(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 979**

(51) Int. CI.:
H04W 12/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06020712 .3**
(96) Fecha de presentación: **02.10.2006**
(97) Número de publicación de la solicitud: **1773089**
(97) Fecha de publicación de la solicitud: **11.04.2007**

(54) Título: **Procedimiento, sistema y dispositivo para la creación y/o el uso de identidades de clientes en un sistema de comunicación**

(30) Prioridad:
05.10.2005 DE 102005047798

(45) Fecha de publicación de la mención BOPI:
05.10.2012

(45) Fecha de la publicación del folleto de la patente:
05.10.2012

(73) Titular/es:
VODAFONE HOLDING GMBH
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:
Stephan, Jungblut y
Bone, Nick

(74) Agente/Representante:
Carpintero López, Mario

DESCRIPCIÓN

Procedimiento, sistema y dispositivo para la creación y/o el uso de identidades de clientes en un sistema de comunicación.

La presente invención se refiere a un procedimiento para la creación de una identidad de clientes en un sistema de comunicación que presenta una red de ordenadores orientada a conexión y una red de telefonía móvil celular. Además, la presente invención se refiere al uso de una identidad de acuerdo con la invención para la autenticación y/o autentificación de un cliente. Además, es objeto de la invención una autorización de un acceso de un aparato terminal de datos a datos y/o servicios de un equipo terminal de datos en una red de ordenadores. Además, la invención se refiere a un sistema de comunicación compuesto de una red de ordenadores orientada a conexión con equipos terminales de datos y una red de telefonía móvil celular con aparatos terminales móviles que se pueden hacer funcionar en la misma, estando configurados los equipos terminales de datos, los equipos de la red de telefonía móvil y los aparatos terminales móviles para la realización y/o el uso de un procedimiento de acuerdo con la invención.

Las identidades de clientes, particularmente procesos y/o usuarios de equipos terminales, se usan en redes de comunicación en numerosas aplicaciones para la autenticación, autentificación y particularmente autorización. La autenticación en el sentido de la presente invención es la comprobación de una identidad de un cliente. La autentificación o autentificar en el sentido de la presente invención es un procedimiento en el que se comprueba la identidad de un cliente mediante una determinada característica. De forma correspondiente a esto, en una comprobación de identidad intervienen un abonado que se autentica y un abonado que autentifica al mismo. Después de una comprobación exitosa de la identidad puede realizarse entonces una autorización de un acceso del abonado que se autentica a datos y/o servicios del sistema de comunicación.

En el estado de la técnica se conocen numerosos procedimientos y sistemas que se usan particularmente para la autenticación, autentificación y/o autorización de clientes, creándose o generándose las respectivas identidades de la forma más diversa.

La autenticación y/o autentificación de la identidad de clientes puede realizarse, dependiendo de la configuración de la identidad, la autenticación y/o autentificación de cinco formas diferentes. A este respecto se comprueban las identidades de los clientes con respecto a las propiedades que definen las mismas en el marco de autenticación o autentificación. A este respecto se diferencia por conocimiento, por posesión y/o características biométricas. Una autentificación puede realizarse a este respecto por cinco vías distintas que se pueden combinar entre sí:

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

2. Se sabe algo, por ejemplo, una contraseña.

3. Se es algo o alguien, por ejemplo, comprobación de propiedades biológicas de personas con respecto a huellas dactilares, características faciales y/o de la voz.

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

5. Se sabe hacer algo, preferentemente algo individual; por ejemplo, la capacidad de firma de una persona.

Con combinación de dos de estas posibilidades existe una denominada autentificación de 2 factores, tal como se da, por ejemplo, en relación con tarjetas SIM que se pueden usar en aparatos terminales móviles que se pueden hacer funcionar en redes de telefonía móvil celulares y el o los PIN respectivamente correspondientes.

Tales procedimientos y sistemas se usan, por ejemplo, en el ámbito de redes de telefónica móvil celulares de forma extendida, por ejemplo, en relación con módulos de identificación de abonado de telefonía móvil que posibilitan a un aparato terminal móvil un acceso en o a la red de telefonía móvil, las denominadas tarjetas SIM (SIM: módulo de identificación de abonado), que se usan para esto por norma general en aparatos terminales móviles que se pueden hacer funcionar en redes de telefonía móvil. Además de un identificador específico de tarjeta dado en el lado de las correspondientes tarjetas SIM y por norma general claro, un acceso a o en la red de telefonía móvil requiere adicionalmente la introducción de un número de identificación personal o un código de acceso numérico, un denominado PIN (PIN: número de identidad personal) en el lado de un aparato terminal móvil que usa la tarjeta SIM por el usuario del aparato terminal móvil. En relación con redes de ordenadores orientadas a conexión, por ejemplo, a internet o una intranet, se conocen también numerosos procedimientos y/o sistemas de autenticación, autentificación y/o autorización que posibilitan un acceso a la red de ordenadores, estando creadas o creándose las identidades usadas correspondientemente por clientes de la forma más diversa y del modo más diverso. Un acceso de un usuario humano a datos y/o servicios de un equipo terminal de datos en una red de ordenadores se realiza desde un equipo terminal de datos conectado a la red de ordenadores del usuario por norma general usando una identidad que por norma general está compuesta de un nombre de usuario y una contraseña secreta asignada al nombre de usuario. Un acceso a los datos y/o servicios del equipo terminal de datos que proporciona los mismos se posibilita por el mismo mediante introducción que se realiza por el usuario de nombre de usuario y contraseña

secreta. Para esto, en el lado del equipo terminal de datos que proporciona los datos y/o servicios están almacenados el nombre de usuario y la contraseña secreta asignada al nombre de usuario. Con solicitud de acceso del usuario se comparan el nombre de usuario introducido por el usuario y la contraseña secreta introducida por el usuario en el lado del equipo terminal de datos que proporciona los datos y/o servicios con el nombre de usuario y la contraseña registrados en el lado del equipo terminal de datos que proporciona los datos y/o servicios y con coincidencia se posibilita al usuario o al equipo terminal de datos asignado al usuario un acceso a los datos y/o servicios.

También se conocen sistemas de comunicación en los que los equipos terminales están conectados mediante una red de ordenadores orientada a conexión y/o una red de telefonía móvil celular entre sí por grupos. Tales sistemas de comunicación forman para miembros individuales del grupo o sus aparatos terminales dentro de una empresa o asociación similar una red privada virtual, una denominada VPN (VPN: red privada virtual). La VPN se basa a este respecto por norma general en procedimientos criptográficos. El acceso posibilitado por la red de ordenadores orientada a conexión, por norma general internet y/o la red de telefonía móvil de miembros individuales del grupo a la red privada virtual del grupo usa a este respecto también identidades de clientes y procedimientos para la autenticación, autentificación y/o autorización. La administración del grupo o de los miembros individuales del grupo se realiza a este respecto en el lado de un equipo terminal de datos de la red de ordenadores, por norma general por un denominado servidor de acceso (access-server) de la empresa y/o un correspondiente servidor de acceso o una pasarela (gateway) en el lado de la red de telefonía móvil. A este respecto se realiza la asignación de miembros del grupo al grupo y/o miembros individuales del grupo o grupos en el sistema de comunicación para aplicaciones de comunicación de servicios disponibles en el lado de un equipo de administración correspondiente en el lado del sistema de comunicación.

Con datos y/o servicios accesibles a través de una red de ordenadores orientada a conexión, particularmente internet, de un equipo terminal de datos se deben evitar accesos y/o usos no autorizados y/o abusivos de los datos y/o servicios. Esto se cumple particularmente con un acceso de un trabajador de una empresa a datos y/o servicios de un equipo terminal de datos de una red de la empresa, una denominada 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, con un acceso del trabajador de la empresa a equipos terminales de datos en la empresa desde su vivienda o lugares externos a la empresa similares. Para evitar accesos no autorizados o abusivos se conocen en el estado de la técnica durante la creación y/o el uso de identidades particularmente en relación con una autenticación, autentificación y/o autorización distintos procedimientos y métodos criptográficos que comprenden un cifrado o descifrado de y/o con identidades. A este respecto se usan particularmente procedimientos y/o sistemas criptográficos asimétricos, que para el aumento de la seguridad de cifrados o descifrados usan por normal general claves conocidas por todos y secretas, siendo las claves secretas secretas o privadas para el abonado que autentica y el abonado que autentifica de una correspondiente comprobación de identidad, a diferencia de los denominados procedimientos y/o sistemas criptográficos simétricos. El denominado procedimiento o sistema de RSA (RSA: Rivest-Shamir-Adleman) proporciona un correspondiente procedimiento criptográfico asimétrico que se usa en el estado de la técnica para las más diversas aplicaciones en internet.

Las identidades conocidas hasta ahora en el estado de la técnica y/o sus usos en el marco de autenticación, autentificación y/o autorización son desventajosas dependiendo de la respectiva configuración porque son complejas y caras con respecto a inicialización, mantenimiento y/o manejo. Además, las identidades conocidas hasta ahora y sus usos en el marco de autenticación, autentificación o autentificación y/o autorización con respecto a la seguridad de usos no autorizados o abusivos requieren mejoras, particularmente 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).

Particularmente en pequeñas y medianas empresas, las denominadas PyMES, la complejidad de autorización asociada en relación con una red privada virtual (VPN) con respecto a un acceso a datos y/o servicios de un equipo terminal de datos de la empresa a través de una red de ordenadores orientada a conexión tal como internet hasta ahora, debido a los gastos requeridos de sistema y/o administración, no es posible o no desde puntos de vista económicos y/o con complejidad defendible.

La solicitud de patente europea EP 1 246 491 A1 desvela un procedimiento para el encargo de nuevos contratos para aparatos de telefonía móvil. Un usuario de un aparato de telefonía móvil posee un contrato válido con un número de llamada correspondiente en la red de telefonía móvil. El número de llamada está asignado a un módulo de identificación del aparato de telefonía móvil. El usuario encarga a través del aparato de telefonía móvil en una unidad central un nuevo contrato. Después del encargo realizado del contrato, el usuario completa, amplía y/o modifica en un terminal las indicaciones para el contrato a través de un acceso por internet a la unidad central. La identificación clara del usuario se lleva a cabo mediante el módulo de identificación del aparato de telefonía móvil antes o después de la introducción de las indicaciones. En caso de que se realice la identificación con el aparato de telefonía móvil antes de la introducción de los datos se puede transmitir al usuario al aparato de telefonía móvil un URL (localizador uniforme de recursos, de "uniform resource locator"), por ejemplo, con una contraseña a través de SMS.

La invención, en vista de este estado de la técnica, se basa en el objetivo de mejorar la creación y/o el uso de identidades de clientes en un sistema de comunicación, particularmente con respecto a los gastos de sistema y/o

manejo, y también con respecto a la seguridad de usos no autorizados o abusivos.

Para la solución técnica se propone con la presente invención un procedimiento para la creación de una identidad de clientes en un sistema de comunicación que presenta una red de ordenadores orientada a conexión y una red de telefonía móvil celular, creándose la identidad de un cliente mediante combinación de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil, cifrándose en el marco de la combinación el identificador del cliente en la red de ordenadores con el identificador del cliente en la red de telefonía móvil.

La invención se basa en el conocimiento de que mediante combinación de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil se puede crear de forma sencilla y económica una identidad del cliente en el sistema de comunicación, que con respecto al gasto de administración y manejo está reducido y además está mejorado con respecto a la seguridad frente a un uso no autorizado o abusivo. La combinación de acuerdo con la invención de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil para la creación de la identidad del cliente en el sistema de comunicación usa ventajosamente las identidades dadas en el lado de una red de ordenadores orientada a conexión y una red de telefonía móvil celular y su procedimientos, sistemas y métodos para la autenticación, autentificación o autentificación y/o autorización, de tal manera que se reduce o se puede reducir el gasto dado o relacionado con la combinación de acuerdo con la invención con respecto a la administración y/o manejo. Mediante la combinación de diferentes identificadores dados en el lado de la red de ordenadores orientada a conexión por un lado y en el lado de la red de telefonía móvil celular por otro lado del cliente y su combinación para la creación de una identidad en el sistema de comunicación está aumentado además de forma sencilla el grado de seguridad de la identidad creada así como de sus usos en el marco de autenticación, autentificación o autentificación y/o autorización.

En una configuración ventajosa de la invención se crea el identificador del cliente en la red de ordenadores con un algoritmo criptográfico, preferentemente en el lado del equipo terminal de datos de la red de ordenadores, de forma particularmente preferente en el lado de un equipo terminal de datos de una pequeña y mediana empresa (PyME), que está conectado a la red de ordenadores orientada a conexión. 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. Una configuración ventajosa adicional de la invención prevé que el identificador del cliente en la red de ordenadores se cree usando un identificador de base del cliente en la red de ordenadores y un equipo de recuento, estando configurado el equipo de recuento preferentemente usando un algoritmo criptográfico y siendo de forma particularmente preferente parte del equipo terminal de datos. Mediante el uso de acuerdo con la invención de un equipo de recuento se realiza ventajosamente una sincronización del identificador del cliente en la red de ordenadores y, por tanto, en el lado del sistema de comunicación, por lo que se puede continuar aumentando la seguridad de la identidad y/o su uso. De este modo, por ejemplo, un identificador captado o escuchado en el marco del uso de forma no autorizada o abusiva ventajosamente no se puede volver a usar, es decir, entonces de forma no autorizada o abusiva.

En una configuración ventajosa adicional de la invención se crea el identificador del cliente en la red de telefonía móvil con un algoritmo criptográfico, preferentemente en el lado de un aparato terminal móvil del cliente que se puede hacer funcionar en la red de telefonía móvil. Una configuración adicional de la invención prevé que el identificador del cliente en la red de telefonía móvil se cree usando un identificador de base del cliente en la red de telefonía móvil y un equipo de recuento, estando configurado el equipo de recuento preferentemente usando un algoritmo criptográfico y siendo de forma particularmente preferente parte del aparato terminal móvil y/o un módulo de identificación de abonado de telefonía móvil usado por el aparato terminal móvil, una denominada SIM (SIM: módulo de identificación de abonado). Una configuración preferente de la invención prevé que el identificador de base del cliente en la red de telefonía móvil contenga datos que identifican el aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil y/o datos que identifican al usuario del aparato terminal móvil en la red de telefonía móvil, conteniendo los datos que identifican el aparato terminal móvil preferentemente el identificador del aparato, el denominado IMEI (IMEI: identidad internacional de equipo móvil, de "international mobile equipment identity") y los datos que identifican al usuario del aparato terminal móvil en la red de telefonía móvil, al menos el número de llamada específico de red asignado al usuario por un operador de red de telefonía móvil, el denominado 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 de abonado de telefonía móvil, la denominada IMSI (IMSI: identificación internacional de abonado móvil, de "international mobile subscriber identification"). Una configuración particularmente ventajosa de la invención prevé que el identificador del cliente en la red de telefonía móvil se cree mediante una aplicación que se puede ejecutar en el lado del módulo de identificación de abonado de telefonía móvil (SIM (SIM: subscriber identity module), una denominada aplicación SAT (SAT: kit de herramientas de aplicación SIM, de "SIM application toolkit").

En una configuración particularmente preferente de la invención se crean los identificadores independientemente entre sí. Mediante esta medida se puede continuar aumentando el grado de la seguridad de la identidad y particularmente de sus usos en el marco de autenticación, autentificación y/o autorización, particularmente ya que para un uso no autorizado o abusivo se tendrían que determinar o registrar tanto el identificador del cliente en la red de ordenadores como el identificador creado independientemente del mismo del cliente en la red de telefonía móvil.

Una configuración particularmente ventajosa adicional de la invención prevé que el identificador del cliente en la red de telefonía móvil se cifre con una clave que se puede determinar a partir del identificador del cliente en la red de telefonía móvil, preferentemente una clave simétrica. De este modo se puede aumentar adicionalmente el grado de la seguridad. Una configuración ventajosa adicional de la invención prevé que el identificador del cliente en la red de ordenadores se cifre con una clave que se puede determinar a partir del identificador del cliente en la red de telefonía móvil y el estado de contador de un equipo de recuento sincronizado de la red de telefonía móvil, preferentemente una clave simétrica. Teniendo en cuenta el estado de contador de un equipo de recuento sincronizado de la red de telefonía móvil adicionalmente a los clientes en la red de telefonía móvil y su uso para el cifrado del identificador del cliente en la red de ordenadores, un aumento adicional de la seguridad de la identidad a crear mediante combinación de acuerdo con la invención y su uso se puede continuar aumentando. Ventajosamente se lleva a cabo el cifrado automáticamente en el lado de un equipo terminal de datos de la red de ordenadores, de forma particularmente preferente en el lado de un equipo terminal de datos de la red de ordenadores, que proporciona datos y/o servicios para un acceso a través de la red de ordenadores o un equipo terminal de datos que está conectado o se puede conectar con un equipo terminal de datos que proporciona datos y/o servicios correspondientes.

En una configuración adicional 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 aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil.

Una configuración ventajosa de la invención prevé que se use la identidad de acuerdo con la invención para la autenticación de un cliente. Ventajosamente se solicita a este respecto la identidad por un equipo terminal de datos de la red de ordenadores a través de una conexión de comunicación de la red de ordenadores al cliente y se transmite por el cliente a través de la conexión de comunicación al equipo terminal de datos de la red de ordenadores. Una configuración adicional de la invención prevé que el identificador del cliente en la red de telefonía móvil se solicite por un equipo terminal de datos de la red de ordenadores a través de la conexión de comunicación de la red de ordenadores al cliente. Ventajosamente, 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 aparato terminal móvil del cliente que se puede hacer funcionar en la red de telefonía móvil, en el lado del aparato terminal móvil del cliente se crea el identificador del cliente en la red de telefonía móvil y el identificador creado del cliente en la red de telefonía móvil se transmite por el aparato terminal móvil del cliente a través de una y/o usando una conexión de comunicación de la red de telefonía móvil al equipo terminal de datos de la red de ordenadores. Una configuración particularmente preferente de la invención prevé que la conexión de comunicación de la red de telefonía móvil sea una conexión de comunicación que posibilite una conexión a la red de ordenadores, preferentemente una conexión de comunicación que use un protocolo de acuerdo con la especificación WAP (WAP: protocolo de aplicaciones inalámbricas, de "wireless application protocol").

Ventajosamente se crea en el lado del equipo terminal de datos de la red de ordenadores el identificador del cliente en la red de ordenadores y se cifra para la creación de la identidad del cliente con el identificador en la red de telefonía móvil. La identidad del cliente que se puede usar de acuerdo con la invención para la autenticación en el sistema de comunicación se continua mejorando a este respecto con respecto a la seguridad, particularmente ya que en primer lugar se solicita el identificador del cliente en la red de telefonía móvil necesario para el cifrado y preferentemente está disponible y se usa solamente a solicitud en el lado del equipo terminal de datos de la red de ordenadores.

Ventajosamente se usa la identidad de acuerdo con la invención para la autenticación o autentificación de un cliente en el sistema de comunicación, pudiéndose usar el uso tanto para la autentificación en la red de telefonía móvil como para la autentificación en la red de ordenadores. De este modo, una identidad de acuerdo con la invención se puede usar ventajosamente para la autentificación de compras que se realizan a través de la red de telefonía móvil y/o la red de ordenadores mediante aparatos terminales correspondientes de artículos y/o prestaciones de servicios o aplicaciones similares del comercio electrónico, el denominado E-Commerce, con un alto grado de seguridad. En total se puede aumentar por ello la confianza en un comercio correspondiente entre los socios comerciales.

En una configuración preferente de la invención se realiza la autentificación de acuerdo con la invención en el lado de un equipo terminal de datos de la red de ordenadores. A este respecto se realiza ventajosamente en el marco de la autentificación 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. Ventajosamente, el identificador del cliente en la red de ordenadores determinado u obtenido en el marco de la descomposición de la identidad se autentifica, preferentemente mediante al menos una comparación en el lado del equipo terminal de datos de la red de ordenadores.

De acuerdo con una configuración particularmente preferente adicional de la invención se usa el procedimiento de acuerdo con la invención para la autorización de un acceso de un aparato terminal de datos a datos y/o servicios de un equipo terminal de datos en una red de ordenadores.

Es objeto de la presente invención además un sistema de comunicación compuesto de una red de ordenadores orientada a conexión con equipo terminal de datos y una red de telefonía móvil celular, preferentemente de acuerdo

con el estándar de red de radio GSM y/o UMTS, con aparatos terminal móviles que se pueden hacer funcionar en la misma estando configurados los equipos terminales de datos, los equipos de la red de telefonía móvil, particularmente los equipos de la red de telefonía móvil que participan para la administración, el establecimiento y/o el mantenimiento de una conexión de comunicación en la red de telefonía móvil y/o los aparatos terminales móviles para la realización y/o el uso de un procedimiento de acuerdo con la invención.

También es objeto de la invención un aparato terminal móvil para el uso en una red de telefonía móvil celular con un módulo de identificación de abonado de telefonía móvil (SIM) así como un módulo de identificación de abonado de telefonía móvil (SIM) para el uso con un aparato terminal móvil para el funcionamiento en una red de telefonía móvil celular, que están configurados para la realización de un procedimiento de acuerdo con la invención en un sistema de comunicación de acuerdo con la invención. En una configuración particularmente ventajosa de la invención, el procedimiento está almacenado como programa de aplicación en el lado del módulo de identificación de abonado de telefonía móvil (SIM) y/o se puede ejecutar en el lado del mismo. El aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil es ventajosamente un teléfono móvil y/o una tarjeta insertable que se puede usar en relación con un equipo terminal de datos, que se puede hacer funcionar en la red de telefonía móvil, preferentemente en el formato PCMCIA, o una mochila (dongle) que se puede hacer funcionar en la red de telefonía móvil, preferentemente con conexión USB para la conexión con un equipo terminal de datos.

Se explican con más detalle a continuación otras particularidades, características y ventajas de la invención mediante los ejemplos de realización de la invención representados en las figuras del dibujo. A este respecto muestran:

La Figura 1, en una representación básica esquemática, dos posibles usos de una identidad de acuerdo con la invención para la autorización de un acceso de un cliente a una intranet de una empresa;

La Figura 2, en una representación esquemática, una representación básica de un sistema de comunicación de acuerdo con la invención para el uso de una identidad de acuerdo con la invención para una autorización de acceso a datos y/o servicios de un equipo terminal de datos en una red de ordenadores;

La Figura 3, en una representación básica esquemática adicional, el sistema de comunicación de acuerdo con la invención de acuerdo con la Figura 2;

La Figura 4, en una representación básica esquemática, un ejemplo de realización de los desarrollos de autenticación y autentificación dados en el marco de una autorización de acuerdo con la invención;

La Figura 5, en una representación básica esquemática, un ejemplo de realización adicional de los desarrollos de autenticación y autentificación dados en el marco de una autorización de acuerdo con la invención;

La Figura 6, en una representación esquemática de diagrama de bloques, un sistema de comunicación de acuerdo con la invención;

La Figura 7, en una representación esquemática, un diagrama de desarrollo de un ejemplo de realización de una autorización de acceso de acuerdo con la invención y

La Figura 8, en una representación esquemática, un diagrama de desarrollo de un ejemplo de realización adicional de una autorización de acceso de acuerdo con la invención.

En la Figura 1 está en una representación esquemática el acceso de un cliente (trabajador móvil, de "mobile worker") a una red privada virtual (VPN), presente en forma de una red de ordenadores que presenta distintos equipos terminales de datos de una empresa en forma de una denominada intranet (LAN corporativa, de "corporate-LAN"). El cliente (trabajador móvil) es a este respecto en el presente caso un empleado de la empresa y realiza, por ejemplo, trabajos para la empresa desde su vivienda o lugares alejados de la empresa similares. Para esto, el cliente (trabajador móvil) usa en el presente caso para el uso móvil de forma correspondiente al cliente (trabajador móvil) representado con la Figura 1 en la parte superior un equipo terminal de datos móvil o portátil, en el presente caso en forma de un portátil (notebook) y un aparato terminal móvil (teléfono móvil, de "mobile phone") que se puede hacer funcionar en una red de telefonía móvil. El cliente (trabajador móvil) representado en la parte inferior de la Figura 1 usa un equipo terminal de datos conectado en su vivienda a una denominada red fija, en el presente caso en forma de un denominado PC y su aparato terminal móvil (teléfono móvil) que se puede hacer funcionar en una red de telefonía móvil.

El cliente (trabajador móvil) representado en la parte superior en la Figura 1 accede a este respecto a través de la red de telefonía móvil a la intranet de la empresa (LAN corporativa). La red de la empresa/intranet (LAN corporativa) está conectada a este respecto ventajosamente a través de una denominada "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 del dispositivo de seguridad (dispositivo de seguridad de red móvil, de "mobile network security appliance") representado simbólicamente en la Figura 1. El cliente (trabajador móvil) representado en la parte inferior en la Figura 1 accede a

través de internet como red de ordenadores orientada a conexión a la red de la empresa/intranet de la empresa (LAN corporativa).

Los accesos a la red de la empresa (LAN corporativa) a través de la red de telefonía móvil (mobile network) o la red de ordenadores orientada a conexión (internet) se realizan a este respecto usando una identidad creada mediante combinación de un identificador del cliente en la red de ordenadores con un identificador del cliente en la red de telefonía móvil, que se realiza mediante un sistema de autentificación (dispositivo de seguridad de red móvil) representado simbólicamente en la Figura 1. A este respecto, el sistema de autentificación se da en el presente caso en el lado de la red de telefonía móvil y pone a disposición una autentificación de 2 factores asegurada para conexiones entre el respectivo cliente (trabajador móvil) y la red de la empresa (LAN corporativa). A este respecto se proporciona un acceso asegurado de los clientes (trabajador móvil) a la red de la empresa (LAN corporativa) (VPN segura). El dispositivo de seguridad se proporciona a este respecto ventajosamente como modelo de una caja, en el que todos los componentes y conexiones requeridos están alojados en una carcasa o como modelo de dos cajas, en el que los componentes y las conexiones requeridos están alojados en dos carcasas separadas. De este modo se posibilita particularmente una conexión simplificada de un correspondiente dispositivo de seguridad a una red de la empresa o intranet similar, particularmente para usuarios finales. Además, de este modo se puede ofrecer y/o usar una combinación simplificada, más extensa, inteligente y agrupable individualmente de características y/o equipos de seguridad, tales como cortafuegos, VPN, anti-virus, anti-spam o aplicaciones de seguridad similares del dispositivo de seguridad con autentificación segura de forma agrupada.

La Figura 2 muestra en una representación más rica en detalles los detalles en el marco de una autentificación de un acceso de un cliente (usuario final, de "enduser") a la red de una empresa (company). El cliente (usuario final) o su aparato terminal de datos, está conectado a través de una conexión de comunicación adecuada con la red de ordenadores orientada a conexión. El acceso a la red de ordenadores orientada a conexión se realiza a este respecto a través de un denominado proveedor de acceso (access-provider), a través de una conexión inalámbrica y/o por cable entre el o los respectivos aparatos terminales de datos del cliente (usuario final), en el presente caso, por ejemplo, a través de un aparato terminal móvil que se puede hacer funcionar en una red de telefonía móvil, una denominada conexión WLAN o una conexión DSL. A través de la red de ordenadores (internet) se puede conectar el cliente (usuario final) entonces 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 que realiza la autentificación de la empresa UA (UA: pasarela de autenticación de usuario, de "user authentication gateway"). La pasarela de UA está dispuesta a este respecto en el presente caso en el lado de la empresa (company) y está conectada a través de internet con el proveedor de acceso para el acceso del cliente (usuario final) a la red de ordenadores (internet) con un banco de datos de reserva en el lado de la red de empresa con entradas de clientes (directorio de base de datos de usuario) y con equipos terminales de datos de un operador de red de telefonía móvil (mobile network provider). En el lado del operador de red de telefonía móvil (mobile network provider) están previstos a este respecto equipos que proporcionan servicios correspondientes que autentifican al cliente (servicio de UA), que afectan particularmente al identificador del cliente (usuario final) en la red de telefonía móvil. El acceso representado en la Figura 2 de un cliente (usuario final) a una red de empresa (company) se corresponde a este respecto con el acceso representado en la Figura 1 en la zona inferior de un cliente (trabajador móvil) a una red de empresa (LAN corporativa). En el ejemplo de realización indicado en la Figura 3 de un acceso de un cliente (usuario final) a la intranet de una empresa (company) se realiza el acceso del cliente (usuario final) a la red de empresa a través de un acceso móvil del cliente (usuario final) a través de una red de telefonía móvil en la red de ordenadores orientada a conexión (internet). A través del acceso a la red de telefonía móvil de un operador de red de telefonía móvil (mobile network provider) se posibilita a través de correspondientes servicios de comunicación (canal de servicio, servicio de red), el acceso móvil del cliente (usuario final) a través de un correspondiente proveedor de acceso mediante equipos terminales de datos adecuados, en el presente caso un servidor de acceso (servidor de AAA) con un acceso asegurado. El acceso del cliente (usuario final) de acuerdo con la Figura 3 se corresponde a este respecto con el acceso representado en la Figura 1 en la zona superior de un cliente (trabajador móvil) a una red de empresa (LAN corporativa).

La Figura 4 muestra el acceso de un usuario (usuario remoto, de "remote user") a un equipo terminal de datos que proporciona datos y/o servicios (recursos de la compañía, de "company resources") de una empresa (company) a través de una red de ordenadores orientada a conexión (network). El usuario (usuario remoto) usa para esto un equipo terminal de datos, en el presente caso en forma de un portátil y para la autentificación de su acceso, un aparato terminal móvil que se puede hacer funcionar en una red de telefonía móvil (operador de red de telefonía móvil), en el presente caso en forma de un teléfono móvil. La empresa (company) presenta un equipo terminal de datos (servidor de VPN/AAA) que se puede conectar a la red de ordenadores orientada a conexión. Además, la empresa (company) presenta un equipo terminal de datos que se puede conectar con la red de telefonía móvil (mobile network). Los dos equipos terminales de datos (servidor de VPN/AAA; UA de compañía) están conectados en el presente caso entre sí. Mediante el equipo terminal de datos (UA de compañía) que se puede conectar con la red de telefonía móvil se realiza en el lado de la empresa un acceso a los datos y/o servicios (recursos de la compañía) en la intranet interna de la empresa.

De acuerdo con la invención se realiza la autentificación del usuario (usuario remoto) según el ejemplo de realización de acuerdo con la Figura 4 ventajosamente antes del propio acceso del mismo a la red de la empresa (recursos de la compañía). Ventajosamente se evitan de este modo los denominados tiempos de espera (timeouts)

en el VPN/servidor de AAA. Además se da de este modo un bucle (loop) cerrado de cliente a través de operador de red de telefonía móvil y empresa (corporación/company), que continua aumentando la seguridad del acceso, particularmente ya que el usuario (usuario remoto) en su aparato terminal (ordenador/portátil) tiene que introducir su identificador creada a través del aparato terminal móvil se puede hacer funcionar en la red de telefonía móvil/teléfono móvil (dispositivo de autenticación) de la identidad (OTP) en la aplicación ejecutada o en marcha en el lado del aparato terminal (Ordenador/portátil) que posibilita el acceso, un denominado cliente de acceso (cliente de UA).

En primer lugar inicia el usuario (usuario remoto) a través de su equipo terminal de datos (portátil) que se puede hacer funcionar en la red de ordenadores orientada a conexión una petición dirigida a través de la red de ordenadores orientada a conexión (network) al equipo terminal de datos (servidor de VPN/AAA) de la empresa (company), como se representa en la Figura 4 simbólicamente mediante la flecha indicada con 4-1. Para esto se ejecuta en el lado del equipo terminal de datos (portátil) del usuario un programa de aplicación, en el presente caso un denominado cliente de UA, como se representa en la Figura 4. El cliente de UA envía a este respecto a través de una conexión de internet no cifrada existente una petición de acceso (petición de identidad, de "identity request") a una aplicación ejecutada en el lado del equipo terminal de datos (servidor de VPN/AAA) de la empresa (company), en el presente caso una denominada UA de compañía, indicada en la Figura 4 con las referencias 4-1 y 4-2.

La petición de acceso (4-1) del usuario (usuario remoto) se transmite por el equipo terminal de datos (servidor de VPN/AAA) a través de la flecha indicada en la Figura 4 con 4-2 al equipo terminal de datos que asume la autentificación del usuario o un programa de aplicación ejecutado en el lado del mismo de la empresa (UA de compañía) para la comprobación de identidad. A este respecto se transfiere o transmite el identificador (identificador de red de ordenadores) del equipo terminal de datos (portátil) del usuario (usuario remoto) en la red de ordenadores (network), en el presente caso internet, a la UA de compañía.

La UA de compañía determina después el identificador de telefonía móvil del usuario (usuario remoto) a partir del identificador de red de ordenadores e inicia una petición de autentificación, una denominada request para la autentificación, transmitiéndose por el aparato terminal de datos que se puede hacer funcionar en la red de telefonía móvil del usuario, en el presente caso por la SIM usada por el mismo, datos a firmar y representar.

En el marco de esta petición de autentificación, el equipo terminal de datos (UA de compañía) accede a un banco de datos (directorio de usuario (ID de usuario, PW, ID de SIM)) que administra identidades de usuario, como se representa en la Figura 4 mediante la flecha indicada con 4-3.

El banco de datos (directorio de usuario) suministra después de vuelta al equipo terminal de datos (UA de compañía) un identificador correspondiente del usuario (usuario remoto) en la red de telefonía móvil, tal como se representa en la Figura 4 mediante la flecha indicada con 4-4.

El equipo terminal de datos (UA de compañía) de la empresa (company) usa las informaciones obtenidas del banco de datos (directorio de usuario) y contacta después con un equipo terminal de datos del operador de red de telefonía móvil (UA de operador de red de telefonía móvil), como se representa mediante la flecha indicada en la Figura 4 con 4-5.

El identificador obtenido por el equipo terminal de datos del operador de red de telefonía móvil (mobile network provider) en el marco de la flecha indicada con 4-5 se transmite en el lado del operador de red de telefonía móvil a un equipo terminal de datos (servidor de T2R/OTA, "T2R/OTA Server") configurado o equipado para la comprobación del identificador, tal como se representa simbólicamente en la Figura 4 mediante la flecha indicada con 4-6.

La autentificación del usuario (usuario remoto) se realiza entonces en el lado de la red de telefonía móvil. El equipo terminal de datos (servidor de T2R/OTA) envía para la autentificación del usuario (usuario remoto) una petición correspondiente de autentificación a un aparato terminal móvil (dispositivo de autenticación) que se puede hacer funcionar en la red de telefonía móvil del usuario (usuario remoto), tal como se puede ver en la Figura 4 mediante la flecha representada con 4-7. En el marco de la petición de autentificación (4-7) se solicita al usuario (usuario remoto) que introduzca un PIN correspondiente en el lado del aparato terminal móvil (dispositivo de autenticación).

Con el PIN introducido por el usuario (usuario remoto) se crea entonces en el lado del aparato terminal móvil (dispositivo de autenticación) una contraseña (OTP) y se transfiere a través de la red de telefonía móvil a través de la conexión indicada en la Figura 4 con 4-8 al equipo terminal de datos (servidor de T2R/OTA) de la red de telefonía móvil, se transmite del equipo terminal de datos (servidor de T2R/OTA) a través de la conexión indicada en la Figura 4 con 4-9 al equipo terminal de datos (UA de operador de red de telefonía móvil) y se transfiere desde el mismo a través de la conexión indicada en la Figura 4 con 4-10 al equipo terminal de datos (UA de compañía) de la empresa (company).

Además, la contraseña (OTP) creada en el lado del aparato terminal móvil (dispositivo de autenticación) con el PIN se indica en el lado del aparato terminal móvil (dispositivo de autenticación) y se introduce por el usuario (usuario remoto) en el lado del aparato terminal de datos (portátil) en el lado de la aplicación (cliente de UA) ejecutada por el mismo y se transfiere a la aplicación ejecutada en el lado del equipo terminal de datos de la empresa (servidor de

VPN/AAA) y en el lado de la misma(cliente de VPN).

La contraseña se proporciona entonces al equipo terminal de datos (UA de compañía) en el marco del establecimiento de conexión o una petición de acceso adicional y, siempre que la transmisión correspondiente se encuentre todavía dentro de un determinado intervalo de tiempo (ventana temporal), se valida el acceso.

Después se realiza en el lado del equipo terminal de datos (UA de compañía) una comparación de la contraseña (OTP) introducida por el usuario (usuario remoto) en el lado del aparato terminal de datos (portátil) en el marco del cliente de UA con la contraseña (OTP) correspondiente trasmitida a través de la red de telefonía móvil al equipo terminal de datos (UA de compañía). Con coincidencia de las contraseñas (OTP) se da una autentificación positiva y en el lado del equipo terminal de datos (UA de compañía) a través de la flecha indicada en la Figura 4 con 4-11 se transmite un resultado correspondiente al equipo terminal de datos (servidor de VPN/AAA) conectado con la red de ordenadores orientada a conexión (network) de la empresa (company) una información, a lo que el usuario obtiene del equipo terminal de datos (servidor de VPN/AAA) acceso a los datos y/o servicios (recursos de la compañía) proporcionados en el lado de la red de la empresa. Ya que la identidad de telefonía móvil ya se validó anteriormente a través del aparato terminal móvil (dispositivo de autentificación) y la red de telefonía móvil, es decir, se desarrolló una autentificación a través de la red de telefonía móvil, es suficiente una comprobación sencilla de la contraseña (OTP) en el lado del equipo terminal de datos (UA de compañía).

El acceso está representado simbólicamente en la Figura 4 mediante las flechas indicadas con 4-12 y 4-13 y se realiza a través del equipo terminal de datos (servidor de VPN/AAA) de la empresa (company). El acceso que se realiza del usuario (usuario remoto) a los datos y/o servicios (recursos de la compañía) se registra correspondientemente en el lado del equipo terminal de datos (UA de compañía).

En una configuración adicional de la invención se indica para el aumento de la seguridad una información de acceso correspondiente al usuario (usuario remoto) en el lado de su aparato terminal móvil (dispositivo de autenticación) a través de conexiones de comunicación correspondientes 4-5, 4-6 y 4-7.

En una configuración adicional se puede detectar y registrar además la indicación de la correspondiente autentificación de un acceso en el lado del aparato terminal móvil (dispositivo de autenticación) a través de la correspondiente conexión 4-8, 4-9 y 4-10 en el lado del equipo terminal de datos (UA de compañía).

En el ejemplo de realización representado en la Figura 5 de una autentificación de un usuario (usuario remoto), el equipo terminal de datos usado por el usuario (usuario remoto), en el presente caso un portátil, transmite en primer lugar un identificador específico de aparato a través de la red de ordenadores orientada a conexión a un equipo terminal de datos (servidor de CUA) previsto para la autenticación en el lado de la empresa (corporación), como se representa simbólicamente en la Figura 5 mediante la flecha representada con 5-1.

El equipo terminal de datos (servidor de CUA) accede después a través de la conexión representada simbólicamente en la Figura 5 con 5-2 a un banco de datos (directorio de usuario (ID de usuario, PW, ID de SIM)) de la empresa (corporación) y extrae del banco de datos (directorio de usuario) una clave registrada para el identificador (5-1) de transmisión del usuario (usuario remoto), que se transmite a través de la conexión indicada en la Figura 5 con 5-3 al equipo terminal de datos (servidor de CUA).

El equipo terminal de datos (servidor de CUA) transmite las claves obtenidas de este modo a través de la conexión representada simbólicamente en la Figura 5 con 5-4 a través de la red de ordenadores orientada a conexión (network) al equipo terminal de datos del usuario (usuario remoto). En el lado del equipo terminal de datos del usuario (usuario remoto) y el equipo terminal de datos (servidor de CUA) de la empresa (corporación) se determina después usando la clave una identidad del usuario (usuario remoto) mediante combinación del identificador del usuario (usuario remoto) en la red de ordenadores orientada a conexión y un identificador del usuario (usuario remoto) o su aparato terminal móvil (dispositivo de autenticación) en la red de telefonía móvil. Para esto, a través de una conexión entre el equipo terminal de datos del usuario (usuario remoto) y el aparato terminal móvil (dispositivo de autenticación) que se puede hacer funcionar en la red de telefonía móvil del usuario en la red de telefonía móvil se transmite la clave obtenida del banco de datos de la Figura 5 con 5-3 y 5-4 a un equipo de terminal de datos (TTF/OTA) de la red de telefonía móvil, como se representa simbólicamente en la Figura 5 mediante la flecha indicada con 5-5. El aparato terminal móvil (dispositivo de autenticación) que se puede hacer funcionar en la red de telefonía móvil del usuario es a este respecto en una configuración preferente de la invención una denominada mochila (dongle) y/o una tarjeta PCMCIA.

En el marco de la transmisión de la clave a través de la conexión indicada en la Figura 5 con 5-5, el usuario (usuario remoto) introduce a través del equipo terminal de datos un PIN, que activa la transmisión de 5-5 o que transmite conjuntamente esta y/o la clave en el lado del equipo terminal de datos (TTF/OTA) de la red de telefonía móvil.

Con una introducción correspondientemente correcta del PIN se transmite en el lado del equipo terminal de datos (TTF/OTA) a través de la conexión indicada en la Figura 5 con 5-6 un identificador correspondiente del usuario (usuario remoto) en la red de telefonía móvil al equipo terminal de datos del usuario (usuario remoto), en el presente caso a través del aparato terminal móvil (dispositivo de autenticación) que se puede hacer funcionar en la red de telefonía móvil del usuario (usuario remoto). Con ello está presente en el lado del usuario (usuario remoto) la

identidad creada o que se puede crear mediante combinación del usuario (usuario remoto), que está compuesta de un identificador (CP) del usuario (usuario remoto) en la empresa (corporación) y un identificador (VP) del usuario (usuario remoto) en la red de telefonía móvil o que se puede formar a partir de los mismos.

A través de la conexión indicada en la Figura 5 con 5-7 se transmite el identificador transferido de forma correspondiente por el equipo terminal de datos (TTF/OTA) de la red de telefonía móvil en el marco de la conexión 5-6 a través de la red de ordenadores orientada a conexión (network) desde el equipo terminal de datos del usuario (usuario remoto) al equipo terminal de datos (servidor de VUA) de la empresa (corporación) y el identificador obtenido de este modo se transmite a través de la conexión indicada en la Figura 5 con 5-7 a un equipo terminal de datos (servidor de CUA) de la red de telefonía móvil previsto para la autentificación.

El equipo terminal de datos (servidor de CUA) de la red de telefonía móvil consulta después en un equipo terminal de datos (TTF/OTA) adicional de la red de telefonía móvil en el marco de la petición indicada en la Figura 5 con 5-9 si en el caso del identificador obtenido en el marco de la conexión indicada con 5-7 se trata de un identificador válido de la red de telefonía móvil o del operador de red de telefonía móvil.

El equipo terminal de datos (TTF/OTA) transmite el resultado de la petición (5-9) a través de la conexión indicada en la Figura 5 con 5-10 al equipo terminal de datos (servidor de VUA) y a través de la conexión indicada en la Figura 5 con 5-11 al equipo terminal de datos (servidor de CUA) de la empresa (corporación).

Después está presente de manera correspondiente en el lado del equipo terminal de datos (servidor de CUA) de la empresa (corporación) de forma correspondiente el identificador (CP) del usuario (usuario remoto) en la red de ordenadores y el identificador (VP) del usuario (usuario remoto) en la red de telefonía móvil. Una confirmación correspondiente de la validez del transmitido (5-7) por el usuario (usuario remoto) puede, con configuración correspondiente de los servidores de CUA del equipo terminal de datos, transmitirse e indicarse correspondientemente (5-12) a través de la red de ordenadores (network) al equipo terminal de datos (usuario remoto).

La identidad presente en el lado del equipo terminal de datos (servidor de CUA), creada o que se puede crear a partir del identificador (CP) en la red de ordenadores y el identificador (VP) en la red de telefonía móvil, se usa a continuación para el acceso del usuario (usuario remoto) a datos y/o servicios (recursos de la compañía) de la empresa (corporación). Para esto el usuario (usuario remoto) transmite su identidad combinada (UA) a través de la conexión indicada en la Figura 5 con 5-13 a través de la red de ordenadores orientada a conexión (network) a un equipo terminal de datos (servidor de VPN) que posibilita el acceso a los datos y/o servicios (recursos de la compañía) de la empresa (corporación).

El equipo terminal de datos (servidor de VPN) transmite la identidad (UA) obtenida por el usuario (usuario remoto) a través de la conexión (5-13) a través de la conexión indicada en la Figura 5 con 5-14 al equipo terminal de datos (servidor de CUA) que presenta la identidad (UA) de la empresa (corporación). En el lado del equipo terminal de datos (servidor de CUA) de la empresa (corporación) se realiza después una comprobación de la identidad transmitida a través de la conexión 5-13 y 5-14 con la identidad (UA) presente en el lado del equipo terminal de datos (servidor de CUA) mediante al menos una comparación.

Con coincidencia de las identidades se libera del equipo terminal de datos (servidor de CUA) al equipo terminal de datos (servidor de VPN) a través de la conexión indicada en la Figura 5 con 5-15 el acceso del usuario (usuario remoto) en el lado del equipo terminal de datos (servidor de VPN).

El usuario (usuario remoto) obtiene después a través de las flechas indicadas en la Figura 5 con 5-16 y 5-17 a través del equipo terminal de datos (servidor de VPN) de la empresa (corporación) acceso a los datos y/o servicios (recursos de la compañía) de la empresa.

El diagrama de bloques de acuerdo con la Figura 6 muestra los sistemas o equipos que intervienen en el marco de una autentificación de un cliente (cliente de VPN) y las peticiones y/o respuestas de comunicación (comunicación de desafío-respuesta, de "challenge response communication") que se dan entre los mismos. Los detalles con respecto a los componentes individuales así como los desarrollos de comunicación que se dan entre los mismos se explican a continuación con más detalle en relación con los ejemplos de realización representados en la Figura 7 y la Figura 8, particularmente con respecto a la creación y el uso de la identidad de un cliente (OTP) mediante uso combinatorio de un identificador del cliente en la red de ordenadores (OTP de compañía) con un identificador del cliente en la red de telefonía móvil (OTP de red de telefonía móvil). Como se puede observar mediante la representación de acuerdo con la Figura 6, de acuerdo con la invención se pueden usar ventajosamente de forma agrupada diferentes sistemas de autenticación, que dependiendo del caso de aplicación se combinan entre sí ventajosamente. En configuraciones preferentes de la invención, la validación está basada en OTP de servidor, ventajosamente con uso de RSA y/o SecurelD, basada en firma de móvil (mobile-signature) y/o basada en TTF.

El diagrama de desarrollo representado esquemáticamente en la Figura 7 muestra un ejemplo de realización básico de una autorización de un acceso a datos y/o servicios de un equipo terminal de datos en una red privada virtual y a este respecto en o entre los distintos equipos de un sistema de comunicación que presenta una red de ordenadores orientada a conexión y una red de telefonía móvil celular.

El usuario (usuario final) de un aparato terminal inicia en la etapa del procedimiento o desarrollo indicada con 1.0 el establecimiento de una conexión con un denominado cliente de VPN. Para esto, el usuario (usuario final) en el lado de su equipo terminal de datos que proporciona el cliente de VPN presiona, por ejemplo, una tecla para el establecimiento de la conexión.

El equipo terminal de datos (cliente de VPN) del usuario (usuario final) establece después una conexión con un equipo terminal de datos (servidor de VPN) en el lado de la empresa (company), como se representa simbólicamente en la Figura 7 mediante la flecha indicada con 1.1.

Después, el servidor de VPN solicita en la etapa del procedimiento o de desarrollo indicada con 1.2 la identidad del usuario (usuario final) en el lado del cliente de VPN del usuario (usuario final).

El cliente de VPN del usuario (usuario final) envía después la identidad del usuario (usuario final) al servidor de VPN en el lado de la empresa (company), transmitiéndose a través de la respuesta (respuesta de EAP) indicada en la Figura 7 con 1.3 la identidad del usuario (usuario final), en el presente caso en forma de una denominada ID de usuario.

A continuación se solicita por el servidor de VPN en la etapa del procedimiento o de desarrollo indicada en la Figura 7 con 1.4 en el lado del cliente de VPN del usuario (usuario final) la introducción de una contraseña perteneciente a la identidad (OTP de SOL. de EAP).

El cliente de VPN del usuario (usuario final) solicita después en la etapa del procedimiento o de desarrollo indicada con 1.5 al usuario la introducción de la contraseña (OTP) asignada a la identidad. El usuario (usuario final) usa para la determinación de la contraseña (OTP) su aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil o la tarjeta inteligente usada por el mismo, en el presente caso en forma de la tarjeta SIM del aparato terminal móvil.

La determinación de la contraseña (OTP) mediante la tarjeta inteligente del aparato terminal móvil del usuario (usuario final) está representada en la Figura 7 mediante la etapa de procedimiento o de desarrollo indicada en la Figura 7 con 1.6 simbólicamente.

La tarjeta inteligente del usuario (usuario final) determina o calcula (etapa del procedimiento 1.7) después usando un identificador del usuario en la red de la empresa y un identificador del usuario en la red de telefonía móvil en el lado de la tarjeta inteligente la identidad usando un equipo de recuento.

La identidad o la contraseña (OTP, OTP1) calculada por la tarjeta inteligente está compuesta de una combinación de un identificador del usuario en la red de ordenadores de la empresa (CTP) y un identificador del usuario en la red de telefonía móvil (VTP). En la Figura 7 se expresa mediante la cifra "1" detrás de la contraseña (OTP) que cada acceso como instancia de la OTP es nuevo y se numera de forma correspondiente, preferentemente de manera continua, de tal manera que el siguiente acceso obtiene como instancia la contraseña OTP2, OTP3, etcétera. La contraseña o la identidad se indica a continuación como identificador del usuario en la red de telefonía móvil en el lado de un equipo de indicación del aparato terminal móvil que usa la tarjeta inteligente del usuario (usuario final), como se representa en la Figura 7 mediante la etapa del procedimiento indicada con 1.8.

La contraseña (OTP1) reproducida en el lado del equipo de indicación del aparato terminal móvil que usa la tarjeta inteligente del usuario, que reproduce el identificador del usuario en la red de telefonía móvil, se introduce por el usuario en el lado del cliente de VPN del usuario (etapa del procedimiento o de desarrollo 1.9) y se transmite por el cliente de VPN a continuación a través de la red de ordenadores orientada a conexión (internet) al servidor de VPN de la empresa (etapa de procedimiento o de desarrollo 1.10).

En la etapa del procedimiento o de desarrollo indicada con 1.11, el servidor de VPN inicia en el lado de la red privada virtual de la empresa a través de una pasarela configurada para la autentificación de la empresa (pasarela de UA/UA de compañía) la comprobación del identificador de usuario (ID de usuario) obtenido en la etapa del procedimiento o de desarrollo 1.11 con el identificador del usuario (usuario final) transmitido correspondientemente en la red de telefonía móvil (OTP1). A este respecto, en el lado de la pasarela de la empresa (pasarela de UA/UA de compañía) en la etapa del procedimiento o de desarrollo indicada con 1.12 se descifra y se descompone en un identificador del usuario en la red de la empresa y un identificador del usuario en la red de telefonía móvil.

En la etapa de procedimiento o de desarrollo indicada con 1.13, la pasarela de la empresa (pasarela de UA/UA de compañía) comprueba mediante petición correspondiente en el lado de la red de telefonía móvil (UA de red de telefonía móvil) la validez del identificador transmitido de forma combinada correspondientemente con la identidad cifrada OTP1 del usuario en la red de telefonía móvil (VF-OTP). Para esto se transmite el identificador del cliente en la red de telefonía móvil (VF-OTP) en la etapa del procedimiento 1.13 a la red de telefonía móvil (UA de red de telefonía móvil) y se comprueba en la etapa del procedimiento 1.14 en el lado de la red de telefonía móvil. A este respecto, en la etapa del procedimiento 1.15 en el lado de la red de telefonía móvil se calcula o se comprueba de otro modo si el identificador transmitido en la etapa de procedimiento 1.13 es válido.

En la etapa del procedimiento indicada con 1.16, la red de telefonía móvil envía de vuelta a la pasarela de la empresa una información de validación correspondiente con respecto al identificador del usuario en la red de telefonía móvil.

Con validación positiva del identificador del usuario en la red de telefonía móvil, a continuación en el lado de la pasarela de la empresa en la etapa del procedimiento indicada con 1.17 se descifra el identificador transmitido con la identidad (OTP1) del usuario en la red de la empresa (OTP de compañía).

El identificador descifrado del usuario en la red de la empresa (OTP de compañía) se valida a continuación en la etapa del procedimiento o de desarrollo indicada con 1.18 en el lado de la pasarela de la empresa (pasarela de UA/UA de compañía).

Con validación positiva, la pasarela de la empresa (pasarela de UA/UA de compañía) en la etapa del procedimiento indicada con 1.19 envía una información de autentificación correspondiente al servidor de VPN de la empresa, a lo que el cliente de VPN en la etapa del procedimiento o la etapa de desarrollo indicada con 1.20 se conecta con el servidor de VPN. El cliente de VPN conectado de este modo con el servidor de VPN puede acceder después a la red de la empresa y los datos y/o servicios proporcionados en la red de la empresa.

El diagrama de desarrollo representado esquemáticamente en la Figura 8 se diferencia del diagrama de desarrollo representado en la Figura 7 de una autorización de un acceso de un usuario a datos y/o servicios en una red de empresa con respecto a la creación de la identidad a partir de un identificador del usuario (usuario final) en la red de ordenadores de una empresa y el identificador del usuario (usuario final) en la red de telefonía móvil. Se dan diferencias a este respecto particularmente en las etapas del procedimiento 1.14 a 1.18.

En el ejemplo de realización representado en la Figura 8, a este respecto, a partir del identificador del usuario en la red de telefonía móvil se realiza de forma simplificada una validez del mismo mediante consulta en la red de telefonía móvil (UA de red de telefonía móvil), calculándose a partir del identificador del usuario en la red de telefonía móvil un valor de validez en la etapa del procedimiento indicada con 1.14 en el lado de la red de telefonía móvil y transmitiéndose en la etapa de procedimiento o de desarrollo indicada con 1.15 a la pasarela (pasarela de UA/UA de compañía). Con transmisión de este valor, en el lado de la pasarela de la empresa a continuación se realiza una comprobación del valor transmitido por la red de telefonía móvil en la etapa del procedimiento 1.15 con un valor registrado en el lado de la pasarela para el acceso correspondiente, tal como se representa en la Figura 8 en la etapa del procedimiento indicada con 1.16. Con una coincidencia correspondiente, a continuación, en la etapa del procedimiento indicada con 1.17 se transmite un valor aleatorio correspondiente por la pasarela a la red de telefonía móvil y se inicia correspondientemente un contador de la red de telefonía móvil. El estado de contador correspondiente del equipo de recuento en la red de telefonía móvil se transmite después a través de la conexión indicada en la Figura 8 con 1.18 a la pasarela (pasarela de UA/ UA de compañía). Con la transmisión del correspondiente estado de contador está presente después en el lado de la pasarela un resultado validado para la comprobación de la identidad y la conexión entre el cliente de VPN del usuario (usuario final) y el servidor de VPN de la empresa se establece de forma correspondiente a las etapas de procedimiento o desarrollo 1.19 y 1.20 descritas en relación con la Figura 7.

Los ejemplos de realización representados en las figuras del dibujo sirven solamente para la explicación de la invención y no son limitantes de la misma.

REIVINDICACIONES

1. Procedimiento para la creación de una identidad de clientes en un sistema de comunicación que presenta una red de ordenadores orientada a conexión y una red de telefonía móvil celular, creándose la identidad de un cliente mediante combinación de un identificador de los clientes en la red de ordenadores con un identificador del cliente en la red de telefonía móvil, cifrándose en el marco de la combinación el identificador del cliente en la red de ordenadores con el identificador del cliente en la red de telefonía móvil.

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** el identificador del cliente en la red de ordenadores se crea con un algoritmo criptográfico, preferentemente en el lado de un equipo terminal de datos de la red de ordenadores.

3. Procedimiento de acuerdo con la reivindicación 1 o la reivindicación 2, **caracterizado porque** el identificador del cliente en la red de ordenadores se crea usando un identificador de base del cliente en la red de ordenadores y un equipo de recuento.

4. Procedimiento de acuerdo con la reivindicación 3, **caracterizado porque** el equipo de recuento está configurado usando un algoritmo criptográfico.

5. Procedimiento de acuerdo con la reivindicación 3 o la reivindicación 4, **caracterizado porque** el equipo de recuento es parte del equipo terminal de datos.

6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado porque** el identificador del cliente en la red de telefonía móvil se crea con un algoritmo criptográfico.

7. Procedimiento de acuerdo con la reivindicación 6, **caracterizado porque** el identificador se crea en el lado de un aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil del cliente.

8. Procedimiento de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado porque** el identificador del cliente en la red de telefonía móvil se crea usando un identificador de base del cliente en la red de telefonía móvil y un equipo de recuento.

9. Procedimiento de acuerdo con la reivindicación 8, **caracterizado porque** el equipo de recuento está configurado usando un algoritmo criptográfico.

10. Procedimiento de acuerdo con la reivindicación 8 o la reivindicación 9, **caracterizado porque** el equipo de recuento es parte del aparato terminal móvil y/o un módulo de identificación de abonado de telefonía móvil, SIM, usado por el aparato terminal móvil.

11. Procedimiento de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado porque** los identificadores se crean independientemente unos de otros.

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 11, **caracterizado porque** el identificador del cliente en la red de ordenadores se cifra con una clave que se puede determinar a partir del identificador del cliente en la red de telefonía móvil.

13. Procedimiento de acuerdo con la reivindicación 12, **caracterizado porque** la clave es una clave simétrica.

14. Procedimiento de acuerdo con una de las reivindicaciones 1 a 13, **caracterizado porque** el identificador del cliente en la red de ordenadores se cifra con una clave que se puede determinar a partir del identificador del cliente en la red de telefonía móvil y el estado de contador de un equipo de recuento sincronizado de la red de telefonía móvil.

15. Procedimiento de acuerdo con la reivindicación 14, **caracterizado porque** la clave es una clave simétrica.

16. Procedimiento de acuerdo con 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 aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil.

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

18. Procedimiento de acuerdo con la reivindicación 17, **caracterizado porque** la identidad se solicita por un equipo terminal de datos de la red de ordenadores a través de una conexión de comunicación de la red de ordenadores al cliente y se transmite por el cliente a través de la conexión de comunicación al equipo terminal de datos de la red de ordenadores.

19. Procedimiento de acuerdo con la reivindicación 17 o la reivindicación 18, **caracterizado porque** el identificador del cliente en la red de telefonía móvil se solicita al cliente por un equipo terminal de datos de la red de ordenadores

a través de una conexión de comunicación de la red de ordenadores.

20. Procedimiento de acuerdo con la reivindicación 19, **caracterizado porque** la solicitud 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 aparato terminal móvil que se puede hacer funcionar en la red de telefonía móvil del cliente, en el lado del aparato terminal móvil del cliente se crea el identificador del cliente en la red de telefonía móvil, y el identificador creado del cliente en la red de telefonía móvil se transmite desde el aparato terminal móvil del cliente a través de una y/o usando una conexión de comunicación de la red de telefonía móvil al equipo terminal de datos de la red de ordenadores.

21. Procedimiento de acuerdo con la reivindicación 20, **caracterizado porque** la conexión de comunicación de la red de telefonía móvil es una conexión de comunicación que posibilita una conexión a la red de ordenadores.

22. Procedimiento de acuerdo con la reivindicación 21, **caracterizado por** una conexión de comunicación que usa un protocolo de acuerdo con la especificación WAP.

23. Procedimiento de acuerdo con una de las reivindicaciones 19 a 22, **caracterizado porque** en el lado del equipo terminal de datos de la red de ordenadores se crea el identificador del cliente en la red de ordenadores y para la creación de la identidad del cliente se cifra con el identificador del cliente en la red de telefonía móvil.

24. Procedimiento de acuerdo con una de las reivindicaciones 1 a 23, **caracterizado porque** la identidad se usa para la autentificación de un cliente.

25. Procedimiento de acuerdo con la reivindicación 24, **caracterizado porque** la autentificación se realiza en el lado de un equipo terminal de datos de la red de ordenadores.

26. Procedimiento de acuerdo con la reivindicación 24 o la reivindicación 25, **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.

27. Procedimiento de acuerdo con una de las reivindicaciones 24 a 26, **caracterizado porque** el identificador determinado en el marco de la descomposición de la identidad del cliente se autentifica en la red de ordenadores.

28. Procedimiento de acuerdo con la reivindicación 27, **caracterizado porque** la autentificación se realiza mediante al menos una comparación en el lado de un equipo terminal de datos de la red de ordenadores.

29. Procedimiento de acuerdo con una de las reivindicaciones 1 a 28, **caracterizado porque** el mismo se usa para la autorización de un acceso de un aparato terminal de datos a datos y/o servicios de un equipo terminal de datos en una red de ordenadores.

30. Sistema de comunicación compuesto de una red de ordenadores orientada a conexión con equipos terminales de datos y una red de telefonía móvil celular con aparatos terminales móviles que se pueden hacer funcionar en la misma, **caracterizado porque** los equipos terminales de datos, los equipos de la red de telefonía móvil y/o los aparatos terminales móviles están configurados para la realización y/o el uso de un procedimiento de acuerdo con una de las reivindicaciones 1 a 29.

31. Aparato terminal móvil para el uso en una red de telefonía móvil celular con un módulo de identificación de abonado de telefonía móvil, SIM, **caracterizado porque** el mismo está configurado para la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 29, preferentemente en un sistema de comunicación de acuerdo con la reivindicación 30.

32. Módulo de identificación de abonado de telefonía móvil, SIM, para el uso con un aparato terminal móvil para el funcionamiento en una red de telefonía móvil celular, **caracterizado porque** el mismo está configurado para la realización de un procedimiento de acuerdo con una de las reivindicaciones 1 a 29, preferentemente en un sistema de comunicación de acuerdo con la reivindicación 30.

33. Módulo de identificación de abonado de telefonía móvil, SIM, de acuerdo con la reivindicación 32, **caracterizado porque** el procedimiento está almacenado y/o se puede ejecutar como programa de aplicación en el lado de la SIM.

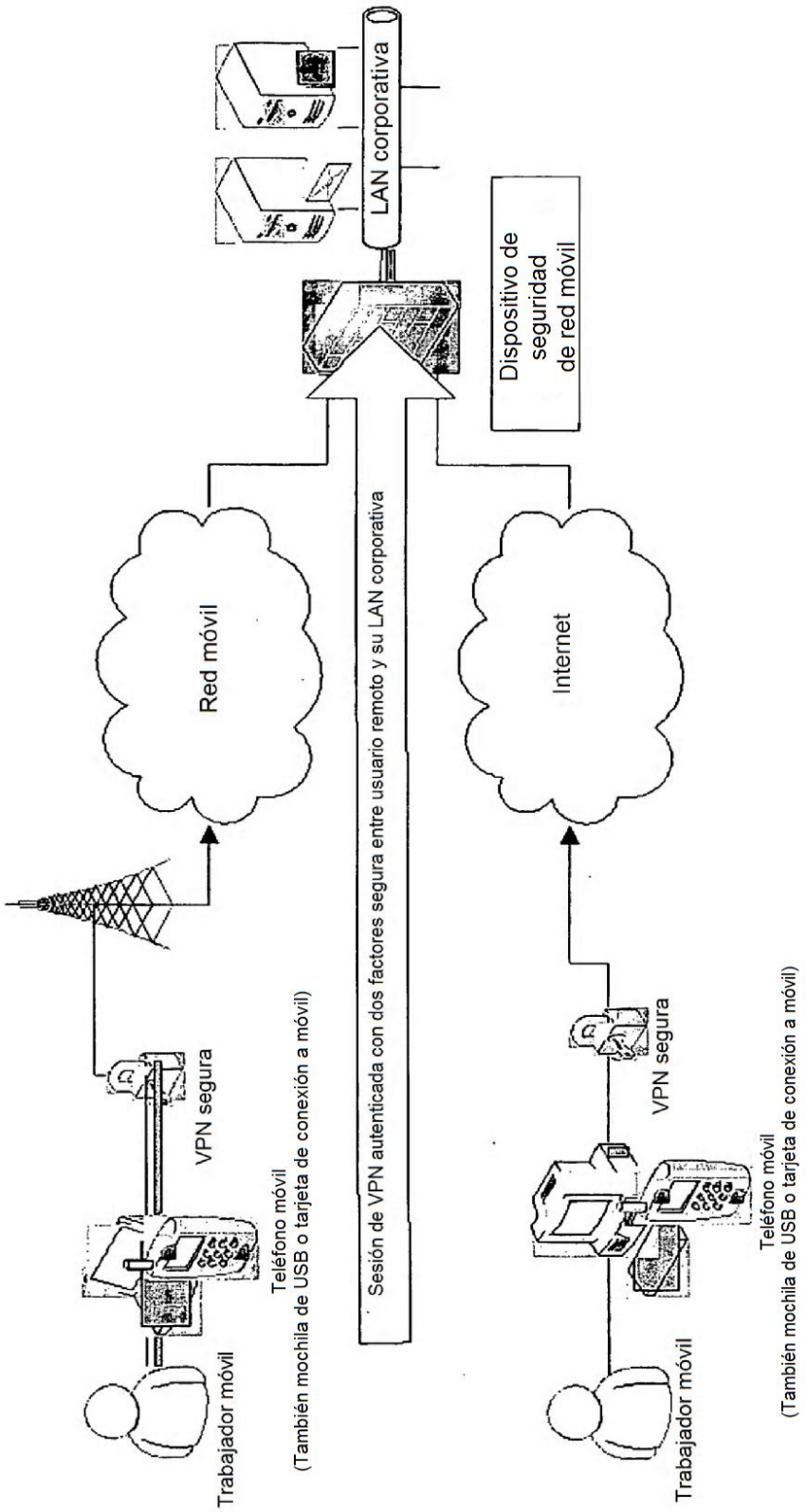
LAN corporativa
Dispositivo de seguridad de red móvil
Red móvil
Internet
Sesión de VPN autenticada con dos factores segura entre usuario remoto y su LAN corporativa
VPN segura
Teléfono móvil
(También mochila de USB o tarjeta de conexión a móvil)
Trabajador móvil
VPN segura
Teléfono móvil
(También mochila de USB o tarjeta de conexión a móvil)
Trabajador móvil

Fig. 1

2/8

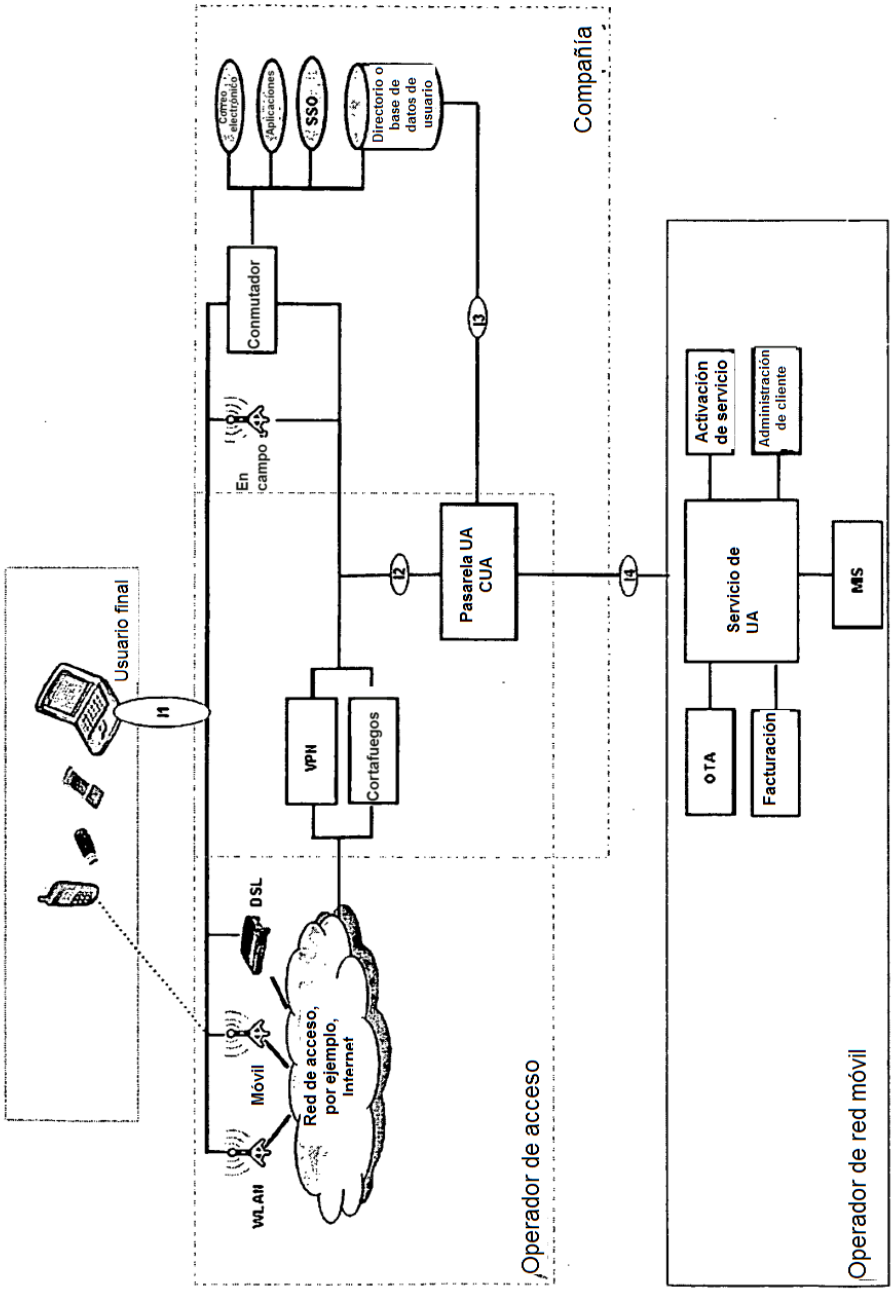
Usuario final
I1
Operador de acceso
Compañía
Correo electrónico
Aplicaciones
SSO
Directorio o base de datos de usuario
Conmutador
En campo
I3
VPN
Cortafuegos
I2
Pasarela UA CUA
I4
DSL
Móvil
WLAN
Red de acceso, por ejemplo, Internet
Operador de red móvil
Activación de servicio
Administración de cliente
Servicio de UA
MS
OTA
Facturación

Fig. 2

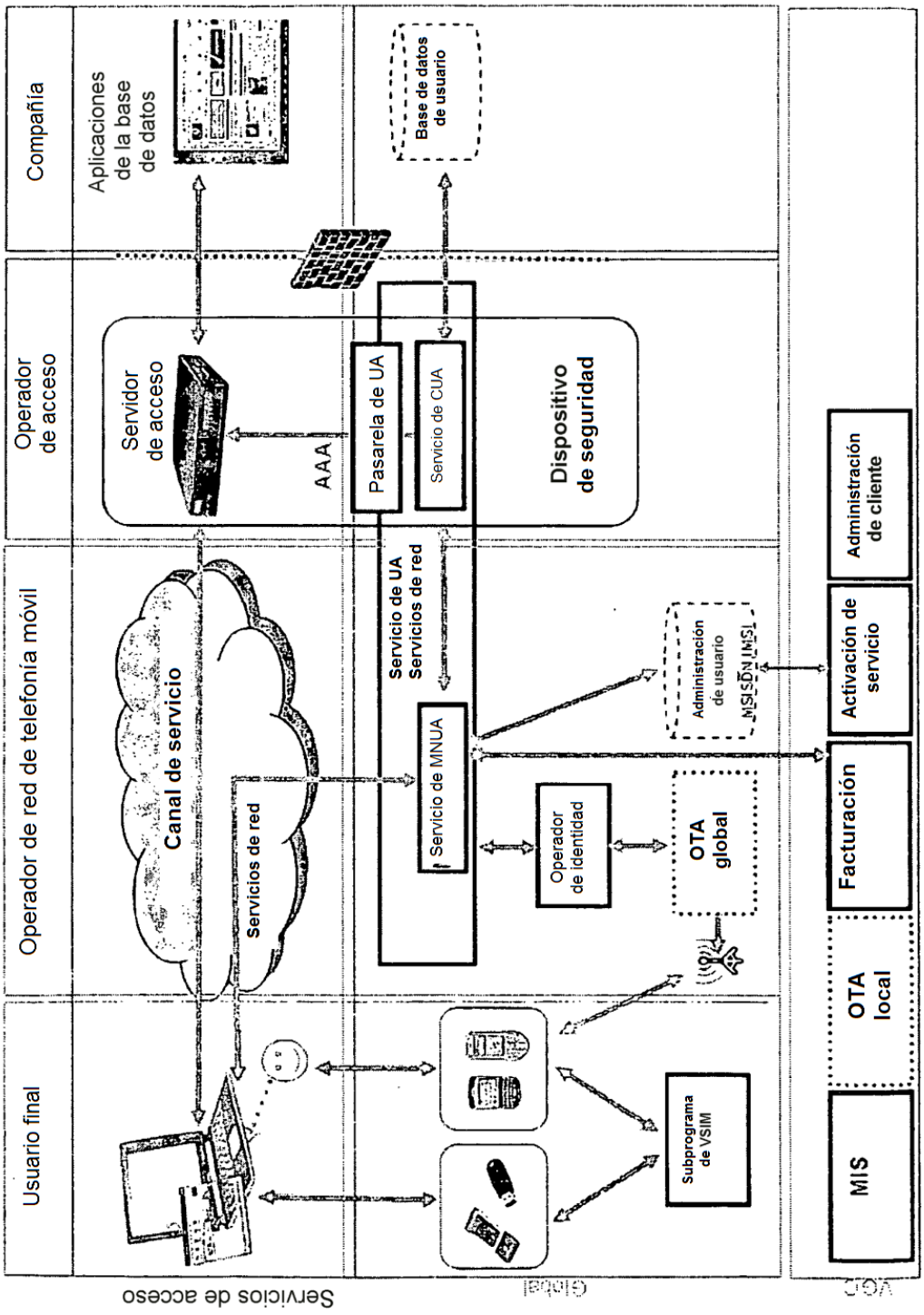
Compañía
Aplicaciones de la base de datos
Base de datos de usuario
Operador de acceso
Servidor de acceso
AAA
Pasarela de UA
Servicio de CUA
Dispositivo de seguridad
Operador de red de telefonía móvil
Canal de servicio
Servicios de red
Servicio de UA
Servicios de red
Servicio de MNUA
Operador de identidad
OTA global
Administración de usuario
MSISDN IMSI
Activación de servicio
Administración de cliente
Usuario final
Subprograma de VSIM
Facturación
OTA local
MIS
Servicios de acceso
Global
VOC

Fig. 3

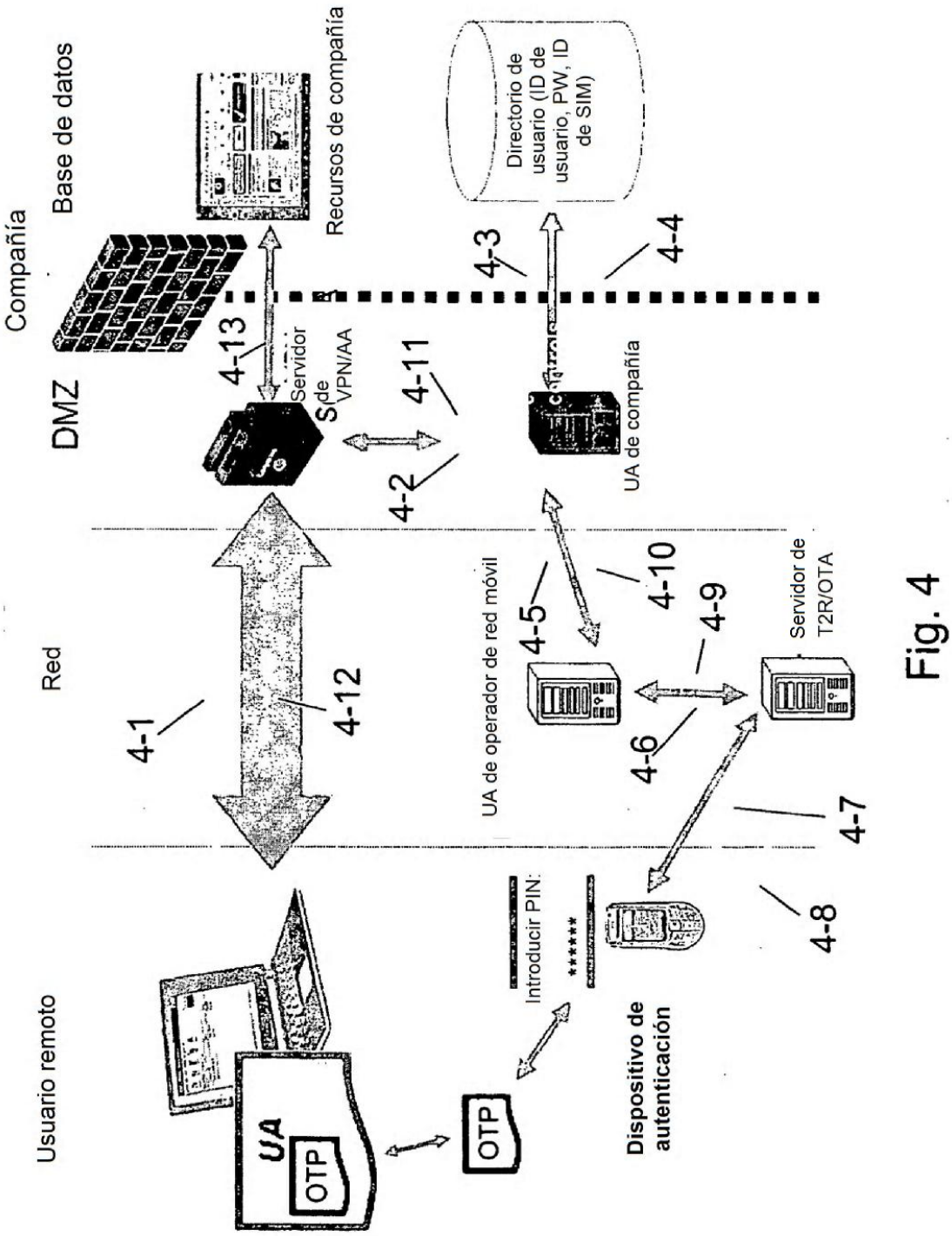
Compañía
Base de datos
Recursos de compañía
Directorio de usuario (ID de usuario, PW, ID de SIM)
DMZ
Servidor de VPN/AA
UA de compañía
Red
UA de operador de red móvil
Servidor de T2R/OTA
Usuario remoto
UA
OTP
OTP
Introducir PIN:
******
Dispositivo de autenticación
4-1
4-2
4-3
4-4
4-5
4-6
4-7
4-8
4-9
4-10
4-11
4-12
4-13

Fig. 4

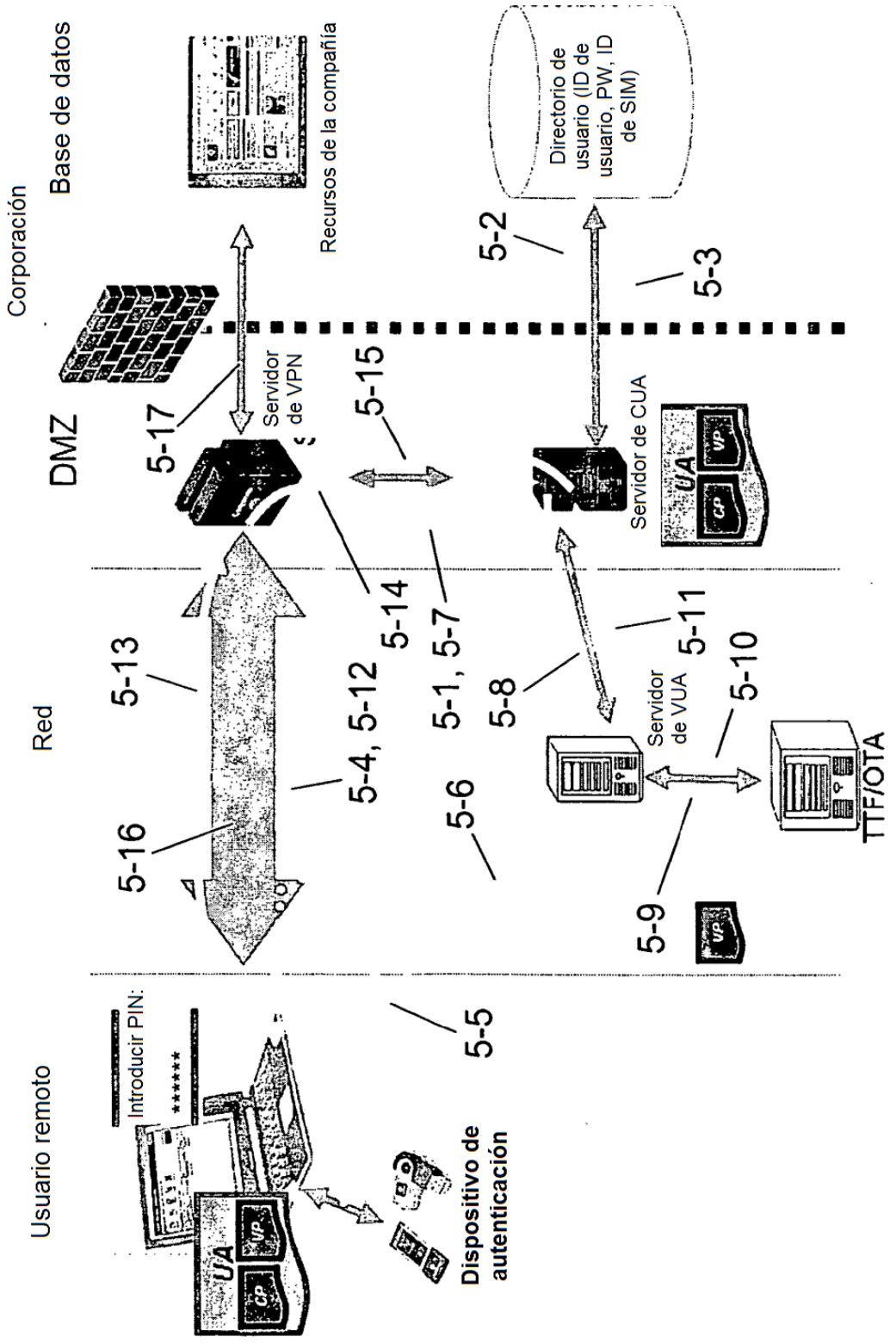
Corporación
Base de datos
Recursos de la compañía
Directorio de usuario (ID de usuario, PW, ID de SIM)
5-2
5-3
DMZ
5-17
Servidor de VPN
5-15
Servidor de CUA
Red
5-13
5-4, 5-12
5-14
5-1, 5-7
5-8
5-11
5-10
5-16
5-6
Servidor de VUA
TTF/OTA
5-9
Usuario remoto
Introducir PIN:
******
5-5
Dispositivo de autenticación

Fig. 5

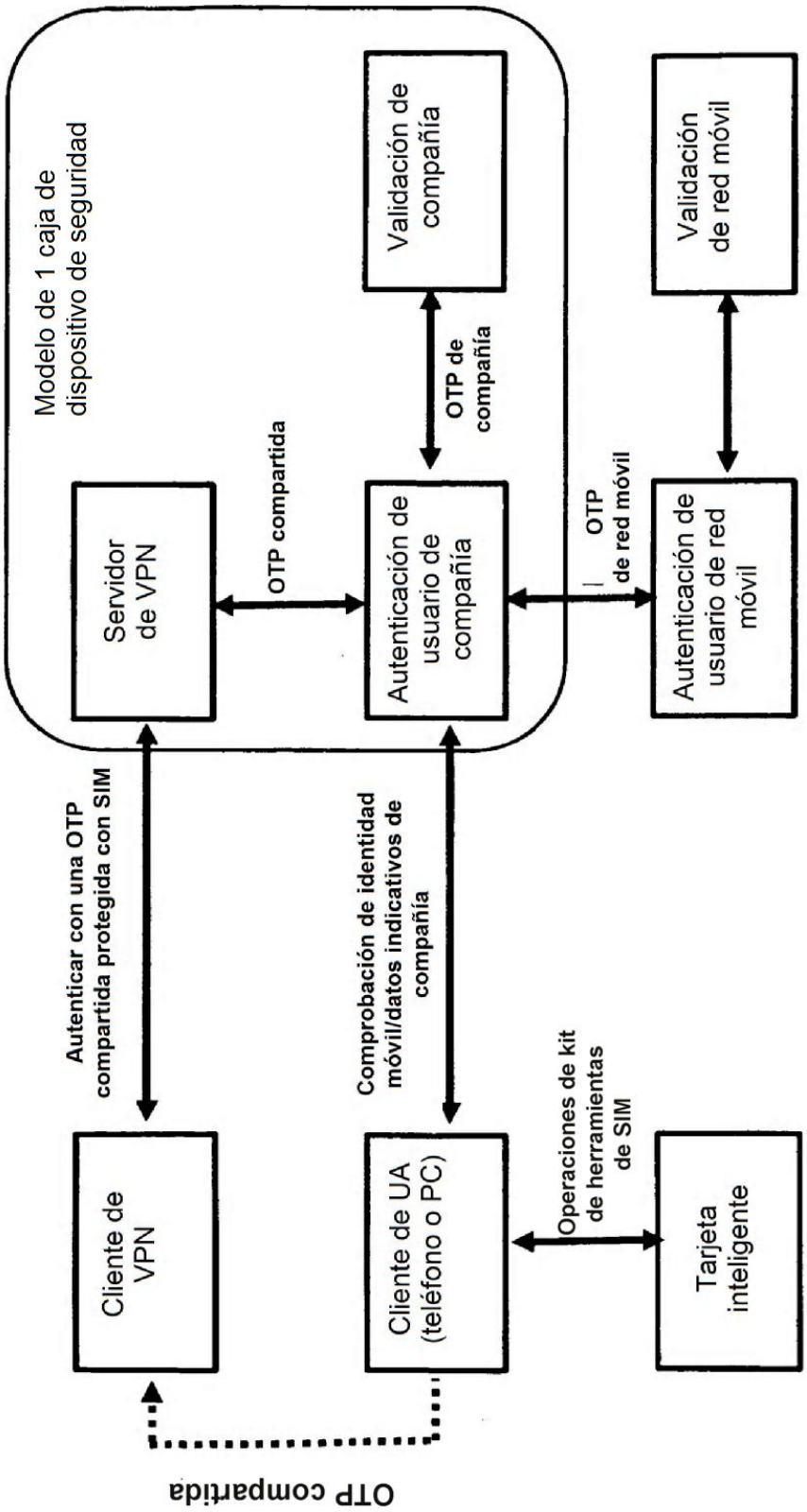
Modelo de 1 caja de dispositivo de seguridad
Servidor de VPN
OTP compartida
Autenticación de usuario de compañía
Validación de compañía
OTP de compañía
OTP de red móvil
Autenticación de usuario de red móvil
Validación de red móvil
Autenticar con una OTP compartida protegida con SIM
Comprobación de identidad móvil/datos indicativos de compañía
Operaciones de kit de herramientas de SIM
Cliente de VPN
Cliente de UA (teléfono o PC)
Tarjeta inteligente
OTP compartida

Fig. 6

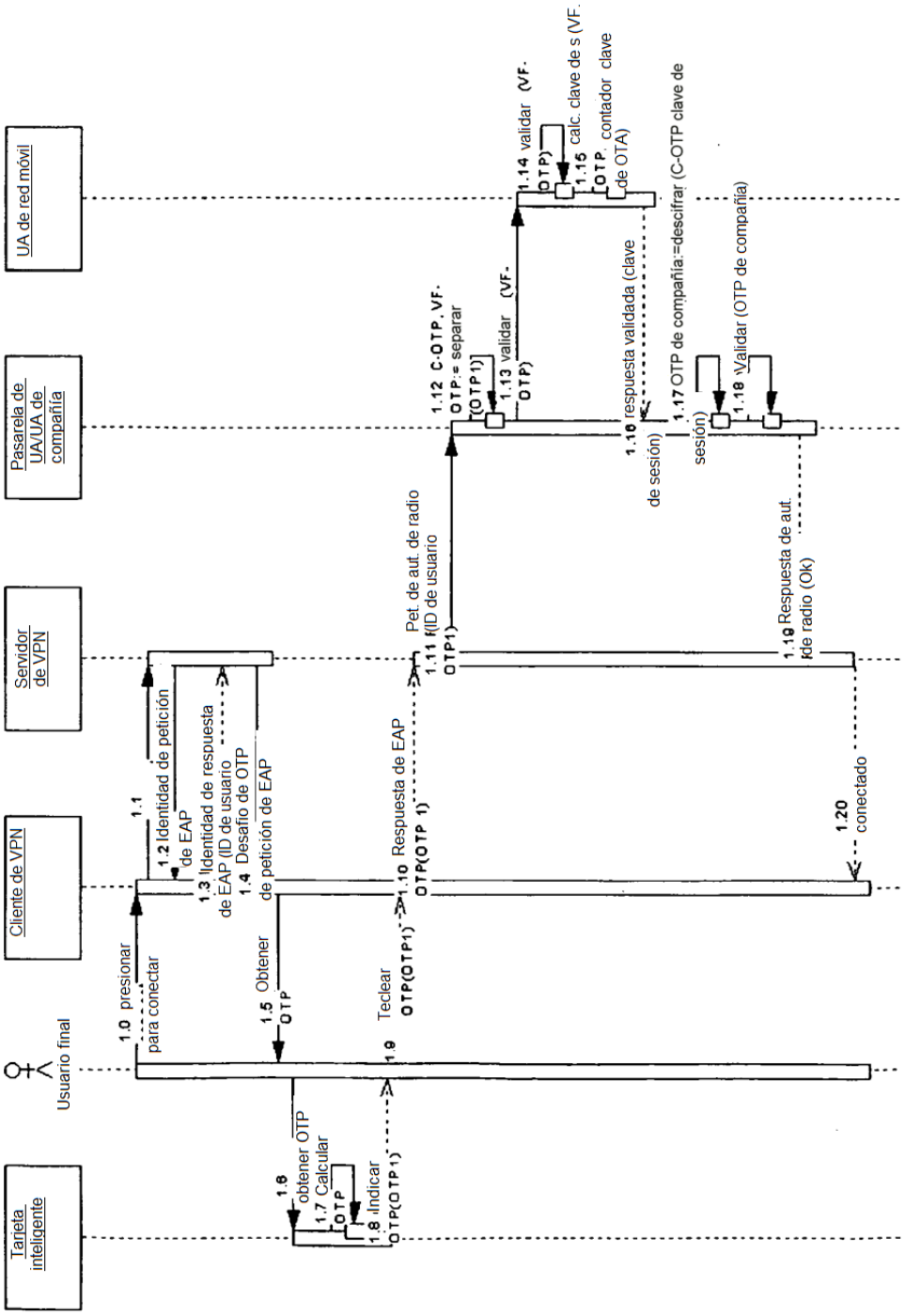
Tarjeta inteligente
Usuario final
Cliente de VPN
Servidor de VPN
Pasarela de UA/UA de compañía
UA de red móvil
1.0 presionar para conectar
1.1
1.2 Identidad de petición de EAP
1.3 Identidad de respuesta de EAP (ID de usuario
1.4 Desafío de OTP de petición de EAP
1.5 Obtener OTP
1.6 obtener OTP
1.7 Calcular OTP
1.8 Indicar OTP(OTP1)
1.9 Teclear OTP(OTP1)
1.10 Respuesta de EAP OTP(OTP 1)
1.11 Pet. de aut. de radio (ID de usuario OTP1)
1.12 C-OTP, VF-OTP:= separar (OTP1)
1.13 validar (VF-OTP)
1.14 validar (VF-OTP)
1.15 calc. clave de s (VF-OTP, contador clave de OTA)
1.16 respuesta validada (clave de sesión)
1.17 OTP de compañía:=descifrar (C-OTP clave de sesión)
1.18 Validar (OTP de compañía)
1.19 Respuesta de aut. de radio (Ok)
1.20 conectado

Fig. 7

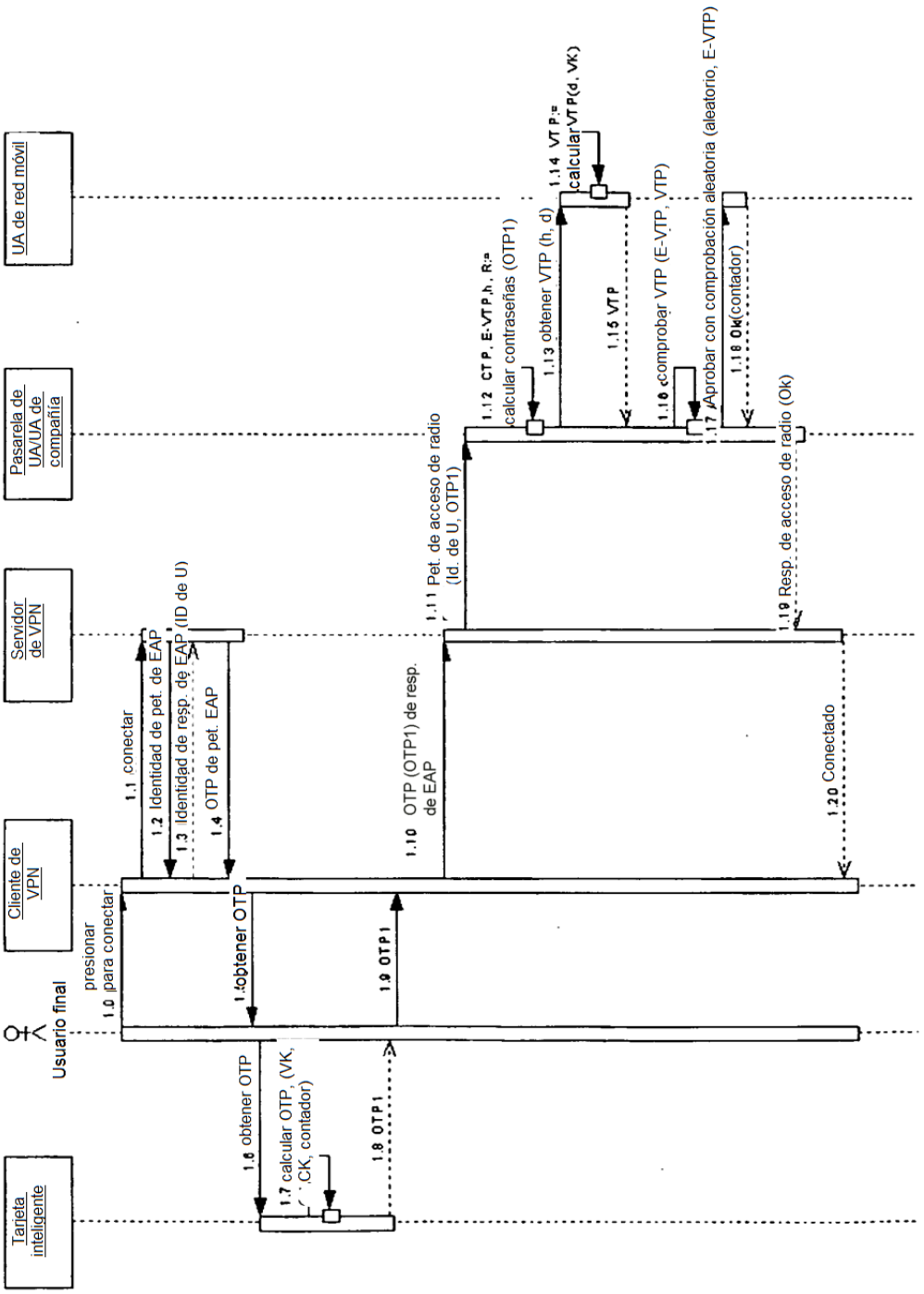
UA de red móvil
Pasarela de UA/UA de compañía
Servidor de VPN
Cliente de VPN
Usuario final
Tarjeta inteligente
1.0 presionar para conectar
1.1 conectar
1.2 Identidad de pet. de EAP
1.3 Identidad de resp. de EAP (ID de U)
1.4 OTP de pet. EAP
1.5 obtener OTP
1.6 obtener OTP
1.7 calcular OTP, (VK, CK, contador)
1.8 OTP1
1.9 OTP1
1.10 OTP (OTP1) de resp. de EAP
1.11 Pet. de acceso de radio (Id. de U, OTP1)
1.12 CTP, E-VTP,h, R:= calcular contraseñas (OTP1)
1.13 obtener VTP (h, d)
1.14 VTP:= calcular VTP(d, VK)
1.15 VTP
1.16 comprobar VTP (E-VTP, VTP)
1.17 Aprobar con comprobación aleatoria (aleatorio, E-VTP)
1.18 Ok(contador)
1.19 Resp. de acceso de radio (Ok)
1.20 Conectado

Fig. 8