(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 705**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **12.07.2017 PCT/EP2017/067553**

(87) Fecha y número de publicación internacional: **18.01.2018 WO18011267**

(96) Fecha de presentación y número de la solicitud europea: **12.07.2017 E 17742978 (4)**

(97) Fecha y número de publicación de la concesión europea: **20.11.2019 EP 3485600**

(54) Título: **Método para proporcionar firmas digitales seguras**

(30) Prioridad:

13.07.2016 LU 93150

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.07.2020

(73) Titular/es:

LUXTRUST S.A. (100.0%)
IVY Building 13-15 Parc d'activité
8308 Capellen, LU

(72) Inventor/es:

KOPP, THOMAS

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método para proporcionar firmas digitales seguras

Campo técnico

[0001] La invención pertenece al campo de las comunicaciones de datos seguras, y en particular a un procedimiento de inscripción de un nuevo usuario en una infraestructura de clave pública, PKI.

Antecedentes de la invención

[0002] El documento de patente publicado con el número US 2014/0316873 A se ocupa del envío de un premio a un usuario de una cuenta de crédito en función de las actividades de compra del usuario. La tarjeta inteligente comprende un teclado para que el usuario introduzca un PIN, o un sensor biométrico para recibir la huella digital del usuario. En ambos casos, una vez que el usuario se ha identificado con la tarjeta inteligente, el procesador de esta última puede activar una parte de la banda magnética de la tarjeta para permitir que un lector de tarjetas magnéticas lea el número de cuenta de la banda magnética (véase [0035]). La enseñanza de este documento corresponde únicamente al paso (d) de la reivindicación 1.

[0003] En el campo de las comunicaciones de datos, como las comunicaciones que tienen lugar a través de canales digitales, el concepto criptográfico de Infraestructuras de clave pública, PKI, es un concepto ampliamente conocido. Una PKI es una configuración que vincula claves públicas con los sujetos respectivos por medio de una Autoridad de Certificación (CA). Dentro del dominio de una CA, cada Sujeto, que es una persona física o jurídica, o un sitio web u otro tipo de activo, debe ser único y estar vinculado/asociado a una clave pública de manera inequívoca. Este vínculo generalmente está representado por un Certificado emitido por la CA y que contiene la clave pública y un nombre distintivo del Sujeto vinculado. Un Suscriptor, que es una persona física que actúa en su propio nombre o una persona jurídica que ha nombrado a una persona física como representante autorizado, solicita un Certificado que vincula un Sujeto determinado a una clave pública. En el caso más típico, el Suscriptor es idéntico al Sujeto (cuando solicita un Certificado que identifica al Suscriptor), pero el Suscriptor también puede ser el propietario del Sujeto (cuando solicita un Certificado para su dispositivo conectado, sitio web u otro activo propio).

[0004] El propósito de una PKI es facilitar la transferencia electrónica segura de información para una variedad de actividades en la red, como el comercio electrónico, la banca por Internet y el correo electrónico confidencial, así como la autenticación fiable ante los servicios en línea. Esto se requiere para actividades para las que las contraseñas simples son un método de autenticación inadecuado y se requieren pruebas más rigurosas para confirmar la identidad de las partes involucradas en la comunicación y validar la información que se transfiere.

[0005] Una vez que se ha establecido un vínculo único entre un Sujeto y una clave pública, la clave privada correspondiente que está vinculada criptográficamente a la clave pública se puede usar para firmar datos de manera digital.

[0006] En cualquier caso, el Suscriptor es responsable de autorizar el uso de la clave privada, mientras que el Sujeto es la entidad vinculada a la clave pública y la clave privada correspondiente y, por lo tanto, autenticada por la clave privada.

[0007] En el contexto de una sesión de comunicación entre un usuario, que en ese caso es el Sujeto y, por ejemplo, una institución bancaria, el dato que se firma criptográficamente por medios electrónicos puede ser un identificador de sesión generado aleatoriamente. Al firmar el identificador de sesión, la sesión de comunicación se vincula o se asocia de forma exclusiva con la identidad del usuario. Alternativamente, el usuario puede firmar criptográficamente los datos comprendidos en un documento a través de medios electrónicos, lo que corresponde a su firma escrita en un documento presentado en papel, en particular si la firma creada electrónicamente cumple los requisitos de una firma cualificada en virtud del Reglamento (UE) nº 910/2014.

[0008] Se puede distribuir una clave privada al Suscriptor en forma de una tarjeta inteligente que tiene un microchip en el que se almacena la clave privada. En tal caso, el Suscriptor puede conectar la tarjeta inteligente a un dispositivo informático conectado a un dispositivo de lectura de tarjeta inteligente apropiado, con el fin de habilitar la tarjeta inteligente y el software auxiliar del dispositivo informático para firmar datos digitalmente.

[0009] Alternativamente, una clave privada puede almacenarse de forma remota en un servidor protegido al que se puede acceder a través de un canal seguro de comunicación de datos. En tal caso, la Autoridad de Certificación suele proporcionar al Suscriptor un *token* de seguridad que implementa un algoritmo de contraseña de un solo uso, OTP. El algoritmo generalmente usa información que vincula el *token* de seguridad de forma inequívoca al Sujeto y a la clave privada almacenada de forma remota. Al suministrar credenciales y una OTP correspondiente a la infraestructura remota donde reside el servidor protegido con la clave privada, el valor de OTP recibido se compara con el valor de OTP esperado además de la verificación de otras credenciales antes de proporcionar acceso al servidor que almacena la clave privada del Sujeto. Este servidor puede entonces dirigirse a la firma

digital de datos usando la clave privada almacenada. Dicha arquitectura proporciona el beneficio de una mayor movilidad. Por ejemplo, una vez que el usuario posee un *token* de seguridad que funciona, puede acceder a la clave privada desde un dispositivo informático arbitrario sin requerir una interfaz de hardware o un lector de tarjetas inteligentes. El uso seguro de una clave privada almacenada de forma remota también se puede habilitar mediante el uso de mecanismos distintos de OTP o mediante *token*s virtuales que se pueden implementar en software.

[0010] En los dos casos mencionados anteriormente, un dispositivo de Sujeto (usuario), a saber, una tarjeta inteligente que comprende la clave privada, o un *token* de seguridad que da acceso a la clave privada remota, se ha vinculado/asociado previamente con el Sujeto y ha sido puesto a disposición del suscriptor de forma segura por la PKI.

[0011] La seguridad de cualquiera de los métodos conocidos mencionados anteriormente se basa fundamentalmente en la identificación correcta del Sujeto y del Suscriptor y, cuando sea necesario, la identificación correcta de un representante de la persona física con autorización (y la autorización correspondiente) y la propiedad del Suscriptor del Sujeto cuando este último es diferente del Suscriptor y la vinculación correcta del Sujeto al par de claves criptográficas pública y privada y el aprovisionamiento seguro del dispositivo del Sujeto que da acceso a la clave privada. Esta vinculación se produce en el paso de inscripción en una PKI.

[0012] Teniendo en cuenta que las partes confiantes consideran que una PKI es fiable con respecto a los procesos citados anteriormente y los dispositivos de Sujeto empleados, las partes confiantes pueden autenticar a un Sujeto mediante la validación de una firma digital creada con la clave privada del Sujeto y el correspondiente certificado emitido por la PKI dada.

[0013] En los métodos de inscripción conocidos, la identificación anteriormente mencionada ocurre al comienzo del proceso. Para este fin, el Suscriptor o una persona física que actúa como representante autorizado proporciona atributos que lo/la caracterizan a él/ella y al Sujeto y, cuando sea necesario, a la organización en cuyo nombre actúa. Esos atributos pueden estar acompañados de elementos adicionales (por ejemplo, entrevista a través de la cámara web, carné de conducir, carné de identificación nacional, etc.) que sirven como prueba para validar los atributos proporcionados. La parte identificante, generalmente un agente autorizado y/o medios informáticos de la Autoridad de Registro, RA, de la PKI, valida los atributos indicados y suministra, cuando el resultado es positivo, un conjunto certificado de atributos a la Autoridad de Certificación, CA, para emitir un Certificado correspondiente al Sujeto.

[0014] En este paso, un par de claves criptográficas pública/privada, que se ha creado aleatoriamente en una tarjeta inteligente o en otro tipo de dispositivo o en un servidor protegido, se asocia con el Sujeto identificado. El resultado se manifiesta mediante la emisión de un Certificado que comprende la clave pública junto con un nombre distintivo de ese Sujeto. Como se ha descrito anteriormente en este documento, la clave privada correspondiente, que en consecuencia también está asociada con el Sujeto dado, se hace accesible de forma segura al Suscriptor mediante la distribución del dispositivo de Sujeto correspondiente (tarjeta inteligente, *token* de seguridad, ...) a través de un canal de comunicación seguro o a través de otro mecanismo de asignación segura para permitir el acceso a la clave privada.

[0015] Dado que los atributos utilizados para identificar al Sujeto y al Suscriptor y, cuando se requiera, a una persona física que actúa como representante autorizado, posiblemente se pueden suministrar durante el proceso de inscripción a través de distintos canales remotos, por ejemplo a través de Internet, es crucial asegurarse de que los atributos proporcionados provengan del mismo solicitante y no hayan sido manipulados. Para abordar estos requisitos de seguridad, los métodos de identificación conocidos suelen ser difíciles y engorrosos para todas las partes involucradas.

[0016] Una debilidad potencial adicional reside en que un dispositivo de Sujeto con la clave privada asociada previamente debe estar disponible para el Suscriptor correspondiente de manera segura. De hecho, la clave privada puede almacenarse en el propio dispositivo del Sujeto o la clave privada puede almacenarse de manera remota y vincularse criptográficamente a un *token* de seguridad, con el Sujeto previamente vinculado a esa clave privada. Al suministrar este dispositivo al Suscriptor apropiado, también se crea una vinculación física entre el dispositivo, con el que está asociada la clave privada, y el Sujeto, por que el dispositivo representa algo que el Suscriptor o un representante autorizado del Suscriptor tiene o posee. Para poder utilizar el dispositivo suministrado, normalmente se requiere que se active un factor de seguridad adicional (una contraseña secreta o PIN que conoce el Suscriptor, o un factor biométrico que pertenece al Suscriptor) antes de que el dispositivo esté operativo y acceda a la clave privada asociada concedida. La contraseña secreta o PIN representa algo que (solo) el Suscriptor o su representante autorizado sabe. El factor biométrico representa algo que (solo) tiene el Suscriptor o su representante autorizado. De hecho, si un dispositivo utilizable con una clave privada y un Sujeto asociado a esa clave privada fueran secuestrados sin haber hecho que el dispositivo sea accesible de forma segura y exclusiva para el usuario autorizado, el secuestrador podría actuar con una identidad falsa, es decir, la identidad previamente vinculada a la clave privada secuestrada.

[0017] Por lo tanto, es habitual proporcionar al suscriptor contraseñas o PIN de activación a través de canales seguros separados, lo que en consecuencia hace que la provisión del dispositivo al que se asocia la clave privada sea compleja e inconveniente, pero aún potencialmente propensa a ataques. De hecho, si se transmite una contraseña o PIN, por ejemplo, mediante el Servicio de mensajes cortos, SMS, un secuestrador puede interceptar el mensaje correspondiente y también puede hacerse con el dispositivo. Al hacerlo, el secuestrador tendría todos los medios necesarios para actuar como el Sujeto previamente vinculado al dispositivo.

Problema técnico por resolver

[0018] Un objetivo es presentar un método y un dispositivo que superen al menos algunos de los inconvenientes de la técnica anterior. Específicamente, un objetivo de la invención es mitigar los riesgos de ataques de intermediario cuando se da acceso a claves privadas a una parte autorizada, reduciendo el número de transmisiones de datos fundamentales para la seguridad. Es un objeto adicional proporcionar firmas electrónicas/digitales con un mayor nivel de seguridad.

Resumen de la invención

[0019] Un objetivo de la invención es proporcionar un método para firmar datos digitalmente usando una clave criptográfica en una red de comunicación que comprende un nodo de servidor y al menos un nodo de red adicional.

[0020] El método comprende los siguientes pasos:

(a) generar un par de claves criptográficas pública/privada utilizando medios de generación de claves criptográficas, en el que dicho par de claves no está asociado con un Sujeto;
(b) en el nodo de red del servidor, almacenar dicha clave pública en un almacenamiento de clave pública, y
(c) almacenar dicha clave privada en un almacenamiento de clave privada, al que se otorga acceso utilizando un factor de autenticación primario asociado predeterminado y al menos un factor de autenticación complementario todavía sin definir;
(d) proporcionar posteriormente a un usuario no identificado, el Suscriptor, dicho factor de autenticación primario, estando asociado dicho Suscriptor con un Sujeto identificable aún desconocido para el nodo del servidor;
(e) definir al menos un factor de autenticación complementario en asociación con dicho almacenamiento de clave privada, con los datos elegidos por dicho Suscriptor y pertenecientes a él, asociando de ese modo de manera exclusiva dicho almacenamiento de clave privada y dicho par de claves al Sujeto asociado con dicho Suscriptor;
(f) recibir posteriormente, en el nodo del servidor de al menos un nodo de red, datos que identifiquen a dicho Suscriptor y al Sujeto asociado, donde dichos datos están firmados criptográficamente con dicha clave privada utilizando medios de creación de firma digital;
(g) en el nodo del servidor, verificar y validar dichos datos recibidos, y asociar el Sujeto provisto a dicho par de claves;
(h) en cualquiera de dichos nodos de red, hacer que los datos se firmen criptográficamente con dicha clave privada utilizando medios de creación de firma digital, siendo certificables dichos datos firmados por dicho Sujeto, en función de la clave pública correspondiente y el Sujeto asociado con ella.

[0021] En el paso (e), el dato que pertenece a dicho Suscriptor (es decir, el al menos un segundo factor de autenticación) proviene exclusivamente de dicho Suscriptor, es decir, es independiente del primer factor de autenticación.

[0022] Ventajosamente, el paso (e) se realiza solo una vez. También ventajosamente, después de la ejecución del paso (e), el Suscriptor puede proporcionar pruebas para controlar únicamente el primer y el segundo factor de autenticación independiente para emplear dicha clave privada de dicho par de claves privada/pública.

[0023] Preferiblemente, en el paso (d), el factor de autenticación primario para acceder al almacenamiento de dicha clave privada puede proporcionarse a dicho usuario/suscriptor no identificado a través de un canal de comunicación no seguro.

[0024] Preferiblemente, después del paso (e), dicho almacenamiento de clave privada y la clave privada se vuelven accesibles para dicho Suscriptor no identificado gracias a que se mantiene un número requerido de factores de autenticación;

[0025] El almacenamiento de clave privada puede comprender preferiblemente un entorno de almacenamiento criptográficamente seguro, tal como un elemento de memoria criptográficamente seguro.

[0026] El factor de autenticación primario puede comprender preferiblemente un dispositivo físico resistente a la manipulación. Alternativamente, el factor de autenticación primario puede comprender preferiblemente medios de código de programa resistentes a la manipulación. La expresión "resistente a la manipulación" se utiliza para

describir un código de dispositivo o programa, que es difícil o complicado de atacar o modificar y que al menos cumple los requisitos de seguridad para lograr el nivel deseado de seguridad.

[0027] Preferiblemente, dicho dispositivo físico o medios de código de programa resistentes a la manipulación pueden comprender dichos medios de generación de clave criptográfica, dicho almacenamiento de clave privada y dichos medios de creación de firma digital. Dicho dispositivo físico o medios de código de programa resistentes a la manipulación se pueden configurar además preferiblemente para transmitir dicha clave pública generada a dicho nodo del servidor después del paso (a), para almacenarla en dicho almacenamiento de clave pública.

[0028] Dicho nodo de servidor puede comprender preferiblemente dichos medios de generación de clave criptográfica.

[0029] Dicho dispositivo físico o medios de código de programa resistentes a la manipulación pueden comprender preferiblemente dicho almacenamiento de clave privada y dichos medios de creación de firma digital. Dicho nodo de servidor se puede configurar preferiblemente para almacenar dicha clave privada generada en dicho almacenamiento de clave privada en el paso (c).

[0030] Dicho nodo de servidor puede comprender preferiblemente dicho almacenamiento de clave privada y dichos medios de creación de firma digital. Dicho dispositivo físico o código de programa resistente a la manipulación puede comprender preferiblemente datos necesarios para acceder a dicho almacenamiento de clave privada a través de un canal de comunicación de datos seguro, en el que dichos datos no están asociados con un Sujeto. El dispositivo puede comprender un *token* de seguridad. El dispositivo puede estar configurado para ejecutar un algoritmo de contraseña de un único uso sincronizado con dicho nodo del servidor.

[0031] Preferiblemente, el dispositivo físico resistente a la manipulación puede comprender un microchip. El dispositivo físico resistente a la manipulación puede comprender preferiblemente una tarjeta inteligente configurada para interactuar con un nodo de red.

[0032] En el paso (e), el factor de autenticación complementario puede transmitirse preferiblemente desde un nodo de red a dicho nodo de servidor a través de un canal seguro de comunicación de datos. Preferiblemente, solo los datos para validar el factor de autenticación complementario se envían a dicho nodo del servidor. Alternativamente, si el factor de autenticación complementario se valida en el dispositivo resistente a la manipulación, siempre que la fiabilidad del canal de comunicación de datos entre dicho segundo y tercer nodo de red pueda garantizar un nivel suficiente de seguridad, la transmisión del factor de autenticación complementario o de datos para validarlo se vuelve obsoleta.

[0033] Alternativamente, en el paso (e), el factor de autenticación complementario puede almacenarse preferiblemente en dicho dispositivo o medios de código de programa resistentes a la manipulación. La información o los datos para validar dicho factor de autenticación pueden transmitirse preferiblemente desde un nodo de red a dicho nodo del servidor a través de un canal de comunicación seguro.

[0034] El paso (f) puede repetirse preferiblemente hasta que se hayan recibido suficientes datos para validar dicho Suscriptor y Sujeto en dicho nodo del servidor.

[0035] El paso (f) puede repetirse preferiblemente hasta que se hayan recibido suficientes datos de identificación en dicho nodo del servidor.

[0036] El nodo del servidor puede ser un dispositivo informático. Alternativamente, el nodo del servidor puede comprender una pluralidad de dispositivos informáticos o nodos de red interconectados usando una red de comunicación. Los recursos informáticos y de memoria de dicha pluralidad de dispositivos informáticos pueden agregarse como una máquina virtual. Los medios de creación de firma digital, los medios de generación de claves o los medios de validación para dicho segundo factor de autenticación, por ejemplo, pueden estar ubicados físicamente en distintos dispositivos informáticos o nodos de red, que están interconectados para formar un nodo de servidor agregado de acuerdo con la presente invención.

[0037] Los medios de generación criptográfica y los medios de creación de firma digital pueden implementarse preferiblemente por un procesador de un ordenador, o sus equivalentes.

[0038] Preferiblemente, el almacenamiento de clave pública puede configurarse para que contenga al menos una clave pública y sea accesible a otros nodos de red en dicha red de comunicación.

[0039] El almacenamiento de clave privada se puede configurar preferiblemente para que contenga solo dicha clave privada.
El almacenamiento de clave privada puede configurarse para que contenga una pluralidad de claves privadas, donde cada clave está asociada al mismo Sujeto.

[0040] Preferiblemente, el nodo del servidor puede comprender una Autoridad de registro, RA y/o una Autoridad de certificación, CA, de una Infraestructura de clave pública, PKI.

[0041] El almacenamiento de clave pública puede comprender preferiblemente un almacenamiento de Certificados, y dicha clave pública puede estar comprendida preferiblemente en un Certificado, que se almacena en dicho almacenamiento de Certificados.

[0042] En el paso (b), un primer Certificado que comprende dicha clave pública, pero que no incluye un Sujeto asociado, puede almacenarse preferiblemente en dicho almacenamiento de Certificados. En el paso (g), un Sujeto puede asociarse con dicho primer Certificado, o dicho primer Certificado puede ser reemplazado por un segundo Certificado que comprende dicha clave pública y dicha asociación del Sujeto (preferiblemente revocando al mismo tiempo dicho primer Certificado).

[0043] El factor de autenticación complementario puede comprender preferiblemente una contraseña, un número de identificación personal, PIN, o datos biométricos relacionados con dicho Sujeto y/o Suscriptor no identificado, o cualquier combinación de estos.

[0044] Los datos de identificación pueden comprender preferiblemente datos de un carné de identificación nacional o pasaporte, información de video digital o información biométrica relacionada con dicho usuario, extractos del registro comercial, otras pruebas de identificación o cualquier combinación de estos.

[0045] De acuerdo con otro aspecto de la invención, se proporciona un programa informático que comprende un medio de código legible por ordenador que, cuando se ejecuta en un ordenador, hace que el ordenador lleve a cabo el método de acuerdo con la invención, o cualquier subconjunto de los pasos de dicho método.

[0046] Según otro aspecto más de la invención, se proporciona un sistema informático configurado para llevar a cabo el método según la invención, o cualquier subconjunto de los pasos de dicho método.

[0047] Mediante el uso de la presente invención, es posible mejorar la seguridad y la fiabilidad de las firmas digitales en el contexto de las infraestructuras PKI. Específicamente, el protocolo propuesto elimina el requisito de transmitir un dispositivo al cual una clave privada y un Sujeto están asociados inequívocamente a un usuario a través de un primer canal de comunicación, al tiempo que se proporciona un código de activación (contraseña, PIN, etc.) a través de un segundo canal de comunicación separado al mismo usuario. Esto es posible porque, de acuerdo con la invención, el dispositivo proporcionado solo está asociado con una clave privada, pero todavía no está asociado con ningún Sujeto antes de su distribución a un usuario. De hecho, el par de claves privada/pública que se genera puede considerarse genérico, y cualquier usuario todavía no identificado puede recibirlo a través de un canal no seguro. Una vez que un usuario posee un factor de autenticación primario para dar acceso al par de claves, siendo el factor primario, por ejemplo, el dispositivo asociado con el par genérico de claves generadas aleatoriamente, el usuario lo aumenta con al menos un factor de autenticación complementario, es decir, una contraseña, un PIN o un factor biométrico. Solo en este paso, el dispositivo y su clave privada asociada se vuelven operativos para fines de firma digital para el usuario que había proporcionado el factor de autenticación adicional, aunque el usuario todavía no esté identificado. Sin embargo, solo el usuario que conozca o posea el factor de autenticación complementario y esté su vez en posesión del dispositivo puede autorizar el uso de la clave privada para firmar datos digitalmente, de modo que se asegura que cualquier dato firmado criptográficamente con la clave privada obtenida habrá sido emitido por el mismo usuario no identificado. Esta característica se explota aún más para proporcionar a la PKI atributos y elementos destinados a identificar dicho usuario no identificado y al Sujeto cuando son diferentes y cuando lo requiere la organización en cuyo nombre actúa el usuario. Mediante un dispositivo informático, el usuario firma criptográficamente estos atributos y elementos con la clave privada a la que ha obtenido acceso exclusivo, y transmite los datos firmados digitalmente mediante un canal de comunicación de datos a la PKI. La PKI, que tiene acceso a la clave pública correspondiente, es capaz de atribuir inequívocamente los elementos y atributos recibidos al mismo solicitante/usuario mediante la validación de la(s) firma(s) adherida(s) a los datos transmitidos, siempre que se tomen medidas para evitar la repetición de las transmisiones (por ejemplo, mediante la imposición por parte de la PKI de la inclusión de un número de sesión aleatorio único con cada transmisión, aunque el mecanismo de protección particularmente empleado esté fuera del alcance de la invención). Esta atribución inequívoca se logra sin incurrir en ninguna transmisión de datos adicional y/o medidas de protección adicionales, a diferencia de los métodos de la técnica anterior. Tras la verificación de los datos recibidos, la PKI está lista para certificar al Sujeto, con el proceso de identificación subyacente y los elementos necesarios que están fuera del alcance de la invención. En este paso, la PKI vincula el Sujeto al par de claves pública/privada mediante un Certificado. Se ha obtenido un fuerte vínculo entre el Sujeto y el par de claves. El par de claves deja de ser genérico y puede usarse para firmar digitalmente cualquier dato de forma verificable. El sujeto ha sido inscrito en la PKI.

[0048] En resumen, en comparación con las técnicas del estado de la técnica, la invención mitiga los riesgos de ataques de intermediario en el contexto del dispositivo del Sujeto y los métodos de distribución de clave pública, mejorando así inherentemente la fiabilidad de los Certificados emitidos por una PKI. Esto se logra al reducir el número de transmisiones de datos fundamentales para la seguridad y al invertir el proceso de identificación y la

provisión del dispositivo del Sujeto con respecto a la técnica anterior. Además, la distribución de dispositivos (es decir, tarjetas inteligentes que comprenden claves privadas o medios para acceder a claves privadas) se facilita enormemente, ya que solo los dispositivos genéricos, que todavía no están vinculados a ningún Sujeto, se pueden distribuir a través de canales no seguros.

Breve descripción de los dibujos

[0049] Varias formas de realización de la presente invención se ilustran a modo de figuras, que no limitan el alcance de la invención, en las que:

- La Figura 1 ilustra la secuencia de los pasos principales del método de acuerdo con una forma de realización preferida, que incluye las entidades principales involucradas en estos pasos;
- La Figura 2 ilustra la secuencia de los pasos principales del método de acuerdo con una forma de realización preferida, que incluye las entidades principales involucradas en estos pasos;
- La Figura 3 ilustra la secuencia de los pasos principales del método de acuerdo con una forma de realización preferida, que incluye las entidades principales involucradas en estos pasos;
- La Figura 4 es un diagrama de estado, que ilustra el conocimiento que una entidad de inscripción tiene sobre un usuario (Suscriptor) a lo largo de los pasos principales del método de acuerdo con una forma de realización preferida de la invención.

Descripción detallada de la invención

[0050] La siguiente descripción se centra en aquellas características que son fundamentales para que se implemente el método de acuerdo con la invención, y que no se conocen del estado de la técnica. Cualquier implementación del método también se basa en conceptos tan conocidos en la técnica que no se describirán en detalle en aras de la claridad. Dichos conceptos ampliamente conocidos incluyen, por ejemplo, entre otros, la generación de pares de claves criptográficas pública/privada. El uso de esquemas criptográficos para claves privadas y públicas no se limitará en el sentido de estar basado en esquemas criptográficos adoptados actualmente en gran medida como RSA o curvas elípticas solamente. También se pueden emplear otros esquemas.

[0051] Debe observarse que las características descritas en el contexto de una forma de realización específica descrita en el presente documento pueden combinarse con las características de otras formas de realización a menos que se mencione explícitamente lo contrario. La descripción de características que son idénticas en varias formas de realización generalmente no se repite para cada una de tales formas de realización. La descripción de diferentes formas de realización se centra en las diferencias entre tales formas de realización.

[0052] El método según la invención tiene lugar en una red de comunicación que conecta un nodo de servidor 110 a una pluralidad de nodos de usuario 120, que pueden considerarse como dispositivos o terminales del Sujeto, utilizando canales de comunicación de datos posiblemente heterogéneos.

[0053] En el contexto de la invención, un Suscriptor es una persona física que actúa en su propio nombre o una organización, es decir, una persona jurídica, que puede estar representada por una persona física autorizada.

[0054] Un Sujeto es la entidad que, al final del proceso de acuerdo con la invención, está certificada por el Certificado emitido por la PKI. Un Sujeto puede ser el propio Suscriptor o un activo propiedad del Suscriptor, como un dispositivo portátil, por ejemplo.

[0055] El suscriptor es responsable de respetar los requisitos de seguridad y, en particular, de gestionar adecuadamente los factores de autenticación del dispositivo del Sujeto, tal como se describe a continuación, que el sujeto utiliza para fines de firma.

[0056] Una primera forma de realización preferida del método de acuerdo con la invención comprende los siguientes pasos como se describe en la Figura 1. En el paso (a) se genera un par de claves criptográficas pública/privada usando medios de generación de claves criptográficas 130. Los medios de generación de claves pueden comprender un sistema criptográfico generador de claves o medios de procesamiento generales de un dispositivo informático, que están configurados para generar un par de claves criptográficas. Los algoritmos para generar tales pares de claves son ampliamente conocidos en la técnica y no se describirán en detalle en el contexto de la presente invención. El par de claves generado no está asociado ni vinculado a la identidad de ningún Sujeto. Por lo tanto, puede considerarse como un par de claves genérico, que puede distribuirse libremente, sin arriesgarse a comprometer el par de claves de un usuario específico. Sin embargo, la distribución debe organizarse de manera que la copia de la clave privada se pueda evitar de manera eficaz en cualquier contexto, lo que significa que la clave privada existe en cualquier momento solo una vez. La clave pública se puede distribuir a través de canales no seguros, pero la clave privada correspondiente debe almacenarse en un almacenamiento de clave privada seguro solo a través de un canal seguro, o generarse directamente dentro de un almacenamiento de clave privada seguro.

[0057] En el paso (b), la clave pública se almacena en un almacenamiento de clave pública 140 en un nodo del servidor 110. El almacenamiento de clave pública puede configurarse preferiblemente para almacenar una pluralidad de claves públicas. El nodo del servidor puede ser un único servidor en una red de comunicación, o una agregación de varios servidores en una red de comunicación que proporciona los servicios requeridos por el nodo del servidor. El almacenamiento de clave pública 140 comprende un elemento de memoria, tal como un elemento de memoria estructurada o una base de datos, a la que todos los nodos en la red de comunicación tienen acceso abierto. Como tal, el nodo del servidor 110 tiene acceso de lectura/escritura al almacenamiento de clave pública 140. Las claves públicas pueden almacenarse ventajosamente en forma de certificados de seguridad, que generalmente se usan para certificar que una clave pública pertenece a un usuario específico. En el caso de la presente invención, en los pasos (a) y (b), la clave pública puede almacenarse en un Certificado que específicamente no contiene ninguna información sobre un usuario específico. Si el formato de datos del Certificado requiere un nombre de usuario, se puede asociar un seudónimo o marcador de posición genérico con la clave pública que se ha generado. El Certificado puede ser un Certificado técnico. En cualquier caso, debe tenerse en cuenta que, antes de los pasos posteriores del método de acuerdo con la invención, el Certificado no pertenece a ningún usuario específico.

[0058] En el paso (c), la clave privada generada se almacena en un almacenamiento de clave privada 150. El almacenamiento de clave privada está configurado preferiblemente para contener solo una clave privada generada. Sin embargo, la provisión de múltiples pares de claves para el mismo usuario es una opción alternativa dentro del alcance de la presente invención, que en consecuencia requiere que el almacenamiento de clave privada sea capaz de almacenar varias claves privadas para un usuario dado. Sin embargo (pero sin limitación), la descripción posterior abstrae de esta opción alternativa y supone, por simplicidad, que se almacena una única clave privada en el almacenamiento de clave privada del usuario. El acceso al almacenamiento de clave privada 150 y, por lo tanto, a la clave privada contenida en él, se otorga a un usuario o nodo de red con la condición de la prueba de posesión de un factor de autenticación primario predeterminado F1, y al menos un factor de autenticación complementario/secundario. La clave privada no es directamente accesible para el usuario ni para ninguna otra parte. En su lugar, el usuario interactúa con medios de creación de firma digital, que utilizan la clave privada que está almacenada en el almacenamiento seguro de clave privada.

[0059] Debe observarse que, en el paso (c), el factor de autenticación primario es predeterminado, por ejemplo, por el nodo del servidor, mientras que el/los factor(es) de autenticación complementario(s) todavía no están definidos. Estos serán definidos más adelante por un usuario.

[0060] El paso (c) puede realizarse antes del paso (b) sin salir del alcance de la presente invención.

[0061] En el paso (d), un usuario no identificado, el Suscriptor, que puede ser una persona física o jurídica, recibe el factor de autenticación principal. El Suscriptor está asociado con un Sujeto identificable, que, sin embargo, aún es desconocido para el nodo del servidor. El Suscriptor puede ser idéntico al Sujeto, o el Sujeto puede ser un activo propiedad del Suscriptor. La provisión del factor de autenticación primario F1 puede tener lugar utilizando un canal de comunicación no seguro. Preferiblemente, el factor de autenticación primario comprende un dispositivo físico asociado con el par de claves generado, de modo que la provisión del factor F1 pone al usuario no identificado en la posición de poseer algo que solo él/ella posee.

[0062] El contenido del almacenamiento de clave privada solo se vuelve accesible una vez que se ha definido al menos un factor de autenticación complementario F2.

[0063] Por lo tanto, el usuario/Suscriptor no identificado aumenta el nivel de seguridad en el almacenamiento de clave privada 150 obtenido mediante la provisión del factor de autenticación primario F1, al definir un factor de autenticación complementario, F2. Este factor complementario puede ser algo que solo él/ella sabe, por ejemplo una contraseña o PIN, o algo que solo él/ella tiene, por ejemplo información biométrica relacionada con su persona o cuerpo. En este paso, la clave privada se vuelve accesible para dicho usuario/suscriptor no identificado (y solo para él/ella) debido a que se mantiene el número requerido de factores de autenticación. Cabe señalar que, al contrario de los esquemas de distribución de clave privada conocidos, el/los) factor(es) de autenticación complementario(s), por ejemplo una contraseña o PIN inicial, no necesita ser transmitida desde una entidad central a un usuario utilizando un canal de comunicación distinto y seguro. Esto se debe a que el usuario todavía no identificado vincula la clave privada a sí mismo por iniciativa propia. En este paso del proceso, solo el usuario no identificado puede usar la clave privada que ha obtenido. Esto corresponde al paso (e), y realizar este último paso es un requisito previo para que la clave privada sea realmente accesible. En todas las formas de realización, el factor de autenticación F2, o al menos los datos que permiten validar el factor de autenticación F2, deberían estar disponibles en un nodo de red que implemente la funcionalidad de validación del factor de autenticación.

[0064] En el paso (f), los datos 124 que identifican al usuario todavía no identificado se firman digitalmente con la clave privada en un nodo de usuario (nodo de red) 120. Solo un único usuario tiene acceso a dicha clave privada. Los datos firmados criptográficamente se transmiten utilizando un canal de comunicación de datos al nodo del servidor 110, que tiene acceso a la clave pública correspondiente. Por lo tanto, el nodo del servidor 110 puede

verificar que cualquier dato que pueda validarse usando dicha clave pública proceda del mismo usuario todavía no identificado. Tras la verificación de los datos proporcionados, que pueden incluir información de pasaporte, información de vídeo que representa al usuario, otros datos de identificación relacionados con el usuario, el Suscriptor cuando es diferente del usuario y el Sujeto y pruebas complementarias según sea necesario (como una autorización), el nodo del servidor 110 puede identificar inequívocamente que los datos recibidos proceden del usuario que está en posesión de dicho factor de autenticación primario y que además ha asociado al menos un segundo factor de autenticación proporcionado por él mismo. El Sujeto identificado de esta manera se asocia con la clave pública en el almacenamiento de clave pública. Si la clave pública se almacena en un Certificado, el Certificado correspondiente, que hasta ahora no estaba vinculado a ningún Sujeto, se vincula al Sujeto identificado o se reemplaza por un nuevo Certificado para incluir los datos de identidad así proporcionados y validados y, al mismo tiempo, revocar el certificado sin consolidar. Esto corresponde al paso (g). La clave privada, al estar implícitamente vinculada a la clave pública, está indirectamente vinculada al mismo Sujeto. En este paso, el usuario identificado posee de forma única e inequívoca el Certificado.

[0065] En este paso del proceso, se ha establecido un fuerte vínculo entre el Sujeto y el par de claves privada/pública generado. El vínculo se ha establecido sin requerir la transmisión de un factor de autenticación primario a través de un primer canal seguro, y la transmisión de los datos de activación correspondientes a través de un segundo canal seguro, como se conoce en la técnica. La seguridad del protocolo para la distribución de la clave privada a un usuario se mejora, ya que el protocolo propuesto implica menos transmisiones de datos cruciales para la seguridad que los protocolos conocidos en la técnica, ya que cada una de esas transmisiones es potencialmente propensa ser espiada por terceros malintencionados. En el caso de la variante en la que solo se deben transmitir datos de validación para un segundo factor o cuando un segundo factor se valida localmente en el dispositivo del Sujeto, no se requieren transmisiones de datos cruciales para la seguridad.

[0066] En el paso (h), se hace que los datos 125 se firmen criptográficamente usando dicha clave privada usando los medios de creación de firma digital 160 en cualquier nodo de red 120. Este paso puede repetirse según sea necesario, una vez que los pasos anteriores se hayan llevado a cabo con éxito. Se puede certificar que los datos firmados han sido firmados por dicho Sujeto identificado hasta ahora en función de la clave pública correspondiente asociada con el mismo en el almacenamiento de clave pública. Los datos firmados pueden ser un identificador de sesión de comunicación, datos relacionados con un contrato comercial o cualquier otro dato.

[0067] Como consecuencia, cualquier firma digital realizada con la clave privada que se ha vinculado al Sujeto utilizando los pasos anteriores es inherentemente más segura y fiable que las firmas digitales realizadas con una clave privada que se ha distribuido utilizando métodos conocidos en la técnica.

[0068] En referencia a la figura 2, se describe una segunda forma de realización preferida del método según la invención. En el paso (a), se genera un par de claves criptográficas pública/privada utilizando medios de generación de clave criptográfica 230. De acuerdo con esta forma de realización, los medios de generación de clave s230 pueden comprender un generador de clave criptográfica o medios de procesamiento generales que forman parte del nodo del servidor 210, o parte de una Infraestructura de clave pública, PKI. En una implementación alternativa, los medios de generación de claves pueden implementarse mediante un nodo de red específico que proporciona uno de los servicios del nodo de servidor 210 descrito. Los medios de procesamiento están configurados para generar un par de claves criptográficas. El par de claves generado no está asociado ni vinculado a ningún Sujeto. Por lo tanto, puede considerarse como un par de claves genéricas, que pueden distribuirse libremente sin arriesgarse a comprometer el par de claves de un Sujeto específico.

[0069] En el paso (b), la clave pública se almacena en un almacenamiento de clave pública 240, también local para el nodo del servidor 210 o PKI. Nuevamente, el almacenamiento de clave pública puede ubicarse alternativamente en un nodo de red dedicado, lo que contribuye a la prestación de los servicios del nodo de servidor 210 descrito.

[0070] En el paso (c), la clave privada generada se almacena en un almacenamiento de clave privada 250. El almacenamiento de clave privada está configurado preferiblemente para contener solo una clave privada generada, aunque es posible que haya configuraciones alternativas para almacenar múltiples claves privadas sin abandonar el alcance de la presente invención. En esta forma de realización, el almacenamiento de clave privada 250, así como los medios de creación de firma digital 260, son preferiblemente locales al nodo de red 210 o PKI. Alternativamente, el almacenamiento de clave privada y los medios de creación de firma digital pueden ser implementados por un nodo de red específico, lo que contribuye a la provisión de los servicios del nodo del servidor descritos. El acceso al almacenamiento de clave privada 250 y, por lo tanto, la clave privada contenida en el mismo, se otorga a un usuario o nodo de red con la condición de la prueba de posesión de un factor de autenticación primario predeterminado F1, y al menos un factor de autenticación complementario/secundario. Debe observarse que, en el paso (c), el factor de autenticación primario está predeterminado, por ejemplo, por el nodo del servidor, mientras que el/los factor(es) de autenticación complementario(s) todavía no están definidos. De acuerdo con esta forma de realización, el factor de autenticación primario F1 es un dispositivo de *token* de seguridad, que implementa preferiblemente un algoritmo de contraseña de un solo uso, con una OTP generada verificable por el nodo 210 del servidor para proporcionar uno de los factores necesarios para otorgar acceso al almacenamiento de clave privada

250 en el nodo de red 210. Se pueden concebir otros mecanismos de autenticación sin salir del alcance de la presente invención.

[0071] El orden de los pasos (b) y (c) puede invertirse sin salir del alcance de la presente invención.

[0072] En el paso (d), un usuario no identificado recibe el factor de autenticación principal en forma de *token* de seguridad. El *token* de seguridad se convierte en algo que solo posee el usuario todavía no identificado.

[0073] El usuario no identificado aumenta el nivel de seguridad en el almacenamiento de clave privada 250 obtenido mediante la provisión del *token* de seguridad, al definir un factor de autenticación complementario, F2. Este factor complementario puede ser algo que solo él/ella sabe, por ejemplo una contraseña o PIN, o algo que solo él/ella tiene, por ejemplo Información biométrica relacionada con su persona o cuerpo. El factor de autenticación complementario puede asociarse, por ejemplo, con el almacenamiento de clave privada 250 a través de una interfaz basada en web del nodo de servidor 210 o PKI, que el usuario puede usar para proporcionar el factor de autenticación complementario. En este paso del proceso, solo el usuario no identificado puede usar la clave privada que ha obtenido. Esto corresponde al paso (e). Los pasos (f) a (g) corresponden a la primera forma de realización descrita.

[0074] En el paso (h), el nodo 210 del servidor firma criptográficamente los datos usando dicha clave privada y los medios de creación de firma digital 260, que se encuentran en el nodo 210 del servidor o son accesibles desde este. El acceso a la clave privada es otorgado por el nodo del servidor 210 tras la validación exitosa de los factores de autenticación suministrados, con el nodo del servidor 210 cumpliendo así con la solicitud y firmando digitalmente los datos recibidos en nombre del Sujeto. Se puede certificar que los datos han sido firmados por dicho Sujeto identificado hasta ahora en función de la clave pública correspondiente y el Sujeto asociado a esta en el almacenamiento de clave pública.

[0075] El paso (h) puede repetirse según lo requiera una aplicación específica, después de que los pasos anteriores se hayan llevado a cabo con éxito una vez.

[0076] En referencia a la figura 3, se describe una tercera forma de realización preferida del método según la invención. En el paso (a), se genera un par de claves criptográficas pública/privada sutilizando medios de generación de clave criptográfica 330. De acuerdo con esta forma de realización, los medios de generación de clave 330 pueden comprender un generador de clave criptográfica o medios de procesamiento generales que forman parte de un dispositivo de tarjeta inteligente. Alternativamente para la presente forma de realización, el dispositivo de tarjeta inteligente puede ser un módulo criptográfico de hardware, HSM o una aplicación de software segura. Los medios de procesamiento están configurados para generar un par de claves criptográficas. El par de claves generado no está asociado ni vinculado a ningún Sujeto. Por lo tanto, puede considerarse como un par de claves genéricas, que pueden distribuirse libremente, mediante la distribución del dispositivo de tarjeta inteligente, utilizando canales de comunicación no seguros, sin arriesgarse a comprometer un par de claves de un usuario específico.

[0077] En el paso (b), la clave pública se almacena en un almacenamiento de clave pública 340, local para el nodo del servidor 310 o PKI. La clave pública, que es generada por el dispositivo de tarjeta inteligente, puede transmitirse con este objetivo desde un dispositivo informático conectado con el dispositivo de tarjeta inteligente, al nodo de servidor 310 o PKI.

[0078] En el paso (c), la clave privada generada se almacena en un almacenamiento de clave privada 350. El almacenamiento de clave privada está configurado para contener solo una clave privada generada. En esta forma de realización, el almacenamiento de clave privada 350 y los medios de creación de firma digital 360 son preferiblemente locales para dicho dispositivo de tarjeta inteligente. El orden de los pasos (b) y (c) puede invertirse.

[0079] En una forma de realización alternativa de los pasos anteriores, los medios de generación de claves pueden comprender un generador de claves criptográficas o medios de procesamiento generales que forman parte del nodo del servidor o parte de una Infraestructura de Clave Pública, PKI. Después de la generación del par de claves en el paso (a), la clave privada puede almacenarse en ese caso en un almacenamiento de clave privada 350 que es local para dicho dispositivo de tarjeta inteligente. Dicha alternativa se indica mediante la reagrupación del nodo del servidor 310 y los medios de generación de clave 330 representada en línea discontinua en la Figura 3. La introducción de la clave privada en dicho dispositivo de tarjeta inteligente tiene lugar preferiblemente en el nodo del servidor 310 usando un canal seguro de comunicación de datos. El paso de transmisión de la clave pública al nodo del servidor es obsoleto en esta forma de realización alternativa, ya que la clave pública ya está disponible en el nodo del servidor después de su generación. Como se ha descrito antes en este documento, el dispositivo de tarjeta inteligente también comprende los medios de creación de firma digital.

[0080] El acceso al almacenamiento de clave privada 350, y por lo tanto a la clave privada contenida en el mismo, se otorga a un usuario o nodo de red condicionalmente gracias a la posesión de dicho dispositivo de tarjeta inteligente que implementa dicho factor de autenticación primario predeterminado F1, y al menos un

complemento/secundario factor de autenticación. En este paso, los factores de autenticación complementarios todavía no están definidos.

[0081] En el paso (d), un usuario no identificado recibe el factor de autenticación principal en forma de dispositivo de tarjeta inteligente. El dispositivo de tarjeta inteligente se convierte en algo que solo el usuario todavía no identificado posee. El usuario todavía no identificado puede interconectar la tarjeta inteligente con un dispositivo informático 320 utilizando medios de interfaz apropiados (por ejemplo, un lector incorporado o conectado) y controladores como los conocidos en la técnica.

[0082] El dispositivo de tarjeta inteligente se configura preferiblemente de modo que, al producirse el primer acceso por parte de cualquier usuario, dicho usuario debe aumentar el nivel de seguridad en el almacenamiento de clave privada 350 obtenido mediante la provisión de la propia tarjeta inteligente, definiendo un factor de autenticación complementario, F2. Este factor complementario puede ser algo que solo él/ella sabe, por ejemplo una contraseña o PIN, o algo que solo él/ella tiene, por ejemplo información biométrica relacionada con su persona o cuerpo. Las credenciales proporcionadas pueden almacenarse preferiblemente en un elemento de memoria seguro de la tarjeta inteligente. En este paso del proceso, solo el usuario no identificado puede usar la clave privada que ha obtenido. Esto corresponde al paso (e). Los pasos (f) a (g) corresponden a la primera forma de realización descrita.

[0083] En el paso (h), se hace que los datos 325 sean firmados criptográficamente por la tarjeta inteligente o dispositivo alternativo usando medios de creación de firma 360 y la clave privada almacenada en el almacenamiento local de clave privada 350. El nodo de usuario 320 otorga acceso a la clave privada proporcionando el segundo factor de autenticación F2, con el factor primario F1 proporcionado implícitamente gracias a que la tarjeta inteligente o alternativa se ha puesto a disposición del nodo de usuario 320 en el paso (d) anteriormente. Se puede certificar que los datos firmados han sido firmados por dicho Sujeto identificado hasta ahora en función de la clave pública correspondiente y el Sujeto asociado a esta en el almacenamiento de clave pública. Los datos firmados pueden ser un identificador de sesión de comunicación, datos relacionados con un contrato comercial o cualquier otro dato.

[0084] Para obtener más información sobre la invención, la Figura 4 ilustra un diagrama de estado que tiene cuatro estados A, B, C y D. Cada estado corresponde al estado de un usuario como lo ve el nodo de red 110 o PKI. En aras de este ejemplo ilustrativo, se supone que, en el estado A, el usuario/suscriptor no está identificado y no posee ninguno de los factores de autenticación F1, F2 necesarios para acceder al almacenamiento de clave privada en el que la clave privada generada, que todavía no está vinculada a ningún Sujeto, se almacena. Como el usuario todavía no está identificado, el estado A está marcado con un signo de interrogación "?". Tras la transmisión del factor de autenticación primario F1 al usuario, correspondiente al paso (d) como se ha descrito antes en este documento, el estado del usuario cambia de A a B. En el estado B, el usuario todavía no está identificado con la PKI, pero posee un primer elemento requerido para acceder al almacenamiento de clave privada 150. Este primer elemento puede ser un *token* de seguridad, un dispositivo de tarjeta inteligente o cualquier otro factor de autenticación primario. Al proporcionar sus propias credenciales como factor de autenticación complementario F2, correspondiente al paso (e) de la invención, el estado del usuario cambia de B a C. En este estado, el usuario todavía no está identificado con la PKI, pero ella/él, y solo ella/él, tiene acceso a la clave privada contenida en el almacenamiento de clave privada 150. Siguiendo los pasos (f) y (g) de acuerdo con la invención, la PKI puede verificar la identidad del usuario (y/o del Suscriptor) y asociar el Sujeto que se identifica en el mismo paso de forma inequívoca y única con el par de claves. El estado del usuario cambia de C a D. En este estado, la PKI ha identificado al usuario (y/o Suscriptor) y al Sujeto, indicado por el signo de exclamación "!". La PKI puede certificar que cualquier dato firmado digitalmente por la clave privada puede atribuirse al Sujeto, que está fuertemente vinculado a la clave privada como resultado de los pasos anteriores. El sujeto ha sido inscrito en la PKI.

[0085] Se pueden prever otras modalidades que no sean un *token* de seguridad o un dispositivo de tarjeta inteligente para implementar el factor de autenticación primario como se ha descrito antes en este documento. Por ejemplo, el acceso a un almacenamiento de claves de software se puede proporcionar utilizando una aplicación de software específica, que por ejemplo se puede ejecutar en un teléfono inteligente. En particular, dicha aplicación de software puede comprender medios de código de programa que implementan el almacenamiento de clave privada y los medios para crear una firma digital usando la clave privada almacenada en dicho almacenamiento de clave privada. La provisión de dicha aplicación de software a un usuario no identificado es una implementación del paso (d) del método como se describe en este documento. Como la clave privada todavía no está vinculada a ningún Sujeto, la distribución de la aplicación de software puede realizarse utilizando un canal de comunicación de datos no seguro. Por ejemplo, el usuario puede descargar una aplicación de software correspondiente de un servidor proveedor en Internet. Al inicializar la aplicación de software en su dispositivo informático o teléfono inteligente, el usuario puede aumentar el nivel de seguridad de la aplicación de software dada utilizando sus credenciales, proporcionando así el factor de autenticación complementario requerido. El experto en la materia puede prever igualmente otras modalidades, como un módulo de seguridad de hardware, sin apartarse del alcance de la presente invención.

[0086] Debe entenderse que la descripción detallada de formas de realización preferidas específicas se proporciona solo a modo de ilustración, ya que diversos cambios y modificaciones dentro del alcance de la invención serán evidentes para el experto en la materia. El alcance de la protección se define mediante el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Método para la firma digital de datos usando una clave criptográfica en una red de comunicación que comprende un nodo de servidor (110, 210, 310) y al menos un nodo de red adicional (120, 220, 320), donde el método comprende los siguientes pasos:

(a) generar un par de claves criptográficas pública/privada utilizando medios de generación de clave criptográfica (130, 230, 330), en donde dicho par de claves no está asociado con la identidad de ningún Sujeto
(b) en el nodo del servidor (110, 210, 310), almacenar dicha clave pública en un almacenamiento de clave pública (140, 240, 340), y
(c) almacenar dicha clave privada en un almacenamiento de clave privada (150, 250, 350), el acceso al cual se otorga utilizando un factor de autenticación primario (F1) asociado predeterminado y al menos un factor de autenticación complementario todavía sin definir;
(d) proporcionar posteriormente a un usuario no identificado, el Suscriptor, dicho factor de autenticación primario (F1), donde dicho Suscriptor está asociado con un Sujeto identificable aún desconocido para el nodo del servidor;
(e) definir dicho al menos un factor de autenticación complementario (F2) todavía sin definir en asociación con dicho almacenamiento de clave privada (150, 250, 350) con los datos elegidos por dicho Suscriptor y que son propiedad de dicho Suscriptor, asociando así de manera única dicho almacenamiento de clave privada (150, 250, 350) y dicho par de claves al Sujeto asociado con dicho Suscriptor;
(f) recibir posteriormente, en el nodo del servidor (110, 210, 310) de al menos un nodo de red (120, 220, 320), datos (124, 224, 324) que identifiquen a dicho Suscriptor y al Sujeto asociado, donde dichos datos (124, 224, 324) se firman criptográficamente con dicha clave privada utilizando medios de creación de firma digital (160, 260, 360);
(g) en el nodo del servidor (110, 210, 310), verificar y validar dichos datos recibidos (124, 224, 324) y asociar el Sujeto identificado con dicho par de claves;
(h) en cualquiera de dichos nodos de red (120, 220, 320), hacer que los datos se firmen criptográficamente con dicha clave privada utilizando medios de creación de firma digital (160, 260, 360), donde se puede certificar que dichos datos han sido firmados por dicho Sujeto, en función de la clave pública correspondiente y el Sujeto asociado a ella.

2. Método según la reivindicación 1, en el que, en el paso (d), el factor de autenticación primario (F1) para acceder a dicho almacenamiento de clave privada (150) se proporciona a dicho usuario no identificado a través de un canal de comunicación no seguro.

3. Método según cualquiera de las reivindicaciones 1 o 2, en el que dicho factor de autenticación primario (F1) comprende un dispositivo físico o medios de código de programa resistentes a la manipulación.

4. Método según la reivindicación 3, en el que dicho dispositivo físico o medios de código de programa resistentes a la manipulación comprende dichos medios de generación de clave criptográfica (130), dicho almacenamiento de clave privada (150) y dichos medios de creación de firma digital (160), y en el que dicho dispositivo físico o medios de código de programa resistentes a la manipulación están configurados para transmitir dicha clave pública generada a dicho nodo de servidor (110) después del paso (a), para almacenarla en dicho almacenamiento de clave pública (140).

5. Método según la reivindicación 3, en el que dicho nodo de servidor (110) comprende dichos medios de generación de clave criptográfica (130), donde dicho dispositivo físico o medios de código de programa resistentes a la manipulación comprenden dicho almacenamiento de clave privada (150) y dichos medios de creación de firma digital (160), y en el que dicho nodo del servidor (110) está configurado para almacenar dicha clave privada generada en dicho almacenamiento de clave privada (150) en el paso (c).

6. Método según la reivindicación 3, en el que dicho nodo del servidor (110) comprende dichos medios de generación de claves criptográficas (130), dicho nodo del servidor (110) comprende dicho almacenamiento de clave privada (150) y dichos medios de creación de firma digital (160), y en el que dicho dispositivo físico o código de programa resistente a la manipulación comprende datos necesarios para acceder a dicho almacenamiento de clave privada (150) a través de un canal seguro de comunicación de datos, en el que dichos datos no están asociados con un Sujeto.

7. Método según cualquiera de las reivindicaciones 3 a 6, en el que el dispositivo físico resistente a la manipulación comprende una tarjeta inteligente configurada para interactuar con un nodo de red (120).

8. Método según cualquiera de las reivindicaciones 6 o 7, en el que, en el paso (e), el factor de autenticación complementario (F2) se transmite desde un nodo de red (120) a dicho nodo de servidor (110) a través de un canal seguro de comunicación de datos, o en el que, en el paso (e), el factor de autenticación complementario (F2) se almacena en dicho dispositivo o medios de código de programa resistentes a la manipulación, y en el que la

información para validar dicho factor de autenticación se transmite desde un nodo de red (120) a dicho nodo de servidor (110) a través de un canal de comunicación seguro.

9. Método según cualquiera de las reivindicaciones 1 a 8, en el que el paso (f) se repite hasta que se hayan recibido suficientes datos para validar dicho Suscriptor y Sujeto en dicho nodo del servidor (110).

10. Método según cualquiera de las reivindicaciones 1 a 9, en el que dicho almacenamiento de clave pública (140) está configurado para contener al menos una clave pública y es accesible a otros nodos de red en dicha red de comunicación, y/o en el que dicho almacenamiento de clave privada (150) está configurado para contener solo dicha clave privada, o una pluralidad de claves privadas, en el que cada clave está asociada con el mismo Sujeto.

11. Método según cualquiera de las reivindicaciones 1 a 10, en el que dicho nodo de servidor (110) comprende una Autoridad de registro, RA y/o una Autoridad de certificación, CA, de una Infraestructura de clave pública, PKI, en donde dicho almacenamiento de clave pública (140) comprende un almacenamiento de Certificados, y en el que dicha clave pública está comprendida en un Certificado, que se almacena en dicho almacenamiento de Certificados, o en el paso (b) un primer Certificado que comprende dicha clave pública, pero sin incluir un sujeto asociado, se almacena en dicho almacenamiento de Certificados, y en donde, en el paso (g), un Sujeto se asocia con dicho primer Certificado, o dicho primer Certificado es reemplazado por un segundo Certificado que comprende dicha clave pública y dicha asociación con el Sujeto, mientras que al mismo tiempo revoca el primer Certificado.

12. Método según cualquiera de las reivindicaciones 1 a 11, en el que dicho al menos un factor de autenticación complementario (F2) comprende datos que dicho Suscriptor conoce, como una contraseña, un número de identificación personal PIN, o datos que tiene dicho Suscriptor, como datos biométricos, o cualquier combinación de estos.

13. Método según cualquiera de las reivindicaciones 1 a 12, en el que los datos (124) que identifican dicho Suscriptor y Sujeto comprenden datos de pasaporte, información de video digital, un extracto de un registro comercial o información biométrica relacionada con el Suscriptor y el Sujeto, o cualquier combinación de estos.

14. Programa informático que comprende medios de código legible por ordenador que, cuando se ejecutan en un sistema informático, hacen que el sistema informático lleve a cabo el método según cualquiera de las reivindicaciones 1 a 13.

15. Sistema informático configurado para llevar a cabo el método según cualquiera de las reivindicaciones 1 a 13.

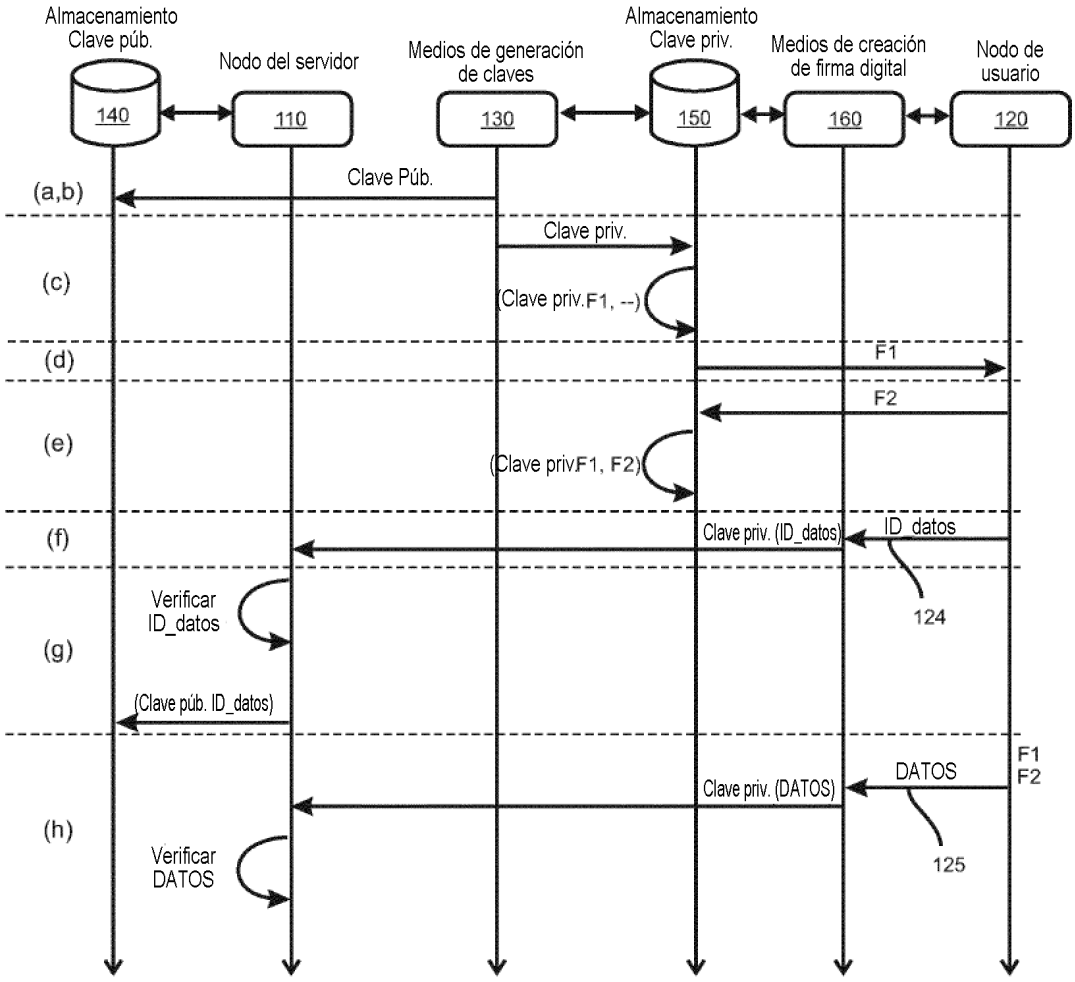
Almacenamiento Clave púb.
140
Nodo del servidor
110
Medios de generación de claves
130
Almacenamiento Clave priv.
150
Medios de creación de firma digital
160
Nodo de usuario
120
(a,b)
Clave Púb.
Clave priv.
(c)
(Clave priv.F1, --)
(d)
F1
F2
(e)
(Clave priv.F1, F2)
(f)
Clave priv. (ID_datos)
ID_datos
124
Verificar ID_datos
(g)
(Clave púb. ID_datos)
F1
F2
DATOS
Clave priv. (DATOS)
125
(h)
Verificar DATOS

Fig. 1

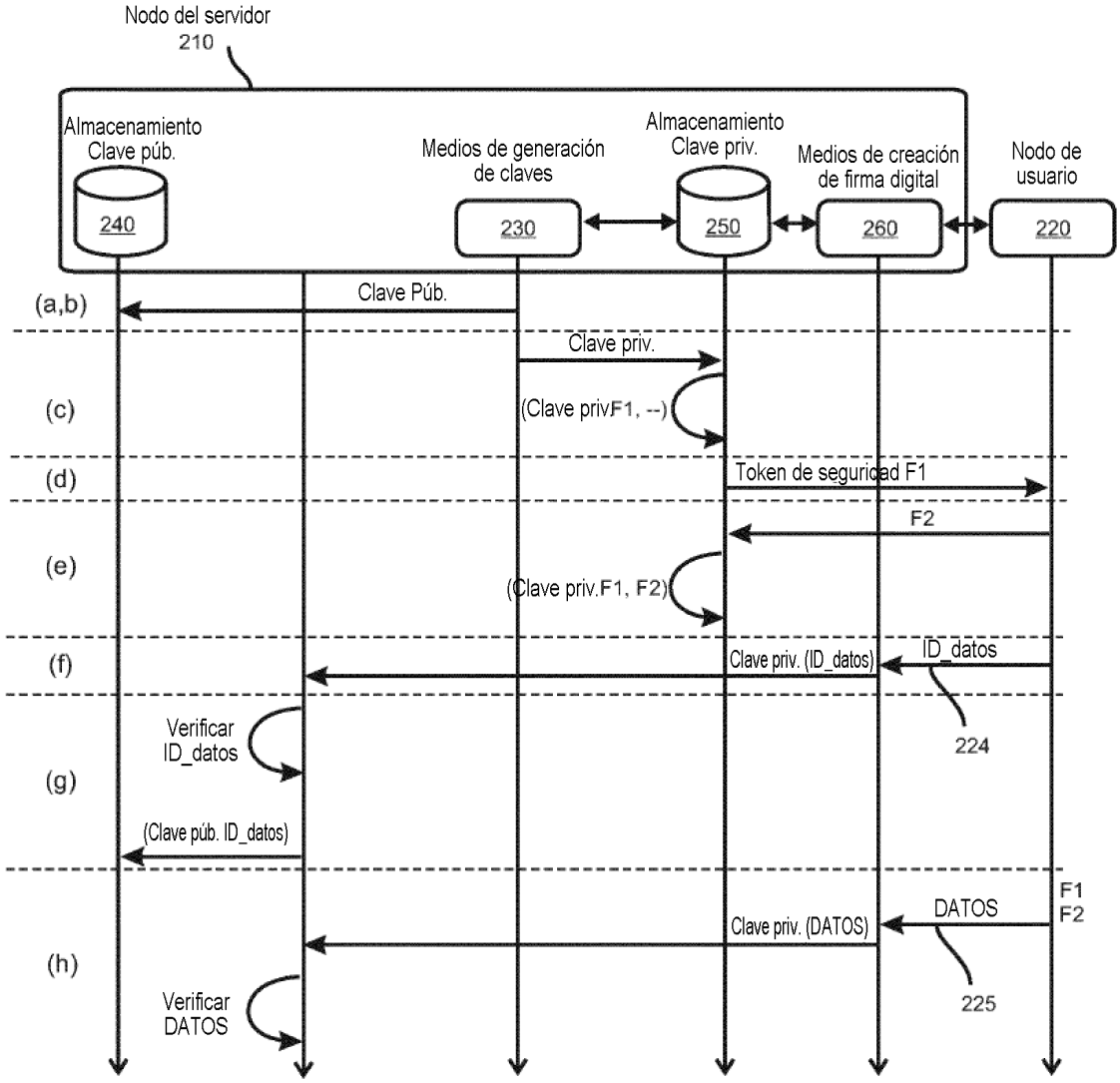
Nodo del servidor
210
Almacenamiento
Clave púb.
240
Medios de generación
de claves
230
Almacenamiento
Clave priv.
250
Medios de creación
de firma digital
260
Nodo de
usuario
220
(a,b)
Clave Púb.
Clave priv.
(c)
(Clave privF1, --)
(d)
Token de seguridad F1
F2
(e)
(Clave priv.F1, F2)
(f)
Clave priv. (ID_datos)
ID_datos
224
Verificar
ID_datos
(g)
(Clave púb. ID_datos)
F1
F2
DATOS
Clave priv. (DATOS)
(h)
225
Verificar
DATOS

Fig. 2

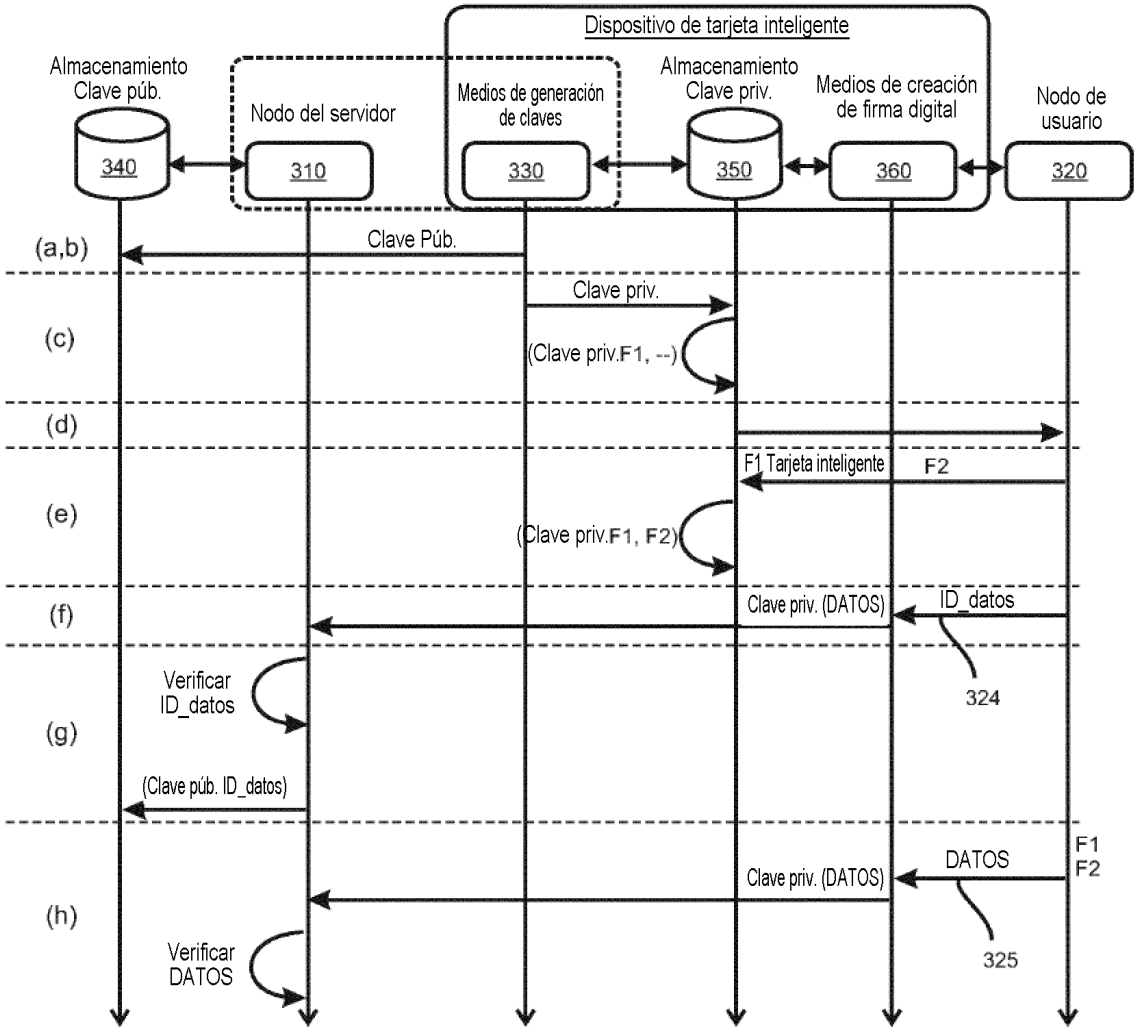
Dispositivo de tarjeta inteligente
Almacenamiento Clave púb.
Nodo del servidor
Medios de generación de claves
Almacenamiento Clave priv.
Medios de creación de firma digital
Nodo de usuario
340
310
330
350
360
320
(a,b)
Clave Púb.
Clave priv.
(c)
(Clave priv.F1, --)
(d)
F1 Tarjeta inteligente
F2
(e)
(Clave priv.F1, F2)
(f)
Clave priv. (DATOS)
ID_datos
324
Verificar ID_datos
(g)
(Clave púb. ID_datos)
F1
F2
DATOS
Clave priv. (DATOS)
(h)
325
Verificar DATOS

Fig. 3

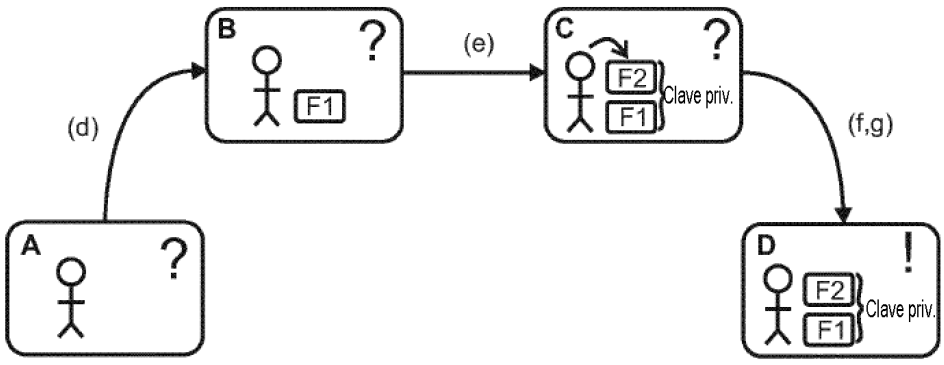
A
B
C
D
F1
F2
Clave priv.
(d)
(e)
(f,g)

Fig. 4