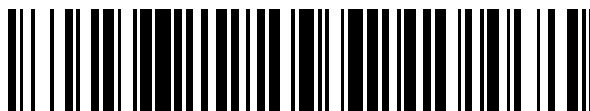


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 752 973**

51 Int. Cl.:

G06F 21/34 (2013.01)

G06F 21/62 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **08.12.2005** **PCT/EP2005/013212**

87 Fecha y número de publicación internacional: **06.07.2006** **WO06069622**

96 Fecha de presentación y número de la solicitud europea: **08.12.2005** **E 05817605 (8)**

97 Fecha y número de publicación de la concesión europea: **07.08.2019** **EP 1844417**

54 Título: **Método y sistema para acceso restringido a servicio**

30 Prioridad:

30.12.2004 US 640877 P

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

06.04.2020

73 Titular/es:

TELEFÓNICA GERMANY GMBH & CO. OHG
(100.0%)

Georg-Brauchle-Ring 50
80992 München, DE

72 Inventor/es:

SCHRÖTER, ANDREAS

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 2 752 973 T3

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

DESCRIPCIÓN

Método y sistema para acceso restringido a servicio

Campo

5 La presente invención se refiere, en general, a comunicaciones inalámbricas, y más particularmente, se refiere a un método y sistema para restringir el acceso a contenido para adultos usando un dispositivo de comunicación inalámbrico.

Antecedentes

10 Es habitual que determinadas personas, especialmente miembros de una familia, compartan dispositivos de comunicación inalámbricos, tales como teléfonos móviles. Por ejemplo, un progenitor puede comprar un teléfono móvil y dejárselo a su hijo durante el día de modo que el hijo pueda llamar al progenitor cuando necesita que lo recojan del colegio. Tras haberlo recogido, el niño puede devolver el teléfono móvil a su progenitor, que puede usar el teléfono móvil durante la tarde.

15 A lo largo del tiempo, se han añadido funcionalidades a teléfonos móviles que permiten que los abonados tengan acceso a un número creciente de servicios. Los teléfonos móviles ya no solo sirven para llamar por teléfono. Hoy en día, un abonado puede consultar su correo electrónico, enviar fotos, y realizar compras en línea usando su teléfono móvil. La cantidad de contenido al que el abonado puede tener acceso parece ser casi ilimitado. Sin embargo, no todo el contenido es apropiado para menores.

20 Proporcionar contenido para adultos es un gran negocio. Sin embargo, los niños no deberían tener acceso a este tipo de contenido. De hecho, puede ser ilegal permitir que menores tengan acceso a contenido para adultos. Cuando tanto adultos como niños usan el mismo teléfono móvil, tiene que existir algún mecanismo que impida que los niños tengan acceso al contenido para adultos, al tiempo que pueda seguir siendo accesible para los adultos.

25 Los mecanismos de seguridad ya existentes (terminal + tarjeta SIM + PIN) usados por operadores móviles no son suficientes. El mantenimiento y entrega personal de PIN adicionales también conlleva un problema (al menos desde un punto de vista comercial). Otros PIN ya existentes (por ejemplo, el PIN i-mode) pueden desactivarse para simplificar el uso de otros tipos de contenido. Por tanto, deben implementarse barreras adicionales.

30 El documento WO 2004/036513 A1 da a conocer un ordenador, tal como un PC basado en Windows, asociado con un módulo de identidad de abonado (o SIM), tal como del tipo usado en un sistema de teléfono celular GSM. El SIM puede autenticarse mediante la red telefónica, de la misma manera que para autenticar los SIM de usuarios de teléfonos móviles en la red, y, de esta manera, puede autenticar al usuario del PC o al propio PC. Tal autenticación puede permitir, por ejemplo, el uso del PC en relación con una aplicación particular que se libera en el PC tras haber completado de manera satisfactoria la autenticación. La aplicación puede liberarse en el PC por un tercero después de y en respuesta a la finalización satisfactoria del proceso de autenticación. Puede adeudarse un cargo por la sesión al usuario por la red de telecomunicaciones y entonces pasarse al tercero.

Sumario

35 Se describe un método y sistema para acceso restringido a servicio. La invención garantiza un grupo de usuario cerrado para ofertas y servicios de contenido. Se usa una tarjeta inteligente (por ejemplo, una tarjeta de datos de microcontrolador con intervalos de datos protegidos (véase la norma ISO/IEC 7816)) con dos niveles de protección. El primer nivel de protección controla el uso normal, mientras que el segundo nivel de protección está destinado a la administración de datos personales específicos. Solo con el conocimiento del número de identificación personal (PIN) del segundo nivel de protección se accede a un método de cálculo basado en microcontrolador (algoritmo) dado, con el que puede calcularse y mostrarse una clave, que puede validarse en otra ubicación con un mismo algoritmo o un algoritmo inverso.

40 La tarjeta inteligente se usa en un terminal y la interfaz de usuario se gestiona mediante el terminal. La tarjeta inteligente (tarjeta SIM) en un terminal de telecomunicaciones también se usa para la identificación del socio contractual dentro de una red de telecomunicaciones.

Los niveles de protección están enlazados con los códigos de acceso PIN1 y PIN2 de una tarjeta SIM (módulo de identificación de abonado).

50 El cálculo de la clave está cifrado por tiempo y la validación también se realiza según tiempo. Alternativa y/o adicionalmente, el cálculo de la clave está cifrado, pero es personal y está basado en datos protegidos (inalterables y/o ilegibles) o datos individuales abiertos en la tarjeta inteligente y la validación en otra ubicación se basa en los mismos datos individuales.

La individualización puede activarse y desactivarse por el usuario. La individualización puede activarse y desactivarse mediante un mensaje enviado a la tarjeta inteligente, que puede enviarse, por ejemplo, al dispositivo de telecomunicaciones y se reenvía a la tarjeta inteligente.

El algoritmo para el cálculo de la clave puede parametrizarse mediante un mensaje enviado a la tarjeta inteligente, que puede enviarse, por ejemplo, al dispositivo de telecomunicaciones y se reenvía a la tarjeta inteligente.

Se envía un mensaje (por ejemplo, SMS) cuando se genera la clave. Es posible recibir un recargo por ese mensaje.

- 5 La validación es un requisito previo para el acceso a ofertas o servicios de contenido en diferentes medios (internet, WAP, i-mode™, MMS,...). La validación es independiente de la red de comunicación y los datos. La validación se realiza en partes de la red de telecomunicaciones y se ofrece a terceros como un servicio.

Pueden generarse números aleatorios para su visualización en lugar de una clave válida, si no se usa el número de identificación personal del segundo nivel de protección.

- 10 Estos, así como otros aspectos y ventajas resultarán evidentes para los expertos habituales en la técnica tras la lectura de la siguiente descripción detallada, con referencia, donde resulte apropiado, a los dibujos adjuntos. Además, se comprende que este sumario es simplemente un ejemplo y no está destinado a limitar el alcance de la invención tal como se reivindica.

La invención se define mediante el alcance de las reivindicaciones adjuntas.

Breve descripción de los dibujos

- 15 A continuación, en el presente documento, se describen realizaciones preferidas junto con las figuras de dibujos adjuntas, en las que los números de referencia similares se refieren a elementos similares en las diversas figuras, y en las que:

La figura 1 es un diagrama de flujo que representa un método para acceso restringido a servicio, según una realización; y

- 20 la figura 2 es un diagrama de bloques que representa un sistema para acceso restringido a servicio, según una realización.

Descripción detallada

- 25 Se describen un método 100 y un sistema 200 para acceso restringido a servicio. La solución se basa en la idea de limitar el acceso a contenido para adultos por medio de un código de acceso basado en tiempo y/o personalizado. La solución impide que los niños tengan acceso al contenido para adultos cuando usan un dispositivo 202 móvil, al tiempo que permiten el acceso a adultos. La solución es independiente de los medios (por ejemplo, i-mode, WAP, internet, MMS).

- 30 La figura 1 es un diagrama de flujo que representa el método 100 para acceso restringido a servicio. El método 100 incluye recibir un PIN 102 de administrador, calcular un código 104 de acceso, y enviar el código de acceso a un proveedor 106 de contenido. Tras la recepción del código de acceso, el proveedor de contenido puede verificar que el usuario que introduce el PIN de administrador está autorizado a recibir el contenido. El método 100 se describe adicionalmente con referencia al sistema 200.

- 35 La figura 2 es un diagrama de bloques que representa el sistema 200 para acceso restringido a servicio. El código de acceso se deriva de una aplicación 206 ejecutada en una tarjeta 204 inteligente (por ejemplo, una tarjeta de módulo de identificación de abonado (SIM)), que está protegida por medio de un código de número de identificación personal (PIN) adicional. Se calcula un código de acceso válido si un usuario ha introducido el PIN de administrador (PIN 2) de la tarjeta 204 SIM y el teléfono 202 móvil ya está activado y/o si el PIN 1 también se conoce.

- 40 Las tarjetas SIM tienen, habitualmente, dos números PIN enlazados con diferentes zonas de seguridad. Normalmente, el primer PIN protege el teléfono móvil/SIM que está usándose sin permiso para llamadas normales y así sucesivamente. El segundo PIN (administrador) cubre ajustes como números restringidos, activación/desactivación de PIN1, y así sucesivamente. El segundo PIN puede ser secreto incluso si el teléfono se usa por diferentes personas.

- 45 Para usar la oferta de contenido, el usuario debe introducir el PIN2 antes de que se genere un código de acceso calculado (por ejemplo, en un navegador), que se proporciona a un proveedor 208 de contenido. El código de acceso se construye de tal manera que el proveedor 208 de contenido puede calcular una ventana de tiempo válida o puede solicitar un mensaje de reconocimiento procedente de un servidor 210 central. Si el uso actual se encuentra dentro de la ventana de tiempo válida, se permite el acceso.

- 50 El código de acceso puede ser personalizado y/o estar basado en tiempo. Para un código de acceso personalizado, se añade un número único (por ejemplo, una identificación de tarjeta de circuito integrado (ICCID)) almacenada en la tarjeta 204 SIM durante la producción al algoritmo para calcular el código de acceso. Este número único también se conoce por el servidor 210 central (por ejemplo, trasladando el número ISDN internacional de estación móvil (MSISDN) a la ICCID). El servidor 210 puede validar la solicitud procedente del proveedor 208 de contenido. Esto es posible si la tarjeta 204 SIM también se usa para establecer la conexión a la red móvil. Esto significa que el código

de acceso personalizado solo puede usarse en combinación con la tarjeta 204 SIM de generación. Alternativa y/o adicionalmente, puede usarse un valor de partida individual (quizá aleatorio) para calcular el código de acceso, que solo se conoce por el proveedor 208 de contenido y el usuario.

5 Con el código de acceso personalizado, es más complicado descifrar o “averiguar” el algoritmo. Cuando se garantiza (por ejemplo, por medio de control de pasaporte) que la tarjeta 204 SIM y los PIN se entregan a la persona adulta adecuada, solo es posible que estas personas obtengan acceso al grupo de usuario cerrado y a la oferta de contenido, incluso si el propio teléfono 202 móvil está usándose por otras personas (por ejemplo, miembros de la familia).

10 El método 100 puede usarse para diferentes tipos de medios (i-mode, WAP.MMS, ...) e incluso puede usarse para ofertas no móviles por medio de internet y PC (solo en modo basado en tiempo). Con medios adicionales (aprovisionamiento inalámbrico) puede garantizarse que los algoritmos puedan modificarse para potenciar la seguridad y/o para conmutar entre modos personalizados y basados en tiempo.

Al enviar un SMS cuando se genera el código de acceso, puede ser posible que exista un recargo relacionado con el código de acceso.

15 Debe comprenderse que las realizaciones ilustradas son solo ejemplos y no deben tenerse en consideración como limitativas del alcance de la presente invención.

REIVINDICACIONES

1. Sistema para proporcionar acceso a contenido restringido o servicios en un proveedor (208) de contenido, que comprende el proveedor (208) de contenido, medios de validación y un terminal (202) con una tarjeta (204) SIM, teniendo la tarjeta (204) SIM niveles de protección primero y segundo enlazados con un primer código de número de identificación personal, PIN1, y un segundo código de número de identificación personal, PIN2, en el que el código PIN1 enlazado al primer nivel de protección protege el terminal/SIM que se está usando sin permiso para llamadas normales y el segundo nivel de protección controla la administración de datos individuales, en el que el código PIN2 del segundo nivel de protección se usa para acceder a un algoritmo de cálculo basado en microcontrolador, y en el que el algoritmo calcula un código de acceso, estando el terminal (202) dispuesto para dotar al proveedor (208) de contenido del código de acceso, validándose, posteriormente, el código de acceso por los medios de validación en otra ubicación (210) o en el proveedor (208) de contenido, usando el mismo algoritmo o un algoritmo inverso, que proporciona acceso al contenido o servicio restringido en el proveedor (208) de contenido, en el que el cálculo del código de acceso está cifrado y personalizado usando un número único almacenado en la tarjeta (204) SIM y la validación se basa en el mismo número único; estando el sistema caracterizado porque comprende, además, medios para activar y desactivar la personalización por el usuario.
2. Sistema según la reivindicación 1, en el que el cálculo del código de acceso está cifrado y está basado en tiempo, y en el que la validación también está basada en tiempo.
3. Sistema según la reivindicación 1, en el que la personalización puede activarse y desactivarse enviando un mensaje a la tarjeta SIM.
4. Sistema según la reivindicación 1, en el que el algoritmo para el cálculo del código de acceso puede parametrizarse mediante un mensaje enviado a la tarjeta SIM.
5. Sistema según la reivindicación 1, en el que se envía un mensaje cuando se genera el código de acceso, y en el que es posible recibir un recargo por ese mensaje.
6. Sistema según la reivindicación 1, en el que la validación es independiente de medios e independiente una red de comunicaciones particular.
7. Sistema según la reivindicación 1, en el que la validación se realiza en partes de la red de telecomunicaciones y se ofrece a terceros como un servicio.
8. Método para proporcionar acceso a contenido o servicios restringidos, proporcionándose los servicios y contenidos por el proveedor (208) de contenido, comprendiendo el método las etapas de
 - dotar a un terminal (202) de una tarjeta (204) SIM, estando la tarjeta (204) SIM comprendida por dos niveles de protección enlazados con un primer código de número de identificación personal, PIN1, y un segundo código de número de identificación personal, PIN2, en el que el código PIN1 enlazado al primer nivel de protección protege el terminal/SIM que está usándose sin permiso para llamadas normales y el segundo nivel de protección controla la administración de datos individuales,
 - tras introducir dicho PIN2 del segundo nivel de protección, usar un algoritmo de cálculo basado en microcontrolador para calcular un código de acceso, en el que el código de acceso está cifrado y es personal usando un número único almacenado en la tarjeta SIM y en el que dicha personalización puede activarse y desactivarse por un usuario,
 - dotar al proveedor (208) de contenido del código de acceso,
 - en respuesta a la provisión del código de acceso, validar el código de acceso en el proveedor (208) de contenido o en otra ubicación (210), usando el mismo algoritmo o un algoritmo inverso, en el que la validación se basa en el mismo número único, con el fin de permitir el acceso al contenido o servicios restringidos.

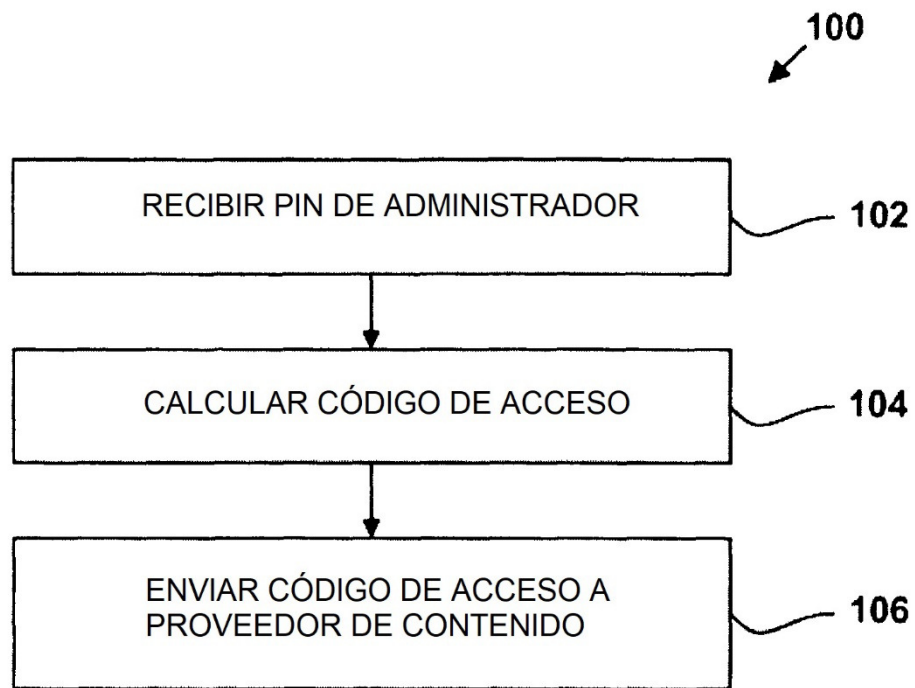


Fig. 1

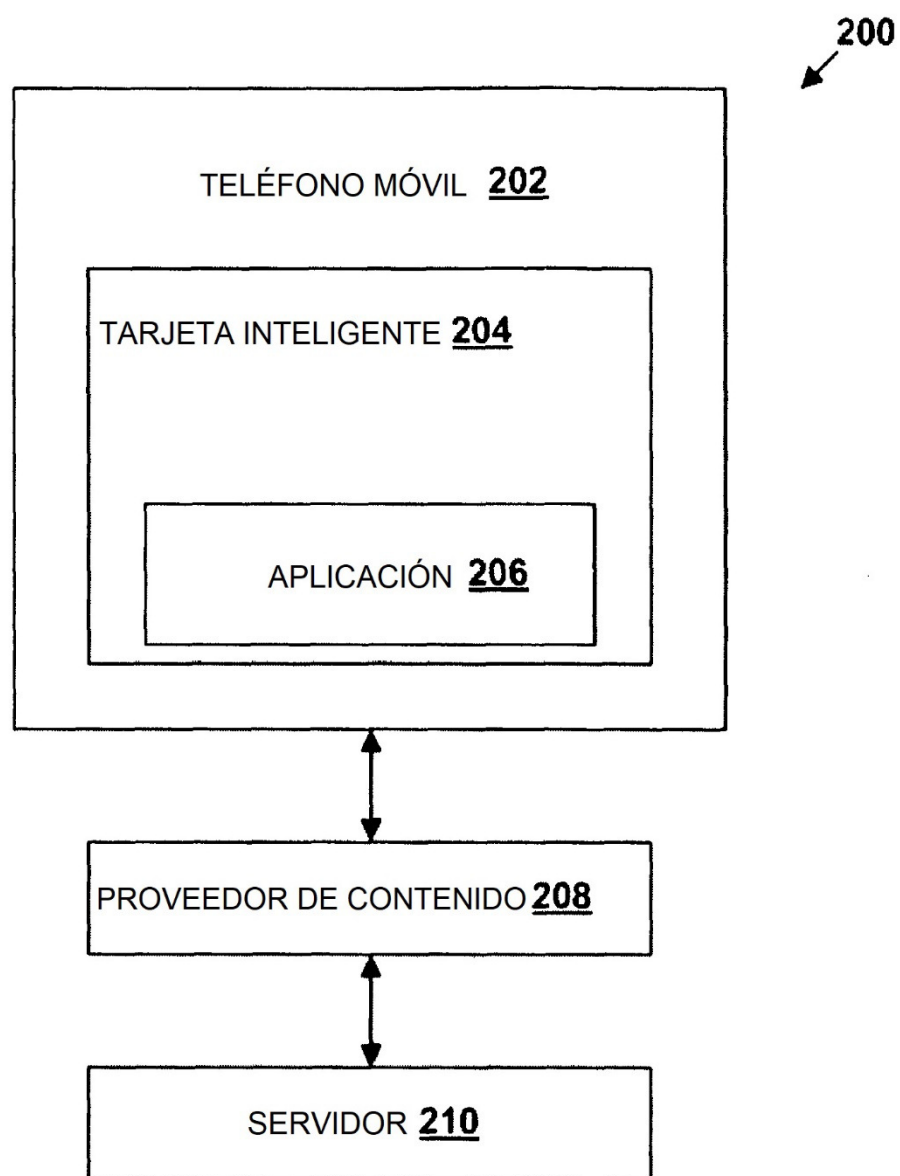


Fig. 2