(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 368**

(21) Número de solicitud: **201130019**

(51) Int. CI.:
H04L 29/06 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación: **11.01.2011**

(43) Fecha de publicación de la solicitud: **20.12.2012**

(43) Fecha de publicación del folleto de la solicitud: **20.12.2012**

(71) Solicitante/s:
TELEFÓNICA, S.A. (100.0%)
GRAN VÍA, 28
28013 MADRID, ES

(72) Inventor/es:
GARCÍA PUGA, Javier;
MARTÍNEZ ÁLVAREZ, Javier y
PÉREZ CUBERO, Roberto

(74) Agente/Representante:
ARIZTI ACHA, Monica

(54) Título: **MÉTODO DE IDENTIFICACIÓN PARA ACCEDER A SERVICIOS O APLICACIONES DE BANDA ANCHA MÓVIL.**

(57) Resumen:
Método de identificación para acceder a servicios o aplicaciones de banda ancha móvil.
Comprende, enviar una credencial a un servidor que proporciona servicios de banda ancha, realizando el método para que un usuario sea identificado las siguientes acciones:
- usar credenciales para ser proporcionadas a dichos servicios de banda ancha, siendo cifradas y almacenadas en una memoria, dicho cifrado comprendiendo:
- obtener un certificado a partir de una tarjeta SIM;
- cifrar la credencial por medio de un algoritmo de cifrado; y
- realizar dicho envío de la credencial.
Para acceder a dicho servicio o aplicación, interaccionando con medios (43) de entrada, el método realiza además:
- acceder a dicha memoria (44) para buscar dicha credencial, y si no se la encuentra:
- enviar una petición de dicha credencial;
- realizar la petición de activación necesaria para activar la cuenta de usuario;y
- enviar la credencial para el servicio solicitado.

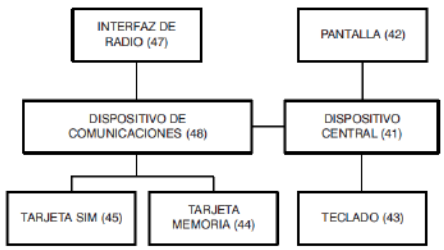


FIG. 2

ES 2 393 368 A1

DESCRIPCIÓN

Método de identificación para acceder a servicios o aplicaciones de banda ancha móvil.

Campo de la técnica

La presente invención se refiere, en general, a un método de identificación para acceder a servicios o aplicaciones de MBB, usando credenciales asociadas a un servicio o aplicación solicitado, y más particularmente a un método que comprende usar un dispositivo de comunicaciones, tal como un dispositivo mochila USB, para participar en el cifrado/descifrado de dichas credenciales para aumentar la seguridad asociada con su acceso.

Estado de la técnica anterior

Generalmente, los métodos de autorización e identidad en servicios y aplicaciones web se realizan mediante la introducción manual de un conjunto de credenciales, normalmente un usuario y una contraseña. Puesto que cada servicio tiene diferentes políticas para configurar estas credenciales, es decir número de caracteres, empleo de símbolos o caracteres alfanuméricos, etc., el usuario se ve obligado a introducir diferentes valores para cada uno de estos servicios.

Existen algunas iniciativas como OpenID que intentan resolver este problema, sin embargo el sistema no llega a un número relevante de servicios web y, una vez más, el usuario tiene que recordar un nuevo conjunto de usuarios/contraseñas.

Otro enfoque para evitar que los usuarios olviden las diferentes credenciales que han configurado para los diferentes servicios son las “cadenas de claves” locales o basadas en red, tal como 1-Password. Este tipo de servicios simplemente permite al usuario almacenar los diferentes conjuntos de credenciales en un repositorio seguro protegido por contraseña. Así, tras introducir la contraseña del repositorio, se pueden encontrar todos los diferentes conjuntos de credenciales que han almacenado previamente. Por tanto, este tipo de iniciativas no evitan la necesidad de que los usuarios generen la cuenta manualmente, simplemente les ayuda a recordarla en el futuro.

Algunos otros servicios web como los relacionados con los operadores de telecomunicaciones aprovechan las credenciales de la red. Por ejemplo, normalmente se usa el MSISDN como inicio de sesión, y la contraseña se genera aleatoriamente y se envía al usuario por SMS.

Como perspectiva general de los métodos actuales indicados anteriormente, se puede concluir que todos ellos requieren que el usuario recuerde la credencial y la necesidad de introducirla manualmente cuando desea acceder al servicio.

Los siguientes documentos y propuestas están relacionados con la presente invención, sin embargo abordan diferentes problemas, y las soluciones técnicas para resolverlos son diferentes de la propuesta en este documento.

La invención propuesta en [1] se centra en el propio dispositivo en lugar de especificar el mecanismo de autenticación. Además, no especifica el procedimiento en el método de activación del primer uso y no especifica la forma en que se almacenan las credenciales y si usa algún método de cifrado para garantizar la privacidad y la seguridad.

Puede observarse que la invención [2] se refiere a credenciales de red en lugar de las credenciales para usar servicios de valor añadido. Mediante el uso de la solución propuesta en esta invención es posible paliar el problema cuando se pasa por diferentes entornos de conectividad de red, pero no se dice nada acerca de las credenciales de los servicios que se están usando dentro de esos entornos de red.

En la invención [3], el dispositivo de identificación no tiene ninguna característica de comunicación, se basa en el dispositivo central para proporcionar al mismo la característica de conectividad. Además, no tiene ninguna capacidad de cifrado, y no especifica el mecanismo de almacenamiento de las credenciales. A diferencia de la presente propuesta, el dispositivo de esta invención actúa como proxy, intercepta todas las peticiones de red, y en caso de que sea necesario, modifica la petición para añadir las credenciales. En la presente invención no se propone ningún tipo de proxy ya que el sistema no modifica las peticiones de red de usuario.

En la patente [4], las peticiones de información sobre credenciales desde una SIM se inician usando EAPSIM. Cubre principalmente un método para autorizar a un sistema informático conectarse a una WLAN. Por tanto esta patente representa un método de autorización de red, no uno a nivel de servicios. La misma característica se observa en [5]. El sistema aprovecha una tarjeta SIM externa para obtener acceso a una red WWAN. Por tanto, de nuevo, esta invención sólo cubre el nivel de red pero no el nivel de servicios.

La propuesta [6] se basa en la implementación en tarjetas inteligentes de procedimientos de tipo EAP, diseñados para autenticar la identidad del usuario en la fase de registro para acceder a la red a través del intercambio de claves. Por tanto no se trata de un procedimiento de autenticación a nivel de servicio, sino de un registro en la red de acceso mediante la autenticación segura del usuario. Esta conclusión puede extenderse también a [7].

La propuesta [8] está orientada al acceso durante la conexión o el registro de un terminal en la red WLAN. Introduce un procedimiento para verificar la identidad del usuario que accede a una conexión a través de un terminal dual WiFi-GSM. Esto se consigue generando una clave de usuario a partir de la red, asociada al número de móvil, que se envía por SMS al mismo. Esta clave se usa entonces para acceder al servicio vía WiFi, verificándose así la identidad del usuario.

El sistema descrito en [9] está orientado al uso del identificador IMSI en el acceso a la red a través de un elemento de IP móvil, de modo que no se trata de un nivel de autenticación de servicio, sino de un nivel de red para proporcionar acceso a los terminales. Esta conclusión puede extenderse también a [10].

En la actualidad, un conjunto importante de aplicaciones y servicios ofrecidos a los usuarios requieren introducir un conjunto de credenciales para obtener acceso a los mismos. En el caso de los usuarios que acceden a estas aplicaciones desde una red de banda ancha móvil (dispositivo mochila móvil o USB), la identificación se lleva a cabo independientemente de las credenciales de inicio de sesión del dispositivo en la red de acceso. Por tanto el usuario se ve obligado a realizar diversos procesos de autenticación de manera secuencial, lo que normalmente constituye un problema, especialmente porque el usuario tiene que enfrentarse a un nuevo conjunto de credenciales y después tiene que recordarlas. La figura 1 ilustra los diferentes elementos implicados en dichos procesos de autenticación.

Descripción de la invención

Es necesario ofrecer una alternativa al estado de la técnica que cubra las lagunas que se encuentran en el mismo.

Con este fin, la presente invención proporciona un método de identificación para acceder a servicios o aplicaciones de banda ancha móvil (MBB), que comprende, por medio de un dispositivo de comunicaciones (tal como un dispositivo mochila USB) de un dispositivo central o equipo informático.

El método de la invención comprende, como es conocido en el estado de la técnica, realizar para que un usuario sea identificado para tener acceso al servicio o aplicaciones, las siguientes acciones:

- usar una o unas credenciales para ser proporcionadas a dichos servicios de banda ancha o aplicaciones, a través de una red de banda ancha móvil, o MBB, de manera que dicha o dichas credenciales son cifradas y almacenadas en una memoria (44) del dispositivo (48) de comunicaciones, dicho cifrado comprendiendo:

- obtener un certificado a partir de una tarjeta SIM de dicho dispositivo de comunicaciones;

- cifrar dicha al menos una credencial por medio de un algoritmo de cifrado, usando dicho certificado como entrada para dicho algoritmo de cifrado; y

- realizar dicho envío de la al menos una credencial, sin cifrar, antes y/o después de dicho cifrado.

El método, comprende además, de manera característica, para acceder a dicho servicio o aplicación, interaccionando con medios (43) de entrada de dicho equipo (41) informático, realizar las siguientes acciones:

- acceder, dicho dispositivo (48) de comunicaciones, a dicha memoria (44) para buscar dicha o dichas credenciales del servicio solicitado, y si no se encuentra dicha o dichas credenciales:

- enviar, el dispositivo (48) de comunicaciones automáticamente o el usuario manualmente, una petición, a través de la red de MBB por medio de una interfaz (47) de radio de MBB del dispositivo (48) de comunicaciones, a un servidor de activación, de dicha o dichas credenciales;

- realizar, dicho servidor de activación, la petición de activación necesaria para activar la cuenta de usuario a un servidor de extremo posterior, obteniendo así del mismo la o las credenciales solicitadas; y

- enviar, el servidor de activación, la o las credenciales para el servicio solicitado al equipo (41) informático, a través de la red de MBB.

Para una realización del método para así obtener el certificado la función “ejecutar algoritmo GSM” es ejecutada en la tarjeta SIM.

Otras realizaciones del método de la invención se describen en las reivindicaciones adjuntas y en una sección posterior de la presente descripción.

Breve descripción de los dibujos

Las ventajas y características anteriores y otras se entenderán más completamente a partir de la siguiente descripción detallada de realizaciones, con referencia a los dibujos adjuntos (algunos de los cuales ya se han descrito en la sección Estado de la técnica anterior), que debe considerarse de manera ilustrativa y no limitativa, en los que:

La figura 1 muestra una arquitectura convencional que requiere la necesidad de realizar un proceso de autenticación para acceder a una aplicación o a un servicio.

La figura 2 muestra los diferentes elementos usados por el método de la invención, en una realización.

La figura 3 muestra un diagrama de flujo de recuperación de credenciales completo con diferentes alternativas, en una realización del método de la invención.

Descripción detallada de varias realizaciones

La invención proporciona un método sencillo para identificar a un usuario para acceder a servicios o aplicaciones, aprovechando la autenticación del usuario proporcionada por los operadores de telecomunicaciones, por medio de conexiones de MBB o mensajes SMS / USSD y las funcionalidades de cifrado que proporciona la tarjeta SIM, que se inserta en el dispositivo, tal como un dispositivo mochila USB de banda ancha móvil.

Mediante el uso del mecanismo del método de la invención, el usuario se registra en el servicio de manera transparente y “silenciosa”, de modo que el usuario no tiene que recordar e introducir las credenciales del servicio cada vez que use el dispositivo mochila de MBB.

A diferencia de otras soluciones, la presente invención se centra en una autenticación a nivel de servicio, en lugar de en una autenticación a nivel de red, por tanto, el proceso de activación y las credenciales almacenadas en esta invención son las credenciales del servicio o aplicación dado.

Otro punto importante de esta invención es el uso de la tarjeta SIM y el certificado de conexión GSM para cifrar las credenciales del servicio. Este certificado se usa habitualmente para conectarse a la red GSM pero no para cifrar contenido en el lado del cliente. En combinación con la tarjeta SIM que está dentro del dispositivo mochila de banda ancha móvil, es posible usar y almacenar las credenciales de usuario de manera segura. Los usuarios sólo tendrán que conocer el código PIN de la tarjeta SIM para obtener acceso a estos servicios o aplicaciones.

La idea principal de esta propuesta es aprovechar la identificación de red de acceso (generalmente IMSI o MSISDN) cuando se obtiene acceso a estos servicios de aplicaciones. Por tanto, el dispositivo mochila USB se convierte en la clave de acceso para este tipo de servicios o aplicaciones, haciéndolo de manera nueva e innovadora, que es protegiendo “la clave” mediante el código privado PIN de la SIM.

Al almacenar las credenciales cifradas usando el certificado GSM almacenado en la tarjeta SIM del dispositivo, no es posible que terceras partes las recuperen sin conocer el código PIN de la SIM. Es por ello que las credenciales están totalmente protegidas frente a un uso no autorizado. Dado que el servicio está protegido por estas credenciales, el acceso al servicio está cerrado a usuarios que no conozcan el PIN de la tarjeta SIM.

Puesto que las credenciales se gestionan mediante un único servidor de servicio de autenticación y activación, es posible centralizar la gestión de todas las peticiones de activación y autenticación necesarias para hacer funcionar el servicio.

Tal como se muestra en la figura 2, el dispositivo 41 central, que puede ser denominado como dispositivo informático, en el que está instalado el dispositivo 48 de comunicación (normalmente un dispositivo mochila USB), ejecuta el software que intenta acceder a un servicio en nombre del usuario. Ese dispositivo (normalmente un ordenador) se compone de, entre otros elementos, un controlador para manejar la comunicación con el dispositivo de comunicaciones, una pantalla 42 y un teclado 43.

El dispositivo de comunicaciones tiene una tarjeta 45 SIM y una tarjeta 44 de memoria, una interfaz de E/S y una interfaz 47 de radio para permitir al dispositivo 41 central acceder a la red en la que está albergado el servicio.

La autenticación tiene varios flujos en función del estado de las credenciales:

1. Cuando un usuario quiere acceder a un servicio, el dispositivo va a la tarjeta 44 de memoria para buscar las credenciales del servicio actual, si no existe, el dispositivo 48 automáticamente, o el usuario, enviará una petición vía HTTP (conectado a través de una conexión de MBB) o mensaje SMS o USSD usando la interfaz 47 de radio para pedir al servidor de activación una credencial para el usuario concreto y servicio concreto.

2. El servidor de activación valida al usuario basándose en la identidad de red móvil (generalmente IMSI o MSISDN) y envía de vuelta un nuevo mensaje que contiene las credenciales para acceder al servicio solicitado.

3. El dispositivo va a la tarjeta 45 SIM para obtener un certificado; el procedimiento usado es ejecutar en la SIM la función estándar “ejecutar algoritmo GSM” pasando una semilla fijada como argumento, si la SIM está bloqueada entonces se muestra un mensaje en la pantalla para permitir a los usuarios introducir el pin. El usuario introduce la clave usando el teclado 43, si la clave introducida es válida se genera un certificado. Si la SIM no está bloqueada, el pin no es necesario. Este certificado es único por SIM, cada SIM tiene su propio certificado y otra SIM tiene un certificado distinto.

4. Una vez obtenido el certificado, la siguiente etapa es usarlo como entrada en un algoritmo de cifrado simétrico para cifrarlo con las credenciales obtenidas en la etapa 2.

5. La credencial cifrada se guarda en la tarjeta de memoria del sistema.

6. La credencial obtenida en la etapa 2 se usa, sin cifrar, para acceder al servicio.

Si el usuario más tarde quiere acceder al servicio, las etapas serían las siguientes ya que las credenciales ya están almacenadas en la tarjeta de memoria:

7. El dispositivo va a la tarjeta (44) de memoria para buscar las credenciales cifradas para el servicio actual que el usuario guardó previamente

8. El dispositivo va a la tarjeta (45) SIM para obtener un certificado; el procedimiento consiste en ejecutar en la SIM la función estándar "ejecutar algoritmo GSM" pasando una semilla fijada como argumento, así si la SIM está bloqueada entonces se muestra un mensaje en la pantalla para permitir al usuario introducir el pin. El usuario introduce la clave usando el teclado (43) y si la clave introducida es válida se genera un certificado. Si la SIM no está bloqueada, el pin no es necesario.

9. Una vez obtenido el certificado, la siguiente etapa es usar una entrada en un algoritmo de cifrado simétrico para descifrarlo con las credenciales obtenidas en la etapa 7.

10. La credencial descifrada en la etapa anterior se usa para acceder al servicio.

La figura 3 muestra el diagrama con el flujo completo con las diferentes alternativas indicadas anteriormente, que se llevará a cabo en función de la respuesta a la pregunta "*¿Hay un archivo de credenciales?"* indicada en el recuadro disyuntivo en la parte superior del diagrama de flujo: si la respuesta es NO se llevarán a cabo las acciones de la rama izquierda del diagrama de flujo, que son las indicadas anteriormente como 1 a 6; y si la respuesta es SÍ se llevarán a cabo las acciones de la rama derecha, que corresponden a las indicadas anteriormente como 7 a 10.

En una realización del método de la invención, están implicados los siguientes elementos:

1. Un procedimiento para enviar el formulario de petición de validación sin necesidad de intervención activa del usuario y basándose en la red de banda ancha móvil. La petición se envía de manera transparente desde el punto de vista del usuario; por tanto no es necesario que el usuario inicie el proceso. Se obtienen entonces las credenciales necesarias para usar el servicio dado.

2. Un servidor que se encarga de redirigir las peticiones entrantes de red de banda ancha (vía SMS o USSD) al servicio web desplegado en el servidor de extremo posterior. Este servidor recibirá peticiones desde los dispositivos mochila MBB de los clientes, entonces realizará la petición de activación necesaria para activar la cuenta de usuario al servidor de extremo posterior. Tras obtener las credenciales, el servidor las enviará de vuelta al dispositivo cliente. La comunicación entre el servidor y el extremo posterior que alberga el servicio web tendrá lugar usando protocolos de Internet seguros como HTTP sobre capa de zócalos seguros o HTTPS.

3. Un procedimiento para entregar credenciales cifradas desde el servidor de extremo posterior al cliente. Una vez realizadas la activación y la generación de las credenciales, éstas se enviarán de vuelta al cliente usando el mismo canal por el que se recibió la petición. Primero desde el servidor de extremo posterior a través del servidor usando HTTP/HTTPS y por último al dispositivo del cliente usando un mecanismo de red tal como SMS o USSD

4. Un procedimiento de almacenamiento seguro de las credenciales en la memoria interna o dispositivo mochila USB de MBB extraíble. Este procedimiento se basa en los algoritmos de certificaciones GSM que proporciona la SIM contenidos en el dispositivo mochila de MBB. Una vez recibidas las credenciales desde el servidor de autenticación y validación, el sistema las almacena de manera segura en la memoria del dispositivo, de modo que puedan reutilizarse en diversas ocasiones, proporcionando así seguridad de usuario por cada usuario. Ninguna persona que no conozca el código PIN de la tarjeta SIM podrá leer y usar las credenciales.

Un experto en la técnica podrá introducir cambios y modificaciones en las realizaciones descritas sin alejarse del alcance de la invención tal como se define en las reivindicaciones adjuntas.

SIGLAS Y ABREVIATURAS

ADSL	Línea de abonado digital asimétrica
GSM	Sistema global para comunicaciones móviles
HTTP	Protocolo de transferencia de hipertexto
HTTPS	Protocolo seguro de transferencia de hipertexto
IMEI	Identidad internacional de equipo móvil

IMSI	Identidad internacional de abonado móvil
MBB	Banda ancha móvil
MSISDN	Número RDSI de abonado móvil
PIN	Número de identificación personal
SIM	Módulo de identidad de abonado
SMS	Servicio de mensajes cortos
UMTS	Sistema universal de telecomunicaciones móviles
USSD	Servicio suplementario de datos no estructurados

BIBLIOGRAFÍA

[1] “Generic Identity Module for Telecommunication Services”, US20090191916A1, Eitan MARDIKS, Raanana (IL).

[2] “Connectivity Manager to Manage Connectivity Services”, WO2009025707A1, COLE, Terry, L (US), TORMO, Jose (US).

[3] “Service access control”, WO20010075885A1, BAUER-HERMANN, Markus (DE), MEYER, Gerand (DE), SEIDL, Robert (DE).

[4] “Enhanced general packet radio service (GPRS) mobility management”, US20040162105A1, RAMGOPAL K. REDDY (US), DHIRAJ BATT (US).

[5] “System including a wireless wide area network (WWAN) module with an external identity module reader and approach for certifying the WWAN module”, US20050288056A1, SUNDEEP M. BAJIKAR (US), FRANCIS X. MCKEEN (US).

[6] 3GPP, 3GPP TSG SA WG3 Security — S3#28 (S3-030198) 6 - 9 May 2003, Berlín, Alemania. “EAP support in smartcards and security requirements in WLAN authentication”.

[7] “SIM-based Subscriber Authentication for Wireless Local Area Networks”, Yuh-Ren Tsai y Cheng-Ju Chang, 2003 IEEE. Proceedings of IEEE 37th Annual 2003 International Carnahan Conference on Security Technology.

[8] “A convenient and secure wireless LAN authentication method and system based on SMS mechanism of GSM”, TW252649B, LEE WEI-BIN (TW); YEH CHANG-KUO (TW).

[9] “Method and system for GSM-authentication during roaming in wireless local networks”, RU2295200, Shtadel Mann Toni (CH); Kauts Mikhel (CH).

[10] “Authentication method e.g. for multimode terminal within wireless network, GSM, GPRS, UMTS, involves authentication of multi-mode terminal in wireless network under use of existing or channel which can be developed to second network”, GRIMMINGER JOCHEN (DE); GROETING WOLFGANG (DE).

REIVINDICACIONES

1. Método de identificación para acceder a servicios o aplicaciones de banda ancha móvil, que comprende, por medio de un dispositivo (48) de comunicaciones de un dispositivo central o equipo (41) informático, realizar, para que un usuario sea identificado para tener acceso al servicio o aplicación solicitado, las siguientes acciones:

- usar una o unas credenciales para ser proporcionadas a dichos servicios de banda ancha o aplicaciones, a través de una red de banda ancha móvil, o MBB, de manera que dicha o dichas credenciales son cifradas y almacenadas en una memoria (44) del dispositivo (48) de comunicaciones, dicho cifrado comprendiendo:

- obtener un certificado a partir de una tarjeta (45) SIM de dicho dispositivo (48) de comunicaciones;

- cifrar dicha o dichas credenciales por medio de un algoritmo de cifrado, usando dicho certificado como entrada para dicho algoritmo de cifrado;

y

- realizar dicho envío de la o las credenciales, sin cifrar, antes y/o después de dicho cifrado,

estando el método caracterizado porque comprende además para acceder a dicho servicio o aplicación, interaccionando con medios (43) de entrada de dicho equipo (41) informático, realizar las siguientes acciones:

- acceder, dicho dispositivo (48) de comunicaciones, a dicha memoria (44) para buscar dicha o dichas credenciales del servicio solicitado, y si no se encuentra dicha o dichas credenciales:

- enviar, el dispositivo (48) de comunicaciones automáticamente o el usuario manualmente, una petición, a través de la red de MBB por medio de una interfaz (47) de radio de MBB del dispositivo (48) de comunicaciones, a un servidor de activación, de dicha o dichas credenciales;

- realizar, dicho servidor de activación, la petición de activación necesaria para activar la cuenta de usuario a un servidor de extremo posterior, obteniendo así del mismo la o las credenciales solicitadas; y

- enviar, el servidor de activación, la o las credenciales para el servicio solicitado al equipo (41) informático, a través de la red de MBB.

2. Método de identificación según cualquiera de las reivindicaciones anteriores, que comprende ejecutar una función en la tarjeta (45) SIM para obtener dicho certificado.

3. Método de identificación según la reivindicación 2, en el que dicha función es la función estándar “ejecutar algoritmo GSM”, comprendiendo dicha ejecución pasar una semilla fijada como argumento en dicha función “ejecutar algoritmo GSM”.

4. Método de identificación según la reivindicación 1, en el que dicho algoritmo de cifrado es un algoritmo de cifrado simétrico.

5. Método de identificación según cualquiera de las reivindicaciones anteriores, en el que, si la SIM se bloquea, el método comprende desbloquearla usando un correspondiente número de identificación personal privado, o PIN, código privado, con el fin de permitir la obtención de dicho certificado.

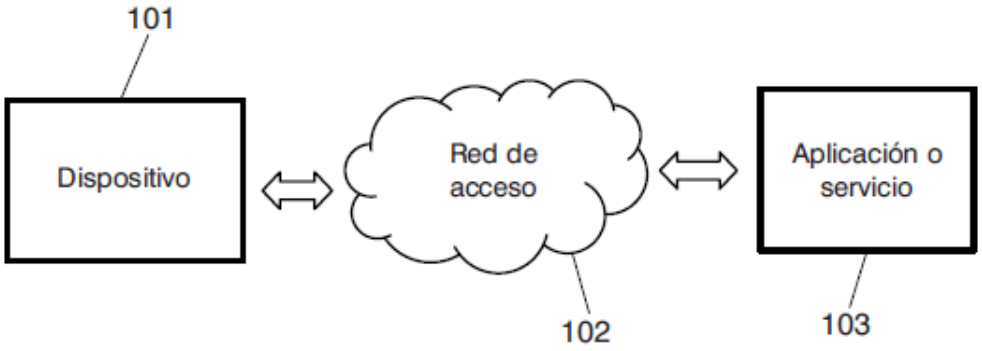

101
Dispositivo
Red de acceso
Aplicación o servicio
102
103

FIG. 1

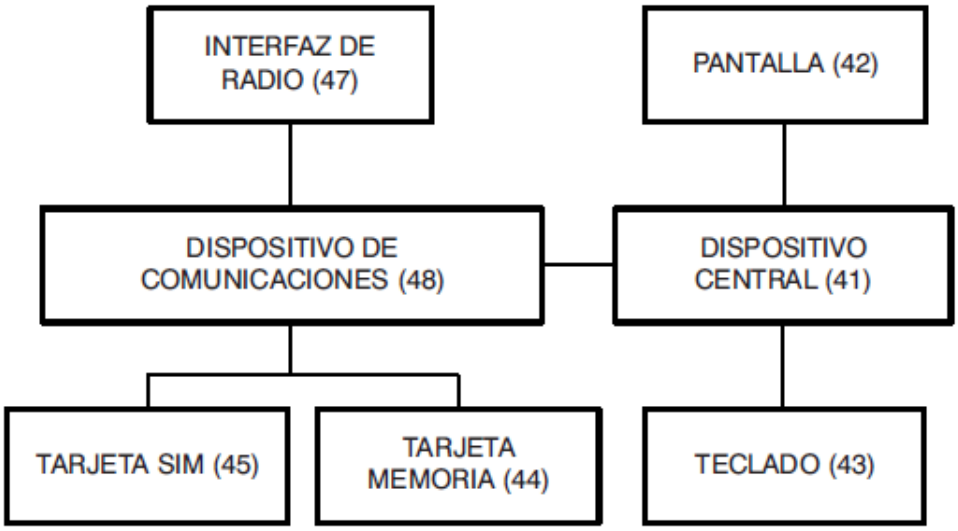

INTERFAZ DE RADIO (47)
PANTALLA (42)
DISPOSITIVO DE COMUNICACIONES (48)
DISPOSITIVO CENTRAL (41)
TARJETA SIM (45)
TARJETA MEMORIA (44)
TECLADO (43)

FIG. 2

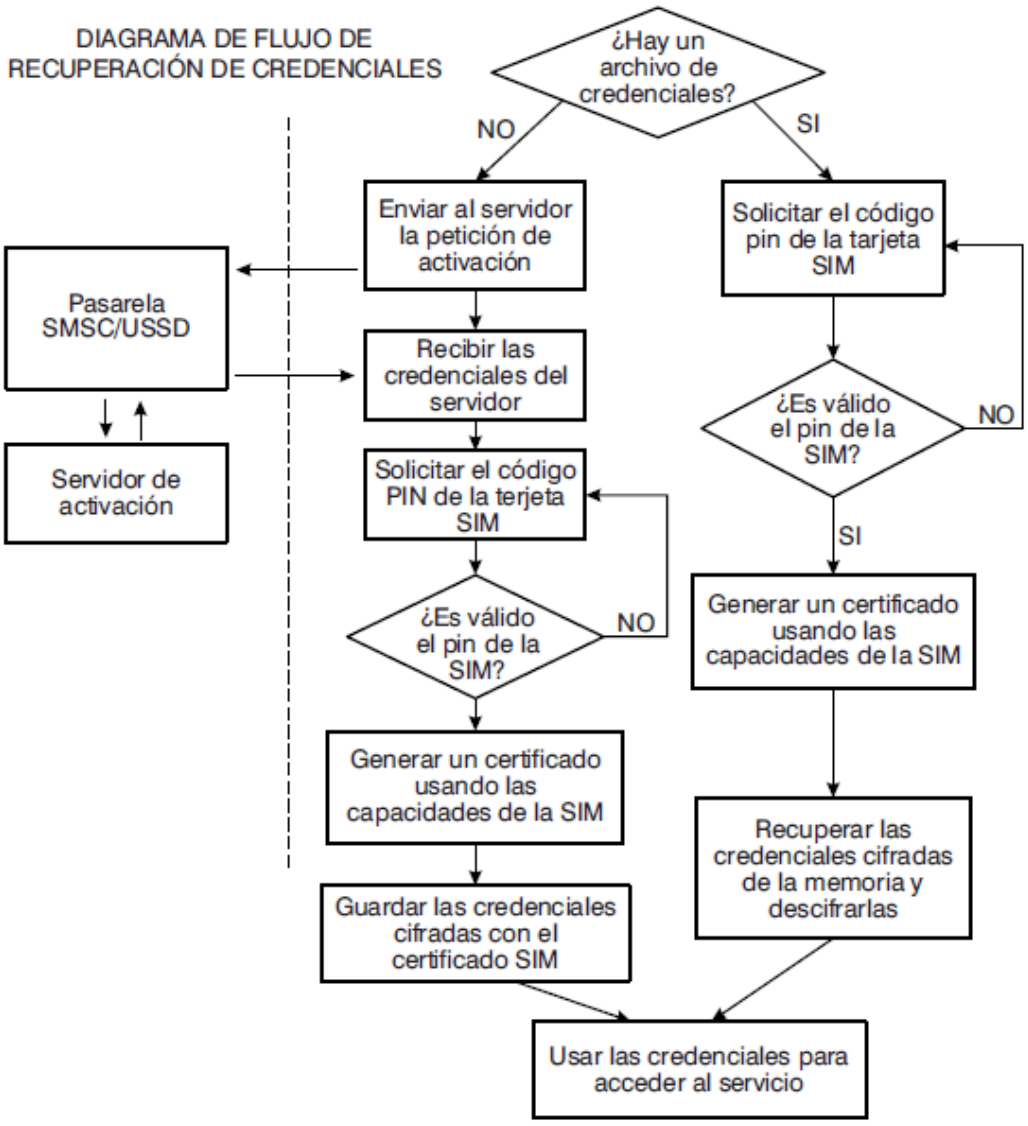

DIAGRAMA DE FLUJO DE RECUPERACIÓN DE CREDENCIALES
¿Hay un archivo de credenciales?
NO
SI
Enviar al servidor la petición de activación
Solicitar el código pin de la tarjeta SIM
Pasarela SMSC/USSD
Recibir las credenciales del servidor
¿Es válido el pin de la SIM?
NO
Servidor de activación
Solicitar el código PIN de la terjeta SIM
SI
¿Es válido el pin de la SIM?
NO
Generar un certificado usando las capacidades de la SIM
Generar un certificado usando las capacidades de la SIM
Recuperar las credenciales cifradas de la memoria y descifrarlas
Guardar las credenciales cifradas con el certificado SIM
Usar las credenciales para acceder al servicio

FIG. 3

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201130019

(22) Fecha de presentación de la solicitud: 11.01.2011

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L29/06*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	WO 2005064430 A1 (TELECOM ITALIA SPA et al.) 14.07.2005, página 5, línea 22 – página 6, línea 20; página 7, línea 18 – página 15, línea 16; página 16, línea10 – página 19, línea 12; figuras 1,2.	1-5
Y	WO 9910793 A1 (SONERA OY et al.) 04.03.1999, página 1, línea 10; página 2, línea 36 – página 3, línea 5; página 5, línea 26 – página 7, línea 3; página 7, línea 25 – página 8, línea 16.	1-5
Y	WO 2009004411 A1 (FREESCALE SEMICONDUCTOR, INC. et al.) 08.01.2009 página 1, líneas 12-16; página 4, línea 21 – página 5, línea 20; página 7, línea 9 – página 8, línea 14; figuras 1-3.	1-5

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
03.12.2012	J. Santaella Vallejo	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 03.12.2012

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-5	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-5	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	WO 2005064430 A1 (TELECOM ITALIA SPA et al.)	14.07.2005
D02	WO 9910793 A1 (SONERA OY et al.)	04.03.1999
D03	WO 2009004411 A1 (FREESCALE SEMICONDUCTOR, INC. et al.)	08.01.2009

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

La invención reivindicada presenta un método que obtiene un certificado a partir de la módulo de identidad de abonado (SIM) de un dispositivo, lo cifra utilizando el algoritmo de la SIM y lo envía al servicio. Pudiendo almacenar el certificado en una memoria.

El documento del estado de la técnica más próximo a la invención es D01 y divulga la utilización de un módulo de identidad de abonado (SIM) que posee un algoritmo de seguridad instalado en un sistema informático (CS) y lo utiliza para generar una clave de cifrado. Esta clave se utiliza para cifrar archivos.

Para mayor claridad, y en la medida de lo posible, se emplea la misma redacción utilizada en la reivindicación 1. Las referencias entre paréntesis corresponden al D01. Las características técnicas que no se encuentran en el documento D01 se indican entre corchetes.

Reivindicación 1

Método de identificación para acceder a servicios o aplicaciones de banda ancha móvil, que comprende, por medio de un dispositivo de comunicaciones de un dispositivo central o equipo informático (figura 1, elemento 10), realizar, para que un usuario sea identificado para tener acceso al servicio o aplicación solicitado, las siguientes acciones (Titulo y resumen):

- usar una o unas credenciales para ser proporcionadas a dichos servicios de banda ancha o aplicaciones, a través de una red de banda ancha móvil, o MBB, de manera que dicha o dichas credenciales son cifradas y almacenadas en una memoria del dispositivo de comunicaciones, dicho cifrado comprendiendo (figura 1, SIM Card),:
- obtener un certificado a partir de una tarjeta SIM de dicho dispositivo de comunicaciones (figura 1, elementos 10 y 20) ;
- cifrar dicha o dichas credenciales por medio de un algoritmo de cifrado, usando dicho certificado como entrada para dicho algoritmo de cifrado(página 8, líneas 6 y 7);

y

- realizar dicho envío de la o las credenciales, sin cifrar, antes y/o después de dicho cifrado, estando el método caracterizado porque comprende además para acceder a dicho servicio o aplicación, interaccionando con medios de entrada de dicho equipo informático(pagina 9, línea 5), realizar las siguientes acciones:
- acceder, dicho dispositivo de comunicaciones, a dicha memoria para buscar dicha o dichas credenciales del servicio solicitado, y si no se encuentra dicha o dichas credenciales (página 9, línea 5):
- enviar, el dispositivo de comunicaciones automáticamente o el usuario manualmente, una petición, a través de la red de MBB por medio de una interfaz de radio de MBB del dispositivo de comunicaciones, a un servidor de activación, de dicha o dichas credenciales(reivindicación 19, figura 1);
- [realizar, dicho servidor de activación, la petición de activación necesaria para activar la cuenta de usuario a un servidor de extremo posterior, obteniendo así del mismo la o las credenciales solicitadas]; y
- enviar, el servidor de activación, la o las credenciales para el servicio solicitado al equipo informático, a través de la red de MBB (figura 1)

En el documento D01 no se menciona la necesidad de petición de activación necesaria para activar la cuenta de usuario para obtener las credenciales. Este paso está implícito en el sistema al obtener las credenciales y poder generar las claves de sesión, ya que al tener una SIM debe de tener una cuenta de usuario.

Por lo tanto a la luz de D01, la invención es nueva pero carece de actividad inventiva tal como se establece en los artículos 6 y 8 de la Ley de Patentes 1986

Reivindicaciones 2-5

Las reivindicaciones 2-5 están incluidas en el documento D01 como la ejecución en la tarjeta SIM, la utilización del algoritmo GSM, o aplicar un cifrado simétrico o la utilización del PIN para desbloqueo.

Por lo tanto a la luz de D01, las reivindicaciones 2-5 son nuevas pero carecen de actividad inventiva tal como se establece en los artículos 6 y 8 de la Ley de Patentes 1986.