

REIVINDICACIONES

1. Un método implementado en computador para generación de datos de certificación (12) de un documento electrónico, que comprende ejecutar en una unidad de cómputo (1) las etapas de:

- a) autenticar un usuario (2) mediante un proceso de verificación de identidad, donde el proceso de verificación de identidad incluye ejecutar al menos una primera autenticación y una segunda autenticación; donde el usuario (2) accede desde una terminal (3) a una aplicación (4) que conecta la terminal (3) con la unidad de cómputo (1);
- b) recibir, desde una terminal (3) del usuario (2), una solicitud de certificación de estado (5) asociada a un archivo (6), donde el archivo (6) se almacena en una base de datos (7), y donde el archivo (6) incluye al menos un documento electrónico;
- c) transmitir, a un servidor validador (9), una solicitud de verificación (8) que incluye el archivo (6), un dato de estampa de tiempo (10) y un dato de identificación (11) asociado al usuario (2), y
- d) recibir, desde el servidor validador (9), un dato de certificación (12) asociado a la solicitud de verificación (8), donde el servidor validador (9) obtiene el dato de certificación (12) mediante un proceso basado en una red blockchain (13).

2. El método de la Reivindicación 1, donde proceso basado en una red blockchain (13) para obtener el dato de certificación (12) comprende las subetapas de:

- i. validar si existe una billetera digital (14) asociada al usuario (2) en una red blockchain (13);
- ii. crear una billetera digital (14) asociada al usuario (2), si la validación es negativa; donde la billetera digital (14) incluye un dato de clave privada, un dato de clave pública, y un dato de identificación (11) asociado al usuario (2);
- iii. generar, con la red blockchain (13) asociada a la billetera digital (14), un dato hash (15) asociado al archivo (6) del dato de solicitud de verificación (8), y
- iv. obtener el dato de certificación (12) a partir del dato hash (15), donde el dato de certificación (12) incluye el dato hash (15), un dato de estado del documento electrónico del archivo (6) y un dato de estampa de tiempo (10), asociado al momento en que se genera el dato hash (15), que se obtiene mediante estampado cronológico en la red blockchain (13).

3. El método de la Reivindicación 1, donde al menos la unidad de cómputo (1), el servidor validador (9) y la red blockchain (13) se conectan mediante una puerta de enlace de API (17), y donde, en la etapa a) la primera autenticación comprende las subetapas:

- a1) transmitir, mediante la puerta de enlace de API (17), una solicitud de autenticación (18) que incluye el dato de identificación (11) del usuario (2) y un dato de credenciales de acceso asociadas al usuario (2), y
- a2) enrutar la solicitud de autenticación (18), mediante la puerta de enlace de API (17), hacia un servicio de backend configurado para validar el dato de credenciales de acceso asociadas al usuario (2) de acuerdo con un protocolo de seguridad predeterminado;
- a3) recibir, a través de la puerta de enlace de API (17), un dato de respuesta (19) con un valor seleccionado entre “aprobado” o “rechazado” generado por el servicio de backend;
donde la puerta de enlace de API (17) está configurada para limitar el acceso de la unidad de cómputo (1) a la billetera digital (14) en la red blockchain (13), de acuerdo con el protocolo de seguridad predeterminado.

4. El método de la Reivindicación 1, donde en la etapa a) la segunda autenticación incluye

- a4) enviar una solicitud de autenticación (18) a un servidor de generación de OTP (20);
- a5) recibir desde la terminal (3) del usuario (2) un comando OTP (22) que incluye un código de único uso (26) generado por el servidor de generación OTP (20) y que es enviado electrónicamente a un dispositivo electrónico (27) del usuario (2).

5. El método de la Reivindicación 1, donde en la etapa a) la segunda autenticación incluye:

- a6) enviar una solicitud de autenticación (18) al servidor validador (9), donde la solicitud de autenticación (18) incluye el dato de identificación (11) del usuario (2);
- a7) recibir desde el servidor validador (9), un dato de respuesta (19) con un valor seleccionado entre “aprobado” o “rechazado”,
donde el servidor validador (9) genera el valor “aprobado” si el valor del dato de identificación (11) de usuario (2) coincide con unas credenciales (24) asociadas a una billetera digital (14) previamente creada por el usuario (2); y
- a8) pasar a la etapa b) si el valor del dato de respuesta (19) es “aprobado”.

6. El método de la Reivindicación 3, en donde posterior a la etapa a2) se realiza una subetapa a9) de balancear una carga de trabajo mediante las siguientes subetapas:

- f. recibir solicitudes de acceso mediante la dirección IP de un balanceador de carga (25);
- g. distribuir las solicitudes de acceso entre instancias del grupo de destino;
- h. seleccionar la instancia del grupo de destino que esté disponible;
- i. comprobar que cada instancia del grupo de destino esté operativa y sea capaz de manejar el tráfico, y
- j. redireccionar respuesta de solicitud de acceso;
- k. registrar en un dato de historial una información sobre las solicitudes y el rendimiento de las instancias;

7. El método de la Reivindicación 3, en donde posterior a la etapa a3) se realiza una subetapa a10) de conectar la unidad de cómputo (1) con la puerta de enlace de API (17) de conexión que se encarga de gestionar la autenticación mediante un protocolo de autorización y permite el acceso a la billetera digital (14).

8. El método de la Reivindicación 2, donde el dato de estampa de tiempo (10) se obtiene mediante las subetapas de:

- l. preparar los datos a estampar en la red blockchain (13) proporcionando una estructura y formato adecuados de la información que se va a estampar;
- m. generar una transacción con los datos de la subetapa anterior;
- n. introducir la información específica a inmutabilizar;
- o. calcular el dato hash (15) de la información incluida en la transacción para garantizar su integridad;
- p. firmar la transacción con una clave privada para autenticar y asegurar la propiedad de la información; y
- q. transmitir la transacción a la red blockchain (13) para su procesamiento y validación.

9. El método de la Reivindicación 3, donde en la subetapa a2 el servicio de backend configurado para validar el dato de credenciales de acceso asociadas al usuario (2) se hace una firma digital mediante las subetapas de:

- r. solicitar una billetera digital (14) para firmar transacciones, mediante un servicio Signer;
- s. crear una billetera digital (14) mediante un servicio Signer;
- t. almacenar la billetera digital (14).

10. El método de la Reivindicación 3, donde en la subetapa a2) el servicio de backend está configurado para autenticar el usuario (2) mediante las subetapas de:

- u. solicitar, mediante una aplicación (4) a la que accede el usuario (2), un inicio sesión por parte del usuario (2), donde el usuario (2) inicia sesión ingresando sus credenciales de acceso;
- v. redirigir la solicitud de autenticación (18) de usuario (2) al servidor donde se aloja el servicio de backend que realiza autenticación (18);
- w. aplicar un protocolo de autorización de las credenciales de acceso del usuario (2), donde, si la autenticación es exitosa se procede a continuar a la etapa siguiente de lo contrario no se genera autorización;
- x. generar un código de autorización mediante el servicio de backend alojado en un servidor;
- y. intercambiar el código de autorización por un token de acceso
- z. utilizar el token de acceso para acceder a recursos protegidos en nombre del usuario (2).
