

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:
 - 10 ○ 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
 - 15 ○ 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

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),
- 20 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

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

- 25 • 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

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
- 35 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),
- 40 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

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),

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
- 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.

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.

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.

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:

- 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
- 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.

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.