(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 053 822**

(21) Número de solicitud: 202430557

(51) Int. CI.:

G06F 21/00 (2013.01)
G06Q 20/00 (2012.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

03.07.2024

(43) Fecha de publicación de la solicitud:

26.01.2026

(71) Solicitantes:

UNIVERSIDAD POLITÉCNICA DE CARTAGENA (100,00%)
Plaza Cronista Isidoro Valverde, s/n Ed. La Milagrosa
30202 CARTAGENA (Murcia) ES

(72) Inventor/es:

CANO BAÑOS, María Dolores

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

(54) Título: **Método y sistema para verificar la autenticidad e integridad de datos preservando la privacidad**

(57) Resumen:

Método y sistema para verificar la autenticidad e integridad de datos preservando la privacidad.

Se describe un método y sistema avanzado para verificar la autenticidad e integridad de datos anonimizados en redes de telecomunicaciones, centrado en la seguridad de la información y la protección de la privacidad del usuario. Se propone una solución novedosa para gestionar datos de forma segura, garantizando anonimato, privacidad y verificación. Mediante el uso de algoritmos criptográficos avanzados y protocolos de procesamiento de datos únicos, el sistema asegura la privacidad y anonimato del usuario, mientras valida la integridad y autenticidad de los datos transmitidos. Esta invención ofrece una mejora significativa en la protección de la información personal y la gestión de datos en una variedad de sectores críticos, destacando por su simplicidad operativa y robustez frente a métodos existentes.

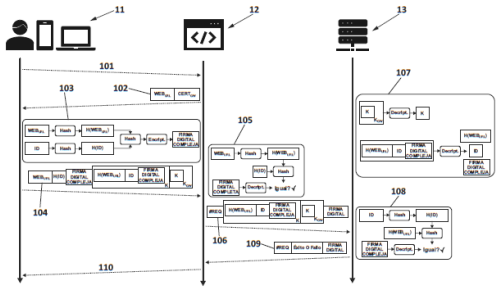

FIG. 1

ES 3 053 822 A1

DESCRIPCIÓN

Método y sistema para verificar la autenticidad e integridad de datos preservando la privacidad

OBJETO DE LA INVENCIÓN

La presente invención tiene su aplicación en el sector de las telecomunicaciones, dentro del campo de la seguridad de la información digital y el procesamiento y comunicación de contenido digital. En particular, en la protección de la información, gestión de datos, enmascaramiento de datos, anonimato y navegación web segura. Más específicamente, la presente invención se refiere a un método y sistema para garantizar integridad y autenticación de los datos transmitidos a través de redes o sistemas de telecomunicación, preservando su privacidad.

ANTECEDENTES DE LA INVENCIÓN

Actualmente, existen una diversidad de metodologías y tecnologías diseñadas para enfrentar los desafíos asociados a la seguridad de la información y la protección de datos personales. En el ámbito de la verificación de datos que son transmitidos a través de redes de telecomunicación, con un enfoque particular en la preservación de la privacidad, el anonimato, la integridad y la autenticación, se presentan a continuación algunos de los desarrollos recientes y limitaciones existentes en el contexto de la protección de la privacidad en la transmisión de datos.

Uno de los grandes bloques para la seguridad y protección de datos está relacionado con la criptografía. La criptografía ha sido la piedra angular en la protección de datos, con avances significativos en algoritmos simétricos y asimétricos, criptografía de clave pública y particularmente en técnicas de cifrado homomórfico, que permiten operaciones en datos cifrados sin necesidad de descifrarlos (obteniendo lo mismo que si se realizan operaciones equivalentes sobre los datos originales sin cifrar). Esto permite que se puedan procesar datos sensibles de manera segura, preservando la privacidad del usuario, y luego obtener resultados cifrados que, una vez descifrados, son equivalentes a si los cálculos se hubieran realizado sobre los datos originales en texto claro (sin cifrar). Sin embargo, se trata de técnicas computacionalmente intensivas y pueden resultar en un procesamiento más lento. A menudo, requieren un compromiso entre la seguridad y la eficiencia computacional puesto que en

numerosas ocasiones necesitan elevados recursos computacionales para poder ejecutarse.

Un segundo bloque son las técnicas de anonimización. El proceso o concepto de anonimización (o disociación de datos) consiste en eliminar o reducir el riesgo remanente de reidentificación de los datos anonimizados, es decir, se trata de una técnica por la cual se eliminan o reducen las posibilidades de identificar al titular de los datos, manteniendo la veracidad y exactitud de los resultados del tratamiento de los mismos. En este campo, se han desarrollado métodos como “k-anonymity”, “l-diversity” y “t-closeness” para anonimizar conjuntos de datos, protegiendo la privacidad del individuo. Aunque estas técnicas son efectivas en ciertos contextos, pueden ser susceptibles a ataques de inferencia, especialmente con el volumen y la variedad de datos disponibles en la actualidad.

Otras opciones en la misma línea son la supresión, la generalización o el “data swapping” (intercambio de datos). La supresión consiste en eliminar directamente información identificativa de un conjunto de datos; esto, aunque efectivo para proteger la privacidad, puede reducir significativamente la utilidad de los datos. La generalización implica reemplazar datos detallados con categorías más amplias; y el “data swapping” modifica el conjunto de datos intercambiando valores de datos entre registros; en ambos casos, se mantiene la distribución general de los datos pero dificulta la identificación de individuos lo que reduce la precisión de los datos pero mejora la privacidad.

Otra técnica reciente es privacidad diferencial (“Differential Privacy”). Es una técnica que permite compartir información sobre un conjunto de datos agregando cierta cantidad de ruido aleatorio a los resultados de las consultas, garantizando que la inclusión o exclusión de un solo individuo en el conjunto de datos no afecte significativamente el resultado. Esto permite obtener percepciones (en inglés “insights”) útiles de los datos sin comprometer la privacidad de los individuos. La principal ventaja de la privacidad diferencial radica en su capacidad para ofrecer garantías matemáticas de privacidad bajo un modelo bien definido de riesgos.

Una alternativa la encontramos en el aprendizaje federado (“Federated Learning” en inglés). Es un enfoque de aprendizaje automático que permite entrenar modelos a través de múltiples dispositivos descentralizados o servidores que contienen muestras de datos locales, sin intercambiarlos. Así, este proceso consiste en entrenar modelos locales en los dispositivos y, a continuación, agregar estos modelos en un servidor central para actualizar un modelo global, que se distribuye de nuevo a los dispositivos. El ciclo se repite, mejorando el modelo con datos

de diversas fuentes sin necesidad de compartir o centralizar los propios datos. Tiene la ventaja de que al mantener los datos en los dispositivos locales y compartir únicamente las actualizaciones de los modelos, el aprendizaje federado protege intrínsecamente los datos de los usuarios, reduciendo el riesgo de violación de la privacidad. Además, es compatible con las técnicas de privacidad diferencial, lo que garantiza que las contribuciones de datos al modelo puedan autenticarse y verificarse sin exponer los datos subyacentes.

Sin embargo, el aprendizaje federado presenta algunas desventajas como, por ejemplo: El proceso de agregar actualizaciones de modelos de numerosos dispositivos puede introducir una sobrecarga de comunicación significativa, lo que afecta a la eficiencia; el aprendizaje federado es susceptible de sufrir ataques de envenenamiento de modelos, en los que actualizaciones malintencionadas influyen negativamente en el modelo global; y el uso de datos que no son distribuidos de forma independiente e idéntica entre dispositivos puede resultar complicado y dar lugar a modelos sesgados.

A su vez, las tecnologías “blockchain” (que se puede traducir como cadena de bloques en español), también conocida como Tecnologías de Libro Mayor Distribuido (en inglés “Distributed Ledger Technologies”, DTL), ofrecen un enfoque innovador para la integridad y autenticación de datos mediante cadenas de bloques inmutables. Aunque prometedoras, la escalabilidad, la gestión de la privacidad y el consumo de energía siguen siendo retos importantes en este tipo de técnicas.

Resumiendo, un problema general de la mayoría de las soluciones criptográficas seguras existentes es que incurren en un alto costo computacional, lo que limita su aplicabilidad en dispositivos con recursos limitados, generando un compromiso entre privacidad y eficiencia. Por otro lado, las técnicas de anonimización pueden no ser suficientemente robustas frente a ataques sofisticados de re-identificación, especialmente en el contexto de grandes volúmenes de datos interconectados. Por su parte, la adición de ruido en “Differential Privacy” para proteger la privacidad puede degradar la utilidad de los datos, especialmente en consultas que requieren alta precisión; además, determinar el nivel adecuado de ruido para equilibrar privacidad y utilidad puede ser desafiante y depende significativamente del contexto específico de aplicación. Por último, aunque el “blockchain” presenta una solución potencial para varios desafíos de seguridad, su adopción está limitada por problemas de escalabilidad, privacidad y costos operativos.

Por lo tanto, se puede decir que el estado del arte en las soluciones de verificación de datos (preservando la privacidad al mismo tiempo), refleja un campo en rápida evolución con avances significativos pero con bastantes limitaciones. La innovación propuesta busca abordarlas ofreciendo una solución integral que resuelve el problema de garantizar la privacidad, el anonimato, la integridad y la autenticación de los datos en una amplia gama de aplicaciones, superando las limitaciones/desventajas existentes.

DESCRIPCIÓN DE LA INVENCIÓN

La presente invención resuelve este problema, mediante un método y sistema para la verificación de datos anonimizados, que mejora la seguridad de la transmisión de datos mediante un sistema que garantiza el anonimato, la integridad y la autenticación sin sacrificar la privacidad del usuario en las redes de telecomunicación. Para ello utiliza algoritmos criptográficos avanzados junto con protocolos de procesamiento de datos novedosos para autenticar y verificar datos, manteniendo el anonimato/privacidad total del usuario. Este sistema se caracteriza por su eficiencia computacional y su aplicabilidad universal, estableciendo un nuevo enfoque en las tecnologías de verificación de datos que preservan la privacidad. A este método y sistema se le llamará VDA2 (de Verificación de Datos Anominizados y su Autenticación).

La solución propuesta comprende un marco único que integra, por ejemplo, la creación de firmas digitales, el uso de funciones hash y de criptografía de clave pública y un protocolo adaptable. El método puede incluir fases de inicialización, de mecanismo de doble firma para la autenticación específica del usuario o fuente de la información, de creación de información cifrada que mantiene el anonimato durante la verificación, de descifrado y de procesos de validación. Una entidad de confianza será la encargada de la generación y distribución de certificados digitales asociados a las claves privadas de los participantes. No obstante, el uso de certificados digitales o una infraestructura de clave pública (en inglés “Public Key Infrastucture” PKI) no es condición necesaria para aplicar esta invención, pudiendo emplearse otras alternativas como FIDO (Fast IDentity Online), un conjunto de estándares abiertos para la autenticación en línea que buscan mejorar la seguridad y simplicidad en el uso de credenciales.

Existe un elemento que actúa como intermediario para la verificación de datos e información. A este dispositivo intermediario verificador, se le denomina "Pulse Gateway" (que se puede

traducir al español como puerta de enlace de pulso o pasarela de pulso), pero en general no tiene por qué ser obligatoriamente un “Gateway” sino que puede ser un dispositivo electrónico de cualquier tipo, con capacidad de comunicación y procesamiento. Pueden ser uno o varios; existirán tantos como sean necesarios para garantizar la escalabilidad y prestaciones del sistema. El método aprovecha esta pasarela para proporcionar una verificación fiable en múltiples aplicaciones, desde el acceso a contenidos en línea hasta transacciones seguras, sin comprometer la integridad de los datos ni la privacidad del usuario.

La invención propuesta se diferencia de las técnicas convencionales por su eficiencia y aplicabilidad universal, ofreciendo una mejora significativa en la protección de la información personal y la gestión de datos en una variedad de sectores críticos (como pueden ser IoT, sanidad…), destacando por su simplicidad operativa y robustez frente a métodos existentes. Así, la presente invención, en comparación con otras soluciones existentes como el “Federated Learning”, propone un mecanismo directo para la verificación y autenticación de datos preservando la privacidad y el anonimato, diseñado específicamente para redes de telecomunicaciones. No requiere el entrenamiento iterativo y descentralizado de modelos, sino que se centra en procesos de verificación seguros y anónimos. La solución propuesta es más sencilla que las del estado del arte en términos de requisitos operativos, minimizando la sobrecarga de comunicación y abordando directamente los riesgos de violación de datos o acceso no autorizado sin las complejidades asociadas al entrenamiento y la agregación de modelos. Además, evita la posibilidad de envenenamiento del modelo al no depender de actualizaciones agregadas para un modelo global, ofreciendo una solución más específica para la integridad de los datos y la autenticación en las comunicaciones digitales.

En concreto, un primer aspecto de la presente invención se refiere a un método para la verificación de datos, que comprende los siguientes pasos:

a) un primer dispositivo electrónico, dispositivo remitente, envía a un segundo dispositivo electrónico, dispositivo destinatario, un mensaje incluyendo una petición de realizar una acción de intercambio de datos (una acción relacionada con datos) con el dispositivo destinatario;

b) el dispositivo destinatario envía al remitente una información referente al dispositivo destinario y una identificación de un tercer dispositivo electrónico, dispositivo intermediario verificador (el llamado Pulse Gateway);

c) el dispositivo remitente realiza un hash de la información referente al dispositivo

destinario un hash de un dato proporcionado por el dispositivo remitente (por ejemplo, un identificador del usuario), calcula un segundo hash de ambos hash concatenados y encripta el resultado, el resultado encriptado se le denomina firma digital compleja;

d) el dispositivo remitente envía un mensaje al dispositivo destinatario que comprende: la información referente al dispositivo destinario, el hash del dato del dispositivo remitente, la firma digital compleja y la siguiente información cifrada con una clave K generada por el dispositivo remitente: el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja y donde el mensaje comprende adicionalmente la clave K cifrada (por ejemplo, con una clave pública del dispositivo intermediario verificador);

e) el dispositivo destinatario realiza el hash de la información referente al dispositivo destinario y lo concatena con el hash del dato del dispositivo remitente recibido hash y el resultado lo compara con el resultado de descifrar la firma digital compleja que ha recibido, si ambos resultados coinciden (se ha mantenido la integridad de los mensajes) se va al paso f), si no, se termina el método (dando un resultado de falta de integridad);

f) el dispositivo destinatario envía al dispositivo intermediario verificador un mensaje que contiene la información cifrada con la clave K recibida del el dispositivo remitente y la clave K cifrada recibida del dispositivo remitente;

g) el dispositivo intermediario verificador utilizando su clave privada descifra la clave K y utilizando la clave K descifra la información recibida, obteniendo el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja;

h) el dispositivo intermediario verificador realiza el hash del dato del dispositivo remitente recibido y lo concatena con el hash de la información referente al dispositivo destinario recibido y el resultado lo compara con el resultado de descifrar la firma digital compleja que ha recibido;

i) el dispositivo intermediario verificador determina, basado al menos en la comparación de ambos resultados, el éxito de la verificación y si se determina que la verificación es exitosa, se envía un mensaje al dispositivo destinatario indicando que la verificación es exitosa y, por lo tanto, se puede realizar la acción de intercambio de datos requerida por el dispositivo remitente;

donde la comunicación entre el dispositivo remitente y el dispositivo destinatario y de éste con el dispositivo intermediario verificador se realiza a través de una o más redes de comunicación (que pueden ser por ejemplo redes de telefonía móvil 2G, 3G, 4G, 5G, redes de área local,

redes de fibra óptica o cualquier otro tipo de redes de comunicación).

En una realización, la acción de intercambio de datos es acceder a información a través del dispositivo destinatario y el dato proporcionado por el dispositivo remitente es un identificador de un usuario del dispositivo remitente. En ese caso, el dispositivo verificador puede determinar que la verificación es exitosa solo si los resultados coinciden o si además de coincidir, el dispositivo intermediario verificador verifica que el usuario cumple una determinada condición la información del remitente es válida. Esta acción puede ser es acceder a una página web a través del dispositivo destinatario (por ejemplo, un servidor web) y la información referente al dispositivo destinario sería la identificación de una página web (por ejemplo, el URL) a la que el usuario quiere acceder.

En una realización la acción de intercambio de datos es proporcionar un dato (o conjunto de datos) al dispositivo destinatario (por ejemplo, un repositorio de datos) para que éste tenga acceso a los mismos (por ejemplo para almacenarlos). En ese caso, la información referente al dispositivo destinario sería un identificador único del dispositivo destinatario y el dato proporcionado por el dispositivo remitente es el dato (o conjunto de datos) al que el dispositivo remitente quiere que el dispositivo destinatario tenga acceso. Además, si en el paso i) se determina que la verificación es exitosa, el dispositivo intermediario verificador incluiría el dato (o conjunto de datos) en el mensaje enviado al dispositivo destinatario en el paso i).

En una realización, la encriptación en el paso c) para obtener la firma digital compleja se realiza mediante una clave privada del dispositivo remitente y en los pasos e) y h) la firma digital compleja se desencripta (descifra) con una clave pública del dispositivo remitente.

En una realización, la identificación del tercer dispositivo electrónico es un certificado digital del tercer dispositivo electrónico.

Un segundo aspecto de la presente invención se refiere a sistema para la verificación de datos preservando la privacidad que realiza el método anteriormente propuesto. En concreto, el sistema comprende un primer dispositivo electrónico, dispositivo remitente, un segundo dispositivo electrónico, dispositivo destinatario, y un tercer dispositivo electrónico, dispositivo intermediario verificador; donde la comunicación entre el dispositivo remitente y el dispositivo destinatario y de éste con el dispositivo intermediario verificador se realiza a través de una o más redes de comunicación y donde:

El dispositivo remitente está configurado para (tiene medios para):

- enviar al dispositivo destinatario, un mensaje incluyendo una petición de realizar una acción de intercambio de datos con el dispositivo destinatario;
- recibir del dispositivo destinatario una información referente al dispositivo destinario y una identificación del dispositivo intermediario verificador;
- realizar un hash de la información referente al dispositivo destinario un hash de un dato proporcionada por el dispositivo remitente, calcular un segundo hash de ambos hash concatenados y encriptar el resultado, al resultado encriptado se le denomina firma digital compleja;
- enviar un mensaje al dispositivo destinatario que comprende: la información referente al dispositivo destinario recibida, el hash del dato del dispositivo remitente, la firma digital compleja y la siguiente información cifrada con una clave K generada por el dispositivo remitente: el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja y donde el mensaje comprende adicionalmente la clave K cifrada con una clave pública del dispositivo intermediario verificador;

El dispositivo destinatario está configurado para (tiene medios para):

- realizar el hash de la información referente al dispositivo destinario, concatenarlo con el hash del dato del dispositivo remitente recibido y comparar el resultado con el resultado de descifrar la firma digital compleja que ha recibido y, si ambos resultados coinciden enviar al dispositivo intermediario verificador un mensaje que contiene la información cifrada con la clave K recibida del el dispositivo remitente y la clave K cifrada recibida del dispositivo remitente;

y el dispositivo intermediario verificador está configurado para (tiene medios para):

- utilizar su clave privada para descifrar la clave K y utilizar la clave K para descifrar la información recibida, obteniendo el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja;
- realizar el hash del dato del dispositivo remitente recibido y concatenarlo con el hash de la información referente al dispositivo destinario recibido y comparar el resultado con el resultado de descifrar la firma digital compleja que ha recibido;
- determinar, basado al menos en la comparación de ambos resultados, el éxito de la

verificación y si se determina que la verificación es exitosa, enviar un mensaje al dispositivo destinatario indicando que la verificación es exitosa y, por lo tanto, se puede realizar la acción de intercambio de datos requerida por el dispositivo remitente.

En una realización la acción de intercambio de datos es acceder a una página web a través del dispositivo destinatario, el dato proporcionado por el dispositivo remitente es un identificador de un usuario del dispositivo remitente; y el dispositivo intermediario verificador determina que la verificación es exitosa si los resultados coinciden y si, a partir de dicho identificador de usuario, el dispositivo intermediario verificador verifica que el usuario cumple una determinada condición la información del remitente es válida.

En una realización la acción de intercambio de datos es enviar un dato al dispositivo destinatario para que lo almacene, donde la información referente al dispositivo destinario es un identificador único del dispositivo destinatario, donde el dato proporcionado por el dispositivo remitente es un dato que el dispositivo remitente quiere que el dispositivo destinatario almacene y donde, si la verificación es exitosa, el dispositivo intermediario verificador envía un mensaje al dispositivo destinatario incluyendo el dato a almacenar.

Aspectos, realizaciones y detalles adicionales, específicos y preferidos, de la invención se enuncian en las reivindicaciones adjuntas, independientes y dependientes. Para un entendimiento más completo de la invención, sus objetos y ventajas, puede tenerse referencia a la siguiente memoria descriptiva y a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LAS FIGURAS

A continuación, se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

FIGURA 1.- Muestra esquemáticamente un diagrama de flujo de mensajes para otro ejemplo de aplicación, según una realización preferente de la invención, donde se verifica un atributo de un usuario (en este caso la edad).

FIGURA 2.- Muestra esquemáticamente un diagrama de flujo de mensajes para un ejemplo de aplicación, según una realización preferente de la invención, donde se verifica el origen no

fraudulento de un dato.

REALIZACIÓN PREFERENTE DE LA INVENCIÓN

La presente invención describe un método y sistema avanzado para verificar la autenticidad e integridad de datos anonimizados en redes de telecomunicaciones, centrado en la seguridad de la información y la protección de la privacidad del usuario, que permite gestionar datos de forma segura, garantizando anonimato, privacidad y verificación. Mediante el uso de algoritmos criptográficos avanzados y protocolos de procesamiento de datos únicos se asegura la privacidad y anonimato del usuario, validando a la vez la integridad y autenticidad de los datos transmitidos.

En pocas palabras, como se explicará a continuación, la presente invención propone un sistema y método de verificación de datos para preservar la privacidad que comprende generar firmas digitales complejas y verificar la autenticidad e integridad de los datos a través de un dispositivo intermedio (Pulse Gateway) sin revelar la identidad del usuario.

En una realización, el método propuesto por la presente invención realiza los siguientes pasos (esto es un ejemplo genérico y no todos los pasos son imprescindibles, otras realizaciones pueden incluir todos o solo algunos de estos pasos):

El dispositivo electrónico que quiere realizar una acción de intercambio de datos (también llamado dispositivo remitente o simplemente remitente) contacta con el dispositivo electrónico con el que quiere realizar dicha acción (dispositivo electrónico destinatario o simplemente destinatario). Esta acción de intercambio de datos puede ser por ejemplo enviar una cierta información al dispositivo destinatario (por ejemplo, para almacenarla en el mismo) o acceder a información (por ejemplo, a una página web) a través del dispositivo destinatario o cualquier otra.

El destinatario le envía al dispositivo remitente datos que permiten su identificación (por ejemplo una web, una IP, etc.…, en otras palabras le envía un identificador único del destinatario), preferiblemente junto con el certificado digital del dispositivo intermediario (Pulse Gateway) que se va a emplear.

El dispositivo remitente procesa estos datos recibidos del destinatario. En una realización, se

calcula un hash (se aplica una función hash) del identificador del destinatario y el hash de un identificador del remitente (o en un caso más general, de un dato proporcionado por el dispositivo remitente). Este identificador del remitente puede ser del dispositivo electrónico remitente o de un usuario de dicho dispositivo electrónico. Los hashes resultantes se concatenan y se calcula otro hash. La salida de este segundo hash es cifrada con una clave privada del remitente (del dispositivo electrónico remitente o de un usuario de dicho dispositivo electrónico) y al resultado se denominará firma digital compleja. A continuación, el remitente envía un mensaje al destinatario, dicho mensaje incluye: el identificador del destinatario, el hash (el resultado del hash) del identificador del remitente y la firma digital compleja. Además, el mensaje puede contener la siguiente información cifrada (por ejemplo, con una clave de un solo uso): el hash del identificador del destinatario, el identificador del remitente y la firma digital compleja. Esta clave de cifrado se adjunta en el mensaje cifrada con la clave publica del dispositivo intermediario verificador (Pulse Gateway) que se va a emplear.

Cuando el destinatario recibe este mensaje podrá acceder el contenido del mensaje que no está cifrado. Procede a calcular el hash del identificador del destinatario y lo concatena con el hash del identificador del remitente que ha recibido y procede a realizar un segundo hash del resultado concatenado (salida 1). Después, descifra con la clave pública del remitente la firma digital compleja recibida (salida 2). Si salida 1 es igual a salida 2, entonces el mensaje mantiene integridad y autenticación. Entonces, el destinatario prepara el mensaje que será enviado al dispositivo intermediario (llamado Pulse Gateway). Este mensaje contiene toda la información que el destinatario recibió cifrada en el mensaje previo (el hash del identificador del destinatario, el identificador del remitente y la firma digital compleja) y el destinatario envía esta información cifrada tal como la ha recibido (es decir, no la descifra, aunque tampoco podría descifrarla aunque quisiera porque no conoce la clave necesaria). Este mensaje se puede firmar digitalmente con una firma digital clásica. Este elemento intermediario (al que también se puede llamar dispositivo verificador) puede ser cualquier tipo de dispositivo electrónico como por ejemplo un servidor, una pasarela o puerta de enlace (más conocido por su denominación en inglés, “gateway”) o de cualquier otro tipo.

La pasarela recibe el mensaje y procede a procesar su contenido. En primer lugar, descifra la clave de un solo uso con su clave privada. A continuación, descifra el resto del contenido con dicha clave y obtiene el hash del identificador del destinatario, el identificador del remitente y la firma digital compleja. Calcula el hash del identificador del remitente. Lo concatena con el hash del identificador del destinatario (salida 3). A continuación, descifra la firma digital

compleja (salida 4). Si salida 3 y salida 4 son iguales, se garantiza integridad y autenticación, enviando un mensaje de éxito al destinatario para que proceda a realizar la acción solicitada (almacenamiento de dato, verificación de dato exitosa, acceso a contenido…). De lo contrario se envía un mensaje de fallo. El mensaje de éxito o de fallo se comunica al remitente.

La comunicación entre dispositivo remitente y destinatario y de estos con el dispositivo intermediario (la pasarela) se realizarán a través de una o más redes de comunicación, cableadas o inalámbricas, que pueden ser de cualquier tipo (red de telefonía móvil 2G, 3G, 4G, 5G, red de área local, red de fibra óptica o cualquier otra inalámbrica o por cable).

Hay muchos casos de uso posibles de este mecanismo. Por ejemplo, se puede utilizar para verificar que una característica/condición/atributo asociado a un origen legal es cierta (figura 1) o, también, se puede emplear para verificar que un dato procede de un origen legal, no fraudulento (figura 2). Esto son solo dos ejemplos no limitativos En todos los casos proporcionando anonimato, integridad y autenticación del origen. Es importante notar que la modularidad del diseño permite incluir niveles adicionales de confidencialidad según se requieran.

Las figuras 1 y 2 muestran esquemáticamente el intercambio de mensajes (junto con el contenido de los mensajes y cálculos necesarios para su creación) para distintos casos de uso.

Se proporciona a continuación un ejemplo del caso de uso en el que se verifica que una determinada una condición (o característica o atributo del usuario) se cumple antes de prestar un determinado servicio u ofrecer cierta información a un usuario. Para facilitar la explicación, se hará sobre un ejemplo concreto (expuesto en la figura 1) en el que se verifica que un internauta que quiere acceder a una determinada página web, cumple ciertos requisitos (como la mayoría de edad, para el acceso a páginas o contenidos web de adultos), al mismo tiempo que se garantiza el anonimato del internauta y se proporciona autenticación e integridad de los mensajes intercambiados (esto es solo un ejemplo no limitativo y en otras realizaciones se pueden incluir solo alguno de los pasos que se explican a continuación):

Paso 1 (101). El usuario solicita acceso a la página web cuyo contenido es para adultos. Esto lo hace a través de su dispositivo electrónico (11) que puede ser un móvil, una tableta, un ordenador personal o cualquier otro. Solicitar el acceso se interpreta como escribir la URL (en

el caso de la figura 3, sería www.xxx.yyy) en el navegador de modo que el cliente web, desde el que el usuario está haciendo uso del servicio, contacta con el servidor web (12) de dicha página de forma normal. En este caso de uso, usando la nomenclatura que se ha empleado anteriormente, el dispositivo remitente sería el dispositivo electrónico del usuario y el dispositivo destinatario sería el servidor web.

Paso 2 (102). El servidor web responde enviando en el mensaje de respuesta el certificado digital ($CERT_{GW}$) de un dispositivo intermediario (13) que se va a usar para la verificación (el llamado Pulse Gateway) y la URL de la página web (WEB_{URL}) a la que el usuario quiere acceder. Hay que tener en cuenta que el usuario ya conoce esta URL pero se hace esto para que el navegador web del cliente disponga directamente de esta información sin necesidad de interactuar con el usuario. En este mensaje se puede incluir información de que para acceder a esta página web es necesario verificar un atributo del usuario (en este caso la edad).

Paso 3 (103). El dispositivo del usuario (por ejemplo, el navegador web) calcula una firma digital compleja. Para ello, se calcula obteniendo el hash de la URL de la web ($H(WEB_{URL})$) y el hash de un identificador ID del usuario que quiere acceder a esa página web (H(ID)); a continuación, ambos hashes se utilizan como entrada para otra función hash (que se puede llamar doble hash) y la salida se cifra con la clave privada del usuario. Así se obtendrá la firma digital compleja. La identificación del usuario debe entenderse como un dato identificativo del usuario que garantiza su edad y que sólo conocerá el dispositivo intermediario (el Pulse Gateway). Es decir, ese identificador del usuario será desconocido para el servidor web y será computacionalmente intratable para el servidor web obtener esta información. Ese identificador de usuario podría estar asociado a un certificado digital del usuario, que en España sólo se puede obtener cuando se alcanza la mayoría de edad, o a una clave de acceso en caso de que exista un registro previo como usuario en la página web, por ejemplo, utilizando FIDO, entre otras opciones. Así se trata de una propuesta modular, y el objetivo es que la información que garantiza la edad del usuario será conocida y evaluada única y exclusivamente por el Pulse Gateway, siendo totalmente desconocida por el servidor web (con lo que se asegura el anonimato del usuario).

Paso 4 (104). El dispositivo del usuario (por ejemplo, el navegador web) envía un mensaje al servidor web que incluye: la URL de la web, el hash del identificador del usuario y la firma digital compleja. Este mensaje también incluye, cifrado con una clave K generada aleatoriamente por el dispositivo de usuario, el hash de la URL de la web, el identificador del

usuario y la firma digital compleja, y, cifrado con la clave pública K_{GW} de la pasarela (el Pulse Gateway), la clave K.

Paso 5 (105). Cuando el servidor web recibe este mensaje, calcula el hash de la URL de la web, lo concatena con el hash del identificador del usuario que ha recibido y, a continuación, calcula el hash doble. Por otro lado, descifra la firma compleja que ha recibido (con la clave pública del usuario). Si ambas salidas son iguales entonces se verifica la integridad (ningún dato de este mensaje ha sido manipulado). Si no, se puede informar al dispositivo de usuario que la verificación ha fallado.

Paso 6 (106). A continuación, si la integridad se ha verificado en el paso anterior, el servidor web reenvía al Pulse Gateway la información cifrada que ha recibido previamente, es decir, el hash de la URL de la web, el identificador del usuario y la firma compleja, todo ello recordemos cifrado con la clave K, y la clave K cifrada con la clave pública de la pasarela K_{GW}. El servidor web puede incluir un número de solicitud (#REQ) para la correspondencia solicitud-respuesta y firmar digitalmente este mensaje con una firma digital tradicional.

Paso 7 (107). Cuando el Pulse Gateway recibe este mensaje, utilizando su clave privada, el Pulse Gateway descifra K. A continuación, utilizando K, descifra (desencripta) la información cifrada que ha recibido, obteniendo el hash de la URL de la web ($H(WEB_{URL})$), el identificador del usuario (ID) y la firma digital compleja. El Pulse Gateway no tiene información sobre la página web a la que quiere acceder el usuario, sólo tiene su hash.

Paso 8 (108). El Pulse Gateway calcula el hash del identificador del usuario, lo concatena con el hash de la web que ha obtenido del mensaje recibido. A continuación, calcula el doble hash y, por otro lado, descifra (por ejemplo, con la clave pública del remitente) la firma digital compleja que ha obtenido en el paso anterior. De nuevo, si ambas salidas coinciden, la integridad está garantizada. De esta manera se puede vincular la característica/condición que se quiere verificar con su origen (el usuario) pero ofreciendo características de seguridad deseables, como puede ser el caso de la privacidad y la integridad.

En caso de que ambas salidas coincidan, a partir del ID del usuario el Pulse Gateway comprueba si el usuario cumple la condición necesaria para el acceso a la página web (en este caso si es mayor de edad). Dependiendo del tipo de ID de usuario que se utilice esta comprobación es automática ya que el usuario solo puede tener ese identificador si cumple

con el criterio (por ejemplo, puede ser un certificado digital del usuario, que en España sólo se puede obtener cuando se alcanza la mayoría de edad). De esta manera, el usuario demuestra que cumple con el criterio sin revelar a la pasarela el sitio web en que quiere entrar (o la información a la que quiere acceder si se tratara de otro ejemplo de caso de uso en el que el usuario quiere acceder a cierta información) y sin que el servidor web tenga que conocer la identidad del usuario.

Paso 9 (109). En caso de éxito en el proceso de verificación, se envía un mensaje de éxito al servidor web. En caso contrario se envía un mensaje de fallo indicando que el usuario no cumple el requisito (de edad). En estos mensajes se puede incluir el número de solicitud (#REQ) que le envió el servidor web en el mensaje anterior (para identificar a qué solicitud se está respondiendo) y también se puede firmar digitalmente este mensaje con una firma digital tradicional. En una realización alternativa, si la verificación es fallida, no se envía mensaje al servidor web y éste, si en un determinado periodo de tiempo no ha recibido un mensaje del Gateway, entenderá que la verificación ha sido negativa.

Paso 10 (110). El servidor web se comunica con el usuario, proporcionándole acceso al sitio web (en caso de éxito) o informándole de que se le deniega el acceso (en caso de fallo).

Se proporciona a continuación un ejemplo del caso de uso en el que se verifica el origen de un dato (que no es fraudulento) que un dispositivo (remitente) quiere que sea accesible por otro dispositivo (destinatario). La solución propuesta asegura que hay una vinculación entre el dato con su origen (el dispositivo remitente), con lo cual el dato no viene de un origen fraudulento, asegurando al mismo tiempo la integridad del dato. Para facilitar la explicación, se hará sobre un ejemplo concreto (expuesto en la figura 2) en el que se verifica que un dato (que un usuario quiere almacenar en un repositorio), no es fraudulento (que está ligado al remitente que lo envía), al mismo tiempo que se garantiza el anonimato de la fuente y se proporciona autenticación e integridad de los mensajes intercambiados (esto es solo un ejemplo no limitativo y en otras realizaciones se pueden incluir solo alguno de los pasos que se explican a continuación):

Paso 1 (201). El usuario quiere enviar un dato (o conjunto de datos) a un dispositivo destinatario, para que tenga acceso al mismo, por ejemplo, para almacenarlo en un repositorio de datos (22). Esto lo hace a través de su dispositivo electrónico (21) que puede ser un móvil, una tableta, un ordenador personal, un módulo de comunicación de un vehículo o cualquier

otro dispositivo electrónico y que, en el ejemplo de la figura 1 se encuentra en un vehículo. En este caso de uso, usando la nomenclatura que se ha empleado anteriormente, el dispositivo remitente sería el dispositivo electrónico del usuario y el dispositivo destinatario sería el repositorio de datos.

Paso 2 (202). El repositorio responde enviando en el mensaje de respuesta el certificado digital ($CERT_{GW}$) de un dispositivo intermediario (23) que se va a usar para la verificación (el llamado Pulse Gateway) y el identificador del repositorio (ID_{REPO}). En este mensaje se puede informar al usuario incluir información de que para almacenar el dato es necesario validarlo. Esto se hará con anonimidad parcial o total de la fuente del dato: será parcial si se emplean certificados digitales (clave pública/clave privada) para la encriptación da la firma digital (ya que en ese caso el repositorio deberá conocer la identidad del que le envía el dato (remitente) para desencriptar la firma digital o total si se emplean otros sistemas de encriptación/autenticación como FIDO para obtener la firma digital compleja.

Paso 3 (203). El dispositivo del usuario calcula una firma digital (a la que se le denomina aquí firma digital compleja). Para ello, se calcula obteniendo el hash del identificador del repositorio ($H(ID_{REPO})$) y el hash del dato que se quiere almacenar (H(dato)); a continuación, ambos hashes se utilizan como entrada para otra función hash (que se puede llamar doble hash) y la salida se cifra con la clave privada del usuario (o usando un sistema de autenticación FIDO). Así se obtendrá la firma digital compleja.

Paso 4 (204). El dispositivo del usuario envía un mensaje al repositorio de datos: el identificador del repositorio, el hash del identificador del dato y la firma digital compleja. Este mensaje también incluye, cifrado con una clave K generada aleatoriamente por el dispositivo de usuario, el hash del identificador del repositorio, el dato y la firma digital compleja, y, cifrado con la clave pública K_{GW} de la pasarela (el Pulse Gateway), la clave K.

Paso 5 (205). Cuando el repositorio recibe este mensaje, calcula el hash del identificador del repositorio, lo concatena con el hash del dato y, a continuación, calcula el hash doble. Por otro lado, descifra la firma compleja que ha recibido. Si ambas salidas son iguales entonces se verifica la integridad (ningún dato de este mensaje ha sido manipulado).

Paso 6 (206). A continuación, si la integridad se ha verificado en el paso anterior, el repositorio reenvía al Pulse Gateway la información cifrada que ha recibido previamente, es decir, el hash

del identificador del repositorio, el dato y la firma digital compleja todo ello recordemos cifrado con la clave K, y la clave K cifrada con la clave pública de la pasarela K_{GW}. El repositorio puede firmar digitalmente este mensaje con una firma digital tradicional.

Paso 7 (207). Cuando el Pulse Gateway recibe este mensaje, utilizando su clave privada, el Pulse Gateway descifra K. A continuación, utilizando K, descifra (desencripta) la información cifrada que ha recibido, obteniendo el hash del identificador del repositorio, el dato y la firma digital compleja.

Paso 8 (208). El Pulse Gateway calcula el hash del dato, lo concatena con el hash del identificador del repositorio que ha obtenido del mensaje recibido. A continuación, calcula el doble hash y, por otro lado, descifra la firma digital compleja que ha obtenido en el paso anterior (por ejemplo, con la clave pública del remitente. De nuevo, si ambas salidas coinciden, la integridad está garantizada. De esta manera, la solución propuesta asegura que hay una vinculación entre el dato que se quiere almacenar con su origen (el dispositivo remitente), con lo cual el dato no viene de un origen fraudulento, asegurando al mismo tiempo la integridad del dato.

De manera adicional, en una realización el Pulse Gateway puede comprobar si el dato es válido y/o que no ha sido manipulado (por ejemplo, consultando una base de datos o comprobando que el formato de dato es el correcto).

Paso 9 (209). En caso de éxito en el proceso de verificación, se envía un mensaje de éxito al repositorio. En caso contrario se envía un mensaje de fallo indicando que el dato no es válido y que por lo tanto no lo debe almacenar. En este mensaje se puede incluir el dato (en el caso de verificación exitosa) para que lo almacene el repositorio (porque hasta ahora, el repositiorio no había tenido acceso al dato sin encriptar); el mensaje (de éxito o error) también se puede firmar digitalmente este mensaje con una firma digital tradicional.

Paso 10 (210). El repositorio se comunica con el (dispositivo de) usuario, indicando que el dato ha sido verificado y almacenado (en caso de éxito) o informándole de que se el dato no ha sido verificado y, por lo tanto, no se ha almacenado (en caso de fallo).

En una realización alternativa, los papeles del repositorio de datos y del Pulse Gateway se puede intercambiar. Es decir, las acciones y pasos que se han explicado anteriormente como

realizados por el repositorio los hará el Pulse Gateway (excepto el almacenamiento del dato que sigue siendo labor del repositorio) y viceversa. De esta manera, el repositorio almacena y verifica el dato sin conocer de ningún modo el dispositivo remitente del dato ya que no tiene contacto alguno con él.

Resumiendo, se describe un método y sistema avanzado para verificar la autenticidad e integridad de datos en redes de telecomunicaciones preservando el anonimato del usuario remitente, centrado en la seguridad de la información y la protección de la privacidad del usuario. Esta innovación técnica se ubica en el sector de las telecomunicaciones y ciencias de la computación, proponiendo una solución novedosa para gestionar datos de forma segura, garantizando anonimato, privacidad y verificación. Mediante el uso de algoritmos criptográficos avanzados y protocolos de procesamiento de datos únicos, el sistema asegura la privacidad y anonimato del usuario, mientras valida la integridad y autenticidad de los datos transmitidos. Esta invención ofrece una mejora significativa en la protección de la información personal y la gestión de datos en una variedad de sectores críticos, destacando por su simplicidad operativa y robustez frente a métodos existentes.

La solución propuesta en la presente invención es extremadamente sencilla, aunque eficiente. Y puede aplicarse en una amplia gama de escenarios como puede ser IoT (Internet de las cosas), sanidad, ciudades inteligentes, fabricación, automoción, acceso a páginas web (como se ilustra en el ejemplo que se ha expuesto) y, en general cualquier aplicación que requiera una transmisión segura de datos, preservando el anonimato del usuario. En otras palabras, la solución propuesta puede aplicarse en cualquier situación en la que sea necesario verificar información, pero garantizando el anonimato (privacidad) del origen (la información o los datos no deben poder asociarse con su creador) y, al mismo tiempo, garantizando que esa información es fiable y procede de una fuente autenticada. Además de su compatibilidad con elementos/dispositivos software y hardware, el enfoque propuesto difiere en eficiencia, aplicabilidad universal y sobre todo simplicidad de otras propuestas en la literatura científica (como las basadas en Differential Privacy, cifrado homomórfico, técnnicas de anonimización de datos o Federated Learning, por ejemplo), sumado al hecho de que no todas ellas son capaces de combinar ambas características de privacidad y autenticación y que el procedimiento propuesto compatible con ellas. Por ejemplo, implementando el procedimiento presentado es tecnológicamente factible (como se ha ilustrado) crear una solución que dé cabida a las pretensiones de los proveedores de contenidos de acceso restringido (por ejemplo, contenido para adultos) y a las libertades de los ciudadanos, garantizando su

anonimato y privacidad, a la vez que protege a los usuarios no autorizados (por ejemplo, protege a los menores de los peligros de acceder a servicios y aplicaciones inadecuados para su edad, en el caso de contenido para adultos).

Obsérvese que en este texto, términos relacionales como primero y segundo, superior e inferior y similares, pueden ser usados únicamente para distinguir una entidad o acción de otra, sin necesariamente requerir o implicar realmente esa relación u orden entre dichas entidades o acciones. Además, el término “comprende” y sus derivaciones (tales como “comprendiendo”, etc.) no deberían ser entendidos en un sentido de exclusión, es decir, estos términos no deberían ser interpretados como excluyentes de la posibilidad de que lo que se describe y define pueda incluir elementos, etapas, etc., adicionales.

Algunas realizaciones preferidas de la invención se describen en las reivindicaciones dependientes que se incluyen seguidamente.

Descrita suficientemente la naturaleza de la invención, así como la manera de realizarse en la práctica, hay que hacer constar la posibilidad de que sus diferentes partes podrán fabricarse en variedad de materiales, tamaños y formas, pudiendo igualmente introducirse en su constitución o procedimiento, aquellas variaciones que la práctica aconseje, siempre y cuando las mismas, no alteren el principio fundamental de la presente invención. La descripción y los dibujos simplemente ilustran los principios de la invención. Por lo tanto, debe apreciarse que los expertos en la técnica podrán concebir varias disposiciones que, aunque no se hayan descrito o mostrado explícitamente en este documento, representan los principios de la invención y están incluidas dentro de su alcance. Además, todos los ejemplos descritos deben considerarse como no limitativos con respecto a tales ejemplos y condiciones descritos de manera específica. Además, todo lo expuesto en este documento relacionado con los principios, aspectos y realizaciones de la invención, así como los ejemplos específicos de los mismos, abarcan equivalencias de los mismos.

REIVINDICACIONES

1. Un método para la verificación de datos preservando la privacidad, que comprende los siguientes pasos:

a) un primer dispositivo electrónico, dispositivo remitente, envía a un segundo dispositivo electrónico, dispositivo destinatario, un mensaje incluyendo una petición de realizar una acción de intercambio de datos con el dispositivo destinatario;

b) el dispositivo destinatario envía al remitente una información referente al dispositivo destinario y una identificación de un tercer dispositivo electrónico, dispositivo intermediario verificador;

c) el dispositivo remitente realiza un hash de la información referente al dispositivo destinario un hash de un dato proporcionado por el dispositivo remitente, calcula un segundo hash de ambos hash concatenados y encripta el resultado, el resultado encriptado se le denomina firma digital compleja;

d) el dispositivo remitente envía un mensaje al dispositivo destinatario que comprende: la información referente al dispositivo destinario, el hash del dato del dispositivo remitente, la firma digital compleja y la siguiente información cifrada con una clave K generada por el dispositivo remitente: el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja y donde el mensaje comprende adicionalmente la clave K cifrada con una clave pública del dispositivo intermediario verificador;

e) el dispositivo destinatario realiza el hash de la información referente al dispositivo destinario y lo concatena con el hash del dato del dispositivo remitente recibido hash y el resultado lo compara con el resultado de desencriptar la firma digital compleja que ha recibido; si ambos resultados coinciden ir al paso f) y si no coinciden, se termina el método;

f) el dispositivo destinatario envía al dispositivo intermediario verificador un mensaje que contiene la información cifrada con la clave K recibida del el dispositivo remitente y la clave K cifrada recibida del dispositivo remitente;

g) el dispositivo intermediario verificador utilizando su clave privada descifra la clave K y utilizando la clave K descifra la información recibida, obteniendo el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja;

h) el dispositivo intermediario verificador realiza el hash del dato del dispositivo remitente recibido y lo concatena con el hash de la información referente al dispositivo destinario recibido y el resultado lo compara con el resultado de desencriptar la firma digital compleja que ha recibido;

i) el dispositivo intermediario verificador determina, basado al menos en la comparación de ambos resultados, el éxito de la verificación y si se determina que la verificación es exitosa, se envía un mensaje al dispositivo destinatario indicando que la verificación es exitosa y, por lo tanto, se puede realizar la acción de intercambio de datos requerida por el dispositivo remitente;

donde la comunicación entre el dispositivo remitente y el dispositivo destinatario y de éste con el dispositivo intermediario verificador se realiza a través de una o más redes de comunicación.

2. Método según la reivindicación 1, donde la acción de intercambio de datos es acceder a información a través del dispositivo destinatario y donde el dato proporcionado por el dispositivo remitente es un identificador de un usuario del dispositivo remitente.

3. Método según la reivindicación 2 donde en el paso i), el dispositivo intermediario verificador determina que la verificación es exitosa si los resultados coinciden y si, a partir de dicho identificador de usuario, el dispositivo intermediario verificador verifica que el usuario cumple una determinada condición la información del remitente es válida.

4. Método según cualquiera de las reivindicaciones 2 ó 3, donde la acción de intercambio de datos es acceder a una página web a través del dispositivo destinatario y la información referente al dispositivo destinario es la identificación de una página web a la que el usuario quiere acceder.

5. Método según cualquiera de las reivindicaciones 2-4, donde el dispositivo destinatario es un servidor web.

6. Método según la reivindicación 1, donde la acción de intercambio de datos es proporcionar un dato al dispositivo destinatario para que éste tenga acceso al mismo, donde la información referente al dispositivo destinario es un identificador único del dispositivo destinatario, donde el dato proporcionado por el dispositivo remitente es el dato al que el dispositivo remitente quiere que el dispositivo destinatario tenga acceso y donde, si en el paso i) se determina que la verificación es exitosa, el dispositivo intermediario verificador incluye el dato en el mensaje enviado al dispositivo destinatario en el paso i).

7. Método según la reivindicación 6, donde el dispositivo destinatario es un repositorio y donde

dicho repositorio almacena el dato si en el paso i) se determina que la verificación es exitosa.

8. Método según cualquiera de las reivindicaciones anteriores donde la encriptación en el paso c) se realiza mediante una clave privada del dispositivo remitente y en los pasos e) y h) se desencripta con una clave pública del dispositivo remitente.

9. Método según cualquiera de las reivindicaciones anteriores donde el dispositivo intermediario verificador es un dispositivo de puerta de enlace o pasarela, Gateway.

10. Método según cualquiera de las reivindicaciones anteriores donde las una o más redes de comunicación son redes inalámbricas.

11. Método según la reivindicación 10 donde las una o más redes de comunicación son redes de al menos uno de los siguientes tipos: red de telefonía móvil 2G, 3G, 4G, 5G, red de área local, red de fibra óptica.

12. Método según cualquiera de las reivindicaciones anteriores donde la identificación del tercer dispositivo electrónico es un certificado digital del tercer dispositivo electrónico.

13. Un sistema para la verificación de datos preservando la privacidad, donde el sistema comprende un primer dispositivo electrónico, dispositivo remitente, un segundo dispositivo electrónico, dispositivo destinatario, y un tercer dispositivo electrónico, dispositivo intermediario verificador; donde la comunicación entre el dispositivo remitente y el dispositivo destinatario y de éste con el dispositivo intermediario verificador se realiza a través de una o más redes de comunicación y donde:

El dispositivo remitente está configurado para:

- enviar al dispositivo destinatario, un mensaje incluyendo una petición de realizar una acción de intercambio de datos con el dispositivo destinatario;
- recibir del dispositivo destinatario una información referente al dispositivo destinario y una identificación del dispositivo intermediario verificador;
- realizar un hash de la información referente al dispositivo destinario un hash de un dato proporcionada por el dispositivo remitente, calcular un segundo hash de ambos hash concatenados y encriptar el resultado, al resultado encriptado se le denomina firma digital compleja;

- enviar un mensaje al dispositivo destinatario que comprende: la información referente al dispositivo destinario recibida, el hash del dato del dispositivo remitente, la firma digital compleja y la siguiente información cifrada con una clave K generada por el dispositivo remitente: el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja y donde el mensaje comprende adicionalmente la clave K cifrada con una clave pública del dispositivo intermediario verificador;

El dispositivo destinatario está configurado para:

- realizar el hash de la información referente al dispositivo destinario, concatenarlo con el hash del dato del dispositivo remitente recibido y comparar el resultado con el resultado de descifrar la firma digital compleja que ha recibido y, si ambos resultados coinciden enviar al dispositivo intermediario verificador un mensaje que contiene la información cifrada con la clave K recibida del el dispositivo remitente y la clave K cifrada recibida del dispositivo remitente;

y el dispositivo intermediario verificador está configurado para:

- utilizar su clave privada para descifrar la clave K y utilizar la clave K para descifrar la información recibida, obteniendo el hash de la información referente al dispositivo destinario, el dato del dispositivo remitente y la firma digital compleja;
- realizar el hash del dato del dispositivo remitente recibido y concatenarlo con el hash de la información referente al dispositivo destinario recibido y comparar el resultado con el resultado de descifrar la firma digital compleja que ha recibido;
- determinar, basado al menos en la comparación de ambos resultados, el éxito de la verificación y si se determina que la verificación es exitosa, enviar un mensaje al dispositivo destinatario indicando que la verificación es exitosa y, por lo tanto, se puede realizar la acción de intercambio de datos requerida por el dispositivo remitente.

14. Sistema según la reivindicación 13, donde la acción de intercambio de datos es acceder a una página web a través del dispositivo destinatario y donde el dato proporcionado por el dispositivo remitente es un identificador de un usuario del dispositivo remitente; y donde el dispositivo intermediario verificador determina que la verificación es exitosa si los resultados coinciden y si, a partir de dicho identificador de usuario, el dispositivo intermediario verificador

verifica que el usuario cumple una determinada condición la información del remitente es válida.

15. Sistema según la reivindicación 13, donde la acción de intercambio de datos es enviar un dato al dispositivo destinatario para que lo almacene, donde la información referente al dispositivo destinario es un identificador único del dispositivo destinatario, donde el dato proporcionado por el dispositivo remitente es un dato que el dispositivo remitente quiere que el dispositivo destinatario almacene y donde, si la verificación es exitosa, el dispositivo intermediario verificador envía un mensaje al dispositivo destinatario incluyendo el dato a almacenar.

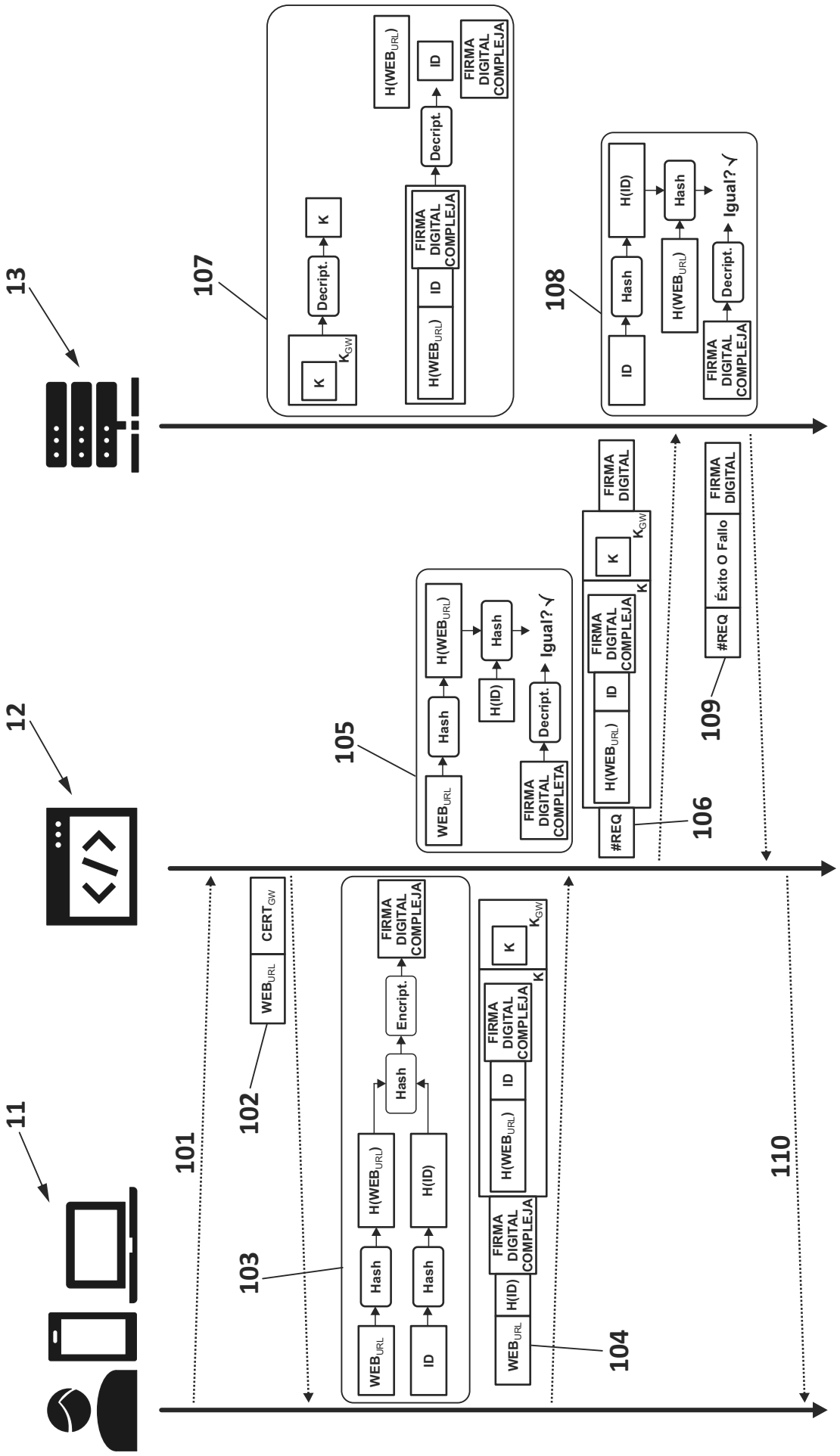
11
12
13
101
102
103
104
105
106
107
108
109
110
WEB_URL
CERT_GW
Hash
H(WEB_URL)
H(ID)
ID
Encript.
FIRMA DIGITAL COMPLEJA
K
K_GW
Decript.
FIRMA DIGITAL COMPLETA
Igual?
#REQ
Éxito O Fallo
FIRMA DIGITAL

FIG. 1

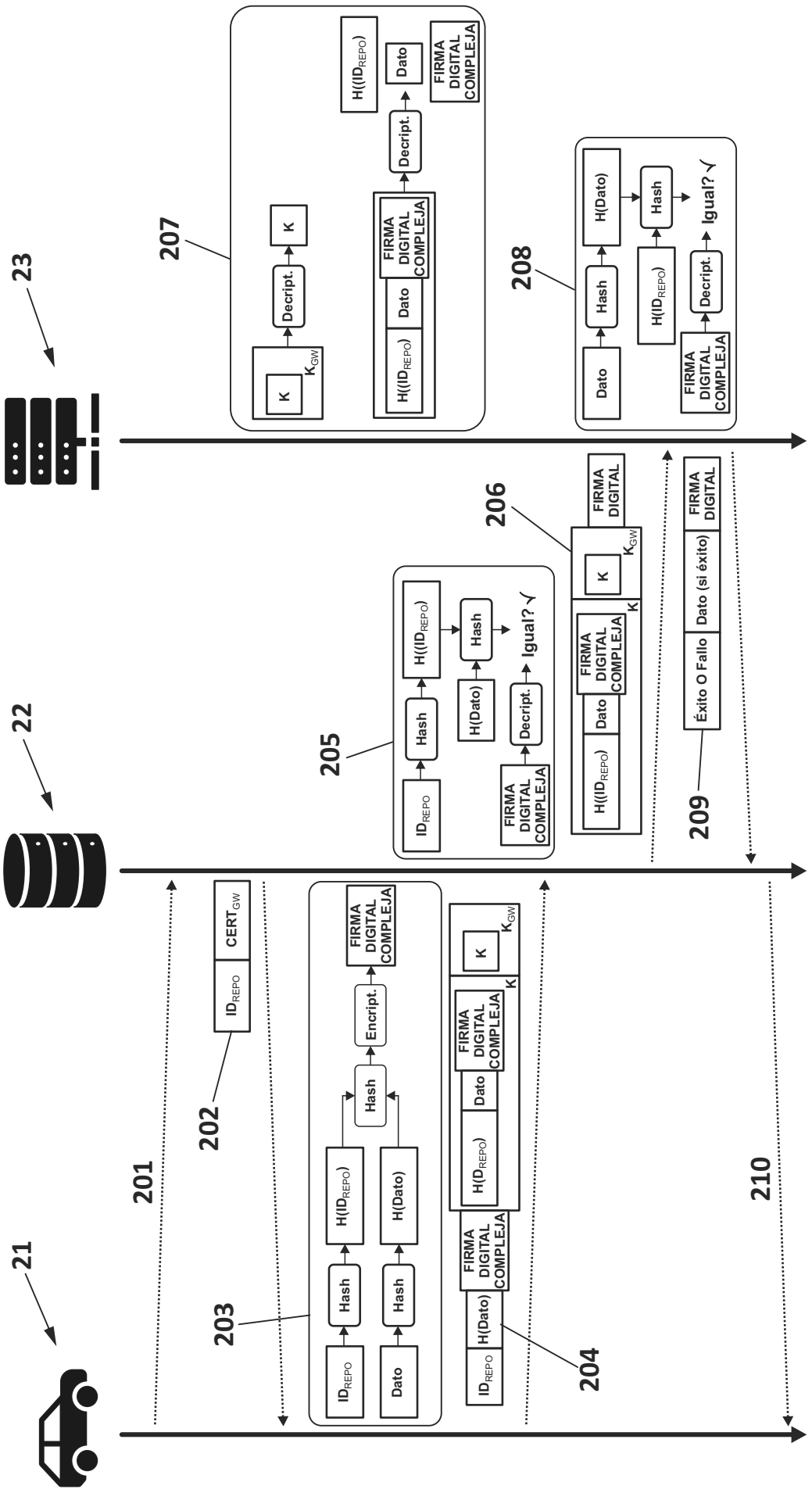
21
22
23
201
202
203
204
205
206
207
208
209
210
ID_REPO
CERT_GW
Hash
H(ID_REPO)
H(Dato)
Dato
Encript.
FIRMA DIGITAL COMPLEJA
K
K_GW
Decript.
Igual?
Éxito O Fallo
Dato (si éxito)
FIRMA DIGITAL

FIG. 2

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 202430557

(22) Fecha de presentación de la solicitud: 03.07.2024

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) Int. CI.: ***G06F21/00*** (2013.01)
G06Q20/00 (2012.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	WO 2013045716 A1 (DIVERSID CONSULTORIA S L et al.) 04/04/2013, reivindicaciones y figura 1.	1-15
A	ES 2859569T T3 (ADVANCED NEW TECHNOLOGIES CO LTD) 04/10/2021, Reivindicaciones y figuras.	1-15
A	ES 2755763T T3 (HUAWEI TECH CO LTD) 23/04/2020, Reivindicaciones.	1-15
A	ES 2456815T T3 (TELECOM ITALIA SPA) 23/04/2014, Reivindicaciones y figuras.	1-15
A	ES 2880458T T3 (ADVANCED NEW TECHNOLOGIES CO LTD) 24/11/2021, Reivindicaciones.	1-15

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
09.10.2024	G. Foncillas Garrido	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, G06Q

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC