(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 029 641**

(51) Int. CI.:

H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.07.2019 E 19186690 (4)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2025 EP 3767909**

(54) Título: **Procedimiento y unidad de comunicaciones para la transmisión de datos unidireccional, protegida criptográficamente, de datos útiles, entre dos redes**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.06.2025

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.00%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

FALK, RAINER;
SELTZSAM, STEFAN;
SEUSCHEK, HERMANN y
WIMMER, MARTIN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento y unidad de comunicaciones para la transmisión de datos unidireccional, protegida criptográficamente, de datos útiles, entre dos redes

La presente invención hace referencia a un procedimiento para la transmisión de datos unidireccional, protegida criptográficamente, de datos útiles (por ejemplo datos de un dispositivo de campo) entre una primera red con un primer requisito de seguridad y una segunda red con un segundo requisito de seguridad, distinto en comparación con la primera red, así como a una unidad de comunicaciones correspondiente y producto de programa informático.

Para la comunicación segura entre una red crítica en cuanto a la seguridad y una abierta, como por ejemplo una red de control industrial (en inglés Industrial Control Network u Operational Network) y una red TI clásica, por ejemplo, pueden utilizarse unidades de comunicaciones unidireccionales, como por ejemplo diodos de datos, para permitir una transmisión de datos unidireccional, libre de interacción. Un diodo de datos con canal de feedback, también denominada como guardia de red bidireccional o pasarela de seguridad, posibilita una transferencia de datos segura entre dos áreas de información con niveles de seguridad diferentes. Una guardia de red en general es una combinación de hardware y software, y permite más funcionalidad que los cortafuegos, debido a lo que puede alcanzarse una mayor protección que en el caso de los cortafuegos convencionales. En particular, la ausencia de interacción puede garantizarse basada en hardware, de manera que esa propiedad se mantenga incluso en caso de un mal funcionamiento del software.

Una guardia de red bidireccional en general está estructurada para realizar dos flujos de datos unidireccionales, separados uno de otro, respectivamente mediante un diodo de datos, donde los flujos de datos circulan en dirección opuesta. Esto permite un intercambio de datos en ambas direcciones, donde respectivamente está garantizada la función unidireccional. Por ejemplo, con una guardia de red bidireccional pueden transmitirse datos desde una primera red con requisito de seguridad elevado, a una segunda red abierta con un requisito de seguridad menor, o desde la red con requisito de seguridad menor a una red con requisito de seguridad elevado. El requisito de seguridad en particular puede referirse a la integridad y/o a la disponibilidad y/o a la confidencialidad. En las redes de control industriales a menudo existen requisitos de seguridad extremadamente elevados en cuanto a la integridad y a la disponibilidad, que también deben cumplirse de manera fiable en el caso de un acoplamiento a una red de fábrica, una red de oficina o una red pública.

En el caso de una transferencia de datos desde la red con requisito de seguridad menor a la red con requisito de seguridad elevado, en general se requiere una prueba adicional para garantizar la integridad y/o la seguridad de la red con requisito de seguridad elevado y/o la disponibilidad de la red.

Entre un dispositivo, por ejemplo un dispositivo de campo en la primera red, y una unidad de comunicaciones en la segunda red, no puede implementarse una encriptación de extremo a extremo convencional, por ejemplo con protocolos de seguridad como IKEv2/IPsec o TLS. La razón de esto reside en que mediante la vía de transferencia unidireccional no puede establecerse un contexto de sesión, por ejemplo mediante mecanismos de handshake (de apretón de manos) habituales.

Por parte del dispositivo deben utilizarse protocolos de pasarela unidireccionales especiales. Es decir, que los protocolos utilizados hasta el momento (por ejemplo MQTT), deben reemplazarse para la utilización de la vía unidireccional y deben implementarse mediante el proxy de protocolo. Una integración de la conexión a la red unidireccional (por ejemplo mediante una unidad de captura de datos, DCU), de este modo, no es posible sin adaptar la implementación y la pila de protocolos del dispositivo.

Por la solicitud DE 10 2017 212 474 A1 se conoce un procedimiento para verificar parámetros de conexión, en el que durante el establecimiento de una conexión de comunicaciones protegida criptográficamente, entre un primer dispositivo de comunicaciones y un segundo dispositivo de comunicaciones, (i) una estructura de datos de certificación que contiene al menos un parámetro de conexión del primer y/o segundo dispositivo de comunicaciones como información de certificación, desde los primeros y/o segundos dispositivos de comunicaciones se envía al segundo y/o primer dispositivo de comunicaciones, (ii) la estructura de datos de certificación es escuchada por un dispositivo de monitorización dispuesto dentro de la vía de transmisión de datos de la conexión de comunicaciones, y (iii) la información de certificación se controla con respecto a una directiva predeterminada.

Por la solicitud DE 10 2015 200 279 A1 se conoce un procedimiento para la detección de datos libre de interacción que se transmiten, protegidos criptográficamente, entre dispositivos en una primera red con requisito de seguridad elevado, y que son escuchados por un dispositivo de transmisión unidireccional en una segunda red con requisito de seguridad menor. En este caso, (i) al menos un parámetro criptográfico se negocia entre los dispositivos que se comunican en la primera red, para la utilización en una comunicación subsiguiente,

(ii) se genera una estructura de transmisión en al menos uno de los dispositivos en el que están contenidos, al menos parcialmente, los parámetros criptográficos negociados, y se transmite dentro de la primera red, y (iii) la estructura de datos de transmisión es escuchada por un dispositivo de transmisión unidireccional y se transmite a la segunda red.

Conforme a ello, un objeto de la presente invención consiste en crear una solución mejorada en comparación con el estado de la técnica mencionado en la introducción, para una transmisión de datos unidireccional entre dos redes con un requisito de seguridad diferente.

El objeto se soluciona mediante las medidas descritas en las reivindicaciones independientes. En las reivindicaciones dependientes se presentan perfeccionamientos ventajosos de la invención. En la presente invención se reivindica un procedimiento para la transmisión de datos unidireccional, protegida criptográficamente, de datos útiles (por ejemplo datos del dispositivo de campo), en particular entre una primera red con un primer requisito de seguridad y una segunda red con un segundo requisito de seguridad, distinto en comparación con la primera red,

donde uno o varios paquetes de datos que comprenden los datos útiles, en una vía de transmisión de datos de extremo a extremo, desde una primera unidad de comunicaciones (por ejemplo cliente) en una primera red, mediante una unidad de comunicaciones unidireccional (por ejemplo DCU), que está dispuesta entre la primera red y una segunda red, se transmiten a una segunda unidad de comunicaciones en la segunda red,

el cual presenta las siguientes etapas del procedimiento:

I. determinación o negociación de al menos un parámetro criptográfico entre la primera unidad de comunicaciones y una tercera unidad de comunicaciones en la primera red para la transmisión de datos protegida criptográficamente, preferentemente unidireccional, de datos útiles, desde la primera unidad de comunicaciones a la segunda unidad de comunicaciones,

II. generación de al menos una estructura de datos de transmisión en la que están contenidos, al menos parcialmente, los parámetros criptográficos negociados para la transmisión de datos, protegida criptográficamente, del paquete de datos o en varios paquetes de datos,

III. encriptación de al menos una estructura de datos de transmisión con una clave (preferentemente clave pública) de la segunda unidad de comunicaciones,

IV. transmisión de al menos una estructura de datos de transmisión encriptada a la segunda unidad de comunicaciones en la segunda red,

V. desencriptado de al menos una estructura de transmisión encriptada,

VI. encriptación de los datos útiles que deben transmitirse a la segunda unidad de comunicaciones, con los parámetros criptográficos negociados, y transmisión de los datos útiles encriptados a la segunda unidad de comunicaciones, y

VII. desencriptado de los datos útiles transmitidos con los parámetros criptográficos contenidos en la estructura de transmisión desencriptada.

La etapa I puede realizarse entre la primera unidad de comunicaciones y una unidad de comunicaciones virtual en la primera red, preferentemente en la primera unidad de comunicaciones. El parámetro criptográfico representa o comprende un parámetro de sesión que comprende una clave de sesión criptográfica (en inglés session key).

La etapa VI puede ser realizada mediante la unidad de comunicaciones unidireccional. La encriptación denomina aquí una protección criptográfica en la que la integridad de los datos útiles está protegida por una suma de verificación criptográfica (código de autenticación de mensaje, firma digital) o en la que los datos útiles están encriptados, o en la que la integridad y la confidencialidad de los datos útiles están protegidas por una encriptación autentificada (en inglés authenticated encryption).

Una tercera unidad de comunicaciones virtual puede estar dispuesta aguas arriba de la unidad de comunicaciones unidireccional que realiza las etapas II, III y IV de la reivindicación 1. (La primera unidad de comunicaciones también puede efectuar la etapa II y/o III y/o IV).

En la vía de transmisión parcial entre la primera unidad de comunicaciones y la tercera unidad de comunicaciones puede utilizarse el protocolo de transmisión de datos Datagram Transport Layer Security, abreviado como DTLS.

Otra unidad de comunicaciones dispuesta aguas arriba de la segunda unidad de comunicaciones puede realizar la etapa V con ayuda de los parámetros criptográficos de la estructura de transmisión (la segunda unidad de comunicaciones puede efectuar la etapa VI, así como VII).

Al menos un parámetro criptográfico resulta del acuerdo de autentificación y de clave, y puede comprender una clave de sesión, un conjunto de cifrado, un token de seguridad, una firma y/o certificado. El acuerdo de autentificación y de clave, preferentemente, tiene lugar entre la primera unidad de comunicaciones, utilizando una credencial (certificado, clave privada o secreta) de la primera unidad de comunicaciones, y una tercera unidad de comunicaciones virtual, utilizando una seudo-credencial. La seudo-credencial es una credencial en general conocida, que en particular también es conocida para la segunda unidad de comunicaciones. Se utiliza para realizar un protocolo de autentificación y de intercambio de clave bidireccional convencional, de forma local (en el primer dispositivo o al menos con un dispositivo previo a la unidad de comunicaciones unidireccional). En función de los mensajes de protocolo intercambiados al realizar el protocolo de autentificación y de intercambio de clave bidireccional, se forma la estructura de datos de transmisión y se encripta con una credencial privada de la segunda unidad de comunicaciones. Gracias a esto se logra que después de la transmisión mediante la unidad de comunicaciones unidireccional, sólo la segunda unidad de comunicaciones pueda desencriptar la estructura de transmisión encriptada. Sin embargo, mediante la primera unidad de comunicaciones puede utilizarse un protocolo de autentificación y de intercambio de clave bidireccional, para finalmente establecer una clave de sesión con la unidad de comunicaciones que puede alcanzarse sólo de forma unidireccional.

El procedimiento según la invención preferentemente está configurado implementado por ordenador. Por "implementado por ordenador", con relación a la invención, puede entenderse una implementación del procedimiento en la cual en particular un ordenador realiza al menos una etapa del procedimiento.

En la invención se prevé que un dispositivo IoT/ dispositivo de campo pueda efectuar una transmisión de datos unidireccional protegida de extremo a extremo, mediante una vía de comunicaciones unidireccional, a un servidor de destino (backend IoT, pasarela de borde IoT), donde una clave de sesión se establece de forma dinámica. En este caso no se necesita otra adaptación de un protocolo de transmisión. Los paquetes (de datos) transmitidos están protegidos criptográficamente, de modo que puede lograrse una protección de extremo a extremo. Junto con la seguridad mejorada de la transmisión de datos, esto ofrece la ventaja adicional de que puede utilizarse una unidad de comunicaciones unidireccional muy sencilla y, debido a ello, poco compleja, y fiable. Además, la misma clase de transmisión puede tener lugar independientemente de si se encuentra presente o no una unidad de comunicaciones unidireccional. Por tanto, una unidad de comunicaciones unidireccional, en caso necesario, también puede equiparse posteriormente de manera sencilla.

Para ello, el protocolo de seguridad DTLS (DTLS Security Protocol) puede emplearse de manera que éste pueda utilizarse estrictamente de forma unidireccional. Esa característica de DTLS también puede denominarse como UDTLS (DTLS unidireccional).

De este modo, los datos útiles pueden transmitirse criptográficamente, protegidos en base a una información de contexto de sesión existente. El desafío reside en que el contexto de sesión DTLS (en particular clave de sesión criptográfica, conjunto de cifrado seleccionado, opciones de protocolo) debe inicializarse al establecerse la sesión (session establishment).

Los protocolos de comunicaciones seguros convencionales se pueden continuar utilizando para encriptar datos útiles (en particular una capa de registro DTLS o alternativamente SRTP (secure real-time transport protocol, protocolo de transporte en tiempo real) o IKEv2/IPsec (internet key exchange, IP security, intercambio de claves de Internet, seguridad IP).

Esos datos pueden transmitirse directamente, es decir, sin conversión de protocolo y, con ello, directamente, mediante una vía de comunicaciones unidireccional (por ejemplo diodo de datos, cortafuegos configurado de manera restrictiva, que por ejemplo bloquea todos los paquetes de datos que ingresan).

Un dispositivo de transmisión es adecuado para la transmisión de datos unidireccional, protegida criptográficamente, de datos útiles, entre una primera red y una segunda red, donde uno o varios paquetes de datos que comprenden los datos útiles, en una vía de transmisión de datos de extremo a extremo, desde una primera unidad de comunicaciones en la primera red, se transmiten a una segunda unidad de comunicaciones en la segunda red, el cual presenta:

- una unidad de puesta a disposición para proporcionar o generar al menos una estructura de datos de transmisión en la que están contenidos (los) parámetros criptográficos negociados al menos de forma parcial, para la transmisión de datos protegida criptográficamente,

- una unidad de encriptación para encriptar al menos una estructura de datos de transmisión con una clave (pública) de una segunda unidad de comunicaciones en la segunda red,

- una unidad de transmisión para transmitir al menos una estructura de datos de transmisión encriptada a la segunda unidad de comunicaciones en la segunda red,

- una unidad de encriptación para encriptar los datos útiles que deben transmitirse a la segunda unidad de comunicaciones con los parámetros criptográficos negociados (con una o con la unidad de comunicaciones virtual antes mencionada), y para transmitir los datos útiles encriptados a la segunda unidad de comunicaciones (mediante una primera unidad de comunicaciones en la primera red o en esa unidad de comunicaciones virtual).

Según otro aspecto, la invención hace referencia a una disposición que comprende el dispositivo de transmisión de la clase antes mencionada y el dispositivo de desencriptado de la clase antes mencionada, que adicionalmente presenta:

- al menos una unidad de sesión de comunicaciones para determinar o negociar al menos un parámetro criptográfico, para la transmisión de datos, protegida criptográficamente, de datos útiles, desde la primera unidad de comunicaciones a otra unidad de comunicaciones.

Una disposición que comprende la unidad de comunicaciones antes mencionada y la unidad de comunicaciones virtual antes mencionada, adicionalmente presenta:

- al menos una unidad de sesión de comunicaciones para determinar/negociar al menos un parámetro criptográfico, para la transmisión de datos, protegida criptográficamente, de datos útiles, desde la primera unidad de comunicaciones a otra unidad de comunicaciones.

Una unidad de comunicaciones unidireccional es adecuada para la transmisión de datos unidireccional, protegida criptográficamente, mediante los datos útiles, entre una primera red con un primer requisito de seguridad y una segunda red con un segundo requisito de seguridad, distinto en comparación con la primera red, que comprende un dispositivo de transmisión de la clase antes mencionada.

Una unidad o componente, en particular una unidad de comunicaciones o un componente de red, en particular puede estar diseñado como un componente de hardware. Un componente en particular puede comprender un procesador. Un procesador en particular puede tratarse de un procesador principal (en inglés central processing unit, CPU), de un microprocesador o de un microcontrolador, por ejemplo de un circuito integrado de forma específica en cuanto a la aplicación, o de un procesador de señal digital, probablemente en combinación con una unidad de almacenamiento para almacenar comandos de programa, etc. Un procesador por ejemplo puede tratarse también de un IC (circuito integrado, en inglés integrated circuit), o de un módulo multi-chip, en particular de una FPGA (en inglés field programmable gate array, matriz de puertas lógicas programable en campo), o de un ASIC (circuito integrado para aplicaciones específicas, en inglés application-specific integrated circuit), de un SoC (sistema en un chip), de un procesador gráfico GPU (graphics processing unit, unidad de procesamiento de gráficos), de un procesador para evaluar una red neuronal, como por ejemplo una TPU (tensor processing unit, unidad de procesamiento tensorial) o de un DSP (procesador de señal digital, en inglés digital signal processor). El procesador puede presentar uno o varios núcleos informáticos (multi-núcleo). Por un procesador puede entenderse también un procesador virtualizado o un microprocesador soft (de núcleo suave). Por ejemplo, también puede tratarse de un procesador programable que está provisto de las etapas de configuración para realizar el procedimiento según la invención mencionado, o que está configurado con etapas de configuración, de manera que el procesador programable implementa las características según la invención del procedimiento u otros aspectos y aspectos parciales de la invención. El procesador puede presentar una protección de terminal tamper para la protección contra manipulaciones físicas, por ejemplo sensores de terminal tamper para la detección de ataques físicos.

Además, la invención hace referencia a un producto de programa informático que puede cargarse directamente en un ordenador programable, que comprende partes de código de programa que son adecuadas para realizar las etapas de un procedimiento implementado por ordenador según la invención.

Un producto de programa informático, como por ejemplo un medio de programa informático, puede proporcionarse o suministrarse como medio de almacenamiento o soporte de datos, como por ejemplo como

tarjeta de memoria, memoria USB, CD-ROM, DVD o también en forma de un archivo que puede descargarse desde un servidor en una red.

En los dibujos, a modo de ejemplo, se representan ejemplos de ejecución del procedimiento implementado por ordenador según la invención y del dispositivo de transmisión, y se explican en detalle mediante la siguiente descripción. Muestran:

Figura 1: una representación esquemática de la interacción de las unidades de comunicaciones o dispositivos según la invención; y

Figura 2: un diagrama de operaciones de un procedimiento según la invención.

En todas las figuras, las partes que se corresponden unas a otras están provistas de los mismos símbolos de referencia.

En particular, los siguientes ejemplos de ejecución muestran solamente posibilidades de realización a modo de ejemplo, en particular de cómo podrían verse las realizaciones de esa clase de la teoría según la invención, ya que es imposible y tampoco es efectivo o necesario para la compresión de la invención enumerar todas esas posibilidades de realización.

Además, en particular para un experto que conoce la/s reivindicación/reivindicaciones relativas al procedimiento, naturalmente son conocidas todas las posibilidades habituales en el estado de la técnica para la realización de la invención, de manera que en particular no se requiere una revelación separada en la descripción. En particular, esas variantes de realización habituales y conocidas por el experto pueden realizarse exclusivamente por (componentes de) hardware o exclusivamente por (componentes de) software. De manera alternativa y/o adicional, el experto, en el marco de su habilidad profesional, puede seleccionar en gran medida cualquier combinación según la invención de (componentes de) hardware y (componentes de) software, para implementar variantes de realización según la invención.

La Figura 1 muestra la interacción de las unidades de comunicaciones según la invención.

A modo de ejemplo, están representadas dos redes NW1 y NW2. En este caso, la red NW1 puede presentar un requisito de seguridad diferente en comparación con la segunda red NW2. La red NW1, por ejemplo, puede corresponder a una red de fábrica y la red NW2 puede ser una red remota para diagnóstico, por ejemplo para un mantenimiento predictivo de los componentes/unidades de la red NW1. En la red NW 1 se encuentra una primera unidad de comunicaciones FD que puede estar diseñada como dispositivo de campo o dispositivo IOT, donde el dispositivo de campo comprende una unidad o componente de cliente C, que por ejemplo puede estar diseñado a modo de una unidad de sesión de comunicaciones. Esa unidad de sesión de comunicaciones puede comprender al menos un parámetro criptográfico, para una transmisión de datos, protegida criptográficamente, de datos útiles PL (payload, carga útil), desde la primera unidad de comunicaciones a otra unidad de comunicaciones. La otra o tercera unidad de comunicaciones, en este caso, preferentemente será una unidad de comunicaciones virtual vSrv. Además, en la red NW2 se encuentra una segunda unidad de comunicaciones que puede estar configurada como servidor retirado (remoto) rSrv.

Por tanto, en la etapa 1 indicada, un handshake HS (por ejemplo DTLS-handshake, DTLS = datagramm transport layer security), es decir, el texto de comunicación y/o uno o varios parámetros criptográficos, se negocian o determinan con una unidad de comunicaciones virtual local vSrv. De este modo, tiene lugar una comunicación bidireccional. Esto tiene lugar mediante el transmisor, aquí la primera unidad de comunicaciones C, un handshake DTLS con un punto del extremo DTLS o servidor virtual, en el ejemplo la unidad de comunicaciones virtual vSrv, que preferentemente está implementada en el mismo hardware que el cliente C. Sin embargo, también puede utilizarse un módulo de seguridad de hardware conectado al cliente C u otro nodo de comunicaciones. En este caso, para la autenticación del servidor virtual puede utilizarse una seudo-credencial en general conocida. La misma no se utiliza aquí solamente para la autenticación efectiva del punto del extremo DTLS, sino que se encuentra presente de forma virtual para poder realizar un handshake DTLS (bidireccional). En todas las formas de ejecución, la unidad de comunicaciones vSrc está dispuesta aguas arriba de una unidad de comunicaciones unidireccional DCU, por ejemplo una pasarela unidireccional, un diodo de datos o también una DCU (unidad de captura de datos sin interacción http://www.siemens.com/dcu), es decir que el handshake DTLS, desde la perspectiva técnica, tiene lugar localmente, sin transmitirse mediante la unidad de comunicaciones unidireccional.

Sin embargo, un handshake registrado o en general una información formada en función de ello, como información de handshake rSrv, mediante la unidad de comunicaciones unidireccional, se transmite al servidor rSrv, de manera que el servidor rSrv puede desencriptar los datos útiles PL (capa de registro) transmitidos igualmente al mismo. Para ello, un par de claves en general conocido (clave pública PubK y clave privada PK)

se utiliza para la unidad de comunicaciones virtual vSrv. Además, para la unidad de comunicaciones virtual vSrv puede utilizarse un parámetro criptográfico en general conocido, como valor aleatorio Diffie-Hellman. La unidad de comunicaciones virtual vServ reúne tanto las funciones del cliente C, así como las funciones de un servidor DTLS, estableciendo así una sesión DTLS "consigo misma". Gracias a esto, las implementaciones DTLS que se encuentran presentes pueden utilizarse sin adaptaciones especiales.

Una información de la sesión DTLS (DTLSSession), así como del handshake DTLS, se transmite de forma unidireccional ahora al cliente C y al servidor de destino efectivo (rSrv), en el ejemplo la segunda unidad de comunicaciones rSrv. Un dispositivo de sesión de comunicaciones implementado preferentemente en el cliente C (no representado de forma explícita en la figura) puede generar y/o proporcionar una estructura de datos de transmisión, registrada como información de handshake HSInfo. La información de handshake HSInfo esencialmente contiene la información del intercambio de claves (handshake) entre el cliente C y la unidad de comunicaciones virtual vSrv.

Preferentemente, la información de handshake HSInfo es encriptada mediante una unidad de encriptación, no representada de forma explícita, en la unidad de comunicaciones virtual vSrv y/o mediante el cliente C, firmada de forma digital, se transmite al servidor de destino propiamente dicho, en el ejemplo el servidor rSrv. Para la encriptación se utiliza una clave pública rSrv o un certificado digital del cliente C. La firma puede realizarse mediante los nodos de puesta a disposición (el transmisor, por ejemplo cliente C, o la unidad de comunicaciones virtual vSrv) o mediante ambos.

En una forma de ejecución, se registra la información de handshake HsInfo Variante, se organiza por completo en una estructura de datos de transmisión y se transmite a la segunda unidad de comunicaciones rSrv de forma unidireccional. En otra forma de ejecución, no se transmite toda la información de handshake HSInfo, sino el contexto de sesión de seguridad que resulta de ello (por ejemplo clave de sesión, conjunto de cifrado). Preferentemente, la información de handshake HSInfo, inmediatamente después de la finalización del handshake DTLS, se transmite a la segunda unidad de comunicaciones rSrv. En una forma de ejecución, otra información de handshake HS-Info se transmite después de una actualización de clave de sesión DTLS (session-key-update). Lo mencionado ofrece la ventaja de que con la información de handshake los datos DTLS encriptados (registros) pueden desencriptarse de forma directa. En otra forma de ejecución, HS-Info se transmite con retardo de tiempo a la segunda unidad de comunicaciones rSrv. Lo mencionado puede suceder después de que haya finalizado la sesión DTLS entre el cliente C y la unidad de comunicaciones virtual vSrv, y/o después de que haya tenido lugar una actualización de clave. Esto ofrece la ventaja de que la segunda unidad de comunicaciones rSrv sólo puede desencriptar los datos posteriormente, es decir, que durante la transmisión de datos encriptada entre el cliente C y la unidad de comunicaciones virtual vSrv, los datos no pueden escucharse ni manipularse.

El punto del extremo propiamente dicho, en el ejemplo la segunda unidad de comunicaciones, recibe la información de handshake y establece el contexto de sesión de seguridad acordado por el cliente C con la unidad de comunicaciones virtual vSrv. Es decir, que el mismo establece un contexto de sesión DTLS que corresponde a la información de handshake HSInfo recibida. Debido a esto, puede desencriptar los datos útiles recibidos y comprobar su integridad.

El envío de los datos útiles encriptados preferentemente es realizado por la unidad de comunicaciones virtual vSrv en dirección de la segunda unidad de comunicaciones rSrv. Lo mencionado ofrece la ventaja de que en la primera unidad de comunicaciones puede utilizarse un cliente C regular, no modificado. Se necesita solamente una unidad de comunicaciones especial vSrv en el dispositivo (de campo) FD, que junto con la información de handshake HSInfo, recibe los datos útiles encriptados (capa de registro DTLS) y, sin un procesamiento, los reenvía al receptor propiamente dicho, en el ejemplo, la segunda unidad de comunicaciones rSrv. Puesto que el dispositivo FD realiza ambas funciones (cliente C y unidad de comunicaciones virtual vSrv), la transmisión encriptada de un registro DTLS desde el transmisor (C) al receptor propiamente dicho (rSrv), está protegida de extremo a extremo.

Mediante la sesión DTLS en particular pueden transmitirse de forma segura mensajes de protocolo IoT, como por ejemplo mensajes publish MQTT o mensajes CoAP.

En otra forma de ejecución, la unidad de comunicaciones virtual vSrv se realiza en un ordenador separado como componente central en la instalación (red de fábrica). Con ello, varios dispositivos de campo FD, mediante la unidad de comunicaciones virtual vSrv, pueden enviar datos como proxy a la segunda unidad de comunicaciones rSrv. El proxy, de ese modo, también puede realizar otra funcionalidad útil como NAT (para el reenvío a la segunda unidad de comunicaciones rSrv). La ventaja esencial de esa forma de ejecución reside en que no debe adaptarse la implementación por parte del dispositivo de campo y pueden alcanzarse efectos de escala. No obstante, la vía de transmisión entre la primera red (por ejemplo red de fábrica), desde la unidad

de comunicaciones virtual vSrv y el receptor propiamente dicho (segunda unidad de comunicaciones rSrv) está protegida de extremo a extremo.

La Figura 2 muestra un diagrama de operaciones de un procedimiento según la invención, donde las etapas individuales están identificadas con las cifras 11 a 25.

El dispositivo (de campo) FD que envía está configurado con una dirección (dirección IP, nombre DNS, URL) del servidor de destino, en el ejemplo la segunda unidad de comunicaciones rSrv, y una clave criptográfica asociada, en el ejemplo una clave pública rSrv PubK, un certificado digital vSrv cert y una clave privada vSrv PK. Además, el dispositivo de campo FD puede presentar un certificado de cliente FD cert y una clave de cliente FD PK.

En el dispositivo de campo FD puede estar implementada una unidad de comunicaciones virtual vSrv. La misma utiliza parámetros criptográficos. El cliente C propiamente dicho, como cliente DTLS, establece una sesión DTLS para su unidad de comunicaciones virtual interna vSrv (véase la etapa 11). La misma puede estar autenticada de forma bilateral desde la perspectiva de protocolo DTLS HS (también es posible una autenticación unilateral o incluso ninguna autenticación). Como resultado, está establecido un contexto de sesión de seguridad en común (por ejemplo clave de sesión y conjunto de cifrado en correspondencia con la información de handshake HSInfo) para el cliente DTLS y la unidad de comunicaciones virtual (véase la etapa 12). La información de handshake HSInfo se encripta con la clave pública rSrv PubK de la segunda unidad de comunicaciones rSrv (etapa 13) y se transmite a la misma (etapa 14 y 15). Preferentemente, además, está firmada por el cliente, es decir, con su clave privada FD PK. Otra unidad de comunicaciones virtual en la segunda unidad de comunicaciones rSrv desencripta la información de handshake HSInfo (etapa 16) y establece el contexto de sesión de seguridad con la HSInfo desencriptada (etapa 17), (etapa 18).

Después de esa fase de establecimiento se encuentra presente el contexto de sesión de seguridad (correspondiente a la HSInfo) en la otra unidad de comunicaciones virtual de la segunda unidad de comunicaciones rSrv. Si ahora el cliente del dispositivo de campo FD envía un paquete de datos (etapa 19), entonces éste puede enviarse encriptado (etapa 20) a la segunda unidad de comunicaciones rSrv (etapa 22, 23) y allí puede desencriptarse (etapa 24) y procesarse (etapa 25). Lo particular reside en que tiene lugar una comunicación estrictamente unidireccional entre el dispositivo de campo FD y la segunda unidad de comunicaciones rSrv. Una pasarela unidireccional (DCU, unidad de captura de datos) guía solamente el paquete de datos o los paquetes de datos desde el dispositivo de campo FD (etapa 21) a la segunda unidad de comunicaciones rSrv, pero no en la dirección opuesta.

En una forma de ejecución, para la negociación de la sesión DTLS (handshake DTLS) se utiliza una clave precompartida secreta (conjunto cifrado PSK). En otra forma de ejecución tiene lugar un handshake DTLS no autenticado.

Si bien la invención fue ilustrada y descrita en detalle mediante el ejemplo de ejecución preferente, la invención no está limitada por los ejemplos descritos, y el experto puede deducir de éstos otras variaciones, sin abandonar el alcance de protección de la invención.

La implementación de los procesos antes descritos o de secuencias del procedimiento, puede tener lugar mediante instrucciones que se encuentran en medios de almacenamiento legibles por ordenador o en memorias del ordenador volátiles (a continuación, de forma resumida, denominados como memorias legibles por ordenador). Las memorias legibles por ordenador, por ejemplo, son memorias volátiles como caché, memorias tampón o RAM, así como memorias no volátiles, como medios de almacenamiento extraíbles, discos duros, etc.

Las funciones o etapas antes descritas pueden estar presentes en forma de al menos un conjunto de instrucciones dentro de/en una memoria legible por ordenador. Las funciones o etapas no están asociadas a un conjunto de instrucciones determinados, a una forma determinada de conjuntos de instrucciones, a un medio de almacenamiento determinado, a un procesador determinado o a esquemas de ejecución determinados, y pueden realizarse mediante software, firmware, microcódigo, hardware, procesadores, circuitos integrados, etc., en un funcionamiento individual o en cualquier combinación. De este modo, pueden emplearse las más diversas estrategias de procesamiento, por ejemplo procesamiento serial mediante un procesamiento individual, multiprocesamiento, multitarea o procesamiento paralelo, etc.

Las instrucciones pueden estar almacenadas en memorias locales, pero también es posible almacenar las instrucciones en un sistema separado y acceder a la mismas mediante la red.

El dispositivo de transmisión puede presentar uno o varios procesadores. El término "procesador", "procesamiento de señales central", "unidad de control" o "medio de evaluación de datos" abarca medios de

procesamiento en el sentido más amplio, por tanto, por ejemplo, servidores, procesadores universales, procesadores gráficos, procesadores de señales digitales, circuitos integrados para aplicaciones específicas (Asdics), circuitos lógicos programables como FPGA, circuitos discretos analógicos o digitales y cualquier combinación de los mismos, incluyendo todos los otros medios de procesamiento conocidos por el experto o desarrollados en el futuro. Los procesadores pueden componerse de uno o de varios dispositivos, equipos o unidades. Si un procesador se compone de varios dispositivos, los mismos pueden estar diseñados o configurados para el procesamiento o la realización de forma paralela o secuencial de instrucciones.

REIVINDICACIONES

1. Procedimiento para la transmisión de datos unidireccional, protegida criptográficamente, de datos útiles, donde

uno o varios paquetes de datos que comprenden los datos útiles, en una vía de transmisión de datos de extremo a extremo, desde una primera unidad de comunicaciones (C) en una primera red (NW1), mediante una unidad de comunicaciones unidireccional (DCU), que está dispuesta entre la primera red (NW1) y una segunda red (NW2), se transmiten a una segunda unidad de comunicaciones (rSrv) en la segunda red (NW2),

el cual presenta las siguientes etapas del procedimiento:

I. negociación de al menos un parámetro criptográfico entre la primera unidad de comunicaciones (C) y una tercera unidad de comunicaciones (vSrV) en la primera red (NW1) para la transmisión de datos protegida criptográficamente, de datos útiles, desde la primera unidad de comunicaciones a la segunda unidad de comunicaciones,

II. generación de al menos una estructura de datos de transmisión (HSinfo) en la que están contenidos, al menos parcialmente, los parámetros criptográficos negociados para la transmisión de datos, protegida criptográficamente, del paquete de datos o de varios paquetes de datos,

III. encriptación de al menos una estructura de datos de transmisión con una clave de la segunda unidad de comunicaciones,

IV. transmisión de al menos una estructura de datos de transmisión encriptada a la segunda unidad de comunicaciones en la segunda red,

V. desencriptado de al menos una estructura de transmisión encriptada,

VI. encriptación de los datos útiles que deben transmitirse a la segunda unidad de comunicaciones, con los parámetros criptográficos negociados, y transmisión de datos útiles encriptados a la segunda unidad de comunicaciones, y

VII. desencriptado de los datos útiles transmitidos con los parámetros criptográficos contenidos en la estructura de transmisión desencriptada.

2. Procedimiento según la reivindicación precedente, caracterizada porque una tercera unidad de comunicaciones (vSrV) se dispone aguas arriba de la unidad de comunicaciones unidireccional, que realiza las etapas II, III y IV de la reivindicación 1.

3. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque en la vía de transmisión de datos parcial entre la primera unidad de comunicaciones y la tercera unidad de comunicaciones, se utiliza el protocolo de transmisión de datos Datagram Transport Layer Security, abreviado DTLS.

4. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque otra unidad de comunicaciones (vSrv), dispuesta aguas arriba de la segunda unidad de comunicaciones, realiza la etapa V con la ayuda de los parámetros criptográficos desde la estructura de transmisión.

5. Procedimiento según una de las reivindicaciones precedentes, caracterizada porque al menos un parámetro criptográfico comprende una clave de sesión, un conjunto de cifrado, una firma y/o certificado.

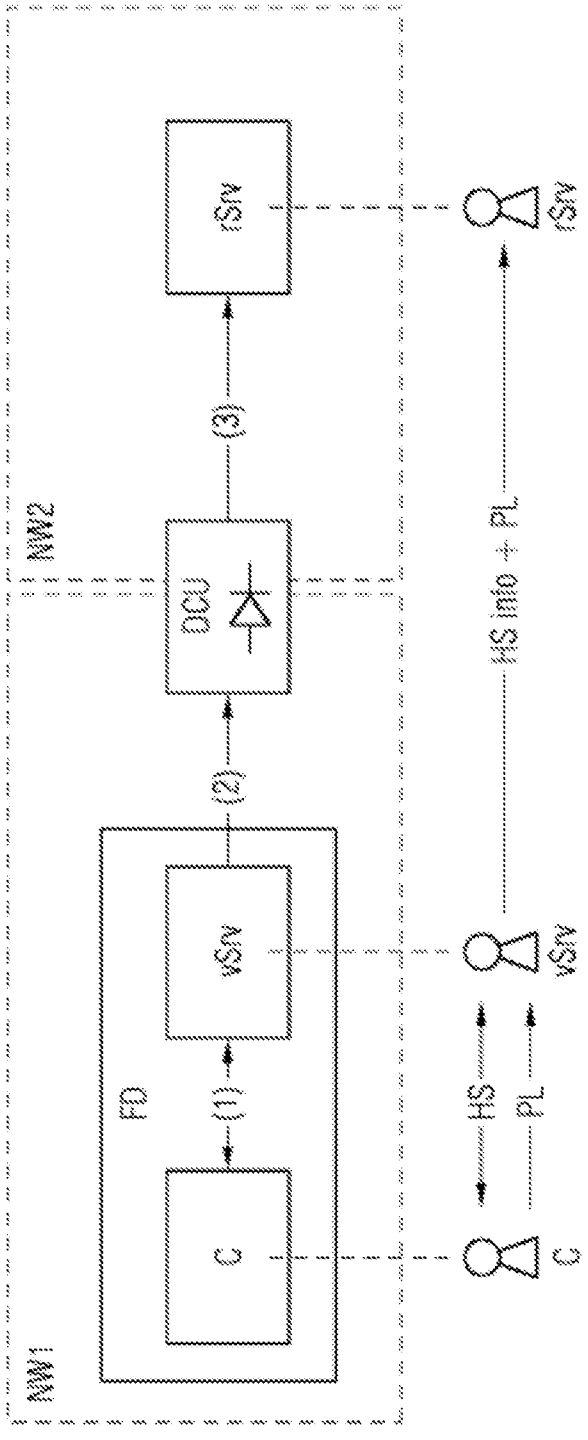
6. Procedimiento según una de las reivindicaciones precedentes, en el que el procedimiento está configurado implementado por ordenador.

7. Disposición para realizar el procedimiento según una de las reivindicaciones 1 a 6.

8. Producto de programa informático que puede cargarse directamente en un ordenador programable, que comprende partes de código de programa que son adecuadas para realizar las etapas del procedimiento implementado por ordenador según la reivindicación 6.

DIBUJOS

FIG 1



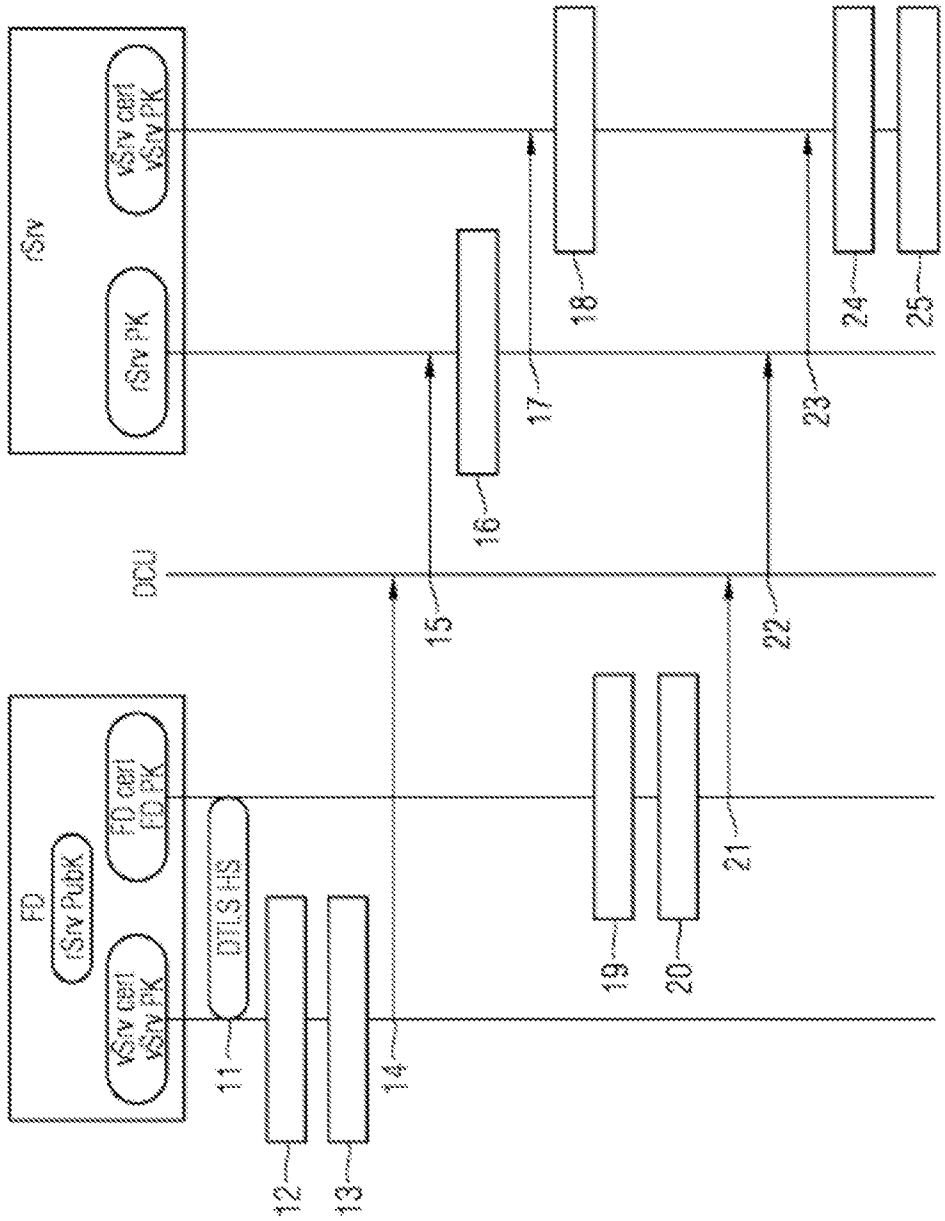

iSrv
iSrv cert
iSrv PK
iSrv PK
18
24
25
17
23
16
DCU
15
22
FD
iSrv PubK
FD cert
FD PK
iSrv cert
iSrv PK
TTLS LHS
21
19
20
11
14
12
13

FIG 2