

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 703 011**

51 Int. Cl.:

H04W 12/06 (2009.01)
H04W 12/08 (2009.01)
H04W 12/02 (2009.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
H04N 1/44 (2006.01)
H04W 88/02 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **18.03.2009 PCT/EP2009/053200**
- 87 Fecha y número de publicación internacional: **24.09.2009 WO09115552**
- 96 Fecha de presentación y número de la solicitud europea: **18.03.2009 E 09721414 (2)**
- 97 Fecha y número de publicación de la concesión europea: **07.11.2018 EP 2266276**

54 Título: **Gestión de identidades de usuarios en un sistema**

30 Prioridad:

18.03.2008 FR 0851754

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
06.03.2019

73 Titular/es:

AIRBUS DS SAS (100.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean
Moulin
78990 Elancourt, FR

72 Inventor/es:

ROUSSEAU, FRÉDÉRIC y
ELOY, STÉPHANE

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 703 011 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

Gestión de identidades de usuarios en un sistema

La presente invención se refiere a la gestión de una identidad de usuario para un terminal electrónico y, más en particular, a la asociación temporal de una identidad de usuario con un terminal de un sistema.

5 Ciertos sistemas ofrecen servicios a usuarios en función de las respectivas identidades de estos usuarios. De este modo, un usuario, cuando, por intermedio de un terminal del sistema, pretende acceder a un servicio con el que, por ejemplo, ha contratado una suscripción, asocia a este terminal del sistema una entidad de identificación a partir de la cual su identidad de usuario es accesible. Tal entidad de identificación puede ser, por ejemplo, un lector de identidad o un soporte de memorización de identidad tal como un carnet de identidad, o una tarjeta de pago o una tarjeta de suscripción a un servicio personalizado por perfil, por ejemplo una tarjeta UICC/USIM (por 'Universal Integrated Circuit Card / Universal Subscriber Identity Module') dentro del contexto de las redes GSM o 3GPP. En el ejemplo relativo a la red GSM que utiliza una entidad de identificación conforme al estándar ISO/IEC 7816, esta última y el terminal están en contacto físico ya que, y aun siendo amovible, esta entidad de identificación se mantiene por lo general en el interior de la caja del terminal. Consecuentemente, cuando el terminal es sustraído, el ladrón puede usurpar la identidad del abonado, ya que, al sustraer el terminal, ha recuperado simultáneamente la entidad de identificación utilizada por este abonado.

Se puede prever, alternativamente, que la interfaz entre el terminal y la entidad de identificación sea una interfaz electromagnética, tal como una interfaz radio sin contacto. Con una interfaz de este tipo, el terminal y la entidad de identificación no están conectados físicamente. Se ve mejorado entonces el nivel de seguridad del mismo, pues, con un robo de terminal, no necesariamente es robada la entidad de identificación.

No obstante, cualquiera que sea el tipo de interfaz utilizada, conviene señalar que se requiere que el terminal y la entidad de identificación estén enlazados durante todo el periodo de utilización del servicio de comunicación de que se trate.

Así puede suceder, por ejemplo, para una transacción económica. En este caso, si, en el transcurso de la transacción económica, la interfaz entre la entidad de identificación y el terminal se detecta como interrumpida, toda la transacción debe ser repetida desde el principio.

De este modo, cuando la interfaz es una interfaz electromagnética, se requiere que la distancia que separa la entidad de identificación y el terminal sea lo suficientemente pequeña como para sobrepasar un umbral de calidad mínima de la interfaz electromagnética, por debajo de la cual se interrumpiría la transacción entre la entidad de identificación y el terminal. Esta distancia umbral es dependiente de la norma puesta en práctica en esta interfaz. En efecto, son conocidas, por ejemplo, las normas de interfaz de proximidad ISO/IEC 14443, ISO/IEC 18092 e ISO/IEC 21481 (ISO/IEC por 'International Organisation for Standardization') que requieren que la distancia entre la entidad de identificación y el terminal sea del orden de unos centímetros como máximo, mientras que otras normas, tal como la norma de interfaz de vecindad ISO/IEC 15693, toleran distancias del orden de varios decímetros.

De este modo, utilizando una interfaz electromagnética entre la entidad de identificación y el terminal, se puede precaverse de una usurpación de identidad, pero pueden producirse cortes de servicio a la ruptura de la interfaz entre el terminal y la entidad de identificación.

Ahora bien, en ciertos ámbitos, puede ser desventajoso padecer la interrupción del servicio a partir del instante en que se rompe la interfaz entre el terminal y la entidad de identificación. Tal es el caso, en especial, para comunicaciones vitales, puestas en práctica, por ejemplo, por profesionales de fuerzas de seguridad y de rescate.

El estado de la técnica anterior se conoce por los documentos US 2006/0288407 A1 y GB 2408180 A.

La presente invención viene a mejorar la situación. La invención queda definida en las reivindicaciones independientes.

Un primer aspecto de la presente invención propone un procedimiento de asociación de una identidad de usuario con un terminal electrónico adaptado para ofrecer un servicio sustentado en dicha identidad de usuario;

comprendiendo dicho procedimiento de asociación, en el terminal, las siguientes etapas:

/1/ establecer una transacción sin contacto con una entidad de identificación;

/2/ recibir, en el transcurso de dicha transacción, una información relativa a una identidad de usuario almacenada en dicha entidad de identificación; y

50 /3/ almacenar dicha identidad de usuario obtenida a partir de dicha información;

en el que la identidad de usuario es borrada en el terminal cuando se somete dicho terminal a una acción específica.

De este modo, el terminal está en condiciones de recuperar y de almacenar, de manera sencilla, una identidad de usuario desde una entidad de identificación, almacenándose de manera temporal en el terminal esta identidad de usuario, ya que es borrada cuando se somete el terminal a una cierta acción.

5 Tal acción específica puede corresponderse especialmente con el apagado del terminal o también con cualquier acción de usuario sobre el terminal, o bien una acción puesta en práctica por una aplicación embarcada en el terminal, como por ejemplo la incidencia de un acontecimiento interno al terminal (por ejemplo, el vencimiento de una temporización o de un contador de fallos).

10 Merced a tales disposiciones, es posible garantizar una continuidad en el servicio al que tiene acceso el usuario, al propio tiempo que se mantiene un elevado nivel de seguridad contra la usurpación de la identidad del usuario. En efecto, por una parte, si al usuario le es sustraído el terminal, al no estar la entidad de identificación ligada físicamente al terminal, ésta no es sustraída también obligatoriamente. Por otra parte, no se requiere que la transacción entre el terminal y la entidad de identificación esté en desarrollo para que el terminal pueda ofrecer el servicio sustentado en la identidad de usuario, ya que esta identidad de usuario se almacena en el terminal.

15 Adicionalmente, el almacenamiento de esta identidad de usuario es temporal. A tal efecto, se prevé ventajosamente borrar esta identidad de usuario bajo una acción aplicada al terminal. Esta acción puede ser aplicada, bien por un usuario, o incluso también por una aplicación embarcada en el terminal.

Una vez que se establece la transacción sin contacto entre el terminal y la entidad de identificación, la identidad se puede transmitir entonces desde esta entidad hacia el terminal. En ese instante, la identidad se puede almacenar en el terminal con el fin de permitir al usuario acceder al servicio que le interese.

20 De este modo, la interfaz sin contacto entre el terminal y la entidad de identificación no sólo permite evitar una usurpación de identidad del usuario, sino que, además, no requiere que la transacción entre el terminal y la entidad de identificación permanezca establecida a lo largo de toda la utilización del servicio de que se trate.

25 Por lo tanto, basta con que el terminal y la entidad de identificación puedan comunicarse unos momentos solamente para que el terminal pueda recibir la identidad de usuario y, a continuación, basándose en ello, disfrutar de un servicio.

Ventajosamente, tal procedimiento según una forma de realización de la presente invención permite obtener la identidad de usuario rápidamente y con independencia de otras transacciones ulteriores efectuadas por el terminal.

Conviene señalar que la desaparición, la retirada o la ausencia de entidad de identificación puede no traer consigo consecuencias sobre las ulteriores comunicaciones o transacciones del terminal.

30 En estas condiciones, la gestión de la protección de las operaciones, comunicaciones o también transacciones del terminal puede no dejar de ser independiente de la gestión de la protección de los intercambios entre el terminal y la entidad de identificación de usuario.

35 Tal característica es una ventaja perseguida en el contexto de los sistemas de comunicaciones vitales profesionales, especialmente porque el robo del terminal que se está utilizando no trae consigo el robo de la entidad de identificación, en contra de lo que ocurre en el caso de un terminal adaptado para una red de tipo GSM o 3GPP. Adicionalmente, una vez obtenida la identidad de usuario y almacenada en el terminal, este último puede efectuar multitud de operaciones sin precisar de una nueva transacción con la entidad de identificación, hasta que se ponga en práctica una acción específica que borre la identidad de usuario, el apagado del terminal, o bien, en el caso en que se pone en práctica una operativa de detección de presencia de la entidad de identificación (o 'watch dog'), hasta el borrado de la identidad de usuario en el terminal.

40 Al poner en práctica un procedimiento de asociación según una forma de realización de la presente invención, ventajosamente se puede suprimir la gestión de una contraseña o código PIN (por 'Personal Identification Number' en inglés) como ocurre especialmente para desbloquear el uso del teclado de un terminal adaptado para las redes de comunicaciones de tipo GSM o UMTS.

45 Ventajosamente, la puesta en práctica de un procedimiento de asociación según una forma de realización de la presente invención está perfectamente adaptada a una utilización de terminal no individualizada, es decir, a la utilización de un terminal por diferentes usuarios sucesivos.

50 Cabe prever que el usuario pueda efectuar una manipulación arbitraria del terminal que permita borrar la identidad de usuario almacenada en el terminal antes de dejar de utilizarlo. El apagado del terminal, en especial, puede permitir este borrado voluntario de la identidad de usuario almacenada.

Se puede adicionalmente proporcionar una función específica de borrado en un menú del terminal, por intermedio de una aplicación embarcada en el terminal, o también ordenar el borrado de esta identidad de usuario mediante la pulsación sobre una o varias teclas del teclado del terminal.

El terminal, no está operativo, es decir, no puede ofrecer el servicio sustentado en una identidad, mientras no cuente con esta identidad de usuario. El terminal puede, antes de obtener una identidad de usuario, operar con otra identidad propia del terminal. Esta identidad de terminal puede ser, por ejemplo, un número de serie del terminal.

5 El servicio ofrecido en el terminal puede ser un servicio local del terminal o también un servicio ofrecido por intermedio de una red de comunicación. Un servicio local puede corresponder, por ejemplo, a un control de documento de identidad efectuado mediante exploración de un documento de identidad en el terminal según una forma de realización de la presente invención. La identidad de usuario se puede utilizar entonces para autorizar o prohibir la utilización del terminal de que se trate basándose en una lista de identificadores de usuario que está almacenada localmente en el terminal. Cabe prever adicionalmente que la entidad de identificación almacene, aparte de la información relativa a la identidad de usuario, un perfil de usuario, o perfil de abonado, que se transmite al terminal para adaptar el servicio o los servicios ofrecidos por el terminal al usuario. La presente invención queda descrita en la presente memoria en su aplicación a una identidad de usuario, pero en absoluto queda limitada a esta sola identidad de usuario. En efecto, es sencillo prever tener en cuenta, en asociación con una identidad de usuario, otras informaciones, tales como parámetros individuales como un número de guía, o un perfil de usuario, o también un elemento de seguridad, como por ejemplo una clave de inicialización ('ignition key' en inglés) o un certificado de seguridad, o una combinación de ellos.

En una forma de realización de la presente invención, la información relativa a la identidad de usuario es la propia identidad de usuario. De este modo, en este caso, la identidad de usuario puede ser recuperada directamente a partir de la entidad de identificación.

20 En una forma de realización de la presente invención, se prevé que el terminal está adaptado para comunicarse en una red de comunicación. Se puede prever entonces que una asociación entre la información relativa a una identidad de usuario y la identidad de usuario esté gestionada en esta red de comunicación, y el terminal obtiene la identidad de usuario en la etapa /3/, según las siguientes etapas:

/i/ proporcionar a la red de comunicación la información relativa a una identidad de usuario; y

25 /ii/ recibir desde la red de comunicación dicha identidad de usuario.

En este punto, la identidad de usuario no está almacenada directamente en la entidad de identificación, almacenando esta última solamente una información a partir de la cual es posible obtener esta identidad de usuario. El nivel de seguridad contra una usurpación de identidad de usuario se ve mejorado.

Cabe prever que el procedimiento comprenda además las siguientes etapas:

30 /4/ determinar si la entidad de identificación está situada en la proximidad del terminal;

/5/ repetir la etapa /4/ N veces, siendo N un número entero;

/6/ decidir borrar la identidad de usuario en el terminal si se determina N veces consecutivas que la entidad de identificación no está situada en la proximidad del terminal.

35 La distancia entre el terminal y la entidad de identificación requerida para detectar en el terminal la presencia de la entidad de identificación es función del protocolo de intercambio de mensajes utilizado.

40 Tal forma de realización de la presente invención permite incrementar aún más el nivel de seguridad de la identidad de usuario, ya que esta identidad de usuario es borrada del terminal si este último detecta varias veces consecutivamente que la entidad de identificación no se halla presente en la vecindad. En efecto, varias detecciones de este tipo pueden infundir serias sospechas de que el usuario real del terminal no es quien dice ser, ya que no parece poseer la entidad de identificación correspondiente.

No se vincula limitación alguna a la presente invención en cuanto a los mensajes intercambiados entre el terminal y la entidad de identificación o también entre el terminal y la red de comunicación. De este modo, en especial, tal detección de presencia de entidad de identificación en la vecindad de un terminal puede ser llevada a la práctica según cualquier protocolo.

45 Cabe prever especialmente que la comunicación radio entre el terminal y la entidad de identificación encaminada a proporcionar al terminal la información relativa a la identidad de usuario sea de tipo NFC (por 'Near Field Communication' en inglés), como por ejemplo las normas de interfaces de proximidad ISO/IEC 14443, ISO/IEC 18092 e ISO/IEC 21481. En este caso, esta comunicación se puede establecer cuando la distancia entre el terminal y la entidad de identificación está comprendida entre 4 cm y 10 cm aproximadamente. Al ser esta distancia relativamente reducida, la protección de la identidad de usuario se ve mejorada y, adicionalmente, el consumo de energía es ventajosamente relativamente reducido en el terminal.

Cabe contemplar la posibilidad de que la interfaz radio entre el terminal y la entidad de identificación sea de otro tipo que soporte mayores distancias entre el terminal y la entidad de identificación, como por ejemplo la norma de

interfaz de vecindad ISO/IEC 15693.

5 En una forma de realización de la presente invención, un terminal puede gestionar una interfaz de vecindad a más de la interfaz de proximidad utilizada para recuperar la identidad según el procedimiento descrito más arriba. En este caso, cabe prever que, cuando el terminal utiliza una entidad de identificación, se active una temporización de validación (watch dog timer).

El procedimiento de asociación temporal de una identidad de usuario y de un terminal puede comprender entonces facultativamente las siguientes etapas en el terminal, pudiéndose realizar estas últimas en paralelo con otras etapas:

- 10 - activar periódicamente la interfaz de comunicación de vecindad durante un cierto periodo de tiempo, por ejemplo al vencimiento de un temporizador; y verificar la presencia, en la proximidad, de la identidad de identificación utilizada;
- si se verifica la presencia de la entidad de identificación, reinicializar el temporizador y, preferentemente, desactivar la interfaz de comunicación de vecindad, para ahorrar el consumo de energía;
- 15 - si el temporizador vence antes de que se haya podido detectar la presencia de una entidad de identificación en la vecindad del terminal; se avisa de ello al usuario del terminal, mediante una señal visual o sonora). Facultativamente, en este caso, la identidad en curso del usuario es borrada del terminal.

En una forma de realización de la presente invención, un terminal puede gestionar a la vez un protocolo de intercambio de mensajes de tipo NFC y un protocolo de otro tipo.

20 Cabe prever que, cuando el terminal está adaptado para comunicarse en una red de comunicación, después de la etapa /3/, el terminal emita una señal, por ejemplo una señal sonora. De este modo, el usuario queda informado de una correcta inicialización del terminal que está utilizando en lo que respecta a su identidad de usuario.

Después de la etapa /3/, el terminal puede a continuación registrarse ventajosamente ante la red de comunicación basándose en la identidad de usuario. A continuación, el usuario puede disfrutar del o de los servicios ofrecidos en esta red en consideración a su identidad de usuario.

25 Cabe prever que, cuando el terminal está adaptado para comunicarse en una red de comunicación, antes de la etapa /3/, el terminal se registre ante la red de comunicación basándose en una identidad del terminal, y luego, después de la etapa /3/, basándose en la identidad de usuario.

En este caso, el terminal, antes incluso de que haya almacenado la identidad de usuario, está en condiciones de disfrutar rápidamente del o los servicios ofrecidos en la red de comunicación sin identidad de usuario, como por ejemplo un acceso a un número de teléfono de emergencias.

30 Cabe prever ventajosamente que las etapas /1/ a /3/ se pongan en práctica con un movimiento de usuario del terminal consistente en aproximar el terminal a la entidad de identificación. Así, por ejemplo, el usuario del terminal puede portar consigo, como una insignia, la entidad de identificación. En este caso, con objeto de poder utilizar un terminal según una forma de realización de la presente invención, puede recuperar su identidad de usuario con un simple gesto de la mano orientado a aproximar el terminal a su entidad de identificación durante un breve periodo de tiempo, que puede ser de unos segundos.

Un segundo aspecto de la presente invención propone un terminal adaptado para la puesta en práctica de un procedimiento de asociación según el primer aspecto.

40 Un tercer aspecto de la presente invención propone un sistema de asociación de una identidad de usuario, que comprende un terminal según el segundo aspecto de la presente invención y una entidad de identificación en la que está almacenada una información relativa a una identidad de usuario.

Otros aspectos, objetivos y ventajas de la invención se irán poniendo de manifiesto con la lectura de la descripción de una de sus formas de realización.

La invención se comprenderá mejor asimismo con la ayuda de los dibujos, en los que:

la figura 1 ilustra una aplicación de una forma de realización de la presente invención;

45 la figura 2 ilustra un intercambio de mensajes entre un terminal y una entidad de identificación según una forma de realización de la presente invención que permite garantizar un cierto nivel de seguridad contra la usurpación de identidad;

la figura 3 ilustra un intercambio de mensajes entre un terminal, una entidad de identificación y la red relativo a un registro de un terminal ante la red, según una forma de realización de la presente invención;

50 la figura 4 ilustra un intercambio de mensajes entre un terminal, una entidad de identificación y una red relativo a la

gestión de un registro doble de un terminal ante la red, según una forma de realización de la presente invención;

la figura 5 ilustra un intercambio de mensajes entre un terminal, una entidad de identificación y una red según una forma de realización de la presente invención, en cuyo transcurso la identidad de usuario se obtiene a partir de la red, y

- 5 la figura 6 ilustra un sistema de asociación de una identidad de usuario según una forma de realización de la presente invención.

La figura 1 ilustra una aplicación de una forma de realización de la presente invención. Un usuario 13 dispone de un terminal 11 y de una entidad de identificación 12 según una forma de realización de la presente invención. Cabe prever en este punto que la entidad de identificación 12 sea portada por el usuario a la altura del pecho y que, en el momento de la inicialización de su terminal 11, el usuario aproxime este terminal 11 al lugar en el que porta esta entidad de identificación 12. De este modo, la transacción entre la entidad de identificación 12 y el terminal puede establecerse según una forma de realización de la presente invención con el fin de que el terminal pueda disponer en lo sucesivo de la identidad de usuario del usuario 13, basándose en la cual puede disponer de un servicio ofrecido. La transacción que permite al terminal recuperar la identidad puede ser llevada a la práctica efectuando un movimiento de aproximación del terminal hacia la entidad de identificación. Cabe prever que el terminal emita una señal tal como una señal sonora en cuanto es recuperada la identidad. De este modo, a continuación de la emisión de esta señal, puede entonces alejarse el terminal de la entidad de identificación.

Conviene prever que el terminal tan solo disponga de una identidad de usuario temporalmente con el fin de anticiparse a un potencial robo.

- 20 A tal efecto, se ha previsto borrar la identidad de usuario poniendo en práctica una acción específica sobre el terminal, como por ejemplo el apagado del terminal. De este modo, el terminal en el mejor de los casos tan solo dispone de la identidad de usuario temporalmente.

En otra forma de realización de la presente invención, con objeto de incrementar la protección contra una potencial usurpación de identidad del usuario, cabe prever ventajosamente implantar un control de tiempo en tiempo de la presencia de la entidad de identificación en la vecindad del terminal que ha almacenado la correspondiente identidad, según una interfaz sin contacto de vecindad, complementaria de la interfaz sin contacto de proximidad utilizada para la anterior transacción.

La figura 2 ilustra un intercambio de mensajes entre un terminal y una entidad de identificación según una forma de realización de la presente invención que permite incrementar el nivel de seguridad contra la usurpación de identidad.

- 30 En este punto, un intercambio de mensajes de identificación 21 <user-id> se corresponde con la transacción entre el terminal 11 y la entidad de identificación 12, en cuyo transcurso es recuperada por el terminal la identidad de usuario user-id. Este intercambio de mensajes puede ser un intercambio de mensajes seguro para incrementar la protección contra una eventual usurpación de la identidad de usuario.

Una vez recuperada de este modo la identidad en el terminal, se almacena en él en una etapa 24. Con objeto de garantizar una seguridad contra la usurpación de identidad, cabe prever ventajosamente la puesta en práctica de una protección mediante un mecanismo de perro de guardia ('watch dog' en inglés) entre el terminal 11 y la entidad de identificación 12 a fin de verificar que, de tiempo en tiempo al menos, el terminal 11 se halla en la proximidad de la entidad de identificación 12 a partir de la cual ha recuperado la identidad de usuario que ha almacenado. De este modo, una vez que se ha establecido la transacción entre el terminal y la entidad de identificación y el terminal 11 ha almacenado la identidad que le permite disponer del servicio de que se trate, el terminal verifica de tiempo en tiempo la presencia en la proximidad de la entidad de identificación 12.

Tal 'watch dog' puede constar de una sucesión de intercambios de mensajes de control de presencia 23 <CTRL>, encaminados cada uno de estos intercambios de mensajes a determinar la presencia o no de la entidad de identificación 12 en la proximidad del terminal 11. Dos intercambios de mensajes 23 sucesivos pueden estar separados, por ejemplo, un periodo de tiempo T.

Cabe prever entonces ventajosamente que, si un número N de ejecuciones sucesivas de intercambios de mensajes 23 permite al terminal determinar que la entidad de identificación 12 no se halla en la proximidad del terminal 11, el terminal borre la identidad almacenada. En efecto, en estas condiciones, cabe sospechar una usurpación de identidad, ya que se asume que el usuario de esta identidad dispone, en la proximidad del terminal que utiliza, de su entidad de identificación y que, por ende, éste puede, de tiempo en tiempo al menos, detectar su presencia.

Cabe prever también que se informe al usuario de este control de presencia negativo y del borrado de la identidad de usuario en el terminal mediante una señal, por ejemplo una señal luminosa o sonora producida en este terminal.

- 55 Los valores de T y de N pueden venir determinados ventajosamente en función de la aplicación de una forma de realización de la presente invención.

El terminal está adaptado para poner en práctica el intercambio de mensajes 23 encaminado a detectar la presencia de la entidad de identificación 12 en su vecindad. No se vincula limitación alguna a la presente invención en cuanto a este intercambio de mensajes.

5 En tales condiciones, incluso si se ve interrumpida la transacción entre el terminal y la entidad de identificación, el terminal todavía dispone de la identidad del usuario. No obstante, puesto que la ausencia de la entidad de identificación 12 es detectada durante cierto tiempo en el terminal 11, como medida de seguridad contra la usurpación de identidad, esta identidad de usuario es borrada en el terminal 11.

10 Consecuentemente, esta forma de realización permite garantizar una continuidad de servicio en el terminal, aun si el terminal 11 a veces está alejado de la entidad de identificación 12, al propio tiempo que garantiza un nivel elevado de seguridad contra el robo de identidad de usuario.

En una modalidad, la verificación de presencia de la entidad de identificación por el terminal se efectúa mediante una interfaz electromagnética sin contacto de vecindad, en lugar de efectuarse mediante la interfaz sin contacto de proximidad utilizada para transferir la identidad.

15 En una forma de realización de la presente invención, el terminal está adaptado para comunicarse en una red de comunicación 31, y la identidad de usuario está destinada a ser utilizada en esta red de comunicación 31 con el fin de acceder en el terminal 11 a uno o varios servicios de comunicación.

La figura 3 ilustra un intercambio de mensajes entre el terminal 11, la entidad de identificación 12 y la red 31 relativo a un registro de un terminal ante la red de comunicación en la que puede comunicarse, según una forma de realización de la presente invención.

20 En primer lugar, el terminal 11 recupera la identidad de usuario user-id de su usuario ante la entidad de identificación 12, en el transcurso del intercambio de mensajes de identificación 21 <user-id>, y la almacena localmente, en la etapa 24.

El terminal 11, a continuación, está en condiciones de registrarse basándose en esta identidad user-id, poniendo en práctica un intercambio de mensajes de registro de usuario 32 <reg user-id> con la red de comunicación 31.

25 La figura 4 ilustra un intercambio de mensajes, entre el terminal, la entidad de identificación y la red, relativo a la gestión de un registro doble de un terminal ante la red, según una forma de realización de la presente invención. Este intercambio puede llevarse a la práctica cuando el terminal 11 tiene una identidad suya propia, id-term.

30 En una forma de realización de la presente invención, al encendido del terminal 11, este último no dispone de ninguna identidad de usuario, como se ilustra en una etapa 40. De este modo, antes de que se ponga en práctica el intercambio de mensajes de identificación 21, en el momento de la inicialización del terminal, este último puede registrarse con su propio identificador id-term según un intercambio de mensajes de registro de terminal 41 <reg id-term>.

35 Seguidamente, una vez que se recupera la identidad de usuario, en la etapa 24, mediante el intercambio de mensajes de identificación 21, el terminal puede proceder entonces a un registro ante la red sustentado en la identidad de usuario por intermedio de un intercambio de mensajes de registro de usuario 32.

Esta forma de realización permite ventajosamente aumentar la eficiencia del procedimiento de registro de un terminal a una red que requiere, a un tiempo, una identidad del terminal y una identidad del usuario, al permitir proceder en primer lugar al registro del terminal antes de que se haya efectuado la operativa de recuperación de la identidad de usuario.

40 Asimismo, ésta puede ser particularmente ventajosa cuando la red de que se trate 31 ofrece además servicios basados solamente en el registro del terminal. En efecto, el usuario puede utilizar entonces estos servicios en espera de disponer de la identidad de usuario user-id y de poner en práctica el registro del usuario 32.

45 En una variante de la forma de realización de la presente invención descrita con referencia a la figura 4, cabe prever proporcionar a la red 31, de manera asociada, a un tiempo la identidad propia del terminal id-term y la identidad de usuario user-id en el transcurso de un mismo intercambio de mensajes, el intercambio de mensajes de registro 32.

La figura 5 ilustra un intercambio de mensajes entre el terminal 11, la entidad de identificación 12 y la red 32, según una forma de realización de la presente invención, en cuyo transcurso la identidad de usuario es recuperada por último a partir de la red.

50 En esta forma de realización, en la inicialización del terminal 11, este último no tiene en su posesión ninguna identidad de usuario almacenada localmente, como se ilustra en la etapa 40. En primer lugar, en su fase de inicialización, el terminal 11 pone en práctica un registro de terminal ante la red de comunicación 31 basándose en los intercambios de mensajes 41 <reg id-term>, proporcionando así a la red 31 su identificador propio id-term.

5 A continuación, pone en práctica la etapa consistente en recuperar una identidad de usuario user-id. En esta forma de realización de la presente invención, la propia identidad de usuario no está almacenada directamente en la entidad de identificación 12 en posesión del usuario del terminal 11. La entidad de identificación 12 almacena solamente, en este caso, una información id-info que permite, en lo sucesivo, recuperar la identidad de usuario ante la red 31.

10 De este modo, la etapa consistente en recuperar la identidad de usuario en el terminal se descompone en dos partes en el terminal, consistiendo una primera parte en recuperar la información de usuario id-info ante la entidad de identificación 12 y consistiendo una segunda parte en recuperar la identidad de usuario user-id ante la red 31 basándose en la información de usuario id-info. En este caso, cabe prever que la red 31 comprenda un servidor de guía que esté adaptado para gestionar una asociación entre una información de usuario y una identidad de usuario.

El terminal pone en práctica, en primer lugar, la primera parte, según un intercambio de mensajes 51 con la entidad de identificación 12, en cuyo transcurso recupera la información de usuario que está almacenada en esta entidad de identificación 12.

15 En una forma particular de realización, cabe prever que el terminal almacene la información de usuario id-info, como se ilustra en una etapa 54 de la figura 5.

Entonces, seguidamente, procede a la recuperación de la identidad de usuario propiamente dicha ante la red 31, basándose en la información de usuario por intermedio de un intercambio de mensajes de identificación con la red, en cuyo transcurso proporciona la información de usuario en un mensaje 52 y a cambio recibe la identidad de usuario user-id asociada, en un mensaje 53.

20 El mensaje 52 puede además indicar la identidad de terminal id-term, para no permitir más que a un terminal registrado previamente poder obtener una identidad de usuario.

A la recepción del mensaje 53 indicativo de la identidad de usuario user-id, el terminal 11 la almacena, en la etapa 24.

25 La figura 6 ilustra un sistema de asociación de una identidad de usuario según una forma de realización de la presente invención.

Tal sistema de asociación 60 comprende una entidad de identificación 12 que almacena una información relativa a una identidad de usuario y un terminal 11 según una forma de realización de la presente invención. Este último comprende:

- 30 - una unidad de interfaz radio 61 adaptada para establecer una transacción 21 con una entidad de identificación 12 y para recibir una información relativa a una identidad de usuario almacenada en dicha entidad de identificación, en el transcurso de dicha transacción;
- una unidad de almacenamiento 62 adaptada para almacenar dicha identidad de usuario obtenida a partir de dicha información relativa a una identidad de usuario; y
- 35 - una unidad de gestión de almacenamiento 63 adaptada para borrar la identidad de usuario cuando el terminal es sometido a una acción específica.

Cuando el terminal está adaptado para comunicarse en la red de comunicación 31, la unidad de interfaz radio 61 puede además estar adaptada para proporcionar a la red de comunicación 31, por intermedio del mensaje 52, la información de usuario, y para recibir desde la red de comunicación 31, por intermedio del mensaje 53, la identidad de usuario.

40 La unidad de interfaz radio 61 puede además estar adaptada para determinar si la entidad de identificación 12 está situada en la proximidad del terminal, y la unidad de gestión de almacenamiento 63 puede además estar adaptada para decidir borrar la identidad de usuario cuando la unidad de interfaz radio determina N veces consecutivas que la entidad de identificación no está situada en la proximidad del terminal, siendo N cualquier número entero.

45 El terminal según una forma de realización de la presente invención es el encargado de proporcionar la energía a la entidad de identificación sin contacto. El terminal puede ser, por ejemplo, un equipo extremo de un sistema de comunicación, tal como un sistema de radiocomunicaciones profesionales móviles o PMR (por 'Professional Mobile Radio' en inglés).

50 La entidad de identificación 12 puede corresponderse con una tarjeta inteligente sin contacto de proximidad. Puede ser, por ejemplo, una tarjeta profesional llevada por el usuario al pecho o en su cartera, o bien un carnet de identidad, un permiso de conducir o un documento de viaje.

Cabe prever que la interfaz radio entre el terminal 11 y la entidad de identificación 12 sea desactivada en cuanto la identidad de usuario se almacena en el terminal, excepto cuando se pone en práctica una operativa de control de

presencia de entidad de identificación tal y como se ilustra en la figura 2.

En efecto, en este caso, se puede prever que el terminal active entonces periódicamente y temporalmente su interfaz radio, solamente durante un periodo determinado, permitiéndole poner en práctica un control de presencia de la entidad de identificación en la vecindad. Al proceder de este modo, se está en condiciones de ahorrar energía en el terminal.

5

REIVINDICACIONES

1. Procedimiento de asociación de una identidad de usuario, user_id, con un terminal electrónico móvil (11) que incluye una identidad del terminal, id-term, y adaptado para ofrecer un servicio sustentado en dicha identidad de usuario, user-id;
- 5 comprendiendo dicho procedimiento de asociación, en el terminal electrónico móvil, las siguientes etapas:
- /1/ establecimiento de una transacción entre el terminal y una entidad de identificación (12) por intermedio de una interfaz sin contacto (21), estando adaptado dicho terminal para detectar la presencia de dicha entidad de identificación (12) en su vecindad, almacenando dicha entidad de identificación una información relativa a la identidad de usuario, user-id;
- 10
- /2/ recepción, en el transcurso de dicha transacción, de la información relativa a la identidad de usuario, user-id, almacenada en dicha entidad de identificación, y obtención de la identidad de usuario, user-id, a partir de dicha información;
 - /3/ almacenamiento temporal de la identidad de usuario, user-id, obtenida,
- 15 estando además caracterizado el procedimiento de asociación por que dicha identidad de usuario es borrada del terminal cuando el terminal es sometido a una acción específica, y por que el terminal se comunica en una red de comunicación (31) y por que, antes de la etapa /3/, el terminal se registra ante la red de comunicación (31) basándose en la identidad del terminal, id-term, y luego, después de la etapa /3/, basándose en la identidad del usuario, user-id.
2. Procedimiento de asociación de una identidad de usuario, user-id, según una cualquiera de las reivindicaciones anteriores, que comprende además, en el terminal (11), las siguientes etapas:
- 20
- /4/ determinar si la entidad de identificación (12) está situada en la proximidad del terminal;
 - /5/ repetir la etapa /4/ N veces, siendo N un número entero; y
 - /6/ decidir borrar la identidad de usuario, user-id, en el terminal si se determina N veces consecutivas que la entidad de identificación no está situada en la proximidad del terminal.
- 25 3. Procedimiento de asociación de una identidad de usuario, user-id, según una cualquiera de las reivindicaciones anteriores, en el que, después de la etapa /3/, el terminal emite una señal sonora o luminosa.
4. Procedimiento de asociación de una identidad de usuario, user-id, según una cualquiera de las reivindicaciones anteriores, en el que el terminal se comunica en una red de comunicación (31); y en el que, antes de la etapa /3/,
- 30
- recepción, en el transcurso de dicha transacción, de una información relativa a una identidad de usuario almacenada en dicha entidad de identificación;
 - transmisión por parte del terminal, a la red de comunicación (31), de la información relativa a la identidad de usuario;
- 35
- recepción, desde la red de comunicación, de una identidad del usuario asociada a la información relativa a la identidad del usuario,
 - almacenamiento temporal, por parte del terminal, de la identidad de usuario recibida, borrándose del terminal dicha identidad de usuario cuando dicho terminal es sometido a una acción específica.
- 40 5. Procedimiento de asociación de una identidad de usuario, user-id, según una cualquiera de las reivindicaciones anteriores, en el que el terminal se comunica en una red de comunicación (31); y en el que, después de la etapa /3/, el terminal se registra ante la red de comunicación (31) basándose en la identidad de usuario, user-id.
6. Procedimiento de asociación de una identidad de usuario según una cualquiera de las reivindicaciones anteriores, en el que las etapas /1/ a /3/ son puestas en práctica con un movimiento de usuario del terminal consistente en aproximar dicho terminal a la entidad de identificación.
- 45 7. Terminal electrónico móvil (11) que incluye una identidad del terminal (id-term) y adaptado para ofrecer un servicio sustentado en una identidad de usuario (user-id), estando adaptado dicho terminal para detectar la presencia de una entidad de identificación (12) en su vecindad, almacenando dicha entidad de identificación (12) una información relativa a la identidad de usuario, user-id; comprendiendo dicho terminal:
- medios (41) para registrarse ante una red de comunicación (31) basándose en la identidad del terminal, id-

term;

- una unidad de interfaz radio (61) adaptada para establecer una transacción sin contacto (21) con una entidad de identificación (12) y para recibir la información relativa a la identidad de usuario, user-id, almacenada en dicha entidad de identificación, en el transcurso de dicha transacción;
- 5
- una unidad de almacenamiento (62) adaptada para almacenar dicha identidad de usuario, user-id, obtenida a partir de dicha información;
 - medios (32, 52, 53) para registrarse ante la red de comunicación (31) basándose en la identidad de usuario, user-id, después del almacenamiento de dicha identidad de usuario, user-id, y basándose en la identidad del terminal antes del almacenamiento de dicha identidad de usuario, user-id;
- 10
- una unidad de gestión de almacenamiento (63) adaptada para borrar la identidad de usuario, user-id, cuando el terminal es sometido a una acción específica.
8. Terminal según la reivindicación anterior, en el que dicho terminal está adaptado para comunicarse en una red de comunicación (31), comprendiendo dicho terminal:
- 15
- medios para proporcionar (52) a la red de comunicación (31) una información relativa a la identidad de usuario proporcionada por la unidad de identificación;
 - medios para recibir (53), desde la red de comunicación, dicha identidad de usuario, siendo gestionada en la red de comunicación (31) una asociación entre la información relativa a una identidad de usuario y la identificación de usuario.
9. Terminal (11) según las reivindicaciones 7 y 8, estando además adaptado para comunicarse en una red de comunicación (31), en el que la unidad de interfaz radio (61) está además adaptada para proporcionar (52) a la red de comunicación (31) la información de usuario y para recibir (53), desde la red de comunicación, dicha identidad de usuario.
- 20
10. Terminal (11) según una de las reivindicaciones 7 a 9, en el que la unidad de interfaz radio está además adaptada para determinar si la entidad de identificación (12) está situada en la proximidad del terminal; y
- 25
- en el que la unidad de gestión de almacenamiento (63) está además adaptada para decidir borrar la identidad de usuario cuando la unidad de interfaz radio determina N veces consecutivas que la entidad de identificación no está situada en la proximidad del terminal, siendo N cualquier número entero.
11. Sistema de asociación (60) de una identidad de usuario, que comprende un terminal (11) según una cualquiera de las reivindicaciones 7 a 10 y una entidad de identificación (12) en la que está almacenada una información relativa a una identidad de usuario, comprendiendo dicho sistema unos medios para ejecutar el procedimiento según una de las reivindicaciones 1 a 6.
- 30

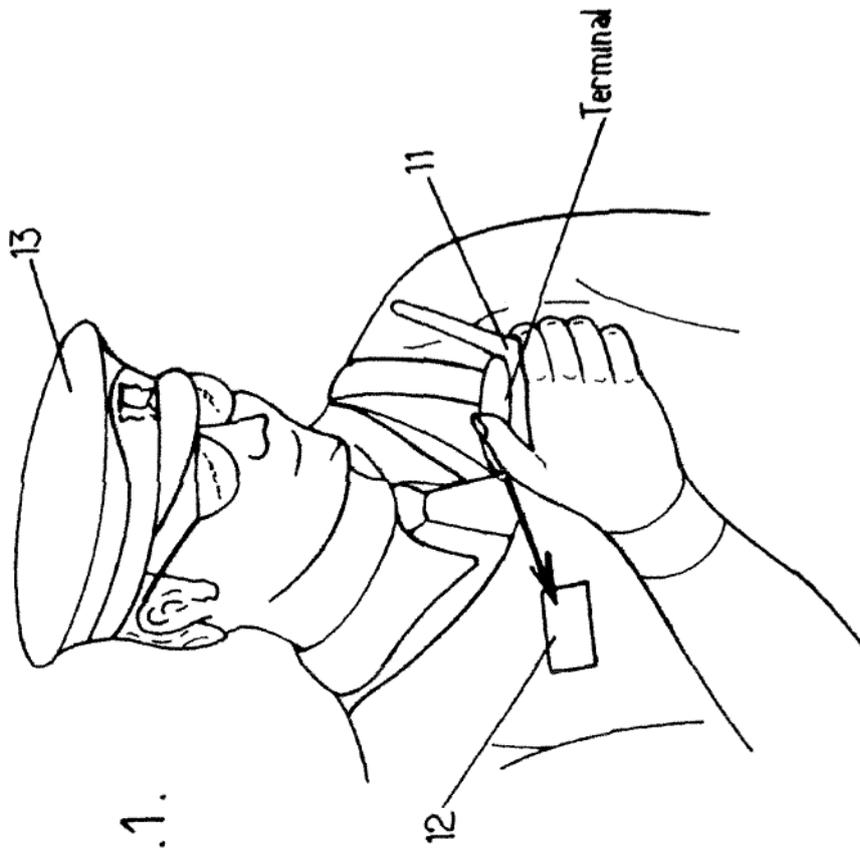


FIG.1.

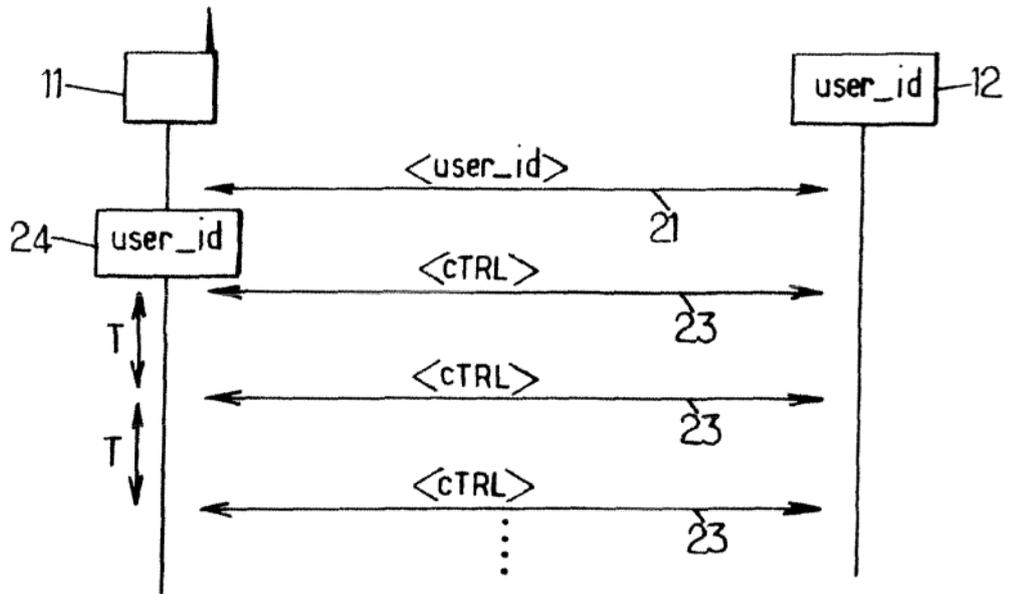


FIG.2.

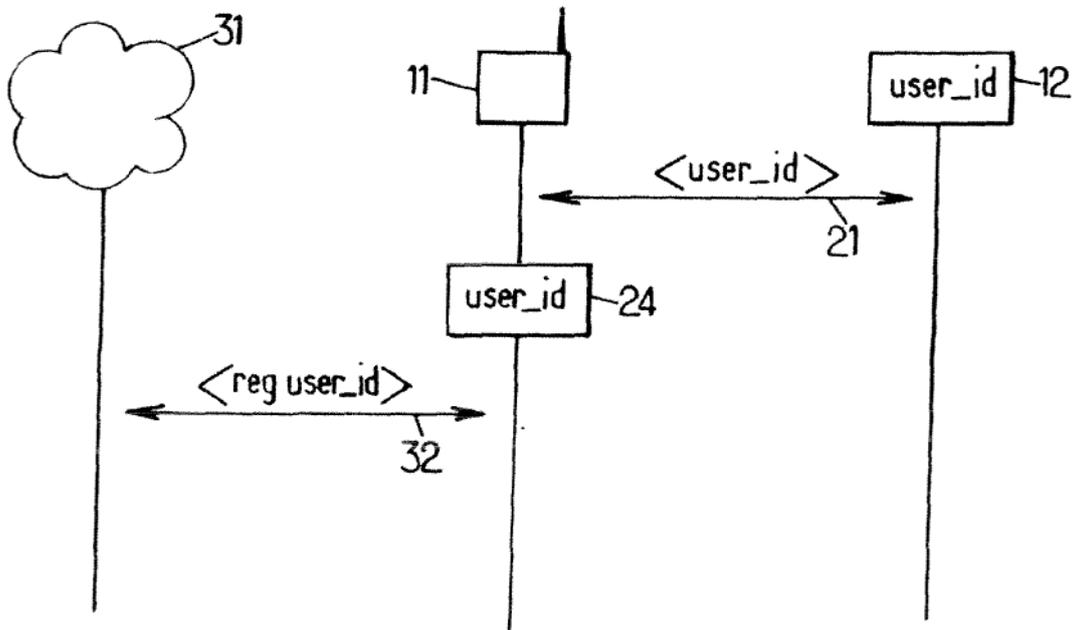
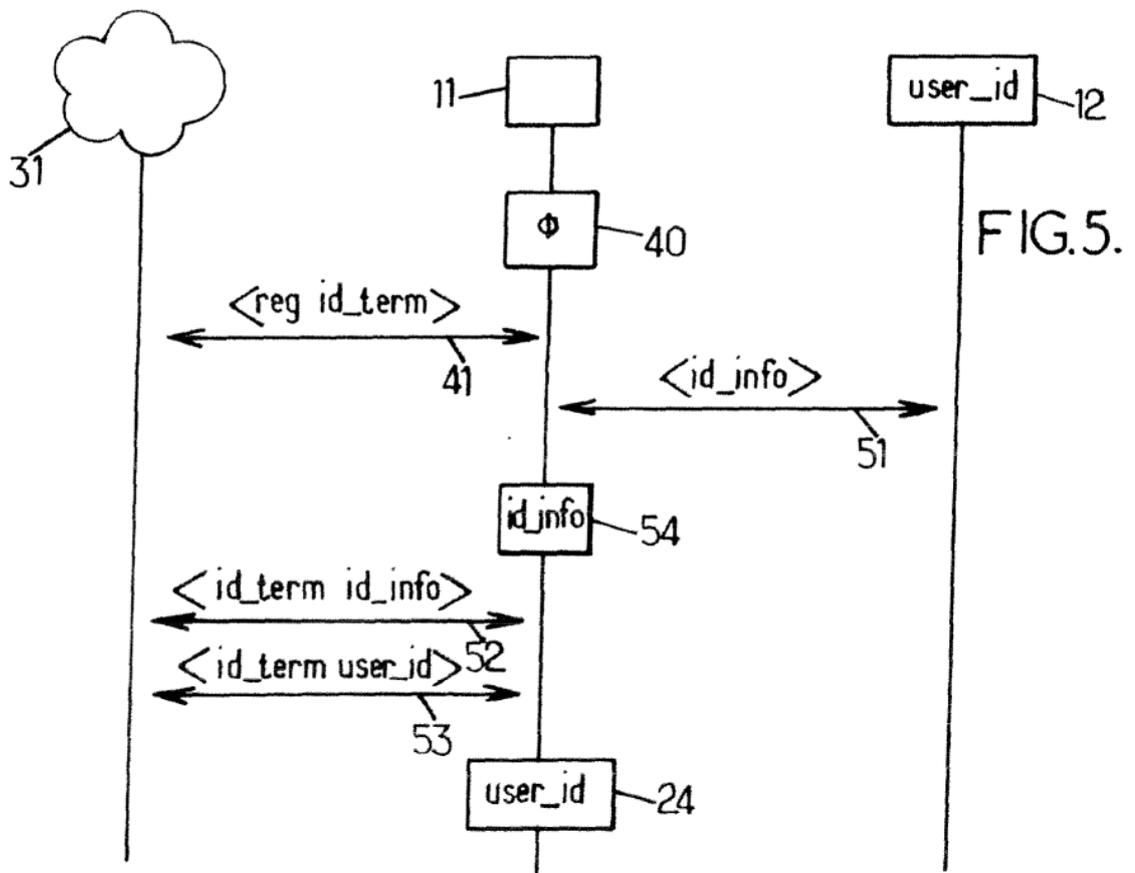
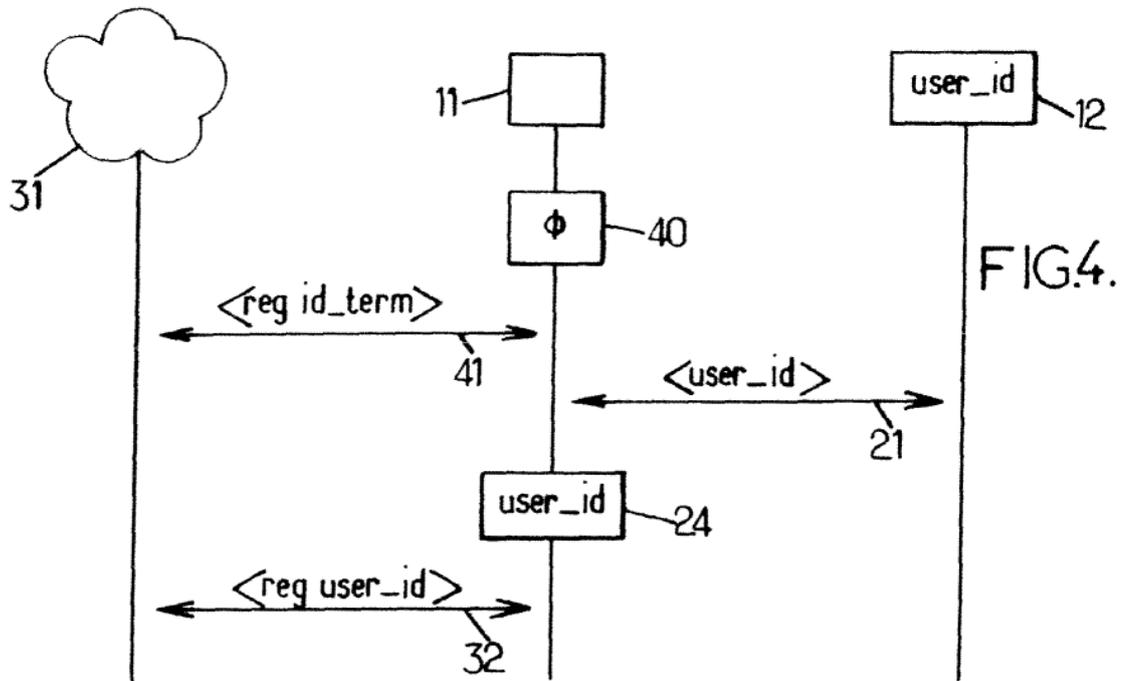


FIG.3.



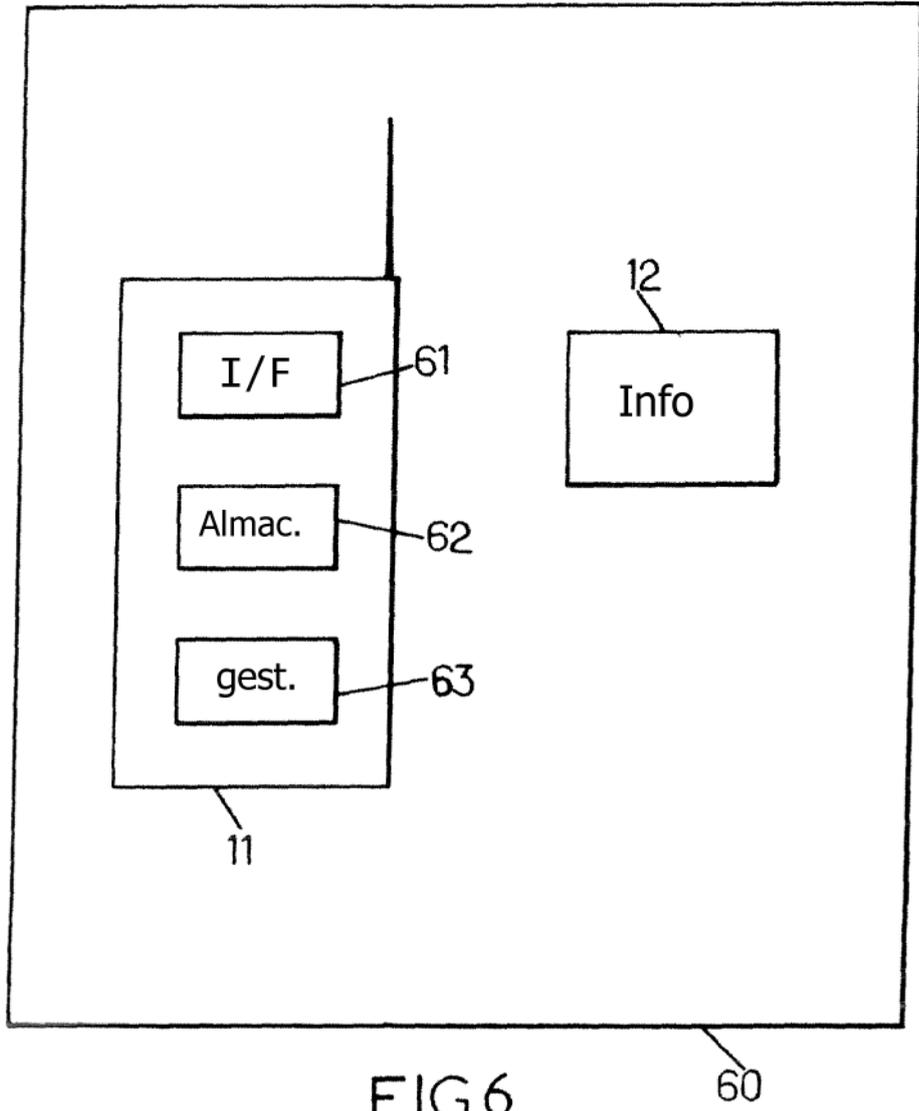


FIG. 6.