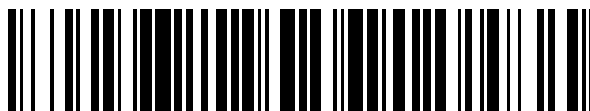


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 393 521**

51 Int. Cl.:

**H04L 29/06** (2006.01)

**H04W 12/08** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **08151937 .3**

96 Fecha de presentación: **26.02.2008**

97 Número de publicación de la solicitud: **2096828**

97 Fecha de publicación de la solicitud: **02.09.2009**

54 Título: **Método y unidad de gestión para gestión de acceso a datos de una red personal**

45 Fecha de publicación de la mención BOPI:

**26.12.2012**

45 Fecha de la publicación del folleto de la patente:

**26.12.2012**

73 Titular/es:

**VODAFONE HOLDING GMBH (100.0%)  
MANNESMANNUFER 2  
40213 DÜSSELDORF, DE**

72 Inventor/es:

**NELISSEN, HANS**

74 Agente/Representante:

**ARPE FERNÁNDEZ, Manuel**

ES 2 393 521 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

Método y unidad de gestión para gestión de acceso a datos de una red personal.

- 5 **[0001]** La presente invención se refiere a un método y a una unidad de gestión para la gestión del acceso a datos de una red personal.
- 10 **[0002]** Internet es usado principalmente para compartir información. Junto con la enorme cantidad de información disponible en Internet llegará a ser cada vez más difícil recuperar fácil y rápidamente la información apropiada. En Internet, la identidad de una persona que accede al servidor y potencialmente se descarga datos desde este, es generalmente de poca importancia. En contraposición en una red personal, la identidad del usuario que intenta acceder a datos podría ser de gran importancia.
- 15 **[0003]** Se conocen servicios, donde los usuarios se subscriben para llegar a ser miembros de una comunidad. La información en relación al usuario, tal como su nombre y dirección de correo electrónico, tendrá que ser proporcionadas por el usuario durante la subscripción y podrán usarse en comunicaciones posteriores dentro de la red personal o comunidad. Una desventaja de esta solución es que la información de la identidad del usuario debe ser introducida manualmente y puede ser manipulada indebidamente.
- 20 **[0004]** Para una conexión entre pares en una red de comunicación móvil la patente KR100623194B1 sugiere un método para compartir datos entre dos terminales móviles. En este método, un usuario de un terminal móvil recibirá una pregunta de autorización para permitir compartir archivos. Si la autorización es concedida, se determina una dirección IP móvil para el terminal móvil por un nodo de la red de comunicación, siendo transmitida al terminal móvil peticionario. Una desventaja de este método es que el intercambio de archivos solo se puede llevar a cabo entre dos terminales móviles. Además, el usuario del terminal móvil desde el que se comparten los datos, no obtendrá información segura del usuario del terminal peticionario.
- 25 **[0005]** Además la patente US 2007/174282 A1, revela un método de control de acceso, un aparato de control de acceso y un producto informático. En este método un aparato cliente manda una petición para recibir un servicio desde un aparato de servicio. Para usuarios no registrados, el aparato de servicio adquiere la meta-información del aparato cliente en cuestión y determina un aparato aprobado a partir de la meta-información adquirida y una petición de aprobación es mostrada en el aparato aprobado. Una desventaja de este método, es que tan solo se refiere a la supervisión del acceso de los aparatos a una red existente. El proceso solo permite al autorizador aprobar o denegar el acceso a un ordenador específico.
- 30 **[0006]** En el documento US 2006/166649 A1 se describe el acceso a la información de directores de un directorio de asistencia. En este método una parte requirente llama a una plataforma de directorio de asistencia y se manda una petición para liberar la información requerida al subscriptor del móvil cuya información ha sido requerida. Por tanto este documento solo se refiere al acceso a las entradas de un directorio que están almacenadas de forma central en un directorio de asistencia. Una desventaja del este método es que no puede ser usado para la gestión del acceso para el acceso a datos en una red personal.
- 35 **[0007]** El problema subyacente en la presente invención es por tanto proporcionar una solución para gestionar el acceso a datos en una red personal de una forma segura.
- 40 **[0008]** La invención está basada en el descubrimiento de que este problema puede ser resuelto mediante la utilización de un identificador único y mejorando el suministro de información a los usuarios.
- 45 **[0009]** De acuerdo con el primer aspecto, el problema es resuelto por un método para gestión de acceso a datos en una red personal, donde una petición de acceso es recibida en una unidad de gestión para la red personal procedente de un dispositivo peticionario de una parte requirente. El método está caracterizado porque la petición de acceso incluye información sobre los datos a consultar, la unidad de gestión extrae el número de módulo de identificación de abonado del dispositivo peticionario como información de identificación de la parte requirente a partir de la petición de acceso, generando una indicación de la parte requirente a partir de la información de identificación extraída y transmitiendo una petición de autorización que incluye la indicación de la parte requirente a un terminal móvil asociada al propietario de los datos a consultar.
- 50 **[0010]** La red personal es preferiblemente una red entre pares. Los dispositivos pares pueden ser cualquier dispositivo electrónico que sea capaz de establecer una conexión a una unidad de red de la red de comunicación. En particular, los dispositivos pares pueden ser ordenadores personales (PC), teléfonos móviles, etc. La conexión entre pares puede también establecerse entre dispositivos pares de diferente naturaleza. Por ejemplo la conexión entre pares puede establecerse entre un teléfono móvil y un PC. La comunicación entre los dispositivos pares puede usar una red de comunicación que podría ser una red de ordenadores, en particular Internet. La red de comunicación podrá, sin embargo, al menos de forma parcial, comprender también una red de telecomunicación, en particular una red de comunicación móvil o una red inalámbrica. La red de telecomunicación puede ser usada como una red de entrada para acceder a Internet. De forma alternativa, la red de telecomunicación podrá ser la red de telecomunicación sobre la que la conexión entre pares está establecida. En la red entre pares los dispositivos pares están en el mismo nivel jerárquico. Esto significa que cada dispositivo en la red suministra funcionalidad y servicios a los otros dispositivos, y utiliza la funcionalidad y los servicios suministrados por los otros. En un medio de este tipo,
- 60 cada usuario puede permitir a otros usuarios acceso a los recursos, tales como discos duros u otros medios de

almacenamiento. Los miembros de la red suministran acceso mutuo a los recursos y por tanto no se suministra un servidor en dichas redes. Para tales redes entre pares la unidad de gestión podría ser proporcionada en la red de comunicación utilizada para comunicación, por ejemplo, Internet o una red de comunicación móvil.

5 **[0011]** De forma alternativa, la red personal puede ser una red establecida con un servidor. Tales redes personales pueden ser cableadas o inalámbricas y podrán, por ejemplo, ser la red doméstica de un usuario. En este caso, la unidad de gestión podrá estar incluida en el servidor de la red.

10 **[0012]** La red personal podrá, sin embargo, ser también una red privada virtual VPN. Estas redes son instaladas utilizando subredes lógicas específicas del cliente dentro de una red de acceso telefónico, tales como ISDN por ejemplo. Una configuración típica para una VPN es el IP VPN (Protocolo de Internet VPN), donde las subredes son conectadas a través de un túnel IP. Una VPN por tanto proporciona una red lógica para un grupo cerrado de usuarios. Ya que la VPN siempre utiliza redes de transmisión públicas, donde el operador público suministra servicios de red, la unidad de gestión podrá estar en este caso incluida en las entidades de red de transmisión pública o de la red del operador público, que es utilizado para instalar una red privada. Preferiblemente, la unidad de gestión podrá ser suministrada dentro o podrá ser conectada a una unidad de identificación o autenticación de la VPN. La VPN podrá hacerse efectiva por una comunicación entre pares.

**[0013]** El acceso a los datos en la red personal que es gestionada por la unidad de gestión podrá ser la mera exploración de los datos disponibles en un dispositivo dentro de una red personal. Preferiblemente, el acceso a los datos, sin embargo incluye la recuperación, tal como la descarga de datos.

20 **[0014]** De acuerdo con la presente invención, los datos a consultar pueden ser contenido, tales como archivos de música o video. Los datos, sin embargo, también pueden ser otros ficheros tales como documentos o datos de información.

**[0015]** La petición de acceso para acceder a los datos en una red personal, incluirá la información de los datos a consultar. La petición podrá ser una petición concreta, donde la parte peticionaria especifica la red personal y posiblemente incluso el dispositivo dentro de la red personal en el que los datos a consultar están almacenados. De forma alternativa, la petición de acceso puede originarse a partir de una petición general no concreta, donde una unidad central identifica la red personal o el dispositivo en donde los datos requeridos están disponibles. En este último caso, la petición de acceso será transmitida a la red personal o al dispositivo a través de la unidad central.

30 **[0016]** En cualquier caso, la petición de acceso incluirá la información de identificación de la parte requirente. La información de identificación de la parte requirente será, preferiblemente, incluida en la petición de acceso de forma automática. De esta forma se puede evitar el fraude. La información de identificación será preferiblemente una identificación única, en particular el número de módulo de identificación de abonado (SIM) de la parte requirente. La información de identificación del usuario podrá ser información almacenada o un Token de usuario en el dispositivo peticionario. La información del usuario podrá ser indicada en la petición de acceso por una variable o un parámetro. Una ventaja en la utilización del número SIM es que la tarjeta SIM podría ser insertada en los dispositivos peticionarios tales como teléfonos móviles y la información almacenada en ella que identificará de forma clara a la parte requirente, estará por tanto disponible en el dispositivo peticionario. Con dispositivos tales como un PC, la información de identificación puede ser también proporcionada por una tarjeta SIM. En este caso, la información almacena en la tarjeta SIM podría ser transmitida al PC mediante la inserción de la tarjeta en el PC o a través de una conexión por cable o inalámbrica de un lector para tarjetas del PC.

40 **[0017]** La petición de acceso puede originarse desde de dentro de la red personal o podría ser recibida desde fuera de la red personal.

**[0018]** La extracción de la información de identificación desde el acceso puede ser leyendo la información a partir de campos predefinidos o etiquetas dentro de la petición. Sin embargo, también puede utilizarse la extracción durante el análisis de la petición de acceso o de otro procedimiento de la petición.

45 **[0019]** La indicación de la parte requirente es, preferiblemente, el nombre de la parte requirente. Adicionalmente, puede ser incluida en la petición la dirección o posición de la parte requirente.

**[0020]** La petición de autorización que es generada por la unidad de gestión, incluirá la indicación de la parte requirente, por ejemplo su nombre, y preferiblemente, también incluirá una descripción de los datos a consultar.

50 **[0021]** Mediante la transmisión de dicha petición de autorización a un propietario de los datos a consultar en el la red personal, el propietario será consciente de la persona que trata de acceder a sus datos. Por tanto, la decisión de permitir o denegar el acceso podrá estar basada en la persona que pide el acceso y posiblemente también en los datos a consultar. De esta forma, se proporciona un nivel de seguridad aumentado, mientras el propietario de la red puede decidir sobre la concesión de la autorización de acceso examinando caso por caso. Mientras algunos datos podrían ser compartidos con una grupo amplio de gente, el propietario de la red personal, podrá, por ejemplo, decidir solo compartir datos sensibles con una número limitado de personas.

55 **[0022]** El propietario de la los datos a consultar es preferiblemente el propietario o el usuario registrado del dispositivo donde los datos a consultar están almacenados. Alternativamente, el propietario de los datos podrá ser el usuario que almaceno los datos en el dispositivo. En este último caso, el dispositivo podrá ser un servidor y los datos en el podrán ser clasificados por usuario.

**[0023]** Mediante la transmisión de la petición de autorización al terminal móvil del propietario de los datos, el propietario siempre estará informado de las peticiones de acceso, incluso si no está usando en ese momento el dispositivo donde están almacenados los datos a consultar.

5 **[0024]** Los dispositivos a utilizar con el método de la invención pueden ser PC, PDA, servidores o terminales móviles, en particular teléfonos móviles. El dispositivo peticionario es preferiblemente un terminal móvil de la parte requirente.

10 **[0025]** De acuerdo con una realización, la unidad de gestión, tras la recepción de una respuesta a la petición de autorización, inicia el suministro del acceso requerido al dispositivo peticionario y/o inicia la transmisión de una notificación al terminal móvil que está vinculado a la información de identificación extraída. El suministro de la petición de acceso al dispositivo peticionario, podrá ser iniciado mediante el envío de una señal de conformación al dispositivo, donde están almacenados los datos requeridos. Esta confirmación será enviada, sí el propietario de los datos permite el acceso a los datos a la parte requirente. La confirmación podrá resultar en que los datos son accesibles, por ejemplo visibles, descargables etc. para la parte requirente. La confirmación podría también resultar en la descarga inmediata de los datos al dispositivo requirente.

15 **[0026]** Si por el contrario, el propietario de los datos deniega el acceso a los datos a la parte requirente, la unidad de gestión transmitirá un mensaje al terminal móvil que está vinculado con la información de identificación que ha sido extraída de la petición original. Preferiblemente, la información de identificación es un número SIM del terminal móvil de la parte peticionaria. De esta forma la unidad de gestión puede transmitir fácilmente y de forma fiable un mensaje al terminal móvil de la parte requirente. La parte requirente puede así ser informada que la petición acceso a los  
20 datos ha sido denegada. Como el mensaje será enviado por la unidad de gestión, la identidad del propietario de los datos no tendrá que ser revelada a la parte requirente.

25 **[0027]** Preferiblemente, la indicación de la parte requirente, que está incluida en la petición de autorización al propietario de los datos, es determinada a partir de la información de identificación extraída. La indicación puede ser generada por la unidad de gestión o puede ser recuperada a partir de los datos almacenados en la unidad de gestión o en una base de datos. Cuando la información de la identificación es un número SIM del terminal móvil de la parte requirente, la indicación, tal como el nombre de la parte requirente podrá ser recuperada de la base de datos de la red de comunicación móvil, en particular de una base de datos del operador de esta red. Este proceso asegura que el usuario correcto será indicado como la parte requirente al propietario de los datos.

30 **[0028]** De acuerdo con una realización preferida, la unidad de gestión determina el propietario de los datos. Esta determinación puede ser realizada a partir de una información almacenada en la unidad de gestión y/o en el dispositivo donde están almacenados los datos a consultar. Para datos almacenados en un servidor, por ejemplo, el usuario que almacena los datos podrá ser determinado como el propietario de los datos. Un vez que la persona que ostenta los datos ha sido identificada, la unidad de gestión podrá buscar o recuperar el número SIM o el número de terminal móvil del propietario en una base de datos respectiva, para contactar al propietario a través de su terminal  
35 móvil. Mediante la determinación del propietario de los datos y la correlación del propietario a un número SIM O MSISDN, será posible transmitir la petición de autorización al terminal móvil del propietario. La posibilidad de que el propietario tenga su terminal móvil disponible es más alta que la posibilidad de que el usuario esté usando el dispositivo concreto desde el que los datos van a ser descargados o consultados de diferente manera. Por tanto se podrá asegurar que el propietario será informado de la petición de autorización rápidamente.

40 **[0029]** Preferiblemente, el terminal móvil del propietario, a donde es transmitida la petición de autorización, es diferente del dispositivo donde están almacenados los datos a consultar. Mediante el envío de la petición de autorización a un dispositivo diferente al dispositivo en el que realmente están almacenados los datos, el nivel de seguridad se puede aumentar más. Además, la flexibilidad del método de la invención es aumentada, ya que la gestión de los accesos a los datos no está limitada al dispositivo donde los datos están realmente almacenados. Por  
45 tanto, el método de la invención puede ser usado de forma fiable para gestionar una red personal completa.

**[0030]** De acuerdo con un aspecto adicional de la invención, el problema se resuelve mediante una unidad de gestión para gestión del acceso a los datos de una red personal de acuerdo con la reivindicación 7.

50 **[0031]** La unidad de generación está preferiblemente conectada a una base de datos donde la información de identificación está correlacionada con el nombre u otras especificaciones de la parte requirente. Esta base de datos podría ser la base de datos del operador de una red de comunicación móvil. En este caso, la información de identificación es preferiblemente el número SIM de la parte requirente, por ejemplo del usuario del dispositivo peticionario. De acuerdo con una realización, la conexión de la unidad de gestión a la base de datos es una conexión de comunicación remota. En este caso, unidad de gestión podrá, por ejemplo, estar incluida en un dispositivo de la red personal doméstica de un usuario. La unidad de gestión puede entonces comunicarse con la  
55 base de datos donde las indicaciones de identificación están vinculadas a la información del respectivo usuario, tal como su nombre.

60 **[0032]** Mediante el suministro de un interfaz de comunicación en la unidad de gestión para la comunicación con el terminal móvil, la unidad de comunicación puede comunicarse con el propietario de los datos a consultar y/o con la parte requirente. De este modo, se suministra una distribución de información mejorada que aumenta el nivel de seguridad así como la flexibilidad de la gestión de acceso a los datos en una red personal.

**[0033]** De acuerdo con una realización preferida, la unidad de gestión además comprende una unidad de determinación, para determinar el propietario de los datos a los que se refiere la solicitud de acceso. La unidad de determinación preferiblemente determina el propietario mediante la información de identificación tal como el número SIM de un terminal móvil del propietario.

5 **[0034]** De acuerdo con una realización, la unidad de gestión es parte de una red personal. En este caso la unidad de gestión podrá ser implementada, al menos de forma parcial, en un dispositivo que pertenezca a la red personal. Este dispositivo podrá ser el dispositivo donde están almacenados los datos a consultar o podrá ser una unidad de procesamiento central de la red personal. De forma alternativa, la unidad de gestión está incluida, al menos de forma parcial, en una unidad de conexión utilizada para la conexión entre el dispositivo requirente y la red personal. En este último caso, la unidad de gestión podrá por ejemplo estar implementada o incluida en un servidor en la red del operador de una red de comunicación móvil. Esta realización es ventajosa, ya que el servidor tendrá acceso a la base de datos donde están almacenados la correlación de un número SIM y el nombre de abonado. Además, será fácil para unidad de gestión transmitir mensajes, tales como la petición de autorización y/o el mensaje de rechazo de la autorización al terminal móvil del propietario y/o de la parte requirente.

15 **[0035]** La unidad de gestión podrá hacerse efectiva como un hardware y/o un software. Las unidades podrán también combinarse al menos de forma parcial.

**[0036]** La unidad de gestión esta preferiblemente diseñada, por ejemplo comprendiendo medios para ser usadas en el método de la invención.

20 **[0037]** Las características y ventajas que son descritas con referencia al método de la invención también se aplican la unidad de gestión de la invención y viceversa.

**[0038]** La presente invención será ahora descrita en detalla con referencia a las figuras adjuntas, donde:

La figura 1 muestra una vista esquemática de una primera realización de una instalación del método de la invención; y

La figura 2 muestra una vista esquemática de una segunda realización de la instalación del método de la invención.

25 **[0039]** En la figura 1 un dispositivo peticionario par 11 es mostrado como un ordenador portátil pero podrá ser cualquier tipo de dispositivo par tal como un PC, un equipo terminal móvil etc. Este dispositivo par 11 puede comunicarse con otros dispositivos pares 12, 13 a través de Internet. Los dispositivos pares 12,13 son parte de una red personal 6. En la instalación representada la red personal podría ser una VPN establecida a través de Internet. El segundo dispositivo par 12 que se muestra en la figura 1 también siendo un PC. También este dispositivo par 30 podría ser, sin embargo, cualquier otro tipo de dispositivo par tal como un PC o un equipo terminal móvil. Los datos 2 están almacenados en el segundo dispositivo par 12. Los datos 2 pueden estar almacenados en medios de almacenamiento, tales como discos duros del ordenador o una base de datos conectada al ordenador. Además en la figura 1, se muestra una unidad de gestión 3. Esta unidad de gestión 3 está conectada a o puede tener acceso a la base de datos 4, preferiblemente a la base de datos del proveedor u operador de la red de comunicación móvil En esta base de datos 4, está almacenada la información relativa a los módulos de identificación de los abonados del red móvil, en particular SIM. Esta información comprende el número SIM así como el nombre y posiblemente información adicional del abonado.

35 **[0040]** La unidad de gestión 3, puede comunicarse con los terminales móviles 51, 52 de la red de comunicación móvil, en particular teléfonos móviles. Esta comunicación es preferiblemente una comunicación de datos más que una comunicación de voz.

40 **[0041]** En una primera utilización se asume que el usuario A es el usuario del dispositivo par 11 y que quiere acceder a los datos del dispositivo par 12 del Usuario B. El usuario A desearía, por ejemplo, descargar datos tales como música. Para acceder a los datos en el dispositivo par 12, una petición de acceso respectiva es enviada desde el dispositivo par 11 del usuario A a través de Internet. La petición de acceso del usuario A puede ser entregada al usuario B de forma específica. Es, sin embargo, también posible que esta petición sea enviada/encaminada de acuerdo con ajustes de de ruta y filtrado.

45 **[0042]** Durante la transmisión de la petición de acceso, la petición es reenviada a la unidad de gestión 3. Tras la recepción de la petición de acceso, la unidad de gestión 3 extrae la información de identificación del remitente de la petición de acceso. Esta información podrá haber sido incluida en la petición por el dispositivo par 11, utilizando la información almacena en él. Tras la extracción de la información de identificación, en particular del número SIM del terminal móvil 51 del usuario A, la unidad de gestión 3 lleva a cabo una búsqueda en la base de datos 4 de la red de comunicación móvil. De este modo, el nombre y otra información, tal como la dirección del remitente de la petición, a saber la parte requirente puede ser determinada.

50 **[0043]** Con esta información disponible, la unidad de gestión 3 genera una petición de autorización. El destinatario de la petición de autorización es el propietario de los datos a consultar. En el presente ejemplo el propietario de los datos es el usuario B. Para transmitir la petición de autorización al usuario B, la unidad de gestión 3 podrá realizar otra búsqueda en la base de datos 4 y determinar el número SIM del terminal móvil del usuario B. De forma alternativa, el número SIM del usuario B, podrá estar almacenada en el dispositivo par 12 o en la unidad de gestión 3.

**[0044]** La petición de autorización así generada, será entonces enviada al equipo terminal móvil 52 del usuario B. La petición podrá incluir opciones de selección para aceptar o rechazar la petición.

5 **[0045]** Si el usuario B concede permiso al usuario A para acceder a los datos de su red personal, esto se realizará mediante el envío de una señal respectiva desde el terminal móvil 52 a la unidad de gestión 3. La señal de respuesta podrá ser generada, por ejemplo, si el usuario B selecciona y pulsa un "botón SI" dentro de la petición de autorización recibida. Tras la recepción del permiso, la unidad de gestión 3 iniciará el suministro del acceso. Esto podrá llevarse a cabo mediante el envío de una señal respectiva al dispositivo par 12 de usuario B. Si el usuario B rechaza la petición de acceso, a saber, presionado un "botón NO" dentro de la petición de acceso recibida, la unidad de gestión 3 mandará una mensaje respectivo al terminal móvil 51 del usuario A.

10 **[0046]** De este modo, el usuario A estará informado de cualquier petición iniciada desde su dispositivo par 11 pero rechazada por el otro usuario B.

**[0047]** Además, el usuario B será informado y tendrá la oportunidad de aceptar o rechazar una petición acceso para el acceso a su red personal.

15 **[0048]** En la instalación mostrada en la figura 1 el dispositivo requirente 11 y el terminal móvil 51 del usuario A y el dispositivo par 12 y el terminal móvil 52 del usuario B, son respectivamente diferentes dispositivos.

20 **[0049]** En la figura 2 por el contrario, el dispositivo peticionario par 11 y el terminal móvil 51 del usuario A son el mismo dispositivo. En esta instalación, el usuario A podrá emitir una petición de acceso desde su terminal móvil 51 como su dispositivo par 11. Esta petición será recibida por la unidad de gestión 3. La transmisión a la unidad de gestión 3, podrá realizarse a través de Internet o a través de una red de comunicación móvil. En esta realización, la unidad de gestión 3, gestiona varios dispositivos 12, 12' y 12" del usuario B. La unidad de gestión 3 podrá ser un servidor de una red doméstica o un servidor en Internet. Tras la recepción de la petición de acceso, la unidad de gestión 3, extraerá el número SIM del usuario A a partir de la petición. El número SIM será utilizado por la unidad de gestión para buscar el nombre e información adicional del usuario A en la base de datos 4. Con la información así recuperada, será generada una petición de autorización en la unidad de gestión 3. Además, la unidad de gestión 3  
25 determinará el propietario de los datos, para los que el usuario A ha pedido acceso. La información del propietario de los datos puede ser usada para determinar la SIM del usuario B. La petición de autorización será entonces mandada al terminal móvil 52 del usuario B. Si el usuario B acepta la petición de autorización, una señal respectiva será retransmitida a la unidad de gestión 3. De este modo será suministrado el acceso desde el equipo terminal móvil 51 al dispositivo 12, 12' y 12" donde están almacenados los datos requeridos.

30 **[0050]** Si el usuario B deniega el acceso, la unidad de gestión 3 también recibirá una señal respectiva. Tras la recepción de dicha señal, la unidad de gestión 3 generará y transmitirá un mensaje al terminal móvil 51 del usuario A, informándole de la denegación de su petición de acceso.

35 **[0051]** Con la presente invención será posible mantener comunicaciones de comunidad, tales como un sitio web entre pares semántico inteligente para comunidades, incluyendo redes familiares o de amigos. Será posible en particular obtener información de la persona que trata de acceder a tus datos. Esto se lleva a cabo mediante el posicionamiento de terminales móviles y de la SIM del usuario en el centro de la comunicación entre pares a través de Internet móvil o fijo.

**REIVINDICACIONES**

1. Método para gestión de acceso a datos en una red personal (6), donde una petición de acceso es recibida en una unidad de gestión (3) para la red personal (6) procedente de un dispositivo petionario (11,51) de una parte requirente, caracterizado porque la petición de acceso incluye información sobre los datos a consultar, la unidad de gestión (3) extrae el número de módulo de identificación de abonado del dispositivo petionario (11,51) como información de identificación de la parte requirente a partir de la petición de acceso, genera un indicación de la parte requirente a partir de la información de identificación extraída y transmite una petición de autorización que incluye la indicación de la parte requirente a un equipo terminal móvil (52) asociada al propietario de los datos (2) a consultar.
2. Método de acuerdo con la reivindicación 1, caracterizado porque la unidad de gestión (3) tras la recepción de una respuesta a la petición de autorización, inicia el suministro del acceso requerido al dispositivo petionario (11,51) y/o inicia la transmisión de una notificación al equipo terminal móvil (51) que está vinculado a la información de identificación extraída.
3. Método de acuerdo con las reivindicaciones 1 o 2, caracterizado porque la indicación de la parte requirente es determinada a partir de la información de identificación extraída.
4. Método de acuerdo con las reivindicaciones 1 a 3, caracterizado porque la unidad de gestión (3) determina el propietario de los datos (2) en la red personal (6).
5. Método de acuerdo la cualquiera de las reivindicaciones de 1 a 4, caracterizado porque el suministro de acceso a los datos (2) consiste en la transmisión de los datos (2) al dispositivo petionario (11, 51).
6. Método de acuerdo la cualquiera de las reivindicaciones de 1 a 5, caracterizado porque el terminal móvil (52) del propietario de los datos (2) es diferente del dispositivo (12, 13) en el que se almacenan los datos (2) a consultar.
7. Unidad de gestión para gestión del acceso a datos en una red personal caracterizada porque la unidad de gestión (3) comprende una unidad de recepción para recibir una petición de acceso que incluye información sobre los datos a consultar, una unidad de extracción para extraer el número de módulo de identificación de abonado del dispositivo petionario (11, 51) como información de identificación a partir de la petición de acceso, una unidad de generación para generar una indicación de la parte requirente a partir de la información de identificación extraída y una interfaz de comunicación para transmitir al equipo terminal móvil (52) del propietario de los datos (2) a consultar, una petición de autorización que incluye la indicación de la parte requirente.
8. Unidad de gestión de acuerdo con la reivindicación 7, caracterizada porque además comprende una conexión a una base de datos (4) para la recuperación de información relativa a la indicación de la identificación.
9. Unidad de gestión de acuerdo con las reivindicaciones 7 o 8, caracterizada porque comprende una unidad de determinación, para determinar el propietario de los datos (2) cuyo acceso es requerido.
10. Unidad de gestión de acuerdo con la reivindicación 7, caracterizada porque dicha unidad de gestión (3) es parte de una red personal (6).
11. Unidad de gestión de acuerdo con las reivindicaciones 7 a 9, caracterizada porque la unidad de gestión (3) es incluida, al menos de forma parcial, en una unidad de conexión utilizada para la conexión entre el dispositivo petionario (11,51) y la red personal (6).

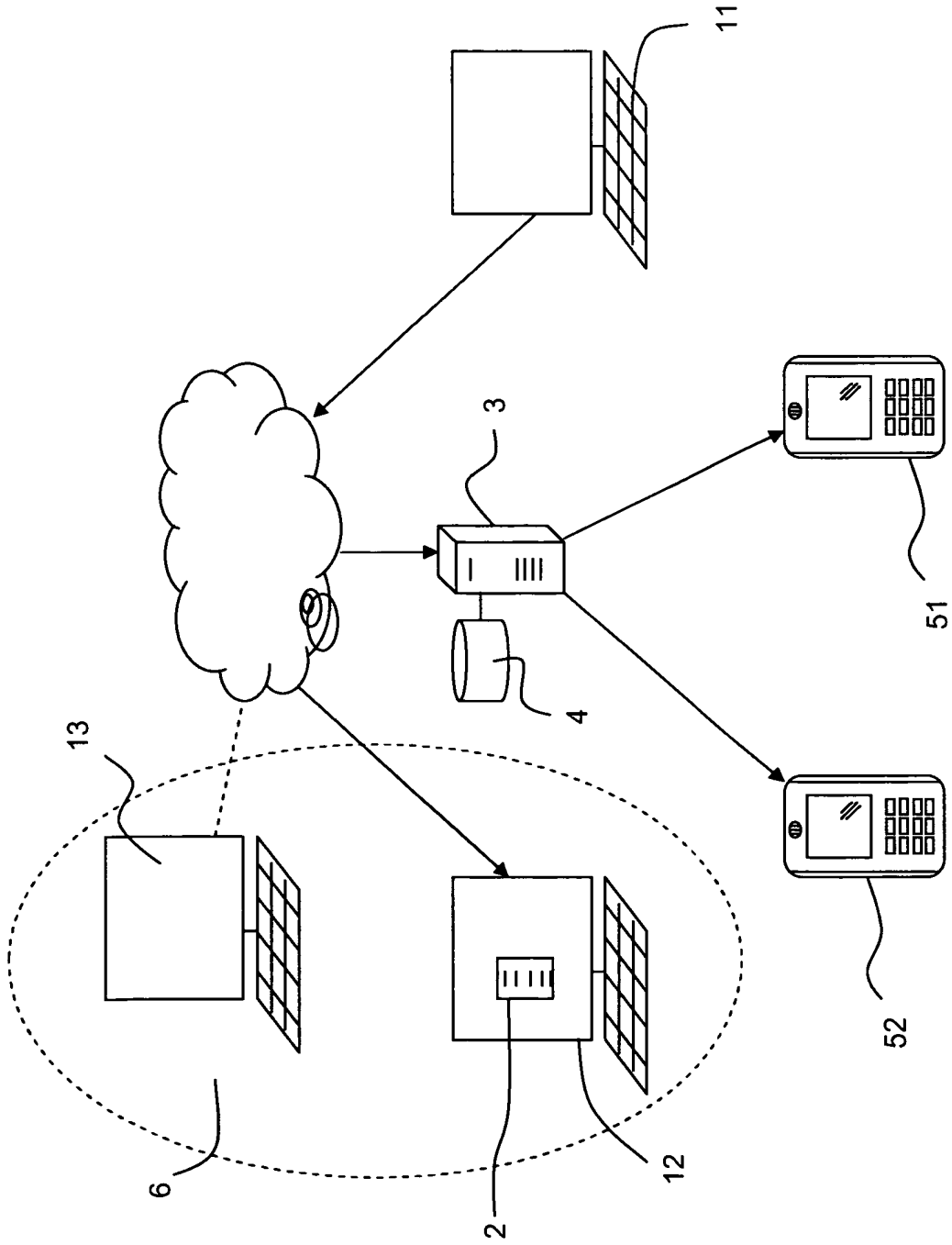


FIG. 1



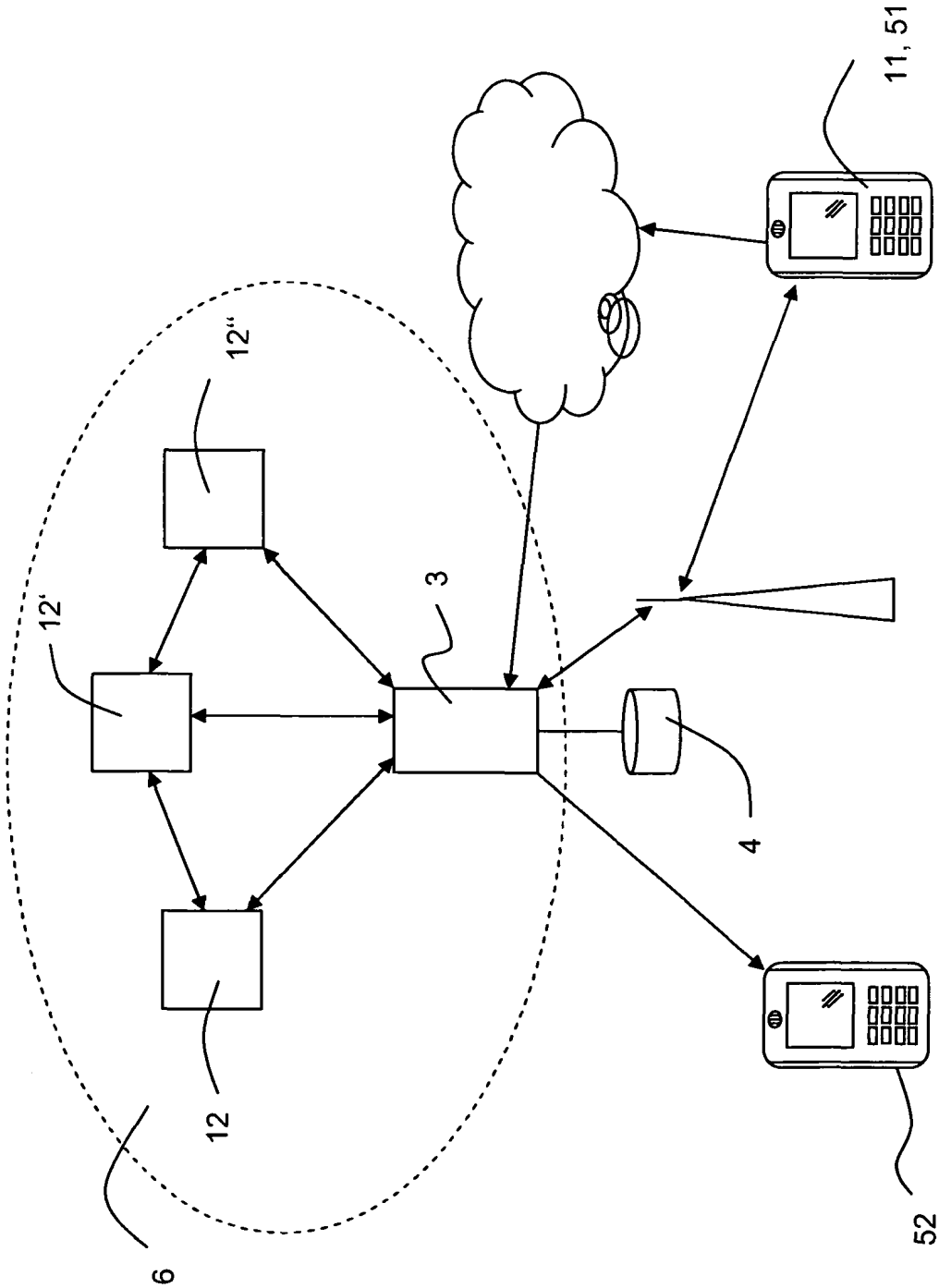


FIG. 2

**REFERENCIAS CITADAS EN LA DESCRIPCIÓN**

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden 5 excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

**Documentos de patente citados en la descripción**

- KR 100623194 B1 [0004]
- US 2006166649 A1 [0006]
- US 2007174282 A1 [0005]