(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 363 165**

(51) Int. Cl.:
H04W 8/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06818828 .3**
(96) Fecha de presentación : **25.11.2006**
(97) Número de publicación de la solicitud: **1955515**
(97) Fecha de publicación de la solicitud: **13.08.2008**

(54) Título: **Generación de identidades de clientes en un sistema de comunicación.**

(30) Prioridad: **01.12.2005 DE 10 2005 057 732**

(45) Fecha de publicación de la mención BOPI:
22.07.2011

(45) Fecha de la publicación del folleto de la patente:
22.07.2011

(73) Titular/es: **VODAFONE HOLDING GmbH**
Mannesmannufer 2
40213 Düsseldorf, DE

(72) Inventor/es: **Jungblut, Stephan**

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Generación de identidades de clientes en un sistema de comunicación

La presente invención se refiere a un procedimiento para la generación de una identidad de clientes en un sistema de comunicación que presenta una red de ordenadores y una red de telefonía móvil celular con las características del preámbulo de la reivindicación 1. Un procedimiento así se divulga, por ejemplo, por el documento WO 2001/31840 A1.

Además, la presente invención se refiere a la utilización de una identidad según la invención para la autenticación y/o autentificación de un cliente. Además, es objeto de la invención una autorización de un acceso de un terminal de datos a datos y/o servicios de un equipo terminal de datos en una red de ordenadores. La invención se refiere también a un sistema de comunicación constituido por una red de ordenadores con equipos terminales de datos y una red de telefonía móvil celular con terminales móviles que pueden funcionar en ella, estando configurados los equipos terminales de datos, los equipos de la red de telefonía móvil y/o los terminales móviles para ejecutar y/o utilizar un procedimiento según la invención.

Las identidades de clientes, especialmente procesos y/o usuarios de los equipos terminales, se utilizan en redes de comunicación en numerosas aplicaciones para la autenticación, autentificación y especialmente la autorización. Autenticar en el sentido de la presente invención es identificar la identidad de un cliente. Autentificación o autentificar en el sentido de la presente invención es un proceso en el que la identidad de un cliente se comprueba mediante una determinada característica. Correspondientemente, en una comprobación de la identidad participan un abonado que se autentica y un abonado que la autentifica. A continuación de una comprobación de la identidad satisfactoria puede realizarse una autorización de un acceso del abonado que se autentica a los datos y/o servicios del sistema de comunicación.

En el estado de la técnica se conocen numerosos procedimientos y sistemas que se utilizan especialmente para la autenticación, autentificación y/o autorización de clientes, generándose o creándose las respectivas identidades de las más diversas maneras.

La autenticación y/o autentificación de la identidad de clientes puede realizarse de cinco formas diferentes en función de la configuración de la identidad, de la autenticación y/o de la autentificación. A este respecto, las identidades de los clientes se comprueban en cuanto a estas características definidoras en el marco de la autenticación o autentificación. A este respecto se diferencian en el dato conocido, la cosa poseída y/o las características biométricas. A este respecto, una autentificación puede realizarse de cinco formas distintas que pueden combinarse entre sí:

1. Se tiene algo, por ejemplo, una clave, una tarjeta o un identificador similar

2. Se sabe algo, por ejemplo, una contraseña

3. Se es algo o alguien, por ejemplo, se comprueban características biológicas de personas: huellas dactilares, rasgos faciales y/o características de la voz

4. Se está en un determinado lugar, por ejemplo, una determinada celda de una red de telefonía móvil celular

5. Se sabe hacer algo, preferentemente algo individual; por ejemplo, estampar la firma personal.

Combinando dos de estas posibilidades existe una llamada autentificación de dos factores como, por ejemplo, en relación con tarjetas SIM insertables en terminales móviles que pueden funcionar en redes de telefonía móvil celular y el o los respectivo(s) PIN correspondiente(s).

Procedimientos y sistemas de este tipo se utilizan ampliamente, por ejemplo, en el campo de las redes de telefonía móvil celular, por ejemplo, en relación con módulos de identificación del abonado de telefonía móvil que permiten a un terminal móvil un acceso en o a la red de telefonía móvil, las llamadas tarjetas SIM (SIM: módulo de identificación de abonado) que generalmente se insertan para este fin en terminales móviles que pueden funcionar en redes de telefonía móvil. Además de un identificador específico de la tarjeta dado por parte de la tarjeta SIM correspondiente y generalmente unívoco, un acceso a o en la red de telefonía móvil requiere adicionalmente que el usuario del terminal móvil introduzca un número de identificación personal o un código de acceso numérico, un llamado PIN (PIN: número de identidad personal) a través del terminal móvil que utiliza la tarjeta. En relación con redes de ordenadores, especialmente redes de ordenadores como, por ejemplo, internet o una intranet, también se conocen numerosos procedimientos y/o sistemas de autenticación, autentificación y/o autorización que hacen posible un acceso a la red de ordenadores, estando generadas o generándose las identidades correspondientemente utilizadas por los clientes de la forma más variada y del tipo más variado. Un acceso de un usuario humano a datos y/o servicios de un equipo terminal de datos en una red de ordenadores se realiza por un equipo terminal de datos del usuario conectado a la red de ordenadores, generalmente utilizando una identidad que generalmente está compuesta por un nombre de usuario y una contraseña secreta asociada al nombre de usuario. Un acceso a los datos y/o servicios del equipo terminal de datos que los proporciona se hace posible por éste al realizar el usuario la

introducción del nombre de usuario y la contraseña secreta. Para ello, el equipo terminal de datos que proporciona los datos y/o servicios almacena el nombre de usuario y la contraseña secreta asociada al nombre de usuario. Cuando el usuario solicita acceso, el equipo terminal de datos que proporciona los datos y/o servicios compara el nombre de usuario y la contraseña secreta introducidos por el usuario con el nombre de usuario y la contraseña registrados en el equipo terminal de datos que proporciona los datos y/o servicios, y si coinciden permite un acceso a los datos y/o servicios al usuario o al equipo terminal de datos asociado al usuario.

También se conocen sistemas de comunicación en los que los equipos terminales están conectados entre sí por grupos a través de una red de ordenadores y/o una red de telefonía móvil celular. Sistemas de comunicación de este tipo crean una red privada virtual, una llamada VPN (VPN: red privada virtual) para los miembros individuales del grupo o sus terminales dentro de una empresa o asociación similar. A este respecto, la VPN se basa generalmente en métodos criptográficos. A este respecto, el acceso de miembros individuales del grupo a la red privada virtual del grupo posibilitado a través de una red de ordenadores, generalmente internet, y/o red de telefonía móvil, también utiliza identidades de los clientes y métodos para la autenticación, autentificación y/o autorización. A este respecto, la administración del grupo o de los miembros individuales del grupo se realiza por parte de un equipo terminal de datos de la red de ordenadores, generalmente por el llamado servidor de acceso de la empresa y/o un servidor de acceso correspondiente o una pasarela (gateway) por parte de la red de telefonía móvil. A este respecto, la asignación de miembros del grupo al grupo y/o miembros individuales del grupo o grupos en el sistema de comunicación para las aplicaciones de comunicaciones para los servicios disponibles se realiza por parte de un equipo de gestión correspondiente por parte del sistema de comunicación.

En el caso de los datos y/o servicios accesibles a través de una red de ordenadores, especialmente internet, de un equipo terminal de datos tienen que evitarse accesos y/o usos no autorizados y/o abusivos de los datos y/o servicios. Esto se aplica especialmente a un acceso de un trabajador de una empresa a datos y/o servicios de un equipo terminal de datos de una red empresarial, una llamada intranet, desde un equipo terminal de datos que se encuentra fuera de la red de ordenadores de la empresa, a través de Internet, por ejemplo, al acceder el trabajador de la empresa a equipos terminales de datos en la empresa desde su domicilio o lugares localizados fuera de la empresa similares. Para impedir accesos no autorizados o abusivos, en el estado de la técnica en la generación y/o utilización de identidades, especialmente en relación con la autenticación, autentificación y/o autorización, se conocen varios procedimientos y criptográficos métodos que comprenden una encriptación o desencriptación de y/o con identidades. A este respecto se consideran especialmente procedimientos criptográficos asimétricos y/o sistemas que utilizan generalmente claves públicas y secretas para aumentar la seguridad de las encriptaciones o desencriptaciones, siendo las clave secretas para el abonado que autentica y el abonado que autentifica de un proceso de comprobación de la identidad correspondiente respectivamente secretas o privadas, al contrario que los llamados procedimientos y/o sistemas criptográficos simétricos. El llamado procedimiento RSA (RSA: Rivest-Shamir-Adelman) proporciona un procedimiento o sistema criptográfico asimétrico correspondiente que se utiliza en el estado de la técnica para diferentes aplicaciones en internet.

En el marco de la autenticación, autentificación y/o autorización es desventajoso en las identidades y/o sus usos conocidos hasta la fecha en el estado de la técnica que, dependiendo de la configuración respectiva en lo que se refiere a la inicialización, mantenimiento y/o manejo, sean complicados y de alto coste. Además, las identidades y sus usos conocidos hasta la fecha en el marco de la autenticación, autentificación o autentificación y/o autorización con respecto a la seguridad contra usos no autorizados o abusivos necesitan mejoras, especialmente en relación con la autorización de un acceso a datos y/o servicios de un equipo terminal de datos en una red privada virtual (VPN).

Especialmente en el caso de pequeñas y medianas empresas, las llamadas PyMES, hasta la fecha no es posible, o no es posible desde el punto de vista económico y/o no es posible con gastos justificables el coste de la autorización asociada a una red privada virtual (VPN) debido a los costes de sistemas y/o de administración necesarios en lo que se refiere a un acceso a datos y/o servicios de un equipo terminal de datos de la empresa a través de una red de ordenadores como internet.

Considerado este estado de la técnica, la invención se basa en el objetivo de proporcionar un procedimiento para la generación de una identidad de clientes en un sistema de comunicación según la invención que sea más eficiente con respecto a la exigencia de recursos de red.

Para la solución técnica, con la presente invención se propone un procedimiento con las características según el preámbulo de la reivindicación 1 que se caracteriza por las características según la parte caracterizadora de la reivindicación 1.

La invención se basa en el conocimiento de que mediante la utilización de al menos una información temporal ($T_{cliente}$) sincronizada con una información temporal (T_{red}) prefijada por parte de la red de telefonía móvil puede generarse de un modo y manera sencillo y económico una identidad del cliente en el sistema de comunicación que sea mejorado con respecto a la seguridad de la utilización no autorizada o abusiva, especialmente ya que la identidad se genera con y/o utilizando una información temporal sincronizada sólo para las partes implicadas, es decir, especialmente el cliente y la parte que hace posible un acceso, que ventajosamente es desconocida para terceros.

Ventajosamente, la información temporal utilizada para la generación de la identidad del cliente ($T_{cliente}$) es proporcionada por un dispositivo de sincronización presente por parte de un terminal móvil del cliente que puede funcionar en la red de telefonía móvil y/o por parte de un módulo de identificación del abonado de telefonía móvil (SIM) que usa el terminal móvil. Así, un terminal móvil, especialmente un teléfono móvil, utiliza ventajosamente un tiempo de la red de telefonía móvil dado normalmente por parte de una red de telefonía móvil o una información temporal similar de la red de telefonía móvil para la sincronización de la información temporal. A este respecto, el tiempo de la red de telefonía móvil o información temporal similar de la red de telefonía móvil proporciona ventajosamente una información de referencia válida y única en toda la red de telefonía móvil.

En otra configuración de la invención, en caso de necesidad, se sincroniza la información temporal utilizada para la generación de la identidad del cliente ($T_{cliente}$) con la información temporal prefijada por parte de la red de telefonía móvil en el marco del intercambio de informaciones de señalización entre el terminal móvil y la red de telefonía móvil. La sincronización eventual por necesidad posibilita ventajosamente especialmente una reducción en cuanto a la carga de la red de telefonía móvil o una descarga de los dispositivos de la red de telefonía móvil en cuanto al intercambio de informaciones de señalización correspondientes para la sincronización. La necesidad se determina ventajosamente considerando al menos una información en cuanto a la disponibilidad del terminal móvil en la red de telefonía móvil. Así puede generarse, por ejemplo, una solicitud de necesidad ventajosamente de forma automática si el terminal móvil no estaba disponible en la red de telefonía móvil, por ejemplo, si no tenía conexión de radio. En la señalización subsiguiente en cuanto a un nuevo registro del terminal móvil en la red de telefonía móvil, es decir, cuando el terminal móvil vuelve a estar disponible, se realiza entonces ventajosamente una sincronización de la información temporal sobre la base de y/o utilizando la información de necesidad.

En otra configuración ventajosa de la invención, la información temporal ($T_{cliente}$) utilizada para la generación de la identidad del cliente se sincroniza con la información temporal (T_{red}) prefijada por parte de la red de telefonía móvil después de un intervalo de tiempo en el marco del intercambio de informaciones de señalización entre el terminal móvil y la red de telefonía móvil. Debido a la sincronización realizada después de un intervalo de tiempo así dada, también se da ventajosamente una reducción en cuanto a la carga de la red de telefonía móvil o una descarga de los dispositivos de la red de telefonía móvil en cuanto al intercambio de informaciones de señalización correspondientes para la sincronización. Ventajosamente, los intervalos pueden ser fijados por parte de la red de telefonía móvil, preferentemente son ajustables de forma automática y a medida.

Otra configuración ventajosa de la invención prevé que la información temporal utilizada para la generación de la identidad del cliente ($T_{cliente}$) se sincronice con la información temporal fijada por parte de la red de telefonía móvil (T_{red}) al menos en el marco del intercambio de informaciones de señalización para el establecimiento, el mantenimiento y/o la terminación de una conexión entre el terminal móvil y la red de telefonía móvil.

La sincronización de la información temporal ($T_{cliente}$) se realiza ventajosamente al menos cuando el terminal móvil no está disponible en la red de telefonía móvil utilizando al menos un dispositivo contador. Así puede lograrse ventajosamente una sincronización cuando el terminal móvil no esté o estuviera disponible en la red de telefonía móvil, por ejemplo, no tuviera conexión de radio con la red de telefonía móvil. Una configuración preferida de la invención prevé que el dispositivo contador esté previsto por parte de la red de telefonía móvil, que se active cuando el terminal móvil no está disponible en la red de telefonía móvil y que transmita un valor del contador calculado por el dispositivo contador al terminal móvil cuando el terminal móvil vuelva a estar disponible en la red de telefonía móvil que utilice por parte del terminal móvil para la sincronización de la información temporal ($T_{cliente}$). Así se aumenta ventajosamente todavía más la seguridad en cuanto a la generación de la identidad.

En otra configuración ventajosa de la invención, la identidad de un cliente se genera mediante la combinación de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil. Combinando un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil puede generarse ventajosamente de un modo y manera sencillo y económico una identidad del cliente en el sistema de comunicación que es reducida en cuanto al coste de gestión y manipulación y además mejora en cuanto a la seguridad contra la utilización no autorizada o abusiva. La combinación según la invención de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil para generar la identidad del cliente en el sistema de comunicación se sirve ventajosamente de las identidades y sus procedimientos, sistemas y métodos para la autenticación, autentificación o autentificación y/o autorización de la red de ordenadores y de la red de telefonía móvil celular, de modo que se reduce o puede reducirse el coste dado o relacionado con la combinación según la invención en cuanto a la gestión y/o la manipulación. Además, combinando diferentes identificadores del cliente dados, por una parte, por parte de la red de ordenadores y, por otra parte, de la red de telefonía móvil celular y su combinación para generar una identidad en el sistema de comunicación aumenta de un modo y manera sencillos la medida de seguridad de la identidad generada y también de sus usos en el marco de la autenticación, autentificación o autentificación y/o autorización.

En una configuración ventajosa de la invención, el identificador del cliente en la red de ordenadores se genera con un algoritmo criptográfico, preferentemente por parte de un equipo terminal de datos de la red de ordenadores, más preferentemente por parte de un equipo terminal de datos de una pequeña y mediana empresa (PyME) que está conectado a la red de ordenadores. En una configuración ventajosa de la invención, el equipo terminal de datos de

la PyME es un servidor AAA de una VPN de la PyME. Otra configuración ventajosa de la invención prevé que el identificador del cliente en la red de ordenadores se genere utilizando un identificador primario del cliente en la red de ordenadores y un dispositivo contador, estando diseñado el dispositivo contador preferentemente de forma que use un algoritmo criptográfico y siendo con especial preferencia un componente del equipo terminal de datos. Con la utilización según la invención de un dispositivo contador se realiza ventajosamente una sincronización del identificador del cliente en la red de ordenadores y, por tanto, por parte del sistema de comunicación, pudiéndose aumentarse todavía más la seguridad de la identidad y/o su uso. Así, por ejemplo, un indicador captado o escuchado sin autorización o abusivo en el marco del uso no puede usarse ventajosamente otra vez; es decir uso no autorizado o abusivo.

En otra configuración ventajosa de la invención, el identificador del cliente en la red de telefonía móvil se genera con un algoritmo criptográfico, preferentemente por parte de un terminal móvil del cliente que puede funcionar en la red de telefonía móvil. Otra configuración de la invención prevé que el identificador del cliente en la red de telefonía móvil se genere utilizando un identificador primario del cliente en la red de telefonía móvil y un dispositivo contador, estando diseñado el dispositivo contador preferentemente de forma que use un algoritmo criptográfico y siendo con especial preferencia componente del terminal móvil y/o un módulo de identificación del abonado de telefonía móvil, un llamado SIM (SIM: módulo de identificación del abonado) usado por el terminal móvil. Una configuración preferida de la invención prevé que el identificador primario del cliente en la red de telefonía móvil contenga los datos identificativos del terminal móvil que puede funcionar en la red de telefonía móvil y/o los datos identificativos del usuario del terminal móvil en la red de telefonía móvil, conteniendo como datos identificativos del terminal móvil preferentemente el identificador del aparato, el llamado IMEI (IMEI: identidad internacional del equipo móvil, de “International Mobile Equipment Identity”) y los datos identificativos del usuario del terminal móvil en la red de telefonía móvil, al menos el número de teléfono específico de la red asignado al usuario por un operador de la red de telefonía móvil, el llamado MSISDN (MSISDN: número ISDN del abonado de la estación móvil, de “Mobile Station Subscriber ISDN number”, ISDN: red digital de servicios integrados, de “Integrated Services Digital Network”) y/o al menos el identificador del abonado de telefonía móvil, el llamado IMSI (IMSI: identificación internacional de abonado móvil, de “International Mobile Subscriber Identifier”). Una configuración particularmente ventajosa de la invención prevé que el identificador del cliente en la red de telefonía móvil se genere mediante una aplicación, una llamada aplicación SAT (SAT: set de aplicaciones SIM, de “SIM Application Toolkit”)) ejecutable por parte de un módulo de identificación de abonado de telefonía móvil, SIM, (SIM: módulo de identidad del abonado, de “Subscriber Identity Module”).

En una configuración particularmente preferida de la invención, los identificadores se generan independientemente entre sí. Con esta medida se puede aumentarse todavía más el grado de seguridad de la identidad y especialmente de sus usos en el marco de la autenticación, autentificación y/o autorización, especialmente ya que para un uso no autorizado o abusivo tendría que determinarse o registrarse tanto el identificador del cliente en la red de ordenadores como también el identificador del cliente en la red de telefonía móvil generado independientemente de éste.

Otra configuración especialmente ventajosa de la invención prevé que se encripte el identificador del cliente en la red de ordenadores con una clave que puede determinarse a partir del identificador del cliente en la red de telefonía móvil, preferentemente una clave simétrica. Así puede aumentarse todavía más la seguridad. Otra configuración ventajosa de la invención prevé que se encripte el identificador del cliente en la red de ordenadores con una clave que puede determinarse a partir del identificador del cliente en la red de telefonía móvil y el estado del contador de un dispositivo contador sincronizado de la red de telefonía móvil, preferentemente una clave simétrica. Al considerar el estado del contador de un dispositivo contador de la red de telefonía móvil además del cliente en la red de telefonía móvil y su uso para encriptar el identificador del cliente en la red de ordenadores puede aumentarse todavía más la seguridad de la identidad y su uso que se han de generar, combinativamente según la invención. Ventajosamente, la encriptación se efectúa automáticamente por parte del equipo terminal de datos de la red de ordenadores, con especial preferencia por parte de un equipo terminal de datos de la red de ordenadores que proporciona datos y/o servicios para su acceso a través de la red de ordenadores o por un equipo terminal de datos que esté conectado o puede conectarse a un equipo terminal de datos puesto a disposición para los datos y/o los servicios correspondientes.

En otra configuración de la invención, el cliente es un proceso y/o un usuario de un equipo terminal de datos en la red de ordenadores y/o un proceso y/o un usuario de un terminal móvil que puede funcionar en la red de telefonía móvil.

Una configuración ventajosa de la invención prevé que se use la identidad según la invención para la autenticación de un cliente. Ventajosamente, a este respecto, al cliente se le pide la identidad desde un equipo terminal de datos de la red de ordenadores a través de una conexión de comunicación de la red de ordenadores, y se transmite desde el cliente a través de la conexión de red de comunicación al equipo terminal de datos de la red de ordenadores. Otra configuración de la invención prevé que al cliente se le pida el identificador del cliente en la red de telefonía móvil desde un equipo terminal de datos de la red de ordenadores a través de la conexión de comunicación de la red de ordenadores. Ventajosamente, la petición del identificador del cliente en la red de telefonía móvil se dirige a través de una conexión de comunicación de la red de telefonía móvil a un terminal móvil del cliente que puede funcionar en la red de telefonía móvil, por parte del terminal móvil del cliente se genera el identificador del cliente en la red de

telefonía móvil y el identificador del cliente generado en la red telefonía móvil lo transmite desde el terminal móvil del cliente a través de y/o usando una conexión de comunicación de la red de telefonía móvil hasta el equipo terminal de datos de la red de ordenadores. Una configuración particularmente preferida de la invención prevé que la conexión de comunicación de la red de telefonía móvil sea una conexión de comunicación que permita una conexión en la red de ordenadores, preferentemente que sea una conexión de comunicación que use un protocolo según la especificación WAP (WAP: protocolo de aplicaciones inalámbricas, de “Wireless Application Protocol”).

Ventajosamente, por parte del equipo terminal de datos de la red de ordenadores se genera un identificador del cliente en la red de ordenadores y se encripta para generar la identidad del cliente con el identificador de la red de telefonía móvil. A este respecto, la identidad del cliente en el sistema de comunicación útil según la invención para la autenticación se mejora todavía más en cuanto a la seguridad, especialmente ya que el identificador del cliente en la red de telefonía móvil necesario para la encriptación se pide en primer lugar y preferentemente sólo está disponible y se utiliza a petición del equipo terminal de datos de la red de ordenadores.

La identidad según la invención se usa ventajosamente para la autenticación o la autentificación de un cliente en el sistema de comunicación, pudiendo utilizarse la utilización tanto para la autentificación en la red de telefonía móvil como para la autentificación en la red de ordenadores. Por tanto, una identidad según la invención puede usarse ventajosamente para la autentificación de compras de mercancías y/o servicios, o aplicaciones similares del comercio electrónico, el llamado E-commerce, que se realicen a través de la red de telefonía móvil y/o la red de ordenadores mediante terminales móviles correspondientes, con un alto grado de seguridad. En conjunto, mediante esto puede aumentarse la confianza en un comercio correspondiente entre dos socios comerciales.

En una configuración preferida de la invención, la autentificación según la invención se realiza por parte de un equipo terminal de datos de la red de ordenadores. A este respecto, en el marco de la autentificación se realiza ventajosamente una descomposición de la identidad en el identificador del cliente en la red de ordenadores y en el identificador del cliente en la red de telefonía móvil, El identificador del cliente en la red de ordenadores determinado o adquirido en el marco de la descomposición de la identidad se autentifica ventajosamente, preferentemente mediante al menos una comparación por parte del equipo terminal de datos de la red de ordenadores.

Según otra configuración particularmente preferida de la invención, el procedimiento según la invención se usa para la autorización de un acceso a los datos y/o servicios de un equipo terminal de datos de una red de ordenadores.

Es además objeto de la presente invención un sistema de comunicación compuesto por una red de ordenadores con un equipo terminal de datos y una red de telefonía móvil celular, preferentemente según el estándar de redes de radio GSM y/o UMTS con terminales móviles que pueden funcionar en ella, estando configurados los equipos terminales de datos, los equipos de la red de telefonía móvil, especialmente aquellos equipos implicados en la gestión, el establecimiento y/o el mantenimiento de una conexión de comunicación en la red de telefonía móvil y/o los terminales móviles, para la ejecución y/o la utilización de un procedimiento según la invención.

Es además objeto de la invención un terminal móvil para su utilización en una red de telefonía móvil celular con un módulo de identificación del abonado de telefonía móvil (SIM), así como un módulo de identificación del abonado de telefonía móvil (SIM) para utilizarlo con un terminal móvil que pueda funcionar en una red de telefonía móvil celular que están configurados para la ejecución de un procedimiento según la invención en un sistema de comunicación según la invención. En una configuración particularmente preferida de la invención, el procedimiento es almacenado por parte del módulo de identificación del abonado de telefonía móvil (SIM) como programa de aplicación y/o también ejecutable por parte del mismo. El terminal móvil que puede funcionar en la red de telefonía móvil es ventajosamente un teléfono de red móvil y/o una tarjeta insertable en relación con un equipo terminal de datos que puede funcionar en la red de telefonía móvil, preferentemente en el formato PCMCIA, o una mochila que se pueda operar en una red de telefonía móvil, preferentemente con una conexión USB para conectarla a un equipo terminal de datos.

Otras particularidades, características y ventajas de la invención se explicarán a continuación mediante los ejemplos de realización de la invención representados en las figuras del dibujo. Muestran:

la Fig 1: en una representación esquemática de la representación del principio un sistema de comunicación según la invención para la utilización de una identidad según la invención para una autorización de acceso a datos y/o servicios de un equipo terminal de datos en una red de ordenadores

la Fig 2: en una representación esquemática un diagrama de flujo de un ejemplo de realización de una sincronización según la invención de una identidad según la invención para una autorización de acceso y

la Fig 3: en una representación esquemática un diagrama de flujo de un ejemplo de realización de una resincronización según la invención de una identidad según la invención para una autorización de acceso cuando o mientras no existe disponibilidad en una red de telefonía móvil

En la Fig. 1 está en una representación esquemática el acceso de un cliente (usuario final, “end user”) a una red privada virtual (VPN), en la presente en forma de una red de ordenadores de una empresa que presenta distintos equipos terminales de datos, la llamada intranet (empresa, “company”). A este respecto, el cliente (usuario final, “end

user") es, en la presente, un empleado de la empresa y realiza, por ejemplo, tareas para la empresa desde su domicilio o sitios similares alejados de la empresa. Para ello, el cliente (usuario final, "end user") utiliza, en la presente, para una utilización móvil un equipo terminal de datos móvil o portátil, en la presente en forma de un ordenador portátil y un terminal móvil que puede funcionar en una red de telefonía móvil (teléfono móvil, de "mobile phone"). A este respecto, el cliente (usuario final, "end user") accede a través de la red de telefonía móvil y/o a través de internet como red de ordenadores a la intranet de la empresa (company). A este respecto, la red empresarial/intranet (company) está conectada ventajosamente a través de un llamado "VPN de sitio a sitio" (Site to Site VPN) a través de Internet, a la red de telefonía móvil de un operador de telefonía móvil, preferentemente a través de un servidor de acceso (access server, access provider) que proporciona un llamado dispositivo de seguridad ("Security Appliance") representado simbólicamente en la Fig. 1.

Los accesos a la red de ordenadores empresarial (company) se realizan a través de la red de telefonía móvil (red móvil, de "mobile network") o la red de ordenadores (internet) utilizando al menos una identidad del cliente generada con una información temporal ($T_{cliente}$) sincronizada con la información temporal fijada por parte de la red de telefonía móvil (T_{red}). A este respecto, la sincronización de las informaciones temporales representadas simbólicamente en la Fig. 1 mediante una línea discontinua entre el equipo OTA/USSD ("OTA/USSD") de la red de telefonía móvil (VGC) representado abajo y la interfaz OTA/USSD ("OTA/USSD interface) colocada encima que representa o proporciona el servicio de autentificación (UA-Service).

Al generar el identificador se utiliza en la presente además una identidad generada mediante combinación de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil. A este respecto, aquí se utiliza un sistema de autentificación que no está explícitamente representado que es dado por parte de la red de telefonía móvil y pone a disposición una autentificación segura de 2 factores para conexiones entre los respectivos clientes (usuario final, de "end user") y la red empresarial (company). Así se proporciona un acceso seguro de los clientes (usuario final, de "end user") a la red de la empresa (company).

La Fig. 1 deja ver además las particularidades en el marco de una autentificación de un acceso de un cliente (usuario final, de "end user") a la red de ordenadores empresarial (company). El cliente (usuario final, de "end user") o su equipo terminal de datos está conectado, como se ha explicado antes, con la red de ordenadores a través de una conexión de comunicación adecuada. El acceso a la red de ordenadores se realiza a este respecto mediante un llamado proveedor de acceso (proveedor de acceso, de "access provider") a través de una conexión inalámbrica y/o unida por cable entre el terminal o los terminales de datos respectivos del cliente (usuario final, de "end user"), en la presente, por ejemplo, a través de un terminal móvil que puede funcionar en una red de telefonía móvil, una llamada conexión WLAN o una conexión DSL. Por tanto, a través de la red de ordenadores (internet) el cliente (usuario final, de "end user") se puede conectar con equipos terminales de datos correspondientes de la empresa (company). El acceso a los equipos terminales de datos de la empresa (company) se realiza a este respecto a través de una pasarela de la empresa UA (UA: pasarela de auteticación del usuario, de "user authentication gateway") que no se representa explícitamente en la Fig. 1 que realiza la autentificación. La pasarela UA está dispuesta en la presente por parte de la empresa (company) y está conectada a través de internet con el proveedor de acceso para el acceso del cliente (usuario final, de "end user") a la red de ordenadores (internet), con una base de datos mantenida por parte de la red empresarial con entradas de clientes (directorio de base de datos de usuario, de "directory of user database") y con equipos terminales de datos de un operador de red de telefonía móvil (mobile network provider). A este respecto, por parte del operador de telefonía móvil (mobile network provider) se prevén dispositivos que proporcionan los servicios de autentificación correspondientes de los clientes (UA-Service) que se refieren especialmente a la sincronización de la información temporal ("OTA/USSD") y el identificador del cliente (usuario final, de "end user") en la red de telefonía móvil. Cuando un cliente accede a la intranet de una empresa (company), el acceso del cliente (usuario final, de "end user") a la red de empresarial se realiza a través de un acceso móvil del cliente (usuario final, de "end user") a través de una red de telefonía móvil a través de la red de ordenadores (internet). A través del acceso de la red de telefonía móvil de un operador de red de telefonía móvil (mobile network provider/MSSP) se hace posible el acceso móvil del cliente (usuario final, de "end user") mediante los servicios de comunicación correspondientes (service channel, Webservices) a través de un proveedor de acceso con equipos terminales de datos apropiados para ello, en la presente, por ejemplo, un servidor de acceso (AAA-Server) de acceso seguro.

El diagrama de flujo representado esquemáticamente en la Fig. 2 muestra un ejemplo de realización básico de una sincronización de una identidad según la invención para una autorización de un acceso a datos y/o servicios de un equipo terminal de datos en una red privada virtual y los a este respecto o entre los distintos dispositivos de un sistema de comunicación que presenta una red de ordenadores y una red de telefonía móvil celular.

El usuario (usuario final, de "end user") de un terminal inicia la generación de una identidad por parte de su terminal móvil en la etapa de procedimiento o de secuencias marcada con "Select OTP".

El terminal móvil (mobile phone) del usuario (usuario final, de "end user") activa a continuación una aplicación de generación de identidad (call OTP applet) por parte de la tarjeta SIM (SIM-card; SIM: módulo de identificación del abonado, de "Subscriber Identity Module") insertada en el terminal móvil (mobile phone). A este respecto, para la sincronización de la información temporal se determina la información temporal (local time) dada por parte del terminal móvil (mobile phone) o la tarjeta SIM (SIM card) y se transmite a través de la interfaz OTA/USSD

representada en la Fig. 1, junto con un identificador para la generación de la identidad (SC; SC: session counter), al sistema que proporciona como valores de referencia informaciones temporales únicas que sirven en toda la red, dadas por parte de la red de telefonía móvil, en la presente OTA/USSD (véanse las Fig. 1 y Fig. 2).

Por parte del OTA/USSD, en la presente se calcula la diferencia entre la información temporal (T_{red}) en la red de telefonía móvil y la información temporal ($T_{cliente}$; local time) por parte del terminal móvil (mobile phone) del usuario (usuario final, de "end user") y se transmite un valor de corrección correspondientemente calculado al terminal móvil (mobile phone) del usuario (usuario final, de "end user") y de éste a la tarjeta SIM (SIM card) de éste. Simultáneamente, en la presente se activa por parte del OTA/USSD un contador en una aplicación correspondiente y/o dispositivo que registra la generación de identidad correspondiente para un comprobación posterior (check session counter).

Por parte de la tarjeta SIM del usuario (usuario final, de "end user"), la información temporal ($T_{cliente}$; local time) se sincroniza por parte del terminal móvil (mobile phone) del usuario (usuario final, de "end user") con el valor de corrección calculado y con la información temporal sincronizada ($T_{cliente}$; local time) se genera, mediante cómputo, una identidad (OTP; OTP=función de (local time, key, SC). La identidad (OTP) se muestra luego por parte del terminal móvil (mobile phone) al usuario (usuario final, de "end user") (display OTP(otp1)) y para la validación la transmite al dispositivo previsto por parte de la red de telefonía móvil (UA validation; UA authentication).

Por parte del sistema de validación (UA validation), de la identidad (OTP(otp1)) se extrae el identificador para la generación de la identidad (SC). Con el indicador extraído para la generación de la identidad (SC) entonces se consulta por parte del OTA/USSD la información temporal asociada (get local time (SC)) y comprueba el contador correspondiente (check session counter). Como resultado (Time=local time or computed time), el OTA/USSD proporciona entonces la información temporal presente por parte del terminal móvil ($T_{cliente}$; local time) o la calculada por parte del terminal móvil ($T_{cliente}$; local time). Esta información se transmite desde sistema de validación (UA validation) a un dispositivo para la validación de la información temporal (time validation) y valida correspondientemente la información temporal determinada de la identidad (OTP(otp1)). En el caso de validación positiva, por ejemplo, coincidencia de la información temporal, en primer lugar se le indica esto al sistema de validación (UV validation). El sistema de validación (UV validation) le indica a continuación o posteriormente la validación de la identidad al usuario (usuario final, de "end user").

El diagrama de flujo representado esquemáticamente en la Fig. 3 muestra una resincronización de una identidad para una autorización de acceso en y/o después de una no disponibilidad de un terminal móvil (mobile phone) de un usuario (usuario final, de "end user") en una red de telefonía móvil.

El usuario (usuario final, de "end user") de un terminal móvil inicia en la etapa de procedimiento o de secuencia marcada con "select resync" la generación de una identidad por parte de su terminal móvil (mobile phone). La iniciación de la etapa de procedimiento o de secuencia "select resync" puede realizarse a este respecto ventajosamente de forma automática cuando se confirma una no disponibilidad en la red de telefonía móvil por parte del terminal móvil.

El terminal móvil (mobile phone) del usuario (usuario final, de "end user") activa a continuación una función de resincronización (call resync function) correspondiente por parte de la tarjeta SIM (SIM-card; SIM: módulo de identificación de abonado, de "Subscriber Identity Module") insertada en el terminal móvil (mobile phone) del usuario. En el marco de la función de resincronización (call resync function), la disponibilidad de la red de telefonía móvil (check coverage) se comprueba por parte de la tarjeta SIM (SIM-card) y genera dos identificadores o identidades (produce two OTP). Los identificadores o identidades generados se muestran (display OTP1, OTP2, time) luego por parte del terminal móvil (mobile phone) al usuario (usuario final, de "end user") junto con la información temporal (time) del terminal móvil (mobile phone) y para la validación (resync OTP1, OTP2, time) se transmiten al dispositivo (UA validation; UA: user authentication) provisto por parte de la red de telefonía móvil.

Por parte del sistema de validación (UA validation), utilizando un sistema (counter validation) se valida inicialmente la primera identidad y luego, si el resultado de la validación es positivo, la segunda identidad (OTP2). Si ambas identidades son validadas positivamente, por parte del dispositivo de validación (UA validation) se calcula una diferencia temporal (compute delta(time, utc time)). Si esta diferencia temporal se mantiene dentro de un intervalo que se puede fijar, dentro del cual tiene o tendría que realizarse la validación de las identidades (OTP1, OTP2), se transmite una información de validación positiva correspondiente desde el dispositivo de validación (UA validation) al usuario (usuario final, de "end user").

Otras particularidades, características y ventajas de la invención se desprenden de los siguientes escenarios de aplicación ventajosos reproducidos de la invención:

1. Disponibilidad en la red de telefonía móvil (in network coverage support)

- sincronización de la información temporal del terminal móvil y de la información temporal de un servidor de validación mediante un servicio de la red de telefonía móvil, por ejemplo, basado en USSD o SMS (Synchronize handset time and Validation Server time via a network service, which may be USSD or SMS based).

- el servicio de la red de telefonía móvil sabe cuándo tiene que hacer un cálculo del tiempo relativo debido a un elemento de información de la sesión (SC) dispuesto por el servidor de validación que puede estar contenido separadamente en la identidad (OTP; OTP One Time Password) (The network service knows when to compute a relative time, by getting presented a session information element (SC) from the Validation Server, which maybe hashed into the One Time Password).

- cuando el dispositivo móvil está conectado a la red de telefonía, es decir, cuando está disponible en la misma, siempre se sincronizan las informaciones temporales (When the handset is connected to the network time sources are always synchronized).

- en caso de que el terminal móvil no esté disponible en la red de telefonía móvil, se siguen (rastrean) los cambios de las informaciones temporales de la tarjeta SIM registra los cambios y se pasan de de un modo y manera inteligente a un servidor de la red de telefonía móvil para poder garantizar una sincronización con la información temporal en la red de telefonía móvil para la mayoría de las necesidades de la aplicación (Timer changes are tracked by the SIM for the out of coverage support and are pushed to the network server in an intelligent way to support a synchronized network time for most out of coverage requests).

2. No disponibilidad en la red de telefonía móvil (Out of network coverage support)

- el tiempo local dado por parte del terminal móvil se utiliza por la tarjeta SIM junto con los cambios de información temporal registrados para generar la identidad (OTP) (Local Time is used by the SIM together with tracked time changes to compute the OTP).

- los cálculos de tiempo en la red de telefonía móvil se basan en la última información temporal positivamente sincronizada (Timing computations in the network are based on the latest positive synchronization time).

- las informaciones temporales relativas proporcionan un mecanismo de seguridad cuando el temporizador o la información temporal del terminal móvil no está apagado (por ejemplo, puesto a cero, al cambiar la batería o cuando hay problemas de batería) (Relative timings provide a secure mechanism when the handset clock has not been switched off (e.g. or reset, e.g. battery change, battery problem).

3. No disponibilidad en la red de telefonía móvil y fuera de una sincronización de la información (Out of Network Coverage and out of time sync)

- el usuario puede utilizar un procedimiento de conteo como un algoritmo de restablecimiento hasta que exista de nuevo disponibilidad en la red de telefonía móvil (user may use a counter method as a fallback algorithm until in coverage again).

- para aumentar la seguridad el usuario puede sincronizar de nuevo los tiempos iniciales mediante un contador basado o que recurra a identidades (OTP) (o a dos identidades consecutivas) y a una información temporal. A este respecto, el usuario tiene que transmitir las identidades (OTP) (o dos identidades consecutivas) y la información temporal a la interfaz de administrador (administrator) o de autoservicio (self-service) (los valores se muestran por una función de resincronización en la SIM) (To increase security user can resynchronize time sources via a counter based OTPs (or 2 consecutive OTP) and a TIME, which the user has to provide to the administrator or the self service interface (these values are displayed by the resynchronize function on the SIM).

Para minimizar el tráfico de la red de telefonía móvil, el servidor de validación puede preguntar a sus fuentes de tiempos locales inicialmente y sólo al servidor de la red de telefonía cuando falle el primer intento de validación. El servidor de red de telefonía móvil puede proporcionar la fuente de tiempos más precisa en función del último instante en el que el terminal móvil o la SIM estaba disponible en la red de telefonía móvil. El servidor de validación puede funcionar o configurarse de forma segura por parte de la empresa o por parte del proveedor de red de telefonía móvil. (To minimize network traffic Validation Server may try with its local time sources first and only ask the network server, when the first validation attempt failed. The network server may provide the more accurate time source depending on the last time the handset/SIM was in coverage. Validation Servers can securely run at the corporate or at mobile network provider).

Los ejemplos de realización de la invención representados en las figuras del dibujo y los escenarios de aplicación de la invención reproducidos sirven simplemente para explicar la invención y no limitan ésta.

REIVINDICACIONES

1. Procedimiento para la generación de una identidad de clientes en un sistema de comunicación que presenta una red de ordenadores y una red de telefonía móvil celular, en el que la identidad de un cliente se genera utilizando al menos una información temporal $T_{cliente}$ sincronizada con una información temporal T_{red} prefijada por parte de la red de telefonía móvil, en el que la información temporal $T_{cliente}$ utilizada para la generación de la identidad del cliente se proporciona por un dispositivo de sincronización presente por parte de un terminal móvil del cliente que puede funcionar en la red de telefonía móvil y/o por parte de un módulo de identificación de abonado de telefonía móvil, SIM, utilizado por el terminal móvil, **caracterizado porque**, en caso de necesidad, la información temporal $T_{cliente}$ utilizada para la generación de la identidad del cliente se sincroniza en el marco del intercambio de informaciones de señalización entre el terminal móvil y la red de telefonía móvil con la información temporal T_{red} prefijada por parte de la red de telefonía móvil.

2. Procedimiento según la reivindicación 1, **caracterizado porque** la necesidad se determina considerando al menos una información en cuanto a la disponibilidad del terminal móvil en la red de telefonía móvil.

3. Procedimiento según la reivindicación 1 o la reivindicación 2, **caracterizado porque** la información temporal $T_{cliente}$ utilizada para la generación de la identidad del cliente se sincroniza con la información temporal T_{red} prefijada por parte de la red de telefonía móvil después de un intervalo de tiempo en el marco del intercambio de informaciones de señalización entre el terminal móvil y la red de telefonía móvil.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado porque** la información temporal $T_{cliente}$ utilizada para la generación de la identidad del cliente se sincroniza con la información temporal T_{red} prefijada por parte de la red telefonía móvil al menos en el marco del intercambio de informaciones de señalización para el establecimiento, el mantenimiento y/o la terminación de una conexión entre el terminal móvil y la red de telefonía móvil.

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado porque** la sincronización de la información temporal $T_{cliente}$ se realiza usando al menos un dispositivo contador por lo menos si el terminal móvil no está disponible en la red de telefonía móvil.

6. Procedimiento según la reivindicación 5, **caracterizado porque** el dispositivo contador está previsto por parte de la red de telefonía móvil, se activa en caso de no disponibilidad del terminal móvil en la red de telefonía móvil y si el terminal móvil vuelve a estar disponible en la red de telefonía móvil transmite un valor del contador determinado por el dispositivo contador al terminal móvil que se utiliza por parte del terminal móvil para sincronizar la información temporal $T_{cliente}$.

7. Procedimiento según una de las reivindicaciones 1 a 6, **caracterizado porque** la identidad del cliente se genera mediante combinación de un identificador del cliente en la red de ordenadores y un identificador del cliente en la red de telefonía móvil.

8. Procedimiento según la reivindicación 7, **caracterizado porque** el identificador del cliente en la red de ordenadores se genera un algoritmo criptográfico, preferentemente por parte de un equipo terminal de datos de la red de ordenadores.

9. Procedimiento según la reivindicación 7 o la reivindicación 8, **caracterizado porque** el identificador del cliente en la red de ordenadores se genera usando un identificador primario del cliente en la red de ordenadores y un dispositivo contador, estando el dispositivo contador preferentemente diseñado para usar un algoritmo criptográfico y siendo especialmente preferido un componente del equipo terminal de datos.

10. Procedimiento según una de las reivindicaciones 7 a 9, **caracterizado porque** el identificador del cliente en la red de telefonía móvil se genera con un algoritmo criptográfico, preferentemente por parte de un terminal móvil del cliente que puede funcionar en la red de telefonía móvil.

11. Procedimiento según una de las reivindicaciones 7 a 10, **caracterizado porque** el identificador del cliente en la red de telefonía móvil se genera usando un identificador primario del cliente en la red de telefonía móvil y un dispositivo contador, estando el dispositivo contador preferentemente configurado para usar un algoritmo criptográfico y siendo especialmente preferido un componente del equipo terminal móvil y/o de un módulo de identificación de abonado de telefonía móvil, SIM, utilizado por el terminal móvil.

12. Procedimiento según una de las reivindicaciones 7 a 11, **caracterizado porque** los identificadores se generan independientemente entre sí.

13. Procedimiento según una de las reivindicaciones 7 a 12, **caracterizado porque** el identificador del cliente en la red de ordenadores se encripta con una clave que puede determinarse a partir del identificador del cliente en la red de telefonía móvil, preferentemente una clave simétrica.

14. Procedimiento según una de las reivindicaciones 7 a 13, **caracterizado porque** el identificador del cliente en la

red de ordenadores se encripta con una clave que puede determinarse a partir del identificador del cliente en la red de telefonía móvil y el estado del contador de un dispositivo contador sincronizado de la red de telefonía móvil, preferentemente una clave simétrica.

15. Procedimiento según una de las reivindicaciones 1 a 14, **caracterizado porque** el cliente es un proceso y/o un usuario de un equipo terminal de datos en la red de ordenadores y/o un proceso y/o un usuario de un terminal móvil que puede funcionar en la red de telefonía móvil.

16. Procedimiento según una de las reivindicaciones 1 a 15, **caracterizado porque** la identidad se usa para la autenticación de un cliente.

17. Procedimiento según la reivindicación 16, **caracterizado porque** un equipo terminal de datos de la red de ordenadores solicita la identidad del cliente a través de una conexión de comunicación de la red de ordenadores y el cliente la transmite a través de la conexión de comunicación al equipo terminal de datos de la red de ordenadores.

18. Procedimiento según la reivindicación 18 o la reivindicación 17, **caracterizado porque** un equipo terminal de datos de la red de ordenadores solicita al cliente el identificador del cliente en la red de telefonía móvil a través de una conexión de comunicación de la red de ordenadores.

19. Procedimiento según la reivindicación 18, **caracterizado porque** la solicitud del identificador del cliente en la red de telefonía móvil a través de una conexión de comunicación de la red de telefonía móvil se dirige a un terminal móvil del cliente que puede funcionar en la red de telefonía móvil, se genera el identificador del cliente en la red de telefonía móvil por parte del terminal móvil del cliente y el identificador generado del cliente en la red de ordenadores se transmite al equipo terminal de datos de la red de ordenadores a través de y/o usando una conexión de comunicación de la red de telefonía móvil.

20. Procedimiento según la reivindicación 19, **caracterizado porque** la conexión de comunicación de la red de telefonía móvil es una conexión de comunicación que hace posible una conexión en la red de ordenadores, preferentemente una conexión de comunicación que usa protocolos según la especificación WAP.

21. Procedimiento según una de las reivindicaciones 18 a 20, **caracterizado porque** el identificador del cliente se genera por parte del equipo terminal de datos en la red de ordenadores y se encripta con el identificador del cliente en la red de telefonía móvil para generar la identidad del cliente.

22. Procedimiento según una de las reivindicaciones 16 a 21, **caracterizado porque** la autentificación se realiza por parte de un equipo terminal de datos de la red de ordenadores.

23. Procedimiento según una de las reivindicaciones 16 a 22, **caracterizado porque** en el marco de la autentificación se realiza una descomposición de la identidad en el identificador del cliente en la red de ordenadores y en el identificador del cliente en la red de telefonía móvil.

24. Procedimiento según una de las reivindicaciones 16 a 23, **caracterizado porque** el identificador del cliente en la red de ordenadores determinado en el marco de la descomposición de la identidad se autentifica, preferentemente mediante al menos una comparación por parte del equipo terminal de datos de la red de ordenadores.

25. Procedimiento según una de las reivindicaciones 1 a 24, **caracterizado porque** éste se usa para la autorización de un acceso de un dispositivo terminal de datos a datos y/o servicios de un equipo terminal de datos en una red de ordenadores.

26. Sistema de comunicación constituido por una red de ordenadores con equipos terminales de datos y una red de telefonía móvil celular con terminales móviles que pueden funcionar en ella, **caracterizado porque** los equipos terminales de datos, los equipos de la red de telefonía móvil y/o los terminales móviles están configurados para ejecutar y/o usar un procedimiento según una de las reivindicaciones 1 a 25.

27. Terminal móvil para su uso en una red de telefonía móvil celular con un módulo de identificación de abonado de telefonía móvil, SIM, **caracterizado porque** éste está configurado para ejecutar un procedimiento según una de las reivindicaciones 1 a 25, preferentemente en un sistema de comunicación según la reivindicación 26.

28. Módulo de identificación de abonado de telefonía móvil, SIM, para su uso con un terminal móvil que puede funcionar en una red de telefonía móvil delular, **caracterizado porque** éste está configurado para ejecutar un procedimiento según una de las reivindicaciones 1 a 25, preferentemente en un sistema de comunicación según la reivindicación 26.

29. Módulo de identificación de abonado de telefonía móvil, SIM, según la reivindicación 28, **caracterizado porque** el procedimiento se almacena y/o puede ejecutarse como programa de aplicación por parte del módulo de identificación de abonado de telefonía móvil, SIM.

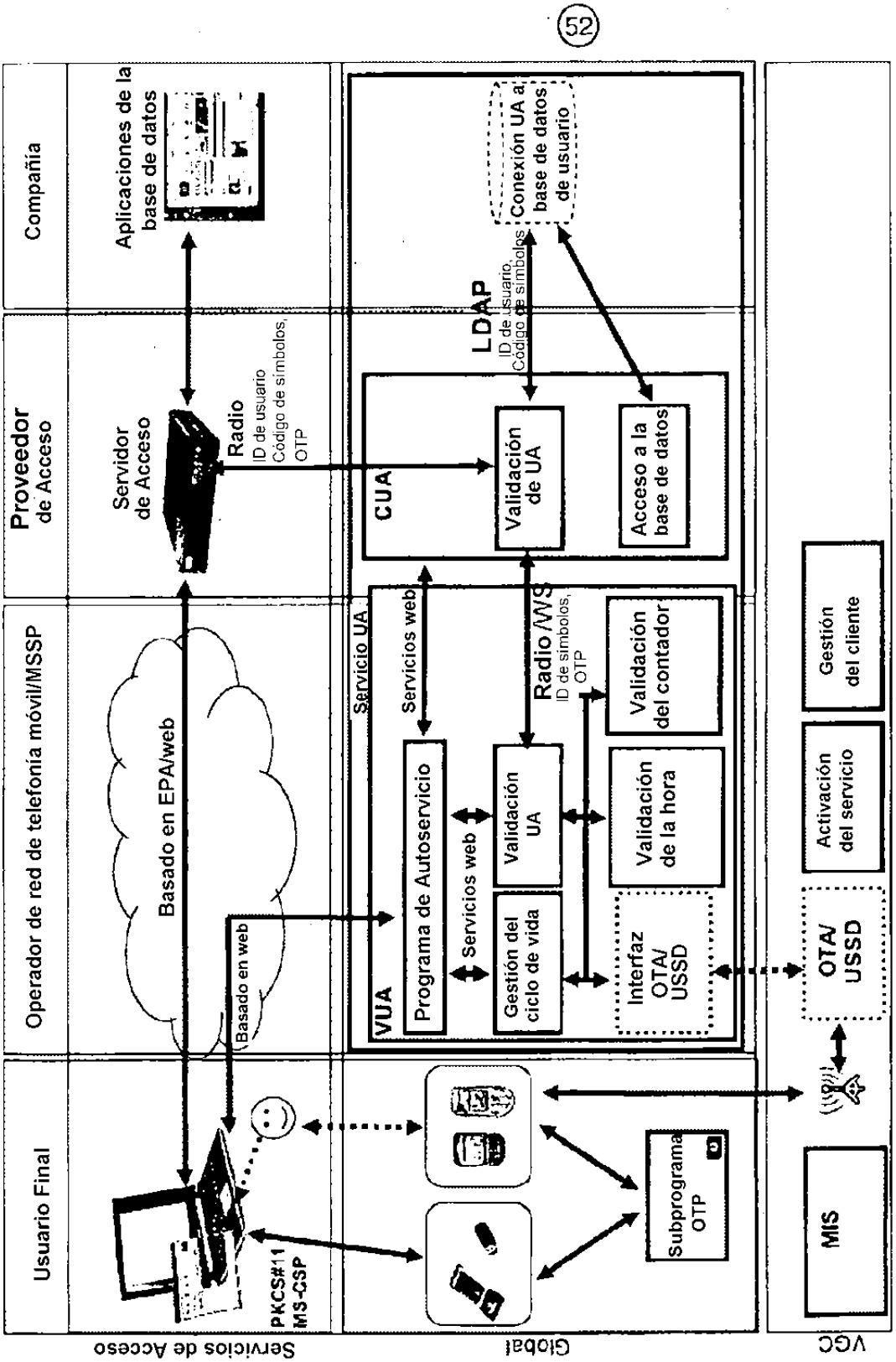
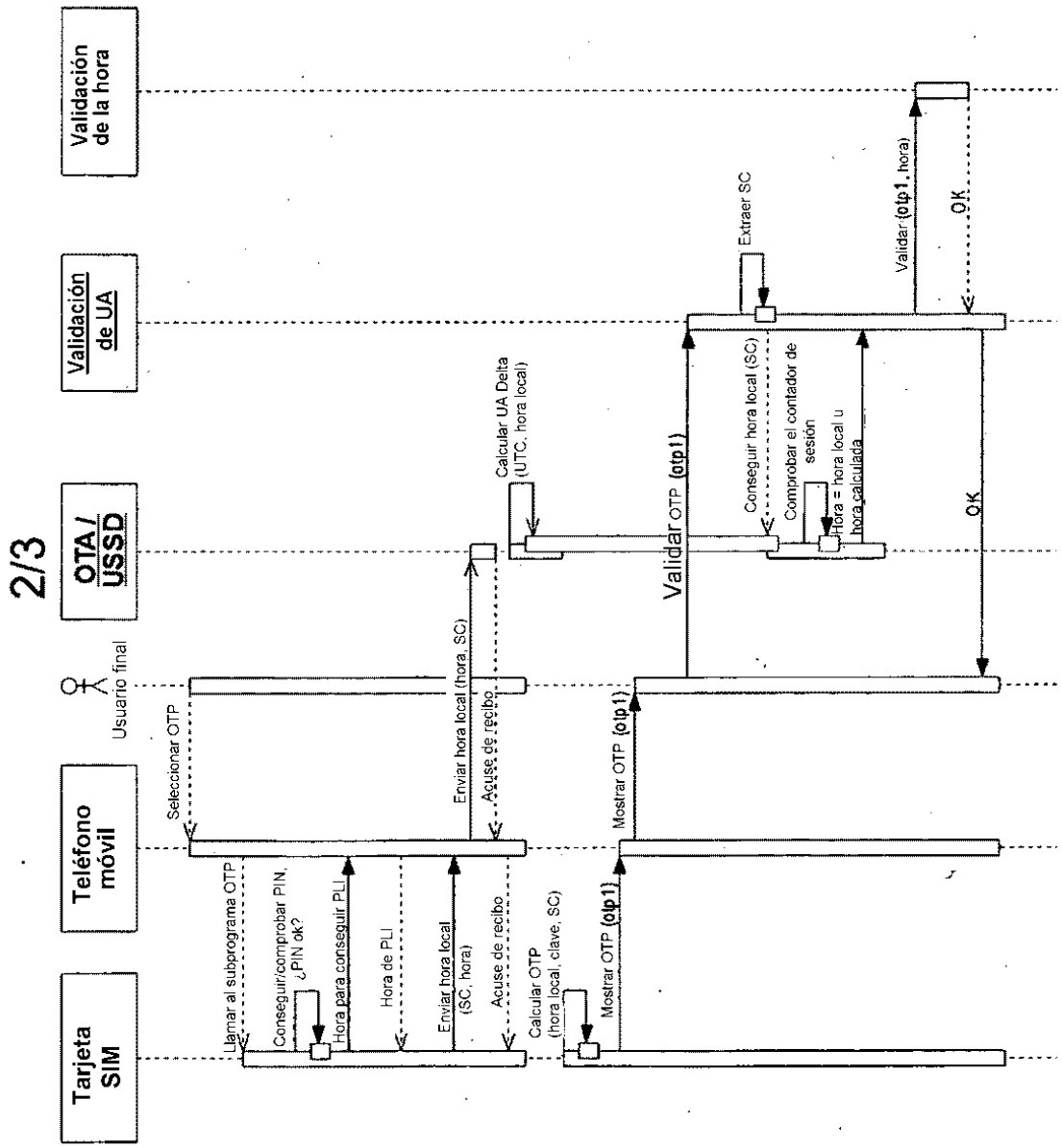

1/3
52
Usuario Final
Operador de red de telefonía móvil/MSSP
Proveedor de Acceso
Compañía
Aplicaciones de la base de datos
Servidor de Acceso
Radio
ID de usuario
Código de símbolos,
OTP
Basado en EPA/web
Basado en web
PKCS#11
MS-CSP
LDAP
ID de usuario,
Código de símbolos
Conexión UA a base de datos de usuario
CUA
Validación de UA
Acceso a la base de datos
Servicio UA
Servicios web
Radio/WS
ID de símbolos,
OTP
VUA
Programa de Autoservicio
Servicios web
Validación UA
Gestión del ciclo de vida
Validación del contador
Validación de la hora
Interfaz OTA/ USSD
Subprograma OTP
OTA/ USSD
Activación del servicio
Gestión del cliente
MIS
Servicios de Acceso
Global
VGC

Fig. 1


Validación de la hora
Validación de UA
OTA / USSD
Usuario final
Teléfono móvil
Tarjeta SIM
Seleccionar OTP
Llamar al subprograma OTP
Conseguir/comprobar PIN, ¿PIN ok?
Hora para conseguir PLI
Hora de PLI
Enviar hora local (SC, hora)
Acuse de recibo
Calcular OTP (hora local, clave, SC)
Mostrar OTP (otp1)
Enviar hora local (hora, SC)
Acuse de recibo
Calcular UA Delta (UTC, hora local)
Validar OTP (otp1)
Extraer SC
Conseguir hora local (SC)
Comprobar el contador de sesión
Hora = hora local u hora calculada
Validar (otp1, hora)
OK
OK

2/3

Fig. 2

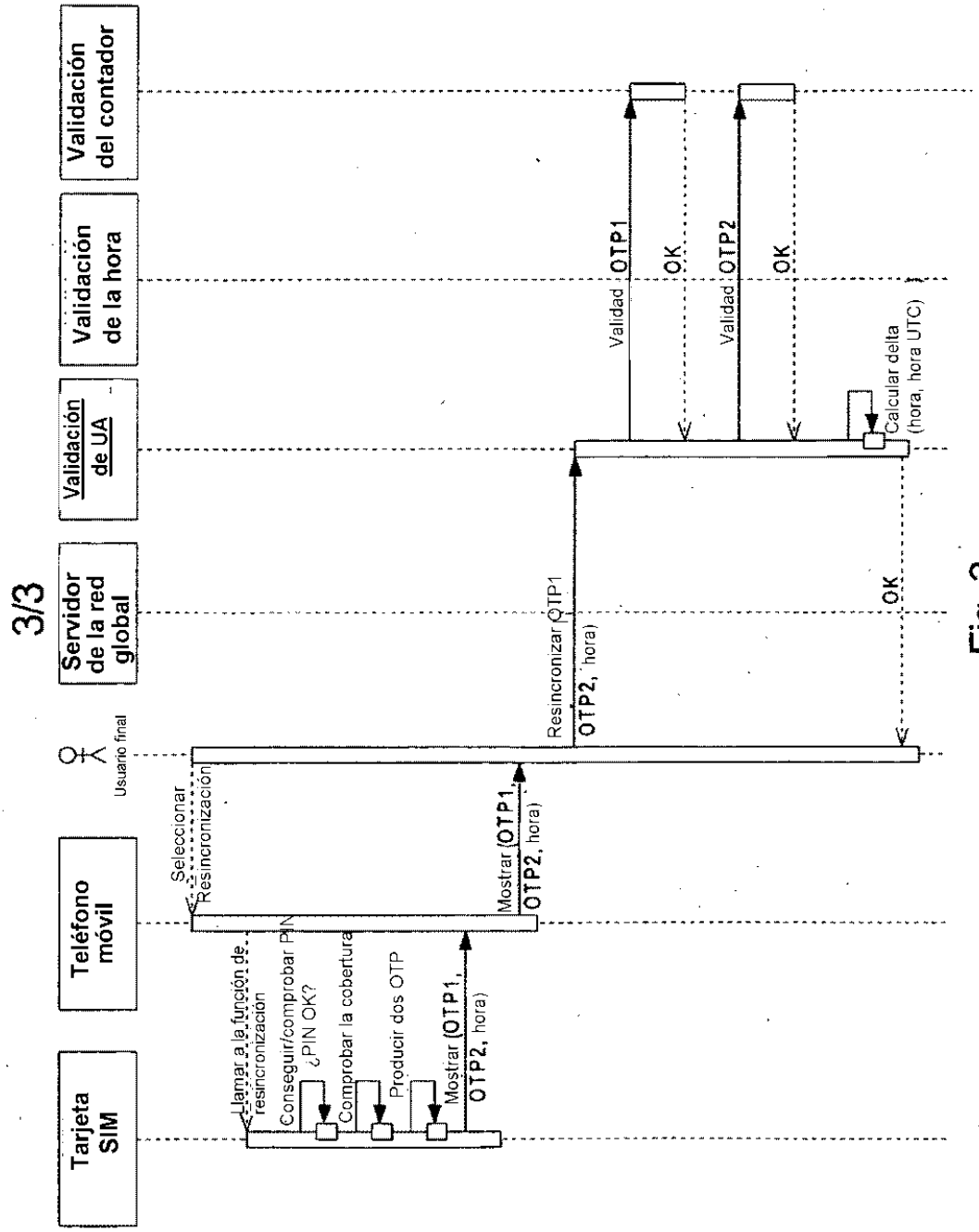

3/3
Tarjeta SIM
Teléfono móvil
Usuario final
Servidor de la red global
Validación de UA
Validación de la hora
Validación del contador
Seleccionar Resincronización
Llamar a la función de resincronización
Conseguir/comprobar PIN
¿PIN OK?
Comprobar la cobertura
Producir dos OTP
Mostrar (OTP1, OTP2, hora)
Mostrar (OTP1, OTP2, hora)
Resincronizar (OTP1 OTP2, hora)
Validad OTP1
OK
Validad OTP2
OK
Calcular delta (hora, hora UTC)
OK

Fig. 3