(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 660 405**

(51) Int. CI.:

G06F 21/40 (2013.01)
G06F 21/60 (2013.01)
G06F 21/64 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.06.2013 PCT/IB2013/001317**

(87) Fecha y número de publicación internacional: **27.12.2013 WO13190372**

(96) Fecha de presentación y número de la solicitud europea: **21.06.2013 E 13745469 (0)**

(97) Fecha y número de publicación de la concesión europea: **20.12.2017 EP 2864924**

(54) Título: **Sistemas, métodos y aparatos para proteger certificados raíz**

(30) Prioridad:

22.06.2012 US 201261663266 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.03.2018

(73) Titular/es:

OLOGN TECHNOLOGIES AG (100.0%)
Landstrasse 123
9495 Triesen, LI

(72) Inventor/es:

IGNATCHENKO,SERGEY y
IVANCHYKHIN, DMYTRO

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Sistemas, métodos y aparatos para proteger certificados raíz.

Solicitudes relacionadas

Esta solicitud reivindica prioridad con respecto a la solicitud provisional de Estados Unidos n.º 61/663.266, presentada el 22 de junio de 2012, y a la solicitud no provisional de Estados Unidos n.º 13/923.756, presentada el 21 de junio de 2013, tituladas ambas “Systems, Methods and Apparatuses for Securing Root Certificates”, incorporándose en su totalidad el contenido de las dos solicitudes a la presente como referencia.

Campo de la exposición

Los sistemas, métodos y aparatos descritos en la presente se refieren a la seguridad de los datos. Más particularmente, se refieren a la sustitución segura de certificados raíz en el interior de dispositivos electrónicos, tales como ordenadores convencionales, ordenadores portátiles, teléfonos inteligentes, consolas de juegos, televisores, tabletas, etcétera.

Antecedentes

Los certificados digitales y la infraestructura de clave pública (PKI) son mecanismos bien conocidos para autenticar electrónicamente individuos. En la PKI, cada entidad tiene un par de claves asimétricas, único, que comprende una clave pública y una clave privada. Una autoridad de certificación (CA) emite un certificado digital, que enumera las credenciales identificativas de la entidad (por ejemplo, nombre y organización) y la clave pública de la entidad, vinculando la identidad de la entidad con su clave pública. A continuación, la entidad puede cifrar la totalidad (o un valor *hash*) de su mensaje saliente con su clave privada, y puede distribuir su certificado digital junto con el mensaje de cifrado. El destinatario del mensaje puede descifrar el mensaje cifrado usando la clave pública del emisor, lo que permite que el destinatario confirme que (i) el emisor tiene acceso a la clave privada correspondiente, y, por tanto, (ii) el emisor es el individuo identificado en el certificado digital.

No obstante, se sabe también que los certificados digitales pueden ser falsificados. Así, habitualmente, cuando una CA emite un certificado digital nuevo, la CA firmará digitalmente el certificado usando una de sus propias claves privadas. A continuación, la CA publicará su propio certificado digital, identificándose a sí misma e identificando la clave pública correspondiente. Esto permitirá que un destinatario de mensaje confirme que el certificado digital del emisor fue emitido por la CA. El certificado digital se ha hecho más difícil de falsificar (ya que requería el uso de la clave privada de la CA) y resulta más fiable.

No obstante, puede ser que la CA pretendida no sea fiable. (Por ejemplo, un usuario malicioso puede haber creado su propia “CA” con el fin de firmar certificados digitales). Como consecuencia, puede resultar deseable que el certificado digital de la CA sea firmado todavía por otra CA. Esta cadena puede continuar todo su recorrido de vuelta hasta un “certificado raíz” en la parte superior de la jerarquía, el cual, preferentemente, ha sido emitido por una CA bien conocida y de confianza. Entre las CA habituales que son poseedoras de certificados raíz se encuentran VeriSign, Entrust, Comodo y GlobalSign.

En el campo de la seguridad de la información, son muy comunes los sistemas que se basan en certificados raíz y claves privadas raíz. En última instancia, la fiabilidad de la cadena depende de la fiabilidad de este certificado raíz. Dos problemáticas bien conocidas en relación con dichos sistemas son (1) el almacenamiento seguro de claves privadas raíz, y (2) la población de certificados raíz dentro de los sistemas que los necesitan para la autenticación.

Habitualmente, se consigue que el certificado raíz sea fiable por medio de algún mecanismo que no sea un certificado digital, por ejemplo por medio de una distribución física segura. Por ejemplo, algunos de los certificados raíz más ampliamente conocidos se incorporan en hardware o software en el momento en el que el hardware se fabrica o el software se instala (por ejemplo, en navegadores de Internet se incorporan normalmente certificados web raíz).

La solicitud de patente europea EP 1 143 658 A1 da a conocer un método de autenticación de datos transmitidos en un sistema de transmisión digital, en el cual el método comprende las etapas de, antes de la transmisión, determinar por lo menos dos valores cifrados para por lo menos algunos de los datos, determinándose cada valor cifrado con el uso de una clave de un algoritmo de cifrado respectivo, y dar salida a dichos por lo menos dos valores cifrados, con dichos datos.

Este método para distribuir certificados raíz se basa en una seguridad que es externa al sistema y a los propios certificados raíz previamente almacenados, lo cual tiene sus inconvenientes. En particular, si dicho certificado raíz (o la clave privada correspondiente al certificado raíz) se ve comprometido, no hay ninguna forma segura de actualizarlo dentro del dispositivo; por el contrario, esto debe ser llevado a cabo por algún mecanismo que sea

externo al sistema. Por ejemplo, podría ser necesario que un administrador del sistema descargase un navegador nuevo desde una fuente supuestamente segura. Por otra parte, una vez comprometido, este certificado raíz no se puede usar para verificar la integridad y la autenticidad de un mensaje que contiene un nuevo certificado raíz a utilizar. Como consecuencia, esencialmente el dispositivo resulta incapaz de verificar la identidad de todo emisor del cual reciba un mensaje. En función del contexto, esto puede convertir al propio dispositivo en inservible.

Se requieren sistemas, métodos y dispositivos para poner, de forma segura, certificados raíz nuevos a disposición de dispositivos electrónicos, después de que un certificado raíz que está en ese momento en vigor llegue a verse comprometido.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques de un sistema ejemplificativo de acuerdo con la presente exposición.

La Figura 2 muestra un mensaje de sustitución de certificado, ejemplificativo, y el contenido de una unidad de gestión de certificados, ejemplificativa.

Las Figuras 3A a 3C muestran procesos ejemplificativos por medio de los cuales un certificado activo se puede sustituir dentro de un dispositivo electrónico.

La Figura 4 muestra un proceso ejemplificativo por medio del cual múltiples certificados se pueden sustituir dentro de un dispositivo electrónico.

La Figura 5 muestra dos mensajes ejemplificativos de sustitución de certificado y el contenido de una unidad ejemplificativa de gestión de certificados.

La Figura 6 muestra un proceso ejemplificativo por medio del cual múltiples certificados se pueden sustituir en un dispositivo electrónico.

La Figura 7 muestra una nota de autorrevocación ejemplificativa, un mensaje de revocación de certificado latente y el contenido de una unidad ejemplificativa de gestión de certificados.

La Figura 8 muestra un proceso ejemplificativo por medio del cual se puede revocar un certificado latente en un dispositivo electrónico.

La Figura 9 muestra un mensaje de certificado nuevo, ejemplificativo, y el contenido de una unidad ejemplificativa de gestión de certificados.

La Figura 10 muestra un proceso ejemplificativo por medio del cual puede añadirse un certificado nuevo a un dispositivo electrónico.

Descripción detallada

En la presente se describen ciertos aspectos ilustrativos de los sistemas, aparatos y métodos de acuerdo con la presente invención, en relación con la siguiente descripción y las figuras adjuntas. No obstante, estos aspectos son indicativos de solamente algunas de las diversas formas según las cuales pueden utilizarse los principios de la invención, y se pretende que la presente invención incluya todos estos aspectos y sus equivalentes. Pueden ponerse de manifiesto otras ventajas y características novedosas de la invención a partir de la siguiente descripción detallada, cuando la misma se considere en combinación con las figuras.

En la siguiente descripción detallada, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión minuciosa de la invención. En otros casos, no se han mostrado de forma detallada estructuras, interfaces y procesos bien conocidos, con el fin de no complicar innecesariamente la invención. No obstante, se pondrá de manifiesto, para alguien con conocimientos habituales en la materia, que no es necesario usar aquellos detalles específicos que se dan a conocer en la presente para llevar a práctica la invención, y que los mismos no representan una limitación sobre el alcance de la invención, excepto por lo que se indique en las reivindicaciones. Se pretende que ninguna parte de esta memoria descriptiva sea considerada con el fin de constituir una exclusión de parte alguna del ámbito completo de la invención. Asimismo, aunque se describen ciertas formas de realización de la presente exposición, estas formas de realización no están destinadas a limitar el alcance completo de la invención.

La invención dada a conocer en la presente proporciona sistemas, métodos y aparatos para la sustitución segura de certificados raíz dentro de dispositivos electrónicos, tales como ordenadores convencionales, ordenadores portátiles, teléfonos inteligentes, consolas de juegos, televisores, tabletas, etcétera. La Figura 1 muestra un dispositivo electrónico ejemplificativo 120 de acuerdo con la presente exposición.

Tal como se muestra en la Figura 1, el dispositivo electrónico 120 se puede comunicar con uno o más dispositivos electrónicos remotos o servidores 180 por medio de un canal de comunicaciones 105 acoplado al dispositivo 120. Por ejemplo, un teléfono inteligente puede tener la capacidad de transmitir y recibir correo electrónico por medio de servidores de correo de Internet. Este canal de comunicaciones puede ser cualquier mecanismo adecuado para transferir datos, ya sea en línea (por ejemplo, Internet) o fuera de línea (por ejemplo, usando una conexión USB o una unidad de almacenamiento *flash*).

Además tal como se muestra en la Figura 1, el dispositivo electrónico 120 se puede conectar por medio del canal de comunicaciones 105 a una o más autoridades de certificación (CAs) 100. Tal como se describirá de forma más detallada posteriormente, la CA 100 se puede configurar para transmitir información referente a sus certificados raíz, a dispositivos electrónicos 120, por medio del canal de comunicaciones 105. Se entenderá que, entre la CA 100 y un dispositivo electrónico 120, puede haber uno o más servidores intermedios 110.

Para implementar la funcionalidad descrita en la presente, el dispositivo electrónico 120 puede ejecutar ciertas aplicaciones o funciones que requieren la autenticación de un certificado digital (mediante el uso de un certificado raíz almacenado) en la realización de ciertas actividades. En el ejemplo anterior, el teléfono inteligente puede autenticar y, según resulte necesario, descifrar todo correo electrónico, el cual incluya un certificado digital, recibido por medio del canal de comunicaciones 105. Se entenderá que el correo electrónico es simplemente un uso ejemplificativo de los certificados raíz; existen muchos otros usos para los certificados raíz, tanto relacionados con actividades que cubren directamente las necesidades de un usuario (tales como la autenticación de correos electrónicos o páginas web), como con actividades que cubren finalidades internas del dispositivo electrónico 120 (tales como, por ejemplo, control seguro del tiempo).

Tal como se muestra en la Figura 1, el dispositivo electrónico 120 puede contener una o más unidades dedicadas de gestión de certificados 166. La unidad de gestión de certificados 166 puede comprender tanto un almacenamiento de certificados raíz 141 y un almacenamiento de atributos asociado de certificados 142. (Estos atributos de certificados se describen de forma más detallada posteriormente). En ciertas formas de realización, el almacenamiento de certificados 141 se puede implementar como una memoria no volátil, de solo lectura, mientras que el almacenamiento de atributos 142 se puede implementar como una memoria no volátil, de lectura/escritura. En formas de realización en las que el dispositivo electrónico 120 está configurado para comunicarse con múltiples CAs, puede resultar preferible configurar la unidad de gestión de certificados 166 de tal manera que los certificados raíz de cada una de las CA 100 se memoricen y gestionen por separado.

Un dispositivo electrónico 120 de acuerdo con la presente exposición puede comprender además un supervisor 160. El supervisor se puede usar para imponer ciertas reglas operativas del dispositivo electrónico 120, con el fin de proporcionar ciertas garantías de seguridad al usuario final. Puede estar configurado para: (1) identificar qué certificado raíz, de los certificados raíz pre-almacenados en la unidad de gestión de certificados 166, se está usando actualmente; (2) validar uno o más certificados digitales, por ejemplo, que pueden ir adjuntos a un mensaje recibido, usando el(los) certificado(s) raíz que está(n) operativo(s) en ese momento; y (3) actualizar uno o más atributos de certificados raíz. Cada una de estas funciones se describe de forma más detallada en la presente. En algunas formas de realización, según se describe de manera más detallada posteriormente, el almacenamiento de certificados 141 se puede implementar como una memoria no volátil, de lectura-escritura, y el supervisor 160 se puede configurar adicionalmente para actualizar uno o más certificados raíz.

El supervisor 160 se puede implementar en hardware y/o software dentro del dispositivo electrónico 120, siempre que en todas las implementaciones, la integridad del supervisor 160 sea mantenida por la implementación seleccionada. Para esta finalidad, se pueden usar, por ejemplo, técnicas resistentes a manipulaciones indebidas y/o de detección de manipulaciones indebidas. Además, si el dispositivo electrónico 120 implementa la opción de cargar y ejecutar código de terceros, deben tomarse medidas para garantizar que ningún código de un tercero tenga la capacidad de influir en o asimilar el estado del supervisor 160.

El supervisor 160 y/o el dispositivo electrónico 120 pueden también incorporar (de manera alternativa, o además de la resistencia a las manipulaciones indebidas) una o más técnicas de detección de manipulaciones indebidas. Por ejemplo, ya se conocen varios métodos de resistencia a manipulaciones indebidas para proteger procesadores criptográficos, y los han sido descritos en la técnica. En algunas de estas formas de realización, el dispositivo electrónico 120 se puede configurar para ejecutar una o más posibles respuestas en caso de que detecte que la integridad del chip se ha visto comprometida, y/o en caso de que detecte intrusión en la caja del dispositivo. Estas respuestas pueden variar desde la eliminación de datos sensibles hasta la destrucción física de la totalidad o parte del dispositivo electrónico 120.

En ciertas formas de realización, el dispositivo electrónico 120 puede comprender además uno o más motores criptográficos 121, los cuales pueden ser usados por el supervisor 160, entre otras cosas, en el soporte de la verificación de certificados digitales. Estos motores criptográficos 121 se pueden configurar para implementar uno o más algoritmos criptográficos, tales como AES o RSA. El motor criptográfico 121 puede recibir datos del supervisor 160 para el cifrado o descifrado, y puede proporcionar el texto cifrado resultante (o texto plano, según

sea adecuado) de vuelta al supervisor 160. Por ejemplo, esta capacidad criptográfica se puede utilizar en la verificación de firmas digitales. En otras formas de realización, el supervisor 160 se puede configurar para ejecutar parte o la totalidad de la funcionalidad del motor criptográfico 121, y puede que no se necesite un motor criptográfico aparte 121.

Tal como se muestra en la Figura 1, el dispositivo electrónico 120 se puede conectar, por medio del enlace de comunicaciones 105, a una o más CAs 100. De acuerdo con la presente exposición, cada autoridad de certificación 100 puede tener un conjunto 101 de por lo menos dos claves privadas raíz 102. Para cada clave privada raíz 102, la CA puede tener un certificado digital raíz correspondiente (que contiene la clave pública correspondiente adecuada).

Cada clave privada raíz también puede tener un atributo de estado asociado, denominado, por ejemplo, “activo”, “latente”, o “revocado”. En una forma de realización de este tipo, una clave privada raíz 102 que tenga un estado “activo” puede ser usada por la CA 100 para firmar datos, tales como certificados digitales. Las claves privadas raíz 102 que presenten el estado “latente” pueden considerarse no disponibles en ese momento para ser usadas por la CA 100, aunque pueden ser elegibles para su uso en el futuro. La CA 100 puede almacenar de forma segura claves latentes, para evitar su pérdida o revelación a terceros no autorizados. Además, por motivos de seguridad, una vez que una clave privada raíz 102 se ha seleccionado como activa, puede resultar preferible garantizar que la misma no se pueda identificar erróneamente como latente. Finalmente, claves privadas raíz 102 que presenten un estado “revocado” pueden estar totalmente indisponibles para su uso por la CA 100. Por ejemplo, el estado revocado se puede usar para identificar toda clave que se haya visto comprometida.

En una forma de realización de acuerdo con la presente exposición, cada CA 100 puede tener un conjunto 101 de por lo menos cinco (5) claves privadas raíz 102. Se entenderá que, aunque el hecho de disponer de un número menor de claves privadas raíz 102 se sitúa dentro del alcance de la presente exposición, esto puede reducir la resistencia del sistema a ciertos tipos de ataques.

Cuando se fabrica un dispositivo electrónico 120, en el almacenamiento de certificados 141, para cada CA 100, se pueden almacenar por lo menos dos certificados digitales raíz (correspondientes a la totalidad o a un subconjunto del conjunto 101 de claves privadas raíz 102). Además, en el almacenamiento de atributos 142 se pueden almacenar uno o más atributos asociados a cada certificado raíz. Por ejemplo, el certificado raíz correspondiente a la clave privada raíz 102 que está siendo usado en ese momento por la CA 100 se puede designar como activo, y la totalidad del resto de certificados raíz se puede identificar como latentes. Después de la fabricación, el supervisor 160 del dispositivo electrónico 120 se puede configurar para usar únicamente certificados activos para la verificación de la firma de mensajes entrantes.

Se entenderá que una vez que los certificados raíz se han almacenado en el almacenamiento de certificados 141 (por ejemplo, durante la fabricación del dispositivo 120), es probable que estos certificados permanezcan en el almacenamiento de certificados 141 durante la vida útil del dispositivo – que puede ser de años. Por ejemplo, muchos dispositivos electrónicos 120, tales como televisores u ordenadores, se sustituyen solamente una vez cada varios años, y algunos se pueden utilizar durante una década o incluso más. Durante este periodo de tiempo prolongado, un usuario malicioso de un dispositivo electrónico 120 puede que disponga de la capacidad de acceder a una o más de las claves públicas de certificados raíz almacenadas en el dispositivo 120, y que intente usar el certificado raíz para obtener la clave privada correspondiente, lo cual puede derivar en que se ponga íntegramente en compromiso todo el sistema. Por lo tanto, en ciertas formas de realizaciones puede resultar preferible seleccionar el método de cifrado para el sistema completo de certificados, de tal manera que, durante un periodo de tiempo correspondiente, sea estadísticamente imposible para un usuario malicioso encontrar (por ejemplo, usando un ataque de fuerza bruta) la clave privada que se corresponde con la clave pública de cualquier certificado raíz almacenado en el dispositivo. Por ejemplo, en la actualidad se cree que una cierta longitud de clave (por ejemplo, 2.048 bits o más) del método de cifrado Rivest-Shamir-Adleman (RSA) puede dar cumplimiento a esta propiedad.

Con independencia del método de cifrado y la longitud de la clave, de cuando en cuando, una CA 100 puede llegar a la determinación de que puede resultar necesario invalidar una clave privada. Por ejemplo, esto puede ocurrir si la clave se ha vista comprometida, o como consecuencia de una política de expiración de claves. En tales casos, puede que sea necesario que la CA 100 sustituya una clave raíz privada con otra clave raíz privada existente o que revoque una clave privada. En los casos en los que la CA 100 ha sustituido o revocado una clave privada, puede que la misma desee además añadir una o más claves privadas nuevas al sistema. En la siguiente descripción se proporcionan sistemas, métodos y aparatos para cada una de estas operaciones.

Las Figuras 2 a 6 ilustran procesos ejemplificativos y estructuras de datos correspondientes mediante los cuales una clave raíz privada, y la correspondiente clave pública raíz y/o certificado raíz, se pueden sustituir por otra clave raíz privada y su correspondiente clave pública raíz y/o certificado.

En una primera forma de realización, la CA 100 puede revocar una clave privada que está activa en ese momento, y puede sustituirla con una clave privada latente (dentro de su conjunto de claves 101), que puede

convertirse en la nueva clave activa. Esta nueva clave privada activa se puede usar para firmar certificados digitales y llevar a cabo otras actividades basadas en claves raíz, y el certificado raíz correspondiente se puede usar para verificar estas firmas digitales. En un caso de este tipo, la CA 100 puede enviar un mensaje de sustitución de certificado a uno o más dispositivos electrónicos 120, que puede contener información referente al certificado raíz a sustituir, y puede contener además información referente a un certificado raíz sustitutorio que se debe activar.

La Figura 2 muestra un mensaje de sustitución de certificado 200, ejemplificativo, y el contenido de una unidad de gestión de certificados 166 ejemplificativa. Las Figuras 3A a 3C muestran procesos ejemplificativos por medio de los cuales un certificado activo en ese momento se puede sustituir en un dispositivo electrónico 120, tras la sustitución de la clave raíz privada 101 correspondiente por parte de una CA 100. Con fines explicativos, los procesos descritos con respecto a las Figuras 3A a 3C harán referencia a los valores del mensaje de sustitución de certificado 200 y la unidad de gestión de certificado 266 mostrados en la Figura 2. No obstante, se entenderá que estos valores son meramente ejemplificativos, y los métodos descritos están destinados a funcionar con cualquier valor adecuado.

La Figura 2 muestra una unidad de gestión de certificados 166 que tiene tres certificados raíz almacenados en el almacenamiento de certificados 141: certificados raíz A, B y C. El almacenamiento de atributos 142 tiene el estado del certificado raíz A listado como activo, y el estado de los certificados raíz B y C como latente.

En la etapa 310 (Figura 3A), el supervisor 160 puede recibir un mensaje 200 (Figura 2) de la CA 100 o por medio de uno o más servidores intermedios, por ejemplo, el servidor 110, y, basándose en el tipo de mensaje 201, puede determinar que el mensaje es un mensaje de sustitución de certificado 200 y se debería de gestionar de forma correspondiente. Este tipo de mensaje 201 puede ser cualesquiera datos adecuados para indicar que se trata de un mensaje de sustitución 200. Por ejemplo, tal como se muestra en la Figura 2, el tipo de mensaje 201 puede ser la cadena “Sustitución de Certificado”. En otras formas de realización, el tipo de mensaje 201 puede ser un entero que identifica de forma exclusiva el mensaje 200, como mensaje de sustitución.

Tal como se muestra en la Figura 2, además de su campo de tipo de mensaje 201, el mensaje de sustitución 200 puede comprender además información que describe el certificado que se debe revocar, y el certificado sustitutorio. Puede usarse un identificador de certificado revocado 210 para identificar el certificado raíz en el almacenamiento de certificados 141 cuya clave privada raíz correspondiente ha sido invalidada por la CA 100. En el ejemplo mostrado en la Figura 2, el identificador de certificado revocado 210 identifica el certificado raíz A como certificado raíz que se debe revocar. El identificador de certificado sustitutorio 215 se puede usar para identificar el certificado raíz del almacenamiento de certificados 141, cuya clave raíz correspondiente ha sido activada por la CA 100. En la Figura 2, el identificador de certificado sustitutorio 215 identifica el certificado raíz B como certificado raíz que debería activarse.

Las etapas 320 a 340 (Figura 3A), que se describen, cada una de ellas, de forma más detallada posteriormente, se pueden usar para verificar la autenticidad del mensaje de sustitución 200. Por ejemplo, en ciertas formas de realización, antes de que el mensaje de sustitución 200 se envíe al dispositivo electrónico 120, la CA 100 puede firmar digitalmente el mensaje de sustitución 200 usando dos o más (“N”) claves “de firma” privadas diferentes (que son un subconjunto del conjunto 101 de claves raíz privadas 102). Tal como se describirá de forma más detallada posteriormente, este uso de firmas digitales puede evitar la invalidación y/o sustitución no autorizadas del certificado raíz que está activo en ese momento. En función de la forma de realización, el número concreto N de claves de firma puede variar (por ejemplo, una forma de realización podría hacer que el mensaje 200 se firmase con cinco claves, mientras que, en otra forma de realización, el mensaje 200 puede haberse firmado solamente con dos claves), aunque, en cualquier forma de realización dada, este número N debe permanecer constante (y no puede superar el tamaño total del conjunto 101 de claves privadas raíz 102).

Por ejemplo, en una forma de realización ejemplificativa, puede que cada dispositivo 120 tenga la capacidad de almacenar hasta cinco claves, pero N puede ser solamente dos. En otra forma de realización ejemplificativa, cada dispositivo 120 puede tener la capacidad de almacenar siete claves, y N puede ser solamente dos. Todavía en otra forma de realización ejemplificativa, puede que cada dispositivo 120 tenga la capacidad de almacenar siete claves, y N puede ser igual a tres.

En ciertas formas de realización, las N claves de firma se seleccionan de entre solamente el subconjunto de claves dentro del conjunto 101 de claves privadas raíz 102 que están latentes; en otras palabras, la clave privada (activa) invalidada no se puede usar para firmar el mensaje de sustitución 200. En otras formas de realización, una de estas N claves de firma puede ser la clave privada raíz (activa) 102 que se está invalidando.

Adicionalmente, puede que se requiera que las N claves de firma incluyan la clave privada raíz sustitutoria; en otras palabras, puede requerirse que las N claves de firma incluyan la clave privada que se corresponde con el certificado digital (ya almacenado en el almacenamiento de certificados 141) que debería ser usado por el supervisor 160 del dispositivo electrónico 120 como nuevo certificado activo. (Se entenderá que, en formas de realización en las que las N claves de firma incluyen la clave privada que se está revocando, la clave privada raíz

sustitutoria no debería ser la clave privada que se está revocando, de tal manera que el certificado activo, nuevo, sea diferente del certificado revocado, antiguo).

En la forma de realización ejemplificativa que se muestra en la Figura 2, el cuerpo del mensaje de sustitución 200 (es decir, el identificador de certificado revocado 210 y el identificador de certificado sustitutorio 215) se puede firmar con dos claves de firma, de tal manera que el mensaje de sustitución 200 incluye dos firmas digitales, "Firma 1" 230 y "Firma 2" 231. Tal como se muestra en la Figura 2, la Firma 1 230 se creó usando la clave privada raíz asociada al certificado B, y la Firma 2 231 se creó usando la clave privada raíz asociada al certificado C. En ciertas formas de realización, puede resultar deseable hacer que una firma cubra la otra firma, por ejemplo, la Firma 2 231 puede cubrir la totalidad del identificador de certificado revocado 210, el identificador de certificado sustitutorio 215 y la Firma 1 230 como campos firmados; en otras formas de realización, la Firma 1 230 y la Firma 2 231 pueden ser independientes. No obstante, debe reconocerse que, opcionalmente, los componentes adicionales del mensaje de sustitución 200 también se pueden firmar de manera similar.

En ciertas formas de realización, el mensaje de sustitución 200 puede comprender además uno o más campos que identifican certificados los cuales se podrían usar para validar las N firmas. Por ejemplo, el mensaje de sustitución 200 puede incluir campos que identifiquen un subconjunto de los certificados asociados al conjunto de claves privadas raíz 101 y almacenados previamente en el almacenamiento de certificados 141. Estos identificadores de certificados se pueden usar para aportar al supervisor 160 alguna idea de los certificados que debería probar, según se describe de forma más detallada posteriormente, con el fin de validar la N firmas. Tal como se muestra en la Figura 2, por ejemplo, los campos identificadores de certificados 220 y 221 identifican los certificados B y C como certificados que se deberían probar con la finalidad de verificar, respectivamente, la Firma 230 y la Firma 1 231. Esto puede hacer que mejore la eficiencia del sistema, ya que, en lugar de que el supervisor 160 pruebe a validar cada firma (por ejemplo, la Firma 1 230) usando cada certificado del almacenamiento de certificados 141, únicamente es necesario que pruebe a usar los certificados específicos identificados (usando los identificadores de certificado, por ejemplo, 220) en el mensaje de sustitución 200.

En la etapa 320 (Figura 3A), el supervisor 160 puede verificar que el mensaje de sustitución recibido 200 presenta la totalidad de las N firmas. Por ejemplo, tal como se muestra en la Figura 2, el mensaje de sustitución tiene dos firmas, según lo esperado.

En la etapa 323 (Figura 3A), el supervisor 160 puede verificar que esas N firmas se pueden verificar usando los certificados digitales correspondientes previamente almacenados (por ejemplo, en el momento de la fabricación) en el almacenamiento de certificados 141. Por ejemplo, tal como se muestra en la Figura 2, las dos firmas 230, 231 se pueden verificar usando certificados raíz B y C almacenados. Así, se entenderá que, puesto que cada mensaje de sustitución 200 se firma usando N claves privadas del conjunto 101 de claves privadas raíz 102, con el fin de invalidar cualquier certificado raíz almacenado en el dispositivo electrónico 120, un atacante debe tener por lo menos N claves privadas. En formas de realización en las que el mensaje de sustitución 200 incluye campos identificadores de certificados, por ejemplo, 220 y 221 según se muestra en la Figura 2, el supervisor 160 puede usar esos identificadores para reducir el número de certificados que se prueba con el fin de validar las dos firmas 230, 231.

En la etapa 326 (Figura 3A), el supervisor 160 puede verificar que los certificados digitales correspondientes ubicados en el almacenamiento de certificados 141 no se ha marcado como revocados en el almacenamiento de atributos 142 correspondientes. En el ejemplo anterior, ninguno de los certificados raíz B o C, según se muestra en la Figura 2, se ha marcado como revocado en el almacenamiento de atributos 141.

En algunas formas de realización, puede resultar preferible garantizar además que las N firmas 230, 231 se puedan verificar únicamente mediante certificados digitales (situados dentro del almacenamiento 141) identificados específicamente como latentes. En el ejemplo anterior, los dos certificados raíz B y C se muestran como latentes en el almacenamiento de atributos 141.

En la etapa 330 (Figura 3A), el supervisor 160 puede confirmar que el identificador de certificado sustitutorio 215 remite a un certificado ya almacenado en el almacenamiento de certificado 141, y en la etapa 335 puede verificar además que cualquier atributo de estado de este certificado (según está almacenado en el almacenamiento de atributos 142) es latente. En el ejemplo mostrado en la Figura 2, el identificador de certificado sustitutorio 215 remite al certificado raíz B, que se muestra como presente en el almacenamiento de certificados 141, y que se muestra de manera que tiene un estado de latente en el almacenamiento de atributos 142.

En la etapa 340 (Figura 3A), el supervisor 160 puede verificar que el certificado sustitutorio identificado por el identificador de certificado sustitutorio 215, es decir, el certificado raíz activo nuevo, se corresponde con una de las N firmas (por ejemplo, 230 o 231 en la Figura 2) del mensaje 200. En el ejemplo mostrado en la Figura 2, el certificado sustitutorio identificado por el identificador de certificado sustitutorio 215 es el certificado raíz B. Se corresponde con la Firma 1, mostrada como 230 en la Figura 2.

Si falla cualquiera de las verificaciones llevadas a cabo en cualquiera de las etapas 320 a 340, el supervisor 160 no puede realizar ninguna operación de sustitución adicional pero, en algunas formas de realización, puede intentar, en la etapa 350, notificar (de manera directa o indirecta por medio de uno o más servidores adicionales) a la CA 100 una infracción de su política. Dicha notificación puede incluir, por ejemplo, el mensaje de sustitución 200 recibido por el dispositivo electrónico 120 y cualquier otra información adecuada, tal como la razón específica por la que falló el método. En caso contrario, si todas las verificaciones llevadas a cabo en las etapas 320 a 340 se superan con éxito, el supervisor 160 puede proseguir con el procesado de la sustitución del certificado.

Las Figuras 3B y 3C muestran métodos diferentes para invalidar el certificado asociado a la clave privada raíz revocada y sustituirlo con el certificado activo, nuevo. En la forma de realización mostrada con respecto a la Figura 3B, en la etapa 360, el supervisor 160 puede determinar si debería revocarse el certificado activo en ese momento. Esto se puede determinar, por ejemplo, comparando el identificador de certificado revocado 210 con el identificador de certificado del certificado activo actual. Por ejemplo, en la Figura 2, el identificador de certificado revocado 210 lista el certificado raíz A como certificado que se debe revocar. El almacenamiento de atributos 142 muestra el estado del certificado raíz A como activo.

Si los dos identificadores coinciden, el método puede proseguir hacia la etapa 365 (Figura 3B) y el supervisor 160 puede actualizar el estado del certificado actual como revocado (por ejemplo, en el almacenamiento de atributos 142). De este modo, en el ejemplo mostrado en la Figura 2, el estado del certificado raíz A debería actualizarse a revocado en el almacenamiento de atributos 142. Si los dos identificadores no coinciden – es decir, el certificado que está siendo revocado por la CA 100 no es el mismo que el certificado activo dentro del dispositivo electrónico 120 – entonces, en la etapa 367, el supervisor 160 puede actualizar como latente el estado del certificado activo en ese momento.

En la etapa 370 (Figura 3B), el supervisor 160 puede actualizar como activo el estado del certificado al que remite el identificador de certificado sustitutorio 215 (por ejemplo, en almacenamiento de atributos 142), y en la etapa 375, el supervisor 160 puede comenzar a usar el nuevo certificado raíz activo para cualquier verificación de certificados. En el ejemplo mostrado en la Figura 2, el certificado raíz B es identificado por el identificador de certificado sustitutorio 215; como consecuencia, su estado en el almacenamiento de atributos 142 debería actualizarse a activo.

En otra forma de realización, el certificado asociado a la clave privada raíz revocada se puede invalidar y sustituir tal como se muestra en la Figura 3C. Muchas de las etapas descritas con respecto a la Figura 3C son análogas a etapas descritas con respecto a 3B.

En el método descrito en la Figura 3C, después de la etapa 340 de la Figura 3A, en la etapa 380, el supervisor 160 puede determinar si debería revocarse el certificado activo en ese momento. Esto se puede determinar, por ejemplo, comparando el identificador de certificado revocado 210 con el identificador de certificado del certificado activo actual. Por ejemplo, en la Figura 2, el identificador de certificado revocado 210 lista el certificado raíz A como certificado que se debe revocar. El almacenamiento de atributos 142 muestra el estado del certificado raíz A como activo.

Si los dos identificadores coinciden, el método puede proseguir a la etapa 382, y el supervisor 160 puede actualizar el estado del certificado actual como revocado (por ejemplo, en el almacenamiento de atributos 142). De este modo, en el ejemplo mostrado en la Figura 2, el estado del certificado raíz A se debería actualizar a revocado en el almacenamiento de atributos 142.

En la etapa 384 (Figura 3C), el supervisor 160 puede actualizar como activo el estado del certificado al que remite el identificador de certificado sustitutorio 215 (por ejemplo, en el almacenamiento de atributos 142), y en la etapa 386, el supervisor 160 puede comenzar a usar el nuevo certificado raíz activo para cualquier verificación de certificados. En el ejemplo mostrado en la Figura 2, el certificado raíz B es identificado por el identificador de certificado sustitutorio 215; como consecuencia, su estado en el almacenamiento de atributos 142 debería actualizarse a activo.

No obstante, si, en la etapa 380, el identificador de certificado revocado 210 y el identificador de certificado correspondiente al certificado activo actual no coinciden – es decir, el certificado que está siendo revocado por la CA 100 no es el mismo que el certificado activo en el dispositivo electrónico 120 – entonces, el supervisor 160 no puede llevar a cabo ninguna operación de sustitución aunque, en algunas formas de realización, en la etapa 390, puede intentar notificar (de manera directa o indirecta por medio de uno o más servidores adicionales) a la CA 100 la incongruencia del mensaje de sustitución 200 con el estado de ese momento de certificados dentro del dispositivo electrónico 120. Esta notificación puede incluir el presente mensaje de sustitución 200 así como el mensaje de sustitución 200 inmediatamente anterior sobre cuya base el último certificado activo recibió su estado (en la medida en la que dicho mensaje de sustitución inmediatamente anterior pueda existir).

El método ejemplificativo descrito con respecto a las Figuras 3A a 3C mostraba cómo puede sustituirse una única clave raíz privada 102 de acuerdo con la presente exposición. De este modo, si solamente se ha visto comprometida una clave privada raíz 102 – suponiendo que la CA 100 conoce específicamente qué clave raíz privada 102 se ha visto comprometida –, la CA 100 puede ejecutar el procedimiento de sustitución descrito con respecto a las Figuras 3A a 3C. No obstante, tal como se describirá posteriormente, este método se puede modificar para sustituir múltiples certificados raíz.

La Figura 4 muestra un procedimiento ejemplificativo de sustitución de claves raíz privadas para dos certificados raíz, en el que una de las claves a sustituir es el certificado activo. No obstante, se entenderá que el método descrito en la presente se puede usar para un número cualquiera de certificados. Como en los métodos descritos con respecto a las Figuras 3A a 3C, el método descrito con respecto a la Figura 4 supone que la CA 100 conoce de manera específica qué dos claves raíz privadas deben sustituirse. La Figura 5 (análoga a la Figura 2) muestra el contenido de una unidad de gestión de certificados 166 ejemplificativa y los valores de dos mensajes de sustitución de certificado. Con fines explicativos, los procesos descritos con respecto a la Figura 4 harán referencia a los valores de los mensajes de sustitución de certificado y la unidad de gestión de certificados 166 mostrados en la Figura 5. No obstante, se entenderá que estos valores son meramente ejemplificativos y los métodos descritos están destinados a funcionar con cualquier valor adecuado.

Tal como se muestra en la Figura 5, una unidad de gestión de certificados 166 ejemplificativa tiene cinco certificados raíz almacenados en el almacenamiento de certificados 141: certificados raíz A, B, C, D y E. El almacenamiento de atributos 142 tiene el estado del certificado raíz A listado como activo, y el estado de los certificados raíz B, C, D y E como latente. La CA sabe que se han visto comprometidas claves privadas raíz correspondientes a los certificados raíz A y B.

En la etapa 405, la CA 100 puede crear un primer mensaje de sustitución 500 que invalida el certificado activo en ese momento (es decir, el certificado correspondiente a una de las dos claves raíz privadas a sustituir) y que lo sustituye con el certificado correspondiente a la segunda clave raíz comprometida. El primer mensaje de sustitución 500 se puede firmar con la segunda clave comprometida y una tercera clave no comprometida. Así, en el ejemplo mostrado en la Figura 5, el certificado raíz A es el certificado activo de ese momento en la unidad de gestión de certificados 166, y debería sustituirse por el certificado raíz B. El primer mensaje de sustitución 500 se ha firmado con las claves privadas raíz correspondientes al certificado B (comprometido) y al certificado C (no comprometido).

En la etapa 410, la CA 100 puede crear un segundo mensaje de sustitución 510 que invalida el certificado activo de ese momento (que, tal como se describirá posteriormente, será el certificado sustitutorio identificado en el primer mensaje de sustitución 500) y que lo sustituye con un certificado correspondiente a una clave no comprometida. Este segundo mensaje de sustitución 510 se puede firmar con dos claves no comprometidas. Así, en el ejemplo mostrado en la Figura 5, el certificado raíz B se considera el certificado activo del momento y debería sustituirse por el certificado raíz C. El segundo mensaje de sustitución 510 se ha firmado con las claves raíz privadas correspondientes a los certificados C y D (ambos no comprometidos).

Cabe indicar que, en formas de realización en las que una de las firmas de un mensaje de sustitución se puede crear usando la clave privada activa de ese momento, entonces el primer certificado se puede sustituir usando las dos claves comprometidas, y el segundo certificado se puede sustituir usando una de las claves comprometidas y una segunda clave, no comprometida.

Tal como se muestra en la Figura 5, cada mensaje de sustitución 500, 510 puede poseer algunos de los mismos campos que el mensaje de sustitución 200 descrito con respecto a la Figura 2, con la añadidura de tres campos adicionales: un indicador de mensaje-previo-requerido 540, 560, un indicador de mensaje-sucesivo-requerido 541, 561, y un valor *hash* del mensaje sucesivo 551, 571. Estos campos se pueden usar para imponer la integridad de mensajes de sustitución usados para sustituir varios certificados en un único proceso.

En una forma de realización ejemplificativa, el primer mensaje de sustitución 500 puede fijar el indicador de mensaje-sucesivo-requerido 541 de manera que requiera un segundo mensaje, subsiguiente, por ejemplo, el segundo mensaje de sustitución 510. (Se entenderá que el valor de este indicador 541 puede ser cualquiera adecuado, incluyendo valores booleanos tales como sí/no, 1/0, etcétera). Por consiguiente, el primer mensaje de sustitución 500 también puede incluir, en el campo 551, un valor *hash* del segundo mensaje de sustitución 510. Este valor *hash* puede ser un valor *hash* del segundo mensaje de sustitución 510 completo, con o sin su firma. Como este es el primer mensaje de sustitución en la cadena, el indicador de mensaje-previo-requerido 540 se puede fijar para indicar que no se requiere ningún mensaje previo.

De manera similar, el segundo mensaje de sustitución 510 se puede crear de tal manera que el indicador de mensaje-previo-requerido 560 se fije para requerir un mensaje previo, por ejemplo, el primer mensaje de sustitución 500. El indicador de mensaje-sucesivo-requerido 561 se puede fijar para indicar que no se requiere ningún mensaje subsiguiente, y el valor correspondiente del campo 571 se puede fijar a cualquier valor.

Se entenderá que, en una forma de realización ejemplificativa del tipo mencionado, puede que resulte necesario calcular todos los valores *hash* y firmas requeridos en un orden particular. Por ejemplo, puede que resulte necesario calcular el valor *hash* y la firma para el último mensaje en la cadena de mensajes en primer lugar, a continuación para el penúltimo mensaje de la cadena de mensajes, y así sucesivamente.

Se entenderá además que la descripción anterior mostrada con respecto a la Figura 5 es meramente ejemplificativa, y que puede lograrse el mismo efecto, por ejemplo, usando un valor *hash* del mensaje previo en lugar de un valor *hash* de un mensaje sucesivo. En tales formas de realización, puede que resulte preferible calcular valores *hash* y firmas comenzando con el primer mensaje y concluyendo con el último mensaje de la cadena de mensajes.

En la etapa 415 (Figura 4), la CA 100 puede enviar el primer mensaje de sustitución 500 al dispositivo electrónico 120, y, en la etapa 420, la CA 100 puede enviar el segundo mensaje de sustitución 510 al dispositivo electrónico 120. Basándose en los tipos de mensaje correspondientes a cada mensaje 500, 510, el supervisor 160 podrá determinar que los mismos son mensajes de sustitución de certificado, y podrá proceder de forma correspondiente.

En la etapa 425, el supervisor 160 puede determinar si se han cumplido las condiciones fijadas por los indicadores en cada uno de los dos mensajes de sustitución (por ejemplo, 540, 541, 560 y 561). Por ejemplo, el supervisor 160, que percibe que el primer mensaje de sustitución 500 tiene el indicador de mensaje-sucesivo-requerido 541 fijado de manera que requiere un mensaje subsiguiente, puede confirmar que (i) recibió un segundo mensaje de sustitución 510, y que (ii) el valor *hash* del segundo mensaje de sustitución 510 tiene el mismo valor que el correspondiente recibido en el campo de datos 551 del primer mensaje de sustitución 500.

De manera similar, al percibir que el segundo mensaje de sustitución 510 tiene el indicador de mensaje-previo-requerido 540 fijado de manera que requiere un mensaje previo, el supervisor 160 puede confirmar que recibió un primer mensaje de sustitución 500.

Si en la etapa 425 se han cumplido todas las condiciones fijadas por los indicadores, en la etapa 430, el supervisor 160 puede procesar el primer mensaje de sustitución 500 (por ejemplo, según se ha descrito con respecto a las Figuras 3A a 3C, anteriormente), y en la etapa 435, el supervisor 160 puede procesar el segundo mensaje de sustitución 510. En el ejemplo mostrado en la Figura 5, tras completarse la etapa 435, se han sustituido los dos certificados A y B, y el certificado C es el certificado activo en ese momento.

En formas de realización que usan esta estructura, la secuencia de mensajes forma efectivamente una “cadena de mensajes” (no confundir con una “cadena de certificados” tradicional). En ciertas formas de realización, puede resultar deseable procesar estos mensajes atómicamente, estando los mensajes vinculados entre sí para garantizar que no se pueden procesar por separado. En su lugar, o bien una cadena completa de mansajes se puede procesar de manera conjunta, o, si, por algún motivo, un mensaje de la cadena es no válido, no se procesa ninguno de los mensajes. En este sentido, cada cadena de mensajes se puede considerar atómica, o indivisible, con vistas al procesado, y el dispositivo electrónico 120 no se puede dejar en un estado intermedio. O bien (i) el estado de las claves públicas raíz se debería cambiar para hacer aplicables todos los mensajes de la cadena, o bien (ii) el estado de las claves públicas raíz no se debería cambiar en absoluto.

En otras formas de realización, puede que resulte deseable usar un segundo tipo de procesado atómico de mensajes, de tal manera que si uno de los mensajes de la cadena de mensajes no es válido (es decir, no se satisfacen las condiciones de validez descritas anteriormente), el mensaje no válido de la cadena de mensajes se salta. Aquellos mensajes que son válidos se usan para formar una segunda cadena (temporal) de mensajes, que comprende los mensajes válidos de la cadena original, y, en el mismo orden, pero sin los mensajes no válidos. A continuación, esta segunda cadena temporal de mensajes se procesa atómicamente, según se ha descrito anteriormente. Esta lógica puede resultar útil en algunos escenarios, tales como, por ejemplo, si diferentes dispositivos existentes 120 presentan estados diferentes (lo cual puede ocurrir, por ejemplo, como consecuencia de ciertos ataques en un sistema que tiene múltiples dispositivos 120). Este segundo tipo de procesado atómico se puede usar para aplicar la misma cadena de manera que los dispositivos 120 – que se encuentran en estados no válidos, diferentes – se lleven a un único estado válido.

Un escenario ejemplificativo del tipo mencionado puede ser el siguiente: un atacante puede tener el control de dos claves latentes D1 y D2, y puede emitir dos conjuntos de mensajes usando estas claves latentes: (a) para algunos dispositivos 120, el atacante puede emitir mensajes que sustituyen la clave activa A por la clave latente D1, y (b) para otros dispositivos 120, el atacante puede emitir mensajes que sustituyen la clave activa A por la clave latente D2. Por consiguiente, algunos dispositivos 120 tendrán la clave D1 como activa, y otros tendrán la clave D2 como activa. Para remediar esta situación, si las claves C1 y C2 no se han visto todavía comprometidas, la CA puede emitir la siguiente cadena de mensajes para todos los dispositivos: (a) “sustituir D1 por C1” (firmado con C1 y C2), y (b) “sustituir D2 por C1” (firmado con C1 y C2). Si se realiza un procesado tal como se ha descrito anteriormente, usando este segundo tipo de procesado atómico, en los dispositivos en los que D1 era la clave activa, la parte (b) de la cadena de mensajes se saltará; en los dispositivos en los que D2 era

la clave activa, la parte (a) de la cadena de mensajes se saltará. Como consecuencia, todos los dispositivos se situarán en el mismo estado válido (siendo C1 la clave activa) con independencia de si un dispositivo específico tiene D1 o D2 como clave activa.

El método descrito con respecto a la Figura 4 consideraba que una de las dos claves raíz privadas comprometidas se correspondía con el certificado entonces activo en el dispositivo electrónico 120. La Figura 6 muestra un método ejemplificativo por el cual los certificados se pueden sustituir cuando las dos claves privadas comprometidas 102 se corresponden con certificados latentes en el dispositivo electrónico 120. Igual que en la Figura 4, la Figura 6 muestra un procedimiento ejemplificativo de sustitución de claves raíz privadas para dos certificados raíz; no obstante, se entenderá que el método descrito en dicha figura se puede usar para un número cualquiera de certificados.

En la etapa 605, la CA 100 puede crear un primer mensaje de sustitución que invalida el certificado activo de ese momento (que no se corresponde con una de las dos claves raíz privadas a sustituir) y que lo sustituye por el certificado correspondiente a la primera clave raíz comprometida. El primer mensaje de sustitución se puede firmar con la primera y la segunda claves comprometidas.

En la etapa 610, la CA 100 puede crear un segundo mensaje de sustitución que invalida el certificado activo de ese momento (que es el certificado sustitutorio correspondiente a la primera clave comprometida e identificado en el primer mensaje de sustitución) y que lo sustituye por un certificado correspondiente a la segunda clave comprometida. Este segundo mensaje de sustitución se puede firmar con la segunda clave comprometida y una clave no comprometida.

En la etapa 615, la CA 100 puede crear un tercer mensaje de sustitución que invalida el certificado activo de este momento (que es el certificado sustitutorio correspondiente a la segunda clave comprometida e identificado en el segundo mensaje de sustitución) y que lo sustituye por un certificado correspondiente a una clave no comprometida. Este tercer mensaje de sustitución se puede firmar con dos claves no comprometidas.

Igual que en la Figura 4, estos tres mensajes de sustitución deberían constituir una secuencia; como consecuencia, cada mensaje de sustitución debería tener fijados de manera correspondiente sus indicadores de mensaje-previo-requerido y mensaje-sucesivo-requerido (y, cuando proceda, el valor *hash* del mensaje sucesivo).

En la etapa 620, la CA 100 puede enviar el primer mensaje de sustitución al dispositivo electrónico 120, en la etapa 625, la CA 100 puede enviar el segundo mensaje de sustitución al dispositivo electrónico 120, y en la etapa 630, la CA 100 puede enviar el tercer mensaje de sustitución al dispositivo electrónico.

En la etapa 635, tras determinar que cada uno de estos mensajes es un mensaje de sustitución, el supervisor 160 puede determinar si se han cumplido las condiciones fijadas por los indicadores en cada uno de los tres mensajes de sustitución. Por ejemplo, el supervisor 160, que percibe que el primer mensaje de sustitución tiene el indicador de mensaje-sucesivo-requerido fijado de manera que requiere un mensaje subsiguiente, puede confirmar que (i) recibió un segundo mensaje de sustitución, y que (ii) el valor *hash* del segundo mensaje de sustitución tiene el mismo valor que el correspondiente recibido en el campo de datos *hash* del primer mensaje de sustitución. Este mismo procedimiento se puede llevar a cabo para el segundo y el tercer mensajes de sustitución.

Si, en la etapa 635, se han cumplido todas las condiciones fijadas por los indicadores, en la etapa 640, el supervisor 160 puede procesar el primer mensaje de sustitución (por ejemplo, según se ha descrito anteriormente con respecto a las Figuras 3A a 3C), en la etapa 645, el supervisor 160 puede procesar el segundo mensaje de sustitución, y en la etapa 650, el supervisor 160 puede procesar el tercer mensaje de sustitución. Al final de la etapa 650, se habrán sustituido tres claves (la clave activa y las dos claves latentes, comprometidas), y se habrá activado una clave no comprometida.

Los métodos y estructuras de datos descritos con respecto a las Figuras 2 y 6 mostraban cómo pueden sustituirse uno o más certificados. No obstante, en el método ejemplificativo mostrado con respecto a la Figura 6, en el cual se sustituyen dos certificados latentes, en el transcurso de la invalidación de las dos claves latentes se revocó también la clave activa vigente en ese momento. Por consiguiente, en ciertas formas de realización, puede que resulte preferible llevar a cabo uno o más procedimientos que simplemente revocan (sin sustituir) una única clave raíz privada.

Se entenderá que es posible que resulte deseable restringir el uso de los procedimientos de revocación descritos en la presente a solamente claves raíz latentes; es decir, puede que no resulte deseable utilizar un procedimiento de revocación con respecto a una clave privada activa. Si fuera a utilizarse un procedimiento de revocación con respecto a una clave raíz activa – sin una sustitución subsiguiente de la clave revocada – los sistemas que usan estos certificados no tendrían ninguna clave activa para ser utilizada con vistas a las verificaciones de certificados.

En una forma de realización, el sistema se puede configurar para procesar una revocación de un certificado latente sobre la base de una o más “notas de autorrevocación”, las cuales pueden ser cualquier tipo de mensaje de auto-autenticación adecuado para identificar una clave raíz privada 102 que se debería revocar. Una nota de autorrevocación puede ser preparada por una CA 100 de antemano con respecto a la ejecución de cualquier operación de revocación. Por ejemplo, en ciertas formas de realización, puede prepararse una nota de autorrevocación inmediatamente tras la producción de una clave privada raíz. Aunque la CA 100 puede preparar notas de autorrevocación 700 de antemano, puede que resulte deseable almacenar estas notas 700 por separado con respecto a las propias claves 101, para reducir la posibilidad de una pérdida simultánea tanto de una clave 102 como de la nota de autorrevocación 700 correspondiente. En ciertas formas de realización, cada nota de autorrevocación se puede almacenar con la misma seguridad con la que se almacena su clave raíz privada correspondiente.

La Figura 7 muestra una nota de autorrevocación 700 ejemplificativa, un mensaje de revocación de certificado latente 710 correspondiente, y el contenido de una unidad de gestión de certificado 166 ejemplificativa. La Figura 8 muestra un proceso ejemplificativo por el cual un certificado latente se puede sustituir en un dispositivo electrónico 120 tras la revocación de la clave raíz privada 101 correspondiente por parte de una CA 100. Con fines explicativos, el proceso descrito con respecto a la Figura 8 hará referencia a los valores de la nota de autorrevocación 700, del mensaje de revocación de certificado latente 710 y de la unidad de gestión de certificados 166 mostrados en la Figura 7. No obstante, se entenderá que estos valores son meramente ejemplificativos y que los métodos descritos están destinados a funcionar con cualquier valor adecuado.

Tal como se muestra en la Figura 7, una nota de autorrevocación 700 puede tener tres campos: (1) un tipo de nota 702, que puede ser cualesquiera datos adecuados que se utilicen para indicar que se trata de una nota de autorrevocación 700 (tal como la cadena “Autorrevocación”, según se muestra en la Figura 7); (2) un identificador de certificado revocado 704, el cual puede identificar el certificado correspondiente a la clave privada raíz latente 102 que se debe revocar; y (3) una firma digital de nota de autorrevocación 706, que puede ser una firma digital que abarca tanto el tipo de nota 702 como el identificador de certificado 704, creado con el uso de la clave raíz privada 102 correspondiente al identificador de certificado revocado 704. Por ejemplo, en la forma de realización ejemplificativa mostrada en la Figura 7, se va a revocar el certificado B, y la nota de autorrevocación 700 incluye una firma digital creada con el uso de la clave privada raíz correspondiente al certificado B.

La Figura 7 muestra también un mensaje de revocación de clave latente 710 ejemplificativo que se puede usar conjuntamente con una nota de autorrevocación 700. Tal como se muestra en la Figura 7, este mensaje de revocación de clave latente puede comprender: (1) tipo de mensaje 701, que puede ser cualesquiera datos adecuados usados para indicar que se trata de un mensaje de revocación 710; (2) una nota de autorrevocación 700, que identifica el certificado correspondiente a la clave latente que se debe revocar; y (3) dos firmas digitales, “Firma 1” 730 y “Firma 2” 731, que firman el mensaje de revocación de clave latente 710. Aunque el ejemplo anterior describe el uso de dos firmas digitales, se entenderá que la invención no se limita a dos firmas, y que, en algunas formas de realización, el número de firmas puede ser diferente, tal como uno, o tres o más.

En una forma de realización, puede que resulte deseable firmar el mensaje de revocación de clave latente 710 usando dos claves latentes. En otra forma de realización, una de las claves de firma puede ser una clave activa en ese momento. Por ejemplo, en la forma de realización ejemplificativa mostrada en la Figura 7, se va a revocar el certificado B, y el mensaje de revocación de clave latente 710 se ha firmado con la clave activa de ese momento (es decir, la clave privada raíz 102 correspondiente al certificado A) y una clave latente (es decir, la clave privada raíz 102 correspondiente al certificado C).

En algunas formas de realización, en lugar de usar la nota de autorrevocación 700 para identificar el certificado que se debe revocar, el mensaje de revocación de clave latente 710 puede comprender un identificador de certificado latente revocado (no mostrado). En tales formas de realización, el mensaje de revocación de clave latente 710 debería venir acompañado por la nota de autorrevocación 700 que se corresponde con el certificado que se está revocando.

Se entenderá que, a efectos de la forma de realización ejemplificativa descrita en este momento, no hay ningún “identificador de certificado sustitutorio” (según se ha descrito con respecto a la Figura 2), ya que no hay necesidad de sustituir el certificado activo en ese momento; solamente se está revocando un certificado latente, es decir, no utilizado.

La Figura 8 muestra un proceso ejemplificativo por el cual puede revocarse un certificado latente en ese momento en un dispositivo electrónico 120, tras la revocación de la clave raíz privada correspondiente 101 por una CA 100. Nuevamente, se entenderá que, a efectos del método ejemplificativo descrito en este momento, no hay ninguna necesidad de sustituir el certificado activo de ese momento, en la medida en la que se está revocando únicamente un certificado latente.

En la etapa 810, el supervisor 160 puede recibir un mensaje de revocación de certificado latente 710 y una nota de autorrevocación asociada 700 (Figura 7). Este mensaje se puede enviar al supervisor 160 directamente por la CA 100 o por medio de uno o más servidores intermedios, por ejemplo, el servidor 110, y se puede identificar como un mensaje de revocación de certificado latente 710 basándose en el tipo de mensaje 701.

Las etapas 820 a 835, cada una de las cuales se describirá de forma más detallada posteriormente, pueden usarse para verificar la autenticidad del mensaje de revocación de certificado latente 710 y la nota de autorrevocación asociada 700.

En la etapa 820, el supervisor 160 puede verificar las firmas digitales recibidas dentro del mensaje de revocación de certificado latente, por ejemplo, la Firma 1 730 y la Firma 2 731. Esto puede incluir una serie de sub-etapas, incluyendo la verificación de que el mensaje de revocación de certificado latente 710 incluye el número correcto de firmas y que las claves de firma no fueron revocadas previamente, según se ha descrito, por ejemplo, con respecto a las etapas 320 a 326 mostradas en la Figura 3.

En formas de realización que requieren todas las firmas digitales en el mensaje de revocación de certificado latente que se va a firmar con las claves latentes, en la etapa 825, el supervisor 160 puede verificar que todas las firmas digitales en el mensaje de revocación de certificado latente fueron firmadas realmente con claves latentes.

En la etapa 830, el supervisor 160 puede verificar que ha recibido una nota de autorrevocación 700 legítima. Esto puede incluir la verificación de que el tipo de nota 702 describe los datos recibidos como nota de autorrevocación 700, y puede incluir además la verificación de que la firma digital 706 (dentro de la nota de autorrevocación 700) y el certificado almacenado correspondiente a la clave raíz privada identificada por el identificador de certificado latente revocado 704 coinciden, es decir, que la nota de autorrevocación 700 se firmó de manera digital realmente con la clave que se debe revocar.

En la etapa 835, el supervisor 160 puede confirmar que el certificado correspondiente a la clave identificada es latente.

Si falla cualquiera de las verificaciones llevadas a cabo en cualquiera de las etapas 820 a 835, el supervisor 160 no puede ejecutar ninguna operación de revocación adicional aunque, en la etapa 850, puede intentar notificar (de manera directa o indirecta por medio de uno o más servidores adicionales) a la CA 100 una infracción de la política. Dicha notificación puede incluir, por ejemplo, el mensaje de revocación de certificado latente 710 y la nota de autorrevocación 700 recibida por el dispositivo electrónico 120 y cualquier otra información adecuada, tal como el motivo específico por el que falló el método. En caso contrario, si todas las verificaciones llevadas a cabo en las etapas 820 a 835 se superan con éxito, en la etapa 840, el supervisor 160 puede cambiar el estado del certificado identificado a revocado.

Se entenderá que, incluso si se roba una clave raíz privada 102 (por ejemplo, de tal manera que la clave 102 se encuentra en posesión de un atacante, pero no en posesión de la CA) o si la misma se destruye, siempre que su nota de autorrevocación 700 permanezca en posesión de la CA 100 respectiva, esta nota de autorrevocación 700 se puede usar para revocar el certificado digital correspondiente. Adicionalmente, incluso si un atacante dispone de dos claves, el atacante no puede revocar ninguna otra clave latente sin una nota de autorrevocación para esa otra clave.

La descripción anterior con respecto a las Figuras 7 y 8 describía un proceso por el cual se puede revocar de manera directa una única clave latente usando una nota de autorrevocación 700. No obstante, en ciertas circunstancias, puede que resulte deseable usar notas de autorrevocación 700 para revocar múltiples claves latentes. En ciertas formas de realización, el método mostrado con respecto a la Figura 8 simplemente se podría repetir para cada clave latente que se debe revocar. En otras formas de realización, puede que resulte preferible usar una variante con respecto al método descrito en relación con la Figura 6, en el que cada mensaje de revocación de clave latente 710 puede comprender además campos de mensaje-sucesivo-requerido, mensaje-previo-requerido, y *hash*-mensaje-sucesivo, por ejemplo, según se ha descrito con respecto a la Figura 5.

Puesto que la revocación de claves reducirá el número de claves válidas restantes, en algunas formas de realización puede que resulte deseable proporcionar un mecanismo por el cual pueda añadirse una nueva clave privada raíz al sistema, y pueda cargarse un certificado correspondiente en el dispositivo electrónico 120. Se entenderá que, en dichas formas de realización, puede que sea necesario que el almacenamiento de certificados 141 sea escribible (es decir, no de solo lectura).

La Figura 9 muestra un mensaje de certificado nuevo 900 ejemplificativo y el contenido de una unidad de gestión de certificados 166 ejemplificativa. La Figura 10 muestra un proceso ejemplificativo por el cual puede añadirse un certificado nuevo a un dispositivo electrónico 120, tras la creación de una nueva clave raíz privada 101 por parte de una CA 100. Con fines explicativos, el proceso descrito con respecto a la Figura 10 hará referencia a los valores del mensaje de certificado nuevo 900 y la unidad de gestión de certificados 166 mostrados en la Figura 9.

No obstante, se entenderá que estos valores son meramente ejemplificativos, y los métodos descritos están destinados a funcionar con cualquier valor adecuado.

Tal como se muestra en la Figura 9, un mensaje de certificado nuevo 900 puede tener cuatro o más campos: (1) tipo de mensaje 901, que puede ser cualesquiera datos adecuados que se usen para indicar que se trata de un mensaje de revocación 900; (2) un identificador de certificado nuevo 902, el cual puede identificar el certificado nuevo correspondiente a la clave privada raíz nueva 102; (3) el certificado nuevo (o clave pública raíz) 904; y (4) una o más firmas digitales, pudiendo una o más claves raíz privadas existentes 102 ser usadas para firmar digitalmente el identificador de certificado nuevo 902 y el certificado nuevo 904. Por ejemplo, para mejorar la seguridad global del sistema, en una forma de realización ejemplificativa, puede que resulte preferible firmar digitalmente el identificador de certificado nuevo 902 y el certificado nuevo 904 con la totalidad de las claves no revocadas, restantes (ya sean activas o latentes). En la forma de realización ejemplificativa mostrada en la Figura 9, se ha revocado el certificado A, y el mensaje de certificado nuevo 900, que identifica el certificado nuevo como certificado D, se ha firmado con las dos claves privadas raíz restantes correspondientes a los certificados B y C (mostradas, respectivamente como Firma 1 930 y Firma 2 931).

Puesto que la capacidad de la unidad de gestión de certificados 166 puede ser limitada, en ciertas formas de realización, por lo menos una clave en la unidad de gestión de certificados 166 debería tener un estado “revocado”, de manera que, cuando se reciba un mensaje de certificado nuevo 900, el certificado nuevo 904 se almacene en lugar de una clave previamente revocada. Para garantizar esta propiedad, en algunas de estas formas de realización, el mensaje de certificado nuevo 900 se puede enviar inmediatamente tras un mensaje de revocación o sustitución de certificado.

La Figura 10 muestra un proceso ejemplificativo por el cual puede añadirse un certificado nuevo a un dispositivo electrónico 120 tras la generación de una clave raíz privada nueva 101 por parte de una CA 100.

En la etapa 1010, el supervisor 160 puede recibir un mensaje de certificado nuevo 900 (Figura 9). Este mensaje se puede enviar directamente al supervisor 160 por la CA 100 o por medio de uno o más servidores intermedios, por ejemplo, el servidor 110, y se puede identificar como mensaje de certificado nuevo 900 mediante el tipo de mensaje 901.

Las etapas 1020 a 1040, cada una de las cuales se describirá de forma más detallada posteriormente, se pueden usar para verificar la autenticidad del mensaje de certificado nuevo 900.

En la etapa 1020, el supervisor 160 puede verificar las firmas digitales recibidas dentro del mensaje de certificado nuevo, por ejemplo, la Firma 1 930 y la Firma 2 931. Esto puede incluir una serie de sub-etapas, incluyendo la verificación de que el mensaje de certificado nuevo 900 incluía el número correcto de firmas (por ejemplo, la totalidad – no solamente un subconjunto – de las claves no revocadas) y de que las claves de firma no fueron revocadas previamente, según se ha descrito, por ejemplo, con respecto a las etapas 320 a 326 mostradas en la Figura 3. Por ejemplo, en la forma de realización mostrada en la Figura 9, el supervisor 160 puede confirmar que (i) el mensaje de certificado nuevo 900 se firmó digitalmente usando claves privadas raíz 102 correspondientes tanto al certificado B como al certificado C, y que (ii) no se firmó usando la clave privada raíz 102 correspondiente al certificado A (que había sido revocado previamente, tal como se muestra en el campo 142).

En la etapa 1030, el supervisor 160 puede verificar que el certificado digital recién recibido 904 no se ha almacenado previamente en la unidad de gestión de certificados 166.

En la etapa 1040, el supervisor 160 puede confirmar que se puede añadir un certificado nuevo a la unidad de gestión de certificados 166. Por ejemplo, en ciertas formas de realización, la unidad de gestión de certificados 166 puede confirmar que tiene por lo menos un certificado “revocado” que se puede sustituir por otro nuevo.

Si falla cualquiera de las verificaciones llevadas a cabo en cualquiera de las etapas 1020 a 1040, el supervisor 160 no puede realizar ninguna actualización adicional aunque, en algunas formas de realización, puede intentar, en la etapa 1060, notificar (de forma directa o indirecta por medio de uno o más servidores adicionales) una infracción de política a la CA 100. Una notificación de este tipo puede incluir, por ejemplo, el mensaje de certificado nuevo 900 y cualquier otra información adecuada, tal como el motivo específico por el que falló el método. En caso contrario, si todas las verificaciones llevadas a cabo en las etapas 1020 a 1040 se superan con éxito, en la etapa 1050, el supervisor 160 puede añadir el certificado nuevo a la unidad de gestión de certificados 166 con un estado de “latente”.

De tanto en tanto, puede darse el caso de que se destruya accidentalmente (o de otra manera) una clave privada raíz 102. Si la clave destruida es una clave latente, la CA 100 simplemente nunca podrá hacer que esa clave sea activa. No obstante, si es una clave activa la que se ha destruido (o robado), el dispositivo 120 todavía puede restaurarse a un estado gestionable ya que los métodos descritos en la presente no requieren el uso de la clave activa para su revocación. Por ejemplo, usando el método descrito con respecto a las Figuras 3A a 3C, la CA 100 puede seleccionar una clave raíz privada nueva 102 para la activación, y puede enviar un mensaje a todos los

dispositivos electrónicos 120 para revocar y sustituir el certificado activo, en el que el mensaje ha sido firmado digitalmente, por ejemplo, con la clave nueva y una o más claves latentes. En otras palabras, la clave activa que se pierde y que se está sustituyendo no es necesaria para revocar el certificado correspondiente.

Debe entenderse que, aunque la descripción anterior consideraba una única clave activa, la presente exposición contempla también el uso de múltiples claves activas. En estas formas de realización, puede que sean necesarias varias firmas para conseguir que un certificado emitido con claves raíz sea válido. Las claves activas en estas formas de realización se pueden gestionar según se ha descrito anteriormente.

Aunque se han ilustrado y descrito formas de realización y aplicaciones específicas de la presente invención, debe entenderse que la invención no se limita a la configuración y componentes precisos que se han dado a conocer en la presente. Los términos, descripciones y figuras usados en este documento se exponen únicamente a título ilustrativo y no pretenden constituirse como limitaciones. En la disposición, el funcionamiento y los detalles de los aparatos, métodos y sistemas de la presente invención que se dan a conocer en este documento, pueden realizarse diversas modificaciones, cambios y variaciones, los cuales resultarán evidentes para aquellos versados en la materia, sin desviarse con respecto al espíritu y el alcance de la invención. A título de ejemplo no limitativo, se entenderá que los diagramas de bloques incluidos en la presente están destinados a mostrar un subconjunto seleccionado de los componentes de cada aparato y sistema, y cada aparato y sistema representados pueden incluir otros componentes que no se muestran en los dibujos. Adicionalmente, aquellos con conocimientos habituales en la materia reconocerán que ciertas etapas y funcionalidades descritas en la presente se pueden emitir o reordenar sin menoscabar el alcance o rendimiento de las formas de realización descritas en este documento.

Los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo, ilustrativos, que se han descrito en relación con las formas de realización dadas a conocer en la presente, se pueden implementar como hardware electrónico, software de ordenador o combinaciones de ambos. Para ilustrar esta intercambiabilidad de hardware y software, varios componentes, bloques, módulos, circuitos, y etapas ilustrativos se han descrito anteriormente de manera general en términos de su funcionalidad. El hecho de que dicha funcionalidad se implemente como hardware o software depende de las restricciones particulares de aplicación y diseño impuestas en el sistema total. La funcionalidad descrita se puede implementar de varias maneras para cada aplicación particular – por ejemplo usando cualquier combinación de microprocesadores, microcontroladores, matrices de puertas programables in situ (FPGAs), circuitos integrados de aplicación específica (ASIC), y/o Sistema en un Chip (SoC) – aunque tales decisiones sobre la implementación no deben interpretarse de manera que provoquen una desviación con respecto al alcance de la presente invención.

Las etapas de un método o algoritmo descrito en relación con las formas de realización dadas a conocer en la presente, se pueden materializar directamente en hardware, en un módulo de software ejecutado por un procesador, o en una combinación de los dos. Un módulo de software puede residir en memoria RAM, en memoria *flash*, en memoria ROM, en memoria EPROM, en memoria EEPROM, en registros, en un disco duro, en un disco extraíble, en un CD-ROM, o en cualquier otra forma de soporte de almacenamiento conocida en la técnica.

Los métodos dados a conocer en la presente comprenden una o más etapas o acciones para lograr el método descrito. Las etapas y/o acciones de los métodos se pueden intercambiar entre sí sin desviarse con respecto al alcance la presente invención. En otras palabras, a no ser que se requiera un orden específico de etapas o acciones para un funcionamiento correcto de la forma de realización, el orden de etapas y/o acciones específicas se puede modificar sin desviarse con respecto al alcance de la presente invención, dentro del alcance de protección conferido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Aparato, que comprende:

- un almacenamiento no volátil que almacena una pluralidad de certificados raíz, presentando por lo menos un certificado raíz de la pluralidad de certificados raíz un atributo de estar activo y presentando por lo menos otro certificado raíz de la pluralidad de certificados raíz un atributo de estar latente;

- un supervisor configurado para:

  - recibir un mensaje que identifica uno de entre la pluralidad de certificados raíz almacenados en el almacenamiento no volátil, que se deben revocar;

  - verificar el mensaje que es firmado por al menos dos claves privadas correspondientes a dos certificados raíz almacenados en el almacenamiento no volátil y que por lo menos una de entre dichas por lo menos dos claves privadas usadas para firmar el mensaje se corresponde con unos certificados raíz almacenados en el almacenamiento no volátil que presenta un atributo de estar latente; y

  - revocar el certificado raíz identificado en el mensaje.

2. Aparato según la reivindicación 1, en el que el mensaje es un mensaje de sustitución que identifica un primer certificado raíz que se debe revocar y un segundo certificado raíz que se debe activar.

3. Aparato según la reivindicación 2, en el que los dos certificados raíz usados para verificar las dos firmas de claves privadas son el segundo certificado raíz y un tercer certificado raíz que no ha sido revocado, o

en el que los dos certificados raíz usados para verificar las dos firmas de claves privadas son el primer y segundo certificados raíz, o

en el que por lo menos un certificado raíz de la pluralidad de certificados raíz presenta un atributo de estar activo y otro certificado raíz de la pluralidad de certificados raíz presenta un atributo de estar latente.

4. Aparato según la reivindicación 2, en el que el mensaje de sustitución es un mensaje de sustitución en una cadena de mensajes de sustitución que identifica, cada uno de ellos, un certificado raíz que se debe revocar y otro certificado raíz que se debe activar, y cada mensaje de sustitución de la cadena incluye un primer campo que identifica si se requiere un mensaje previo, y un segundo campo que identifica si se requiere un mensaje sucesivo.

5. Aparato según la reivindicación 1, en el que el mensaje es un mensaje de revocación de certificado latente que incluye una nota de autorrevocación, la nota de autorrevocación contiene un identificador de un certificado raíz que se debe revocar y una firma firmada por una clave privada correspondiente al certificado raíz identificado que se debe revocar.

6. Aparato según la reivindicación 1, en el que el almacenamiento no volátil tiene un espacio de solo lectura para almacenar la pluralidad de certificados raíz y un espacio escribible para almacenar atributos asociados, o

en el que el almacenamiento no volátil tiene un espacio escribible para almacenar la pluralidad de certificados raíz.

7. Método implementado por ordenador, que comprende las etapas siguientes:

- almacenar, en un almacenamiento no volátil de un aparato, una pluralidad de certificados raíz, presentando por lo menos un certificado raíz de entre la pluralidad de certificados raíz un atributo de estar activo y por lo menos otro certificado raíz de la pluralidad de certificados raíz un atributo de estar latente;

- recibir un mensaje que identifica uno de entre la pluralidad de certificados raíz almacenados en el almacenamiento no volátil, que se deben revocar;

- verificar el mensaje que es firmado por al menos dos claves privadas correspondientes a dos certificados raíz almacenados en el almacenamiento no volátil y que por lo menos una de entre dichas por lo menos dos claves privadas usadas para firmar el mensaje se corresponde con certificados raíz almacenados en el almacenamiento no volátil que presenta un atributo de estar latente; y

- revocar el certificado raíz identificado en el mensaje.

8. Método implementado por ordenador según la reivindicación 7, en el que el mensaje es un mensaje de sustitución que identifica un primer certificado raíz que se debe revocar y un segundo certificado raíz que se debe activar.

9. Método implementado por ordenador según la reivindicación 8, en el que los dos certificados raíz usados para verificar las dos firmas de claves privadas son el segundo certificado raíz y un tercer certificado raíz que no ha sido revocado, o en el que los dos certificados raíz usados para verificar las dos firmas de claves privadas son el primer y segundo certificados raíz, o

en el que por lo menos un certificado raíz de la pluralidad de certificados raíz presenta un atributo de estar activo y otro certificado raíz de la pluralidad de certificados raíz presenta un atributo de estar latente.

10. Método implementado por ordenador según la reivindicación 8, en el que el mensaje de sustitución es un mensaje de sustitución en una cadena de mensajes de sustitución que identifica, cada uno de ellos, un certificado raíz que se debe revocar y otro certificado raíz que se debe activar, y cada mensaje de sustitución en la cadena incluye un primer campo que identifica si se requiere un mensaje previo, y un segundo campo que identifica si se requiere un mensaje sucesivo.

11. Método implementado por ordenador según la reivindicación 7, en el que el mensaje es un mensaje de revocación de certificado latente que incluye una nota de autorrevocación, la nota de autorrevocación contiene un identificador de un certificado raíz que se debe revocar y una firma firmada con una clave privada correspondiente al certificado raíz identificado que se debe revocar.

12. Método implementado por ordenador según la reivindicación 7, que además comprende las etapas siguientes:

- recibir un mensaje de certificado nuevo que incluye un identificador de certificado nuevo, un certificado nuevo y una o más firmas digitales;
- verificar que una o más firmas digitales que firman el mensaje de certificado nuevo son generadas con claves privadas correspondientes a los certificados raíz almacenados en el almacenamiento no volátil; y
- añadir el certificado nuevo al almacenamiento no volátil.

13. Método implementado por ordenador, que comprende las etapas siguientes:

- determinar, en una autoridad de certificación, que es necesario revocar una primera clave privada;
- generar un mensaje que identifica un primer certificado raíz que se debe revocar en un dispositivo de cliente, correspondiente al primer certificado raíz a la primera clave privada;
- firmar el mensaje mediante por lo menos dos claves privadas correspondientes a dos certificados raíz almacenados en el dispositivo de cliente y que por lo menos una de entre dichas por lo menos dos claves privadas usadas para firmar el mensaje se corresponde con los certificados raíz almacenados en el almacenamiento no volátil que presenta un atributo de estar latente; y
- enviar el mensaje firmado al dispositivo de cliente.

14. Método implementado por ordenador según la reivindicación 13, en el que el mensaje es un mensaje de sustitución que identifica un segundo certificado raíz que se debe activar, correspondiéndose el segundo certificado raíz con una segunda clave privada en la autoridad de certificación.

15. Método implementado por ordenador según la reivindicación 14, en el que el mensaje de sustitución es un mensaje de sustitución en una cadena de mensajes de sustitución que identifica, cada uno de ellos, un certificado raíz que se debe revocar y otro certificado raíz que se debe activar, y cada mensaje de sustitución de la cadena incluye un primer campo que identifica si se requiere un mensaje previo, y un segundo campo que identifica si se requiere un mensaje sucesivo.

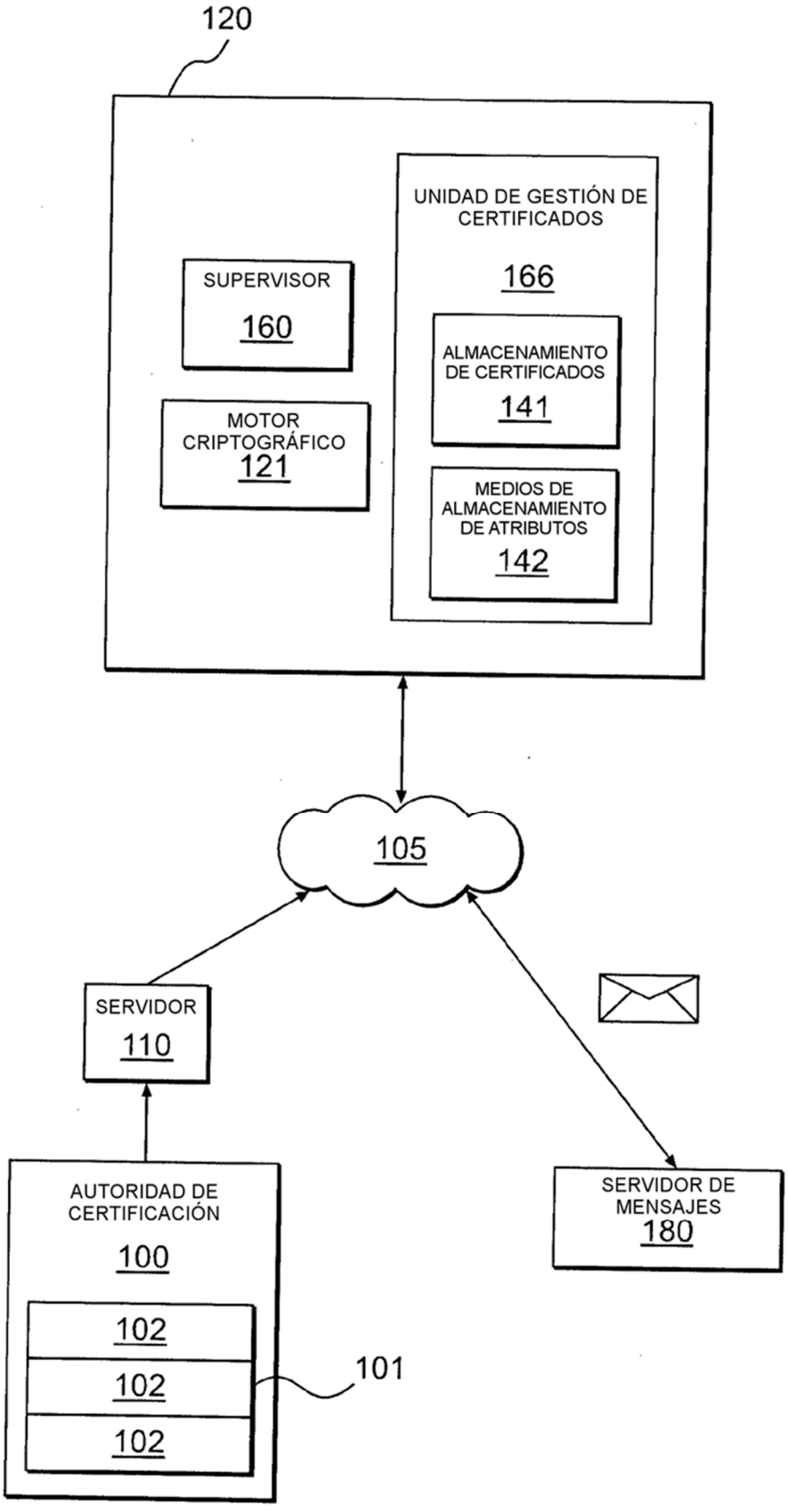
120
UNIDAD DE GESTIÓN DE CERTIFICADOS
166
SUPERVISOR
160
ALMACENAMIENTO DE CERTIFICADOS
141
MOTOR CRIPTOGRÁFICO
121
MEDIOS DE ALMACENAMIENTO DE ATRIBUTOS
142
105
SERVIDOR
110
AUTORIDAD DE CERTIFICACIÓN
100
102
102
102
101
SERVIDOR DE MENSAJES
180

FIG. 1

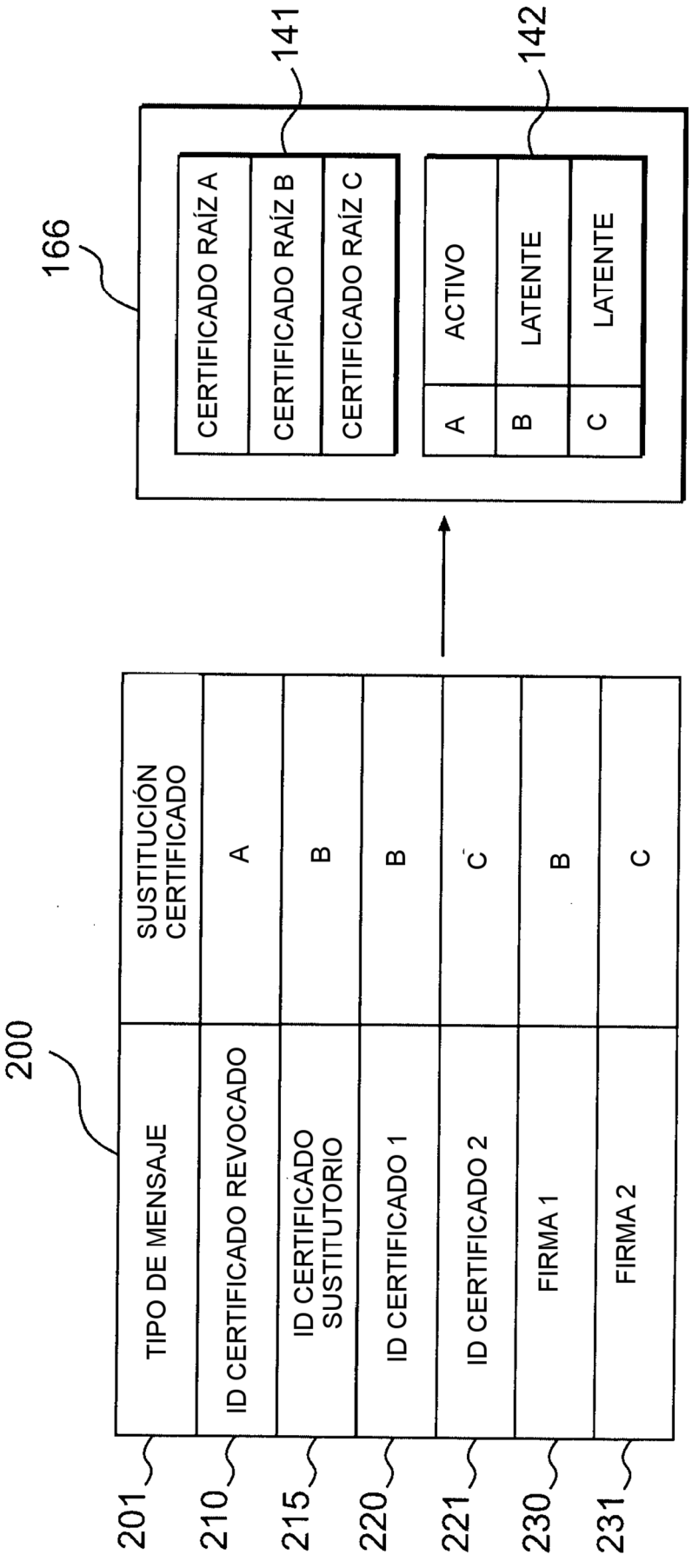
200
TIPO DE MENSAJE
ID CERTIFICADO REVOCADO
ID CERTIFICADO SUSTITUTORIO
ID CERTIFICADO 1
ID CERTIFICADO 2
FIRMA 1
FIRMA 2
SUSTITUCIÓN CERTIFICADO
A
B
B
C
B
C
201
210
215
220
221
230
231
166
141
142
CERTIFICADO RAÍZ A
CERTIFICADO RAÍZ B
CERTIFICADO RAÍZ C
A
ACTIVO
B
LATENTE
C
LATENTE

FIG. 2

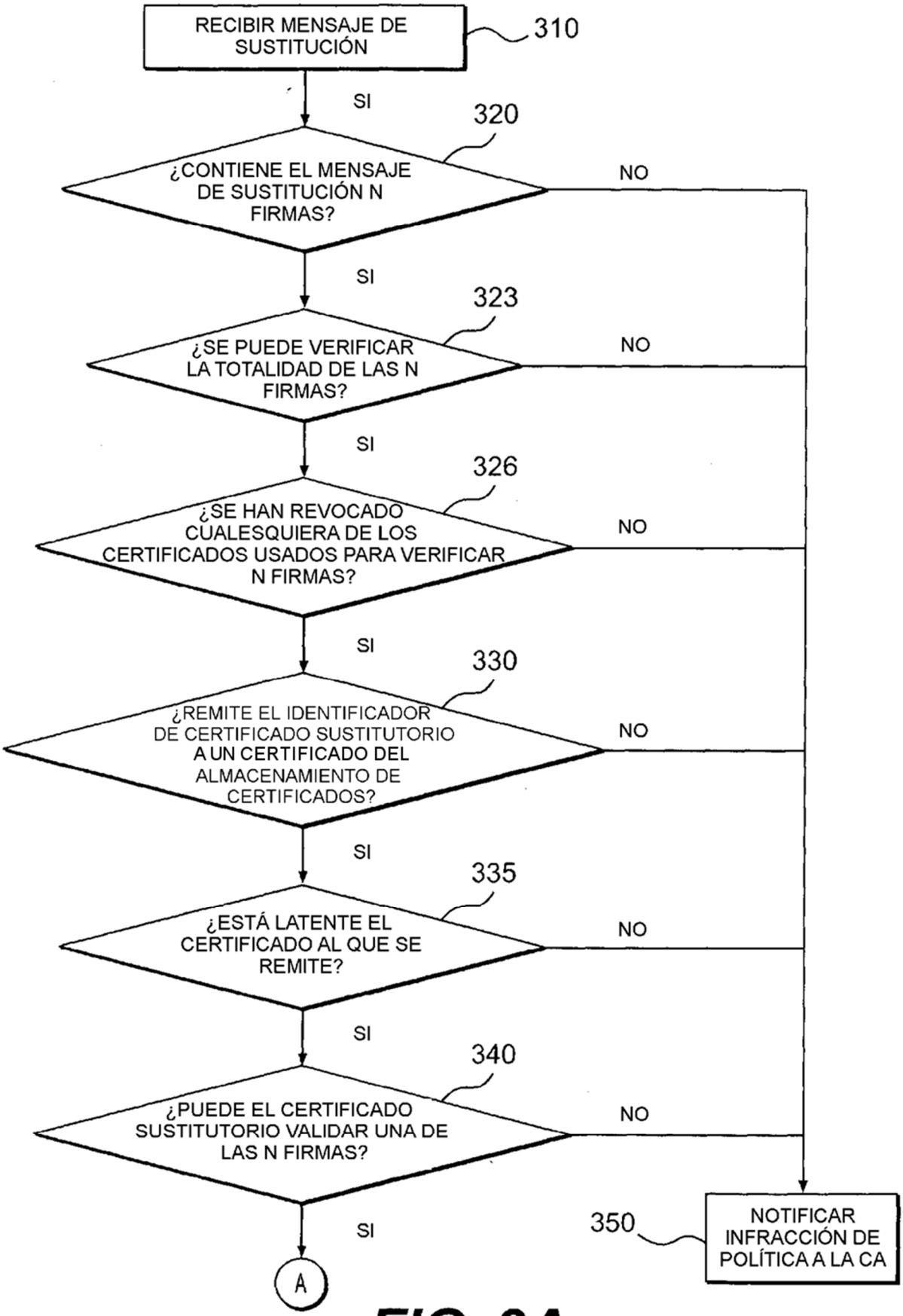
RECIBIR MENSAJE DE SUSTITUCIÓN
310
SI
320
¿CONTIENE EL MENSAJE DE SUSTITUCIÓN N FIRMAS?
NO
SI
323
¿SE PUEDE VERIFICAR LA TOTALIDAD DE LAS N FIRMAS?
NO
SI
326
¿SE HAN REVOCADO CUALESQUIERA DE LOS CERTIFICADOS USADOS PARA VERIFICAR N FIRMAS?
NO
SI
330
¿REMITE EL IDENTIFICADOR DE CERTIFICADO SUSTITUTORIO A UN CERTIFICADO DEL ALMACENAMIENTO DE CERTIFICADOS?
NO
SI
335
¿ESTÁ LATENTE EL CERTIFICADO AL QUE SE REMITE?
NO
SI
340
¿PUEDE EL CERTIFICADO SUSTITUTORIO VALIDAR UNA DE LAS N FIRMAS?
NO
SI
A
350
NOTIFICAR INFRACCIÓN DE POLÍTICA A LA CA

FIG. 3A

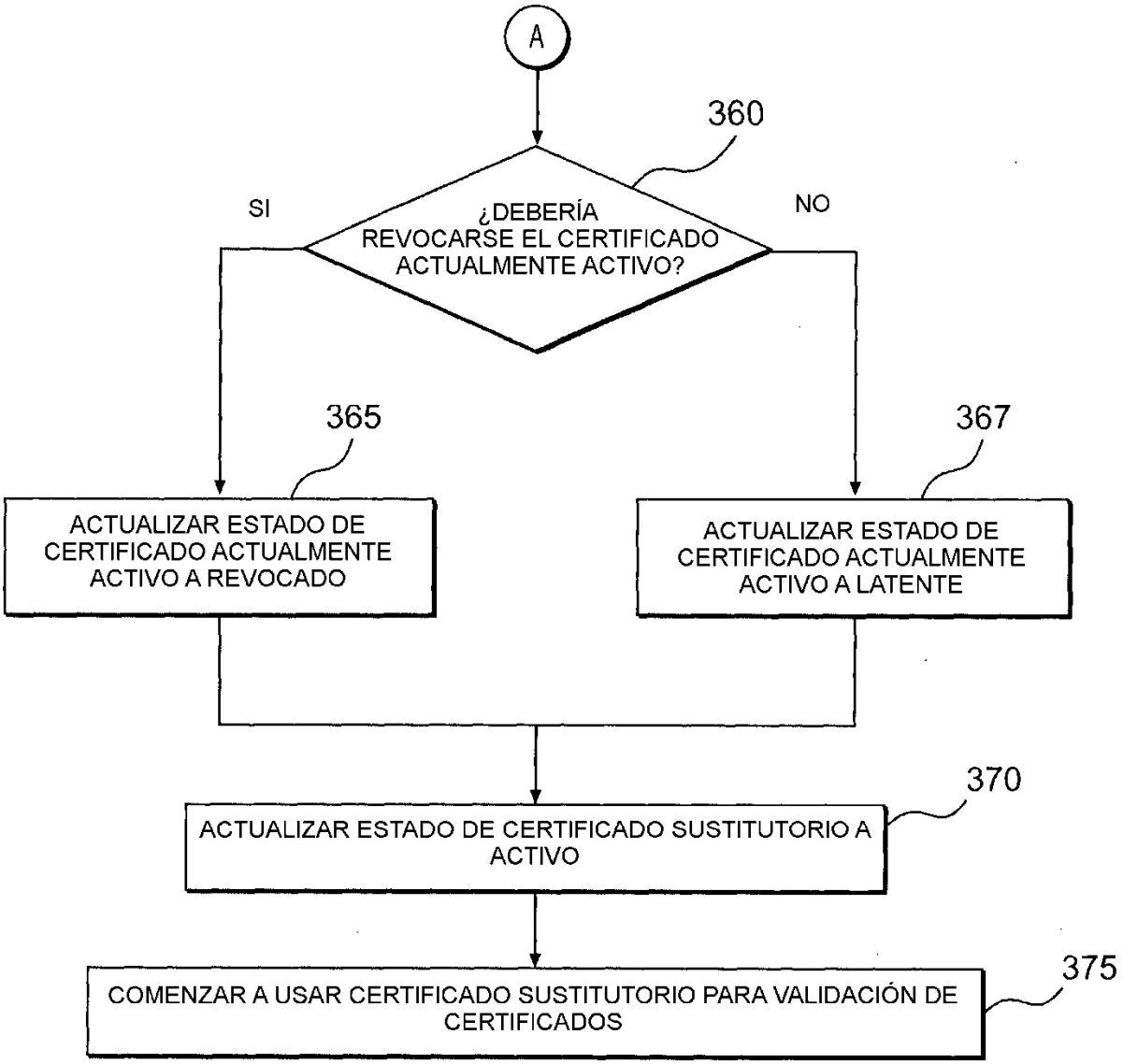
A
360
SI
¿DEBERÍA REVOCARSE EL CERTIFICADO ACTUALMENTE ACTIVO?
NO
365
367
ACTUALIZAR ESTADO DE CERTIFICADO ACTUALMENTE ACTIVO A REVOCADO
ACTUALIZAR ESTADO DE CERTIFICADO ACTUALMENTE ACTIVO A LATENTE
370
ACTUALIZAR ESTADO DE CERTIFICADO SUSTITUTORIO A ACTIVO
375
COMENZAR A USAR CERTIFICADO SUSTITUTORIO PARA VALIDACIÓN DE CERTIFICADOS

FIG. 3B

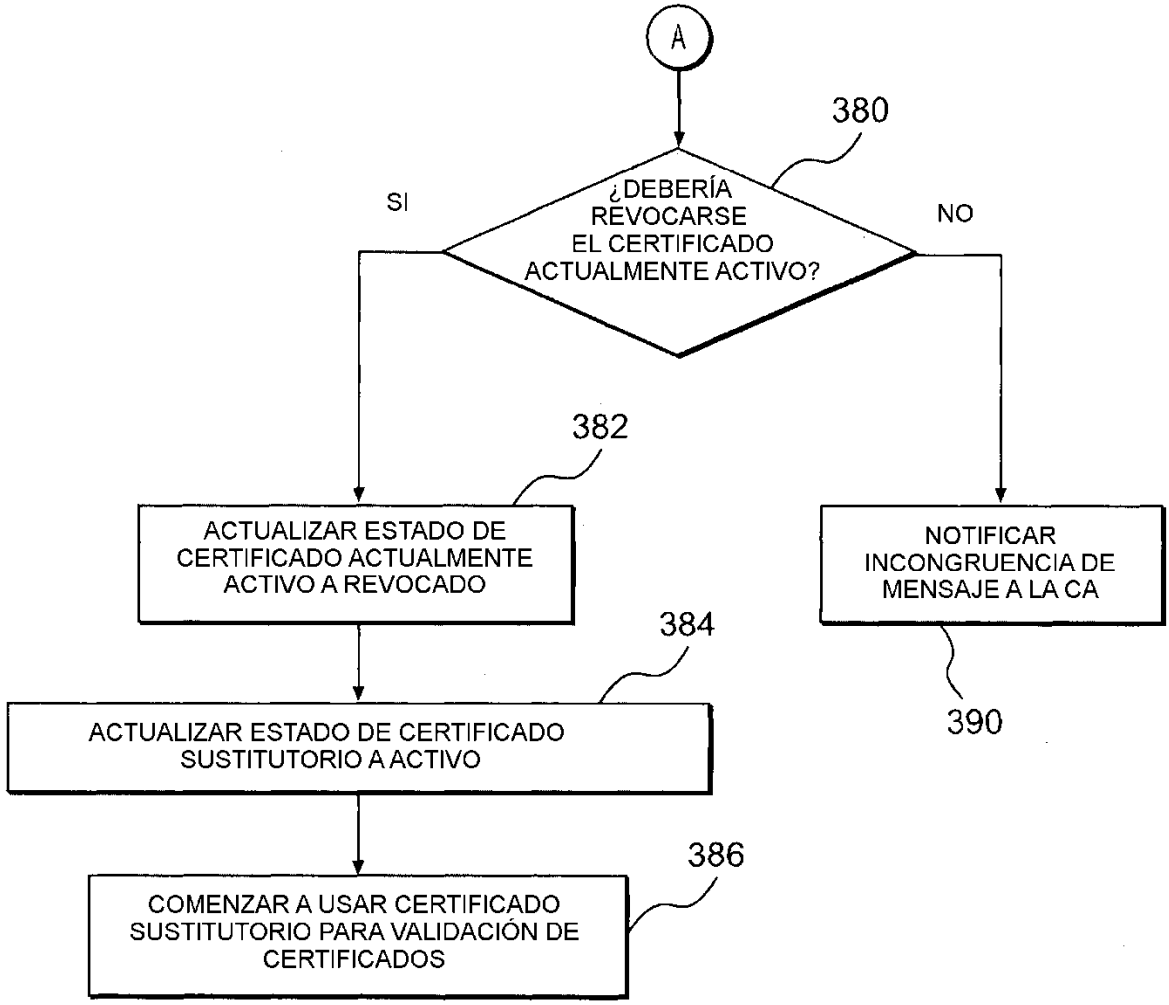
A
380
¿DEBERÍA REVOCARSE EL CERTIFICADO ACTUALMENTE ACTIVO?
SI
NO
382
ACTUALIZAR ESTADO DE CERTIFICADO ACTUALMENTE ACTIVO A REVOCADO
NOTIFICAR INCONGRUENCIA DE MENSAJE A LA CA
390
384
ACTUALIZAR ESTADO DE CERTIFICADO SUSTITUTORIO A ACTIVO
386
COMENZAR A USAR CERTIFICADO SUSTITUTORIO PARA VALIDACIÓN DE CERTIFICADOS

FIG. 3C

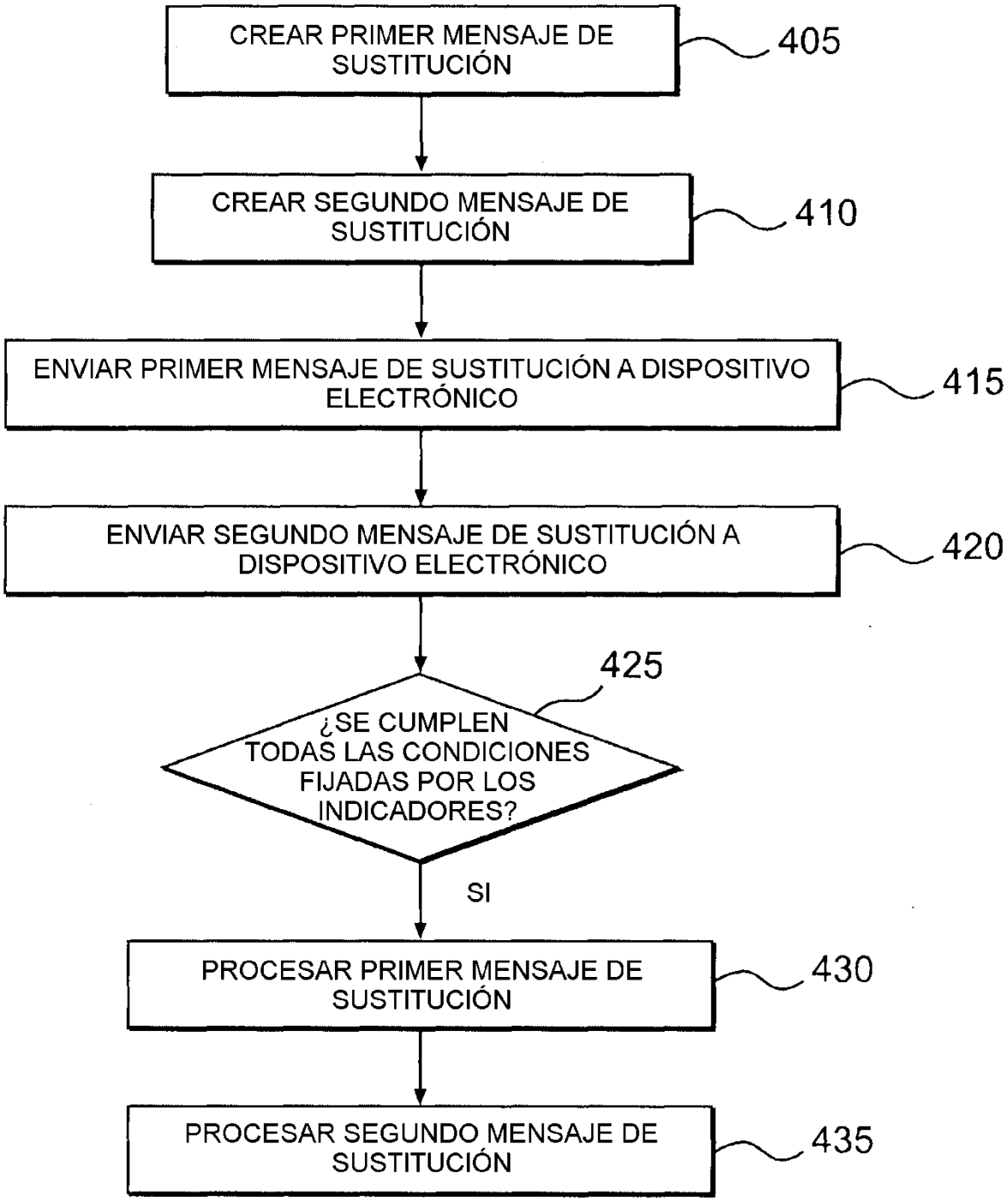
CREAR PRIMER MENSAJE DE SUSTITUCIÓN
405
CREAR SEGUNDO MENSAJE DE SUSTITUCIÓN
410
ENVIAR PRIMER MENSAJE DE SUSTITUCIÓN A DISPOSITIVO ELECTRÓNICO
415
ENVIAR SEGUNDO MENSAJE DE SUSTITUCIÓN A DISPOSITIVO ELECTRÓNICO
420
425
¿SE CUMPLEN TODAS LAS CONDICIONES FIJADAS POR LOS INDICADORES?
SI
PROCESAR PRIMER MENSAJE DE SUSTITUCIÓN
430
PROCESAR SEGUNDO MENSAJE DE SUSTITUCIÓN
435

FIG. 4

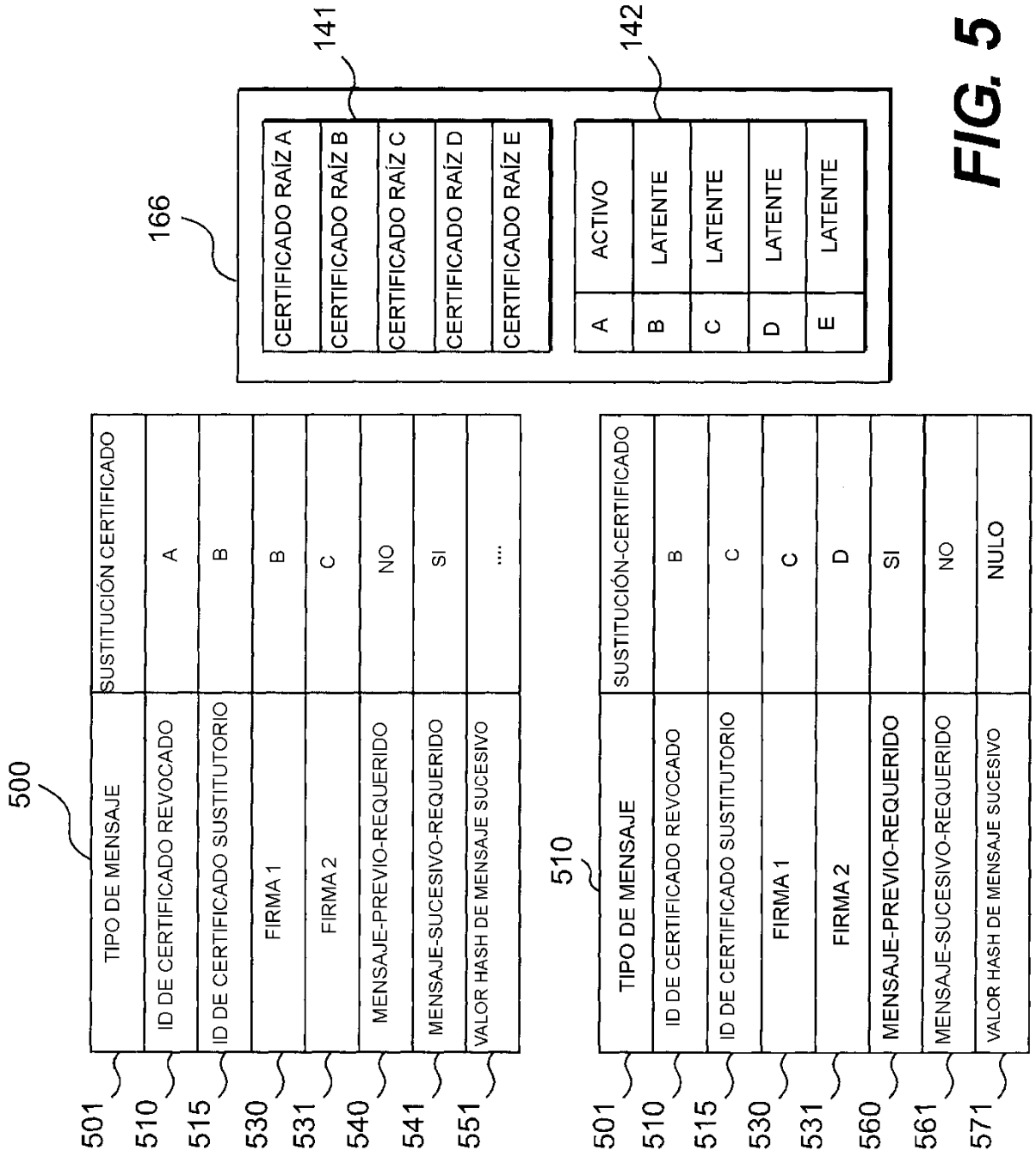
500
TIPO DE MENSAJE
SUSTITUCIÓN CERTIFICADO
ID DE CERTIFICADO REVOCADO
A
ID DE CERTIFICADO SUSTITUTORIO
B
FIRMA 1
B
FIRMA 2
C
MENSAJE-PREVIO-REQUERIDO
NO
MENSAJE-SUCESIVO-REQUERIDO
SI
VALOR HASH DE MENSAJE SUCESIVO
....
501
510
515
530
531
540
541
551
166
141
142
CERTIFICADO RAÍZ A
CERTIFICADO RAÍZ B
CERTIFICADO RAÍZ C
CERTIFICADO RAÍZ D
CERTIFICADO RAÍZ E
A
ACTIVO
B
LATENTE
C
LATENTE
D
LATENTE
E
LATENTE
510
TIPO DE MENSAJE
SUSTITUCIÓN-CERTIFICADO
ID DE CERTIFICADO REVOCADO
B
ID DE CERTIFICADO SUSTITUTORIO
C
FIRMA 1
C
FIRMA 2
D
MENSAJE-PREVIO-REQUERIDO
SI
MENSAJE-SUCESIVO-REQUERIDO
NO
VALOR HASH DE MENSAJE SUCESIVO
NULO
501
510
515
530
531
560
561
571

FIG. 5

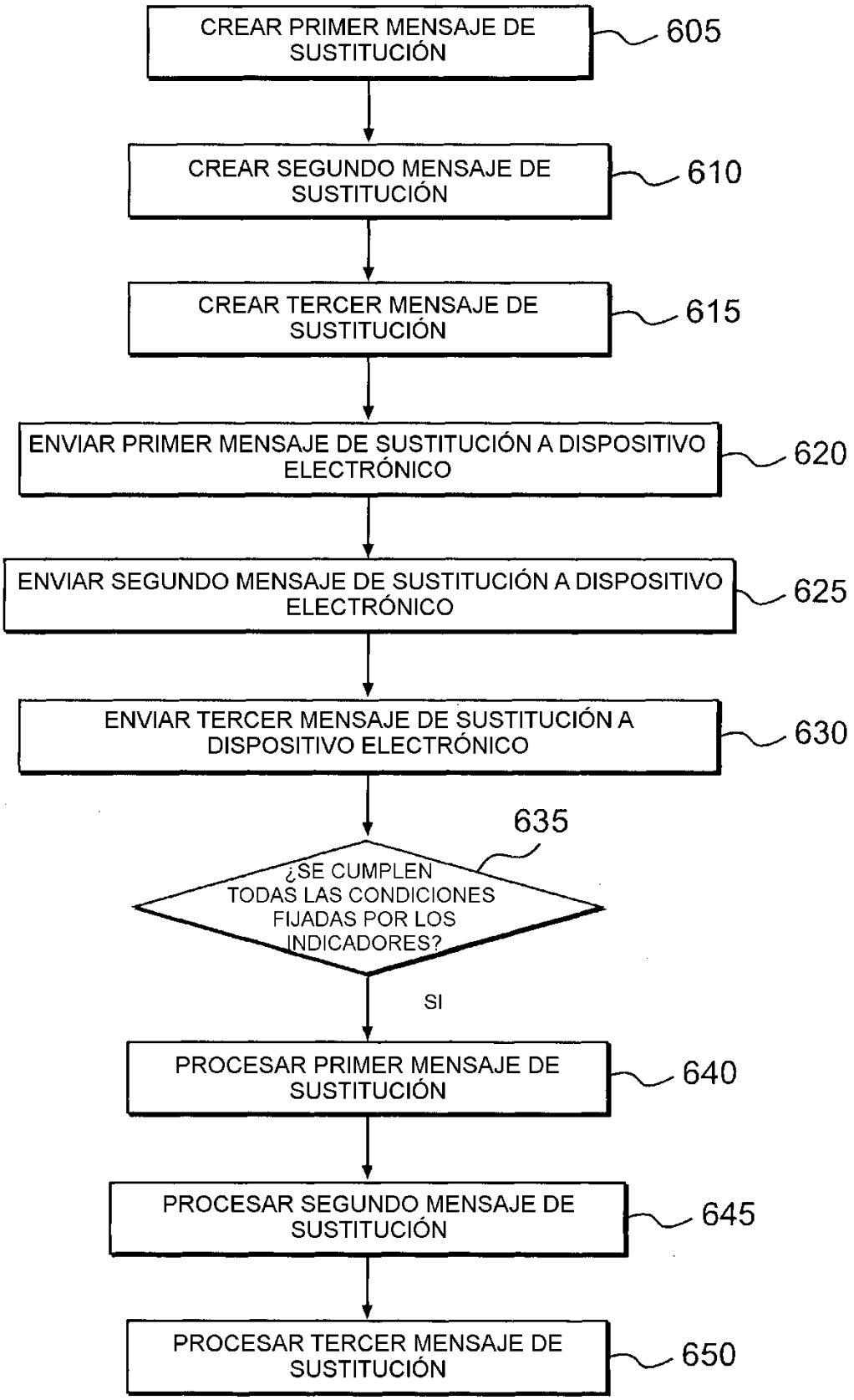
CREAR PRIMER MENSAJE DE SUSTITUCIÓN
605
CREAR SEGUNDO MENSAJE DE SUSTITUCIÓN
610
CREAR TERCER MENSAJE DE SUSTITUCIÓN
615
ENVIAR PRIMER MENSAJE DE SUSTITUCIÓN A DISPOSITIVO ELECTRÓNICO
620
ENVIAR SEGUNDO MENSAJE DE SUSTITUCIÓN A DISPOSITIVO ELECTRÓNICO
625
ENVIAR TERCER MENSAJE DE SUSTITUCIÓN A DISPOSITIVO ELECTRÓNICO
630
635
¿SE CUMPLEN TODAS LAS CONDICIONES FIJADAS POR LOS INDICADORES?
SI
PROCESAR PRIMER MENSAJE DE SUSTITUCIÓN
640
PROCESAR SEGUNDO MENSAJE DE SUSTITUCIÓN
645
PROCESAR TERCER MENSAJE DE SUSTITUCIÓN
650

FIG. 6

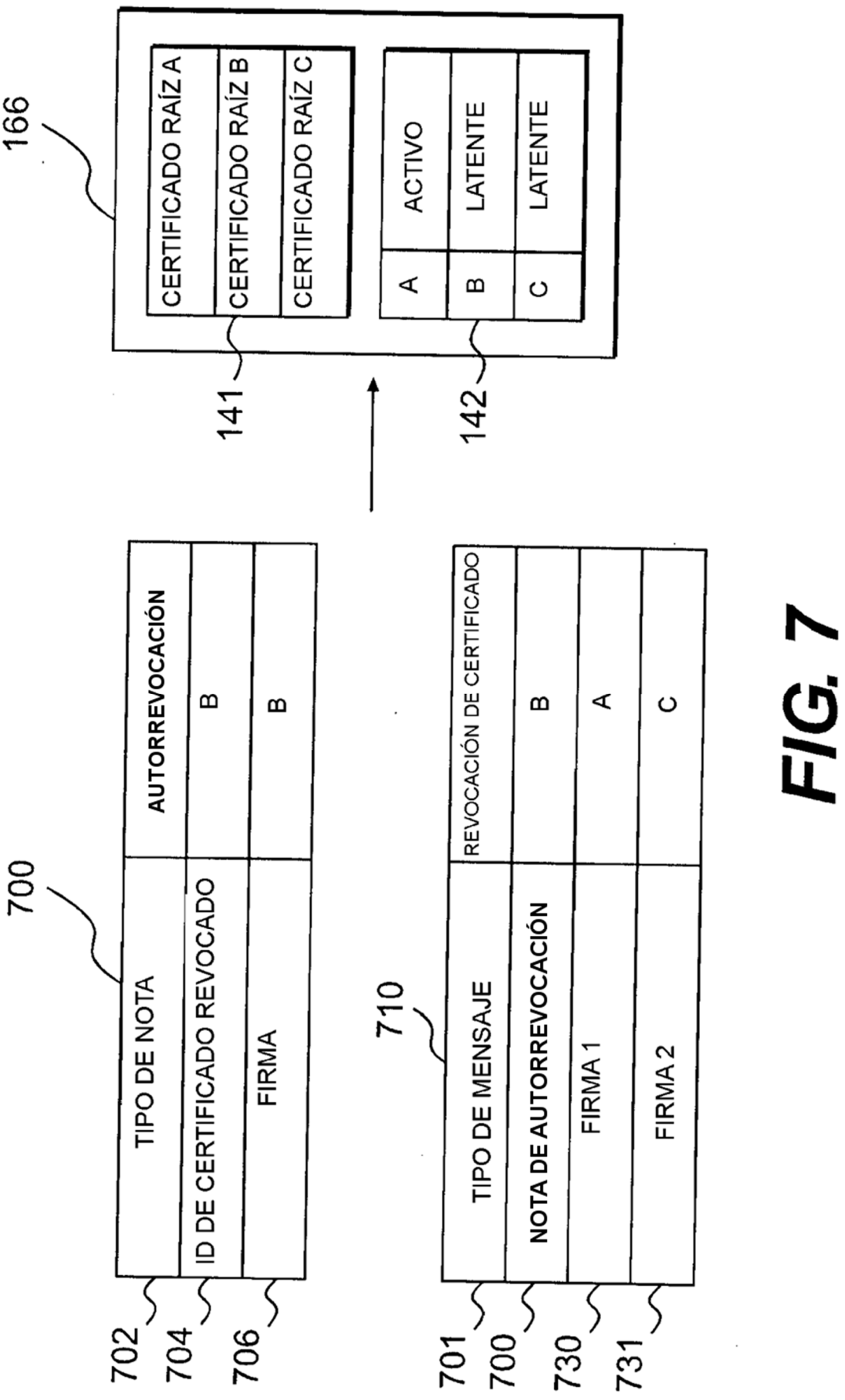
166
CERTIFICADO RAÍZ A
CERTIFICADO RAÍZ B
CERTIFICADO RAÍZ C
141
A
ACTIVO
B
LATENTE
C
LATENTE
142
700
TIPO DE NOTA
ID DE CERTIFICADO REVOCADO
FIRMA
AUTORREVOCACIÓN
B
B
702
704
706
710
TIPO DE MENSAJE
NOTA DE AUTORREVOCACIÓN
FIRMA 1
FIRMA 2
REVOCACIÓN DE CERTIFICADO
B
A
C
701
700
730
731

FIG. 7

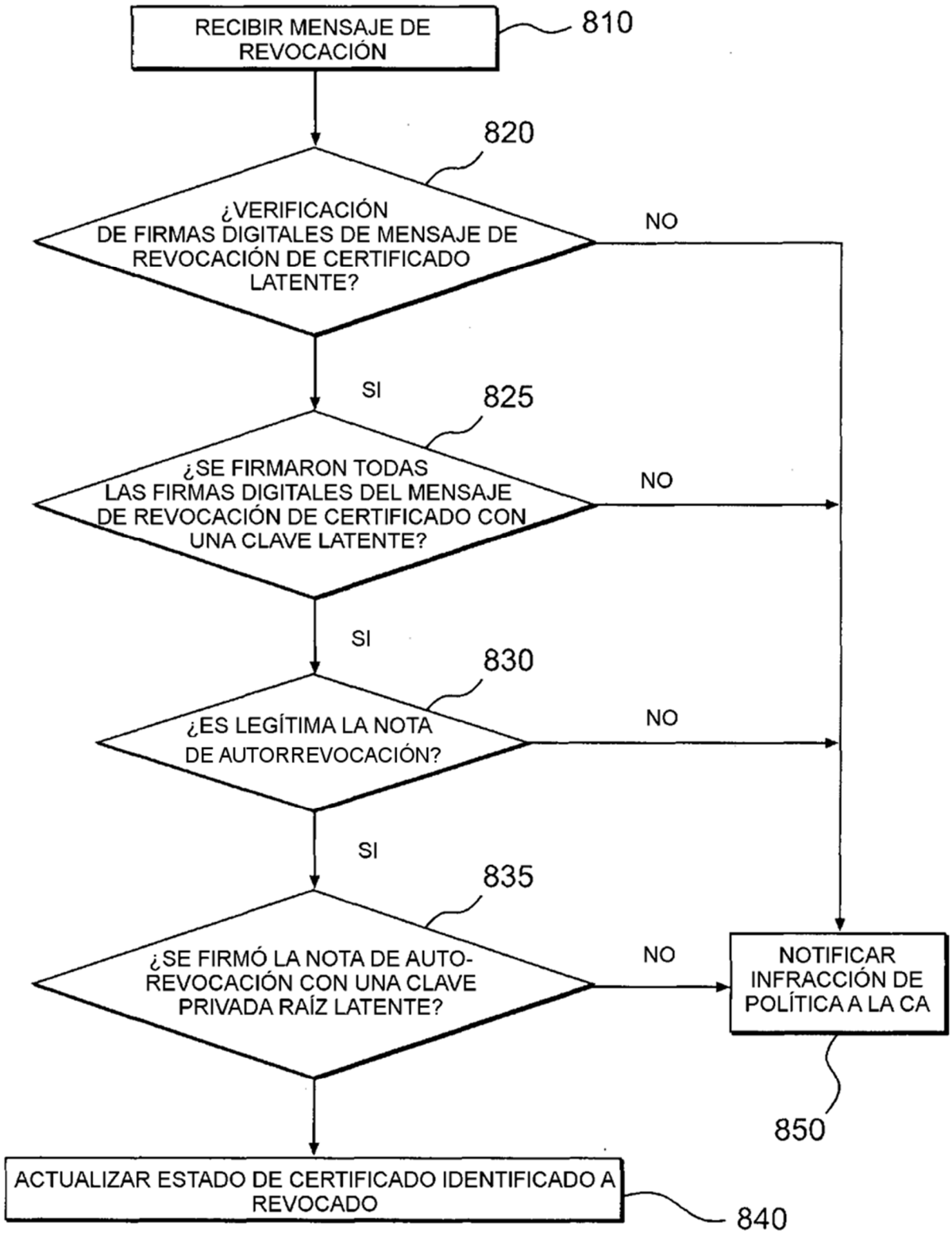
RECIBIR MENSAJE DE REVOCACIÓN
810
820
¿VERIFICACIÓN DE FIRMAS DIGITALES DE MENSAJE DE REVOCACIÓN DE CERTIFICADO LATENTE?
NO
SI
825
¿SE FIRMARON TODAS LAS FIRMAS DIGITALES DEL MENSAJE DE REVOCACIÓN DE CERTIFICADO CON UNA CLAVE LATENTE?
NO
SI
830
¿ES LEGÍTIMA LA NOTA DE AUTORREVOCACIÓN?
NO
SI
835
¿SE FIRMÓ LA NOTA DE AUTO-REVOCACIÓN CON UNA CLAVE PRIVADA RAÍZ LATENTE?
NO
NOTIFICAR INFRACCIÓN DE POLÍTICA A LA CA
850
ACTUALIZAR ESTADO DE CERTIFICADO IDENTIFICADO A REVOCADO
840

FIG. 8

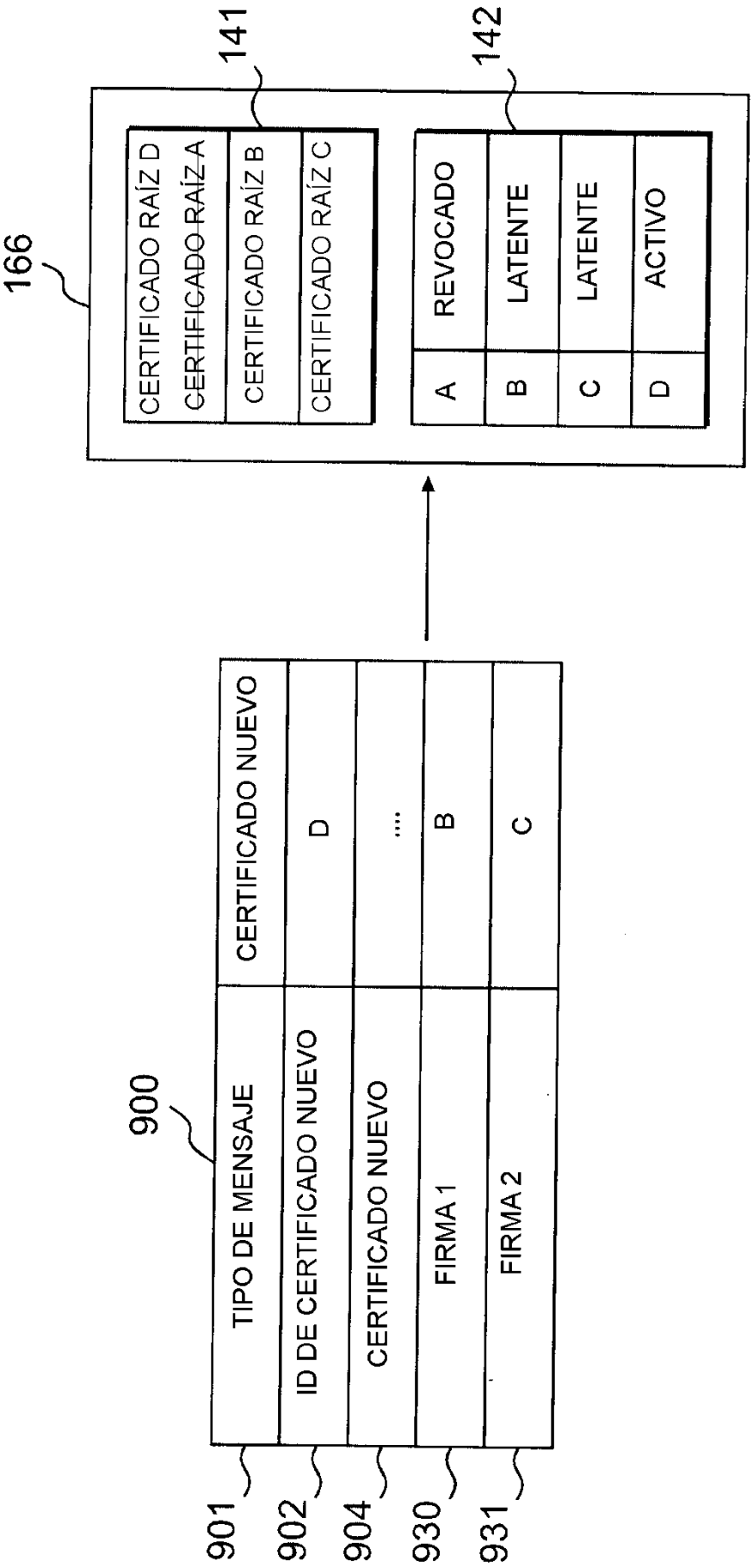
166
141
142
CERTIFICADO RAÍZ D
CERTIFICADO RAÍZ A
CERTIFICADO RAÍZ B
CERTIFICADO RAÍZ C
A
REVOCADO
B
LATENTE
C
LATENTE
D
ACTIVO
900
TIPO DE MENSAJE
CERTIFICADO NUEVO
ID DE CERTIFICADO NUEVO
D
CERTIFICADO NUEVO
....
FIRMA 1
B
FIRMA 2
C
901
902
904
930
931

FIG. 9

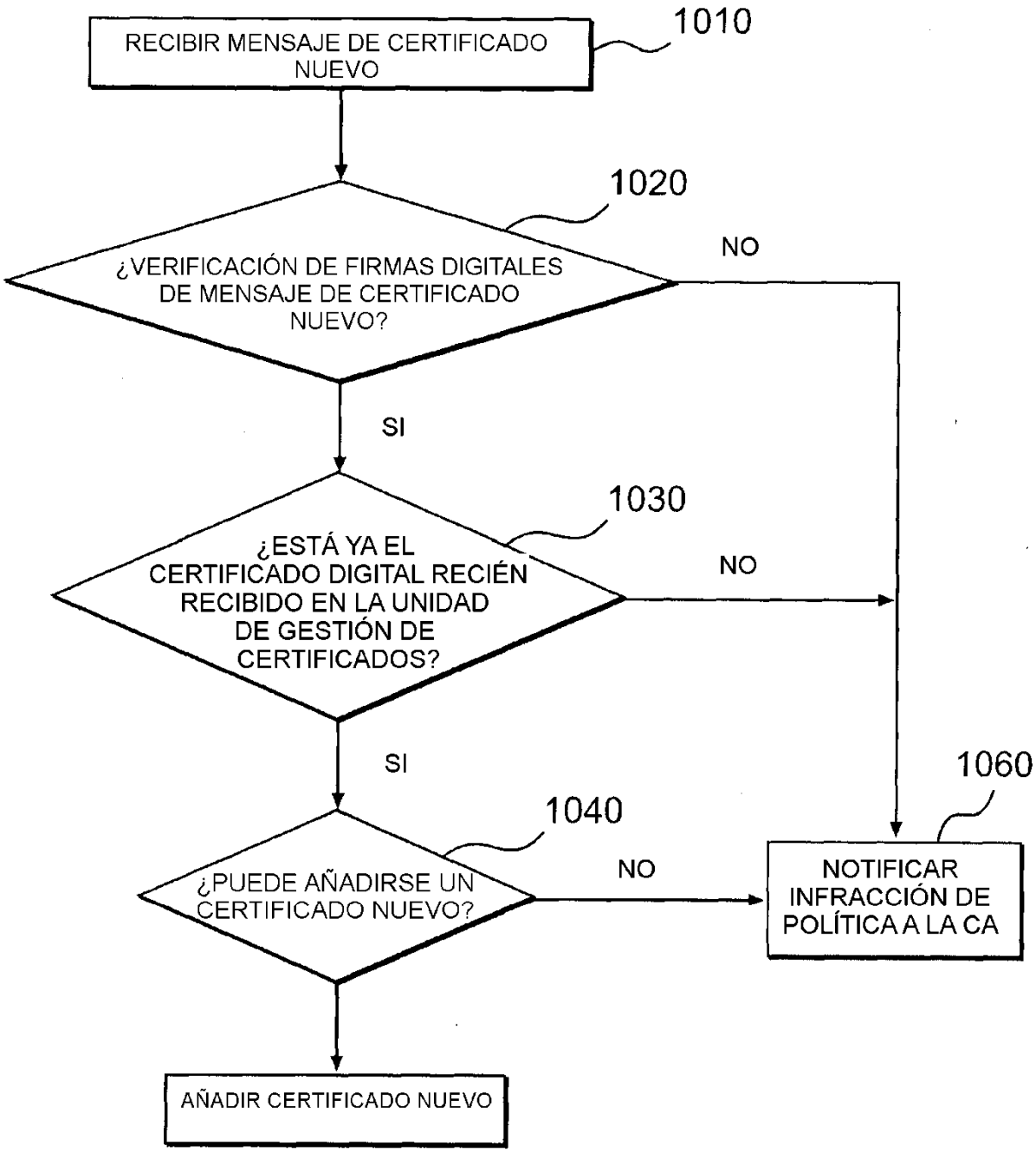
RECIBIR MENSAJE DE CERTIFICADO NUEVO
1010
¿VERIFICACIÓN DE FIRMAS DIGITALES DE MENSAJE DE CERTIFICADO NUEVO?
1020
NO
SI
¿ESTÁ YA EL CERTIFICADO DIGITAL RECIÉN RECIBIDO EN LA UNIDAD DE GESTIÓN DE CERTIFICADOS?
1030
NO
SI
¿PUEDE AÑADIRSE UN CERTIFICADO NUEVO?
1040
NO
NOTIFICAR INFRACCIÓN DE POLÍTICA A LA CA
1060
AÑADIR CERTIFICADO NUEVO

FIG. 10