(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 560 312**

(51) Int. CI.:

H04M 17/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.10.2000 E 00121574 (8)**

(97) Fecha y número de publicación de la concesión europea: **30.12.2015 EP 1102465**

(54) Título: **Cargo por servicios de telecomunicaciones**

(30) Prioridad:

22.11.1999 FI 992485

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.02.2016

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

SIVULA, TIMO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Cargo por servicios de telecomunicaciones

Los teléfonos móviles más recientemente desarrollados tienen una serie de funciones diferentes que se pueden actualizar mediante información descargada de un operador de red de telecomunicaciones. Las mismas se descargan de la red o son proporcionadas por un operador o algún otro proveedor de servicios. Por ejemplo, las señales de llamada se pueden descargar a un teléfono móvil desde la red móvil. Por ejemplo, un operador de telecomunicaciones finlandés Sonera tiene un servicio, en el que se envía una solicitud de un nuevo tono de llamada desde un teléfono móvil por un mensaje corto (SM) con el apoyo del servicio de mensajes cortos (SMS). El SMS es conocido desde el Sistema Global para Comunicaciones Móviles (GSM). En respuesta a un mensaje corto recibido de un usuario, se proporciona la señal de llamada solicitada al teléfono móvil por un SM. Se realiza un cobro por este servicio en una factura posterior para el uso del teléfono móvil.

Mientras que una red de telecomunicaciones proporciona una manera conveniente para que un proveedor de servicios preste un servicio a un usuario y cobre al usuario por el servicio, un problema surge cuando el proveedor de servicio no es el propio operador de la red de telecomunicaciones. En ese caso, el proveedor de servicios debe tener un acuerdo de cobro con el operador de red de telecomunicaciones para que el cobro se incluya en una factura de teléfono del usuario. Por lo tanto, el proveedor de servicios debe tener un contrato con cada operador de la red de telecomunicaciones que transmite cualquiera de sus servicios. Para un proveedor de servicios que presta servicios a nivel mundial, el número actual de los operadores de redes de telecomunicaciones es demasiado grande para que esto sea razonable. Claramente, dado que hay un periodo de tiempo entre la prestación del servicio y el pago al proveedor de servicios, en efecto, el proveedor de servicios está dando un préstamo a corto plazo al usuario del servicio. Esto implica un riesgo de crédito. Sería conveniente que el pago pudiera ser recibido antes de la prestación del servicio para que el proveedor de servicios reciba el pago de antemano.

Como ejemplo de pagar por adelantado por un servicio, Sonera tiene un acuerdo de suscripción de pago adelantado denominado "Easy" para establecer y mantener una suscripción de teléfono móvil con pago adelantado de llamadas telefónicas y envío de mensajes cortos. Utilizando el servicio permite las operaciones de telefonía móvil ordinarias tales como la realización de llamadas de telefonía móvil y el envío y recepción de mensajes cortos. En esta disposición, un usuario inicialmente compra una tarjeta de módulo de identificación del suscriptor (SIM) con un valor monetario predeterminado que puede utilizarse para realizar llamadas telefónicas y para el envío de SMS. El precio inicial de la tarjeta SIM es de unos 65 dólares. A continuación, el usuario tiene que llamar a un contestador automático de Sonera y proporcionar un número de serie para establecer una cuenta para la tarjeta SIM. La cuenta será acreditada inmediatamente con la suma de 52 USD. La cuenta se debitará cuando se realizan llamadas telefónicas y los mensajes cortos enviados. Por otra parte, cuando el valor restante en la cuenta se aproxima a cero, el usuario puede abonar en la cuenta mediante la compra de un billete que lleva un código de serie de una tienda, llamar a un número de teléfono dedicado, e introducir el código de serie. Cada billete vale 17 USD. Cuando se verifica el código de serie y el valor aceptado relacionado con el billete, que es de 17 USD, se acredita a la cuenta del usuario. En efecto, el arreglo de suscripción es una extensión al propio sistema de facturación de un operador móvil. En lugar de mantener una cuenta de usuario corriente para debitar después, se establece una cuenta de antemano y luego se debita con el uso. Debitar en la cuenta requiere la identificación fiable del usuario de modo que nadie más pueda acceder a la cuenta del usuario. Esto sucede automáticamente en llamadas telefónicas GSM y en el envío de mensajes cortos con el procedimiento de identificación del abonado utilizando la tarjeta SIM. Sin embargo, la identificación del usuario confiable es un requisito previo para este acuerdo de suscripción.

Una forma alternativa de pagar por los servicios de telecomunicaciones prestados por un proveedor de servicios sería el pago mediante tarjeta de crédito. En este caso, el riesgo de crédito recaería entonces en el proveedor de la tarjeta de crédito. Sin embargo, esta disposición se limita a los usuarios que tienen un tipo aprobado de tarjeta de crédito. Además, las tarjetas de crédito no son una manera conveniente de hacer frente a los pagos pequeños, como cinco dólares o menos. Además, algunas personas no quieren proporcionar su información de tarjeta de crédito a través de una red de telecomunicaciones por motivos de seguridad.

Otro método de pago es utilizar el llamado dinero electrónico o e-dinero en forma de datos cargados en una tarjeta inteligente. Si un terminal telefónico tiene un lector de tarjeta inteligente y una aplicación para el envío de e-dinero desde la tarjeta inteligente a un proveedor de servicios mediante un enlace de telecomunicaciones, entonces es posible que pagar por los servicios de telecomunicaciones con una tarjeta inteligente. Sin embargo, tal disposición requiere que se proporcionen las tarjetas inteligentes y lectores de tarjetas inteligentes.

El documento EP 0 921 487 divulga un método y sistema para la facturación de servicios obtenidos a través de la Internet. EP 0 921 487 divulga informar al usuario de la disponibilidad de una pluralidad de diferentes servicios, que recibe desde el usuario una indicación de un servicio deseado y una solicitud para el servicio deseado y proporcionar el servicio solicitado al usuario. En el documento EP 0 921 487 el sistema incluye un terminal, que está equipado con un lector de tarjetas para acceder a una tarjeta de circuito integrado de pago adelantado, un servidor de contenido y un servidor de gestión de tarjetas. El terminal utiliza un navegador web para solicitar un menú de servicio del servidor de contenido. El menú de servicios presenta, por ejemplo, una lista de clips de vídeo o

programas para ser descargados en el terminal. El menú del servicio se devuelve al terminal. Un usuario selecciona un hiperenlace desde el menú y una solicitud de servicio se envía al servidor de contenido. El servidor de contenido contacta con el servidor de gestión de tarjetas con el fin de tener autenticada la tarjeta IC en el terminal y con el fin de tener el servicio facturado. Una tarjeta de identificación se solicita desde el terminal. La tarjeta se autentica con un método de desafío y respuesta que utiliza una función de un solo sentido en una contraseña fija y un número aleatorio que están concatenados. La contraseña se almacena en la tarjeta IC y en el servidor de gestión de tarjetas. Tras la autenticación exitosa, se proporciona al terminal un saldo asociado con la tarjeta y el servicio de contenido con una indicación para iniciar la prestación del servicio al terminal. La cuenta asociada a la tarjeta de identificación se puede depositar a través de una cuenta de vuelta normal o una tarjeta de crédito.

El documento FR 2 747 962 divulga una tarjeta de pago remunerable para servicios de Internet. La tarjeta de pago tiene un número de serie, una tabla de cantidades de divisas, cada una de las cuales tiene asociado un código oculto, y una serie de códigos de control, que pueden ser rayados para verificar la autenticidad de la tarjeta, pero no deben ser rayados por el propietario de la tarjeta. Con el fin de realizar una operación de compra a través de Internet, el comprador debe proporcionar una suma de moneda y el código oculto asociado revelado por el rascado. El documento FR 2 747 962 no divulga que los códigos ocultos serían las claves de autenticación, la validez de las cuales es determinable a partir de los propios códigos utilizando un algoritmo usado para generar los códigos.

Es un objeto de la presente invención evitar o al menos mitigar los problemas descritos anteriormente.

De acuerdo con un primer aspecto de la invención, se proporciona un método para el pago anticipado de contenidos, comprendiendo el método: generar una clave de autenticación; mantener una base de datos de validez de claves de autenticación de claves de autenticación usadas para la verificación de la validez de cualquiera de las claves de autenticación generadas; entregar la clave de autenticación generada a un usuario; informar al usuario de la disponibilidad de una pluralidad de diferentes contenidos; recibir desde el usuario a través de un primer enlace de comunicaciones una indicación de un contenido deseado y una solicitud para el contenido deseado; recibir por parte del usuario de la clave de autenticación generada para indicar el pago adelantado por el contenido solicitado, permitiéndose que dicha clave de autenticación generada sea utilizada una sola vez; verificar si la clave de autenticación generada es válida usando un algoritmo utilizado para la generación de dicha clave de autenticación generada; comprobar que dicha clave de autenticación generada no está contenida en dicha base de datos de claves de autenticación usadas; grabar dicha clave de autenticación generada en dicha base de datos de claves de autenticación usadas; proporcionar el contenido solicitado al usuario por un segundo enlace de comunicaciones, si la clave de autenticación generada es válida y dicha clave no está contenida en dicha base de datos de claves de autenticación usadas; y modificar la base de datos de validez al proporcionar el contenido solicitado de modo que un valor monetario que corresponde a la clave de autenticación generada indicando el pago se reduce de acuerdo con un precio del contenido solicitado por el usuario.

Un método de acuerdo con la invención permite a un proveedor de servicios poner una pluralidad de diferentes servicios a disposición de los usuarios contra un pago anticipado. El usuario puede seleccionar libremente entre los servicios ofrecidos. El pago adelantado permite a cualquier proveedor de servicios prestar los servicios a los usuarios que son suscriptores de una red de telecomunicaciones con independencia de cualquier contrato celebrado entre el proveedor de servicios y el operador de telecomunicaciones.

Ventajosamente, el pago adelantado permite a los clientes que no tienen una tarjeta de crédito acceder a los servicios del proveedor de servicios. Incluso los servicios más baratos pueden estar disponibles. Por lo tanto, se convierte en económicamente razonable para un proveedor de servicios vender servicios que cuestan relativamente poco valor monetario.

La clave de autenticación puede ser necesaria cada vez que se proporciona un servicio o, alternativamente, puede ser necesaria en una primera vez y luego se utiliza para autenticar un cierto número de servicios subsiguientes. En el primer caso no es necesario ningún tipo de identificación de usuario y los servicios pueden ser proporcionados sin ningún procedimiento de identificación de usuario.

Los enlaces de comunicación primero y segundo pueden ser diferentes o el segundo enlace de comunicaciones pueden ser parte de, o una continuación del primer enlace de comunicaciones. Preferentemente, el primer enlace de comunicación se basa en al menos uno de los siguientes: una radiofrecuencia de baja potencia del enlace (LPRF), un enlace de infrarrojos, una red de datos, una red telefónica, una red de comunicaciones móvil, una red de área local y una red de área amplia.

En una realización alternativa, un intento de reutilizar la misma clave de autenticación se detecta mediante el uso de una base de datos. La base de datos puede ser una base de datos que comprende cualquiera de las claves de autenticación no utilizadas o claves de autenticación usadas. De esta manera, es fácil verificar si la clave de autenticación es válida y el servicio solicitado deberá ser proporcionado. En esta realización, el método comprende las siguientes etapas antes de recibir la petición del usuario:

generar la clave de autenticación;

mantener una base de datos de validez de claves de autenticación para verificar la validez de cualquiera de las claves de autenticación generadas; y
entregar la clave de autenticación a un usuario.

Preferentemente, la generación de las claves de autenticación se ajusta a cierto algoritmo(s), por lo que la validez de la clave de autenticación se puede determinar en sí misma. El algoritmo(s) utilizado es / son preferentemente de tal manera que es difícil o imposible determinar cuáles claves de autenticación son válidas. De esta manera, no hay necesidad de mantener una base de datos de claves de autenticación no utilizadas, debido a que la validez de una clave de autenticación se puede determinar mediante la aplicación del algoritmo(s) para verificar la clave de autenticación enviada por el usuario. En este caso, se mantiene una base de datos de todas las claves de autenticación usadas.

Preferentemente, el método comprende la etapa de disponer cada una de las claves de autenticación para indicar un período de tiempo durante el cual es válida; y la etapa de verificación de la validez de la clave de autenticación comprende la etapa de comparar la fecha actual con el período de tiempo durante el cual la clave de autenticación es válida y la etapa de rechazar la clave de autenticación si ha expirado su período de validez. Preferentemente, el procedimiento comprende además la etapa de exploración de la base de datos de claves de autenticación usadas para detectar las claves de autenticación caducadas para sacarlas de la base de datos de claves de autenticación usadas. De esta manera, la base de datos de las claves de autenticación usadas no crece infinitamente y la base de datos es más fácil de mantener.

Preferentemente, el método comprende la etapa de modificar la base de datos de validez al proporcionar el servicio solicitado de modo que el valor monetario que corresponde a la clave de autenticación que indica que el pago se reduce de acuerdo con un precio del servicio solicitado por el usuario. Mediante la modificación de la base de datos de validez al proporcionar el servicio solicitado, el servicio se puede cobrar solo cuando se proporciona con éxito al usuario.

Alternativamente, la modificación puede llevarse a cabo independientemente de si la prestación del servicio se ha completado o no. Entonces no importa si el modificador precede a la real prestación del servicio.

La clave de autenticación se puede proporcionar en la forma de un código impreso en una tarjeta.

Esta tarjeta puede fácilmente ser vendida al usuario. Esto proporciona un método listo para vender la clave de autenticación al usuario, por ejemplo, en una tienda. De esta manera, el proveedor de servicios solo necesita tener un servidor que proporcione el servicio conectado a una red telefónica pública para permitir a los usuarios acceder al servidor para la recuperación de los servicios y no requiere ninguna funcionalidad de recogida de ingresos asociados con el servidor. De esta manera, el proveedor de servicios puede recibir automáticamente los ingresos por venta de tarjetas de lugar de tener que recogerlos por algún otro medio. Normalmente, el proveedor de servicios puede recibir ingresos en función de la parte del precio de venta de las tarjetas. Así, el proveedor de servicios puede utilizar los anticipos para pagar los honorarios de telecomunicaciones en que se incurrirá por la prestación de los servicios. Por lo tanto, en lugar de prestar dinero a los usuarios, el proveedor de servicios puede recibir dinero del usuario antes de la prestación del servicio. Por lo tanto, el proveedor de servicios no tendrá que soportar un riesgo de crédito.

Preferentemente, el método comprende la etapa de ocultar la clave de autenticación con medios de ocultación extraíbles no reversibles. Esto permite al usuario detectar fácilmente si una clave de autenticación ya haya sido divulgada para su uso y por lo tanto se convertirá en sin valor, y también hace que sea posible para el usuario transferir la tarjeta a otro usuario, tal vez para pagos adicionales. Por supuesto, cualquier "nuevo" comprador del servicio también puede verificar que la clave de autenticación no se ha divulgado para su uso. Una vez que se da a conocer la clave de autenticación, el usuario puede suministrarla al proveedor de servicios.

Preferentemente, el método comprende la etapa de proporcionar la tarjeta con más de una clave de autenticación para que el valor nominal pueda ajustarse a una suma conveniente, tal como una sola unidad monetaria, por ejemplo, un dólar. Sin embargo, al menos algunas de las claves de autenticación pueden tener un valor arbitrario, por ejemplo, 0,19 USD.

La etapa de la prestación del servicio puede comprender las etapas adicionales de:

permitir al usuario probar un servicio solicitado; y
recibir una verificación final por parte del usuario para asegurar que el servicio corresponde a las necesidades del usuario.

Estas etapas pueden ocurrir antes de que el servicio se proporcione al usuario y antes de que la base de datos de validez de clave de autenticación se modifique.

Proporcionar una versión de prueba se lleva a cabo preferentemente de una manera que evita que el usuario utilice plenamente el objeto del servicio. Si el servicio es la entrega de señales de llamada, la provisión de una prueba

puede implicar hacer una llamada telefónica al usuario y la reproducción del tono de llamada para el usuario. El usuario puede escuchar el tono de llamada y determinar si cumple con las expectativas del usuario. Preferentemente, con el fin de solicitar la versión de prueba, el usuario puede proporcionar primero una clave de autenticación. El uso de pruebas previsto se puede determinar mediante la introducción de una clave de autenticación que vale menos de la que se requiere para el servicio real. La clave de autenticación utilizada para la prueba puede tener un valor suficiente para cubrir los costes de hacer esta llamada.
Preferentemente, al menos algunos de los servicios están relacionados con el contenido que proporcionan. En este caso, la etapa de informar al usuario de la disponibilidad de una pluralidad de diferentes servicios informa al usuario de la disponibilidad de una pluralidad de diferentes contenidos, y, correspondientemente, la etapa de proporcionar el servicio solicitado proporciona el contenido solicitado. El contenido es la información que se pone a disposición de forma que el usuario puede conseguirla y utilizarla para algún propósito, tales como la mejora de la operación de un terminal móvil o proporcionar entretenimiento o noticias.

De acuerdo con un segundo aspecto de la invención, se proporciona un servidor para el pago adelantado de contenidos, comprendiendo el servidor: medios para generar una clave de autenticación; medios para mantener una base de datos de validez de clave de autenticación de las claves de autenticación usadas para la verificación de la validez de cualquiera de las claves de autenticación generadas; medios para suministrar la clave de autenticación generada a un usuario; medios para informar al usuario de la disponibilidad de una pluralidad de diferentes contenidos; medios para recibir desde el usuario en un primer enlace de comunicaciones una indicación de un contenido deseado y una solicitud para el contenido deseado; medios para recibir del usuario la clave de autenticación generada para indicar el pago adelantado por el contenido solicitado, permitiendo que dicha clave de autenticación generada sea utilizada solo una vez; medios para verificar si la clave de autenticación generada es válida utilizando un algoritmo utilizado para la generación de dicha clave de autenticación generada; medios para la comprobación de que dicha clave de autenticación generada no está contenida en dicha base de datos de claves de autenticación usadas; medios para la grabación de dicha clave de autenticación generada en dicha base de datos de claves de autenticación usadas; y medios para proporcionar el contenido solicitado en un segundo enlace de comunicaciones, si la clave de autenticación generada es válida y dicha clave no está contenida en dicha base de datos de claves de autenticación usadas; y medios para modificar la base de datos de validez al proporcionar el contenido solicitado de modo que un valor monetario que corresponde a la clave de autenticación generada indicando el pago se reduce de acuerdo con un precio del contenido solicitado por el usuario.

De acuerdo con un tercer aspecto de la invención, se proporciona un producto de programa de ordenador para el pago anticipado de contenidos, comprendiendo el producto de programa de ordenador: medios de programa legibles por ordenador para generar una clave de autenticación; medios de programa legibles por ordenador para mantener una base de datos de validez de la clave de autenticación de claves de autenticación usadas para la verificación de la validez de cualquiera de las claves de autenticación generadas; medios de programa legibles por ordenador para suministrar la clave de autenticación generada a un usuario; medios de programa legibles por ordenador para hacer que un ordenador informe al usuario de la disponibilidad de una pluralidad de diferentes contenidos; medios de programa legibles por ordenador para hacer que un ordenador reciba desde el usuario, por un primer enlace de comunicaciones, una indicación de un contenido deseado y una solicitud para el contenido deseado; medios de programa legibles por ordenador para hacer que un ordenador reciba por parte del usuario la clave de autenticación generada para indicar el pago adelantado por el contenido solicitado, permitiendo que dicha clave de autenticación generada sea utilizada solo una vez; medios de programa legibles por ordenador para hacer que un ordenador verifique si la clave de autenticación generada es válida utilizando un algoritmo utilizado para la generación de dicha clave de autenticación generada; medios de programa legibles por ordenador para hacer que un ordenador compruebe que dicha clave de autenticación generada no está contenida en dicha base de datos de claves de autenticación usadas; medios de programa legibles por ordenador para hacer que un ordenador grabe dicha clave de autenticación generada en dicha base de datos de claves de autenticación usadas; medios de programa legibles por ordenador para hacer que un ordenador proporcione al usuario el contenido solicitado en un segundo enlace de comunicaciones, si la clave de autenticación generada es válida y dicha clave no está contenida en dicha base de datos de claves de autenticación usadas; y medios de programa legibles por ordenador para la modificación de la base de datos de validez al proporcionar el contenido solicitado de modo que un valor monetario que corresponde a la clave de autenticación generada indicando el pago se reduce de acuerdo con un precio del contenido solicitado por el usuario.

Ventajosamente, el producto de programa de ordenador puede convertir a un servidor conectado a una red de telecomunicaciones como Internet en un servicio de pago adelantado capaz de manejar las acciones relacionadas con el pago por adelantado de un servicio o de una pluralidad de servicios.

La presente invención se puede utilizar en un teléfono o terminal móvil de datos, así como en un teléfono o terminal de datos por cable, generalmente un dispositivo que puede ser conectado a una red de comunicaciones para utilizar un servicio de telecomunicaciones.

La invención se describirá ahora, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en los cuales:

La figura 1 muestra un diagrama de flujo de un método para el pago anticipado de un servicio de

telecomunicaciones;

La figura 2 muestra etapas adicionales para el método en la figura 1;

La figura 3 muestra un teléfono móvil utilizando el método de la figura 1 o el método de las figuras 1 y 2;

La figura 4 muestra una tarjeta de clave de autenticación de pago adelantado para el pago de los servicios de telecomunicaciones; y

La figura 5 muestra un diagrama de bloques de un sistema de pago adelantado.

La figura 1 muestra un diagrama de flujo de un método para el pago anticipado de un servicio de telecomunicaciones. El método que se muestra en la figura 1 comienza desde la etapa 11, que puede ser un estado normal o de reposo de un sistema en el que el sistema está realizando procesos. Estos procesos pueden no estar relacionados con la operación de la invención. Después de la etapa 11 sigue la etapa 12, en la que se mantiene una base de datos de validez de autenticación que comprende claves de autenticación y sus respectivos valores. Las claves de autenticación son certificados que prueban el pago anticipado de un servicio como se explicará más adelante con más detalle. Un ordenador conectado a la base de datos de validez de clave de autenticación genera las claves de autenticación. El mantenimiento de la base de datos de validez de clave de autenticación implica recibir y / o generación de nuevas claves de autenticación y el registro de las mismas de modo que correspondan a sus respectivos valores monetarios. Se trata además de invalidar las claves de autenticación cuando se utilizan de modo que cada clave de autenticación en particular solo puede ser usada una vez. Esta nulidad se puede disponer para que tenga lugar antes o después de que un servicio se ofrece al usuario.

Una vez que una base de datos de validez de clave de autenticación adecuada se ha configurado, una clave de autenticación se entrega a un usuario del servicio. Esto se muestra en la etapa 13. Las claves de autenticación se imprimen en tarjetas mostradas en la figura 4. Las claves de autenticación son secuencias de números de modo que son fáciles de escribir.

Una vez que el usuario tiene una clave de autenticación, la clave de autenticación puede ser utilizada para obtener un servicio que cuesta una cantidad económica como máximo igual al valor de la clave de autenticación. Supongamos que el usuario desea solicitar un nuevo tono de llamada para su teléfono móvil desde un proveedor de servicios. Una lista de los servicios puede ser presentada en una página WWW (World Wide Web) de un servidor del proveedor de servicios. Un usuario puede acceder al servidor con un ordenador personal que puede estar conectado a Internet. Cada elemento de la lista (por ejemplo, cada nombre de tono de llamada) puede estar asociado con un hipervínculo para que al seleccionar el nombre de la señal de llamada, el usuario pueda solicitar la señal de llamada desde el servidor. Un mensaje de petición se envía entonces al servidor en un mensaje de petición de servicio que también comprende un identificador de la señal de llamada. En respuesta a tal mensaje de solicitud de servicio, un servidor solicita una clave de autenticación del usuario, como se muestra en la etapa 14. El usuario lee la clave de autenticación y entra en el servidor para pagar por el servicio. La validez de la clave de autenticación se verifica en la etapa 15. En respuesta a una entrada exitosa de una clave de autenticación válida, el número de teléfono del usuario se solicita al usuario. El servicio solicitado se proporciona a continuación al usuario en la etapa 16 mediante el envío de la señal de llamada solicitada como un mensaje corto al número de teléfono móvil del usuario. Si la clave de autenticación no es válida, se solicita de nuevo la clave de autenticación en la etapa 14. Cuando el servicio solicitado, un tono de llamada en este caso, se proporciona al usuario, la clave de autenticación propuesta por el usuario se invalida en la etapa 17 para que no pueda ser utilizada de nuevo.

La invalidación implica el cambio de la base de datos de validación de la clave de autenticación de manera que muestre que la clave de autenticación ya ha sido utilizada cuando se recibe desde el usuario. Las claves de autentificación no utilizadas se mantienen en una base de datos de modo que la presencia de una clave de autenticación en la base de datos demuestra que la clave de autenticación está sin utilizar y es válida. En otra realización, las claves de autenticación usadas se mantienen en la base de datos de validez de la clave de autenticación de modo que la presencia de la clave de autenticación en la base de datos muestra que la clave de autenticación está utilizada y no es válida. Un nuevo control se puede realizar para comprobar si una clave de autenticación ha caducado y ya no es válida por ser demasiado vieja, por ejemplo, de más de 12 meses.

En una realización alternativa, un teléfono móvil se utiliza para obtener una lista de los servicios que ofrece el proveedor de servicios. En este caso, el usuario envía un mensaje corto al servidor y recibe un mensaje corto de respuesta que transporta una lista de los servicios. La lista puede entonces ser mostrada a un usuario en una pantalla del teléfono móvil. El usuario puede solicitar la señal de llamada del proveedor de servicios, por ejemplo, mediante el envío de un mensaje de solicitud mediante el servicio de mensajes cortos conocido de GSM. Por supuesto, otros métodos de petición pueden ser utilizados, tales como enviar un fax o un mensaje de correo electrónico. En estos casos, es ventajoso incluir la clave de autenticación en el mensaje de modo que no se solicita la clave de autenticación del usuario. En este caso, el usuario debe incluir su número de teléfono móvil en el mensaje para que el servidor sepa dónde enviar la señal de llamada, si la clave de autenticación es válida. Si el mensaje es un mensaje corto, entonces el número de teléfono puede ser incluido automáticamente como un identificador del remitente del mensaje corto.

En el caso más simple y directo cada clave de autenticación otorga al usuario tener un servicio proporcionado una vez. En una realización alternativa, la misma clave de autenticación puede ser utilizada para pagar más de una

transacción. En este caso, el valor asociado a la clave de autenticación en la base de datos se reduce en una cuota del servicio. Una cuenta se da entonces al usuario y el valor restante de la clave de autenticación se mantiene en la cuenta de modo que el usuario puede comprobar el valor restante identificándose a sí mismo. Esta identificación se puede automatizar utilizando la tecnología de cookies conocida desde los navegadores WWW actuales en caso de solicitud basada en WWW o usando el identificador de remitente de mensajes cortos en el caso de una solicitud originada en la telefonía móvil. Con esta automatización el usuario simplemente puede ponerse en contacto con el proveedor de servicios de nuevo y utilizar los servicios con el valor restante sin tener que introducir ningún código de identificación.

La figura 2 muestra una adición al método mostrado en la figura 1. La adición comprende dos etapas, la etapa 22 y la etapa 23. En esta realización, si la clave de autenticación se verifica como válida, el método pasa a la etapa 22 después de la etapa 15. En la etapa 22 se ofrece una versión de prueba de un servicio al usuario y en la etapa 23 se realiza una comprobación para ver si el usuario en efecto, solicita el servicio. Si el usuario ordena el servicio, el método prosigue a la etapa 16. Si el usuario no ordena el servicio, el método pasa a la etapa 17 o 11, dependiendo de la forma de realización. Si no se requiere el pago de la prueba, entonces la etapa 11 será la próxima, si no en la etapa 17 una clave de autenticación utilizada para tener la versión de prueba se invalida.

La figura 3 muestra un MS de telefonía móvil adecuado para su uso con los métodos de la figura 1, o las figuras 1 y 2. El teléfono móvil MS comprende una antena 32, un bloque de radio 34, una interfaz de usuario 35, un medio de procesamiento 36 y un programa 38. La antena está conectada al bloque de radio, que a su vez está conectado a los medios de procesamiento. Los medios de procesamiento comprenden un microprocesador para ejecutar instrucciones y una memoria para el mantenimiento de las instrucciones. Los medios de procesamiento comprenden, además, el programa 38 que se utiliza para controlar el teléfono móvil MS. La interfaz de usuario 35 comprende unos medios de entrada y salida, que tienen una o más claves de autenticación, una pantalla, un altavoz y un micrófono. El teléfono móvil MS está dispuesto para recibir una señal de llamada de una emisora de radio y utilizar ese tono de llamada para alertar a su usuario de una llamada telefónica entrante. El teléfono también permite al usuario enviar la solicitud de una señal de llamada mediante el uso de su interfaz de usuario y el bloque de radio 34.

La figura 4 muestra una tarjeta de clave de autenticación de pago adelantado 40 para el pago de los servicios de telecomunicaciones. La tarjeta de clave de autenticación 40 comprende cinco claves de autenticación 42, 44, 44, 46 y 48. Junto a cada clave de autenticación se imprime un valor correspondiente. Las claves de autenticación (44, 46, y 48) están cubiertas inicialmente con una capa opaca de un material fácil de eliminar, por ejemplo, cera o laca blanda. Así, las claves de autentificación no son legibles hasta que el usuario las descubre, por ejemplo por el rascado de la capa opaca. Por lo tanto, en la compra de la tarjeta, el usuario puede verificar fácilmente que la tarjeta no se ha utilizado y que todas las claves de autenticación son válidas. Cuando se retira la capa de material, la clave de autenticación por debajo de ella se hace visible para el usuario. Por lo tanto la cobertura de una clave de autenticación demuestra la validez de la clave de autenticación. En este ejemplo las claves de autenticación 42 a 44 corresponden a un valor de 20 centavos de dólar, mientras que las claves de autenticación 46 y 48 corresponden a 10 y 29 centavos de dólar. Así, el precio total (49) 0,99 USD de la tarjeta está impreso en la tarjeta de modo que el usuario puede verlo inmediatamente, por ejemplo, cuando se compra en una tienda.

La figura 5 muestra un diagrama de bloques de un sistema de pago adelantado de acuerdo con una realización de la invención. El sistema comprende un servidor pago adelantado 50, un bloque de control de servicio 52, una base de datos de validez de clave de autenticación 53 y un bloque de generación de claves de autenticación 54 en el servidor. El servidor de pago adelantado 50 es un equipo servidor ordinario unido a la Internet y que comprende el software que hace que se aplique el método de pago adelantado como se ha descrito antes. El sistema comprende además una impresora de tarjetas 56, una red de telecomunicaciones 58, y una pluralidad de dispositivos de usuario MS. El servidor pago adelantado genera las claves de autenticación, controla la impresión de las claves de autenticación y controla el pago de los servicios. La red retransmite el tráfico de datos entre el servidor y los dispositivos de usuario MS. El bloque de generación produce las claves de autentificación y los envía tanto a la impresora para la impresión como al bloque de control de servicio 52. La impresora imprime conjuntos de claves de autentificación en tarjetas (como se muestra en la figura 4). El bloque de control de servicio mantiene la base de datos 53 de claves de autenticación y almacena las claves de autenticación y sus respectivos valores en la base de datos 53. Cuando la tarjeta se entrega a un usuario, él o ella puede ponerse en contacto con el proveedor de servicio y solicitar un servicio. En respuesta a esta solicitud, el proveedor de servicios comprueba el pago adelantado del servicio con el bloque de control de servicio 52 del servidor de pago adelantado. El usuario envía la clave de autenticación por red al bloque de control de servicio del servidor de pago adelantado, que verifica la validez de la clave de autenticación y si el valor asociado a la clave de autenticación es suficiente para el precio del servicio solicitado. Si la clave de autenticación es válida y corresponde a un valor monetario al menos igual al precio, entonces el servidor permite la entrega del servicio solicitado y reduce el valor monetario que corresponde a la clave de autenticación que se utilizó. El servidor de pago adelantado puede proporcionar, además, el servicio solicitado. En este caso el servidor 50 proporciona el servicio en la red 58 al dispositivo de usuario MS del usuario.

En una realización preferida, se proporciona además un segundo servidor para proporcionar una lista de servicios al usuario y para recibir la entrada del usuario, tales como la selección de servicio y la clave de autenticación. En este

caso, el segundo servidor puede residir en cualquier lugar, siempre que la información puede ser intercambiada entre el segundo servidor y el servidor de pago adelantado. Ambos servidores están conectados a la Internet para que ninguna red de los operadores de telefonía móvil estuviera involucrada en casos distintos de la prestación de un servicio a través de una red de telecomunicaciones móviles. Usando el ejemplo de señal de llamada, el segundo servidor que reside en Internet puede recibir una solicitud de un tono específico de llamada de un usuario que tiene un acceso a Internet y tener un teléfono móvil que pueda recibir una señal de llamada de una red de telecomunicaciones móviles. En respuesta a la solicitud, se pide una clave de autenticación de pago adelantado y el número de teléfono móvil del usuario y se verifica la clave de autenticación, y si es aceptada, la señal de llamada específica se envía al teléfono móvil como mensaje (por ejemplo, un mensaje corto). El envío de la señal de llamada en la red de telecomunicaciones móviles implica el uso de los servicios de una red de telecomunicaciones, pero al menos muchos operadores de telefonía GSM permiten el reenvío de mensajes cortos originados en el extranjero a los teléfonos móviles que residen en sus redes. Las señales de llamada y otros servicios suplementarios tales que proporcionan contenido eléctrico a un teléfono móvil por lo tanto pueden ser enviados prácticamente de todo el mundo. Otros ejemplos de proporcionar contenido eléctrico disponible en las telecomunicaciones móviles incluyen imágenes que se utilizarán en mensajes de imagen, imágenes de grupo de llamada y logotipos del operador. También es posible proporcionar canciones de música o videoclips. Se espera que las futuras estaciones móviles de tercera generación tengan una funcionalidad multimedia que permita el uso de este tipo de información.

En lo anterior, un servicio significa cualquier servicio que puede ser proporcionado a través de un canal de comunicación, por ejemplo, la entrega de una señal de llamada o una tarjeta de felicitación eléctrica, una grabación musical o vídeo de una compañía discográfica, una donación a la caridad, el pago de la cuota de aparcamiento o una tarifa de transporte público, para lo cual la información es simplemente enviada a un servidor, y nada es necesariamente recibido. Así, el servicio puede ser una transferencia de información en cualquier dirección, como por ejemplo a un usuario, de un usuario, o en ambas direcciones.

Tarjetas de claves de autenticación baratas se pueden comprar con poco dinero. Así, el servicio es fácil de pagar, lo que es probable que promocione la venta de nuevos tonos de timbre, imágenes y otros servicios comerciales como estos.

En este trabajo se presenta la implementación y realizaciones de la invención con la ayuda de ejemplos. Es obvio para una persona experta en la técnica que la invención no se limita a los detalles de las realizaciones presentadas anteriormente, y que la invención se puede implementar en otra forma de realización sin desviarse de las características de la invención. Por lo tanto, las realizaciones presentadas deben considerarse ilustrativas, pero no restrictivas. Hay numerosas maneras de variar dentro del alcance de la invención como se ilustra a continuación.

El ocultamiento de la clave de autenticación puede disponerse mediante la impresión de la clave en un papel, plegarlo y cerrarlo de forma sellada para que el código no sea visible hasta que se abra el billete.

Una clave de autenticación impresa puede ser una secuencia de caracteres. Puede haber solo una única clave de autenticación en una tarjeta.

La clave de autenticación puede ser impresa en la tarjeta como un código de barras, o la clave de autenticación puede estar unida como algún otro código de lectura mecánica. El código legible por la máquina puede ser una forma especial de una tarjeta o una banda magnética. El código legible por máquina puede ser leído por una máquina tal como un lector de un terminal de ordenador o teléfono equipado con un lector de este tipo.

El envío de la solicitud puede ser enviar la clave de autenticación a una página de la World Wide Web en el servidor o el envío de un correo electrónico o mensaje corto o un datagrama de cualquier otra forma. Tanto la solicitud y el servicio pueden ser enviados en mensajes cortos. De esta manera, un centro de mensajes cortos de una red de telecomunicaciones móvil puede amortiguar los mensajes si la parte receptora no puede recibir mensajes cortos temporalmente.

La clave de autenticación puede ser enviada directamente al usuario a través de un enlace de comunicaciones, si el usuario paga directamente al proveedor de servicios.

Las etapas 16 y 17 pueden estar en cualquier orden, aunque es conveniente comprobar, por ejemplo, de forma automática, si el servicio de hecho se puede proporcionar al usuario si se presta el servicio antes de invalidar la clave de autenticación o cambiar el valor correspondiente de la misma. Esto se puede aplicar en una situación en la que el dispositivo del usuario está para recibir una señal de llamada pero no recibe completamente por ejemplo si el terminal móvil se queda sin energía.

La etapa 22 puede comprender el envío de la versión de prueba del servicio a través de Internet o hacer una llamada telefónica al usuario y ejecutar de forma audible la señal de llamada al usuario de manera que el usuario puede escuchar el tono y decidir si es un timbre de llamada que el usuario desea tener. Si es así, el usuario puede pagar por el servicio completo, por ejemplo al dar otra clave de autenticación correspondiente al precio del servicio. La prueba puede tener un precio más bajo que solo puede cubrir los costos de proveer al usuario con la versión de

prueba. Alternativamente, la prueba puede ser gratuita.

En lugar de imprimir las tarjetas cerca del servidor, se puede proporcionar un conjunto de impresoras distribuidas en los puntos de entrega (por ejemplo, tiendas) para mejorar la logística de las tarjetas que contienen las claves de autenticación.

En otra realización alternativa, el operador de telecomunicaciones entrega las claves de autenticación en respuesta al uso de un servicio de telecomunicaciones de calidad superior (llamada de calidad superior o mensajes cortos). El usuario paga por un servicio mediante el servicio de calidad superior produciendo ingresos para el operador de telecomunicaciones. El operador de telecomunicaciones comparte los ingresos con el proveedor de servicios. A cambio del pago, el usuario es provisto de una o más claves de autenticación. En este caso, la clave(s) de autenticación puede ser transmitida eléctricamente al usuario. La ventaja de la forma de realización es que ninguna tarjeta existente físicamente necesita tiene que ser enviada al usuario.

Por lo tanto, las posibilidades de implementar y usar la invención solo están limitadas por las reivindicaciones adjuntas. En consecuencia, las diversas opciones de implementación de la invención según lo determinado por las reivindicaciones, incluyendo las implementaciones equivalentes, también pertenecen al alcance de la presente invención.

REIVINDICACIONES

1. Método para el pago anticipado de contenidos, que comprende las etapas de:

generar una clave de autenticación;
mantener una base de datos de autenticación de la validez de clave de las claves de autenticación usadas para verificar la validez de cualquiera de las claves de autenticación generadas;
entregar la clave de autenticación generada a un usuario;
informar al usuario de la disponibilidad de una pluralidad de diferentes contenidos;
recibir (14) desde el usuario, por un primer enlace de comunicaciones, una indicación de un contenido deseado y una solicitud para el contenido deseado;
recibir por parte del usuario la clave de autenticación generada para indicar el pago adelantado por el contenido solicitado, permitiéndose que dicha clave de autenticación generada sea utilizada una sola vez;
verificar (15) si la clave de autenticación generada es válida usando un algoritmo utilizado para la generación de dicha clave de autenticación generada;
comprobar que dicha clave de autenticación generada (42) no está contenida en dicha base de datos de claves de autenticación usadas;
grabar (17) dicha clave de autenticación generada en dicha base de datos de claves de autenticación usadas;
proporcionar (16) el contenido solicitado al usuario por un segundo enlace de comunicaciones, si la clave de autenticación generada es válida y dicha llave no está contenida en dicha base de datos de claves de autenticación usadas; y
modificar la base de datos de validez al proporcionar el contenido solicitado de modo que un valor monetario que corresponde a la clave de autenticación generada indicando el pago se reduce de acuerdo con un precio del contenido solicitado por el usuario.

2. El método según la reivindicación 1, **caracterizado por que** se requiere una clave de autenticación cada vez que se proporciona un servicio.

3. El método según la reivindicación 1 o la reivindicación 2, **caracterizado por que** el método comprende además:

la etapa de disponer cada una de las claves de autenticación generadas para indicar un período de tiempo durante el cual son válidas;
la etapa de verificación de la validez de la clave de autenticación generada comprende la etapa de comparar la fecha actual con el período de tiempo durante el cual la clave de autenticación generada es válida; y
la etapa de rechazar las claves de autenticación caducadas.

4. El método según la reivindicación 3, **caracterizado por que** el método comprende además:

la etapa de exploración de la base de datos de las claves de autenticación usadas para detectar las claves de autenticación caducadas para sacarlas de la base de datos de claves de autenticación usadas.

5. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** la clave de autenticación generada es un código impreso legible por usuario.

6. El método según cualquiera de las reivindicaciones anteriores, **caracterizado por que** el método comprende además la etapa de ocultar la clave de autenticación generada con medios de ocultación extraíbles no reversibles.

7. El método según las reivindicaciones 5 y 6, **caracterizado por que** el método comprende además la impresión en una tarjeta de un grupo de claves de autenticación generadas.

8. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** la primera conexión de comunicación se basa en al menos una de las siguientes: una red de datos, una red telefónica, una red de telecomunicaciones móvil, una red de área local y una red de área amplia.

9. El método de acuerdo con cualquiera de las reivindicaciones anteriores, **caracterizado por que** el método comprende además las etapas de:

permitir al usuario probar un contenido solicitado; y
recibir una verificación final por parte del usuario antes de que se le proporcione al usuario el contenido.

10. Servidor (50) para el pago adelantado de contenidos, comprendiendo el servidor:

medios para generar una clave de autenticación;
medios para mantener una base de datos de validez de la clave de autenticación de claves de autenticación usadas para la verificación de la validez de cualquiera de las claves de autenticación generadas;
medios para suministrar a un usuario la clave de autenticación generada;

medios para informar al usuario de la disponibilidad de una pluralidad de diferentes contenidos;
medios para recibir (52) desde el usuario, por un primer enlace de comunicaciones, una indicación de un contenido deseado y una solicitud para el contenido deseado;
medios para recibir del usuario la clave de autenticación generada para indicar el pago adelantado por el contenido solicitado, permitiéndose que dicha clave de autenticación generada sea utilizada solo una vez;
medios para comprobar (15) si la clave de autenticación generada es válida utilizando un algoritmo usado para la generación de dicha clave de autenticación generada;
medios para la comprobación de que dicha clave de autenticación generada (42) no está contenida en dicha base de datos de claves de autenticación usadas;
medios para la grabación (17) de dicha clave de autenticación generada en dicha base de datos de claves de autenticación usadas; y
medios para proporcionar (16) el contenido solicitado por un segundo enlace de comunicaciones, si la clave de autenticación generada es válida y dicha clave no está contenida en dicha base de datos de claves de autenticación usadas; y
medios para modificar la base de datos de validez al proporcionar el contenido solicitado de modo que un valor monetario que corresponde a la clave de autenticación generada indicando el pago se reduce de acuerdo con un precio del contenido solicitado por el usuario.

11. Producto de programa informático para el pago adelantado de contenidos, comprendiendo el producto de programa de ordenador:

medios de programa legibles por ordenador para generar una clave de autenticación;
medios de programa legibles por ordenador para mantener una base de datos de validez de clave de autenticación de las claves de autenticación usadas para la verificación de la validez de cualquiera de las claves de autenticación generadas;
medios de programa legibles por ordenador para suministrar la clave de autenticación generada a un usuario;
medios de programa legibles por ordenador para hacer que un ordenador informe al usuario de la disponibilidad de una pluralidad de diferentes contenidos;
medios de programa legibles por ordenador para hacer que un ordenador reciba (52) desde el usuario, por un primer enlace de comunicaciones, una indicación de un contenido deseado y una solicitud para el contenido deseado; y
medios de programa legibles por ordenador para hacer que un ordenador reciba por parte del usuario la clave de autenticación generada para indicar el pago adelantado para el contenido solicitado, permitiendo que dicha clave de autenticación generada sea utilizada solo una vez;
medios de programa legibles por ordenador para hacer que un ordenador verifique (15) si la clave de autenticación generada es válida utilizando un algoritmo utilizado para la generación de dicha clave de autenticación generada;
medios de programa legibles por ordenador para hacer que un ordenador compruebe que dicha clave de autenticación generada (42) no está contenida en dicha base de datos de claves de autenticación usadas;
medios de programa legibles por ordenador para hacer que un ordenador grabe (17) dicha clave de autenticación generada en dicha base de datos de claves de autenticación usadas;
medios de programa legibles por ordenador para hacer que un ordenador proporcione (16) al usuario el contenido solicitado por un segundo enlace de comunicaciones, si la clave de autenticación generada es válida y dicha clave no está contenida en dicha base de datos de claves de autenticación usadas; y
medios de programa legibles por ordenador para modificar la base de datos de validez al proporcionar el contenido solicitado de modo que un valor monetario que corresponde a la clave de autenticación generada indicando el pago se reduce de acuerdo con un precio del contenido solicitado por el usuario.

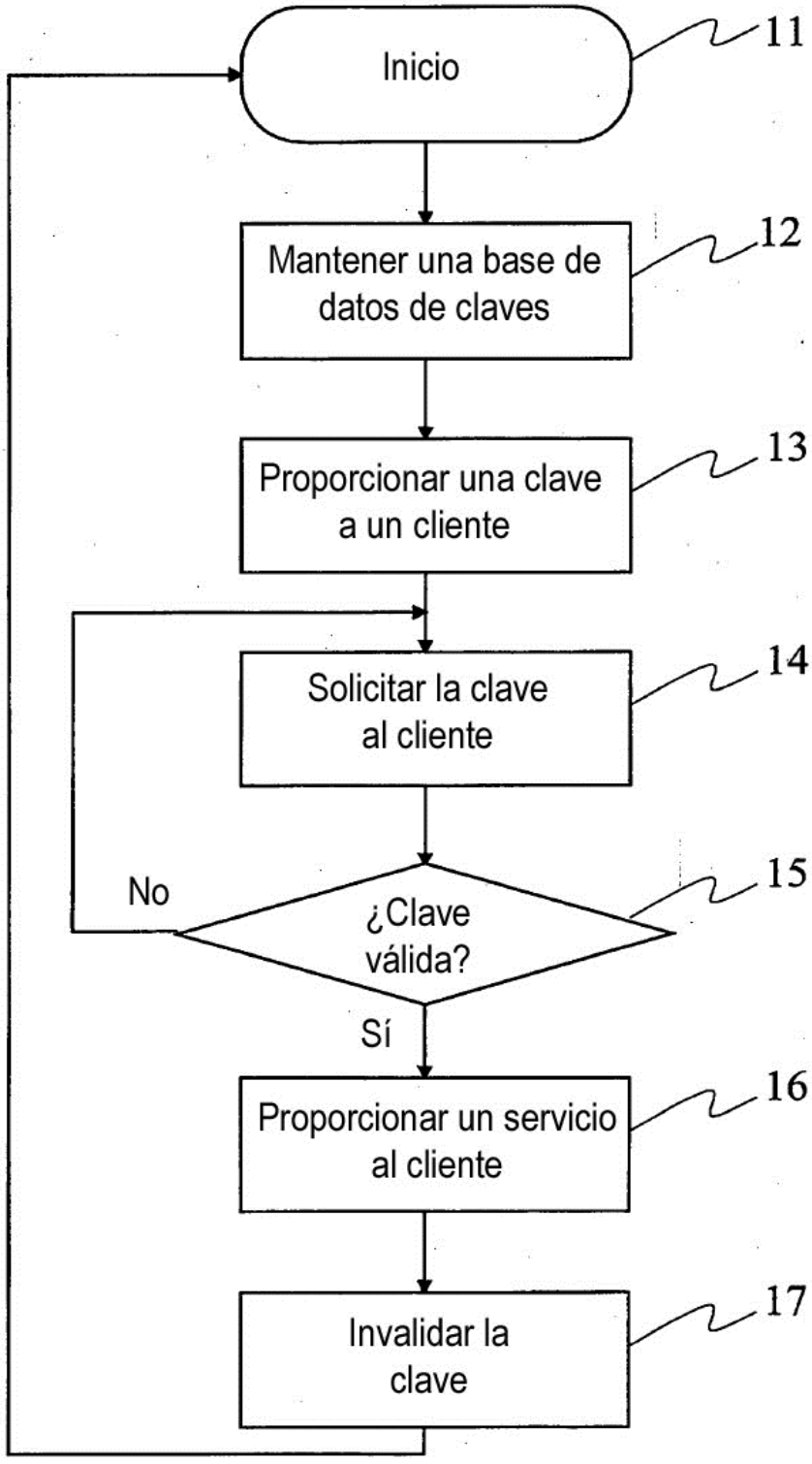
Inicio
11
Mantener una base de datos de claves
12
Proporcionar una clave a un cliente
13
Solicitar la clave al cliente
14
No
¿Clave válida?
15
Sí
Proporcionar un servicio al cliente
16
Invalidar la clave
17

Fig. 1

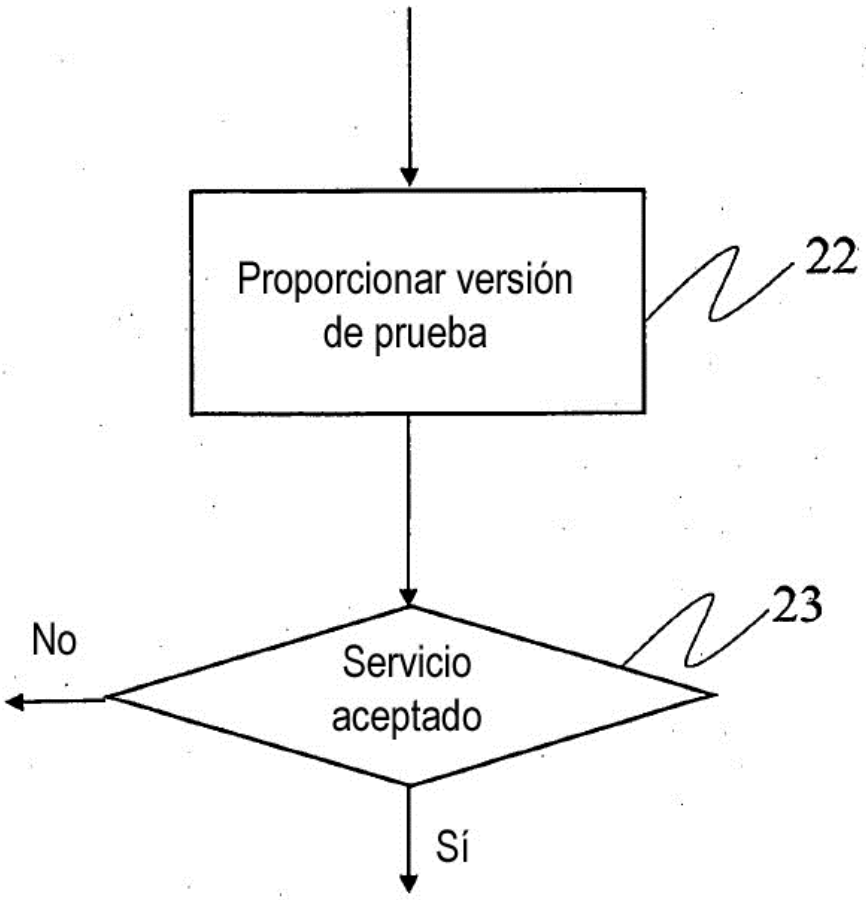
Proporcionar versión de prueba
22
Servicio aceptado
23
No
Sí

Fig. 2

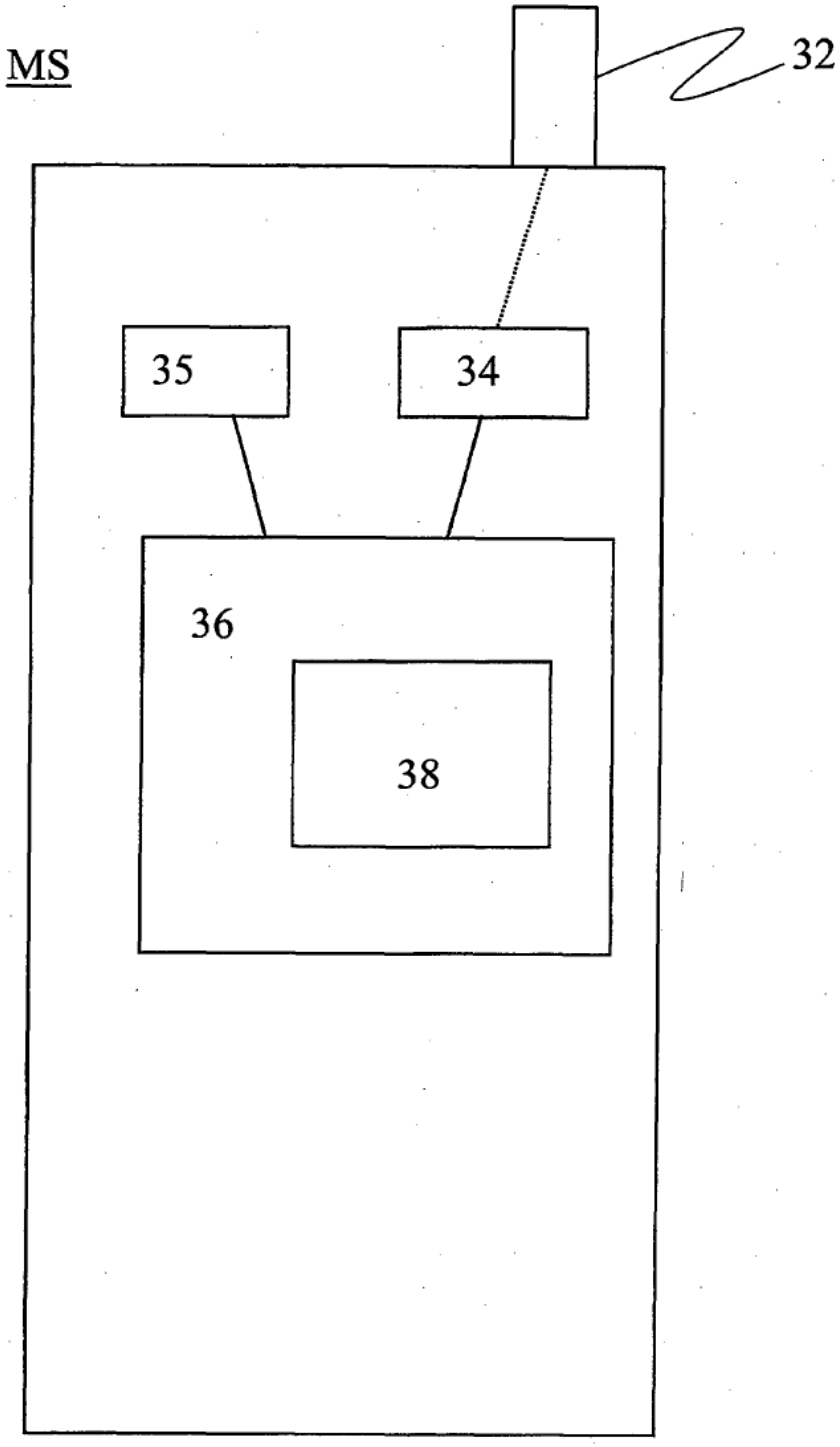

Fig. 3

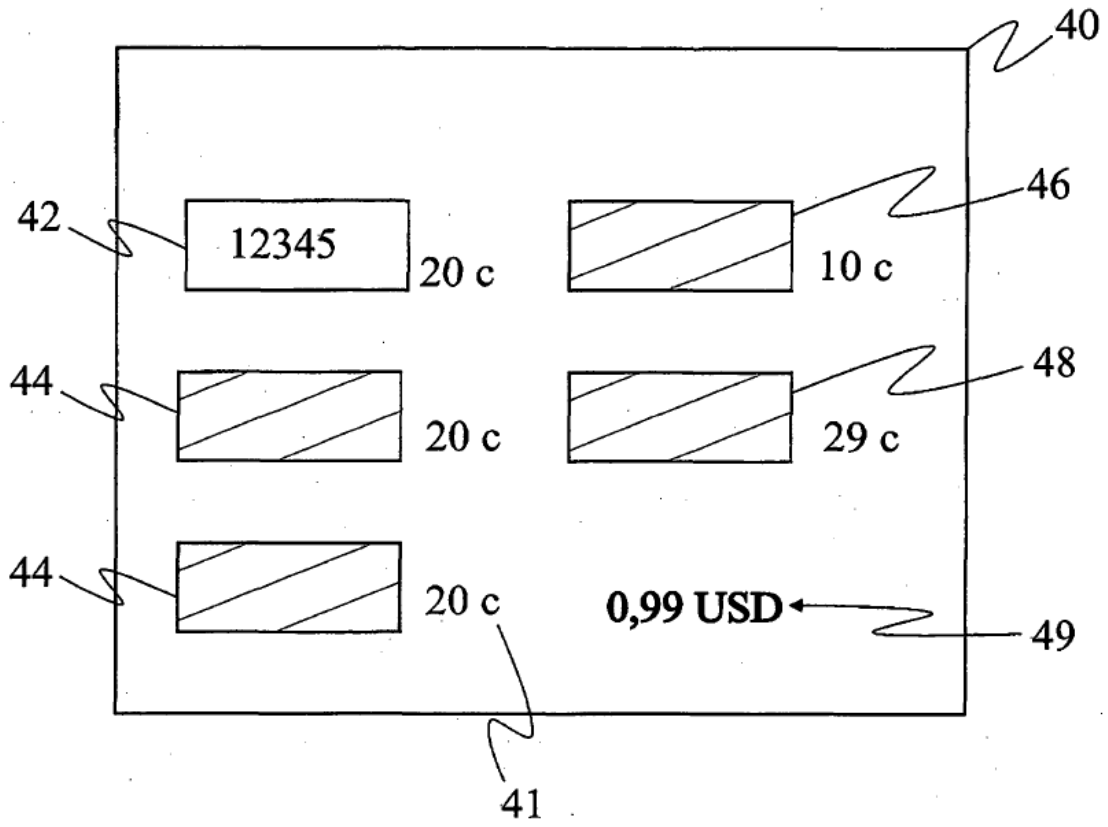

Fig. 4

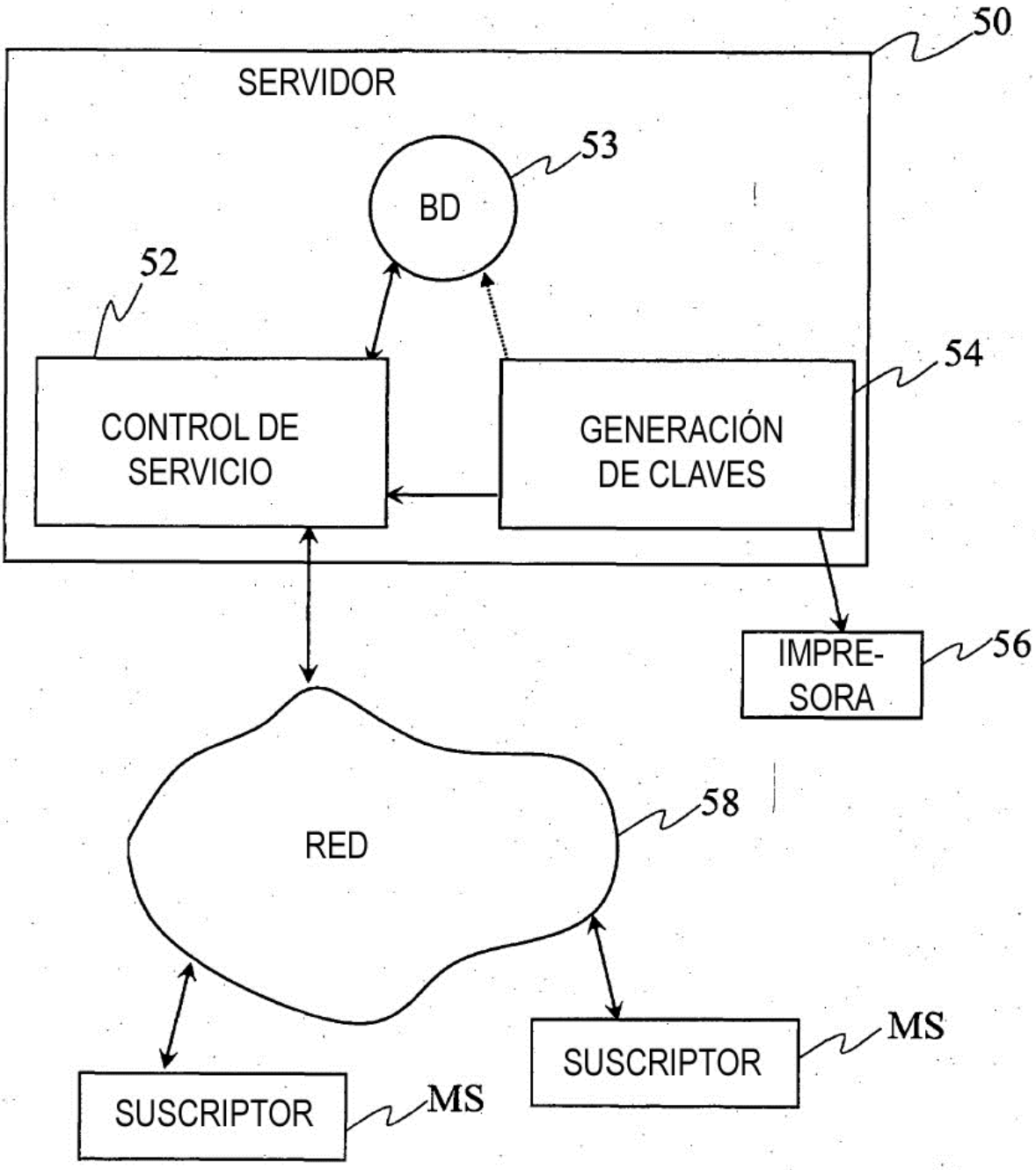
50
SERVIDOR
53
BD
52
54
CONTROL DE SERVICIO
GENERACIÓN DE CLAVES
IMPRE-SORA
56
RED
58
SUSCRIPTOR
MS
SUSCRIPTOR
MS

Fig. 5