(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
14 de julio de 2016 (14.07.2016)

WIPO | PCT

(10) Número de Publicación Internacional
WO 2016/110601 A1

(51) Clasificación Internacional de Patentes:
H04W 12/06 (2009.01) *G06F 21/44* (2013.01)
G06F 21/33 (2013.01)

(21) Número de la solicitud internacional:
PCT/ES2015/070001

(22) Fecha de presentación internacional:
5 de enero de 2015 (05.01.2015)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(71) Solicitante: **EBIID,PRODUCTS & SOLUTIONS, S.L.** [ES/ES]; Av. de la Torre Blanca, 57, Edificio ESADECREAPOLIS - 1B13, 08173 Sant Cugat del Vallès, Barcelona (ES).

(72) Inventores: **MASÍAS, Jordi**; Av. de la Torre Blanca, 57, Edificio ESADECREAPOLIS - 1B13, 08173 Sant Cugat del Vallès, Barcelona (ES). **TARRÉS, Xavier**; Av. de la Torre Blanca, 57, Edificio ESADECREAPOLIS - 1B13, 08173 Sant Cugat del Vallès, Barcelona (ES). **OLIVET, Roger**; Av. de la Torre Blanca, 57, Edificio Esadecreapolis - 1B13, 08173 Sant Cugat del Vallès, Barcelona (ES).

(74) Mandatario: **VALLEJO LÓPEZ, Juan Pedro**; Paseo de la Castellana 93, 28046 Madrid (ES).

(81) Estados designados *(a menos que se indique otra cosa, para toda clase de protección nacional admisible)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Estados designados *(a menos que se indique otra cosa, para toda clase de protección regional admisible)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, RU, TJ, TM), europea (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continúa en la página siguiente]

(54) Title: METHOD FOR GENERATING A DIGITAL IDENTITY FOR A USER OF A MOBILE DEVICE, DIGITAL USER IDENTITY, AND AUTHENTICATION METHOD USING SAID DIGITAL USER IDENTITY

(54) Título : PROCEDIMIENTO DE GENERACIÓN DE UNA IDENTIDAD DIGITAL DE UN USUARIO DE UN DISPOSITIVO MÓVIL, IDENTIDAD DIGITAL DE USUARIO, Y PROCEDIMIENTO DE AUTENTICACIÓN USANDO DICHA IDENTIDAD DIGITAL DE USUARIO

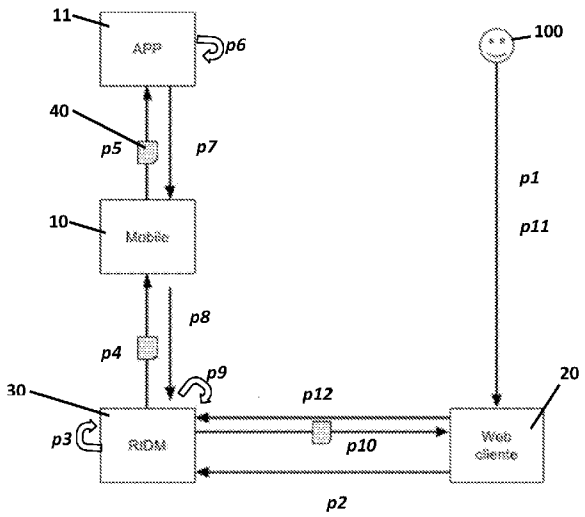

FIG. 2

20 Web client

(57) Abstract: The invention relates to a method for generating a digital identity for a user (100) of a mobile device (10), based on a digital certificate generated by a certification authority. A first mobile identification number (MSISDN) is associated with the mobile device (10). The user has access to an executable application (11) installed on the mobile device or on a second device that can run the application, which: contains a key-containing element that can store at least one public key and a private key associated with said first mobile identification number; has a unique application identifier associated therewith; and includes a connection logic with a mobile identity server (30). The method comprises a series of steps wherein the mobile digital identity of the user is generated from the first mobile identity number (MSISDN), the digital certificate of said user and the unique application identifier. The invention also relates to the digital identity generated for a user (100), to a method for the authentication of a user using said digital identity, and to an application (11) that can be installed on a mobile device (10) or on a second device that can run said application, in order to generate a digital identity for a user (100) of said mobile device (10).

(57) Resumen:

[Continúa en la página siguiente]

WO 2016/110601 A1

Publicada:

— *con informe de búsqueda internacional (Art. 21(3))*

La invención se refiere a un procedimiento de generación de una identidad digital de un usuario (100) de un dispositivo móvil (10), basada en un certificado digital generado por una autoridad de certificación. El dispositivo móvil (10) tiene asociado un primer número e identificación móvil (MSISDN). El usuario tiene acceso a una aplicación (11) ejecutable instalada en el dispositivo móvil o en un segundo dispositivo capaz de ejecutar la aplicación, que: - contiene un contenedor de claves capaz de almacenar al menos una clave pública y una clave privada asociadas a dicho primer número de identificación móvil; - tiene asociado un identificador único de aplicación; e - incluye una lógica de conexión con un servidor de identidades móviles (30). El procedimiento comprende una serie de etapas en la que se genera la identidad digital móvil del usuario a partir del primer número de identidad móvil (MSISDN), del certificado digital de dicho usuario y del identificador único de aplicación. La invención también se refiere a la identidad digital de un usuario (100) generada, a un procedimiento de autenticación de un usuario que utiliza dicha identidad digital. Y a una aplicación (11) instalable en un dispositivo móvil (10) o en un segundo dispositivo capaz de ejecutar dicha aplicación, para generar una identidad digital de un usuario (100) de dicho dispositivo móvil (10).

Procedimiento de generación de una identidad digital de un usuario de un dispositivo móvil, identidad digital de usuario, y procedimiento de autenticación usando dicha identidad digital de usuario

DESCRIPCIÓN

Objeto de la invención

La presente invención se engloba dentro de los sistemas de autenticación entre dos partes, siendo una de ellas un usuario de un equipo móvil, basado en tecnología PKI (*Public Key Infrastructure)* y con certificados electrónicos, con independencia de la Autoridad de Certificación y del Operador de telefonía.

Antecedentes de la invención

En general, el objetivo principal de un sistema de autenticación es poder verificar la veracidad la identidad de un usuario que pretende acceder a un sistema remoto o verificar la autoría de un acto.

Para ello se pueden utilizar distintos elementos o factores de autenticación: algo que se tiene (tarjeta, teléfono, línea de teléfono móvil,...); algo que se sabe (contraseña, PIN, clave de un único uso u OTP (One Time Password)); o alguna característica biométrica del usuario (iris, voz, huella dactilar,…)

En ciertos sistemas, uno solo de los factores no es suficiente para garantizar la identidad, es por ello que se en algunos sistema se utiliza la combinación de dos de esos factores. Se suele hablar entonces de sistemas de autenticación fuerte o dual.

La parte que solicita la autenticación suele ser una aplicación online, a la que se accede desde un navegador, mediante una aplicación o físicamente. Por ahora la mayoría de sistemas utilizan un solo factor de autenticación, que suele ser una clave o contraseña, que ellos mismos se encargan de validar, o incluso delegan la tarea de verificación de la autenticación a terceras partes (p.ej. Facebook connect, OAuth…).

Para incrementar la seguridad y mitigar el riesgo de compromiso de la contraseña, algunos

sistemas implementan un segundo factor, y para ello se acostumbra a combinar el uso de algo que el usuario sabe (PIN o contraseña) con algo que el usuario tiene, que es único y muy difícil de replicar. Este segundo factor suele ser un dispositivo físico que sólo el usuario tiene y que permite garantizar al sistema que solicita la autenticación que el usuario identificado dispone de ese dispositivo en el preciso momento que está solicitando la autenticación (por ej., mediante llamada al móvil garantizando la posesión de la tarjeta SIM; envío de una clave de un único uso vía SMS o una aplicación generadora de OTPs).

En los casos en los que la autenticación del usuario se realiza sobre una red o un canal diferente a la red o canal principal ("out-of-band"), existe el riesgo de recibir un ataque man-in-the-middle. El atacante puede hacer creer al usuario que está accediendo a un sitio legítimo, e iniciar el proceso de autenticación out-of-band al que el usuario responderá, creyendo que la operación la ha solicitado él realmente.

Este riesgo se puede mitigar utilizando sistemas de autenticación mutua, es decir, que el cliente pueda verificar la identidad del sitio donde se conecta (gracias a certificados SSL por ejemplo).

En el caso de transacciones que requieran una autorización, el sistema Mobile Signature que utiliza claves criptográficas asimétricas proporciona ventajas interesantes, ya que mitiga el riesgo inherente de un sistema de autenticación out-of-band, dado que el sistema exige que el sitio legítimo mande al usuario un resumen de la operación que va a autorizar. El usuario pues sabe siempre qué está a punto de autorizar.

Este sistema Mobile Signature se basa en el uso de certificados digitales como sistema de autenticación. El uso de una clave privada protegida por un PIN, generada y almacenada en un dispositivo móvil, permite a terceras aplicaciones verificar la identidad del solicitante, que ha sido certificada anteriormente por una Autoridad de Certificación.

La arquitectura de un sistema Mobile Signature consiste básicamente en tres partes: 1) el usuario, que intenta acceder al sistema del 2) cliente que solicita la autenticación del usuario al 3) sistema de registro y autenticación, quien se encarga de mantener un registro de los usuarios y de las identidades registradas, y a su vez de establecer un canal seguro entre el cliente y el usuario durante el proceso de autenticación.

Para que un usuario pueda autenticarse ante un cliente utilizando un sistema Mobile Signature es necesario que 1) el usuario haya generado sus claves (pública y privada) en el dispositivo móvil, 2) haya habido un registro de la identidad del usuario asociándola a sus claves, 3) el cliente haya formalizado la interconexión de su sistema con el sistema de registro y autenticación.

Sin embargo, la tecnología del Mobile Signature requiere el uso de SIMs criptográficas, no existentes masivamente en la actualidad, lo que imposibilita ponerlo en marcha de forma totalmente interoperable entre los distintos operadores de telefonía móvil. Tanto la aplicación de gestión de las claves (embebida dentro de la tarjeta), como el sistema de registro y autenticación son gestionados por el operador, lo que dificulta un despliegue masivo y, por consiguiente, la escalabilidad de la solución puesto que añade una dependencia de hardware y de red con el operador.

Teniendo en cuenta los factores mencionados, existe en el estado de la técnica la necesidad de un sistema y método de autenticación en redes inalámbricas que sea seguro y no dependa del hardware del dispositivo móvil o del operador de telefonía móvil.

Descripción de la invención

La presente invención soluciona los problemas anteriormente descritos mediante un sistema distribuido de generación de identidad digital, estando esta identidad digital asociada al dispositivo móvil en el que se crean unas claves a través de una aplicación móvil.

Un primer aspecto de la invención se refiere a un procedimiento de generación de una identidad digital de un usuario de un dispositivo móvil, estando la identidad digital del usuario basada en un certificado digital generado por una autoridad de certificación, en donde el dispositivo móvil tiene asociado un primer número de identificación móvil (por ej., MSISDN);

teniendo el usuario acceso a una aplicación ejecutable instalada bien en el dispositivo móvil o bien en un segundo dispositivo capaz de ejecutar la aplicación, que:

- contiene un contenedor de claves capaz de almacenar al menos una clave pública y una clave privada asociadas a dicho primer número de identificación móvil;
- tiene asociado un identificador único de aplicación; e

- incluye una lógica de conexión con un servidor de identidades móviles;

comprendiendo el procedimiento:

- inicializar el contenedor de claves;
- verificar frente al servidor de identidades móviles el número de identificación móvil;
- crear el servidor de identidades móviles un código único de activación;
- generar dicha aplicación una solicitud de creación de la identidad digital de dicho usuario formada por dicho primer número de identificación móvil (MSISDN), por una clave pública y por una clave privada;
- generar la autoridad de certificación el certificado digital de dicho usuario a partir de dicho primer número de identificación móvil y de la clave pública, en respuesta a introducir en la aplicación dicho código único de activación; y
- generar la identidad digital móvil del usuario a partir del primer número de identidad móvil (MSISDN), del certificado digital de dicho usuario y del identificador único de aplicación.

Es decir, de acuerdo con la invención es posible tener instalada la aplicación en un segundo dispositivo, como por ejemplo una Tablet, u otro dispositivo inteligente diferente del dispositivo móvil al que está asociado el primer número de identificación móvil. La identidad digital móvil del usuario estará asociada a dicho primer número de identificación móvil, pero residirá en la aplicación que está en el segundo dispositivo.

En cualquier caso es importante señalar que el certificado y la identidad digital generada residen en la aplicación, no en la tarjeta SIM del dispositivo móvil, por lo que la invención da libertad al usuario al no depender de requerimientos del operador de telefonía móvil.

El procedimiento preferiblemente además comprende una etapa previa de registro el usuario del dispositivo móvil que comprende:

i) enviar desde el dispositivo móvil una solicitud de registro de dicho primer número de identificación móvil al servidor de identidades móviles;

ii) verificar que dicho primer número de identificación móvil no está ya contenido en el servidor de identidades móviles; y,

iii) enviar el servidor de identidades móviles al dispositivo móvil un código aleatorio que es introducido en la aplicación del móvil para confirmar dicho registro.

El procedimiento de la invención preferiblemente además comprende informar al servidor de identidades móviles de la identidad digital creada para ese primer número de identidad móvil dicho identificador único de aplicación.

De acuerdo con un segundo aspecto de la invención, ésta se refiere a una identidad digital de un usuario de un dispositivo móvil, teniendo el dispositivo móvil asociado un primer número de identificación móvil (como puede ser el MSISDN) y teniendo el usuario acceso a una aplicación ejecutable instalada en dicho dispositivo móvil o en un segundo dispositivo capaz de ejecutar la aplicación. La identidad digital es generada por y reside en la aplicación móvil, y se descarga en dicho dispositivo móvil o en dicho segundo dispositivo capaz de ejecutar la aplicación, y comprende el primer número de identidad móvil, un certificado digital de dicho usuario generado por una autoridad de certificación, y un identificador único de dicha aplicación.

Como se ha indicado antes, al no residir en la tarjeta SIM se consigue independencia respecto al operador de telefonía móvil. El hecho que no exista una dependencia tecnológica con un operador en concreto que provea la SIM ni con una única autoridad de certificación, garantiza la elección del usuario, siendo un claro hecho diferenciador.

La identidad digital además puede comprender datos adicionales relacionados con la identidad del usuario, como puede ser nombre, apellidos, dirección postal y/o de correo electrónico, etc.

La invención también se refiere a un procedimiento de autenticación de un usuario de un dispositivo móvil frente a un servidor de un cliente a través de un servidor de identidades móviles, comprendiendo el procedimiento:

- que el usuario del dispositivo móvil presente una identidad digital del usuario generada según ha sido definido en lo anterior; y
- que dicho servidor de identidades móviles verifique esta identidad digital del usuario.

Con esa identidad digital móvil el usuario puede firmar documentos y transacciones con plena garantía jurídica.

El proceso de firma de documentos puede ser llevado a cabo *on-line,* en caso de haber

conexión con el servidor de identidades móviles, o en *off-line*, si por ejemplo en ese momento no hay cobertura, realizándose la firma en un entorno sin conexión al exterior gracias a la aplicación instalada y residente en el dispositivo móvil (o en su caso, en el segundo dispositivo del usuario en el que tenga instalada la aplicación).

Este aspecto que proporciona el procedimiento de autenticación de la invención de poder autenticar al usuario, y firmar documentos o realizar trámites tanto online como offline es muy importante pues el usuario no siempre tiene una buena cobertura en su dispositivo móvil.

De esta forma, el procedimiento de la invención permite realizar trámites, firmar documentos y acceder a otros servicios sin conexión, y que posteriormente se sincronicen de forma automática con el servidor cuando se recupere la conexión, sin intervención y de forma transparente para el usuario,

Finalmente la invención también se refiere a una aplicación instalable en un dispositivo móvil o en un segundo dispositivo con capacidad para ejecutar dicha aplicación, para generar una identidad digital de un usuario de dicho dispositivo móvil, teniendo asociado el dispositivo móvil un primer número de identificación móvil. La aplicación:

- tiene medios para conectarse con un contenedor de claves –residente en el dispositivo móvil– que puede almacenar al menos una clave pública y una clave privada asociadas a dicho primer número de identificación móvil;
- tiene asociado un identificador único de aplicación; e
- incluye una lógica de conexión con un servidor de identidades móviles;

y la aplicación está configurada para generar la identidad digital móvil del usuario a partir del primer número de identidad móvil, de un certificado digital de dicho usuario generado por una autoridad de certificación y del identificador único de aplicación.

La aplicación es descargable preferiblemente desde una plataforma de aplicaciones segura, esto es, que garantice la integridad de las aplicaciones en el momento de ser instaladas en los dispositivos.

De esta forma la invención permite generar –y, de acuerdo con las realizaciones preferidas de la invención, preferiblemente también gestionar– una identidad digital del usuario en su

dispositivo móvil, o identidad digital móvil.

Con esta identidad digital móvil el usuario puede acceder a una serie de productos o servicios ofrecidos por un cliente, tras un proceso de autenticación de dicha identidad digital móvil, con las mismas garantías jurídicas que si el usuario accediera a través de la autentificación con certificado digital de persona física.

Así, de acuerdo con la invención, esta identidad digital generada e instalada en el dispositivo del usuario puede servir para múltiples registros y servicios y no va vinculada a un único servicio ni a una autoridad de certificación, soportando todos los certificados estándar de mercado reconocidos.

Los diferentes aspectos y realizaciones de la invención definidos en los párrafos anteriores pueden combinarse entre sí, siempre y cuando sean compatibles.

Otras ventajas y características adicionales de la invención serán evidentes de la descripción detallada que sigue y serán particularmente señaladas en las reivindicaciones adjuntas.

Descripción de las figuras

Con objeto de ayudar a una mejor comprensión de las características de la invención de acuerdo con un ejemplo preferente de realización práctica de la misma, y para complementar esta descripción, se acompañan como parte integrante de la misma las siguientes figuras, cuyo carácter es ilustrativo y no limitativo:

La Figura 1 muestra un esquema de los elementos principales que intervienen en el sistema de la invención de acuerdo una implementación particular del mismo.

La Figura 2 muestra un esquema del intercambio de mensajes realizados entre los diferentes elementos del sistema para llevar a cabo la autenticación.

Realización preferente de la invención

De acuerdo con la invención, la autenticación se realiza a través de un sistema de gestión de identidades basado en certificados digitales que se distribuye a partir de aplicaciones instaladas en el dispositivo móvil inteligente o Smartphone de un usuario.

La solución propuesta utiliza el propio dispositivo móvil del usuario como dispositivo de custodia del certificado, minimizando los costes, y facilitando el uso.

Como se muestra en la Figura 1, el sistema está formado principalmente por tres elementos:

- un usuario 100 que tiene un teléfono móvil o smartphone 10 en el que está instalada una aplicación 11 móvil;
- un servidor 20 de un cliente (o "Relying Party") en el que el usuario quiere autenticarse; y,
- un servidor 30 de registro y autenticación de identidades móviles, RIDM.

A diferencia de Mobile Signature, la aplicación 11 instalada en el Smartphone 10 del usuario es distribuida a través de plataformas de aplicaciones como Google Play o Apple AppStore, plataformas que de por sí garantizan el origen (autenticidad) e integridad (las aplicaciones van firmadas digitalmente por el editor) del software que se instala en los dispositivos móviles. Embebida dentro esta aplicación está la lógica de conexión con el servidor RIDM 30, así como con un contenedor de claves asimétricas –pública y privada– y del certificado digital que genere la aplicación.

El servidor de registro y autenticación de identidades digitales móviles está basado en una infraestructura de clave pública (PKI, en inglés), es decir, una entidad vinculada a una Autoridad de Certificación habilitada a gestionar la verificación de identidades para la emisión de certificados digitales.

La identidad digital móvil se constituye a partir del número de teléfono móvil, el MSISDN, un número de identidad del usuario, como por ej., puede ser su DNI, más un identificador único asociado a cada aplicación. Opcionalmente la identidad digital móvil del usuario puede incluir otros datos asociados a la identidad del usuario como son el nombre, apellidos y/o dirección de correo electrónico del usuario.

Adicionalmente a los datos propios de la identidad del usuario, el servidor RIDM 30 se

encarga de registrar el número de móvil del usuario con el objetivo de poder verificar el número de teléfono móvil MSISDN. Para ello, como primer paso en el proceso de registro, la aplicación móvil realiza una solicitud de alta para el número de teléfono móvil MSISDN al servidor RIDM 30 enviándose para ello el número de teléfono móvil MSISDN.

Al recibir la petición, el servidor RIDM 30 comprueba que el número de teléfono móvil MSISDN recibido no está registrado, o que la identidad asociada a ese número no se encuentra en un estado activo, y genera un código aleatorio (por ej., de 5 dígitos) que envía por SMS al número de teléfono móvil proporcionado, y cuyo hash (SHA1) almacena. Al recibir el SMS con el código aleatorio, éste debe ser introducido en la aplicación móvil para indicar al servidor RIDM 30 que el proceso de registro se ha realizado correctamente. Para ello, al recibir el código, el servidor RIMD 30 verifica si el código recibido coincide con el código enviado previamente.

En el caso de una Tablet, igualmente puede registrarse el usuario recibiendo el SMS en un teléfono móvil, e introducirse seguidamente en la aplicación que se encuentra instalada en la Tablet para verificar la posesión de la línea de teléfono de ese número de teléfono móvil MSISDN.

Una vez realizado el registro del MSISDN, la aplicación 11 lleva a cabo el proceso de creación de una identidad digital para el usuario.

En primer lugar, el usuario comunica al servidor RIDM sus datos identificativos (por ej: nombre, apellidos, DNI, email) pudiendo utilizar para ello la aplicación 11 u otros medios no automatizados (email, introducción manual), y una vez dichos datos registrados el servidor RIDM 30 genera un código único de activación. Este código único de activación debe ser comunicado al usuario mediante algún tipo de canal *out-of-band*, por ejemplo, por correo o entregado en mano. Este código único de activación debe ser introducido por el usuario en la aplicación 11 móvil. Al ser introducido el código de activación en la aplicación, ésta procede a mandarlo al servidor RIDM para verificar que coincide con el mandado inicialmente y que corresponde con la identidad del usuario.

El siguiente paso se inicia con la respuesta positiva del servidor RIDM 30 a la aplicación 11. Se inicializa entonces el contenedor de las claves utilizando para ello un contenedor PKCS#12, que está protegido por un PIN definido por el usuario; y se generan un par de

claves asimétricas: una clave privada y una clave pública.

Seguidamente, estas claves son utilizadas por la aplicación para generar una solicitud de creación de certificado (Certificate Signing Request) en formato PKCS#10, que es enviado al servidor RIDM. El RIDM usa la información contenida en el PKCS#10 (solicitud de emisión de certificado digital no sellado) para completar el registro de la identidad digital móvil del usuario. Una vez el registro actualizado, el RIDM manda la solicitud de creación de certificado CSR a la autoridad de certificación CA para que lo firme y se emita así el certificado. Una vez emitido, el certificado se manda de vuelta al RIDM que a su vez lo entrega a la aplicación del usuario mediante un mensaje PUSH. Es decir, el certificado digital no se guarda en el servidor RIDM sino en la aplicación, por lo que, pueden generarse firmas electrónicas y realizarse el proceso de autenticación sin necesidad de estar conectado al RIDM.

Además, mediante esta gestión de la comunicación con el servidor mediante tecnología PUSH se evitan costes para el usuario que conllevan otro tipo de mensajes, como, por ej., los SMSs.

La aplicación, y en concreto una parte de la aplicación dedicada exclusivamente a tal efecto dentro del mecanismo para ejecutar programas con seguridad y de manera separada (conocido como *Sandbox*), custodia el par de claves y el certificado, y por tanto, la aplicación es capaz de realizar operaciones criptográficas sin necesidad de disponer de conexión a internet.

En el momento en el que un usuario intenta acceder a un servidor remoto de un cliente 20 que requiere autenticación previa (paso p1), se inicia un proceso de autenticación.

Para ello, como se muestra en la Figura 2, el servidor del cliente 20 solicita al servidor RIDM 30 la verificación de la identidad digital que el usuario ha presentado (paso p2). El servidor RIDM 30 verifica si la identidad digital para ese número de teléfono móvil MSISDN ha sido creada (paso p3). El servidor RIDM 30, utilizando sistemas de notificación de las plataformas de aplicaciones (tales como 'GCM' Google Cloud Manager o 'APN' Apple Push Notifications) manda una notificación a la aplicación 11 (paso p4). Cada aplicación tiene un identificador único de aplicación que se comunica la primera vez que la aplicación contacta con el servidor RIDM 30. Este hecho posibilita la convivencia de distintos sistemas y diferentes aplicaciones para un mismo usuario. Gracias a este identificador único el

servidor RIDM 30 puede mandarle mensajes PUSH a la aplicación. Si la identidad digital para ese número de teléfono móvil MSISDN ha sido creada, envía una notificación PUSH (paso p5) a la aplicación 11 del usuario. En esta notificación envía un token 40 generado con datos aleatorios e información relativa al proceso que se quiere autenticar (un mensaje, el número de teléfono y el tipo de operación).

La aplicación 11 del usuario recibe la notificación de autenticación y solicita al usuario introducir el PIN que protege su clave privada para firmar el token recibido (paso p6). Se podría utilizar el reconocimiento biométrico como alternativa al PIN para aquellos dispositivos móviles o smartphones que lo soporten. Una vez firmado digitalmente mediante la clave privada del certificado digital contenido en el móvil (paso p7), la aplicación 11 instalada en el móvil devuelve el token firmado digitalmente –por ej., utilizando como protocolo de transporte un servicio web (SOAP) sobre https– al servidor RIDM (paso p8), que procede a verificar la firma realizada (paso p9) y a notificar al sitio remoto del cliente (paso p10) que la autenticación se ha realizado exitosamente. El usuario 100 expresa su deseo de continuar con la ejecución de la transacción para la cual ha sido autenticado (paso p11), y el servidor 20 del cliente autoriza la transacción correspondiente (paso p12).

El servidor 20 genera una serie de evidencias que se centran alrededor de un "*ticket*" como unidad de información. Una vez se ha finalizado todo el proceso de autenticación, el ticket es firmado y se le añade un sello de tiempo. El sistema custodia estas evidencias. De acuerdo con lo manifestado en el reglamento europeo No. 910/2014 el tercero de confianza deberá proveer y custodiar estas evidencias dentro de un entorno confiable.

El sistema descrito en lo anterior puede ser usado para firmar digitalmente cualquier documento electrónico. El proceso de firma digital se realiza análogamente al proceso de autenticación, enviándose en lugar del token, el hash (un 'resumen' de longitud fija del documento, por ej. SHA-1) del documento a firmar, una URL con una imagen renderizada del documento a firmar y otra URL con el documento original a firmar. El usuario puede pues verificar visualmente en su terminal móvil cuáles son los datos que va a firmar digitalmente. A diferencia de un sistema Mobile Signature, en el que la capacidad del canal es limitada por diseño, el uso de canales de alta capacidad de los dispositivos móviles tipo *smartphone* (como 3G, 4G, WiFi...) permite adjuntar datos como un documento entero o imágenes que servirán al usuario poder comprobar los datos a firmar.

El actor que lanza el acto de firma puede elegir en que formato quiere que se realice la acción, PADES, XADES y otros formatos que puedan venir en el futuro, dada la capacidad de ampliación del módulo encargado de la gestión de firma electrónica.

El sistema de la presente invención permite también añadir la funcionalidad de autenticación directamente en las aplicaciones (app) de clientes que se distribuyen y se instalan en los dispositivos móviles mediante el uso de librerías. El proceso de autenticación se realiza directamente entonces en local, en el dispositivo móvil que contiene las dos aplicaciones.

Mediante el procedimiento y sistema de la presente invención el usuario puede identificarse remotamente de forma segura a través de la identidad digital residente en su aplicación, cuya aplicación puede estar instalada en el propio dispositivo móvil que proporciona el MSISDN o en otro dispositivo inteligente –como una tablet o similar– al que también tiene acceso el usuario de la identidad digital. El servidor o registro de identidades digitales móviles RIDM asocia el número de teléfono móvil de cada usuario a datos específicos de dicho usuario (por ej., a través de su certificado digital), disponiendo así cada usuario de una identidad o acreditación digital móvil.

Cualquier usuario que tenga un dispositivo móvil inteligente o smartphone conectado a internet, sea con línea de datos o a través de Wi-Fi puede solicitar, crear y utilizar su identidad digital a través de la aplicación de la invención, que puede ser compatible con iPhone, Android y Windows Phone.

Como se puede desprender de lo descrito, la invención tiene como principal campo de aplicación aquel en el que se precise un "uso seguro de servicios electrónicos", con vocación de que cualquier prestador de servicios telemáticos pueda consumir esta identidad digital móvil de forma abierta desde la nube; igualmente, en aquellos servicio en los que se requiera "privacidad" ya que se garantiza al usuario capacidad de acceso y firma electrónica de un nivel equivalente a la firma avanzada basada en certificado reconocido, según la Ley de Firma Electrónica de España y Directiva Europea de Firma Electrónica.

A la vista de esta descripción y figuras, el experto en la materia podrá entender que la

invención ha sido descrita según algunas realizaciones preferentes de la misma, pero que múltiples variaciones pueden ser introducidas en dichas realizaciones preferentes, sin salir del objeto de la invención tal y como ha sido reivindicada.

En este texto, el término "comprende" y sus derivaciones (como "comprendiendo", etc.) no deben entenderse en un sentido excluyente. Es decir, estos términos no deben interpretarse como excluyentes de la posibilidad de que lo que se describe y define pueda incluir más elementos, etapas, etc.

REIVINDICACIONES

1. Un procedimiento de generación de una identidad digital de un usuario (100) de un dispositivo móvil (10), basada en un certificado digital generado por una autoridad de certificación, en donde el dispositivo móvil (10) tiene asociado un primer número de identificación móvil (MSISDN); y, teniendo el usuario acceso a una aplicación (11) ejecutable instalada bien en el dispositivo móvil o bien en un segundo dispositivo capaz de ejecutar la aplicación, que:

- contiene un contenedor de claves capaz de almacenar al menos una clave pública y una clave privada asociadas a dicho primer número de identificación móvil;
- tiene asociado un identificador único de aplicación; e
- incluye una lógica de conexión con un servidor de identidades móviles (30);

comprendiendo el procedimiento:

- inicializar el contenedor de claves;
- verificar frente al servidor de identidades móviles (30) que dicho número de identificación móvil (MSISDN) no ya tiene asociada una identidad digital;
- crear el servidor de identidades móviles (30) un código único de activación;
- generar dicha aplicación (11) una solicitud de creación de la identidad digital de dicho usuario formada por dicho primer número de identificación móvil (MSISDN), por una clave pública y por una clave privada;
- generar la autoridad de certificación el certificado digital de dicho usuario a partir de dicho primer número de identificación móvil y de la clave pública, en respuesta a introducir en la aplicación (11) dicho código único de activación; y
- generar la identidad digital móvil del usuario a partir del primer número de identidad móvil (MSISDN), del certificado digital de dicho usuario y del identificador único de aplicación.

2. Procedimiento según la reivindicación 1, que además comprende una etapa previa de registro del usuario del dispositivo móvil (10) que comprende:

i) enviar desde el dispositivo móvil (10) una solicitud de registro de dicho primer número de identificación móvil (MSISDN) al servidor de identidades móviles (30);

ii) verificar que dicho primer número de identificación móvil no está ya contenido en el servidor de identidades móviles (30);

iii) enviar el servidor de identidades móviles (30) al dispositivo móvil (10) un código

aleatorio que es introducido en la aplicación del móvil para confirmar dicho registro.

3. Procedimiento según cualquiera de las reivindicación 1-2, que además comprende informar al servidor de identidades móviles (30) de la identidad digital creada para ese primer número de identidad móvil (MSISDN) y dicho identificador único de aplicación.

4. Procedimiento según cualquiera de las reivindicaciones 1-3, en el que dicha aplicación (11) es descargable desde una plataforma de aplicaciones segura.

5. Identidad digital de un usuario (100) de un dispositivo móvil (10), teniendo el dispositivo móvil (10) asociado un primer número de identificación móvil (MSISDN) y teniendo el usuario acceso a una aplicación (11) ejecutable instalada en dicho dispositivo móvil o en un segundo dispositivo capaz de ejecutar la aplicación;
en donde la identidad digital está caracterizada por que es generada por la aplicación (11) y reside en la aplicación, y se descarga en dicho dispositivo móvil o en dicho segundo dispositivo capaz de ejecutar la aplicación, y comprende:

- el primer número de identidad móvil (MSISDN),
- un certificado digital de dicho usuario (100) generado por una autoridad de certificación, y
- un identificador único de dicha aplicación (11).

6. Identidad digital según la reivindicación 5, que además comprende datos adicionales relacionados con la identidad del usuario (100).

7. Procedimiento de autenticación de un usuario (100) de un dispositivo móvil (10) frente a un servidor (20) de un cliente a través de un servidor de identidades móviles (30), que comprende:

- presentar el usuario (100) del dispositivo móvil (10) una identidad digital generada de acuerdo con una de las reivindicaciones 5-6; y
- verificar dicho servidor de identidades móviles (30) la identidad digital del usuario (100).

8. Una aplicación (11) instalable en un dispositivo móvil (10) o en un segundo dispositivo capaz de ejecutar dicha aplicación, para generar una identidad digital de un usuario (100) de dicho dispositivo móvil (10), teniendo asociado el dispositivo móvil (10) un primer

número de identificación móvil (MSISDN);

estando la aplicación (11) caracterizada por que:

- tiene medios para conectarse con un contenedor de claves capaz de almacenar al menos una clave pública y una clave privada asociadas a dicho primer número de identificación móvil;

- tiene asociado un identificador único de aplicación; e

- incluye una lógica de conexión con un servidor de identidades móviles (30);

y estando la aplicación (11) configurada para:

- generar la identidad digital móvil del usuario a partir del primer número de identidad móvil (MSISDN), de un certificado digital de dicho usuario generado por una autoridad de certificación y del identificador único de aplicación.

1/1

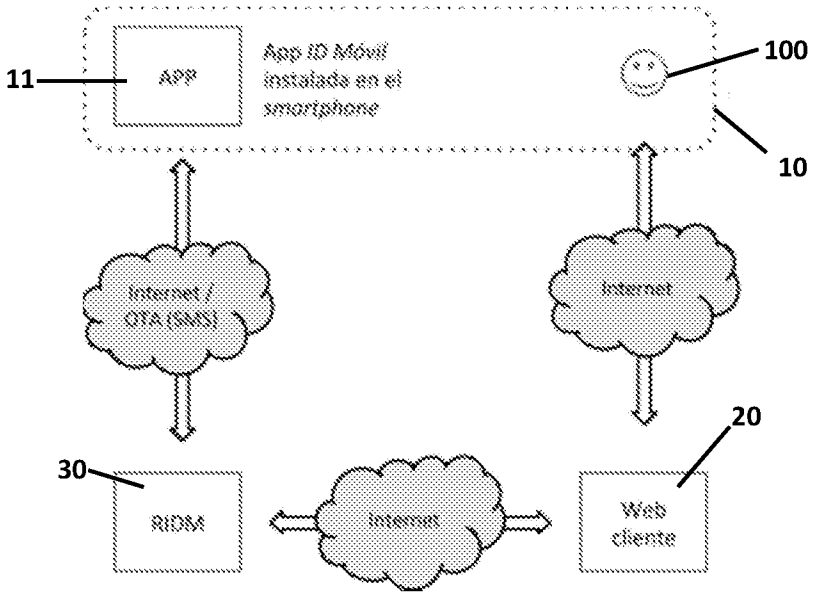
11
APP
App ID Móvil instalada en el smartphone
100
10
Internet / OTA (SMS)
Internet
20
30
RIDM
Internet
Web cliente

FIG. 1

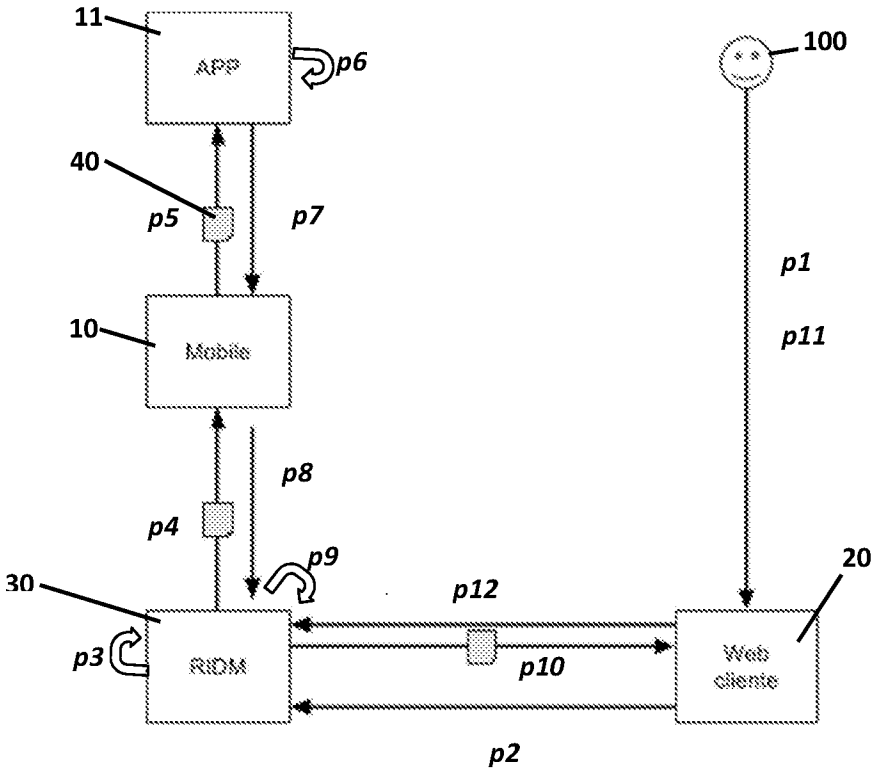
11
APP
p6
100
40
p5
p7
p1
p11
10
Mobile
p8
p4
p9
20
30
p12
p3
RIDM
Web cliente
p10
p2

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES2015/070001

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, INVENES, WPI, INTERNET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012066767 A1 (VIMPARI MARKKU KALEVI) 15/03/2012, paragraphs[1 - 3]; paragraphs[19 - 27]; paragraphs[31 - 45]; paragraphs[51 - 54]; paragraph [58]; paragraph [71]; figures 1 - 9.	1-8
A	US 2014075524 A1 (HO CHRIS YI-CHENG ET AL.) 13/03/2014, paragraph [3]; paragraphs[8 - 10]; paragraphs[28 - 32]; figures 1 - 3.	1-8
A	WO 2008141948 A1 (IBM ET AL.) 27/11/2008, page 2, line 26 - page 3, line 16; page 5, lines 8 - 9; lines 16 - 21; page 7, lines 15 - 30; page 8, lines 23 - 25; page 9, line 26 - page 10, line 6; lines 14 - 15; page 10, line 30 - page 11, line 7; page 12, lines 19 - 22; page 15, lines 11 - 12; figures 4 - 8.	1-8

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance.
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure use, exhibition, or other means.
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other documents , such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21/09/2015	**(24/09/2015)**
Name and mailing address of the ISA/ OFICINA ESPAÑOLA DE PATENTES Y MARCAS Paseo de la Castellana, 75 - 28071 Madrid (España) Facsimile No.: 91 349 53 04	Authorized officer J. Vazquez Burgos Telephone No. 91 3495513

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES2015/070001

C (continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of documents, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010045426 A1 (VERISIGN INC ET AL.) 22/04/2010, paragraphs[9 - 10]; paragraphs[19 - 26]; paragraphs[35 - 39]; figures 1 - 5.	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/ES2015/070001

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
US2012066767 A1	15.03.2012	RU2013114716 A	20.10.2014
		CN103109509 A	15.05.2013
		TW201218730 A	01.05.2012
		WO2012035495 A1	22.03.2012
		EP2617175 A1	24.07.2013
US2014075524 A1	13.03.2014	WO2014042992 A2	20.03.2014
		WO2014042992 A3	15.05.2014
		US9122865 B2	01.09.2015
WO2008141948 A1	27.11.2008	TW200917755 A	16.04.2009
		JP2010532019 A	30.09.2010
		CN101682620 A	24.03.2010
		CN101682620B B	20.11.2013
		KR20090113273 A	29.10.2009
		KR101120714B B1	22.03.2012
		US2008293378 A1	27.11.2008
		US8107952 B2	31.01.2012
WO2010045426 A1	22.04.2010	US2013219477 A1	22.08.2013
		CA2740698 A1	22.04.2010
		US2010100946 A1	22.04.2010
		US8402519 B2	19.03.2013
		EP2345235 A1	20.07.2011
		EP2345235 A4	06.08.2014

INTERNATIONAL SEARCH REPORT

International application No.

PCT/ES2015/070001

CLASSIFICATION OF SUBJECT MATTER

H04W12/06 (2009.01)
G06F21/33 (2013.01)
G06F21/44 (2013.01)

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES2015/070001

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD
Ver Hoja Adicional

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)
H04W, G06F

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)
EPODOC, INVENES, WPI, INTERNET

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	US 2012066767 A1 (VIMPARI MARKKU KALEVI) 15/03/2012, párrafos[1 - 3]; párrafos[19 - 27]; párrafos[31 - 45]; párrafos[51 - 54]; párrafo [58]; párrafo [71]; figuras 1 - 9.	1-8
A	US 2014075524 A1 (HO CHRIS YI-CHENG ET AL.) 13/03/2014, párrafo [3]; párrafos[8 - 10]; párrafos[28 - 32]; figuras 1 - 3.	1-8
A	WO 2008141948 A1 (IBM ET AL.) 27/11/2008, página 2, línea 26 - página 3, línea 16; página 5, líneas 8 - 9; líneas 16 - 21; página 7, líneas 15 - 30; página 8, líneas 23 - 25; página 9, línea 26 - página 10, línea 6; líneas 14 - 15; página 10, línea 30 - página 11, línea 7; página 12, líneas 19 - 22; página 15, líneas 11 - 12; figuras 4 - 8.	1-8

☒ En la continuación del recuadro C se relacionan otros documentos ☒ Los documentos de familias de patentes se indican en el anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional.	Fecha de expedición del informe de búsqueda internacional.
21/09/2015	**24 de septiembre de 2015 (24/09/2015)**
Nombre y dirección postal de la Administración encargada de la búsqueda internacional OFICINA ESPAÑOLA DE PATENTES Y MARCAS Paseo de la Castellana, 75 - 28071 Madrid (España) Nº de fax: 91 349 53 04	Funcionario autorizado J. Vazquez Burgos Nº de teléfono 91 3495513

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES2015/070001

C (Continuación). DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría *	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	WO 2010045426 A1 (VERISIGN INC ET AL.) 22/04/2010, párrafos[9 - 10]; párrafos[19 - 26]; párrafos[35 - 39]; figuras 1 - 5.	1-8

INFORME DE BÚSQUEDA INTERNACIONAL

Informaciones relativas a los miembros de familias de patentes

Solicitud internacional nº

PCT/ES2015/070001

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
US2012066767 A1	15.03.2012	RU2013114716 A	20.10.2014
		CN103109509 A	15.05.2013
		TW201218730 A	01.05.2012
		WO2012035495 A1	22.03.2012
		EP2617175 A1	24.07.2013
US2014075524 A1	13.03.2014	WO2014042992 A2	20.03.2014
		WO2014042992 A3	15.05.2014
		US9122865 B2	01.09.2015
WO2008141948 A1	27.11.2008	TW200917755 A	16.04.2009
		JP2010532019 A	30.09.2010
		CN101682620 A	24.03.2010
		CN101682620B B	20.11.2013
		KR20090113273 A	29.10.2009
		KR101120714B B1	22.03.2012
		US2008293378 A1	27.11.2008
		US8107952 B2	31.01.2012
WO2010045426 A1	22.04.2010	US2013219477 A1	22.08.2013
		CA2740698 A1	22.04.2010
		US2010100946 A1	22.04.2010
		US8402519 B2	19.03.2013
		EP2345235 A1	20.07.2011
		EP2345235 A4	06.08.2014

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº

PCT/ES2015/070001

CLASIFICACIONES DE INVENCIÓN

H04W12/06 (2009.01)
G06F21/33 (2013.01)
G06F21/44 (2013.01)