(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 906 343**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.04.2018 E 18166847 (6)**

(97) Fecha y número de publicación de la concesión europea: **24.11.2021 EP 3554001**

(54) Título: **Método de transmisión segura y método de intercambio bidireccional seguro de paquetes de datos electrónicos en una red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.04.2022

(73) Titular/es:

UBIRCH GMBH (100.0%)
Im Mediapark 5
50670 Köln, DE

(72) Inventor/es:

MERZ, MICHAEL y
JUGEL, MATTHIAS

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Método de transmisión segura y método de intercambio bidireccional seguro de paquetes de datos electrónicos en una red

La invención se refiere a un método para la transmisión segura de paquetes de datos electrónicos en una red y a un método para el intercambio bidireccional seguro de paquetes de datos electrónicos en una red.

Antecedentes

Para asegurar la transmisión de paquetes de datos electrónicos entre componentes de red, cada uno de los cuales tiene uno o más procesadores y opcionalmente un medio de almacenamiento asignado para datos electrónicos, en una red, se conoce el uso de protocolos de transmisión de datos encriptados. Además, puede proporcionarse una autenticación de los componentes de red involucrados en la transmisión de datos por medio de certificados. Esto garantiza que la transmisión de datos desde el componente de red de envío al componente de red de recepción sea confiable y segura. La transmisión de datos adicional de los paquetes de datos electrónicos recibidos por parte del componente de red receptor a otro componente de red puede tener lugar entonces de la misma manera.

También se conoce el uso de claves criptográficas para la transmisión de paquetes de datos. Por ejemplo, se proporcionan pares de claves criptográficas, cada uno de los cuales comprenden una clave pública y una privada, para componentes de red. Esto permite la autenticación de paquetes de datos electrónicos intercambiados entre componentes de la red. Normalmente, el paquete de datos electrónicos a transmitir se firma digitalmente en el componente de red de envío mediante el uso de la clave privada del componente de red de envío. A continuación, el paquete de datos electrónicos no cifrados y la firma digital se transmiten al componente de red receptor. El componente de red receptor recibe previamente la clave pública del componente de red emisor y puede utilizarla para verificar el paquete de datos electrónicos (firmados digitalmente). La verificación, que se conoce como tal, utiliza la clave pública para verificar si la firma digital recibida se origina en el remitente (componente de red de envío) del paquete de datos y coincide con el paquete de datos recibido.

El estado de la técnica solo puede establecer confiabilidad transitiva para la transmisión de datos, en la que todos los componentes de red involucrados deben confiar entre sí, desde el componente de red de envío hasta el componente de red de recepción final. Además, la manipulación en los componentes intermedios de la red de procesamiento y transporte de datos es posible y no puede detectarse por el receptor sin una verificación completa de toda la ruta de transmisión. Se excluye una transferencia confiable de datos a través de rutas no cifradas.

Una gran debilidad de los métodos conocidos (cifrado en tránsito) es que los datos deben descifrarse para su procesamiento/análisis en el componente de red receptor. Después del descifrado, quedan prácticamente desprotegidos, lo que es particularmente grave porque basta con piratear un servidor para comprometer la confiabilidad de todas las etapas/sistemas de procesamiento posteriores.

El documento US 2003/0182552 A1 divulga un método para manejar una firma digital para el intercambio de datos entre componentes de red.

El documento DE 10 2015 202 935 A1 se refiere a un método y un aparato para la protección contra manipulaciones, que comprende el método: firmar un enlace de un primer valor hash con el primer parámetro variable en el tiempo y una identificación del segundo dispositivo por medio de una clave privada, asociado con el segundo dispositivo, de un proceso de cifrado asimétrico, en el que las instrucciones del programa o los datos almacenados en el segundo dispositivo y destinados a la ejecución en funcionamiento del segundo dispositivo se utilizan para determinar el valor hash; generar un segundo paquete de datos que comprende la firma y el enlace; enviar el segundo paquete de datos desde el segundo dispositivo al primer dispositivo.

El documento US 2013/0166 917 A1 se refiere a un método para verificar el registro de un usuario para un evento.

El documento DE 102 34 815 A1 se refiere a un método para firmar digitalmente información digital. Aquí, la información se almacena en un primer conjunto de datos y se genera una primera firma al firmar digitalmente este conjunto de datos. En un segundo conjunto de datos, se proporciona información sobre la primera firma y/o una segunda firma aún por generar. La información de este conjunto de datos se combina con la del primer conjunto de datos y/o la primera firma y la segunda firma se genera al firmar digitalmente la combinación de datos así obtenida. Se genera un sello digital mediante el uso del método.

El documento US 2004/006692 A1 se refiere al uso de las denominadas listas de bloqueo de firmas en cadena para asegurar la validez de un original.

Resumen

El problema que aborda la invención es el de proporcionar métodos mejorados para la transmisión segura y el intercambio de paquetes de datos electrónicos entre componentes de red de una red que se configura para enviar y recibir paquetes de datos electrónicos por medio de componentes de red.

Para solucionar esto, se proporciona un método para la transmisión segura de paquetes de datos de acuerdo con la reivindicación independiente 1. Además, se proporciona un método para el intercambio bidireccional seguro de paquetes de datos electrónicos en una red de acuerdo con la reivindicación independiente 4. Las reivindicaciones dependientes se refieren a las modalidades.

En las tecnologías propuestas, en el caso de la transmisión sucesiva de paquetes de datos, se proporciona en particular incluir la firma digital para un paquete de datos electrónicos transmitido en una transmisión posterior de otro paquete de datos electrónicos. Los métodos propuestos aseguran la transmisión de los paquetes de datos electrónicos contra la manipulación.

En el método para la transmisión segura de paquetes de datos electrónicos, también puede proporcionarse lo siguiente en el primer componente de red en el contexto de una n-ésima (n>2) operación de procesamiento de datos: proporcionar una n-ésima carga útil que es al menos diferente de las primera y segunda cargas útiles; crear un n-ésimo paquete de datos electrónicos que comprende el primer ID de componente, la n-ésima carga útil y una (n-1)ésima firma digital que se creó mediante el uso de la primera clave privada para un (n-1)ésimo paquete de datos con una (n-1)ésima carga útil, el primer ID de componente y una (n-2)ésima firma digital; crear una n-ésima firma digital, en el que el n-ésimo paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada; y enviar el n-ésimo paquete de datos electrónicos y la n-ésima firma digital desde el primer componente de red al segundo componente de red. En el segundo componente de red, el n-ésimo paquete de datos electrónicos y la n-ésima firma digital se reciben y guardan en el dispositivo de almacenamiento.

En el método, también puede proporcionarse lo siguiente en el segundo componente de red: verificar el primer paquete de datos electrónicos por medio de la primera clave pública; verificar el segundo paquete de datos electrónicos por medio de la primera clave pública. Además, pueden analizarse el primer y el segundo paquete de datos electrónicos verificados, en el que se ejecuta aquí al menos una de las siguientes tareas de verificación: verificar si el primer y el segundo paquete de datos electrónicos se recibieron del mismo componente de red, es decir, la primera red componente; comprobar si los paquetes de datos electrónicos primero y segundo se transmitieron sin alteraciones desde el primer al segundo componente de red; y comprobar si el primer y el segundo paquete de datos electrónicos se recibieron en el orden especificado por el primer componente de red, es decir, el primero antes del segundo paquete de datos electrónicos.

En el método para la transmisión segura de componentes electrónicos de datos, en el segundo componente de red puede preverse que el n-ésimo paquete de datos electrónicos se verifique por medio de la primera clave pública y el n-ésimo paquete de datos electrónicos verificado se analice, en el que se ejecuta aquí al menos una de las siguientes tareas de verificación: verificar si el paquete de datos electrónico n-ésimo se recibió del primer componente de red; comprobar si el n-ésimo paquete de datos electrónicos se transmitió sin cambios desde el primer al segundo componente de red; y comprobar si el n-ésimo paquete de datos electrónicos se recibió en el orden especificado por el primer componente de red, es decir, el (n-1) antes del n-ésimo paquete de datos electrónicos.

En el método para el intercambio bidireccional seguro de paquetes de datos electrónicos en la red, también puede proporcionarse lo siguiente en el segundo componente de red: recibir el segundo paquete de datos de solicitud electrónica y la segunda firma de solicitud digital; guardar al menos la segunda firma de solicitud digital en el segundo dispositivo de almacenamiento; proporcionar una segunda carga útil de respuesta como reacción a la recepción del segundo paquete de datos de solicitud electrónica, en el que la segunda carga útil de respuesta se relaciona con una segunda respuesta a la segunda solicitud; crear un segundo paquete de datos de respuesta electrónica que comprende el segundo ID de componente, la segunda carga útil de respuesta y la segunda firma de solicitud electrónica; crear una segunda firma de respuesta digital, en el que el segundo paquete de datos de respuesta electrónica se firma digitalmente mediante el uso de la segunda clave privada; enviar el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital desde el segundo componente de red al primer componente de red. En el primer componente de red, se reciben el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital, y al menos la segunda firma de respuesta digital se guarda en el primer dispositivo de almacenamiento. Además, el segundo paquete de datos de respuesta electrónica también puede guardarse en el dispositivo de almacenamiento.

En el método para el intercambio bidireccional seguro de paquetes de datos electrónicos, puede proporcionarse lo siguiente en el segundo componente de red: proporcionar una carga útil de respuesta adicional que indica una respuesta adicional a la primera solicitud; crear un paquete de datos de respuesta electrónica adicional que comprende el segundo ID de componente, la carga útil de respuesta adicional y la primera firma de respuesta electrónica; crear una firma de respuesta digital adicional, en el que el paquete de datos de respuesta electrónica adicional se firma digitalmente mediante el uso de la segunda clave privada; enviar el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional desde el segundo componente de red al primer

componente de red. En el primer componente de red se reciben el paquete de datos de respuesta electrónico adicional y la firma de respuesta digital adicional y al menos la firma de respuesta digital adicional se guarda en el primer dispositivo de almacenamiento.

También puede darse el caso de que el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional se creen en el segundo componente de red y se transmitan al primer componente de red antes de que se creen el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital en el segundo componente de red.

En la red, los paquetes de datos y/o los datos relativos a las firmas pueden transmitirse entre un componente de red de envío y uno de recepción en rutas de transmisión iguales o diferentes dentro de la red. Esto hace posible, por ejemplo, transmitir paquetes de datos y firmas en rutas de transmisión diferentes y al menos parcialmente separadas desde el componente de red de envío hasta el de recepción, ya sea simultáneamente o con un retardo de tiempo. La verificación mediante la firma digital incluye tanto la verificación del remitente (verificación de autenticidad) como la verificación de la integridad de los paquetes de datos (verificación de integridad).

Descripción de las modalidades

A continuación, se describirán modalidades adicionales con referencia a las figuras de los dibujos, en los que:

La Figura 1 muestra esquemáticamente una red con componentes de red entre los que pueden transmitirse paquetes de datos electrónicos a través de enlaces de comunicación de datos;
Las Figuras 2a a 2c muestran esquemáticamente un método para la transmisión segura de paquetes de datos electrónicos en la red y
Las Figuras 3a a 3e muestran esquemáticamente un método para el intercambio bidireccional de paquetes de datos electrónicos en la red.

La Figura 1 muestra esquemáticamente una disposición con componentes de red 10.1,..., 10.m (m>2) que se disponen en una red y pueden intercambiar paquetes de datos electrónicos a través de enlaces de comunicación de datos 20.1,..., 20.k (k>2). Los componentes de red 10.1,... 10.m tienen cada uno al menos un procesador que se configura para procesar datos electrónicos, por ejemplo para crear paquetes de datos electrónicos y proporcionarlos para transmisión, o para analizar paquetes de datos electrónicos recibidos.

Los enlaces de comunicación de datos 30.1, ..., 30.k pueden diseñarse para ser de largo o corto plazo entre componentes de la red, por ejemplo limitados a un solo proceso de transmisión para un paquete de datos electrónicos.

La Figura 2 muestra esquemáticamente un método para la transmisión segura de paquetes de datos electrónicos entre dos de los componentes de red 10.1,..., 10.n, concretamente, por ejemplo, entre un primer componente de red 10.1 y un segundo componente de red 10.2.

A continuación, se describirán primero los pasos en el contexto de una primera operación de procesamiento de datos en el primer componente de red 10.1 Se proporciona un primer par de claves criptográficas para la firma digital con una primera clave pública y una primera clave privada en el paso 100. En el paso 101, se proporciona un primer ID (ID – identificación) de componente que identifica de forma biunívoca el primer componente de red 10.1 en la red. Se proporciona una primera carga útil en el paso 102. Se crea un primer paquete de datos electrónicos que comprende el primer ID de componente y la primera carga útil (paso 103). La carga útil puede relacionarse con cualquier contenido de datos deseado, por ejemplo, datos de medición, datos de audio y/o video. En el paso 104, se crea una primera firma digital, en el que el primer paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada. El primer paquete de datos electrónicos y la primera firma digital se envían desde el primer componente de red 10.1 al segundo componente de red 10.2 en el paso 105. Además, en el paso 106 se envía la primera clave pública desde el primer al segundo componente de red 10.1, 10.2, en el que puede realizarse previamente la transmisión de la clave pública una vez proporcionado el primer par de claves criptográficas en el primer componente de red.

A continuación, se describirán otros pasos en el contexto de una segunda operación de procesamiento de datos en el primer componente de red 10.1. En el paso 107, se proporciona una segunda carga útil que es diferente de la primera carga útil. Se crea un segundo paquete de datos electrónicos que comprende el primer ID de componente, la segunda carga útil y la primera firma digital (paso 108). En el paso 109, se crea una segunda firma digital, en el que el segundo paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada. El segundo paquete de datos electrónicos y la segunda firma digital se envían desde el primer componente de red 10.1 al segundo componente de red 10.2 (paso 110).

De acuerdo con el método, en el segundo componente de red 10.2 se proporciona lo siguiente: recibir el primer paquete de datos electrónicos y la primera firma digital, y el segundo paquete de datos electrónicos y la segunda firma digital (paso 111), que puede tener lugar simultáneamente o con un tiempo de retraso. El primer y el segundo

paquete de datos electrónicos y la primera y la segunda firma digital se guardan en un dispositivo de almacenamiento (etapa 112) que se asigna al segundo componente de red. La primera clave pública se recibe en el segundo componente de red (paso 113) y se guarda en el dispositivo de almacenamiento (paso 114).

El método para la transmisión segura de paquetes de datos electrónicos puede comprender además una n-ésima (n>2) operación de procesamiento de datos en el primer componente de red 10.1. Esto puede comprender los siguientes pasos: proporcionar una n-ésima carga útil que es diferente de al menos la primera y la segunda carga útil (paso 115); crear un n-ésimo paquete de datos electrónicos que comprende el primer ID de componente, la n-ésima carga útil y una (n-1)ésima firma digital que se creó mediante el uso de la primera clave privada para un (n-1)ésimo paquete de datos con una (n-1)ésima carga útil, el primer ID de componente y una (n-2)ésima firma digital (paso 116); crear una n-ésima firma digital, en el que el n-ésimo paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada (paso 117); y enviar el n-ésimo paquete de datos electrónicos y la n-ésima firma digital desde el primer componente de red al segundo componente de red (paso 118).

En el segundo componente de red, el n-ésimo paquete de datos eléctricos y la n-ésima firma digital se reciben y guardan en el dispositivo de almacenamiento (pasos 119 y 120).

Entonces puede realizarse una o varias tareas de control en el segundo componente de red 10.2 para comprobar la transmisión correcta y sin manipulaciones de los paquetes de datos electrónicos. En este contexto, puede proporcionarse para primero verificar (verificar) el primer paquete de datos electrónicos en el paso 121 mediante el uso de la primera clave electrónica para determinar si la firma digital transmitida del primer paquete de datos electrónicos coincide con el contenido del primer paquete de datos electrónicos. En el paso 122, dicha verificación se lleva a cabo para el segundo paquete de datos electrónicos mediante el uso de la primera clave pública. En este caso, no solo se verifica la integridad de los datos de los paquetes de datos recibidos, sino que la verificación mediante la firma digital incluye tanto la verificación del remitente (autenticidad) como la verificación de la integridad de los paquetes de datos (integridad).

A continuación, pueden evaluarse los paquetes de datos electrónicos primero y segundo verificados (paso 123). En este caso, puede ejecutarse al menos una de las siguientes tareas de verificación: verificar si los paquetes de datos electrónicos primero y segundo se recibieron del mismo componente de red, a saber, el primer componente de red 10.1; verificar si los paquetes de datos electrónicos primero y segundo se transmitieron sin cambios desde el primer al segundo componente de red, 10.1, 10.2; y comprobar si los paquetes de datos electrónicos primero y segundo se recibieron en el orden especificado por el primer componente de red 10.1, es decir, el primero antes del segundo paquete de datos electrónicos.

De manera similar, el método puede permitir la evaluación y verificación del n-ésimo paquete de datos electrónicos.

La Figura 3 muestra esquemáticamente un método para el intercambio bidireccional seguro de paquetes de datos electrónicos en la red. En el paso 200, se proporciona un primer par de claves criptográficas para firmar digitalmente con una primera clave pública y una primera privada en el primer componente de red 10.1. En el segundo componente de red, en el paso 201 se proporciona un segundo par de claves criptográficas para firmar digitalmente con una segunda clave pública y una segunda privada. En los pasos 202 y 203, se proporcionan un primer ID de componente y un segundo ID de componente en el primer y segundo componente de red 10.1, 10.2 e identifican de forma biunívoca el primer y el segundo componente de red en la red.

De acuerdo con el método, en el primer componente de red 10.1 se proporciona lo siguiente: recibir la segunda clave pública (paso 204); proporcionar una primera carga útil de solicitud que se relaciona con una primera solicitud (paso 205); crear un primer paquete de datos de solicitud electrónica que comprende el primer ID de componente y la primera carga útil de solicitud (paso 206); crear una primera firma digital, en el que el primer paquete de datos de solicitud electrónica se firma digitalmente mediante el uso de la primera clave privada (paso 207); enviar el primer paquete de datos de solicitud electrónica y la primera firma de solicitud digital desde el primer componente de red al componente de red (paso 208); y enviar la primera clave pública desde el primer al segundo componente de red (paso 209).

En el segundo componente de red 10.2 se proporciona lo siguiente: recibir la primera clave pública (paso 210); recibir el primer paquete de datos de solicitud electrónica y la primera firma de solicitud digital (paso 211); guardar al menos la primera firma de solicitud digital en un segundo dispositivo de almacenamiento que se asigna al segundo componente de red (paso 212); proporcionar una primera carga útil de respuesta como reacción a la recepción del primer paquete de datos de solicitud electrónica, en el que la primera carga útil de respuesta se relaciona con una primera respuesta a la primera solicitud (paso 213); crear un primer paquete de datos de respuesta electrónica que comprende la ID del segundo componente, la primera carga útil de respuesta y la primera firma de solicitud electrónica (paso 214); crear una primera firma de respuesta digital, en el que el primer paquete de datos de respuesta electrónica se firma digitalmente mediante el uso de la segunda clave privada (paso 215); y enviar el primer paquete de datos de respuesta electrónica y la primera firma de respuesta digital desde el segundo componente de red al primer componente de red (paso 216).

También se proporciona lo siguiente en el primer componente de red 10.1: recibir el primer paquete de datos de respuesta electrónica y la primera firma de respuesta digital (paso 217); guardar al menos la primera firma de respuesta digital en un primer dispositivo de almacenamiento que se asigna al primer componente de red (paso 218); proporcionar una segunda carga útil de solicitud que se relaciona con una segunda solicitud (paso 219); crear un segundo paquete de datos de solicitud electrónica que comprende el primer ID de componente, la segunda carga útil de solicitud y la primera firma de respuesta digital (paso 220); crear una segunda firma digital, en el que el segundo paquete de datos de solicitud electrónica se firma digitalmente mediante el uso de la primera clave privada (paso 221); y enviar el segundo paquete de datos de solicitud electrónica y la segunda firma de solicitud digital desde el primer componente de red al segundo componente de red (paso 222).

En el método para el intercambio bidireccional seguro de paquetes de datos electrónicos, también se puede proporcionar lo siguiente en el segundo componente de red: recibir el segundo paquete de datos de solicitud electrónica y la segunda firma de solicitud digital (paso 223); guardar al menos la segunda firma de solicitud digital en el segundo dispositivo de almacenamiento (paso 224); proporcionar una segunda carga útil de respuesta como reacción a la recepción del segundo paquete de datos de solicitud electrónica, en el que la segunda carga útil de respuesta se relaciona con una segunda respuesta a la segunda solicitud (paso 225); crear un segundo paquete de datos de respuesta electrónica que comprende el segundo ID de componente, la segunda carga útil de respuesta y la segunda firma de solicitud electrónica (paso 226); crear una segunda firma de respuesta digital, en el que el segundo paquete de datos de respuesta electrónica se firma digitalmente mediante el uso de la segunda clave privada (paso 227); enviar el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital desde el segundo componente de red al primer componente de red (paso 228).

En el primer componente de red 10.1, se reciben el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital (paso 229), y al menos la segunda firma de respuesta digital se guarda en el primer dispositivo de almacenamiento (paso 230).

Además, en el método para el intercambio bidireccional de paquetes de datos puede proporcionarse lo siguiente en el segundo componente de red: proporcionar una carga útil de respuesta adicional que indica una respuesta adicional a la primera solicitud (paso 231); crear un paquete de datos de respuesta electrónica adicional que comprende el segundo ID de componente, la carga útil de respuesta adicional y la primera firma de respuesta electrónica (paso 232); crear una firma de respuesta digital adicional, en el que el paquete de datos de respuesta electrónica adicional se firma digitalmente mediante el uso de la segunda clave privada (paso 233); enviar el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional desde el segundo componente de red al primer componente de red (paso 234).

En el primer componente de red 10.1 se reciben el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional (paso 235) y se guarda al menos la firma de respuesta digital adicional (paso 236).

La verificación de los paquetes de datos electrónicos por medio de una clave pública en el lado del receptor correspondiente puede llevarse a cabo entonces como se describe anteriormente, y pueden llevarse a cabo una o más de las tareas de verificación explicadas.

En los métodos, se establece una relación de confianza entre el componente de red de envío (creador, por ejemplo, dispositivo sensor) de paquetes de datos y todos los componentes de red de recepción reales y potenciales (receptores). Para ello, se proporciona un par de claves asimétricas al creador (criptografía asimétrica convencional) y la clave pública se comunica a todos los receptores de la red o se proporciona de forma que estos receptores tengan un acceso seguro y eficaz a la misma. Por el contrario, para establecer la confiabilidad de las respuestas necesarias (confirmaciones o similares) del receptor, el receptor también genera un par de claves y, a su vez, pone la parte pública a disposición del creador de datos (componente de red de envío). Se asumen medidas adecuadas para verificar la propiedad de la clave privada (por ejemplo, intercambio de claves en base a Diffie-Hellmann).

Para que los receptores de los paquetes de datos puedan asegurarse de que proceden del creador de los paquetes de datos, el creador firma todos los paquetes de datos con su clave privada y la firma resultante se conserva junto con el paquete de datos como un “paquete” en la ruta completa de procesamiento o transmisión. Esta firma puede verificarse por el destinatario mediante el uso de la clave pública obtenida previamente por el creador (no es posible crear firmas mediante el uso de la clave pública). Esto resuelve dos problemas importantes: (i) la integridad de los paquetes de datos se asegura porque la manipulación de los paquetes de datos o de la firma daría lugar a un error en la verificación; y (ii) se asegura la autenticidad de los paquetes de datos (originalmente producidos por el componente de red de envío).

Esto descarta la manipulación de toda la transmisión de datos (o esto puede detectarse fácilmente mediante la comprobación de la firma) y asegura el origen de los paquetes de datos (solo este remitente está en posesión de la clave privada necesaria para generar esta firma). Siempre que ambas partes (creador y receptor, es decir, componentes de red de envío y recepción) completen el intercambio y la verificación de las claves respectivas de antemano, la transmisión a través de rutas de datos no seguras, no confiables o no autenticadas no conduce a una restricción de la confiabilidad de los datos.

El sellado único de los datos por parte del remitente garantiza la confiabilidad en todos los pasos de procesamiento reales y potenciales posteriores.

A continuación, se dan explicaciones en relación con asegurar la integridad, autenticidad y secuencia en la transmisión de datos. Se usan los siguientes términos abreviados: S - remitente (componente de red de envío); R - receptor (componente de red de envío); sig[n,X] - n-ésima firma de X; ID_x - característica de identificación del dispositivo x; carga útil n - “carga útil” del n-ésimo paquete de datos.

El requisito previo es que el remitente S genere un par de claves que consiste en una clave secreta y una clave pública. El remitente genera una identificación biúnica ID_S en la red o lo recibió durante la producción; al receptor R se le da acceso a la clave pública del emisor S antes de recibir el primer paquete de datos. Los métodos para el intercambio seguro de claves públicas de pares de claves en el contexto de la criptografía asimétrica se conocen como tales en varias modalidades.

El remitente desea transmitir varios paquetes de datos (más de uno) al receptor y estos datos (carga útil 1, carga útil 2, etc.) están disponibles. El método para transmitir los múltiples paquetes de datos puede representarse esquemáticamente de la siguiente manera:

1) Inicial (paquete de datos 1 de S --> R): $[ID_S, 0, \text{carga útil 1}]^{sig[1,S]}$
2) Secuencia 1 (paquete de datos 2 de S --> R): $[ID_S, sig[1,S], \text{carga útil 2}]^{sig[2,S]}$
n) Secuencia n (paquete de datos n+1): $[ID_S, sig[n,S], \text{carga útil n}]^{sig[n+1,S]}$

La adopción de la firma del paquete de datos anterior, así como también la firma de cada paquete de datos individual, permite al receptor asegurarse de que (i) todos los paquetes se originan en el mismo remitente (S); (ii) todos los paquetes se transmiten sin alteraciones; y (iii) todos los paquetes se reciben en el orden iniciado por el remitente.

R siempre guarda la última firma sig[n, S] para cada remitente.

La autenticidad se establece cuando ambos socios, es decir, el emisor y el receptor, confían en el otro socio debido a una verificación previa de las claves públicas. Entonces es irrelevante qué socio actúa como emisor y receptor durante la transmisión. La transmisión de datos puede tener lugar en ambas direcciones con las garantías dadas.

Con este tipo de transmisión de datos, también es irrelevante cuántos destinatarios se recibieron y reenviaron los datos. La confiabilidad de los datos puede verificarse en cualquier punto de la transmisión o en los pasos de procesamiento.

A continuación se explica un caso de uso para la seguridad bidireccional de la transmisión de paquetes de datos en la red.

Se aplican los siguientes requisitos previos:

a. El emisor S y el receptor R generan cada uno un par de claves que consiste en una clave secreta y una clave pública. El emisor S y el receptor R generan o reciben cada uno un ID único durante la producción (ID de hardware).

b. El receptor R obtiene acceso a la clave pública del emisor S antes de recibir el primer paquete de datos. El remitente S tiene acceso a la clave pública del receptor R antes de recibir el primer paquete de datos. Los métodos para el intercambio seguro de claves públicas de pares de claves en el contexto de la criptografía asimétrica se conocen como tales en varias modalidades.

c. El código de programa del remitente desea transmitir múltiples paquetes de datos (más de uno) al receptor y estos datos (carga útil 1, carga útil 2, etc.) están disponibles.

En un caso A, se supone un ciclo de solicitud-respuesta simple (ciclo de solicitud-respuesta) sin continuidad. Esto da como resultado lo siguiente:

1. Inicial (paquete de datos 1)

S->R [IDS, 0, SOLICITUD 1]sig[1,S]
S<-R [IDR, sig[1,S], RESPUESTA 1]sig[1,R]
S<-R [IDR, sig[1,R], RESPUESTA 1a]sig[2,R] (opcional)

2. Secuencia 1 (paquete de datos 2)
S->R [ID, sig[1,S], SOLICITUD2]sig[2,S]
S<-R [IDR, sig[2,S], RESPUESTA2]sig[2,R]

n. Secuencia n (paquete de datos n+1)

S->R [ID, sig[n,S], SOLICITUDn]sig[n+1,S]
S<-R [IDR, sig[n+1,S], RESPUESTAn]sig[n+1,R]

El caso A, además del método 1, da seguridad al remitente de que la respuesta a una solicitud realmente se dio solo a esa solicitud. Después de recibir la RESPUESTA correcta, no se acepta ninguna otra RESPUESTA a esta solicitud. Si una SOLICITUD desencadena múltiples RESPUESTAS, estas a su vez deben encadenarse.

El receptor R siempre guarda la última firma sig[n, S] de cada remitente.

Un caso B proporciona una protección completa para la comunicación bidireccional. Esto da como resultado lo siguiente:

1. Inicial (paquete de datos 1)

S->R [IDS, 0, SOLICITUD 1]sig[1,S]
S<-R [IDR, sig[1,S], RESPUESTA 1]sig[1,R]

2. Secuencia 1 (paquete de datos 2)

S->R [ID, sig[1,R], SOLICITUD2]sig[2,S]
S<-R [IDR, sig[2,S], RESPUESTA2]sig[2,R]

n. Secuencia n (paquete de datos n+1)

S->R [ID, sig[n,R], SOLICITUD n]sig[n+1,S]
S<-R [IDR, sig[n+1,S], RESPUESTA n]sig[n+1,R]

El caso B asegura una secuencia de SOLICITUD/RESPUESTA con absoluta confiabilidad de la secuencia en ambas direcciones. El receptor E siempre debe guardar la última firma sig[n,S] para cada remitente.
Las características de la invención divulgada en la descripción anterior, las reivindicaciones y los dibujos pueden ser relevantes para la realización de la invención en sus diversas modalidades, tanto individualmente como en cualquier combinación.

REIVINDICACIONES

1. Un método para la transmisión segura de paquetes de datos electrónicos en una red, que tiene:

- proporcionar componentes de red, que en cada caso tienen un procesador para procesamiento de datos electrónicos y se configuran para enviar y/o recibir paquetes de datos electrónicos entre los componentes de red en una red a través de conexiones de comunicación de datos;
- en uno primero de los componentes de red,

- en el contexto de una primera operación de procesamiento de datos,

- proporcionar un primer par de claves criptográficas para firmar digitalmente con una primera clave pública y una primera clave privada;
- proporcionar un ID de primer componente, que identifica de forma biunívoca el primer componente de red en la red;
- proporcionar una primera carga útil;
- crear un primer paquete de datos electrónicos, que comprende el primer ID de componente y la primera carga útil;
- crear una primera firma digital, en que el primer paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada;
- enviar el primer paquete de datos electrónicos y la primera firma digital desde el primer componente de red a un segundo de los componentes de red; y
- enviar la primera clave pública desde el primer al segundo componente de red; y

- en el contexto de una segunda operación de procesamiento de datos,

- proporcionar una segunda carga útil, que es diferente de la primera carga útil;
- crear un segundo paquete de datos electrónicos, que comprende el primer ID de componente, la segunda carga útil y la primera firma digital;
- crear una segunda firma digital, en que el segundo paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada; y
- enviar el segundo paquete de datos electrónicos y la segunda firma digital desde el primer componente de red al segundo componente de red; y

- en el segundo componente de red,

- recibir el primer paquete de datos electrónicos y la primera firma digital, y el segundo paquete de datos electrónicos y la segunda firma digital;
- guardar el primer paquete de datos electrónicos y la primera firma digital, y el segundo paquete de datos electrónicos y la segunda firma digital en un dispositivo de almacenamiento, que se asigna al segundo componente de red;
- recibir la primera clave pública; y
- guardar la primera clave pública en el dispositivo de almacenamiento;
en donde además se proporciona lo siguiente:

- en el primer componente de red, en el contexto de una n-ésima (n>2) operación de procesamiento de datos,

- proporcionar una n-ésima carga útil, que es al menos diferente de la primera y la segunda carga útil;
- crear un n-ésimo paquete de datos electrónicos, que comprende el primer ID de componente, la n-ésima carga útil y una (n-1)ésima firma digital, que se creó mediante el uso de la primera clave privada para un (n-1)ésimo paquete de datos con una (n-1)ésima carga útil, el primer ID de componente y una (n-2)ésima firma digital;
- crear una n-ésima firma digital, en la que el n-ésimo paquete de datos electrónicos se firma digitalmente mediante el uso de la primera clave privada; y
- enviar el n-ésimo paquete de datos electrónicos y la n-ésima firma digital desde el primer componente de red al segundo componente de red; y

- en el segundo componente de red,

- recibir el n-ésimo paquete de datos electrónicos y la n-ésima firma digital, y
- guardar el n-ésimo paquete de datos electrónicos y la n-ésima firma digital en el dispositivo de almacenamiento.

2. El método de acuerdo con la reivindicación 1, en donde además se proporciona lo siguiente en el segundo componente de red:

- verificar el primer paquete de datos electrónicos por medio de la primera clave pública;
- verificar el segundo paquete de datos electrónicos por medio de la primera clave pública; y
- analizar el primer y el segundo paquete de datos electrónicos verificados, en donde se ejecuta aquí al menos una de las siguientes tareas de comprobación:

  - comprobar si los paquetes de datos electrónicos primero y segundo se recibieron desde el mismo componente de red, concretamente el primer componente de red;
  - comprobar si los paquetes de datos electrónicos primero y segundo se transmitieron sin alteraciones desde el primer al segundo componente de red; y
  - comprobar si el primer y el segundo paquete de datos electrónicos se recibieron en el orden especificado por el primer componente de red, es decir, el primero antes del segundo paquete de datos electrónicos.

3. El método de acuerdo con las reivindicaciones 1 y 2, en donde además se proporciona lo siguiente en el segundo componente de red:

   - verificar el n-ésimo paquete de datos electrónicos por medio de la primera clave pública;
   - analizar el n-ésimo paquete de datos electrónicos verificado, en donde se ejecuta aquí al menos una de las siguientes tareas de comprobación:

     - comprobar si se recibió el n-ésimo paquete de datos electrónicos desde el primer componente de red;
     - comprobar si el n-ésimo paquete de datos electrónicos se transmitió sin alteraciones desde el primer al segundo componente de red; y
     - comprobar si el n-ésimo paquete de datos electrónicos se recibió en el orden especificado por el primer componente de red, es decir, el (n-1)ésimo antes del n-ésimo paquete de datos electrónicos.

4. Un método para el intercambio bidireccional seguro de paquetes de datos electrónicos en una red, que tiene:

   - proporcionar componentes de red, que en cada caso tienen un procesador para procesamiento de datos electrónicos y se configuran para enviar y/o recibir paquetes de datos electrónicos entre los componentes de red en una red a través de conexiones de comunicación de datos;
   - proporcionar un primer par de claves criptográficas para firmar digitalmente con una primera clave pública y una primera clave privada, en uno primero de los componentes de red;
   - proporcionar un segundo par de claves criptográficas para firmar digitalmente con una segunda clave pública y una segunda privada, para firmar digitalmente en uno segundo de los componentes de red;
   - proporcionar un ID de primer componente, que identifica de forma biunívoca el primer componente de red en la red;
   - proporcionar un ID de segundo componente, que identifica de forma biunívoca el segundo componente de red en la red;
   - en el primer componente de red,

     - recibir la segunda clave pública;
     - proporcionar una primera carga útil de solicitud, que se relaciona con una primera solicitud;
     - crear un primer paquete de datos de solicitud electrónica, que comprende el primer ID de componente y la primera carga útil de solicitud;
     - crear una primera firma digital, en que el primer paquete de datos de solicitud electrónica se firma digitalmente mediante el uso de la primera clave privada;
     - enviar el primer paquete de datos de solicitud electrónica y la primera firma de solicitud digital desde el primer componente de red al componente de red; y
     - enviar la primera clave pública desde el primer al segundo componente de red;

   - en el segundo componente de red,

     - recibir la primera clave pública;
     - recibir el primer paquete de datos de solicitud electrónica y la primera firma de solicitud digital;
     - guardar al menos la primera firma de solicitud digital en un segundo dispositivo de almacenamiento, que se asigna al segundo componente de red;
     - proporcionar una primera carga útil de respuesta como reacción a la recepción del primer paquete de datos de solicitud electrónica, en donde la primera carga útil de respuesta se relaciona con una primera respuesta a la primera solicitud;
     - crear un primer paquete de datos de respuesta electrónica, que comprende el segundo ID de componente, la primera carga útil de respuesta y la primera firma de solicitud electrónica;
     - crear una primera firma de respuesta digital, en el que el primer paquete de datos de respuesta electrónica se firma digitalmente mediante el uso de la segunda clave privada; y
     - enviar el primer paquete de datos de respuesta electrónica y la primera firma de respuesta digital desde el segundo componente de red al primer componente de red; y

- en el primer componente de red,

- recibir el primer paquete de datos de respuesta electrónica y la primera firma de respuesta digital;
- guardar al menos la primera firma de respuesta digital en un primer dispositivo de almacenamiento, que se asigna al primer componente de red;
- proporcionar una segunda carga útil de solicitud, que se relaciona con una segunda solicitud;
- crear un segundo paquete de datos de solicitud electrónica, que comprende el primer ID de componente, la segunda carga útil de solicitud y la primera firma de respuesta digital;
- crear una segunda firma digital, en el que el segundo paquete de datos de solicitud electrónica se firma digitalmente mediante el uso de la primera clave privada; y
- enviar el segundo paquete de datos de solicitud electrónica y la segunda firma de solicitud digital desde el primer componente de red al segundo componente de red.

5. El método de acuerdo con la reivindicación 4, que tiene además:

- en el segundo componente de red,

- recibir el segundo paquete de datos de solicitud electrónica y la segunda firma de solicitud digital;
- guardar al menos la segunda firma de solicitud digital en el segundo dispositivo de almacenamiento;
- proporcionar una segunda carga útil de respuesta como reacción a la recepción del segundo paquete de datos de solicitud electrónica, en el que la segunda carga útil de respuesta se relaciona con una segunda respuesta a la segunda solicitud;
- crear un segundo paquete de datos de respuesta electrónica, que comprende el segundo ID de componente, la segunda carga útil de respuesta y la segunda firma de solicitud electrónica;
- crear una segunda firma de respuesta digital, en el que el segundo paquete de datos de respuesta electrónica se firma digitalmente mediante el uso de la segunda clave privada;
- enviar el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital desde el segundo componente de red al primer componente de red; y

- en el primer componente de red,

- recibir el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital, y
- guardar al menos la segunda firma de respuesta digital en el primer dispositivo de almacenamiento.

6. El método de acuerdo con la reivindicación 4 o 5, que tiene además:

- en el segundo componente de red,

- proporcionar una carga útil de respuesta adicional, que indica una respuesta adicional a la primera solicitud;
- crear un paquete de datos de respuesta electrónica adicional, que comprende el segundo ID de componente, la carga útil de respuesta adicional y la primera firma de respuesta electrónica;
- crear una firma de respuesta digital adicional, en el que el paquete de datos de respuesta electrónica adicional se firma digitalmente mediante el uso de la segunda clave privada;
- enviar el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional desde el segundo componente de red al primer componente de red; y

- en el primer componente de red,

- recibir el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional; y
- guardar al menos la firma de respuesta digital adicional en el primer dispositivo de almacenamiento.

7. El método de acuerdo con las reivindicaciones 5 y 6, en el que el paquete de datos de respuesta electrónica adicional y la firma de respuesta digital adicional se crean en el segundo componente de red y se transmiten al primer componente de red, antes que el segundo paquete de datos de respuesta electrónica y la segunda firma de respuesta digital se creen en el segundo componente de red.

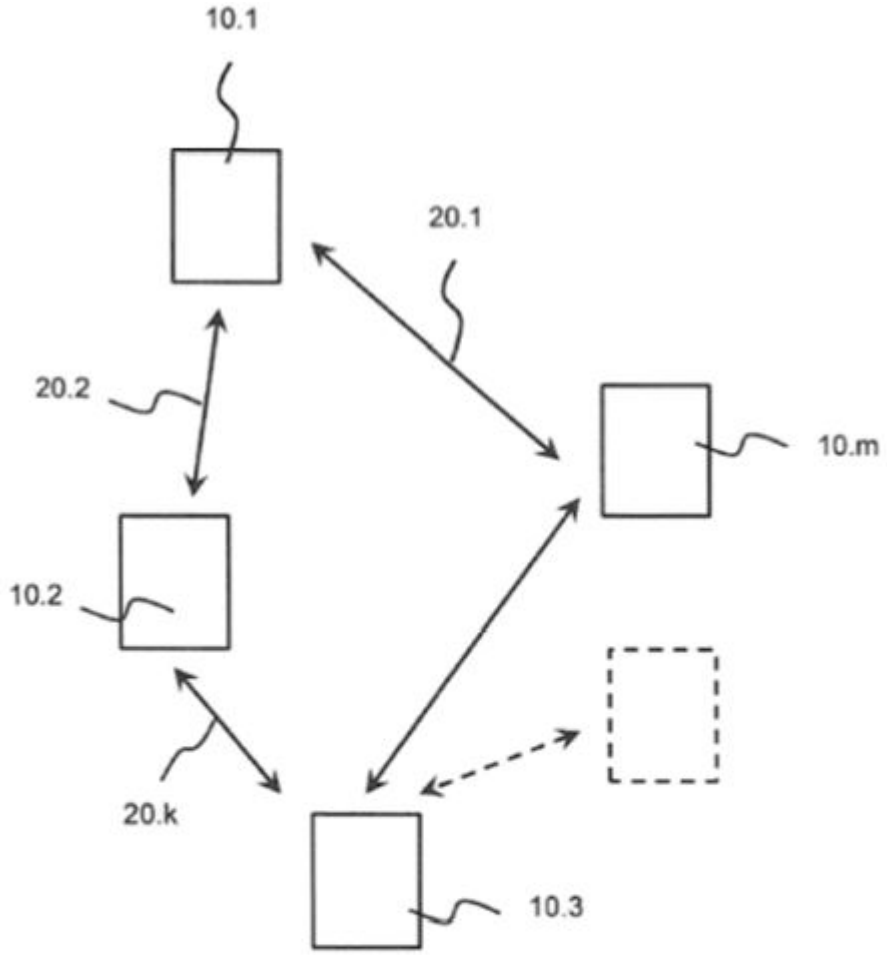

Figura 1

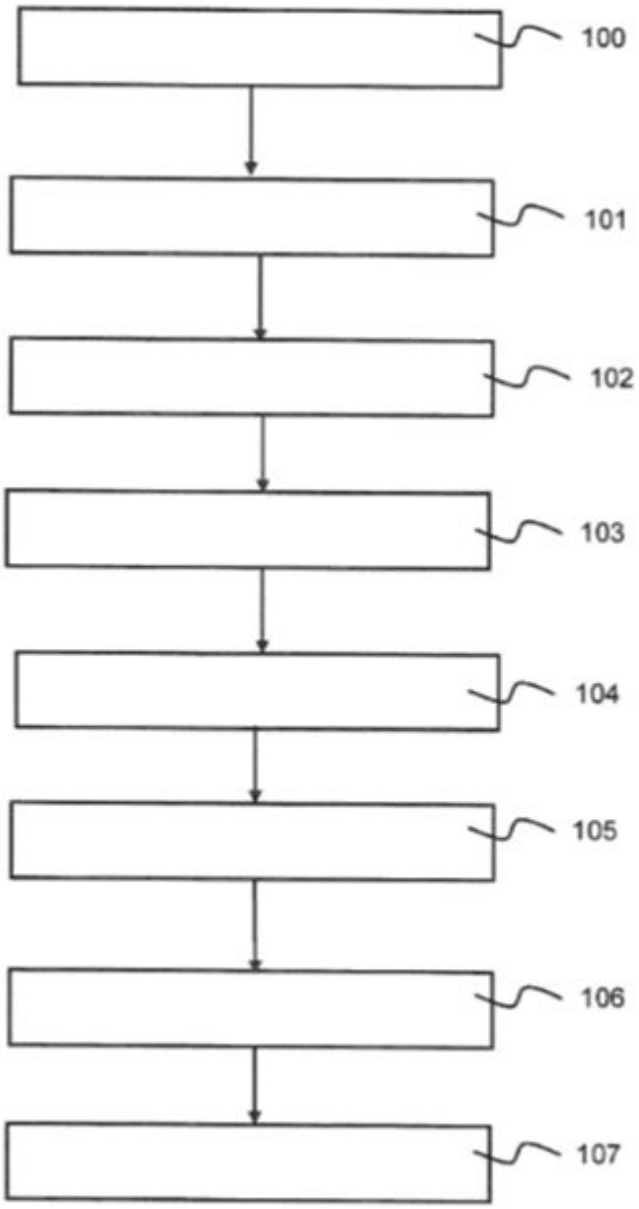

Figura 2a

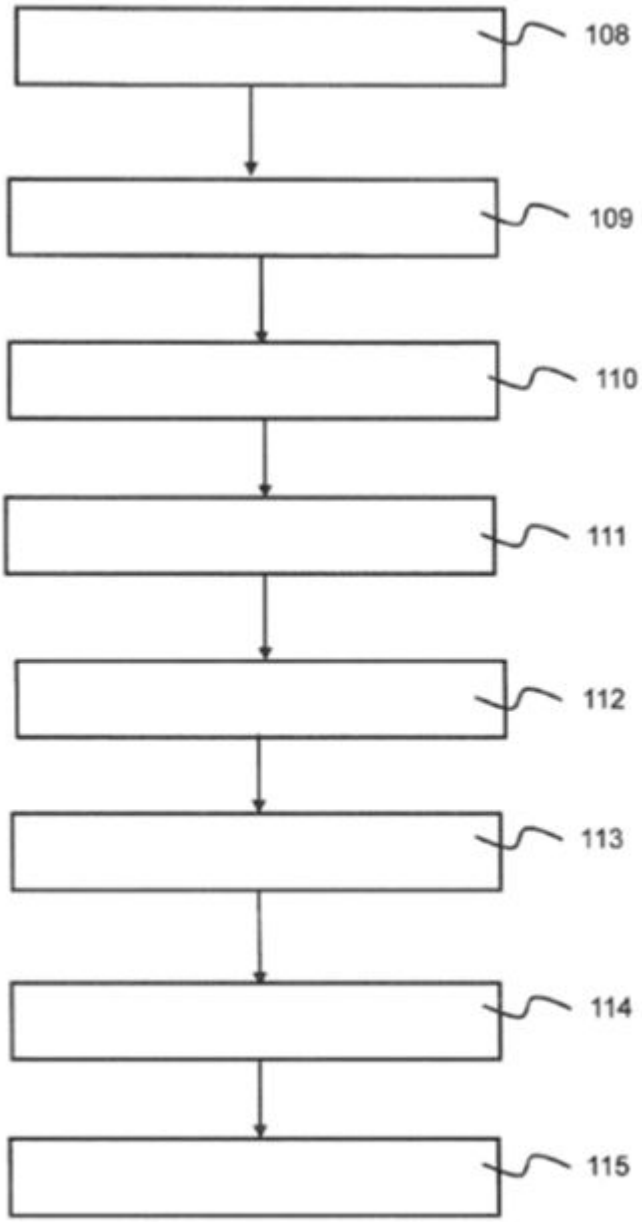

Figura 2b

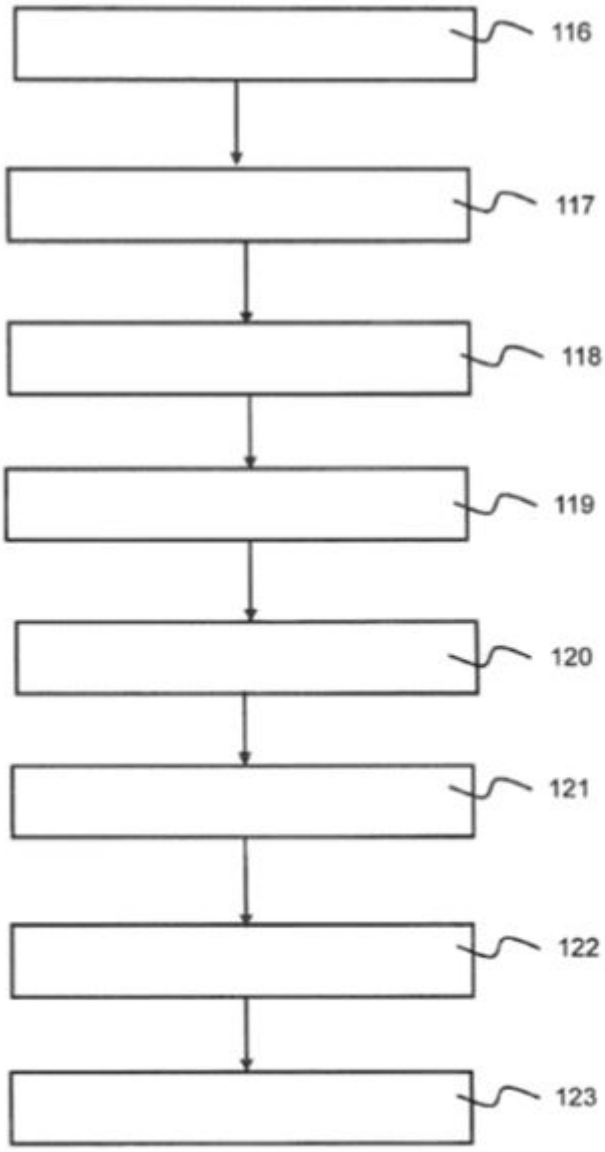

Figura 2c

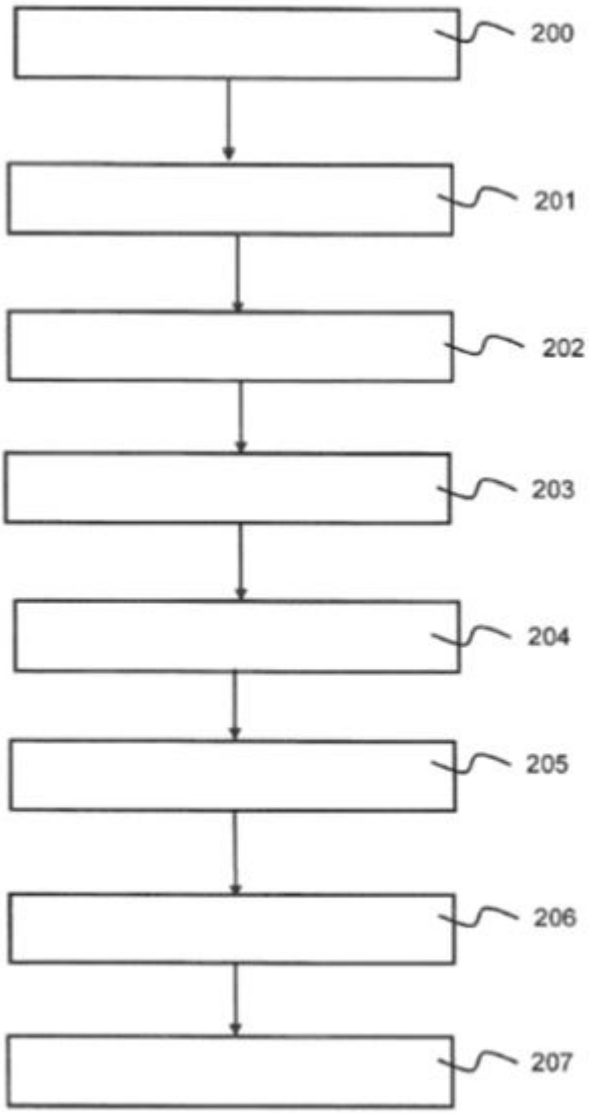

Figura 3a

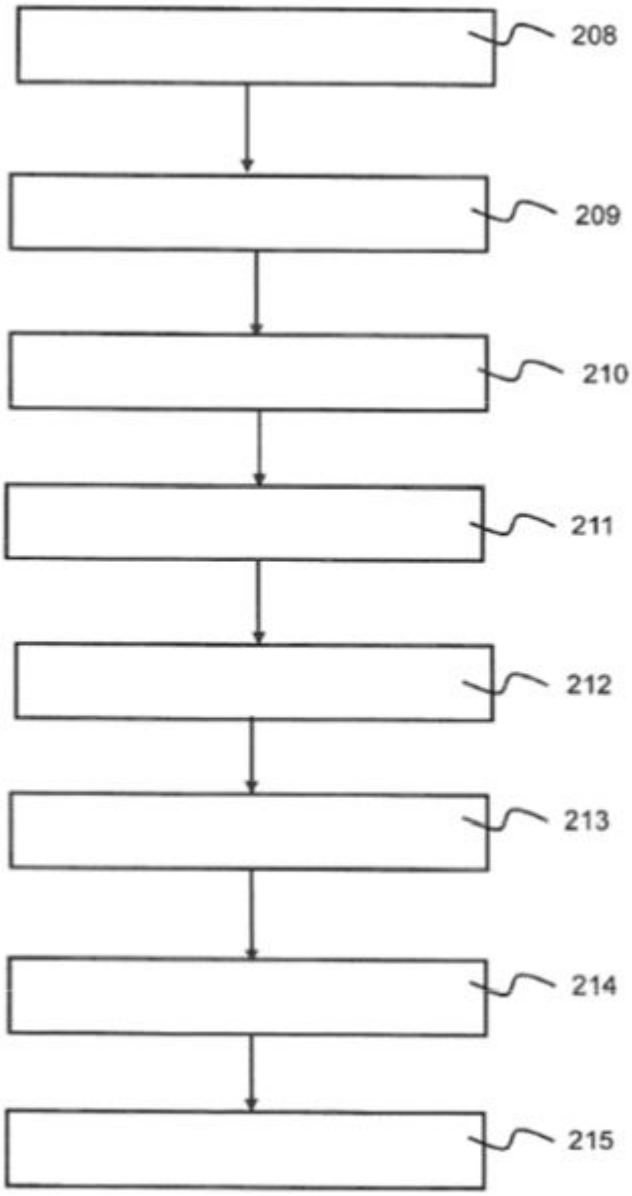

Figura 3b

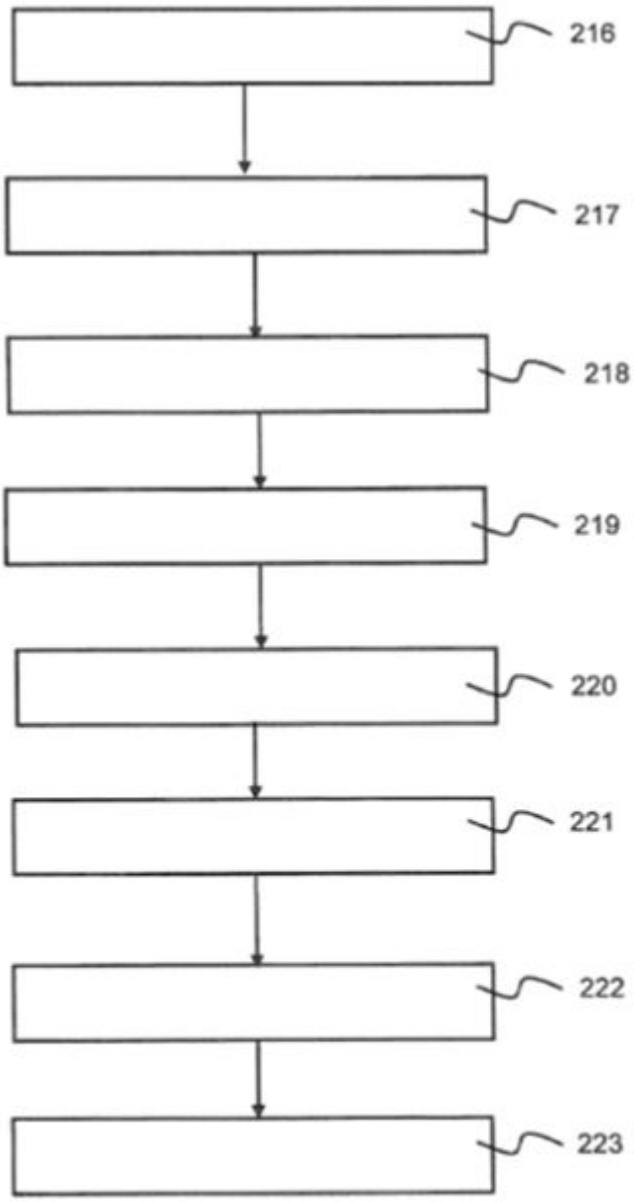

Figura 3c

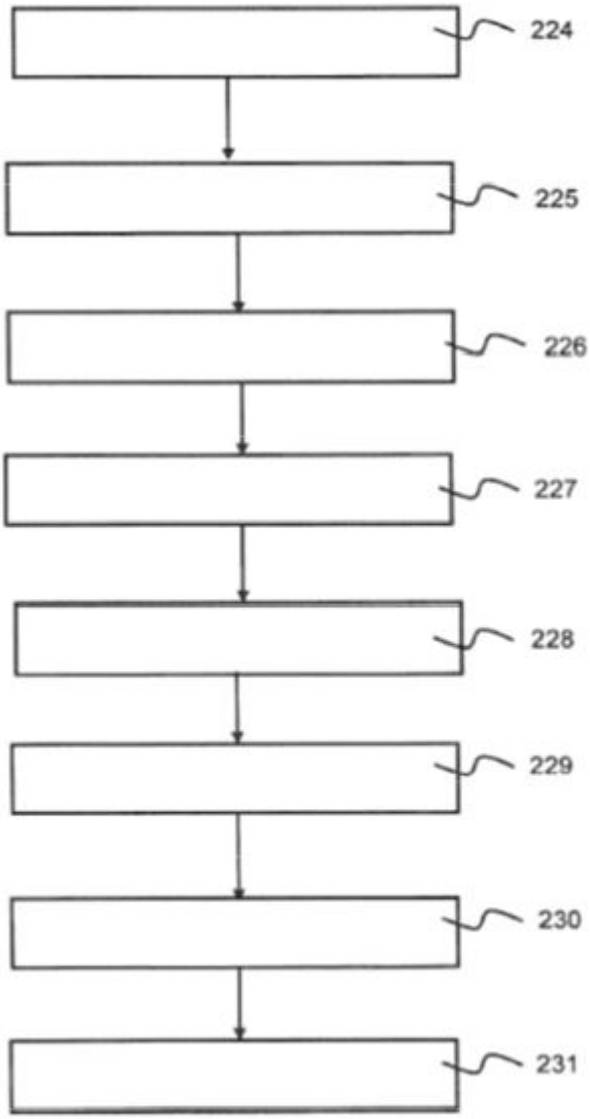

Figura 3d

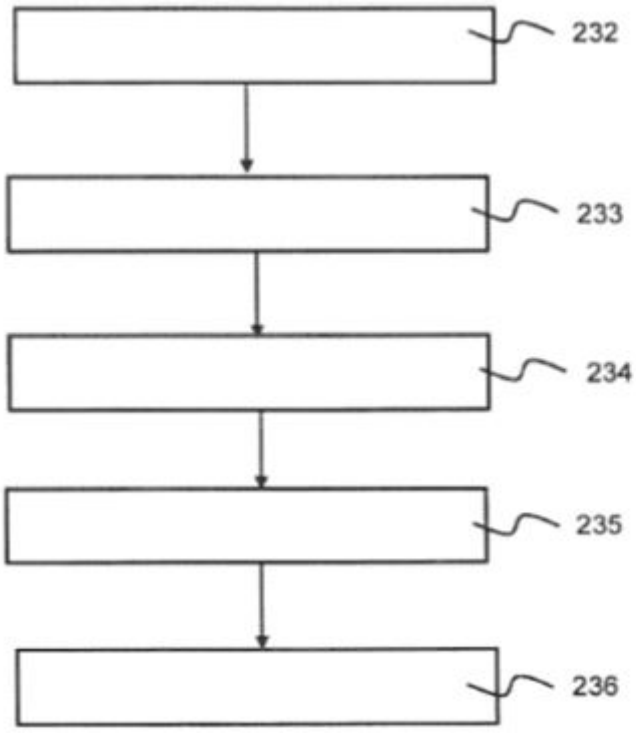

Figura 3e