(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 411 579**

(21) Número de solicitud: 201131968

(51) Int. CI.:

***H04W 12/04*** (2009.01)
***G06F 21/31*** (2013.01)
***H04L 9/32*** (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

**05.12.2011**

(43) Fecha de publicación de la solicitud:

**05.07.2013**

(88) Fecha de publicación diferida del informe sobre el estado de la técnica:
**26.09.2013**

Fecha de la concesión:

**01.08.2014**

(45) Fecha de publicación de la concesión:

**08.08.2014**

(73) Titular/es:

**TELEFÓNICA, S.A. (100.0%)**
**Gran Vía, 28**
**28013 Madrid (Madrid) ES**

(72) Inventor/es:

**AMAYA CALVO, Antonio Manuel y**
**OCHOA FUENTES, Miguel**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

(54) Título: **SISTEMA Y PROCEDIMIENTO DE CONTROL DE CREDENCIALES DE USUARIO PARA EL ACCESO A SERVICIOS DE TERCERAS PARTES EN REDES MÓVILES**

**ES 2 411 579 B1**

(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 411 579**

(21) Número de solicitud: 201131968

(57) Resumen:
Sistema y procedimiento de control de credenciales de usuario para el acceso a servicios de terceras partes en redes móviles.
Sistema y procedimiento para controlar credenciales proporcionadas por un usuario, en una red móvil con un servidor de terceras partes (2) y una aplicación de lado de cliente (1) que solicita acceso al servidor de terceras partes (2) en nombre del usuario, que comprenden:
- un administrador de credenciales (21) para recuperar una identidad inequívoca del usuario y permitir al usuario identificado proporcionar credenciales auténticas para su uso por servicios protegidos del servidor de terceras partes (2) y credenciales falsas para su uso por la aplicación de lado de cliente (1),
- un repositorio de almacenamiento de credenciales (23) en el que el administrador de credenciales (21) almacena las credenciales tanto auténticas como falsas en asociación con la identidad del usuario,
- un reemplazador de credenciales (22) para detectar mensajes de autenticación en la comunicación entre la aplicación de lado de cliente (1) y el servidor de terceras partes (2) y reemplazar las credenciales falsas en los mensajes de autenticación detectados por las credenciales auténticas asociadas del repositorio de almacenamiento de credenciales (23).

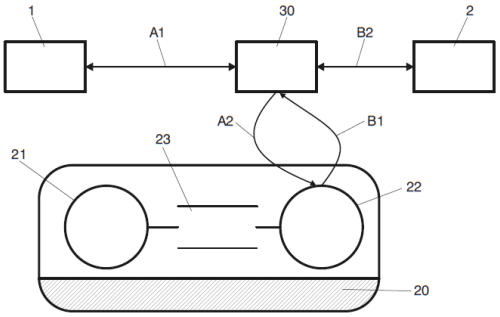


**FIG. 2**

ES 2 411 579 B1

# SISTEMA Y PROCEDIMIENTO DE CONTROL DE CREDENCIALES DE USUARIO PARA EL ACCESO A SERVICIOS DE TERCERAS PARTES EN REDES MÓVILES

## DESCRIPCIÓN

### CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención trata de la manipulación y administración segura de información privada y confidencial (es decir, credenciales) usada por usuarios finales para el acceso a un servicio de terceros o terceras partes (en inglés, “third party services”), por ejemplo, servicio de web 2.0, y más particularmente, se refiere a un sistema y procedimiento para controlar credenciales de usuario desde el lado de la red móvil.

### ANTECEDENTES DE LA INVENCIÓN

EL auge de los servicios web implica un aumento de información privada y confidencial depositada por individuos y empresas en los proveedores de servicios de Internet (ISP). Por ejemplo, los servicios de web 2.0, asociados con aplicaciones web que facilitan tendencias sistémicas interactivas, interoperabilidad, diseño orientado al usuario y desarrollo de la *World Wide Web*, usan determinada información de usuario para identificar de manera unívoca a un único individuo o cliente. Ejemplos de servicios de web 2.0 incluyen sitios de redes sociales, tales como *Facebook*, *Twitter*, *Tuenti*, *Orkut*, etc.

En el panorama actual de aplicaciones móviles, existe un completo espectro de aplicaciones móviles (lado de cliente) que hacen uso de servicios de terceras partes (habitual pero no necesariamente servicios de web 2.0), o bien como la funcionalidad primaria de la aplicación o bien como una funcionalidad secundaria. Por tanto, por ejemplo, existen varias aplicaciones de mensajería instantánea que permiten conexiones con los servidores de *Google Talk*, y existen bastantes aplicaciones que permiten al usuario publicar algo en *Twitter* o *Facebook*, directamente desde la aplicación.

Puesto que se solicitan credenciales al usuario final para posibilitar el acceso al servicio de terceras partes, y por tanto el usuario debe realizar una declaración de confianza implícita con respecto al desarrollador de la aplicación de lado de cliente cuando proporciona a esta aplicación las credenciales del usuario, esta situación presenta un posible problema de seguridad. De hecho, el usuario le confía sus credenciales al desarrollador de la aplicación para el servicio de terceras partes. Aún peor, en algunos casos, tal como el mencionado anteriormente de *Google Talk*, puede usarse la misma credencial para acceder a más servicios del mismo proveedor (por ejemplo, la credencial

de *Google* da acceso a todas las aplicaciones de *Google*). Esto significa que un desarrollador deshonesto puede recopilar, fácilmente, cientos o miles de credenciales del usuario para servicios de terceras partes. Por tanto, en el panorama actual, los usuarios finales pierden el control efectivo de sus credenciales cada vez que las proporcionan.

Con el fin de aliviar este problema, las soluciones existentes establecen un mecanismo mediante el cual el usuario no proporciona las credenciales directamente a la aplicación; en su lugar, se implementa un mecanismo de autenticación delegado, tridireccional, tal como se muestra en la figura 1. Cuando el usuario final desde una aplicación de lado de cliente (1) solicita acceso (10) a un servidor de terceras partes (2) a través de un navegador web (3), que puede estar integrado o ser independiente, el navegador web (3) se conecta a una página específica en respuesta a una petición de acceso (11) proporcionada por el servidor de terceras partes (2). Esta página exige las credenciales (12) al usuario a través del navegador web (3). El usuario las proporciona a dicho navegador web (3), que a su vez envía las credenciales (13) al servidor de terceras partes (2). Tras comprobar la validez de las credenciales del usuario, el servidor de terceras partes (3) genera entonces un testigo de acceso (14) que se retransmite (15) por el navegador web (3) a la aplicación de lado de cliente (1). Luego el testigo de acceso se usa para acceder (16) al servidor de terceras partes (2) por la aplicación de lado de cliente (1) como el usuario, sin que dicha aplicación tenga acceso a las credenciales del usuario.

Por tanto, el mecanismo que acaba de describirse, como el implementado por la comunidad de *OAuth*, intenta permitir que una aplicación móvil obtenga acceso a un servicio de terceras partes sin tener acceso real a la credencial del usuario. Tal como se define por el Grupo de trabajo de ingeniería de Internet (IETF) en la Petición de Comentarios, RFC 5849 (abril de 2010), *OAuth* permite al usuario conceder acceso a recursos del usuario privados en un sitio (que se denomina el proveedor de servicios), a otro sitio (denominado consumidor, no debe confundirse con el usuario). *OAuth* se refiere a dar acceso a información o contenido personal de un usuario sin compartir la identidad del usuario en absoluto (o sus partes secretas, es decir, las credenciales). *OAuth* se soporta por varios de los grandes actores de la web 2.0, tales como *Google*, *Facebook* o *Twitter*. *OAuth* proporciona un procedimiento para que los clientes accedan a los recursos de servidor en nombre de un propietario de recurso (tal como un cliente diferente o un usuario final) y también proporciona un proceso para que usuarios finales autoricen el acceso de terceras partes a sus recursos de servidor sin compartir sus credenciales (normalmente, un par de nombre de usuario y contraseña), usando redirecciones de agente de usuario. *OAuth* es la normalización y sabiduría combinada de muchos protocolos del sector bien

establecidos: similar a otros protocolos actualmente en uso (*Google AuthSub*, *aol OpenAuth*, *Yahoo BBAuth*, *Upcoming api*, *Flickr api*, *Amazon Web Services api*, etc.). Cada protocolo proporciona un procedimiento propietario para intercambiar las credenciales de usuario por un testigo o ticket de acceso.

En el presente contexto, se usa la siguiente terminología (RFC 5849):

Recurso protegido: Un recurso de acceso restringido que puede obtenerse del servidor de terceras partes del proveedor de servicios.

Propietario de recurso: Una entidad que puede acceder y controlar recursos protegidos usando credenciales para autenticarse con el servidor de terceras partes.

Credenciales: *OAuth* define las credenciales como un par de un identificador único y un secreto compartido coincidente. *OAuth* especifica tres clases de credenciales: cliente, temporal y testigo, usadas para identificar y autenticar al cliente que realiza la petición, la petición de autorización y la concesión de acceso, respectivamente.

Testigo: Un identificador único emitido por el servidor y usado por el cliente para asociar peticiones autenticadas con el propietario de recurso cuya autorización se solicita o se ha obtenido por el cliente. Los testigos tienen un secreto compartido coincidente que se usa por el cliente para establecer su propiedad del testigo, y su autoridad para representar al propietario de recurso.

Normalmente, las credenciales de *OAuth* 2.0 consisten en los siguientes elementos:

- ID de cliente - Identifica de manera unívoca la aplicación.
- Secreto de cliente - Usada como parte de la petición de testigo por un cliente.
- URI de redirección - Una lista de URI (identificadores de recursos uniformes) de redirección válidos permitidos en una petición de autorización. La primera vez que una aplicación solicita un testigo de autorización, se envía una petición que incluye un URI de redirección. El URI de redirección indica dónde *Google* debe redirigir el navegador después de que el usuario permita (o deniegue) la petición de autorización. Las aplicaciones basadas en web proporcionan el URI de una página gestora para llamar después de que se complete la petición de autorización; las aplicaciones instaladas usan una cadena de URI convencional. Si una petición basada en web no incluye un URI enumerado aquí, el usuario obtendrá un error de autorización.
- Información de marca - Se trata de información acerca del propietario de recurso (un individuo o una empresa) que se muestra cuando su aplicación solicita por primera vez una autorización *OAuth*.

Los mecanismos existentes, tales como la implementación de *OAuth*, mostrada en

la figura 1, presentan tres problemas principales:

1) Soporte: Debe implementarse y soportarse por el servidor de terceras partes. Además, debe soportarse en todos los servicios del servidor. Aunque algunos de los más grandes actores (*Google*, *Facebook*, *Twitter*) soportan un mecanismo de autorización como el descrito anteriormente, no todos los servicios de web 2.0 lo soportan. Aún más, algunos de los servicios de *Google* no soportan un mecanismo de autenticación delegado (por ejemplo, *Google Talk* no lo soporta).
2) Verificabilidad por el usuario: Es prácticamente imposible para el usuario, incluso para un usuario avanzado, verificar si un navegador integrado (o navegador de sistema operativo) está usándose en realidad para proporcionar las credenciales al navegador web (3), en la figura 1, o si el usuario en realidad está proporcionándolas directamente a la aplicación, que implementará entonces el mecanismo de autenticación completo. Además, en esquemas *OAuth* se confía implícitamente en el navegador, puesto que las credenciales deben proporcionarse a través de éste para el primer acceso.
3) Verificabilidad por el servidor de terceras partes: Aún peor, también es imposible para el servidor de terceras partes distinguir entre una aplicación de fiar que implementa el protocolo correctamente (es decir, la aplicación de fiar no tiene acceso a las credenciales) y una aplicación fraudulenta que implementa directamente la totalidad de la interfaz de usuario y tiene acceso a las credenciales.

El problema técnico objetivo es permitir a los usuarios finales conservar la seguridad y control en el uso de sus credenciales para acceder a servicios de terceras partes, en cualquier caso independientemente del servidor de terceras partes e incluso si la aplicación cliente que solicita acceso en el nombre del usuario al servidor de terceras partes es malintencionada.

## SUMARIO DE LA INVENCIÓN

La presente invención sirve para resolver el problema mencionado anteriormente proporcionando un sistema y procedimiento que reside en el lado de la red móvil para permitir el uso de servicios de terceras partes autenticados por parte de cualquier aplicación de lado de cliente (móvil) y mantener la seguridad completa de las credenciales del usuario. De hecho, este sistema y procedimiento evitan que los usuarios proporcionen

sus credenciales directamente a las aplicaciones, ya que la invención permite que la red móvil sea la única encargada de introducir de manera transparente las credenciales cuando se necesiten por el servicio de terceras partes, basándose en la identidad de un usuario (obtenida a partir de la identidad de abonado de red móvil) y credenciales previamente proporcionadas al proveedor de la red móvil. Por tanto, los usuarios finales no tienen que introducir nunca sus credenciales en sus terminales móviles, en caso de elegir no hacerlo. La invención garantiza la seguridad de las credenciales del usuario incluso si la aplicación móvil es de naturaleza malintencionada puesto que la aplicación nunca accede a las credenciales del usuario ya que se introducen directamente en el flujo de comunicación fuera de la aplicación potencialmente comprometida o incluso del terminal del usuario.

Según un aspecto de la invención, se proporciona un sistema para controlar credenciales de usuario suministradas por un usuario, en una red móvil con una comunicación establecida entre un servidor de terceras partes y una aplicación de lado de cliente que solicita acceso al servidor de terceras partes en nombre del usuario, que comprende:

- un administrador de credenciales que comprende medios para recuperar una identidad del usuario definida de manera inequívoca (es decir, es única e identifica al usuario inequívocamente) en la red móvil y medios de acceso a través de los cuales el usuario proporciona credenciales auténticas para su uso en un servicio de terceras partes protegido del servidor de terceras partes y credenciales falsas para su uso por la aplicación de lado de cliente,

- un repositorio o base de datos de almacenamiento de credenciales en el que el administrador de credenciales almacena tanto las credenciales auténticas como las credenciales falsas en asociación con la identidad del usuario recuperada (unívoca),

- un reemplazador de credenciales que comprende medios de detección de datos para detectar mensajes de autenticación en la comunicación establecida entre la aplicación de lado de cliente y el servidor de terceras partes, y medios de reemplazo para reemplazar las credenciales falsas en los mensajes de autenticación detectados, que son para el servicio de terceras partes protegido, por las credenciales auténticas asociadas obtenidas del repositorio de almacenamiento de credenciales.

Según otro aspecto de la invención, se proporciona un procedimiento para controlar credenciales de usuario en una comunicación establecida entre un servidor de terceras partes y una aplicación de lado de cliente que solicita acceso en nombre del usuario a cualquier servicio protegido del servidor de terceras partes, comprendiendo el

procedimiento las siguientes etapas:

- Recuperar una identidad del usuario definida de manera inequívoca en la red móvil (por ejemplo, MSISDN, IMSI). Esta identidad del usuario se recupera mediante un administrador de credenciales que permite el acceso al usuario identificado.

- Luego, el usuario accede y proporciona (por ejemplo, a través de un portal web), al administrador de credenciales, credenciales auténticas para su uso en los servicios de terceras partes protegidos y credenciales falsas para la aplicación de lado de cliente.

- Almacenar las credenciales tanto auténticas como falsas en asociación con la identidad del usuario en una base de datos o repositorio de almacenamiento de credenciales usado por el administrador de credenciales.

- Detectar mensajes de autenticación en la comunicación establecida entre la aplicación de lado de cliente y el servidor de terceras partes y reemplazar las credenciales falsas en los mensajes de autenticación detectados para el servicio de terceras partes protegido por las credenciales auténticas. Esto se realiza mediante un reemplazador de credenciales que obtiene las credenciales auténticas, asociadas con las credenciales falsas y la identidad del usuario, del repositorio de almacenamiento de credenciales.

**DESCRIPCIÓN DE LOS DIBUJOS**

Para completar la descripción que está realizándose y con el objeto de ayudar a un mejor entendimiento de las características de la invención, según un ejemplo preferido de realización práctica de la misma, acompañando a dicha descripción como una parte integrante de la misma, se proporciona un juego de dibujos en los que, a modo de ilustración y de forma no restrictiva, se ha representado lo siguiente:

La figura 1. – Muestra un diagrama de flujo de un procedimiento de autenticación en un sistema de proveedor de servicios de Internet basado en el uso de credenciales y testigos delegados a un navegador web, tal como se conoce en la técnica anterior.

La figura 2. – Muestra un diagrama de flujo de un sistema para la comunicación entre un usuario final y un servicio de terceras partes con control de las credenciales del usuario en la red móvil, según una posible realización de la invención.

**DESCRIPCIÓN DETALLADA DE LA INVENCIÓN**

Tal como se muestra en la figura 2, una realización preferida de la invención se refiere a un sistema (20) para el control de credenciales de usuario en una red móvil, en el

que se establece una comunicación entre una aplicación de lado de cliente (1), que normalmente se ejecuta en un terminal móvil de un usuario final, y un servidor de terceras partes (2) con el fin de acceder a recursos de acceso restringido o protegidos del servidor de terceras partes (2).

La aplicación de lado de cliente (1) puede ser cualquier aplicación existente en el mercado que accede a servicios de terceras partes autenticados, alojados en el servidor de terceras partes (2).

El servidor de terceras partes (2) es un sistema administrado por un proveedor de servicios de Internet que proporciona uno o más servicios de acceso restringido, autenticados o protegidos, es decir, el servidor de terceras partes (2) exige a un usuario que se autentique usando credenciales antes de permitir el uso de los servicios. Adicionalmente, el servidor de terceras partes (2) puede proporcionar acceso a servicios no autenticados, para los que no se solicitan credenciales a los usuarios y por tanto no se necesita administración de credenciales.

Además y opcionalmente, un interceptor de cifrado (30) puede estar en medio de la comunicación establecida de la aplicación de lado de cliente (1), con el servidor de terceras partes (2), con el fin de interceptar comunicaciones cifradas, de una manera que permite que las comunicaciones continúen también sin interceptarse después de un punto determinado. Por ejemplo, esquemas de autenticación actuales usan un canal cifrado para proteger la confidencialidad de credencial en tránsito. Este elemento es una parte externa (no forma parte de la invención, sino que forma parte de su caso de uso).

La arquitectura del sistema (20) para el control de credenciales en la red móvil comprende los siguientes bloques funcionales:

Un reemplazador de credenciales (22) que analiza todos los flujos de tráfico entre la aplicación de lado de cliente (1) y el servidor de terceras partes (2) en comunicación y realiza dos acciones en el tráfico analizado: detección de mensajes de autenticación y reemplazo de credenciales en los mensajes de autenticación.

Un administrador de credenciales (21) que permite a los usuarios finales proporcionar sus credenciales reales, auténticas, directamente al sistema (20), en lugar de al servidor de terceras partes (2) o a la aplicación de lado de cliente (1). Los usuarios finales también proporcionan una credencial falsa o ficticia con el fin de usarse por el servidor de terceras partes (2) o la aplicación de lado de cliente (1), pero las credenciales auténticas del usuario se introducen por el usuario final de manera correcta a través del administrador de credenciales (21) en un repositorio de almacenamiento de credenciales (23) y no se proporcionan directamente a elementos externos tales como el servidor de

terceras partes (2) y la aplicación de lado de cliente (1). El reemplazador de credenciales (22) está encargado de reemplazar las credenciales ficticias por las credenciales del usuario auténticas en los mensajes de autenticación detectados.

Un repositorio de almacenamiento de credenciales (23) es una base de datos en la que se almacenan las credenciales auténticas y las falsas, proporcionadas por los usuarios finales usando el administrador de credenciales (21).

El procedimiento de funcionamiento global del sistema (20) para el control de las credenciales del usuario es de la siguiente manera:

Antes de usar cualquier aplicación de lado de cliente (1) para acceder a cualquiera de los servicios de terceras partes protegidos proporcionados por el servidor de terceras partes (2), el usuario accede al sistema (20) a través de un portal web proporcionado por el administrador de credenciales (21), que identifica automáticamente al usuario basándose en una identidad de abonado única definida en la red móvil, por ejemplo, MSISDN o IMSI, y solicita al usuario que introduzca a través del portal web las credenciales, reales, que el usuario quiere que el sistema (20) proteja cuando se solicite acceso a los servicios de terceras partes protegidos. Como parte de la definición de credencial, el usuario también proporciona credenciales ficticias o falsas para su uso por el sistema (20) más adelante, cuando el usuario quiere que se reemplacen estas credenciales. Todas las credenciales, reales y falsas, se almacenan por el administrador de credenciales (21) en el repositorio de almacenamiento de credenciales (23).

En un momento posterior, el usuario requiere o proporciona acceso a un servicio de terceras partes por medio de una aplicación de lado de cliente (1) instalada en su terminal móvil. La aplicación de lado de cliente (1) pide al usuario que proporcione credenciales, directamente o a través de un procedimiento de autenticación delegado tal como *Oauth*, y el usuario simplemente proporciona sólo las credenciales ficticias previamente anteriormente en el repositorio de almacenamiento de credenciales (23).

Cuando la aplicación de lado de cliente (1) intenta acceder, o proporciona acceso, al servicio de terceras partes, la aplicación de lado de cliente (1) se conecta al servidor de terceras partes (2) y envía un primer mensaje de autenticación (A1).

De manera opcional, si el flujo de datos y por tanto el mensaje de autenticación (A1) está cifrado, un interceptor de cifrado (30) descifra cada mensaje, paquete de datos, y lo pasa al reemplazador de credenciales (22).

El reemplazador de credenciales (22) detecta si el mensaje, descifrado, (A2) contiene un mensaje de autenticación, es decir, comprueba si las siguientes condiciones son ciertas:

- el mensaje (A2) comprende un mensaje de autenticación,
- el destino del mensaje de autenticación es un servidor/servicio protegido,
- el usuario (identificado automáticamente por la red móvil, por ejemplo, usando el MSISDN) ha definido credenciales para ese servicio protegido,
- el mensaje de autenticación incluye las credenciales ficticias definidas por el usuario para ese servicio protegido

Entonces, el reemplazador de credenciales (22) reemplaza las credenciales ficticias por las credenciales reales, estas últimas tomadas del repositorio de almacenamiento de credenciales (23), en el mensaje de autenticación; de lo contrario, si el mensaje (A2) no incluye datos de autenticación, los datos se dejan intactos. El reemplazador de credenciales (22) devuelve un mensaje modificado (B1), o el original, si el mensaje permanece intacto sin datos de autenticación.

En caso de que el mensaje (A2) proceda de un interceptor de cifrado (30), el reemplazador de credenciales (22) envía el mensaje modificado (B1) al interceptor de cifrado (30). El reemplazador de credenciales (22) puede indicar adicionalmente al servidor de terceras partes (2) que este flujo de comunicación ya no debe monitorizarse más.

El interceptor de cifrado (30) cifra el mensaje modificado (B1) recibido del reemplazador de credenciales (22) y transmite un mensaje modificado, cifrado en este caso, final (B2) hacia el servidor de terceras partes (2). Si el flujo de comunicación está marcado/indicado como que no debe monitorizarse adicionalmente, el elemento interceptor de cifrado (30) interrumpe el descifrado del flujo de comunicación y por tanto, también detiene el paso de más mensajes al reemplazador de credenciales (22).

Obsérvese que en este texto, el término “comprende” y sus derivaciones (tales como “que comprende”, etc.) no debe entenderse en un sentido excluyente, es decir, estos términos no deben interpretarse como que excluyen la posibilidad de que lo que se describe y define pueda incluir elementos, etapas, etc. adicionales.

## REIVINDICACIONES

1. Un sistema (20) para controlar credenciales de usuario proporcionadas por un usuario, en una red móvil con una comunicación establecida entre un servidor de terceras partes (2) y una aplicación de lado de cliente (1) que solicita acceso al servidor de terceras partes (2) en nombre del usuario, **caracterizado porque** comprende:

- un administrador de credenciales (21) que comprende medios para recuperar una identidad del usuario definida de manera inequívoca en la red móvil y medios de acceso a través de los cuales el usuario proporciona credenciales auténticas para su uso en un servicio de terceras partes protegido del servidor de terceras partes (2) y credenciales falsas para su uso por la aplicación de lado de cliente (1),

- un repositorio de almacenamiento de credenciales (23) que es una base de datos en la que el administrador de credenciales (21) almacena tanto las credenciales auténticas como las credenciales falsas en asociación con la identidad recuperada del usuario,

- un reemplazador de credenciales (22) que comprende medios de detección de datos para detectar mensajes de autenticación que contienen credenciales falsas en la comunicación establecida entre la aplicación de lado de cliente (1) y el servidor de terceras partes (2), y medios de reemplazo para reemplazar, en los mensajes de autenticación detectados para el servicio de terceras partes protegido, las credenciales falsas por las credenciales auténticas almacenadas en asociación con el repositorio de almacenamiento de credenciales (23).

2. El sistema (20) según la reivindicación 1, en el que los medios de acceso del administrador de credenciales (21) consisten en un portal web.

3. El sistema (20) según cualquier reivindicación anterior, en el que la identidad del usuario recuperada por el administrador de credenciales (21) es el MSISDN.

4. El sistema (20) según cualquier reivindicación anterior, en el que los medios de detección de datos del reemplazador de credenciales (22) detectan unos mensajes de autenticación cuando se cumplen las condiciones siguientes: existe una indicación de mensaje de autenticación en los datos, los datos están destinados a un servicio de terceras partes protegido, existen credenciales auténticas almacenadas en el repositorio de almacenamiento de credenciales (23) proporcionadas por el usuario para el servicio de terceras partes protegido, los datos incluyen credenciales falsas proporcionadas por el usuario y también

almacenadas en el repositorio de almacenamiento de credenciales (23) para el servicio de terceras partes protegido.

5. Un procedimiento para controlar credenciales de usuario proporcionadas por un usuario, en una red móvil con una comunicación establecida entre un servidor de terceras partes (2) y una aplicación de lado de cliente (1) que solicita acceso al servidor de terceras partes (2) en nombre del usuario, **caracterizado porque** comprende:

- recuperar mediante un administrador de credenciales (21) una identidad del usuario definida de manera inequívoca en la red móvil,
- acceder mediante el usuario identificado al administrador de credenciales (21),
- proporcionar mediante el usuario identificado, al administrador de credenciales (21), credenciales auténticas para su uso en un servicio de terceras partes protegido del servidor de terceras partes (2) y credenciales falsas para su uso por la aplicación de lado de cliente (1),
- almacenar en un repositorio de almacenamiento de credenciales (23) usado por el administrador de credenciales (21) tanto las credenciales auténticas como las credenciales falsas en asociación con la identidad del usuario recuperada por el administrador de credenciales (21),
- detectar mensajes de autenticación que contienen credenciales falsas en la comunicación establecida entre la aplicación de lado de cliente (1) y el servidor de terceras partes (2), comprobando si se cumplen las condiciones siguientes: existe una indicación de mensaje de autenticación en los datos, los datos están destinados a un servicio de terceras partes protegido, existen credenciales auténticas almacenadas en el repositorio de almacenamiento de credenciales (23) proporcionadas por el usuario para el servicio de terceras partes protegido, los datos incluyen credenciales falsas proporcionadas por el usuario y también almacenadas en el repositorio de almacenamiento de credenciales (23) para el servicio de terceras partes protegido;
- reemplazar mediante un reemplazador de credenciales (22) las credenciales falsas, en los mensajes de autenticación detectados para el servicio de terceras partes protegido, por las credenciales auténticas que el reemplazador de credenciales (22) obtiene del repositorio de almacenamiento de credenciales (23) y almacenadas en asociación con dichas credenciales falsas.

6. El procedimiento según la reivindicación 5, en el que el acceso por el usuario al administrador de credenciales (21) es a través de un portal web.

7. El procedimiento según cualquiera de las reivindicaciones 5-6, en el que la identidad del usuario recuperada por el administrador de credenciales (21) es el MSISDN.

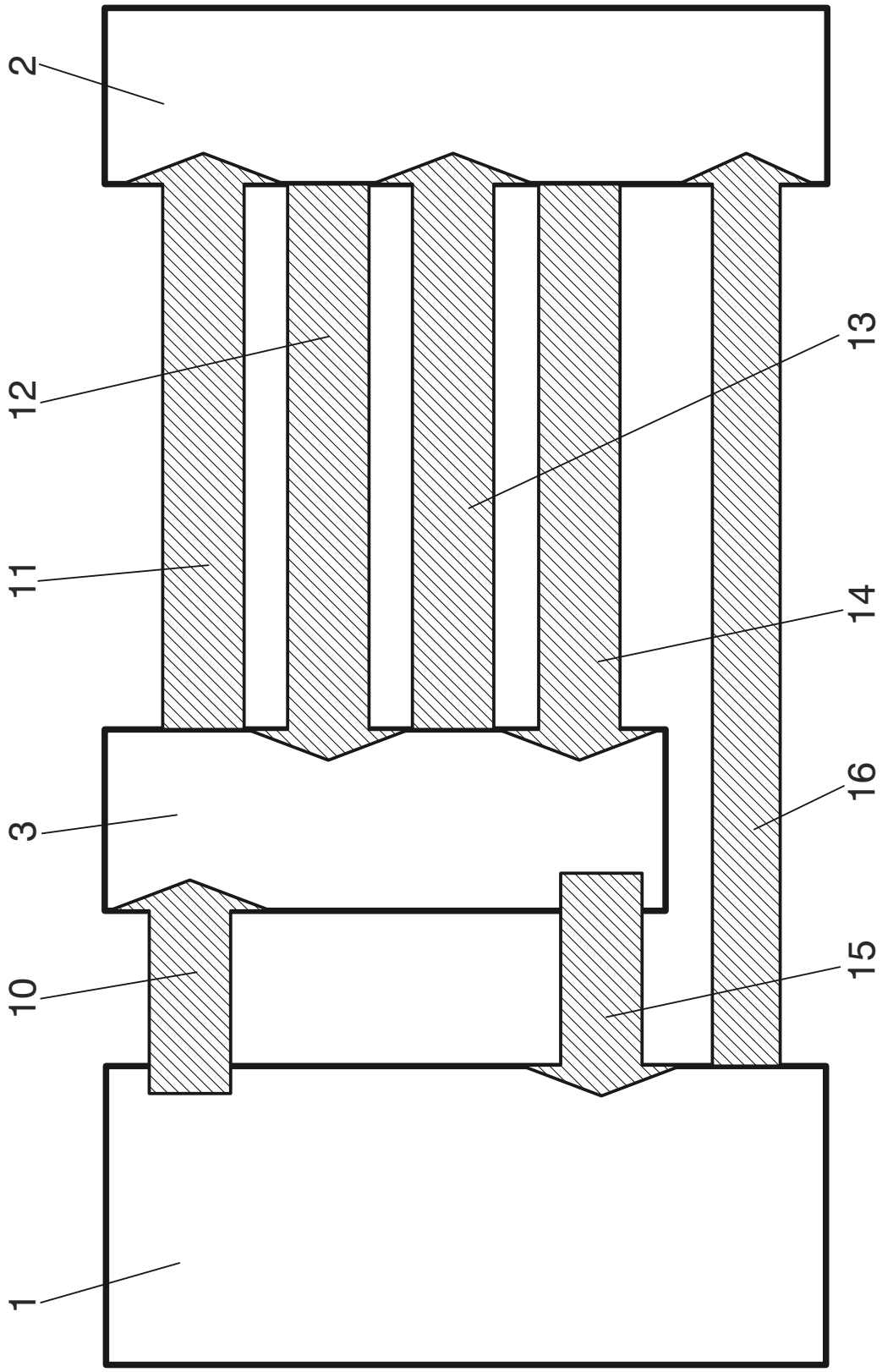


FIG. 1
(ESTADO DE LA TÉCNICA)

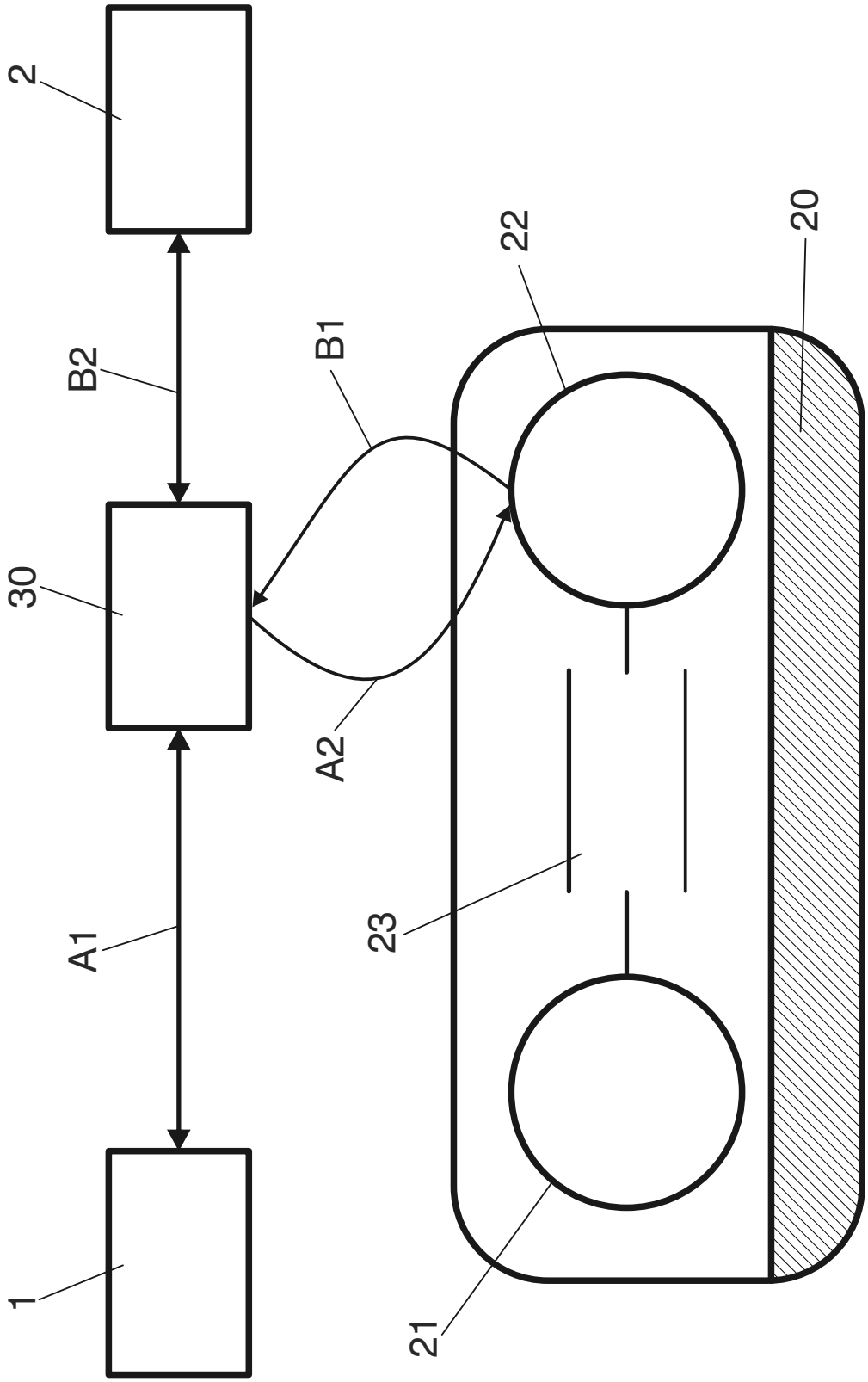


FIG. 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201131968

(22) Fecha de presentación de la solicitud: 05.12.2011

(32) Fecha de prioridad:

# INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

| **Categoría** | (56) **Documentos citados** | **Reivindicaciones afectadas** |
|---|---|---|
| X | US 2011154459 A1 (KUANG RANDY et al.) 23.06.2011, párrafos [100-102],[111],[122],[127-140],[146-154],[197]; reivindicaciones 9,11,18; figuras 2-3,5-7,9-10. | 1-4 |
| Y | | 5-7 |
| Y | US 2007005801 A1 (KUMAR SANDEEP et al.) 04.01.2007, resumen; párrafos [48-51],[55-56],[216],[321],[332],[335]; figuras 3,25A,25B,26. | 5-7 |
| A | US 5586260 A (HU WEI-MING) 17.12.1996, columna 4, líneas 5-17; columna 5, líneas 4-40; reivindicación 1; figuras 1-4. | 1,5 |
| A | ES 2233641 T3 (E PLUS MOBILFUNK GMBH & CO KG) 16.06.2005, figura 1; reivindicación 1. | 1,3 |
| A | US 2009125993 A1 (DELIA WAYNE M et al.) 14.05.2009, párrafos [16],[18],[20-21]; figuras 1-2; reivindicaciones 4-5. | 1,4-5 |
| A | US 2007006299 A1 (ELBURY IAN et al.) 04.01.2007, párrafos [23-24],[27]; figuras 2-6; reivindicaciones 1-2,5,8. | 1 |

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** |
|---|---|---|
| 12.09.2013 | J. M. Vázquez Burgos | 1/6 |

CLASIFICACIÓN OBJETO DE LA SOLICITUD

***H04W12/04*** (2009.01)
***G06F21/31*** (2013.01)
***H04L9/32*** (2006.01)

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

H04W, G06F, 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, INTERNET

Fecha de Realización de la Opinión Escrita: 12.09.2013

**Declaración**

| | | | |
|---|---|---|---|
| **Novedad (Art. 6.1 LP 11/1986)** | Reivindicaciones | 4-7 | **SI** |
| | Reivindicaciones | 1-3 | **NO** |
| **Actividad inventiva (Art. 8.1 LP11/1986)** | Reivindicaciones | | **SI** |
| | Reivindicaciones | 1-7 | **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 | US 2011154459 A1 (KUANG RANDY et al.) | 23.06.2011 |
| D02 | US 2007005801 A1 (KUMAR SANDEEP et al.) | 04.01.2007 |
| D03 | US 5586260 A (HU WEI-MING) | 17.12.1996 |
| D04 | ES 2233641 T3 (E PLUS MOBILFUNK GMBH & CO KG) | 16.06.2005 |
| D05 | US 2009125993 A1 (DELIA WAYNE M et al.) | 14.05.2009 |
| D06 | US 2007006299 A1 (ELBURY IAN et al.) | 04.01.2007 |

**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 divulga un sistema y un procedimiento para el control de credenciales de usuario cuando estas son necesarias para la comunicación entre un servidor de terceras partes y una aplicación del lado del cliente, en una red móvil. El sistema utiliza en primer lugar un administrador de credenciales, que recupera la identidad del usuario definida en la red móvil, y recibe de él las credenciales auténticas para el servidor de terceras partes, junto con otras falsas. En segundo lugar dispone de un repositorio de almacenamiento de credenciales, tanto verdaderas como falsas, asociadas a la identidad del usuario. Comprende también un reemplazador que sustituye las credenciales falsas utilizadas por el cliente, por las auténticas, de manera que el servidor recibe estas últimas. De esta manera, la aplicación cliente puede utilizar credenciales falsas en origen, lo que mejora la seguridad de la conexión, de manera que el sistema consigue que en destino el servidor reciba las verdaderas.

El documento del estado de la técnica más próximo a la invención es D01 y divulga un método y un sistema para las transacciones seguras entre clientes y servidores de aplicaciones, basado en el uso de credenciales locales (asimilables a falsas) que son reemplazadas por las credenciales verdaderas, en un servidor proxy intermedio de seguridad, que las almacena en un repositorio.

Reivindicación 1

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.

Un sistema (figura 5) para controlar credenciales de usuario proporcionadas por un usuario, en una red móvil con una comunicación establecida entre un servidor de terceras partes (120) y una aplicación de lado de cliente (100) que solicita acceso al servidor de terceras partes (120) en nombre del usuario, caracterizado porque comprende:

- Un administrador de credenciales (párrafo 138, 502) que comprende medios para recuperar una identidad del usuario definida de manera inequívoca en la red móvil (reivindicación 9) y medios de acceso a través de los cuales el usuario proporciona credenciales auténticas para su uso en un servicio de terceras partes protegido del servidor de terceras partes (120) y credenciales falsas para su uso por la aplicación de lado de cliente (100),
- Un repositorio de almacenamiento de credenciales (1090, párrafo 122) que es una base de datos en la que el administrador de credenciales almacena tanto las credenciales auténticas como las credenciales falsas en asociación con la identidad recuperada del usuario,
- Un reemplazador de credenciales (502, párrafo 111) que comprende medios de detección de datos (párrafos 151-152) para detectar mensajes de autenticación que contienen credenciales falsas en la comunicación establecida entre la aplicación de lado de cliente (100) y el servidor de terceras partes (120), y medios de reemplazo (1095) para reemplazar, en los mensajes de autenticación detectados para el servicio de terceras partes protegido, las credenciales falsas por las credenciales auténticas almacenadas en asociación con el repositorio de almacenamiento de credenciales (1090).

Por lo tanto a la luz de D01 la invención reivindicada en 1 no es nueva tal como se establece en el artículo 6 de la Ley de Patentes de 1986.

Reivindicación 5

Para mayor claridad, y en la medida de lo posible, se emplea la misma redacción utilizada en la reivindicación 5. Las referencias entre paréntesis corresponden al D01. Las características técnicas que no se encuentran en el documento D01 se indican entre corchetes y en negrita.

Un procedimiento (figuras 6A, 8A, 9A) para controlar credenciales de usuario proporcionadas por un usuario, en una red móvil con una comunicación establecida entre un servidor de terceras partes (120) y una aplicación de lado de cliente (100) que solicita acceso al servidor de terceras partes (120) en nombre del usuario, caracterizado porque comprende:

- recuperar mediante un administrador de credenciales una identidad del usuario definida de manera inequívoca en la red móvil (párrafo 138),
- acceder mediante el usuario identificado al administrador de credenciales (párrafos 115, 138),
- proporcionar (609, párrafos 127-133, 138) mediante el usuario identificado, al administrador de credenciales, credenciales auténticas para su uso en un servicio de terceras partes protegido del servidor de terceras partes (120) y credenciales falsas para su uso por la aplicación de lado de cliente (100),
- almacenar (631, párrafo 138) en un repositorio de almacenamiento de credenciales usado por el administrador de credenciales (502) tanto las credenciales auténticas como las credenciales falsas en asociación con la identidad del usuario recuperada por el administrador de credenciales,
- detectar mensajes de autenticación (párrafo 151), que contienen credenciales falsas en la comunicación establecida entre la aplicación de lado de cliente (100) y el servidor de terceras partes (120), comprobando si se cumplen las condiciones siguientes (párrafo 139): existe una indicación de mensaje de autenticación en los datos, los datos están destinados a un servicio de terceras partes protegido, existen credenciales auténticas almacenadas en el repositorio de almacenamiento de credenciales proporcionadas por el usuario para el servicio de terceras partes protegido, los datos incluyen credenciales falsas proporcionadas por el usuario y también almacenadas en el repositorio de almacenamiento de credenciales para el servicio de terceras partes protegido (párrafo 151);
- reemplazar mediante un reemplazador de credenciales (párrafos 151, 154) las credenciales falsas, en los mensajes de autenticación detectados para el servicio de terceras partes protegido, por las credenciales auténticas que el reemplazador de credenciales (502) obtiene del repositorio de almacenamiento de credenciales y almacenadas en asociación con dichas credenciales falsas.

La principal diferencia entre el procedimiento reivindicado en 5 y el descrito en D01 es que en el segundo es necesario (párrafos 149-150) un registro previo del usuario frente al administrador, paso que no se requiere en 5, ya que se procede simplemente a detectar los mensajes de de autenticación y verificar su contenido. Los principales efectos técnicos de esta diferencia son una mayor complejidad del procedimiento en D01 (por implicar dicho registro adicional), y una menor flexibilidad en la topologías de red aplicables (en D01 el equipo del cliente debe ser el mismo que el del administrador o estar conectado por LAN a él). En este sentido el documento D02 muestra un sistema de gestión de identidades en red, donde un equipo (un router o un switch) intermedia entre un cliente y un servidor de aplicaciones, y que, entre otras funciones, analiza los paquetes intercambiados e identifica los de autenticación (párrafo 321, figuras 25A-25B), verificando si el destino (párrafos 67-68, figura 2) u otros datos que contenga (párrafo 216) son correctos y procesándolos conforme una política preestablecida, que puede incluir el cambio de las credenciales de información (párrafo 332). Teniendo en cuenta el contenido de ambos documentos, se considera que un experto en la materia combinaría el contenido del documento D01 más próximo al estado de la técnica, con los aspectos principales de D02, con el fin de obtener un proceso como el reivindicado en 5 con una expectativa razonable de éxito.

En consecuencia cabe concluir que, a la luz los documentos D01 y D02 tomados en combinación, el contenido de la reivindicación 5 carecería de actividad inventiva tal como se establece en el artículo 8 de la Ley de Patentes de 1986.

Reivindicaciones 2 a 4

La reivindicación 2 particulariza el sistema con un acceso al administrador de credenciales mediante un portal web, mientras que la 3 lo hace vinculando las credenciales al MSISDN del usuario, y la 4 a la verificación de que el mensaje sea de señalización, destinado a un servidor de aplicaciones y a la existencia de claves falsas y verdaderas. Dado que estas tres reivindicaciones se refieren a un sistema (dependen de la 1), sus requisitos deben entenderse en el sentido de que el sistema reivindicado es apto para funcionar conforme se establece en ella.

En el caso de 2, se reivindica un método de acceso muy conocido del estado de la técnica, que está recogido en D01 (párrafos 127-133, 137-138) para el mismo elemento, mientas que en el de 3 cabe razonar de igual manera en cuanto al uso del MSISDN como vínculo de la tabla de claves, pudiendo considerarse que el sistema divulgado en D01 es apto para dicho uso (reivindicación 9), siendo también el documento D04 un ejemplo de vinculación de datos relativos a un usuario con la de su MSISDN.

En cuanto a las condiciones reivindicadas en 4, el sistema descrito en D01 (párrafos 149-152) es apto para verificarlas, y de ello se desprende que un experto en la materia podría utilizar dicho sistema para ello sin el uso de la actividad inventiva.

En consecuencia, teniendo en cuenta las relaciones de dependencia de las reivindicaciones 2 y 3, así como las consideraciones anteriores, cabe concluir que las mismas carecen de novedad tal como se define en el artículo 6 de la Ley de Patentes de 1986.

Asimismo, teniendo en cuenta las relaciones de dependencia de la reivindicación 4, así como las consideraciones anteriores, cabe concluir que ésta carece de actividad inventiva tal como se define en el artículo 8 de la Ley de Patentes de 1986.

Reivindicaciones 6 y 7

Las reivindicaciones 6 y 7 particularizan al procedimiento reivindicado en 5 los mismos requisitos que las reivindicaciones 2 y 3 al sistema reivindicado en 1.

El uso del acceso web al administrador de credenciales se menciona explícitamente en D01 (párrafos 127-133, 137-138), y la vinculación de los datos de usuario al MSISDN se puede considerar implícita en D01 por cuanto (reivindicación 9), se incluye la posibilidad de que la identidad del usuario que identifica su perfil sea la correspondiente a un teléfono celular o un Smartphone, lo que puede incluir el MSISDN.

Por lo tanto, teniendo en cuenta las relaciones de dependencia de las reivindicaciones 6 y 7, así como las consideraciones anteriores, cabe concluir que ambas carecen de actividad inventiva, tal y como se definen en el artículo 8 de la Ley de Patentes de 1986.