(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
3 de septiembre de 2015 (03.09.2015) WIPO | PCT

(10) Número de Publicación Internacional
WO 2015/128523 A1

(51) Clasificación Internacional de Patentes:
G09C 1/00 (2006.01) *H04L 9/14* (2006.01)

(21) Número de la solicitud internacional:
PCT/ES2015/070118

(22) Fecha de presentación internacional:
23 de febrero de 2015 (23.02.2015)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(30) Datos relativos a la prioridad:
P201430260
26 de febrero de 2014 (26.02.2014) ES
P201430340 13 de marzo de 2014 (13.03.2014) ES

(71) Solicitante: **UNIVERSIDAD DE GRANADA** [ES/ES]; Hospital Real, Avda. del Hospicio S/n, E-18071 Granada (ES).

(72) Inventores: **CAMACHO PÁEZ, José**; OTRI - Universidad de Granada, Centro de Transferencia Tecnológica, 3ª planta, Gran Vía de Colón, 48, E-18071 Granada (ES). **MACIÁ FERNÁNDEZ, Gabriel**; OTRI - Universidad de Granada, Centro de Transferencia Tecnológica, 3ª planta, Gran Vía de Colón, 48, E-18071 Granada (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).

Publicada:

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

(54) **Title**: DEVICE, SYSTEM AND METHOD FOR THE SECURE EXCHANGE OF SENSITIVE INFORMATION OVER A COMMUNICATION NETWORK

(54) **Título** : DISPOSITIVO, SISTEMA Y PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN SENSIBLE EN UNA RED DE COMUNICACIÓN

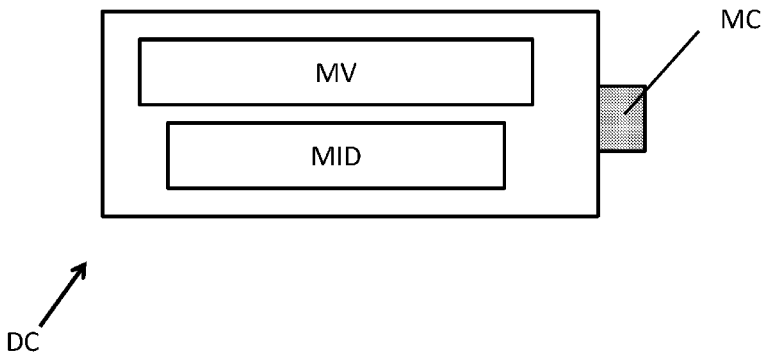

Figura 1

(57) **Abstract**: The invention ensures the secure transmission of sensitive information via the Internet, including by means of a non-reliable device (DNC). The invention relates to a reliable device (DC), to a system comprising said reliable device (DC), and to a method for the secure transmission of sensitive information by means of a system comprising the reliable device (DC).

(57) **Resumen**: La invención garantiza la seguridad al enviar información sensible por internet incluso mediante un dispositivo no confiable (DNC). Se describe un dispositivo confiable (DC), un sistema que comprende dicho dispositivo confiable (DC), y un procedimiento de envío seguro de información sensible mediante un sistema que comprende el dispositivo confiable (DC).

WO 2015/128523 A1

DISPOSITIVO, SISTEMA Y PROCEDIMIENTO PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN SENSIBLE EN UNA RED DE COMUNICACIÓN

OBJETO DE LA INVENCIÓN

La presente invención pertenece al campo de las comunicaciones, y más concretamente al campo de los sistemas y procedimientos de seguridad en el intercambio de información sensible a través de una red de comunicación, como por ejemplo Internet.

Un objeto de la presente invención es un nuevo dispositivo auxiliar seguro capaz de comunicarse con un dispositivo del usuario para firmar y cifrar la información sensible que éste va a intercambiar con un servidor de destino de tal modo que dicha información sólo pueda ser descifrada en dicho servidor. La información sensible no es accesible o modificable ni siquiera para el propio dispositivo del usuario, de modo que se evita la posibilidad de que malware residente en dicho dispositivo pueda acceder a ella o modificarla.

Otro objeto de la presente invención está dirigido a un sistema para el intercambio de información sensible que comprende un dispositivo auxiliar seguro como el descrito.

Otro objeto más de la invención está dirigido a un procedimiento de operación de un sistema para el intercambio de información sensible como el mencionado. Además, la invención también se extiende a programas de ordenador configurados para hacer que un dispositivo electrónico lleve a cabo dicho procedimiento y a aplicaciones en la nube basadas en dicho procedimiento.

ANTECEDENTES DE LA INVENCIÓN

En la actualidad, la utilización de dispositivos conectados a redes de comunicación, eminentemente Internet, para la consulta y envío de información está ampliamente extendida. Numerosas organizaciones ponen a disposición de sus clientes servicios de compras, consulta, almacenamiento de información, etc., a través de servicios telemáticos que hacen uso de las redes de comunicación. Un ejemplo notorio de este tipo de servicios es el servicio web. Este servicio permite a un usuario, mediante la utilización de un software de navegación (navegador), acceder a determinados servidores web en los que se le ofrece numerosos y variados servicios a través de diferentes tecnologías (HTML, CSS, Scripting,

etc.).

Dada la naturaleza sensible y confidencial de muchos de estos servicios (acceso a datos bancarios, datos de salud, envío de contraseñas, etc.), y con el objetivo de garantizar el éxito de los mismos, ha sido necesario el desarrollo paralelo de tecnologías de seguridad que permitieran al usuario tener la confianza necesaria para su utilización. En este campo se han realizado numerosos esfuerzos, encaminados a desarrollar tecnologías que permitan el envío seguro de información sin posibilidad de que ésta fuera accedida, modificada o replicada por terceras partes. Como resultado de estos esfuerzos, en la actualidad se puede destacar la utilización de dos protocolos seguros: IPSec y TLS, éste último utilizado en la denominada navegación web segura (HTTPS).

Las tecnologías comentadas persiguen establecer un túnel seguro entre los dispositivos finales conectados. En el caso de la navegación web segura, dichos dispositivos se corresponden con el navegador web y el servidor web. El túnel seguro es un recubrimiento criptográfico en el canal de comunicaciones, comprendiendo éste todos los medios de transmisión y dispositivos intermedios por lo que pasa la información compartida por los dispositivos finales. El recubrimiento criptográfico evita ciertos ataques a la seguridad por parte de intrusos que pudieran estar ubicados en algún punto del canal de comunicaciones. En primer lugar, evita que se pueda escuchar la información intercambiada (eavesdropping). En segundo lugar, evita que se pueda modificar, falsificar o replicar la información intercambiada (tampering) sin que este hecho se perciba por parte de los receptores. Finalmente, evita también el ataque denominado Man in the Middle (MitM), que consiste en hacer pensar a las dos entidades finales que se están comunicando entre sí, mientras que en realidad la comunicación se realiza en dos partes: entidad origen-intruso e intruso-entidad destino.

Aunque el uso de tecnologías tales como HTTPS permite alcanzar un grado de confianza alto en un servicio de este tipo, dichas tecnologías sólo se centran en evitar amenazas de seguridad o ataques en el canal de comunicaciones. Sin embargo, existe un elevado número de amenazas de seguridad localizadas directamente en los propios dispositivos de comunicación.

En efecto, en la actualidad, el número de virus y, en general, software malicioso (malware) se ha incrementado exponencialmente, haciendo vulnerable la utilización de los dispositivos de comunicación. La presencia de malware en un ordenador puede permitir a un atacante

robar la información que un usuario está introduciendo cuando accede a un determinado servicio, como por ejemplo la contraseña de acceso, el número de cuenta corriente, etc. Los atacantes han hecho evolucionar el malware de forma considerable para conseguir una funcionalidad muy avanzada que permite por ejemplo enviar al atacante lo que el usuario del ordenador teclea (keyloggers), o aquellas páginas por las que está navegando (spyware), etc. El malware puede ser un software independiente o estar oculto como parte de un software previamente instalado en el sistema (troyano). Un ejemplo importante relativo al servicio web es el denominado ataque *Man in the Browser* (MitB), que es el equivalente al MitM cuando lo que ha hecho el atacante es, en realidad, modificar el software del navegador.

Herramientas de última generación permiten el diseño de nuevo malware sin requerir conocimientos técnicos, lo que ha llevado a una explosión en el número de variantes de malware desarrollados por unidad de tiempo. Esta explosión cuestiona la viabilidad y eficacia de las herramientas tradicionales de detección de malware, los llamados antivirus, cuya base de datos difícilmente puede ser actualizada a la suficiente velocidad para realizar una detección exitosa. Adicionalmente, los atacantes diseñan el malware con mecanismos de ofuscación u ocultamiento que permiten en numerosos casos evitar su detección por parte de antivirus o antimalware.

Este efecto se ha agravado con la aparición y extensión de los denominados *smartphone*, los cuales permiten el acceso a muchos de los servicios a los que tradicionalmente se accedía mediante PC, pero en movilidad. Estos terminales han recibido la atención de los atacantes, los cuales han diseñado un alto porcentaje del malware para este tipo de plataformas. Debido a las limitaciones de batería de estos dispositivos, se suele limitar el uso de antivirus a los períodos de carga, lo que hace que la proliferación de malware esté siendo drástica.

Por otro lado, la actual tendencia en redes corporativas a la proliferación de accesos “Bring Your Own Device” (BYOD), donde el trabajador accede a su puesto de trabajo con un dispositivo de uso general, expone la seguridad de la red a dispositivos comprometidos con malware.

En resumen, en la actualidad, a pesar de la utilización de tecnologías de seguridad tales como las que se proporcionan en el protocolo HTTPS, dichas tecnologías no evitan el acceso de información sensible por parte de malware en el dispositivo del usuario.

DESCRIPCIÓN DE LA INVENCIÓN

Mientras que otras soluciones para conseguir comunicaciones seguras han evolucionado en la línea de tratar de asegurar que el dispositivo del usuario se mantenga seguro (antivirus, antimalware), la solución propuesta en este documento asume que no es posible mantener la seguridad en un dispositivo cuya configuración y funcionamiento es muy variable en el tiempo (instalación de aplicaciones, modificación de la configuración por el usuario, etc.), especialmente considerando la evolución actual en el desarrollo de código malware.

Por tanto, la presente invención se centra en extraer del dispositivo de usuario solamente aquellas funcionalidades imprescindibles para el envío y recepción de información sensible a través de la red y garantizar la seguridad en dichas funcionalidades. Además, esta invención aporta al usuario una percepción de seguridad adicional al ubicar estas funcionalidades en un dispositivo físico separado e independiente.

En definitiva, la presente invención resuelve los problemas anteriores gracias a que extiende la cobertura criptográfica al dispositivo del usuario, denominado aquí "dispositivo no confiable". Para ello, se propone la introducción de un nuevo dispositivo auxiliar,denominado "dispositivo confiable", que se conecta al dispositivo del usuario y que ejecutará un software muy reducido sobre el que no se podrá instalar software de terceros. Se evita así la posibilidad de infección por malware, ya que un atacante no podrá aprovechar la existencia de fallos y vulnerabilidades en el software del "dispositivo confiable" para ejecutar un ataque y modificar su funcionamiento.

Es más, ni siquiera se permite la instalación o modificación de software o firmware de este novedoso "dispositivo confiable" por parte del usuario. Esto garantiza que no se pueda modificar tampoco por parte de un atacante el funcionamiento del dispositivo. Como se explicará más adelante en la descripción detallada de la invención, en todo caso solamente se permitirá la realización de ciertas actualizaciones en el software orientadas a eliminar potenciales riesgos de seguridad, siempre bajo ciertas circunstancias y en un entorno muy controlado, de forma que se garantice que no se produce instalación alguna de malware.

Adicionalmente, el "dispositivo confiable" de la invención podrá establecer un túnel seguro con un servidor, de manera que el dispositivo del usuario (ej. smartphone, tablet, portátil), y por tanto el malware instalado en el mismo, no pueda acceder o modificar la información

sensible así enviada.

A lo largo de la presente invención se utilizarán una serie de términos cuyo significado se describe a continuación:

Envío de información en una red de comunicaciones: Se entenderá por "*envío de información en una red de comunicaciones*" como el envío de datos con significado utilizando una determinada tecnología de comunicaciones.

Dispositivo Confiable: Se entenderá por "*dispositivo confiable*", o DC, un dispositivo que interviene en la comunicación entre dos entidades, posibilitando que dicha información sea intercambiada de forma segura entre el dispositivo y la entidad destino, incluso a través de una entidad origen no confiable.

Dispositivo No Confiable: Se entenderá por "*dispositivo no confiable*", o DNC, un dispositivo sobre el cual no hay garantía de seguridad. A modo de ejemplo, los smartphones, tablets, PCs, etc. que se comunican a través de Internet se consideran dispositivos no confiables.

Entidad: Se entenderá por "*entidad*" cualquier dispositivo que participe en una comunicación.

Entidad Origen: Se entenderá por "*entidad origen*" aquella que inicia una comunicación.

Entidad Destino: Se entenderá por "*entidad destino*" aquella que responde a la solicitud de comunicación en una entidad origen.

Servidor: Se entenderá por "*servidor*" aquel proceso, o por extensión dispositivo que ejecuta dicho proceso, que ofrece algún tipo de servicio telemático en una red de comunicaciones.

Servicio Telemático: Se entenderá por "*servicio telemático*" cualquier tipo de actividad realizada en una red de comunicaciones como respuesta a una solicitud de una entidad cliente.

Cliente: Se entenderá por "*cliente*" aquel proceso, o por extensión programa o dispositivo que ejecuta dicho proceso, que solicita algún tipo de servicio telemático en una red de comunicaciones.

Proxy: Se entenderá por "*proxy*" aquel proceso, o por extensión programa o dispositivo que ejecuta dicho proceso, que actúa como intermediario a nivel de aplicación entre un servidor y un cliente en algún tipo de servicio telemático en una red de comunicaciones. En particular, el proxy puede ser el propio servidor.

Servidor de Seguridad: Se entenderá por "*servidor de seguridad*" aquél dispositivo que permita, con su participación, establecer comunicaciones seguras entre otros dos dispositivos.

Comunicaciones Seguras: Se entenderá por "*comunicaciones seguras*" aquellas que garanticen la integridad y privacidad de la comunicación.

Certificado Digital: Se entenderá por "*certificado digital*" aquél documento software que incluye la identificación de una entidad, la clave pública emitida por dicha entidad y que está firmado por la firma digital de una Autoridad Certificadora cuya clave pública está disponible públicamente.

Firma Digital: Se entenderá por "*firma digital*" de un documento software al resultado de aplicar a dicho documento un algoritmo de firma con una clave privada de una entidad, y que puede ser cotejado utilizando un algoritmo de comprobación con la clave pública de la misma. La "firma digital" se añade al documento software para que pueda ser cotejada por el receptor del mismo.

Clave privada: Se entenderá por "*clave privada*" de una entidad a una clave software generada por la misma conjuntamente con la clave pública y mantenida en secreto para su uso en cifrado asimétrico.

Clave pública: Se entenderá por "*clave pública*" de una entidad a una clave software generada por la misma conjuntamente con la clave privada y hecha pública para su uso en cifrado asimétrico.

Autoridad Certificadora: Se entenderá por "*autoridad certificadora*", o AC, aquella entidad cuya firma digital permite, sin participación de terceros, aceptar la validez de un documento software.

Documento Software: Se entenderá *por "documento software" cualquier* fichero digital.

Red: Se entenderá por "*red*" cualquier tecnología, incluidos dispositivos de interconexión, que permita la comunicación de información entre dos o más entidades, como por ejemplo Internet o las redes de comunicaciones móviles GSM, UMTS, u otras.

La invención consiste en un dispositivo (en adelante "*dispositivo confiable*" o DC) que interviene en la comunicación entre un dispositivo de usuario (en adelante, "*dispositivo no confiable*" o DNC) y un servidor de destino (en adelante, "*servidor*" o S) cuando la información a intercambiar es sensible, de tal modo que garantiza que dicha información sea intercambiada de forma segura incluso a pesar de llevar a cabo la comunicación a través del dispositivo no confiable (DNC). Para ello, el dispositivo confiable (DC) firma y cifra la información sensible utilizando una o varias claves desconocidas para el dispositivo no confiable (DNC), de manera que dicho dispositivo no confiable (DNC)no pueda acceder a o modificar dicha información sensible introducida por el usuario. De esta forma, se evita que cualquier malware residente en el dispositivo no confiable (DNC) pueda intervenir o modificar la información.

Además, para evitar la posibilidad de que el propio dispositivo confiable (DC) pueda ser infectado por software malicioso o malware, el dispositivo confiable (DC)tendrá restringida la instalación de software de terceros.

Un primer aspecto de la invención está dirigido a un dispositivo confiable (DC) para el intercambio seguro de información en una red de comunicación entre un usuario y un servidor (S), donde dicho dispositivo confiable (DC) fundamentalmente comprende los siguientes elementos:

a) Medio de visualización (MV)

El medio de visualización permite al dispositivo confiable (DC) mostrar instrucciones o datos al usuario. En principio puede implementarse de diferentes modos, aunque de acuerdo con una realización particular, puede tratarse de una pantalla LCD o una pantalla táctil.

b) Medio de introducción de datos (MID)

El medio de introducción de datos permite que el usuario pueda introducir la información sensible que desea transmitir en el dispositivo confiable (DC) para su posterior envío. Preferentemente se utiliza un teclado alfanumérico o una pantalla táctil. Evidentemente, en caso de utilizar una pantalla táctil ésta constituirá conjuntamente tanto el medio de visualización (MV) como el medio de introducción de datos (MID).

c) Medio criptográfico

El medio criptográfico se encarga de firmar y cifrarla información sensible introducida por el usuario de tal modo que dicha información sensible no sea accesible o modificable por el dispositivo no confiable (DNC). Similarmente, este mismo medio descifrará y autenticará la información sensible que pueda recibirse como respuesta desde el servidor (S), y que sigue sin ser accesible para el dispositivo no confiable (DNC). Así, a pesar de que el dispositivo confiable (DC) se comunica siempre a través del dispositivo no confiable (DNC), este último no puede acceder a la información sensible cifrada o modificarla, y por tanto cualquier posible malware presente en dicho dispositivo no confiable (DNC) resulta inocuo. El modo en que se realiza la firma y cifrado se describirá más adelante con referencia al procedimiento de operación de este sistema de comunicación.

d) Medio de conexión (MC)

Se trata de un medio de conexión con dicho dispositivo no confiable (DNC) para comunicar la información sensible firmada y cifrada a dicho dispositivo no confiable (DNC) para su transmisión al servidor (S) y recibir información del mismo. El medio de conexión puede ser cableado o bien puede utilizarse una conexión inalámbrica. Por ejemplo, de acuerdo con realizaciones preferidas de la invención, se puede utilizar una conexión USB, una conexión WiFi, o una conexión Bluetooth.

e) Medio de comprobación

El medio de comprobación de software comprueba la legitimidad de un software que se ejecuta en el dispositivo confiable (DC) mediante la comprobación de que una firma digital del software emitida por una autoridad certificadora (AC) es válida.

Además, el dispositivo confiable (DC) de la invención está configurado de tal modo que dicho software o bien no es modificable, o bien sólo es modificable si el nuevo software está firmado por una entidad con un certificado digital válido. Es decir, el dispositivo confiable (DC) nopermite ninguna actualización de software salvo, en todo caso, software que esté firmado con un certificado emitido por una autoridad certificadora (AC) o por un servidor seguro (SS) con certificado válido. Un ejemplo de autoridad certificadora (AC) es la Fábrica Nacional de Moneda y Timbre. En el caso de la invención, la autoridad certificadora (AC) podrá ser creada expresamente y, por tanto, estar únicamente destinada a firmar los certificados y el software de los elementos constituyentes de la invención.

El dispositivo confiable (DC) puede así tener una interfaz que permita la actualización del firmware o software del dispositivo de forma controlada. En este procedimiento de actualización, para evitar la instalación de software malicioso, se podrá habilitar un mecanismo seguro, implementado en hardware o firmware y no modificable, para comprobar que el nuevo software está firmado con el certificado de la autoridad certificadora (AC) o por un servidor seguro (SS) con certificado válido.

El objetivo de este diseño, tal y como se ha justificado anteriormente, es minimizar la funcionalidad del dispositivo confiable (DC) para evitar su manipulación por parte de algún software malicioso o malware. De ese modo, se puede asegurar que implementa exclusivamente las funcionalidades para las que está diseñado.

La presente invención también está dirigida a un sistema para el envío seguro de información sensible en una red de comunicación que comprende:

a) Dispositivo no confiable (DNC)

Se trata del dispositivo que utiliza el usuario normalmente para intercambiar información con diversos servidores a través de una red de comunicación (RC), como Internet. Por ejemplo, puede tratarse de un teléfono móvil "inteligente", o smartphone, una tableta, un ordenador, etc.

b) Servidor (S)

Se trata de un servidor (S) en comunicación con el dispositivo no confiable (DNC) a través de la red de comunicación (RC). Por ejemplo, puede ser el servidor (S) donde se aloja la página web del banco del usuario.

c) Servidor de seguridad (SS)

El servidor de seguridad (SS) está en comunicación con el servidor (S) para descifrar y autenticar la información sensible que se envía a dicho servidor (S) por el dispositivo confiable (DC) o firmar y cifrar la información sensible en el sentido inverso de la comunicación. A este respecto, nótese que pueden existir múltiples servidores de seguridad (SS) asociados a diferentes servidores (S).

d) Proxy (P)

El proxy (P) es un dispositivo intermediario entre la comunicación del dispositivo no confiable (DNC) y el servidor (S) que sirve para derivar la información sensible al servidor seguro (SS) para su firma y cifrado o descifrado y autenticación.

d) Dispositivo confiable (DC)

Se trata de un dispositivo confiable (DC) según la descripción anterior que recibe, firma y cifra la información sensible introducida por un usuario para su envío a un servidor (S),o recibe, descifra y autentica la información desde el servidor (S) al usuario, utilizando una clave o claves (K_2) compartida/s exclusivamente por dicho dispositivo confiable (DC) y el servidor de seguridad (SS). El dispositivo confiable (DC) está en comunicación con el dispositivo no confiable (DNC) para transmitirle o recibir dicha información sensible.

e) Autoridad certificadora (AC)

La autoridad certificadora se encarga de firmar los certificados digitales del servidor de seguridad (SS) y del dispositivo confiable (DC) para verificar su legitimidad. También podrá encargarse de firmar el código de actualización de firmware del dispositivo confiable (DC), en su caso.

En otra realización, el servidor seguro (SS) y el proxy (P) están implementados en la misma máquina física. En otra realización, el servidor (S) y el proxy (P) están implementados en la misma máquina física. En otra realización, el servidor (S), el servidor seguro (SS) y el proxy (P) están implementados en la misma máquina física.

Un tercer aspecto de la presente invención está dirigido a un procedimiento para el intercambio seguro de información sensible en una red de comunicación por medio del sistema que se acaba de describir. Preferentemente, este procedimiento se ejecuta cuando bien el usuario o bien el servidor (S) determina que se va a intercambiar información sensible durante una sesión convencional de comunicación entre ambos, y lo notifican al DC como se describirá con mayor detalle más adelante en este documento.

En una realización, el procedimiento se emplea para que un usuario, típicamente una persona, a través de un DC, envíe datos privados de forma segura a un servidor. Este procedimiento es de utilidad, por ejemplo, para el envío de contraseñas, número PIN, y similares en la autenticación en sistemas de acceso telemático.

En otra realización, el procedimiento se emplea para que un servidor remita información privada a un usuario a través de su DC. Este caso es de utilidad, por ejemplo, para la confirmación de operaciones bancarias, como una alternativa al uso del SMS tan extendido en la autenticación en dos factores.

En ambas realizaciones, se llevan a cabo los siguientes pasos:

1) El dispositivo confiable (DC) se comunica, a través del dispositivo no confiable (DNC) y de la red de comunicación (RC), con el servidor seguro (SS) y establece una sesión de comunicación segura con dicho servidor seguro (SS) para obtener una o varias claves (K_2) seguras compartidas exclusivamente por dicho dispositivo confiable (DC) y dicho servidor seguro (SS).

El establecimiento de la sesión de comunicación segura entre el dispositivo confiable (DC) y el servidor seguro (SS) preferentemente comprende a su vez los siguientes pasos previos:

- El dispositivo no confiable (DNC) comprueba que está conectado con el dispositivo confiable (DC).

- El dispositivo no confiable (DNC) comprueba que el servidor (S) dispone de un servidor seguro (SS) asociado.
- El dispositivo no confiable (DNC) envía al dispositivo confiable (DC) la dirección IP del servidor seguro (SS).

Además, el establecimiento de una sesión de comunicación segura entre el dispositivo confiable (DC) y el servidor seguro (SS) a través del dispositivo no confiable (DNC) para obtener la/s clave/s segura/s (K_2) se realiza de acuerdo con un segundo protocolo ($PROT_2$), preferentemente el protocolo TLS Handshake.

A partir de este punto, los pasos seguidos dependen de si la información sensible es enviada desde el usuario al servidor (S) o en sentido inverso.

En el primer caso, en el que es el usuario el que envía la información sensible, los pasos seguidos son:

2.a) Un usuario introduce información sensible en el dispositivo confiable (DC) a través del medio de introducción de datos (MID).

3.a) El dispositivo confiable (DC) envía al dispositivo no confiable (DNC) la información sensible firmada y cifrada con K_2.

4.a) El dispositivo no confiable (DNC) envía, a través de la red de comunicación (RC), la información sensible firmada y cifrada con K_2 como parte de un mensaje al proxy (P)

De acuerdo con una realización preferida de la invención, antes de este envío se lleva a cabo el paso adicional de identificar, por parte del dispositivo no confiable (DNC), la información sensible recibida del dispositivo confiable (DC) por medio de una etiqueta que permite al proxy (P) reconocer dicha información dentro del mensaje. Otra opción es que el propio dispositivo confiable (DC) haya llevado a cabo esta operación en alguno de los pasos anteriores, de modo que la información sensible ya esté identificada con una etiqueta cuando llega al dispositivo no confiable (DNC).

Por otro lado, preferentemente la comunicación entre el dispositivo no confiable (DNC) y el proxy (P) a través de la red de comunicación (RC) se realiza de acuerdo con un primer protocolo ($PROT_1$) que puede elegirse de entre la siguiente lista: http, https, ftp, ssh y smtp.

5.a) El proxy (P) detecta la existencia de información sensible y la envía al servidor seguro (SS).

6.a) El servidor seguro (SS) descifra y autentica la información sensible recibida y la envía descifrada al proxy (P).

7.a) El proxy (P) remite el mensaje completo al servidor (S).

Si, alternativamente, es el servidor (S) el que remite la información sensible, los pasos son los siguientes:

2.b) El servidor (S) remite al proxy (P) un mensaje que incluye la información sensible convenientemente etiquetada.

3.b) El proxy (P) detecta la existencia de información sensible y la envía al servidor seguro (SS).

4.b) El servidor seguro (SS) envía al proxy (P) la información sensible firmada y cifrada con la clave o claves (K_2) correspondientes al DC destino.

5.b) El proxy (P) envía, a través de la red de comunicación (RC), la información sensible firmada y cifrada con K_2 al dispositivo no confiable (DNC).

6.b) El dispositivo no confiable (DNC) detecta la existencia de información sensible y la envía al dispositivo confiable (DC).

7.b) El dispositivo confiable (DC) descifra y autentica la información sensible recibida y la muestra en el medio de visualización (MV).

En otra realización preferida más, la comunicación correspondiente a los pasos 3.a, 4.a y 5.a o los pasos 4.b, 5.b y 6.b entre el dispositivo confiable (DC) y el servidor seguro (SS)

que se realiza a través del dispositivo no confiable (DNC), la red de comunicación (RC), y el proxy (P) para el envío de la información sensible firmada y cifrada con la clave o claves seguras (K_2) se realiza de acuerdo con un tercer protocolo ($PROT_3$), como el TLS Record Protocol.

En otra realización, los pasos 6.a y 7.a se sustituyen por una comunicación directa entre el servidor seguro (SS) y el servidor (S). En otra realización, los pasos 2.b y 3.b se sustituyen por una comunicación directa entre el servidor (S) y el servidor seguro (SS).

Es fácil apreciar que con este procedimiento la información sensible transmitida no ha sido nunca accesible para el dispositivo no confiable (DNC), quedando así a salvo de posibles ataques relacionados con software malicioso presente en dicho dispositivo no confiable (DNC). Más adelante en el presente documento se describe con mayor detalle este procedimiento con referencia a las figuras.

La invención descrita está dirigida a dispositivos dotados de una funcionalidad similar a la de un ordenador, incluyendo smartphones o teléfonos inteligentes, tabletas, portátiles, ordenadores, servidores, etc., así como a procesos ejecutados en tales dispositivos. Sin embargo, la invención se extiende no sólo a tales dispositivos y procesos, sino también a programas de ordenador adaptados para que cualquiera de tales equipos pueda llevar a la práctica dichos procesos. Tales programas pueden tener la forma de código fuente, código objeto, una fuente intermedia de código y código objeto, por ejemplo, como en forma parcialmente compilada, o en cualquier otra forma adecuada para uso en la puesta en práctica de los procesos según la invención. Los programas de ordenador también abarcan aplicaciones en la nube basadas en dicho procedimiento.

En particular, la invención abarca programas de ordenador dispuestos sobre o dentro de una portadora. La portadora puede ser cualquier entidad o dispositivo capaz de soportar el programa. Cuando el programa va incorporado en una señal que puede ser transportada directamente por un cable u otro dispositivo o medio, la portadora puede estar constituida por dicho cable u otro dispositivo o medio. Como variante, la portadora podría ser un circuito integrado en el que va incluido el programa, estando el circuito integrado adaptado para ejecutar, o para ser utilizado en la ejecución de, los procesos correspondientes.

Por ejemplo, los programas podrían estar incorporados en un medio de almacenamiento, como una memoria ROM, una memoria CD ROM o una memoria ROM de semiconductor,

una memoria USB, o un soporte de grabación magnética, por ejemplo, un disco flexible o un disco duro. Alternativamente, los programas podrían estar soportados en una señal portadora transmisible. Por ejemplo, podría tratarse de una señal eléctrica u óptica que podría transportarse a través de cable eléctrico u óptico, por radio o por cualesquiera otros medios.

BREVE DESCRIPCIÓN DE LAS FIGURAS

La Fig. 1 muestra un esquema simplificado de un dispositivo confiable (DC) de acuerdo con la invención.

La Fig. 2 muestra un esquema general del sistema de la invención.

La Fig. 3 muestra de manera esquemática los protocolos de comunicación empleados para llevar a cabo el procedimiento de acuerdo con la presente invención.

La Fig. 4 muestra las torres de protocolos utilizadas en el envío de información sensible entre dispositivo confiable (DC) y el servidor seguro (SS).

La Fig. 5 muestra un esquema general del sistema de la invención cuando el servidor (S) y el proxy (P) están implementados en la misma máquina física.

La Fig. 6 muestra de manera esquemática los protocolos de comunicación empleados para llevar a cabo el procedimiento de acuerdo con la presente invención cuando el servidor (S) y el proxy (P) están implementados en la misma máquina física.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

Se describe a continuación con mayor detalle un ejemplo de procedimiento de acuerdo con la presente invención haciendo referencia a las figuras adjuntas.

La Fig. 1 muestra esquemáticamente un dispositivo confiable (DC) donde se aprecia el medio de visualización (MV) o pantalla a través de la cual se muestran datos al usuario y el medio de introducción de datos (MID) o teclado para que el usuario pueda introducir la información sensible. Como se ha comentado anteriormente, estos dos elementos podrían

estar integrados en un único elemento en caso de que se emplee una única pantalla táctil, o incluso pertenecer a dispositivos distintos (por ejemplo, pantalla y teclado independientes). Se aprecia también el medio de comunicación (MC) con el dispositivo no confiable (DNC). Por ejemplo, puede ser una conexión de tipo USB o Bluetooth.

El dispositivo confiable (DC) también comprende un medio criptográfico de la información sensible que se va a enviar y un medio de comprobación de software. Sin embargo, estos medios no aparecen representados en la Fig. 1 por estar implementados a través de procesos gobernados por el software del propio dispositivo confiable (DC). Además, como se ha descrito previamente en este documento, el dispositivo confiable (DC) está configurado de tal modo que no permite la modificación de su software interno excepto en casos muy particulares.

La Fig. 2 muestra un ejemplo de sistema para el envío seguro de información sensible según la presente invención. Se aprecia cómo el dispositivo confiable (DC) está en comunicación con el dispositivo no confiable (DNC), el cual, a su vez, se puede comunicar con el proxy (P) a través de la red de comunicación (RC). Un servidor seguro (SS) también conectado a la red de comunicación (RC) descifrará y autenticará la información sensible enviada desde el dispositivo confiable (DC) y firmará y cifrará la información sensible enviada hacia el dispositivo confiable (DC). Un servidor (S) también conectado a la red de comunicación (RC) llevará a cabo el servicio telemático tradicional.En otra realización preferida más, tanto el servidor (S) como el servidor seguro (SS) conectan a la red de comunicación (RC) a través del proxy (P), en lugar de directamente.

El dispositivo confiable (DC) puede disponer de un certificado ($CERT_{DC}$) y el servidor de seguridad (SS) puede disponer de un certificado ($CERT_{SS}$). Estos certificados permitirán su autenticación y el establecimiento de una sesión segura entre ambos. La Fig. 2 también muestra la autoridad certificadora (AC) que firmará dichos certificados ($CERT_{DC}$) y ($CERT_{SS}$). El caso particular en el que el servidor (S) y el proxy (P) están implementados en la misma máquina se puede ver representado esquemáticamente en la Figura 5.

Aunque aquí se ha representado el proxy (P), el servidor (S) y el servidor seguro (SS) como entidades diferentes, sería posible que todos o algunos de ellos estuviesen alojados en la misma máquina, en cuyo caso podrían estar implementados por procesos diferentes. De la misma forma, podría existir un servidor seguro (SS) asociado a cada uno de los servidores (S) de una misma corporación, o bien existir un servidor seguro (SS) asociado a un grupo de

servidores (S). Cualquier alternativa sería válida siempre que se mantenga la funcionalidad aquí descrita.

A continuación, según se ha representado esquemáticamente en la Figura 3, se describen los mecanismos y protocolos de comunicación entre las entidades descritas que componen el ejemplo de sistema de la invención. La Figura 6 representa esquemáticamente el caso particular en el que servidor (S) y el proxy (P) están implementados en la misma máquina física.

a) Comunicación dispositivo no confiable (DNC) - proxy (P).

Se trata de una comunicación basada en un protocolo tradicional ($PROT_1$) de comunicaciones, como HTTP, HTTPS, FTP, SMTP, etc. En caso de utilizar un protocolo seguro (como HTTPS), la información transmitida en esta conexión va cifrada con una clave K_1 compartida entre el dispositivo no confiable (DNC) y el proxy (P), que ha sido generada de forma segura siguiendo las reglas de funcionamiento de un protocolo como TLS.

El protocolo seguro HTTPS puede requerir que el proxy (P) disponga de un certificado convenientemente firmado por una autoridad certificadora, que en principio será distinta a la autoridad certificadora (AC) del sistema. Esto es así con el objetivo de que el protocolo ($PROT_1$) pueda seguir los estándares de uso más extendidos de forma que sea compatible con el mayor número posible de dispositivos y sistemas.

La realización de la invención requiere incluir ciertos elementos adicionales en $PROT_1$. En primer lugar, el proxy (P) debe publicar que puede realizar conexiones seguras de acuerdo a la presente invención. Para ello, al enviar una solicitud de información, por ejemplo un formulario, incluirá un meta parámetro (meta-tag) con la información de acceso al servidor seguro (SS):

```
<meta name="secure_server" content="secs.midominio.es:port">
```

Con objeto de que el proxy (P) y/o el dispositivo no confiable (DNC) puedan distinguir los elementos de información sensible remitida (a los que se hace referencia a

continuación como SEC), dicha información será destacada con una etiqueta o "*tag*" específica para tal propósito, por ejemplo:

```
<secret> SEC </secret>
```

b) Comunicación dispositivo confiable (DC) - servidor (S).

Esta comunicación constituye el núcleo de la invención, ya que es la que permite el envío de la información sensible a través del trayecto dispositivo confiable (DC) - dispositivo no confiable (DNC) - red de comunicación (RC) –proxy (P) - servidor (S) sin que el dispositivo no confiable (DNC) pueda obtener información alguna sobre los datos sensibles transmitidos. La comunicación se realiza en dos fases, cada una controlada por un protocolo diferente.

1. Establecimiento de una sesión segura entre dispositivo confiable (DC) y el servidor seguro (SS) ($PROT_2$).

El establecimiento de una sesión segura entre el dispositivo confiable (DC) y el servidor de seguridad (SS) requiere que se cumplan, al menos, tres condiciones:

i) que el dispositivo confiable (DC) esté conectado al dispositivo no confiable (DNC),

ii) que el servidor (S) disponga de un servidor de seguridad (SS) asociado, y

iii) que el dispositivo confiable (DC) pueda establecer la localización del servidor seguro (SS).

Las dos primeras condiciones pueden ser comprobadas por parte del dispositivo no confiable (DNC), que puede a su vez remitir la información requerida al dispositivo confiable (DC) para cumplir la tercera condición. Este hecho no implica ninguna vulnerabilidad en el sistema que implique el riesgo de captación de los datos sensibles por el dispositivo no confiable (DNC): si el dispositivo no confiable (DNC) no responde a la comunicación con el dispositivo confiable (DC) o si no confirma la existencia de un servidor seguro (SS), no se remitirán los datos sensibles.

La comprobación de la conexión del dispositivo confiable (DC) al dispositivo no confiable (DNC), condición *(i)*, se puede llevar a cabo con la instalación en el dispositivo no confiable (DNC) de un driver específico para el dispositivo confiable (DC) que avise de cuándo se ha producido la inserción/conexión de este último en/con el primero.

La disponibilidad de un servidor de seguridad (SS), condición *(ii)*, puede ser transmitida por el proxy (P) al dispositivo no confiable (DNC) como parte de la comunicación entre ambos usando el protocolo ($PROT_1$). Por ejemplo, si el protocolo ($PROT_1$) es el protocolo HTTP, la disponibilidad de un servidor seguro (SS) puede ser publicada en el código fuente de la propia página web que contenga cualquier formulario con solicitud de datos susceptibles de ser sensibles. Para ello, se incluirá en la página web remitida con el formulario el nombre de dominio o bien la dirección IP del servidor seguro (SS). Si se incluyera el nombre de dominio, sería el dispositivo no confiable (DNC) el encargado de convertirlo a una dirección IP accesible. Finalmente, el dispositivo no confiable (DNC) remitirá al dispositivo confiable (DC) la dirección IP del servidor seguro (SS) para que éste último inicie la conexión, condición *(iii)*. Éste último paso tampoco implica una vulnerabilidad del sistema que pudiera consistir en el envío por parte del dispositivo no confiable (DNC) de una IP falsa que redireccionara las comunicaciones del dispositivo confiable (DC) a un servidor falso controlado por un potencial atacante, ya que las comunicaciones seguras aseguran la identidad de los dos extremos de la comunicación, o al menos del servidor seguro (SS), con los certificados firmados por la autoridad certificadora (AC).

A partir de este momento, el dispositivo confiable (DC) podrá iniciar una sesión segura con el servidor seguro (SS). Dado que el dispositivo confiable (DC) no dispone de una interfaz de red propia, debe utilizar al dispositivo no confiable (DNC) como puente para establecer dicha sesión. El dispositivo no confiable (DNC) debe actuar en este caso como un mero intermediario entre el dispositivo confiable (DC) y el servidor de seguridad (SS), reenviando los mensajes entre uno y otro. La sesión segura debe asegurar la confidencialidad e integridad de la información así como evitar los ataques de repetición. Adicionalmente, se deberá comprobar la identidad de, al menos, el servidor seguro (SS), que la acreditará con el certificado ($CERT_{SS}$), firmado

por la autoridad certificadora (AC).Idealmente se comprobará también la identidad del dispositivo confiable (DC), si éste dispone del certificado ($CERT_{DC}$), para evitar la potencial proliferación de réplicas fraudulentas del dispositivo confiable (DC) que realicen conexiones con terceros servidores para robar la información sensible. Es ésta la razón por la que, sin pérdida de generalidad, se concibe la existencia de una autoridad certificadora (AC) que firma los certificados para ambos dispositivos. La negociación correspondiente a los algoritmos criptográficos a utilizar durante la sesión segura, así como las claves asociadas y la comprobación de certificados de autenticación, se llevará a cabo durante el establecimiento de la conexión.

Para el ($PROT_2$), que es un protocolo de establecimiento de sesión segura, se puede recurrir a estándares bien conocidos, como por ejemplo el TLS Handshake Protocol (TLSHP, RFC 2246). Dicho protocolo permite que dos entidades negocien de forma segura un conjunto de parámetros para establecer una sesión segura. En particular, se negocian los algoritmos de compresión, integridad y cifrado de los datos utilizados en ambos finales, así como las correspondientes claves para su uso en ambas direcciones de la comunicación. Si se usa TLSHP, el dispositivo no confiable (DNC) actuará como proxy TLS. Cada sesión segura se identifica con un identificador de sesión segura (ISS), de forma que el servidor seguro (SS) pueda identificar al dispositivo confiable (DC) que envía los datos y pueda descifrar y autenticar, o firmar y cifrar, con la clave o claves K_2 correspondiente.

En definitiva, como resultado final de este protocolo ($PROT_2$) se habrá establecido una sesión segura entre el dispositivo confiable (DC) y el servidor seguro (SS), que será identificada mediante un identificador de sesión segura (ISS), junto con una o varias claves compartidas entre ambas entidades (K_2) con la que firmar y cifrar la información intercambiada.

2. Envío de la información sensible a través de un túnel entre el dispositivo confiable (DC) y el servidor seguro (SS) ($PROT_3$).

Una vez realizado el establecimiento de la sesión segura entre el dispositivo confiable (DC) y el servidor seguro (SS), obteniéndose la clave K_2, el envío de la información sensible se realizará como se describe a continuación.

Envío de información sensible desde el usuario hacia el servidor (S). Cuando la información sensible se envía desde el usuario hacia el servidor(S), dicha información se encapsulará en un túnel seguro que se establece entre el dispositivo confiable (DC) y el servidor seguro (SS), para posteriormente ser enviada hacia el servidor (S). En esta comunicación se siguen los siguientes pasos:

- En primer lugar, el dispositivo confiable (DC) realiza las transformaciones necesarias sobre la información para su envío seguro de acuerdo a la negociación en el inicio de la sesión del protocolo ($PROT_2$). En concreto, dicha información seráfirmada y cifrada de forma segura utilizando la clave o claves K_2 obtenida mediante el protocolo ($PROT_2$)de forma que no pueda ser interpretada en ningún punto intermedio de la comunicación, incluido el dispositivo no confiable (DNC). Adicionalmente, incorporará el identificador de la sesión segura (ISS) con cuyo material criptográfico se ha cifrado y firmado la información ($PROT_3$).

- En segundo lugar, el dispositivo confiable (DC) remitirá la información al dispositivo no confiable (DNC) usando el protocolo ($PROT_4$), que se describirá más adelante.

- El dispositivo no confiable (DNC) incorporará la información cifrada recibida al mensaje que enviará al proxy (P), basado en el protocolo ($PROT_1$). Para ello, debe identificar la información sensible enviada, por ejemplo a través de una etiqueta (ej. <secret>). Dicha etiqueta podría ser incorporado por el dispositivo no confiable (DNC) en este paso o por el dispositivo confiable (DC) en uno de los pasos anteriores.

- El proxy (P), al recibir el mensaje, detectará el distintivo de información sensible (ej. <secret>) y remitirá la información sensible al servidor seguro (SS) usando el protocolo ($PROT_5$), que se describirá más adelante.

- El servidor seguro (SS) comprobará el ISS de la información sensible cifrada recibida y, si se corresponde con alguna sesión activa, procederá a descifrar la información de acuerdo los parámetros negociados para la misma con el protocolo ($PROT_2$). Si todo es correcto, remitirá la información descifrada al proxy (P) usando el protocolo ($PROT_5$), que se describirá más adelante.

- El proxy (P) sustituirá la información sensible cifrada por la recibida en el paso anterior y la enviará al servidor usando el protocolo ($PROT_6$), que se describirá más adelante.

- El servidor interpretará la información de forma convencional.

Envío de información sensible desde el servidor (S) hacia el usuario. Alternativamente, el envío de información sensible se puede originar en el servidor (S) con destino al usuario. En este caso, se siguen los siguientes pasos:

- El servidor (S) envía el mensaje al proxy (P) siguiendo el protocolo ($PROT_6$) que se describe más adelante. En éste, debe identificar la información sensible enviada, por ejemplo a través de una etiqueta (ej. <secret>).

- El proxy (P), al recibir el mensaje, detectará el distintivo de información sensible (ej. <secret>) y remitirá la información sensible al servidor seguro (SS) usando el protocolo ($PROT_5$), que se describirá más adelante.

- El servidor seguro (SS) realiza las transformaciones necesarias (cifrado y firmado) sobre la información para su envío seguro, de acuerdo a la negociación en el inicio de la sesión del protocolo ($PROT_2$). En concreto, dicha información será firmada y cifrada de forma segura utilizando la clave o claves K_2 obtenida mediante el protocolo ($PROT_2$) de forma que no pueda ser interpretada en ningún punto intermedio de la comunicación, incluido el dispositivo no confiable (DNC). Adicionalmente, incorporará el identificador de

la sesión segura (ISS) con cuyo material criptográfico se ha cifrado y firmado la información.

- El servidor seguro (SS) remitirá la información de nuevo al proxy (P) usando el protocolo ($PROT_5$), que se describirá más adelante.

- El proxy (P) incorporará la información cifrada recibida al mensaje que enviará al dispositivo no confiable (DNC), basado en el protocolo ($PROT_1$).

- El dispositivo no confiable (DNC), al recibir la información, detectará el distintivo de información sensible (ej. <secret>) y remitirá dicha información al dispositivo confiable (DC) usando el protocolo ($PROT_4$), que se describirá más adelante.

- El dispositivo confiable (DC) comprobará el ISS de la información sensible cifrada recibida y, si se corresponde con alguna sesión activa, procederá a descifrar la información de acuerdo los parámetros negociados para la misma con el protocolo ($PROT_2$). Si todo es correcto, mostrará la información en el medio de visualización (MV).

Se puede observar que la información sensible enviada viajafirmada y cifrada con la clave o claves K_2, compartida entre el dispositivo confiable (DC) y el servidor seguro (SS), a través de la red de comunicación (RC) y el dispositivo no confiable (DNC) sin que ninguno pueda obtener información alguna sobre la información original o modificarla, tal y como se pretende en esta invención. En la Figura 4 se puede observar la torre de protocolos en el envío de la información sensible y se aprecia el túnel que se construye entre DC y SS mediante el $PROT_3$.

Finalmente, hay que hacer notar también que cada valor sensible que el dispositivo confiable (DC) envía al servidor seguro (SS) o viceversa no implica necesariamente la creación de una sesión nueva con el servidor seguro (SS), con su valor ISS correspondiente, sino que una vez establecida una sesión, se podría reutilizar para el envío subsecuente de nueva información.

Como protocolo ($PROT_3$) se puede utilizar el protocolo TLS Record Protocol (TLSRP, RFC 2246). En ese caso, la realización de la invención debe incorporar algunos elementos adicionales para el uso de TLSRP, ya que la comunicación entre dispositivo confiable(DC) y el servidor seguro(SS) no se realiza a través de una única conexión en capa de transporte, como es común en TLS, sino que se establecen tres conexiones (véase la Figura 4): entre dispositivo confiable (DC) y el dispositivo no confiable (DNC), entre el dispositivo no confiable (DNC) y el proxy (P), y entre el proxy (P) y el servidor seguro (SS). No obstante, la implementación de TLSRP puede mantenerse fiel a su especificación. En primer lugar, el dispositivo confiable (DC) realiza los pasos del cliente TLSRP. Primero se calcula un código de autenticación del mensaje (MAC por sus siglas en inglés) que incluye el texto original del formulario y un número de secuencia dentro de la conexión. El número de secuencia permite evitar ataques de reenvío. Posteriormente, el texto original junto con el MAC es encriptado usando la clave para tal efecto. El resultado es un registro seguro TLS, especificado anteriormente como SEC, que incorpora información de la sesión segura (ISS) a la que pertenece y que se enviará al dispositivo no confiable (DNC).

c) Comunicación dispositivo confiable (DC) - dispositivo no confiable (DNC) ($PROT_4$):

Cada vez que hay que introducir un dato especificado como sensible en un formulario (por ejemplo, un formulario web, un diálogo de autenticación en FTP, etc.), o bien se recibe información sensible del servidor, se producirá un diálogo entre el dispositivo confiable (DC) y el dispositivo no confiable (DNC).En esta comunicación se pueden definir diferentes casos para el inicio del citado diálogo

i. Iniciado por el usuario.

Cuando está accediendo al servicio y va a enviar un campo con información, el usuario puede decidir que cierta información es sensible y utilizar el dispositivo confiable (DC) para introducirla. El usuario, por tanto, debe disponer de un mecanismo en el propio cliente (por ej. en el navegador) que le permita iniciar este diálogo dispositivo confiable (DC) - dispositivo no confiable (DNC). Este mecanismo se puede implementar, entre otras

alternativas, mediante un plug-in instalado en el cliente que permita al usuario seleccionar un campo como sensible, e iniciar para dicho campo el diálogo dispositivo confiable (DC) - dispositivo no confiable (DNC). El plug-in sería instalado junto con el software (driver) del dispositivo confiable (DC) en el sistema operativo del dispositivo no confiable (DNC).

ii. Iniciado por el servidor (S).

Es también posible que el servidor (S) decida que el valor de un campo de información deba ser transmitido como información sensible. Para notificar al dispositivo no confiable (DNC) este hecho, el servidor (S) podrá usar tecnologías de scripting (ej. Javascript), de modo que cuando el usuario seleccione el campo en cuestión se inicie automáticamente el diálogo dispositivo confiable (DC) - dispositivo no confiable (DNC) si el dispositivo confiable (DC) está conectado, o bien emerja un mensaje de solicitud del dispositivo confiable (DC) en la interfaz de usuario del dispositivo no confiable (DNC).

Una vez clarificados los escenarios en los que se iniciaría la comunicación dispositivo confiable (DC) - dispositivo no confiable (DNC), se van a describir los pasos en los que se podría desarrollar dicha comunicación.

1) Solicitud de confirmación al usuario.

El inicio del diálogo seguro debe ir seguido de una petición al usuario en la que se le solicite confirmar el uso del dispositivo confiable (DC). Esta confirmación se puede considerar realizada cuando el diálogo esté iniciado por el usuario. Sin embargo, si el diálogo es iniciado por el servidor (S) será obligatoria, sirviendo de información al usuario para que conecte e introduzca los datos en el dispositivo confiable (DC).

2) Comprobación de la conexión dispositivo confiable (DC) con el dispositivo no confiable (DNC).

Seguidamente se produce la comprobación de que existe comunicación entre el dispositivo confiable (DC) y el dispositivo no confiable (DNC). En caso de

que ésta no exista o falle, se notificará al usuario este evento, dando oportunidad a reintentar la conexión entre ambos dispositivos.

3) Notificación en DNC del traspaso de control al DC.

Una vez se ha realizado la comprobación de la conexión, se notificará al usuario que el control para la introducción y lectura de los datos sensibles se ha pasado al dispositivo confiable (DC), imposibilitando la introducción de otros datos en el navegador residente en el dispositivo no confiable (DNC). Para ello, se utilizará una notificación mediante ventana emergente o similar.

En este punto, se deben distinguir los pasos en la comunicación de información sensible desde o hacia el dispositivo confiable (DC). En el primer caso, esto es, cuando la información sensible se envía desde el dispositivo confiable (DC) al dispositivo no confiable (DNC):

4.a) Envío de mensaje de solicitud de dato sensible.

El dispositivo no confiable (DNC) solicitará el envío del valor para el campo identificado como sensible. Para ello, enviará un mensaje con la siguiente información.

- Nombre del campo de información. Este nombre servirá para que el dispositivo confiable (DC) pueda mostrar un mensaje al usuario solicitando dicho campo.

- Nombre del servidor de seguridad asociado al servicio. El dispositivo no confiable (DNC) podrá obtener el servidor de seguridad (SS) asociado siguiendo varios mecanismos posibles, como por ejemplo, indicándolo en el script que inicia el diálogo por el servidor, o mediante una TAG en la información remitida por el servidor (S) o el proxy (P), o mediante una extensión fija del dominio en el que está ubicado el servicio (por ejemplo, servidorseguridad.midominio.es). Para evitar complejidad en el dispositivo confiable (DC), lo que lo haría posiblemente vulnerable, si fuera necesario realizar una

resolución DNS del nombre del servidor de seguridad (SS), ésta se realizaría en el dispositivo no confiable (DNC).

5.a) Introducción de los datos sensibles en el dispositivo confiable (DC).

El dispositivo confiable (DC) presentará al usuario un diálogo preguntando por el valor del campo de información solicitado. En el teclado habilitado en el dispositivo confiable (DC), el usuario introducirá dicha información.

6.a) Envío de mensaje de respuesta con datos sensibles.

El dispositivo confiable (DC) establecerá una sesión con el servidor de seguridad siguiendo el protocolo ($PROT_2$), firmará y cifrará la información sensible con la clave o claves K_2 y la enviará cifrada al dispositivo no confiable (DNC).

En el caso en que se envíe información sensible hacia el dispositivo confiable (DC):

4.b) Envío de mensaje con dato sensible.

El dispositivo no confiable (DNC) remitirá el valor de un campo identificado como sensible. Para ello, enviará un mensaje con la siguiente información.

- Nombre del campo de información. Este nombre servirá para que el dispositivo confiable (DC) pueda mostrar un mensaje al usuario con dicho campo.

- Registro TLS codificado (SEC), que incluye el ISS, con el valor del campo de información firmado y cifrado.

5.b) Descifrado y autenticación del campo

El dispositivo confiable (DC) descifrará y autenticará el registro SEC utilizando la clave o claves K_2 asociadas al ISS.

6.b) Visualización del dato sensible

Si la autenticación ha sido correcta, el dispositivo confiable (DC)mandará la información descifrada al medio de visualización (MV).

d) Comunicación proxy (P) - servidor de seguridad (SS) ($PROT_5$):

Debe existir un procedimiento a partir del cual el proxy (P) envíe al servidor de seguridad (SS) la información sensible para su desencriptación y autenticación o, alternativamente, para su firma y cifrado. La naturaleza de dicho procedimiento dependerá particularmente de la ubicación del servidor de seguridad (SS). Si el servidor de seguridad (SS) se ubica en la misma máquina que el proxy (P), la comunicación se basará en procedimientos de comunicación entre procesos. Si el servidor de seguridad (SS) se ubica en una máquina distinta pero dentro de una red corporativa con un elevado nivel de seguridad, la comunicación se puede basar en protocolos de red no seguros. Si el servidor de seguridad (SS) se ubica en una red distinta, la comunicación debe utilizar recubrimientos criptográficos, por ej. VPNs, para garantizar que esta información no es capturada por elementos intermedios en la red. Finalmente, siempre existe la posibilidad de que el proxy (P) y el servidor de seguridad (SS) estén implementados por el mismo proceso, lo que eliminaría la necesidad del protocolo ($PROT_5$).

Cada vez que el proxy (P) recibe una información sensible codificada e identificable por una etiqueta (por ejemplo, la etiqueta <secret>), remitirá el contenido al servidor seguro (SS) para su decodificación. Al recibir la información codificada, el servidor seguro (SS) comprobará si existe una sesión activa con el identificador ISS contenido en el registro recibido. Si existe, utilizará la correspondiente clave o claves(K_2) para comprobar la integridad del registro y decodificar su contenido. El contenido decodificado se remitirá al proxy (P).

Cada vez que el proxy (P) recibe una información sensible con destino al dispositivo confiable (DC), debe en primer lugar iniciar un diálogo seguro, como se ha comentado anteriormente, notificando al dispositivo no confiable (DNC) este hecho, por ejemplo con tecnologías de scripting (por ejemplo, Javascript). Si el diálogo seguro entre el dispositivo confiable (DC) y el servidor seguro (SS) ya ha sido iniciado, el proxy (P) mandará la información sensible que quiere remitir al servidor seguro (SS) con el ISS asociado. El servidor seguro (SS) comprobará si existe una

sesión activa con el identificador ISS. Si existe, utilizará la correspondiente clave o claves (K_2) para firmar y cifrarla información. El resultado se remitirá al proxy (P).

e) Comunicación proxy (P) - servidor (S) ($PROT_6$):

Debe existir un procedimiento de comunicación del proxy (P) y el servidor (S). La naturaleza de dicho procedimiento dependerá particularmente de la ubicación del servidor (S). Si el servidor (S) se ubica en la misma máquina que el proxy (P), la comunicación se basará en procedimientos de comunicación entre procesos. Si el servidor (S) se ubica en una máquina distinta pero dentro de una red corporativa con un elevado nivel de seguridad, la comunicación se puede basar en protocolos de red no seguros. Si el servidor (S) se ubica en una red distinta, la comunicación debe utilizar recubrimientos criptográficos, por ej. VPNs, para garantizar que esta información no es capturada por elementos intermedios en la red. Finalmente, siempre existe la posibilidad de que el servidor (S) y el proxy (P) estén implementados por el mismo proceso, lo que eliminaría la necesidad del protocolo ($PROT_6$).

Cada vez que el servidor (S) quiera remitir una información sensible al dispositivo confiable (DC), la identificará con una etiqueta (por ejemplo, la etiqueta <secret>), y remitirá el contenido al proxy (P).Si es necesario iniciar un diálogo seguro, notificará al dispositivo no confiable (DNC) este hecho, por ejemplo con tecnologías de scripting (por ejemplo, Javascript). Alternativamente, como se ha comentado anteriormente, este paso puede realizarlo el proxy (P).

El $PROT_6$ puede ser el mismo protocolo que el $PROT_1$, de forma que el proxy se limita a sustituir la información sensible por su versión firmada y cifrada cuando el destino es el usuario, y a sustituir la información sensible firmada y cifrada por su versión descifrada y autenticada cuando el destino es el servidor (S).

f) Comunicación servidor seguro (SS) - servidor (S) ($PROT_7$):

Algunos de los pasos antes mencionados se pueden solucionar alternativamente usando una comunicación directa entre servidor seguro (SS) - servidor (S).

Por último, se realiza en primer lugar un resumen de los pasos seguidos en una realización concreta para el envío de información sensible de un usuario a un servidor (S) de acuerdo con el procedimiento de la presente invención. En orden cronológico, los pasos a seguir son los siguientes:

a) En primer lugar, bien por parte del usuario, bien por parte del servidor (S), se identifica un campo sensible. Como se ha especificado con anterioridad, el servidor (S) o el proxy (P) publicará la información de acceso a servidor de seguridad (SS). El dispositivo no confiable (DNC) mantiene una caché de servidores seguros (SS) conectados, de forma que le es posible identificar si es necesario establecer una nueva conexión o ya existe conexión abierta dispositivo confiable (DC) - servidor de seguridad (SS) debido al envío previo de información sensible.

b) Se inicia la conexión entre dispositivo confiable (DC) - servidor de seguridad (SS), el cual pasa el control a dispositivo confiable (DC). Se remite un mensaje de aviso al usuario en la interfaz del dispositivo no confiable (DNC) avisando de dicho paso de control. Adicionalmente, el dispositivo no confiable (DNC) remite al dispositivo confiable (DC) la información del localización de servidor de seguridad (SS), y si es necesario o no iniciar una nueva conexión.

c) Si fuera necesario, se inicia el establecimiento de conexión segura entre el dispositivo confiable (DC) y el servidor de seguridad (SS), utilizando TLSHP como protocolo ($PROT_3$). En dicho establecimiento, el driver del dispositivo confiable (DC) instalado en el dispositivo no confiable (DNC) realiza la retransmisión de los mensajes correspondientes utilizando la interfaz de red del dispositivo no confiable (DNC), que actúa como proxy de red. Los mensajes originados en el dispositivo confiable (DC) son reenviados a través de la interfaz de red del dispositivo no confiable (DNC) y con destino a servidor de seguridad (SS). Los mensajes enviados por el servidor de seguridad (SS) y recibidos por el dispositivo no confiable (DNC) son reenviados al dispositivo confiable (DC).

d) El usuario escribe la información sensible en la interfaz del dispositivo confiable (DC), que puede ser contemplada en el medio de visualización (MV).

e) El dispositivo confiable (DC), a partir de la información introducida, obtiene el registro TLS codificado SEC, que incluye el ISS, información de integridad y orden en la sesión, y lo remite al dispositivo no confiable (DNC).

f) El dispositivo no confiable (DNC) incorpora el registro SEC entre las etiquetas <secret> y </secret>y lo envía como parte de un mensaje al proxy (P).

g) El proxy (P) detecta que en alguno de los campos remitidos aparecen las etiquetas <secret> y </secret>, y remite el registro SEC al servidor de seguridad (SS).

h) El servidor de seguridad (SS) recibe el registro SEC y extrae el ISS. Si existe una sesión activa con ese identificador, utiliza las claves asociadas para comprobar la integridad del registro SEC y proceder a su descifrado. Si todo es correcto, remite la información descifrada al proxy (P).

i) El proxy (P) remite el mensaje completo al servidor (S) que interpreta la información en la forma habitual.

Finalmente, se realiza un resumen de los pasos seguidos para el envío de información sensible desde un servidor (S) a un usuario, de acuerdo con una realización concreta del procedimiento de la presente invención. En orden cronológico, los pasos a seguir son los siguientes:

a) En primer lugar, el servidor (S) identifica un campo como sensible. Adicionalmente, el servidor (S) publicará la información sobre cómo acceder al servidor de seguridad (SS). El dispositivo no confiable (DNC) mantiene una caché de servidores seguros (SS) conectados, de forma que le es posible identificar si es necesario establecer una nueva conexión o ya existe conexión abierta dispositivo confiable (DC) - servidor de seguridad (SS) debido al envío previo de información sensible.

b) Se inicia la conexión entre dispositivo confiable (DC) - servidor de seguridad (SS), el cual pasa el control al dispositivo confiable (DC). Se remite un mensaje de aviso al usuario en la interfaz del dispositivo no confiable (DNC) avisando de dicho paso de control. Adicionalmente, el dispositivo no confiable (DNC) remite al dispositivo confiable (DC) la información del localización de servidor de seguridad (SS), y si es necesario o no iniciar una nueva conexión.

c) Si fuera necesario, se inicia el establecimiento de conexión segura entre el dispositivo confiable (DC) y el servidor de seguridad (SS), utilizando por ejemplo TLSHP como protocolo ($PROT_3$). En dicho establecimiento, el driver del dispositivo confiable (DC) instalado en el dispositivo no confiable (DNC) realiza la retransmisión de los mensajes correspondientes utilizando la interfaz de red del dispositivo no confiable (DNC), que actúa como proxy de red. Los mensajes originados en el dispositivo confiable (DC) son reenviados a través de la interfaz de red del dispositivo no confiable (DNC) y con destino a servidor de seguridad (SS). Los mensajes enviados por el servidor de seguridad (SS) y recibidos por el dispositivo no confiable (DNC) son reenviados al dispositivo confiable (DC).

d) El servidor (S) remite el mensaje completo al proxy (P) incluyendo la información sensible entre las etiquetas `<secret>` y `</secret>`.

e) El proxy (P) remite la información sensible al servidor seguro (SS).

f) El servidor seguro (SS), a partir de la información introducida, obtiene el registro TLS codificado (SEC), que incluye el ISS, información de integridad y orden en la sesión, y lo remite al proxy (P)

g) El proxy (P) incorpora el registro SEC entre las etiquetas `<secret>` y `</secret>`y lo envía al dispositivo no confiable (DNC)

h) El dispositivo no confiable (DNC) detecta que en alguno de los campos remitidos aparecen las etiquetas `<secret>` y `</secret>`, y remite el registro SEC al dispositivo confiable (DC),

i) El dispositivo confiable (DC) recibe el registro SEC y extrae el ISS. Si existe una sesión activa con ese identificador, utiliza las claves asociadas para comprobar la integridad del registro SEC y proceder a su descifrado. Si todo es correcto, remite la información descifrada al medio de visualización (MV).

REIVINDICACIONES

1. Dispositivo confiable (DC) para el intercambio seguro de información sensible en una red de comunicación entre un usuario y un servidor (S) a través de un dispositivo no confiable (DNC), caracterizado porque comprende:

- un medio de visualización (MV) para mostrar datos o instrucciones al usuario;

- un medio de introducción de datos (MID) para que el usuario pueda introducir la información sensible que se va a enviar;

- un medio criptográfico para firmar y cifrar, o descifrar y autenticar, la información sensible de tal modo que dicha información sensible no sea accesible o modificable por el dispositivo no confiable (DNC);

- un medio de conexión (MC) con dicho dispositivo no confiable (DNC) para comunicar la información sensible a dicho dispositivo no confiable (DNC) para su transmisión al servidor (S); y

- un medio de comprobación de software que comprueba la legitimidad de un software que se ejecuta en el dispositivo confiable (DC) mediante la comprobación de que la firma digital de dicho software es válida, donde el dispositivo confiable (DC) está configurado de tal modo que dicho software o bien no es modificable, o bien sólo es modificable si el nuevo software está firmado por un certificado digital válido emitido por una autoridad certificadora (AC).

2. Dispositivo confiable (DC) de acuerdo con la reivindicación 1, donde el medio de visualización (MV) comprende una pantalla LCD o una pantalla táctil.

3. Dispositivo confiable (DC) de acuerdo con cualquiera de las reivindicaciones anteriores, donde el medio de introducción de datos (MID) comprende un teclado alfanumérico o una pantalla táctil.

4. Dispositivo confiable (DC) de acuerdo con cualquiera de las reivindicaciones anteriores, donde el medio de conexión (MC) comprende una conexión USB, una conexión WiFi o una conexión Bluetooth.

5. Sistema para el intercambio seguro de información sensible en una red de comunicación, que comprende:

- un dispositivo no confiable (DNC);

- un servidor (S) en comunicación con el dispositivo no confiable (DNC) a través de una red de comunicación (RC);

- un proxy (P) que actúa de intermediario en la comunicación entre el dispositivo no confiable (DNC) y el servidor (S);

- un servidor de seguridad (SS) en comunicación con el proxy (P)para descifrar y autenticar la información sensible que se envía al servidor (S) por el dispositivo no confiable (DNC), y para firmar y cifrar la información sensible que se remite al usuario;

- un dispositivo confiable (DC) de acuerdo con cualquiera de las reivindicaciones anteriores, que recibe la información sensible introducida por un usuario, firma y cifra dicha información sensible utilizando una clave o claves (K_2) compartidas exclusivamente por el dispositivo confiable (DC) y el servidor de seguridad (SS), y que está en comunicación con el dispositivo no confiable (DNC) para transmitirle dicha información sensible, y que recibe la información sensible enviada por el servidor (S), descifra y autentica dicha información sensible utilizando una clave o claves (K_2) compartidas exclusivamente por el dispositivo confiable (DC) y el servidor de seguridad (SS), que está en comunicación con el dispositivo no confiable (DNC) para recibir dicha información sensible y que la muestra al usuario; y

- una autoridad certificadora (AC) que se encarga de firmar unos certificados digitales del servidor de seguridad (SS) y del dispositivo confiable (DC) para verificar su legitimidad.

6. Sistema de acuerdo con la reivindicación 5, donde el servidor de seguridad (SS) y el proxy (P) están implementados en la misma máquina física.

7. Sistema de acuerdo con cualquiera de las reivindicaciones 5-6, donde el servidor (S) y el proxy (P) están implementados en la misma máquina física.

8. Procedimiento para el envío seguro de información sensible desde un usuario a un servidor a través de una red de comunicación que utiliza el sistema de acuerdo con cualquiera de las reivindicaciones, 5-7, caracterizado por que comprende los siguientes pasos:

- un usuario introduce información sensible en el dispositivo confiable (DC) a través del medio de introducción de datos (MID);

- el dispositivo confiable (DC) se comunica, a través del dispositivo no confiable (DNC) y de la red de comunicación (RC), con el servidor seguro (SS) y establece una sesión de comunicación segura con dicho servidor seguro (SS) para obtener una clave o claves (K_2) seguras compartidas exclusivamente por dicho dispositivo confiable (DC) y dicho servidor seguro (SS);

- el dispositivo confiable (DC) envía al dispositivo no confiable (DNC) la información sensible firmada y cifrada con la clave o claves (K_2);

- el dispositivo no confiable (DNC) envía, a través de la red de comunicación (RC), la información sensible firmada y cifrada con la clave o claves (K_2) al proxy (P);

- el proxy (P) detecta la existencia de información sensible y la envía al servidor seguro (SS);

- el servidor seguro (SS) descifra y autentica la información sensible recibida y la envía descifrada al proxy (P); y

- el proxy (P) la información al servidor (S).

9. Procedimiento para el envío seguro de información sensible desde un servidor a un usuario a través de una red de comunicación que utiliza el sistema de acuerdo con cualquiera de las reivindicaciones 5-7, caracterizado por que comprende los siguientes pasos:

- el servidor (S) notifica a un dispositivo confiable (DC) el inicio de una sesión segura, a través del dispositivo no confiable (DNC).

- el dispositivo confiable (DC) se comunica, a través del dispositivo no confiable (DNC) y de la red de comunicación (RC), con el servidor seguro (SS) y establece una sesión de comunicación segura con dicho servidor seguro (SS) para obtener una clave o claves (K_2) seguras compartidas exclusivamente por dicho dispositivo confiable (DC) y dicho servidor seguro (SS);

- el servidor (S) envía al proxy (P) la información sensible;

- el proxy (P) envía al servidor seguro (SS) la información sensible;

- el servidor seguro (SS) envía al proxy (P) la información sensible firmada y cifrada con la clave o claves (K_2);

- el proxy (P) envía, a través de la red de comunicación (RC), la información sensible firmada y cifrada con la clave o claves (K_2) al dispositivo no confiable (DNC);

- el dispositivo no confiable (DNC) detecta la existencia de información sensible y la envía al dispositivo confiable (DC); y

- el dispositivo confiable (DC) descifra y autentica la información sensible recibida y la muestra por el medio de visualización (MV).

10. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-9, donde la comunicación entre el dispositivo no confiable (DNC) y el proxy (P) a través de la red de comunicación (RC) se realiza de acuerdo con un primer protocolo ($PROT_1$) que se elige de entre la siguiente lista: http, https, ftp, ssh, y smtp.

11. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-10, donde la comunicación a través de una sesión de comunicación segura entre el dispositivo confiable (DC) y el servidor seguro (SS) a través del dispositivo no confiable (DNC) para obtener la clave o claves seguras (K_2) se realiza de acuerdo con un segundo protocolo ($PROT_2$) como el TLS Handshake Protocol.

12. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-11, donde la comunicación entre el dispositivo confiable (DC) y el servidor seguro (SS) a través del dispositivo confiable (DC), de la red de comunicación (RC), y del proxy (P) para el envío de la información sensible firmada y cifrada con la clave o claves seguras (K_2) se realiza de acuerdo con un tercer protocolo ($PROT_3$) como el TLS Record Protocol.

13. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-12, donde el establecimiento de la sesión de comunicación segura entre el dispositivo confiable (DC) y el servidor seguro (SS) según el segundo protocolo ($PROT_2$) comprende los siguientes pasos previos:

- el dispositivo no confiable (DNC) comprueba que está conectado con el dispositivo confiable (DC);
- el dispositivo no confiable (DNC) comprueba que el servidor (S) dispone de un servidor seguro (SS) asociado; y
- el dispositivo no confiable (DNC) envía al dispositivo confiable (DC) la dirección IP del servidor seguro (SS).

14. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-13, que además comprende el paso intermedio de identificar, por parte del dispositivo no confiable (DNC) o el dispositivo confiable (DC), la información sensible recibida del dispositivo confiable (DC) por medio de una etiqueta que permite al proxy (P) reconocer dicha información y remitirla al servidor seguro (SS).

15. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-14, que además comprende el paso intermedio de identificar, por parte del servidor (S), proxy (P) o servidor seguro (SS), la información sensible recibida del servidor seguro (SS) por medio de una etiqueta que permite al dispositivo no confiable (DNC) reconocer dicha información y remitirla al dispositivo confiable (DC).

16. Procedimiento de acuerdo con cualquiera de las reivindicaciones 8-15, que se ejecuta cuando el usuario o el servidor (S) determinan que se va a intercambiar información sensible durante una sesión de navegación entre ambos según el primer protocolo ($PROT_1$).

17. Programa de ordenador que comprende instrucciones de programa para hacer que un ordenador lleve a la práctica el procedimiento de acuerdo con cualquiera de las reivindicaciones 8-16.

18. Programa de ordenador según la reivindicación 17, incorporado en medios de almacenamiento.

19. Programa de ordenador según la reivindicación 18, soportado en una señal portadora.

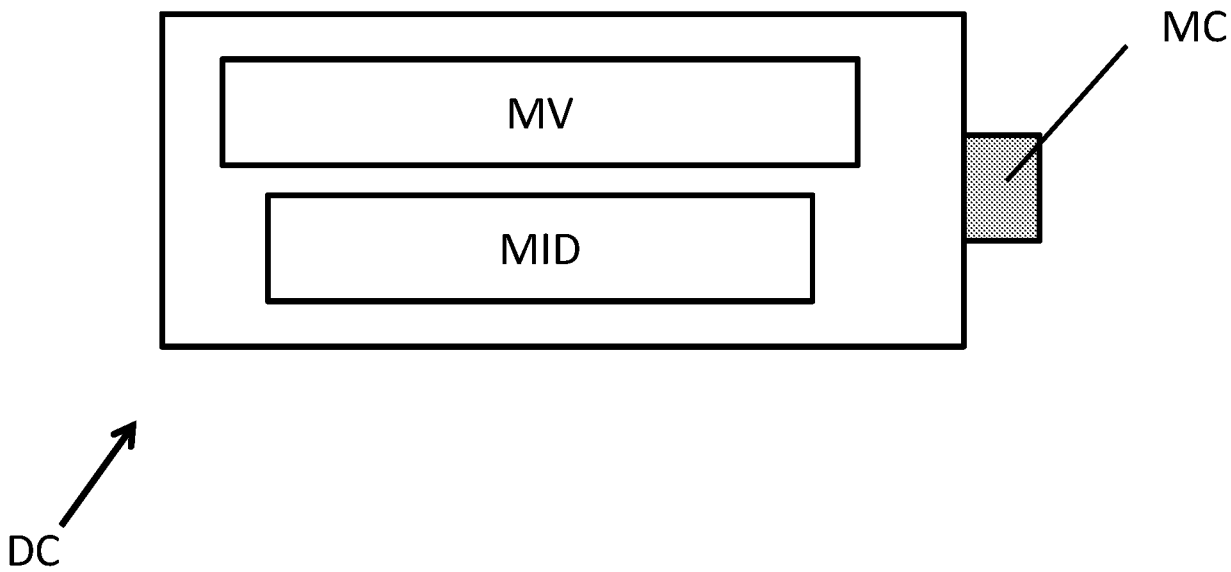

Figura 1

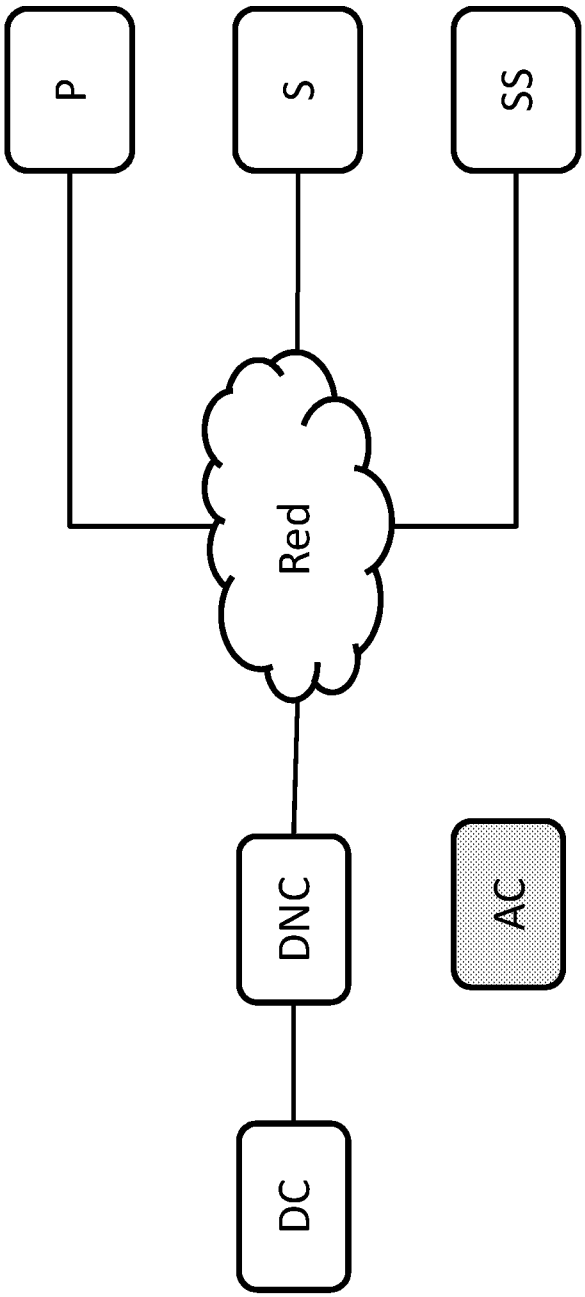

Figura 2

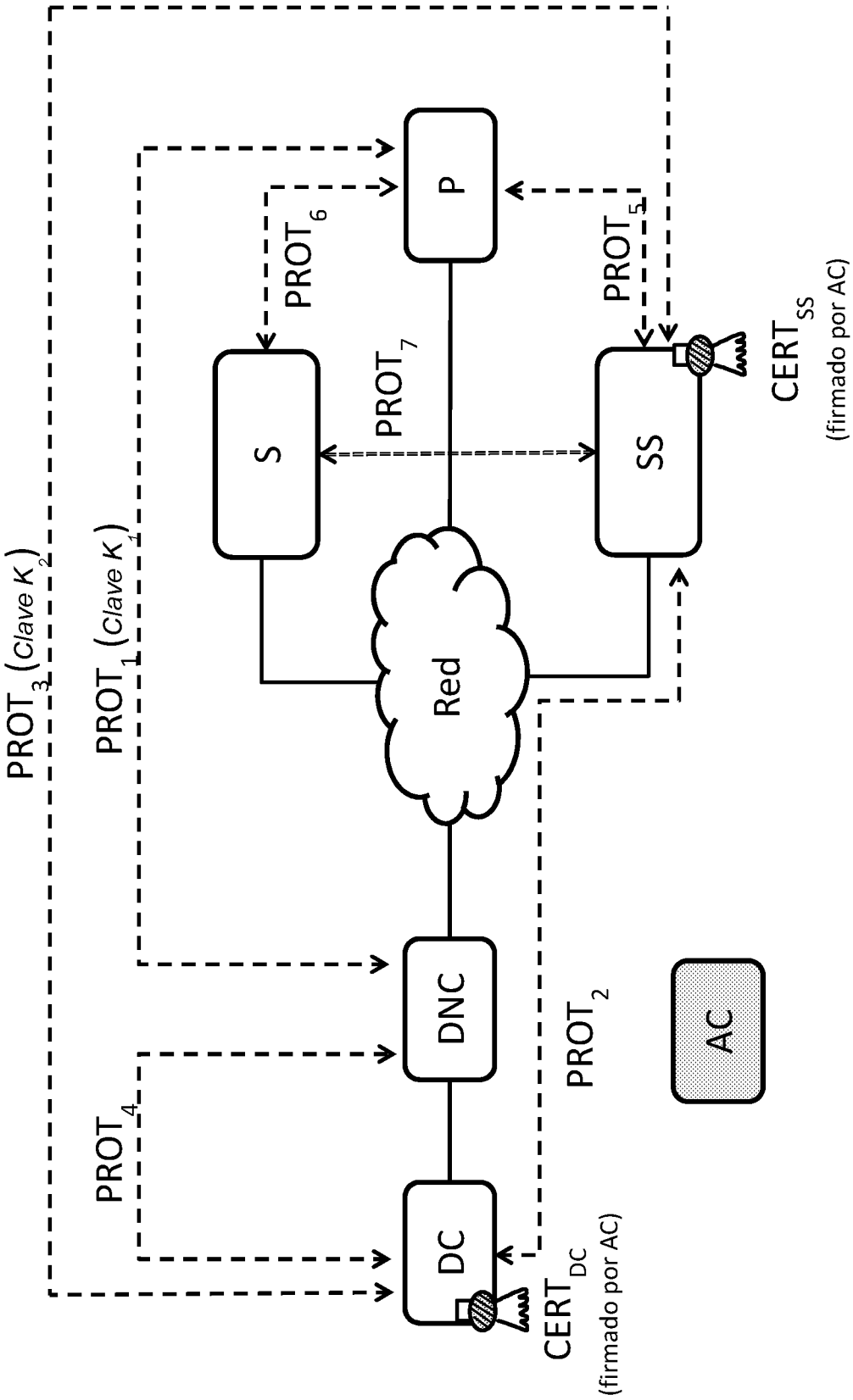
PROT3 (Clave K2)
PROT1 (Clave K1)
PROT4
PROT2
PROT5
PROT6
PROT7
DC
DNC
S
P
SS
Red
AC
CERTDC
(firmado por AC)
CERTSS
(firmado por AC)

Figura 3

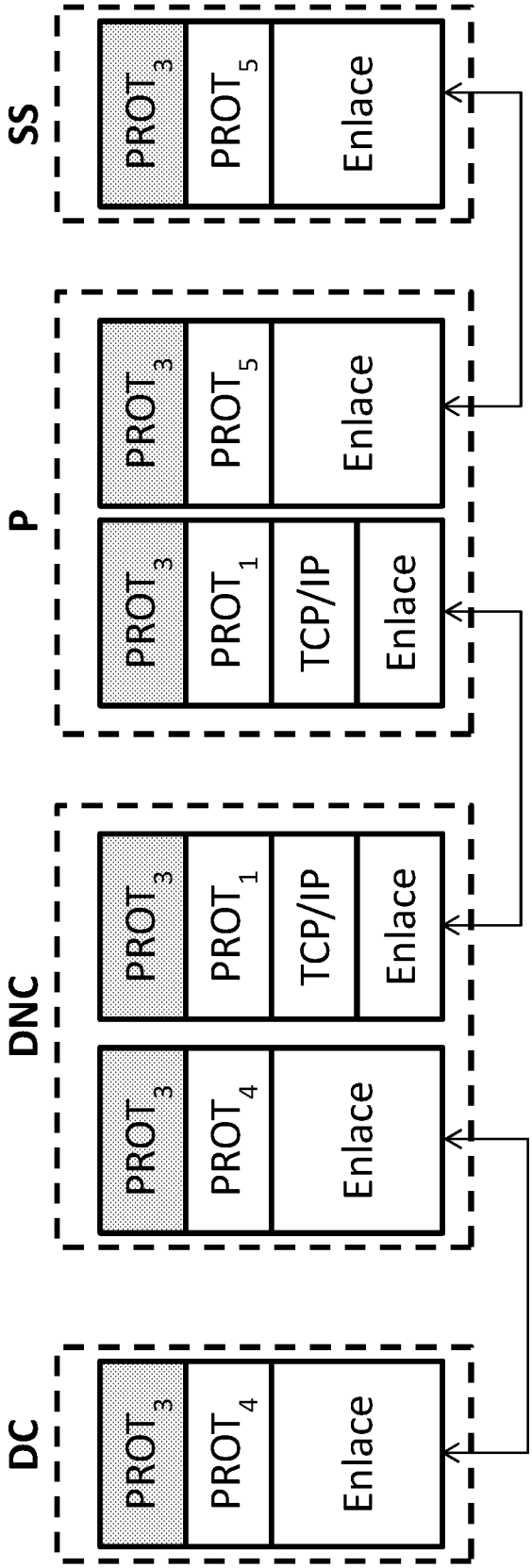
DC
PROT3
PROT4
Enlace
DNC
PROT3
PROT4
Enlace
PROT3
PROT1
TCP/IP
Enlace
P
PROT3
PROT1
TCP/IP
Enlace
PROT3
PROT5
Enlace
SS
PROT3
PROT5
Enlace

Figura 4

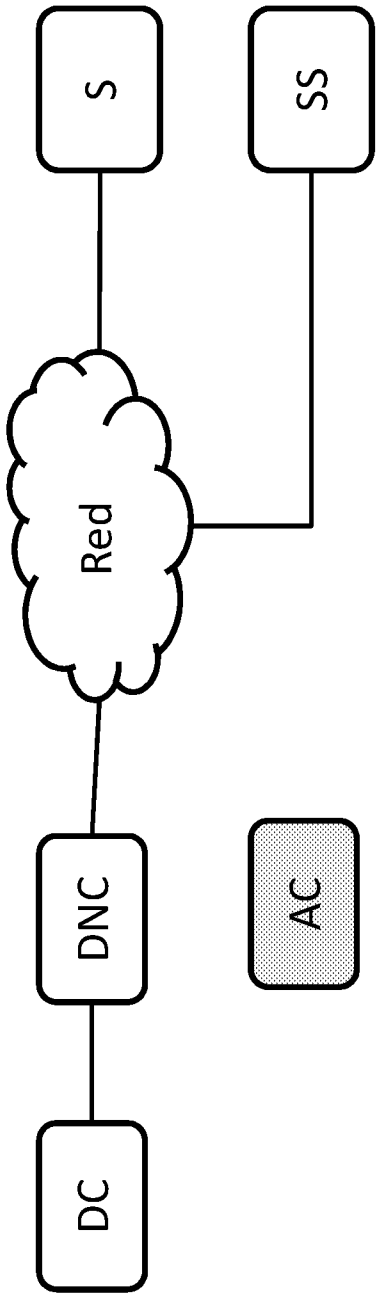

Figura 5

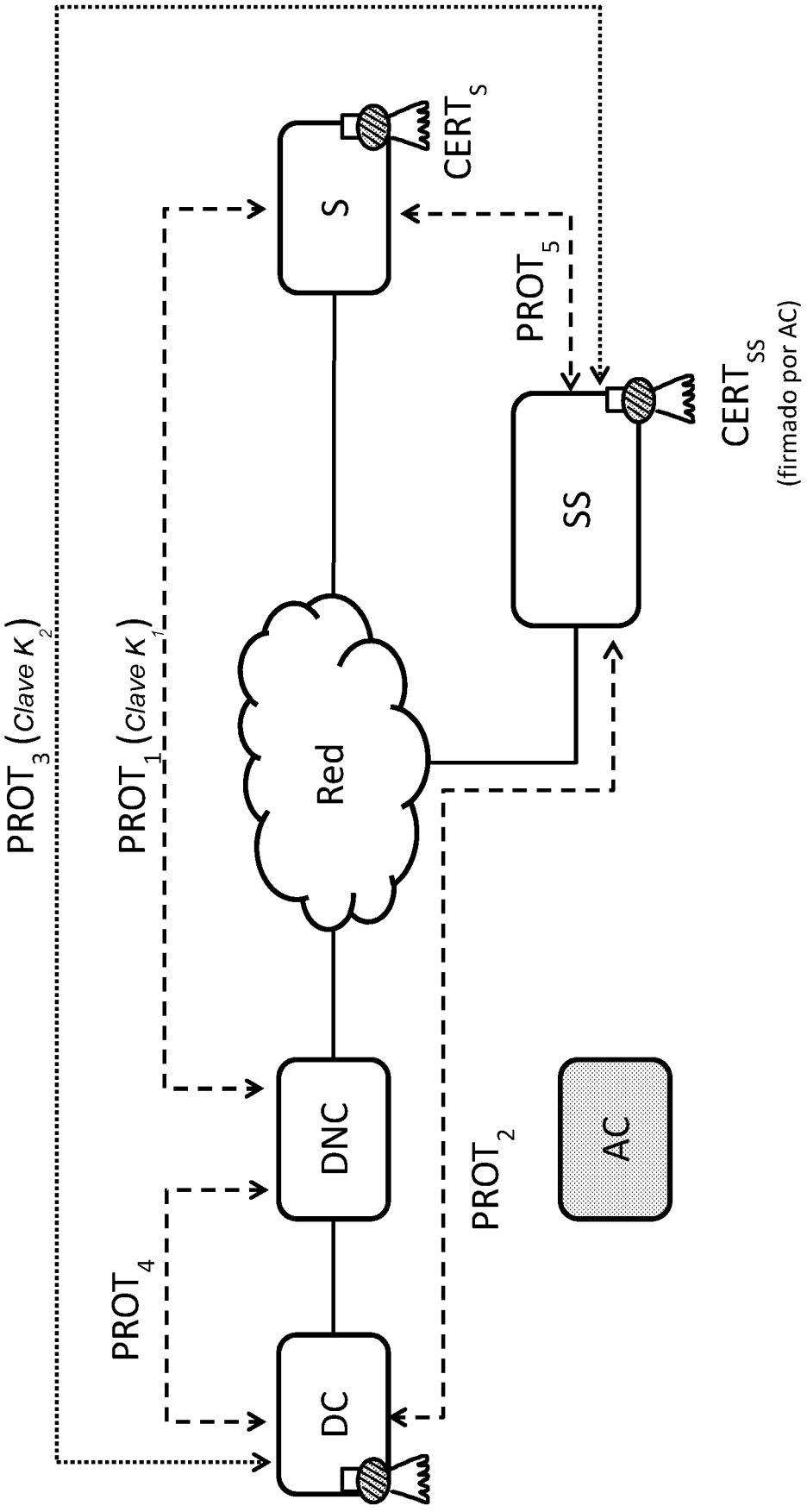
PROT3 (Clave K2)
PROT1 (Clave K1)
S
CERTS
PROT5
SS
CERTSS
(firmado por AC)
Red
DNC
DC
PROT4
PROT2
AC

Figura 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES2015/070118

A. CLASSIFICATION OF SUBJECT MATTER

G09C1/00 (2006.01)
H04L9/14 (2006.01)
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)
G09C, H04L

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.
X	US 2010180120 A1 (FRENKEL LIOR ET AL.) 15/07/2010, paragraphs[5 - 60]; paragraphs[71 - 82]; paragraphs[87 - 100]; paragraphs[103 - 114];	1-4
Y		5-19
Y	US 2003191970 A1 (DEVINE CAROL Y ET AL.) 09/10/2003, paragraph [14]; paragraph [42]; paragraphs[53 - 55]; paragraph [57]; paragraphs[68 - 74]; paragraphs[78 - 79]; paragraph [83]; paragraph [86]; paragraphs[89 - 90]; paragraphs[95 - 98]; paragraph [100]; paragraph [129]; paragraphs[136 - 140]; paragraph [148]; paragraph [153]; paragraph [160]; claim 1, claim 3, figure 1, figures 4 - 5. figures 8 - 9. figure 14,	5-19

☒ 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
28/05/2015	**(01/06/2015)**
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/ES2015/070118

C (continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of documents, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011202427 A1 (GARCIA JURADO SUAREZ CARLOS ET AL.) 18/08/2011, paragraphs[15 - 18]; paragraph [33]; paragraphs[36 - 39]; paragraphs[48 - 62]; paragraphs[63 - 64]; paragraphs[67 - 72]; paragraphs[75 - 77]; paragraph [79]; figures 1 - 6. figure 8,	1-4
A	US 2003079120 A1 (HEARN TINA ET AL.) 24/04/2003, paragraphs[25 - 26]; paragraphs[61 - 2]; paragraphs[67 - 70]; paragraphs[72 - 73]; paragraphs[88 - 108]; claim 1, claim 8, claim 14, claim 28, figures 1 - 2.	14-15
A	US 2013179685 A1 (WEINSTEIN DAVID ET AL.) 11/07/2013, paragraph [23]; paragraph [35]; paragraphs[38 - 40]; paragraph [42]; paragraphs[51 - 59]; paragraphs[63 - 64]; paragraphs[66 - 71]; paragraphs[76 - 80]; paragraph [84]; figures 1 - 10. figure 13,	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/ES2015/070118

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
US2010180120 A1	15.07.2010	IL185795 A	31.12.2013
		WO2009031140 A2	12.03.2009
		WO2009031140 A3	04.03.2010
		EP2188942 A2	26.05.2010
		EP2188942 A4	26.02.2014
US2003191970 A1	09.10.2003	US2013111576 A1	02.05.2013
		US8935772 B2	13.01.2015
		US2010024012 A1	28.01.2010
		US8479259 B2	02.07.2013
		US2002054587 A1	09.05.2002
		US6956845 B2	18.10.2005
		US2005172018 A1	04.08.2005
		US7447736 B2	04.11.2008
		US2004019808 A1	29.01.2004
		US6968571 B2	22.11.2005
		US7114083 B2	26.09.2006
		US2006129499 A1	15.06.2006
		US2006098583 A1	11.05.2006
		US7236486 B2	26.06.2007
		US6763376 B1	13.07.2004
		US6574661 B1	03.06.2003
		US6032184 A	29.02.2000
		US7225249 B1	29.05.2007
		US6377993 B1	23.04.2002
		US6473407 B1	29.10.2002
		US6470386 B1	22.10.2002
		US6115040 A	05.09.2000
		US2003041263 A1	27.02.2003
		US6598167 B2	22.07.2003
		US2001052013 A1	13.12.2001
		US6381644 B2	30.04.2002
		US6385644 B1	07.05.2002
		US6611498 B1	26.08.2003
		US6615258 B1	02.09.2003
		US6515968 B1	04.02.2003
		US6631402 B1	07.10.2003
		US6587836 B1	01.07.2003
		US6490620 B1	03.12.2002
		US6606708 B1	12.08.2003
		US6745229 B1	01.06.2004
		US7058600 B1	06.06.2006
		US2002087383 A1	04.07.2002
		US6859783 B2	22.02.2005
		US6714979 B1	30.03.2004
		US2005210296 A1	22.09.2005
		US7814533 B2	12.10.2010
		US2005216421 A1	29.09.2005
		US8073777 B2	06.12.2011
		WO9916203 A2	01.04.1999

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/ES2015/070118

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
		WO9916203 A3	07.10.1999
		WO9919803 A1	22.04.1999
		WO9916202 A2	01.04.1999
		WO9915979 A1	01.04.1999
		WO9915979 A9	14.10.1999
		WO9915978 A1	01.04.1999
		WO9915989 A1	01.04.1999
		WO9915989 A9	26.08.1999
		WO9916099 A2	01.04.1999
		WO9916099 A3	20.05.1999
		WO9916218 A1	01.04.1999
		WO9915950 A1	01.04.1999
		WO9916002 A1	01.04.1999
		WO9915996 A2	01.04.1999
		WO9915996 A3	20.05.1999
		WO9915988 A2	01.04.1999
		WO9915988 A3	28.10.1999
		WO9916207 A1	01.04.1999
		WO9915977 A1	01.04.1999
		WO9916198 A1	01.04.1999
		WO9916206 A1	01.04.1999
		WO9915975 A1	01.04.1999
		WO9915974 A1	01.04.1999
		WO9916230 A1	01.04.1999
		WO9915960 A2	01.04.1999
		WO9915960 A3	20.05.1999
		WO9915984 A1	01.04.1999
		US2005114712 A1	26.05.2005
		US8495724 B2	23.07.2013
		JP2003526126 A	02.09.2003
		JP2003525475 A	26.08.2003
		JP2003522342 A	22.07.2003
		EP1015986 A1	05.07.2000
		EP1015986 A4	23.07.2003
		EP1015970 A2	05.07.2000
		EP1015970 A4	30.07.2003
		EP1015995 A1	05.07.2000
		EP1015995 A4	30.07.2003
		CA2304619 A1	01.04.1999
		CA2304554 A1	01.04.1999
		CA2304543 A1	22.04.1999
		BR9814050 A	13.11.2001
		BR9814049 A	20.11.2001
		BR9814046 A	02.01.2002
		AU9777398 A	12.04.1999
		AU9777298 A	12.04.1999
		AU9777098 A	12.04.1999
		AU9668298 A	03.05.1999
		AU755614B B2	19.12.2002

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/ES2015/070118

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
		AU9668098 A	12.04.1999
		AU9667998 A	12.04.1999
		AU9667898 A	12.04.1999
		AU9667698 A	12.04.1999
		AU9667598 A	12.04.1999
		AU9667298 A	12.04.1999
		AU9667198 A	12.04.1999
		AU753269B B2	10.10.2002
		AU9666398 A	12.04.1999
		AU752622B B2	26.09.2002
		AU9584098 A	12.04.1999
		AU9583698 A	12.04.1999
		AU9583598 A	12.04.1999
		AU9583398 A	12.04.1999
		AU9583298 A	12.04.1999
		AU9583198 A	12.04.1999
		AU9582998 A	12.04.1999
		AU9582798 A	12.04.1999
		AU1062499 A	12.04.1999
US2011202427 A1	18.08.2011	US2013246637 A1	19.09.2013
		US8966096 B2	24.02.2015
		CN102763115 A	31.10.2012
		WO2011102979 A2	25.08.2011
		WO2011102979 A3	22.12.2011
		US8438288 B2	07.05.2013
US2003079120 A1	24.04.2003	GB2368691 A	08.05.2002
		GB2368691 B	31.03.2004
		WO0075754 A2	14.12.2000
		WO0075754 A3	06.06.2002
		EP1228407 A2	07.08.2002
US2013179685 A1	11.07.2013	US8615656 B2	24.12.2013
		WO2013106286 A1	18.07.2013

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES2015/070118

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD
G09C1/00 (2006.01)
H04L9/14 (2006.01)
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)
G09C, H04L

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
X	US 2010180120 A1 (FRENKEL LIOR ET AL.) 15/07/2010, párrafos[5 - 60]; párrafos[71 - 82]; párrafos[87 - 100]; párrafos[103 - 114];	1-4
Y		5-19
Y	US 2003191970 A1 (DEVINE CAROL Y ET AL.) 09/10/2003, párrafo [14]; párrafo [42]; párrafos[53 - 55]; párrafo [57]; párrafos[68 - 74]; párrafos[78 - 79]; párrafo [83]; párrafo [86]; párrafos[89 - 90]; párrafos[95 - 98]; párrafo [100]; párrafo [129]; párrafos[136 - 140]; párrafo [148]; párrafo [153]; párrafo [160]; reivindicación 1, reivindicación 3, figura 1, figuras 4 - 5. figuras 8 - 9. figura 14,	5-19

☒ 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.
28/05/2015	**01 de Junio de 2015 (01/06/2015)**
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/ES2015/070118

C (Continuación). DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría *	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
X	US 2011202427 A1 (GARCIA JURADO SUAREZ CARLOS ET AL.) 18/08/2011, párrafos[15 - 18]; párrafo [33]; párrafos[36 - 39]; párrafos[48 - 62]; párrafos[63 - 64]; párrafos[67 - 72]; párrafos[75 - 77]; párrafo [79]; figuras 1 - 6. figura 8,	1-4
A	US 2003079120 A1 (HEARN TINA ET AL.) 24/04/2003, párrafos[25 - 26]; párrafos[61 - 2]; párrafos[67 - 70]; párrafos[72 - 73]; párrafos[88 - 108]; reivindicación 1, reivindicación 8, reivindicación 14, reivindicación 28, figuras 1 - 2.	14-15
A	US 2013179685 A1 (WEINSTEIN DAVID ET AL.) 11/07/2013, párrafo [23]; párrafo [35]; párrafos[38 - 40]; párrafo [42]; párrafos[51 - 59]; párrafos[63 - 64]; párrafos[66 - 71]; párrafos[76 - 80]; párrafo [84]; figuras 1 - 10. figura 13,	1-19

INFORME DE BÚSQUEDA INTERNACIONAL

Informaciones relativas a los miembros de familias de patentes

Solicitud internacional nº

PCT/ES2015/070118

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
US2010180120 A1	15.07.2010	IL185795 A	31.12.2013
		WO2009031140 A2	12.03.2009
		WO2009031140 A3	04.03.2010
		EP2188942 A2	26.05.2010
		EP2188942 A4	26.02.2014
US2003191970 A1	09.10.2003	US2013111576 A1	02.05.2013
		US8935772 B2	13.01.2015
		US2010024012 A1	28.01.2010
		US8479259 B2	02.07.2013
		US2002054587 A1	09.05.2002
		US6956845 B2	18.10.2005
		US2005172018 A1	04.08.2005
		US7447736 B2	04.11.2008
		US2004019808 A1	29.01.2004
		US6968571 B2	22.11.2005
		US7114083 B2	26.09.2006
		US2006129499 A1	15.06.2006
		US2006098583 A1	11.05.2006
		US7236486 B2	26.06.2007
		US6763376 B1	13.07.2004
		US6574661 B1	03.06.2003
		US6032184 A	29.02.2000
		US7225249 B1	29.05.2007
		US6377993 B1	23.04.2002
		US6473407 B1	29.10.2002
		US6470386 B1	22.10.2002
		US6115040 A	05.09.2000
		US2003041263 A1	27.02.2003
		US6598167 B2	22.07.2003
		US2001052013 A1	13.12.2001
		US6381644 B2	30.04.2002
		US6385644 B1	07.05.2002
		US6611498 B1	26.08.2003
		US6615258 B1	02.09.2003
		US6515968 B1	04.02.2003
		US6631402 B1	07.10.2003
		US6587836 B1	01.07.2003
		US6490620 B1	03.12.2002
		US6606708 B1	12.08.2003
		US6745229 B1	01.06.2004
		US7058600 B1	06.06.2006
		US2002087383 A1	04.07.2002
		US6859783 B2	22.02.2005
		US6714979 B1	30.03.2004
		US2005210296 A1	22.09.2005
		US7814533 B2	12.10.2010
		US2005216421 A1	29.09.2005
		US8073777 B2	06.12.2011
		WO9916203 A2	01.04.1999

INFORME DE BÚSQUEDA INTERNACIONAL

Informaciones relativas a los miembros de familias de patentes

Solicitud internacional nº

PCT/ES2015/070118

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
		WO9916203 A3	07.10.1999
		WO9919803 A1	22.04.1999
		WO9916202 A2	01.04.1999
		WO9915979 A1	01.04.1999
		WO9915979 A9	14.10.1999
		WO9915978 A1	01.04.1999
		WO9915989 A1	01.04.1999
		WO9915989 A9	26.08.1999
		WO9916099 A2	01.04.1999
		WO9916099 A3	20.05.1999
		WO9916218 A1	01.04.1999
		WO9915950 A1	01.04.1999
		WO9916002 A1	01.04.1999
		WO9915996 A2	01.04.1999
		WO9915996 A3	20.05.1999
		WO9915988 A2	01.04.1999
		WO9915988 A3	28.10.1999
		WO9916207 A1	01.04.1999
		WO9915977 A1	01.04.1999
		WO9916198 A1	01.04.1999
		WO9916206 A1	01.04.1999
		WO9915975 A1	01.04.1999
		WO9915974 A1	01.04.1999
		WO9916230 A1	01.04.1999
		WO9915960 A2	01.04.1999
		WO9915960 A3	20.05.1999
		WO9915984 A1	01.04.1999
		US2005114712 A1	26.05.2005
		US8495724 B2	23.07.2013
		JP2003526126 A	02.09.2003
		JP2003525475 A	26.08.2003
		JP2003522342 A	22.07.2003
		EP1015986 A1	05.07.2000
		EP1015986 A4	23.07.2003
		EP1015970 A2	05.07.2000
		EP1015970 A4	30.07.2003
		EP1015995 A1	05.07.2000
		EP1015995 A4	30.07.2003
		CA2304619 A1	01.04.1999
		CA2304554 A1	01.04.1999
		CA2304543 A1	22.04.1999
		BR9814050 A	13.11.2001
		BR9814049 A	20.11.2001
		BR9814046 A	02.01.2002
		AU9777398 A	12.04.1999
		AU9777298 A	12.04.1999
		AU9777098 A	12.04.1999
		AU9668298 A	03.05.1999
		AU755614B B2	19.12.2002

INFORME DE BÚSQUEDA INTERNACIONAL

Informaciones relativas a los miembros de familias de patentes

Solicitud internacional nº

PCT/ES2015/070118

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
		AU9668098 A	12.04.1999
		AU9667998 A	12.04.1999
		AU9667898 A	12.04.1999
		AU9667698 A	12.04.1999
		AU9667598 A	12.04.1999
		AU9667298 A	12.04.1999
		AU9667198 A	12.04.1999
		AU753269B B2	10.10.2002
		AU9666398 A	12.04.1999
		AU752622B B2	26.09.2002
		AU9584098 A	12.04.1999
		AU9583698 A	12.04.1999
		AU9583598 A	12.04.1999
		AU9583398 A	12.04.1999
		AU9583298 A	12.04.1999
		AU9583198 A	12.04.1999
		AU9582998 A	12.04.1999
		AU9582798 A	12.04.1999
		AU1062499 A	12.04.1999
US2011202427 A1	18.08.2011	US2013246637 A1	19.09.2013
		US8966096 B2	24.02.2015
		CN102763115 A	31.10.2012
		WO2011102979 A2	25.08.2011
		WO2011102979 A3	22.12.2011
		US8438288 B2	07.05.2013
US2003079120 A1	24.04.2003	GB2368691 A	08.05.2002
		GB2368691 B	31.03.2004
		WO0075754 A2	14.12.2000
		WO0075754 A3	06.06.2002
		EP1228407 A2	07.08.2002
US2013179685 A1	11.07.2013	US8615656 B2	24.12.2013
		WO2013106286 A1	18.07.2013