(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 377**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.04.2015 E 15162466 (5)**

(97) Fecha y número de publicación de la concesión europea: **09.10.2019 EP 3076583**

(54) Título: **Gestión central de certificados**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.06.2020

(73) Titular/es:

Totemo AG (100.0%)
Freihofstrasse 22
8700 Küsnacht, CH

(72) Inventor/es:

MOCK, MARCEL

(74) Agente/Representante:

CURELL SUÑOL, S.L.P.

DESCRIPCIÓN

Gestión central de certificados.

Campo de la invención

La presente invención se refiere a la gestión central de certificados.

Descripción de técnica anterior

La S/MIME es una norma común usada para el cifrado de correos electrónicos entre un remitente y un destinatario. La S/MIME es un cifrado asimétrico que utiliza un par de una clave pública y una clave privada. La clave pública del destinatario es proporcionada a todos los remitentes para cifrar correos electrónicos enviados al destinatario. No obstante, solamente el destinatario tiene la clave privada correspondiente necesaria para descifrar el correo electrónico cifrado del remitente. Con el fin de garantizar, en el lado del remitente, que la clave pública proviene realmente del destinatario y no de un tercero, la clave pública se transmite en un certificado, por ejemplo, con la norma X.509. El certificado comprende la clave pública del destinatario, un campo de emisor con información sobre un emisor fiable del certificado y un campo de sujeto con información del destinatario. Finalmente, el certificado se firma digitalmente por medio de un certificado correspondiente al emisor. La figura 1 muestra una situación del tipo mencionado, en la que el destinatario envía un certificado con su clave pública. El remitente comprueba la validez del certificado. Esto se realiza comprobando la firma del certificado recibido sobre la base del certificado correspondiente al emisor, usado para firmar el certificado correspondiente al destinatario, y comprobando si en una lista de certificados de confianza se encuentra una copia del certificado correspondiente al emisor. Si se confirma su validez, la clave pública se usa para cifrar un mensaje, por ejemplo, un correo electrónico. Finalmente, el mensaje cifrado se envía al destinatario el cual, a continuación, puede descifrar el mensaje por medio de su clave privada correspondiente.

No obstante, con frecuencia los certificados del destinatario no son emitidos/firmados directamente por un emisor fiable, sino por los denominados intermediarios cuya fiabilidad queda garantizada, entonces, por otro emisor. La figura 2 muestra una cadena de certificación del tipo mencionado. Un emisor raíz tiene un certificado que, normalmente, está firmado por él mismo, es decir, el campo de emisor y el campo de sujeto son idénticos para el certificado raíz. El emisor raíz emite un certificado correspondiente a un intermediario, firmado con el certificado correspondiente al emisor raíz. El campo de emisor del certificado de intermediario contiene el emisor raíz y el campo de sujeto del certificado de intermediario contiene el intermediario. A continuación, el intermediario puede emitir el certificado correspondiente al destinatario, firmado con el certificado correspondiente al intermediario. El campo de emisor del certificado correspondiente al destinatario contiene el intermediario, y el campo de sujeto del certificado correspondiente al destinatario contiene el destinatario. El número de niveles entre el destinatario y el emisor raíz es arbitrario. Al certificado raíz se le denomina también ancla de confianza de dicha cadena de certificación. A esto se le denomina, también, ruta de certificación o cadena de certificación.

La figura 3 muestra, a continuación, el proceso de validación de la cadena de certificación. Cuando el cliente de mensajería recibe el certificado correspondiente al destinatario, el mismo va subiendo por la jerarquía de los certificados, hasta que se encuentra un ancla de confianza. El ancla de confianza es el primer certificado de la cadena de certificación cuya copia se encuentra en la lista de certificados de confianza. Normalmente es el certificado raíz, aunque también puede ser un certificado de intermediario que se encuentre en la lista de certificados de confianza. Por lo tanto, todos los certificados de la cadena (hasta el ancla de confianza) deben estar presentes en el remitente. La información del siguiente nivel superior se puede encontrar en el propio certificado. Si el certificado del siguiente nivel superior no está presente, en algunos casos el mismo se puede descargar de una ubicación de acceso predeterminada basándose en una extensión de Acceso a Información de Autoridad (AIA). A este proceso se le denomina construcción de la cadena. Si no se encuentra ningún ancla de confianza, no puede comprobarse la validez de la cadena de certificación. Si se encuentra un ancla de confianza, es decir, en caso de que, en la lista de certificados de confianza, esté el certificado raíz o un certificado de intermediario, la validez de la cadena de certificación se controla por medio del proceso denominado de validación de cadena. Tal como se muestra en la figura 2, a continuación se comprueba la validez de cada certificado de la cadena de certificación comenzando desde arriba hacia abajo sobre la base del siguiente certificado superior, respectivamente. Entre otros aspectos, la autenticación se comprueba sobre la base del siguiente certificado superior, y se comprueba si el campo de emisor se corresponde con el siguiente campo de sujeto superior. En este caso, la firma del certificado correspondiente al intermediario se controla sobre la base de la firma del certificado correspondiente al certificado raíz (en este caso el ancla de confianza). A continuación, la firma del certificado correspondiente al destinatario se controla sobre la base de la firma del certificado correspondiente al intermediario. Si la validación resultase satisfactoria, un mensaje se puede cifrar con el certificado del destinatario. No obstante, este proceso es complejo y propenso a errores. Son errores comunes que no se encuentre ningún ancla de confianza y que la cadena de certificación no se pueda construir debido a la ausencia de certificados y debido a la ausencia de información de AIA. El AIA es opcional y, por lo tanto, normalmente está ausente en los certificados.

Especialmente para grandes compañías con muchos clientes de mensajería, es deseable gestionar los certificados correspondientes a los destinatarios en un servidor de gestión central de certificados. Esto hace que se reduzca el esfuerzo administrativo y hace que mejore el control. No obstante, en muchos sistemas de mensajería, el mensaje solamente se cifra cuando pasa por la pasarela del sistema interno. Por lo tanto, el mensaje podría ser interceptado fácilmente entre el remitente y la pasarela del sistema de mensajería. Resultaba deseable cifrar también el mensaje entre el remitente y la pasarela. En el documento EP1536601 se propuso cifrar el mensaje entre el remitente y la pasarela por medio de un certificado proforma correspondiente al destinatario, con una clave pública diferente que la del certificado correspondiente al destinatario. Esto permitía descifrar el mensaje en la pasarela, llevar a cabo algunas operaciones sobre el mensaje y a enviar el mensaje cifrado con el certificado verdadero correspondiente al destinatario desde la pasarela al destinatario. Esto permite un cifrado desde el remitente al destinatario.

No obstante, hay situaciones en las que resulta deseable materializar, para una gestión central de certificados, un cifrado de extremo-a-extremo desde el remitente al destinatario sin ningún cambio de cifrado en la pasarela, por ejemplo, para una mayor seguridad. La figura 4 muestra una situación de este tipo. El servidor de gestión central de certificados 4, tras una solicitud de un cliente de mensajería remitente, envía al remitente un certificado correspondiente al destinatario. El remitente comprueba la validez del certificado según se ha descrito anteriormente, cifra el mensaje con la clave pública contenida en el certificado correspondiente al destinatario, y envía el mensaje cifrado al destinatario. El problema de este planteamiento es que el servidor central de gestión 4 devuelve solamente el certificado correspondiente al destinatario. El cliente de mensajería remitente tiene que seguir llevando a cabo la construcción de la cadena, recuperar todos los certificados de nivel superior, si los mismos no están ya presentes, y llevar a cabo la validación de la cadena. Consecuentemente, la carga administrativa principal sigue encontrándose en los clientes de mensajería remitentes y el proceso es igualmente propenso a errores como en una gestión descentralizada de certificados.

Surgen problemas similares a la hora de comprobar la validez de firmas de mensajes sobre la base de un certificado correspondiente a un remitente. En general, la comprobación de la validez de certificados de sujetos del estado de la técnica es propensa a errores y compleja.

El documento US2006/0282670 divulga un sistema para autorizar solicitudes de usuario mediante una combinación de credenciales de usuario y un certificado de usuario. Se sugiere cambiar el proceso de validación para el certificado de usuario, de tal manera que también se acepten certificados de usuario autofirmados.

El documento US2002/0147905 divulga el acortamiento de cadenas de certificación largas por parte de la autoridad de ancla de confianza.

El documento US2003/0163687 divulga un proceso alternativo de validación de certificados que evita el certificado del ancla de confianza.

Breve sumario de la invención

Es un objetivo de la invención proporcionar una gestión de certificados para sujetos que reduce los errores en los clientes.

Esto se resuelve por medio de las reivindicaciones independientes, especialmente transmitiendo, desde un sistema de gestión de certificados a un cliente, en lugar del certificado verdadero del sujeto, otro certificado con la misma clave pública, el mismo campo de emisor y el mismo campo de número de serie, pero firmado con otro certificado. Esto permite que múltiples sujetos con varias anclas de confianza diferentes para sus certificados usen siempre la misma ancla de confianza dentro del sistema de gestión de certificados. Por lo tanto, el número de anclas de confianza que se deben descargar, almacenar y comprobar en los clientes puede reducirse a una. Puesto que el proceso de recuperación de certificados de terceros normalmente falla, esta solución reduce enormemente los errores para comprobar la validez de un certificado en un cliente.

Las reivindicaciones dependientes se refieren a otras formas de realización ventajosas.

En una forma de realización, la etapa de llevar a cabo una acción sobre la base de la primera clave pública del segundo certificado correspondiente al primer sujeto incluye cifrar un mensaje con la clave pública del segundo certificado correspondiente al primer sujeto y enviar el mensaje cifrado al primer sujeto.

En una forma de realización, la etapa de llevar a cabo una acción sobre la base de la primera clave pública del segundo certificado correspondiente al primer sujeto incluye comprobar una firma digital de un documento sobre la base de la clave pública del segundo certificado correspondiente al primer sujeto.

En una forma de realización el/los cliente(s) es/son cliente(s) de correo electrónico.

En una forma de realización, el primer certificado correspondiente al sujeto y el segundo certificado

correspondiente al sujeto son certificados x.509. Estos certificados se configuran para cifrar un correo electrónico cifrado con S/MIME y/o para comprobar la firma de un correo electrónico.

Breve descripción de los dibujos

La invención se entenderá mejor con la ayuda de la descripción de una forma de realización aportada a título de ejemplo e ilustrada por medio de las figuras, en las cuales:

la figura 1 muestra un proceso de la técnica anterior para un cifrado de extremo-a-extremo con gestión descentralizada de certificados;

la figura 2 muestra un proceso de la técnica anterior para generar y validar una cadena de certificación;

la figura 3 muestra un proceso de la técnica anterior para la construcción de cadenas de certificación;

la figura 4 muestra un sistema de la técnica anterior para un cifrado de extremo-a-extremo con gestión centralizada de certificados;

la figura 5 muestra una forma de realización de un sistema de mensajería con gestión centralizada de certificados;

la figura 6 muestra una sustitución del primer certificado correspondiente al destinatario por un segundo certificado correspondiente al destinatario en un sistema de gestión de certificación;

la figura 7 muestra una primera forma de realización correspondiente a un procedimiento para la gestión centralizada de certificados;

la figura 8 muestra una forma de realización para un cifrado de extremo-a-extremo con gestión centralizada de certificados;

la figura 9 muestra una forma de realización para comprobar la validez de una firma con gestión centralizada de certificados; y

la figura 10 muestra una segunda forma de realización correspondiente a un procedimiento para gestión centralizada de certificados.

Descripción detallada de posibles formas de realización de la invención

Antes de describir posibles formas de realización de la invención, se definirán más detalladamente los siguientes términos.

Un par de claves consiste en una clave pública y una clave privada. La clave pública se puede usar para cifrar un mensaje o documento para el propietario de la clave privada y/o para comprobar la autenticación de un mensaje o documento firmado con la clave privada. La clave privada correspondiente se puede usar para descifrar un mensaje o documento cifrado con la clave pública y/o para firmar digitalmente un mensaje o documento con una clave privada.

Un cifrado asimétrico será cualquier cifrado que use un par de claves, es decir, que use una clave pública para el cifrado y una clave privada para el descifrado. Esto incluye, también, procedimientos de cifrado híbridos como, por ejemplo, el S/MIME que cifra el mensaje o documento con una clave simétrica (creada aleatoriamente), cifra la clave simétrica con la clave pública, descifra la clave simétrica con la clave privada y descifra el mensaje de documento con la clave simétrica descifrada.

El término firma o firmar se usa, en la presente memoria, en el sentido de una firma digital de un mensaje o documento electrónico. Por lo tanto, el mensaje o documento se firma con una clave privada de un par de claves. Esto permite autenticar el mensaje o documento mediante la clave pública de dicho par de claves. Normalmente, las claves públicas usadas para la autenticación de una firma están contenidas en un certificado. Por motivos de brevedad, en esta invención la fórmula “firmar un documento (normalmente otro certificado) con/mediante un certificado” se usa en el sentido de “firmar un documento (normalmente otro certificado) con la clave privada correspondiente a la clave pública contenida en el certificado”.

Un certificado contiene datos de certificado y una firma. Los datos de certificado comprenden una clave pública de un par de claves, un campo de emisor y un número de serie. Los datos de certificado se firman con otro certificado correspondiente al emisor indicado en el campo de emisor de los datos de certificado. La combinación de los datos de certificado y la firma proporciona el certificado. El campo de emisor identifica la entidad que ha firmado y emitido el certificado. Este podría ser un nombre del emisor, preferentemente un nombre distinguido

(DN) no vacío, un código de identificación/número del emisor, la dirección postal del emisor, la dirección electrónica del emisor (por ejemplo, correo electrónico o dirección de internet), etc., o cualquier combinación o subcombinación de las mencionadas. Al emisor también se le denomina, en ocasiones, Autoridad de Certificación (CA). El campo de número de serie identifica el certificado entre los certificados emitidos por el emisor indicado en el campo de emisor. En una forma de realización, el número de serie es un entero positivo. No obstante, en otras formas de realización, el campo de número de serie podría contener también códigos alfanuméricos y/o enteros negativos. En una forma de realización, el certificado sigue la norma X.509 del Sector de Normalización de la Unión Internacional de Telecomunicaciones (ITU-T) que se incluye en la presente memoria a título de referencia. En una forma de realización, el certificado sigue la estructura definida en la rfc5280 de la versión de mayo de 2008, que se incluye en la presente memoria a título de referencia y en la cual a los datos de certificado se les hace referencia como TBSCertificate. Los datos de certificado pueden contener otros campos. En una forma de realización, los datos de certificado podrían contener un campo de sujeto que identifica la entidad (sujeto) asociada a la clave pública almacenada en los datos de certificado. El nombre del sujeto se puede incluir en el campo de sujeto y/o una extensión como la extensión subjectAltName. En lo sucesivo, cuando hablamos sobre el campo de sujeto, se incluyen las dos posibilidades. El campo de sujeto podría ser un nombre del sujeto, un código de identificación/número del sujeto, la dirección postal del sujeto, la dirección electrónica del sujeto (por ejemplo, correo electrónico o dirección de internet), etc., o cualquier combinación o subcombinación de las anteriores. Incluso si la RFC5280 considera dos campos distintos para el nombre de sujeto y para la dirección de correo electrónico del sujeto, los mismos no se tratarán por separado en la presente. Posibles campos adicionales de los datos de certificados son un campo de versión con la versión de la norma del certificado, un campo de ID de algoritmo, un campo de validez con un periodo de validez correspondiente al certificado, un campo de algoritmo de clave pública que indica el algoritmo usado para el par de claves, un campo de extensión o varios campos de extensión. Una de las posibles extensiones es la extensión de Acceso a Información de Autoridad (AIA). Esta extensión contiene la dirección de acceso para descargar el certificado correspondiente al emisor del certificado, que permite que un cliente de mensajería descargue automáticamente el certificado del emisor, si es que no está presente ya en el cliente de mensajería. La extensión de AIA podría ser un Identificador Uniforme de Recursos (URI) de HTTP o un URI del Protocolo Ligero de Acceso a Directorios (LDAP) o un URI del FTP u otras direcciones de protocolo. El AIA puede apuntar a un archivo .cer, es decir, un certificado codificado por DER individual según se especifica en la RFC 2585 (este contiene normalmente el certificado de emisor) o a un archivo .p7c, es decir, un mensaje CMS “certs-only” según se especifica en la RFC 2797. El .p7c puede contener uno o más certificados; esto significa que podría contener el certificado de emisor de emisores (*issuers issuer certificate*), ..., e incluso el certificado raíz. Se definen detalles sobre la extensión de AID en la RFC 4325, que se incorpora a la presente memoria a título de referencia. Una extensión de AIA también se podría configurar para descargar también diversos certificados de una cadena de certificación. También es posible añadir diversas extensiones de AIA para diferentes certificados.

Una cadena de certificación comprende por lo menos dos certificados en diferentes niveles. Cada certificado en el nivel uno es emitido por el propietario del certificado del siguiente nivel superior y se firma con el certificado del siguiente nivel superior excepto para el certificado que se encuentra en el nivel más alto (=certificado raíz). El campo de emisor de cada certificado coincide con el campo de sujeto del certificado del nivel superior excepto para el certificado que se encuentra en el nivel más alto. El certificado del nivel más alto, denominado también certificado raíz, es normalmente emitido por él mismo y/o es firmado por él mismo. Los detalles correspondientes a la validación de una cadena de certificación ya se han explicado en el contexto de la figura 2 y 3 y no se repiten por motivos de brevedad.

Si las reivindicaciones mencionan una primera cosa cualquiera, esto no implicará que también exista una segunda cosa cualquiera a no ser que dicha segunda cosa cualquiera se defina explícitamente en esta reivindicación.

La figura 5 muestra una forma de realización correspondiente a un sistema de mensajería que comprende una pluralidad de clientes de mensajería 11, 12, 13, un sistema de gestión de certificados 31 y una pluralidad de sujetos 21, 22.

La pluralidad de clientes de mensajería 11, 12, 13 están configurados, cada uno de ellos, para validar un certificado correspondiente a un sujeto 21, 22, y para llevar a cabo una acción sobre la base de la clave pública del certificado validado correspondiente al sujeto 21, 22. Dicha acción podría ser cifrar un mensaje correspondiente al destinatario como sujeto 21, 22 sobre la base de los certificados validados correspondientes al destinatario 21, 22 y enviar el mensaje cifrado al destinatario 21, 22. En otra forma de realización, la acción podría ser comprobar la validez de una firma, por ejemplo, de un mensaje recibido de un remitente como sujeto 21, 22, sobre la base de la clave pública del certificado correspondiente al sujeto 21, 22. En este último caso, el sujeto 21, 22 podría ser el remitente de un mensaje firmado digitalmente con el certificado correspondiente al sujeto. No obstante, también son posibles cualesquiera otras acciones sobre la base de la clave pública del certificado correspondiente al sujeto. En una forma de realización, la pluralidad de clientes de mensajería 11, 12, 13 están configurados, cada uno de ellos, para solicitar un certificado correspondiente a un sujeto 21, 22, si el mismo fuera necesario. Esta solicitud se puede enviar a unos medios de almacenamiento locales para certificados o al sistema de gestión de certificados 31. En una forma de realización, la pluralidad de clientes de

mensajería 11, 12, 13 están configurados, cada uno de ellos, para almacenar certificados correspondientes a sujetos 21, 22 localmente, y para comprobar, antes de llevar a cabo dicha acción, si un certificado válido correspondiente a un sujeto deseado 21, 22 está almacenado en el cliente de mensajería 11, 12, 13. Si hay presencia de dicho certificado, la validación y/o la acción se puede llevar a cabo sin contactar con el sistema de gestión de certificados 31. En caso contrario, se envía una solicitud del certificado correspondiente al sujeto 21, 22 al sistema de gestión de certificados 31 desde el cual el cliente de mensajería solicitante 11, 12, 13 recibirá el certificado solicitado correspondiente al sujeto 21, 22. En otra forma de realización, los certificados no se almacenan localmente, y cada vez que el cliente de mensajería 11, 12, 13 desea enviar un mensaje cifrado a un destinatario 21, 22 o desea llevar a cabo otra acción en relación con un sujeto 21, 22, es necesario que el cliente de mensajería 11, 12, 13 envíe una solicitud correspondiente al sistema de gestión de certificados 31. En una forma de realización, los clientes de mensajería están configurados, cada uno de ellos, para recibir un certificado correspondiente a un sujeto 21, 22 del sistema de gestión de certificados 31. Esto se puede materializar también mediante una respuesta a la solicitud antes mencionada. No obstante, son posibles también otras formas de recibir un certificado, por ejemplo, mediante un mensaje enviado sin solicitud previa (*push*) del servidor, un mensaje con una tarjeta *V-card* que contenga el certificado, o un mensaje con un certificado adjunto. Los clientes de mensajería 11, 12, 13 pueden ser diferentes dispositivos, como ordenadores, ordenadores portátiles de tipo *notebook*, paneles táctiles, teléfonos inteligentes, o cualquier otro dispositivo configurado para trabajar con un *software* de cliente de mensajería. Los clientes de mensajería 11, 12, 13 pueden referirse, por ejemplo, a distintos usuarios. Dos o más de los clientes de mensajería 11, 12, 13 también pueden estar dispuestos en el mismo dispositivo, por ejemplo, para diferentes usuarios. En una forma de realización, los clientes de mensajería 11, 12, 13 son clientes de correo electrónico. La figura 5 muestra solamente tres clientes de mensajería ejemplificativos. No obstante, resulta evidente que la pluralidad de clientes de mensajería 11, 12, 13 gestionados por el sistema de gestión de certificados 31 puede tener un número cualquiera de clientes de mensajería 11, 12, 13.

El sistema de gestión de certificados 31 está configurado para gestionar certificados para la pluralidad de clientes de mensajería 11, 12, 13. El sistema de gestión de certificados 31 está configurado para recibir un primer certificado correspondiente a un sujeto 21, 22 (véase también la etapa S1, S1'' posteriormente). El sistema de gestión de certificados 31 está configurado para generar un segundo certificado correspondiente a dicho sujeto 21, 22 para el cual se recibió el primer certificado (véanse más detalles con la etapa S3, S3'' posteriormente). El sistema de gestión de certificados 31 está configurado para transmitir el segundo certificado correspondiente al sujeto 21, 22 (véase también la etapa S4, S4'' posteriormente) a por lo menos uno de la pluralidad de clientes de mensajería 11, 12, 13. En una forma de realización, el sistema de gestión de certificados 31 está configurado para recibir una solicitud de un certificado correspondiente al sujeto 21, 22 desde uno de la pluralidad de clientes de mensajería 11, 12, 13 (véase también la etapa S2'' posteriormente). En una forma de realización, el sistema de gestión de certificados 31 está configurado para almacenar, para todos los sujetos 21, 22, los segundos certificados generados. Esto tiene la ventaja de que si el mismo cliente de mensajería u otro 11, 12, 13 solicita el certificado correspondiente a un sujeto 21, 22, para el cual ya se generó el segundo certificado, puede evitarse una nueva generación del segundo certificado correspondiente al sujeto 21, 22 y se puede recuperar el mismo segundo certificado generado previamente que se almacenó en el sistema de gestión de certificados 31 y este puede ser devuelto al cliente de mensajería solicitante 11, 12, 13. Sin embargo, la invención no se limitará a esto, y el sistema de gestión de certificados 31 también podría crear los segundos certificados correspondientes a los sujetos 21, 22 cada vez, cuando ello fuese necesario. El sistema de gestión de certificados 31 se puede implementar en uno o varios dispositivos de procesado, como un ordenador, un servidor, electrodomésticos, dispositivos pequeños como el *raspberry PI* y otros dispositivos de procesado.

En una forma de realización, la totalidad de la pluralidad de clientes de mensajería 11, 12, 13 y/o sus dispositivos respectivos pueden estar dispuestos en una red interna, como una Red de Área Local (LAN) o una LAN Inalámbrica (WLAN), de manera que no se necesita ninguna red externa, como internet o una red de telefonía móvil (GSM, GPRS, UMTS, LTE, etc.) para contactar con el sistema de gestión de certificados 31. En otra forma de realización, algunos o la totalidad de los clientes de mensajería 11, 12, 13 se conectan por medio de una red externa al sistema de gestión de certificados 31. También es posible que diferentes subgrupos de clientes de correo electrónico 11, 12, 13 estén dispuestos en redes internas distintas, presentando cada red interna distinta (o por lo menos algunas de ellas) uno o más servidores de gestión de certificados para gestionar los certificados correspondientes al subgrupo de clientes de mensajería 11, 12, 13 conectados en esta red interna. Los diferentes servidores de gestión de certificados correspondientes a los diferentes subgrupos forman juntos el sistema de gestión de certificados 31. En una forma de realización, diferentes servidores de gestión de certificados del mismo sistema de gestión de certificados 31 podrían sincronizar sus segundos certificados almacenados correspondientes a los destinatarios solicitados.

Los sujetos 21, 22 son las entidades asociadas a la clave pública almacenada en el certificado correspondiente al sujeto 21, 22. Técnicamente, un dispositivo o una aplicación está relacionada normalmente con dicho sujeto, por ejemplo, mediante un *log-in* de usuario. En una forma de realización de cifrado de extremo-a-extremo, los sujetos 21, 22 se corresponden con destinatarios de los mensajes cifrados. Los mensajes se envían a direcciones de mensaje relacionadas con el destinatario 21, 22. El dispositivo o cliente de mensajería de los destinatarios 21, 22 que recibe dicho mensaje cifrado están configurados para recibir mensajes, con el fin de

descifrar mensajes cifrados con su clave pública sobre la base de la clave privada correspondiente del par de claves correspondiente. En una forma de realización, el cliente del destinatario 21, 22 está configurado para identificar el certificado usado para cifrar el mensaje. Esto último se podría realizar comprobando información del certificado usado para el cifrado, la cual está incluida en el mensaje cifrado. En una forma de realización, el campo de emisor y el campo de número de serie del certificado se incluyen en el mensaje cifrado y se usan para comprobar el mensaje cifrado en el cliente del destinatario. Esto es así, por ejemplo, para los mensajes cifrados con S/MIME, en particular para correos electrónicos cifrados con S/MIME. No obstante, también es posible que el cliente del destinatario simplemente pruebe todas las claves privadas disponibles para descifrar el mensaje. En otra forma de realización, el sujeto 21, 22 es en realidad un remitente de un mensaje que firma el mensaje con un primer certificado correspondiente al sujeto 21, 22. En una forma de realización, el cliente de sujeto 21, 22 no es gestionado por el sistema de gestión de certificados 31, es decir, es un sujeto externo 21, 22. No obstante, también es posible que el cliente del sujeto 21, 22 sea uno de la pluralidad de clientes de mensajería 11, 12, 13 gestionados por el sistema de gestión de certificados 31.

La figura 7 muestra una primera forma de realización de un procedimiento para una gestión central de certificados. Las etapas también se muestran parcialmente en la figura 5.

En una etapa S1, el sistema de gestión de certificados 31 recibe un primer certificado correspondiente a un primer sujeto 21. Hay muchas formas según las cuales se puede recibir el primer certificado correspondiente al primer destinatario 21, y la invención no se limita a una de ellas. En una forma de realización, el primer certificado correspondiente al primer sujeto 21 se podría recibir del primer sujeto 21. El primer certificado del primer sujeto 21 se podría recibir directamente por una solicitud proveniente del sistema de gestión de certificados 31, por ejemplo, tras una solicitud de uno de los clientes de mensajería 11, 12, 13, hacia el primer sujeto 21 u otro dispositivo que ofrezca el certificado del primer sujeto 21, por ejemplo, un sistema de gestión de certificados del primer sujeto 21. En una forma de realización, el primer certificado correspondiente al primer sujeto puede ser un anexo de un mensaje enviado a uno de la pluralidad de clientes de mensajería 11, 12, 13. En este caso, una pasarela del sistema de mensajería o del sistema de gestión de certificados 31 podría interceptar o recolectar dicho primer certificado correspondiente al primer sujeto antes de que el mismo llegue a uno de los clientes de mensajería 11, 12, 13. A un proceso de este tipo se le denomina “recolección de certificados”. Por lo tanto, se evita que el cliente de mensajería 11, 12, 13 pueda almacenar el primer certificado del primer sujeto 21. No obstante, también es posible que el sistema de gestión de certificados 31 reciba el certificado correspondiente al primer sujeto 21 de uno de los clientes de mensajería 11, 12, 13 que lo recibió del primer sujeto 21. El primer certificado correspondiente al primer sujeto 21 se puede recibir en cualquier momento, es decir, antes o después o sin recibir una solicitud del certificado correspondiente al primer sujeto 21. La figura 2 muestra una cadena de certificación ejemplificativa del primer certificado 41 correspondiente al primer sujeto 21. El primer certificado 41 correspondiente al primer sujeto 21 se firma con un primer certificado correspondiente a un intermediario (como primer emisor). El primer certificado 45 correspondiente al intermediario se firma con un certificado raíz 46. No obstante, esto es solamente ejemplificativo, y el primer certificado 41 también se podría firmar directamente con un certificado raíz, o la cadena de certificación podría contener niveles adicionales.

En una etapa opcional S2, un primer cliente de mensajería 11 (uno de la pluralidad de clientes de mensajería) desea enviar un mensaje cifrado, por ejemplo, un correo electrónico, al primer sujeto 21 como destinatario. Preferentemente, en primer lugar el mismo comprueba localmente si, en el cliente de mensajería 11, hay almacenado un certificado válido correspondiente al primer sujeto 21. Si esto es así, el procedimiento podría saltar a la etapa S5. De lo contrario, el primer cliente de mensajería 11 envía una solicitud de un certificado correspondiente al primer sujeto 21. El sistema de gestión de certificados 31 recibe la solicitud de un certificado correspondiente al primer sujeto 21 del primer cliente de mensajería 11. Dicha solicitud podría ser una solicitud LDAP, aunque también es posible cualquier otro tipo de solicitud como EWS (Servicios Web de Exchange), WebDAV, ActiveSync, RPC sobre HTTP, SMP o FTP, etc. Tal como se ha mencionado anteriormente, una solicitud de este tipo no es obligatoria para la invención y el cliente de mensajería podría recibir el segundo certificado generado en S3 también sin ninguna solicitud previa.

En la etapa S3, el sistema de gestión de certificados 31 genera un segundo certificado correspondiente a dicho primer destinatario 21.

La figura 6 muestra una forma de realización del proceso de generación del segundo certificado 42 correspondiente al primer sujeto 21 sobre la base del primer certificado 41 correspondiente al primer sujeto 21. El segundo certificado generado 42 correspondiente al primer sujeto 21 comprende la misma clave pública leída del primer certificado 41 correspondiente al primer sujeto 21, pero está firmada con otro certificado 43 diferente al primer certificado 41 correspondiente al primer sujeto 21. Preferentemente, por lo menos una parte de la otra información de los datos de certificado del primer certificado 41 correspondiente al primer sujeto 21 se leen y se escriben en los datos de certificado del segundo certificado 42 correspondiente al primer sujeto 21. En una forma de realización, el contenido del campo de número de serie del primer certificado 41 se copia en el campo de número de serie del segundo certificado 42. En una forma de realización, el contenido del campo de emisor del primer certificado 41 se copia en el campo de emisor del segundo certificado 42. En una forma de realización, el contenido del campo de sujeto del primer certificado 41 se copia en el campo de sujeto del segundo certificado

42. En una forma de realización, el contenido del campo de validez del primer certificado 41 se copia en el campo de validez del segundo certificado 42. En una forma de realización, el contenido del campo de algoritmo de clave pública del primer certificado 41 se copia en el campo de algoritmo de clave pública del segundo certificado 42. En una forma de realización, el contenido de campos de extensión del primer certificado 41 se copia en los campos de extensión del segundo certificado 42. No obstante, el campo de extensión de AIA del primer certificado 41, en caso de que estuviera presente, preferentemente no se copia en el segundo certificado 42. En una forma de realización, un campo de extensión de AIA del segundo certificado 42 se genera con la dirección de acceso para descargar el segundo certificado 43 correspondiente al primer emisor. Teóricamente, la extensión de AIA generada o una extensión de AIA adicional podría incluir información de acceso para descargar el certificado raíz 44. No obstante, en la mayoría de clientes de mensajería 11, 12, 13, el ancla de confianza debe estar disponible localmente en la lista de certificados de confianza. Por lo tanto, en muchas formas de realización se prefiere generar solamente la información de AIA del segundo certificado 43 correspondiente al primer emisor.

Cuando los datos de certificado del segundo certificado 42 correspondiente al primer sujeto 21 se han completado, el segundo certificado 42 se firma con el segundo certificado 43 correspondiente al intermediario (primer emisor). Incluso si el campo de sujeto del certificado 43 contiene el intermediario y/o se corresponde con el campo de emisor del certificado 42, no es el mismo que el primer certificado 45 correspondiente al intermediario. Puesto que el sistema de gestión de certificados 31 no conoce la clave privada que se corresponde con la clave pública del primer certificado 45 correspondiente al intermediario, el sistema de gestión de certificados 31 genera también un nuevo segundo certificado 43 correspondiente al intermediario con un nuevo par de claves. Si el segundo certificado 43 ya se generó previamente, el mismo también se podría generar simplemente recuperándolo de unos medios de almacenamiento en lugar de crearlo de nuevo. Por lo tanto, el segundo certificado 42 correspondiente al primer sujeto 21 se puede firmar con el segundo certificado 43 correspondiente al intermediario. El segundo certificado 43 correspondiente al intermediario podría ser directamente un certificado raíz. No obstante, se prefiere que el segundo certificado 43 correspondiente al intermediario se firme con un certificado raíz 44 (diferente del certificado raíz 46). De este modo, el sistema de gestión de certificados 31 dispone de la clave privada que se corresponde con el certificado raíz 44 con el fin de firmar el segundo certificado 43 correspondiente al intermediario, con el certificado raíz 44. El campo de emisor del segundo certificado 43 correspondiente al intermediario debería corresponderse con el contenido del campo de sujeto del certificado raíz. La sustitución de la ruta de certificación/certificado raíz 46 del primer certificado 41 correspondiente al primer sujeto 21 por la ruta de certificación/el certificado raíz 44 del segundo certificado 42 correspondiente al primer sujeto 21, tiene la ventaja de que, en la totalidad de los clientes de mensajería 11, 12, 13, solamente debe incluirse el certificado raíz único 44 en la lista de certificados de confianza. Puesto que la mayoría de los errores en sistemas de la técnica anterior son debidos a certificados raíz ausentes o que no son de confianza, esto permite reducir los errores para el tratamiento de certificados en los clientes de mensajería 11, 12, 13. En una forma de realización, un campo de extensión de AIA del segundo certificado 43 correspondiente al intermediario se genera con la dirección de acceso para descargar el certificado raíz 44 de los clientes de mensajería 11, 12, 13. En esta forma de realización, el certificado 44 es el certificado raíz.

En la forma de realización preferida, la cadena de certificación del segundo certificado 42 correspondiente al primer sujeto 21 contiene el segundo certificado 43 correspondiente al primer emisor y el certificado raíz 44. No obstante, en otras formas de realización, es posible que el certificado 44 no sea el certificado raíz, sino que esté firmado él mismo con otro certificado o certificado raíz. El número de niveles de la cadena de certificación para el segundo certificado 42 correspondiente al primer sujeto 21 es arbitrario. También es posible que cualquier otro certificado que no sea el certificado raíz de la cadena de certificación del segundo certificado 42 correspondiente al primer sujeto 21 se almacene en la lista de certificados de confianza en los clientes de mensajería 11, 12, 13 como ancla de confianza.

El segundo certificado 42 correspondiente al primer sujeto 21 se podría interpretar como certificado proforma correspondiente al primer sujeto 21. El certificado proforma 42 tiene el mismo contenido o por lo menos parte del mismo contenido que el certificado original 41 correspondiente al primer sujeto 21, pero con otra firma y otra cadena de certificación.

La etapa S3 puede incluir, además, una comprobación, si el segundo certificado 42 correspondiente al primer sujeto 21 ya está almacenado en el sistema de gestión de certificados 31. En caso afirmativo, la etapa de creación descrita anteriormente se puede omitir y el segundo certificado 42 correspondiente al primer sujeto 21 se puede recuperar de unos medios de almacenamiento o base de datos del sistema de gestión de certificados 31. En caso contrario, la etapa de generación para el segundo certificado 42 correspondiente al primer sujeto 21 se lleva a cabo tal como se ha descrito anteriormente. La etapa de generación del segundo certificado 42 correspondiente al primer sujeto 21 puede incluir, además, una comprobación, si el segundo certificado 43 correspondiente al intermediario ya está almacenado en el sistema de gestión de certificados 31. Esto podría ser así si, para el mismo intermediario que emitió el primer certificado 41 correspondiente al primer sujeto 21, pero correspondiente a otro sujeto, se recibió un primer certificado y se creó un segundo con el respectivo segundo certificado 43 correspondiente al intermediario. En caso afirmativo, la etapa de generación del segundo certificado 43 correspondiente al intermediario antes descrita se puede omitir, y el segundo certificado 42 correspondiente al intermediario se puede recuperar de unos medios de almacenamiento o base de datos del

sistema de gestión de certificados 31. En caso contrario, la etapa de generación para el segundo certificado 43 correspondiente al intermediario se lleva a cabo tal como se ha descrito anteriormente. En otras palabras, el segundo certificado 43 correspondiente al intermediario se puede usar para todos los sujetos cuyo primer certificado fue emitido por el mismo intermediario.

Antes de generar el segundo certificado (S3) o antes de transmitir el segundo certificado 42 al cliente de mensajería 11, se podría llevar a cabo, además, una etapa de validación del primer certificado recibido 41 correspondiente al primer sujeto 21, por ejemplo, según se ha descrito con las figuras 2 y 3. Si el primer certificado 41 se confirma como válido, puede llevarse a cabo la generación del segundo certificado 42 (S3) o la transmisión del segundo certificado generado 42 (S4). Si el primer certificado 41 se confirma como no válido, hay varias acciones posibles: puede omitirse la etapa S3 o S4 y, finalmente, se podría informar al cliente de mensajería solicitante 11; podría solicitarse al primer sujeto 21 un certificado válido; de todos modos podría llevarse a cabo la etapa S3 o S4 y se podría avisar al cliente de mensajería solicitante 11 de que la autenticación/validación de la clave pública resultó problemática.

En la etapa S4, el sistema de gestión de certificados 31 transmite el segundo certificado 42 correspondiente al primer sujeto 21 hacia el primer cliente de mensajería 11. El primer cliente de mensajería solicitante 11 recibe el segundo certificado 42 correspondiente al primer sujeto 21. En una forma de realización, la transmisión se materializa como respuesta a la solicitud de la etapa S2. No obstante, la transmisión también se podría materializar sin ninguna solicitud previa del primer cliente de mensajería 11. En una forma de realización, la transmisión del segundo certificado 42 correspondiente al primer sujeto 21 se podría llevar a cabo mediante un mensaje enviado sin solicitud previa (*push*), un mensaje con un segundo certificado adjunto 42 correspondiente al primer sujeto 21, por ejemplo, en una tarjeta *V-card*. Si el primer certificado 41 correspondiente al primer sujeto 21 se recolectó de un mensaje, el primer certificado 41 correspondiente al primer sujeto 21 de este mensaje se podría sustituir por el segundo certificado 42, recién generado, correspondiente al primer sujeto 21 antes de entregarlo al primer cliente de mensajería 11. El mensaje podría provenir, por ejemplo, del propio primer sujeto 21.

En la etapa S5, el primer cliente de mensajería 11 valida el segundo certificado 42 correspondiente al primer sujeto 21. De este modo, el primer cliente de mensajería 11 llevará a cabo la etapa de construcción de la cadena de certificación hasta obtener el certificado raíz 44. Si el segundo certificado 43 correspondiente al intermediario no está presente, la etapa S5 podría comprender, además, descargar el segundo certificado 43 correspondiente al intermediario sobre la base de una extensión de AIA. Teóricamente, es posible también descargar el certificado raíz 44 sobre la base de una extensión de AIA, pero muchos clientes de mensajería 11, 12, 13 requieren que el certificado raíz 44 ya esté presente localmente. Por lo tanto, el cliente de mensajería 11 ni siquiera sabe que el segundo certificado recibido 42 correspondiente al primer sujeto 21 y su cadena de certificación no se corresponden con el primer certificado original 41 correspondiente al primer sujeto 21 y su cadena de certificación. Por lo tanto, la presente solución no necesita ningún enchufable o complemento de *software* o configuraciones especiales en el cliente de mensajería 11, excepto que el certificado raíz 44 se debe incluir en la lista de certificados de confianza, en caso de que esto no sea ya así. Preferentemente, el cliente de mensajería 11 se configura de tal manera que confía en el certificado raíz 44. Esto se materializa normalmente incluyendo el certificado raíz 44 en la lista de certificados de confianza en cada uno de la pluralidad de clientes de mensajería 11, 12, 13. Se comienza, por tanto, con la etapa de validación de la cadena de certificación, comprobando la firma del segundo certificado 43 correspondiente al intermediario sobre la base de la clave pública del certificado raíz 44 y comprobando la firma del segundo certificado 42 correspondiente al primer sujeto 21 sobre la base de la clave pública del segundo certificado 43 correspondiente al intermediario. Si la validación se aprueba, el procedimiento continúa con la etapa S6. En caso contrario, existen diferentes posibilidades: se podría enviar una nueva solicitud al sistema de gestión de certificados 31 (especialmente, si el segundo certificado 42 correspondiente al primer sujeto 21 y/o el segundo certificado 43 correspondiente al intermediario y/o el certificado raíz 44 no se reciben del sistema de gestión de certificados 31, sino que se recuperó/recuperaron localmente y podría(n) haber caducado(s)); se podría emitir un mensaje de error en relación con que el cifrado no se puede llevar a cabo o que el cifrado podría no ser seguro.

En la etapa S10, se lleva a cabo una acción en el primer cliente de mensajería 11 sobre la base de la clave pública incluida en el segundo certificado 42 correspondiente al primer sujeto 21.

La figura 8 muestra un primer ejemplo correspondiente a dicha etapa S10 para un cifrado de extremo-a-extremo. En la etapa S6, un mensaje que se enviará al primer sujeto 21 se cifra sobre la base de la clave pública contenida en el segundo certificado 42 correspondiente al primer sujeto 21. Preferentemente, parte de la información de los datos de certificado del segundo certificado 42 se incluye en el mensaje con el fin de identificar, en el destinatario 21, la clave privada que se corresponde con el segundo certificado 42. Dicha información podría ser el número de serie y el emisor. Como cifrado podría usarse el S/MIME, en el que solamente se cifra, con la clave pública, una clave simétrica usada para cifrar el mensaje. El mensaje podría ser un correo electrónico, un SMS, un mensaje instantáneo, ... En la etapa S7, el mensaje cifrado se envía al primer sujeto 21. El mensaje cifrado se puede enviar directamente o por medio de una pasarela. Puesto que solamente el primer sujeto 21 tiene la clave privada correspondiente, solamente el primer sujeto 21 podrá descifrar el

mensaje.

La figura 9 muestra un segundo ejemplo correspondiente a dicha etapa S10 para comprobar una firma de un mensaje recibido. En la etapa S8, se comprueba una firma de un mensaje recibido, preferentemente del primer sujeto 21, sobre la base de la clave pública del segundo certificado 42 correspondiente al primer sujeto 21.

Las etapas S1 a S10 muestran uno de los órdenes posibles, pero no imponen dicho orden y no limitarán la invención al mismo. Las etapas se describen con el ejemplo del primer sujeto 21 y el primer cliente de mensajería 11. No obstante, se aplican las mismas etapas para la totalidad del resto de clientes de mensajería 12, 13 de la pluralidad de clientes de mensajería 11, 12, 13 y para la totalidad de los otros sujetos 22.

La figura 10 muestra una segunda forma de realización de un procedimiento para una gestión central de certificados. Las etapas también se muestran parcialmente en la figura 5. Dichas etapas se podrían llevar a cabo después de las etapas de la figura 7.

Las etapas S1'' a S10'' se corresponden con las etapas S1 a S10, con la diferencia de que, en lugar del primer cliente de mensajería 11, un tercer cliente de mensajería 13 diferente del primer cliente de mensajería 11 recibe el segundo certificado, y/o el sujeto es, en este caso, un segundo sujeto 22 diferente del primer sujeto 21. En una forma de realización ventajosa, se usa el mismo certificado raíz 44 para el segundo certificado 42 correspondiente al primer sujeto 21 y para el segundo certificado correspondiente al segundo sujeto 22, incluso si el primer certificado 41 correspondiente al primer sujeto 21 y el primer certificado correspondiente al segundo sujeto 22 tuvieran diferentes certificados raíz. En una forma de realización, si el primer certificado 41 correspondiente al primer sujeto 21 y el primer certificado correspondiente al segundo sujeto 22 son emitidos por el mismo certificado de intermediario 45, el mismo segundo certificado 43 correspondiente al intermediario también se podría usar para el segundo certificado 42 correspondiente al primer sujeto 21 y para el segundo certificado correspondiente al segundo sujeto 22.

El sistema antes mencionado se ha descrito para un sistema de mensajería que permite que usuarios de los clientes de mensajería respectivos envíen y reciban mensajes. No obstante, la invención no se limita a sistemas de mensajería de este tipo. Los clientes también se podrían referir a otro sistema de órdenes y respuestas como, por ejemplo, para la internet de las cosas. Cada objeto/cosa se correspondería con un cliente y se configuraría para recibir órdenes y/o respuestas y/o para enviar órdenes y/o respuestas. Las órdenes y/o respuestas se podrían cifrar y/o firmar. Para comprobar la validez de los certificados, podría usarse la gestión de certificados antes descrita para los clientes 11, 12, 13. También es posible aplicar un sistema de este tipo a clientes web, por ejemplo, para un cifrado https.

La invención no se limita a las formas de realización descritas, sino que quedarán protegidas todas las formas de realización que se sitúen bajo el alcance de protección de las reivindicaciones.

REIVINDICACIONES

1. Procedimiento de gestión de certificados para una pluralidad de clientes (11, 12, 13) que comprende las etapas de:

recibir (S1), en un sistema de gestión de certificados (31), un primer certificado (41) correspondiente a un sujeto (21), comprendiendo el primer certificado (41) correspondiente al sujeto (21) una primera clave pública, un campo de emisor con un primer emisor y un campo de número de serie con un primer número de serie, firmándose el primer certificado (41) correspondiente al sujeto (21) con un primer certificado (45) correspondiente al primer emisor;

generar (S3), en el sistema de gestión de certificados (31), un segundo certificado (42) correspondiente al sujeto (21);

transmitir (S4) el segundo certificado (42) correspondiente al sujeto (21) desde el sistema de gestión de certificados (31) a uno de la pluralidad de clientes (11, 12, 13);

caracterizado por que

el segundo certificado generado (42) correspondiente al sujeto (21) comprende la primera clave pública, un campo de emisor con el primer emisor y un campo de número de serie con el primer número de serie, firmándose el segundo certificado generado (42) correspondiente al sujeto (21) con un segundo certificado (43) correspondiente al primer emisor, que es diferente del primer certificado (45) correspondiente al primer emisor.

2. Procedimiento según la reivindicación 1, en el que

el primer certificado (45) correspondiente al primer emisor comprende un campo de emisor con un segundo emisor y el segundo certificado (43) correspondiente al primer emisor comprende un campo de emisor con un tercer emisor, que es diferente del segundo emisor; y/o

el primer certificado (45) correspondiente al primer emisor comprende un campo de número de serie con un segundo número de serie y el segundo certificado (43) correspondiente al primer emisor comprende un campo de número de serie con un tercer número de serie que es diferente del segundo número de serie; y/o

el primer certificado (45) correspondiente al primer emisor comprende una segunda clave pública y el segundo certificado (43) correspondiente al primer emisor comprende una tercera clave pública que es diferente de la segunda clave pública.

3. Procedimiento según una de las reivindicaciones anteriores, en el que el segundo certificado (43) correspondiente al primer emisor comprende un campo de emisor con un segundo emisor y el segundo certificado (43) se firma con un certificado (44) correspondiente al segundo emisor.

4. Procedimiento según una de las reivindicaciones anteriores, en el que

el segundo certificado (42) correspondiente al primer sujeto (21) comprende una Extensión de Acceso a Información de Autoridad con el fin de permitir que el mencionado de la pluralidad de clientes (11, 12, 13) que recibe el segundo certificado (42) correspondiente al sujeto (21) descargue el segundo certificado (43) correspondiente al primer emisor para la construcción de la cadena de certificación.

5. Procedimiento según una de las reivindicaciones anteriores, en el que una cadena de certificación del primer certificado (41) correspondiente al sujeto (21) presenta un primer certificado raíz (46) y una cadena de certificación del segundo certificado (42) correspondiente al sujeto (21) presenta un segundo certificado raíz (44) que es diferente del primer certificado raíz (46).

6. Procedimiento según una de las reivindicaciones anteriores, que comprende las etapas de:

recibir (S1''), en el sistema de gestión de certificados (31), un primer certificado correspondiente a otro sujeto (22) que comprende otra primera clave pública, un campo de emisor con otro primer emisor y un campo de número de serie con otro primer número de serie, firmándose el primer certificado correspondiente al otro sujeto (22) con un primer certificado correspondiente al otro primer emisor;

generar (S3''), en el sistema de gestión de certificados (31), un segundo certificado correspondiente al otro sujeto (22) que comprende la otra primera clave pública, un campo de emisor con el otro primer emisor y un campo de número de serie con el otro primer número de serie, firmándose el segundo certificado correspondiente al otro sujeto (22) con un segundo certificado correspondiente al otro primer emisor, que es

diferente del primer certificado correspondiente al otro primer emisor, firmándose el segundo certificado correspondiente al primer emisor y el segundo certificado correspondiente al otro primer emisor con el mismo certificado y/o presentando el mismo certificado raíz;

transmitir (S4'') el segundo certificado correspondiente al otro sujeto (22) desde el sistema de gestión de certificados (31) a uno (13) de la pluralidad de clientes (11, 12, 13).

7. Procedimiento según una de las reivindicaciones anteriores, que comprende las etapas de

almacenar (S3), en el sistema de gestión de certificados (31), el segundo certificado (42) correspondiente al sujeto (21);

recuperar (S3'), en el sistema de gestión de certificados (31), el segundo certificado (42) correspondiente al sujeto (21); y

enviar (S4') el segundo certificado correspondiente al sujeto (21) desde el sistema de gestión de certificados (31) a otro (13) de la pluralidad de clientes (11, 12, 13).

8. Procedimiento según una de las reivindicaciones anteriores, que comprende las etapas de

recibir (S4), en uno (11) de la pluralidad de clientes (11, 12, 13), el segundo certificado correspondiente al sujeto (21);

llevar a cabo, en el mencionado (11) de la pluralidad de clientes (11, 12, 13), un proceso de validación de cadena de certificación (S5) para el segundo certificado recibido correspondiente al sujeto (21);

llevar a cabo, en el mencionado de la pluralidad de clientes (11, 12, 13), sobre la base de la primera clave pública del segundo certificado correspondiente al sujeto (21):

el cifrado (S6) de un mensaje con la primera clave pública del segundo certificado correspondiente al sujeto (21) y el envío (S7) del mensaje cifrado al sujeto (21); o

la comprobación de la firma de un mensaje del sujeto (21) sobre la base de la primera clave pública del segundo certificado correspondiente al sujeto (21).

9. Procedimiento de tratamiento, en un cliente (11), de un certificado correspondiente a un sujeto (21), en el que un primer certificado (41) correspondiente al sujeto (21) comprende una primera clave pública, un campo de emisor con un primer emisor y un campo de número de serie con un primer número de serie, en el que el primer certificado (41) correspondiente al sujeto (21) se firma con un primer certificado (45) correspondiente al primer emisor, caracterizado el procedimiento por

solicitar (S1), en el cliente (11), un segundo certificado (42) correspondiente al sujeto (21);

proporcionar (S2, S3, S4), en el cliente (11), el segundo certificado (42) correspondiente al sujeto (21), que comprende la primera clave pública, un campo de emisor con el primer emisor y un campo de número de serie con el primer número de serie, firmándose el segundo certificado (42) correspondiente al sujeto (21) con un segundo certificado (43) correspondiente al primer emisor, que es diferente del primer certificado (45) correspondiente al primer emisor;

llevar a cabo, en el cliente (11), un proceso de validación de cadena de certificación (S5) para el segundo certificado recibido (42) correspondiente al sujeto (21);

llevar a cabo, en el cliente (11), una acción sobre la base de la primera clave pública del segundo certificado correspondiente al sujeto.

10. Procedimiento según la reivindicación 8 o 9, en el que la etapa de proporcionar el segundo certificado correspondiente al sujeto (21) comprende:

comprobar si el segundo certificado (42) correspondiente al sujeto (21) está almacenado en una sección de almacenamiento del cliente de mensajería;

si el segundo certificado (42) correspondiente al sujeto (21) está almacenado en la sección de almacenamiento, recuperar el segundo certificado (42) correspondiente al sujeto (21) de la sección de almacenamiento; y

si el segundo certificado (42) correspondiente al sujeto (21) no está almacenado en la sección de

almacenamiento, enviar una solicitud de un certificado correspondiente al sujeto (21) a un sistema de gestión de certificados (31) y recibir el segundo certificado (43) correspondiente al sujeto (21) del sistema de gestión de certificados (31).

11. Procedimiento según una de las reivindicaciones 8 a 10, en el que un primer certificado correspondiente a otro sujeto (22) comprende otra clave pública, un campo de emisor con otro primer emisor y un campo de número de serie con otro primer número de serie y en el que el primer certificado correspondiente al otro sujeto (22) se firma con un primer certificado correspondiente al otro primer emisor, comprendiendo el procedimiento las etapas de:

recuperar un segundo certificado correspondiente al otro sujeto (22), que comprende la otra clave pública del primer certificado correspondiente al otro sujeto (22), un campo de emisor con el otro primer emisor y un campo de número de serie con el primer número de serie, en firmándose el segundo certificado correspondiente al otro sujeto (22) con un segundo certificado correspondiente al otro primer emisor, que es diferente del primer certificado correspondiente al otro primer emisor, firmándose el segundo certificado (43) correspondiente al primer emisor y el segundo certificado correspondiente al otro primer emisor con el mismo certificado (44) y/o presentando el mismo certificado raíz;

llevar a cabo un proceso de validación de cadena de certificación (S5") para el segundo certificado recibido correspondiente al otro sujeto (22);

llevar a cabo, en el cliente (11), una acción sobre la base de la otra primera clave pública del segundo certificado correspondiente al otro sujeto (22).

12. Programa informático configurado para llevar a cabo las etapas del procedimiento según una de las reivindicaciones anteriores, cuando se ejecuta en uno o más procesador(es).

13. Sistema de gestión de certificados (31) para gestionar certificados para una pluralidad de clientes (11, 12, 13), que comprende:

una sección de recepción para recibir (S1) un primer certificado (41) correspondiente a un sujeto (21), comprendiendo el primer certificado (41) correspondiente al sujeto (21) una primera clave pública, un campo de emisor con un primer emisor y un campo de número de serie con un primer número de serie, firmándose el primer certificado (41) correspondiente al sujeto (21) con un primer certificado (45) correspondiente al primer emisor;

una sección de generación de certificados para generar (S3) un segundo certificado (42) correspondiente al sujeto (21);

una sección de transmisión para transmitir (S4) el segundo certificado (42) correspondiente al sujeto (21) al mencionado de la pluralidad de clientes (11, 12, 13);

caracterizado por que

el segundo certificado generado (42) correspondiente al sujeto (21) comprende la primera clave pública, un campo de emisor con el primer emisor y un campo de número de serie con el primer número de serie, firmándose el segundo certificado generado (42) correspondiente al sujeto (21) con un segundo certificado (43) correspondiente al primer emisor, que es diferente del primer certificado (45) correspondiente al primer emisor.

14. Dispositivo de cliente que comprende:

una sección de validación para llevar a cabo un proceso de validación de cadena de certificación (S5) para un segundo certificado correspondiente a un sujeto (21, 22);

una sección de provisión de certificados para proporcionar (S2, S3, S4) el segundo certificado (42) correspondiente al sujeto (21, 22) en calidad de dicho certificado correspondiente al sujeto (21, 22) que es diferente de un primer certificado verdadero (41) correspondiente al sujeto (21, 22), comprendiendo el primer certificado (41) correspondiente al sujeto (21, 22) una primera clave pública, un campo de emisor con un primer emisor y un campo de número de serie con un primer número de serie (21, 22), firmándose el primer certificado (41) correspondiente al sujeto (21, 22) con un primer certificado (45) correspondiente al primer emisor;

una sección de procesado de certificados para llevar a cabo una acción sobre la base de la primera clave pública del segundo certificado correspondiente al sujeto (21, 22);

caracterizado por que

el segundo certificado proporcionado (42) correspondiente al sujeto (21, 22) comprende la primera clave pública, un campo de emisor con el primer emisor y un campo de número de serie con el primer número de serie, firmándose el segundo certificado proporcionado (42) correspondiente al sujeto (21, 22) se firma con un segundo certificado (43) correspondiente al primer emisor, que es diferente del primer certificado (45) correspondiente al primer emisor.

15. Sistema de tratamiento de certificados, que comprende:

una pluralidad de dispositivos de cliente (11, 12, 13) configurados, cada uno de ellos, para validar un certificado correspondiente a un sujeto (21, 22) antes de usar una clave pública del certificado correspondiente al sujeto (21, 22);

un sistema de gestión de certificados (31) para la gestión del certificado correspondiente al sujeto (21, 22);

caracterizado por que

la pluralidad de dispositivos de cliente (11, 12, 13) son dispositivos del cliente según la reivindicación 14; y/o

el sistema de gestión de certificados (31) es un sistema de gestión de certificados según la reivindicación 13.

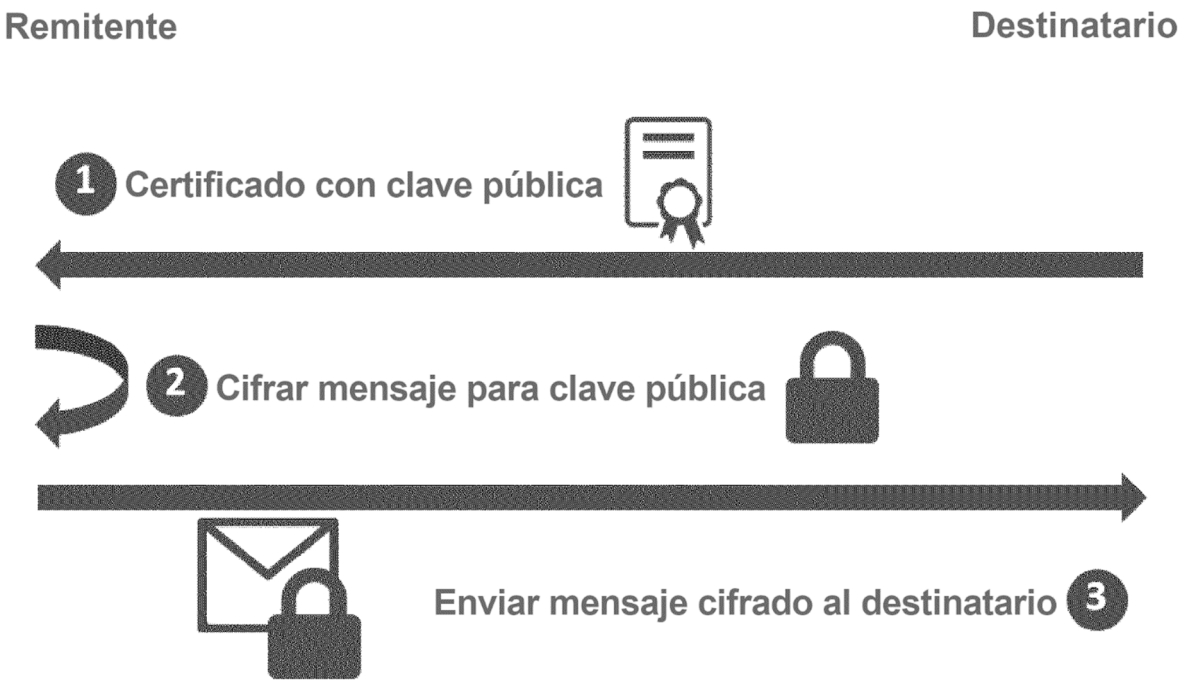

Fig. 1 Técnica Anterior

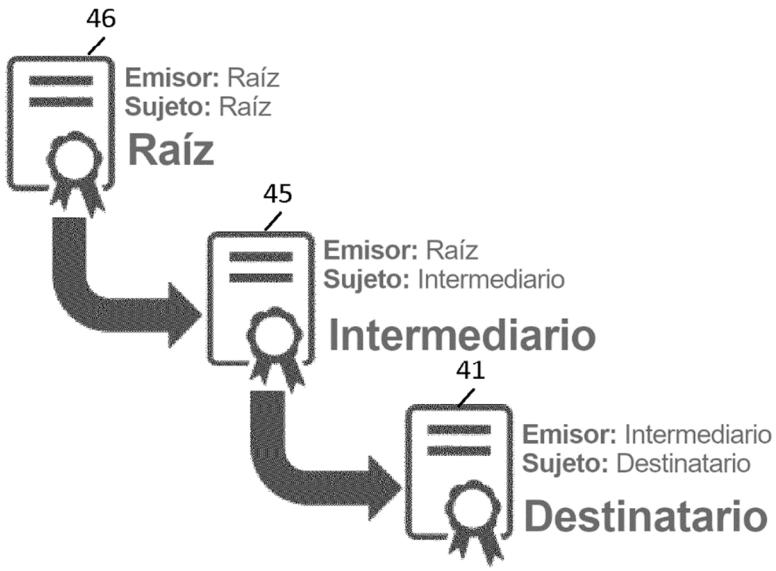

Fig. 2 Técnica Anterior

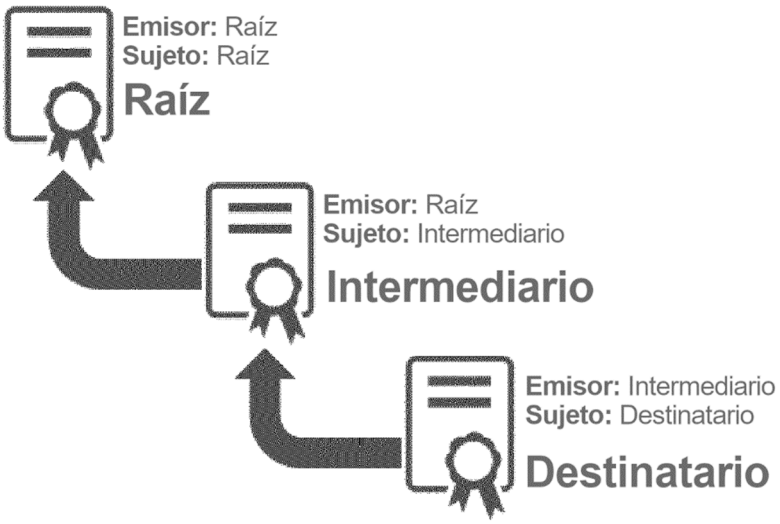

Fig. 3 Técnica Anterior

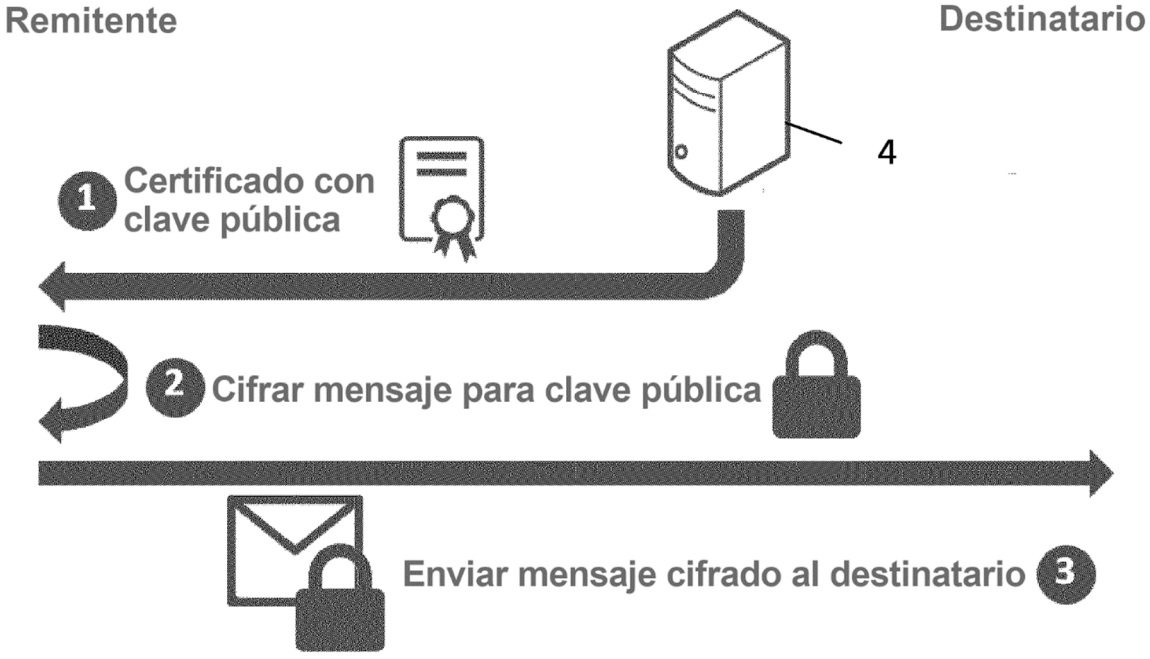

Fig. 4 Técnica Anterior

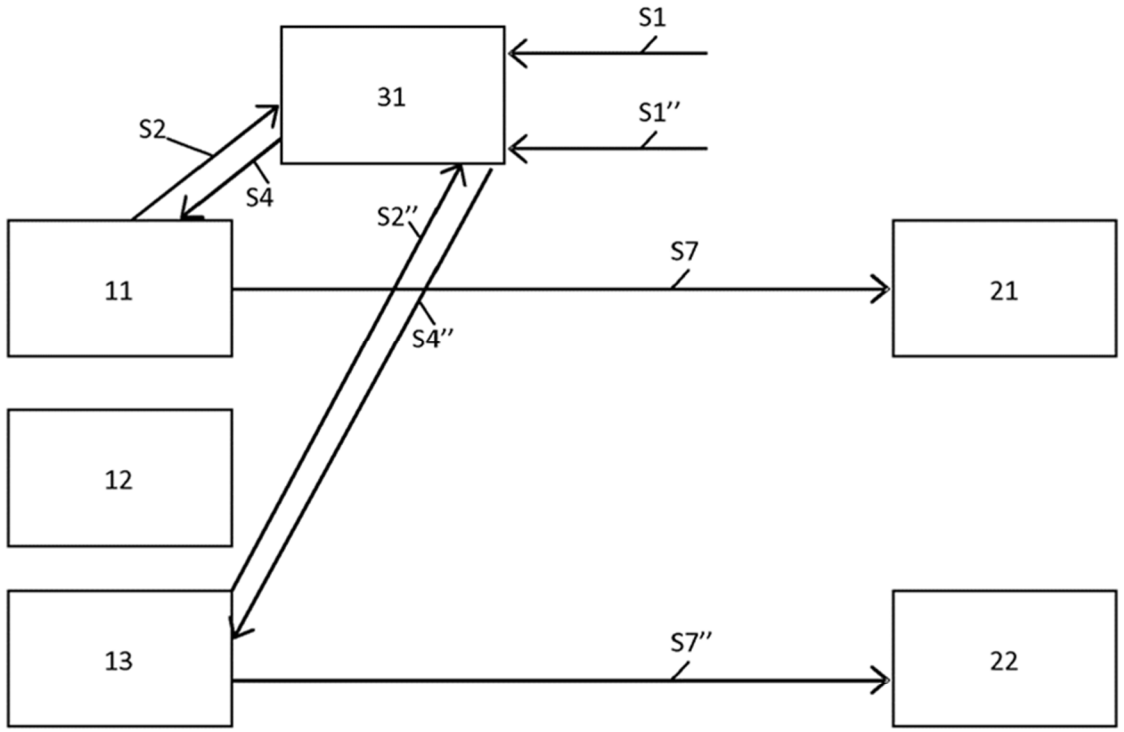
S1
31
S1''
S2
S4
S2''
S7
11
21
S4''
12
13
S7''
22

Fig. 5

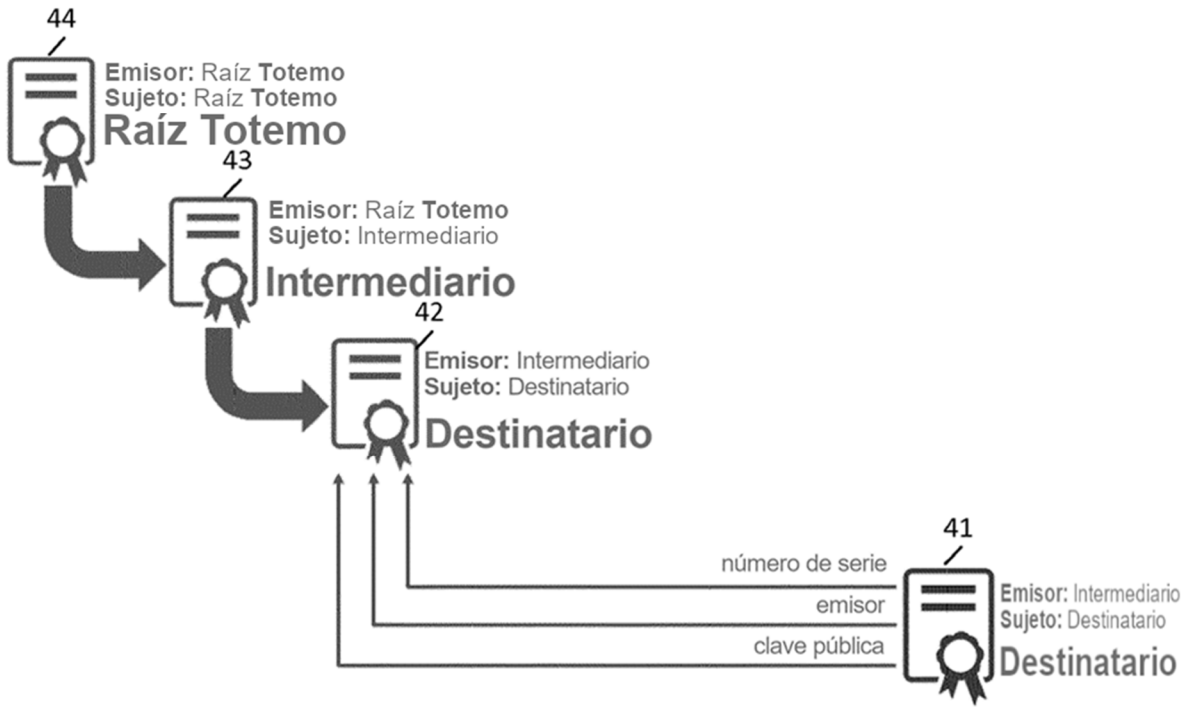
44
Emisor: Raíz Totemo
Sujeto: Raíz Totemo
Raíz Totemo
43
Emisor: Raíz Totemo
Sujeto: Intermediario
Intermediario
42
Emisor: Intermediario
Sujeto: Destinatario
Destinatario
41
número de serie
emisor
clave pública
Emisor: Intermediario
Sujeto: Destinatario
Destinatario

Fig. 6

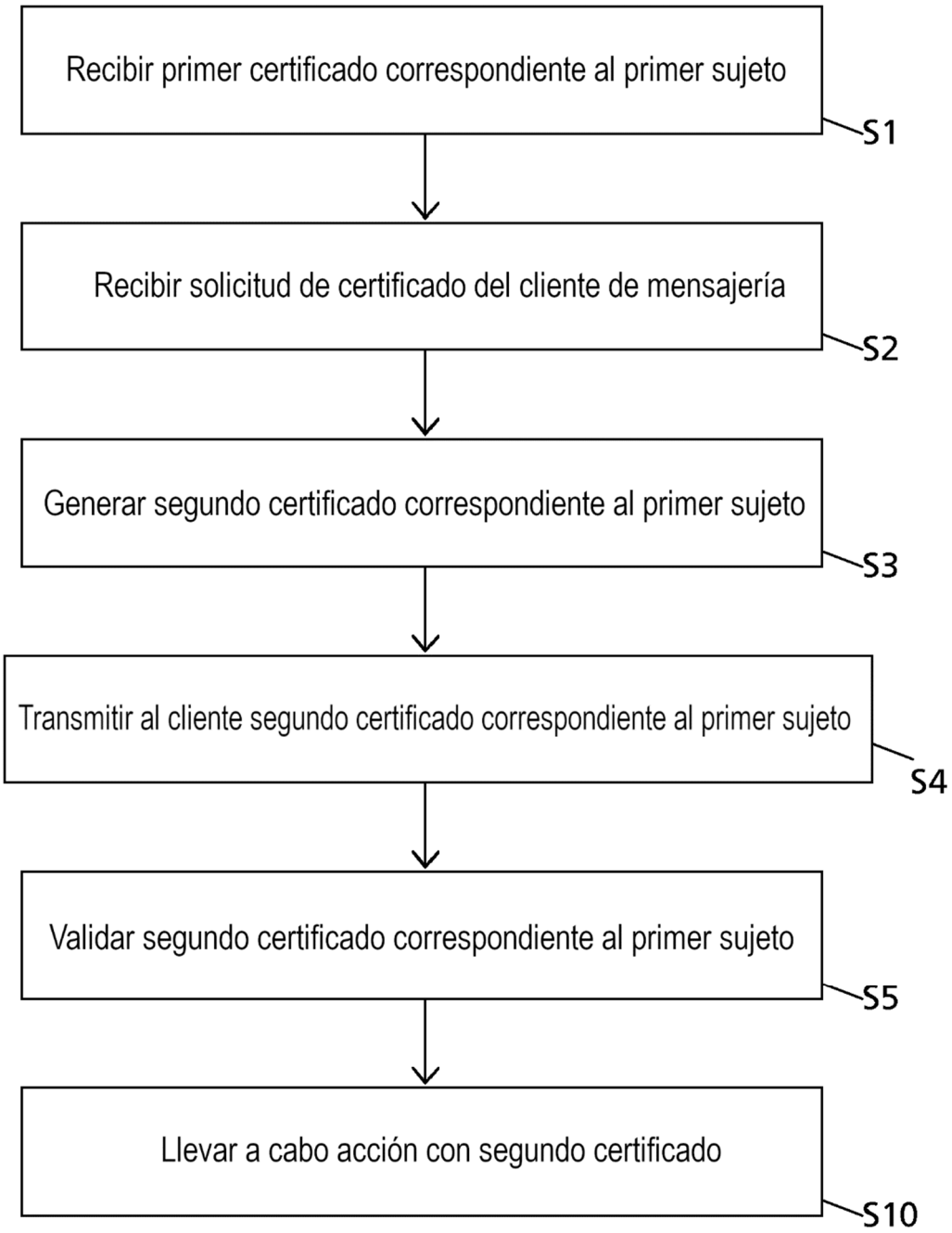
Recibir primer certificado correspondiente al primer sujeto
S1
Recibir solicitud de certificado del cliente de mensajería
S2
Generar segundo certificado correspondiente al primer sujeto
S3
Transmitir al cliente segundo certificado correspondiente al primer sujeto
S4
Validar segundo certificado correspondiente al primer sujeto
S5
Llevar a cabo acción con segundo certificado
S10

Fig. 7

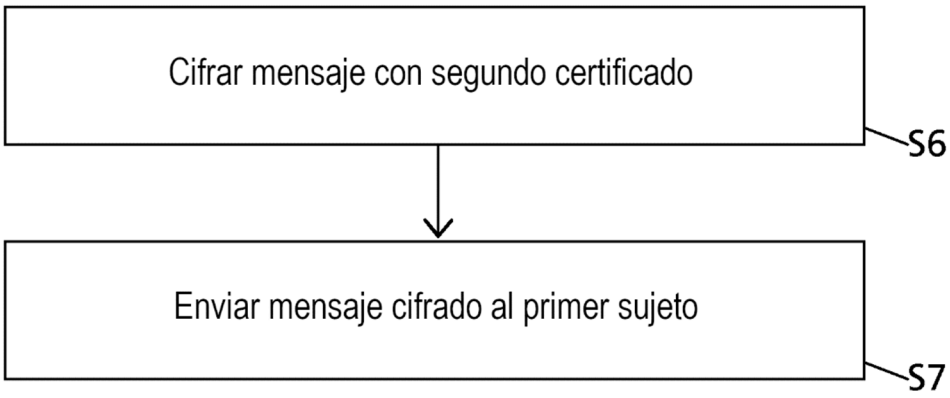
Cifrar mensaje con segundo certificado
S6
Enviar mensaje cifrado al primer sujeto
S7

Fig. 8

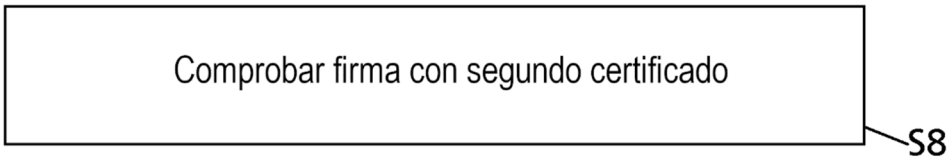
Comprobar firma con segundo certificado
S8

Fig. 9

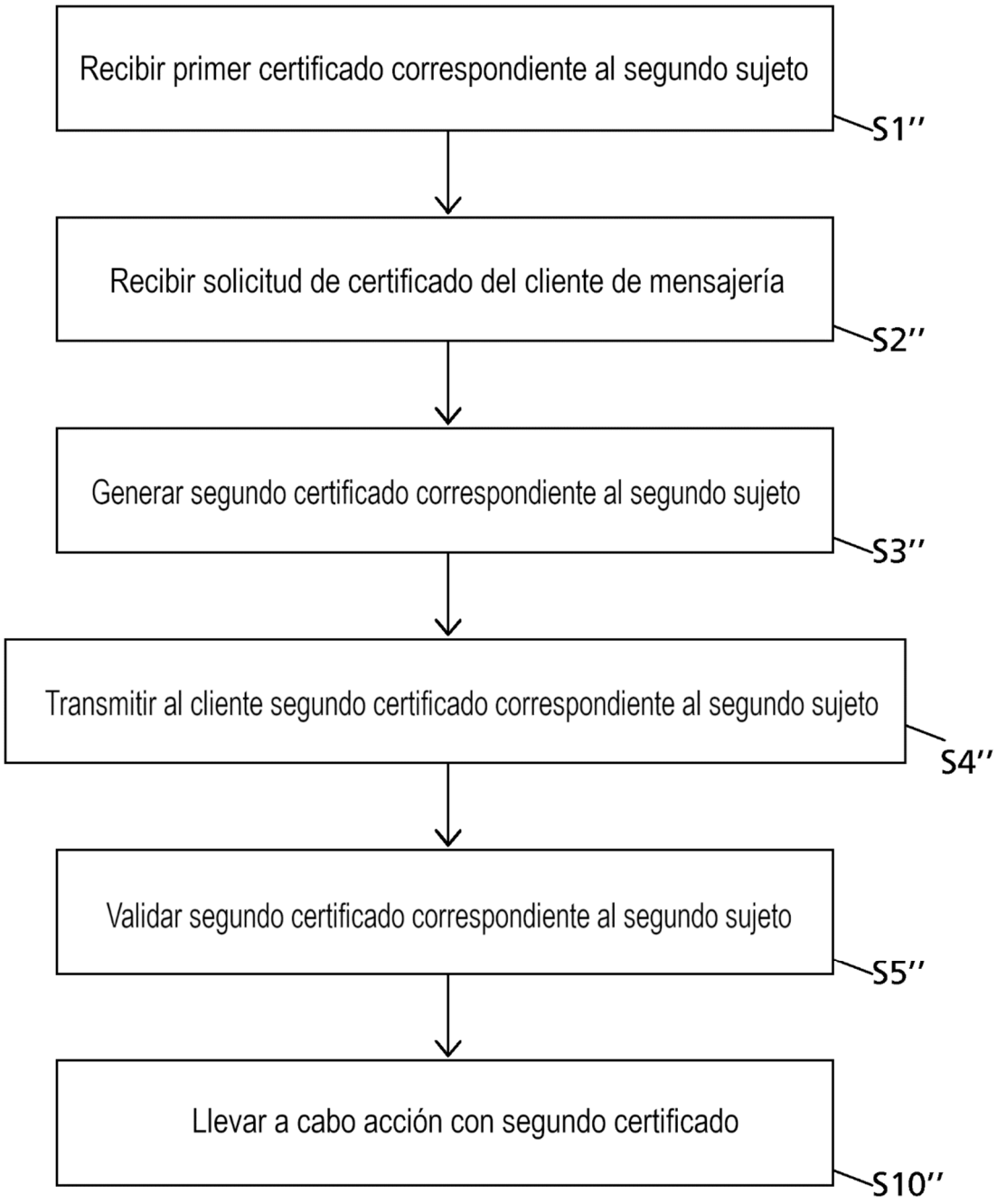
Recibir primer certificado correspondiente al segundo sujeto
S1''
Recibir solicitud de certificado del cliente de mensajería
S2''
Generar segundo certificado correspondiente al segundo sujeto
S3''
Transmitir al cliente segundo certificado correspondiente al segundo sujeto
S4''
Validar segundo certificado correspondiente al segundo sujeto
S5''
Llevar a cabo acción con segundo certificado
S10''

Fig. 10