(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 835 025**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/64 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.02.2015 E 15153552 (3)**

(97) Fecha y número de publicación de la concesión europea: **09.09.2020 EP 2905925**

(54) Título: **Sistema y procedimiento de acceso remoto, firma digital remota**

(30) Prioridad:

10.02.2014 US 201414176963

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.06.2021

(73) Titular/es:

IQVIA INC. (100.0%)
100 IMS Drive
Parsippany, NJ 07054, US

(72) Inventor/es:

BLAIR, CHARLES;
FLOREZ, ELKIN;
ANNAN, DAVID;
FUNG, RYAN y
MAHGOUB, HUSSAM

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema y procedimiento de acceso remoto, firma digital remota

ANTECEDENTES

Campo de la invención

Las realizaciones de la presente invención se refieren de manera general a documentos firmados digitalmente y, en particular, a un sistema y un procedimiento para el acceso y el uso de credenciales remotos automatizados en un entorno de servicios digitales.

Descripción de la técnica relacionada

Salud móvil ("mHealth") es un término para la práctica médica y de salud pública respaldada por dispositivos móviles, como teléfonos móviles, dispositivos de monitorización de pacientes, asistentes digitales personales (PDA) y otros dispositivos inalámbricos. La mHealth implica el uso de servicios de voz y mensajes cortos (SMS), así como funcionalidades más complejas, como los sistemas 3G, los sistemas de posicionamiento global (GPS) y la tecnología Bluetooth.

La capacidad informática avanzada de los teléfonos inteligentes que típicamente están optimizados para el uso de Internet significa que las personas pueden acceder a información y asesoramiento (incluido el relacionado con la atención médica) desde cualquier lugar y en cualquier momento. Los teléfonos inteligentes también brindan una funcionalidad que no está disponible a través de un ordenador portátil, como una capacidad de capturar información de sensores en movimiento y la adición de GPS y funciones de cámara.

Una aplicación móvil (o app móvil) es una aplicación de software diseñada para ejecutarse en teléfonos inteligentes, ordenadores de tableta y otros dispositivos móviles. Algunas aplicaciones móviles se usan para brindar información sobre atención médica a los consumidores o para recopilar y enviar información sobre el estado de salud de un consumidor a un proveedor de cuidados médicos. No todas las aplicaciones móviles que se han desarrollado en el cuidado de la salud están ampliamente disponibles para los consumidores. Algunas de las aplicaciones médicas más avanzadas no están diseñadas necesariamente para dirigirse a los consumidores en general. Algunas aplicaciones móviles se han diseñado para profesionales del cuidado de la salud, otras son para pacientes, pero requieren receta médica, y otras están destinadas solo a un pequeño subconjunto de pacientes. Algunas aplicaciones móviles requieren la aprobación de la Administración de Alimentos y Medicamentos de los EE.UU. (FDA). Una aplicación móvil también puede ejecutarse en otras plataformas, como un ordenador personal (PC), si se ha adaptado al sistema operativo subyacente, por ejemplo, de Android a Windows o iOS. Como se usa en esta invención, el término "aplicación móvil" puede incluir una aplicación que se ejecuta en un PC (por ejemplo, un ordenador de escritorio, de torre, un ordenador portátil, una netbook, etc.) u otro dispositivo informático de uso general para el consumidor, sin limitación a un dispositivo móvil, a menos que la movilidad proporcione un beneficio declarado o que al menos esté claramente restringido por el contexto de uso.

Cierta información del paciente está protegida por la ley (por ejemplo, la Ley de portabilidad y responsabilidad de la información médica (HIPAA) en los EE.UU.) y debe tratarse de manera que se mantenga la privacidad del paciente. Tal información se denomina información médica protegida (PHI). Con respecto a la PHI, es importante que exista transparencia y conocimiento de cómo se usan los datos ingresados en una aplicación móvil, y que se obtenga el consentimiento del paciente para el uso de los datos de PHI. Si una aplicación móvil de atención médica recopila, almacena y/o transmite la PHI, es esencial que lo haga en total cumplimiento con la Ley de responsabilidad y portabilidad del seguro médico (HIPAA) y cualquier otra ley o reglamentación aplicable del país en cuestión. Cualquier aplicación móvil que esté destinada a conectarse a un registro médico electrónico (EHR) o registro médico personal (PHR), que permite a los usuarios enviar y recuperar información del paciente entre un dispositivo móvil y el EHR/PHR, debe hacerlo de manera segura y todas las partes interesadas involucradas deben aceptar su función de administración para proteger los datos de la PHI que contiene.

El cifrado es una herramienta estándar para garantizar la privacidad de las comunicaciones. Hay una variedad de esquemas de cifrado disponibles comercialmente para asegurar la información protegida, por ejemplo, el Estándar de cifrado avanzado (AES), promulgado por el Instituto Nacional de Estándares y Tecnología (NIST) como la Publicación 197 de Estándares de procesamiento de información federal, del 26 de noviembre de 2001. El AES es un esquema de cifrado simétrico, de modo que se usa una misma clave de cifrado tanto para la codificación como para la decodificación. El esquema AES en sí mismo existe en múltiples variaciones, como el modo de contador AES, el

encadenamiento de bloques de cifrado AES (CBC) + robo de texto cifrado (CTS), RSA, y así sucesivamente. Algunas variaciones del AES pueden describirse en la Solicitud de comentario (RFC) 3962, "Encriptación de estándar de cifrado avanzado (AES) para Kerberos 5", de febrero de 2005, y las referencias allí citadas.

Una firma escrita convencional es un indicio generado por humanos que se puede usar para indicar la autenticidad de un documento o para indicar que está de acuerdo con las declaraciones dentro del documento. Una firma digital es un esquema matemático para demostrar la autenticidad de un mensaje o documento digital. Una firma digital válida le da al destinatario una razón para creer que un remitente conocido creó el mensaje, de modo que el remitente no puede negar haber enviado el mensaje (es decir que garantiza la autenticación y la ausencia de repudio) y que el mensaje no se modificó en tránsito (es decir que garantiza la integridad). Las firmas digitales se usan comúnmente para la distribución de software, transacciones financieras y en otros casos en los que es importante detectar falsificaciones o alteraciones. La creación y el uso de firmas digitales normalmente implica cifrado.

La gestión de claves de cifrado públicas y privadas es integral a la firma digital y/o el cifrado. Un certificado digital es un documento electrónico que usa una firma digital para vincular una clave pública con una identidad, por ejemplo, el nombre de una persona u organización, su dirección y así sucesivamente. El certificado se puede usar para verificar que una clave pública pertenece a una persona. La infraestructura de clave pública (PKI) es un conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales. La PKI es conocida en la técnica, como se describe en la Patente de los EE.UU. No. 5.864.667 para Barkan.

La PKI vincula una clave pública con una identidad de usuario respectiva por medio de una autoridad de certificación (CA). La identidad del usuario debe ser única dentro de cada dominio de la CA. Una autoridad de validación (VA) de terceros puede proporcionar esta información en nombre de la CA. La vinculación se establece a través del procedimiento de registro y concesión, que, dependiendo del nivel de garantía de la vinculación, se puede realizar mediante software en una CA o bajo supervisión humana. La función de PKI que garantiza esta vinculación se denomina autoridad de registro (RA), la cual asegura que la clave pública está vinculada a la persona a la que se asigna de una manera que asegura la ausencia de repudio.

Un inconveniente del uso de los servicios de PKI en un entorno disperso con aplicaciones móviles es que existen muchos obstáculos requeridos para la utilización de los servicios de PKI. Los usuarios de aplicaciones móviles normalmente deben tener algunos conocimientos técnicos o conocimientos de seguridad para comenzar. Los usuarios de aplicaciones móviles deben tener algunos conocimientos sobre la gestión de claves asimétricas (por ejemplo, claves públicas y privadas), almacenar claves de manera segura y cambiar claves de manera segura localmente. Los usuarios de aplicaciones móviles suelen tener dificultades con el procedimiento de PKI, por ejemplo, con cómo empezar y qué hacer. Los usuarios de aplicaciones móviles normalmente no son expertos en seguridad, pero se les pide que gestionen las credenciales o claves de PKI. Algunos usuarios de aplicaciones móviles pueden estar gestionando credenciales de PKI y solicitudes de certificado para múltiples dispositivos, y pueden tener dificultades para realizar un seguimiento del estado de los distintos dispositivos y sus credenciales de PKI.

Las soluciones conocidas han abordado la gestión y los procedimientos de PKI de manera manual, de modo que los usuarios deben crear un par de claves de PKI manualmente y luego gestionarlas manualmente. Esto resulta muy demandante para los usuarios de aplicaciones móviles que, por lo general, no conocen bien estos procedimientos. Si el par de claves de PKI no se gestiona correctamente, la seguridad puede verse comprometida.

Otras soluciones conocidas han empleado elementos seguros como tarjetas inteligentes, tarjetas de acceso común (CAC) y dispositivos especialmente configurados que se usan para alojar de manera segura las credenciales de PKI de los usuarios finales. Para tales soluciones, el usuario debe llevar dispositivos y tarjetas adicionales para utilizar los servicios de PKI. La práctica comercial actual también incluye servicios en línea, productos y conjuntos de herramientas para desarrolladores y usuarios finales para gestionar las credenciales y los servicios de PKI. En estos casos, todavía se usa un procedimiento manual para la gestión de PKI.

El documento WO 2014/077698 describe un procedimiento para la firma digital de documentos. Esto lo proporciona un sistema de transferencia de firmas que extrae la firma de un documento firmado y transfiere la firma extraída a un documento preparado. Esto permite la firma múltiple de un documento.

El documento US 2013/311772 describe una firma digital que se aplica a documentos/información de tipo digital. En ciertos casos, se logran firmas digitales jurídicamente sólidas. Las tecnologías de informática en la nube se pueden usar para ayudar en la producción de firmas digitales autenticadas y criptográficamente seguras. Las firmas digitales se pueden producir con una notarización digital. Es posible que las técnicas de generación de una firma digital no

requieran el uso de la infraestructura de clave pública tradicional (PKI).

El documento US 2013/219181 describe un procedimiento para leer al menos un atributo que está almacenado en un token de ID, siendo el token de ID asignado a un usuario. El procedimiento comprende las siguientes etapas: autenticar al usuario con respecto al token de ID; autenticar un primer sistema de ordenador con respecto al token de ID; después de que el usuario y el primer sistema de ordenador se hayan autenticado con éxito con respecto al token de ID, proporcionar al primer sistema de ordenador acceso de lectura al, al menos un, atributo almacenado en el token de ID a fin de transmitir el al menos un atributo a un segundo sistema de ordenador.

El documento US2011293098 describe un procedimiento y sistema para la recuperación de claves para una clave privada de un certificado digital para un cliente y la transmisión de dicho certificado digital.

El documento US2003035548 describe procedimientos y sistemas para permitir que las claves privadas de los usuarios correspondientes a sus certificados digitales se almacenen y archiven fuera del control de una autoridad de certificación ("CA"). Una CA puede tener una política de que la clave privada de un usuario debe ser archivada para recibir un certificado digital cuando el usuario lo solicite. Normalmente, la CA sabe que la clave privada del usuario está archivada porque implementa el archivo de la clave, por ejemplo, en un gestor de recuperación de datos y una base de datos interna asociada que la CA controla. Los procedimientos y sistemas según la presente invención permiten la aplicación de dicha política al tiempo que permiten que el archivo de las claves privadas esté fuera del control de la CA al hacer que un gestor de recuperación de datos proporcione una prueba de token de archivo firmada digitalmente con una solicitud de certificado digital a una CA. A la CA se le garantiza que la clave ha sido archivada. Los procedimientos y sistemas permiten que el gestor de recuperación de datos y una base de datos de claves archivadas sean controlados por otras entidades, incluyendo el usuario o cliente, por ejemplo.

Por lo tanto, lo que se necesita es un procedimiento más automatizado de gestión de PKI sin los inconvenientes de usar dispositivos adicionales.

RESUMEN

La presente descripción proporciona un procedimiento como se detalla en la reivindicación 1 y un sistema según la reivindicación 6. Las características ventajosas se proporcionan en las reivindicaciones dependientes.

En una realización, un procedimiento para validar digitalmente un documento puede incluir: recibir, mediante una plataforma de desarrollo segura (SDP), una información de seguridad de un usuario final, comprendiendo la SDP un procesador SDP acoplado a una memoria SDP segura; intercambiar un token de seguridad con un dispositivo de usuario basado en la información de seguridad; recibir, desde el dispositivo del usuario, una solicitud de certificado digital; generar el par de claves de PKI de usuario y almacenarlo en el almacenamiento de claves seguro SDP, transmitir, al procesador de servicios de PKI, una solicitud de certificado digital; si la información de la solicitud de certificado digital es correcta: crear el certificado digital; recibir el certificado digital del procesador de servicios de PKI; y almacenar el certificado digital en la memoria SDP segura, siendo la memoria SDP segura no accesible directamente para el dispositivo del usuario, y estando el procesador SDP configurado para solicitar una validación mediante el uso del certificado digital.

En algunas realizaciones, el procedimiento puede incluir además: recibir, desde el dispositivo de usuario, un documento a firmar digitalmente; transmitir, al procesador de servicios de PKI, una solicitud para validar un certificado digital relacionado con el dispositivo de usuario; recibir, del procesador de servicios de PKI, una indicación de validez del certificado digital; y, si la indicación indica un certificado digital válido, firmar digitalmente el documento en base al certificado digital.

En algunas realizaciones, el procedimiento puede incluir además: recibir, desde el dispositivo de usuario, un documento a validar y el certificado digital; proporcionar, al procesador de servicios de PKI, el certificado digital; recibir, del procesador de servicios de PKI, una indicación de validez del certificado digital; y, si la indicación indica un certificado digital válido, proporcionar una indicación de validez del documento al dispositivo del usuario.

En una realización, un sistema para validar digitalmente un documento puede incluir: una plataforma de desarrollo segura (SDP), comprendiendo la SDP un procesador SDP acoplado a una memoria SDP segura y a un receptor, el receptor configurado para recibir una información de seguridad desde un usuario final; una interfaz de comunicación configurada: para intercambiar un token de seguridad con un dispositivo de usuario en base a la información de seguridad; y recibir, desde el dispositivo de usuario, una solicitud de certificado digital; un transmisor configurado para transmitir, al procesador de servicios de PKI, una solicitud de certificado digital; y un receptor configurado para recibir

el certificado digital del procesador de servicios de PKI; donde el certificado digital almacenado en la memoria SDP segura no es directamente accesible para el dispositivo de usuario.

En algunas realizaciones, el sistema puede incluir además: un transmisor configurado para transmitir un certificado digital y un documento a validar, donde el certificado digital es validado por el procesador de servicios de PKI; y un receptor configurado para recibir, del procesador de servicios de PKI, una indicación de validez del certificado digital, donde la SDP proporciona la indicación de validez al dispositivo de usuario.

En algunas realizaciones, el sistema puede incluir además: un transmisor configurado para transmitir al procesador de servicios de PKI un certificado digital a validar; y un receptor configurado para recibir, del procesador de servicios de PKI, una indicación de validez del certificado digital, donde la SDP firma digitalmente el documento basándose en la indicación de validez.

Lo anterior es un resumen simplificado de las realizaciones de la descripción para proporcionar una comprensión de algunos aspectos de la descripción. Este resumen no es un panorama general extenso ni exhaustivo de la descripción y sus diversas realizaciones. No pretende identificar los elementos claves o fundamentales de la descripción ni delinear el alcance de la descripción, sino presentar los conceptos seleccionados de la descripción de manera simplificada como una introducción a la descripción más detallada que se presenta a continuación. Como se podrá apreciar, otras realizaciones de la descripción son posibles utilizando, solos o en combinación, uno o más de las características indicadas anteriormente o descritas de manera más detallada a continuación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Las características y las ventajas anteriores e incluso adicionales de la presente invención serán evidentes tras considerar la siguiente descripción detallada de las realizaciones de la misma, especialmente cuando se toman en conjunto con los dibujos adjuntos, en los que números similares en las diversas figuras se utilizan para designar componentes similares y donde:

la FIG. 1 es un diagrama de bloque que representa una red de comunicación móvil según una realización de la presente invención;

la FIG. 2A es un diagrama de bloques a nivel del sistema que representa un dispositivo móvil según una realización de la presente invención;

la FIG. 2B es un diagrama de bloques a nivel de sistema que representa un dispositivo no móvil de usuario final según una realización de la presente invención;

la FIG. 3 es un diagrama de bloques que representa un sistema y un procedimiento para soportar de PKI y certificados digitales según una realización de la presente invención;

la FIG. 4 es un diagrama de bloques que representa un sistema y un procedimiento para crear un certificado digital según una realización de la presente invención;

la FIG. 5 es un diagrama de bloques que representa un sistema y un procedimiento para firmar un documento con un certificado digital según una realización de la presente invención; y

la FIG. 6 es un diagrama de bloques que representa un sistema y un procedimiento para validar un documento firmado mediante el uso de un certificado digital según una realización de la presente invención.

Los títulos que se usan en esta invención tienen solamente una finalidad de organización y no pretenden usarse para limitar el alcance de la descripción o las reivindicaciones. Como se usa a lo largo de esta solicitud, la palabra "puede" se usa en un sentido permisivo (*es decir,* que significa que tiene el potencial de), en lugar de un sentido obligatorio (*es decir,* que significa que debe). De modo similar, las palabras "incluir", "incluyendo" y "que incluye(n)" significan que incluye, pero sin limitarse a eso. Para facilitar la comprensión, se usaron números de referencia similares, dentro de lo posible, para designar elementos similares comunes a las figuras. Las porciones opcionales de las figuras pueden ilustrarse usando líneas punteadas o cortadas, a menos que el contexto de uso indique lo contrario.

DESCRIPCIÓN DETALLADA

La descripción se ilustrará a continuación junto con un sistema de información digital ejemplar. Si bien es adecuada

para uso, por ejemplo, con un sistema que usa uno más servidores y/o bases de datos, la descripción no se limita al uso con cualquier tipo particular de sistema o configuración de elementos del sistema. Los expertos en la técnica reconocerán que las técnicas descritas se pueden usar en cualquier sistema o procedimiento en el que sea deseable proporcionar un permiso transferible para acceder a información o controlar una decisión.

Los sistemas y procedimientos ejemplares de esta descripción se describirán también en relación con el software, los módulos y el hardware asociado. Sin embargo, para evitar que la presente descripción resulte poco clara de manera innecesaria, la siguiente descripción omite estructuras, componentes y dispositivos bien conocidos que pueden mostrarse en forma de diagrama de bloques, que son bien conocidos o se resumen de otra manera.

En la siguiente descripción detallada, se exponen numerosos detalles específicos a fin de proporcionar una comprensión rigurosa de las realizaciones u otros ejemplos descritos en esta invención. En algunos casos, no se han descrito de manera detallada procedimientos, técnicas, componentes y circuitos con el fin de no complicar las realizaciones descritas en la siguiente descripción. Además, los ejemplos descritos solo tienen un fin ejemplar y se pueden emplear otros ejemplos en lugar de, o en combinación con, los ejemplos descritos. Cabe señalar también que los ejemplos que se incluyen en esta invención no deben interpretarse como una limitación del alcance de las realizaciones de la presente invención, ya que son posibles y probables otros ejemplos igualmente efectivos.

Tal como se usa en esta invención, el término "módulo" hace referencia, de manera general, a una secuencia o asociación lógica de etapas, procedimientos o componentes. Por ejemplo, un módulo de software puede comprender un conjunto de rutinas o subrutinas asociadas dentro de un programa de ordenador. De manera alternativa, un módulo puede comprender un dispositivo de hardware sustancialmente autónomo. Un módulo puede comprender también un conjunto lógico de procedimientos independientemente de cualquier implementación de software o hardware.

Como se usa en esta invención, el término "transmisor" puede comprender generalmente cualquier dispositivo, circuito o aparato capaz de transmitir una señal. Como se usa en esta invención, el término "receptor" puede comprender generalmente cualquier dispositivo, circuito o aparato capaz de recibir una señal. Como se usa en esta invención, el término "transceptor" generalmente puede comprender cualquier dispositivo, circuito o aparato capaz de transmitir y recibir una señal. Como se usa en esta invención, el término "señal" puede incluir una o más de una señal eléctrica, una señal de radio, una señal óptica, una señal acústica y así sucesivamente.

El término "medio legible por ordenador", como se usa en esta invención, se refiere a cualquier medio que participa en el almacenamiento y/o la proporción de instrucciones a un procesador para su ejecución. Dicho medio puede adoptar muchas formas, lo que incluye, entre otros, medios no volátiles y medios volátiles. Los medios no volátiles incluyen, por ejemplo, NVRAM o discos magnéticos u ópticos. Los medios volátiles incluyen la memoria dinámica, como la memoria principal. Las formas comunes de medios legibles por ordenador incluyen, por ejemplo, un disquete, un disco flexible, disco duro, una cinta magnética, cualquier otro medio magnético, un CD-ROM, cualquier otro medio óptico, tarjetas perforadas, una cinta de papel, cualquier otro medio físico con patrones de orificios, una RAM, una PROM, una EPROM, una FLASH-EPROM, un medio en estado sólido como una tarjeta de memoria, cualquier otro chip o cartucho de memoria, una onda portadora como se describirá en lo sucesivo o cualquier otro medio a partir del cual pueda leer un ordenador. Un archivo digital adjunto a un correo electrónico u otro archivo o conjunto de archivos de información autónomo se considera un medio de distribución equivalente a un medio de almacenamiento tangible. Cuando el medio legible por ordenador se configura como una base de datos, se debe entender que la base de datos puede ser cualquier tipo de base de datos, como relacional, jerárquica, orientada a objetos y/o similares. En consecuencia, se considera que la descripción incluye un medio de almacenamiento o medio de distribución tangible y equivalentes y medios sucesores reconocidos en la técnica anterior, en los que se almacenan las implementaciones de software de la presente descripción.

Las realizaciones según la presente descripción pueden proporcionar un procedimiento digital y/o un sistema para facilitar la seguridad de la información.

Las realizaciones según la presente descripción mejoran la técnica conocida realizando operaciones de iniciación de PKI, operaciones de gestión de claves, gestión de certificados X.509 y operaciones de gestión de uso dentro de un dominio seguro de una plataforma de desarrollo de aplicaciones móviles segura. Con una plataforma de desarrollo tan segura, los usuarios pueden solicitar la creación y el almacenamiento de claves asimétricas dentro de la plataforma de desarrollo segura. Los usuarios pueden utilizar las operaciones de PKI, incluida la firma y la validación de datos de salud o PHI. La plataforma de desarrollo segura puede incluir un contenedor móvil seguro con un almacenamiento de datos seguro. La plataforma de desarrollo segura permite a un desarrollador de software desarrollar aplicaciones de software en un entorno seguro. El entorno seguro puede incluir la ausencia de amenazas externas, así como el acceso a información confidencial, como datos de PHI, operaciones de PKI, certificados digitales y así sucesivamente. Más

tarde, después de que una aplicación de software se completa y se publica para su uso, la plataforma de desarrollo segura puede permitir a los usuarios finales usar la aplicación de software, sin necesidad de gestionar la seguridad de la información, pares de claves públicas/privadas y otras credenciales, y así sucesivamente. La plataforma de desarrollo segura opera protegiendo los datos y el acceso a los datos en un nivel de aplicación de una pila de redes.

El usuario puede acceder al almacenamiento seguro de datos móviles mediante la autenticación del PIN de usuario. El almacenamiento seguro de datos móviles está protegido por una clave simétrica derivada que se deriva de un número de factores, incluido el PIN del usuario. La plataforma de desarrollo segura puede incluir seguridad integrada para autenticación dual y cifrado de contenido y datos por sesión. Una clave simétrica usada para el cifrado de datos se cambia por sesión, lo que ayuda a garantizar una transferencia segura de datos entre el servidor seguro de IMS y los dispositivos móviles.

La plataforma de desarrollo segura puede crear credenciales únicas para cada usuario, de modo que cada usuario esté vinculado a un par de claves de PKI específico (por ejemplo, claves públicas y privadas). La plataforma de desarrollo segura gestiona el par de claves de PKI de manera independiente por usuario. Una ventaja de la plataforma de desarrollo segura es que se proporcionan credenciales únicas por usuario, lo que reduce la posibilidad de uso no autorizado. Otra ventaja es que las claves de cifrado de datos o las claves simétricas se basan en sesiones (es decir, son efímeras). Las claves basadas en sesiones reducen la posibilidad de que una clave sea violada durante el tiempo en que aún se está usando. Otra ventaja es que se usan sesiones cifradas con autenticación dual, lo que protege las sesiones incluso cuando una clave está comprometida. Otra ventaja es que el almacenamiento seguro de datos se proporciona en un contenedor móvil y un contenedor de servidor, lo que aísla el almacenamiento seguro de datos de otros procedimientos que se ejecutan en el terminal móvil o la plataforma de desarrollo segura y ayuda a habilitar un sistema de PKI fácil de usar. La plataforma de desarrollo segura puede proporcionar una PKI integrada como un servicio adicional relacionado con la gestión de seguridad de datos PHI.

La plataforma de desarrollo segura puede gestionar de manera centralizada las credenciales y los servicios de PKI para los usuarios. Los usuarios no tendrán que ser expertos en PKI, expertos en seguridad o expertos técnicos para usar los procedimientos de PKI. La seguridad está integrada y no se requiere que el usuario sea un experto en seguridad ni que gestione componentes de PKI.

Las realizaciones según la presente descripción pueden usar un token de seguridad y un sistema de contraseña de un solo uso (OTP) para simplificar el uso de la PKI de un usuario. El usuario no necesita ningún conocimiento de PKI específico o detallado para gestionar su uso de PKI. No es necesario implementar protocolos de PKI en el dispositivo móvil de un usuario.

Las realizaciones según la presente descripción usan un procedimiento de PKI automatizado y proporcionan una gestión automatizada de pares de claves de PKI (pares de claves públicas/privadas). El uso y la gestión automatizada pueden incluir generación de claves, gestión, almacenamiento y/o el uso de pares de claves de PKI en el lado del servidor, liberando así al usuario de gran parte de esta carga. Si el dispositivo móvil de un usuario necesita ser reemplazado (por ejemplo, debido a la pérdida de un dispositivo o su actualización), a continuación, el procedimiento de reemplazo de ese dispositivo se simplifica sin necesidad de gestionar pares de claves de PKI en el dispositivo móvil u otro dispositivo informático compatible.

Las realizaciones según la presente descripción permiten a un usuario en un dispositivo móvil acceder de manera remota y segura a las operaciones de pares de claves de PKI realizadas por la plataforma de desarrollo segura. Por ejemplo, las realizaciones permiten que el dispositivo móvil delegue las operaciones de PKI a la plataforma de desarrollo segura, de modo que la plataforma de desarrollo segura actúe en la función de un servidor remoto (es decir, un editor de pares de claves de PKI públicas para la plataforma móvil). Además, las realizaciones pueden soportar la generación y validación de firmas digitales, de modo que los documentos confiables puedan intercambiarse entre la plataforma móvil y la plataforma de desarrollo segura u otras plataformas informáticas remotas.

Las realizaciones según la presente descripción proporcionan servicios de PKI expandidos para aplicaciones de salud y de otro tipo. Dichas realizaciones pueden ser útiles para intercambiar PHI u otra información protegida con usuarios o generadores de dicha información, como la Iniciativa Automate Blue Button (ABBI) (es decir, un sistema que permite a los pacientes ver en línea y descargar sus propios registros médicos personales), el Gobierno de los Estados Unidos (por ejemplo, la Administración de Veteranos (VA), el Departamento de Defensa (DoD), el Departamento de Salud y Servicios Humanos (HHS), empresas financieras (por ejemplo, bancos, corretaje), etc.).

Las realizaciones según la presente descripción proporcionan soporte universal para sustancialmente cualquier dispositivo de usuario de capacidades suficientes, como plataformas móviles, ordenadores personales de escritorio y

así sucesivamente. Las realizaciones no están ligadas a la arquitectura patentada de un único dispositivo cerrado. Mediante dicho soporte universal, las realizaciones proporcionan soporte para traer su propio dispositivo (BYOD), de manera que un usuario de dispositivo móvil puede continuar usando su dispositivo móvil existente cuando practica las realizaciones según la presente descripción.

Las realizaciones según la presente descripción proporcionan y logran las ventajas mencionadas anteriormente, al menos en parte, al mover las operaciones de PKI desde el dispositivo móvil de un usuario a un servidor de credenciales/claves de una plataforma de desarrollo segura. Alojar las operaciones de credenciales en el servidor de credenciales proporciona varias ventajas. En primer lugar, el uso del servidor de credenciales permite que a los usuarios les resulte más fácil realizar operaciones tales como la generación de claves, la firma, el cifrado y así sucesivamente.

Otra ventaja de usar un servidor de credenciales es que el servidor de credenciales puede proporcionar una instalación de almacenamiento segura y sólida para las claves privadas en el servidor, en lugar de en el dispositivo. Todas las claves privadas se protegerán y bloquearán mediante una clave de pases múltiples que no necesariamente se almacena, sino que puede derivarse de diferentes fuentes. Esto puede proporcionar una mayor seguridad contra ataques maliciosos, en comparación con el almacenamiento disperso de claves privadas en los dispositivos móviles de los usuarios. El costo de la seguridad gestionada profesionalmente del servidor de credenciales puede distribuirse entre todos los usuarios móviles, reduciendo así potencialmente el costo para los usuarios individuales.

Otra ventaja de usar un servidor de credenciales es que el servidor de credenciales puede proporcionar una mejor calidad de generación de pares de claves públicas/privadas, mediante el uso de un generador de números aleatorios de mayor calidad, por ejemplo, un generador de números aleatorios que ha sido validado según la Publicación 140-2 del Estándar federal de procesamiento de información (FIPS), (FIPS PUB 140-2)", Requisitos de seguridad para módulos criptográficos", concedida el 25 de mayo de 2001. A menudo, se usa un número aleatorio como valor original para inicializar una función u operación criptográfica. Por lo tanto, un valor original que sea aleatorio de manera más uniforme en un sentido estadístico será más difícil de adivinar y, por consiguiente, será más difícil predecir la secuencia completa del generador de números aleatorios.

Otra ventaja de usar un servidor de credenciales es que el servidor de credenciales puede proporcionar un almacenamiento seguro de mejor calidad en el servidor, por ejemplo, un módulo de seguridad de hardware (HSM) u otro aparato dedicado y/o basado en hardware a fin de proporcionar la seguridad de los datos.

Otra ventaja de usar un servidor de credenciales es que el servidor de credenciales puede proporcionar un servicio de restauración de tokens, desde el servidor de credenciales a un dispositivo móvil, en ciertas condiciones. Por ejemplo, el servicio de restauración de tokens se puede usar cuando un usuario pierde su dispositivo móvil, o si el usuario compra un nuevo dispositivo móvil, y así sucesivamente. Al almacenar las credenciales en el servidor de credenciales, en lugar de en el dispositivo móvil, la clave privada puede asociarse con el usuario en lugar de con el dispositivo móvil del usuario. Sin este servicio de restauración de tokens, si un usuario perdiera o cambiara su dispositivo, la clave privada se perdería y el certificado tendría que agregarse a una lista de revocación de certificados (CRL). La CRL es una lista de certificados (o una lista de números de serie de certificados) que han sido revocados y, por lo tanto, una entidad que presenta un certificado revocado ya no debería ser confiable. Convencionalmente, si un usuario perdiera o reemplazara su dispositivo móvil, se debe generar un nuevo par de claves públicas/privadas y se deben producir y distribuir nuevos certificados que dependan de la clave pública.

Otra ventaja de usar un servidor de credenciales es que el servidor de credenciales puede proporcionar un canal de comunicación autenticado y cifrado bilateralmente (es decir, de manera bidireccional) para todas las transacciones entre el dispositivo y el servidor, usando una contraseña de un solo uso (OTP).

Otra ventaja de usar un servidor de credenciales es que el servidor de credenciales puede proporcionar servicios de PKI a los usuarios que pueden estar usando una amplia variedad de dispositivos remotos y dispositivos móviles (por ejemplo, dispositivos compatibles con Java 2 Micro Edition (J2ME), BlackBerry, Android, Apple, etc.)/ un ordenador personal/ procesadores integrados, y así sucesivamente, habilitados con capacidad de OTP. La capacidad de la OTP se puede usar para proporcionar la autenticación del usuario principal para un procedimiento de inscripción y registro de PKI.

Las realizaciones según la presente descripción proporcionan acceso remoto a los procedimientos de PKI usando una aplicación móvil, mediante el uso de un token digital y un esquema de acceso de OTP. Hacerlo ayuda a garantizar que solo un usuario final autorizado tenga acceso a su información de PKI privada. Se puede usar un protocolo de sincronización para proporcionar autenticación mutua y cifrado de mensajes de extremo a extremo. El token digital y/o

la tecnología de OTP se pueden usar para derivar una clave de cifrado única para un usuario, con el fin de gestionar las credenciales de PKI del usuario. Las realizaciones también pueden proporcionar un punto de entrada seguro para los procedimientos de PKI cuando un usuario está usando un programa de aplicación móvil.

La FIG. 1 ilustra un sistema para acceder, validar y firmar digitalmente información confidencial según una realización de la invención. Las realizaciones descritas en este documento se refieren a un sistema para generar y usar una PKI digital (o un certificado digital basado en una PKI) entre dos partes: en este caso, un usuario de dispositivo móvil y un servidor de credenciales en un dominio confiable. El teléfono móvil tiene la capacidad de comunicación suficiente para conectarse al servidor de credenciales para la gestión del acceso a información confidencial, como la PHI.

Se muestra un número de dispositivos móviles 20 en comunicación inalámbrica con estaciones base celulares 24 a través de comunicaciones celulares. Las estaciones base celulares 24 permiten comunicaciones a través de una gran red pública, tal como Internet 28, a través de un número de servidores intermedios operados por uno o más portadores de comunicaciones celulares (no mostrados). La FIG. 1 ilustra además un número de dispositivos informáticos no móviles 21 en contacto comunicativo con Internet 28. Un servidor de transacciones 32 también puede estar en comunicación con Internet 28. El servidor de transacciones 32 también puede estar en comunicación con un servidor de validación 36 a través de una red privada. Además, el servidor de transacciones 32 puede estar en comunicación con uno o más depósitos de información confidencial, como una institución financiera 40, donde los usuarios de los dispositivos móviles 20 y/o los dispositivos de ordenador no móviles 21 pueden tener una relación de algún tipo, como de negocios o de atención médica.

Las realizaciones según la presente descripción no se limitan a los tipos de dispositivos móviles 20 y/o los dispositivos informáticos no móviles 21 ilustrados en la FIG. 1. Las realizaciones pueden usarse sustancialmente con cualquier tipo de dispositivo de entrada/salida dispositivo o terminal, incluyendo un ordenador personal, MacBooks, una tableta, clientes ligeros o sustancialmente cualquier otro tipo de dispositivo informático accesible a través de una red.

Cabe destacar la configuración de los elementos como se muestra en la FIG. 1 es sólo con fines ilustrativos y no debe interpretarse como realizaciones limitantes de la presente invención a ninguna disposición particular de los elementos.

El servidor puede ser un sistema controlado por software que incluye un conjunto de procesamiento (CPU), un microprocesador u otro tipo de procesador de datos digitales que ejecuta software o un circuito integrado de aplicación específica (ASIC), así como varias porciones o combinaciones de dichos elementos. La memoria puede comprender una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM) o combinaciones de estos y otros tipos de dispositivos de memoria electrónica. Las realizaciones de la presente invención se pueden implementar como software, hardware (tal como, entre otros, un circuito lógico) o una combinación de los mismos.

Con referencia a la FIG. 2A, se muestra un número de componentes del dispositivo móvil 20. Como se ilustra, en esta realización, el dispositivo móvil 20 es un teléfono móvil típico que tiene funciones básicas. El dispositivo móvil 20 tiene una interfaz de entrada 60 para recibir información de un usuario, y se proporciona una pantalla 64 para presentar información visualmente al usuario. El dispositivo móvil 20 también incluye una memoria 68 para almacenar un sistema operativo que controla la funcionalidad principal del dispositivo móvil 20, junto con un número de aplicaciones que se ejecutan en el dispositivo móvil 20, y datos. Un procesador 72 ejecuta el sistema operativo y las aplicaciones. Una tarjeta SIM 76 proporciona memoria adicional para almacenar aplicaciones y datos, y tiene un microprocesador para ejecutarlos. Además, la tarjeta SIM 76 tiene un código de identificación de hardware único que permite la identificación del dispositivo 20 móvil. Cuando está instalada, la tarjeta SIM 76 forma parte del dispositivo móvil 20. Otros tipos de dispositivos móviles pueden tener una memoria de dispositivo cifrada en lugar de la tarjeta SIM 76, que ofrece la funcionalidad equivalente. Una interfaz de comunicaciones 80 permite las comunicaciones con una red celular para voz y datos.

Con referencia a la FIG. 2B, se muestra un número de componentes del dispositivo informático no móvil 21. Como se ilustra, en esta realización, el dispositivo no móvil 21 es un ordenador de escritorio o torre típico que tiene funciones básicas. El dispositivo no móvil 21 tiene una interfaz de entrada de usuario 251 para recibir la entrada de un usuario (por ejemplo, un teclado, pantalla táctil y/o micrófono), y se proporciona una interfaz de salida de usuario 253 para presentar información de manera visual o auditiva al usuario. El dispositivo no móvil 21 también incluye una memoria 255 para almacenar un sistema operativo que controla la funcionalidad principal del dispositivo no móvil 21, junto con un número de aplicaciones que se ejecutan en el dispositivo no móvil 21, y datos. Un procesador 257 ejecuta el sistema operativo y las aplicaciones. El dispositivo 21 no móvil puede tener un código de identificación de hardware único que permite la identificación del dispositivo 21 no móvil (por ejemplo, una dirección de control de acceso al medio (MAC)). Al menos una porción de la memoria 255 puede estar cifrada. Una interfaz de comunicaciones 259 permite las comunicaciones con una LAN o Internet 28, por ejemplo, mediante una interfaz Ethernet o Wi-Fi.

La FIG. 3 ilustra, a un nivel alto de abstracción, una realización 300 de un sistema y un procedimiento según la presente descripción. La realización 300 puede ser útil al gestionar pares de claves públicas/privadas y certificados digitales que incluyen claves públicas, con el fin de proporcionar una arquitectura de soporte de PKI y un procedimiento para su uso. La realización 300 incluye una interfaz de máquina para el usuario final 301. La interfaz de la máquina puede incluir un ordenador (o terminal) convencional de ubicación fija 303 y/o un dispositivo móvil 305. Los dispositivos móviles 20 y/o los dispositivos informáticos no móviles 21 ilustrados en la FIG. 1 se pueden usar como terminal 303 y/o dispositivo móvil 305. El dispositivo móvil 305, si está presente, puede incluir una aplicación móvil 307 tal como una aplicación de contenedor móvil segura. La aplicación de contenedor móvil segura, si está presente, puede incluir, además, o estar en contacto comunicativo con uno o más almacenamientos de datos seguros con el fin de proporcionar la confidencialidad y la integridad de la información confidencial almacenada en la misma, y proporcionar la protección de las credenciales del usuario final usadas por la realización 300.

La realización 300 puede operar en un modo de cliente/servidor, en el que el terminal fijo 303 y/o el dispositivo móvil 305 se pueden usar como cliente de PKI, con el fin de interactuar con el servidor de servicios de seguridad 311. El servidor de servicios de seguridad 311 puede incluir una o más aplicaciones del lado del servidor, como la aplicación de registro de clientes 313, la aplicación de servidor de credenciales/ la plataforma de desarrollo segura (SDP) 317 (también denominada servidor de credenciales 317 o SDP 317) y/o una aplicación de PKI/CA de un tercero confiable 315. Una o más de las aplicaciones del lado del servidor pueden estar en contacto comunicativo con el servicio de autenticación primario 321, que puede estar ubicado como parte del servidor de servicios de seguridad 311 o ser externo al servidor de servicios de seguridad 311. El servidor de validación de certificados 36 (véase la FIG. 1) se puede usar como servidor de servicios de seguridad 311.

Las aplicaciones del lado del servidor pueden interactuar con una plataforma de desarrollo segura/un servidor de credenciales (SDP) 317, que está adaptada(o) para ejecutar uno o más servicios a nivel de servidor tales como ser un gestor de publicación, un módulo de autenticación, un módulo de aprovisionamiento, un módulo gestor de servicios de mensajería segura (SMS) y así sucesivamente. La SDP 317 puede proporcionar una plataforma de desarrollo segura (es decir, protegida de intrusiones no autorizadas) para el desarrollo de aplicaciones de mHealth. La SDP 317 puede proporcionar además una plataforma de uso segura de modo que los usuarios finales de las aplicaciones de mHealth puedan usar dichas aplicaciones de manera segura y sin necesidad de gestionar información de PKI, certificados digitales y similares. La información confidencial, como contraseñas, contraseñas de un solo uso, certificados, información de capa de sockets seguros (SSL), y/o la información de seguridad de nivel de transmisión (TLS) puede almacenarse en una memoria segura accesible para la SDP 317. La plataforma de desarrollo segura 317 puede incluir además o estar en contacto comunicativo con uno o más almacenamientos de datos seguros para proporcionar la confidencialidad y la integridad de la información confidencial almacenada en la misma, y proporcionar la protección de las credenciales usadas por el servidor de servicios de seguridad 311. La plataforma de desarrollo segura/el servidor de credenciales 317 puede operar como un filtro o controlador de acceso a datos al respecto de la información confidencial. Puede proporcionarse una interfaz de gestor 319 a fin de permitir que un gestor configure y, de otro modo, gestione la SDP 317.

En el funcionamiento de la realización 300, el usuario final 301 puede comenzar intentando iniciar sesión al principio en el sistema, mediante el uso de una de las interfaces de la máquina, como un ordenador (o terminal) de ubicación fija convencional 303 y un enlace seguro. El terminal 303 y el servidor de servicios de seguridad 311 pueden intercambiar credenciales, como información de registro, códigos de cuenta, contraseñas (incluida la OTP) e información de seguridad que soporte SSL/TLS, y así sucesivamente.

A continuación, la aplicación de registro de cliente 313 puede recibir solicitudes de registro desde el terminal 303. La aplicación de registro de cliente 313 puede, a continuación, interactuar con otras aplicaciones del lado del servidor y/o servicios a nivel de servidor que se ejecutan en una plataforma de desarrollo segura/un servidor de credenciales 317 para gestionar las solicitudes de registro de usuario, devolver códigos de activación de usuario específicos y solicitar la autenticación primaria para cada usuario con el fin de confirmar su identidad. La aplicación de registro de cliente 313 puede usar esta información para registrar usuarios válidos en la plataforma de desarrollo segura 317.

A continuación, en algún momento posterior, el usuario final 301 puede intentar acceder a información confidencial a través de la aplicación móvil 307, como una aplicación de contenedor móvil segura. La aplicación móvil puede transmitir al servidor de servicios de seguridad 311 una solicitud de que se genere un certificado digital, una solicitud de firma digital o la validación de una firma digital, una solicitud de autenticación o mensajes similares. El servidor de servicios de seguridad 311 puede responder con suficiente información de seguridad y/o autorizaciones para que la aplicación de contenedor móvil segura procese solicitudes del usuario final 301. La información del servidor de servicios de seguridad 311 puede incluir contraseñas de un solo uso, una sesión autenticada segura, información SSL,

información TLS y así sucesivamente.

La FIG. 4 ilustra con un alto nivel de abstracción una realización 400 de un sistema y un procedimiento según la presente descripción, de manera similar, aunque con un nivel diferente de abstracción, a la realización 300 de la FIG. 3. La realización 400 puede ser útil al gestionar pares de claves públicas/privadas y certificados digitales que incluyen claves públicas. Los elementos con numeración similar también se pueden ilustrar en la FIG. 3. La realización 400 incluye un dispositivo de usuario 303 en contacto comunicativo con el servicio de PKI 415. El servicio de PKI 415 actúa como un registrador para generar y validar certificados digitales. El servicio de PKI 415 puede incluir la funcionalidad de una o más aplicaciones del lado del servidor, como la aplicación de registro de cliente 313 y/o una aplicación de PKI/CA de un tercero de confianza 315. En algunas realizaciones, el servicio de PKI 415 puede estar integrado lógicamente con la plataforma de desarrollo segura 317, mientras que, en otras realizaciones, el servicio de PKI 415 puede estar físicamente alejado pero en contacto comunicativo con la plataforma de desarrollo segura 317. El contacto comunicativo puede ser a través de una red (no ilustrada en la FIG. 4) como Internet 28 (véase la FIG. 1) o una LAN. La realización 400 puede incluir además otro dispositivo de usuario 305 (que puede ser o no el mismo que el dispositivo de usuario 303). El dispositivo de usuario 305 puede estar en contacto comunicativo con la plataforma de desarrollo segura 317 y el almacenamiento de datos de seguridad 407. La plataforma de desarrollo segura 317 puede estar en contacto comunicativo con el almacenamiento de claves 447. El almacenamiento de claves es una memoria protegida que se usa para almacenar información confidencial. El almacenamiento de claves puede usar técnicas conocidas en la técnica para almacenar información confidencial, como el cifrado de datos almacenados, el uso del control de acceso, como un cortafuegos y así sucesivamente. El almacenamiento de claves 447 puede estar físicamente separado de la plataforma de desarrollo segura 317, pero en contacto comunicativo con la misma. De manera alternativa, al menos una porción del almacenamiento de claves 447 puede implementarse como al menos una porción de una memoria dentro de la plataforma de desarrollo segura 317.

El almacenamiento de claves 447 proporciona una memoria que es accesible para la plataforma de desarrollo segura 317 pero no es directamente accesible para el dispositivo de usuario 305 y el servicio de PKI 415. Por ejemplo, al no ser directamente accesible para el dispositivo de usuario 305 y el servicio de PKI 415, el almacenamiento de claves 447 no es parte del dispositivo de usuario 305 y el servicio de PKI 415, no es gestionado por el dispositivo de usuario 305 y el servicio de PKI 415, y no se accede al mismo mediante un procedimiento que se ejecuta en el dispositivo de usuario 305 y el servicio de PKI 415. Sin embargo, si el dispositivo de usuario 305 necesita usar información almacenada en el almacenamiento de claves 447, los procedimientos que se ejecutan en otro dispositivo, como la plataforma de desarrollo segura 317, pueden acceder al almacenamiento de claves 447 para realizar la solicitud del dispositivo de usuario 305 y comunicar los resultados al dispositivo de usuario 305.

Un procedimiento según la realización 400 para crear un certificado digital puede incluir primero que el dispositivo de usuario 303 transmita el mensaje 451 al servicio de PKI 415. El mensaje 451 puede incluir información de registro relevante para el usuario del dispositivo de usuario 303 y/o el dispositivo de usuario 305. La información de registro del mensaje 451 se puede usar para configurar inicialmente el servicio de PKI 415 para poder gestionar la PKI y la información del certificado para el dispositivo de usuario 303 y/o el dispositivo de usuario 305.

A continuación, el servicio de PKI 415 puede devolver un mensaje 452 al dispositivo del usuario 303 y/o al dispositivo de usuario 305 que incluye un mensaje de código de activación, que confirma al dispositivo de usuario 303 y/o al dispositivo de usuario 305 que la SDP 317 está habilitada para gestionar pares de claves de PKI y certificados para el dispositivo de usuario 303 y/o el dispositivo de usuario 305. Para facilitar la referencia, el dispositivo de usuario 303 y/o el dispositivo de usuario 305 en lo sucesivo se denominará colectivamente como dispositivo de usuario 305, a menos que se pretenda claramente una distinción entre el dispositivo de usuario 303 y el dispositivo de usuario 305.

A continuación, el dispositivo de usuario 305 y la plataforma de desarrollo segura 317 pueden participar en un intercambio de mensajes 453 que incluye una solicitud del dispositivo de usuario 305 para un token de aprovisionamiento. En respuesta, el token de aprovisionamiento es generado por la plataforma de desarrollo segura 317 y enviado de vuelta al dispositivo de usuario 305. El token de aprovisionamiento y las credenciales son recibidos por el dispositivo de usuario 305 y, a su vez, son enviados a través del mensaje 454 al almacenamiento seguro de datos de claves 407 para su almacenamiento. El almacenamiento seguro de datos de claves 407 puede incluir una memoria protegida y puede implementarse como una porción de la memoria dentro del dispositivo de usuario 305.

A continuación, en algún momento posterior, el dispositivo de usuario 305 envía el mensaje 455 a la plataforma de desarrollo segura 317 para crear un certificado digital y el par de claves de PKI correspondiente (el par de claves públicas/privadas). La plataforma de desarrollo segura 317 creará el par de claves públicas/privadas y, a su vez, generará el mensaje 457 para solicitar una generación de un certificado digital. El mensaje 457 se envía al servicio de PKI 415. Aproximadamente al mismo tiempo, la plataforma de desarrollo segura 317 puede generar el mensaje 456 y

enviar el mensaje 456 al almacenamiento de claves 447 para almacenar la clave privada del par de claves de PKI para el dispositivo de usuario 305.

Después de que el servicio de PKI 415 recibe el mensaje 457 de la plataforma de desarrollo segura 317, el servicio de PKI 415 puede crear el certificado digital usando la información dentro del mensaje 457. Si la información es válida, a continuación, el servicio de PKI 415 generará un certificado digital con la clave pública en el mensaje 457. El certificado digital es enviado por el servicio de PKI 415 a la plataforma de desarrollo segura 317 mediante el uso del mensaje 458. A continuación, el certificado recibido se envía mediante el uso del mensaje 459 al almacenamiento de claves 447 con el fin de que sea almacenado de manera segura para su uso futuro por la plataforma de desarrollo segura 317.

Tras la conclusión del intercambio de mensajes de la realización 400 descrita anteriormente, el certificado digital y la clave privada en poder de la SDP 317 están listos para ser usados por el dispositivo de usuario 305. Por ejemplo, una aplicación móvil relacionada con la salud que se ejecuta en el dispositivo de usuario 305 ahora puede acceder, firmar y/o validar información confidencial mediante el uso de la clave privada y el certificado digital.

La FIG. 5 ilustra, a un nivel alto de abstracción, una realización 500 de un sistema y un procedimiento según la presente descripción. La realización 500 puede ser útil en una arquitectura de soporte de PKI segura, a fin de firmar un documento de manera segura mediante el uso de certificados digitales de clave privada. Los elementos de numeración similar también se pueden ilustrar en las FIG. 3-4.

La realización 500 incluye un dispositivo de usuario 305 que está acoplado de manera comunicativa a una plataforma de desarrollo segura 317. A su vez, la plataforma de desarrollo segura 317 se acopla de manera comunicativa a un servicio PKI 415 y a un almacenamiento de claves 447. Como en el caso de la reivindicación 400, el almacenamiento de claves 447 puede estar físicamente separado de la plataforma de desarrollo segura 317, pero en contacto comunicativo. De manera alternativa, al menos una porción del almacenamiento de claves 447 puede implementarse como al menos una porción de una memoria dentro de la plataforma de desarrollo segura 317.

Un procedimiento según la realización 500 puede incluir primero el dispositivo de usuario 305 que transmite el mensaje 501 a la plataforma de desarrollo segura 317. El mensaje 501 puede incluir un documento a ser firmado digitalmente, junto con una solicitud para que se firme.

A continuación, la plataforma de desarrollo segura 317 puede enviar el mensaje 502 al servicio de PKI 415. El mensaje 502 incluye una solicitud para validar un certificado digital perteneciente al dispositivo de usuario 305 y/o el usuario del dispositivo de usuario 305, y puede incluir el certificado digital que se busca validar.

A continuación, después de que el servicio de PKI 415 haya podido determinar si el certificado digital es válido o no, el servicio de PKI 415 puede enviar un mensaje 503 a la plataforma de desarrollo segura 317 con una indicación de si el certificado digital es válido o no.

A continuación, si se determina que el certificado digital es válido, a continuación, la plataforma de desarrollo segura 317 puede enviar el mensaje 504 al dispositivo de usuario 305 para proporcionar un documento firmado al dispositivo de usuario 305, siendo el documento firmado digitalmente por una clave privada de certificado digital asociada con el dispositivo de usuario 305 o el usuario del dispositivo de usuario 305 en el almacenamiento de claves seguro 447. En cualquier momento durante la práctica de la realización ilustrada en la FIG. 5, la plataforma de desarrollo segura 317 puede interactuar con el almacenamiento de claves 447 para leer/escribir datos necesarios para la plataforma de desarrollo segura 317 a fin de firmar digitalmente el documento.

La FIG. 6 ilustra, a un nivel alto de abstracción, una realización 600 de un sistema y un procedimiento según la presente descripción. La realización 600 puede ser útil en una arquitectura de soporte de PKI segura, a fin de validar una firma de documento mediante el uso de la clave pública distribuida en el certificado digital. Los elementos de numeración similar también se pueden ilustrar en las FIG. 3-5.

La realización 600 incluye un dispositivo de usuario 305 que está acoplado de manera comunicativa a una plataforma de desarrollo segura 317. A su vez, la plataforma de desarrollo segura 317 se acopla de manera comunicativa a un servicio de PKI 415 y a un almacenamiento de claves 447. Como en el caso de la reivindicación 400, el almacenamiento de claves 447 puede estar físicamente separado de la plataforma de desarrollo segura 317, pero en contacto comunicativo. De manera alternativa, al menos una porción del almacenamiento de claves 447 puede implementarse como al menos una porción de una memoria dentro de la plataforma de desarrollo segura 317.

Un procedimiento según la realización 600 puede incluir primero el dispositivo de usuario 305 que transmite el mensaje 601 a la plataforma de desarrollo segura 317. El mensaje 601 puede incluir una solicitud para validar un documento. En algunas realizaciones, el mensaje 601 puede incluir el propio documento. En otras realizaciones, el mensaje 601 puede incluir una característica del documento que se busca validar, siendo la característica suficiente para determinar, junto con la seguridad y/o la información de certificado mantenida por la realización 600, sea o no válido el documento.

A continuación, la plataforma de desarrollo segura 317 puede enviar el mensaje 602 al servicio de PKI 415. El mensaje 602 incluye una solicitud para validar el certificado digital y la cadena de certificados.

A continuación, después de que el servicio de PKI 415 haya podido determinar si el certificado digital es válido o no, el servicio de PKI 415 puede enviar un mensaje 603 a la plataforma de desarrollo segura 317 con una indicación de si el certificado digital es válido o no. La plataforma de desarrollo segura 317 usa esta información junto con la clave pública del certificado digital y cualquier otra información que pueda ser necesaria para validar el documento recibido del dispositivo de usuario 305.

A continuación, la plataforma de desarrollo segura 317 puede enviar el mensaje 604 al dispositivo de usuario 305 para proporcionar un resultado de validación al dispositivo de usuario 305. Si el documento es válido, a continuación, el dispositivo de usuario 305 y el usuario del mismo pueden acceder al documento y controlarlo. Si el documento no es válido, a continuación, el dispositivo de usuario 305 y el usuario del mismo no podrán acceder al documento y controlarlo.

En cualquier momento durante la práctica de la realización ilustrada en la FIG. 6, la plataforma de desarrollo segura 317 puede interactuar con el almacenamiento de claves 447 para leer/escribir datos necesarios para la plataforma de desarrollo segura 317.

Las realizaciones de la presente invención incluyen un sistema que tiene un o más conjuntos de procesamiento acoplados a una o más memorias. Es posible configurar una o más memorias para almacenar software que, cuando es ejecutado por uno o más conjuntos de procesamiento, permite la práctica de las realizaciones que se describen en esta invención, al menos por medio del uso de los procedimientos descritos en esta invención, incluso, al menos, en las FIG. 3-4 y en textos relacionados.

Los procedimientos descritos pueden implementarse fácilmente en programas, tal como a través del uso de entornos de desarrollo de programas orientados al objeto u objetos que proporcionan un código de fuente portátil que puede ser usado en una variedad de plataformas de estaciones de trabajo u ordenadores. De manera alternativa, el sistema descrito puede ser implementado parcial o completamente en el hardware, tal como a través del uso de circuitos lógicos estándares o el diseño VLSI. Si bien se puede usar software o hardware para implementar los sistemas según diversas realizaciones de la presente invención, esto puede depender de distintas consideraciones, tales como los requisitos de velocidad o eficiencia del sistema, la función particular y los sistemas de software y hardware particulares que se estén utilizando.

Si bien lo anterior se refiere a realizaciones de la presente invención, pueden concebirse otras realizaciones adicionales de la presente invención sin alejarse del alcance básico de la misma. Se entiende que varias realizaciones descritas en esta invención pueden utilizarse en combinación con cualquier otra realización descrita, sin apartarse del alcance aquí contenido. Además, la descripción anterior no pretende ser taxativa o limitar la invención a la forma exacta descrita. Las modificaciones y variaciones son posibles en virtud de los conocimientos anteriores o pueden adquirirse a partir de la práctica de la invención. Pueden identificarse determinados ejemplos de realizaciones usando una lista abierta que incluye una redacción que indica que los elementos de la lista son representativos de las realizaciones y que la lista no pretende representar una lista cerrada que excluya realizaciones adicionales. Esta redacción puede incluir "por ejemplo", "etc.", "tal como", "y así sucesivamente", "y similares", etc., y otras redacciones que serán evidentes a partir del contexto que las rodea.

Ningún elemento, acto o instrucción usado en la descripción de la presente solicitud debería interpretarse como fundamental o esencial para la invención, a menos que se describa explícitamente como tal. También, como se usa en esta invención, el artículo "un(una)" pretende incluir uno o más elementos. Cuando se pretende que sea únicamente un elemento, se usa el término "uno(una)" o un lenguaje similar. Además, los términos "cualquiera de" seguido por un listado de una pluralidad de elementos y/o una pluralidad de categorías de elementos, como se usa en esta invención, pretenden incluir "cualquiera de", "cualquier combinación de", "cualquier múltiplo de" y/o "cualquier combinación de múltiplos de" los elementos y/o las categorías de elementos, de manera individual o en conjunto con otros elementos y/u otras categorías de elementos.

Por otra parte, las reivindicaciones no deberían considerarse como limitadas al orden o elementos descritos a menos que se especifique a esos efectos.

REIVINDICACIONES

1. Un procedimiento para firmar digitalmente un documento, que comprende:

recibir, mediante una plataforma de desarrollo segura, SDP, desde un dispositivo de usuario (305), una solicitud de un certificado digital y el par de claves públicas-privadas correspondientes;
crear, mediante la SDP (317), el par de claves públicas-privadas y generar una solicitud del certificado digital, comprendiendo la SDP (317) un procesador SDP acoplado a una memoria SDP segura (447);
transmitir, mediante la SDP, la clave privada del par de claves públicas-privadas a la memoria SDP segura (447);
transmitir, mediante la SDP, al procesador de servicios (415) de una infraestructura de clave pública, PKI, la solicitud del certificado digital;
si la información en la solicitud del certificado digital es correcta: crear, mediante el procesador de servicios de PKI, el certificado digital con la clave pública del par de claves públicas-privadas en la solicitud; y recibir, mediante la SDP, el certificado digital del procesador de servicios de PKI (415);
almacenar el certificado digital en la memoria SDP segura (447);
recibir, mediante la SDP desde el dispositivo de usuario (305), un documento para firmar digitalmente;
transmitir, al procesador de servicios de PKI (415), una solicitud para validar el certificado digital, almacenado en la memoria SDP segura, relacionada con el dispositivo de usuario (305);
recibir, desde el procesador de servicios de PKI (415), una indicación de validez del certificado digital; y
si la indicación indica un certificado digital válido:

firmar digitalmente mediante la SDP el documento basándose en la clave privada del certificado digital creado por la SDP (317); y
proporcionar mediante la SDP el documento firmado al dispositivo de usuario (305).

2. El procedimiento de la reivindicación 1, donde la validación comprende el uso de una clave simétrica usada para la transferencia de datos que se cambia por sesión.

3. El procedimiento de la reivindicación 1, donde la SDP (317) está configurada para gestionar las credenciales y los servicios de PKI para un usuario final (301).

4. El procedimiento de la reivindicación 1, donde la SDP (317) está configurada para usar una clave simétrica que se deriva de más de una fuente.

5. El procedimiento de la reivindicación 1, donde la SDP (317) está configurada para proporcionar un canal cifrado y autenticado bilateralmente.

6. Un sistema (300; 400) para la firma digital de un documento, que comprende:

una plataforma de desarrollo segura, SDP, (317), comprendiendo la SDP (317) un procesador SDP, acoplado una memoria SDP segura, un receptor, una interfaz de comunicación y un transmisor;
la interfaz de comunicación está configurada para recibir, desde un dispositivo de usuario (305), una solicitud de un certificado digital y el correspondiente par de claves públicas-privadas;
el procesador SDP está configurado para crear el par de claves públicas privadas y generar una solicitud para el certificado digital;
el transmisor está configurado para transmitir la clave privada del par de claves públicas privadas a la memoria SDP segura y para transmitir, al procesador de servicios (415) de una infraestructura de clave pública, PKI, la solicitud del certificado digital;
el receptor está configurado para recibir el certificado digital del procesador de servicios de PKI (415) si la información en la solicitud del certificado digital es correcta, donde el certificado digital es creado, por el procesador de servicios de PKI, con la clave pública del par de claves públicas-privadas;
el procesador SDP está configurado además para almacenar el certificado digital en la memoria SDP segura acoplada al procesador SDP;
la interfaz de comunicación está configurada además para recibir desde el dispositivo de usuario, un documento a firmar digitalmente;
el transmisor está configurado además para transmitir al procesador de servicios de PKI (415) el certificado digital a validar, almacenado en la memoria SDP segura; y
el receptor está configurado además para recibir, desde el procesador de servicios de PKI (415), una indicación de validez del certificado digital, donde el procesador SDP firma digitalmente el documento basándose en la

indicación de validez y la clave privada del certificado digital creada por el procesador SDP;
el transmisor se configura además para proporcionar el documento firmado al dispositivo de usuario (305).

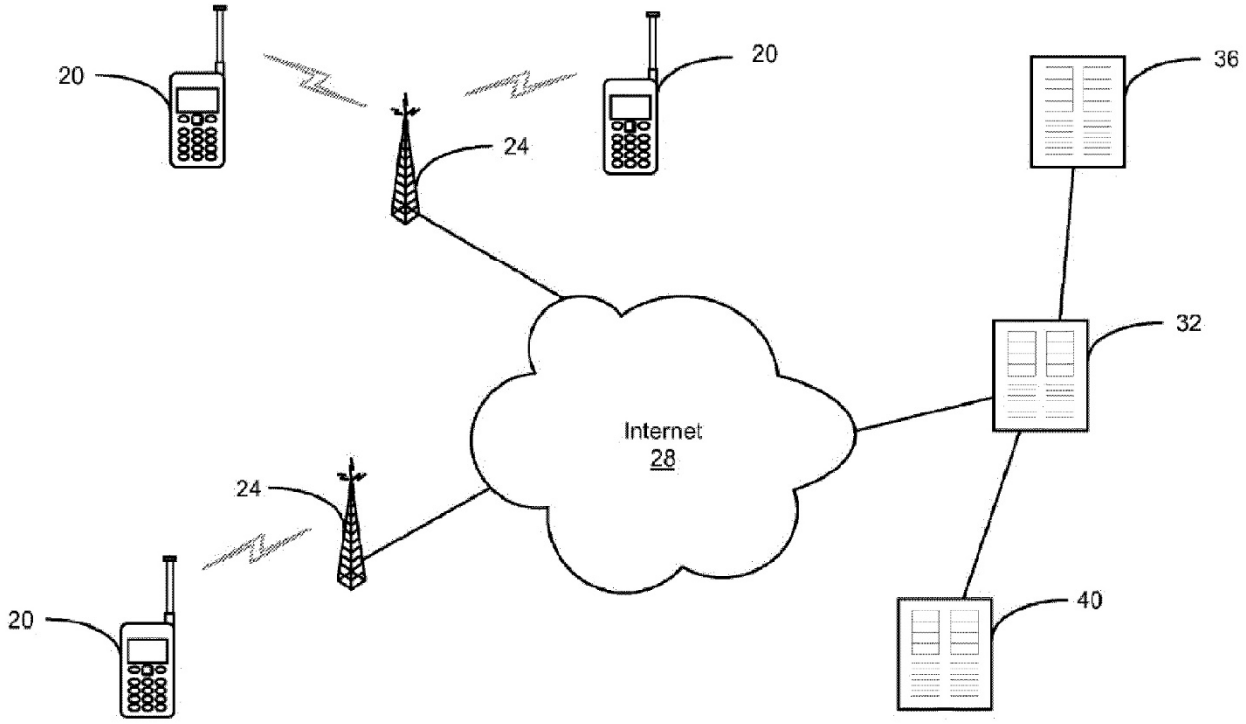
7. El sistema (300; 400) de la reivindicación 6, donde la validación comprende el uso de una clave simétrica usada para la transferencia de datos que se cambia por sesión.

8. El sistema (300; 400) de la reivindicación 6, donde la SDP (317) está configurada para gestionar las credenciales y los servicios de PKI para un usuario final.

9. El sistema (300; 400) de la reivindicación 6, donde la validación comprende el uso de un procedimiento de autenticación dual.

FIG. 1

100



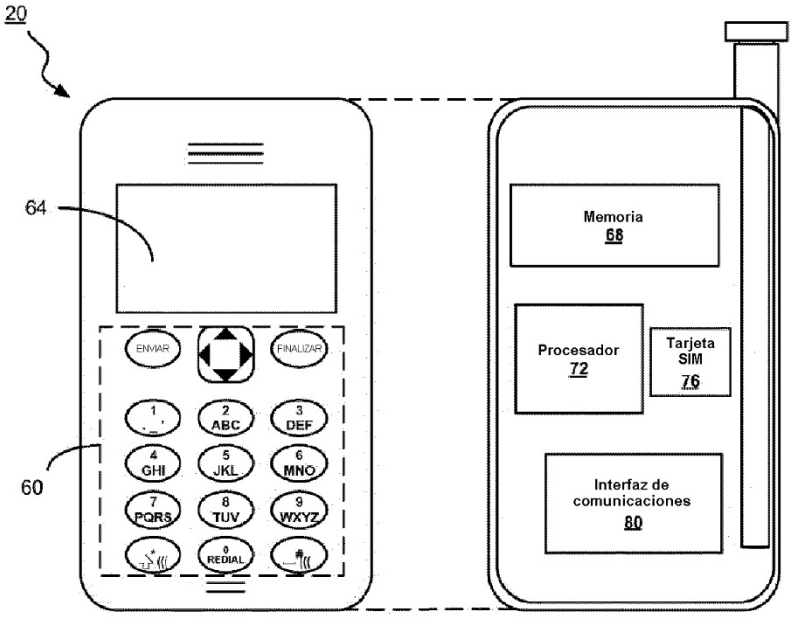


FIG. 2A

200

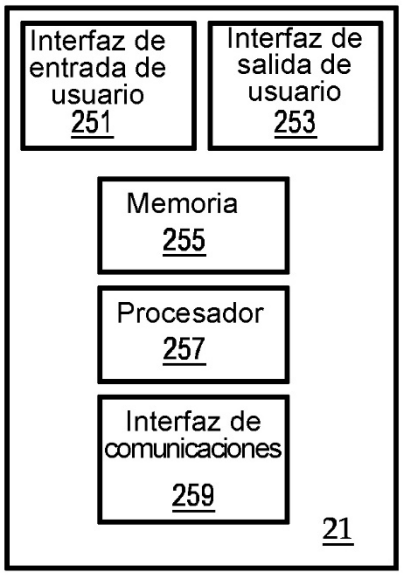


FIG. 2B

250

FIG. 3

300

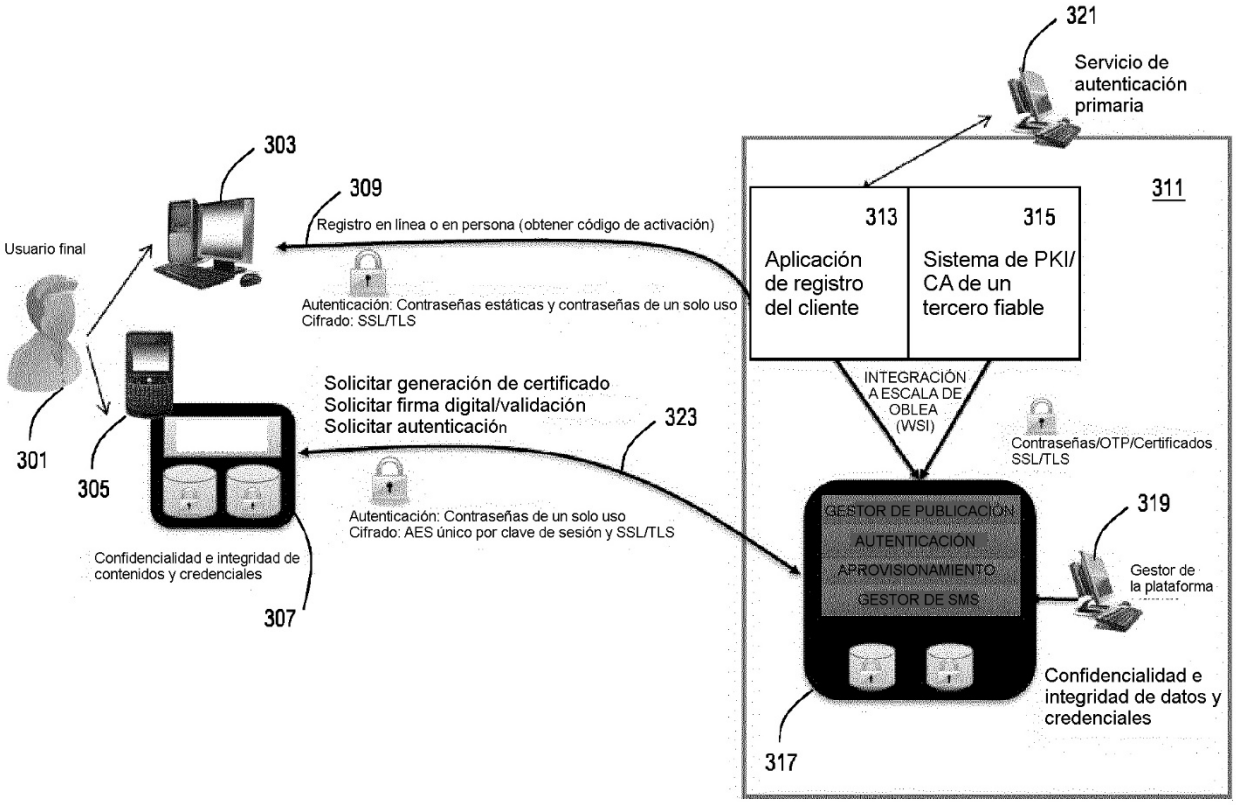

321
Servicio de autenticación primaria
303
309
Registro en línea o en persona (obtener código de activación)
Usuario final
Autenticación: Contraseñas estáticas y contraseñas de un solo uso
Cifrado: SSL/TLS
311
313
Aplicación de registro del cliente
315
Sistema de PKI/ CA de un tercero fiable
INTEGRACIÓN A ESCALA DE OBLEA (WSI)
Contraseñas/OTP/Certificados SSL/TLS
Solicitar generación de certificado
Solicitar firma digital/validación
Solicitar autenticación
323
301
305
Autenticación: Contraseñas de un solo uso
Cifrado: AES único por clave de sesión y SSL/TLS
GESTOR DE PUBLICACIÓN
AUTENTICACIÓN
APROVISIONAMIENTO
GESTOR DE SMS
319
Gestor de la plataforma
Confidencialidad e integridad de contenidos y credenciales
307
Confidencialidad e integridad de datos y credenciales
317

FIG. 4

400

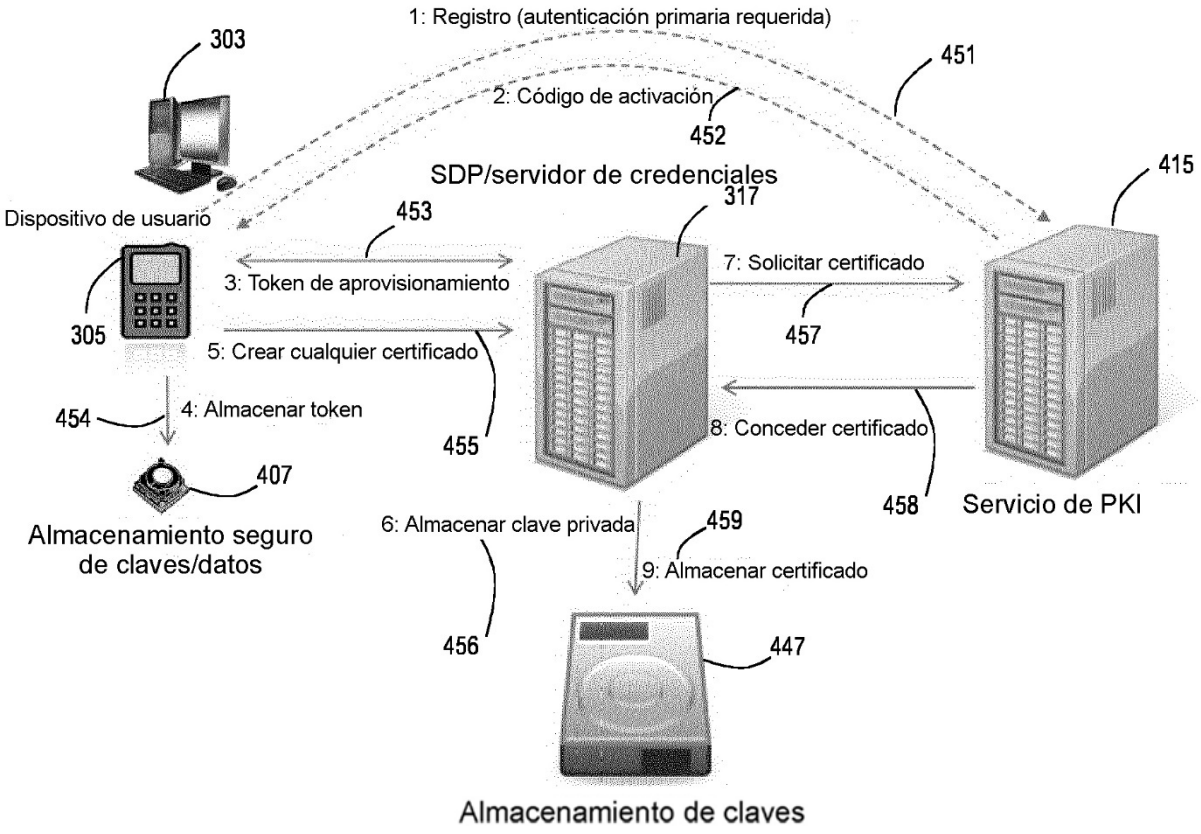

1: Registro (autenticación primaria requerida)
303
451
2: Código de activación
452
SDP/servidor de credenciales
415
317
Dispositivo de usuario
453
3: Token de aprovisionamiento
7: Solicitar certificado
305
457
5: Crear cualquier certificado
454
4: Almacenar token
455
8: Conceder certificado
458
Servicio de PKI
407
Almacenamiento seguro de claves/datos
6: Almacenar clave privada
459
9: Almacenar certificado
456
447
Almacenamiento de claves

FIG. 5

500

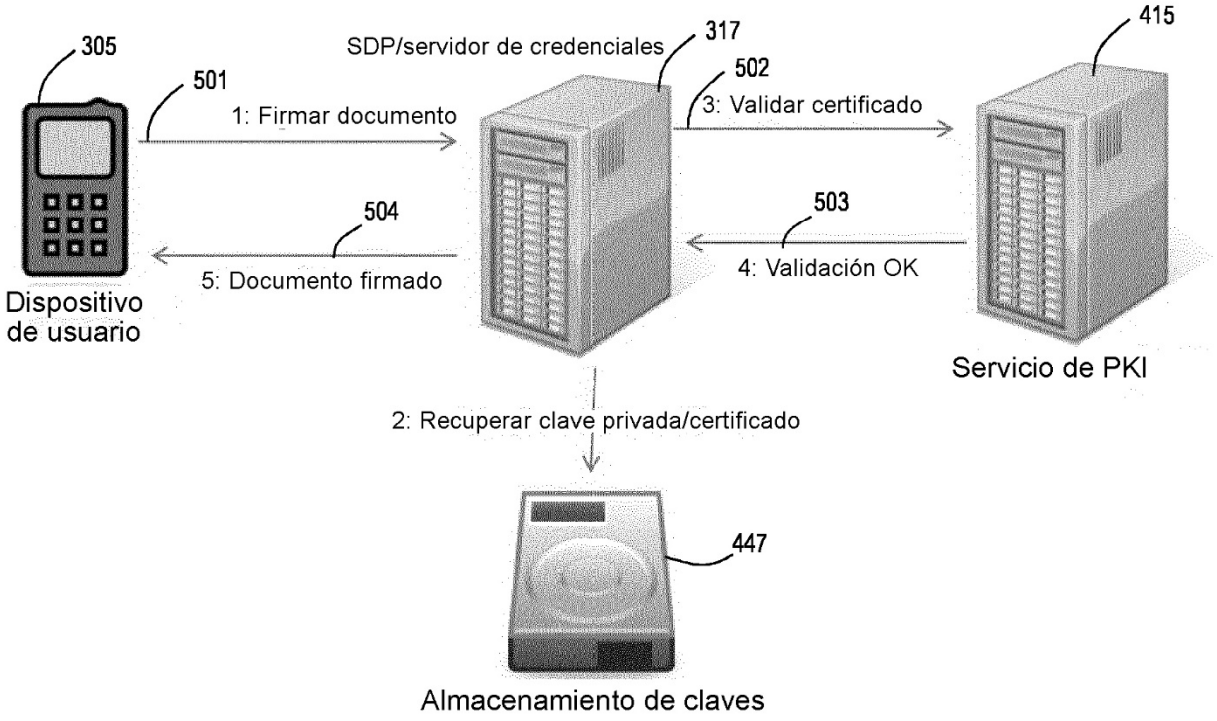

305
501
1: Firmar documento
SDP/servidor de credenciales
317
502
3: Validar certificado
415
504
5: Documento firmado
503
4: Validación OK
Dispositivo de usuario
Servicio de PKI
2: Recuperar clave privada/certificado
447
Almacenamiento de claves

FIG. 6

600


305
601
1: Validar documento
SDP/servidor de credenciales
317
602
2: Validar cadena de certificados
415
604
4: Resultado de la validación
603
3: Validación OK
Dispositivo de usuario
Servicio de PKI
447
Almacenamiento de claves