(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 717**

(21) Número de solicitud: 201730639

(51) Int. CI.:

H04L 9/00 (2006.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

26.04.2017

(43) Fecha de publicación de la solicitud:

26.10.2018

(71) Solicitantes:

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

(72) Inventor/es:

URUEÑA PASCUAL, Manuel y
SOTO CAMPOS, Ignacio

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Método y dispositivo móvil para emitir certificados digitales a dispositivos electrónicos**

(57) Resumen:

Método y dispositivo móvil para emitir certificados digitales a dispositivos electrónicos.

La presente invención se refiere a un método y un sistema para emitir un certificado digital desde un dispositivo de certificación móvil (10) a un dispositivo electrónico (11) a través de una interfaz cableada punto-a-punto que comprende: conectar ambos dispositivos, generar en el dispositivo electrónico un par de claves criptográficas asimétricas y una solicitud de firma de certificado; enviar dicha solicitud al dispositivo de certificación móvil a través de la interfaz cableada; verificar, por un operador del dispositivo de certificación móvil, la información incluida en dicha solicitud, la cual se muestra en una interfaz gráfica del dispositivo de certificación móvil; emitir el certificado digital para el dispositivo electrónico, firmado con una clave privada almacenada en un elemento seguro del dispositivo de certificación móvil; y enviar, al dispositivo electrónico, el certificado digital emitido y la cadena de confianza que incluye todos los certificados de las autoridades de certificación intermedias hasta la autoridad de certificación raíz.

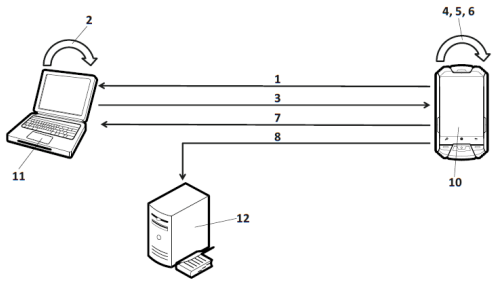

FIG. 1

ES 2 687 717 A1

DESCRIPCIÓN

Método y dispositivo móvil para emitir certificados digitales a dispositivos electrónicos

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención tiene aplicación en el campo de la seguridad informática y más específicamente en los métodos y dispositivos para emitir certificados digitales X.509 a otros dispositivos electrónicos, tales como servidores, ordenadores personales, dispositivos móviles, puntos de acceso, impresoras o similares.

ANTECEDENTES DE LA INVENCIÓN

Hoy en día, las partes involucradas en intercambios de información digital requieren que se establezca un cierto marco de seguridad para realizar cualquier interacción sensible y, en particular, que se compruebe la autenticidad de identidades entre dispositivos electrónicos. Una de las formas más seguras de realizar este proceso de autenticación es mediante el uso de certificados digitales.

Un certificado digital X.509 es un documento que recoge ciertos datos de su titular y su clave pública, y está firmado digitalmente por una autoridad de certificación. Una autoridad de certificación (o 'CA' del inglés "Certification Authority") es la entidad de confianza encargada de emitir y revocar certificados digitales. Actualmente sólo unas pocas organizaciones son reconocidas mundialmente para avalar la legitimidad de la relación entre la identidad de una entidad y su clave pública.

Los protocolos de seguridad más avanzados, como TLS [RFC5246], IPsec/IKE [RFC7296] o 802.1X [IEEE802.1X-2010], permiten utilizar certificados digitales X.509 para verificar la identidad de las partes que se comunican. El protocolo de Internet más popular que emplea certificados digitales es HTTPS, o HTTP [RFC7230-7235] sobre SSL/TLS, y hay todo un ecosistema de autoridades de certificación, normalmente denominado "Web PKI", para emitir certificados a servidores web seguros. Además, los certificados digitales X.509 se pueden utilizar también como un mecanismo de autenticación de usuarios seguro, empleando el procedimiento de autenticación mutua de TLS).

Es habitual que las grandes corporaciones tengan una infraestructura de clave pública ('PKI'

del inglés “Public Key Infrastructure”) propia para emitir certificados a sus empleados y servicios internos (dado que las CAs públicas, que serían la alternativa a una PKI privada, históricamente han cobrado sumas significativas por cada certificado emitido, y en muchos casos tienen que ser capaces de conectarse al servicio al que se emite el certificado para realizar una validación del mismo). Por otro lado, para las organizaciones pequeñas y medianas tener una PKI propia puede implicar unos costes inasumibles para poder protegerla y operarla adecuadamente, lo que termina derivando en una peligrosa desprotección de sus actividades internas al no poder emplear certificados digitales.

El procedimiento habitual para emitir un certificado X.509 consiste en generar localmente un par de claves criptográficas asimétricas, idealmente utilizando un chip criptográfico o elemento seguro (‘SE’ del inglés “Secure Element”), para luego generar una solicitud de firma de certificado (‘CSR’ del inglés “Certificate Signing Request”) que incluya la clave pública generada, y que esté firmada con la clave privada asociada, probando así su posesión. El CSR se envía a una CA (normalmente a través de una autoridad de registro o RA – del inglés “Registration Authority”– para verificar la identidad del sujeto del certificado), que emite un certificado para el sujeto con la clave pública incluida en el CSR y que está firmado digitalmente usando la clave privada de la CA (que, a su vez, debería estar almacenada en un módulo hardware de seguridad o HSM – del inglés “Hardware Security Module” -). Finalmente, se proporciona al sujeto el nuevo certificado, así como la cadena de confianza (secuencia de certificados de las CAs intermedias hasta la CA raíz de confianza). Para proteger la CA que emite los certificados, el equipo con su clave privada suele estar desconectado de la red o, a lo sumo, conectado a una red restringida y de alta seguridad.

Por lo tanto, el intercambio CSR-certificado normalmente requiere realizar algunos pasos manuales para poder acceder a la CA, lo que puede no ser un problema importante cuando se genera un número reducido de certificados (ej. a nuevos empleados o nuevos servicios). Sin embargo, incluso una organización pequeña puede tener cientos o miles de dispositivos (ej. ordenadores, dispositivos móviles, servidores, puntos de acceso, impresoras, dispositivos IoT, etc.) que son renovados periódicamente, por lo que este proceso manual para generar certificados para dispositivos con una CA desconectada de la red tiene problemas de escalabilidad que limitan su uso.

El estado del arte ofrece alguna solución de dispositivo portátil para acelerar en cierta medida este proceso, y permitir la comunicación segura de dispositivos de diferentes agencias en una red ad hoc móvil utilizando una CA de confianza. Es el caso de la solicitud

US2008046716A1, que emplea un dispositivo portátil precargado con varios pares de claves e incluso los certificados asociados (emitidos por una autoridad de certificación padre con sujetos genéricos), con las que genera o asigna certificados a otro dispositivo de red para que sea utilizado por éste en procedimientos de autenticación. Sin embargo, el dispositivo portátil propuesto por US2008046716A1 no actúa como una autoridad de certificación completa, sino que, a lo sumo, firma certificados usando la clave privada de la CA padre. Tampoco emplea el mecanismo de CSR expuesto anteriormente, puesto que las claves privadas asociadas a los certificados emitidos están pre-generadas por la CA padre. El problema de este esquema simplificado es que las claves privadas almacenadas en el dispositivo portátil son ciertamente vulnerables ante un eventual ataque al dispositivo portátil, o durante su transferencia al dispositivo de red. Por el contrario, en el mecanismo habitual basado en el intercambio CSR-certificado el par de claves se genera localmente en el dispositivo a certificar, por lo que la clave privada puede generarse y almacenarse de manera segura en un elemento seguro local, y con la CA sólo se intercambia información pública, esto es, el CSR y el certificado, que sólo contienen la clave pública del dispositivo.

Por otro lado, el documento “On the Generation of X.509v3 Certificates with Biometric Information” de Martínez-Silva *et al.* describe la implementación de una CA de certificados de usuario en una PDA (del inglés “Personal Digital Assistant”) que permite incorporar información biométrica del usuario en el propio certificado. Sin embargo, no considera ningún tipo de comunicación de dicha CA con otros dispositivos electrónicos, sino que toda la información del certificado se rellena manualmente a través de un formulario y las claves se generan localmente en la PDA. Además, tampoco se especifica cómo integrar dicha CA móvil en una PKI existente.

En US2004122960A1 se propone un método para demostrar una red inalámbrica a un cliente. El objetivo es desplegar una infraestructura móvil en las dependencias del cliente con la que demostrar el funcionamiento de una red inalámbrica. Como parte de la infraestructura se puede incluir una autoridad de certificación autónoma, instalada en un ordenador portátil junto con un servidor de autenticación. De esta manera la autoridad certificadora puede emitir certificados localmente y comprobar su validez, para que puedan usarse en la política de autenticación implementada en la red inalámbrica. Lo que no se define es el método de cómo un usuario o dispositivo de la red inalámbrica podría solicitar la generación de un certificado. Es decir, la autoridad certificadora definida sólo se emplea para validar certificados en beneficio del servidor de autenticación en el mismo ordenador portátil, que es parte de la infraestructura móvil de demostración de la red inalámbrica, pero

no se usa como autoridad certificadora portátil para generar y distribuir certificados de forma segura y simple para terceros fuera del entorno de demostración.

Por lo expuesto anteriormente, los métodos y dispositivos portátiles conocidos para la emisión de certificados digitales a dispositivos electrónicos carecen del equilibrio necesario entre seguridad, usabilidad y escalabilidad para adaptarse a las distintas situaciones de usuarios y organizaciones, con lo que se echa en falta en el estado del arte alguna alternativa que reúna todo lo anterior, y ofrezca una solución adecuada para pequeñas y medianas empresas.

DESCRIPCIÓN DE LA INVENCIÓN

La presente invención resuelve los problemas mencionados anteriormente mediante una solución flexible, fácil de usar, y segura. Así, en un primer aspecto de la invención, se presenta un método para emitir un certificado digital desde un dispositivo de certificación móvil a un dispositivo electrónico a través de una interfaz cableada punto-a-punto, donde el método comprende:

a) conectar el dispositivo de certificación móvil al dispositivo electrónico mediante la interfaz cableada;

b) como resultado del paso a), generar, en el dispositivo electrónico, un par de claves criptográficas asimétricas que comprende una clave pública y una clave privada; (dichas claves se podrían generar, por ejemplo, en un elemento seguro del dispositivo electrónico, si es que éste dispone de tal elemento seguro);

c) generar, en el dispositivo electrónico, una solicitud de firma de certificado que incluye información relativa al dispositivo electrónico y la clave pública generada, donde dicha solicitud está firmada con la clave privada asociada;

d) enviar la solicitud de firma de certificado al dispositivo de certificación móvil a través de la interfaz cableada;

e) verificar, por un operador del dispositivo de certificación móvil, la información relativa al dispositivo electrónico incluida en la solicitud de firma de certificado, donde dicha información se muestra en una interfaz gráfica del dispositivo de certificación móvil;

f) emitir, por el dispositivo de certificación móvil, el certificado digital para el dispositivo electrónico, donde dicho certificado digital está firmado con una clave

privada almacenada en el dispositivo de certificación móvil; donde en el caso de que se contase con un elemento seguro, se contemplaría proteger en él la clave privada de la autoridad de certificación móvil para prevenir un eventual ataque que propiciase la extracción de dicha clave y la emisión de certificados maliciosos.

g) enviar, al dispositivo electrónico a través de la interfaz cableada, el certificado digital emitido y una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz.

En una realización de la invención, la cadena de confianza comprende únicamente una autoridad de certificación raíz, que consiste en un certificado auto-firmado emitido por dicha autoridad de certificación móvil.

Una realización de la presente invención además contempla integrar el dispositivo de certificación móvil en una infraestructura de clave pública (PKI) como una autoridad de certificación subordinada. Específicamente, de acuerdo a una de las posibles realizaciones, se contemplan los pasos previos de:

a) generar, en el dispositivo de certificación móvil, un par de claves criptográficas asimétricas que comprende una clave pública y una clave privada;

b) generar, en el dispositivo de certificación móvil, una solicitud de firma de certificado que incluye información relativa al dispositivo de certificación móvil y la clave pública generada en el paso a), y donde dicha solicitud está firmada con la clave privada asociada;

c) enviar la solicitud de firma de certificado desde el dispositivo de certificación móvil a la autoridad de certificación padre; donde la autoridad de certificación padre puede ser la autoridad de certificación raíz o cualquier otra autoridad de certificación intermedia de la PKI;

d) emitir, por la autoridad de certificación padre, un certificado de autoridad de certificación subordinada para el dispositivo de certificación móvil, donde dicho certificado contiene la clave pública incluida en la solicitud de firma de certificado enviada en el paso c);

e) enviar el certificado de autoridad de certificación subordinada emitido en el paso d) y una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias (si las hubiere) hasta una autoridad de certificación raíz, al

dispositivo de certificación móvil.

De manera adicional**,** la operación de emitir un certificado digital firmado con la clave privada del dispositivo de certificación móvil, puede comprender autenticar al operador del dispositivo de certificación móvil mediante al menos un mecanismo de autenticación y, como resultado de la autenticación, descifrar la clave privada de la autoridad de certificación móvil o desbloquear el elemento seguro del dispositivo de certificación móvil que gestiona dicha clave privada. De acuerdo a una de las realizaciones de la presente invención, la operación de autenticar al operador se basa, al menos, en introducir una contraseña o código PIN (del inglés “Personal Identification Number”) en el dispositivo de certificación móvil y/o la utilización de un identificador biométrico.

En una de las realizaciones de la presente invención se contempla montar el dispositivo de certificación móvil como una unidad de almacenamiento en el dispositivo electrónico, por lo que la transferencia de la solicitud de firma y del certificado consiste en copiar ficheros desde el dispositivo electrónico a la unidad de almacenamiento del dispositivo de certificación móvil y viceversa. Los ficheros que se intercambian entre el dispositivo electrónico y el dispositivo de certificación móvil comprenden, de acuerdo a una de las realizaciones, la solicitud de firma de certificado, el certificado emitido o la cadena de confianza.

El dispositivo de certificación móvil de la presente invención, de acuerdo a una de sus realizaciones, restringe toda posibilidad de comunicación con otros dispositivos a una única interfaz cableada punto-a-punto, preferiblemente USB, que permite usar la presente invención de una manera local, sin requerir acceso a Internet u otras redes de comunicaciones, lo que reduce la superficie de ataque del dispositivo de certificación móvil.

Adicionalmente, de acuerdo a una realización particular, el método de la presente invención además comprende conectar el dispositivo de certificación móvil a una estación de trabajo o servidor para publicar la información de los nuevos certificados digitales emitidos en el servicio de directorio de la organización, para que puedan ser gestionados de manera centralizada, incluyendo su revocación, utilizando cualesquiera de los mecanismos de revocación de certificados X.509 existentes, en caso de que el dispositivo de certificación móvil o el dispositivo electrónico certificado resulten comprometidos.

Un segundo aspecto de la presente invención se refiere a un dispositivo de certificación móvil (10) para emitir certificados digitales a dispositivos electrónicos. El dispositivo de certificación móvil comprende:

- una interfaz cableada punto-a-punto configurada para conectar el dispositivo de certificación móvil con un dispositivo electrónico e intercambiar información;

- una interfaz gráfica configurada para mostrar información incluida en la solicitud de firma de certificado enviada desde el dispositivo electrónico conectado al dispositivo de certificación móvil y verificar o editar dicha información por el operador del dispositivo de certificación móvil; y

- un módulo procesador configurado para recibir la solicitud de firma de certificado; emitir un certificado digital para el dispositivo electrónico, donde dicho certificado digital está firmado con una clave privada previamente almacenada en el dispositivo de certificación móvil; y enviar, al dispositivo electrónico a través de la interfaz cableada, dicho certificado digital junto con una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz.

Adicionalmente, en una realización de la invención se contempla que el dispositivo de certificación móvil se integre en una infraestructura de clave pública como una autoridad de certificación subordinada, donde el módulo procesador además está configurado para generar un par de claves criptográficas asimétricas, que comprende una clave pública y una clave privada; generar una solicitud de firma de certificado que incluye información relativa al dispositivo de certificación móvil para actuar como autoridad de certificación subordinada y la clave pública generada anteriormente, donde dicha solicitud está firmada con la clave privada asociada; enviar la solicitud de firma de certificado a una autoridad de certificación padre; y recibir desde la autoridad de certificación padre, el certificado de autoridad de certificación subordinada emitido, junto con una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz.

El módulo procesador incluye, en una de las realizaciones de la invención, un elemento seguro o chip criptográfico configurado para generar un par de claves asimétricas, almacenar la clave privada generada, y firmar las solicitudes de firma de certificado y los certificados digitales para los dispositivos electrónicos con dicha clave privada.

De acuerdo a una realización de la invención, el dispositivo de certificación móvil comprende además un módulo de almacenamiento configurado para recibir copias de las solicitudes de firma de certificados enviadas desde el dispositivo electrónico conectado al dispositivo de certificación portátil mediante la interfaz cableada; copiar, desde el dispositivo electrónico, el certificado digital emitido por el dispositivo de certificación móvil, así como la cadena de confianza con todas las autoridades de certificación intermedias hasta la autoridad de certificación raíz; y almacenar una copia de todos los certificados digitales emitidos.

Adicionalmente, una de las realizaciones contempla unos medios de autenticación para identificar al operador del dispositivo de certificación móvil. Así, una de las soluciones incluye un sensor biométrico, de forma que el operador es autenticado mediante un identificador biométrico antes de autorizar la emisión de un certificado digital.

Otro aspecto de la presente invención se refiere a un sistema para emitir un certificado digital que comprende un dispositivo de certificación móvil, como los mencionados anteriormente, y además un dispositivo electrónico, conectable al dispositivo de certificación móvil a través de la interfaz cableada, configurado para detectar la conexión del dispositivo de certificación móvil, generar un par de claves criptográficas asimétricas que comprende una clave pública y una clave privada; generar una solicitud de firma de certificado que incluye información relativa a dicho dispositivo electrónico y la clave pública generada, donde dicha solicitud está firmada con la clave privada asociada; enviar la solicitud generada al dispositivo de certificación móvil a través de la interfaz cableada; y recibir el certificado digital emitido por el dispositivo de certificación móvil, así como la cadena de confianza hasta la CA raíz.

Opcionalmente, la presente invención contempla, en una de sus realizaciones, un servidor de directorio, de forma que el dispositivo de certificación móvil también permite conectarse a una estación de trabajo o servidor y publicar información de los nuevos certificados digitales emitidos en el servidor de directorio de la organización. Esto permite ventajosamente mantener un control centralizado de todos los certificados emitidos, incluyendo su revocación, sin comprometer la seguridad del dispositivo de certificación móvil.

Un último aspecto de la invención se refiere a un producto de programa de ordenador que comprende código de programa de ordenador, adaptado para realizar el procedimiento de la presente invención cuando dicho código de programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en el terreno,

un circuito integrado específico de la aplicación, un microprocesador, un micro-controlador o cualquier otra forma de hardware programable.

La presente invención, por tanto, permite a una organización emitir certificados digitales X.509 a sus dispositivos electrónicos de una manera segura, fácil y rápida, donde el operador apenas necesita conectar el dispositivo de certificación móvil al dispositivo electrónico para el que quiere emitir un certificado y autorizar la operación.

DESCRIPCIÓN DE LOS DIBUJOS

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

Figura 1.- ilustra la secuencia de pasos que se producen en la emisión de un certificado digital para un cierto dispositivo electrónico, de acuerdo a una realización de la presente invención.

Figura 2.- ilustra la secuencia de pasos que se producen para integrar un dispositivo de certificación móvil en la PKI de una organización, de acuerdo a una realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Esta descripción detallada se proporciona para ayudar a una comprensión exhaustiva de la presente invención. Por tanto, las personas medianamente expertas en la técnica serán conscientes de las eventuales variaciones, cambios y modificaciones de las realizaciones aquí descritas sin apartarse del ámbito de la invención. Además, la descripción de funciones y elementos bien conocidos en el estado del arte se omite por claridad y concisión.

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

La presente invención divulga un método y un dispositivo móvil dedicado para emitir

certificados digitales X.509 a otros dispositivos electrónicos mediante una autoridad de certificación móvil. Así, en una de las realizaciones de la invención, se define un dispositivo de certificación móvil (al que también puede hacerse referencia a lo largo de este documento como 'dispositivo de certificación' o 'autoridad de certificación móvil') que se comporta como una autoridad de certificación (CA), y el procedimiento correspondiente para emitir certificados digitales a dispositivos electrónicos (a los que también puede hacerse referencia en este documento como 'dispositivos' o 'dispositivos objetivos'), como por ejemplo servidores, ordenadores personales, dispositivos móviles, puntos de acceso, impresoras, etc., mediante la conexión de dicho dispositivo de certificación móvil directamente a ellos a través de una interfaz cableada punto-a-punto, preferiblemente USB.

En una de las realizaciones de la presente invención, el dispositivo de certificación móvil, dispone de los siguientes elementos:

- Un elemento seguro ('SE' del inglés "Secure Element"), que gestiona de forma segura la clave privada de una autoridad de certificación (CA) móvil y puede firmar certificados digitales con dicha clave.

- Una interfaz gráfica de usuario con la que el operador (al que también puede hacerse referencia como 'usuario') del dispositivo de certificación móvil de la presente invención, puede revisar y editar la solicitud de firma de certificado (CSR) del dispositivo que solicita el certificado. Si el operador está de acuerdo con la emisión de un certificado para dicho dispositivo, puede autorizar a través de la interfaz gráfica la firma de dicho certificado.

  Para autorizar la emisión del certificado, que debe estar firmado con la clave privada del dispositivo de certificación móvil, el operador debe utilizar un mecanismo de autenticación seguro, como puede ser por ejemplo la utilización de una contraseña, un PIN y/o un sensor biométrico, antes de solicitar al elemento seguro mencionado anteriormente que firme el certificado generado.

- Una interfaz cableada punto-a-punto, preferiblemente USB (del inglés "Universal Serial Bus"), que permite conectar el dispositivo de certificación móvil directamente al dispositivo objetivo. En una de las realizaciones de la invención, éste es el único interfaz de comunicación del dispositivo de certificación móvil. Así, de cara a reducir su superficie de ataque se evita cualquier interfaz de comunicación inalámbrica.

- Adicionalmente, el dispositivo de certificación móvil puede comprender otros elementos accesorios, como por ejemplo una pantalla táctil para la interacción del usuario mediante la interfaz gráfica, por ejemplo, para introducir una contraseña, PIN o, por ejemplo, sensores biométricos para la autenticación segura de usuarios.

De acuerdo a una de las realizaciones de la presente invención, el dispositivo de certificación móvil se comporta de manera similar a un dispositivo de almacenamiento USB, de forma que el procedimiento de emisión de certificados se basa esencialmente en la copia de ficheros desde el dispositivo electrónico objetivo al dispositivo de certificación móvil (CSR) y viceversa (certificado y cadena de confianza).

Para ser compatible con un gran número de dispositivos electrónicos diferentes y no requerir la pre-instalación de controladores específicos en cada uno de ellos, el dispositivo de certificación móvil, tal y como se ha mencionado anteriormente, puede comportarse como un dispositivo de almacenamiento USB, que además almacena el software y/o los manuales necesarios para generar los pares de claves criptográficas asimétricas y CSRs apropiados para los distintos sistemas operativos de dispositivos electrónicos soportados, así como para instalar posteriormente los certificados emitidos y las cadenas de confianza en los lugares adecuados de los dispositivos electrónicos (por ejemplo para incluir el certificado de la CA raíz en la lista de CAs de confianza, para usar el certificado en un servidor web de gestión seguro, para establecer un túnel IPsec, o para acceder a una red inalámbrica protegida con 802.1X). De este modo, tanto el proceso para emitir el certificado para un dispositivo electrónico e instalarlo en el mismo, o incluso para integrar el propio dispositivo de certificación móvil en una infraestructura de clave pública (PKI), se puede basar simplemente en la escritura/lectura de ficheros desde la unidad de almacenamiento del dispositivo de certificación móvil, ya sea automáticamente por software, o siguiendo manualmente las instrucciones detalladas paso a paso en los manuales almacenados en dicha unidad de almacenamiento por el administrador del dispositivo electrónico (que puede ser diferente al operador del dispositivo de certificación móvil).

Caso de uso 1: emitir un certificado digital para un dispositivo

La **figura 1** muestra una realización particular de la invención donde se detallan los pasos implicados en la emisión de un nuevo certificado para un dispositivo electrónico. En primer lugar, el dispositivo de certificación móvil (10) es conectado (1) al dispositivo electrónico objetivo (11). Esta operación se realiza mediante una conexión cableada punto-a-punto, que puede consistir en conectar una toma USB del dispositivo de certificación móvil con un puerto USB del dispositivo objetivo. De acuerdo a diferentes realizaciones, el dispositivo de certificación móvil puede estar provisto de un cable USB macho para conectarlo a otros dispositivos electrónicos con soporte USB, aunque también se contempla que únicamente comprenda una conexión USB hembra, lo que hace necesario utilizar un cable adicional para su conexión.

Una vez conectado el dispositivo de certificación móvil (10) al dispositivo objetivo (11), dicho dispositivo de certificación móvil se monta como una unidad de almacenamiento USB **(1)**.

Una vez montado el volumen de almacenamiento del dispositivo de certificación móvil en el dispositivo objetivo para el que se quiere emitir un certificado digital, el administrador del dispositivo objetivo procede a generar un par de claves criptográficas asimétricas (preferiblemente usando un elemento seguro, como por ejemplo un módulo TPM – del inglés “Trusted Platform Module” – disponible en la mayoría de servidores y PCs actuales), y generar **(2)** un fichero de solicitud de firma de certificado (CSR) que, además de incluir la clave pública generada previamente, contiene información relativa al dispositivo electrónico, como por ejemplo su nombre de dominio DNS completo y/o las direcciones de red estáticas configuradas en el dispositivo. El fichero CSR se firma con la clave privada asociada para demostrar su posesión. A continuación, el fichero CSR se copia **(3)** en el dispositivo de certificación móvil y el dispositivo objetivo queda a la espera del fichero con el certificado emitido.

De acuerdo a diferentes realizaciones de la invención, y en función del sistema operativo instalado en el dispositivo objetivo, las operaciones mencionadas para generar el par de claves, generar el fichero CSR y copiarlo en el dispositivo de certificación móvil, pueden ser realizadas de manera automática por una aplicación software, que puede estar ya pre-instalada en el dispositivo objetivo o disponible en el volumen de almacenamiento del dispositivo de certificación móvil, o bien, de manera alternativa, puede realizarse manualmente por el administrador del dispositivo (que puede ser diferente al operador del dispositivo de certificación móvil), el cual puede buscar una guía correspondiente al sistema

operativo del dispositivo objetivo en la unidad de almacenamiento del dispositivo de certificación móvil, y seguir las instrucciones paso a paso para completar el proceso.

Una vez que se ha recibido el nuevo fichero CSR en el dispositivo de certificación móvil, se muestran **(4)** todos los campos del CSR en una interfaz gráfica de usuario, de manera que el operador del dispositivo de certificación móvil puede verificarlos (actuando por tanto como una autoridad de registro – RA, del inglés “Registration Authority”). Si alguna información es incorrecta, está incompleta o falta, se puede editar manualmente. Si el operador está de acuerdo con la emisión del certificado, autoriza **(5)** la operación de firma, idealmente por medio de algún mecanismo de autenticación seguro, como puede ser la introducción de una contraseña, un código PIN y/o un identificador biométrico que desbloquee el elemento seguro. Una vez la operación ha sido autorizada por el operador, se genera **(6)** el certificado para el dispositivo objetivo, firmado con la clave privada del dispositivo de certificación móvil.

El fichero con el nuevo certificado emitido se escribe en el volumen de almacenamiento USB del dispositivo de certificación móvil de manera que, ya sea automáticamente mediante una aplicación software ejecutando en el dispositivo objetivo o manualmente por el administrador del dispositivo objetivo, es copiado **(7)** de vuelta, junto con la cadena de confianza con todas las CAs intermedias hasta la CA raíz, en los lugares adecuados del dispositivo objetivo, de manera que éste comience a confiar en la CA raíz de la organización y pueda empezar a usar el certificado emitido (por ejemplo, para configurar un servidor web seguro, establecer un túnel IPsec o para acceder a una red protegida con 802.1X).

Adicionalmente, se contempla la opción de conectar cada cierto tiempo, por ejemplo al final de cada día, el dispositivo de certificación móvil en una estación de trabajo o servidor **(12)** para descargar **(8)** en ella todos los certificados emitidos, para que estos puedan, por ejemplo, ser publicados en el servicio de directorio o directorio activo de la organización, así como para establecer el estado de vigencia de los certificados digitales y revocarlos en caso de ser necesario, ya sea basándose en listas de revocación de certificados (‘CRL’ del inglés “Certificate Revocation List”), mediante el protocolo OCSP (del inglés “Online Certificate Status Protocol”), o usando cualquier otro mecanismo (ej. “Certificate Transparency”). De esta manera, se puede mantener un control centralizado de todos los certificados emitidos y el estado de los mismos, incluyendo el del propio dispositivo de certificación móvil. Así, si el dispositivo de certificación móvil se extravía o resulta comprometido, es posible revocar el certificado de la CA móvil, de forma que todos los certificados emitidos por la misma también dejarán de ser válidos.

Una realización particular de la invención se refiere a una pequeña variación del caso de uso

descrito anteriormente. Así, se contempla el caso en el que el dispositivo objetivo no es capaz de generar sus propias claves criptográficas (ej. debido a la falta de un generador de números aleatorios criptográficamente seguros, o a la falta de software criptográfico disponible para su sistema operativo), o en el caso que la organización implemente una política de custodia de claves ("key escrow", en inglés) por la que debe almacenarse una copia de respaldo de todas las claves empleadas en la organización.

Ante esta situación, el procedimiento de emisión de certificados es el siguiente: el administrador del dispositivo electrónico objetivo puede crear un fichero de texto, a modo de CSR, con el nombre de dominio DNS del dispositivo y/o sus direcciones de red estáticas (alternativamente, esta información también puede ser introducida manualmente por el operador del dispositivo de certificación móvil usando la interfaz gráfica de usuario), de manera que el dispositivo de certificación móvil se encargue de generar el par de claves criptográficas asimétricas para el dispositivo objetivo. Así, tanto el certificado y la cadena de confianza, como el par de claves generadas (incluyendo la clave privada) son copiados manualmente en el dispositivo objetivo. Finalmente las claves generadas para el dispositivo electrónico son eliminadas del dispositivo de certificación móvil, salvo en el caso de que se implemente una política de custodia de claves, en cuyo caso el dispositivo de certificación móvil siempre generará los pares de claves de los certificados emitidos, y las almacenará temporalmente antes de ser transferidas al servidor de custodia de claves de la organización, de una manera similar a la que se emplea para publicar los certificados emitidos en el servicio de directorio de la organización, tras lo cual serán eliminadas del dispositivo de certificación móvil.

Caso de uso 2: incorporar el dispositivo de certificación móvil en una infraestructura de clave pública (PKI) como una CA subordinada.

El dispositivo de certificación móvil de la presente invención puede comportarse como una CA raíz, generando un certificado auto-firmado, aunque también se contempla que forme parte de la infraestructura de clave pública (PKI) privada de una organización y, en ese caso, ser una CA subordinada de la misma, empleando un certificado firmado por la CA raíz de la organización u otra CA intermedia que le autorice a realizar ese rol.

La **figura 2** muestra una realización particular de la invención donde se detallan los pasos para integrar un dispositivo de certificación móvil (10) dentro de la PKI privada de una

organización, que es un procedimiento similar al caso de uso anterior, pero en sentido contrario, puesto que ahora es el dispositivo de certificación móvil el que solicita la emisión de un certificado a otra autoridad de certificación (20) (que será su CA 'padre' dentro de la jerarquía de la PKI). Es decir, la sucesión de pasos, de acuerdo a una realización particular es la siguiente:

- en primer lugar, el dispositivo de certificación móvil genera un par de claves asimétricas (21), preferentemente en un elemento seguro, y con la clave pública se genera un fichero CSR para la solicitar la emisión de un certificado de CA subordinada (22). Esta operación puede requerir mecanismos de protección adicionales y obligar al operador del dispositivo de certificación móvil a autenticarse mediante la introducción de una contraseña, un PIN y/o un identificador biométrico para desbloquear el dispositivo de certificación móvil y/o su elemento seguro interno.

- El fichero CSR del dispositivo de certificación móvil se transfiere a la CA padre (23) (bien conectándolo directamente a la CA padre a través de la interfaz cableada, a una estación de trabajo que pueda comunicarse con la misma, o mediante cualquier otro mecanismo), y ésta lo procesa de acuerdo con las políticas sobre PKI de la organización para generar nuevas CAs subordinadas (que serán considerablemente más estrictas que para generar certificados y podrán requerir múltiples pasos de autorización, aunque estos aspectos quedan fuera del ámbito de esta invención) hasta que se emite el certificado de CA subordinada resultante (24), firmado con la clave privada de la CA padre.

- Finalmente se transfiere el certificado de CA subordinada resultante en el dispositivo de certificación móvil (25), junto con la cadena de confianza con los certificados de todas las CAs intermedias hasta la CA raíz. La CA móvil añadirá su certificado a dicha cadena de confianza, para generar así la cadena de confianza que se transfiere a los dispositivos electrónicos a los que se emite un certificado digital.

Desde este momento, el dispositivo de certificación móvil puede operar como una CA subordinada de la PKI de la organización y emitir certificados para otros dispositivos electrónicos con el procedimiento descrito en el primer caso de uso.

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

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

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

REIVINDICACIONES

1.- Método para emitir un certificado digital desde un dispositivo de certificación móvil (10) a un dispositivo electrónico (11) a través de una interfaz cableada, donde el método está caracterizado porque comprende los siguientes pasos:

a) conectar el dispositivo de certificación móvil al dispositivo electrónico mediante una interfaz cableada punto-a-punto;

b) como resultado del paso a), generar, en el dispositivo electrónico, un par de claves criptográficas asimétricas que comprende una clave pública y una clave privada;

c) generar, en el dispositivo electrónico, una solicitud de firma de certificado que incluye información relativa a dicho dispositivo electrónico y la clave pública generada en el paso b), donde dicha solicitud está firmada con la clave privada asociada;

d) enviar la solicitud de firma de certificado generada en el paso c) al dispositivo de certificación móvil a través de la interfaz cableada;

e) verificar, por el operador del dispositivo de certificación móvil, la información relativa al dispositivo electrónico incluida en la solicitud de firma de certificado, donde dicha información se muestra en una interfaz gráfica del dispositivo de certificación móvil;

f) emitir, por el dispositivo de certificación móvil, el certificado digital para el dispositivo electrónico, donde dicho certificado digital está firmado con una clave privada almacenada en el dispositivo de certificación móvil;

g) enviar, al dispositivo electrónico a través de la interfaz cableada, el certificado digital emitido en el paso f) y una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz.

2.- Método de acuerdo a la reivindicación anterior que además comprende integrar el dispositivo de certificación móvil en una infraestructura de clave pública como una autoridad de certificación subordinada.

3.- Método de acuerdo a la reivindicación 2 donde integrar el dispositivo de certificación móvil en una infraestructura de clave pública como una autoridad de certificación

subordinada comprende los siguientes pasos:

a) generar, en el dispositivo de certificación móvil, un par de claves criptográficas asimétricas que comprende una clave pública y una clave privada;

b) generar, en el dispositivo de certificación móvil, una solicitud de firma de certificado que incluye información relativa al dispositivo de certificación móvil para actuar como autoridad de certificación subordinada y la clave pública generada en el paso a), donde dicha solicitud está firmada con la clave privada asociada;

c) enviar la solicitud de firma de certificado desde el dispositivo de certificación móvil a la autoridad de certificación padre;

d) emitir, por la autoridad de certificación padre, un certificado de autoridad de certificación subordinada para el dispositivo de certificación móvil con la clave pública incluida en la solicitud de firma de certificado recibida;

e) enviar el certificado de autoridad de certificación subordinada, emitido por la autoridad certificadora padre en el paso d), y una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz, al dispositivo de certificación móvil.

4.- Método de acuerdo a cualquiera de las reivindicaciones anteriores donde la operación de emitir un certificado digital firmado con la clave privada del dispositivo de certificación móvil, además comprende autenticar al operador mediante al menos un mecanismo de autenticación y, como resultado de la autenticación, desbloquear el dispositivo de certificación móvil que almacena dicha clave privada.

5.- Método de acuerdo a la reivindicación 4, donde la operación de autenticar al operador del dispositivo de certificación móvil se basa, al menos, en introducir una contraseña o PIN en el dispositivo de certificación móvil y/o un identificador biométrico.

6.- Método de acuerdo a cualquier de las reivindicaciones anteriores donde la interfaz cableada es una interfaz USB.

7.- Método de acuerdo a cualquiera de las reivindicaciones anteriores que además comprende montar el dispositivo de certificación móvil como una unidad de almacenamiento USB en el dispositivo electrónico y copiar al menos un fichero en o desde dicha unidad de almacenamiento USB, donde el al menos un fichero comprende la solicitud de firma de

certificado, el certificado emitido o la cadena de confianza.

8.- Método de acuerdo a cualquiera de las reivindicaciones anteriores que además comprende comunicar el dispositivo de certificación móvil con un servidor de directorio para publicar la información de nuevos certificados digitales emitidos.

9.- Dispositivo de certificación móvil (10) para emitir un certificado digital a un dispositivo electrónico, caracterizado porque comprende:

- una interfaz cableada punto-a-punto configurada para conectar el dispositivo de certificación móvil con el dispositivo electrónico e intercambiar información;
- una interfaz gráfica configurada para mostrar información incluida en una solicitud de firma de certificado generada por el dispositivo electrónico conectado al dispositivo de certificación móvil y verificar o editar dicha información por un operador;
- un módulo procesador configurado para recibir la solicitud de firma de certificado; emitir un certificado digital para el dispositivo electrónico, donde dicho certificado digital está firmado con una clave privada previamente almacenada en el dispositivo de certificación móvil; y enviar, al dispositivo electrónico a través de la interfaz cableada, dicho certificado digital junto con una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz.

10.- Dispositivo de acuerdo a la reivindicación 9 además configurado para ser integrado en una infraestructura de clave pública como una autoridad de certificación subordinada, donde el módulo procesador además está configurado para generar un par de claves criptográficas asimétricas, que comprende una clave pública y una clave privada; generar una solicitud de firma de certificado que incluye información relativa al dispositivo de certificación móvil para actuar como autoridad de certificación subordinada y la clave pública generada anteriormente, donde dicha solicitud está firmada con la clave privada asociada; enviar la solicitud de firma de certificado a una autoridad de certificación padre; y recibir desde la autoridad de certificación padre, el certificado de autoridad de certificación subordinada emitido, junto con una cadena de confianza que incluye los certificados de todas las autoridades de certificación intermedias hasta una autoridad de certificación raíz.

11.- Dispositivo de acuerdo a cualquiera de las reivindicaciones 9-10 que además comprende un módulo de almacenamiento configurado para:

- recibir copias de las solicitudes de firma de certificados enviadas desde el dispositivo electrónico conectado al dispositivo de certificación portátil mediante la interfaz cableada;
- copiar, desde el dispositivo electrónico, el certificado digital emitido por el dispositivo de certificación móvil, así como la cadena de confianza con todas las autoridades de certificación intermedias hasta la autoridad de certificación raíz; y
- almacenar una copia de todos los certificados digitales emitidos.

12.- Dispositivo de acuerdo a cualquiera de las reivindicaciones 9-11 que además comprende unos medios de autenticación con, al menos, un sensor biométrico, donde dichos medios están configurados para autenticar al operador del dispositivo de certificación móvil mediante un identificador biométrico.

13.- Sistema para emitir un certificado digital que comprende un dispositivo de certificación móvil de acuerdo a cualquiera de las reivindicaciones 9-12, donde el sistema además comprende:

- un dispositivo electrónico (11), conectable al dispositivo de certificación móvil a través de la interfaz cableada, configurado para detectar la conexión del dispositivo de certificación móvil, generar un par de claves criptográficas asimétricas que comprende una clave pública y una clave privada; generar una solicitud de firma de certificado que incluye información relativa a dicho dispositivo electrónico y la clave pública generada, donde dicha solicitud está firmada con la clave privada asociada; enviar la solicitud generada al dispositivo de certificación móvil a través de la interfaz cableada; y recibir el certificado digital emitido por el dispositivo de certificación móvil.

14.- Sistema de acuerdo a la reivindicación 13 que comprende además un servidor de directorio (12) y donde el dispositivo de certificación móvil está además configurado para comunicarse con dicho servidor de directorio y publicar la información de nuevos certificados digitales emitidos.

15.- Producto de programa de ordenador que comprende código de programa de ordenador, adaptado para realizar el procedimiento de acuerdo a cualquiera de las reivindicaciones 1 a 8 cuando dicho código de programa es ejecutado en un ordenador, un procesador de señales digitales, una formación de compuertas programables en el terreno, un circuito

integrado específico de la aplicación, un microprocesador, un micro-controlador o cualquier otra forma de hardware programable.

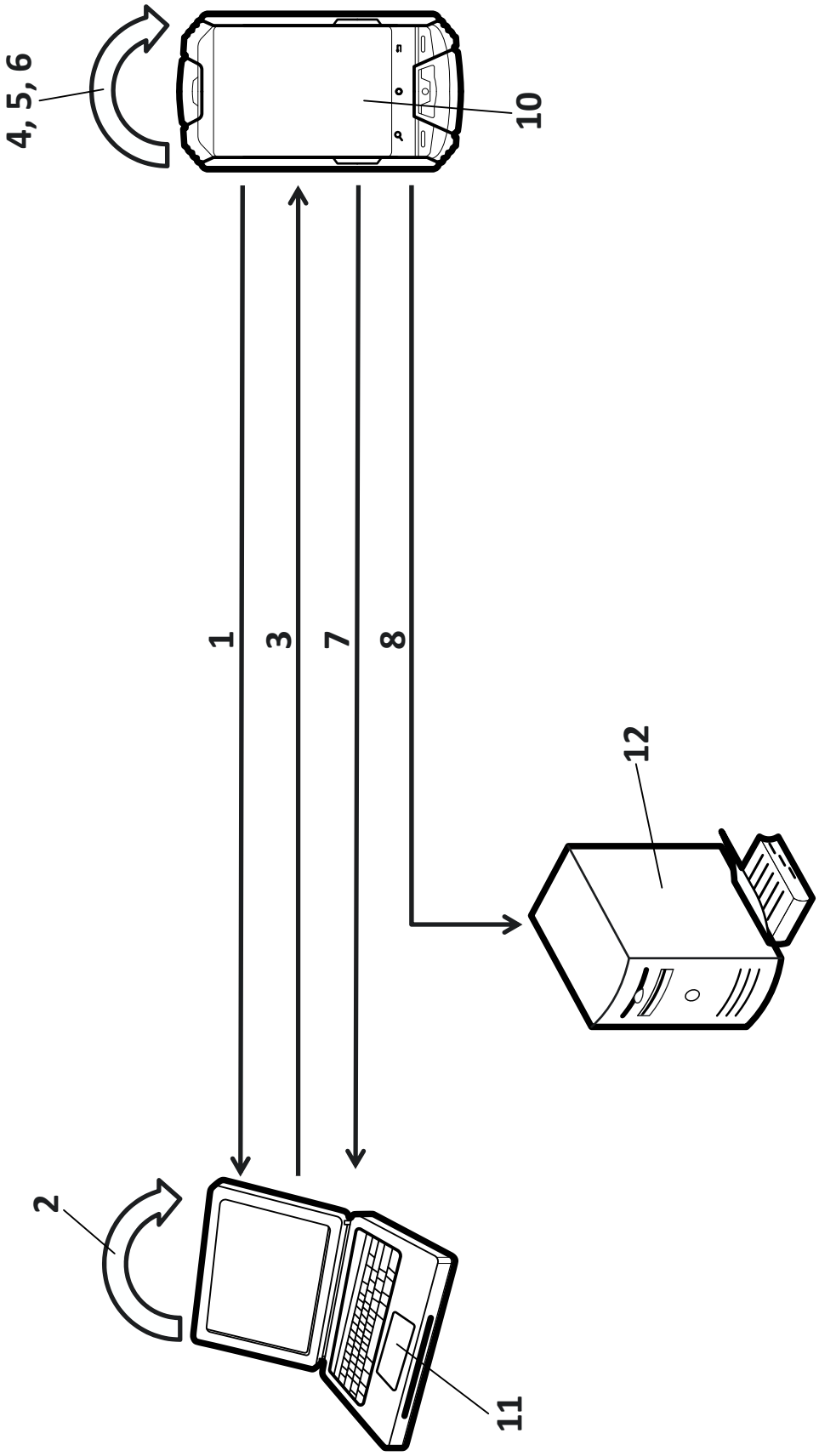

FIG. 1

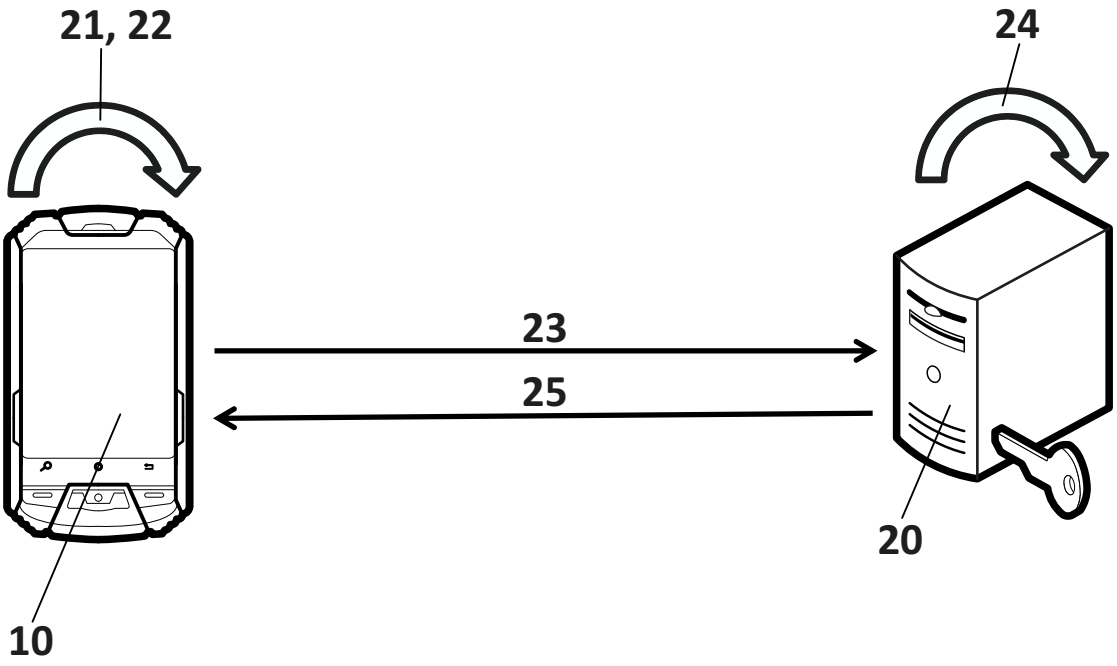

FIG. 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201730639

(22) Fecha de presentación de la solicitud: 26.04.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/00*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2013019093 A1 (SEIDL ROBERT et al.) 17/01/2013, Todo el documento.	1-15
X	US 2016142216 A1 (TURNER STEVEN K et al.) 19/05/2016, Todo el documento.	1-15
A	US 2012216035 A1 (LEGGETTE WESLEY et al.) 23/08/2012, Todo el documento.	1-15
A	US 2011302411 A1 (LIANG JIEHUI et al.) 08/12/2011, Todo el documento.	1-15
A	EP 2843873 A1 (CHINA IWNCOMM CO LTD) 04/03/2015, Todo el documento.	1-15
A	US 2004122960 A1 (HALL ERIC P et al.) 24/06/2004, Todo el documento.	1-15
A	EP 1653656 A2 (XEROX CORP) 03/05/2006, Todo el documento.	1-15
A	US 2009319796 A1 (KIM JOHN H et al.) 24/12/2009, Todo el documento.	1-15

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

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
03.04.2018	M. Muñoz Sanchez	1/3

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201730639

(22) Fecha de presentación de la solicitud: 26.04.2017

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/00*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
A	CN 101651540 A (CHINA MOBILE COMM CORP) 17/02/2010, Todo el documento.	1-15
A	CA 2871392 A1 (HONEYWELL INT INC) 17/11/2014, Todo el documento.	1-15
A	WO 2016153423 A1 (SIXSCAPE COMMUNICATIONS PTE LTD) 29/09/2016, Todo el documento.	1-15

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

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
03.04.2018	M. Muñoz Sanchez	2/3

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

H04L

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

INVENES, EPODOC, WPI