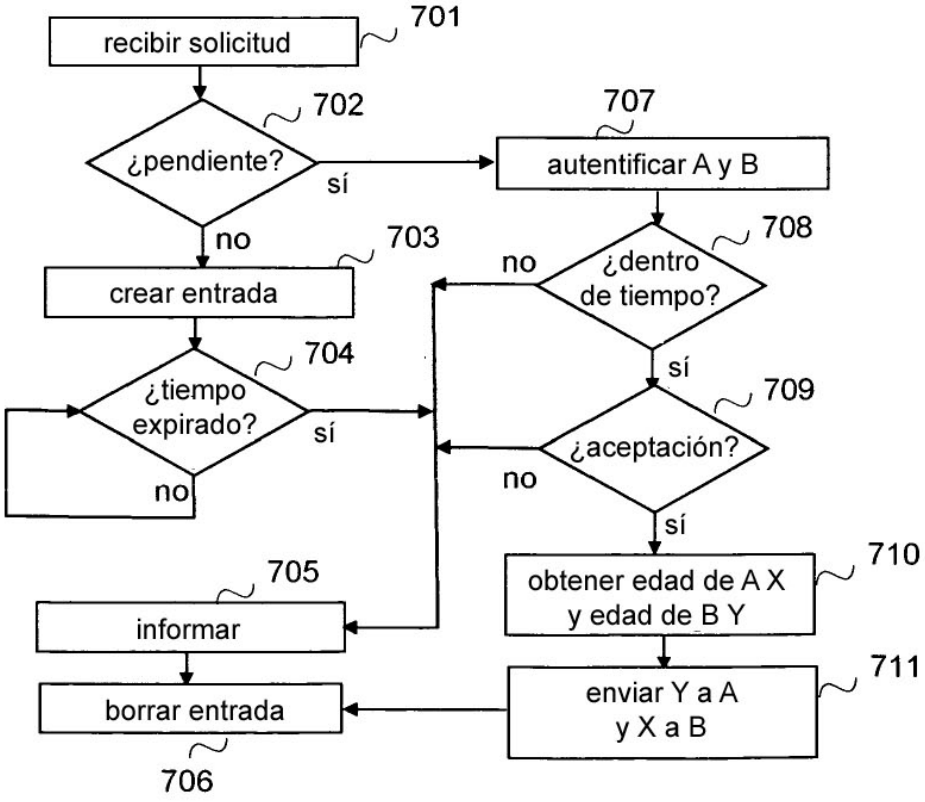
recibir solicitud
701
¿pendiente?
702
sí
no
crear entrada
703
¿tiempo
expirado?
704
sí
no
informar
705
borrar entrada
706
autentificar A y B
707
¿dentro
de tiempo?
708
no
sí
¿aceptación?
709
no
sí
obtener edad de A X
y edad de B Y
710
enviar Y a A
y X a B
711

FIG.7

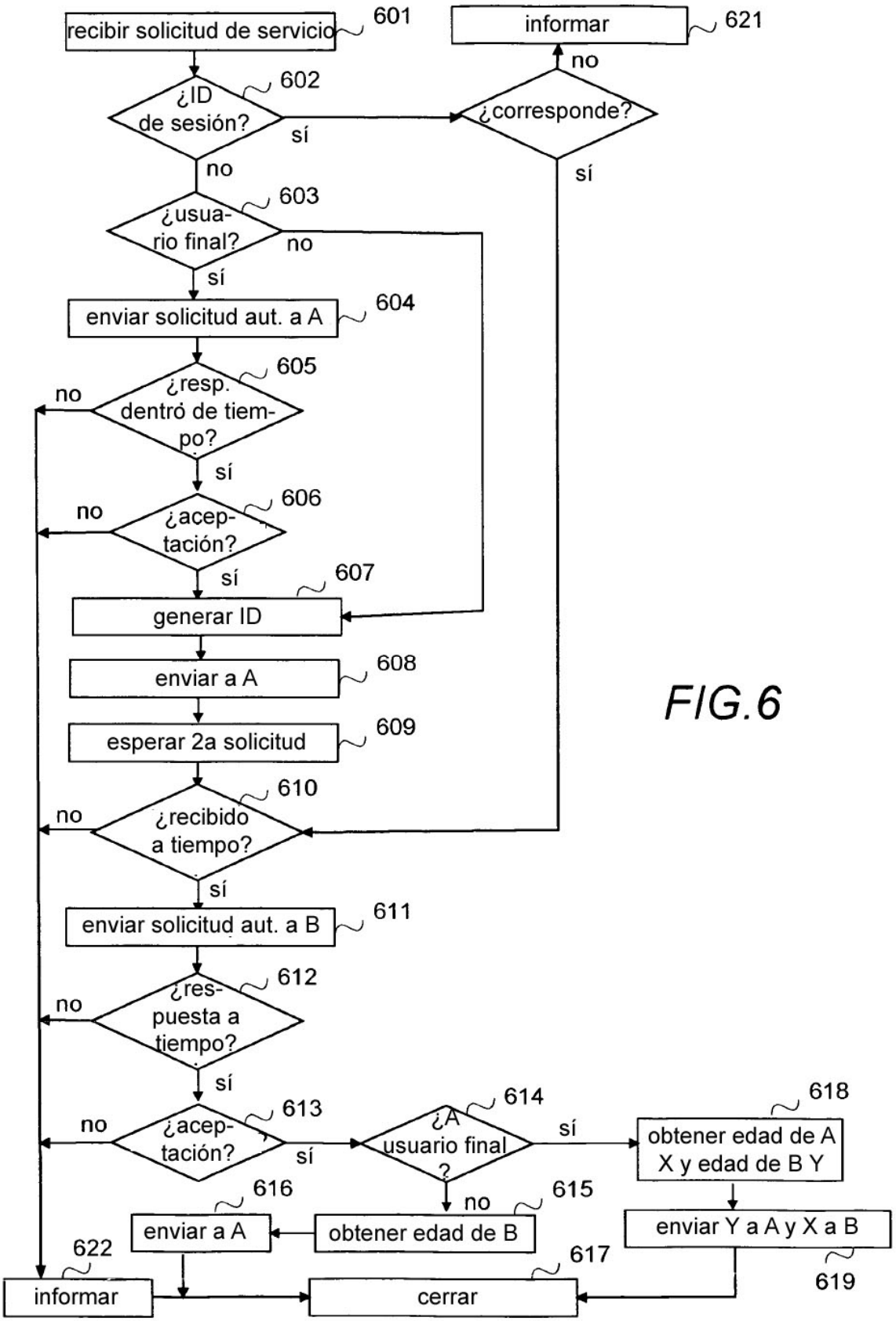
recibir solicitud de servicio
601
¿ID de sesión?
602
sí
no
¿usuario final?
603
no
sí
enviar solicitud aut. a A
604
¿resp. dentró de tiempo?
605
no
sí
¿aceptación?
606
no
sí
generar ID
607
enviar a A
608
esperar 2a solicitud
609
¿recibido a tiempo?
610
no
sí
enviar solicitud aut. a B
611
¿respuesta a tiempo?
612
no
sí
¿aceptación?
613
no
sí
¿A usuario final ?
614
sí
no
obtener edad de B
615
enviar a A
616
informar
622
cerrar
617
obtener edad de A X y edad de B Y
618
enviar Y a A y X a B
619
¿corresponde?
no
sí
informar
621

FIG.6