

DESCRIPCIÓN

Método para monitorizar certificados digitales

Objeto de la invención

5 La presente invención está dirigida a un método implementado por ordenador para monitorizar, registrar y validar certificados digitales en una red privada de ordenadores no conectada a Internet.

Antecedentes de la invención

10 Los certificados digitales son una pieza fundamental en las comunicaciones seguras hoy en día en términos de confidencialidad, autenticación y autorización. Este campo, aunque ha sido muy desarrollado en las últimas décadas, aún tiene una serie de retos importantes a solucionar como son la seguridad frente a robos y falsificaciones, la reducción de costes en la gestión y distribución, la compatibilidad de los protocolos de comunicaciones y la verificación de dichos certificados digitales en escenarios sin conexión a Internet.

15 La solución estándar para gestionar certificados digitales son las *infraestructuras de clave pública (PKI en inglés)*, que cuentan con dos tipos de autoridades diferenciadas, *CA (autoridad de certificación)* y *RA (autoridad de registro)*. La persona o software, es decir un cliente en un sistema cliente-servidor, que tenga que verificar la legitimidad de un certificado digital necesita tener las claves públicas de la CA que creó los certificados para la verificación de parámetros y de la firma digital.

20 Esta configuración de las PKI conlleva un problema de base. Al asumir que las CAs son elementos estáticos, que se crean en un momento dado y que probablemente vaya creciendo poco a poco, cada cambio en la CA o cada creación de una nueva CA requiere modificar los clientes que necesiten realizar una validación (al menos conocer su clave pública). Por lo tanto, cuando se requieren certificados de corta duración o nuevas CAs según la demanda del sistema, este problema conlleva una gestión ineficiente de los certificados y unos costes muy elevados.

25 En lo relativo a la seguridad, PKI presenta un problema adicional porque no puede hacer frente a los nuevos tipos de ataques que han ido apareciendo en la última década. Por ejemplo, PKI no permite posible detectar fácilmente cuando un certificado robado o falsificado está siendo utilizado en algún sistema. La única forma de detectar este tipo de actuaciones cuando el certificado es consultado de forma activa, lo cual permite revocarlo o denunciarlo a la CA. Por lo tanto, esto supone un gran riesgo de seguridad en cualquier red de ordenadores.

Un aspecto negativo adicional de PKI es el despliegue de las infraestructuras. Esta tecnología no puede adaptarse a los diferentes sistemas existentes en una organización que, probablemente, no utilicen los protocolos o estándares actuales. Consecuentemente, son habituales los problemas de conectividad y de aislamiento de sistemas.

30 En lo relativo al problema de gestión de certificados y reducción de costes han surgido nuevas tendencias. Especialmente significativa es la tecnología *Let's Encrypt*, que genera certificados criptográficos de forma gratuita bajo demanda. Sin embargo, esta solución requiere que la red tenga acceso a Internet, lo que imposibilita su uso en redes privadas sin acceso a Internet, como por ejemplo una organización bancaria.

35 Para solventar los problemas de seguridad de PKI, están apareciendo nuevas propuestas como la tecnología *HSTS (HTTP Strict Transport Security)* o *HPKP (HTTP Public Key Pinning)* que, además de PKIs, emplean protocolo SSL. Sin embargo, no son suficientes para solventar los nuevos escenarios de ataques que han aparecido en los últimos años.

40 El documento "Certificate Transparency with Privacy", publicado en nombre de Saba Eskandarian, describe un mecanismo que permite que navegadores web auditen un registro de transparencia de certificados sin violar la privacidad del usuario y que amplíen la transparencia del certificado para soportar subdominios no públicos.

La siguiente invención propone una solución a los anteriores problemas mediante un método seguro, eficiente y flexible para monitorizar, registrar y verificar certificados digitales en redes privadas heterogéneas, particularmente en redes no conectadas a Internet.

Descripción de la invención

45 La presente invención propone una solución a los problemas anteriores mediante un método implementado por ordenador para monitorizar certificados digitales en una red privada de ordenadores no conectada a Internet según la reivindicación 1, un sistema de monitorización, registro y validación de certificados según la reivindicación 13, un programa de ordenador según la reivindicación 14 y un medio legible por ordenador según la reivindicación 15. En las reivindicaciones dependientes se definen realizaciones preferidas de la invención.

50 Un primer aspecto inventivo proporciona un método implementado por ordenador para monitorizar y validar certificados digitales en una red privada de ordenadores no conectada a Internet, en donde la red privada de ordenadores comprende:

- *al menos un servidor de registros configurado para registrar dichos certificados digitales, albergándolos en una primera base de datos basada en un árbol de Merkle, y*
- *al menos un servidor de monitorización configurado para:*

- o *albergar al menos una regla de auditoría,*
- 5 o *aplicar sobre los certificados de la primera base de datos del servidor de registros al menos una regla de auditoría, y*
- o *emitir una alerta si al menos un certificado no cumple dicha al menos una regla de auditoría,*

en donde al menos una regla de auditoría se define por al menos un miembro seleccionado de la red privada de ordenadores, y

10 *en donde el método comprende las siguientes etapas:*

a) *acceder por parte del al menos un servidor de monitorización a la primera base de datos del al menos un servidor de registros,*

b) *aplicar por parte del al menos un servidor de monitorización sobre los certificados digitales de la primera base de datos del al menos un servidor de registros la al menos una regla de auditoría, y*

15 c) *emitir, por parte del al menos un servidor de monitorización, una alerta si al menos un certificado no cumple dicha al menos una regla de auditoría;*

en donde el servidor de registros (2) está configurado además para albergar al menos un requisito de validez (9) que:

- *está relacionado con la información de los certificados digitales contenidos en dicho servidor de registros (2), y*

20 • *está definido por al menos un miembro seleccionado (8) de la red privada de ordenadores (1); y*

en donde el servidor de registros (2) está configurado además para validar (400) certificados digitales particulares bajo solicitud de la red privada de ordenadores (1),

en donde dicho método (100) comprende además las etapas de:

25 i. *recibir (410) por parte del al menos un servidor de registros (2) al menos una solicitud de validación de certificado digital emitida por la red privada de ordenadores (1),*

ii. *consultar (420) por parte del al menos un servidor de registros (2), si el certificado digital bajo solicitud está contenido en su base de datos (4), y*

30 iii. *en caso de que el certificado digital bajo solicitud esté contenido en la base de datos (4), consultar (430) por parte del servidor de registros (2) si se cumple el al menos un requisito de validez (9) albergado en dicho servidor de registros (2), en donde:*

a. *en caso de cumplirse, el certificado digital bajo solicitud se valida (440), o*

b. *en caso de no cumplirse, el certificado digital bajo solicitud no se valida (450),*

iv. *en caso de que el certificado digital bajo solicitud no esté contenido en la base de datos (4), el certificado bajo solicitud no se valida (450); y*

35 *en donde al menos un miembro seleccionado (8) de la red privada de ordenadores (1) está configurado para comunicarse con el al menos un servidor de monitorización (3) y/o con el al menos un servidor de registros (2) mediante una API o mediante una página web de administración (10); y*

en donde el servidor de registros (2) comprende además un módulo adicional (11) configurado para convertir las solicitudes de validación emitidas por parte de la red privada de ordenadores (1) en un formato determinado, preferiblemente API, de manera que estas solicitudes sean entendibles por el servidor de registros (2).

40 *A lo largo de este documento, se entenderá que **red privada de ordenadores** es una intranet situada en cualquier red de área local, LAN en inglés, o una intranet corporativa de una organización, entidad o compañía no conectada a Internet, por ejemplo, la red privada de una organización bancaria sin acceso a Internet por cuestiones de seguridad.*

45 *A lo largo de este documento, se entenderá que **regla de auditoría** es una condición que han de cumplir los certificados digitales para considerarlos válidos o aptos para su uso, por ejemplo, que el tiempo restante hasta su caducidad sea de al menos dos meses o que no tengan un determinado número de serie que ha sido dado de baja.*

A lo largo de este documento, se entenderá como *aplicar una regla de auditoría* al proceso de comprobar que los certificados digitales cumplen dicha regla de auditoría.

A lo largo de este documento, se entenderá como *base de datos* a un repositorio centralizado.

5 A lo largo de este documento, se entenderá como *alerta* a un mensaje de texto en el que se expone qué certificado no cumple una determinada regla de auditoría.

A lo largo de este documento, se entenderá como *miembro seleccionado de la red privada de ordenadores* a un miembro escogido de entre todos los disponibles en la red privada de ordenadores como responsable de definir las reglas de auditoría y almacenarlas en el servidor de monitorización.

10 Ventajosamente, el uso de una base de datos basada en un *árbol de Merkle* permite un registro de certificados digitales *append-only*, es decir, cualquier certificado añadido no puede ser eliminado y es posible detectar quién y en qué momento ha modificado la información contenida en el *árbol de Merkle*. Esto garantiza la auditoría del sistema al poderse trazar las conexiones para identificar usos fraudulentos de certificados digitales.

Una ventaja adicional es el aumento de la seguridad de los certificados digitales registrados. Esto es debido a que el *árbol de Merkle* está construido mediante algoritmos de *hash* criptográfico encadenados.

15 Adicionalmente, la designación de un miembro de la red privada de ordenadores para crear las reglas de auditoría permite ventajosamente que sea imposible que un tercero cree otras reglas, elimine o modifique las existentes sin la autorización correspondiente.

20 A lo largo de este documento, se entenderá como *requisito de validez* a una condición que han de cumplir los certificados digitales para ser considerados válidos o aptos para su uso, por ejemplo, que no estén caducados o que la firma digital del solicitante sea correcta.

Ventajosamente, la designación de un miembro de la red privada para definir los requisitos de validez imposibilita que un tercero intente introducir nuevos requisitos, eliminar o modificar los ya existentes sin la correspondiente autorización.

25 Ventajosamente, para posibilitar la conexión de un miembro a la red privada de ordenadores han de cumplirse dos premisas: que el certificado digital esté contenido en el servidor de registros y que cumpla unos requisitos de validez, lo que aumenta la seguridad del sistema. Adicionalmente, la existencia de requisitos de validez conlleva la ventaja de que miembros con certificados digitales caducados y/o miembros que no hayan empleado correctamente la firma digital no puedan acceder a la red.

30 Ventajosamente, la conexión entre el miembro seleccionado de la red privada de ordenadores y el servidor de monitorización permite la existencia de reglas de auditoría, y la conexión entre el miembro seleccionado de la red privada de ordenadores y el servidor de registros permite la existencia de requisitos de validez, lo que posibilita la detección de certificados digitales caducados, robados, revocados y/o fraudulentos. De forma aún más ventajosa, al existir dos vías diferentes de comunicación se asegura que dicha comunicación pueda establecerse en caso de que una de las vías no esté disponible.

35 A lo largo de este documento, se entenderá como *módulo adicional* a un módulo VA (*autoridad de verificación*) que está configurado para:

- recibir peticiones de un determinado protocolo de validación de certificados digitales, por ejemplo OSCP,
 - comunicar dicha petición al servidor de registros de modo que pueda entender dicha petición, y
 - transformar la respuesta del servidor de registros a ese mismo protocolo para que el solicitante de la red
- 40 privada de ordenadores pueda entender dicha respuesta.

Ventajosamente, la existencia de este módulo permite que la red privada de ordenadores sea heterogénea y, por lo tanto, no es necesario que todos los miembros de la red se comuniquen con el mismo protocolo ya que este módulo actúa como traductor de protocolos de forma que todos los miembros de la red puedan entenderse entre sí.

45 En una realización particular, *la red privada de ordenadores además comprende al menos una autoridad de certificación, seleccionada de la red privada de ordenadores, que está configurada para crear y enviar los certificados digitales al al menos un servidor de registros para ser registrados por dicho al menos un servidor de registros,*

en donde el método además comprende las siguientes etapas:

- i. *crear por la al menos una autoridad de certificación al menos un certificado digital,*
- 50 ii. *asignar por parte del al menos un servidor de registros un identificador a dicho certificado para permitir que*

sea localizable por al menos dicho servidor de registros, y

iii. registrar el al menos un certificado digital creado por dicha al menos una autoridad de certificación en el al menos un servidor de registros, albergándolos en su base de datos.

5 Ventajosamente, la designación de un miembro de la red privada de ordenadores para crear los certificados imposibilita que un tercero intente crear certificados sin la correspondiente autorización, lo que dificulta la creación de certificados fraudulentos. De manera aún más ventajosa, la necesidad de registrar estos certificados en la base de datos basada en un *árbol de Merkle* supone que no se pueda interactuar con certificados digitales que no estén contenidos en dicha base de datos, lo que impide el uso de certificados caducados o revocados aumentando la seguridad del sistema.

10 Adicionalmente, la asignación de un identificador para cada certificado tiene la ventaja de agilizar la búsqueda de dicho certificado en la base de datos.

En una realización particular, la al menos una autoridad de certificación está configurada para crear certificados digitales bajo servicio.

15 Ventajosamente, los certificados pueden ser creados a petición de los diferentes miembros de la red privada de ordenadores de forma temporal o permanente, siempre que se haya comprobado la autenticidad de la autoridad de certificación mediante la identificación de su dirección IP y de sus claves criptográficas.

En una realización particular, al emitir una alerta por parte del al menos un servidor de monitorización, se envía una notificación a un destinatario de la red privada de ordenadores predefinido en dicho servidor de monitorización.

20 A lo largo de este documento, se entenderá como *destinatario de la red privada de ordenadores* a un miembro de la red privada de ordenadores que se ha seleccionado previamente y al que se le ha dado permiso para recibir alertas de forma explícita en el servidor de monitorización.

25 Ventajosamente, la designación de un miembro de la red privada de ordenadores para recibir alertas imposibilita la recepción de dichas alertas por parte de un tercero sin la correspondiente autorización. Esto asegura que sólo un miembro con permisos recibe información de certificados susceptibles de ser considerados como fraudulentos, robados, caducados o de ser revocados, teniendo plena autoridad para decidir cómo gestionar la alerta; por ejemplo, puede ordenar la revocación de un certificado caducado para imposibilitar su uso futuro.

En una realización particular, el al menos un servidor de monitorización además está configurado para registrar tanto el al menos un certificado digital que incumple la regla de auditoría, como la correspondiente alerta emitida en una segunda base de datos basada en un *árbol de Merkle*.

30 Ventajosamente, el registro de certificados que incumplen las reglas de auditoría y de sus correspondientes alertas en un *árbol de Merkle* cumple la propiedad de *append-only*, es decir, se imposibilita que un tercero elimine el registro de un certificado que no cumple las reglas de auditoría. De esta forma, aumenta la seguridad del sistema al cerciorarse de que todos los certificados inválidos están contenidos con total seguridad en dicha base de datos.

35 En una realización particular, el al menos un servidor de monitorización está configurado para comunicarse con el al menos un servidor de registros mediante una API.

A lo largo de este documento, se entenderá como API (*Interfaz de Programación de Aplicaciones*) a un mecanismo para conectar dos softwares entre sí para el intercambio de mensajes o datos en formato estándar.

40 Ventajosamente, la conexión entre ambos servidores permite que el servidor de monitorización consulte la base de datos del servidor de registros para poder aplicar las reglas de auditoría y poder detectar así la presencia de certificados fraudulentos, robados, revocados y/o caducados. Además, el establecimiento de la conexión mediante una API ventajosamente evita la existencia de incompatibilidades en el intercambio de datos e información entre los servidores.

En una realización particular, la al menos una autoridad de certificación está configurada para comunicarse con el al menos un servidor de registros mediante una API o mediante una página web de administración.

45 A lo largo de este documento, se entenderá como *página web de administración* a una página web a la que sólo pueden acceder miembros seleccionados de la red privada de ordenadores para llevar a cabo gestiones relacionadas con los certificados digitales de dicha red privada de ordenadores.

50 Ventajosamente, la comunicación entre la autoridad de certificación y el servidor de registros permite la creación y registro de certificados digitales. De forma aún más ventajosa, al existir dos vías diferentes de comunicación se asegura que dicha comunicación pueda establecerse en caso de que una de las vías no esté disponible.

En una realización particular, la página web de administración está configurada para:

- recibir certificados digitales por parte de la al menos una autoridad de certificación y enviar dichos certificados al al menos un servidor de registros, y/o
 - recibir al menos un requisito de validez definido por al menos un miembro seleccionado de la red privada de ordenadores y enviar dicho requisito de validez al al menos un servidor de registros, y/o
- 5 • recibir al menos una regla de auditoría definida por al menos un miembro seleccionado de la red privada de ordenadores y enviar dicha regla de auditoría al al menos un servidor de monitorización.

Ventajosamente, la existencia de una página web de administración permite que sólo los usuarios autorizados puedan hacer cambios en los servidores a través de ella. De manera aún más ventajosa, la interfaz de la web de administración permite que la autoridad de certificación y/o el o los miembros encargados de definir las reglas de auditoría y/o los requisitos de validez puedan operar de forma rápida, directa y eficaz.

En un segundo aspecto inventivo, la invención proporciona un sistema de monitorización, registro y validación de certificados digitales que comprende medios para llevar a cabo las etapas del método descrito en el primer aspecto inventivo.

En un tercer aspecto inventivo, la invención proporciona un programa de ordenador que comprende instrucciones que, cuando el programa es ejecutado por un ordenador, hacen que el ordenador lleve a cabo las etapas del método descrito en el primer aspecto inventivo.

En un cuarto aspecto inventivo, la invención proporciona un medio legible por ordenador que comprende instrucciones que, cuando son ejecutadas por un ordenador, hacen que el ordenador lleve a cabo las etapas del método descrito en el primer aspecto inventivo.

Todas las características y/o las etapas de métodos descritas en esta memoria (incluyendo las reivindicaciones, descripción y dibujos) pueden combinarse en cualquier combinación, exceptuando las combinaciones de tales características mutuamente excluyentes.

Descripción de los dibujos

Estas y otras características y ventajas de la invención se pondrán más claramente de manifiesto a partir de la siguiente descripción detallada de una forma preferida de realización, dada únicamente a título de ejemplo ilustrativo y no limitativo, con referencia a las figuras que se acompañan.

La figura 1 muestra un diagrama de flujo del método de monitorización, registro y validación de certificados digitales según una realización de la presente invención.

La figura 2 muestra la arquitectura de la red privada de ordenadores del método de monitorización, registro y validación de certificados digitales según una realización de la presente invención.

Descripción detallada de la invención

La presente invención describe un método implementado por ordenador (100) para monitorizar (200), registrar (300) y validar (400) certificados digitales en una red privada de ordenadores (1) no conectada a Internet.

La figura 1 muestra un diagrama de flujo de una realización particular del método (100) en el que las fases de monitorización (200), registro (300) y validación (400) de certificados digitales pueden realizarse de forma simultánea. Tanto el registro (300) como la validación (400) de certificados digitales se realizan bajo demanda de los miembros de la red privada de ordenadores (1) mientras que la fase de monitorización (200) es un proceso periódico con una frecuencia definida por un miembro seleccionado (8) de la red privada de ordenadores (1).

La fase de registro (300) de certificados digitales comprende las siguientes etapas:

- crear (310) por la al menos una autoridad de certificación (7) al menos un certificado digital,
- asignar (320) por parte del al menos un servidor de registros (2) un identificador a dicho certificado digital para permitir que sea localizable por al menos dicho servidor de registros (2), y
- registrar (330) el al menos un certificado digital creado por dicha al menos una autoridad de certificación (7) en el al menos un servidor de registros (2), albergándolos en su base de datos (4).

La base de datos (4) del servidor de registros (2) basada en un árbol de Merkle se va completando según se reciben peticiones de creación de certificados digitales. Para ello, una autoridad de certificación (7) crea (310) el certificado digital y le asigna (320) un identificador concreto según la posición del árbol de Merkle en la que vaya a registrarse dicho certificado digital, con el objetivo de ser fácilmente localizable dentro del árbol de Merkle. Finalmente, el servidor de registros (2) registra (330) el certificado digital en el árbol de Merkle de su base de datos (4).

La fase de validación (400) del método comprende las siguientes etapas:

- recibir (410) el al menos un servidor de registros (2) al menos una solicitud de validación de certificado emitida por la red privada de ordenadores (1),
- 5 • consultar (420) por parte del al menos un servidor de registros (2), si el certificado digital bajo solicitud está contenido en su base de datos (4), y
- en caso de que el certificado digital bajo solicitud esté contenido en la base de datos (4), consultar (430) por parte del servidor de registros (2) si se cumple el al menos un requisito de validez (9) albergado en dicho servidor de registros (2), en donde:
 - o en caso de cumplirse, el certificado digital bajo solicitud se valida (440), o
 - 10 o en caso de no cumplirse, el certificado digital bajo solicitud no se valida (450),
- en caso de que el certificado digital bajo solicitud no esté contenido en la base de datos (4), el certificado bajo solicitud no se valida (450).

15 Desde el momento en que empieza a crearse la base de datos (4) del al menos un servidor de registros (2), dicho servidor de registros (2) puede empezar a recibir peticiones de validación de certificados digitales. En primer lugar, el al menos un servidor de registros (2) recibe (410) una solicitud de validación de certificado digital por parte de un miembro de la red privada de ordenadores (1); a continuación, el servidor de registros (2) consulta (420) si el certificado digital se encuentra registrado en su base de datos (4). En caso de que sí esté registrado, se procede a comprobar si el certificado cumple los requisitos de validez (9) almacenados en el servidor de registros (2) de forma que, si el certificado digital cumple los requisitos de validez (9), el certificado digital se valida (440) pero si no cumple dichos requisitos de validez (9), el certificado no se valida (450). En caso de que no esté registrado en la base de datos (4), el certificado digital tampoco se valida (450).

En un ejemplo particular de esta realización, cuando un certificado digital no se valida (450) se produce un mensaje de error y si el certificado digital se valida (440), el solicitante de la validación obtiene permiso para acceder a la red.

25 En otro ejemplo particular de esta realización, los requisitos de validez (9) comprenden la comprobación de la fecha de expiración del certificado digital y la verificación de la firma digital del solicitante de validación.

La fase de monitorización (200) del método comprende las siguientes etapas:

- a) acceder (210) por parte del al menos un servidor de monitorización (3) a la primera base de datos (4) del al menos un servidor de registros (2),
- 30 b) aplicar (220) por parte del al menos un servidor de monitorización (3) sobre los certificados digitales de la primera base de datos (4) del al menos un servidor de registros (2) la al menos una regla de auditoría (6), y
- c) emitir (230), por parte del al menos un servidor de monitorización (3), una alerta si al menos un certificado digital no cumple dicha al menos una regla de auditoría (6).

35 Desde el momento en que empieza a crearse la base de datos (4) del servidor de registros (2) puede comenzar a ejecutarse la fase de monitorización (200) sobre los certificados digitales contenidos en dicha base de datos (4). En primer lugar, el servidor de monitorización (3) accede (210) a la base de datos (4) del servidor de registros (2) para aplicar (220) sobre ellos las reglas de auditoría (6) que están contenidas en el propio servidor de monitorización (3). En caso de que algún certificado digital no cumpla alguna regla de auditoría (6), el servidor de monitorización (3) emite (230) una alerta informando de esta situación.

En un ejemplo particular de esta realización, las reglas de auditoría (6) comprenden:

- 40 • verificar que no existen certificados con un determinado número de serie;
- verificar que no existen certificados que utilicen ciertos algoritmos criptográficos;
- verificar que no existen más de un número determinado de certificados emitidos para un uso concreto, como para acceder a una red corporativa determinada, y/o
- avisar de los certificados a los que les quedan menos de dos meses para caducar,
- 45 pudiendo proveerse dichas las reglas de auditoría (6) por separado, en combinaciones de dos, en combinaciones de tres o en su totalidad.

En otro ejemplo particular de esta realización, la alerta es un mensaje de texto emitido a un miembro de la red privada de ordenadores (1) seleccionado con anterioridad, teniendo dicho miembro de la red privada de ordenadores

(1) autoridad para decidir cómo gestionar el certificado; por ejemplo, revocarlo, marcarlo como caducado, informar de su fraudulencia y/o exponer su susceptibilidad de haber sido robado.

En otro ejemplo particular de esta realización, la periodicidad en que se aplica la fase de monitorización (200) abarca desde un minuto hasta al menos un día.

- 5 La figura 2 muestra la arquitectura de la red privada de ordenadores (1) donde se aplican las fases de monitorización (200), registro (300) y validación (400) de certificados digitales de una realización particular de la invención.

En esta realización se dispone de un servidor de registros (2) con una base de datos (4) no relacional basada en un *árbol de Merkle* y de un servidor de monitorización (3) con una base de datos (5) no relacional también basada en un *árbol de Merkle*, ambos servidores ubicados en la red privada de ordenadores (1) no conectada a Internet.

- 10 Además, se designa a un miembro seleccionado (8) de la red privada de ordenadores (1) configurado para diseñar

- unas reglas de auditoría (6) que se albergarán en el servidor de monitorización (3), y
- unos requisitos de validez (9) que se albergarán en el servidor de registros (2).

Dicho miembro seleccionado (8) de la red privada de ordenadores (1) puede conectarse con ambos servidores directamente mediante una API o a través de una página web de administración (10).

- 15 También se designa una autoridad de certificación (7) capaz de crear certificados digitales para ser registrados (300) en el servidor de registros (2). Dicha autoridad de certificación (7) puede conectarse con el servidor de registros directamente mediante una API o a través de una página web de administración (10).

- 20 Adicionalmente, cuando un miembro de la red privada de ordenadores (12) solicita la validación de un certificado digital (400) al servidor de registros (2), el servidor de registros (2) comprueba si dicho certificado digital bajo solicitud se encuentra en su base de datos (4) y, en tal caso, comprueba si el certificado digital cumple con los requisitos de validez (9) albergados en el servidor de registros (9). Es necesario que se cumplan ambas premisas para que el miembro de la red privada de ordenadores (12) reciba autorización para conectarse a la red.

- 25 El miembro de la red privada de ordenadores (12) puede solicitar la validación de un certificado digital (400) mediante una API o mediante un protocolo de validación diferente, como por ejemplo un protocolo *OSCP*. En el segundo caso, el *módulo autoridad de verificación* (11) del servidor de registros (2) traduce el protocolo diferente a la API para que el miembro de la red privada de ordenadores (12) pueda comunicarse con el servidor de registros (2).

- 30 Además, periódicamente el servidor de monitorización (3) monitoriza (200) los certificados digitales contenidos en la base de datos (4) del servidor de registros (2) para comprobar si cumplen las reglas de auditoría (6) contenidas en dicho servidor de monitorización (3). La comunicación entre ambos servidores se realiza preferiblemente vía API. En caso de que algún certificado no cumpla alguna de las reglas de auditoría (6) se emite una alerta al miembro de la red privada de ordenadores (1) designado a tal fin, y se registra tanto el certificado digital como la alerta correspondiente generada en la base de datos (5) del servidor de monitorización (3).

En un ejemplo particular de esta realización, las tecnologías utilizadas en la arquitectura son:

- 35
- *Python* como código de desarrollo de las diferentes operaciones,
 - *AngularJS*, *HTML* y *CSS* como código de desarrollo de la página web de administración,
 - *Mongodb* para las bases de datos no relacionales,
 - *Flask* para ambos servidores

pudiendo darse dichas tecnologías por separado, en combinaciones de dos, en combinaciones de tres o en su totalidad.

- 40 En una realización ilustrativa preferida como “realización 1”, se presenta un

método implementado por ordenador (100) para monitorizar (200) certificados digitales en una red privada de ordenadores (1) no conectada a Internet, en donde la red privada de ordenadores (1) comprende:

- 45
- al menos un servidor de registros (2) configurado para registrar dichos certificados digitales, albergándolos en una primera base de datos (4) basada en un *árbol de Merkle*, y
 - al menos un servidor de monitorización (3) configurado para:
 - o albergar al menos una regla de auditoría (6),
 - o aplicar sobre los certificados digitales de la primera base de datos (4) del servidor de registros (2) al menos

una regla de auditoría (6), y

- o emitir una alerta si al menos un certificado no cumple dicha al menos una regla de auditoría (6),

en donde al menos una regla de auditoría (6) se define por al menos un miembro seleccionado (8) de la red privada de ordenadores (1), y

5 en donde el método (100) comprende las siguientes etapas:

- a) acceder (210) por parte del al menos un servidor de monitorización (3) a la primera base de datos (4) del al menos un servidor de registros (2),
- b) aplicar (220) por parte del al menos un servidor de monitorización (3) sobre los certificados digitales de la primera base de datos (4) del al menos un servidor de registros (2) la al menos una regla de auditoría (6), y

10 c) emitir (230), por parte del al menos un servidor de monitorización (3), una alerta si al menos un certificado digital no cumple dicha al menos una regla de auditoría (6).

“Realización 2”. El método (100) según la “realización 1”, en donde la red privada de ordenadores (1) además comprende al menos una autoridad de certificación (7), seleccionada de la red privada de ordenadores (1), que está configurada para crear y enviar los certificados digitales al al menos un servidor de registros (2) para ser registrados (300) por dicho al menos un servidor de registros (2),

15

en donde el método (100) además comprende las siguientes etapas:

- i. crear (310) por la al menos una autoridad de certificación (7) al menos un certificado digital,
- ii. asignar (320) por parte del al menos un servidor de registros (2) un identificador a dicho certificado digital para permitir que sea localizable por al menos dicho servidor de registros (2), y
- 20 iii. registrar (330) el al menos un certificado digital creado por dicha al menos una autoridad de certificación (7) en el al menos un servidor de registros (2), albergándolos en su base de datos (4).

“Realización 3”. El método (100) según las “realizaciones” anteriores, en donde la al menos una autoridad de certificación (7) está configurada para crear certificados digitales bajo servicio.

25 “Realización 4”. El método (100) según cualquiera de las “realizaciones” anteriores, en donde al emitir (230) una alerta por parte del al menos un servidor de monitorización (3), se envía una notificación a un destinatario de la red privada de ordenadores (1) predefinido en dicho servidor de monitorización (3).

30 “Realización 5”. El método (100) según cualquiera de las “realizaciones” anteriores, en donde el al menos un servidor de monitorización (3) además está configurado para registrar tanto el al menos un certificado digital que incumple la regla de auditoría (6), como la correspondiente alerta emitida, en una segunda base de datos (5) basada en un árbol de Merkle.

“Realización 6”. El método (100) según cualquiera de las “realizaciones” anteriores, en donde el al menos un servidor de monitorización (3) está configurado para comunicarse con el al menos un servidor de registros (2) mediante una API.

35 “Realización 7”. El método (100) según cualquiera de las anteriores “realizaciones 2 a 6”, en donde la al menos una autoridad de certificación (7) está configurada para comunicarse con el al menos un servidor de registros (2) mediante una API o mediante una página web de administración (10).

“Realización 8”. El método (100) según cualquiera de las “realizaciones” anteriores, en donde el servidor de registros (2) además está configurado para albergar al menos un requisito de validez (9) que:

- está relacionado con la información de los certificados digitales contenidos en dicho servidor de registros (2), y

40 • está definido por al menos un miembro seleccionado (8) de la red privada de ordenadores (1).

“Realización 9”. El método (100) según la “realización” anterior, en donde el servidor de registros (2) además está configurado para validar (400) certificados digitales particulares bajo solicitud de la red privada de ordenadores (1),

en donde dicho método (100) además comprende las etapas de:

- 45 v. recibir (410) por parte del al menos un servidor de registros (2) al menos una solicitud de validación de certificado digital emitida por la red privada de ordenadores (1),
- vi. consultar (420) por parte del al menos un servidor de registros (2), si el certificado digital bajo solicitud está contenido en su base de datos (4), y

- vii. en caso de que el certificado digital bajo solicitud esté contenido en la base de datos (4), consultar (430) por parte del servidor de registros (2) si se cumple el al menos un requisito de validez (9) albergado en dicho servidor de registros (2), en donde:
- c. en caso de cumplirse, el certificado digital bajo solicitud se valida (440), o
- 5 d. en caso de no cumplirse, el certificado digital bajo solicitud no se valida (450),
- viii. en caso de que el certificado digital bajo solicitud no esté contenido en la base de datos (4), el certificado bajo solicitud no se valida (450).
- 10 “Realización 10”. El método (100) según cualquiera de las “realizaciones” anteriores, en donde al menos un miembro seleccionado (8) de la red privada de ordenadores (1) está configurado para comunicarse con el al menos un servidor de monitorización (3) y/o con el al menos un servidor de registros (2) mediante una API o mediante una página web de administración (10).
- 15 “Realización 11”. El método (100) según la “realización” anterior, en donde el servidor de registros (2) además comprende un módulo adicional (11) configurado para convertir las solicitudes de validación emitidas por parte de la red privada de ordenadores (1) en un formato determinado, preferiblemente API, de manera que estas solicitudes sean entendibles por el servidor de registros (2).
- “Realización 12”. El método según cualquiera de las “realizaciones 7 a 11”, en donde la página web de administración (10) está configurada para:
- recibir certificados digitales por parte de la al menos una autoridad de certificación (7) y enviar dichos certificados al al menos un servidor de registros (2), y/o
 - 20 • recibir al menos un requisito de validez (9) definido por al menos un miembro seleccionado (8) de la red privada de ordenadores (1) y enviar dicho requisito de validez (9) al al menos un servidor de registros (2), y/o
 - recibir al menos una regla de auditoría (6) definida por al menos un miembro seleccionado (8) de la red privada de ordenadores (1) y enviar dicha regla de auditoría (6) al al menos un servidor de monitorización (3).
- 25 “Realización 13”. Un sistema de monitorización (200), registro (300) y validación (400) de certificados digitales que comprende medios para llevar a cabo las etapas del método según cualquiera de las “realizaciones” anteriores.
- “Realización 14”. Un programa de ordenador que comprende instrucciones mediante las cuales, cuando el programa es ejecutado por un ordenador, se hace que dicho ordenador lleve a cabo las etapas del método según cualquiera de las “realizaciones 1 a 12”.
- 30 “Realización 15”. Un medio legible por ordenador que comprende instrucciones mediante las cuales, cuando dichas instrucciones son ejecutadas por un ordenador, se hace que dicho ordenador lleve a cabo las etapas del método según las “realizaciones 1 a 12”.

REIVINDICACIONES

1. Un método implementado por ordenador (100) para monitorizar (200) y validar (400) certificados digitales en una red privada de ordenadores (1) no conectada a Internet, en donde la red privada de ordenadores (1) comprende:

- 5
- al menos un servidor de registros (2) configurado para registrar dichos certificados digitales, albergándolos en una primera base de datos (4) basada en un árbol de Merkle, y
 - al menos un servidor de monitorización (3) configurado para:
 - albergar al menos una regla de auditoría (6),
 - aplicar sobre los certificados digitales de la primera base de datos (4) del servidor de registros (2) al menos una regla de auditoría (6), y
 - emitir una alerta si al menos un certificado no cumple dicha al menos una regla de auditoría (6),
- 10

en donde al menos una regla de auditoría (6) se define por al menos un miembro seleccionado (8) de la red privada de ordenadores (1), y

15 en donde el método (100) comprende las siguientes etapas:

- a) acceder (210) por parte del al menos un servidor de monitorización (3) a la primera base de datos (4) del al menos un servidor de registros (2),
 - b) aplicar (220) por parte del al menos un servidor de monitorización (3) sobre los certificados digitales de la primera base de datos (4) del al menos un servidor de registros (2) la al menos una regla de auditoría (6), y
 - c) emitir (230) una alerta, por parte del al menos un servidor de monitorización (3), si al menos un certificado digital no cumple dicha al menos una regla de auditoría (6); y
- 20

en donde el servidor de registros (2) además está configurado para albergar al menos un requisito de validez (9) que:

- está relacionado con la información de los certificados digitales contenidos en dicho servidor de registros (2), y
 - está definido por al menos un miembro seleccionado (8) de la red privada de ordenadores (1); y
- 25

en donde el servidor de registros (2) además está configurado para validar (400) certificados digitales particulares bajo solicitud de la red privada de ordenadores (1),

30 en donde dicho método (100) además comprende las etapas de:

- i. recibir (410) por parte del al menos un servidor de registros (2) al menos una solicitud de validación de certificado digital emitida por la red privada de ordenadores (1),
 - ii. consultar (420) por parte del al menos un servidor de registros (2), si el certificado digital bajo solicitud está contenido en su base de datos (4), y
 - iii. en caso de que el certificado digital bajo solicitud esté contenido en la base de datos (4), consultar (430) por parte del servidor de registros (2) si se cumple el al menos un requisito de validez (9) albergado en dicho servidor de registros (2), en donde:
 - a. en caso de cumplirse, el certificado digital bajo solicitud se valida (440), o
 - b. en caso de no cumplirse, el certificado digital bajo solicitud no se valida (450),
 - iv. en caso de que el certificado digital bajo solicitud no esté contenido en la base de datos (4), el certificado bajo solicitud no se valida (450); y
- 35
- 40

en donde al menos un miembro seleccionado (8) de la red privada de ordenadores (1) está configurado para comunicarse con el al menos un servidor de monitorización (3) y/o con el al menos un servidor de registros (2) mediante una API o mediante una página web de administración (10); y

45 en donde el servidor de registros (2) además comprende un módulo adicional (11) configurado para convertir las solicitudes de validación emitidas por parte de la red privada de ordenadores (1) en un formato

- determinado, preferiblemente API, de manera que estas solicitudes sean entendibles por el servidor de registros (2).
2. El método (100) según la reivindicación anterior, en donde la red privada de ordenadores (1) además comprende al menos una autoridad de certificación (7), seleccionada de la red privada de ordenadores (1), que está configurada para crear y enviar los certificados digitales al al menos un servidor de registros (2) para ser registrados (300) por dicho al menos un servidor de registros (2),
- 5 en donde el método (100) además comprende las siguientes etapas:
- i. crear (310) por la al menos una autoridad de certificación (7) al menos un certificado digital,
 - 10 ii. asignar (320) por parte del al menos un servidor de registros (2) un identificador a dicho certificado digital para permitir que sea localizable por al menos dicho servidor de registros (2), y
 - iii. registrar (330) el al menos un certificado digital creado por dicha al menos una autoridad de certificación (7) en el al menos un servidor de registros (2), albergándolos en su base de datos (4).
3. El método (100) según la reivindicación anterior, en donde la al menos una autoridad de certificación (7) está configurada para crear certificados digitales bajo servicio.
- 15 4. El método (100) según cualquiera de las reivindicaciones anteriores, en donde al emitir (230) una alerta por parte del al menos un servidor de monitorización (3), se envía una notificación a un destinatario de la red privada de ordenadores (1) predefinido en dicho servidor de monitorización (3).
5. El método (100) según cualquiera de las reivindicaciones anteriores, en donde el al menos un servidor de monitorización (3) además está configurado para registrar tanto el al menos un certificado digital que incumple la regla de auditoría (6), como la correspondiente alerta emitida, en una segunda base de datos (5) basada en un árbol de Merkle.
- 20 6. El método (100) según cualquiera de las reivindicaciones anteriores, en donde el al menos un servidor de monitorización (3) está configurado para comunicarse con el al menos un servidor de registros (2) mediante una API.
- 25 7. El método (100) según cualquiera de las reivindicaciones anteriores 2 a 6, en donde la al menos una autoridad de certificación (7) está configurada para comunicarse con el al menos un servidor de registros (2) mediante una API o mediante una página web de administración (10).
8. El método según la reivindicación 7, en donde la página web de administración (10) está configurada para:
- 30 • recibir certificados digitales por parte de la al menos una autoridad de certificación (7) y enviar dichos certificados al al menos un servidor de registros (2), y/o
 - recibir al menos un requisito de validez (9) definido por al menos un miembro seleccionado (8) de la red privada de ordenadores (1) y enviar dicho requisito de validez (9) al al menos un servidor de registros (2), y/o
 - 35 • recibir al menos una regla de auditoría (6) definida por al menos un miembro seleccionado (8) de la red privada de ordenadores (1) y enviar dicha regla de auditoría (6) al al menos un servidor de monitorización (3).
9. Un sistema de monitorización (200), registro (300) y validación (400) de certificados digitales que comprende medios para llevar a cabo las etapas del método según cualquiera de las reivindicaciones anteriores.
- 40 10. Un programa de ordenador que comprende instrucciones mediante las cuales, cuando el programa es ejecutado por un ordenador, se hace que dicho ordenador lleve a cabo las etapas del método según cualquiera de las reivindicaciones 1 a 8.
11. Un medio legible por ordenador que comprende instrucciones mediante las cuales, cuando dichas instrucciones son ejecutadas por un ordenador, se hace que dicho ordenador lleve a cabo las etapas del método según las reivindicaciones 1 a 8.
- 45

RESUMEN

La presente invención se refiere a un método implementado por ordenador para monitorizar, registrar y validar certificados digitales en una red privada de ordenadores no conectada a Internet.

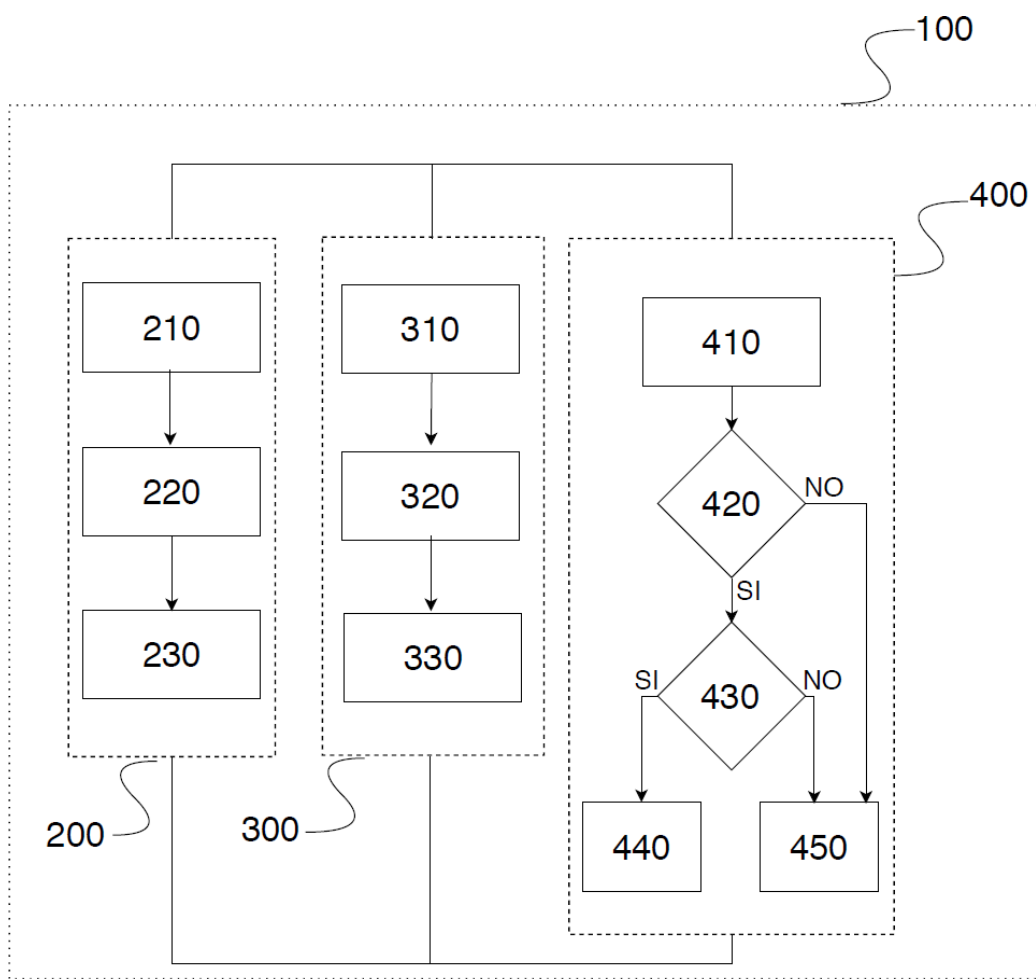


FIG 1

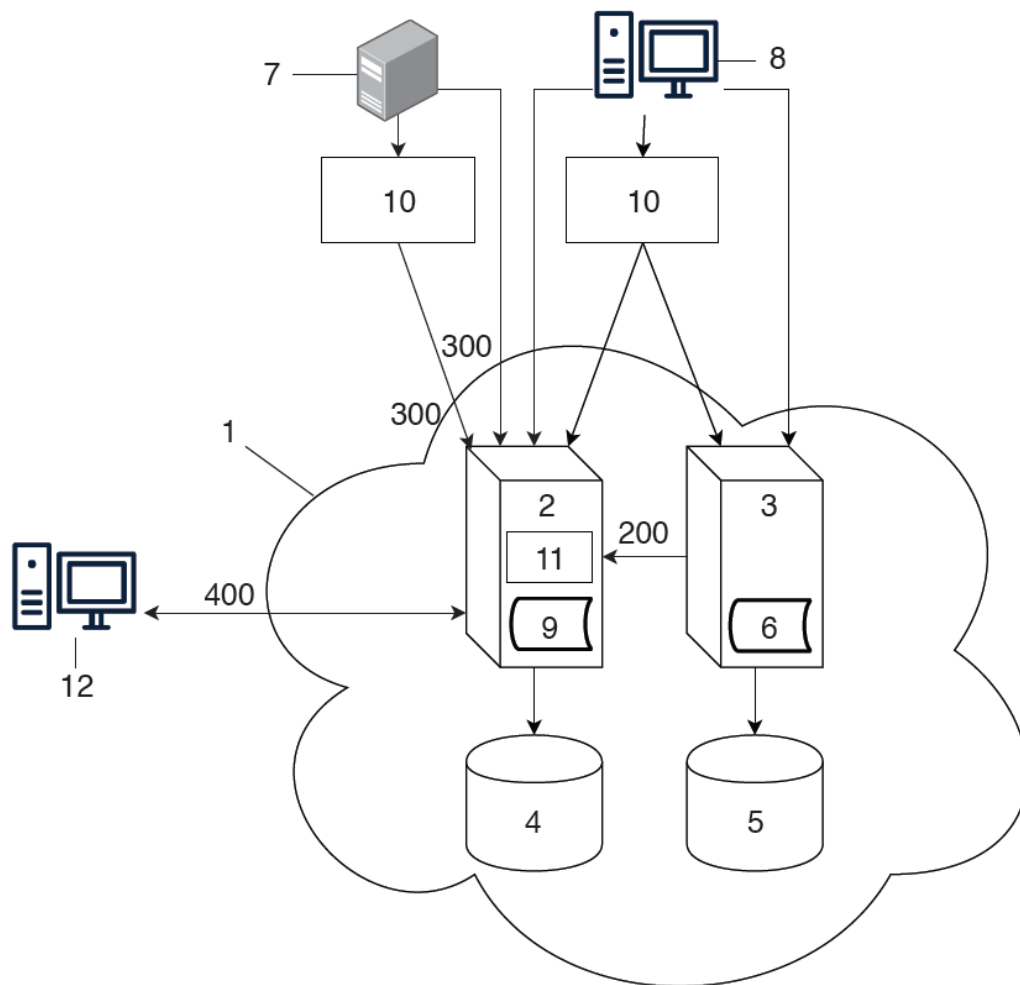


FIG 2