(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 305 469**

(51) Int. Cl.:
G06F 21/00 (2006.01)
H04Q 7/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **03733773 .0**
(86) Fecha de presentación : **18.06.2003**
(87) Número de publicación de la solicitud: **1634133**
(87) Fecha de publicación de la solicitud: **15.03.2006**

(54) Título: **Una disposición y un método relacionados con el acceso a redes IP.**

(45) Fecha de publicación de la mención BOPI:
01.11.2008

(45) Fecha de la publicación del folleto de la patente:
01.11.2008

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (publ)
164 83 Stockholm, SE

(72) Inventor/es: **Norefors, Arne y**
Schuberth, Ulf

(74) Agente: **Elzaburu Márquez, Alberto**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Una disposición y un método relacionados con el acceso a redes IP.

Campo del invento

El presente invento se refiere a una disposición y a un método para proporcionar a un usuario final acceso a una red IP (protocolo Internet), es decir para registro de identificación de entrada de un usuario final. El invento se refiere también a un servidor de acceso de una red de acceso sobre la cual se proporciona acceso, es decir sobre la cual el usuario final puede registrar su identidad para entrada en la red IP.

Estado de la técnica

Para obtener acceso a algún tipo de servicio en general, se necesita la introducción de una contraseña y un nombre de usuario. Sin embargo, en la sociedad actual el número de contraseñas, etc, que un solo usuario necesita recordar, almacenar con seguridad, etc, es alto y podría aumentar aún adicionalmente. Podría existir una contraseña particular para acceso a redes de área local inalámbricas, para servicios de Internet, etc.

Los proveedores de servicios de Internet inalámbricos (WISP) ofrecen acceso a redes IP en base a un diálogo con el usuario a través de páginas web para comunicación de identificación de entrada y comunicación con protocolo Radius con un servidor Radius. El procedimiento típico es utilizar un nombre de usuario y una contraseña estática. Se han descrito prácticas preferidas sobre como podría hacerse esto, por ejemplo a través del WI-Fi Alliance industry forum accesible en el documento de mejores prácticas de proveedores de servicios Internet inalámbricos. Los protocolos implicados son HTTP y Radius definidos por IETF (página web www.ietf.org). Sin embargo, se utiliza normalmente un nombre de usuario estático en el registro de identificación de entrada. Un nombre de usuario estático puede ser copiado fácilmente y por tanto ser utilizado por varias personas. Un intento de resolver este problema consiste en utilizar una contraseña de un solo uso (OTP), que puede ser utilizada solamente durante un período de tiempo limitado, después del cual se bloquea. Para obtener acceso o entrar en Internet, por ejemplo en lugares públicos, tales como aeropuertos, estaciones de ferrocarril, hoteles, etc, puede utilizarse en general una red de área local de banda ancha como red de acceso. En general la cobertura no es demasiado grande y depende de la construcción, etc, del edificio, y además no existen demasiadas frecuencias disponibles. La construcción e integración de redes por radio es complicada y costosa. Los problemas relacionados con el acceso son así complicados por varias razones, tanto para operadores, como para usuarios y propietarios de redes.

El documento GB-A-2379040 describe un método para controlar el acceso de usuarios a un servicio remoto a través de una red enviando una contraseña de un solo uso al dispositivo portátil del usuario, realizándose a continuación un procedimiento de identificación de entrada normal. El documento US2003/0051041 describe la autentificación de un abonado a una red WLAN (red de área local inalámbrica) que intenta acceder a una red de área local. En el documento WO-A-02/084-456 se describe un método adicional de verificación de un usuario que intenta acceder a recursos de un sistema a través de una red inalámbrica.

Por consiguiente, se necesita una disposición a través de la cual pueda proporcionarse acceso a una red IP, con identificación de entrada, de un modo sencillo, tanto desde el punto de vista del usuario final como desde el punto de vista del operador. Se necesita también una disposición a través de la cual pueda proporcionarse identificación de entrada con un riesgo mínimo de abuso, por ejemplo mediante la copia de nombres de usuario, el encuentro de nombres de usuario inscritos en algún lugar, etc. Aun adicionalmente, se necesita una disposición a través de la cual pueda proporcionarse acceso/identificación de entrada sin un impacto sustancial sobre los servidores de acceso, y a través de la cual puedan utilizarse servidores de acceso existentes sin que se requiera actualización con aumento de prestaciones del servidor de acceso. Este es un aspecto importante puesto que la organización en la que funciona el servidor de acceso puede ser diferente de la del operador que controla la web y los nodos de autentificación, y tiene la relación comercial con el usuario. La reutilización de una red de acceso existente es especialmente ventajosa cuando se utiliza un sistema de acceso por radio, ya que una red de radio adicional podría interferir con la ya instalada. Aun adicionalmente, se necesita un método mediante el cual puedan conseguirse uno o más de los objetivos mencionados anteriormente. Aun adicionalmente, se necesita un servidor de acceso a través del cual puedan conseguirse uno o más de los objetivos mencionados, y que pueda utilizarse para proporcionar identificación de entrada.

Se necesita también una disposición mediante la cual se consiga una interfaz uniforme de identificación de entrada, incluso si el usuario final es atendido por proveedores de servicios de Internet inalámbricos independientes entre sí.

Resumen del invento

Por consiguiente, se crea un sistema que comprende una disposición como la referenciada anteriormente que incluye una estación de usuario final, un servidor de acceso a una red de acceso, un servidor de web y un servidor de autentificación que tiene las características específicas de de la reivindicación 1ª. La estación de usuario final puede considerarse como una unidad que comprende dos medios, primeros medios, por ejemplo un computador personal, y segundos medios, por ejemplo un teléfono móvil, siendo un aspecto importante, sin embargo, que una contraseña de un solo uso o código similar que se utiliza durante la primera fase se proporciona o transfiere al usuario a través de una red de telecomunicaciones móviles, y que el procedimiento de identificación de entrada se realiza en dos pasos o

fases. Se crea también un método para proporcionar a usuarios finales acceso (entrada con identificación) a una red IP que tiene las características específicas de la reivindicación 21ª.

Se crea también un servidor de acceso para una red de acceso que establece comunicación con una estación de usuario final para dar acceso a dicha estación de usuario final a una red IP, y con un servidor de acceso y un servidor de autentificación. El servidor de acceso tiene las características específicas de la reivindicación 19ª.

Las reivindicaciones auxiliares especifican implementaciones preferidas o ventajosas.

Un sistema de acuerdo con el presente invento comprende así una estación de usuario final, un servidor de acceso y una red de acceso, un servidor de web y un servidor de autentificación. Comprende una estación de usuario final con primeros medios para comunicación con un servidor de acceso, y segundos medios para establecer comunicación con un servidor de autentificación a través de un sistema de telecomunicaciones móviles, y el procedimiento de acceso/identificación de entrada comprende una primera y una segunda fases. El servidor de autentificación controla la primera fase, comprendiendo dicha primera fase una secuencia de entrada de identificación por contraseña de un solo uso (OTP), y la segunda fase de identificación de entrada se realiza creando/modificando una cuenta provisional para la cual están definidas las credenciales del usuario para dar entrada al usuario final en el servidor de acceso. En particular, la segunda fase de identificación de entrada se realiza si es válida la contraseña de un solo uso. Para la segunda fase, se crea/modifica una cuenta de usuario en el servidor de acceso, que en particular es transitoria, es decir permite la identificación de entrada solamente durante un período de tiempo limitado. El servidor de acceso es operado en particular por un proveedor de servicios de Internet inalámbricos. La contraseña de un solo uso utilizada en la primera fase es reutilizada en una implementación en la segunda fase. Particularmente, la contraseña de un solo uso es creada por el servidor de acceso y es transferida desde el mismo a los segundos medios de la estación de usuario final a través del sistema de telecomunicación móvil. Los primeros medios de la estación de usuario final pueden comprender un computador personal, y los segundos medios pueden comprender un teléfono móvil. Son también posibles otras alternativas.

La contraseña de un solo uso es transferida más particularmente mediante un mensaje de texto alfanumérico, por ejemplo un mensaje SMS o un mensaje de voz, a los segundos medios (por ejemplo, un teléfono móvil) de la estación de usuario. Cuando es transferida a la estación de usuario (teléfono móvil), la contraseña de un solo uso ha de ser introducida en los primeros medios de la estación de usuario (computador personal o PC) y suministrada al servidor de acceso para autentificación/validación. Si la contraseña de un solo uso es válida, puede reutilizarse la contraseña de un solo uso de la primera fase en la segunda fase. Si la contraseña de un solo uso es válida, se definen en particular un nombre de usuario y una contraseña de la cuenta creada/modificada, datos que están vinculados singularmente a la secuencia de contraseña de un solo uso. La segunda fase puede ser realizada de diferentes modos, y el nombre y la contraseña de usuario pueden utilizarse de diferentes maneras.

En una realización, en la segunda fase se utiliza el mismo nombre de usuario que en la primera fase y la contraseña de un solo uso se utiliza como contraseña. En otra realización se utiliza un nombre de usuario dinámico y la contraseña de un solo uso (de la primera fase) se utiliza como contraseña. Aun adicionalmente, puede utilizarse un nombre de usuario estático (común para todos los usuarios) y puede utilizarse como contraseña la contraseña de un solo uso (de la primera fase). Aun en otra realización se utiliza un nombre de usuario estático (común para todos los usuarios) y se utiliza como contraseña un número aleatorio. Aun adicionalmente, puede utilizarse un nombre de usuario dinámico y puede utilizarse como contraseña un valor aleatorio. Son posibles también otras alternativas.

Ventajosamente, el servidor de páginas redirige el mensaje de identificación de entrada a la página de identificación de entrada del servidor de acceso cuando ha de crearse/modificarse una cuenta en el servidor de autentificación, y se ajusta un temporizador a un período de tiempo dado durante el cual se comprueban las credenciales del usuario, y si no son válidas, se retorna un mensaje de error al usuario. En particular, si las credenciales de usuario comprenden un nombre de usuario y una contraseña, y si se verifican/autentifican dentro del período de tiempo dado, se proporciona acceso al usuario y la cuenta de usuario provisional añadida o modificada es eliminada/inhabilitada. En una implementación, el servidor de autentificación comprende un servidor Radius, y en otra implementación un servidor Diameter. Sin embargo, puede utilizarse cualquier servidor de autentificación adecuado. En algunas realizaciones están dispuestos uno o más servidores proxy entre el servidor de acceso (AS) y el servidor de autentificación (Radius, Diameter, etc). La red de acceso comprende en particular una red de área local inalámbrica (WLAN), una red Ethernet o similar.

Ventajosamente, la sintaxis de identificación de entrada está almacenada en el servidor de acceso, y esta información es transferida al servidor de páginas para formar parte subsiguientemente de un mensaje redirigido. Alternativamente, la sintaxis de identificación de entrada se almacena con el operador lo cual, sin embargo, es más difícil de administrar porque el operador necesita un conocimiento detallado de los diferentes servidores de acceso de los proveedores de servicios de Internet (inalámbricos). (Para un operador han de utilizarse normalmente servidores de acceso de varios fabricantes).

El invento crea también un servidor de acceso en una red de acceso que comunica con una estación de usuario final, para proporcionar a dicha estación de usuario final acceso a una red IP, a un servidor de páginas o a un servidor de autentificación. El servidor de acceso permite a cualquier usuario realizar un intento de acceso al servidor de páginas, por ejemplo utilizando una función de lista en blanco o un enlace de identificación de entrada con el operador, y soporta la modalidad de deambulación de servidor de autentificación. El servidor de acceso soporta una segunda fase

de un procedimiento de identificación de entrada a continuación de una primera fase durante la cual se proporciona una contraseña de un solo uso. Para dicha segunda fase se crea/modifica una cuenta de usuario provisional, cuya contraseña y nombre de usuario están asociados singularmente con la contraseña de un solo uso dada por el servidor de autentificación y proporcionada a la estación de usuario a través de un sistema de comunicaciones móviles, por ejemplo un mensaje SMS, un mensaje de voz o sistema similar al utilizado en la primera fase. El sistema puede incluir, por ejemplo, un servidor de acceso de una red de área local inalámbrica, una red Ethernet, operado por un Proveedor de Servicios de Internet, por ejemplo un Proveedor de Servicios de Internet inalámbrico.

El invento crea también un método para proporcionar a un usuario final acceso a una red IP a través de una red de acceso que comprende un servidor de acceso. Para el procedimiento de identificación de entrada, el método comprende las operaciones de:

- realizar una primera fase de un procedimiento de identificación de entrada mediante el cual es proporcionada por un servidor de autentificación una contraseña de un solo uso y es transferida al usuario final a través de un sistema de comunicaciones móviles, por ejemplo mediante un mensaje SMS o un mensaje de voz,
- comprobar la validez/autenticidad de la contraseña de un solo uso (y si es válida),
- añadir/modificar una cuenta provisional en el servidor de autentificación, para una segunda fase del procedimiento de identificación de entrada,
- definir un nombre de usuario y una contraseña vinculada singularmente a la contraseña de un solo uso de la primera fase,
- comprobar la validez del nombre de usuario y la contraseña en el servidor de autentificación, y si es válida,
- admitir la solicitud de identificación de entrada del usuario,
- eliminar/inhabilitar la cuenta de usuario provisional después de transcurrir un período de tiempo predeterminado.

En particular, las operaciones asociadas con la realización de la primera fase comprenden las operaciones de:

- enviar una solicitud de identificación de entrada a un servidor de acceso desde la estación de usuario,
- recibir una respuesta del servidor de acceso si la estación de usuario habilita la activación de un enlace al servidor de la página del operador (identificación de entrada),
- acceder al servidor de páginas e introducir la identidad de la estación de usuario en el servidor de páginas,
- proporcionar una contraseña de un solo uso a la estación de usuario desde el servidor de autentificación y transferirla a la estación de usuario a través del sistema de comunicaciones móviles, por ejemplo mediante un mensaje SMS o un mensaje de voz,
- solicitar la contraseña de un solo uso mediante el servidor de páginas y verificar la validez/autenticidad de la contraseña de un solo uso, mientras que la segunda fase comprende ventajosamente las operaciones de:
- redirigir la solicitud de identificación de entrada a la página de identificación de entrada del servidor de acceso,
- ajustar un temporizador, comprobar la validez/autenticidad de las credenciales del usuario, por ejemplo contraseña, nombre de usuario, en el servidor de autentificación, y si estos datos son válidos,
- eliminar/inhabilitar la cuenta provisional al expirar el intervalo del temporizador ajustado.

En particular, puede utilizarse en la segunda fase el mismo nombre de usuario que en la primera fase, y puede utilizarse la contraseña de un solo uso como contraseña. En una realización, el método comprende las operaciones de; en la segunda fase:

- utilizar un nombre de usuario dinámico,
- utilizar la contraseña de un solo uso de la primera fase como contraseña.

Alternativamente, comprende las operaciones de:

- utilizar un nombre de usuario estático común a todos los usuarios,
- utilizar la contraseña de un solo uso de la primera fase o un número aleatorio como contraseña,

Aun adicionalmente, puede comprender las operaciones de, en la segunda operación:

- utilizar un nombre de usuario dinámico,
- utilizar como contraseña un valor aleatorio.

Breve descripción de los dibujos

Se describirá el invento adicionalmente a continuación, de un modo no limitativo, y con referencia a los dibujos que se acompañan, en los cuales:

La figura 1 es un diagrama de bloques muy esquemático que ilustra una disposición de acuerdo con el presente invento,

La figura 2 es un diagrama de flujo esquemático que describe el concepto del invento, y

La figura 3 es un diagrama de transferencia de señales que describe una implementación del concepto del invento.

Descripción detallada del invento

La figura 1 representa un usuario 1 con una estación 2 de usuario que comprende primeros medios, un terminal, por ejemplo un computador personal PC 2ª, y segundos medios, por ejemplo un teléfono móvil 2B. El terminal 2A establece comunicación con un servidor 3 de acceso que es operado por un Proveedor de Servicios de Internet (ISP) o un proveedor de servicios de Internet inalámbricos (WISP). El servidor 3 de acceso es un servidor de acceso de una red de acceso, por ejemplo una red de área local inalámbrica o una red Ethernet, que comunica con un servidor 4 de páginas y un servidor 5 de autentificación. Mediante la implementación del concepto del invento, puede utilizarse sustancialmente cualquier servidor de acceso en principio sin modificación (solamente necesita alguna reconfiguración). Solamente se imponen requerimientos limitados y poco importantes al servidor de acceso, tales como la adición de un enlace de identificación de entrada con el operador, la capacidad de soportar deambulación en el servidor de autentificación y proporcionar una lista blanca o información similar, es decir el usuario puede llegar al servidor de páginas antes de una autentificación con éxito. El servidor 5 de autentificación puede ser, por ejemplo, un servidor Radius (Servidor de Marcación de Acceso Remoto) o un servidor Diameter o similar. El servidor Radius se describe en Radius, IEEE RFC (Request for Comments: solicitud de comentarios) 2865. Puede haber también más de un servidor de autentificación. Por ejemplo, pueden estar dispuestos dos servidores de autentificación, cada uno de los cuales soporta una fase del procedimiento de identificación de entrada.

El sistema 6 de telecomunicaciones móviles con el centro 7 de servicio de mensajes cortos (SMS-C), se utiliza en este caso para proporcionar al usuario una contraseña de un solo uso, como se describirá con más detalle posteriormente.

Para iniciar el procedimiento, el terminal, por ejemplo un computador personal 2A, establece comunicación con el servidor 3 de acceso operado por un proveedor de servicios de Internet (inalámbricos), lo cual permite al usuario entrar en contacto con el servidor 4 de páginas, a través del cual puede solicitarse una contraseña de un solo uso del servidor 5 de autentificación. El servidor de autentificación proporciona entonces una contraseña de un solo uso y la transfiere a la estación de usuario (segundos medios, teléfono móvil 2B) a través del sistema 6 de telefonía móvil por medio de un centro 7 de servicio de mensajes cortos. El procedimiento de identificación de entrada es manejado en una primera fase y una segunda fase, de las cuales la primera es una secuencia de contraseña de un solo uso controlada por el servidor 5 de autentificación. Si esta primera fase tiene éxito, es decir cuando se entrega y verifica una contraseña de un solo uso, se realiza a continuación la segunda fase de identificación de entrada que da entrada al usuario al servidor 3 de acceso. La contraseña de un solo uso obtenida y utilizada en la primera fase puede ser reutilizada en la segunda fase. Son también posibles, sin embargo, otras alternativas que se describirán posteriormente con más detalle.

De acuerdo con el invento, operadores propietarios de redes y que tienen una gran cantidad de clientes, son habilitados para ofrecer servicios con marca, en base a contraseñas de un solo uso, a sus clientes en virtud de acuerdos de sociedad con proveedores de redes de acceso que tienen servidores de acceso, sin que existan requerimientos considerables sobre los servidores de acceso. La entrada con identificación a diferentes tipos/marcas de servidores de acceso puede ser gestionada fácilmente puesto que la sintaxis de identificación de entrada es manejada por un proveedor de servicios de Internet (inalámbricos). De acuerdo con el invento, se crea una cuenta provisional que permite el acceso durante un período de tiempo limitado y se utiliza durante la segunda fase de identificación de entrada.

En el diagrama de flujo de la figura 2, se ilustra una implementación general del concepto del invento. Se supone así que se establece comunicación entre la estación de usuario final (es decir, los primeros medios de la estación de usuario final, por ejemplo un computador personal) y el servidor de acceso en base a que el usuario solicita una página de identificación de entrada (operación 100). El servidor de acceso responde a la solicitud suministrando al usuario final una página de identificación de entrada (operación 101). El usuario pulsa un botón de enlace con el operador en la página de identificación de entrada del servidor de acceso para llegar al servidor de páginas (operación 102). El servidor de páginas solicita a continuación una identidad de usuario del usuario final (operación 103). La identidad del usuario final es introducida entonces por el usuario en la página del servidor de páginas (operación 104).

Subsiguientemente, un servidor de autentificación puede comprobar la identidad del usuario. Esta es, sin embargo, una operación opcional y por tanto el bloque de la operación 105 está indicado dentro de líneas discontinuas en la figura. A no ser que se haya obtenido una identidad de usuario válida, el procedimiento se interrumpe y el usuario recibe un mensaje de error.

El servidor de autentificación es, en una implementación ventajosa, un servidor Radius. En otra realización, comprende un servidor Diameter. Puede ser, sin embargo, cualquier servidor de autentificación.

El servidor de autentificación envía subsiguientemente, a través de un sistema de telefonía móvil, una contraseña de un solo uso, por ejemplo mediante un mensaje SMS o un mensaje de voz, al usuario final (operación 106). (También en este caso el procedimiento se interrumpe, y por ejemplo se envía un mensaje de error al receptor a no ser que se haya obtenido una identidad de usuario válida dentro de un período de tiempo predeterminado). Subsiguientemente, el servidor de páginas solicita la contraseña de un solo uso del usuario final (operación 107), que introduce la contraseña de un solo uso recibida, por ejemplo mediante un mensaje SMS. Después de esto, el servidor de autentificación comprueba la contraseña de un solo uso (operación 109). Si se introdujo una contraseña de un solo uso válida (operación 110), se procede con la segunda fase del procedimiento de identificación de entrada, como se describirá posteriormente. (De este modo, la primera fase del procedimiento de identificación de entrada comprende las operaciones 100-110). Si no se introdujo una contraseña de un solo uso válida, se retorna al usuario un mensaje de error (operación 110A) y se interrumpe el procedimiento.

En la segunda fase del procedimiento de identificación de entrada (suponiendo que el usuario introdujo una contraseña de un solo uso válida), el servidor de autentificación añade/modifica una cuenta provisional (operación 111). Se proporcionan credenciales de usuario (por ejemplo, el nombre y contraseña del usuario) para la cuenta provisional. El servidor de páginas redirige entonces el mensaje de solicitud de identificación de entrada a la página de identificación de entrada del servidor de acceso (operación 112). A continuación, se dispara el inicio de un temporizador T1 (operación 113). Se envía entonces una solicitud de autentificación desde el servidor de acceso hasta el servidor de autentificación, que comprueba las credenciales de usuario (operación 114) para verificar si son válidas. Si no es así, se retorna un mensaje de error al usuario final (operación 114A). Si son válidas, por ejemplo al expirar el período del temporizador T1 (o antes), la cuenta provisional del usuario se elimina o inhabilita (operación 115).

Se describirá ahora una implementación algo más elaborada con referencia al diagrama de transferencia de señales de la figura 3. En primer lugar, se envía una solicitud HTTP desde la estación de usuario (primeros medios) hasta el servidor de acceso (operación 1). La solicitud se introduce en la página de identificación de entrada del servidor de acceso. El servidor de acceso retorna al usuario una respuesta con la página de identificación de entrada (operación 2). La página de identificación de entrada contiene un botón o dispositivo virtual similar, cuya activación da lugar a un enlace con el servidor de identificación de entrada del operador. Se supone que el usuario subsiguientemente pulsa el enlace y llega entonces al servidor de páginas del operador, puesto que el acceso a este servidor de páginas está abierto en el servidor de acceso por configuración (operación 3). Particularmente, la sintaxis del mensaje de identificación de entrada a utilizar en la segunda fase del procedimiento de identificación de entrada puede transferirse en este mensaje. A continuación, el servidor de páginas solicita la identidad del usuario (operación 4), y en respuesta a esta solicitud el usuario introduce su identidad, por ejemplo MSISDN (operación 5). Esta identidad es cursada al servidor de autentificación (operación 6), que crea una contraseña de un solo uso y la transfiere al centro de servicio de mensajes cortos (SMS-C) de un sistema de comunicaciones móviles, que transfiere la contraseña de un solo uso al usuario, por ejemplo mediante un mensaje SMS (operación 7). La información contenida en la misma es proporcionada al servidor de acceso y al servidor de páginas (operación 8) y se solicita al usuario que introduzca la contraseña de un solo uso mediante el servidor de autentificación (operación 9) y el servidor de páginas (operación 10). El usuario introduce entonces la contraseña de un solo uso proporcionada, por ejemplo, por el mensaje SMS o por un mensaje de voz, en los primeros medios de la estación de usuario (por ejemplo, un computador personal), y la contraseña de un solo uso se introduce en el servidor de autentificación a través del servidor de páginas (operaciones 11, 12). El servidor de autentificación verifica entonces la contraseña de un solo uso para ver si es válida. Si la respuesta es afirmativa, se envía al servidor de páginas (operación 13) un mensaje con información relativa a ese hecho. (En una implementación podría crearse una cuenta dinámica antes de haber sido retornada una contraseña de un solo uso correcta, por ejemplo por razones de rendimiento). En esta etapa del procedimiento de identificación de entrada, se termina la primera fase y se continúa con la segunda fase de identificación de entrada.

A continuación, en esta implementación se crea una cuenta provisional de usuario o se modifica para convertirla en una cuenta con un identificador de usuario y una contraseña de un solo uso como contraseña (operación 14). Se envía a continuación un mensaje de redirección a la estación de usuario con el localizador universal de recursos (URL), por ejemplo http://<access server IP address> /login? user name = <username> & <password = OTP>, donde cualquiera que sea lo que está entre los símbolos <> se sustituye por valores en curso (operación 15). El mensaje de identificación de entrada es enviado entonces al servidor de acceso operado por el proveedor de servicios de Internet (inalámbricos) (operación 16). Se envía subsiguientemente una solicitud de autentificación al servidor de autentificación, posiblemente a través de uno o más servidores proxy (operación 17). En esta realización particular, el servidor de autentificación comprende un servidor Radius, como se ha comentado anteriormente en esta solicitud. El servidor Radius (en este caso) responde con un mensaje de aceptación de acceso dirigido al servidor de acceso y este servidor abre la comunicación, después de verificar que las credenciales del usuario son correctas. El usuario recibe la respuesta cuando/si la autentificación tiene éxito (operación 19). Puede contener un portal de página web forzada y una ventana de sesión registrada comercialmente por el operador.

Finalmente, las credenciales almacenadas para la segunda fase del procedimiento de identificación de entrada son bloqueadas después de un retardo correspondiente a un período de tiempo dado para identificaciones múltiples, a no ser que se produzca inmediatamente a continuación la secuencia de contraseña de un solo uso de identificación de entrada (operación 20). En una implementación, se utiliza un temporizador para este fin. Son también posibles otros modos de operación.

La segunda fase del procedimiento de identificación de entrada puede realizarse de diferentes maneras. Las credenciales (por ejemplo el nombre de usuario y la contraseña) de la cuenta provisional pueden definirse de modos diferentes de acuerdo con diferentes realizaciones. Pueden tener valores estáticos o dinámicos. La combinación del nombre de usuario y la contraseña debe estar ligada singularmente a la secuencia anterior de contraseña de un solo uso (de la primera fase de identificación de entrada). En una implementación, se utiliza el mismo nombre de usuario que en la primera fase (parte de contraseña de un solo uso), y la contraseña de un solo uso se utiliza como contraseña. En otra implementación se utiliza un nombre de usuario dinámico y la contraseña de un solo uso se utiliza como contraseña.

Aun adicionalmente, puede utilizarse un nombre de usuario dinámico, mientras que se utiliza como contraseña un valor aleatorio. De acuerdo con otra realización aun adicional, se utiliza un nombre de usuario estático que es común para todos los usuarios. A continuación, puede utilizarse como contraseña la contraseña de un solo uso, o alternativamente puede utilizarse un valor aleatorio. Son también posibles varias otras alternativas. En otros aspectos, el invento no está limitado a las realizaciones ilustradas específicamente, sino que pueden introducirse variantes de varias maneras dentro del ámbito de las reivindicaciones anexas.

REIVINDICACIONES

1. Un sistema para dar acceso a un usuario final, por medio de un procedimiento de acceso/identificación de entrada, a una red IP (protocolo Internet), que comprende una estación (2) de usuario, un servidor (3) de acceso de una red de acceso, un servidor (4) de páginas y un servidor (5) de autentificación, comprendiendo la estación (2) de usuario primeros medios (2A) para comunicación con el servidor (3) de acceso y el servidor (4) de páginas, y segundos medios (2B) para comunicación con el servidor (5) de autentificación a través de un sistema de telecomunicación móvil, **caracterizado** porque el procedimiento de acceso/identificación de entrada comprende una primera y una segunda fases, y porque el servidor (3) de acceso está preparado para, en la primera fase, al recibir una solicitud de identificación de entrada de la estación (2) de usuario, proporcionar una respuesta a la estación (2) de usuario activando un enlace con el servidor (4) de páginas del operador, y almacenar la sintaxis de identificación de entrada, porque la estación (2) de usuario está preparada para proporcionar al servidor (4) de páginas, al recibir dicha respuesta, un mensaje de identificación de entrada pulsando el enlace o un botón, que incluye información de sintaxis de identificación de entrada del mensaje de identificación de entrada, porque el servidor (4) de páginas está destinado a solicitar la entrada de la identidad del usuario final y, al recibir la identidad del usuario final, proporcionar la identidad del usuario final al servidor (5) de autentificación, estando preparado el servidor (5) de autentificación para crear una contraseña de un solo uso y transferirla a la estación (2) de usuario a través del sistema (6) de comunicaciones móviles, y el servidor (4) de páginas está destinado a solicitar al usuario final la introducción de la contraseña de un solo uso, estando destinado el servidor (5) de autentificación a verificar la validez de la contraseña de un solo uso, y porque, en la segunda fase si la contraseña de un solo uso es válida, se crea una cuenta provisional de usuario en el servidor (5) de autentificación, y el servidor (5) de autentificación está preparado para enviar a la estación (2) de usuario un mensaje de identificación de entrada de redirección que incluye la sintaxis de identificación de entrada del mensaje de identificación de entrada para redirigir al servidor (3) de acceso la página de identificación de entrada, y eliminar/inhabilitar la cuenta provisional de usuario después de un retardo dado.

2. Un sistema de acuerdo con la reivindicación 1ª, **caracterizado** porque el servidor (3) de acceso es operado por un Proveedor de Servicios de Internet.

3. Un sistema de acuerdo con la reivindicación 2ª, **caracterizado** porque el Proveedor de Servicios de Internet ofrece un servicio inalámbrico, es decir es un proveedor de servicios de Internet inalámbricos.

4. Un sistema de acuerdo con cualquiera de las reivindicaciones 1ª a 3ª, **caracterizado** porque la contraseña de un solo uso utilizada en la primera fase es reutilizada en la segunda fase.

5. Un sistema de acuerdo con cualquiera de las reivindicaciones 1ª a 4ª, **caracterizado** porque los primeros medios de la estación de usuario comprenden un computador personal (2A), y porque los segundos medios comprenden un teléfono móvil (2B).

6. Un sistema de acuerdo con la reivindicación 5ª, **caracterizado** porque el servidor (5) de autentificación está destinado a transferir la contraseña de un solo uso, a través de un mensaje alfanumérico, a los segundos medios (2B) de la estación de usuario a través del sistema (6) de telecomunicación móvil.

7. Un sistema de acuerdo con la reivindicación 5ª, **caracterizado** porque los primeros medios (2A) de la estación (2) de usuario están destinados a proporcionar una contraseña de un solo uso introducida por el usuario final en el servidor (5) de autentificación para autentificación/validación.

8. Un sistema de acuerdo con la reivindicación 7ª, **caracterizado** porque si la contraseña de un solo uso es válida, la contraseña de un solo uso de la primera fase se reutiliza en la segunda fase.

9. Un sistema de acuerdo con cualquiera de las reivindicaciones precedentes, **caracterizado** porque si la contraseña de un solo uso es válida, se definen el nombre de usuario y una contraseña de la cuenta creada/modificada, que están vinculados singularmente a la secuencia de la contraseña de un solo uso.

10. Un sistema de acuerdo con la reivindicación 9ª, **caracterizado** porque en la segunda fase se utiliza el mismo nombre de usuario que en la primera fase, y porque la contraseña de un solo uso se utiliza como contraseña.

11. Un sistema de acuerdo con la reivindicación 10ª, **caracterizado** porque para la segunda fase se utiliza un nombre de usuario dinámico, y porque la contraseña de un solo uso de la primera fase se utiliza como contraseña.

12. Un sistema de acuerdo con la reivindicación 9ª, **caracterizado** porque para la segunda fase se utiliza un nombre de usuario estático, común para todos los usuarios, y porque la contraseña de un solo uso de la primera fase se utiliza como contraseña.

13. Un sistema de acuerdo con la reivindicación 9ª, **caracterizado** porque para la segunda fase se utiliza un nombre de usuario estático, común para todos los usuarios, y porque se utiliza como contraseña un número aleatorio.

14. Un sistema de acuerdo con la reivindicación 9ª, **caracterizado** porque para la segunda fase se utiliza un nombre de usuario dinámico, y porque se utiliza como contraseña un valor aleatorio.

15. Un sistema de acuerdo con cualquiera de las reivindicaciones precedentes, **caracterizado** porque el servidor (4) de páginas está destinado a redirigir el mensaje de identificación de entrada a la página de identificación de entrada del servidor (3) de acceso cuando ha sido creada/modificada una cuenta en el servidor (5) de autentificación, y porque se ajusta un temporizador a un período de tiempo dado durante el cual el servidor (5) de autentificación está destinado a comprobar credenciales de usuario, y si no son válidas, retornar un mensaje de error al usuario.

16. Un sistema de acuerdo con cualquiera de las reivindicaciones precedentes, **caracterizado** porque el servidor (5) de autentificación comprende un servidor Radius o un servidor Diameter.

17. Un sistema de acuerdo con la reivindicación 16ª, **caracterizado** porque están dispuestos uno o más servidores Proxy entre el servidor (3) de acceso y el servidor (5) de autentificación.

18. Un sistema de acuerdo con cualquiera de las reivindicaciones precedentes, **caracterizado** porque la red de acceso comprende una red de área local inalámbrica, una red Ethernet o una red de acceso similar.

19. Un servidor (3) de acceso en una red de acceso cuya finalidad consiste en estar en comunicación con una estación (2) de usuario final para proporcionar acceso a dicha estación de usuario final a una red IP (protocolo Internet), un servidor (4) de páginas y un servidor (5) de autentificación, **caracterizado** porque el servidor (3) de acceso está destinado a utilizar una función de lista en blanco para permitir a cualquier usuario realizar un intento de acceso al servidor (4) de páginas, a través de un enlace de identificación de entrada con el operador de la red IP, y está destinado a soportar el modo de funcionamiento de deambulación en el servidor de autentificación, estando destinado el servidor (3) de acceso a soportar una segunda fase de un procedimiento de identificación de entrada a continuación de una primera fase durante la cual se proporciona una contraseña de un solo uso, con lo cual el servidor (3) de acceso está destinado, en la primera fase y al recibir un mensaje de solicitud de identificación de entrada de la estación (2) de usuario final, a dar una respuesta a la estación (2) de usuario final activando un enlace con el servidor (4) de páginas, para almacenar información de sintaxis del mensaje de solicitud de identificación de entrada, estando destinado adicionalmente el servidor (3) de acceso, en la segunda fase, al recibir un mensaje de identificación de entrada redirigido y para una contraseña de un solo uso verificada con credenciales de usuario para una cuenta provisional y sintaxis de identificación de entrada de la contraseña de un solo uso, a enviar una solicitud de autentificación al servidor (5) de autentificación para verificación de las credenciales de usuario y, al producirse la recepción de un mensaje de aceptación de autentificación, enviar una respuesta a la estación (2) de usuario final y abrir la comunicación.

20. Un servidor de acceso de acuerdo con la reivindicación 19ª, **caracterizado** porque es un servidor (3) de acceso de una red de área local inalámbrica, una red Ethernet o similar, y porque es operado por un Proveedor de Servicios de Internet, por ejemplo un proveedor de servicios de Internet inalámbricos.

21. Un método para proveer a una estación de usuario final de acceso a una red IP (protocolo Internet) a través de una red de acceso que comprende un servidor (3) de acceso, por medio de un procedimiento de acceso/identificación de entrada, **caracterizado** porque el procedimiento de acceso/identificación de entrada comprende una primera fase y una segunda fase, y porque la primera fase comprende las operaciones de: enviar una solicitud de identificación de entrada a un servidor (3) de acceso desde la estación (2) de usuario final, enviar una respuesta desde el servidor (3) de acceso hasta la estación (2) de usuario final activando un enlace con el servidor (4) de páginas que hace las funciones de operador, establecer acceso de usuario final con el servidor de páginas con un mensaje de identificación de entrada que incluye información de sintaxis de identificación de entrada, almacenar la sintaxis de identificación de entrada en el servidor de acceso, introducir la identidad del usuario final en el servidor (4) de páginas al recibirse una solicitud en este sentido, transferir la identidad del usuario final del servidor de páginas al servidor de autentificación, crear una contraseña de un solo uso en el servidor (5) de autentificación, transferir la contraseña de un solo uso a la estación (2) de usuario final a través del sistema (6) de comunicaciones móviles, mediante un mensaje SMS o un mensaje de voz, solicitar del usuario final, mediante el servidor de páginas, la contraseña de un solo uso, y verificar la validez/autenticidad de la contraseña de un solo uso en el servidor (5) de autentificación; y porque la segunda fase comprende las operaciones de: crear una cuenta provisional en el servidor de autentificación y definir credenciales de usuario vinculadas singularmente con la contraseña de un solo uso de la primera fase, redirigir la solicitud de identificación de entrada que comprende la sintaxis de identificación de entrada a la página de identificación de entrada del servidor de acceso, activar un temporizador, enviar una solicitud de autentificación desde el servidor de acceso hasta el servidor de autentificación para comprobar la validez/autenticidad de las credenciales de usuario, y si son válidas, enviar un mensaje de aceptación de acceso al servidor de acceso, activar la solicitud de identificación de entrada de usuario, y eliminar/inhabilitar la cuenta provisional al finalizar el intervalo del temporizador ajustado.

22. Un método de acuerdo con la reivindicación 21ª, **caracterizado** porque comprende las operaciones de: utilizar en la segunda fase el mismo nombre de usuario que en la primera fase, y utilizar la contraseña de un solo uso como contraseña.

23. Un método de acuerdo con cualquiera de las reivindicaciones 21ª o 22ª, **caracterizado** porque comprende las operaciones de: utilizar un nombre de usuario dinámico, y utilizar como contraseña la contraseña de un solo uso de la primera fase.

24. Un método de acuerdo con cualquiera de las reivindicaciones 21ª o 22ª, **caracterizado** porque comprende las operaciones de, en la segunda operación: utilizar un nombre de usuario estático común para todos los usuarios, y utilizar como contraseña la contraseña de un solo uso de la primera fase o un número aleatorio.

25. Un método de acuerdo con la reivindicación 21ª, **caracterizado** porque comprende las operaciones de, en la segunda operación: utilizar un nombre de usuario dinámico, y utilizar como contraseña un valor aleatorio.

26. Un método de acuerdo con cualquiera de las reivindicaciones 21ª a 25ª, **caracterizado** porque la red de acceso comprende una red de área local inalámbrica, una red Ethernet o similar, y porque el servidor de autentificación comprende, por ejemplo, un servidor Radius o un servidor Diameter.

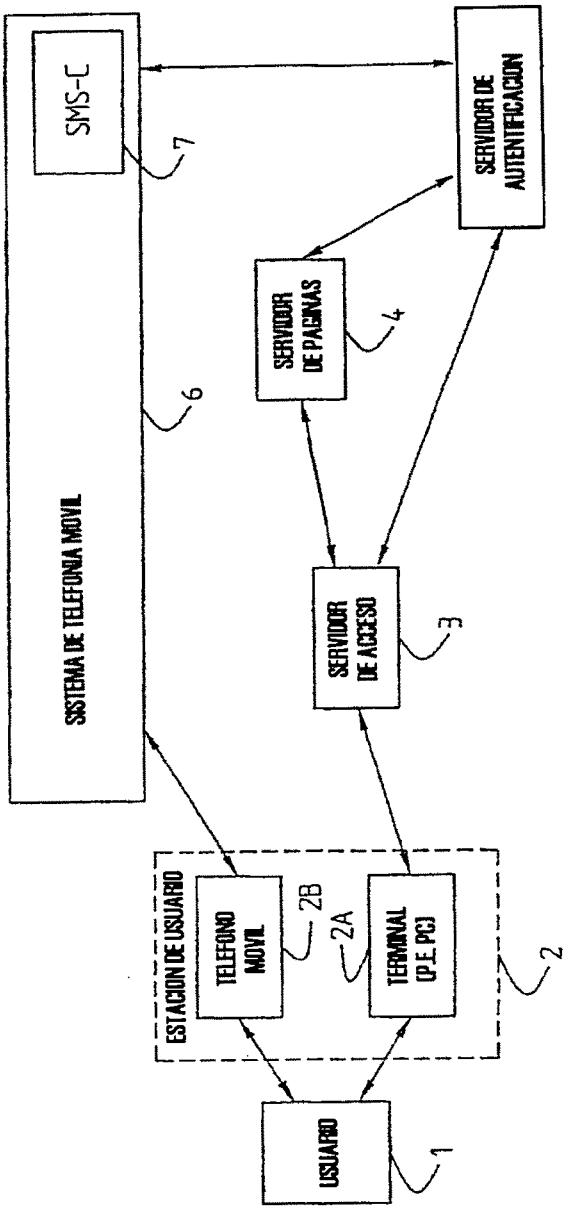

SMS-C
SERVIDOR DE AUTENTIFICACION
SERVIDOR DE PAGINAS
SISTEMA DE TELEFONIA MOVIL
SERVIDOR DE ACCESO
ESTACION DE USUARIO
TELEFONO MOVIL
TERMINAL (P.E. PC)
USUARIO
7
6
4
3
2B
2A
2
1

Fig. 1

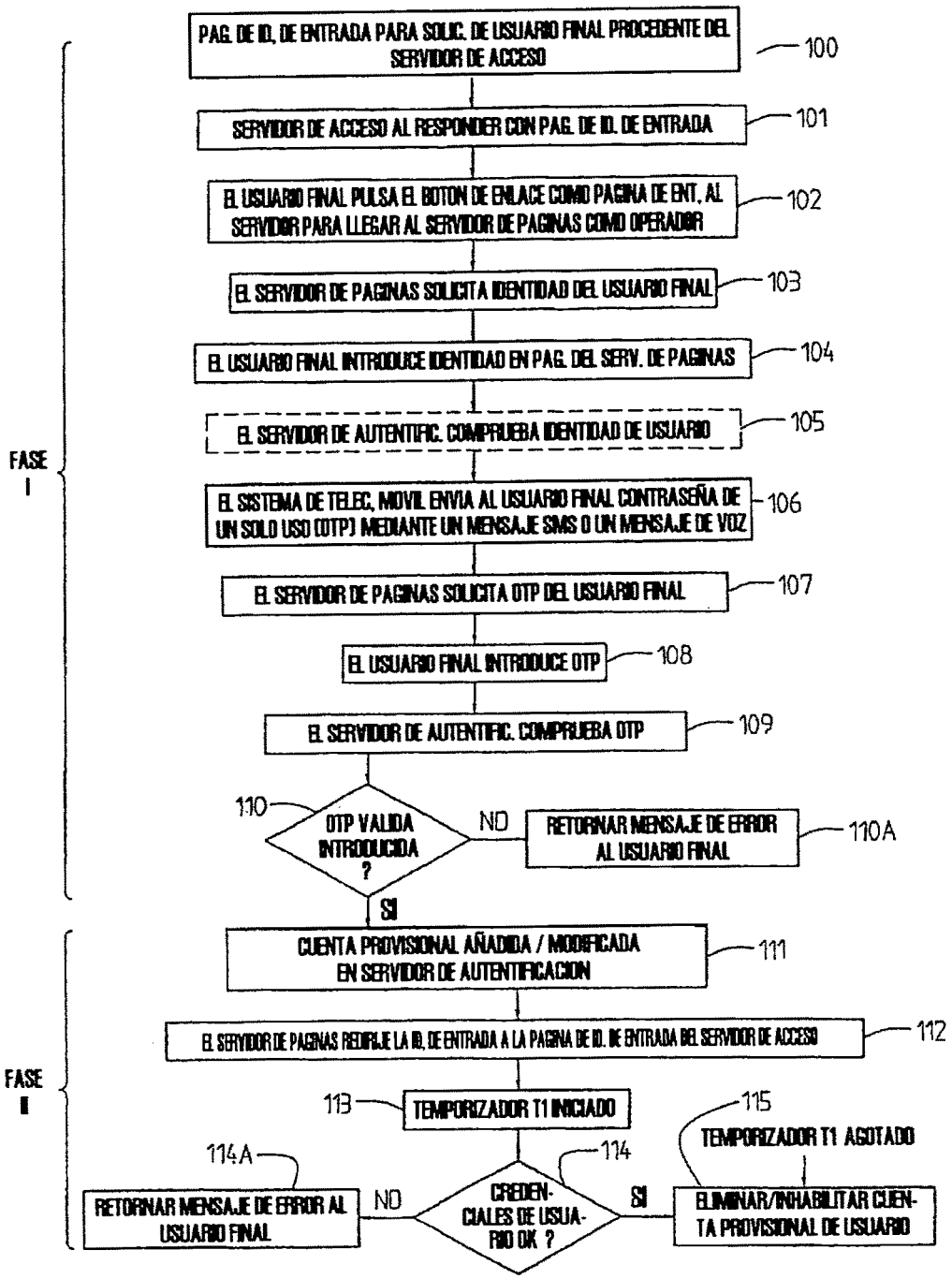

PAG. DE ID. DE ENTRADA PARA SOLIC. DE USUARIO FINAL PROCEDENTE DEL SERVIDOR DE ACCESO
100
SERVIDOR DE ACCESO AL RESPONDER CON PAG. DE ID. DE ENTRADA
101
EL USUARIO FINAL PULSA EL BOTON DE ENLACE COMO PAGINA DE ENT. AL SERVIDOR PARA LLEGAR AL SERVIDOR DE PAGINAS COMO OPERADOR
102
EL SERVIDOR DE PAGINAS SOLICITA IDENTIDAD DEL USUARIO FINAL
103
EL USUARIO FINAL INTRODUCE IDENTIDAD EN PAG. DEL SERV. DE PAGINAS
104
EL SERVIDOR DE AUTENTIFIC. COMPRUEBA IDENTIDAD DE USUARIO
105
EL SISTEMA DE TELEC. MOVIL ENVIA AL USUARIO FINAL CONTRASEÑA DE UN SOLO USO (OTP) MEDIANTE UN MENSAJE SMS O UN MENSAJE DE VOZ
106
EL SERVIDOR DE PAGINAS SOLICITA OTP DEL USUARIO FINAL
107
EL USUARIO FINAL INTRODUCE OTP
108
EL SERVIDOR DE AUTENTIFIC. COMPRUEBA OTP
109
110
OTP VALIDA INTRODUCIDA ?
NO
RETORNAR MENSAJE DE ERROR AL USUARIO FINAL
110A
SI
FASE I
CUENTA PROVISIONAL AÑADIDA / MODIFICADA EN SERVIDOR DE AUTENTIFICACION
111
EL SERVIDOR DE PAGINAS REDIRIJE LA ID. DE ENTRADA A LA PAGINA DE ID. DE ENTRADA DEL SERVIDOR DE ACCESO
112
113
TEMPORIZADOR T1 INICIADO
115
TEMPORIZADOR T1 AGOTADO
114A
114
RETORNAR MENSAJE DE ERROR AL USUARIO FINAL
NO
CREDEN-CIALES DE USUA-RIO OK ?
SI
ELIMINAR/INHABILITAR CUEN-TA PROVISIONAL DE USUARIO
FASE II

Fig. 2

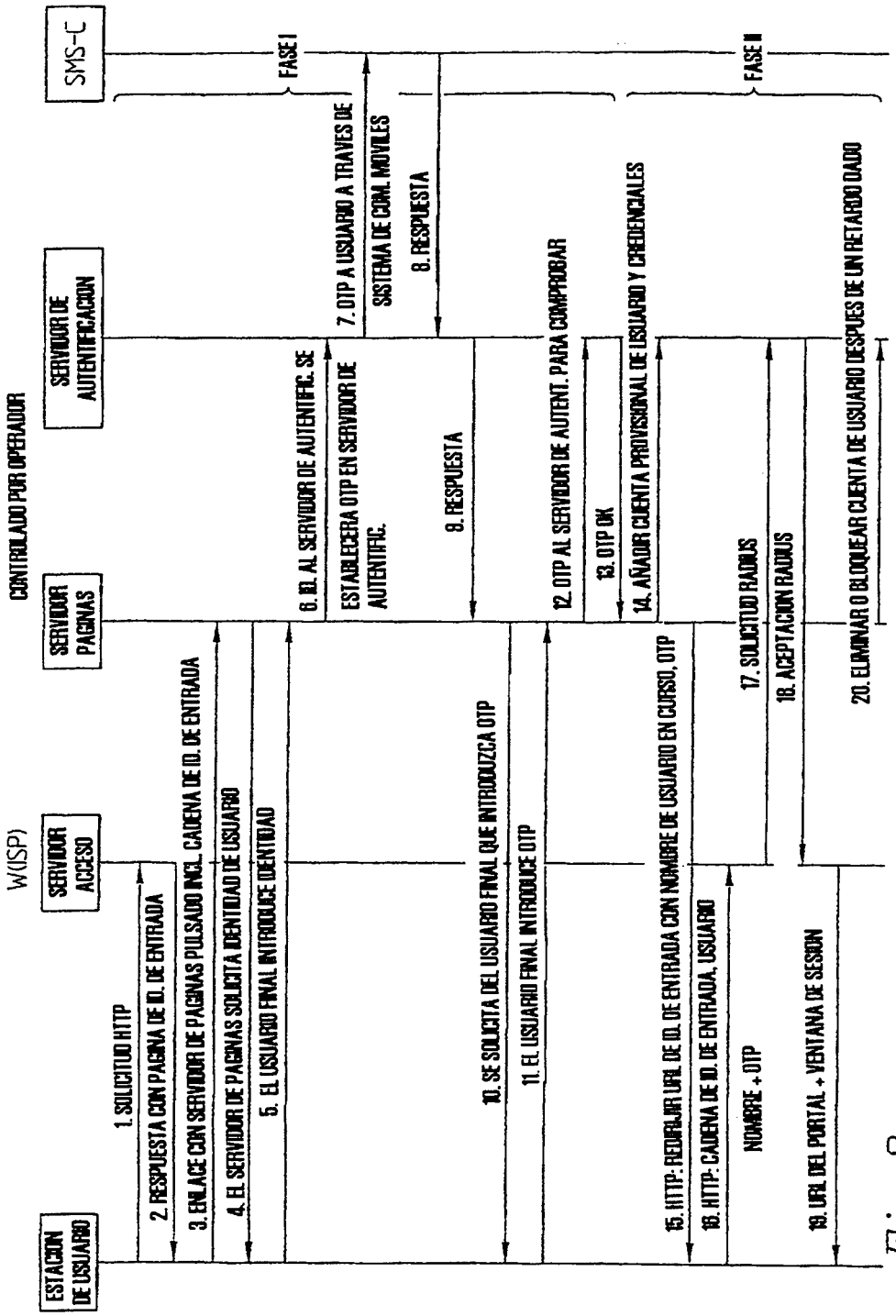

W(ISP)
CONTROLADO POR OPERADOR
ESTACION DE USUARIO
SERVIDOR ACCESO
SERVIDOR PAGINAS
SERVIDOR DE AUTENTIFICACION
SMS-C
FASE I
FASE II
1. SOLICITUD HTTP
2. RESPUESTA CON PAGINA DE ID. DE ENTRADA
3. ENLACE CON SERVIDOR DE PAGINAS PULSADO INCL. CADENA DE ID. DE ENTRADA
4. EL SERVIDOR DE PAGINAS SOLICITA IDENTIDAD DE USUARIO
5. EL USUARIO FINAL INTRODUCE IDENTIDAD
6. ID. AL SERVIDOR DE AUTENTIFIC. SE ESTABLECERA OTP EN SERVIDOR DE AUTENTIFIC.
7. OTP A USUARIO A TRAVES DE SISTEMA DE COM. MOVILES
8. RESPUESTA
8. RESPUESTA
9. SE SOLICITA DEL USUARIO FINAL QUE INTRODUZCA OTP
10. EL USUARIO FINAL INTRODUCE OTP
11. OTP AL SERVIDOR DE AUTENT. PARA COMPROBAR
12. OTP OK
13. AÑADIR CUENTA PROVISIONAL DE USUARIO Y CREDENCIALES
14. HTTP: REDIRIJIR URL DE ID. DE ENTRADA CON NOMBRE DE USUARIO EN CURSO, OTP
15. HTTP: CADENA DE ID. DE ENTRADA, USUARIO
16. NOMBRE + OTP
17. SOLICITUD RADIUS
18. ACEPTACION RADIUS
19. URL DEL PORTAL + VENTANA DE SESION
20. ELIMINAR O BLOQUEAR CUENTA DE USUARIO DESPUES DE UN RETARDO DADO

Fig. 3