(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 671 196**

(21) Número de solicitud: 201631551

(51) Int. CI.:

G06F 21/31 (2013.01)
H04L 9/32 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

05.12.2016

(43) Fecha de publicación de la solicitud:

05.06.2018

(71) Solicitantes:

UNIVERSIDAD CARLOS III DE MADRID (100.0%)
Parque Científico Universidad Carlos III Leganés Tecnológico Avda. Gregorio Peces Barba, 1
28919 LEGANES (Madrid) ES

(72) Inventor/es:

URUEÑA PASCUAL, Manuel y
SOTO CAMPOS, Ignacio

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Método y sistema para autenticar automáticamente un usuario mediante un dispositivo de autenticación**

(57) Resumen:

Método y sistema para autenticar automáticamente un usuario mediante un dispositivo de autenticación.

La presente invención se refiere a un método y un sistema para autenticar automáticamente un usuario que comprende: almacenar en un dispositivo de autenticación unas credenciales del usuario; comprobar, desde un dispositivo electrónico, los dispositivos de autenticación accesibles; establecer una comunicación entre los dispositivos mediante una interfaz radio de corto alcance; enviar, desde el dispositivo electrónico al dispositivo de autenticación una solicitud de autenticación; comprobar el cumplimiento de un conjunto de parámetros de acceso; si se cumplen los parámetros de acceso, enviar un mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance; y autenticar al usuario en el dispositivo electrónico de acuerdo al mensaje de respuesta recibido.

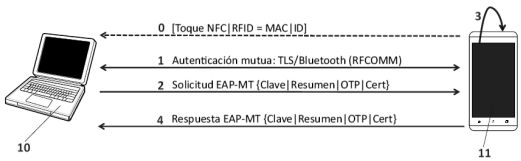

FIG. 1

ES 2 671 196 A1

DESCRIPCIÓN

Método y sistema para autenticar automáticamente un usuario mediante un dispositivo de autenticación

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención tiene aplicación en el campo de la seguridad informática y más específicamente en los métodos y sistemas para autenticar usuarios en el entorno de los sitios web, aplicaciones informáticas, y dispositivos electrónicos.

ANTECEDENTES DE LA INVENCIÓN

La autenticación de usuarios en dispositivos electrónicos de comunicaciones es un proceso de seguridad fundamental. La mayoría de servicios y dispositivos electrónicos no conciben ser utilizados por usuarios anónimos, o al menos no sus funcionalidades más delicadas. Por ello la autenticación de un usuario resulta un proceso esencial que hoy en día forma parte de la rutina de acceso a la mayoría de servicios o dispositivos electrónicos.

Actualmente, el principal mecanismo que se usa para la autenticación de usuario son las contraseñas. Eso obliga a los usuarios a tener que crear y recordar un número importante de contraseñas para usar con las distintas cuentas que poseen, que normalmente tienen diferentes niveles de seguridad. Esto inevitablemente hace que los usuarios, además de verse obligados a realizar una tarea tediosa como es el introducir continuamente una contraseña, recurran a reutilizar contraseñas y/o a usar contraseñas sencillas que acarrean importantes problemas de seguridad y abren oportunidades de ataques informáticos, mediante el uso de diccionarios de contraseñas conocidas o por fuerza bruta. Aunque los “gestores de contraseñas” (*password managers*, en inglés) permiten reducir el riesgo del uso de contraseñas al generarlas de manera aleatoria y almacenarlas de manera segura, la participación directa del usuario en el proceso de autenticación posibilita ataques de ingeniería social, técnicas de suplantación de identidad (*phishing* en inglés), o el uso de dispositivos o software malicioso que registra la secuencia de teclas pulsadas (*keyloggers*, en inglés).

El estado del arte ofrece algunas alternativas más seguras a las contraseñas, como son las contraseñas de un solo uso (OTP – *One Time Password*, en inglés), las tarjetas inteligentes

(*Smart Cards*. en inglés), técnicas biométricas o el envío de códigos de autenticación por SMS, aunque todas ellas tienen un uso práctico muy limitado, ya que o bien requieren pasos adicionales que implican molestas pérdidas de tiempo para el usuario (ej. OTPs o códigos por SMS) y donde el usuario todavía tiene que teclear una contraseña, lo que hace que persista la posibilidad de ataques de *phishing*; o requieren periféricos dedicados en cada equipo desde el que se solicita hacer una autenticación, como es el caso de las tarjetas inteligentes o las técnicas basadas en biometría.

Otros documentos, que reflejan el estado del arte relativo a la autenticación de usuarios utilizando dispositivos de autenticación externos para evitar estas deficiencias, son por ejemplo el documento US2015281227 A1, donde se describe un mecanismo de autenticación en sitios web en el que las contraseñas están almacenadas en un teléfono móvil. Se utiliza una etiqueta (*tag*, en inglés) NFC para descifrar el repositorio de contraseñas almacenado en el teléfono y este se comunica con el ordenador del usuario a través de un servidor de notificación alojado en Internet. Sin embargo, no se contempla el uso de otro tipo de credenciales ni métodos de autenticación local, o su uso en escenarios sin cobertura de Internet.

Por otro lado, el documento WO 2013/089777 A1 describe un sistema de autenticación para sitios web que emplea un dispositivo inalámbrico externo para almacenar las contraseñas del usuario y que las comunica con el ordenador del usuario mediante NFC. Sin embargo, únicamente soporta contraseñas y se reduce al escenario de autenticación web sin mayores posibilidades de configuración o modificación de niveles de seguridad.

Por lo expuesto anteriormente, los métodos y sistemas conocidos para la autenticación de usuarios carecen del equilibrio necesario entre seguridad, usabilidad y flexibilidad para adaptarse a las distintas situaciones de usuarios y servicios, con lo que se echa en falta en el estado del arte alguna solución que aúne todo lo anterior, elimine en la medida de lo posible la intervención del usuario en el proceso de autenticación, a la vez que lo mantiene al tanto y con el control de cómo y cuándo realizar autenticaciones, y que además no se restringa únicamente al uso de contraseñas como credenciales de usuario.

DESCRIPCIÓN DE LA INVENCIÓN

La presente invención resuelve los problemas mencionados anteriormente mediante una solución flexible, de alta seguridad y de mínima intervención para el usuario que almacena

sus credenciales en un dispositivo externo de autenticación con un interfaz radio de corto alcance para que este pueda autenticarse donde necesite (ej. dispositivos electrónicos locales o sitios web remotos). Las credenciales pueden ser de distintos tipos, desde contraseñas, códigos RFID/NFC de control de acceso físico, contraseñas de un solo uso, certificados digitales o cualquier otro tipo de credenciales. Así, en un primer aspecto de la invención, se presenta un método para autenticar automáticamente un usuario que comprende los siguientes pasos:

a) almacenar en un dispositivo de autenticación unas credenciales del usuario;

b) comprobar, desde un dispositivo electrónico, los dispositivos de autenticación accesibles por una interfaz radio de corto alcance;

c) establecer, entre el dispositivo electrónico y el dispositivo de autenticación, una comunicación segura mediante la interfaz radio de corto alcance;

d) enviar, desde el dispositivo electrónico al dispositivo de autenticación una solicitud de autenticación a través de la interfaz radio de corto alcance;

e) comprobar en el dispositivo de autenticación el cumplimiento de un conjunto de parámetros de acceso previamente definidos;

f) si se cumplen los parámetros de acceso previamente definidos, enviar, desde el dispositivo de autenticación al dispositivo electrónico, un mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance;

g) autenticar al usuario en el dispositivo electrónico de acuerdo al mensaje de respuesta recibido.

Una realización de la presente invención comprueba periódicamente que el dispositivo de autenticación continúa siendo accesible por el dispositivo electrónico mediante la interfaz radio de corto alcance y, en caso de que el dispositivo de autenticación deje de estar accesible, se bloquee la sesión del usuario en el dispositivo electrónico.

Adicionalmente, la presente invención contempla en una de sus realizaciones los pasos de:

- enviar desde el dispositivo electrónico, una solicitud de acceso a un sitio web alojado en un servidor web remoto, a través de un navegador web;
- identificar, mediante una extensión del navegador web, el sitio web solicitado;
- enviar, desde la extensión del navegador web al dispositivo de autenticación, una solicitud de los nombres de usuario registrados en el sitio web, a través de una interfaz radio de corto alcance;
- comprobar, en el dispositivo de autenticación, que el sitio web se corresponde con

algún sitio web registrado previamente;

- si el sitio web se corresponde con algún sitio web registrado previamente, enviar los nombres de usuario registrados para ese sitio web a la extensión del navegador web, a través de la interfaz radio de corto alcance;
- seleccionar, por el usuario, uno de los nombres de usuario registrados que han sido enviados a la extensión del navegador web;
- enviar, desde la extensión del navegador web al dispositivo de autenticación, una solicitud de autenticación para el nombre de usuario seleccionado a través de la interfaz radio de corto alcance;
- enviar, desde el dispositivo de autenticación a la extensión del navegador web, un mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario almacenadas, a través de la interfaz radio de corto alcance;
- autenticar al usuario en el sitio web de acuerdo al mensaje de respuesta recibido.

De acuerdo a una de las realizaciones de la invención, el paso de establecer una comunicación entre el dispositivo electrónico y el dispositivo de autenticación, mediante la interfaz radio de corto alcance, comprende previamente los pasos de:

- realizar un emparejamiento inicial de ambos dispositivos, donde el emparejamiento incluye un consentimiento explícito del usuario, en el que ambos dispositivos intercambian sus certificados digitales, para que puedan autenticarse posteriormente de manera segura;
- comprobar, por el dispositivo de autenticación, la autenticidad del certificado del dispositivo electrónico obtenido a través de la interfaz radio de corto alcance comparando el resumen (*digest*, en inglés) de su clave pública, con el valor mostrado por el dispositivo electrónico, por ejemplo mediante un código QR que pueda ser escaneado por el dispositivo de autenticación;
- guardar en el dispositivo de autenticación el certificado del nuevo dispositivo electrónico emparejado en una lista blanca de dispositivos de confianza que pueden conectarse al dispositivo de autenticación sin confirmación por parte del usuario, o en la lista gris, donde se almacenan los dispositivos electrónicos conocidos pero cuya conexión requiere una confirmación por parte del usuario;

Alternativamente, en una realización de la invención, los dispositivos confían en los certificados de una autoridad de certificación, de forma que los dispositivos electrónicos que dispongan de certificado de dicha autoridad de certificación puedan conectarse al dispositivo de autenticación (y viceversa) sin necesidad de

emparejamiento previo, aunque en ese caso la conexión de un dispositivo electrónico nuevo se notificará al usuario, que podrá guardarlo en la lista blanca, en la lista gris, o en una lista negra si no desea permitir que dicho dispositivo electrónico pueda conectarse al dispositivo de autenticación en el futuro.

De acuerdo a una de las realizaciones de la invención, establecer una comunicación segura entre el dispositivo de autenticación y el dispositivo electrónico mediante la interfaz radio de corto alcance comprende adicionalmente los pasos de:

- establecer un canal radio entre el dispositivo electrónico y el dispositivo de autenticación usando el interfaz radio de corto alcance;
- iniciar desde el dispositivo de autenticación una conexión TLS [RFC5246] sobre dicho canal radio;
- validar en el dispositivo de autenticación el primer certificado enviado desde el dispositivo electrónico, y comprobar si se encuentra en la lista negra, cancelando en ese caso el establecimiento de la sesión TLS;
- proporcionar desde el dispositivo de autenticación un segundo certificado al dispositivo electrónico;
- completar el establecimiento de la sesión TLS en el caso de que el primer y el segundo certificados sean válidos y aparezcan en la lista blanca o la lista gris del dispositivo de autenticación, solicitando confirmación al usuario si es necesario (si aparece en la lista gris);
- posteriormente la sesión TLS negociada se puede resumir, evitando la necesidad de volver a intercambiar los certificados de ambos dispositivos y demostrar la posesión de las claves privadas asociadas a los mismos.

En una de las realizaciones de la invención, el paso de enviar desde el dispositivo de autenticación al dispositivo electrónico las credenciales de autenticación a través de la interfaz radio de corto alcance, además comprende solicitar, en el dispositivo de autenticación, al usuario su autorización para acceder a las credenciales solicitadas por el dispositivo electrónico.

Opcionalmente, la autorización puede ser mediante un toque del usuario en una pantalla táctil del dispositivo de autenticación, agitar el dispositivo de autenticación, introducir en el dispositivo de autenticación un PIN o contraseña asociados a la credencial correspondiente, o usar un sensor biométrico en el dispositivo de autenticación.

El conjunto de parámetros de acceso también se contempla que recoja un parámetro de horario y un parámetro de localización y, de acuerdo a una de las realizaciones de la presente invención, el paso de comprobar el cumplimiento de dicho conjunto de parámetros de acceso comprende determinar si la hora y la localización asociadas a la solicitud de autenticación recibida por el dispositivo de autenticación cumplen los requisitos de hora y localización previamente definidos para el credencial o repositorio de credenciales siendo accedido.

En caso de descubrirse más de un dispositivo de autenticación conocido dentro del alcance de la interfaz radio de corto alcance del dispositivo electrónico al que se desea acceder, se contempla en una de las realizaciones de la invención el paso de seleccionar, por el usuario, su dispositivo de autenticación mediante una interacción con el dispositivo electrónico.

Opcionalmente, la selección del dispositivo de autenticación, cuando haya varios accesibles desde el dispositivo electrónico al que se desea acceder, se realiza acercando el propio dispositivo de autenticación o una tarjeta de acceso del usuario a un lector RFID/NFC en el dispositivo electrónico, para así proporcionar la dirección física del dispositivo de autenticación al dispositivo electrónico, directamente o mediante un identificador único que se pueda traducir a la misma (por ejemplo, preguntando a un servidor de gestión o comprobando cuál de los dispositivos de autenticación cercanos anuncia dicho identificador).

En una de las realizaciones de la invención, la instalación de credenciales del usuario en el dispositivo de autenticación, se contempla que comprenda los siguientes pasos:

- proporcionar, por el usuario, una información de registro de usuario en el servidor de registro del sitio web;
- enviar la información de registro desde el servidor de registro a un servidor de credenciales;
- generar un código QR en el servidor de registro;
- generar, en el servidor de credenciales, unas credenciales de usuario asociadas a la información de registro;
- escanear, mediante el dispositivo de autenticación, el código QR generado por el servidor de registro;
- como resultado del escaneo del código QR, mostrar en el dispositivo de autenticación, un mensaje de solicitud de confirmación de registro en el sitio web;

- en caso de que el usuario confirme el registro, establecer una conexión entre el dispositivo de autenticación y la dirección codificada en el código QR que apunta al servidor de credenciales;
- proporcionar, desde el servidor de credenciales al dispositivo de autenticación, las credenciales de usuario generadas, a través de la conexión establecida.

El paso de proporcionar las credenciales generadas desde el servidor de credenciales comprende, de acuerdo a una realización de la invención, al menos una de las siguientes técnicas:

- proporcionar una contraseña aleatoria;
- proporcionar una semilla para generar contraseñas de un solo uso;
- negociar una clave compartida mediante un intercambio de claves Diffie-Hellman.
- proporcionar un certificado para el usuario

En una de las realizaciones de la invención, proporcionar las credenciales de usuario en forma de certificado digital comprende el uso del protocolo de registro en infraestructura de clave pública sobre transporte seguro (EST – *Enrolment over Secure Transport*, en inglés) según RFC7030.

Un segundo aspecto de la presente invención se refiere a un sistema para autenticar automáticamente un usuario que comprende:

- un dispositivo de autenticación configurado para almacenar de manera segura las credenciales del usuario; establecer una comunicación segura con un dispositivo electrónico mediante una interfaz radio de corto alcance; comprobar el cumplimiento de un conjunto de parámetros de acceso previamente definidos; y, si se cumplen los parámetros de acceso previamente definidos, enviar al dispositivo electrónico, un mensaje de respuesta a una solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance;
- un dispositivo electrónico configurado para comprobar los dispositivos de autenticación accesibles por la interfaz radio de corto alcance; establecer una comunicación segura con el dispositivo de autenticación mediante la interfaz radio de corto alcance; enviar al dispositivo de autenticación una solicitud de autenticación a través de la interfaz radio de corto alcance; y autenticar al usuario de acuerdo al mensaje de respuesta recibido.

Adicionalmente, de acuerdo a una de las realizaciones de la presente invención, el sistema además comprende opcionalmente:

- un servidor de registro configurado para recibir una información de registro de un usuario en un sitio web; enviar la información de registro a un servidor de credenciales; generar un código QR; y
- un servidor de credenciales configurado para recibir la información de registro desde el servidor de registro; generar unas credenciales de usuario asociadas a la información de registro; establecer una conexión segura con el dispositivo de autenticación; proporcionar al dispositivo de autenticación las credenciales de usuario generadas, a través de la conexión segura establecida entre ambos;

donde el dispositivo de autenticación está además configurado para:

- escanear el código QR generado por el servidor de registro; como resultado del escaneo del código QR, mostrar un mensaje de solicitud de confirmación de registro en el sitio web; en caso de que el usuario confirme el registro, establecer una conexión segura con la dirección codificada en el código QR que apunta al servidor de credenciales;
- recibir, desde el servidor de credenciales, las credenciales de usuario generadas, a través de la conexión segura establecida y guardarlas en un repositorio seguro de credenciales dentro del dispositivo de autenticación.

De acuerdo a una de las realizaciones de la presente invención, el dispositivo de autenticación además comprende un reloj que proporciona un parámetro de hora y unos medios de localización que proporcionan un parámetro de localización, y donde el dispositivo de autenticación está además configurado para determinar si los parámetros de hora y la localización, proporcionados por el reloj y los medios de localización respectivamente, asociados a la solicitud de autenticación recibida por el dispositivo de autenticación, cumplen unos requisitos de hora y localización previamente definidos.

Un último aspecto de la invención se refiere a un producto de programa de ordenador que comprende código de programa de ordenador, adaptado para realizar el procedimiento de la presente invención cuando dicho código de programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en el terreno, un circuito integrado específico de la aplicación, un microprocesador, un micro-controlador o cualquier otra forma de hardware programable.

La presente invención por tanto, permite a un usuario autenticarse de forma segura y rápida donde necesite, ya sea el mundo físico, ordenadores locales, sitios web remotos, etc. El usuario solo necesita tener el dispositivo de autenticación cerca, es decir dentro de la cobertura de la interfaz radio de corto alcance utilizada, preferiblemente Bluetooth, de dónde se solicita su autenticación. Además, la presente invención tiene una gran flexibilidad y posibilidades de configuración que permiten por ejemplo que la autenticación se realice o no en función de unos parámetros de acceso como la hora o la localización.

El dispositivo de autenticación, de acuerdo a la presente invención, puede comprender capacidades de procesamiento y almacenamiento, interfaz gráfica de usuario, pantalla táctil, reloj, sistema de navegación y/u otros mecanismos de localización, acelerómetro, cámara, sensores biométricos, interfaces inalámbricas de corto alcance Bluetooth y NFC, y/o comunicaciones de red. Los sensores mencionados anteriormente pueden ser usados para mejorar la usabilidad y la protección de las credenciales del usuario, por ejemplo limitando la localización y las horas en las que se pueden usar las credenciales almacenadas y/o solicitando autorización explícita al usuario, utilizando diferentes métodos, para acceder a un credencial.

A diferencia de los tokens de seguridad tradicionales (como los llaveros OTP o las tarjetas inteligentes) que normalmente solo soportan un tipo específico de credenciales, la presente invención soporta diferentes tipos de credenciales, incluyendo contraseñas, certificados digitales o contraseñas de un solo uso, y puede usarse tanto para autenticación local como remota. Además, la comunicación entre el dispositivo de autenticación y el ordenador del usuario se realiza a través una comunicación inalámbrica de corto alcance, basada preferiblemente en Bluetooth, que permite usar la presente invención en situaciones sin acceso a Internet, además de reducir la superficie de ataque (de todo Internet a solo los dispositivos Bluetooth próximos).

Por último, aunque otras soluciones del estado del arte utilizan interfaces radio de muy corto alcance como etiquetas RFID/NFC, estas se utilizan para descifrar el repositorio de contraseñas almacenado en el teléfono, mientras que los escenarios que se plantea la presente invención de “Toque-para-acceder” la interfaz NFC del teléfono o una etiqueta RFID/NFC externa se emplean solamente para identificar al dispositivo de autenticación con el que debe contactar el dispositivo electrónico siendo accedido, puesto que para el intercambio de credenciales se sigue empleando la conexión segura TLS sobre Bluetooth.

DESCRIPCIÓN DE LOS DIBUJOS

Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, se acompaña como parte integrante de dicha descripción, un juego de figuras en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

Figura 1.- ilustra el intercambio de mensajes en un escenario de acceso a un ordenador local utilizando el método y sistema de la presente invención.

Figura 2.- ilustra el intercambio de mensajes en un escenario de acceso a un sitio web remoto que requiere autenticación utilizando el método y sistema de la presente invención.

Figura 3.- ilustra el procedimiento contemplado por una de las realizaciones de la invención para la instalación de credenciales en un dispositivo de autenticación.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Lo definido en esta descripción detallada se proporciona para ayudar a una comprensión exhaustiva de la invención. En consecuencia, las personas medianamente expertas en la técnica reconocerán que son posibles variaciones, cambios y modificaciones de las realizaciones descritas en la presente memoria sin apartarse del ámbito de la invención. Además, la descripción de funciones y elementos bien conocidos en el estado del arte se omite por claridad y concisión.

Por supuesto, las realizaciones de la invención pueden ser implementadas en una amplia variedad de plataformas, protocolos, dispositivos y sistemas, por lo que los diseños e implementaciones específicas presentadas en este documento, se proporcionan únicamente con fines de ilustración y comprensión, y nunca para limitar aspectos de la invención.

La presente invención divulga en una de sus realizaciones un dispositivo de autenticación, (como por ejemplo un teléfono móvil, pero también puede implementarse en un dispositivo electrónico dedicado), que almacena y gestiona las credenciales de un usuario, de manera que cuando este necesite autenticarse ante cualquier dispositivo electrónico (un ordenador local, un sitio web al que se accede desde un ordenador local, un torno de control de acceso físico, etc.) lo puede hacer gracias a dicho dispositivo de autenticación, que se comunica mediante una interfaz radio de corto alcance, preferiblemente Bluetooth, con el dispositivo electrónico que está solicitando la autenticación del usuario, y a continuación usar las

credenciales almacenadas para realizar la autenticación local o remota, de forma que el usuario solo tiene que confirmar que quiere autenticarse, en lugar de tener que recordar e introducir dicha credencial manualmente.

Así, la presente invención propone un dispositivo de autenticación fácil de usar, escalable, y flexible, donde los usuarios almacenan sus credenciales en un dispositivo portable distinto del dispositivo electrónico frente al que se quieren autenticar. De este modo, aunque un atacante fuese capaz de comprometer el dispositivo electrónico, típicamente un ordenador personal, las credenciales del usuario quedarían a salvo en su dispositivo de autenticación, cifradas por software con una clave maestra que solo conoce el usuario o dentro de un Elemento Seguro (SE - *Secure Element* en inglés) hardware. Además, las interfaces radio de corto alcance, como Bluetooth o NFC, utilizadas para establecer las comunicaciones locales con otros dispositivos (como por ejemplo, un ordenador local o un torno de control de acceso físico) permiten ventajosamente realizar la autenticación sin necesidad de usar periféricos adicionales como un lector de tarjetas inteligentes (*Smart Cards*, en inglés) o sensores biométricos dedicados, ni tampoco requerir comunicación a través de Internet.
El dispositivo de autenticación de la presente invención, de acuerdo a una de sus realizaciones, será referido en adelante como “MobiToken” para distinguirlo de otros dispositivos. Este dispositivo MobiToken organiza las credenciales de usuario en uno o más repositorios de credenciales (por ejemplo un repositorio “trabajo”, otro repositorio “personal”, etc.) que pueden tener diferentes políticas de acceso. Cada credencial de usuario dispone de un dominio al cual pertenece (por ejemplo pc01.example.org o *.example.org), una identidad o nombre de usuario (de manera que los usuarios pueden tener múltiples cuentas en un mismo servicio), y uno o más tipos de credencial (ej. contraseña y un generador de OTPs) para autenticación de dos factores (2FA – *two factor authentication*, en inglés) o verificación en dos pasos (2SV - *two step verification*, en inglés).

El dispositivo MobiToken de la presente invención, permite habilitar o deshabilitar el acceso a una credencial dada manualmente, de forma que una credencial sólo será accesible si el usuario la habilita manualmente. Además, permite asignar diferentes políticas de acceso a las distintas credenciales dependiendo de su nivel de seguridad. Por ejemplo, se puede asignar una política de “Permitir Siempre” a sitios de baja seguridad (ej., una red social), mientras que el acceso a un servicio de alta seguridad puede requerir teclear un código PIN para desbloquear el Elemento Seguro que almacena la credencial y/o usar un mecanismo biométrico para autorizar su uso, bien cada vez que se accede a la misma, o con validez durante un cierto tiempo. Una de las políticas utilizadas se basa en presentar un diálogo de

autenticación “Permitir/Denegar” siempre que se intente acceder a una credencial, que puede ser autorizado por el usuario mediante gestos como tocar en la pantalla o agitar el dispositivo (incluso estando dentro de un bolso, por ejemplo) lo que puede detectarse mediante un acelerómetro del dispositivo MobiToken (especialmente si este se implementa en un teléfono móvil inteligente, ya que es habitual que incorpore este y otros sensores). MobiToken también permite políticas de acceso avanzadas basadas en el uso de los sensores adicionales del dispositivo MobiToken, como por ejemplo, habilitando un repositorio de credenciales corporativo solo en una determinada franja horaria (09:00 a 18:00 por ejemplo), o cerrándolo si el usuario se aleja de la oficina (detectándolo mediante los correspondientes medios de localización presentes habitualmente en cualquier teléfono móvil inteligente). Como las políticas de acceso se pueden asignar a las distintas entidades de la jerarquía de credenciales, se aplica la más específica (por ejemplo, las estaciones de trabajo de *.example.org pueden requerir un código PIN cada vez que son accedidas, pero el acceso al ordenador personal del usuario pc01.example.org puede requerirlo solo una vez al día).

El dispositivo MobiToken de la presente invención, también puede especificar qué dispositivos pueden conectarse al mismo (para autenticar al usuario) mediante el uso de listas blancas, grises y negras. Los dispositivos en la lista blanca son confiables y pueden conectarse al dispositivo MobiToken automáticamente (aunque luego puede solicitarse confirmación al usuario para acceder a una credencial protegida), mientras que las conexiones desde dispositivos de la lista gris requieren confirmación del usuario, y los dispositivos de la lista negra no pueden conectarse al dispositivo MobiToken. Además, si el usuario deniega el acceso de un dispositivo a su MobiToken o a una de las credenciales almacenadas, adicionalmente puede informar del posible ataque, de manera que el dispositivo se añade a la lista negra, y todos los datos del intento de acceso (como por ejemplo el dispositivo del atacante, hora, credencial solicitada) pueden ser registrados y enviados automáticamente al servicio de seguridad de la organización. En cuanto a los ataques de ingeniería social y suplantación de identidad o “*phishing”*, un atacante podría intentar engañar al usuario para que le envíe sus credenciales por correo electrónico o por teléfono. Sin embargo, siempre que el usuario intente acceder manualmente a una credencial (puesto que en la mayoría de los casos el acceso debería ser automático), el dispositivo MobiToken puede configurarse, de acuerdo a una de las realizaciones, para mostrar una pantalla de información al usuario explicándole de forma didáctica que nunca debe divulgar sus contraseñas cuando se lo soliciten por correo o teléfono, así como los pasos a seguir para comprobar que realmente está accediendo a un servicio de manera segura (es decir, comprobando el nombre de dominio DNS, el candado verde de HTTPS, y

la última autoridad de certificación observada para dicho sitio web).

A continuación se describen distintos casos de uso para un dispositivo de comunicación o "MobiToken" de acuerdo a la presente invención:

Caso de uso 1: acceso a un ordenador local.

El primer caso de uso de un dispositivo MobiToken es el acceso local a un ordenador, lo que normalmente requiere que el usuario teclee su contraseña muchas veces al día. Desde el punto de vista de los usuarios, el acceso a su ordenador personal con MobiToken se reduce a presionar alguna tecla del teclado o mover el ratón para despertar el ordenador o quitar el salvapantallas. Sin embargo, en lugar de mostrar la pantalla de acceso para introducir la contraseña, los usuarios de MobiToken simplemente continúan con sus sesiones inmediatamente, como si el ordenador no estuviese protegido con contraseña.

La **Figura 1** ilustra el intercambio de mensajes que se produce en este escenario. Un proceso está ejecutándose en el ordenador personal (**10**) del usuario, intentando conectarse continuamente mediante una interfaz radio de corto alcance, en este caso Bluetooth, al dispositivo MobiToken (**11**) del usuario (se asume que el ordenador tiene un único usuario y que el dispositivo MobiToken correspondiente ya ha sido emparejado con el ordenador y está asociado a dicho usuario). En primer lugar, se establece (**1**) una conexión Bluetooth RFCOMM entre el PC y el dispositivo MobiToken, y se establece una sesión TLS [RFC5247] con autenticación mutua con certificados sobre la misma. La sesión TLS se inicia desde el dispositivo MobiToken, de manera que puede validar el certificado del ordenador antes de proporcionar el suyo. Si ambos certificados son válidos (es decir, iguales a los intercambiados en la asociación segura inicial) y el ordenador está en la lista blanca o gris del dispositivo MobiToken (pero no en la lista negra), la sesión TLS sobre Bluetooth se completa, y el ordenador y el dispositivo MobiToken pueden comunicarse de manera segura. Cuando el usuario inicia el proceso de acceso al ordenador, el ordenador le solicita (**2**) al dispositivo MobiToken que proporcione la credencial apropiada para autenticar al usuario (nótese que la sesión TLS solo autentica a los dispositivos –es decir, al ordenador y al dispositivo MobiToken-, no al usuario en sí). Una realización de la invención, para permitir distintos mecanismos de autenticación MobiToken, emplea una versión adaptada del protocolo EAP (*Extensible Authentication Protocol*) [RFC3748], que denominaremos EAP-MT, de manera que se pueden emplear los métodos EAP de autenticación existentes, como

la autenticación de reto-respuesta (EAP MS-CHAPv2 [RFC2759]) o usar un certificado del usuario (EAP-TLS [RFC5216]). Finalmente, después de solicitar al usuario que apruebe (**3**) el acceso a la credencial necesaria para acceder al ordenador (normalmente la autorización del usuario solo será necesaria en el acceso inicial, mientras que en las ocasiones subsiguientes durante cierto periodo de tiempo puede ser automática), el dispositivo MobiToken usa dicha credencial para enviar (**4)** un mensaje de Respuesta EAP al ordenador para completar el proceso de autenticación.

Una variante de este primer caso de uso es cuando el dispositivo electrónico accedido, el ordenador en este caso, es compartido por múltiples usuarios (y no es conveniente o no se puede pre-configurar con la dirección MAC Bluetooth y la clave pública de los dispositivos MobiToken de todos los usuarios posibles). En este caso, primero tiene que decidirse con qué dispositivo MobiToken se debe contactar desde el ordenador. En una realización de la invención, este problema se resuelve mediante una pantalla de diálogo que muestra todos los dispositivos MobiToken cercanos usando SDP (*Service Discovery Protocol*), el protocolo de descubrimiento de servicios Bluetooth, de manera que los usuarios pueden elegir su dispositivo MobiToken para completar la autenticación. Sin embargo, también se contempla en otras realizaciones establecer correspondencias entre los mecanismos de seguridad lógicos y las acciones físicas de los usuarios, como por ejemplo usando un escenario llamado “Toque-para-acceder” (“*Tap-to-login*”, en inglés). Así, los usuarios pueden indicar fácilmente su identidad a un dispositivo compartido, simplemente tocando con el dispositivo MobiToken sobre un lector NFC conectado al ordenador. Con esta acción únicamente se indica al ordenador qué dispositivo de autenticación debe contactar (0), bien proporcionando su dirección MAC Bluetooth o cualquier otro identificador único (por ejemplo, un UUID) por NFC, o más convenientemente para grandes organizaciones, preguntando por la dirección MAC asociada a un ID a una base de datos centralizada. El resto del proceso de autenticación ocurre a través de la interfaz Bluetooth igual que se ha explicado anteriormente. Sin embargo, en este caso, como el dispositivo compartido probablemente no esté incluido en la lista blanca del dispositivo MobiToken del usuario, sino en la lista gris, este podrá pedir al usuario que confirme explícitamente el acceso a su MobiToken desde dicho ordenador, y le permita añadirle a la lista blanca de dispositivos de confianza para simplificar accesos futuros.

Una realización de la invención contempla implementar el evento de “Toque-para-acceder” usando una tarjeta RFID/NFC de empleado, que está asociado al dispositivo MobiToken. Así se reaprovechan, las tarjetas que los empleados usan para el control de acceso físico al

recinto.

Caso de uso 2: acceso a un sitio web remoto.

Un caso de uso práctico de la presente invención se refiere al acceso a un sitio web remoto a través de un ordenador local. La presente invención contempla este escenario y según una de sus realizaciones es posible gestionar el acceso a cualquier recurso lógico o servicio remoto, incluyendo los basados en tecnologías web. El aspecto clave es cómo enviar, sin involucrar al usuario en el proceso, las credenciales almacenadas de forma segura en el dispositivo de autenticación MobiToken, al servicio que está siendo accedido. La solución comprende instalar una extensión específica (a la que se hará referencia también como "Extensión MobiToken") en el navegador web utilizado para acceder al sitio web, donde dicha extensión se comunica con el dispositivo MobiToken, bien directamente o a través de otro proceso local que establezca la comunicación TLS/Bluetooth con el mismo.

La **Figura 2** muestra cómo un dispositivo de comunicación MobiToken puede emplearse, de acuerdo a una de las realizaciones de la invención, para acceder a un servicio en la web que requiere autenticación. En primer lugar, el usuario intenta acceder (**20**) al sitio web mediante su navegador web como lo haría normalmente. El servidor web (**21**) puede mostrar (**22**) el típico formulario de acceso solicitando el nombre del usuario y su contraseña, aunque este paso puede saltarse en caso de sitios web que implementen funcionalidad MobiToken específica para acceder a la cuenta del usuario directamente. La extensión MobiToken del navegador web reconoce la página de autenticación por el tipo y/o el nombre en los campos del formulario, y le pregunta (**23**) al dispositivo MobiToken por la lista de usuarios registrados en ese dominio. Para ello se usa el mismo protocolo EAP-MT/TLS/RFCOMM explicado anteriormente para el caso de acceso a un ordenador local. Es importante mencionar que, dado que ambos, la extensión del navegador y el dispositivo MobiToken, comprueban el nombre de dominio DNS del sitio web siendo accedido (en lugar de ser responsabilidad del usuario), este mecanismo impide ventajosamente la mayoría de ataques de "*phishing*", porque aunque un dominio podría engañar a un usuario (por ejemplo https://secure.bank.com.evil.com), este no se correspondería con ningún dominio registrado en el dispositivo MobiToken (de acuerdo al ejemplo: https://secure.bank.com), y así no se proporcionarán ni credenciales, ni nombres de usuario registrados siquiera. En el caso de que el usuario sí tenga una cuenta en ese servicio, primero el dispositivo MobiToken devolverá (**24**) los nombres de usuario registrados para ese dominio a la Extensión del

navegador, que a su vez se los presentará al usuario. El usuario selecciona (**25**) la cuenta deseada directamente en el navegador web (en principio no hace falta manejar el dispositivo MobiToken), y la extensión del navegador solicita (**26**) las credenciales del usuario seleccionado, de acuerdo con los campos requeridos en el formulario de la página web de acceso (por ejemplo: contraseña y/o código de un solo uso OTP) al dispositivo MobiToken vía Bluetooth. A continuación, en función del nivel de seguridad escogido, puede requerirse desde el dispositivo MobiToken que el usuario confirme explícitamente si desea permitir (**27**) el acceso a la credencial solicitada, utilizando el mecanismo de autorización especificado. Una vez el usuario ha aprobado el acceso a la credencial, el dispositivo MobiToken envía (**28**) dicha credencial a la extensión del navegador, que rellena el campo correspondiente (contraseña y/o OTP) (nótese que aunque los OTPs se usan normalmente como sistema de autenticación de segundo factor, también podrían llegar a reemplazar a las contraseñas como un factor único, al ser más seguro que estas puesto que nunca se envía el secreto compartido), y finalmente se rellena el formulario de acceso y se envía (**29**) al servidor web original que aloja el sitio web.

Si la credencial empleada es una contraseña, el escenario anterior es como un acceso a web típico con nombre de usuario/contraseña usando la función de auto-rellenado presente en muchos navegadores hoy en día. Sin embargo, en el caso de la presente invención, las credenciales no se almacenan en el navegador web o en el ordenador local sino que únicamente se almacenan en el dispositivo de autenticación MobiToken, por lo que un atacante nunca tendría acceso a las credenciales del usuario aunque comprometiese el navegador web del usuario y/o su ordenador (que son más vulnerables al emplearse para navegar por todo tipo de páginas web y tener acceso directo, continuo y de alta capacidad a Internet).

Además, el dispositivo MobiToken también permite emplear mecanismos de autenticación más avanzados que impiden que las credenciales puedan ser espiadas y robadas en nodos intermedios, por ejemplo el uso de autenticación HTTP o autenticación mutua TLS con certificados. Aunque la mayoría de los sitios web utilizan mecanismos de autenticación personalizados a nivel de aplicación, HTTP proporciona su propio mecanismo de autenticación [RFC 2617] que no requiere el envío de la contraseña sino una respuesta a un reto basado en la misma. Por lo tanto, si se usa autenticación HTTP en el servidor web, la extensión MobiToken instalada en el navegador gestiona la solicitud de autenticación y reenvía sus parámetros (usando un método EAP propio llamado EAP-MT-HTTP-DIGEST) al dispositivo MobiToken, que calcula el resumen HTTP (después de pedir la aprobación del

usuario si es necesario), de manera que la extensión del navegador puede finalmente enviarla al servidor web. Por lo tanto, el navegador nunca llega a ver la credencial de usuario, solo su resumen, con lo que la credencial no podría ser robada por software malicioso ejecutándose en el ordenador.

De la misma manera, el protocolo TLS [RFC 5246] permite autenticación mutua que, además de autenticar al servidor, también requiere que el cliente presente su certificado y pruebe que está en posesión de la clave privada correspondiente. Como en el caso anterior, si la autenticación mutua está habilitada en el servidor, la Extensión del navegador gestiona la solicitud del certificado de cliente, la reenvía al dispositivo MobiToken y este devuelve el certificado y calcula la prueba de la posesión de la clave privada, de manera que la clave privada nunca sale del dispositivo MobiToken, por lo que no es vulnerable si el ordenador intermedio está comprometido.

Los escenarios de autenticación basados en certificados, contemplados por la presente invención, son interesantes en la medida en que su utilidad abarca no solo las interacciones con servidores web, sino también con cualquier protocolo de nivel de aplicación que pueda transportarse encima de TLS, como los de correo electrónico (por ejemplo, SMTP, IMAP, POP3), u otros protocolos seguros como SSH.

Caso de uso 3: instalación de credenciales.

Los casos de uso descritos anteriormente asumen que el dispositivo MobiToken ya tiene las credenciales de usuario. En una de las realizaciones de la invención se permite la instalación de las credenciales de usuario fuera de banda (*out-of-band*, en inglés), por ejemplo, la instalación de un certificado de usuario desde fichero. Sin embargo, una de las realizaciones también contempla instalar las credenciales de forma segura haciendo uso de la conexión a Internet del dispositivo MobiToken. Así, este tercer caso de uso abarca cualquiera de los anteriores, pero además añade un método y un sistema particulares para la instalación de las credenciales de usuario.

El modelo de amenazas (*threat model*, en inglés) contemplado por la presente invención asume que los dispositivos electrónicos accesibles por el usuario podrían albergar software malicioso (*malware*), que extraiga sin permiso información sensible, como por ejemplo almacenando todas las teclas pulsadas por el usuario (*keylogger*, en inglés). Por lo tanto, la

introducción manual de credenciales en el dispositivo MobiToken a través de otro dispositivo electrónico utilizado por el usuario (por ejemplo un ordenador) puede verse comprometida. Para evitar esta amenaza, la presente invención permite el intercambio seguro de credenciales directamente desde el dispositivo MobiToken usando la capacidad de conexión a Internet de dicho dispositivo.

La **figura 3** ilustra el procedimiento que se contempla en una de las realizaciones de la invención para el intercambio seguro de credenciales. Si un usuario accede (**31**) a un cierto sitio web para registrarse, rellena (**32**) la información de usuario como de costumbre, pero sin especificar una contraseña, dado que esta podría ser potencialmente débil y es susceptible de ser interceptada por software malicioso residente en el ordenador local, tal y como se ha explicado anteriormente. En lugar de eso, cuando el usuario termina de introducir sus datos de registro, el Servidor de Registro (**37**), envía (**33**) la información del nuevo usuario (o algún identificador que permita relacionarlo con la nueva credencial) a un Servidor de Credenciales (**38**), y genera y presenta (**34**) una imagen con un código QR al usuario (alternativamente se puede mostrar la dirección URL correspondiente por si el dispositivo MobiToken no tuviese cámara para captar el código QR). El usuario procede entonces a escanear (**35**) el código QR con la cámara del dispositivo MobiToken y confirma explícitamente que quiere registrarse en el correspondiente sitio web. En ese caso, el dispositivo MobiToken, se conecta (**36**) con la dirección URL codificada en el código QR, y que apunta al Servidor de Credenciales, para negociar la nueva credencial. En función del tipo de credenciales almacenadas por el dispositivo MobiToken y soportadas por el servidor de credenciales, se eligen una o más tipos de credenciales compatibles y comienzan a intercambiarse de forma segura.

Como la conexión entre el dispositivo y el Servidor de Credenciales está protegida por TLS, en una de las realizaciones de la invención, la introducción de credenciales consiste simplemente en crear una contraseña aleatoria o una semilla OTP y enviarlas al otro extremo. Pero, de acuerdo a otras realizaciones de la invención, se contemplan otros mecanismos más complejos, como implementar un intercambio de claves Diffie-Hellman (DH) o usar el protocolo de registro en PKI sobre Transporte seguro (PKI-EST) [RFC 7030]. En este último caso, el servidor MobiToken de Credenciales tendría el papel de una autoridad de certificación (CA) que puede proporcionar certificados a los usuarios, bien generando el correspondiente par de claves directamente, o idealmente usando una clave pública proporcionada por el dispositivo MobiToken (generada por el elemento seguro hardware).

Nótese que en el caso de que un servicio despliegue una autoridad de certificación (CA) privada dedicada para dar certificados a sus usuarios, y esta solo se emplea para autenticarlos, entonces la CA puede generar certificados bajo demanda, sin verificar la identidad real de los usuarios (de forma similar a tener cuentas anónimas en un servicio, con un nombre de usuario que no identifica a la persona real). Los certificados generados no se podrán usar para otro propósito excepto para autenticar a los usuarios de dicho servicio. En ese caso los servidores TLS deberán configurase para solicitar certificados de cliente generados por esa CA privada del propio servicio, mientras que el servidor en sí se puede seguir validando con un certificado emitido por una CA pública.

El Servidor de Registro y el Servidor de Credenciales son entidades lógicas, en una realización de la invención ambos están implementados en un mismo elemento físico.

Aunque el escenario descrito en este apartado requiere servidores con las funcionalidades descritas anteriormente, una de las realizaciones de la invención también contempla usar el dispositivo de comunicación MobiToken con servidores tradicionales. En ese caso, el dispositivo MobiToken genera una contraseña aleatoria y le solicita al usuario que la introduzca en el correspondiente campo de registro en el servidor. Es un mecanismo menos seguro frente a software malicioso ejecutando en el ordenador del usuario, pero permite el uso de MobiToken en servicios legados que no soporten el intercambio seguro de credenciales.

Remarcando algunos de los ventajosos efectos de la presente invención, hay que destacar que, al contrario que con los tokens de seguridad tradicionales (como los llaveros OTP o las tarjetas inteligentes) que normalmente solo soportan un tipo específico de credenciales, la presente invención es flexible y permite implementar diferentes tipos de mecanismos de autenticación, por lo que es capaz de almacenar y gestionar todas las credenciales de los usuarios (independientemente de su tipo). Adicionalmente, puede incluir características como una interfaz gráfica de usuario, cámaras, acelerómetro, sistemas de localización, sensores biométricos, o acceso a Internet, que se pueden usar para mejorar la seguridad y adaptarse a diferentes escenarios de control de acceso según los requisitos de los usuarios. Por ejemplo, para sitios en los que los requisitos de seguridad sean bajos (como una red social) el acceso puede ser automático o simplemente pedir al usuario que confirme el acceso a la credencial asociada (con un diálogo Permitir/Denegar, o agitando el teléfono). Para servicios que requieran mayor seguridad (como el acceso a la red corporativa) se

puede pedir al usuario que confirme el acceso a la credencial introduciendo un PIN al menos una vez al día, cuando se acceda fuera de las horas de trabajo, o cuando el usuario se aleje más de, por ejemplo, 1 Km de su oficina.

Adicionalmente, un servicio remoto de alta seguridad o el ordenador local puede pedirle al usuario, a través del dispositivo de autenticación de la presente invención, que se re-autentique cada 5 minutos (es decir, autenticación continua) de manera que la sesión de usuario se bloquea automáticamente si el usuario se aleja con su dispositivo de autenticación más allá del radio de corto alcance del ordenador.

Finalmente, para servicios de alta seguridad (por ejemplo, un servicio de banca electrónica), la confirmación del usuario se puede basar en mecanismos de autenticación biométrica disponibles en el dispositivo de autenticación del usuario, como por ejemplo un lector de huellas dactilares o reconocimiento de cara usando una cámara frontal.

Por otro lado, la versatilidad y flexibilidad de la presente invención, se refleja también en su capacidad para funcionar en escenarios de autenticación basados en certificados digitales, así como su integración en sistemas de control de acceso físico usando una interfaz NFC.

Algunas realizaciones preferidas de la invención se describen en las reivindicaciones dependientes que se incluyen seguidamente.

En este texto, la palabra “comprende” y sus variantes (como “comprendiendo”, etc.) no deben interpretarse de forma excluyente, es decir, no excluyen la posibilidad de que lo descrito incluya otros elementos, pasos, etc.

La descripción y los dibujos simplemente ilustran los principios de la invención. Por lo tanto, debe apreciarse que los expertos en la técnica podrán concebir varias disposiciones que, aunque no se hayan descrito o mostrado explícitamente en este documento, representan los principios de la invención y están incluidas dentro de su alcance. Además, todos los ejemplos descritos en este documento se proporcionan principalmente por motivos pedagógicos para ayudar al lector a entender los principios de la invención y los conceptos aportados por el (los) inventor(es) para mejorar la técnica, y deben considerarse como no limitativos con respecto a tales ejemplos y condiciones descritos de manera específica. Además, todo lo expuesto en este documento relacionado con los principios, aspectos y realizaciones de la invención, así como los ejemplos específicos de los mismos, abarcan

equivalencias de los mismos.

Aunque la presente invención se ha descrito con referencia a realizaciones específicas, los expertos en la técnica deben entender que los anteriores y diversos otros cambios, omisiones y adiciones en la forma y el detalle de las mismas pueden realizarse sin apartarse del alcance de la invención tal como se definen mediante las siguientes reivindicaciones.

REIVINDICACIONES

1.- Método para autenticar automáticamente un usuario que comprende los siguientes pasos:

a) instalar en un dispositivo de autenticación unas credenciales del usuario;

b) comprobar, desde un dispositivo electrónico, los dispositivos de autenticación accesibles por una interfaz radio de corto alcance;

c) establecer, entre el dispositivo electrónico y el dispositivo de autenticación, una comunicación mediante la interfaz radio de corto alcance;

d) enviar, desde el dispositivo electrónico al dispositivo de autenticación una solicitud de autenticación a través de la interfaz radio de corto alcance;

e) comprobar en el dispositivo de autenticación el cumplimiento de un conjunto de parámetros de acceso previamente definidos;

f) si se cumplen los parámetros de acceso previamente definidos, enviar, desde el dispositivo de autenticación al dispositivo electrónico, un mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance;

g) autenticar al usuario en el dispositivo electrónico de acuerdo al mensaje de respuesta recibido.

2.- Método de acuerdo a la reivindicación 1 que además comprende:

- enviar, por el usuario desde el dispositivo electrónico, una solicitud de acceso a un sitio web, a través de un navegador web;
- identificar, mediante una extensión del navegador web, un formulario de acceso asociado al sitio web solicitado;
- enviar, desde la extensión del navegador web al dispositivo de autenticación, una solicitud de los nombres de usuario registrados en el sitio web;
- comprobar, en el dispositivo de autenticación, que el sitio web se corresponde con algún sitio web registrado previamente;
- si el sitio web se corresponde con algún sitio web registrado previamente, enviar los nombres de usuario registrados para ese sitio web a la extensión del navegador web;
- seleccionar, por el usuario, uno de los nombres de usuario registrados que han sido enviados a la extensión del navegador web;
- enviar, desde la extensión del navegador web al dispositivo de autenticación, una solicitud de autenticación a través de la interfaz radio de corto alcance;
- enviar, desde el dispositivo de autenticación a la extensión del navegador web, un

mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance;

- rellenar el formulario de acceso para autenticar al usuario en el sitio web que aloja el servicio web de acuerdo al mensaje de respuesta recibido.

3.- Método de acuerdo a cualquiera de las reivindicaciones anteriores, donde instalar unas credenciales del usuario en el dispositivo de autenticación comprende previamente los siguientes pasos:

- proporcionar, por el usuario, una información de registro para un sitio web a un servidor de registro;
- enviar la información de registro desde el servidor de registro a un servidor de credenciales;
- generar un código QR en el servidor de registro;
- generar, en el servidor de credenciales, unas credenciales de usuario asociadas a la información de registro;
- escanear, mediante el dispositivo de autenticación, un código QR generado por el servidor de registro;
- como resultado del escaneo del código QR, mostrar en el dispositivo de autenticación, un mensaje de solicitud de confirmación de registro en el sitio web;
- en caso de que el usuario confirme el registro, establecer una conexión segura entre el dispositivo de autenticación y una dirección codificada en el código QR que apunta al servidor de credenciales;
- proporcionar, desde el servidor de credenciales al dispositivo de autenticación, las credenciales de usuario generadas, a través de la conexión establecida.

4.- Método de acuerdo a la reivindicación 3, donde proporcionar las credenciales generadas comprende al menos una de las siguientes técnicas:

- proporcionar una contraseña aleatoria;
- proporcionar una semilla para un generador de contraseñas de un solo uso;
- realizar un intercambio de claves Diffie-Hellman;
- proporcionar un certificado para el usuario.

5.- Método de acuerdo a la reivindicación 3, donde las credenciales de usuario están basadas en certificados digitales, y el paso de instalar dichas credenciales comprende utilizar un protocolo de registro en infraestructura de clave pública sobre transporte seguro

"EST – *Enrolment over Secure Transport*" según RFC 7030.

6.- Método de acuerdo a cualquiera de las reivindicaciones de la invención donde, el paso de establecer una comunicación entre el dispositivo electrónico y el dispositivo de autenticación, mediante la interfaz radio de corto alcance, comprende previamente los pasos de:

- emparejar ambos dispositivos, donde el emparejamiento incluye un consentimiento explícito del usuario, en el que ambos dispositivos intercambian unos certificados digitales;
- comprobar, por el dispositivo de autenticación, la autenticidad del certificado del dispositivo electrónico obtenido a través de la interfaz radio de corto alcance comparando el resumen de su clave pública con un valor mostrado por el dispositivo electrónico;
- guardar en el dispositivo de autenticación el certificado del nuevo dispositivo emparejado en una primera lista de dispositivos electrónicos de confianza que no requieren confirmación del usuario para conectarse con el dispositivo de autenticación, o en una segunda lista de dispositivos electrónicos que requieren confirmación del usuario para conectarse con el dispositivo de autenticación.

7.- Método de acuerdo a cualquier de las reivindicaciones anteriores donde establecer una comunicación entre el dispositivo electrónico y el dispositivo de autenticación mediante la interfaz radio de corto alcance además comprende los pasos de:

- iniciar desde el dispositivo de autenticación una sesión TLS;
- validar en el dispositivo de autenticación un primer certificado enviado desde el dispositivo electrónico;
- proporcionar desde el dispositivo de autenticación un segundo certificado al dispositivo electrónico;
- establecer una sesión TLS en el caso de que el primer y el segundo certificados sean válidos.

8.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde enviar, desde el dispositivo de autenticación al dispositivo electrónico el mensaje de respuesta de acuerdo a las credenciales del usuario a través de la interfaz radio de corto alcance, además comprende solicitar, en el dispositivo de autenticación, al usuario autorización para acceder

a las credenciales proporcionadas.

9.- Método de acuerdo a la reivindicación 8, donde la autorización para el acceso a las credenciales comprende un toque del usuario en una pantalla táctil del dispositivo de autenticación, agitar el dispositivo de autenticación, utilizar un sensor biométrico, y/o introducir en el dispositivo de autenticación un PIN o contraseña asociados a la credencial correspondiente.

10.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde el conjunto de parámetros de acceso comprende un parámetro de horario y un parámetro de localización y donde comprobar el cumplimiento de dicho conjunto de parámetros de acceso comprende determinar si la hora y la localización asociadas a la solicitud de autenticación recibida por el primer dispositivo de comunicación cumplen los requisitos de hora y localización previamente definidos.

11.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde el paso de comprobar los dispositivos de autenticación accesibles desde el dispositivo electrónico, además comprende seleccionar por el usuario su dispositivo de autenticación mediante una interacción con el dispositivo electrónico.

12.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde el paso de la selección del dispositivo de autenticación, cuando haya varios accesibles desde el dispositivo electrónico, comprende los siguientes pasos:

- acercar el dispositivo de autenticación a una cierta distancia de un lector RFID/NFC en el dispositivo electrónico;
- proporcionar una dirección física del dispositivo de autenticación al dispositivo electrónico, donde la dirección física se proporciona directamente o mediante un identificador único.

13.- Sistema para autenticar automáticamente un usuario que comprende:

- un dispositivo de autenticación configurado para instalarle credenciales del usuario; establecer una comunicación con un dispositivo electrónico mediante una interfaz radio de corto alcance; comprobar el cumplimiento de un conjunto de parámetros de acceso previamente definidos; y, si se cumplen los parámetros de acceso previamente definidos, enviar al dispositivo electrónico, un mensaje de respuesta a una solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance;

- un dispositivo electrónico configurado para comprobar los dispositivos de autenticación accesibles por la interfaz radio de corto alcance; establecer una comunicación con el dispositivo de autenticación mediante la interfaz radio de corto alcance; enviar al dispositivo de autenticación una solicitud de autenticación a través de la interfaz radio de corto alcance; y autenticar al usuario de acuerdo al mensaje de respuesta recibido.

14.- Sistema de acuerdo a la reivindicación 13 que además comprende:

- un servidor de registro configurado para recibir una información de registro en un sitio web; enviar la información de registro a un servidor de credenciales; generar un código QR con una dirección asociada al servidor de credenciales;
- un servidor de credenciales configurado para recibir la información de registro desde el servidor de registro; generar unas credenciales de usuario asociadas a la información de registro; establecer una conexión con el dispositivo de autenticación; proporcionar al dispositivo de autenticación, las credenciales de usuario generadas, a través de la conexión establecida;

donde el dispositivo de autenticación está además configurado para:

- escanear el código QR generado por el servidor de registro; como resultado del escaneo del código QR, mostrar un mensaje de solicitud de confirmación de registro en el sitio web; en caso de que el usuario confirme el registro, establecer una conexión con una dirección codificada en el código QR que apunta al servidor de credenciales;
- recibir, desde el servidor de credenciales, las credenciales de usuario generadas, a través de la conexión establecida y almacenarlas en un repositorio seguro de credenciales dentro del dispositivo.

15.- Sistema de acuerdo a una cualquiera de las reivindicaciones 13 y 14, donde el dispositivo de autenticación además comprende un reloj que proporciona un parámetro de hora y unos medios de localización que proporcionan un parámetro de localización, y donde el dispositivo de autenticación está además configurado para determinar si los parámetros de hora y la localización, proporcionados por el reloj y los medios de localización respectivamente, asociados a la solicitud de autenticación recibida, cumplen unos requisitos de hora y localización previamente definidos para dicho credencial o repositorio de credenciales.

16.- Producto de programa de ordenador que comprende código de programa de ordenador, adaptado para realizar el procedimiento de acuerdo a cualquiera de las reivindicaciones 1 a 12 cuando dicho código de programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en el terreno, un circuito integrado específico de la aplicación, un microprocesador, un micro-controlador o cualquier otra forma de hardware programable.

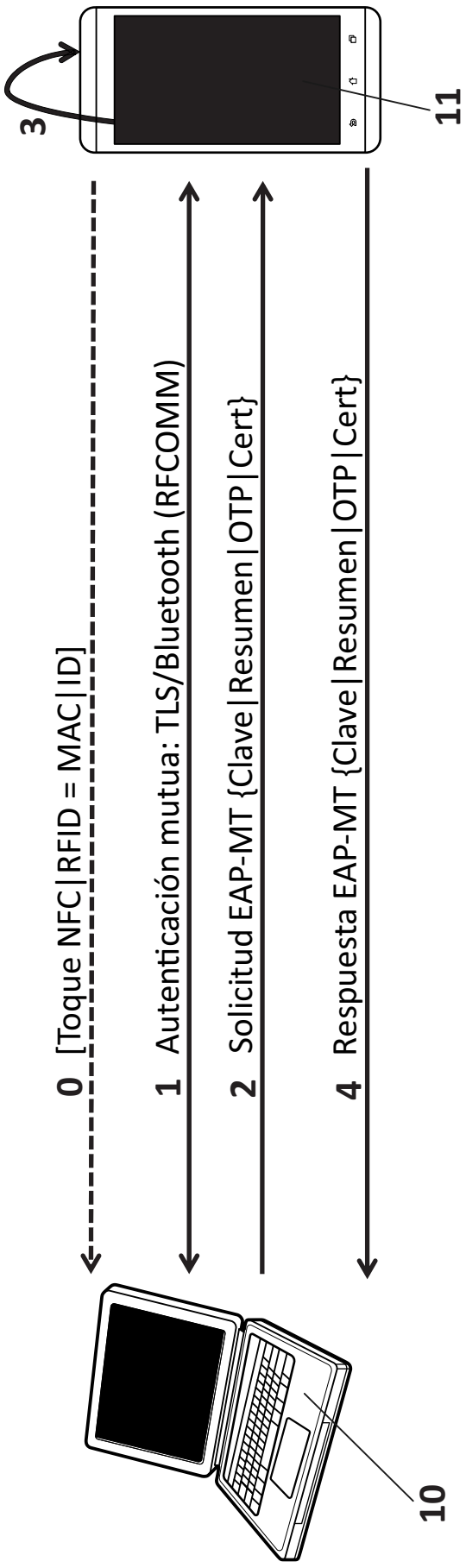
3
11
0 [Toque NFC|RFID = MAC|ID]
1 Autenticación mutua: TLS/Bluetooth (RFCOMM)
2 Solicitud EAP-MT {Clave|Resumen|OTP|Cert}
4 Respuesta EAP-MT {Clave|Resumen|OTP|Cert}
10

FIG. 1

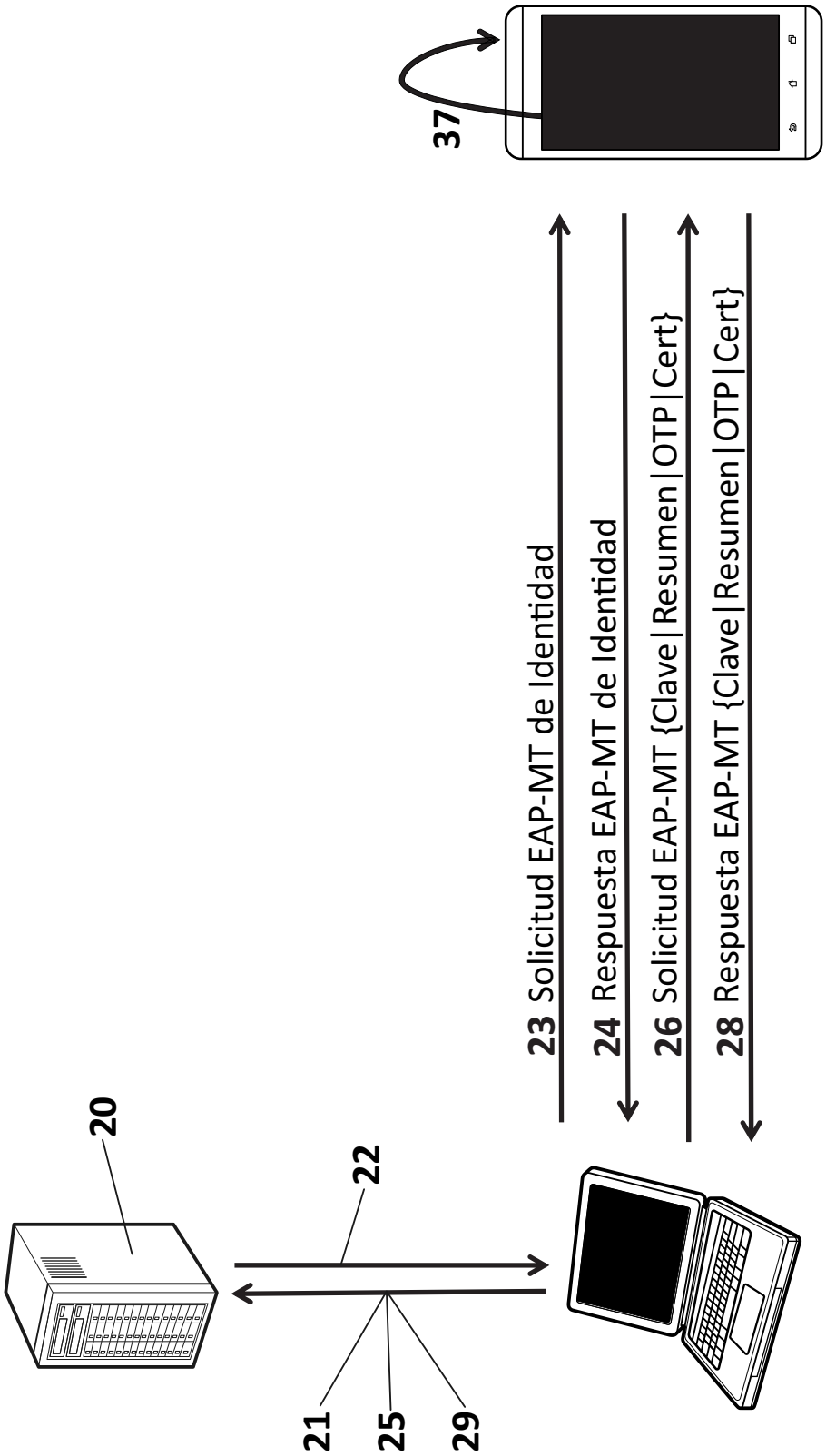
37
23 Solicitud EAP-MT de Identidad
24 Respuesta EAP-MT de Identidad
26 Solicitud EAP-MT {Clave|Resumen|OTP|Cert}
28 Respuesta EAP-MT {Clave|Resumen|OTP|Cert}
20
22
21
25
29

FIG. 2

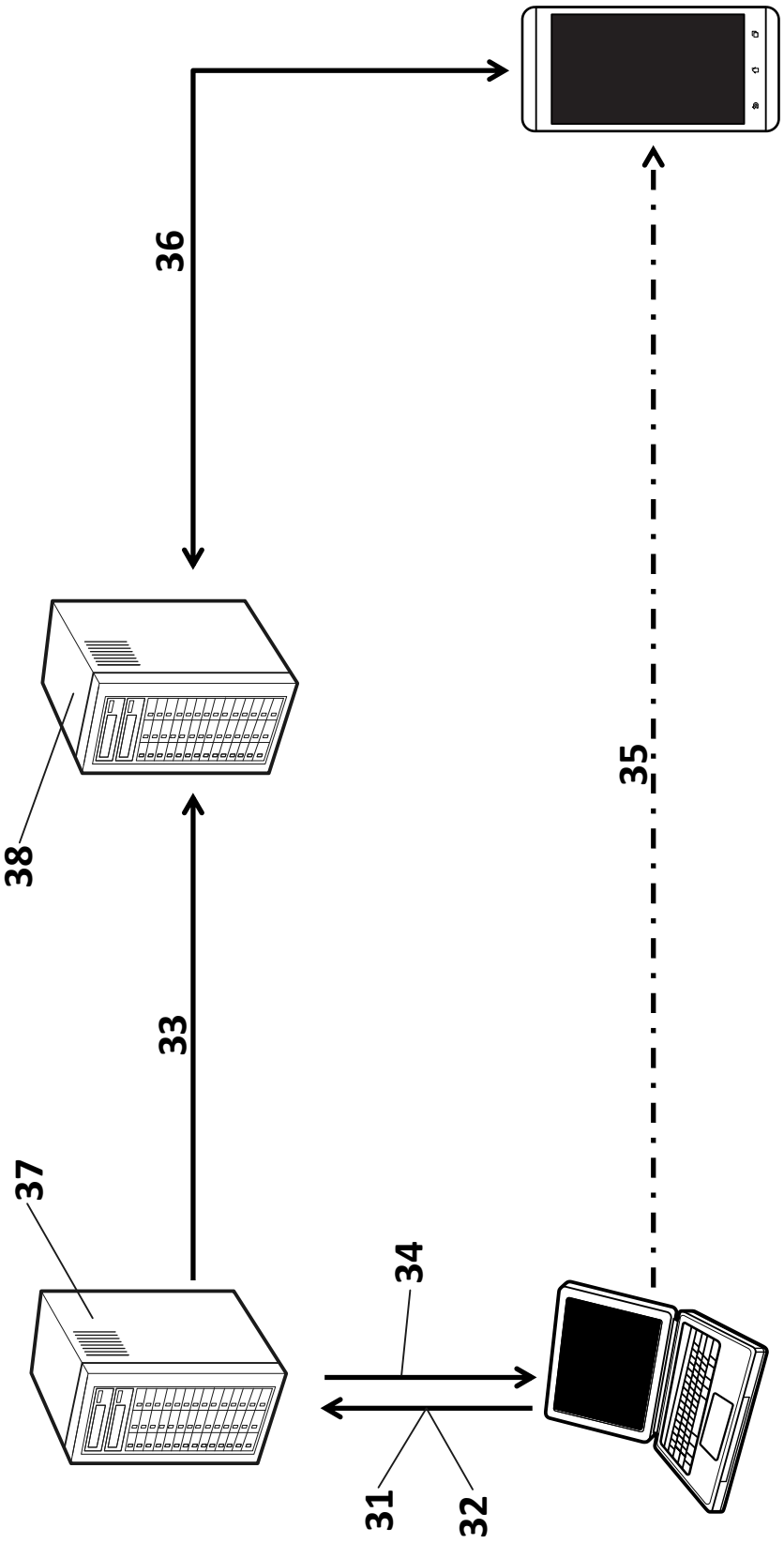

FIG. 3

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201631551

(22) Fecha de presentación de la solicitud: 05.12.2016

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***G06F21/31*** (2013.01)
H04L9/32 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
X	US 2015281227 A1 (FOX IVEY RICHARD GORDON et al.) 01/10/2015. Resumen; figuras 1, 2; párrafos [17 - 23, 27 - 29, 39 - 42, 55 - 61, 80, 96].	1-5, 8, 9, 11, 13, 14, 16
Y		10, 12, 15
X	US 2015096001 A1 (MORIKUNI JAMES J et al.) 02/04/2015. Resumen; figuras 1, 2; párrafos [15, 16, 18 - 31, 37 - 39].	1, 2, 6, 7, 13, 16
X	US 2014317708 A1 (ADRANGI FARID et al.) 23/10/2014. Resumen; figura 1, párrafos [13, 18 - 20, 24, 27 - 30].	1 , 2, 13, 16
X	US 2014344904 A1 (VENKATARAMANI SRINATH et al.) 20/11/2014. Resumen; figura 4, párrafos [17, 18, 20, 22, 24, 25].	1, 13, 16
Y	US 2015143508 A1 (HALIBARD MOISHE) 21/05/2015. resumen; párrafo [27];	10, 15
Y	US 2016212141 A1 (BANERJEE ANIRBAN) 21/07/2016. Resumen; párrafos [27 - 29, 52].	12
A	TRANSPORT LAYER SECURITY. WIKIPEDIA, Publicado el 27/11/2016; URL:// https://web.archive.org/web/20161127073701/https://en.wikipedia.org/wiki/Transport_Layer_Security	6, 7
A	RFC 7030 - ENROLLMENT OVER SECURE TRANSPORT. Standard propuesto. Publicado el 20/08/2016. URL://https://web.archive.org/web/20160820112048/https://tools.ietf.org/html/rfc7030	5

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

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
12.01.2018	B. Pérez García	1/6

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

G06F, H04L, H04W

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, INSPEC

Fecha de Realización de la Opinión Escrita: 12.01.2018

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	5 - 7, 9 - 12, 15	**SI**
	Reivindicaciones	1 - 4, 8, 13, 14, 16	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1 - 16	**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 2015281227 A1 (FOX IVEY RICHARD GORDON et al.)	01.10.2015
D02	US 2015096001 A1 (MORIKUNI JAMES J et al.)	02.04.2015
D03	US 2014317708 A1 (ADRANGI FARID et al.)	23.10.2014
D04	US 2014344904 A1 (VENKATARAMANI SRINATH et al.)	20.11.2014
D05	US 2015143508 A1 (HALIBARD MOISHE)	21.05.2015
D06	US 2016212141 A1 (BANERJEE ANIRBAN)	21.07.2016
D07	TRANSPORT LAYER SECURITY. WIKIPEDIA	27.11.2016
D08	RFC 7030 - ENROLLMENT OVER SECURE TRANSPORT.	20.08.2016

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

Se considera D01 el documento del estado de la técnica anterior más cercano al objeto de la invención.

Con el fin de identificar de la forma más clara posible las diferencias entre la invención reivindicada en 1 y el documento del estado de la técnica más próximo, se reproduce seguidamente el texto de dicha reivindicación, eliminando del mismo sus referencias originales, si las hubiere e introduciendo donde se considere oportuno las del documento D01.

Siguiendo la redacción de la primera reivindicación, D01 describe un método para autenticar automáticamente a un usuario que comprende los siguientes pasos:
a) instalar en un dispositivo de autenticación *(101 + 103)* unas credenciales del usuario;
b) comprobar, desde un dispositivo electrónico *(104)*, los dispositivos de autenticación accesibles por una interfaz radio de corto alcance *(NFC o cualquier método de comunicación inalámbrica de corto alcance)*;
c) establecer, entre el dispositivo electrónico y el dispositivo de autenticación, una comunicación mediante la interfaz radio de corto alcance *(párrafos 40, 57: "Smartphone 101 se empareja a PC/laptop/Tablet 104")*;
d) enviar, desde el dispositivo electrónico *(primer dispositivo comunicación 104)* al dispositivo de autenticación *(segundo dispositivo comunicación 101)* una solicitud de autenticación a través de la interfaz radio de corto alcance *(párrafo 39)*;
e) comprobar en el dispositivo de autenticación el cumplimiento de un conjunto de parámetros de acceso previamente definidos *(párrafos 42 y 57: compara la URL candidata con la librería de URLs almacenada)*;
f) si se cumplen los parámetros de acceso previamente definidos, enviar, desde el dispositivo de autenticación al dispositivo electrónico, un mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance *(párrafo 39)*;
g) autenticar al usuario en el dispositivo electrónico de acuerdo al mensaje de respuesta recibido *(párrafo 80)*.

No se han encontrado diferencias entre D01 y la primera reivindicación, por lo que ésta no cumple el requisito de novedad, según el Art. 6 de la Ley Española de Patentes.

Para la segunda reivindicación, se han encontrado igualmente coincidencias en D01, que se detallan a continuación:
- enviar, por el usuario desde el dispositivo electrónico *(104)*, una solicitud de acceso a un sitio web, a través de un navegador web *(105)- (párrafos 39 y 60)*;
- identificar, mediante una extensión del navegador web *(106)*, un formulario de acceso asociado al sitio web solicitado *(párrafos 39 y 60)*;
- enviar, desde la extensión del navegador web *(106)* al dispositivo de autenticación (*101)*, una solicitud de los nombres de usuario registrados en el sitio web *(párrafos 39 y 60)*;
- comprobar, en el dispositivo de autenticación, que el sitio web se corresponde con algún sitio web registrado previamente *(párrafos 18, 19, 39 y 60)*;
- si el sitio web se corresponde con algún sitio web registrado previamente, enviar los nombres de usuario registrados para ese sitio web a la extensión del navegador web *(párrafos 18, 19, 39 y 60)*;
- seleccionar, por el usuario, uno de los nombres de usuario registrados que han sido enviados a la extensión del navegador web *(párrafo 19)*;
- enviar, desde la extensión del navegador web al dispositivo de autenticación, una solicitud de autenticación a través de la interfaz radio de corto alcance *(párrafos 39 y 60)*;
- enviar, desde el dispositivo de autenticación a la extensión del navegador web, un mensaje de respuesta a la solicitud de autenticación recibida, de acuerdo a las credenciales del usuario, a través de la interfaz radio de corto alcance *(párrafos 39 y 60)*;
- rellenar el formulario de acceso para autenticar al usuario en el sitio web que aloja el servicio web de acuerdo al mensaje de respuesta recibido *(párrafo 80)*.

Al igual que en el caso anterior, no se han encontrado diferencias entre D01 y la segunda reivindicación, por lo que ésta también carece de novedad.

La reivindicación tres aclara que instalar unas credenciales del usuario en el dispositivo de autenticación comprende previamente los siguientes pasos: el usuario proporciona una información de registro para un sitio web a un servidor de registro; se envía la información de registro desde el servidor de registro a un servidor de credenciales; se genera un código QR en el servidor de registro; se genera en el servidor de credenciales, unas credenciales de usuario asociadas a la información de registro; el dispositivo de autenticación escanea un código QR generado por el servidor de registro y muestra un mensaje de solicitud de confirmación de registro en el sitio web; si el usuario confirma el registro, se establece una conexión segura entre el dispositivo de autenticación y una dirección codificada en el código QR que apunta al servidor de credenciales y el servidor de credenciales proporciona al dispositivo de autenticación, las credenciales de usuario generadas, a través de la conexión establecida.

D01 realiza la instalación de las credenciales del usuario en el dispositivo de autenticación a partir del servidor seguro *107* que proporciona canales seguros de comunicación entre el dispositivo de autenticación *101* y el dispositivo electrónico *104*. Las credenciales del usuario, almacenadas en el dispositivo de autenticación *101* son encriptadas con una clave almacenada en el token *103.* Dicha clave de encriptación se comunica al dispositivo de autenticación a través de un enlace NFC, o bien, mediante una imagen escaneada como un código de barras o código QR *(párrafo 96).* Es decir, D01 aunque no cita tan explícitamente todos los pasos de esta reivindicación, consigue el mismo efecto. Se considera que un experto en la materia no tendría dificultad en desarrollar esta reivindicación, a partir de la información divulgada en D01. Sin actividad inventiva, según el Art. 8 de la LEP.

La cuarta reivindicación define que para proporcionar las credenciales generadas se utiliza al menos una de las siguientes técnicas: proporcionar una contraseña aleatoria, proporcionar una semilla para un generador de contraseñas de un solo uso, realizar un intercambio de claves Diffie-Hellman o proporcionar un certificado para el usuario.
D01 utiliza una contraseña aleatoria *(párrafo 58).* No tiene actividad inventiva.

Las reivindicaciones 5-7 añaden la utilización de certificados digitales en la invención.
La reivindicación cinco instala las credenciales con un protocolo de registro en infraestructura de clave pública sobre transporte seguro "EST – *Enrolment over Secure Transport*" según RFC 7030.
D01 utiliza otra técnica diferente para instalar las credenciales (contraseña aleatoria), tal y como se ha comentado para la cuarta reivindicación. Por tanto, la diferencia se encuentra en cómo se instalan las credenciales y el efecto técnico que produce realizarlo mediante una infraestructura de clave pública sobre EST es poder obtener mayor seguridad en el proceso al utilizar este protocolo criptográfico. No obstante, este protocolo es ampliamente conocido y consiste en utilizar un protocolo de gestión de certificados X.509 enfocado a clientes con infraestructura de clave pública. No se considera que el hecho de introducir este protocolo para instalar las credenciales suponga un efecto técnico inesperado a la luz del documento D01 y considerando que este protocolo es ampliamente usado en el sector (ver D08 como ejemplo). Sin actividad inventiva.

La sexta reivindicación, dependiente de la primera, especifica que para establecer una comunicación entre el dispositivo electrónico y el dispositivo de autenticación, mediante la interfaz radio de corto alcance, previamente se realizan los pasos de emparejar ambos dispositivos con un intercambio de certificados digitales; comprobar, por el dispositivo de autenticación, la autenticidad del certificado del dispositivo electrónico obtenido a través de la interfaz radio de corto alcance comparando el resumen de su clave pública con un valor mostrado por el dispositivo electrónico; guardar en el dispositivo de autenticación el certificado del nuevo dispositivo emparejado en una primera lista de dispositivos electrónicos de confianza que no requieren confirmación del usuario para conectarse con el dispositivo de autenticación, o en una segunda lista de dispositivos electrónicos que requieren confirmación del usuario para conectarse con el dispositivo de autenticación.
La reivindicación número siete añade que establecer una comunicación entre el dispositivo electrónico y el dispositivo de autenticación mediante la interfaz radio de corto alcance además comprende los pasos de: iniciar desde el dispositivo de autenticación una sesión TLS; validar en el dispositivo de autenticación un primer certificado enviado desde el dispositivo electrónico; proporcionar desde el dispositivo de autenticación un segundo certificado al dispositivo electrónico; establecer una sesión TLS en el caso de que el primer y el segundo certificados sean válidos.

D01 no realiza estos pasos al no utilizar certificados digitales.
Sin embargo, el documento D02, que también anula la actividad inventiva de las reivindicaciones 1 y 2, utiliza una comunicación segura SSL/TLS entre un dispositivo navegador 205 y un dispositivo móvil 210 para el intercambio de credenciales.
D07, que se cita a modo de ilustración, describe las características que proporciona un protocolo TLS a una comunicación y cómo se desarrolla ésta: criptografía pública, protocolos, intercambio de certificados digitales. Es decir, dado que D02 incorpora una comunicación TLS entre los dispositivos, está implícito que ambos se autentican utilizando certificados digitales y que pueden crear listas de dispositivos de confianza. D02 anticipa estas reivindicaciones 6 y 7 que no presentan actividad inventiva, según el Art. 8 de la Ley 11/1986.

La octava reivindicación implica que se solicita, en el dispositivo de autenticación, autorización al usuario para acceder a las credenciales proporcionadas, lo que está implícito en D01 al ser necesario que el usuario acerque el token NFC *103* al dispositivo de autenticación *101.* No presenta novedad.

La reivindicación 9 describe posibles tipos de autorizaciones: un toque del usuario en una pantalla táctil del dispositivo de autenticación, agitar el dispositivo de autenticación, utilizar un sensor biométrico, y/o introducir en el dispositivo de autenticación un PIN o contraseña asociados a la credencial correspondiente. Son distintas alternativas que producen un efecto semejante al obtenido en D01. Sin actividad inventiva.

En la reivindicación 10, el conjunto de parámetros de acceso comprende un parámetro de horario y un parámetro de localización y comprobar el cumplimiento de dicho conjunto de parámetros de acceso comprende determinar si la hora y la localización asociadas a la solicitud de autenticación recibida por el primer dispositivo de comunicación cumplen los requisitos de hora y localización previamente definidos.
Esta característica no aparece en D01. El efecto técnico que implica esta diferencia es un mayor control en el acceso por hora y/o localización. El problema técnico objetivo es como añadir esos parámetros para obtener un mayor acceso.
No obstante, este detalle se encuentra recogido en D05 *(ver párrafo 27)*, que precisamente añade estos parámetros para proporcionar credenciales de acceso. No tiene actividad inventiva.

La reivindicación 11 establece que para comprobar los dispositivos de autenticación accesibles desde el dispositivo electrónico, el usuario selecciona su dispositivo de autenticación mediante una interacción con el dispositivo electrónico. Esto está implícito en cualquier proceso de emparejamiento entre dispositivos, aunque D01 no lo cite explícitamente, depende de la configuración. No implica esfuerzo inventivo.

La reivindicación número 12 menciona que la selección del dispositivo de autenticación, cuando haya varios accesibles desde el dispositivo electrónico, comprende los siguientes pasos:
- acercar el dispositivo de autenticación a una cierta distancia de un lector RFID/NFC en el dispositivo electrónico;
- proporcionar una dirección física del dispositivo de autenticación al dispositivo electrónico, donde la dirección física se proporciona directamente o mediante un identificador único.
D01 utiliza tecnología NFC entre el token *103* y el dispositivo de autenticación *101* y empareja los dispositivos *101* y *104,* si bien no menciona que ellos se comuniquen concretamente por NFC.
Sin embargo, aplicar la tecnología NFC descrita en D01 a la comunicación entre dichos dispositivos *101* y *104,* no se considera inventivo. Falta el parámetro de añadir una dirección física del dispositivo de autenticación al dispositivo electrónico (en NFC dada la necesidad de proximidad de ambos dispositivos no tiene sentido) pero aun así, se cita D06 que divulga esta característica. Sin actividad inventiva.

Las reivindicaciones 13 – 15 se refieren al sistema que implementa el método anterior y corren la misma suerte que sus semejantes (1, 3 y 10 respectivamente).
La reivindicación 16 es declarativa y va ligada a la primera reivindicación.

En resumen, las reivindicaciones 1-4, 8, 13, 14 y 16 no cumplen el requisito de novedad, según el Art. 6 y las reivindicaciones 5-7, 9-12 y 15 no tienen actividad inventiva para un experto en la materia según el Art. 8 de la Ley Española de Patentes.