(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 927 040**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/14 (2006.01)
H04L 9/32 (2006.01)
H04L 12/66 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.11.2020 E 20209836 (4)**

(97) Fecha y número de publicación de la concesión europea: **27.07.2022 EP 3829101**

(54) Título: **Procedimiento de protección de flujos de datos entre un equipo de comunicación y un terminal remoto, equipo que implementa el procedimiento**

(30) Prioridad:

29.11.2019 FR 1913458

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.11.2022

(73) Titular/es:

SAGEMCOM BROADBAND SAS (100.0%)
250, route de l'Empereur
92500 Rueil-Malmaison, FR

(72) Inventor/es:

KORBER, NICOLAS y
NGUYEN DINH HIEN, MICHAËL THIEN BAO

(74) Agente/Representante:

ANGOLOTI BENAVIDES, Joaquín

DESCRIPCIÓN

Procedimiento de protección de flujos de datos entre un equipo de comunicación y un terminal remoto, equipo que implementa el procedimiento

Campo técnico

La presente invención se refiere a dispositivos para redes informáticas. Más concretamente, la invención se refiere a la configuración remota de dispositivos de comunicación destinados a la conexión de dispositivos a una red informática, tales como puertas de enlace, por ejemplo.

Estado de la técnica

Es habitual que los dispositivos adaptados para permitir la conexión a una red informática, tales como una puerta de enlace de red, un rúter, un dispositivo de almacenamiento de datos o de impresión, a modo de ejemplos no limitativos, permitan la configuración remota de algunos de sus parámetros de funcionamiento. Esta configuración remota del dispositivo, realizada a través de un terminal de configuración remota, utiliza con frecuencia una interfaz de gestión para introducir o modificar parámetros útiles para el funcionamiento del dispositivo. Así, a modo de ejemplo, puede resultar útil ser capaz de conectarse a una puerta de enlace de acceso a Internet para configurar parámetros de funcionamiento como una lista de dispositivos clientes autorizados a conectarse, una configuración de red local inalámbrica, horarios de funcionamiento de una red local inalámbrica o incluso parámetros relativos al control parental de los accesos realizados. El terminal de configuración remota puede ser un ordenador, un smartphone, una tableta o cualquier otro dispositivo compatible en términos de protocolos de intercambio y configurado para conectarse al dispositivo que va a configurarse. La configuración remota de dispositivos utiliza frecuentemente un servidor integrado, conocido como "servidor web", que permite visualizar los parámetros modificables, desde un terminal de configuración, e introducir nuevos valores de parámetros a través de una interfaz gráfica (interfaz denominada “de usuario”) que se muestra en el terminal de configuración. La ventaja del uso a través de un servidor web que opera desde el dispositivo que se va a configurar es que es posible visualizar y modificar los parámetros de configuración desde un terminal de configuración remota, utilizando una aplicación cliente del servidor web, es decir, un navegador (conocido como "navegador de internet"). Si la configuración puede realizarse cuando el dispositivo configurable y el terminal de configuración están conectados por un enlace físico tal como una interfaz alámbrica que implementa un protocolo de comunicación Ethernet, por ejemplo, el uso masivo de conexiones inalámbricas, incluso en un contexto local, debilita la fiabilidad de los intercambios. Por lo tanto, incluso cuando se está físicamente cerca del dispositivo que se va a configurar, una conexión inalámbrica no segura no garantiza que el dispositivo de destino que realiza los intercambios con vistas a la configuración sea el dispositivo objetivo real y la suplantación de "identidad" sigue siendo posible. Por ejemplo, la suplantación de identidad puede llevarse a cabo desde un dispositivo de terceros, dentro del alcance del dispositivo que se va a configurar y del terminal de configuración. Este tipo de ataque es bien conocido y pone en práctica una técnica de usurpación llamada convencionalmente “ataque de intermediario” o “*man in the middle*” en inglés. Según esta técnica, el dispositivo de terceros, situado en el centro de los intercambios entre el dispositivo que se va a configurar y el terminal de configuración, se hace pasar por el dispositivo que va a configurar frente al terminal, y por el terminal, frente al dispositivo que se va a configurar. En esta configuración, ni el dispositivo que se va a configurar ni el terminal de configuración pueden detectar la presencia de un dispositivo central, capaz de recibir información sensible, y de hacer un mal uso de la misma. Para resolver este problema durante los intercambios en Internet, es habitual utilizar procedimientos de autenticación y cifrado destinados, por un lado, a garantizar que los intercambios se realicen efectivamente con un dispositivo objetivo y que puedan ser cifrados para evitar la interceptación por parte de un dispositivo de terceros de los datos sensibles que pasan entre dos dispositivos.

Existen técnicas para superar estas vulnerabilidades. Es posible, por ejemplo, crear un acceso seguro utilizando una parte de la red conocida como "DMZ", acrónimo del inglés "*Demilitarized Zone*" y que significa "zona desmilitarizada", combinada con un servidor de retransmisión, todo ello basado en un protocolo de intercambio seguro HTTPS entre un servidor web y un cliente web. El protocolo HTTPS y sus desarrollos utilizan intercambios seguros. HTTPs es un protocolo de transferencia de hipertexto seguro que utiliza una capa de cifrado. Sin embargo, esta solución requiere elementos de arquitectura de red adicionales para la implementación de la zona desmilitarizada y el servidor de retransmisión. Existe otra técnica que utiliza un enlace de comunicación paralela para enviar un mensaje de autenticación, como el envío de un SMS (acrónimo del inglés "*Short Message System*" y que significa "sistema de mensajes cortos").

Existen otras técnicas que tienen como objetivo utilizar servicios de terceros que proporcionan certificados de autenticidad para dispositivos que implementan un servidor web. El servicio de terceros distribuye certificados de autenticidad para los dispositivos que avala. Dichos certificados pueden ser verificados por dispositivos destinados a conectarse a un servidor web certificado, tal como un terminal de configuración, por ejemplo. Uno de los principales inconvenientes es que dicho certificado se emite en correspondencia con un nombre de dominio. Sin embargo, los dispositivos de conexión a una red informática, como, por ejemplo, una puerta de enlace, a menudo no están asociados con nombres de dominio. Estos dispositivos se identifican generalmente mediante una dirección IP

(acrónimo del inglés "*Internet Protocol*", que significa "protocolo de internet"), siendo esta dirección susceptible de ser modificada, en ocasiones periódicamente. Además, la implementación de un servicio de este tipo parece compleja para los dispositivos de conexión a una red ya implantados en el terreno y no diseñados de forma nativa para este fin. Por último, en ocasiones se requiere una configuración o reconfiguración según parámetros definidos de fábrica para los dispositivos de conexión a la red, lo que también dificultaría la implementación de la distribución de certificados por parte de un tercero en la medida en que volver a los parámetros establecidos de fábrica rompería la cadena de certificación creada y requeriría entonces una nueva certificación. La complejidad de la implementación de estos servicios de autenticación de terceros no es adecuada para proteger los intercambios entre los dispositivos de conexión de red ampliamente implantados en el terreno y los terminales. Además, dicho servicio no aborda el riesgo de suplantación de identidad en una red local no conectada a Internet y que utiliza conexiones inalámbricas. Por lo tanto, la situación es mejorable.

Divulgación de la invención

La presente invención tiene como objetivo, en particular, proteger la autenticación de los intercambios con un dispositivo de comunicación y la seguridad de los flujos de datos con ese mismo dispositivo, desde un terminal de configuración remota.

A tal efecto, el objeto de la invención es proponer un procedimiento de protección de flujos de datos en un dispositivo de comunicación que puede ser configurado desde un terminal de configuración remota, comprendiendo el procedimiento las etapas de:

- registrar una primera clave de cifrado en una memoria de dicho dispositivo (100),
- generar y registrar una segunda clave de cifrado, denominada clave privada, y una tercera clave de cifrado, denominada clave pública, insertándose la clave pública en un certificado de autenticidad firmado por la primera clave y pudiendo utilizarse la clave pública para el cifrado de un flujo de datos que pueden ser descifrados por medio de la clave privada,

- recibir, desde el terminal remoto, una solicitud con vistas a realizar intercambios seguros entre dicho dispositivo y el terminal remoto,
- verificar que dicha solicitud se recibe a través de dicha primera interfaz,
- si dicha solicitud se recibe a través de dicha primera interfaz, enviar, por medio dicho dispositivo, la clave pública al terminal remoto, en respuesta a la solicitud y habilitar la configuración remota de dicho dispositivo a través de al menos la segunda interfaz, a partir del flujo de datos cifrados mediante dicha clave pública.

De manera ventajosa, es posible, gracias a la transmisión de una clave pública que puede ser utilizada para el cifrado de un flujo de datos descifrables por medio de la clave privada, realizar una autenticación del dispositivo de comunicación que puede ser configurado de forma remota por el terminal de configuración. Para ello, con la clave pública se envía un certificado de autenticación, firmado por la primera clave. Este certificado de autenticación se genera al mismo tiempo que la clave pública. Este certificado contiene información tal como, por ejemplo, su vida útil, así como información representativa del equipo de comunicación que lo emite. De forma igualmente ventajosa, es posible utilizar la clave pública recibida para el cifrado de la totalidad o parte de los datos que se van a enviar al dispositivo de comunicación configurable de forma remota.

La expresión red local privada debe interpretarse aquí como una red de tipo LAN (acrónimo del inglés "*Local Area Network*") que conecta dispositivos u ordenadores en una misma área limitada, tal como una vivienda, un edificio o un edificio residencial, un una empresa, un laboratorio, una escuela o una universidad, en contraposición a una red de tipo WAN (acrónimo del inglés "*Wide Area Network"*) que conecta dispositivos u ordenadores ubicados en una gran área, normalmente una región, un país, un grupo de países, o incluso a escala planetaria, como Internet, por ejemplo.

En una red WAN, los dispositivos u ordenadores pueden estar conectados, respectivamente, a ramas de diferentes redes de tipo LAN y conectados entre sí mediante dispositivos intermedios como rúteres, nodos de conexión o puertas de enlace domésticas, por ejemplo.

El procedimiento según la invención también puede incluir las siguientes características, consideradas solas o en combinación:

- El procedimiento comprende una etapa de autenticación del dispositivo de comunicación frente al terminal de configuración remota o viceversa.
- El procedimiento comprende una etapa de cifrado de un flujo de datos que se va a transmitir, entre el dispositivo de comunicación y el terminal remoto, realizándose el cifrado mediante la clave pública.
- La etapa de envío de la clave pública al terminal de configuración remota comprende, además, enviar la clave pública a un dispositivo de almacenamiento remoto. Otro objeto de la invención es proporcionar un dispositivo de comunicación configurable desde un terminal remoto, estando configurado el dispositivo de comunicación para
- i) registrar una primera clave de cifrado en una memoria de dicho dispositivo,

- ii) generar y registrar una segunda clave de cifrado, denominada clave privada, y una tercera clave de cifrado, denominada clave pública, insertándose la clave pública en un certificado de autenticidad firmado por la primera clave, y pudiendo utilizarse la clave pública para el cifrado de un flujo de datos descifrables por medio de la clave privada,
- iii) recibir, del terminal remoto, una solicitud con vistas a realizar intercambios seguros entre dicho dispositivo y el terminal remoto a través de una red local privada,
- iv) enviar la clave pública desde dicho dispositivo al terminal remoto a través de una red local privada.

El dispositivo de comunicación también puede comprender una o más de las siguientes características, tomadas solas o en combinación:

- El dispositivo de comunicación está destinado a realizar funciones de puerta de enlace de conexión entre la red local y una red extendida.
- El dispositivo de comunicación está configurado para realizar una modificación de al menos un registro de configuración a partir de datos recibidos cifrados mediante la ejecución de un algoritmo de cifrado utilizando la clave pública y descifrados mediante la ejecución de un algoritmo de descifrado utilizando la clave privada.
- El dispositivo de comunicación está configurado para implementar un servidor web que permite la modificación de al menos un registro de configuración mediante el uso de una interfaz gráfica mostrada en el terminal remoto.
- La interfaz gráfica, controlada por el dispositivo de comunicación, está adaptada para introducir un comando de protección de flujos de datos entre el dispositivo de comunicación y el terminal de configuración remota.

Otro objeto de la invención es un sistema de comunicación que comprende un dispositivo de comunicación configurable de forma remota y un terminal de configuración remota, estando el dispositivo de comunicación y el terminal de configuración remota configurados para ser conectados a una misma red y para:

- registrar, por parte del dispositivo, una primera clave de cifrado en una memoria del dispositivo,
- generar y registrar, por parte del dispositivo, una segunda clave de cifrado, denominada clave privada, y una tercera clave de cifrado, denominada clave pública, insertándose la clave pública en un certificado de autenticidad firmado por la primera clave, y pudiendo utilizarse la clave pública para el cifrado de un flujo de datos que pueden ser descifrados por medio de la clave privada,
- recibir, por el dispositivo y desde el terminal de configuración, una solicitud con vistas a realizar intercambios seguros entre el dispositivo de comunicación y el terminal de configuración remota,
- verificar, mediante el dispositivo de comunicación, que la solicitud se recibe a través de la primera interfaz configurada para una conexión a una red local,
- si dicha solicitud se recibe a través de dicha primera interfaz, enviar, por medio del dispositivo de comunicación, la clave pública al terminal de configuración remota, en respuesta a la solicitud y habilitar la configuración remota del dispositivo de comunicación a través de al menos la segunda interfaz a partir de flujos de datos cifrados mediante la clave pública. La invención se refiere, además, a un producto de programa informático que comprende instrucciones de código de programa para ejecutar las etapas del procedimiento mencionado anteriormente, cuando el programa se ejecuta en un ordenador, así como a un dispositivo de almacenamiento de información que comprende dicho producto de programa informático. El término ordenador debe interpretarse aquí de manera amplia y aplicable a cualquier dispositivo electrónico que comprenda una unidad de control, uno o más módulos de memoria y uno o más módulos de interfaz de red adecuados para la conexión con dispositivos remotos tales como un terminal de configuración remota, además del conjunto habitual de circuitos útiles para el funcionamiento de los elementos mencionados (fuente de alimentación, circuitos de reinicio, circuitos de reloj, etc.).

Breve descripción de los dibujos

Las características mencionadas y otras características de la invención resultarán más evidentes a partir de la lectura de la siguiente descripción de al menos un ejemplo de realización, realizándose dicha descripción en relación con los dibujos adjuntos, entre los cuales:

La [Fig. 1] ilustra un dispositivo de comunicación que realiza funciones de puerta de enlace de acceso entre una primera red local privada LAN y una segunda red, implementando un procedimiento de protección de flujos de datos transmitidos entre un terminal de configuración remota y el dispositivo de comunicación, según una realización particular y no limitante de la invención.
La [Fig. 2] es una representación esquemática de la arquitectura del dispositivo de comunicación ya mostrado en la Fig. 1.
La [Fig. 3] es un diagrama que representa un procedimiento de protección de flujos de datos según la invención, implementado por el dispositivo de comunicación ya mostrado en la Fig. 1 y la Fig. 2.

Descripción detallada de realizaciones

La Fig. 1 ilustra un dispositivo de comunicación 100 adecuado para implementar funciones de puerta de enlace de interconexión entre una red 10 y una red local privada 120.

La red local privada 120 es una red de tipo LAN. Según una realización preferida de la invención, la red 10 es una red extendida de tipo WAN. Según una variante, la red 10 puede ser una red local de tipo LAN. El dispositivo de comunicación comprende una interfaz para la conexión inalámbrica a la red de tipo LAN 120 a través de un sistema de antena 124. Esta interfaz de conexión inalámbrica está configurada para el establecimiento de una conexión inalámbrica 122 entre el equipo de comunicación 100 y un ordenador remoto 140. La red LAN 120 está configurada para interconectar una pluralidad de dispositivos. Según el ejemplo descrito, la red LAN 120, de tipo local y privada, está configurada para interconectar el dispositivo de comunicación 100, el ordenador 130, el ordenador 140 y un terminal de configuración remota 150.

Así, el dispositivo de comunicación 100 que realiza funciones de puerta de enlace de red entre la red 100 y la red 10 permite, por ejemplo, el establecimiento de flujos de datos entre un dispositivo de almacenamiento de datos 11 conectado a la red extendida 10 y el ordenador 130 conectado a la red local privada 120. El terminal de configuración 150 es, por ejemplo, un ordenador configurado para ejecutar una aplicación de navegador web capaz de conectarse a un servidor web remoto identificado por su dirección IP o incluso por un nombre de dominio. Cuando el servidor web remoto es identificado por un nombre de dominio, el nombre de dominio es resuelto por un servidor de nombres de dominio remoto (servidor DNS, del inglés "*Domain Name Server*" y que significa "servidor de resolución de nombres de dominio") que no se muestra en el figura. El dispositivo de comunicación 100 que realiza funciones de puerta de enlace de red puede configurarse de forma remota. Ciertos parámetros de funcionamiento del dispositivo de comunicación 100 pueden modificarse cambiando los valores o datos accesibles a través de los registros de configuración. Estos datos son, por ejemplo, franjas horarias de funcionamiento de una interfaz wifi que permite una conexión inalámbrica desde un ordenador al dispositivo de comunicación 100 con vistas a acceder a servidores remotos accesibles a través de la red WAN 10. En otras palabras, se trata de definir, por ejemplo, franjas horarias que autoricen el acceso a Internet a uno o más ordenadores conectados a la red local privada 120. Estos datos se almacenan en una o más memorias no volátiles durante el apagado del dispositivo de comunicación 100. De este modo, puede restablecerse la configuración después de que el dispositivo de comunicación 100 se encienda de nuevo. La configuración del dispositivo de comunicación 100 se simplifica mediante la provisión de una interfaz de configuración, también denominada interfaz de gestión o interfaz de gestión de configuración, implementada en el dispositivo de comunicación 100, que funciona bajo el control de una unidad de control interna, en forma de un servidor web que implementa un protocolo de hipertexto no seguro (el protocolo HTTP, por ejemplo). El servidor web integrado en el dispositivo de comunicación 100 permite mostrar menús de configuración en forma de una interfaz gráfica de usuario en una pantalla del ordenador terminal de configuración remota 150 que ejecuta una aplicación de navegador web, conectada al servidor web de configuración del dispositivo de comunicación 100. Por ejemplo, un usuario que desee modificar los parámetros de funcionamiento del dispositivo de comunicación 100 utilizará la aplicación de navegador web del terminal de configuración remota 150 y se dirigirá al servidor web identificándolo por su dirección IP: 192.168.1.1. En efecto, la dirección IP 192.168.1.1 se define ampliamente como la que da acceso a los parámetros de configuración de un dispositivo de comunicación de tipo puerta de enlace de red que puede utilizarse para la interconexión de una red local privada LAN, alámbrica o inalámbrica, y una red extendida WAN.

Las diversas opciones de configuración del dispositivo de comunicación 100 se hacen así accesibles desde el terminal de configuración remota 150, a través de menús de configuración y campos de entrada representados e implementados a través de la interfaz gráfica mostrada en el navegador web del terminal de configuración remota 150. El terminal de configuración remota 150 comprende al menos una pantalla de visualización y una interfaz de entrada para introducir parámetros, como, por ejemplo, un teclado, un ratón, un lápiz óptico o incluso un dispositivo táctil, posiblemente combinado con la pantalla. Los menús de configuración se implementan mediante intercambios entre el servidor web del dispositivo de comunicación 100 y la aplicación de navegador web del terminal de configuración remota 150. Estos intercambios constituyen flujos de datos entre el dispositivo de comunicación 100 y el terminal de configuración remota 150. Según la realización preferida, los intercambios útiles para configurar el dispositivo de comunicación 100 se realizan según un protocolo de comunicación de hipertexto HTTP o cualquiera de sus desarrollos. Según una variante, la conexión entre el dispositivo de comunicación 100 y el terminal de configuración remota 150 se establece mediante la implementación de un protocolo de comunicación seguro de tipo SSH o cualquiera de sus desarrollos.

Según la realización preferida de la invención, la interfaz de configuración (o interfaz de gestión) comprende un campo de configuración adaptado a la implementación de un procedimiento de protección de flujos de datos entre el terminal de configuración 150 y el dispositivo de comunicación 100 en forma de una casilla de verificación combinada con una indicación de la función de la casilla de verificación (es decir, la implementación de la protección del flujo de datos). De manera ventajosa, la protección de flujos de datos implementada según la invención comprende la autenticación del dispositivo de comunicación 100 por el terminal de configuración 150 y el cifrado de los flujos de datos entre estos dos dispositivos para evitar los riesgos de interceptación de datos sensibles, y garantizar que el dispositivo al que está conectado el terminal de configuración 150 es realmente el dispositivo de comunicación 100 y no otro dispositivo, ubicado dentro del alcance del terminal de configuración 150 y/o el dispositivo de comunicación 100, y que realiza un ataque de intermediario.

El dispositivo de comunicación 100 comprende una primera clave de cifrado almacenada en una memoria interna no

volátil, reservada para este fin. Por ejemplo, la memoria interna está integrada en un circuito microcontrolador dedicado a una unidad de control del dispositivo de comunicación 100, de forma que sea imposible acceder a la clave. Esta clave de cifrado, denominada clave "raíz", se utiliza para firmar un certificado de autenticidad generado en el equipo de comunicación 100, que comprende un resumen obtenido a partir de información única del dispositivo de comunicación 100 y en el que se inserta la clave pública utilizada para futuras autenticaciones. La primera clave de cifrado puede haber sido programada de fábrica durante la fabricación del dispositivo de comunicación 100 o puede haber sido descargada durante una actualización de software de bajo nivel ejecutada por una unidad de control del dispositivo de comunicación 100 y que implementa, entre otras cosas, funciones de interconexión de dispositivos, específicas de una puerta de enlace de red entre una red LAN y una red WAN. Este software de bajo nivel se conoce comúnmente como "*firmware*".

A continuación, se describe una implementación de un procedimiento según la invención. Cuando un usuario del terminal de configuración 150, que desee poder realizar una configuración del dispositivo de comunicación 100, de manera segura, es decir, poder autenticar el dispositivo de comunicación 100 para evitar la usurpación "de 'identidad' por parte de un dispositivo de terceros, y cifrar los flujos de datos entre el terminal de configuración 150 y el dispositivo de comunicación 100, marca la casilla de entrada proporcionada en la interfaz gráfica de usuario con el fin de solicitar la protección de los flujos de datos. A continuación, se transmite un mensaje representativo de este comando al servidor web integrado en el dispositivo de comunicación 100, mensaje que constituye una solicitud con vistas a realizar intercambios seguros entre el dispositivo de comunicación 100 y el terminal de configuración remota 150. La solicitud se almacena en una memoria intermedia de la interfaz de gestión integrada en el dispositivo de comunicación 100 y se procesa inmediatamente después por la unidad de control del dispositivo de comunicación 100 que genera un par de claves e_c y d_d, respectivamente pública y privada, para el cifrado y descifrado de los flujos de datos entre el terminal de configuración remota 150 y el dispositivo de comunicación 100. La unidad de control genera entonces otro par de claves e_a y d_a, respectivamente pública y privada, posiblemente encadenadas con la primera clave denominada clave raíz, respectivamente utilizables para la autenticación del dispositivo de comunicación 100. Así, de acuerdo con el funcionamiento de los sistemas de cifrado de clave pública utilizados en criptografía asimétrica, si C es una función de cifrado predeterminada y D es una función de descifrado predeterminada, entonces, para cualquier mensaje m de un flujo de datos que se va a transmitir, m = C (D (m, d_d), c_e). De este modo se construye un esquema de firma a partir de este sistema criptográfico.

La firma de un mensaje m es s = D (h (m), d) donde h es una función hash pública, resistente a colisiones. La firma s puede verificarse comparando h (m) con C (s, e_c). De manera alternativa, puede utilizarse una función de redundancia en lugar de una función hash. La clave pública de autenticación e_a está integrada en un certificado de autenticación disponible para un usuario del terminal de configuración remota. El servidor web de la interfaz de gestión del dispositivo de comunicación 100 transmite un mensaje que solicita al usuario del terminal de configuración remota 150 que descargue este certificado e_a para su uso posterior. El certificado de autenticación (incluida la clave pública de autenticación e_a) se descarga y se registra en una memoria no volátil del terminal de configuración remota 150.

Según una variante, el procedimiento no se limita a un encadenamiento de un solo nivel y puede implicar una cadena de certificados, obtenidos de forma iterativa a partir de certificados creados previamente, para reforzar el procedimiento de autenticación.

Del mismo modo, la clave pública de cifrado e_c se transmite al terminal de comunicación remota 150 en respuesta al mensaje de solicitud de protección de flujos de datos entre el dispositivo de comunicación 100 y el terminal de configuración remota 150, previamente enviado por el terminal de configuración 150. La clave pública de cifrado e_c también se almacena en una memoria no volátil del terminal de configuración remota 150. La memoria del terminal de configuración remota 150 donde se almacena el certificado de autenticación e_a creado por el dispositivo de comunicación 100 corresponde, por ejemplo, a un "almacenamiento de certificados" del navegador web del terminal de configuración 150.

Las claves privadas, d_a y d_d respectivamente, necesarias para la autenticación del terminal de configuración 150 y/o del dispositivo de comunicación 100 y para el descifrado de los flujos de datos entre el terminal de configuración remota 150 y el dispositivo de comunicación 100 no se transmiten, sino que se almacenan de manera segura en el dispositivo de comunicación 100. Estas claves se almacenan, por ejemplo, en una partición de memoria dedicada, o se cifran localmente mediante un mecanismo de cifrado de hardware. Por ejemplo, el cifrado de hardware puede lograrse a través de un mecanismo de cifrado localizado implementado en un componente dedicado, almacenándose la versión cifrada de la clave luego en un área de memoria a la que no se puede acceder directamente, sino solo a través del módulo de cifrado/descifrado de claves. Tras la recepción y el registro del certificado de autenticación e_a y de la clave pública de cifrado e_c, puede lograrse un flujo de datos seguro entre el dispositivo de comunicación 100 y el terminal de configuración remota 150.

El certificado de autenticación e_a se crea a partir de uno o más elementos de información únicos del dispositivo de comunicación 100. Preferiblemente, el certificado de autenticación e_a se crea a partir de un gran número de elementos que tienden a hacer que el certificado de autenticación e_a sea único. Los elementos de información únicos utilizados para la generación del certificado de autenticación e_a son, a modo de ejemplos no limitativos: un número

de serie del dispositivo de comunicación 100, uno o más identificadores únicos de componentes electrónicos implementados en la arquitectura de hardware del dispositivo de comunicación 100 , un código que representa un país de uso y/o una región de uso del dispositivo de comunicación 100, una dirección IP vista desde la red WAN 10, una dirección de tipo MAC de una interfaz de red del dispositivo de comunicación 100, o incluso una cadena de caracteres que representan un correo electrónico de contacto almacenado en un área de memoria del dispositivo de comunicación 100.

Según una realización alternativa, los elementos de información introducidos por el usuario del terminal de configuración remota 150 con anterioridad a la generación del certificado de autenticación e_a son utilizados para su generación. Estos elementos de información son, por ejemplo, respuestas a preguntas predeterminadas. En el caso de que el establecimiento del certificado de autenticación e_a utilice información susceptible de cambiar, tal como una dirección IP, por ejemplo, será necesario generar un nuevo certificado. Cada nuevo certificado requerirá tener que implementar el procedimiento de protección según la invención.

De acuerdo con una segunda realización de la invención, se realiza un encadenamiento de certificados a dos o más niveles. Así, se crea un primer certificado de autenticación denominado “certificado de autenticación raíz” o “certificado raíz” y se crea un certificado de autenticación denominado “certificado de servicio”, encadenado al certificado raíz, para la gestión de la configuración. Según esta variante, es este certificado de servicio el que se transmitirá al terminal de configuración remota 150 tras la recepción de un mensaje de solicitud de protección de flujos de datos por parte del dispositivo de comunicación 100.

Según la invención, es imperativo que las etapas de recepción de una solicitud con vistas a proteger los flujos de datos entre el dispositivo de comunicación 100 y el terminal de configuración remota 150, transmitidos por el terminal de configuración remota 150, y el envío de la clave pública e_a utilizable para la autenticación, se ejecuten cuando los dos dispositivos están conectados a la misma red local privada. De hecho, esta característica garantiza la autenticidad del certificado y su posterior uso. Se entiende por conexión a la misma red local privada, una conexión punto a punto protegida contra la intrusión o interceptación de datos mediante el uso de un dispositivo de terceros. Tal conexión de los dos dispositivos, es decir, el dispositivo de comunicación 100 y el terminal de configuración remota 150 a la misma red local privada se realiza por ejemplo mediante un enlace físico que implementa una comunicación según un protocolo Ethernet o cualquiera de sus desarrollos, o incluso una conexión segura y cifrada a través de una red local inalámbrica privada segura.

De manera ventajosa, y gracias a la implementación del procedimiento según la invención, es posible iniciar comunicaciones seguras, implementando por ejemplo el protocolo HTTPS, inmediatamente después de la ejecución del procedimiento según la invención, o posteriormente, con el terminal configurable remotamente conectado al dispositivo de comunicación fuera de la misma red local privada. De manera ventajosa, el dispositivo de comunicación está configurado de forma nativa (a la salida de fábrica) para no permitir la configuración remota a través de su interfaz de conexión a la red WAN 10, y la transmisión de una clave pública desde el dispositivo de comunicación 100 al terminal de configuración 150 va acompañada de una reconfiguración del equipo de comunicación 100 destinada a permitir su posterior configuración remota a través de su interfaz de conexión a la red WAN 10, a partir de flujos de datos cifrados por la clave pública transmitida. Los intercambios que utilizan el protocolo HTTPS pueden entonces realizarse cuando el terminal de configuración remota 150 está conectado, por ejemplo, a otra red LAN privada, conectada a la red extendida WAN10 a través de una puerta de enlace distinta del dispositivo de comunicación 100. Así, cuando el terminal de configuración remota 150 está conectado a cualquier rama de Internet, puede establecer una conexión cifrada con el dispositivo de comunicación 100 por medio de su aplicación de navegador web y el servidor web integrado en el dispositivo de comunicación 100. El establecimiento de la conexión se realiza utilizando la dirección IP del dispositivo de comunicación 100 y un número de puerto dedicado a intercambios seguros, o utilizando un nombre de dominio resuelto por un servidor de nombres de dominio que traduce el nombre de dominio en una dirección IP. A continuación, el terminal de configuración remota 150 verifica la autenticidad del dispositivo de comunicación 100 utilizando el certificado de autenticación firmado por la clave raíz (primera clave), y la clave pública e_a. La autenticación del dispositivo de comunicación 100 por parte del terminal de configuración remota 150 utiliza el descifrado de un resumen cifrado insertado en el certificado transmitido al terminal de configuración remota 150, utilizando la propia clave pública insertada en el certificado. El resumen es una huella digital obtenida mediante una función hash. Durante la autenticación del dispositivo de comunicación 100, el resumen descifrado se compara con los resúmenes obtenidos a partir de información única relacionada con el dispositivo de comunicación 100. Si los dos resúmenes son idénticos, se considera que el certificado de autenticación es auténtico, es decir que efectivamente ha sido firmado por la clave raíz del equipo de comunicación 100. Una vez que el dispositivo de comunicación 100 es autenticado por el terminal de configuración remota 150, se implementa un canal de comunicación cifrada entre el terminal de configuración 150 y el dispositivo de comunicación 100. Para ello, los flujos de datos que se van a transmitir se cifran utilizando la clave pública e_c antes de su envío al dispositivo de comunicación 100 y se descifran a su recepción, por el dispositivo de comunicación 100, utilizando la clave privada d_d.

La **Fig. 2** ilustra la arquitectura interna del equipo de comunicación 100 configurado para realizar funciones de puerta de enlace de red entre la red WAN 10 y la red LAN 120. El dispositivo de comunicación 100 comprende una unidad de control 111. La unidad de control 111 comprende un circuito electrónico configurado para ejecutar funciones

habituales de puerta de enlace entre dos redes. Según una realización preferida de la invención, la unidad de control comprende un microprocesador. La unidad de control 111 está conectada a un módulo de memoria no volátil 113 por medio de un bus compartido 112. El módulo de memoria 113 comprende áreas de memoria dedicadas al almacenamiento de códigos de software ejecutables correspondientes a las funciones implementadas por el equipo de comunicación 100. Un módulo de memoria de acceso aleatorio 115 también está conectado a la unidad de control 111 por medio del bus compartido 112, y se utiliza, en particular, para la ejecución de los códigos de software antes mencionados. La unidad de control 111, el módulo de memoria no volátil 113 y el módulo de memoria de acceso aleatorio 115 están, por tanto, conectados entre sí a través del bus compartido 112, al que también están conectadas una interfaz de conexión 119 a una red LAN y una interfaz de conexión 114 a una red WAN de área amplia. La interfaz de conexión 119 es, por ejemplo, una interfaz cableada de tipo Ethernet. Tal interfaz Ethernet proporciona un alto nivel de seguridad, especialmente cuando el terminal de configuración remota 150 se conecta directamente al equipo de comunicación 100 a través de esta interfaz por medio de un cable. La interfaz de conexión 119 a una red LAN también está conectada a un módulo de comunicación inalámbrica 118 que comprende el sistema de antena 124. Tal interfaz también aporta un alto nivel de seguridad, cuando se establece una conexión directa con el terminal de configuración remota 150, mediante un cifrado. El módulo de memoria no volátil 113 comprende un conjunto de áreas dedicadas a la configuración del equipo de comunicación 100. Estas áreas contienen valores de parámetros útiles para configurar el equipo de comunicación 100 según varios modos de funcionamiento. Cada uno de los parámetros puede modificarse reescribiendo el área de memoria no volátil que le corresponde. La modificación de un parámetro puede realizarse bajo el control de la unidad de control 111, en particular cuando la unidad de control ejecuta la interfaz de gestión de la configuración del equipo de comunicación 100.

Cuando la unidad de control 111 ejecuta la interfaz de gestión de la configuración del equipo de comunicación 100, ejecuta funciones de servidor web adaptadas para mostrar una página web, dedicada a la configuración, en un terminal remoto tal como el terminal de configuración 150 conectado al dispositivo de comunicación 100 a través de la interfaz de conexión 119 (red LAN) o la interfaz de conexión 114 (red WAN). Según una realización preferida de la invención, el equipo de comunicación 100 está configurado de forma nativa para que la configuración remota solo pueda realizarse a través de la interfaz de red 119 o la interfaz de red 118 que implementa una comunicación segura (cifrada), y esto hasta la ejecución del procedimiento de protección de flujos de datos según la invención. En otras palabras, la configuración remota del equipo de comunicación 100 a través de una red WAN conectada a la interfaz de red WAN se inhibe durante la configuración de la puerta de enlace de red en fábrica, o durante el retorno a una llamada configuración "de fábrica".

El equipo de comunicación 100 está así adaptado a la ejecución del procedimiento de protección de flujos de datos según la invención.

La **Fig. 3** es un diagrama de flujo que ilustra un procedimiento de protección de flujos de datos entre el equipo de comunicación 100 y el terminal de configuración remota 150 según una realización particular y no limitativa de la invención. Una inicialización general del dispositivo de comunicación 100 tiene lugar durante una etapa S0. Durante esta inicialización general, el dispositivo de comunicación 100 está configurado para poder realizar un conjunto de funciones útiles para la implementación de una puerta de enlace de red entre una primera red de tipo LAN conectada a la interfaz de red 119, y una segunda red, de tipo LAN o tipo WAN conectada a la interfaz de red 117. Al final de esta etapa, el equipo de comunicación es capaz, después de una fase de puesta en marcha, de ejecutar funciones de puerta de enlace de red y de ejecutar una interfaz de gestión de configuración remota mediante la implementación de un servidor web de configuración, accesible a través de la interfaz de conexión de red LAN 119. En esta fase, el equipo de comunicación 100 no puede configurarse de forma segura a distancia a través de su interfaz de red 114, ya que esta función está inhibida de forma nativa. Durante una etapa S1 se realiza el registro de una primera clave de cifrado, denominada clave raíz. Según una realización de la invención, este registro se lleva a cabo durante la fabricación en fábrica. Según una variante, este registro de clave raíz se realiza mediante descarga, durante una operación de configuración segura posterior a la fabricación, tal como una operación de mantenimiento, por ejemplo.

A continuación, se realiza una primera generación de un par de claves privada/pública durante una etapa S2, así como una segunda generación de claves privada/pública durante una etapa S3. El primer par de claves se proporciona para operaciones de autenticación y el segundo par de claves se proporciona para operaciones de cifrado. Estas generaciones de pares de claves públicas y privadas se realizan, por ejemplo, cuando el equipo de comunicación 100 se enciende por primera vez o incluso más tarde durante una operación de configuración, reconfiguración o mantenimiento.

La ejecución de la interfaz de gestión de configuración tiene lugar durante una etapa S4, cuando el terminal de configuración remota 150 se conecta al servidor web de configuración del equipo de comunicación 100, a través de la interfaz de red 119. Esta ejecución se lleva a cabo mediante el intercambio de mensajes de protocolo, por ejemplo, según el protocolo HTTP, y permite la visualización de una página web de configuración del equipo de comunicación 100 en una pantalla del terminal de configuración 150. La página web de configuración está adaptada para implementar menús de configuración, permitiendo la definición de parámetros de configuración almacenados en registros de configuración del equipo de comunicación 100 o en las áreas de memoria no volátil dedicadas a este

fin. Normalmente, la página web permite que un usuario que maneja el terminal de configuración remota 150 seleccione parámetros y ajuste sus valores respectivos. Según una realización preferida de la invención, la página web de configuración también permite activar o desactivar funciones marcando casillas de verificación asociadas a una descripción de la función. Así, la página web incluye una función que puede activarse marcando una casilla y que se titula "protección de flujos de datos para configuración remota".

Cuando un usuario del terminal de configuración remota 150 solicita la activación de la protección de flujos de datos entre el terminal de configuración remota 150 y el equipo de comunicación 100, marcando la casilla en la página web de configuración, el terminal de configuración 150 envía una solicitud HTTP al equipo de comunicación 100, con vistas a solicitar la protección de intercambios posteriores mediante operaciones de autenticación y cifrado de flujos de datos, hasta que una reconfiguración habilite eventualmente de nuevo los intercambios no seguros.

A continuación, el equipo de comunicación recibe la solicitud de protección de flujos de datos durante una etapa S5.

De forma inteligente, el equipo de comunicación 100 comprueba, al recibir la solicitud con vistas a proteger los flujos de datos entre el equipo de configuración remota y él mismo, si la solicitud se ha recibido a través de la interfaz de red LAN 119 o la interfaz de red WLAN 118, o bien a través de la interfaz de red 114, que puede ser utilizada para la conexión a una red extendida de tipo WAN.

Si la solicitud se ha recibido a través de la interfaz de red LAN 119, y a través de un puerto Ethernet 116, es decir, una conexión por cable que refleja un alto nivel de seguridad, el equipo de comunicación 100 transmite, en respuesta a la solicitud, las claves públicas de cifrado y autenticación al terminal de configuración remota 150. De lo contrario, el equipo de comunicación no transmite las claves públicas y dirige un mensaje de error a través de la página web de la interfaz de gestión de configuración, destinado a indicar que no es posible proteger los flujos de datos. Según una realización alternativa, el equipo de comunicación 100 comprueba, en caso de que la solicitud con vistas a proteger los flujos de datos no se haya recibido a través de la interfaz de red LAN 119 y el puerto Ethernet 116, si la solicitud se ha recibido a través de la interfaz de red WLAN 118 que realiza intercambios cifrados con el terminal de configuración remota 150. Según esta variante, el equipo de comunicación 100 considera que los intercambios con el terminal de configuración 150 se realizan con un nivel de seguridad suficientemente alto y transmite, en respuesta a la solicitud, las claves públicas de cifrado y autenticación al terminal de configuración remota 150. En su defecto, el equipo de configuración dirige un mensaje de error a través de la página web de la interfaz de gestión de configuración, destinado a indicar que no es posible proteger los flujos de datos. En el caso de que no se permita la protección de flujos de datos y no se envíen las claves públicas, el equipo de comunicación se posiciona en espera de una nueva solicitud de configuración remota. Esta nueva solicitud puede ser una solicitud con vistas a proteger los flujos de datos u otra solicitud de configuración.

Además de la transmisión de las claves públicas de cifrado y autenticación, el equipo de comunicación 100 se reconfigura, bajo el control de la unidad de control 111 que ejecuta el procedimiento según la invención, para habilitar una configuración remota a través de la interfaz de red 114, que puede configurarse para la conexión a una red extendida de tipo WAN.

Según una variante de realización de la invención, las claves públicas de autenticación y cifrado también se transmiten a un dispositivo de almacenamiento remoto tal como el dispositivo de almacenamiento 11, configurado para almacenar claves públicas de cifrado. El dispositivo de almacenamiento remoto está configurado, además, para establecer una conexión remota segura con un terminal de configuración remota que no tiene las claves públicas de autenticación y cifrado y está configurado para descargar estas claves desde el dispositivo de almacenamiento 11.

De manera ventajosa, la transmisión de las claves públicas de autenticación y cifrado al terminal de configuración remota 150 permite al terminal de configuración remota 150 autenticar el equipo de comunicación durante una conexión posterior y cifrar los flujos de datos al equipo de comunicación 100, con el fin de evitar cualquier ataque de tipo ataque de intermediario durante las operaciones de configuración remota. Según una realización de la invención, el o los certificados transmitidos al terminal de configuración remota 150, y la o las claves públicas relacionadas, pueden ser revocados y una nueva ejecución del procedimiento de protección según la invención es entonces requerida y hecha posible a través de la interfaz de configuración gráfica implementada por el servidor web del dispositivo de comunicación 110. De manera ventajosa, la reconfiguración de la dirección IP del dispositivo de comunicación 100 o la modificación de los parámetros de un servidor DNS dinámico de destino del dispositivo de comunicación 100, conduce a la nueva ejecución del procedimiento de protección de flujos de datos según la invención.

Según una realización de la invención, una reconfiguración en modo salida de fábrica no borra el o los certificados transmitidos, ni la o las claves públicas transmitidas y un comando dedicado permite proceder a su borrado, con independencia de la reconfiguración en modo salida de fábrica.

Según una realización de la invención, puede realizarse una copia de seguridad de todos los parámetros en un medio interno o externo al dispositivo de comunicación 110 e incluir el o los certificados, así como la o las claves públicas transmitidas.

La invención no se limita únicamente a las realizaciones descritas anteriormente y se aplica, de forma más general, a cualquier procedimiento de protección de flujos de datos en un dispositivo de comunicación configurable desde un terminal remoto, comprendiendo el procedimiento las etapas de registrar una primera clave de cifrado en una memoria del dispositivo, generar, en el dispositivo de comunicación, a partir de la primera clave, una clave pública y una clave privada correspondiente a la clave pública, y luego recibir una solicitud de protección enviada por el terminal remoto y enviar la clave pública desde el dispositivo de comunicación al terminal remoto, en respuesta a la solicitud de protección, siendo las operaciones de recepción de la solicitud así como de transmisión de la clave pública necesariamente realizadas cuando el dispositivo y el terminal están conectados a la misma red local privada. La invención se refiere a cualquier dispositivo que implemente dicho procedimiento.

REIVINDICACIONES

1. Procedimiento de protección de un flujo de datos entre un dispositivo de comunicación (100) y un terminal remoto (150), comprendiendo dicho dispositivo de comunicación (100) una primera interfaz de comunicación (118, 119) para la conexión a una primera red local (120) de tipo LAN, y una segunda interfaz de comunicación (114) para la conexión a una segunda red (10), siendo dicho dispositivo (100) configurable desde el terminal remoto (150), y comprendiendo el procedimiento las etapas de:

- registrar, mediante dicho dispositivo de comunicación (100), una primera clave en una memoria de dicho dispositivo (100),
- generar y registrar, mediante dicho dispositivo (100), una segunda clave de cifrado, denominada clave privada, y una tercera clave de cifrado, denominada clave pública, insertándose la clave pública en un certificado de autenticidad firmado por la primera clave y pudiendo utilizarse la clave pública para el cifrado de un flujo de datos que pueden ser descifrados por medio de la clave privada,
- recibir, desde el terminal remoto (150), una solicitud con vistas a proteger los flujos de datos entre dicho dispositivo de comunicación (100) y el terminal remoto (150),
- verificar que dicha solicitud se recibe a través de dicha primera interfaz (118, 119) para una conexión a una primera red local (120) de tipo LAN, y
- si dicha solicitud se recibe a través de dicha primera interfaz (118, 119) para una conexión a una primera red local de tipo LAN, enviar, por medio de dicho dispositivo de comunicación (100), la clave pública al terminal remoto (150), en respuesta a la solicitud, y habilitar la configuración remota de dicho dispositivo de comunicación (100) a través de al menos dicha segunda interfaz (114) a partir del flujo de datos cifrados mediante dicha clave pública.

2. Procedimiento según la reivindicación anterior, comprendiendo el procedimiento una etapa de autenticación de dicho dispositivo (100) frente al terminal remoto (150) o viceversa.

3. Procedimiento según una de las reivindicaciones 1 o 2, comprendiendo el procedimiento una etapa de cifrado de un flujo de datos que se va a transmitir entre dicho dispositivo (100) y el terminal remoto (150), realizándose el cifrado mediante dicha clave pública.

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, comprendiendo la etapa de enviar la clave pública al terminal remoto (150), además, el envío de la clave pública a un dispositivo de almacenamiento remoto (11).

5. Dispositivo de comunicación (100) configurable desde un terminal remoto (150), comprendiendo dicho dispositivo de comunicación (100) una primera interfaz de comunicación (118, 119) para la conexión a una primera red local (120) de tipo LAN, y un segunda interfaz de comunicación (114) para la conexión a una segunda red (10), estando configurado dicho dispositivo de comunicación (100) para:

- registrar una primera clave en una memoria de dicho dispositivo (100),
- generar y registrar una segunda clave de cifrado, denominada clave privada, y una tercera clave de cifrado, denominada clave pública, insertándose dicha clave pública en un certificado de autenticidad firmado por la primera clave, pudiendo utilizarse la clave pública para el cifrado de un flujo de datos que pueden ser descifrados por medio de la clave privada,
- recibir, desde el terminal remoto (150), una solicitud con vistas a realizar intercambios seguros entre dicho dispositivo de comunicación (100) y el terminal remoto (150),
- verificar que dicha solicitud se recibe a través de dicha primera interfaz (118, 119) para la conexión a una primera red local de tipo LAN, y
- si dicha solicitud se recibe a través de dicha primera interfaz (118, 119) para la conexión a una primera red local (120) de tipo LAN, enviar, por medio de dicho dispositivo de comunicación (100), la clave pública al terminal remoto (150), en respuesta a la solicitud y habilitar una configuración remota de dicho dispositivo de comunicación (100) a través de al menos dicha segunda interfaz (114) a partir del flujo de datos cifrados mediante dicha clave pública.

6. Dispositivo de comunicación (100) según la reivindicación anterior, estando destinado dicho dispositivo (100) a ejecutar funciones de puerta de enlace de conexión entre dicha red local (120) de tipo LAN y una red extendida (10) de tipo WAN.

7. Dispositivo de comunicación (100) según una de las reivindicaciones 5 a 6, configurado para realizar una modificación de al menos un registro de configuración a partir de los datos recibidos cifrados mediante la ejecución de un algoritmo de cifrado utilizando la clave pública y descifrables mediante la ejecución de un algoritmo de descifrado utilizando la clave privada.

8. Dispositivo de comunicación (100) según una cualquiera de las reivindicaciones 5 a 7, configurado para implementar un servidor web que permite modificar al menos un registro de configuración mediante el uso de una

interfaz gráfica visualizada en el terminal remoto (150).

9. Dispositivo según la reivindicación anterior, estando la interfaz gráfica adaptada para introducir un comando para proteger los flujos de datos entre dicho dispositivo de comunicación (100) y el terminal remoto (150).

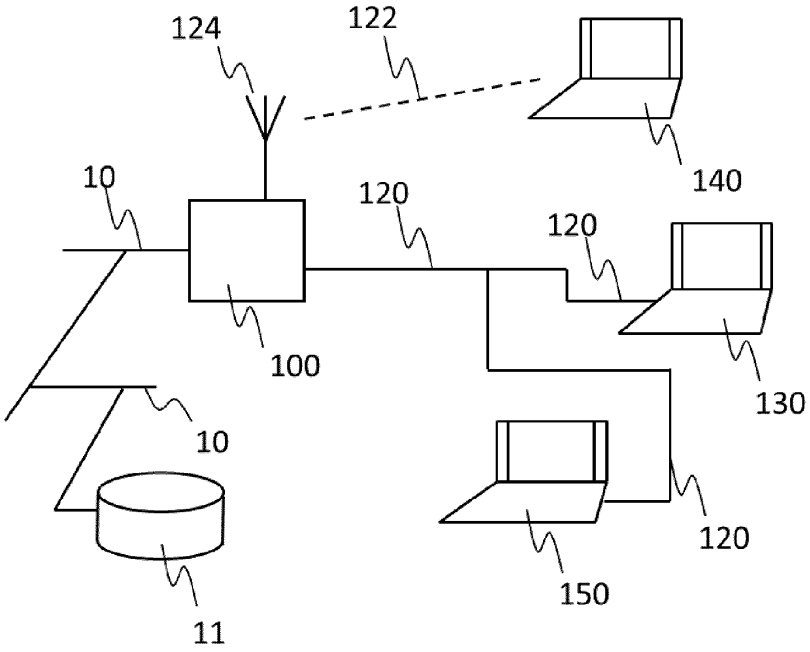
10. Sistema de comunicación que comprende un dispositivo de comunicación (100) configurable de forma remota y un terminal de configuración (150), comprendiendo dicho dispositivo de comunicación (100) una primera interfaz de comunicación (118, 119) para la conexión a una primera red local (120) de tipo LAN, y una segunda interfaz de comunicación (114) para la conexión a una segunda red (10), siendo dicho dispositivo de comunicación (100) configurable desde el terminal remoto (150), y estando dicho dispositivo (100) y el terminal de configuración (150) configurados para estar conectados a la misma red y para:

- registrar, mediante dicho dispositivo de comunicación (100), una primera clave de cifrado en una memoria de dicho dispositivo (100),
- generar y registrar, mediante dicho dispositivo (100), una segunda clave de cifrado, denominada clave privada, y una tercera clave de cifrado, denominada clave pública, insertándose la clave pública en un certificado de autenticidad firmado por la primera clave, pudiendo utilizarse la clave pública para el cifrado de un flujo de datos que pueden ser descifrados por medio de la clave privada,
- recibir, mediante dicho dispositivo de comunicación (100) y desde el terminal de configuración (150), una solicitud con vistas a realizar intercambios seguros entre dicho dispositivo de comunicación (100) y el terminal de configuración (150),
- verificar, mediante el dispositivo (100), que la solicitud se recibe a través de dicha primera interfaz (118, 119) para una conexión a la primera red local (120) de tipo LAN,
- si dicha solicitud se recibe a través de dicha primera interfaz para la conexión a una primera red local (120) de tipo LAN, enviar, por medio de dicho dispositivo de comunicación (100), la clave pública al terminal remoto (150), en respuesta a la solicitud, y habilitar una configuración remota de dicho dispositivo (100) a través de al menos dicha segunda interfaz (117) a partir de flujos de datos cifrados mediante dicha clave pública.

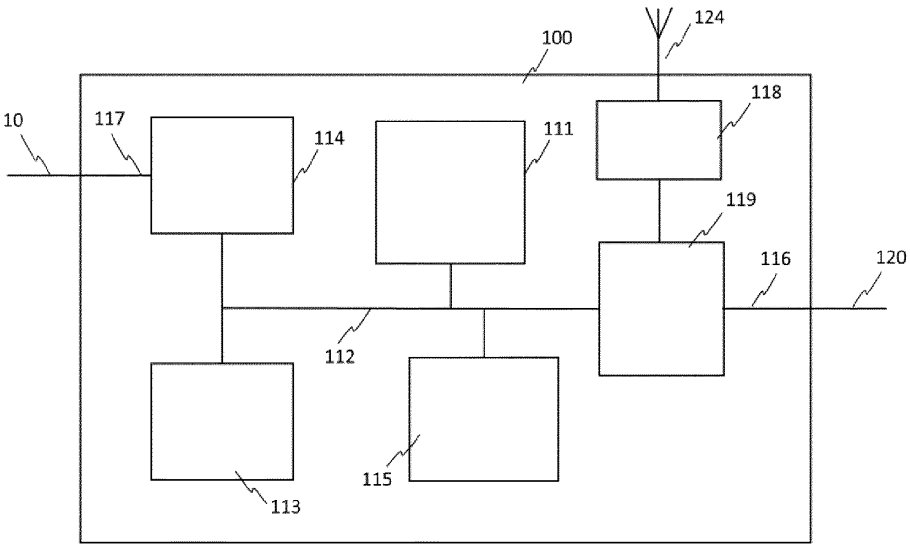
11. Producto de programa informático, **caracterizado por que** comprende instrucciones de código de programa para ejecutar las etapas del procedimiento según la reivindicación 1, cuando dicho programa se ejecuta en un ordenador.

12. Medio de almacenamiento de información, que comprende un producto de programa informático según la reivindicación anterior.

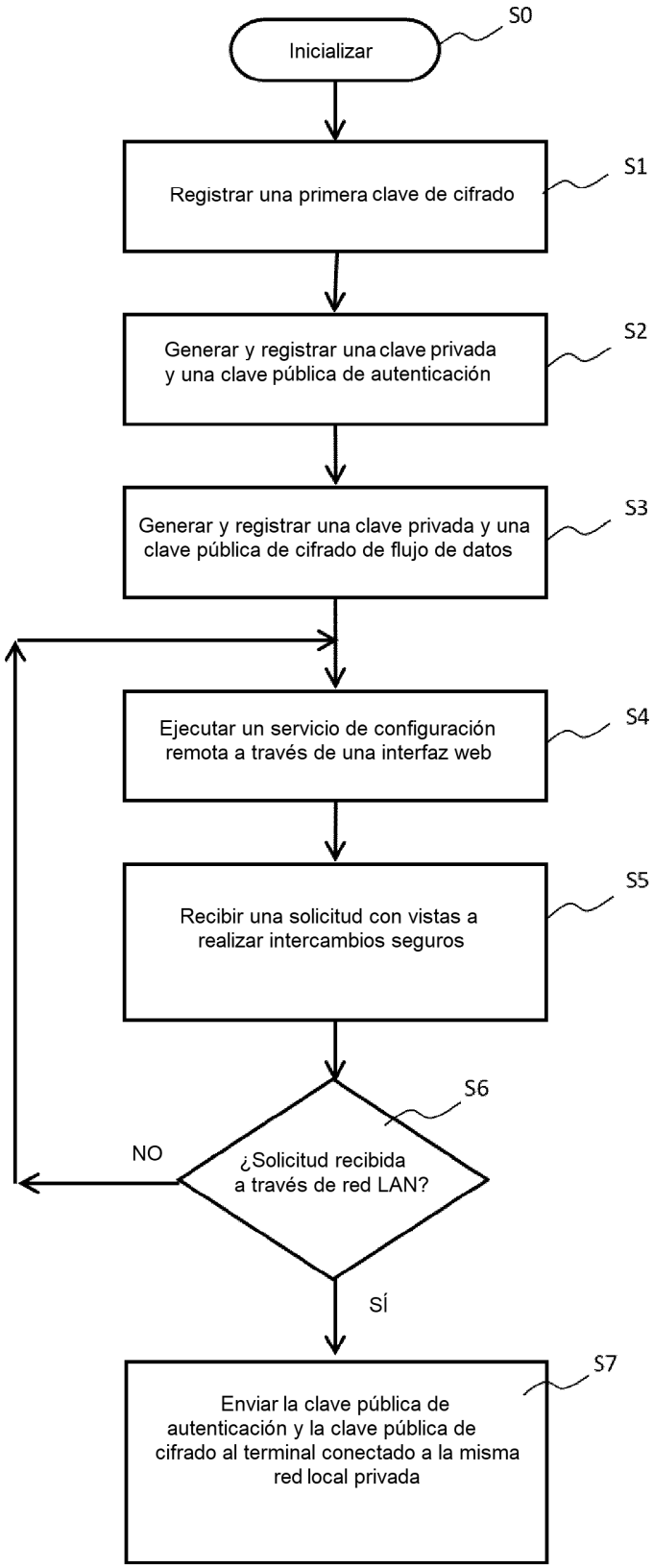
[Fig. 1]


124
122
140
10
120
120
100
130
10
120
150
11

[Fig. 2]


100
124
118
10
117
114
111
119
116
120
112
115
113

[Fig. 3]


S0
Inicializar
Registrar una primera clave de cifrado
S1
Generar y registrar una clave privada y una clave pública de autenticación
S2
Generar y registrar una clave privada y una clave pública de cifrado de flujo de datos
S3
Ejecutar un servicio de configuración remota a través de una interfaz web
S4
Recibir una solicitud con vistas a realizar intercambios seguros
S5
S6
¿Solicitud recibida a través de red LAN?
NO
SÍ
Enviar la clave pública de autenticación y la clave pública de cifrado al terminal conectado a la misma red local privada
S7